



FACULTY OF  
COMPUTER SCIENCE

## **An effective security warning approach for malware attacks on mobile devices**

### **DISSERTATION**

zur Erlangung des akademischen Grades  
Doktoringenieurin (Dr.-Ing.)

angenommen durch die Fakultät für Informatik  
der Otto-von-Guericke-Universität Magdeburg

von Dipl.-Inform. Jana Fruth  
geboren am 21. März 1977 in Magdeburg

#### **Gutachter/Gutachterinnen:**

Prof. Dr. i. R. Edgar Nett, Otto-von-Guericke-Universität Magdeburg  
Prof. Dr. Jana Dittmann, Otto-von-Guericke-Universität Magdeburg  
Dr. Zinaida Benenson, Universität Erlangen-Nürnberg

Magdeburg, den 24. Oktober 2018

**Fruth, Jana:**

*An effective security warning approach for malware attacks on mobile devices*

PhD Thesis, Otto-von-Guericke-University  
Magdeburg, 2018.

# Abstract

Today, mobile devices are widely spread, because they offer lots of functions. However, these devices are also valuable targets of cyber-criminals, because they store huge amounts of personal data. One instrument of attackers to gather these data is malware. However, today mobile devices are also used in private environments for remote control of coupled systems, such as mobile robots. So malware on a mobile device could spread to a coupled system and cause malfunctions, which could potentially impact users' health.

This thesis focuses on scenarios, in which humans and technical systems are interacting with each other, so called human-machine-interaction (HMI) scenarios. Non-professional environments of HMI scenarios are researched, where lay users have full control over their system and interact with modern technical systems. In cases humans interact with technical systems it is to ensure that humans are not threatened by the technology. Beside security prevention and detection strategies, warnings are one option to help users to protect themselves against malware incidents. A challenge in this case are the considerable expertise and effort to use and configure technical systems. Lay users could often not use them offered design possibilities of the technical system, because of their nescience. In this thesis a warning approach is introduced, which is so designed, that lay users could understand the warning information and handle the instructions for technical design. That includes the clear separation of warnings in different views, simple texts for personal risks, personal consequences of a malware attack, and simple expressed instructions to minimise or prevent consequences of malware attacks, respectively.

Today, there exist no adequate user-centred malware warnings on mobile devices, because these applications focus the protection of the system not the user. Furthermore, the research field of security warnings is relatively new. Most warning research results are published after the year 2009 and often focus browser warnings (e.g. malware, SSL). This thesis want to fill this research gap by introducing a new effective malware warning approach.

The four research questions for this thesis are:

- How are current mobile malware warnings designed?
- Which personal consequences may malware attacks have to users of mobile devices?
- How does an effective malware warning concept to be designed to fulfil the needs of specific user-groups of mobile devices?
- How does an effective malware warning concept to be evaluated to measure the warning effectiveness?

To answer these questions the state-of-the-art of security warnings in general and malware warnings on mobile devices are intensively researched. Furthermore, a new warning approach is created, which adapts Wogalter's safety warning concept to raise warning effectiveness with user-group specific personal information. Users are warned about personal risks and personal consequences of malware attacks. Amongst personal information also instructions, an established education method, are included into the warnings. Instructions should support lay users to minimise or impede their personal consequences of malware attacks against mobile devices

and their coupled systems. Furthermore, multimodal feedback (visual, acoustic, haptic) is used to design different risk levels and the general warning information.

Amongst the new warning design concept also an own evaluation concept for the both tested warning instances is created. The two warning instances for user-groups (generic users and primary-school children) are evaluated using user studies to find indicators for their practical relevance. The evaluation concept in this thesis is based on state-of-the-art concepts for user-interfaces, which is adapted to specific test scenarios and test groups of malware warnings on mobile devices. Standard statistical analysis are used to find indicators for the practical relevance of evaluation results. The results of the introduced effective security warning approach are discussed using the human-in-the-loop security framework (HITL) of Cranor to rank the received results and show possibilities of improvements.

The evaluation results of the two warning test cases show tendencies, that partly the warning effectiveness can be increased using the new warning approach. Nevertheless, future studies are necessary to validate the generalisation of the evaluation results. Furthermore, this work shows future possible usage of the new warning concept.

## Deutschsprachige Version des Abstract

Heutzutage sind mobile Geräte weit verbreitet, da sie eine Vielzahl an Funktionen bieten. Aber diese Geräte sind auch lohnende Ziele für Cyberkriminelle, da sie große Datenmengen (z.B. personenbezogene Daten) speichern. Schadsoftware (Malware) ist ein Werkzeug für Angreifer an diese Daten zu gelangen. Nichtsdestotrotz, werden mobile Geräte auch in privaten Bereichen zum Beispiel für die Fernsteuerung von mit ihnen gekoppelten Geräten eingesetzt. Ein Beispiel sind mobile Roboter. So könnte sich Schadsoftware von einem mobilen Gerät auf das damit verbundene System ausbreiten und Fehlfunktionen verursachen, die potentiell der Gesundheit von Nutzern schaden könnte.

Diese wissenschaftliche Arbeit fokussiert Szenarien, in denen Menschen und technische Systeme miteinander interagieren, so genannte Mensch-Maschine-Interaktions-Szenarios (human-machine-interaction, HMI). Es werden nicht-professionelle Umgebungen von HMI-Szenarios untersucht, wo Laien die volle Kontrolle über ihr System haben und mit modernen technischen Systemen interagieren. In diesen Fällen der Mensch-Maschine-Interaktion ist sicherzustellen, dass Menschen nicht von der Technik gefährdet werden. Neben den Security-Präventions- und Detektionsstrategien sind Warnmeldungen eine Möglichkeit, dass Nutzer sich selbst gegen Malwarevorfälle schützen können. Eine Schwierigkeit ist hierbei, dass es oft mit erheblichen Sachverstand und Aufwand verbunden ist, technischen Systeme zu bedienen und einzustellen. Laien können daher oftmals aufgrund ihrer Unwissenheit die ihnen angebotenen Gestaltungsmöglichkeiten der Technik nicht nutzen. In dieser Arbeit wird daher ein Warnmeldungsansatz vorgestellt, der so gestaltet ist, das Laien-Nutzer ihn verstehen und die Anweisungen zur Technikgestaltung umsetzen können. Dazu gehören die klare Aufteilung der Warnmeldungen in verschiedene Sichten, mit einfachen Texten zu persönlichen Risiken, persönlichen Konsequenzen des Schadsoftwareangriffs bzw. einfach formulierten Instruktionen zur Verhinderung der Konsequenzen.

Derzeit existieren keine angemessenen nutzerzentrierten Malwarewarnmeldungen auf mobilen Geräten, da diese Anwendungen den Schutz des Systems und nicht der Nutzer fokussieren. Weiterhin ist das Forschungsfeld der Security-Warnmeldungen noch ziemlich jung. Die meisten Forschungsergebnisse wurden nach 2009 veröffentlicht und fokussieren oft Browser-Warnungen (z.B. Malware, SSL). Diese Arbeit möchte diese Forschungslücke füllen und stellt einen neuen effektiven Security-Warnmeldungsansatz vor.

Die vier Forschungsfragen dieser Arbeit sind:

- Wie sind aktuelle mobile Malwarewarnungen gestaltet?
- Welche persönlichen Konsequenzen könnten Malwareangriffe für Nutzer mobiler Geräte haben?
- Wie sollte ein effektives Malwarewarnungskonzept gestaltet werden, um die Bedürfnisse bestimmter Nutzergruppen mobiler Geräte zu erfüllen?
- Wie sollte ein effektives Malwarewarnungskonzept evaluiert werden, um die Warnmeldungseffizienz messen zu können?

Um diese Fragen zu beantworten, wurde der Stand der Technik der aktuellen Sicherheitswarnungen generell und der Malwarewarnungen auf mobilen Geräten intensiv erforscht. Weiterhin wurde ein neues Warnmeldungskonzept kreiert, welches Wogalter's Safety Warnmeldungsansatz adaptiert, um die Effektivität von Warnungen für nutzergruppen-spezifische persönliche Informationen zu erhöhen. Nutzer werden vor persönlichen Risiken und persönlichen Konsequenzen von Malwareangriffen gewarnt. Dabei werden neben den persönlichen Informationen auch Anweisungen, eine etablierte Lehrmethode, in den Warnungen verwendet. Diese sollen Nicht-Experten dabei unterstützen persönliche Konsequenzen von Malwareangriffen auf mobile Geräte und ihrer gekoppelten Systeme zu minimieren oder zu verhindern. Weiterhin, wird ein multimodales Feedback (visuell, akustisch, haptisch) verwendet, um verschiedene Risikostufen und Informationen in Warnungen darzustellen.

Ebenfalls wurde ein eigenes Evaluationskonzept für beide getesteten Warnungsmeldungsinstanzen kreiert. Die realisierten Warnmeldungen für beide Nutzergruppen (generischer Nutzer und Grundschulkinder) wurden mit Nutzerstudien evaluiert, um Hinweise für deren praktische Relevanz zu finden. Das Evaluationskonzept dieser Arbeit basiert auf Stand-der-Technik Konzepten für Nutzerschnittstellen. Diese wurden für die bestimmten Evaluationsszenarien und Testgruppen der Schadsoftwarewarnungen für mobile Geräte angepasst. Etablierte statistische Analysen wurden verwendet, um Hinweise für die praktische Relevanz der Evaluationsergebnisse zu finden. Die Ergebnisse der Evaluation werden anhand des human-in-the-loop security framework (HITL) von Cranor diskutiert, um die erreichten Ergebnisse zu bewerten und Verbesserungsmöglichkeiten aufzuzeigen.

Die Evaluierungsergebnisse der zwei getesteten Warnungsmeldungsinstanzen zeigen tendenziell, dass die Effektivität der Warnungen teilweise verbessert werden konnte. Allerdings sind zukünftig umfangreichere Studien nötig, um eine Generalisierung der Ergebnisse zu validieren. Weiterhin werden zukünftige Verwendungsmöglichkeiten des neuen Warnmeldungskonzepts aufgezeigt.

# Acknowledgements

This work was carried out during my time as a research assistant at the Faculty of Computer Science of the Otto-von-Guericke University Magdeburg. During the years 2008 till 2017 I was a member of three working groups of Prof. Dr.-Ing. Jana Dittmann (Multimedia and Security), Prof. Dr. Edgar Nett (Realtime Systems and Communication), and Prof. Dr. Mesut Güneş (Communication and Networked Systems). First of all, I thank Prof. Dittmann for giving me the chance to start my scientific work in the project ViERforES and her fruitful collaboration and feedback through the five years. This project was founded by the German Federal Ministry of Education and Research (BMBF) under contract number 01IM08003C. I would like to show my gratitude to the BMBF for funding my work. Furthermore, I thank Prof. Nett for the support and valuable feedback throughout the last years of my research and writing of this thesis. Also, I thank Prof. Güneş for the chance of finalisation of my thesis in his workgroup. Furthermore, I would like to thank Zina Benenson my external supervisor.

I am deeply grateful to all my colleagues and co-authors of my publications from the three workgroups for our joint work, plentiful discussions and valuable exchange. I especially thank Christian Krätzer for his fruitful hints and his motivation to finalise this work. Additionally, I thank Michael Knuth and Sven Kuhlmann for their help with statistics.

Furthermore, I would like to thank my students Wiebke Menzel, Marcus Wulfänger, Tony Gieseler, Christoph Neubüser, and Fred Samland for their participation in the form of bachelor and master theses.

I also thank dear friends, such as Jane, Manuela, Kristin and the MeCoSa team. I especially thank the trio, Frank, Marian and Kai, who create just for me such a nice smart doctoral cap.

Zum Schluss möchte ich meiner Familie danken: Besonders danken möchte ich meinem Mann für seine Geduld mit mir und für seine jahrelange Unterstützung für mein Promotionsprojekt. Ich danke weiterhin meiner Mutter und meinem Vater für die Betreuung meiner Kinder, besonders in der heißen Phase der Promotion. Nicht zuletzt möchte ich meine beiden Mädels grüßen. Falls ihr solch oder ein ähnliches Projekt vorhabt, so unterstütze ich euch gern dabei. Jetzt aber freue ich mich auf die Abende und Wochenenden mit euch :)



<b>1</b>	<b>Introduction and Motivation</b>	<b>1</b>
1.1	Exemplary application scenarios of the research field . . . . .	4
1.2	Research questions . . . . .	6
1.3	Research objectives . . . . .	7
1.4	Main contributions . . . . .	9
1.4.1	Contributions to ROs . . . . .	9
1.4.2	Contributions to RQs . . . . .	14
1.5	Thesis outline . . . . .	22
<b>2</b>	<b>Thesis Fundamentals</b>	<b>25</b>
2.1	Mobile devices and examples of coupled systems . . . . .	25
2.2	Security and Safety . . . . .	28
2.3	Mobile malware . . . . .	30
2.3.1	Mobile malware attack vectors . . . . .	30
2.3.2	Mobile malware classification . . . . .	31
2.3.3	Mobile malware defence strategies . . . . .	35
2.4	Human information processing of warnings . . . . .	37
2.5	Effective warnings . . . . .	44
2.5.1	Security warning types . . . . .	45
2.5.2	Design guidelines for effective active security warnings . . . . .	47
2.5.3	User-groups . . . . .	49
2.6	Evaluation of security warning effectiveness . . . . .	52
2.6.1	Terms and Definitions . . . . .	52
2.6.2	User studies . . . . .	53
2.6.3	Evaluation methods and metrics to measure warning effectiveness . . . . .	56
2.6.4	Children specific user tests . . . . .	61
2.7	Statistical analysis methods . . . . .	65
<b>3</b>	<b>Related Work</b>	<b>67</b>
3.1	Why users ignore warnings . . . . .	69
3.1.1	Human-information processing . . . . .	70
3.1.2	Invalid user studies . . . . .	82
3.2	Malware warning approaches . . . . .	83
3.3	Other relevant related work . . . . .	86
<b>4</b>	<b>Methodology and Concept</b>	<b>89</b>
4.1	Malware warning design study of current mobile Android security apps . . . . .	91
4.2	Personal risks of mobile malware attacks . . . . .	96
4.3	General warning design concept . . . . .	104
4.3.1	User-group specific warning design . . . . .	106
4.3.2	Adaption to mobile device characteristics . . . . .	106
4.3.3	Effective warning design . . . . .	107
4.3.4	Multimodal feedback . . . . .	107
4.3.5	Generic warning layout . . . . .	110
4.3.6	Generic warning design for primary-school children . . . . .	113
4.4	Evaluation methodology and concept . . . . .	115

## CONTENTS

---

4.4.1	Generic design of both test cases . . . . .	115
4.4.2	General evaluation methods and test metrics . . . . .	120
4.4.3	Evaluation concept . . . . .	121
<b>5</b>	<b>Realisation of test cases</b>	<b>127</b>
5.1	Generic user - Mobile robot warnings . . . . .	127
5.1.1	Security Warnings . . . . .	128
5.1.2	Test program . . . . .	135
5.1.3	User study . . . . .	138
5.2	Children - Smartphone warnings . . . . .	141
5.2.1	Security Warnings . . . . .	141
5.2.2	Test Program . . . . .	150
5.2.3	User study . . . . .	153
<b>6</b>	<b>General Results and Discussion</b>	<b>157</b>
6.1	Generic user - Mobile robot warnings . . . . .	157
6.1.1	Descriptive analysis . . . . .	158
6.1.2	Inference statistical analysis and Discussion . . . . .	166
6.1.3	Quality criteria and Limitations . . . . .	179
6.2	Children - Smartphone warnings . . . . .	180
6.2.1	Descriptive analysis . . . . .	180
6.2.2	Interference statistical analysis and discussion . . . . .	186
6.2.3	Quality criteria and Limitations . . . . .	190
6.3	Discussion with HITL framework . . . . .	191
<b>7</b>	<b>Summary, conclusions, related and future work</b>	<b>197</b>
7.1	Summary and conclusions . . . . .	197
7.2	Selected topics of own related research work . . . . .	198
7.3	Possible directions for future work . . . . .	204
7.3.1	Future improvements . . . . .	204
7.3.2	Future research . . . . .	206
<b>8</b>	<b>Appendix</b>	<b>209</b>
8.1	Adults - Mobile robot warnings . . . . .	210
8.1.1	Application scenarios . . . . .	210
8.1.2	Questionnaire . . . . .	212
8.1.3	Original Questionnaire . . . . .	215
8.1.4	Structured observation protocol . . . . .	218
8.1.5	Results . . . . .	218
8.2	Children - Smartphone warnings . . . . .	223
8.2.1	Questionnaire . . . . .	223
8.2.2	Original Questionnaire . . . . .	225
8.2.3	Structured observation protocol . . . . .	234
<b>9</b>	<b>Bibliography</b>	<b>235</b>

---

## Abbreviations

<b>ASD</b>	adaptive security dialogs
<b>BSI</b>	German Federal Office of Information Security
<b>CARO</b>	Computer Antivirus Research Organization
<b>CG</b>	control group
<b>C-HIP</b>	Communication-Human Information Processing model
<b>CPS</b>	cyber-physical system
<b>(D)DOS</b>	(distributed) denial-of-service attack
<b>DiD</b>	Defence-in-Depth approach
<b>EG</b>	evaluation group
<b>EICAR</b>	European Institute for Computer Anti-Virus Research
<b>EQ</b>	evaluation question
<b>fMRI</b>	functional magnetic resonance imaging
<b>GEMS</b>	Generic Error-Modeling System
<b>H</b>	hypothesis
<b>HITL</b>	human-in-the-loop security framework
<b>HMI</b>	Human-Machine-Interaction
<b>HUD</b>	head-up displays
<b>ICS</b>	industrial control systems
<b>IDS</b>	intrusion detection system
<b>MITM</b>	man-in-the-middle attack
<b>PUA</b>	potentially unwanted application
<b>RO</b>	research objective
<b>RQ</b>	research question
<b>VDE</b>	Association for Electrical, Electronic and Information Technologies
<b>VDI</b>	Association of German Engineers



# List of Figures

1.1	Main contributions of this thesis . . . . .	11
1.2	Outline of this thesis . . . . .	23
2.1	Generic structure of a mobile device . . . . .	25
2.2	Human information processing in human-in-the-loop framework . . . . .	38
2.3	Human threat identification and mitigation process . . . . .	43
2.4	Warning design recommendation of Bauer et al. . . . .	49
2.5	Unipolar and bipolar scales in continuous analogue and discrete rating scales . . . . .	59
2.6	Example of an asymmetric response scale . . . . .	59
3.1	Related work field regarding 'Warning ignoring' and solution approaches . . . . .	69
3.2	Related work field for 'Warning impediments' . . . . .	70
3.3	Related work field for 'User's characteristics' . . . . .	71
3.4	Related work field for 'Warning processing' . . . . .	75
3.5	Related work field for 'Behaviour' . . . . .	81
4.1	Methodology of this thesis . . . . .	90
4.2	Screenshot of McAfee . . . . .	95
4.3	Screenshot of Cheetah guide . . . . .	95
4.4	Screenshot of Cheetah guidance information . . . . .	95
4.5	Screenshot of Psafe guidance information . . . . .	95
4.6	Overview of the personal risk model . . . . .	96
4.7	Major components of the warning design concept published in this thesis . . . . .	105
4.8	Generic warning design layout . . . . .	112
4.9	Example of different warning views . . . . .	112
4.10	Test cases of two instances of the generic warning approach in this thesis . . . . .	116
5.1	UML activity diagram for warning 1 for both test groups . . . . .	131
5.2	Risk level 'low': Warning 2 . . . . .	131
5.3	Risk level 'high': Warning 9 . . . . .	131
5.4	Mobile robot platform SCITOS G5 from MetraLabs . . . . .	135
5.5	Communication of drive command data between main prototype components . . . . .	136
5.6	GUI screenshot of remote control via tablet . . . . .	137
5.7	Warning display and generation of logfile information . . . . .	138
5.8	Exemplary excerpt from a logfile for a member of evaluation group . . . . .	138
5.9	Test environment of the mobile robot warnings prototype . . . . .	139
5.10	Screenshot of test environment on GUI of tablet . . . . .	139
5.11	UML activity diagram for display of warnings . . . . .	140
5.12	Warning 1: Update check with positive result . . . . .	145
5.13	Warning 2: Update virus check with negative result . . . . .	145
5.14	Warning 3: Attack via Bluetooth . . . . .	146
5.15	Warning 4: Sending a virus infected file to smartphone . . . . .	146
5.16	Warning 5: Smartphone is virus infected . . . . .	147
5.17	Warning 6: Current app is virus infected . . . . .	147
5.18	'Why?' view of warning 1 . . . . .	148
5.19	Game menu . . . . .	151
5.20	Game . . . . .	151

## LIST OF FIGURES

---

5.21	Installed update 'Sesamstreet'	151
5.22	Control program after start	152
5.23	Optional warning: activated and highlighted with red text	152
5.24	Information for the assistant	152
5.25	Excerpt of logfile	153
5.26	Test environment of the smartphone warnings prototype	154
6.1	Responsible groups with a (very) strong involvement in malware distribution	159
6.2	Responsible user activities with a (very) strong support of malware distribution	160
6.3	'Very dangerous' risk level ratings for all warnings	162
6.4	'Very dangerous' risk level ratings for risk level 3 warnings	163
6.5	'Very dangerous' risk level ratings for risk level 2 warnings	163
6.6	'Dangerous' risk level ratings for risk level 2 warnings	164
6.7	'Very comprehensible' rating of all warnings	165
6.8	Average clicking times in risk and consequences warning view	166
6.9	Correlation of average 'usefulness' and support by a step-by-step instruction	167
6.10	Correlation of average 'usefulness' and support by a technical-savvy friend	168
6.11	Correlation of average 'usefulness' and support by a technical expert	168
6.12	Correlation of average 'usefulness' and support by a user guide	169
6.13	Correlation of group and support by a technical expert	170
6.14	Correlation of average 'usefulness' and age	172
6.15	Correlation of average 'comprehension' and support by a technical expert	174
6.16	Correlation of average 'decision' and average 'risk level'	175
6.17	Correlation of average 'decision' and 'concern'	176
6.18	Correlation of average 'decision' and support by a technical expert	177
6.19	Correlation of 'victim of malware' and 'buy an IoT device in the near future'	178
6.20	Reactions according to observations	182
6.21	Warning comprehension	182
6.22	Frequency of 'Why?' button use	183
6.23	Identification of risk levels by colours	183
6.24	Remembered colours of cartoon character	184
6.25	Influence of timely order on warning reading	185
6.26	Frequency of 'Why?' button use	186
6.27	Frequency of display of warning 5 and 6	189
7.1	Potential implications of a Conficker worm infection to an industrial robot	199
7.2	Exemplary warning for threat level 'low'	201
7.3	Exemplary warning for threat level 'high'	201
8.1	Application scenarios for test of test case 1 (scenario 1-3d)	210
8.2	Application scenarios for test of test case 1 (scenario 3e-5)	211
8.3	Translated questionnaire for test case 1 (EQ1-2)	212
8.4	Translated questionnaire for test case 1 (EQ3-4)	213
8.5	Translated questionnaire for test case 1 (EQ4-6)	214
8.6	Original questionnaire for test case 1 (page 1/3)	215
8.7	Original questionnaire for test case 1 (page 2/3)	216
8.8	Original questionnaire for test case 1 (page 3/3)	217
8.9	Structured observation protocol for test case 1	218

8.10 Rating results of risk level of warning 5 . . . . . 218

8.11 Translated questionnaire for test case 2 (EQ1,2,4) . . . . . 223

8.12 Translated questionnaire for test case 2 (EQ1,2,4,5) . . . . . 224

8.13 Original questionnaire for test case 2 (page 1/9) . . . . . 225

8.14 Original questionnaire for test case 2 (page 2/9) . . . . . 226

8.15 Original questionnaire for test case 2 (page 3/9) . . . . . 227

8.16 Original questionnaire for test case 2 (page 4/9) . . . . . 228

8.17 Original questionnaire for test case 2 (page 5/9) . . . . . 229

8.18 Original questionnaire for test case 2 (page 6/9) . . . . . 230

8.19 Original questionnaire for test case 2 (page 7/9) . . . . . 231

8.20 Original questionnaire for test case 2 (page 8/9) . . . . . 232

8.21 Original questionnaire for test case 2 (page 9/9) . . . . . 233

8.22 Structured observation protocol for test case 2 . . . . . 234



# List of Tables

2.1	Main classes and main characteristics of mobile malware . . . . .	32
2.2	Cases of behaviour . . . . .	41
2.3	Main user characteristics for usability evaluations . . . . .	50
3.1	Comparison of related work against characteristics of the new warning approach	68
4.1	Study results for current mobile security Android apps with malware detection .	92
4.2	Generic translation of examples of malware activities on mobile devices (first level impacts) to personal risks of mobile device users . . . . .	101
4.3	Generic translation of malware activity example on coupled systems of mobile devices to personal risks of mobile device users . . . . .	103
4.4	General logical multimodal feedback design for a generic user . . . . .	108
4.5	Definition of risk levels on basis of violation of personal requirements of the generic user . . . . .	109
4.6	Included and adapted parts of warning design guidelines of Bauer et al. . . . .	110
4.7	General logical multimodal feedback design for user-group children . . . . .	115
4.8	Hypothesis of both test cases . . . . .	119
4.9	Evaluation methods for qualitative and quantitative factors . . . . .	121
4.10	Evaluation environment and methods for test case 1 . . . . .	122
4.11	Relation of dependent variables to specific evaluation questions for test case 1 .	123
4.12	Evaluation environment and methods for test case 2 . . . . .	125
4.13	Relation of dependent variables to specific evaluation questions for test case 2 .	126
5.1	Specific logical design of risk levels for test case 1 . . . . .	129
5.2	Logical warning design for test case 1 . . . . .	130
5.3	Risk-Consequences-Instruction matrix for test case 1 . . . . .	134
5.4	Specific logical design of risk levels for test case 2 . . . . .	143
5.5	Event matrix for test case 2 . . . . .	149
6.1	Warning comprehension according to three parameters . . . . .	187
6.2	Results of both warning test cases evaluated with HITL framework . . . . .	194
8.1	Risk level ratings for warnings with RL1 . . . . .	219
8.2	Risk level ratings for warnings with RL2 . . . . .	219
8.3	Risk level ratings for warnings with RL3 . . . . .	220
8.4	Comprehension ratings for warnings with RL1 . . . . .	220
8.5	Comprehension ratings for warnings with RL2 . . . . .	221
8.6	Comprehension ratings for warnings with RL3 . . . . .	221
8.7	Two-sided correlation results according to Pearson for decision vs. reaction (EG)	221
8.8	Two-sided correlation results according to Pearson . . . . .	222
8.9	Strong and middle effects after Cohen's d analysis . . . . .	222



# 1

## Introduction and Motivation

Today, mobile devices, such as tablets<sup>1</sup> and smartphones make our daily life more comfortable. We use them mainly for communication, like phoning, e-mailing, chatting, sharing personal information in social networks, and online shopping. However mobile devices could also be used as remote controls for various systems, which are coupled with them. Examples for private usage are the remote control of navigation systems in cars<sup>2</sup>, flying robots<sup>3</sup>, and domestic mobile robots<sup>4</sup>. Nevertheless, amongst remotely controlled systems also autonomous systems, which initially do not need user interaction, are sometimes also remotely controlled with mobile devices [MN99, NS03]. Examples are mobile robots. In cases where safety functionality could not be guaranteed autonomous robot control is given up. So the control falls back into the hand of human users, to handle an acute problem.

However mobile devices are also valuable targets of cyber-criminals, because they are widely spread<sup>5</sup>, provide increased contact to the outside world through wireless technologies<sup>6</sup> and they store huge amounts of personal data. Cyber-criminals often use malware<sup>7</sup> to realise their aims. Examples are spying and theft of users login credentials for selling or realising online-banking frauds. The amount of malware, especially for smartphones, has increased through the years. In the year 2016 nearly 3,600 new mobile malware variants for Android were detected by anti-virus application developers [Sym17]. Mostly these attacks against mobile devices are related to users' privacy<sup>8 9</sup>, and financial aspects.

Nevertheless, also safety aspects have to be considered. In cases where malware spreads from the mobile device to a remotely controlled system, such as a mobile *cyber-physical system* (CPS). In the literature these attacks are called *cyber-physical attacks* [Lou15]. Those intentional manipulations of technical systems in cyberspace (security) could lead to malfunctions of

---

<sup>1</sup>In this thesis the term 'tablet' is used instead of 'tablet computer'.

<sup>2</sup>Android Headlines, Alexander Maxham, 'Featured Review: 2017 Audi Q7 And Android Auto', <http://www.androidheadlines.com/2016/03/featured-review-2017-audi-q7-and-android-auto.html>, accessed: 16.03.18

<sup>3</sup>Parrot, <https://www.parrot.com/global/drones/parrot-ardrone-20-elite-edition#parrot-ardrone-20-elite-edition>, accessed: 03.11.18

<sup>4</sup>iRobot, <http://www.irobot.co.uk/>, accessed: 16.03.18

<sup>5</sup>Gartner, 'Gartner Says Worldwide Sales of Smartphones Recorded First Ever Decline During the Fourth Quarter of 2017', <https://www.gartner.com/newsroom/id/3859963>, accessed: 16.03.18

<sup>6</sup>Alisa Shevchenko, 'An Overview of Mobile Device Security', 2005, <https://securelist.com/an-overview-of-mobile-device-security/36059/>, accessed: 16.03.18

<sup>7</sup>In this thesis the term 'malware' is related to the term 'malicious codes' (see chapter 2.3).

<sup>8</sup>SecureWorld, Rebecca Herold, '10 Big Data Analytics Privacy Problems', <https://www.secureworldexpo.com/10-big-data-analytics-privacy-problems>, accessed: 16.03.18

<sup>9</sup>IBM Big Data and Analytics Hub, 'Engaging the insurance consumer', <http://www.ibmbigdatahub.com/blog/engaging-insurance-consumer>, accessed: 16.03.18

technical systems in physical space (safety) [HKD09, Lou15]. The main risks of cyber-physical attacks are functional failures of these systems, which potentially endanger its environment, e.g. the personal safety of humans [FN14]. The strong influence of devices, which are remotely connected to and control other systems, is illustrated by two examples. One first impressive example is the resolution case of theft of a BMW car, in which the thief is caught using remote tracking and remote locking of the car<sup>10</sup>. Another example is the remote control of a Chrysler Jeep over its vulnerable wireless entertainment interface<sup>11</sup>. Beside the adequate usage of remote functions, these functionality could also be used by cyber-criminals (e.g. by using malware) to do damage. Although these risks are proven to date only within academic studies, they may represent a real problem in the future. What is underlined by a statement of the CIO of the German Federal Office of Information Security (BSI)<sup>12</sup>, who warned of possible injuries or deaths caused by cyber-attacks against cars and airplanes.

This thesis focuses on scenarios, in which humans and technical systems are interacting with each other, so called human-machine-interaction (HMI) scenarios. Non-professional environments of HMI scenarios are researched, where lay users have full control over their system and interact with modern technical systems. In cases humans interact with technical systems it is to ensure that humans are not threatened by the technology. Beside security prevention and detection strategies, warnings are one option to help users to protect themselves against malware incidents, such as spying of private data and injuries by malfunction of coupled systems.

The aim of the approach in this thesis is not to remove the causes of system failures, such as malware. However the introduced warning approach symbolises a *first-aid-measure* to protect lay users in unprofessional environments from personal impacts of malware attacks, before the cause of the failure or malfunction is eliminated. These warnings are no substitution for final recovery of a stable/secure system status, e.g. through malware removal. The main problem of the above described mobile devices and potentially coupled systems are their open design, which make them prone to cyber-attacks in general and malware attacks in particular [Lou15]. Because the security of these systems cannot ensured 100 percent, warnings are an additional measure to protect humans rapidly from intentional attacks (security) and caused unintended system failures (safety), which may impact users personally. This thesis focuses on malware attacks against mobile devices and their coupled systems as one example of cyber-attacks.

One main problem is the ignoring of security warnings by many users. The main reason for this problematic user behaviour are *habituation effects* caused by an overwhelming confrontation of users with security warnings in often threat-less situations. One generic solution is to raise warning effectiveness<sup>13</sup> (e.g. [WGF<sup>+</sup>87, Wog06b]). Specific solutions are the redesign of warnings, individual designed warnings or polymorphic warnings. There exist various approaches for individual warning designs (e.g. [BV13, DKYT<sup>+</sup>09]) and polymorphic warnings (e.g. [BVS07, JKB<sup>+</sup>18]). Because of individual requirements the effort to implement this

---

<sup>10</sup>The Washington Post, Karen Turner, 'BMW uses remote locking to trap car thief suspect inside stolen vehicle', <https://www.washingtonpost.com/news/the-switch/wp/2016/12/06/bmw-uses-remote-locking-to-trap-car-thief-suspect-inside-stolen-vehicle/>, accessed: 16.03.18

<sup>11</sup>Wired, Andy Greenberg, 'Hackers remotely kill a jeep on the highway with me in it', <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>, accessed: 16.03.18

<sup>12</sup>Welt, Manuel Bewarder, Florian Flade, Lars-Marten Nagel, 'BSI-Chef warnt vor Toten durch Hackerangriffe auf Autos', <http://www.welt.de/wirtschaft/article154677618/BSI-Chef-warnt-vor-Toten-durch-Hackerangriffe-auf-Autos.html>, Die Welt, accessed: 16.03.18

<sup>13</sup>In this thesis effectiveness of warnings is related to human information processing. Focus lies on comprehension, and behaviour/reaction of users of mobile devices.

---

warning type is very high. Therefore, contrary to these recommendations in this thesis a *user-group specific* approach is preferred to handle the trade-off between implementation effort and effective risk communication. In this thesis '*warning effectiveness*' is related to user's comprehension of warning contents and user's ability to find adequate solutions on basis of warning instructions, because non-expert users with full system control are focused. The new effective warning design approach adapts Wogalter's safety warning concept [Wog06b] to raise warning effectiveness with user-group specific personal information [KPV<sup>+</sup>12]. Users are warned about *personal risks* and *personal consequences* of malware attacks. Amongst personal information also *instructions* an established education method [SK14] are included into the warnings. Instructions should support lay users to minimise or impede their personal consequences of malware attacks against mobile devices and their coupled systems. Furthermore, multimodal feedback (visual, acoustic, haptic) is used to design different risk levels and the general warning information.

Amongst the warning design concept also an own evaluation concept for the both tested warning instances is created. The two warning instances for user-groups (generic users and primary-school children) are evaluated using user studies to find indicators for their practical relevance [PD10]. The evaluation concept in this thesis is based on state-of-the-art concepts for user-interfaces, which is adapted to specific test scenarios and test groups of malware warnings on mobile devices. Standard statistical analysis are used to find indicators of the practical relevance of evaluation results. The results of the evaluation of the introduced effective security warning approach are discussed using the human-in-the-loop security framework methodology of Cranor [Cra08] to rank the received results and show possibilities of improvements.

### **Overview of the following sections in chapter 1:**

*Section 1.1* describes the exemplary application scenarios of the research field of the thesis. *Section 1.2* introduces the research gaps addressed in this thesis labelled as 'research questions'. *Section 1.3* introduces research aims for this thesis labelled as 'research objectives' based on the research gaps of the previous section. Chapter 1 is finalised with the summary of the main contributions of this thesis in *section 1.4* and the thesis outline in *section 1.5*.

### 1.1 Exemplary application scenarios of the research field

---

In the following two scenarios are described, where the new warning approach could be used.

#### **Scenario 1: No timely handling of malware attacks**

This scenario could concern the timely realising of malware attack detection and reaction on mobile devices and coupled systems.

*Detection:* In some situations cyber-attacks, e.g. via malware, could not be detected timely. One reason could be a not updated signature data-basis of an anti-virus software. After an update the anti-virus application will detect an till then unknown malware, but the update takes time. Detection processes are often very resource consuming. In specific situations these detection processes are stopped, because the resources on the mobile device or coupled system are needed for other applications, e.g. navigation. This lack and the potential personal consequences have to be communicated to the user, that users could protect themselves.

*Reaction:* After a malware attack the system has to be recovered. An exemplary measure is the remove of malware from the system. But in some cases the timely recovery could not be realised, because it could cause malfunctions of the system. That are cases where malware has placed within safety or security relevant components or code. Exemplary safety relevant automotive components are motor and brake control elements (e.g. antilock braking system - ABS, speed control). Exemplary security relevant components are security applications, such as anti-virus applications. The remove of these malware infiltrated safety or security relevant components or code could have negative consequences for the security and safety of the whole system. In this cases where malware removing is not possible, the prevention of humans for negative consequences with warnings is one security measure. Tuchscheerer et al. published a first approach of malware warnings for cars [TDHK10]. It is a challenging task to design warnings for moving vehicles, which inform drivers, but do not disturb them from driving and do not cause accidents. If mobile devices are coupled with cars, these warnings could also be displayed on mobile device's display.

#### **Scenario 2: Transparent applications**

Transparency is one design criteria of applications for *general services* and especially if these services concern privacy aspects<sup>14</sup>. Warnings are one possibility to make processes transparent to the user. One example is asking users for their agreement to install new updates, if the user has full system control and therefore the update mechanism is not automatised. In this case warnings are important, because an update could change system settings, which could introduce new security vulnerabilities into the system [BFS+18].

Transparency is also important in *privacy*-related processes on technical systems. In Europe the new European 'General Data Protection Regulation' [GDP16] encourages the rights of users. They have, for example, to be informed which personal data are processed for which purpose by which organisation or application. This could be realised with warnings.

---

<sup>14</sup>Disclaimer: The author of this thesis has no training to be a lawyer. She cited some laws and regulations in the best of her knowledge and on a perspective of a novice in this field.

## **1.1. Exemplary application scenarios of the research field**

---

Transparency is also important to ensure *non-repudiation*. Exemplary cases are failed recovery processes. Warnings could be used to make such failures transparent and to warn users for potential negative consequences of that failure. One example is the failure of an anti-virus program, which could not completely remove a specific malware from the system. This incident could cause various further malware attack scenarios. For example, the malware could steal the e-signature of the electronic identity card of a user to use it for further crime. The legitimate owner of the e-signature could only disclaim to committed a crime by prove the failure of the anti-virus program, which causes the identity theft. So warnings, which are displayed to users and logged by the system could be an evidence for these technical failures.

### 1.2 Research questions

---

The research questions addressed in this thesis are summarised by four research questions :

**RQ1: How are current mobile malware warnings designed?**

**RQ2: Which personal consequences may malware attacks have to users of mobile devices?**

**RQ3: How does an effective malware warning concept to be designed to fulfil the needs of specific user-groups of mobile devices?**

**RQ4: How does an effective malware warning concept to be evaluated to measure the warning effectiveness?**

There exist a few malware warning approaches for browsers (e.g. [BLCD<sup>+</sup>11, AFRC14, MA14, AF13, SBO15]), but no malware warning approach for mobile devices. But mobile devices are valuable targets for cyber-criminals. Malware attacks could threaten the privacy and also life and limb of users, if mobile devices are coupled with other mobile systems, such as cars or robots.

One possibility is to warn users of mobile devices for personal malware related consequences and give them instructions to solve malware related consequences. Currently, there exist no malware warning approach and no malware warnings on mobile devices, which are designed in that way, because these warnings focus the protection of the system not the user. Though specific differences and requirements of warnings on mobile devices in comparison to desktop computers have to take into account. One aspect is the small display size of mobile devices, which limits the display of warning information. Another aspect is the usage of mobile devices in different environments under different conditions (e.g. light, noise) in comparison to constant environmental conditions of static desktop computers. Therefore a multimodal feedback of warning information on mobile devices is important, that users notice the warning. The approach in this thesis want to fill the gap of the state-of-the-art.

### 1.3 Research objectives

---

In this section the research objectives (RO) of this thesis are introduced, which based on the research questions in chapter 1.2. Following five ROs are defined:

**Research objective 1 (RO1): Research of current malware warnings on mobile devices.**

In order to create the in RO3 destined approach, the design of malware warnings of current free Android security apps with malware detection are investigated. The study investigates whether selected free mobile Android security apps fulfil the design criteria of the new malware warning approach. Investigated criteria are using of multimodel design elements, coding of different threat scales, using additional malware / threat information, user guidance in general, handling instructions of countermeasures against the current threat, and suitability for user-group specific needs. The research on this objective is to answer the main question of research question (1): 'How are current mobile malware warnings designed?'. The research objective is answered in section 4.1.

**Research objective 2 (RO2): Research of personal consequences of malware attacks to users of mobile devices.**

In order to create the in RO3 destined approach, the direct and indirect personal risks of malware attacks to mobile device users are investigated. This also includes the analysis of security and safety influences and the stages of malware infection, malicious functions on the infected system, and distribution to other systems. The research on this objective is to answer the main question of research question (2): 'Which personal consequences may malware attacks have to users of mobile devices?'. The research objective is answered in section 4.2.

**Research objective 3 (RO3): Design of a general user-group specific effective malware warning concept for mobile devices.**

In order to create the destined approach, the state-of-the-art of effective warning methods and concepts has to be analysed. Additionally, the usage of parts of existing warning design approaches for the intended approach has to be discussed. The main research questions are: 'Which existing warning methods and concepts can be used for the destined approach? Which novel concepts and methods have to be created to fulfil the desired requirements of the intended approach?'. The research objective is answered in chapter 3.

The destined approach is designed for a generalised user, which could be adapted to specific user groups. The research on this objective is to answer the main question of research question (3): 'How does an effective malware warning concept to be designed to fulfil the needs of specific user-groups of mobile devices'. The research objective is answered in 4.3.

**Research objective 4 (RO4): Evaluation of the general user-group specific effective malware warning concept to measure the warning effectiveness.**

In order to measure the effectiveness of the new warning approach existing warning evaluation methodologies and concepts have to be analysed. The important questions are: 'Which evaluation methods could be used to measure the effectiveness of the realised warning examples? In which manner the evaluation methods have to be adapted for specific user groups (e.g. adults, primary school children) and for selected mobile devices (e.g. smartphone, tablet)?'. The research objective is answered in sections 2.6.3, 2.6.4 and 4.4.

## Chapter 1. Introduction and Motivation

---

The evaluation of an warning approach includes the test with users. The main question is: 'How should warnings for specific test cases be realised for specific user groups and application scenarios to fulfil the requirements of the generalised approach?'. The research objective is answered in chapter 5.

**Research objective 5 (RO5): Investigation how personal information and instructions in malware warnings on mobile devices influence user's comprehension of warnings and support of users' adequate reaction.**

In order to measure the influence of warning design decisions the evaluation results have to be analysed. The main questions are: 'How comprehensible are user-group specific security warnings for the target user group? How adequately the target user group react to the warnings?'. The research objective is answered in section 6.

Both research objectives RO4 and RO5 answer the main question of research question (4): 'How does an general user-group specific effective malware warning concept to be evaluated to measure the warning effectiveness?'.

## 1.4 Main contributions

---

The main contributions of this thesis are summarised in figure 1.1. Furthermore, the main contributions are discussed related to the research objectives (section 1.4.1) and research questions (section 1.4.2).

### 1.4.1 Contributions to research objectives

---

#### **Research objective 1 (RO1): Research of current malware warnings on mobile devices**

The effective security warning approach for mobile devices in this thesis is discussed on the example of malware attacks. Therefore, current free Android security apps with malware detection functions are analysed whether they fulfil the design criteria of the new warning approach (see section 4.1). Investigated criteria are the using of multimodel feedback elements, coding of different threat scales, using of additional malware / threat information, user guidance in general, instructions for countermeasures, and suitability for user-group specific needs. The study show main lacks of the investigated security apps regarding the investigated warning design criteria. All apps are designed for a standard user, and most apps are designed with visual elements, short risk information, less information about potential personal consequences, and short instructions. That is related to the functionality of these apps, which focus on the protection of the system, not the user. They automatically detect malware on mobile devices, give users a short feedback of the result of a malware search, and offers users options to ignore or remove the malware. Current malware warnings on mobile devices are not designed for application scenarios, where users remotely control other coupled systems (e.g. IoT systems) with the mobile device and therefore users may be threatened by other risks, e.g. violation of personal safety. This thesis introduce a warning design which focus on such application scenarios and specific user-groups.

#### **Research objective 2 (RO2): Research of personal consequences of malware attacks to users of mobile devices**

The warning approach in this thesis based on a so called *personal risk model*, which describes exemplary the direct and indirect personal risks of malware attacks to mobile device users (see section 4.2). This personal risk model based on two models, an own metadata model for a secure data-management on embedded systems [FDOF10] and a classification model of mobile malware activities by Becher [Bec09]. The *metadata model* is based on different submodels, examples are models for components, data on components, security and safety requirements per component and data. The personal risk model adapts and uses these submodels to describe personal risk of users of malware infected mobile devices and their coupled systems.

On basis of *Becher's mobile malware impacts* an own description of so called *personal user requirements* is created. Personal user requirements are requirements of a mobile device user which are related to her person. The model distinguishes two cases, direct and indirect personal user requirements. *Direct personal requirements* are mobile device user requirements which are directly related to users health or life, e.g. protection of user's privacy or her personal safety. *Indirect personal requirements* are indirectly related to users life, e.g. protection of user's finances and private environment ('environmental safety').

## Chapter 1. Introduction and Motivation

---

The model distinguishes between two application scenarios: first, the *single usage of a mobile device*, and second, the *remote control* of a coupled system by a mobile device. Therefore, in the personal risk model three main impact scenarios of malware attacks are classified. In the *first impact scenario*, malware attacks against a single mobile device are focused. They are referred to as '*first level impacts*', because the mobile device is the first target of the malware attack. The *second impact scenario* describes malware attack impacts, which have their seeds in a malware infection of a mobile device which is coupled with another system for remote control. They are referred to as '*second level impacts*'. The malware on the mobile device could spread to the coupled system, which could have manifold impacts to the system security and safety as well as to mobile device user's requirements. The malware infected coupled system could also be spread malware to other coupled systems. These impact scenarios are referred to as '*third level impacts*'.

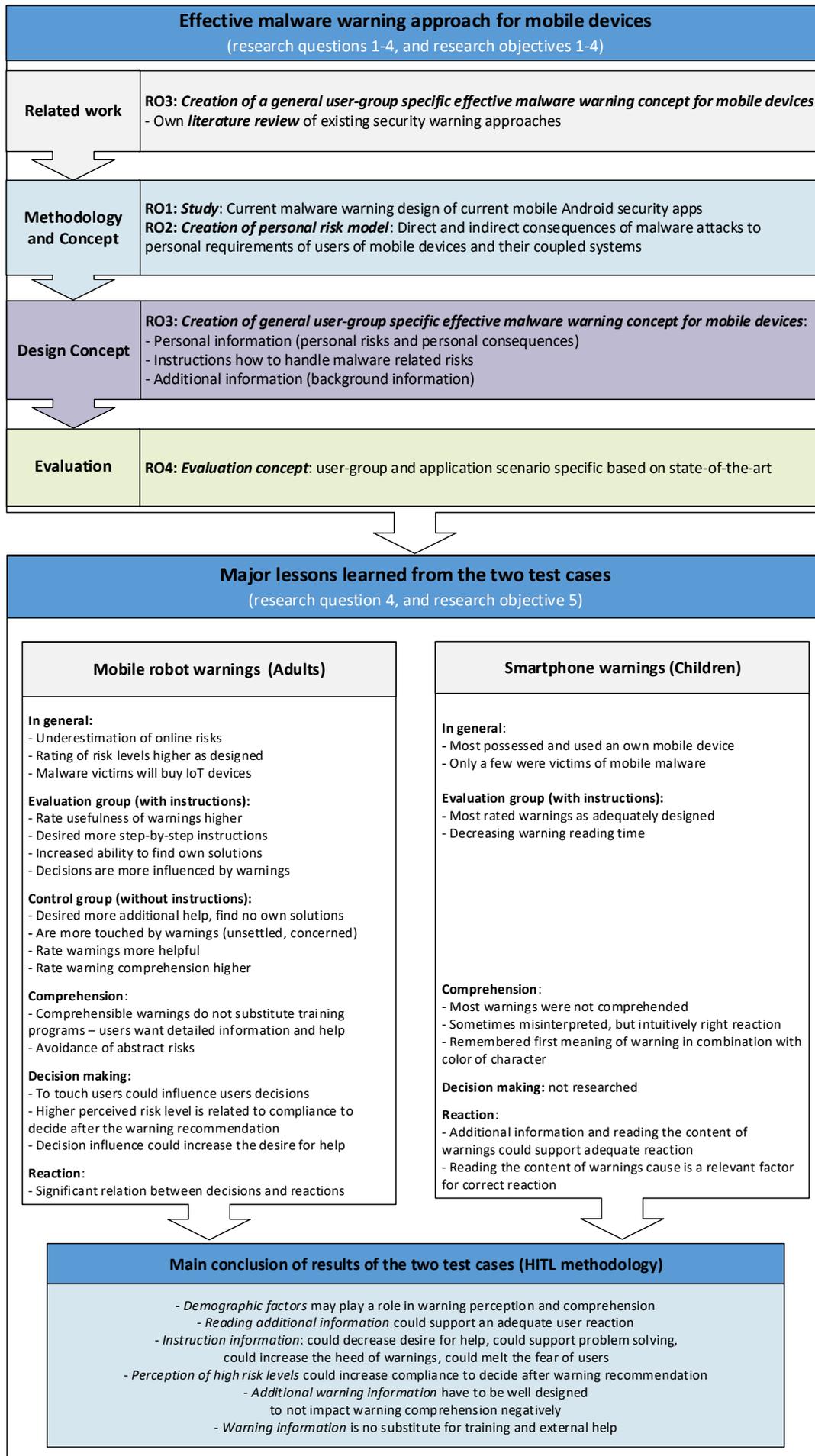


Figure 1.1: Main contributions of this thesis

### **Research objective 3 (RO3): Design of a general user-group specific effective malware warning concept for mobile devices.**

This research objective involves two parts, the review of the *related work* and creation of an own *warning concept*. Due to the lack of an existing **literature review** an own research of existing warning approaches is realised in common scientific databases (chapter 3). The found articles are filtered whether their content is related to the research topic of this thesis, ordered to phases of human-warning-processing based on Cranor's HITL framework [Cra08] and categorised in three different classes (reasons why users ignore warnings, malware warning approaches, other relevant research work). Furthermore, the selected warning approaches are compared against characteristics of the new warning approach.

The **new warning approach** is determined by two main aspects, *user-group specific* characteristics and *mobile device specific* characteristics. These both aspects also influence the both other elements of the warning approach, the *effective* warning design and the usage of *multimodal feedback* information (see section 4.3).

This thesis focused on a **user-group specific** warning approach to handle the trade-off between implementation effort and effective risk communication. It is assumed, that the user is a non-expert and the user controls the system. So the user has to be informed by the system about all system changes. The new warning approach based on a **generic user as standard case** (adult with standard literacy, no mental and physical handicaps, and familiar with the European culture, e.g. European colour coding). On basis of the definition of the generic user other user-groups could be modelled by individual or class-specific variations and extensions of the standard case. One example for a *class-specific variation* are the user-group of children, which differ in multiple user characteristics (e.g. literacy and mental development) to the generic user class.

The warning design is also determined by **mobile device specific** characteristics for warning representation. Mainly responsible is the limited user-interface and mobile device configurations, which limit the usage of multimodal feedback information in warnings.

The new warning approach based on recommendations of safety and security warning literature to raise warning **effectiveness**. Wogalter's [Wog06b] design criteria for static safety warnings are adapted to active malware warnings on mobile devices. Instead of warn users about system-based risks, consequences, and give them instructions users are warned for *personal impacts* of malware attacks against mobile devices and coupled systems (e.g. [KPV<sup>+</sup>12, HHWS14, MMHE17]). That are *personal risks* and *personal consequences* to users of mobile devices if malware attacks occur. Furthermore, also **instructions** are included into the warnings to give non-expert users a support to minimise or impede their personal consequences of malware attacks against mobile devices and their coupled systems.

Following recommendations for human-machine interaction scenarios from industrial usability standards and guidelines (e.g. [VDI00, WHW09, KNB<sup>+</sup>09]) **multimodal feedback** are used. The main aim is to attract users attention to warnings and to ease the warning comprehension. That means warnings are designed as a combination of sensory information using visual, acoustic, and haptic information, called 'logical design'. The general logical design is determined by a *threat scale* and the *information design*.

A *threat scale* is used to differentiate specific *risk levels* by their combination of visual, acoustic and haptic design criteria to warn users for specific personal risks and potential consequences of the current malware attack. The definition of risk levels is inspired by the protection requirement categories of BSI [BSI08] and adapted to damage scenarios of users related to their *personal requirements* (section 4.2). Only three risk levels are used to simplify the risk communication with non-expert users:

Amongst the realisation of the threat scale also the warning information itself based on visual and acoustic information. The *information design* based on recommendations of warning research regarding design of texts, usage of symbols/icons and combinations of text and icons.

The above described four requirements determine the **generic warning layout**. The warning layout recommendations of Bauer et al. [BBLCF13] are adapted to be useful for the requirements of the new warning approach for the generic user. On basis of this generic warning layout the generic warning design approach for *primary-school children* as class-specific variation of the generic user is introduced and differences to the standard case are described (section 4.3.6).

### **Research objective 4 (RO4): Evaluation of the general user-group specific effective malware warning concept to measure the warning effectiveness.**

The *main research goal* of this thesis is to investigate the impact of a user-group specific warning design on users' warning comprehension and support users' adequate reaction. This research objective is realised in two different ways. At first, the theoretical aspects of a warning evaluation are described in section 4.4.3 in form of an *evaluation concept* and second, the realisation of the two *warning instances* and their evaluation as *test cases* are introduced in chapter 5.

In the **theoretical part**, the general and specific *evaluation methods* and *test metrics* are defined to measure the influence of warning effectiveness of the both test cases. Thereby, qualitative and quantitative evaluation methods are differentiated. *Qualitative factors* are subjective values (e.g. test persons opinions and their behaviour), which are collected with questionnaires and expressed in a quantitative/numerical format. *Quantitative factors* are objective values, which measure for example user interaction with warnings and could be gained with logging methods and observations. Beside the theoretical description of the test case designs some test case specific *hypothesis*<sup>15</sup> are defined, and *study ethics* are described.

In the **practical part**, two specific user-group specific warning designs are created and realised on a specific mobile device and tested with a user-study. The application scenario of the first test case is a human-robot-interaction of adults (generic user) via tablet remote control in a domestic environment. The second test case simulates warnings in an interaction scenario of primary-school children with a smartphone.

---

<sup>15</sup>Note: In this thesis no classical hypothesis testing [BS10] is realised, because of the small samples of test persons. The author has some 'ideas/assumptions' over the evaluation results, which are named 'hypothesis'. These could be supported or not supported by the evaluation results.

**Research objective 5 (RO5): Investigation how personal information and instructions in malware warnings on mobile devices influence user's comprehension of warnings and support of users' adequate reaction.**

The generated data of the both user-studies of both warning instances are statistically analysed (see section 6). The main aim is to find indicators if warning effectiveness could be increased by the taken warning design decisions. That means in detail if the warning design has an influence on user's warning comprehension and if it supports users' adequate reaction. The statistical analysis of the results of both warning instances includes a *descriptive* and an *inference statistical* part inclusive discussion. Two different analysis types are used for the inference statistical analysis. The first analysis method, *Cohen's effect size d*, indicates how practical relevant are the test results. The second analysis method, the *correlation according to Pearson*, measures whether there is a linear dependency between two specific characteristics. On basis of the statistical analysis the results are *discussed* for both test cases regarding the test case specific hypothesis (see sections 6.1.2 and 6.2.2). Furthermore, the *quality criteria and limitations* of both test cases are described in sections 6.1.3 and 6.2.3.

### 1.4.2 Contributions to research questions

---

**Research question 1 (RQ1): How are current mobile malware warnings designed?**

Today, cheap IoT applications with less security protection measures getting more and more wide spread [Ang17]. With less security protections malware activities could have impacts to security of mobile systems as well as to their coupled systems (as well as private and industrial systems). Furthermore, cyber-physical attacks could have potentially safety impacts to coupled systems and users. So common warning design concepts of mobile security apps should be improved. This thesis focused on effective warning design after Wogalter using additional information for current risk, potential consequences, and instructions. Furthermore, current warning designs of mobile apps are not adapted to user-group specific properties, e.g. comprehension, reading ability, and scenarios of cyber-physical influences of malware. Additional information could be better used to inform users about personal consequences of malware attacks and to guide users better with instructions. The study of malware warnings of selected Android security apps in this thesis is a contribution to mobile malware warnings research.

**Research question 2 (RQ2): Which personal consequences may malware attacks have to users of mobile devices?**

Some researchers in the embedded system security field introduces models for **interrelations of security and safety**. Examples are the work by Hoppe et al. for automotive systems (e.g. [HKD09, HD14]), and an own work for embedded systems [NFHD11]. Hoppe et al. described direct influences of security attacks as *functional implications* of attacks, which are often intended influences of attacked systems. Malware attacks could also have indirect consequences, which were not intended by cyber-criminals. Hoppe et al. call them 'structural implications'. Regarding mobile devices these could be malfunctions of interconnected systems, such as person-related risks of users of mobile devices and remote-controlled robots or cars (privacy, life and limb). Loukas [Lou15] called them *cyber-physical attacks*. The introduced *personal risk model* in this thesis is a contribution to security-safety interrelation research. The model describes exemplarily the direct and indirect personal risks of malware attacks to mobile device users (see section 4.2). The personal risk model extended the security-safety interrelation models by a human-related view expressed by personal requirements of users.

### **Research question 3 (RQ3): How does an effective malware warning concept to be designed to fulfil the needs of specific user-groups of mobile devices?**

This research question leads to two research parts: first, the analysis of *state-of-the-art* of effective warning methods and concepts and second, the creation of specific *warning design concept*. Due to the lack of an existing **literature review** an own research of existing warning approaches is realised in chapter 3. To the best of the author's knowledge, this is the first comprehensive literature review for security warnings. Furthermore, it is investigated, which existing warning approaches could be used for the new warning approach and which novel concepts and methods have to be created.

There is no specific definition for 'warning effectiveness' in the security warning literature. Effectiveness of warnings in this thesis is defined by two characteristics: first, the user comprehends warning contents, and second, the user is able to find adequate solutions on basis of warning instructions. Therefore, the **new malware warning approach for mobile devices** is mainly designed with warning information for the current personal risks, consequences and instructions how to handle countermeasures based on safety, security warning research recommendations and an own personal risk model (see section 4.3). The main contribution of this new warning approach in this thesis is the extension of warning information with personal information and instructions. Some security warning researchers recommend the usage of individualised warnings (e.g. [DKYT<sup>+</sup>09, KPV<sup>+</sup>12, BV13, BV14]). Because of individual requirements the effort to implement this warning type is very high. Therefore, contrary to these recommendations in this thesis a *user-group specific* approach is preferred to handle the trade-off between implementation effort and effective risk communication. In this thesis 'warning effectiveness' is related to user's comprehension of warning contents and user's ability to find adequate solutions on basis of warning instructions, because non-expert users with full system control are in focus. Another feature of the warning approach is the usage of **multi-modal feedback** to attract users attention to warnings and to ease the warning comprehension based on recommendations from industrial usability (e.g. [VDI00, WHW09, KNB<sup>+</sup>09]). Another feature is the warning adaption to *mobile device characteristics*, such as display size and environmental influences (e.g. light, noise).

**Research question 4 (RQ4): How does an effective malware warning concept to be evaluated to measure the warning effectiveness?**

This research question is answered by two research parts: first, creation of an evaluation concept and second, the realisation of user studies to evaluate the both test cases including analysis of test results. The **evaluation concept** determines how warning effectiveness (comprehension, find adequate solutions) is measured. It is a contribution to the creation and realisation of a user-group specific evaluation concept for specific application scenarios.

The evaluation of the **warning instance on mobile robots for adult users** shows:

- *Usefulness*: Evaluation group members (EG) (participants with instructions) rate usefulness of warnings higher than the control group (CG) (participants without instructions), which supports hypothesis 1 (H1) and is supported by a strong Cohen's d effect size. Users in general (both test groups) who recognised warnings as 'little useful' and 'small useful' desired more external help. The inference statistical analysis supports that younger test persons (all participants were aged between 19 and 57 years) rated the warnings in general as 'little useful' in comparison to elder participants, who better rated the warning usefulness.
- *Desire for help*: It is *not* supported by the inference statistical analysis that EG members will be more likely to desire less external help than the CG (no support of hypothesis 2). Nevertheless, there are indicators that participants with instructions (EG) desire less external help than participants without instructions (CG). Furthermore, there are indicators that the instructions have to be improved. More EG members than CG members rated a 'step-by-step instruction' as 'very helpful'.
- *Touch of users' emotions*: In the test CG participants were more emotionally touched by the warnings than EG members. This could be an indicator that warnings with instructions could melt the fear of users of malware-related personal impacts, because they know what to do against it because they are instructed by the warnings.
- *Helpfulness*: More members of CG than EG members rated the warnings in general as '(very) helpful'. Potentially the complete warning design presented to the experimental group (including information about the risk, personal consequences, and instructions) is too complex.
- *Risk level*: Most participants rate the risk level of the warnings higher as designed. Furthermore, differences between design and interpretation of risk levels could be explained by priming effects and inaccurate warning design. These result indicate that the warnings has to be improved to communicate the right risk level to non-expert users. The interpretation of the both warning icons indicate a well designed icon for the highest risk level and a middle risk level icon, which has to be improved.
- *Comprehension*: It is *not* supported by the inference statistical analysis that EG members will be more likely to rate the comprehension of warnings higher than the CG (no support of hypothesis 3). CG members achieved better results than EG members, which is supported by a middle Cohen's d effect size. Nevertheless, warnings, which address personal risk directly are rated by both test groups as 'very comprehensible' (unauthorised sending of pictures or audio signals to the Internet). Interestingly, more CG members than EG members also rated all other warnings as 'very comprehensible'. This could be indicate that the presentation of risk and personal consequences in all warnings were well designed for CG members. The warnings in general include information about personal impacts of malware attacks. But in test case 1 only the comparison of warning with and without instructions are investigated. In future experiments state-of-the-art warnings have to be compared to the new warning approach to find indicators that personal risks seem to be a valuable warning approach according to the theory of De Keukelaere et al. and Kauer et al. [DKYT<sup>+</sup>09, KPV<sup>+</sup>12]. Nevertheless, comprehensible warnings should not substitute training programs. The study show, that test persons who rated

the warnings as 'very much comprehensible', wished external help. Test persons seem to be sensitised by the current warning about a specific dangerous situation, but do not understand the complex interrelations. So they want external help to clear the current threat situation.

- *Decision influence:* It is supported by the inference statistical analysis that EG members will be more likely to decide to heed the warning than the CG, which supports hypothesis 4 (H4) and is supported by a strong Cohen's d effect size. Warnings which touch users could influence their decisions. That is underlined by the comments of test persons, who said that their decisions were '(very) strongly influenced' by warnings, and at once they were concerned by these warnings. Additionally, the study shows that the higher users perceived the danger level, the rather they are compliant to decide after the warning. The touch of users' emotions seem to be a valuable approach for warning design, which confirmed the research results of [HPB09]. But the study also shows that if users are influenced in their decisions their desire for external help could increase. This could be interpreted that users understand the importance to decide after warning recommendation, but they wish external help to understand the complex relations of the warning.
- *Reaction influence:* There are a statistically significant relation between decisions and reactions of users related to warning messages. That could be an indicator for well designed warnings, but also for a normal user-warning interaction, which based on short-time decisions and reactions.
- *Future of IoT:* The inference statistical analysis shows, that most participants, which were victims of a malware attack said that they will buy an IoT device in the near future. This indicates that the participants were not well sensitised for potential cyber-attacks against such cheap-produced and simple to attack devices.
- *Knowledge:* Both test groups agreed that cyber-criminals are a very strongly involved user-group for malware distribution, but they disagree for the group 'user'. Most CG members (than the half of EG members) thought that users are very strongly involved in distributing malware. This correlates with the information in the annual report of the BSI to information security in Germany 2016 [BSI17], that most malware is installed with help of users. Most users of both test groups have an adequate awareness for specific user activities which are responsible to distribute malware (e.g. 'download of files' and 'open email attachments'). Nevertheless, participants underestimated user actions such as 'surf the Internet', 'click on links in social media' and 'forwarding in social media'. Here users need more education to raise their awareness to cyber-threats in the Internet.

The evaluation of the **warning instance on smartphones for primary-school children** shows:

- *Previous experiences and knowledge:* Most participants possessed and used an own mobile device or used their parents' computers, laptops or mobile phones. Only a few children were victims of computer viruses or mobile device viruses. Nevertheless, half of the children answered in the questionnaire to know about the existence of such malware. The answers were surprising, because some warnings about viruses were not comprehended by the children.
- *Comprehension of warnings:* The warning comprehension based on three parameters: adequate and inadequate reaction to the warning (protocol and logfile), childrens' warning interpretation (questionnaire), and the 'Why?' button usage (logfile). Analysing the three parameters it is assumed, that most warnings were not comprehended by the children. Conspicuous is the *discrepancy between the warning interpretation and reaction to warnings*. On the one side, one warning ('infected update installation') is adequately interpreted by participants, but children reacted inadequately. On the other side, two warnings ('Bluetooth attack', 'infected file') were misinterpreted, but children react to them intuitively in the right way. Furthermore, two warnings have no results of the think aloud protocols, which made the comprehension interpretation difficult. In the future the design of these warnings has to be improved to increase the warning comprehension of children.
- *Warning design:* In general the results of the questionnaire showed that the children rated the warnings and the comic character as adequately designed. Nevertheless, foreign and technical terms should be avoided. Furthermore, the usage of vibrations have to be weigh up, because children could be frightened. Although, most children remembered only the red coloured cartoon character the children *remembered the first meaning of a warning in combination with the colour of character*. This result could be used in further warning realisations, so different characters could be used for different warning messages with different risk levels. An idea for improvement could be the personalisation of the character by giving it a name.
- *Influence of time and order of showing warnings to reaction:* The analysis of the log files of the warning display time span and the written observation protocol showed a decreasing reading time during the test. This is an indication for habituation effects, which are normal reactions, when the human brain is confronted with similar stimuli, such as warnings [AVK<sup>+</sup>14]. The lack of usage of one warning ('virus infected app') could also caused by habituation effects or a systematic error of warning display.
- *Reaction:* The inference statistical analysis shows that children who used the 'Why?' button will be more likely to react adequately according to the warning instructions, which supports hypothesis 1 (H1). But it is only statistically supported for one warning ('malware infected update'). Furthermore, a significant correlation is found, that children who read background information ('Why?' view) will be more likely to react adequately relating to the warning instructions, which supports hypothesis 2 (H2). Nevertheless, this result is only statistically supported for one warning ('Bluetooth attack'), too.

## Chapter 1. Introduction and Motivation

---

The results of the evaluation of the introduced effective security warning approach are discussed using the framework of Cranor [Cra08]. **HITL** is a human-in-the-loop security framework to evaluate human failures during interacting with security applications. The comparison of the both prototypes with HITL show following **tendencies**, which have to be evaluated in future studies with larger test-groups:

- Demographic factors may play a role in warning perception and warning comprehension. So the most younger participants in test case 1 ('mobile robot warnings') rated the 'warning usefulness' as 'less useful' than elder participants. Most children in test case 2 do not comprehend the warnings, but react intuitively in the right way. Some children remembered the first meaning of a security warning in combination with the colour of the cartoon character.
- Reading additional information in security warnings (instructions and background information) could support the adequate reaction of users.
- Instruction information in security warnings could decrease the wish of users for additional help and could support their problem solving.
- Instruction information in security warnings could increase the heed of the warning by users.
- The perception of a high risk level by users could increase their compliance to decide after the warning recommendation.
- Instructions in warnings could melt the fear of users of malware-related personal impacts.

### Main lacks:

- Effects of *habituation* and *focus on the main task* were observed in both user studies. Some test persons were annoyed by warnings and therefore their were less motivated to read the warning messages carefully.
- The *attention switch* to warnings in the adults study is not relevant, because of the test situation where the tester talks to the participants.
- *Not all users are capable* to handle malware related situations only by reading warning information. Especially children have to supported by (technical-savvy) peers and/or parents to solve complex malware problems. But it has to be also evaluated whether security decisions in domestic environments are solvable by *non-security experts*.
- Additional warning information have to be well designed, because it *could negative influence user's comprehension*.
- The effects of *knowledge acquisition* and *application* of warning messages of the both prototypes has to be evaluated in future studies.
- Warning information is *no substitute for training, and external help*. It should be evaluated, whether a specific user-group is able to comprehend and process the recommended warning instructions or whether training and additional help is needed.
- Participants showed a less awareness for security threats on mobile devices and IoT devices although they knew about mobile malware.

Amongst the contributions related to the research objectives and research questions future research topics are sketched in chapter 7. It shows, how the introduced warning approach could be **generalised** and used in other research fields:

- **Different security warning types:** different to the introduced malware warnings on mobile devices could be improved by using parts of the new warning approach. Examples are SSL warnings and individualised warnings. Users could be sensitised with personal information about risk and consequences of cyber-attacks. Security warnings could be improved if users are supported with warning instructions for cyber-attack related problem solving. A future research topic could be the evaluation of differences of *habituation effects* of specific security warning types.
- **Non-professional application scenarios:** The new warning approach could be adapted for example for *modern automotive systems* and *IoT devices*. However, the system-specific characteristics, such as specific technological and safety requirements, have to take into account.
- **Professional application scenarios:** The new warning approach could be adapted for professional *human-machine-interaction scenarios* for trained expert users, such as operators or pilots. It could be used for risk communication on basis of interrelations of security impacts to safety functions. Furthermore, the instruction concept could be used as basis for expert education, training, and practices.
- **Different user-groups:** The warning approach could be also adapted for other user-groups, such as further mentioned *experts* with specific capabilities and user-groups with *limited capabilities* (e.g. hearing, vision). During the adaption process it has to be weighed up if warning effectiveness is influenced by adaption decisions and countermeasures to keep warning effectiveness have to take into account.

### 1.5 Thesis outline

---

The thesis based on 7 chapters and 1 appendix. It is structured as follows:

**Chapter 2** presents the fundamentals of this thesis. Section 2.1 introduces briefly mobile devices and examples of potentially coupled systems to mobile devices. Section 2.2 introduces briefly the terms of security and safety including the interrelations between security and safety. Section 2.3 presents mobile malware fundamentals including malware attack vectors, malware classes and malware defence strategies. In section 2.4 a fundamental model for human information processing of warnings is introduced. Section 2.5 presents the basics related to warning effectiveness, including warning design guidelines and differentiation of user groups. Section 2.6 introduces the fundamentals for the evaluation of security warning effectiveness. At the end of chapter 2 section 2.7 introduces briefly used statistic analysis methods to prove the relevance of the evaluation results.

Figure 1.2 (page 22) illustrated the outline of the chapters 3 to 7. **Chapter 3** introduces an *own literature review* of existing security warning approaches. **Chapter 4** presents the methodology and concepts of this thesis. It includes a *study* of malware warning design of current mobile Android security apps (section 4.1) and a *personal risk model*, which maps malware attacks against mobile devices and coupled systems to personal risks of users (section 4.2). In **section 4.3** the general warning design concept and in the **section 4.4** the general evaluation methodology and concept are introduced.

**Chapter 5** presents the realisation and evaluation of the both test cases of the generic user-specific warning approach for two specific application scenarios: mobile robot warnings for a generic user (section 5.1), and smartphone warnings for primary-school children (section 5.2).

**Chapter 6** presents the general results and discussion: for mobile robot warnings for a generic user (section 6.1), and smartphone warnings for primary-school children (section 6.2). At the end of this chapter the results of the two application scenarios are discussed based on the HITL model (section 6.3).

In **chapter 7** briefly summarises the work presented and draws conclusions to the defined research questions and objectives. The end of this chapter presents the ongoing and future work related to this thesis, which is outside the focus of this work.

The **appendix** present all necessary documents for the user studies, including evaluation documents, questionnaires and additional results.

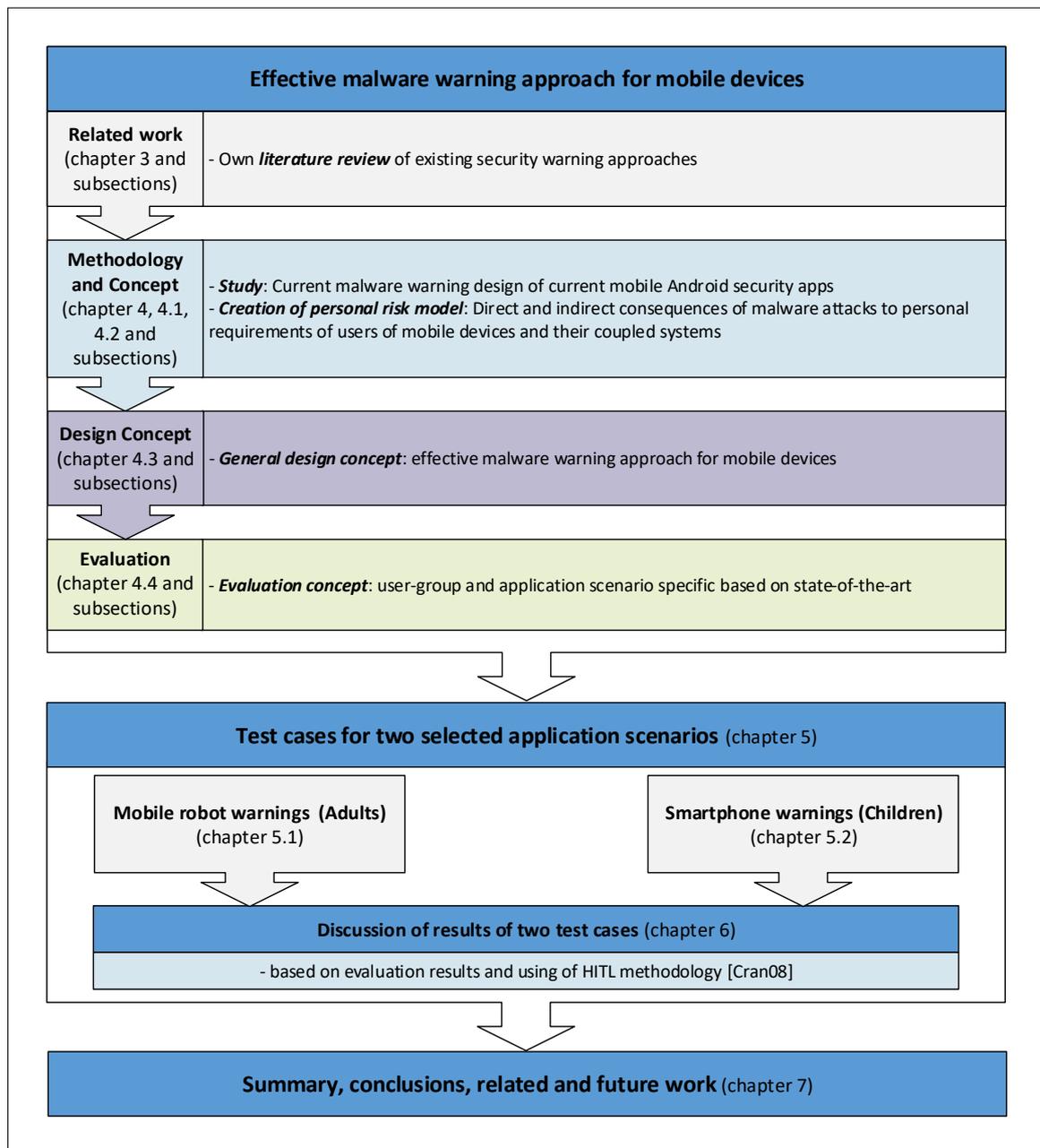


Figure 1.2: Outline of this thesis



# 2

## Thesis Fundamentals

This chapter should clarify all necessary fundamental terms to understand the context of this thesis.

### 2.1 Mobile devices and examples of coupled systems

This section clarifies the definition of the term 'mobile devices' used in this thesis and focused systems, which could be coupled with them.

The German Federal Office for Information Security (BSI) [BSI06] defines a *mobile device* as high-performance computer, which is structured similar to common desktop PCs. Furthermore, mobile devices have application specific hardware components and specific user interfaces for mobile usage. All system parts are developed for less power consumption. The hardware of mobile devices is changeable only with very high efforts compared to desktop PCs. There is no possibility to change or expand internal hardware components of a mobile device. Figure 2.1 illustrates a generic structure of a mobile device after [BSI06]:

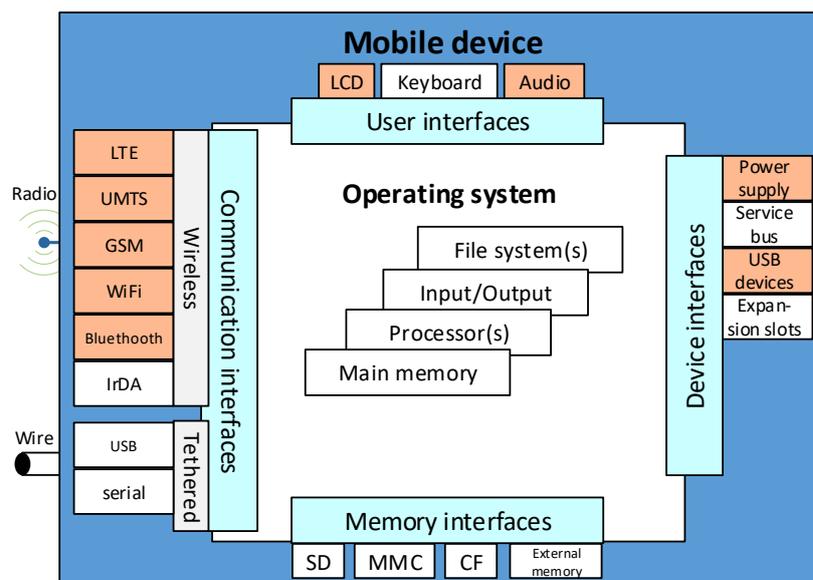


Figure 2.1: Generic structure of a mobile device (according to [BSI06],  
Note: orange blocks: typical tablet interfaces)

This thesis focuses on mobile devices, which are comfortable to carry for humans, are easy usable to control by normal persons, are easy to control mobile systems, and have user interfaces to allow the display of warning information. Therefore smartphones and tablets are in focus. A smartphone offers in comparison to a mobile phone more applications amongst telephone calls. The Oxford dictionary describes a smartphone as '*a mobile phone that performs many of the functions of a computer, typically having a touch-screen interface, Internet access, and an operating system capable of running downloaded apps.*'<sup>16</sup>. Amongst functions, such as communication via phone calls or in social networks, smartphones are also usable to remotely control other devices. Tablets are similar structured in comparison to smartphones, but they are constructed to realise specific tasks. Examples are reading of texts, surfing the Internet, remotely control of other devices, e.g. cameras, TV, or mobile robots. The tasks are realised through direct interaction of users with its screen<sup>17</sup>. Because of their specific structure, the interface components of tablets are limited (see orange blocks in figure 2.1).

Becher et al. [BFH<sup>+</sup>11] introduced *specific characteristics* of smartphones as class of mobile devices in comparison to desktop PCs, which have to be considered from the security point of view. These characteristics are similar to tablets:

1. *Limited device resources*: Smartphones have limited computation power (CPU and RAM) in comparison to high-end computers. So security solutions from ordinary computers are not transferable to these devices without adaptation. Examples are intrusion detection algorithms. Another limited resource is the battery, which restricts common security applications on mobile devices.
2. *Associated costs*: Using malware attackers could generate costs for users of both, desktop PCs and mobile devices, and for his own benefit. One mobile device specific aspect are services supported by mobile network operators (MNO) and used by smartphone owners, such as phone calls or messages. Another aspect are payment systems, which uses mobile phones to transmit trustworthy authorisation information, such as online banking using mobile transaction numbers (TANs).
3. *Network environment*: Smartphones have a specific network environment based on three columns. First, there is a strong influence possibility of the mobile device by the MNO. Smartphones and many tablets include a smartcard, which is owned by the MNO and is seen as trusted device. Second, firmware updates of focused mobile devices are realised remotely. If no connection to an ordinary computer is established, updates are processed over an mostly expensive wireless interface. Mobile malware is often masked as regular firmware update [BSI06] or distributed over third party application market places [FSK13]. Third, mobile devices could be managed by a remote entity, which has more influence on the device in comparison to ordinary computer environments. Examples are configuration updates or remote deleting functionality of MNOs, device manufacturers, or corporate IT departments.

---

<sup>16</sup>Oxford dictionary, 'smartphone', <https://en.oxforddictionaries.com/definition/smartphone>, accessed: 5.12.17

<sup>17</sup>Oxford dictionary, 'tablet', <https://en.oxforddictionaries.com/definition/tablet>, accessed: 5.12.17

4. *Limited user interface*: Mobile devices and their user interfaces, such as screens, are smaller in comparison to desktop PCs [Ram12]. Hence, security warnings have to be adapted to limited screen size and limited auditory system. Many mobile devices integrate components, which could generate haptic feedback, such components as vibration motors in the iPhone<sup>18</sup> and Android<sup>19</sup> based smartphones. Warnings could be improved using multimodal warning information (section 4.3).

Mobile devices, such as smartphones, are different in their physical structure in comparison to desktop PCs. Therefore, new attack vectors of malware have to take into account (section 2.3), and the warning design as to be adapted to mobile device characteristics (section 4.3.2).

### Potentially coupled systems:

As already mentioned in the introduction in the private field various systems could be coupled with mobile devices. One main function is the remote control of coupled systems by using standardised communication interfaces, such as WiFi and Bluetooth. Exemplary application scenarios are the remote control of mobile systems, such as domestic robots and remote control of navigation systems in cars. In the literature these coupled mobile systems are called 'embedded systems' (ES) and '*cyber-physical systems*' (CPS) [Lou15]. **Embedded systems** are hidden information processing systems, which are embedded into a larger product, such as a mobile robot. Their limited functions are tailored to a set of specific tasks (e.g. to increasing comfort, efficiency, safety) required by the system in which they are embedded. They communicate internal with sensors and actors to monitor and control physical processes in real-time. Embedded systems are valuable targets of attackers and malware, because they run some form of software and often have network communication capabilities.

In contrast to embedded systems **cyber-physical systems** are not controlled by one embedded system, they include several embedded systems to realise different functions. These ES are networked with each other and according to Loukas their '*computation, communications and physical processes are closely related and depend on each other*' [Lou15]. Furthermore, CPS intensively communicate using global communication infrastructures, such as the Internet. One specific class of cyber-physical systems are **mobile CPS**, e.g. manned and unmanned vehicles, such as modern cars. In contrast to classical CPS mobile CPS are restricted by unstable mobile networks, power limitations, and a high dynamic environment [GHH<sup>+</sup>18]. A cyber-attack on these systems could have direct impacts to the physical world [Lou15]. Because of their mobile functionality the physical impacts of mobile CPS are not locally limited. That means the environment, including persons, is potentially concerned.

This example of an impact of persons is communicated with the new warning approach to users of mobile devices, which could be connected to mobile systems, such as mobile service robots, or mobile CPS.

---

<sup>18</sup>Elizabeth, Apple Toolbox, 'iPhone System Haptics, Overview', <https://appletoolbox.com/2016/10/iphone-system-haptics-overview/>, accessed: 7.12.17

<sup>19</sup>Jerry Hildenbrand, 'Android A to Z: Haptic feedback', <https://www.androidcentral.com/android-z-haptic-feedback>, accessed: 7.12.17

### 2.2 Security and Safety

---

This section introduces terms of both protection worlds of security and safety, which are necessary to understand this thesis. This work focuses warnings about malware attacks on mobile devices and their coupled systems. Therefore the interrelation between safety and security incidents starts with a security perspective.

In [BSI08] the term **security** is named as 'information security' and specified as 'protection of information'. Its main goal is to protect the system against intentional attacks from the cyber-space, such as unauthorised manipulation or spying of data by attackers or their tools, such as malware. This thesis focus on the protection of user requirements of mobile devices regarding information security, e.g. the protection of their personal data processed by their mobile devices.

The three classical *security aims* are confidentiality, integrity and availability [Bis02]. *Confidentiality* is defined as concealment of data, information and resources. *Integrity* is the aim to prevent data, information and resources for improper or unauthorised change. Distinguished are two integrity types: data integrity (information content) and origin integrity (data source or authentication). *Availability* is defined as ability to use data, information or resources if desired. Amongst these three classical security aims also other security aspects are defined, such as authenticity and non-repudiation. Eckert defined [Eck08]: *authenticity* as originality and credibility of a object and subject, which can be proofed on basis of a unique identity and specific characteristics, and *non repudiation* is the guaranty of the system that executed actions could not be repudiated after the event.

Security aims are realised by *security measures*. These could be divided into technical mechanisms and organisational measures [BSI08]. Whereas technical security mechanisms are realised through the technical system itself, organisational measures include management and organisational aspects of the IT security, such as user awareness raising methods. Exemplary technical mechanisms to realise confidentiality and integrity are access control and authentication mechanisms using encryption. Violation of data integrity can be detected using cryptographic hash mechanisms. Security mechanisms to protect the system availability are quota, which regularise the usage of system resources, such as CPU time and memory [Eck08]. After an attack the replay of backuped uncorrupted data is an important mechanisms to re-store system availability.

Some security researchers add also *privacy* on the security aims. In this thesis privacy is seen as a personal requirement of a user, which is regulated by various laws. Examples are the German law (e.g. Federal Data Protection Act<sup>20</sup>) and European law (e.g. General Data Protection Regulation [GDP16]). Various security measures, which realised security aims could be used to realise privacy on technical systems. One example is the encryption of private data on mobile devices to realise as well as privacy as confidentiality. The term 'privacy' in this thesis focus on the protection of personal data of users of mobile devices.

---

<sup>20</sup>German Federal Data Protection Act, [https://www.gesetze-im-internet.de/englisch\\_bdsbg/index.html](https://www.gesetze-im-internet.de/englisch_bdsbg/index.html), accessed: 09.05.18

The term **safety** is defined by Storey as '*property of a system that it will not endanger human life or the environment*' [Sto96]. Its main goal is the protection of the environment and the system against hazards of the system with physical impacts, such as electric shocks or system malfunction.

Safety is divided into three categories [Sto96]: first, *primary safety*, the safety of the system itself, that the system itself will not endanger the users or the environment (e.g. through electric shock, burns), second, *functional safety*, which covers aspects of the correct functioning of the system's hardware and software components, third, the *indirect safety*, which is related to indirect consequences of a system failure or incorrect information. This thesis focuses on consequences of malware attacks (security) on mobile devices and interconnected systems (e.g. cyber-physical systems) to the correct functioning of these systems (functional safety).

Security-safety-interrelations are described differently in the literature. In this thesis these interrelations are considered from a security perspective. **Impacts of security attacks to functional safety of mobile systems** are in focus. Therefore the description of Hoppe et al. [HKD09] is used. They define security-safety-interrelations as 'structural impacts', which are indirect implications of a cyber-attack to the system functionality. They give the example of a manipulation on a car's TV system, which could lead to functional safety implications, such as unexpected activation of the steering lock. Loukas introduced the term 'cyber-physical attack' to describe attacks in cyber-space (e.g. malware attacks) which could have a physical impact in the real world (e.g. malfunction of mobile device coupled system) [Lou15]. In this thesis 'structural impacts' of malware attacks on mobile devices and coupled systems are in focus, which could influence user requirements. The author of this thesis also introduces in cooperation with other researchers a new methodology to describe interrelations between security incidents, which impacts the functional safety of embedded systems and vice versa [NFHD11]).

In this thesis the information about malfunction of malware influenced systems are used to warn users for potential personal consequences, such as impacts to users' personal safety. It is a basis for a personal risk model in section 4.2, which is a basis for the new warning approach introduced in section 4.3.

### 2.3 Mobile malware

---

This section introduces the term (section 2.3.1), classes and potentially malicious functions of malware on mobile devices (section 2.3.2), and sketches malware defense strategies for mobile devices (section 2.3.3).

#### 2.3.1 Mobile malware attack vectors

---

This section introduces mobile device specific access methods of malware, called *attack vectors*. There exist several attack vector classifications. One example is the publication of the BSI for mobile devices [BSI06], which classifies potential threats roughly whether the attacker has physical access to the mobile device, its applications, services, operating system, hardware, and its infrastructure. Nevertheless, the BSI classification focus on cyber-attacks in general, which is too detailed, and therefore not usable for the desired malware warning approach.

In contrast to the BSI classification, Becher introduced attack vectors of mobile malware [Bec09]. He defines four different **attack vector classes**: hardware-centric attacks, device-independent attacks, software-centric attacks and user-layer attacks. *Hardware-centric attacks* need physical access to the mobile device, such as forensic analysis which violates the confidentiality of personal data. These attacks are out of the focus of this theses, because they are not realisable remotely for malware. *Device-independent attacks* focuses the infrastructure supporting the mobile device, such as wireless connections and central data storage for phoning and messaging. These attacks could violate personal data of mobile users, but mobile network operators and not the user are responsible for security protection. Therefore, these attacks are also not in focus of this thesis. The last both attack classes correlating with the warning approach in this thesis. Therefore both are described in more detail.

*Software-centric attacks*: exploits the software, which is executed on mobile devices. In comparison to desktop PCs, mobile devices offers new attack vectors for malware, whereof malware could be quickly distributed. Exemplary attacks are buffer overflows, which allow attackers to execute their malicious codes/malware. Amongst the operating system, services, and applications also the mobile communication is an attractive target of malware. Classical threats are the passive attacks, such as sniffing of information and creation of movement profiles, and active attacks, such as spoofing.

*User-layer attacks*: not exploit the technical vulnerability of mobile devices, but it trick the user to realise malware attacks. One example is the method of *social engineering*, whereby users are manipulated to override technical security mechanisms. Thereby, on the one hand, the *security awareness* of users play an important role. One example is the check of inquired access rights of an app. One current example of an keyboard app<sup>21</sup> collects massive amount of personal data of smartphone users, e.g. address book contacts, IMEI number. On the other hand, the lack of *usability* of several security applications and mechanism including their warning mechanisms [CG05] are also an important factor, if user-centric attacks have to be avoided. This thesis introduces a new approach of warnings, which give users instructions how to avoid personal consequences of malware in their personal environment.

---

<sup>21</sup>Dennis Schirmacher, heise Security, 'Daten von 31 Millionen Nutzern der App ai.type Keyboard geleakt', <https://www.heise.de/security/meldung/Daten-von-31-Millionen-Nutzern-der-App-ai-type-Keyboard-geleakt-3910522.html>, accessed: 7.12.17

### 2.3.2 Mobile malware classification

There are several concepts to classify malware (e.g., [SZ04, Kas08, Szo05]). Antimalware software developers often classify mobile malware by their *general appearance*. Classical categories are: viruses, worms, and trojan horses. Specific categories are ransomware, backdoors, and rootkits. Furthermore, malware researchers differentiate other malware categories, e.g. spyware. In this thesis not the name of the malware rather the behavior of malware is important to give users guidance to defend personal impacts of malware. Therefore in table 2.1 main malware classes are introduced based upon their main characteristics. 'Current examples' of mobile malware in table 2.1 are based on current publications in the online press<sup>22232425</sup>. These malware could often not be differentiated clearly, because their characteristics are defined in more than one malware class. Skoudis named them 'combination malware' [SZ04]. Examples are trojan horses, which could install backdoor or rootkit functionalities on the target system.

Generally systems, which are wide spread are profitable targets of cyber-criminals, because they could reach a crowd of similar systems with one attack [Kas08]. According to the latest malware report from Nokia [Nok17] smartphones with the Android operational system are currently one of the most attacked systems by mobile malware, because they dominate the market<sup>26</sup>. Furthermore, Android allows its users the download and installation of applications from untrusted third-party sources, where mobile malware is distributed as trojan horses. These malware class camouflage itself as useful application and hides its malicious functionality from users. In the future, more attacks against mobile devices and IoT are predicted by malware researchers [Nok17, Kas17].

A theoretical example for mobile malware classification is the *formalisation methodology* of Kiltz et al. [KLD06] to classify trojan horses regarding their specific properties. This methodology could be used to compare different malware and to weight their damage potential. In [DKF<sup>+</sup>10] the seven different categories of the methodology are introduced in English<sup>27</sup>: the distribution method (D), the activation method (A), the placement method (P), the mode of operation (O), the communication method (C), the payload function (F) and the self protection measures (S). The distribution method (D) specifies the way, how the malware gets on the system. After its first placement on the target system, the category *Activation Method (A)* describes the way, how the malware ensures its further execution, especially in terms of automatic activation after future reboots. The category *Mode of Operation (O)* specifies different techniques for malicious activity at the infected system. The category *Communication Method (C)* describes the possibilities of the malicious code to communicate with the attacker.

<sup>22</sup>Roman Unuchek et al., Securelist, 'IT threat evolution Q3 2017. Statistics': <https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/>, accessed: 7.12.17

<sup>23</sup>Roman Unuchek et al., Securelist, 'IT threat evolution Q2 2017. Statistics': <https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/>, accessed: 7.12.17

<sup>24</sup>Roman Unuchek et al., Securelist, 'IT threat evolution Q1 2017. Statistics': <https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/>, accessed: 7.12.17

<sup>25</sup>Andrea Lelli, Symantec official Blog, 'A Smart Worm for a Smartphone WinCE.PmCryptic.A', <https://www.symantec.com/connect/blogs/smart-worm-smartphone-wincepmcryptica>, accessed: 13.12.17

<sup>26</sup>Gartner, 'Gartner Says Demand for 4G Smartphones in Emerging Markets Spurred Growth in Second Quarter of 2017', <https://www.gartner.com/newsroom/id/3788963>, accessed: 12.12.17

<sup>27</sup>The abbreviations of the tuple's categories from [KLD06] have been translated to English counterparts.

Mobile malware class	Main characteristics	Current examples
Virus	Infection of host file (e.g. executable), Self-replication, Requirement of human interaction to replicate (e.g. open a file, executing an infected program)	-
Worm	Self-distribution across a network, Self-replication, No requirement of human interaction to spread	Infomeiti/ Infojack, Pmcrptic
Trojan horse	Camouflage as useful program, Mask of hidden malicious functions (e.g. steal of user credentials, unauthorised banking, remote control, DDoS), Requirement of human interaction to spread, Using of social engineering techniques	Asacup, Svpeng, FakeToken, Zbot
Ransomware	Restriction/prohibition of data and system access, freeing of resources after paying a ransom	Zebt, Congur (trojan horses)
Backdoor	Remote control of victim's system	Ztorg family (backdoor and trojan horse), Shiz
Rootkit	Utilities to realise malicious activities, Camouflage for antivirus applications, Two types: <i>User-level rootkit</i> : Replacement or modification of executable programs of system administrators and users, <i>Kernel-level rootkit</i> : Manipulation of operating system kernel, Hiding and creation of backdoors	Neurevt (trojan horse)

Table 2.1: Main classes and main characteristics of mobile malware (after [SZ04])

The *Payload Function (F)* describes the purpose or task for which the malicious code is placed on the victim's system, e.g. what services or commands it offers to the attacker. To protect itself against detection or deletion, the malicious code can use different self defense mechanisms, named here as *Self Protection Measures (S)*. These malware properties are arranged to a tuple. These formalisation is to complex for the desired warning approach, which focuses on user education and guidance.

The malware classification of Becher [Bec09] offers a *simplified categorisation of mobile malware*. Becher distinguished between three phases of malware activities: *infection*, *malicious functionality*, and *spreading*.

During the **infection** phase malware infiltrates the mobile device ('Mode of Operation' (O) in [KLD06]). Exemplary attack vectors (section 2.3.1) are software-centric attacks, exploiting the technical vulnerability of the device and user-layer attacks, such as social engineering. Becher distinguished four classes of malware infection regarding user interaction:

- *Explicit permission*: The user is asked to allow the infection of her device. Thereby the malicious malware property is clearly communicated to the user. Typically proof-of-concept malware shows such characteristics.
- *Implicit permission*: The user is asked implicitly during the standard installation process for (unsigned) software. Most users are familiar with such installation procedures. Trojan horses are often installed this way. Users are allured with social engineering techniques, so they wish to install the offered software. One example is a text such as: 'Free World of Warcraft Game - just install'.
- *Common interaction*: The user performs a typical interaction on her mobile phone. One example are malware attacks using MMS messages, such as MMS buffer overflow.
- *No interaction*: The malware does not need any user interaction to infect the mobile device. It is the most dangerous type of malware for mobile devices regarding their infection potential. Examples are smartphone worms, such as Infojack.

If the malware is on the targeted system it could commit its **malicious functionality** (Payload Function (F) in [KLD06]). At this time the two market leaders of mobile operational systems Apple's iOS and Google's Android have different system structures and security protection strategies, which ease or complicate malware to attack these systems [RBG14]. That are the control of public online market places, handling of personal data by apps, and security protection layers. The control of the market place is out of scope in this thesis because it is not related to the warning approach in this thesis.

*Handling of personal data by apps* [RBG14]: *Android* users have to agree to the all permissions automatically generated during the installation process, requested by the app. These permissions are passive warnings, which include access and manipulation rights for different data types, e.g. contacts, messages. If users do not agree, they could not install this app. Since iOS6 (Sept. 2016) *iOS* offers its users a new handling policy of personal data. Users have a runtime consent for many data types, e.g. photos, social network accounts, contacts. Furthermore, users could customise their data disclosure policy. Han et al. [HYG+13] found out, that future display of *Android* permissions support a '*more restrictive use of personal data by app developers*' in comparison to *iOS* apps.

*Security protection layers* [Mil11][XSJ+16]: *iOS* provides a layered approach to prevent exploitation. *iOS*'s first layer includes a data execution prevention (DEP) technique to distinguish between data and code. DEP mechanism prevents code injection attacks, which write payloads into memory and execute it. Address space layout randomisation (ASLR) makes memory regions in the process address space unpredictable. ASLR is used to prevent code reuse. *iOS* has several restrictions to prevent damages if malware could get run a process through an exploit. The second defence layer includes that apps run in a sandbox, which limited app privileges,

such as interaction with other apps or access of resources of other apps. Furthermore, the app runs with restricted access rights in comparison to the root level. In addition, the installation and running of additional software or tools is prohibited on iOS devices. Whereby malware could not install additional attack tools, such as keyboard sniffers. Furthermore, the lack of a shell or further useful tools in iOS complicate the malware attack. So malware could only be active within the exploited process, which restrict their persistence on the mobile device. *Android* uses the Linux kernel with its Discretionary Access Control (DAC). So Android apps could only access resources in their own sandbox. The DAC-based application sandbox is the only security boundary of Android apps<sup>28</sup>. Androids primary security assumption based on the prevention of users or high-level apps to get system/root privileges. Many malware attacks against Android undermine this assumption by so called 'jailbreak' to get root rights and so Androids fundamental protection mechanism fail. Main reason is the customisation of Android to its mobile hardware, which make Android unique in comparison to traditional Linux-based systems [XSJ+16].

Furthermore, these malicious functionality of mobile malware could have **personal impacts** for users:

- *Monetary damage*: The user has to notice such malware impact, because she<sup>29</sup> has to pay money for it. Current examples are ransomware attacks, which encrypt users private data on their system and threat to only decrypt the data after a specific amount of money is payed. Other examples are attacks with banking trojan horses, which steal bank credentials to draw out money. Classical attacks against mobile phones are the sending of premium SMS or telephone calls to premium numbers. Additionally, attacks could be differentiated, which effect a higher power consumption and therefore generate more costs for users.
- *Data damage*: could be divided into *data theft* and *data destruction*. Mobile malware, like trojan horses could spy out personal data stored on and communicated with mobile devices. Examples are emails or personal data, such as pictures, short messages, audio or video recordings, general memory content of file system or memory cards. The easiest way for cyber-criminals to demonstrate malicious power of their malware is to destroy data. Exemplary targets for *data destruction* are previously introduced data types, which could be manipulated or deleted. Furthermore, device configuration settings or file system parts could be attacked by denial-of-service attacks, which could impact the availability of mobile services. Examples are blocking of user interfaces or disabling the booting of the device. These attacks also could have monetary effects.
- *Hidden damage*: Mobile device users are mostly the owners of these systems. They carry it the most of the time. These personalised device offers specific attacks, such as spying of users privacy by making audio or video recordings. Other malware track locations of mobile device users, if malware could access and forward local information (e.g. GPS signal or cell identification). Another hidden malware activity is the adding of a mobile device as member of a botnet for sending spam emails or realise denial-of-service attacks.

---

<sup>28</sup>The Dalvik Virtual Machine (VM), in which many Android apps run, does not provide sandboxing comparable to the Java VM [XSJ+16].

<sup>29</sup>In general, for the sake of simplicity the author has chosen to use the female form. But any female term also apply to men.

**Spreading** is the phase, where malware spread itself to infect other devices (Distribution (D) in [KLD06]). Classical exemplary distribution channels are local connections via wireless LAN or Bluetooth, remote connections over the data network using IP addresses, and email. Mobile device specific distribution channels are remote connections over the phone network using phone numbers stored in the address book on the phone or external memory. If mobile devices are coupled with mobile systems amongst security aspects also safety aspects could play an important role. Reasons could be the malfunction or fail of mobile systems caused of malware infection. These malware impacts are introduced by Hoppe et al. [HKD09].

**Mobile Malware Portability:** This lead to the question, whether mobile malware is able to infect connected systems of mobile devices. Mobile malware researchers, such as Becher [Bec09] and Fedler et al. [FSK13] have shown, that it is realisable, if malware uses specific application frameworks with run time environments or different executables on different platforms and if malware is portable. One exemplary malware using PC-to-device infection is 'Zeus in the Mobile' (ZitMo). This trojan horse was discovered in the year 2012. It first infects Windows PCs and then smartphones to gather mobile TANs for online banking<sup>30</sup>. Device-to-PC infection was first observed in 2013 for trojan horse 'Super clean', which first infects Android devices and then PCs, if these would be connected to them<sup>31</sup>.

### 2.3.3 Mobile malware defence strategies

---

These section introduces defence strategies for mobile devices, which could be handled by non-security expert users. Malware defence strategies are technical and organisation measures to prevent, detect and react to malware attacks against mobile devices and their coupled systems.

#### **Prevention:**

Users of mobile devices can educate themselves how they have to change their behaviour to prevent malware infections of their systems. Skoudis published some countermeasures for malware in general on systems, which are included into technical infrastructures [SZ04]. These measures are adapted for non-security expert users in private environments. In the following **user education measures** are sketched:

- *Using malware defence mechanisms*, such as SPAM-filter in email applications or antivirus software (see 'Detection' paragraph).
- *No disabling of defence mechanisms* (e.g. antivirus software) when something do not work. Users should instead call a support. That could be also a technical-savvy friend or relation.
- *Do not open or execute executable files*. User should be cautious handle attachments (e.g. email) they not routinely work with, even attachments from friends.
- *Rarely download and installation of apps* from external sources. Because of potential including of malware users should think about if the installation of apps is even necessary. They should download these apps from secure sources, such as official online market places for mobile apps. The both current leaders for mobile devices Apple and Google

---

<sup>30</sup>SECURELIST, Denis Maslennikov, 'New ZitMo for Android and Blackberry', <https://securelist.com/new-zitmo-for-android-and-blackberry/57860/>, accessed: 15.12.17

<sup>31</sup>SECURELIST, Victor Chebyshev, 'Mobile attacks!', <https://securelist.com/mobile-attacks/65379/>, accessed: 15.12.17

prevent their online market places by malware detection mechanism and realise malware removing on mobile systems, which installed their operating system. Nevertheless, malware infected apps are as well found in official online stores [RBG14].

- *Check app access rights.* During the installation process apps demand several access rights to specific mobile device components (e.g. microphone, camera) or data (e.g. address book, pictures). The enabled access rights allow malicious apps to realise their malign activities [RBG14], such as spying. Users should proof if they really need this app and if an alternative app, which demands less access rights is available.
- *Learning recognising signs of a virus infection.* Users could minimise virus attack damages if they recognise virus infection signs. Examples are decreased performance, system crashes, bounced emails, and antivirus software warnings. Users should contact technical support, technical-savvy friend or relation.

### Detection and reaction:

The main detection strategy of mobile malware is the usage of **antivirus applications**, which detect most of the main malware types introduced in section 2.3.2. Classically, malware detection strategies of antivirus applications<sup>32</sup> are categorised in signature-based and heuristic detection techniques [Kas08]. The 'signature' of a malware program is a specific part of the malware code, which is stored in antivirus databases to compare the current signature with already known malware examples. In contrast to the classical antivirus scanner the *behaviour blocker* monitors the behaviour of running code and stop code execution if the behaviour is detected as conspicuous or malicious. It based on a specific rule catalogue, a guide what to do in a specific case. Signature-based techniques detect all known malware, but overlook currently unknown malware. The antivirus database size and high resource consumption are further disadvantages. Behaviour blocker could detect unknown malware. But it's difficult to register all malicious behaviour in a consistent rule catalogue, because the behaviour of current malware is manifold and malware programmer change their malware quickly to protect their code for detection. Another disadvantage are the potential false alarms, when legal applications are detected as malicious and blocked. Another detection method is the *heuristic analysis*. It analysis the probable behaviour of an application before it runs and concludes their potential malicious actions. But proactive technologies, such as heuristics or behaviour blockers are only efficient for a short time, before malware developers find ways to circumvent it.

On mobile devices energy consumption play an important role. So mobile detection strategies are could be also differentiated in host-based vs. cloud-based solutions [Ram12]. Whereas *host-based techniques* run directly on mobile devices, *cloud-based techniques* use an external server to improve the computation efficiency. One energy efficient mobile malware detection solution was published by Lee et al. [LKK09], where a mobile and a binary inspection server cooperated. Amongst the introduced malware detection techniques various additional techniques are researched. Examples are analysis of application permissions [EOM09], techniques based on social collaboration [YGI11], and battery life monitoring [KSS08, LYZC09].

---

<sup>32</sup>This thesis focus on solutions for normal mobile device users. Therefore, advanced malware analysis techniques [SH12], such as static code analysis without program executing and dynamical analysis with program executing in an isolated environment, are out of scope in this thesis.

Antivirus applications warn users for detected malware on their systems, such as mobile devices. If mobile devices are coupled with other systems, such as embedded systems or cyber-physical systems, malware may spread to coupled systems and could potentially endanger humans in the vicinity by malfunction of these systems. Warnings of security software could be improved if users are educated about counter measures to save themselves. In this thesis in section 4.3 a new warning approach is introduced, which offers such a feature.

## 2.4 Human information processing of warnings

---

This section gives a brief introduction to main parts of human information processing, because the design and evaluation of the effective security warning approach in this thesis are based on it.

Humans are seen in the context of secure systems as 'the weakest link in the chain' [Sch00]. They often fail while they perform security-critical-functions. Automated solutions seems to be a good alternative. But sometimes human interaction to realise security-critical-functions is necessary. Aloud Cranor these are two cases [Cra08]. First, tasks which need human knowledge that are difficult for technical systems to process, e.g. the judgement of suspicious email attachments. Second, if its to complex or expensive to implement all specific cases of a whole security policy. Other reasons for human interaction are the delay in malware attack handling and transparency reasons introduced in section 1.1.

Cranor proposed a systematic approach [Cra08] which should aid software designers to understand and design out human-related security problems while users interact with security applications [BLCDK10]. It is called 'human-in-the-loop security framework'. The framework could be used in two stages of a software development life-cycle: first, the phase of system design to prevent human errors and second, the maintenance of existing software to analysing causes of security failures. This framework could be used for analysis of a variety of secure systems depending on humans. Examples are warnings of security software, like anti-phishing toolbars or anti-virus programs. The analysis focuses on the behaviour of non-malicious humans, who are users which could threat system security by their actions accidentally and administrators, who maintain the security of the system.

In this thesis HITL is used to evaluate the effectiveness of the introduced both warning test cases in section 6.3. The human-in-the-loop security framework is based on the Communication-Human Information Processing (C-HIP) model from the safety warning science [Wog06b]. The framework is based on an unpretentious communication-processing model (figure 2.2). A sender sent a 'communication' to a human receiver, triggering specified behaviour. The behaviour is affected by several internal and external influences, like internal information processing steps and personal characteristics of the human receiver, and communication impediments from the environment. The author of the framework offers some interpretation recommendations. So the internal information processing steps in figure 2.2 should not be understand as linear process, rather as steps which could be omitted or repeated. Furthermore, Cranor depicted her framework as no exact model of human information processing, rather as checklist for systematically analysis of the human part in secure systems.

The framework is based on *four major components*: the communication, communication impediments, human receiver characteristics, and the behaviour of the human receiver.

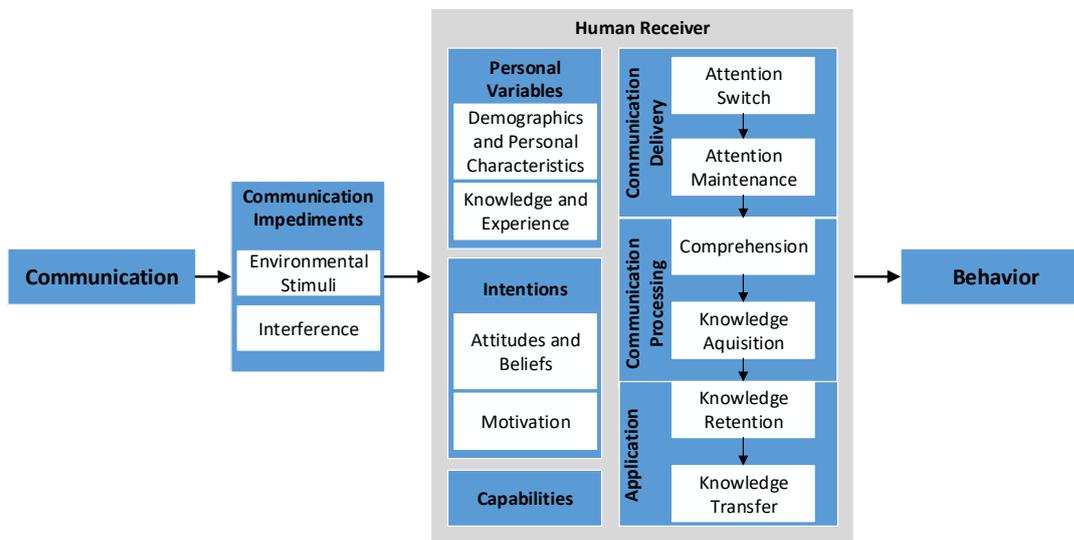


Figure 2.2: Human information processing in human-in-the-loop framework (according to [Cra08])

The first component of the framework is the **communication**. Cranor distinguished *five types of communications*, which could have an impact to security tasks: warnings, notices, status indicators, training, and policies. This thesis focuses on *warnings*. According to Cranor warnings are communications which alarm users to avoid a hazard or threat by their action. Examples are passive warning indicators in web browsers to alert users to expired SSL certificates or phishing web sites and active warnings about malware risks which interrupt users primary-task to enforce a user security decision (section 2.5). In the safety warning science literature warnings are described as last alternative, so called 'third line-of-defence' if the protection against a hazard is not realisable by a safe system design [Wog06c]. This concept is transferable to security warnings. If the use of warnings is not avoidable, warnings have to be designed with a major effect. According to Wogalter effective warnings '*clearly communicate the risk, consequences of not complying, and instructions to comply*' [BLCDK10] (section 2.5). The introduced warning approach for mobile devices in this thesis based on Wogalters concept of warning effectiveness (see section 4.3).

The second component of the framework are **communication impediments**, which could disturb the communication between sender (here: mobile device) and receiver (here: human user). Cranor distinguished *two classes* of communication impediments: Environmental stimuli and interferences. While *environmental stimuli* divert user's attention away from the communication, *interferences* prevent the communication to the receiver. Examples of environmental stimuli are other related or unrelated communications, light and noise in the vicinity, and the primary task of the user, which may interrupt the security communication. Examples of interferences are malicious actions, technology failures, and environmental stimuli that mask the communication.

The third component of the framework is the **human receiver**. The communication to the receiver is affected by receiver's personal variables, intentions, and capabilities, which impact the *three steps of internal information processing*:

**Step 1: Communication delivery:** consists of *two phases*, the attention switch and the attention maintenance. The basis of a successful communication is that users notice (*attention switch*) the communication 'or are made aware of rules, procedures or training messages'. Furthermore, users have to pay attention to it a specific time to process the communication (*attention maintenance*). This is the time users need to read, watch, or listen to it completely. Cranor indicates three factors, which may have influence on the communication delivery: First, communication impediments, like environmental stimuli and interferences; Second, communication characteristics, like format, font size, length, and delivery channel; Third, habituation effects, which describe a decreasing impact of a stimulus over time (e.g. a warning) when humans are accustomed themselves to it. So over time users may ignore communications, such as warnings, which they observe frequently.

**Step 2: Communication processing:** consists of *two stages*, comprehension and knowledge acquisition. *Comprehension* is the ability of users to understand what is communicated. Cranor identifies various factors which may influence the comprehension: the user's familiarity with indicator symbols and their analogy to similar symbols, vocabulary and sentence structure, and the conceptual complexity of the communication. Factors that aid comprehension are sentences, which are short and jargon-free, familiar symbols, and clear statements about risk [HBRF06]. *Knowledge acquisition* is the ability of users of both understanding and learning to response to communications. There is a difference between comprehension of a security warning - the user understand that she has to take action to avoid a threat<sup>33</sup>, and knowledge of steps to avoid the threat the user knows what she has to do to avoid the threat. The stage of knowledge acquisition is based on training of users. Cranor argued that training increases the ability of users to understand and know what to do when recognising the warning. Another alternative to training is an effective warning design, which includes clear instructions to users how to avoid the threat.

**Step 3: Application:** includes two phases, knowledge retention and knowledge transfer. *Knowledge retention* is the ability of users to remember the communication in a specific situation to apply it, and to identify and remember meanings of symbols and instructions. Knowledge retention is influenced by various factors: user's long term memory, frequency and familiarity of communication, and the user's involvement during training activities. *Knowledge transfer* is the ability of users to recognise situations where the communication is suitable and to identify steps to apply to it. Knowledge transfer is influence by two factors: user's involvement during training activities, and the level of similarity between examples in the training and in real situations, where users have to apply their knowledge.

---

<sup>33</sup>Cranor uses the term 'hazard' for a dangerous situation which is caused by accidental system failures, which endangers the environment. The term is derived from the safety terminology. However, this thesis focus on security warnings. In the security terminology a 'hazard' is a 'threat', which endangers the system, caused by intentional attacks of cyber-criminals and their tools (e.g. malware). Therefore, the term 'threat' instead of 'hazard' is used.

Amongst the internal information processing steps the communication to the human receiver is also influenced by **personal variables**. That includes the two domains of demographics and personal characteristics, and knowledge and experience, respectively. *Demographics and personal characteristics*, which may impact the receiver, are gender, age, education, culture, occupation, and disabilities. Cranor admonish designers of secure systems to know their users well and their likely behaviour, which is suggested by their personal characteristics. Furthermore, *knowledge and experience* is impacted by user's education, occupation, and prior experiences. Aloud Cranor personal variables may influence users' comprehension, apply of communications, users' intention and capability to take adequate actions. For example expert users with previous technical knowledge and training will better comprehend detailed warning instructions in comparison to novice users. However, experts may also be more likely to question warnings and could make a wrong decision to ignore the warning although the situation is risky.

Communication to human receivers is also influenced by **intentions**, including attitudes and beliefs, and motivation. Aloud Cranor these factors may influence user's decisions to pay attention to a communication and to comply with it or not. There exist various theories and models of behavioural compliance, which describe users receiving, comprehension, and compliance or ignorance of communication [KW06]. *Attitudes and beliefs* include various factors, such as beliefs about the reliability of the communication, user's ability to finish recommended actions successfully (referred to as self-efficacy), effectiveness of recommended actions (referred to as response-efficacy) including the period to conclude these actions, and general attitude towards the communication (e.g. annoyance and trust) [CDC06]. *Motivation* is related to user's incentives to take the appropriate intervention carefully. Cranor indicated that security communications may have negative influences on user's motivation, because they distract users from their primary tasks. So there is a conflict between user's primary goals and security goals.

The attitudes and motivation of users are influenced by their perception of security risks in concurrence to their primary task. Cranor reasoned users tend to ignore security communications, if they consider that is more important to avoid delays while finalising their primary task than to avoid security risks. Further influences of attitudes and beliefs could be past experiences of users with specific security communications. If users were confronted with erroneous warnings, called false positives, users may see them as suspect, mistrust them and do not follow their instructions (see also section 3.1). Cranor referred to *four motivation strategies*. First, the *design of security tasks* should be *sophisticated* with the ability of users to perform it easily and with minimal interruption of user's workflow. Second, *user's awareness* has to be raised for security risks, so they can estimate consequences of their actions provoke of security failures or prevention of hazard. Third, the identification and addressing of *cultural norms*, which constrain good security practice. Fourth, useful motivation tools within an organisation are *rewards and punishments*.

Amongst the above described criteria the communication also depend on the **capabilities** of the receiver. Although the receiver comprehends a communication, understand how and in which situation to apply it, the communication could fail, if the receiver does not have the capability to perform the required actions. Factors that influence receiver capabilities, which depend on specific actions, are specific knowledge, cognitive or physical skills, memorability, and required software or devices.

## 2.4. Human information processing of warnings

The **fourth component** of the framework is the triggered **behaviour** of the human receiver. In the best case the receiver understands the desired action and is able to proceed it. But sometimes the behaviour of receivers of a communication could be impediment, in which *two main reasons for failures* are called to account: the failures in system interface design, and the human error (table 2.2).

Cases of Behaviour	Success of execution	Impediment for behaviour	Warning examples	Solution
Failure free / Best case	Yes	-	No problem with warning interaction	-
<b>Cause of failure: System interface design</b>				
Gulf of Execution [Nor88]	No	Inability to proceed the desired action	Inability to find the 'further' warning button	<i>Design:</i> Clear instructions, Obvious functionality of interfaces
Gulf of Evaluation [Nor88]	Not determinable	Inability to verify the successful choice of an action	Inability to check if press of a specific warning button has an effect	<i>Design:</i> Adequate feedback
<b>Cause of failure: Human Error</b>				
Mistake [Rea90]	No	Wrong action plans	Open a worm-infected email from a friend despite a warning	<i>Design:</i> Clear communications
Lapse [Rea90]	No	Missing to perform a planned action	Skipping to read warning background information for decision making	<i>Design:</i> Minimal number of steps to complete a task and guidance
Slip [Rea90]	No	Incorrect performance of a planned action	Press wrong warning button	<i>Design:</i> Location of controls with ease access arrangement, unmistakable labelling
Exploit by attackers [Cra08]	Yes	Predictable behaviour	Click-through tendencies of users	<i>Organisation:</i> Encourage / Prevention of less predictable behaviour

Table 2.2: Cases of behaviour (according to Cranor [Cra08] and complemented by own examples)

Two types of **failures in system interface design** could be distinguished: First, the receiver is *unable to proceed the action*, although he understands what to do; second, the receiver performs an action, but *could not determine if it was successful*. The reason of the failure in the first case is identified by Norman as 'Gulf of Execution' [Nor88], which describes the gap between user's intentions to perform an action and the supporting system mechanisms to facilitate that action. For example the user is unable to click-through one warning view to another view. The reason of the second case of inability of determination of successful action completion is described by Norman as 'Gulf of Evaluation' [Nor88]. For example the user is unable to check, if the choice of an option in the warning was successful.

According to Norman *good design* could minimise the Gulf of Execution and Gulf of Evaluation [Nor88]. There are two approaches to minimise the Gulf of Execution (table 2.2): First, the design of security communications using *clear instructions* about how to perform the favoured actions; Second: the *obvious functionality of interface components* or hardware for human-machine-interaction. For example the user has sufficient visual hints to find the 'further' button to click-through one warning view to another view. To minimise the Gulf of Evaluation the design of software and devices should provide an *adequate feedback* to users, so they are able to determine the result of their executed actions. For example the user is able to check on basis of visual feedback, if the choice of an action in the warning was successful.

Cranor distinguished **four types of human errors** in secure systems (table 2.2), *mistakes*, *lapses*, *slips* and *predictable user behaviour* which could be exploited by attackers. The first three types are based on James Reason's theory of human error - the Generic Error-Modelling System (GEMS) [Rea90]. *Mistakes* could occur when human plan actions which will not reach the desired goal. For example the user plan to check if she knows the receiver of an email message before opening an email attachment to verify the email integrity. This planned action will result in a mistake when the friend's computer is infected with a worm that propagates to everyone in her email address book. The human failure could be caused by a wrong mental model of the email receiver, which will ignore a warning because she believes it is sufficient to trust the sender of the warning to verify the email integrity. *Lapses* are another form of human error. They occur when humans have suitable action plans, but forget to perform the planned action, e.g. skip a step in an action series. One example is to forget to read warning background information for better decision making. *Slips* occur when human perform an action inadequate, e.g. if the user selected and press a wrong button, such as the acknowledgement button instead of the disagreement of the current option. A good design could reduce human errors (mistakes, lapses, and slips). Cranor recommended that designers have to create *clear communications* including specific instructions to reduces that users make mistakes while completing security-critical tasks. Furthermore, according to Cranor the number of steps to complete the task have to be minimised and users have to be guided through the sequence of task steps.

The security of a system often based on randomness to prevent attacker exploits of predictable patterns to breach system security. However, *predictable user behaviour* that follows predictable patterns, which could be exploited by attackers could melt the strength of a security measure. For example attackers know that similar warnings are ignored by users expressed by increasing click-through tendencies of users. So an attack could be successful although a warning is presented, but users ignore the warning, because they are habituated to the warning.

**Applying the framework:**

Figure 2.3 illustrates the human-in-the-loop security framework as a four-step iterative process tool to *identify and mitigate human threats* to system security. Cranor recommend to use her framework in the design and deployment phase.

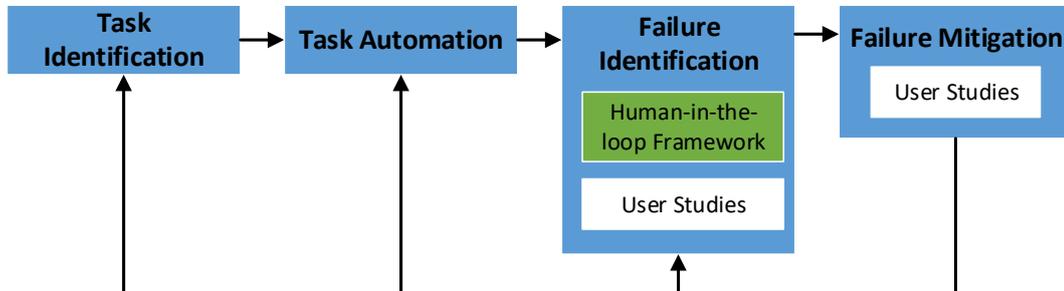


Figure 2.3: Human threat identification and mitigation process including the human-in-the-loop framework (according to [Cra08])

In the first phase, the *task identification step* the secure system designer has to identify all aspects, where a human interaction is needed for security-critical functions. In the second phase, the *task automation step*, the designer identifies security-critical human tasks, which could be partially or fully automated. One example is the use of well-chosen defaults or automated decision making to replace user decision steps. However, Edwards et al. [EPS08] published the **limits of security automation**. They discuss the danger of user overload in cases the automation will fail and users have no experiences to handle this specific failure case. They recommended to allow users to *monitor the system*. So users could *verify the correct performing* of the system and could recover the system from automation failures. Edwards et al. published a set of *guidelines* to decide pro or contra user security decision making. Examples are questions about the accurateness of the system, whether automation reduces the end-user information overload or simplifies the security decision making, alternatives to automation, mechanisms to 'keep the human in the loop', and user-friendly mechanisms to deal with automation failures.

In the third phase, the *failure identification step*, the potential failure modes for the remaining human tasks are identified. On basis of user studies failures which occur in practice and their reasons could be determined. If no empirical data is available recommendations for user studies could be given on basis of the framework. In the last phase, the *failure mitigation step*, the designer determines how users could be better supported while they perform these tasks. Examples are context-sensitive help in warnings and decision-support tools or decision-support by warning information.

After a first pass through the process Cranor recommend to revisit selected or all of the steps of the process to try to reduce human security failures. So decisions regarding the automation or no automation of human interaction with security applications could be made.

In section 6.3 the HITL is used to compare the both warning test cases in this thesis and find indicators for warning improvements.

### 2.5 Effective warnings

---

This section describes the definition of the terms related to *warning effectiveness*, and introduces different *warning types* in section 2.5.1.

The Oxford dictionary defines the term **warning** as:

'A hypothesis or event that warns of something or that serves as a cautionary example.'<sup>34</sup>.

The security warning researcher L. Cranor defines **security warnings** in [Cra08] as:

'Communications that alert users to take immediate action to avoid a hazard.'

This thesis focuses human-computer interaction scenarios where mobile devices could be connected to other mobile systems, such as embedded systems (ES) or cyber-physical systems (CPS). If mobile devices or their coupled systems are malware infected, classical security threats (e.g. data manipulation) could have impacts to safety functions of ES or CPS. That means potential personal consequences for users of mobile devices are related to both: security (e.g. privacy) and safety (e.g. life and limb). So the definition of classical security warnings has to be adapted to define **focused malware warnings** in this thesis:

'Malware warnings are communications, which inform users of mobile devices about malware-related personal consequences so users could protect themselves and their environment.'

The focused malware warnings have **three main purposes or functions**, which are adapted from Wogalter for safety warnings [Wog06c]:

1. *Communication of important security information*: The aim is to inform users of mobile devices adequately about potential personal malware threats. So users could make informed decisions to protect themselves. That includes the protection of their data on mobile devices against malware threats (e.g. harm of their privacy) or the prevention of potential personal safety impacts (e.g. to their life and limb). Warnings have to call attention to users of mobile devices by using salient design characteristics to realise the adequate communication of security information.
2. *Influence or modify of user's behaviour*: Malware warnings are used to promote users of mobile devices to handle after directives to avoid personal consequences of malware threats and potential malfunctions of coupled systems (functional safety).
3. *Reduce or prevent of personal impacts*: Malware warnings are intended to reduce or prevent negative impacts to personal requirements of users of mobile devices and potential coupled systems, e.g. privacy and personal safety (see personal risk model in section 4.2).

In the following the term '*effective security warning*' is explained and defined. In general effectiveness of warnings is closely related to human-information processing [Cra08] (see security warning literature review in chapter 3). In this thesis an **effective warning** is defined as:

---

<sup>34</sup>Online Oxford dictionary, <https://en.oxforddictionaries.com/definition/warning>, accessed: 17.10.17

'Warning, which is noticed by users, which warning information is adequately comprehended and interpreted by users, and which support users in their security decisions to protect themselves for personal risk of malware attacks.'

As introduced in section 3 warning effectiveness is influenced by users characteristics (e.g. motivation, comprehension), as well as environmental influences (e.g. noise, light), the warning layout (design of the warning appearance, e.g. colours, text, icons) and timing of warning display.

The interaction with a warning is an additional task for users, which often distract users from their primary task, e.g. write an e-mail. If warnings are displayed, users have to interrupt their current task and fulfil the intermediate tasks of reading, comprehension and reaction to the current displayed warning. After interaction with the warning users could continue with their former task. Because users focus on their primary task, users tend to ignore warnings, they are familiar with and they do not comprehend. In this thesis a warning approach is introduced, which want to increase warning effectiveness by using effective warning design characteristics (section 4.3) to support users' comprehension of warning information and users' secure decisions.

### 2.5.1 Security warning types

---

On basis of warning literature and own ideas security warning types are classified by their *characteristics*, *modality*, and *communicated security threat* in this section to make them comparable for their usage. In focus are selected security warning types for non-professional usage. Warnings in complex systems [Mey01], such as in airplanes or trains, are not relevant for this thesis, because this thesis focuses non-expert users not trained expert users in professional environments.

Security warnings in general could be classified by their **characteristics**. Warning literature (e.g., [Cra08]) differentiate in passive and active warnings, which may have different control to interrupt user's primary task and therefore influence to take user's attention. **Active warnings** interrupt the primary task of users and force them to pay attention. As the literature review in chapter 3 show, current active warnings are often poorly understood by users, so most active warnings today are very ineffective. Examples are operating system alerts for prohibited access rights or antivirus warnings. In contrast to active warnings, **passive warnings** are an offer to users, which do not interrupt users' primary task. Therefore passive warnings could be easily ignored and are often poorly understood [SDOF07], which make them very ineffective. Examples are security indicators in browsers, which indicate if the communication between the browser and web-servers is secured (e.g. green lock in current Firefox browser). According to Cranor [Cra08] security system designers have to choose the appropriate warning type, which is the most effective for the desired system. Furthermore, designers should consider the severity and frequency of the hazard/threat, which have to be avoided, to define which user action is necessary to avoid the hazard/threat.

Furthermore, security warnings in general could be differentiated according to their **modality**: visual, acoustical, haptical, or multimodal media usage. Examples are visual warnings (e.g. text and graphics), acoustical warnings (e.g. alarm signals), or multimodal warnings (e.g. combination of visual-acoustic-haptic warning information).

Additionally, security warnings could be classified by the underlying **security threat** they warn for.

**Malware warnings** warn users about potential risk related to malware. A malware attack could risk the whole security of the system in comparison to other cyber-attacks (see methodology of Kiltz in section 2.3.2), which only endanger selected security aspects of the system. Examples are SSL browser warnings and phishing warnings, which are currently the best researched warning types.

Akhawe and Felt [AF13] introduced the differences of most **browser warning types**:

**SSL browser warnings:** The secure communication channel between browsers and web servers based on the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol. SSL browser warnings warn of authentication failures in this communication, could endanger privacy aspects of browser users. These failures could have benign and malign reasons. Exemplary benign scenarios are server misconfiguration, such as self-signing of SSL certificates. An exemplary malign scenario is a man-in-the-middle (MITM) attack, where an attacker established a communication between browser and web-server with full control of the bidirectional data transfer [Eck08]. However, usually browsers cannot distinguish 'benign failures' from a real MITM attack, so false positives could be bypass by users. In cases of SSL warnings bypass of warnings by click-through the warning is in most cases the right decision of users, because nearly 100% of SSL warnings are false positives.

**Browser phishing warnings:** want to prevent users from visiting websites, whose pretend to be serious websites. Phishing websites want to steal users' identity data or other personal data to realise illegal cyber-attacks, such as online-banking or online-shopping frauds. In contrast to most malware attacks against browsers for phishing user interaction is needed. Current browsers using blacklisting of websites, which are known for phishing, based on Google's Safe Browsing list<sup>35</sup>. Browsers do not block detected phishing websites, because the Safe Browsing service could have false positives, although its very low. Most phishing warnings based on Safe Browsing are true positives. So users are recommended to heed these warnings to protect themselves for phishing.

**Browser malware warnings:** want to prevent users from visiting websites, which users' systems could be infected with malware by download of supposed serious software applications or without users' intervention. Browsers also detect malware distributing websites using the further mentioned blacklist of Google and the same non-blocking behaviour of malware websites to prevent blocking of rare false positives. Users also should heed browser malware warnings to protect their systems for malware infection. So malware warnings should be taken more seriously by users in comparison to other warning types, such as SSL warnings. But Almuhimedi et al. [AFRC14] study results show, that *sometimes users confuse browser malware warnings with SSL warnings*, which are often false positives. This is a good motivation to improve the design of malware warnings to make them distinguishable from other warning types.

In this thesis an approach to create *active malware warnings* is introduced in section 4.3. The warning effectiveness of this approach is reached by using a user-group adapted warning design, which includes multimodal feedback to users and information about current personal risk, consequences and instructions to handle the risks.

---

<sup>35</sup>Google transparency report, Safe Browsing: Malware and Phishing, <https://transparencyreport.google.com/safe-browsing/overview>, accessed: 01.03.2018

### 2.5.2 Design guidelines for effective active security warnings

---

This section describes guidelines for the design of effective active security warnings.

As described in the related work discussion (chapter 3) one main disturbing aspect when display warnings is the *habituation effect*. That means, users tend to ignore warnings they are familiar with. Potential reasons are learning effects of the human brain [AVK<sup>+</sup>14] and lack of consequences if warnings are ignored [Ege09]. Exemplary countermeasures against habituation effects are warnings which change their visual appearance, so called polymorphic warnings (e.g.[ECH08, AKJ<sup>+</sup>15]).

Another challenge for warning design is the *comprehension* of warnings. As discussed in chapter 3 the security warning research community is at strife about the importance of warning design for warning comprehension. Many warning researchers (e.g. [DHC06, BLCDK10, ECH08]) found out, that users ignore warnings they do not comprehend. Many researchers recommended the *redesign* of security warnings (e.g. [AF13]). The introduced approach in this thesis is based on an improved malware warning design concept to increase warning comprehension of users (section 4.3). It partly based on the **six design guidelines for security warnings** of Bauer et al. [BBLCF13], which are briefly introduced in this section.

1. *Comprehensively description of risk*: is realised by a clearly specification of the current *risk*, a clearly description of potential *consequences* if not complying with intended course-of-action, and instructions for risk avoidance.
2. *Concise and accurate warning content*: is realised by brief textual descriptions (no redundant texts), usage of users jargon (avoidance of technical jargon), avoidance of ambiguous terms, and usage of a politely, supportive, and encouraging style.
3. *Offer of meaningful options*: includes the presentation of decisions to made (no dilemma) to guide users to make safe decisions. Furthermore, the safest choice should displayed as default option, and the close action should not be labeled with 'OK', 'Close' or 'Chancel'. Instead close buttons should be labeled with a choice, e.g. 'Chancel this update', to make a choice explicit to users. Warning dialogs are defined as dialogs with two or more options, otherwise they are notifications or status indicators.
4. *Presentation of relevant contextual information*: is suggested for processes of access granting and of trust building to unknown/unverified applications and known/unknown agents to known/unknown objects on the system. Furthermore, this guideline include any options, that have been discarded before warnings are displayed. Users should be check the sensitivity of information before sending potential personal information over an unsecured channel. Additional information about a known application can be given with a link to a public online forum.
5. *Presentation of relevant auditing information*: is realised by warning triggering applications, which include information about access grants, access requests, and changes. Warnings should include selected percentages of an audit record.

6. *Consistent layout design*: is realised by:
  - (a) No usage of *close button* in the upper right corner<sup>36</sup>.
  - (b) Only usage of *one icon*, which conveys level of urgency.
  - (c) Shade rest of the screen while presenting the warning and *modal* characteristic, where no interaction with other applications is possible.
  - (d) Usage of a *primary text* with single sentence in newspaper style<sup>37</sup>.
  - (e) Usage of a *secondary text* with more risk information in a conversational style<sup>38</sup>.
  - (f) Position of an *explicit question* immediately above the options.
  - (g) Usage of *two or more options* below the question with brief action descriptions and brief explanatory text.
  - (h) All *options* are designed as *possible answers* to the explicit question.
  - (i) If usage of *technical terms* could not be prevented, the term should be transformed to a link to a pop-up with brief explanation of the term.

In figure 2.4 Bauer et al. also suggest a *warning layout* [BBLCF13]. It is based on a common layout of warnings for three operational systems Windows, Linux, and Apple for software developers. The suggested warning layout includes:

1. A single **icon**, which symbolises the severity level of the warning. The icon is always visible.
2. A **primary text**, which informs about the warning reason. The text is always visible.
3. A **secondary text**, which shows additional information about the warning. The text is initially hidden and only shown when the user clicks on the secondary option 'More information'.
4. A **question**, which is presented to the user. The text is always visible.
5. A set of **primary options**, which are placed one upon the other and presented as command links. The default and safest one should be placed on top of the others. They all include an action description in a larger font, which begins with a verb. These descriptions should be always visible. Furthermore, primary options explain briefly the action in more detail, in a smaller font. The explanatory text is initially hidden and only shown when the user clicks on the secondary option 'More information'.
6. A set of **secondary options**, which do not respond directly to the question in the warning. 'Help', 'Ignore this warning', and 'More information' are the most common secondary options. According to this recommendation the 'More information' should always be displayed to the user. It can be used to switch between showing and hiding specific warning information.

---

<sup>36</sup>A 'close' icon in the warning provides, that the user ignores warning information by closing the warning dialog.

<sup>37</sup>The newspaper style is described as complete sentence, which briefly describes the communicated warning message.

<sup>38</sup>The conversational style is described as an task explanation to the user with the imagination of looking over the user's shoulder.

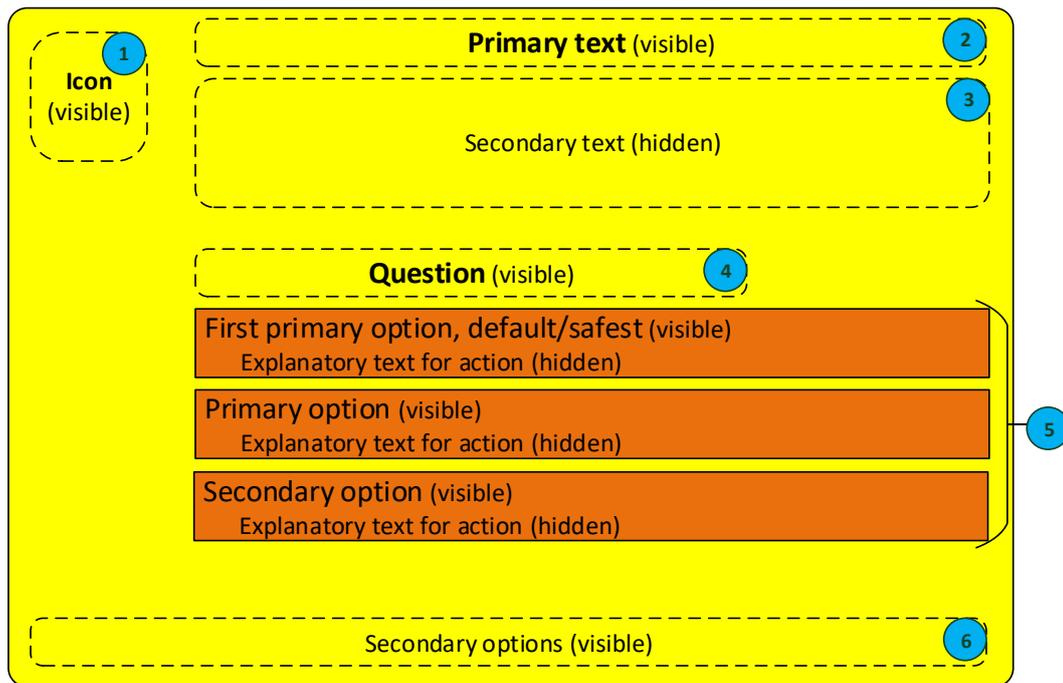


Figure 2.4: Warning design recommendation of Bauer et al. [BBLCF13]

The new warning design concept in section 4.3 based partly on recommendations of Bauer et al. [BBLCF13]. However, for the new warning design some adaption (see table 4.6) have to made to realise effective malware warnings according to the definition in section 2.5 and to fulfil the needs of mobile devices (see sections 4.3.4 and 4.3.5).

### 2.5.3 User-groups

This section describes the differentiation of specific user-groups based on the usability research [PD10], which is also important for warning design. Knowing the characteristics of future users is an important factor to design systems, which are useful for specific user-groups, because the skills and competencies of developers and users often differ strongly. The findings of the usability research are a basis for the new user-group specific warning design approach (section 4.3) and the evaluation concept (section 4.4.3).

A fundamental part to prepare usability user-studies is the *analysis of target user-groups*. User-groups are differentiated according to their skills and their competencies. The user analysis for a usability user-study should determine the group composition: *homogeneous groups* have similar skills and competencies, whereas *heterogeneous groups* differ in their skills and competencies. Depending on the user-group composition the design of user-interfaces could be adapted, e.g. for websites so-called user-group specific views are used. Table 2.3 illustrates the main characteristics of users, which could be determined with interviews or questionnaires [May99]. The table is extended by examples and categorisation of user aspects later used in the concept to evaluate the new warning approach in section 4.4.3.

Characteristic	Examples	Categorisation
Age and sex	Age in years, female/male	Sociodemographics
Education	Profession, field of study, specific trainings	
Cultural area	Semantic of colours and icons	
Familiarisation with computer technology	Desktop PCs, mobile devices	Previous experiences and knowledge
Familiarisation with specific computer platform	Windows, Linux, iOS, Android	
Familiarisation with a specific problem or application scenario	Usage of emails, office programs	
Intensity of usage	Daily/weekly/monthly usage of Internet-enabled devices	
Physical abilities/disabilities	Hearing/deafness, vision/blindness	Capabilities
Mental abilities/disabilities	Literacy/dyslexia	
Motivation for usage	Entertainment, professional usage	Personal interests

Table 2.3: Main user characteristics for usability evaluations (according to [May99])  
 (Note: Extended with examples and categorisation)

**User-group classification according to their previous experiences:**

Depending on the categorised characteristics different user-groups could be classified. For example on basis of *previous experiences* with the system novices, occasional users, experienced users, and experts are differentiated. *Novices* begin to use the system and have to develop a mental model of the system to use it effectively. *Occasional users* use the system rarely, so that they could not develop pregnant usages and they often forget system specifics. Mostly they have no aim to become acquainted with the system, because the familiarisation effort is too high for them. *Experienced users* work frequently and over long periods with the system. Their mental model of the system is highly developed and as far as possible correct. In most cases the efficient usage of system functions is for experienced users more important in comparison to comprehensible labelled control elements. *Experts* are a subset of the group of experienced users. They often prefer to automatise and to individualise functions. In comparison to the other user-groups the expert group is relatively small, but their expert knowledge could help to improve the usability of the system.

### **User-group classification according to their age:**

Another example is the differentiation according to the age. Examples are adults, children, and senior users. The generic warning approach in this thesis is adapted for a user-group specific warning design for the user-group 'primary-school children' (section 4.3.6).

As previously published in [FSRD13] children differ to adults in their thinking. In general they are used to thinking in a world of fantasy and dream of magic [FMD11]. Furthermore, young children have problems reading long and especially complicated texts [Nie10]. Therefore, texts should be short, easy to understand and the information has to be limited. If the children are overwhelmed with too much information, they will easily feel frustrated, lose their concentration on the task at hand [Ber12]. The use of multimedia is appropriate to support the learning process of children [MTF<sup>+</sup>12]. But gender particularities must be observed. Research results of the developmental psychology validate developmental differences in cognitive skills between girls and boys [Ber12]. Girls in comparison to boys tend to have better verbal skills (e.g. spelling, writing, linguistic understanding), while boys tend to have an affinity for techniques resulting in comparatively more interest in the functionality of technical devices [Ber12]. Not only for the design of applications and warnings specific characteristics of children have to be considered. This is also important for evaluation processes (section 2.6.4).

### **User-group classification according to other characteristics:**

In the usability literature there are other classification principles. Examples are the classification according to different *organisational roles* (e.g. students, professors), *individual differences/personality types* (e.g. extraverts, introverts), and *cultural differences* (e.g. Asian vs. European users). These classifications are out of scope for this thesis, but are mentioned in the future work chapter 7. The user-group centred warning approach in this thesis differentiate user-groups based on a generic user (adult with standard literacy, no mental and physical handicaps, and familiar with the European culture), which have variant or extended skills or capabilities in comparison to the generic user (section 4.3).

### 2.6 Evaluation of security warning effectiveness

---

This section introduces the used evaluation methods to measure the effectiveness of the malware warning approach introduced in section 4.3. At first in section 2.6.1 terms and definitions are introduced to ease the understanding of the evaluation topic. The following section 2.6.2 describes relevant aspects of user studies, which are used to evaluate user interfaces as well as security warnings.

#### 2.6.1 Terms and Definitions

---

There exist no specific methods to evaluate security warnings in general and their effectiveness in special. State-of-the-art is the usage of classical methods for evaluating *usability* of human-machine interfaces, also called user interfaces [PD10]. Krol et al. are the first, who publish recommendations to realise robust experimental design of user studies for security and privacy [KSPS16]. Nevertheless, these recommendations based on classical usability evaluation methods. Therefore, in this section usability-specific terms are introduced, which are necessary to understand the warning evaluation.

Generally, usability evaluation is categorised in **formative and summative evaluations** [PD15]:

*Formative evaluations* are realised during the software development. Main aim is to find out the optimising potential for further product development. In comparison *summative evaluations* are at the end of product development and present an overall impression of final product. The test cases of this warning approach are evaluated in a formative form, to get first impressions of first design approaches of the warning concept.

The two common types to **evaluate user interfaces** are *empirically* and *informally* [Nie]. Whereas with empirical usability evaluations real users test the interface, in informal usability evaluations usability evaluators test the interface on basis of rules of thumb and their experiences, called usability inspection methods. If user-centred development of user-interfaces are in focus, empirical studies with representative users are very important [PD15]. Because the warning approach in this thesis focus the user it is evaluated empirical (section 4.4).

There exist different **types of empirical evaluations** [PD15]: Examples are controlled laboratory experiments, usability tests, and field tests. *Laboratory experiments* are very focused on a specific scientific question and want to prove a theoretic hypothesis<sup>39</sup>. They are more used in academic contexts in comparison to industrial context, because of an inappropriate cost-benefit ratio. One example of laboratory experiments are eye-tracking techniques. In *usability tests* participants have to solve specific tasks. These tests are used to evaluate an overall impression of the interface, and rate or improve early forms of designs. The detection of problems are in focus. The amount of test persons is relative small. *Field tests* are performed in realistic user contexts of the developed interface, e.g. in office or industrial environments. In comparison to laboratory tests users could be distracted by their normal work environment.

---

<sup>39</sup>Disclaimer: In this thesis no classical hypothesis testing [BS10] is realised, because of the small samples of test persons. The author wrote this thesis - including the evaluation - from her 'computer science' perspective. She has no education in psychology to realise classical empirical studies in this field. The author has some 'ideas/assumptions' over the evaluation results, which are named 'hypothesis' (see table 4.8). These could be supported or not supported by the evaluation results.

The malware warning approach in this thesis is evaluated with *user studies* in laboratory environments. These evaluation type is used to get an overall impression if the new warning approach is effective. Another reason is a relative small realisation effort.

### 2.6.2 User studies

---

This section gives an overview of basic design aspects, quality criteria, and preparation aspects of user studies.

Mainly different aspects have to be considered while **designing a user study**. In the usability literature [PD15][AT13] basic study design aspects are described: independent and dependent variables, quantitative and qualitative usability factors, hypothesis, and both experimental types 'between subjects' or 'within subjects design'. The evaluation design of security warning effectiveness of the desired approach is described in section 4.4.

- *Independent and dependent variables*: The test should prove how specific independent variables influence dependent variables. *Independent variables* are related to design decisions, which are manipulated by the interface or warning designer. Examples for warning dialogues are the colours of a warning symbol, and the location of buttons. *Dependent variables* are factors, which could be measured. Examples for warnings are click-through rates or preferences of test persons. Dependent variables are also called outcome or response variables, because they symbolise the result of the study.
- *Quantitative usability factors*: are dependent variables and used in summative evaluations for nearly finalised prototypes.
- *Qualitative usability factors*: are subjective criteria<sup>40</sup>. Examples are questioning of test persons in written (*questionnaires*) or verbal form (*interviews*). Structured interviews [PD15] based on questionnaires (QNs) which are filled in by test supervisors during the interview. There are several disadvantages, if test persons fill in QNs alone. They could misunderstand questions or could have less motivation, which often lead to incomplete QNs. These questionnaires are difficult to use for a reliable analysis of evaluation results [PD15] (Note: Design principles of questionnaires are found in section 2.6.3.). Interviews also have several disadvantages. Comments of test persons during the test are notated with a delay in the interview. So participants could forget some aspects. Furthermore, in comparison to QNs interviews need more effort for realisation. For these reasons interviews are often combined with other empirical evaluation methods, for example with *observations*. Verbal comments and user behaviours, called '**method of thinking aloud**' [ES80], are notated in written and verbal protocols (e.g. reading of warning contents).
- *Hypothesis*: declares if for example a design (e.g. layout, colour scheme) is better in comparison to another design. It's a rating of *objective values* (e.g. error rate, learn effort, durations to fulfil a task) and *subjective values* (e.g. usefulness of warnings) on basis of the selection of dependent variables. Where subjective values are opinions of single test persons, objective values are general criteria of a usability evaluation. The usability study has to be designed in that form, that previously defined hypothesis are evaluated with that study.

---

<sup>40</sup>The method (e.g. questionnaires) collect quantitative data of an qualitative attribute, e.g. subjective preferences of users.

- *Experimental types 'between subjects' or 'within subjects design'*: are two different experimental types to compare design variants. In a *within-subjects experiment* all test persons test different variants and the results of all test persons are compared to each other. In the *between-subjects experiment* users are separated in different test groups, which test different designs of user interfaces. Both experimental types have characteristic advantages and disadvantages. The within subjects design has two main disadvantages. First, the order of single experiments could impact results significantly. One countermeasure is the method of *counter balancing* by change the order of single experiments/tasks. Second, these test often lasts longer. In comparison the between subjects design has no such disadvantages, but it is questionable if the observed differences based on characteristics of the tested user interfaces or test persons. In small test groups significant differences of characteristics of test persons (e.g. previous knowledge) could overlay differences of interface designs. One solution is the usage of great amount of test persons, which are randomised distributed in different test groups. Another solution are mixed studies, where between-subjects factors (e.g. gender) and within-subjects factors (e.g. trials distributed over time) are combined.

User studies are often very extensive, so it's important to validate how 'good', reliable, and reproducible user studies are [PD15]. The **quality criteria of user studies** could structure the study design and help to rate the study and its results. Main criteria are:

- *Plausibility* is given, if the study has clear definitions of target groups and foci. So test results are usable and could correlated with test aims. Test persons should match to real users in main characteristics, e.g. age, sex, previous knowledge. But test persons should be independent, which is difficult to realise. Often technophiles are more willing to test technical user interfaces. Furthermore, the chosen tasks in the test should be realistic.
- *Internal validity*: A test should show the influence of independent variables to dependent variables. The dependent variables are also dependent from so called disturbing factors, which could disturb the test results. Examples of disturbing factors are time of day dependent convergence and motivation of test persons, illumination, quality of user interfaces (e.g. display resolution), and concrete selection of users. A main aspect is a clear structured process of introduction of participants into the test. Internal validity is given, if disturbing factors are analysed and limited. Thereby, both strategy of 'keep constant' and 'minimising' are used. Disturbing factors could be kept constant by realise same test conditions for all participants (e.g. same mobile device). Minimising disturbing factors could be realised through equal test groups and changing order of tasks (counterbalancing).
- *Portability/external validity*: is given, if test results are not only plausible but also portable, so similar results are expected in other environments. Experiments in realistic environments, including real future users, are more valid in comparison to laboratory experiments.
- *Reliability*: A reliable study produces in comparison to the compared study, equal results with large amount of test persons or longer test duration. If test groups have homogeneous characteristics reliable results could be realised with less amount of participants. If test persons differ in various different personal characteristics significant more participants are necessary.

According to Preim and Dachsel [PD15] a study could not realise all criteria, so prioritisation and documentation is essential. Information about quality criteria for the both test cases in this thesis are found in section 4.4.1.

The **preparation of empirical evaluations** [PD15] has to consider which aspects influence the measure of security warning effectiveness. Particularly, disturbing factors which could decrease the validity of test results have to be reflected. Preim and Dachsel [PD15] list several aspects for user study preparation, which are supplemented by recommendations for security user studies of Krol et al. [KSPS16] (bold printed terms). Here only relevant aspects for this thesis are introduced:

- *Selection of test tasks*: is important during the test preparation. The tasks are used to focus the test, find vulnerabilities or impose quantitative values. The tasks should be realistic, that test results are portable to practice. Furthermore, tasks should be chosen that tests last not too long, because test results could be biased by tired and unmotivated participants. In warning experiments a **primary task** is important to create a real scenario, where the user is busy with his main task and a warning interrupts user's primary task. Another important design principle for security experiments is the introducing of a **realistic risk** to participants. Because participants behave differently in situations that are simulated and appear not realistic (e.g. laboratory study with no usage of users' technical equipment [SDOF07]).
- *Aims and hypothesis*: An aim defines what should be reached with this study. In comparison to an aim a hypothesis is an assumption, that the aim will be reached. Whereas aims are often used in practical developments, hypotheses are used in scientific environments, where statistical analysis should prove that a new warning design is better in comparison to a past design. In this thesis no classical hypothesis testing [BS10] is realised<sup>41</sup>, because of the small samples of test persons. The author has some 'ideas/assumptions' over the evaluation results, which are named '*hypothesis*'. These could be supported or not supported by the evaluation results.
- *Involved persons*: The amount of involved persons in a user study depends on the specific test and its environment. If minors, such as primary school children, are test persons the *parents* have to agree by filling so called letters of agreement. If classrooms are used for tests, also *school headship* has to be involved and has to agree (section 5.2.3). Furthermore, *technicians* have to be included, if technical infrastructures are used, for example, to install an online questionnaire. For security research Krol et al. suggest to realise **double blind experiments**, where neither participant nor tester know details of the study. This should minimise the capacity of influence of study outcomes.
- *Test guideline*: includes the most important information regarding the planned test. Contents of test guidelines are the evaluated usability aspects, evaluation methods, and the selection procedure of test persons. Parts of the test guideline, such as description of application scenario of warnings and single test tasks, are also given to the participants.

---

<sup>41</sup>Disclaimer: The author wrote this thesis - including the evaluation - from her 'computer science' perspective. She has no education in psychology to realise classical empirical studies in this field.

- *Role of moderator*: A moderator is important for the successful result of the study. Typical tasks of the moderator are welcome and obliging handle of participants, introducing and explaining the test as far as possible, and creating a constructive working atmosphere. In most test cases for security warnings, it's common to keep the real aim of the test secret to test persons to obtain internal validity (**Avoidance of priming** of participants).

### 2.6.3 Evaluation methods and metrics to measure warning effectiveness

---

This thesis focuses on *effectiveness of warnings*, which is related to human information processing. So focused evaluated issues are *comprehension of warning information* and support of users' *behaviour or reaction* after reading warning recommendations. There are different metrics in usability literature [PD15, AT13], which could be used to measure the effectiveness of security warnings. Both, objective values (usability values, e.g. durations) and subjective values (opinions and behaviour of single test persons), could be used to measure security warning effectiveness.

**Subjective values** could be measured with so called *self-reported metrics* and *behavioral metrics* [AT13] about users' perception of the warning and users' influenced behaviour by warning instructions. Self-reported metrics are measured for example with **questionnaires**.

#### *Self-reported metrics - questionnaires:*

Standardised or adapted questionnaires are often used to rise opinions of test persons in a structured form. For evaluation of user interfaces standardised questionnaires are used. Exemplary questionnaires to evaluate characteristics of interactive systems are ISONORM and ISOMETRICS<sup>42</sup>. Questionnaires to measure the satisfaction of users during interaction with software are QUIS<sup>43</sup> and SUMI<sup>44</sup>. In [HZGH<sup>+</sup>10] a standardised questionnaire to collect *sociodemographic characteristics* is published. For evaluation of effectiveness of security warnings above described standardised questionnaires for usability are not usable, because it do not cover question categories, which have to evaluated to measure warning effectiveness. Main reasons are the different evaluation methods to measure the usability of interactive systems with focus on users' tasks in comparison to warning effectiveness with focus on human information processing. But selected questions of standardised questionnaire for sociodemographic characteristics [HZGH<sup>+</sup>10] are usable. Therefore, an own questionnaire on basis of [HZGH<sup>+</sup>10] is created (section 4.4). Because of the great technical effort the self-created question categories are not clarified in the context of test theory [MK07]. Furthermore, no data exist which prove the objectivity, validity, and reliability of these new question categories. But the new questionnaire is developed in teamwork with test theorists and also evidently proved by them<sup>45</sup>.

---

<sup>42</sup>ISOMETRICS questionnaire, University of Osnabrück, <http://www.isometrics.uni-osnabrueck.de/>, accessed: 23.20.17

<sup>43</sup>QUIS questionnaire, University of Maryland, <http://lap.umd.edu/quis/>, accessed: 23.20.17

<sup>44</sup>SUMI questionnaire, University of Cork, <http://sumi.uxp.ie/>, accessed: 23.20.17

<sup>45</sup>The new question categories are developed with help of psychologists Dr. Knuth and Dr. Kuhlmann from the Otto-von-Guericke University of Magdeburg.

In the psychology literature the construction of questionnaires are introduced. The questionnaires in section 4.4.3 based on recommendations of Moosbrugger and Kelava [MK07]. The questionnaires include the best suitable response types to measure warning effectiveness (definition in section 2.6).

Questionnaires are based on questions or hypothesis and corresponding response formats. Response formats are classified by their level of structuredness. They could be non-attached, bounded, and atypical.

In *non-attached responds* no response alternatives are specified. Responders have to find the answer of their own. A challenge is the coding of the different answers of responders according to a previous specified system of categories. Two typical task forms of non-attached response formats are *short essay tasks* and *completion tasks*. **Short essay tasks** facilitate participants to give creative responses. Therefore, it is best suitable to measure if test persons comprehend warning message information, give comments to warning design, their previous experiences, and their sociodemographic background. In short essay tasks test persons have to answer maximum with a short essay and minimum with a single sentence or word. The responders of short essay tasks have to reproduce knowledge and self-create responds, respectively. Therefore, randomly correct responds such as in selection tasks are not possible. Main disadvantages are the big processing effort for respondent and assessor, restricted assessment objectivity, and ambiguity of responds.

Because of their structured characteristics *bounded response formats* are more easy to analyse in comparison to the two other types. Two typical task forms of bounded response formats are *selection tasks* and *rating tasks*. Bounded response formats are best suitable to measure all kind of evaluated items in a structured form. Therefore, both bounded response formats are used in questionnaires in section 4.4.3 and are briefly introduced in this section.

While answering **selection tasks** test persons had to choose the suitable response from several alternatives. Moosbrugger and Kelava [MK07] classified them in:

- *Dichotomous tasks*: provide two response alternatives (e.g. yes and no). Main advantages are their simple construction, response, and analysis. Main disadvantages are the 50% guess probability and acquiescence of test persons.
- *Multiple choice tasks*: offer several response alternatives, where test persons have to select the hypothesis, which they think is right or which are apply to them personally. Multiple choice tasks have to be constructed that the respondents are able to make a choice. Examples are instructions 'Select a response alternative which rather than anything else apply to you!'. In comparison to dichotomous tasks multiple choice tasks are equally simple, economic and objective in realisation and analysis. The guess probability decreases because of different response alternatives. Main disadvantages are that test persons only recognise the correct responses, and the questions include clues for the right response.

In **rating tasks** respondents give a response in form of agreement or disagreement to a hypothesis. Main advantages of rating tasks are the simple handling and analysis, and very short respond time for test persons. The design of rating categories is very challenging. For analysis the scale levels (e.g. ordinal scale, interval scale) have to be considered, if rating categories are labelled with numbers [BS10]. According to Moosbrugger and Kelava [MK07] *six design aspects* have to be considered for the response format of rating tasks:

1. *Scale levels*: are related to the complexity of the rating scale. In general two scale level categories are distinguished: continuous analogue scales and discrete rating scales (figure 2.5). Main advantage of *continuous analogue scales* is the complexity for test persons to express their opinion. But in reality analogue scales are rarely used, because complexity of rating not correlates to the complexity of opinions. *Discrete rating scales* visualise graded scale points. They also known as *Likert scales* [Lik32]. Commonly scales with maximum seven levels are used, because humans could not process more information. So respondents tend to choose levels which are divisible through 5 or 10 in scales with many scale points. Discrete rating scales are very common to measure attitudes and meanings of test persons. Every response is weighted after a previous defined scheme. So every response get a specific score.
2. *Polarity of response scale*: could be categorised in unipolar and bipolar (figure 2.5). An unipolar scale has a reference point (zero point), which symbolise the minimal level of agreement (or disagreement) as well as a positive (or negative) pole, which symbolises the strong agreement (or disagreement). The intensity or level of agreement (or disagreement) only increases in one direction. In comparison to unipolar scales bipolar scales have two poles, one for strong agreement and another for strong disagreement. The usage of the two response scale types is dependent on the characteristic, which is desired to measure.
3. *Labelling of scale points*: could be realised in forms of numbers, words, optical, symbols, or combinations of different forms. *Numeric scales* are marked with numbers, which seems to be a precise measure and interval scale. But similar intervals between scale points are often not correlated with similar intervals of opinions of respondents, because test persons sometimes interpret numbers different to the desired design. *Verbal scales* are marked with words. The interpretation of scale points tend to be more similar for all test persons, because test persons do not have to guess what single scale points mean. Test persons are more satisfied if not only extreme values, but also other scale points are described with words. But is very difficult to label every scale point with a word, which symbolises equal scale intervals. *Optical and symbol scales* use graphics or symbols, such as rectangles or icons with plus/minus labelling. Their interpretation is not dependent on verbal labelling. *Combined scales* combine different labeling forms. Examples are verbal-numeric scales and optic-numeric scales. It's important that the labelling corresponds with the numbers to ease their interpretation.
4. *Neutral middle category*: Test persons tend to mark neutral answers as avoiding option. There are different reasons for that phenomena: test persons rate wording as improperly, do not understand the question, deny response or do not know a response. Motivated respondents avoid using the neutral middle category. So if the neutral middle category is used test results are not clear, and the interpretation could be distorted. Therefore, the neutral middle category is not recommended by Moosbrugger and Kelava [MK07].

## 2.6. Evaluation of security warning effectiveness

5. *'No hypothesis' category*: is added to response scales to minimise the negative effect of a neutral middle category. So the neutral middle category has the function of the middle of rating scale and is not misused if respondents have problems to respond to questions.
6. *Asymmetric rating scales*: are used if it's probable that test persons will not use a complete symmetric response spectrum. Examples are ratings of general positive or negative con-notated aspects, which do not need a bipolar rating scale and do not find differences in rating. A variant of asymmetric scales are item specific response formats, whose categories are asymmetric adapted to item contents. Typical examples are rating scales to evaluate previous experiences, such as using of the Internet (figure 2.6).

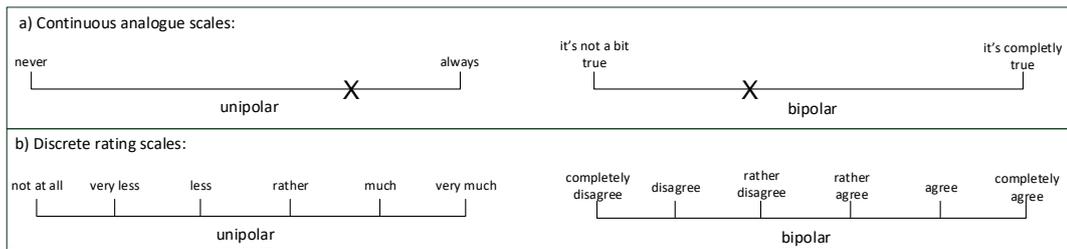


Figure 2.5: Unipolar and bipolar scales in continuous analogue and discrete rating scales (according to [MK07])

After Moosbrugger and Kelava [MK07] there exist no general rules how a questionnaire for a specific research question have to designed with specific combinations of response formats. Response formats could be combined in questionnaires, but not all results of different response formats could be summated and analysed. Examples are question categories which combine dichotomous selection tasks and rating tasks. According to test theory these ratings should not combined with each other, because the margins of the normal distribution are increased, which could falsify test results [MK07].

[Q14] How often you use the Internet?  
Please select only one response:

- several times a day
- once a day
- several times a week
- once a week
- occasionally
- rare till never

Figure 2.6: Example of an asymmetric response scale (Questionnaire excerpt for test case adults, section 8.1.2)

The questionnaires in this thesis in section 4.4.3 are combinations of short essay tasks, selection tasks (dichotomous, and multiple choice tasks) and rating tasks, because they are the best suitable response formats to measure criteria of warning effectiveness.

Beside test persons opinions in questionnaires subjective values could also be measured the behaviour of participants during the test. These are called behavioural metrics. One simple method to collect behavioural values are observations.

*Behavioural metrics - observations* [AT13]:

Behavioural values could be categorised in verbal and non-verbal behaviours. *Verbal behaviours* are anything test persons pronounce. *Nonverbal behaviours* include all things test persons do. Tullis et al. [AT13] recommend to prepare a *structured protocol* before the test, which evaluators could use during the test to write down observed participant's behaviour. Examples for the both test cases are find in the appendix (sections 8.1.4 and 8.2.3).

*Verbal behaviours* provide information about test person's emotions and mental state while interacting with the warning. A method to motivate participants to verbalise their thoughts is called 'method of thinking aloud' [ES80]. Typical metrics to classify verbalisation of participants is the measure of their 'positive' and 'negative' comments. All other comments that are neutral or difficult to interpret are classified as 'neutral'. Tullis et al. [AT13] also recommend a differential classification of verbal behaviours, such as suggestions for improvement, questions, variation from expectation, stated confusion or lack of understanding, stated frustration.

*Nonverbal behaviours* can be good indicators how participants could handle the warning. Examples are facial expressions (e.g. smiling, surprising, frowning) or body language (e.g. fidgeting, scratch the head). It's very challenging to derive meaningful metrics from these non-verbal behaviours, but it could be very helpful to find problems while users interact with the warnings. Some of non-verbal behaviours need specific equipment to be captured. Examples are facial expressions recoded with video techniques, and eye movements with eye-tracking techniques. Detailed body movements could be captured, but the realisation and analysis could be very extensive.

**Objective values** are general criteria of a usability evaluation, which express specific dependent usability factors. One example is the *effectiveness*, which is the ability to successfully complete a task - in our case the reading, comprehension of warning information and behaviour after warning instructions. *Log-information* of user interactions is often useful to measured how often and in which relation functions are used, and how they are differ. Privacy protection laws have to considered, and therefore anonymisation methods have to used. Reading of warning information could be measured with logging of users' interaction with the warning, e.g. clicking of buttons. But logging is not sufficient to measure reading of warnings. Therefore, additional evaluation methods such as questionnaires and observations have to be used.

### 2.6.4 Children specific user tests

---

This section introduces specific aspects of user tests with children, because one test case of the security warning approach was developed for *primary-school children*, aged 7 till 11 (section 5.2.3) and children are different in their cognitive and physical development in comparison to adults [BB02] (section 2.5.2). This section includes preparation of user test, selection of test environment, children specific evaluation methods and guidelines.

Usability tests are a challenging task for children, because they have several other tasks to do beside the handling of the test object. Examples are familiarisation with the test environment, interaction with the supervisor, and speak out of their thoughts loudly [LE11]. Hence social skills, adequate communication strategies and careful formulation of tasks are more important in tests with children in comparison to adults [MBG07].

#### *Test preparation:*

The preparation of the test includes decisions about amount of *test persons* and their demographic and required characteristics. Nielsen [Nie94] claimed that three till five test persons are enough to find 80% of main usability problems of a software product. Barendregt et al. [BB05] recommended minimum eight participants for tests with children. But in tests with younger children the amount of participants has to increased, because the loss of participants have to take into account. Reasons could be development deficits and less motivation of children [MBG07]. Furthermore, the differences regarding experiences, age, and sex have to take into account.

Regarding *experience differences* Hanna et al. [HRA97] recommend to select participants with minimal experiences of 6 months with input and output media, such as mouse, because of the limited time in usability tests, where no intensive technique introduction is possible. Furthermore, children with computer experiences above average should excluded from tests, because they not represent the populace. Additionally, own children and children with parents in IT professions should not participate the test, because they have extensive experiences with technical problems, and could inhibited to clearly comment their parents product [MBG07]. Children also have different capabilities and skills depending on their stage of *age*. Two- till five-year-old could poorly concentrate, are easy distractable, could feelings less verbalise, and could not follow permanent instructions from supervisor. In comparison older children six-till ten-year-old could easy integrated into tests, because their ability to concentrate on one specific task is much higher. But they also have problems to verbalise their impressions and feelings. Children till eleven years could participate in usability tests without problems, because they only slightly differ in comparison to accrue participants [LE11]. But also *sex differences* has to considered. Recommended are an equal distribution of sexes. Usability problems are equal for girls and boys, but they differ significantly in their interests [MBG07]. So user-interface designers have to consider for boys different contents and design of user-interfaces in comparison to girls [LE11].

#### *Selection of test environment [LE11]:*

In general two test environments are categorised: familiar environment (e.g. kindergarten, school), and usability laboratory. It is recommended to prepare the selected environment suitable for children, because it could strongly influence the psyche and thereby the test results. Children are more confident in *familiar environments* in comparison to laboratory environments.

Therefore, they explore more usability problems. Tests should not influence the typical daily routine, including the lessons. Main disadvantages are variable disturbances, such as noise of playing children or interruptions through teachers and educators. Furthermore, evaluation equipment has to be setup and dismantled. Additionally, several permissions regarding the test execution are obtained, for example from headmasters, and responsible agencies (only for public institutions), and parents of children. The main advantage of *laboratory* test environment are the constant disturbances for all test persons, which allows a better comparison of test results. Furthermore, technical equipment, such as cameras, are present and setup and dismantling is not applicable. In comparison to familiar environments, such as schools, amongst permission of parents also their attendance is necessary, which is often a great organisational effort. Potentially the unfamiliar environment could discourage or frighten children, that they do not want to evaluate the product self-reliant. The usability of user-interfaces is well compared and assessed, if a test series is realised in one of the introduced test environments.

*Methods* [LE11]:

Hypothesis and comments of test persons in usability test are the most important resource to identify usability problems. Specific methods are verbalisation, non-verbalisation and miscellaneous techniques. Liebal et al. [LE11] introduce *five verbalisation techniques* for children, whereas in two of them two children work together:

1. *Method of think aloud* is the most known technique for verbalisation of usability problems. Children have to speak out loudly their thoughts and feelings during the test. The concentration on the test task and simultaneously verbalisation of thought is a double cognitive overload especially for younger children. So children often could only fulfil one of both task. Additionally, children often feel unnatural to speak without a contact person. One recommendation is to request children, if they forget verbalisation.
2. *Active intervention*: The test supervisor interviews the child during its work on test tasks about her procedure. The questions are prepared and task-specific designed before the test. The main advantage in comparison to think aloud method is less cognitive overload through verbalisation of thoughts. Children have to be pointed out, that they are questioned during the test.
3. *Retrospection*: The test is recorded via video camera and analysed together with the child. The test supervisor interviews the child during watching the video about its interaction and problems with the product. Here the children has a less cognitive overload during the test, because of omitted through verbalisation. But children younger then 11 age have problems to follow the start of their thoughts. So they often do not remember after the test, what they thought during the test. Furthermore, this method is very time consuming, because it lasts twice as long as the original test.
4. *Codiscovery*: Two children solve the test tasks together in a team. The idea is to benefit from natural way children communicate with each other. Before the test children have to instructed, that is important to solve the task together, and not important which of both children is the best. Therefore, both children get separated different tasks, which are only solvable in a team work. According to developmental psychology [Pia70] children aged 6 or 7 are able to cooperate. But during usability tests Kesteren et al. [VKBVLO3] observed that each child work alone on its task.

5. *Peer tutoring*: is exclusively developed for usability tests with children. During the peer tutoring the child gets through two test procedures in two different roles: as tutor and tutee. In the first test procedure the child as tutee solves the test tasks, and could be familiar with the product. In the second procedure, the child as tutor explained another child how the product works and how it has to interact with it. Main advantages are the natural talk between tutor and tutee in comparison to thinking aloud, and the divided cognitive overload between two children.

According to Kesteren et al. [VKBVL03] suggest *active intervention* as effective usability evaluation technique for children, because of most effective proportion of amount of verbalisation, time efforts, and amount of test persons. But children have more fun during the *peer tutoring*, which is an important factor in usability tests with children [HHT03].

*Nonverbalisation techniques* are used especially for younger children, which have problems to verbalise their opinions about a product. One example is the *picture cards method*. On each card a different icon is printed, which symbolises a different feeling or usability problem. Exemplary icons show faces that are bored, has fun, find something difficult, and think something takes too long. During the test children could choose a card and put it in a specific box. After the test in the video analysis the supervisor could clearly identify a specific problem on basis of these cards.

*Miscellaneous techniques* are observations and post-task interviews. *Observations* are useful to identify negative emotions of children expressed by their body language and mimic, because children tend to give positive verbal feedback. *Post-task interview* is an interview after the test in which a post-test questionnaire is used. It's a similar technique to retrospection.

In this thesis the evaluation of the test case for children (section 5.2.3) methods of thinking aloud in combination with active intervention, and observation are used. Because these techniques are effective evaluation methods and useful in a classroom test environment.

Usability researchers recommend some *guidelines for tests with children* [LE11]. Examples are:

- *Make contact to the child*: by asking for things the child likes, e.g. TV series or hobbies. This reduces the stress for the child during the test situation. Communication should on the same level with the child.
- *Explaining the test situation to the child*: The child should explained that only the software is tested, not children's efforts. A small prepared structured protocol for introducing the child into the test is helpful.
- *Motivate older children*: with highlighting their role as tester or researcher. It could be explained that the help of the child is very important to improve the software, because the supervisor do not remember what children prefer.
- *Give assistance*: If children fell unconfined they often ask very quickly for help. The child has to be motivated to try it again or tried to request a counter question.
- *Praise the child*: During and after the test the child has to be praised, because it raises its motivation. It should be highlighted how important its collaboration is.
- *Do not pass one hour*: Children could get tired after some test time. Hanna et al. [HRA97] recommend for older children (primary school children) a short break after 45 minutes.
- *Prepare the child for end of the test*: Sometimes its difficult for children to find to an end, e.g. if games are tested. Therefore, supervisors should define an aim before test beginning starts.
- *Give small thank-you gifts*: Children are glad to get a small gift after the test, that represents their successful work as product testers. Additionally, it raise their motivation during the test, if it's communicated to them before the test starts.

The above introduced guidelines are considered in the test case for children in this thesis (section 5.2.3).

## 2.7 Statistical analysis methods

This section introduces the statistical fundamentals, including the statistical analysis methods, which are used to analyse the evaluation results in this thesis in chapter 6. The contents of this section mainly based on the book of Bortz and Schuster [BS10].

### Sample size:

In the statistical literature different statements about the size of a sample are made to assume a normal distribution. Often a sample size larger than 30 is mentioned. Due to resource limitations both warning instances in this thesis are evaluated with sample sizes lesser than 30. Therefore, the results are represent only tendencies, which are not generalisable for the whole population.

In the literature the analysis methods are differentiated in descriptive and inference statistical analysis. **Descriptive analysis** summarises and arranges the results of an evaluation with tables, statistical values and diagrams to better overview the evaluation results (see sections 6.1.1 and 6.2.1). In comparison to the descriptive analysis the **inference statistical analysis** want to prove on basis of previous defined hypothesis that the test results are generalisable for a larger population. In this thesis no classical hypothesis testing is realised, because of the small samples of test persons of both test cases (adults: 23, children: 13 participants). The author has some 'ideas/assumptions' about the evaluation results (table 4.8 in section 4.4.1), which are named 'hypothesis', but these are no classical hypothesis. These could be supported or not supported by the evaluation results. Inference statistical analysis methods<sup>46</sup> are used in this thesis to show tendencies for realistic effects, and correlations of evaluation results. Two different analysis types are used: Cohen's d effect size, and the single- and two-sided correlation according to Pearson.

**Cohen's d effect size** is a reference for practical relevance of test results. It is applicable for small sample sizes of independent samples. There exists different calculations of Cohen's d depending on the standard deviation of an attribute in different samples. The Cohen's d effect size is calculated for results of test case 1 (mobile robot warnings for adults). Before Cohen's d is calculated the outliers are removed from the data set to prevent a falsification of the results. All values are eliminated from the data set, which lay over the threshold in formula 2.1. (Note:  $\bar{X}$ : mean value,  $s$ : standard deviation of one group):

$$threshold = \bar{X} + 2 * s \quad (2.1)$$

<sup>46</sup>Due to the small sample size in both test cases a test of significance of differences with a t-test is not realised.

After the outlier elimination Cohen's d is calculated. If the standard deviations of both test groups, experimental group (EG) and control group (CG), were approximately homogeneous Cohen's d effect size is calculated with Cohen's formula 2.2 [Coh77]. In cases, where the standard deviation of the test results of both groups are not homogeneous, the Cohen's d formula 2.2 is calculated with the formula 2.3 for joint variance after Bortz [FEPS09]. (Note:  $\bar{X}$ : mean value, s: standard deviation of one group):

$$d = \frac{(\bar{X}_{EG} - \bar{X}_{CG})}{s} \quad (2.2)$$

$$s = \frac{\sqrt{s_{EG}^2 + s_{CG}^2}}{2} \quad (2.3)$$

The **bivariant correlation according to Pearson** measures if there's a linear relationship between two specific attributes, e.g. rating of warning comprehension and desire for additional help. Differentiated are two-sided and one-sided correlations according to Pearson. Whereas a '*two-sided*' significance test verifies a non-directional hypothesis (e.g. attribute a and b are different), a '*one-sided*' significance test verifies a directional hypothesis (e.g. attribute a is larger than attribute b). The two-sided correlation is used for test case 1 (mobile robot warnings for adults) to find correlations between attributes with no specific hypothesis. The one-sided correlation is used for test case 2 (smartphone warnings for primary-school children), because several directional hypotheses exists.

# 3

## Related Work

This chapter describes the scientific work related to the introduced warning approach. It is related to research objective 3 (section 1.3).

### **RO3: Design of a general user-group specific effective malware warning concept for mobile devices.**

The main research questions are: 'Which existing warning methods and concepts can be used for the destined approach? Which novel concepts and methods have to be created to fulfil the desired requirements of the intended approach?'

#### **Literature search methodology:**

The research field of computer security warnings is relatively young. Most papers are published in the second decade of this millennium (see table 3.1). Due to the lack of an appropriate literature review paper an own literature review is realised in February 2018 on four common scientific databases: IEEE Xplore<sup>47</sup>, Scopus<sup>48</sup>, Springer link<sup>49</sup>, and Web of Science<sup>50</sup>. Search queries were combinations of the terms security, malware, mobile, cyber, risk, computer and the terms warning, dialogue, message, and communication. Furthermore, the articles are filtered whether their content is related to the research topic of this thesis. That includes research topics related to *active security warnings for non-expert users*. Furthermore, articles are selected which include security warning research topics for *mobile devices* or *cyber-physical systems*, warning designs which communicate potential *personal impacts* of the warned attacks, and whether they evaluated their approaches with user studies.

Afterwards, the filtered articles are categorised in three different classes: First, related work regarding the reasons why users ignore warnings (section 3.1), second, *malware warning approaches* (section 3.2), third, *other relevant research work* related to the introduced approach different from the classical security warning research field (safety, automotive security, mobile robot IDS) (section 3.3). Table 3.1<sup>51</sup> illustrates the results of the filtered literature research arranged by their classification and highlights the differences and similarities of related work warning approaches against characteristics of the new warning approach.

---

<sup>47</sup>IEEE Xplore, Digital Library, <http://ieeexplore.ieee.org>, accessed: 22.02.18

<sup>48</sup>Scopus, <https://www.scopus.com/>, accessed: 22.02.18

<sup>49</sup>Springer link, <https://link.springer.com>, accessed: 22.02.18

<sup>50</sup>Web of Science, <https://webofknowledge.com>, accessed: 22.02.18

<sup>51</sup>Due to economic reasons only the first author of the publication is shown in the table.

First author and reference(s)	Type of security warning	Non-experts	Multi-modality	Personal risks	Personal consequences	Instructions
<b>Redesigned warnings</b>						
Almuhimedi [AFRC14]	Browser malware (Chrome)	+	Visual	-	-	-
Modic [MA14]	Browser malware	+	Wording	-	-	-
Akhawe [AF13]	Malware, phishing, SSL (Chrome, Firefox)	+	Visual	+/-	+/-	-
Silic [SBO15]	Browser malware	+	Visual	+/-	+/-	Options
Bauer [BBLCF13]	Security applications	+	Visual	-	-	Options
Bravo-Lillo [BLCD+11]	Browser and e-mail	+	Visual	-	-	Options
Krol [KMS12]	Browser	+	Visual	-	-	Options
Bravo-Lillo [BLKC+13]	Browser	+	Visual	-	-	Options
Sunshine [SEA+09]	SSL (Firefox, IE)	+	Visual	+/-	+/-	+/-
Felt [FAR+15]	SSL (Chrome)	+	Visual	+/-	+/-	-
Egelman [ECH08]	Phishing (Firefox, IE)	+	Visual	+/-	+/-	Options
Egelman [ES13]	Phishing (IE)	+	Visual	+/-	+/-	Options
<b>Polymorphic warnings</b>						
Brustoloni [BVS07]	Email malware (Thunderbird)	+	Visual	-	-	Options
Jenkins [JKB+18]	Mobile privacy permission	+	Visual	Privacy	+	Options
<b>Individualised warnings</b>						
De Keukelaere [DKYT+09]	Email	+	Visual	-	-	Options
Bartsch [BV13, BVTK13, BV14]	Browser	+/-	Visual	+	+	Options
<b>Warnings with personal risks</b>						
Kauer [KPV+12]	SSL	+	Visual	+	+	-
Harbach [HHWS14]	Smartphone permissions	+	Visual	Privacy	+	-
Malkin [MMHE17]	SSL	+	Textual	+	+	Recommendation
<b>Safety warnings</b>						
Wogalter [Wog06b]	Static	+/-	Visual	+/-	+/-	+
Meyer [Mey01, Mey04]	Dynamic	-	Visual	+/-	+/-	-
<b>Automotive security warnings</b>						
Tuchscheerer [TDHK10]	Static	+	+	Privacy	-	-
Hoppe [HD14]	Static	+	+	Privacy	-	-

Table 3.1: Comparison of related warning approaches against characteristics of the new warning approach  
(Note: +: fully implemented, +/-: partly implemented, -: not implemented)

### 3.1 Why users ignore warnings

Camp [Cam09] criticised in the year 2009 that the methods of risk communication have to be applied to computer security. Since this time lots of warning approaches are developed and tested with users. But these warnings are often ignored by users. Angela Sasse [Sas15] appeals for do not bulling users with warnings and rethink the usage of warnings. Beside the bad warning design and inappropriate usage of warnings, the reasons why users ignore security warnings are manifold. Most<sup>52</sup> are associated with the human-information processing and processes of decision making, but also bad user study design. Therefore, the following section is divided into two parts. In *part A* the *reasons* for humans' warning ignoring are presented using the structure of Cranor's human-in-the-loop security framework, which models human information processing [Cra08]. Furthermore, *warning solution approaches* against ignoring of warnings are presented. Figure 3.1 illustrates the related work mapped on the parts of human-in-the-loop security framework of Cranor [Cra08]. Related work regarding the *reasons why users ignore warnings* are symbolised with yellow boxes in figure 3.1. Scientific work for *malware warnings* are marked with red frames in figure 3.1. Warning solution approaches are classified in warning redesign, polymorphy, and individualised warnings illustrated as green boxes in figure 3.1.

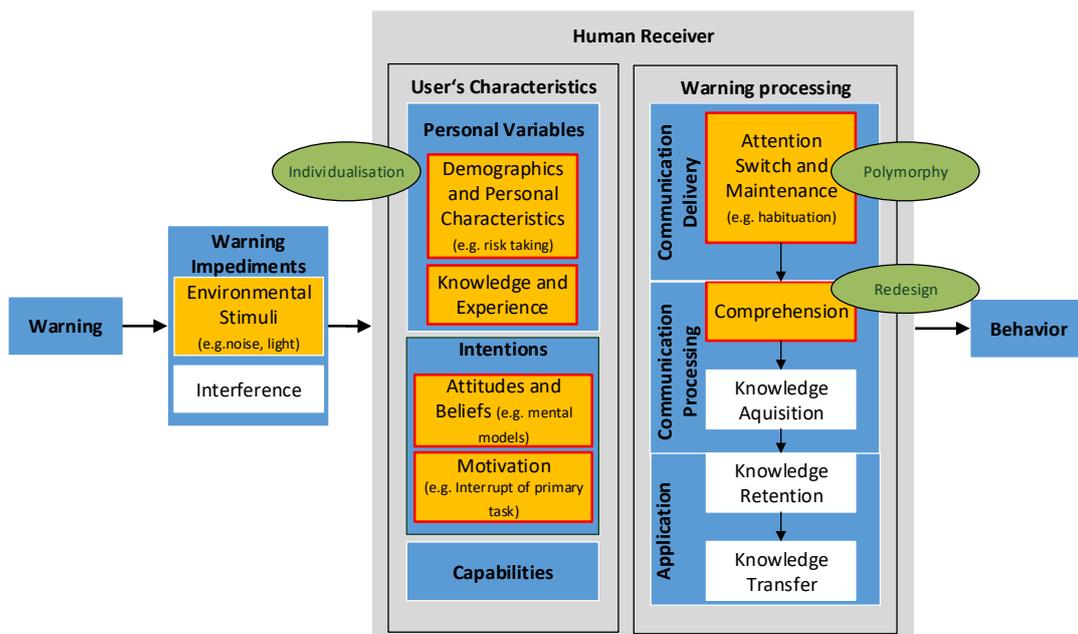


Figure 3.1: Related work field regarding 'Warning ignoring' (yellow boxes), warning approaches against the ignoring (green ovals), and malware warning research (red frames)

(Note: Adapted human-in-the-loop framework of Cranor for warnings [Cra08])

Amongst the described reasons some researchers hold invalid user study design responsible for observed security inattentive behaviour of test persons, e.g. ignoring of warnings [KMS12]. Related scientific work regarding study design are presented in the *part B* in section 3.1.2.

<sup>52</sup>Note: Due to lack of malware warning approaches findings of other security warning types, e.g. SSL warnings, are described in this section. Scientific work regarding malware warnings are described in detail in section 3.2.

3.1.1 Human-information processing

There are several models of human-information processing, such as the C-HIP model of Wogalter [Wog06a] or HITL of Cranor [Cra08], which included Wogalters C-HIP model. The HITL model of Cranor is introduced in section 2.4. It models the internal processing in the human brain of communications, such as warnings. Relevant communications in this thesis are *active security warnings*. Amongst the individual processing of warning information impediments, such as environmental stimuli and interferences, also user characteristics might impact user's behaviour regarding warnings. In the following, main reasons for ignoring warnings are systematically described with related works categorised with Cranors' model.

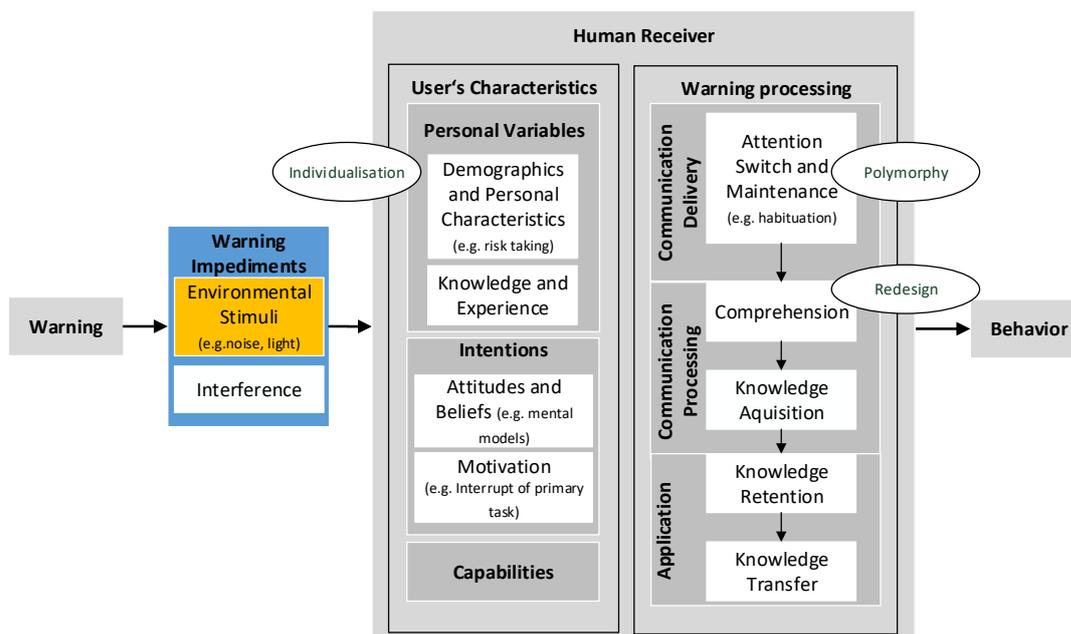


Figure 3.2: Related work field for 'Warning impediments' (coloured box) (Based on [Cra08])

**Distraction (Warning impediments):**

According to Cranor's model users attention could be distracted by their primary task, environmental stimuli (e.g. noise, ambient light), and other interferences (e.g. malicious attackers, technology failures). Several of the available security warning articles make users' focus on their *primary task* responsible for distraction from warnings (e.g. [BLCDK10, Her09, AVK<sup>+</sup>14, Sas15]).

Amongst the focus on their primary task users also could be distracted by *environmental stimuli*, such as noise, and ambient light. But most experimental studies took place under laboratory conditions due to economic reasons and to have stable environmental conditions for comparable results. Nevertheless, there are only a few studies, which evaluate security warnings under realistic conditions. Exceptions are large field studies of Felt et al. [AF13, FAR<sup>+</sup>15] for Google Chrome SSL warnings and Jenkins et al. [JKB<sup>+</sup>18] for privacy permission warnings on mobile devices.

To the best of the author's knowledge, no research work for security warnings is not found, which focus on distraction from warnings by interferences, such as malicious attackers, and technology failures. Potential reasons may be the less importance for users distraction of warning messages or the focus of the relatively young research field of computer security warnings on obvious research gaps in this field.

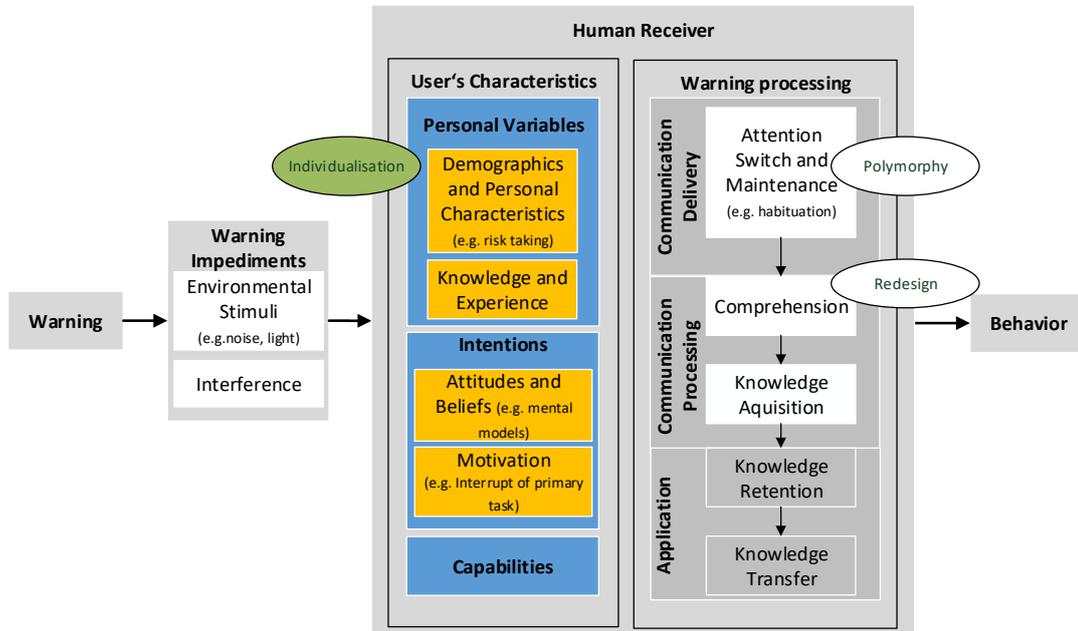


Figure 3.3: Related work field for 'User's characteristics' (coloured boxes)  
(Based on [Cra08])

#### User's characteristics:

Beside the disturbing environmental or intentional factors also the characteristics of a user may impact whether and how the warning is processed by the user.

#### **Interrupt of primary task (Motivation):**

As mentioned before a main reason why people ignore computer warnings is their focus on their primary task, e.g. writing an e-mail. Sasse et al. [SBW01] explained, that users trade off losses of security issues against losses of not completing their task. Users will ignore security advice to complete their primary task if losses for not successfully completing their primary task are higher in comparison to security losses. To describe this phenomenon Beutement et al. [BSW09] introduced the new paradigm 'compliance budget'. For warnings, it is the weigh of persons between individual costs and benefits, e.g. to complete their primary task, against benefits to comply with the warning, e.g. remove malware from their system.

Interruption of users' primary task is a problem. Nevertheless, experimental studies indicate that active warnings, which interrupt users from their primary task, are more effective in contrast to passive warnings, which do not interrupt the current user activity (e.g. [Cra08, ECH08], section 2.5.1).

In general, Angela Sasse [Sas15] complained about, that current warning approaches work against humans nature to focus on their primary task. She appeals for '*more accurate detection and better security tools, rather than scare, trick, and bully users into complying with security measures*'.

Herley [Her09] motivates to rethink the role of users of security advices. In his opinion users are not lazy if they reject security advice, rather they take a rational decision. One main problem is the lack of actual compromise data as basis for security advices. Commonly, most security advice based on worst-case scenarios. But Herley mentioned that users do not think in worst-case scenarios rather they estimate average outcomes. In some cases, e.g. false positive SSL warnings, the ignoring of security advice seem to be the right decision of users [AF13]. Herley believes that current security advice ignores cost of users, e.g. time and effort to read and follow warning instructions. He recommended to estimate a 'victimization rate' for any exploit for future improved security advice. The warning approach in this thesis introduces a design concept (section 4.3), which is a contribution to more user-centric advice in warnings. In the warnings *personal risks and consequences* of malware attacks against mobile devices and *instructions* in a user comprehensible language are given.

### **Differences between individuals (Personal variables):**

According to Cranor's model warning processing could also be influenced by individual characteristics of users, such as demographics, knowledge, previous experiences, and risk taking. Various studies, such as [BLCDK10, BLCD<sup>+</sup>11, AF13], indicate that *novice and advanced users* have different sets of cues, other mental models of risks, and respond differently to warnings. So an adaption of warnings to user-group characteristics, as the introduced warning approach in this thesis, seems a fruitful approach.

Akhawe and Felt [AF13] assumed, that *demographic factors* or other unknown variables are more likely to impact click-through rates of warnings, rather than for example the styling of warnings. But other researchers argued that warning design has a significant influence whether users decide to follow warning instructions (see section 3.2).

Furthermore, several studies (e.g. [Gus98, BMS99]) show that risk perception is influenced by gender. So most women are more less risk-averse in contrast to men. Several studies for browser warnings support these findings (e.g. [KMS12, MA14]).

### *Solution against general warning design: Individualised warnings:*

In the literature several warning approaches addresses individual differences of users by *individual warning designs* to increase warning effectiveness. There exist various approaches for warnings of web applications. Main scientific works in this field are those of De Keukelaere et al. [DKYT<sup>+</sup>09], Bartsch and Volkamer [BV13, BVTK13, BV14], Kauer et al. [KPV<sup>+</sup>12], Harbach [HHWS14] and Malkin [MMHE17].

**De Keukelaere et al.** introduced a design approach and software architecture to realise **adaptive security dialogs** (ASD) for email applications [DKYT<sup>+</sup>09]. Their framework displays specific layout security dialogues depending on the current individual user behaviour and her previous experiences. The dialogues differ in warning contents and difficulty for users to continue with their primary task in the email program. Exemplary obstacles are the answer of questions via multiple choice or manual input. They tested two different variants of their dialogues based on their framework against a standard e-mail malware warning - each variant with one test group with 8 participants. An empirical study of the ASD approach shows a small reduction of 5% users opening an e-mail attachment. De Keukelaere et al. resumed from increasing durations for reading the warnings and times for making decisions, that their participants were more careful in contrast to standard warnings. But because of lack of further measurements of decision processes (e.g. with neuro-science methods) and due to a small sample size these results could only be indicators and are not generalisable. Future studies have to evaluate the results of De Keukelaere et al. for larger and different test groups.

Recommendations how to individualise warnings are also published by **Bartsch and Volkamer**.

In [BV13] they introduced their research on **perception of web risk of users** with a card-sorting experiment with 7 expert and 7 lay users (non-experts). Their study results support risk communication literature findings of different mental models of expert and lay users. Their first results indicate that lay users' argumentation are more concerned with the website type, whereas experts more often consider concrete risk factors. Furthermore, lay users considered less often specific consequences during categorisation of websites, so Bartsch and Volkamer indicate a lower risk awareness of lay users in comparison to experts, which correlates with risk communication literature (e.g. [BLCDK10, BLCD<sup>+</sup>11]). They argued that more specific user mental models could help to increase warning effectiveness by identifying current user's knowledge gaps, concreteness of current knowledge and user's individual risk perception. Due to a small sample size these results are not generalisable to the whole population. Furthermore, the studies have to be repeated in realistic scenarios while users interact with browser warnings to obtain field data, which are more representative in comparison to a card-sorting experiment.

Hence Bartsch et al. [BVTK13] introduced the concept of '**contextualised warnings**' by using current risks of the context for decisions to warn. Furthermore, they conducted a user laboratory study with 36 participants divided into test groups to evaluate their previous findings of [BV13]. The participants had to solve twelve browser tasks, which were five times interrupted by warnings of different design depending on their threat level (e.g. online-banking, insurance). Afterwards, test candidates explained their reasons of their behaviour with a card-sorting exercise of screen shots of warning scenarios and answered questions about the risks regarding their behaviour in every situation. They observed in their study, that contextualised warnings have a significant impact that participants *comply with the warning* and participants are *more able to understand the risk of proceeding* in comparison to the control group. Amongst the positive effects they also observed using contextualised warnings could lead to *warning distrust*. They considered two reasons: first, whether users' do not comprehend the more concrete information, and second, whether users' doubts are raised if they perceived warnings as imprecisely or exaggerated. Due to the small amount of participants this laboratory study is not representative and has to be repeated with more test candidates in a field test.

In a further work [BV14] of Bartsch and Volkamer introduced a *holistic methodology* for abstract risk assessment including the encoding of security experts knowledge to implement contextualised warnings. They show in a case study the theoretical usage of the model. The risk is computed by current online risk type (e.g. financial) related to the current scenario (e.g. visit website unprotected) and incident (e.g. unauthorised transfer). This *abstract risk model* of Bartsch and Volkamer should be the basis to implement different warning types (e.g. active or passive) according to the context of the threat.

*Comparison to the three exemplary individualised warning approaches:* The new approach also wants to increase the effectiveness of warnings. But the implementation effort for individualised warnings is very high. Therefore, this thesis introduces a group-centred approach in contrast to an individualised approach to handle the trade-off between implementation effort and effective risk communication. So these works are out of focus in this thesis, but are a good basis to improve the introduced warning approach in the future (section 7).

*Solution against general warning design: Communication of personal risks*

There are some scientific works which uses personal risks to improve warning comprehension.

**Kauer et al.** [KPV<sup>+</sup>12] conducted a user study with 30 participants to evaluate **browser SSL certificate warnings**. They confronted their test candidates with four different websites (online banking, online shopping, social network, pure information site) and four different standard browser warnings. Kauer et al. found out that participants prevented entering the website, if the perceived risk is the spying of personal data. They found that warnings with *personal risks* are less ignored by users. So they assumed that the effectiveness of warnings could be improved if personal risks instead of technical risks are communicated. This result is not positive for SSL warnings, because most of them are false-positives. But for warning types with less false positive rates, such as malware warnings, this concept could increase their effectiveness. The introduced warning approach in this thesis is based on communication of personal risk and personal consequences of malware attacks against mobile devices.

**Harbach et al.** [HHWS14] introduced a novel **permission granting warning approach with personal examples** for Android smartphones. The warnings display amongst textual information also personal data on users' smartphone (e.g. photos, location data) to draw users' attention to data at risk and to improve users' decision making and their warning response. They realised a lab study with 36 participants and online study with 157 participants. The study results indicate, that their modified permission dialogues significantly decreases the installation of specific apps (e.g. financial, note, and search app). Furthermore, the comments of test candidates indicate that the improved permission dialogue design increases users' reflection about potential consequences of installing a specific app including their access rights to personal data. But because of the small sample size future large field studies are necessary to generalise these findings.

**Malkin et al.** [MMHE17] introduced a **novel browser SSL warning design** customised to users' decision making capabilities. They designed their warning textual contents ('nudges') for five stable personality traits (social, expertise, positive frame, negative frame, statistics, difficulty). They conducted an between-subjects experiment with 1.276 participants, which are faced with simulated HTTPS errors while reviewing websites on Mechanical Turk. Malkin et al.

found a significant correlation only for one of their six nudges (statistic warning information). But these results could not be replicated in a follow-up experiment, so the design effectiveness could not be validated. Malkin et al. mentioned different reasons for this results, e.g. small sample size, relational rejection, habituation effects, and reactant behaviour of users. The approach of Malkin et al. is a basis to further improve security warning designs in the future.

*Comparison to the three exemplary warning approaches with personal risks:* All three approaches are based on the clear communication and visualisation of personal risks to raise user's awareness to decision processes relating to her personal data. In comparison to the new approach in this thesis neither is related to malware attacks against mobile devices and uses multimodal feedback channels to users. Additionally, amongst the two exemplary personal risks by Kauer et al. [KPV+12] additional personal risks are included in the new approach.

#### Capabilities:

Amongst other characteristics also personal capabilities of users influence their processing of warnings. Exemplary capabilities are specific knowledge, cognitive or physical skills. Several warning study results (e.g. [BLCDK10, BLCD+11, AF13]) indicate differences between *novice and advanced users*. The both user groups are usually divided regarding their previous knowledge of computers, security risks, and risk handling strategies.

Warning studies which investigate the influence of *cognitive or physical skills* on warning processing and reaction are rare. In the future the usage of cognitive neuro science methods will be a promising approach to evaluate this correlations. First research work for warnings using neuro science technologies is published by B.B. Anderson et al. (see habituation section). In chapter 7 the future work of security warning research for e.g. handicapped people is sketched.

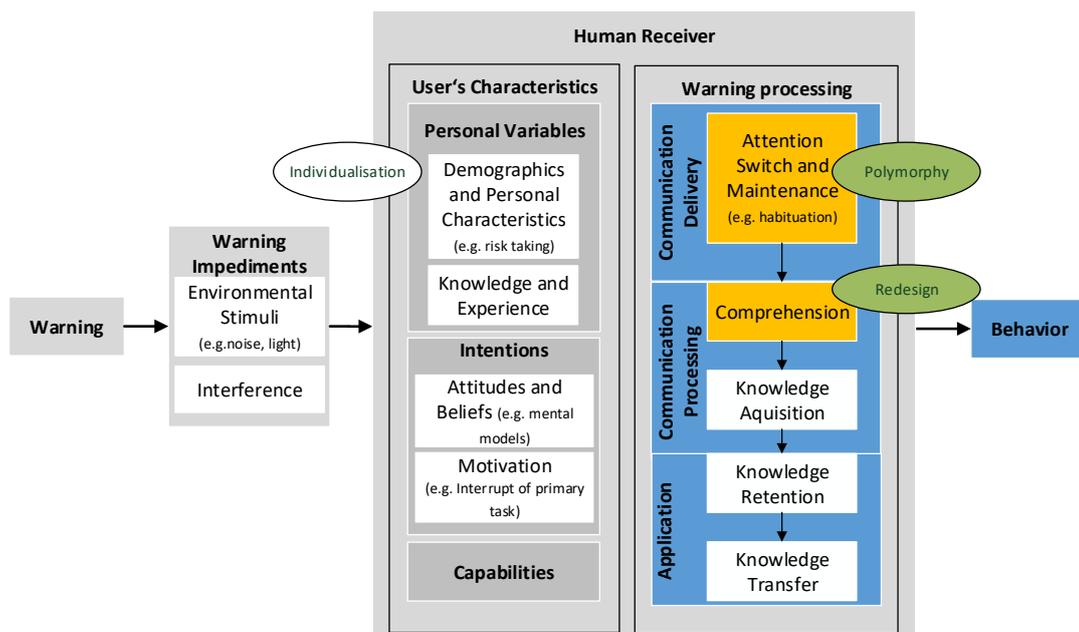


Figure 3.4: Related work field for 'Warning processing' (coloured boxes)  
(Based on [Cra08])

### **Warning processing:**

Beside the personal characteristics also the processing of warnings in the human brain has an influence whether and how humans react on warnings.

### **Habituation effects (Attention):**

Users are daily confronted with an overwhelming amount of warnings [MA14]. Results of many experimental studies indicate that most users do not read warnings (e.g. [ECH08, SEA+09, BLCDK10]). Potential reasons are habituation effects, caused by too many false positive warnings of specific warning types, especially browser SSL warnings. Interestingly, Akhawe and Felt [AF13] receive in their non-representative studies with malware, SSL, and phishing browser warnings less habituation effects for malware warnings (see section 3.2). The relation of habituation effects to specific warning types has to be detailed researched in the future (section 7).

But users often *could not differ specific warning types*. Almuhammedi et al. [AFRC14] observed that study participants confused browser malware warnings with SSL warnings. One reason may be bad designed warnings, which are not distinguishable by non-expert users. So users have learned that ignoring of many warnings has no negative consequences for them [Her09]. These warnings appear to be false alarms, also called 'crying wolf' syndrome [Bre13]<sup>5354</sup>.

Modic and Anderson argued that the great amount of warnings make the distinction of real threats from many trivial ones difficult for users [MA14]. So Krol et al. [KMS12] recommended to desensitise users by less amount of warnings with an improved design. Therefore, warning researchers developed several redesigned warning approaches to minimise warning habituation effects (see subsection 3.2 for malware warnings). The introduced warning approach in this thesis is one example.

Since several years warning researchers also use methods of cognitive neuro sciences for information systems, called 'NeuroIS' (e.g. [AVK+14, AVK+16, NSK+14]). NeuroIS methods, such as functional magnetic resonance imaging (fMRI), are also used to explain human brain warning processing and decision processes. Main researchers in this field are B. B. Anderson et al.. They found significant indicators in the brain for habituation processes [AVK+14]. Their study results show that already after 10 till 15 warnings habituation effects occur [AKJ+15]. B.B. Anderson et al. argued that the reasons for habituation effects are not the laziness of human users, but rather natural effects of human brain functionality. An approach to inhibit habituation effects of security warnings are the use of *polymorphic warnings*.

### **Solution against habituation: Polymorphic warnings:**

There are several approaches to minimise habituation effects. Warning researchers, such as Egelman et al. [ECH08], recommended to *design warnings differently to standard warnings* to avoid habituation effects. Other warning researchers around B. B. Anderson use neuro science technologies and found indicators in the human brain that polymorphic warnings reduce habituation effects [AKJ+15]. This is a motivation for well designed warnings, which are distinguishable from standard warnings. Habituation effects could also be minimised, if warnings are only displayed, if there is a real danger [ECH08].

---

<sup>53</sup>The English idiom 'crying wolf' is derived from Aesop's Fable 'The boy who cried wolf' (Perry Index number 210)

<sup>54</sup>Storyarts, The Boy Who Cried Wolf, <http://www.storyarts.org/library/aesops/stories/boy.html>, accessed: 05.02.18

**Brustoloni and Villamarín-Salomón** [BVS07] introduces two new techniques for **context-sensitive guidance (CSG)** - polymorphic dialogues and audited dialogues - to prevent habituation effects. The both dialog types are adapted for malware warnings of an email application (Thunderbird). They conducted a between-subjects laboratory experiment with 30 participants. Their significant study results show that untrained users accept less 'unjustified' risk with both dialogue types in comparison to conventional dialogues. Further larger field studies have to show, whether these promising results are generalisable and adaptable for other warning types.

**Jenkins et al.** [JKB<sup>+</sup>18] are the first, from the authors knowledge, who conducted a three week field study to evaluate the habituation effects of polymorph designed warnings for **privacy permission warnings on mobile devices**. They realised a between subjects study with 108 participants. The polymorphic permission warnings randomly change their design each time they were shown including visual design changes and text animations. Their study results show significant lower habituation effects for their polymorphic warnings in comparison to standard static warnings within three weeks. These results show that habituation occurs also for polymorphic warnings, but with a slower rate in comparison to traditional static warnings. Nevertheless, the results are not generalisable, because of the exclusive recruitment of test persons (all students, most male, average age of 22 years).

*Comparison to the both exemplary polymorphic warning approaches:* The warning approach Jenkins et al. is designed for mobile devices and also uses personal risks (e.g. record microphone audio, change user's credit card purchases) during app installing. In comparison to the approach in this theses only the single usage of mobile devices and not the coupling with other systems is in focus. As both approaches show, polymorphic warnings are a promising solution to reduce habituation effects on warnings, but are out of scope for this thesis and could be used in future works (section 7).

#### **Incomprehensible design (Comprehension):**

The warning research community is at strife about the importance of warning design for warning comprehension. Many warning researchers (e.g. [DHC06, BLCDK10, ECH08]) found out that users ignore warnings they do not comprehend. Egelman et al. [ECH08, SEA<sup>+</sup>09, EMC<sup>+</sup>10] studied delays by security applications, phishing and SSL warnings. They observed that bad designed warnings, which do not explain the *risks* and underlying *threat model*, are hard to understand by users. Additional results of warning studies indicate, that warnings with *technical jargon* are hard to understand by novice users and these users tend to ignored these warnings (e.g. [BLCDK10, EMC<sup>+</sup>10]). Many researchers recommended the *redesign* of security warnings (e.g. [AF13]). The introduced approach in this thesis is based on an improved malware warning design concept to increase warning comprehension of users (section 4.3).

Contrary to their opinions pro warning redesign in [AF13] Felt et al. hold - on basis of their SSL warning research [FAR<sup>+</sup>15] - that the design did not improve in all cases (SSL) warning comprehension. The results of their study are presented in the following subsection ('Redesigned warnings').

In the following exemplary research work for specific warning types (see section 2.5.1) is introduced on basis of the literature research.

### *Solutions for improved comprehension:* **Redesigned warnings**

**Bauer et al.** introduced on basis of their studies **security warning guidelines** to increase warning effectiveness [BBLCF13] (details in section 2.5.2). These six guidelines are 1) a comprehensively description of risk, 2) using concise and accurate warning content, 3) offer of meaningful options, 4) presentation of relevant contextual information and 5) relevant auditing information, and the 6) use of a consistent layout design. Amongst the textual description of warning content Bauer et al. recommend a specific warning layout (see figure 2.4) based on visual information. Warning basics are a warning icon, primary and secondary warning texts, a question, which is related to minimum one option of security mechanisms, wherewith the user could minimise the risks.

*Used parts of the approach:* are all guidelines, excluding the audit guideline, which are all adapted regarding the requirements of the new warning approach (see table 4.6).

*Differences:* The approach of Bauer et al. only focuses on visual warning information, such as icons and texts. The new approach includes amongst visual, also acoustical and haptic warning information. Furthermore, the approach of Bauer et al. is system-centric, which means security measures are used to protect the system for cyber-attacks. The new approach introduce a more user-centric approach, where users are warned about personal consequences of mobile malware attacks. Instead of options warning instructions guide users to handle security measures and mechanisms. In contrast to Bauer's approach the new warning approach also take mobile device properties into account (section 4.3).

### **General browser warning design:**

There are several research work how to design browser warnings in general. Two examples are discussed in this section.

**Krol et al.** [KMS12] evaluated a **browser warning design** for a pdf download scenario. They realised a laboratory study with 120 participants which used their own laptops for usability study of a novel academic article summary tool. Krol et al. evaluated the impact of warning design, demographic factors, and previous experiences to users' decision processes. Their redesigned warnings include detailed textual information about the threat (malware) and consequences ('damage to your system'). Their study show no significant differences between a general and their specific warning design. But the results show significant indicators that user decision processes are related to *gender* (persons do not download were mostly women), *computing skills* ('The higher the level of computer literacy, the more likely were the participants to download an article with a warning.'), and *previous experiences with computer crime* (more experienced participants more often refused to download the pdf). On basis of their findings the appeal for rethink of security warnings, including to *re-sensitise users* because of the high amount of false positives, *less usage* of browser warnings, and provide users *education and training* outside the warning.

**Bravo-Lillo et al.** [BLKC<sup>+</sup>13] researched design variants of **browser security dialogs**, which 'draw users' attention to the most important information for making decisions ('**attractors**'). They designed five inhibitive attractors, which prevent users from making risky choices through delaying of visibility of risky option button or users' performing of a required action (e.g. insert specific text). Bravo-Lillo et al. realised three between-subjects experiments with 2.277, 573, and 872 participants showing warnings with attractors for a game download, game permission granting, and repeating attractor warnings to measure habituation effects. The study results show that inhibitive attractors had a significant positive impact that users choose the safest option (e.g. no installation of software from illegal sources). But the usage of inhibitive attractors in warnings delay users' workflow and could demotivate users to do useful actions in cases no risk is present.

*Comparison to the both exemplary browser warning design approaches:* Both work researches warning design effects (e.g. attractors) on users' behaviour. This new warning approach also deals with these topics. In comparison to the new warning approach their work focus on browser warning applications (e.g. pdf download), only uses visual design criteria, and offers no specific personal risks, personal consequences, and no specific instructions to users.

#### **Browser SSL warning design:**

SSL browser warnings warn about authentication failures in the communication between browsers and web servers, which could endanger the privacy of browser users [AF13]. Two illustrating examples of research work in this field are described.

**Sunshine et al.** [SEA<sup>+</sup>09] researched whether the design of SSL warnings has an influence on users behaviour. They designed two variants of new SSL warnings: single-page and multi-page redesigned warning. In the multi-page warnings users had to answer specific questions to gather contextual information for browser risk assessment and to reach their destined website. In their between-subjects laboratory study with 100 participants they compare these new warnings with three existent SSL warnings of different browsers (Firefox 2 and 3, Internet Explorer 7). Sunshine et al. found, that their redesigned warnings preventing more users from entering a banking website in comparison to existing SSL warnings in those days. On basis of their findings they recommended an improved SSL warning design and the minimal usage of SSL warnings in benign situations, including block of malign website access to users.

**Felt et al.** [FAR<sup>+</sup>15] redesigned **SSL warnings** of Google's browser Chrome. Following recommendations from the warning research the warning text design were simple, non-technical, brief, and specific. Their new warning approach uses visual design methods to highlight the safe choice as the preferred option. In the first survey they tested their warning proposal against four SSL warnings of current browsers (ca. 300 participants each) against three metrics (comprehension of threat source, data risk, false positives). The test results do not indicate that warning texts of all five variants could improve comprehension for all three metrics. Felt et al. concluded that potentially their warning design was not optimal for comprehension because they made tradeoffs between text length and non-technical information. In the second large field study they tested SSL warning prototypes, which differ in texts and background colours. They could improve the adherence rates (measurement whether users heed warnings) of their warnings. The study show that their proposed text had no affect on adherence rates, but moderately improved users' comprehension of threat source. But their study focus on ad-

herence rates and do not differ between warning scenarios of real attacks and false positives. Furthermore, the results are only analysed descriptively. Therefore, there are no information about the significance of these results. So further research is necessary in the future to support these findings.

*Comparison to the both exemplary browser SSL warning design approaches:* Sunshine et al. also used a multi-page visual warning design with instructions (see design approach for adults in section 4.3). But these instructions are only examples and did not base on a general model or concept. Both warning approaches offer personal risks and Sunshine et al. personal consequences, but this information is used exemplary and do not base on a specific risk model. Against the background of many false positive SSL warnings both works offer specific recommendations for SSL warning design. Future studies with malware warnings and application scenarios where users have the full system control have to evaluate if these findings are applicable for malware warnings.

### **Browser phishing warning design:**

Browser phishing warning want to prevent users from visiting websites, whose want to steal users' identity data or other personal data to realise illegal cyber-attacks [AF13]. Two illustrating examples of research work of Egelman et al. are described.

In an early work of **Egelman et al.** [ECH08] they evaluated the design of **passive and active browser phishing warnings** for two different browsers (Firefox 2.0, Internet Explorer 7.0) with the C-HIP model of Wogalter [Wog06a] for cognitive warning processing. They conducted a between-subject study with 70 participants with a simulated spear phishing attack<sup>55</sup> on Amazon and eBay websites. Their results show that active phishing warnings are more heeded (80% of participants) and comprehended in comparison to passive warnings, and there are browser differences (more users heeded and comprehended Firefox warnings).

**Egelman and Schechter** [ES13] published results of a laboratory study with 59 participants. They investigate how **phishing warning design** (background color and text) influences user's decision process to comply with the warning. They observed that background colour and text had a significant effect on the amount of time test persons look at the warning. But they could not find any significant differences in participant's behaviour to obey the warning. Furthermore, Egelman and Schechter observed that participants with incorrect threat models disobey warnings or warned about irrelevant threats. Both researchers recommended warning designers should more highlight the *consequences of the risk* when warnings are ignored, so users understand that the warnings are belong to them.

*Comparison to the both exemplary browser phishing warning design approaches:* These both works of Egelman et al. indicates that active (browser phishing) warnings are better comprehended and heeded by users in comparison to passive warnings. These findings are used for the new warning approach, which also uses active warnings. Both works used personal risks and consequences of phishing attacks for users without using a specific model.

---

<sup>55</sup>A spear phishing attack is a targeted attack to specific persons or groups of persons. It uses personalised emails or emails of a targeted group, e.g. users of specific email providers.

#### Warning design for other security applications:

There is other research work for other warning types as the above described, but this is out of scope for this thesis. Examples are the work of Good et al. [GDG+05] for *spyware warnings*, Amer and Maris [AM07] of *IT exception warnings*, Raja et al. [RHH+11] for *firewall warnings* and Felt et al. [FEF+12] for *permission granting dialogues*. Section 7 describes the usage of the new approach for future work researches including warning designs of different security applications.

#### Application:

According to Cranors model the last step of information processing is application, categorised in knowledge retention and knowledge transfer. With *knowledge retention* users are able to remember warnings in specific situations, and could recognise and recall the meaning of the warning including symbols or instructions. *Knowledge transfer* means that users are able to recognise applicable situations for the communication and identify how to apply to it. Cranor mentioned for security warnings knowledge transfer is unnecessary because hazards are detected automatically by the system. So users do not need to find out of their own when the warning is applicable. But this is not so for cases when users mainly control the system. Here the users decide whether the warning is applicable to the current situation. Examples are SSL warnings, which are often false positives [Her09]. In this cases the non-compliance to warning instructions are the correct application of the warning. Here long-time studies are needed to measure the effects of knowledge retention and knowledge transfer (section 7).

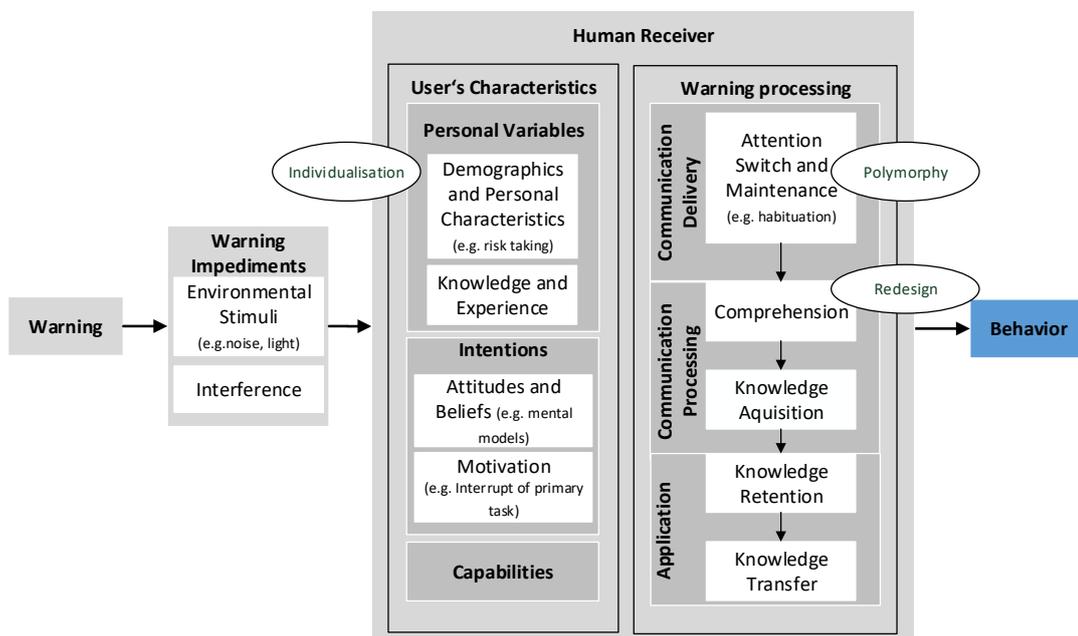


Figure 3.5: Related work field for 'Behaviour' (coloured boxes)  
(Based on [Cra08])

### **Behaviour:**

The objective of a security warning is to give users advice, that they could make the right decisions, which results in a user behaviour, e.g. heed or disregard the warning. Common procedure to measure warning effectiveness is the observation of user behaviour [AVK<sup>+</sup>14]. All the warning processing steps, influenced by users characteristics and distractions, influence users behaviour to warnings. In the best case, the user understands what action to take and she takes the specific action. According to Donald Norman, one of the main usability researchers, two failures could occur at this stage: first, the user is unable to complete the action successfully ('Gulf of Execution' [Nor02]) and second, a user is unable to determine whether she had carried out the action correctly ('Gulf of Evaluation' [Nor02]). According to Norman both failures could be minimised through good design. According to Cranor the gulf of execution could be minimised if security communications (e.g. warnings) give users clear instructions how the desired actions have to be executed. The gulf of evaluation could be minimised by providing relevant feedback to users. On this basis users could determine whether their actions were successfully or not.

In this thesis a warning approach is introduced, which offers users guidance with instructions. The effectiveness of this approach is evaluated with two small user studies (section 5). In the future the gulf of execution and gulf of evaluation of the warning approach should be researched in more detail (section 7).

### **3.1.2 Invalid user studies**

---

Beside the steps of human-information processing some researchers also make the design of user studies responsible for results, that indicate security inattentive behaviour of test persons. Krol et al. mentioned in [KMS12] that invalid tests with *no real risks* might be responsible for these negative results. Egelman et al. [EMC<sup>+</sup>10] defined valid tests as '*if users believe they are really at risk*'. Realistic scenarios could be created, if participants could use their own technical equipment [KMS12] or own credentials [SDOF07]. Krol et al. [KMS12] investigate the reaction of users to malware warnings during download of pdf files with their own laptops. Participants in their study mentioned that they trust the laboratory and the researchers to prevent them from download something malicious. Schechter et al. [SDOF07] investigates authentication processes in online banking scenarios. They measure amongst others the effect of role-playing on the study. They found significant indicators, that role playing (here: not using own online-banking credentials) has a negative effect on security vigilance of participants. The valid design of user studies are described in section 2.6.2 and discussed for the novel warning approach in section 5.

## 3.2 Malware warning approaches

This section introduces active security malware warning approaches of the literature survey. The related work is discussed on their similarity or used parts of the approach<sup>56</sup> and the differences to the new introduced warning approach in this thesis.

Rare are works about *malware warnings*. Only two other scientific works are published for warnings on mobile devices [HHWS14, JKB<sup>+</sup>18].

**Bravo-Lillo et al.** [BLCD<sup>+</sup>11] researched the relation of warning design of selected e-mail and **browser malware warnings**, users' warning comprehension and users' motivation to respond to warnings, users' tendency to choose the safest option, and demographic factors. They realised an online study with 733 participants. They evaluated four existing security warnings (MS Office Outlook and MS Internet Explorer): warnings for e-mail encryption, access request for an e-mail address book, malware infected download file and malware infected website (certificate warning). Furthermore, they created two versions of redesigned warnings on basis of warning literature, and mental models of non-expert users. Their redesigned warnings significant increase test candidates' comprehension only in 3 out of 16 test cases. Furthermore, they observed increasing levels of motivation for 2 of 6 warnings in high risk scenarios. Nevertheless, these result are no significant indicators for test candidate ability to differ between low and high risk scenarios. Bravo-Lillo et al. made their ineffective warning design (e.g. too long texts) and inadequate study conditions (e.g. several warnings per participant, no control group) responsible for these results. So they could not isolate the impact of any of their design changes.

*Similarities:* The work of Bravo-Lillo et al. found significant correlations between motivation and choosing the safest option, and significant correlation between motivation and comprehension. Furthermore, their study indicates that redesigned warnings could increase users' motivation to heed the warning, users' comprehension of warnings, and tendency to pick the safest option. The new warning approach introduces a new design to improve further described aspects.

*Differences:* This early work of Bravo-Lillo et al. evaluates different variants of security warnings at that time. Their warning design approach includes different option layouts, descriptive text for options, and contextual information. The design based only on visual information and has no relation to mobile devices.

<sup>56</sup>This selection is seen as 'either or' decision. If no parts are used for the new approach similarities are discussed and vice versa.

**Almuhimedi et al.** [AFRC14] evaluates influence of website reputation on warning adherence for **browser malware warnings** on the example of browser Chrome 32. They analysed ca. 4 million Chrome malware warning statistics and realised an online, survey-based experiment with 1.387 participants from Amazon's Mechanical Turk worker. Their study results that participants which have experiences with a website and refer a high reputation to this website tend to ignore the malware warning related to this website. But according to Almuhimedi et al. the ignoring of warnings is unpredictable, because users behave differently from day to day. Furthermore, they observed some participants which confused malware and SSL warnings. But nevertheless these are no generalisable results, because most participants were active Internet users.

*Similarities:* Almuhimedi et al. recommended to improved malware warning design. Some of their participants desire more clear and contextual information as basis to make better decisions. Due to these requests they extended the 'advanced options' button in the Chrome malware warning. So users have amongst the 'Go back' button, two more options 'Details about problems on this website' and 'Proceed at your own risk'. The new warning approach also offers users additional information about their personal risks and consequences of a malware attack.

*Differences:* In comparison to the work of Almuhimedi et al. this work introduces a multi-modal malware warning concept on mobile devices and offers non-expert users instructions to help them reducing their personal risk related to malware attacks.

**Modic and Anderson** [MA14] investigated the **redesign of wording in browser malware warnings** and reasons why users turn off browser malware warnings. Their new warning wording concept uses social-psychological techniques. They designed five wording variants: control (Chrome warning, June 2013), authority, social compliance, concrete threats and vague threats. They evaluated their new warning approach with an online survey with 496 Amazon Mechanical Turk participants. The results of Modic and Anderson showed that most participants do not turn off the malware warnings. Especially test candidates with advanced computer skills and woman tend to turn on these warnings. One reason participants turn warnings off is their inability to comprehend warnings. These results show that comprehension has to take into account for an effective malware warning design, beside demographic and previous knowledge aspects.

*Similarities:* Modic and Anderson recommended two aspects to increase malware warning effectiveness: first, a clear and non-technical description of potential negative outcome for users, and second, an '*informed direct warning given from a position of authority*'. Both aspects are realised with the new malware warning approach in this thesis addressing personal aspects of malware attacks with concrete warning information.

*Differences:* The work of Modic and Anderson focus on malware warnings of browsers, and introduced a warning design concept for wording. No other feedback channel to users or personal information in warnings are discussed. The new approach introduces here a more holistic warning design concept for mobile devices.

**Akhawe and Felt [AF13]** researches amongst other warning types **Firefox and Chrome browser malware warnings** to validate warning effectiveness. Their study based on more than 25 million warning impressions of both browser telemetry platforms (versions: year 2013). Both browser differ in their warning mechanism: Firefox displays fewer warnings, because it blocks third-party resources without a warning in comparison to Chrome, which only stops the load of a suspicious page and replaces it with a warning. Furthermore, the warning design of both browsers differ in their visual appearance and possibilities for users to gather more detailed information. The warning effectiveness is measured with so called 'clickthrough rates', the time users need to click through a warning to bypass it. They found indicators that the increased amount of effort to bypass warnings (i.e. number of clicks) does not always impact users' behaviour significantly. Akhawe and Felt assumed that users first cognitive decision how to handle the warning could not be changed by additional clicks or information until they reach a specific threshold of difficulty. Furthermore, their user studies indicates less habituation effects for malware warnings in comparison to other warning types. But these results seem to depend on different variables, such as browser type, date, demographic characteristics of users (e.g. higher clickthrough rates for Linux users). Although, these results are not representative, future work have to clarify the influencing factors to malware warnings.

*Similarities:* The work of Akhawe and Felt also researches the effectiveness of malware warnings, including presenting of additional information. Users in their study rarely clicked on explanatory links ('More Information' or 'Learn More'). So they recommend that such links should avoid to hide important details, which users need for their decision-making processes. The new approach offers such information in form of personal risk, personal consequences and instructions to help users to decide.

*Differences:* In comparison to the new approach they focus on browser malware warnings instead of malware warnings on mobile devices, and use existing visual malware browser warnings instead of creating own warning designs. Instead of using a specific model for personal risks Akhawe and Felt used warnings, which warn of personal risks and consequences for users in a more general manner.

**Silic et al. [SBO15]** introduced a new **browser malware warning** approach based on Wogalters C-HIP model [Wog06a] to increase users' attention and secure behaviour. Their warning design approach based mainly on textual information and two option buttons to exit or to continue a download process. Silic et al. tested in their first online field-study 16 warning variations with 253 participants. The warnings were combinations of information about severity of threat (e.g. large loss of private information), probability of threat occurrence ('certainty'), *personal benefit and personal barrier* for users' exiting the simulated unauthorised software. One example for an user's benefit is the text: '*If you choose to exit now, you will protect your computer and information from harm.*'. Their pilot study get significant results for the severity and barrier statement as well. They concluded that the presentation of 'personal barrier' information increases participants motivation to heed the warning and to choose the safest option (exit the download). In the future they plan a larger study with different user groups and an improved warning design.

*Similarities:* The approach of Silic et al. also addresses *personal threats* of malware attacks against example of a download process of an unauthorised application.

*Differences:* In comparison to the new approach no personal risk or threat model is introduced and only visual information are used.

### 3.3 Other relevant related work

---

This section introduces related work from research fields different to above described *active security malware warnings*. Introduced are selected papers from the *safety warning* research, *security warning* approaches for *automotive systems*, and one *mobile robot IDS* paper.

#### **Safety warnings:**

Safety warnings warn of damages of objects or injuries of creatures caused by accidental system failures (e.g. nuclear power plant) or caused by the product itself (e.g. medicine). Usual static safety warnings are printed icons or signs used in different public and professional environments. Examples are traffic signs or signs in industrial plants in areas where human and machine work together and humans are in danger. In contrast to dynamic warnings these static warnings are persistent visible for humans. This type of warning is in cases of no danger a false positive. In contrast to safety warnings security warnings warn of intended threats caused by cyber-criminals and their tools (e.g. malware). But this thesis focus on side-effects of cyber-attacks - functional failures caused by malware which could impact human users. So main safety warning concepts are highlighted and related to this thesis.

#### **Effective safety warning approaches:**

**Michael S. Wogalter** is a leading researcher in the field of **static safety warnings**. In [Wog06b] he gives recommendations how to raise their effectiveness. According to Wogalter warnings are effective if they inform users about current *risks*, give *instructions* how to handle the risks, and show *consequences* if not complying to instructions.

*Used parts of the approach:* The new effective security warning approach includes the concept of Wogalter to raise security warning effectiveness. It informs users about the current risks and consequences and give instructions to users.

*Differences:* Wogalter's approach to raise warning effectiveness focuses static safety warnings printed as pictogram. As mentioned above static warnings are always visible and are often false positives. Users are not forced to look at a static warning. That means in contrast to active warnings, static warnings do not interrupt users' primary task to get users' attention. The new approach focuses dynamic security warnings, which are displayed on screens of mobile devices. It uses Wogalters' concept to offer users quantitative more and more personal security warning information to protect themselves for mobile malware attacks. This concept could lead to a better warning comprehension, but also to exhaustion and frustration of users. The results of two user studies in section 6 will highlight the success of this concept.

**Joachim Meyer** researches concepts and methods to increase **dynamic safety warning effectiveness** in complex systems with expert users. Exemplary application scenarios are flying a plane, monitoring chemical or nuclear facilities. In [Mey01] he introduced the terms 'compliance' and 'reliance', which are two different responses to warnings of operators. *Compliance* describes the operators response according to a warning signal, e.g. shut down a robot after a warning. If the warning system produces many false positive warnings, operators do not trust warnings ('cry wolf' effect) but favour additional information. *Reliance* describes the response if no warning is displayed. That indicates the system is intact and the operator has to do no precautions, e.g. no shut down of robot when there was no warning. This could lead to 'misuse of automation' also called 'automation bias' [PR97], when operators fully trust in warnings, but do not consider additional information. The article did not clear describe

the meaning of 'additional information', maybe Meyer means contextual information from the system or environment. Meyer resumed from his studies with operators [Mey01, Mey04], that with increasing experience operators reliance in warning system decreases and that '*warnings that were integrated with the additional information led to greater compliance than did warnings that were presented separately from additional information.*'.

Furthermore, Meyer [Mey04] introduces an economic cost-benefit analysis to evaluate operator responses to warnings and a **decision process model** to describe factors which influence the response of experienced operators to an active safety warning. It is assumed that operators notice and understand the warning. But, trigger users' attention and design comprehensible content are two main challenges of warnings for non-experts. Furthermore, Meyer gives cause to concern, that in some cases to comply the warning is not the correct decision. That is comparable with the amount of false positive SSL warnings users ignore (see part A, Incomprehensible design (Comprehension)).

*Similarities:* This warning concept in this thesis also provides the user *additional information* in form of personal risks, personal consequences of malware attacks against mobile devices, and instructions to handle this situation.

*Differences:* The concepts and methods of Meyer are adapted to dynamic safety warnings in complex systems for trained expert users. These are out of focus of this work. But the transfer of Meyers' approaches into design concepts of security malware warnings on mobile devices is a valuable goal for future research activities (see section 7.3).

#### **Security warnings for automotive systems:**

With the ongoing usage of embedded systems in modern cars the possibility of successful cyber-attacks is increased. The two first security warning approaches for automotive systems are introduced.

**Tuchscheerer et al.** introduced a *security warning approach for automotive malware* [TDHK10]. The removal of malware in a modern car could lead to malfunctions of the car, because the malware could manipulate internal processing units (EDU). The removal of malware - especially if the car moves with high velocity - could endanger the driver and it's environment. Therefore, warnings are a first aid security measure to show drivers, that the system has been manipulated and has to be checked by an automotive expert. The warning approach of Tuchscheerer et al. was evaluated with a user study in a driving simulator. Warnings are designed as combination of visual, acoustic, and haptic information appropriate to the risk level. Visual warning information is a combination of a known security icon (e.g. protection shield with lettering 'Virus') and a known pictogram of the attacked system component (e.g. engine). In the user study only visual and acoustical warning design criteria are realised. Because of the small sample size only tendencies could be derived from this study. It shows two main problems of test persons: first, the problem to correlate the known desktop IT threats with the known automotive components, and second, the problem to access and rate the potential resulting threats and hazards.

*Similarities:* The new warning design also uses multi-modal warning information. Such as in the concept of Tuchscheerer et al. also security-safety-impacts of malware on a cyber-physical system are in focus. The both mentioned malware-related privacy impacts, spying attacks against camera and microphone, are also included in the new concept.

*Differences:* In contrast to the above concept the warnings are designed for mobile devices not for other mobile systems. Furthermore, personal mobile malware impacts are in focus.

**Hoppe** published amongst other aspects a *methodical analysis of malware attacks* on automotive systems [HD14]. A reaction model of an automotive Intrusion Response System (IRS) is introduced, including multi-model warnings. Depending on current environmental influences and the severity of the detected security threat single or combined visual (uncritical impacts), acoustical (critical impacts), and haptic information (very critical impacts) are used in the warning.

*Similarities:* Such as Hoppe's concept the new warning design also uses multi-modal warning information.

*Differences:* Hoppe's warning research was a small part of a comprehensive analysis and concept of automotive malware prevention, detection, and reaction strategies. This thesis exclusively focuses a warning concept for mobile devices as part of a reaction strategy.

### **Physical effects of cyber-attacks against mobile robots:**

Vuong et al. introduced an *intrusion detection system* (IDS) for mobile robots in [VLG15]. The IDS could detect several cyber-attacks on basis of the physical effects of these attacks. In their study they investigated the '*physical indicators*' of four security attacks (DoS, command injection, malware attack against network, and malware attack against CPU) and compared it with a normal robot operation. For three of the four security attacks they could observe physical impacts, such as 'inconsistent stops' (DoS), 'frequent consistent jittering' (command injection), and 'frequent consistent stops' (malware attack against network).

*Used parts of the approach:* Observed effects of cyber-attacks against mobile robots in the study of Vuong et al. are used in the personal risk model to illustrate potential personal consequences for users of malware attacks against mobile devices, which are spread to coupled systems, such as mobile robots. One exemplary attack is a Denial of service (DoS) attack against a mobile robot. Vuong et al. observed that the attacked mobile robot function was interrupted by 'inconsistent stops' [VLG15].

*Differences:* The research of Vuong et al. focus on the development and research of an IDS for mobile robots. This research do not include a creation of a security warning approach, therefore it is not presented in table 3.1.

### **Research gaps:**

To the best of the author's knowledge (see table 3.1) there is currently no security warning concept for mobile devices, which focuses personal impacts of mobile malware regarding the described application scenarios in section 1.1. However, the introduced warning approach in section 4.3 based on above mentioned parts of other warning research (see figure 4.7 in chapter 4). One example is the safety warning concept of Wogalter [Wog06b] to create *effective security warning information* (risk, consequences, instructions). This concept is adapted based on the recommendation of Kauer et al. [KPV<sup>+</sup>12] to create *personal risk information*, and instructional education concepts [SK14] to guide users with *instructions*. Additionally, warning guidelines of Bauer et al. [BBLCF13] and recommendations of a German information security standard [BSI08] are included into the new warning design. Furthermore, the evaluation methodology and concept in section 4.4 based on state-of-the-arts usability standards and guidelines from the academic field [PD10], industrial field [VDI00] and security warning research [KSPS16] (see section 2.6).

# 4

## Methodology and Concept

This chapter introduces the methodology and concepts of the general user-group specific effective malware warning approach for mobile devices. Figure 4.1 gave an overview to the methodology. It based on *three main parts*.

The *first part* includes the two previous works. The first work is a *study* of current malware warnings of Android security apps (section 4.1), which overviews the state-of-the-art of malware warnings, and the main lacks as motivation for the new warning approach. As second previous work an own *personal risk model* is introduced, which maps malware attacks against mobile devices and coupled systems to personal risks of users (section 4.2). This model is a basis for the information design of the new warning approach (section 4.3).

The *second part* of this chapter introduces the *new warning design* approach. It is determined by the *user-group specific characteristics* (section 4.3.1) and the *mobile device specific characteristics* (section 4.3.2). These both aspects also influence the both other elements of the warning approach, the *effective warning design* (section 4.3.3) and the usage of *multimodal feedback* (section 4.3.4). These previous sections describe the four requirements, which determine the generic layout of the new warning approach for a generic adult user in section 4.3.5. In section 4.3.6 the generic warning design for primary-school children is described.

The *third part* of the methodology introduces the *general evaluation methodology and concept*. This section is separated into three subsections. In section 4.4.1 the experimental design of the two different *test cases* of the two instances of the generic warning approach are described. The next section 4.4.2 introduces the chosen *evaluation methods and test metrics* of the introduced warning approach based on fundamentals in section 2.6.3. In the last section 4.4.3 the specific *evaluation concept* for the two specific test cases is described.

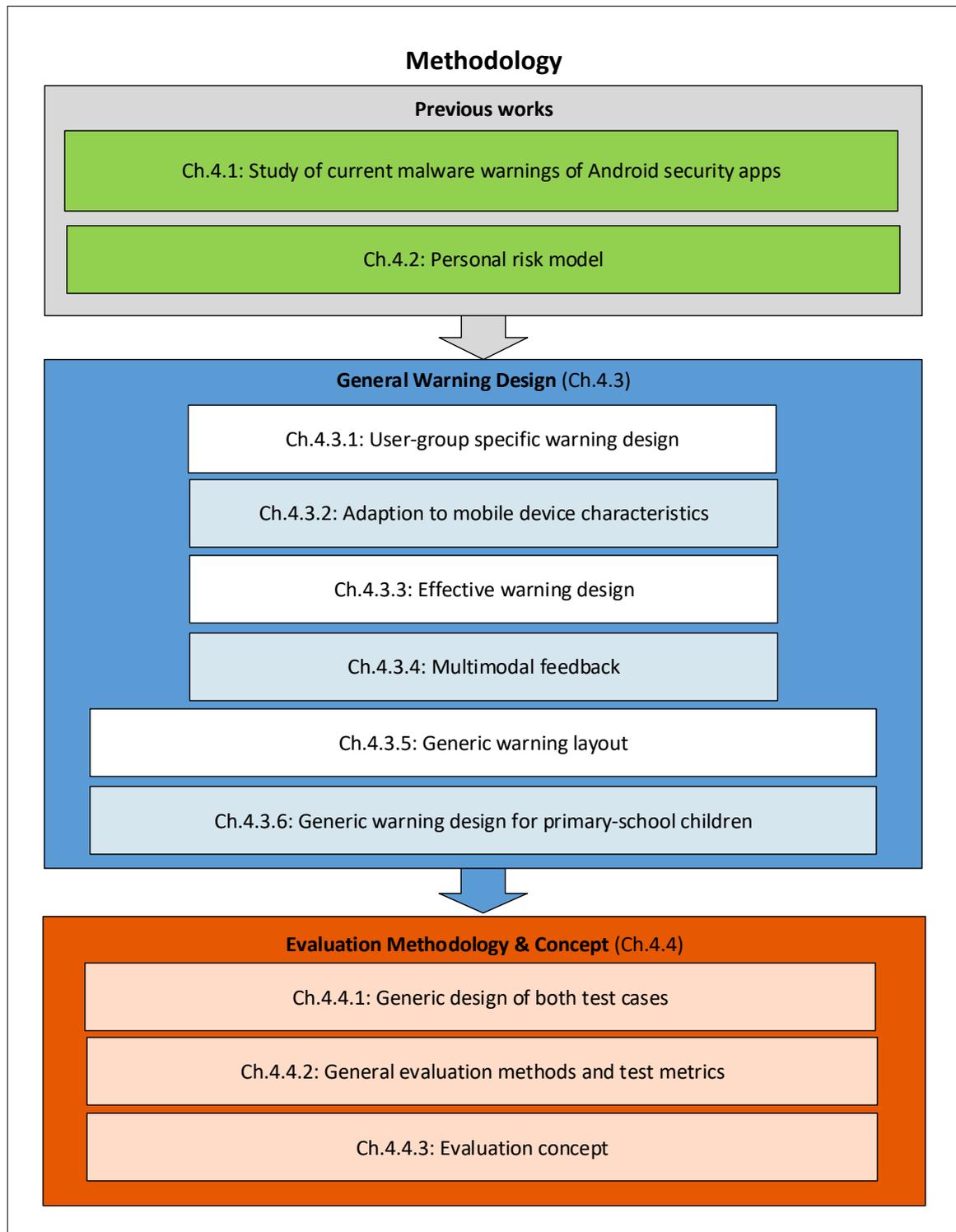


Figure 4.1: Methodology of this thesis

### 4.1 Malware warning design study of current mobile Android security apps

---

This section introduces the research results of a study of free mobile security apps on tablets and smartphones with malware detection based on the operation system Android. It is related to research objective 1 (section 1.3).

#### **RO1: Research of current malware warnings on mobile devices.**

The study was realised in August 2017. Android apps are chosen, because Android was at this time the current market leader for operation systems on tablets and smartphones<sup>57</sup>. The wide spread use of Android and various sources for downloading apps are motivation for cyber-criminals to attack Android systems with malware. The Android apps are selected from the last available test<sup>58</sup> of AV-TEST - an independent German security research institute with focus on malware analysis and detection. iOS is currently the second market leader for smartphones and tablets. But currently no mobile security app is available which provides malware detection for iOS<sup>59</sup>. The main reason is iOS's system protection by sandboxing - restricted execution of apps on host system, which prevents malware activities on iOS, e.g. spying of personal data. So Apple removes all antivirus apps from the App Store in March 2015.

Table 4.1 summarises the results of the study regarding the investigated design criteria, which are multimodel feedback elements, coding of different threat scales, additional information about the malware or threat, user instructions what to do against the current threat, and user guidance. Only 15 of the 20 mobile security apps could be tested. The other five apps could not be tested, because the apps were not available any more, or were written in languages, which were not comprehensible by the tester (e.g. Chinese), or the apps were not compatible with the test system.

The test was realised by download of mobile security apps from the corresponding Google app store on a smartphone (Nexus 5, Android 6.0.1) and tablet (Samsung Google Nexus 10, Android 5.1.1). Only one app was installed at once to avoid conflicting activities of concurrent antivirus apps. To simulate malware activities without have the risk of real malware infection the EICAR test file<sup>60</sup> was used. It was developed by the EICAR, the European Institute for Computer Anti-Virus Research, and CARO, the Computer Antivirus Research Organization. After app installing, the EICAR test file was downloaded. Depending on the app the test file was detected simultaneous by realtime scanners or after scanning by on-demand scanners. Two of the 15 tested apps could not detect the EICAR test file (marked with exclamation marks in table 4.1).

---

<sup>57</sup>Gartner, Global mobile OS market share in sales to end users from 1st quarter 2009 to 1st quarter 2017, <https://www.gartner.com/newsroom/id/3859963>, accessed: 02.08.17

<sup>58</sup>AV-TEST, The best antivirus software for Android, Test report from May 2017, <https://www.av-test.org/en/antivirus/mobile-devices/>, accessed: 02.08.17

<sup>59</sup>Henry T. Casey, Why Apple iPhones Don't Need Antivirus Software, <https://www.tomsguide.com/us/iphones-dont-need-antivirus-software,news-23111.html>, accessed: 03.08.17

<sup>60</sup>EICAR, Anti malware test file, [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm), accessed: 26.07.17

## Chapter 4. Methodology and Concept

Criteria/ App	Multimodal feedback			Risk/ Threat	Consequences	Instructions	Guide	Threat scale
	Visual	Acoustic	Haptic					
AhnLab (3.1.11.4)	✔, ⚠	Long single tone	Long vibration	Malware, Trojan	Modify & leak personal info.	Remove	-	Normal, Threat
AVL (2.2.0)	○, ⚠	-	-	Threat, in danger	-	Remove	-	Normal, Threat
Avast (6.4.4)	○, ⚠	-	-	Malware	Device damage	Eliminate	-	Normal, Threat
Avira (5.0.2)	Shield: ✔, !	Standard app notification tone	-	Virus, malware	Direct threat to personal data/ device security	Remove	-	Normal, Threat
Cheetah (4.1.5)	Soap bubble: ✔	!	!	!	!	!	yes	Normal, Threat
ESET (3.6.46)	✔, ⚠	-	-	Testfile, Link to online info.	Harmless file for testing	More info., Remove	-	Normal, Threat
G Data (26.0.6)	✔, ⚠	!	!	!	!	!	-	Normal, Threat
Ikarus (1.7.87)	✔, ⚠, Shield: !	Long single tone	Long single vibration	Virus, Malware, System is infected	-	Remove	-	Normal, Activity, Threat
Kaspersky (11.14.4)	Shield: ok, threat	Monster tone	-	Threat neutralised	-	-	-	Normal, Threat
McAfee (4.9.2.709)	Background: ok, activity, threat	-	-	Threat	Damage of device/ personal data	General info., Remove	-	Normal, Activity, Threat
Norton (3.21.0.3302)	✔, ✘	?	?	Malware	-	No installation	-	Normal, Activity, Threat
ONE App Max (1.1.7)	Shield: ✔, ⚠	?	?	Virus, In danger	-	Resolve button	-	Normal, Threat
Psafe (3.12)	Shield: ok, ⚠	?	?	Low security level (4 level)	-	Resolve button	yes	Normal, Activity, Threat
SOPHOS (7.05.2355)	✔, ⚠	-	-	Threat or PUA, Link	-	Remove, further, details	-	Normal, Activity, Threat
Trend Micro (8.2.4)	✔, ⚠	-	-	Intervention needed	-	Search button	-	Normal, Activity, Threat

Table 4.1: Study results for current mobile security Android apps with malware detection

(Note: Visual column: e.g. 'shield: ✔' symbolises a shield with an included green checkmark;

○ symbolises a blue circle for normal state;

'-': not implemented, '!': EICAR test file not detected, '?': no hint for realisation

Threat scale: e.g. 'Normal,Threat' - 'normal system state', 'threat state')

### **Multimodal feedback:**

Most of the investigated apps use mainly *visual design* parts, like icons, textual descriptions (e.g. 'ok'), and colour coding for specific app states. For three apps the usage of acoustical and/or haptic feedback could not be investigated (marked with interrogation marks in table 4.1). The most used *icons* are round icons or shields including a checkmark for normal state and exclamation mark for threat state (see second column of table 4.1). Only two apps used a combination of *acoustic and haptic design* elements. Examples are AhnLab and Ikarus. The alarm signal and vibration duration and vibration pattern are similar and played synchronous. The acoustical signals for detection of a threat differ from standard app notification tone to four tone signal. The app of Kaspersky uses only acoustical signals without haptic information. Instead to inform users about a detected malware it automatically removes the malware from the mobile device. In this moment the sound of a crying monster was played.

### **Risk/Threat:**

The apps, which detected the EICAR test file uses simple *general descriptions* of the current detected risk/threat. The ESET app inform users that EICAR is a test file and no real malware. All others call it in general 'threat', 'virus', 'Trojan' or 'malware'. The threat is described different, from one single sentence 'In danger, 1 threat.' (AVL) till long descriptions, e.g. 'This app or file includes viruses or other malware, which is a direct threat to your personal data and/or the security of your device.' (Avira). Additional threat information could be also presented in the app or linked to online information. Only two apps use this format. The ESET app presents an information button, where the user is directed to additional information in the app or to the Internet. The SOPHOS app warning includes a link to additional online information, too.

### **Potential consequences:**

Only four apps of the 15 tested apps inform users in more detail about potential consequences of detected malware. Examples are unauthorised change of audio settings, read and change of synchronisation and system settings, spying of device and user activities. But users are only informed in general about potential consequences. In most cases the information is not threat specific. McAfee gives separated information for specific threat classes, but the descriptions are very general, e.g. damage of your device.

### **Instructions:**

Instructions for users reach from simple 'remove' to general information how to handle threats. Here are also no threat specific instructions presented. The composition of warning information differs. Most apps uses additional information about the threat and instructions in one window. One example is the Avira app, where additional information is presented: 'This app or file includes viruses or other malware, which is a direct threat to your personal data and/or the security of your device.'. Furthermore, users are instructed by: 'We recommend to remove these immediately.'

### Guidance:

Only two apps, Cheetah and Psafe, offer guidance information to users (table 4.1 'Guide' column). Figures 4.4 and 4.5 show guidance examples, where both applications prompt their users to enable automated scan and block of mobile malware. Cheetah was the only one app, which uses a cartoon guide to ease users the app handling (figure 4.3). The usage of cartoon guides are a playful method for children to offer general information or warning information. The warning design example in section 4.3.6 for primary-school children also based on a cartoon guide.

### Threat scales:

Most of the apps uses simple two or three level *threat scales*, where the 'lowest' state is the normal state without any threat. There are four types of color coding for threat scales detected. First, some Asian apps, e.g. AhnLab and AVL, use light blue for normal state and orange for threat state. Second, some European and one Asian app, e.g. Avast, Avira, and Cheetah, uses the classical European color coding [VDI00], where light green symbolise the normal state and red an emergency state. Third, in comparison to that a mixed form of color coding is detected. Some European apps, e.g. ESET and G Data, uses light green for normal state and orange for threat state. Fourth, five apps uses three threat levels, examples are Ikarus and McAfee. Most of these apps use a scale from green for normal state, orange for states where user activity is needed (e.g. give app access rights to personal data, figure 4.2), and red for threat state (see figure 4.3).

### Conclusion:

The investigated security apps with malware detection are designed for standard users. Most apps are designed with visual elements, short risk information, less information about potential personal consequences, and short instructions. That is related to the functionality of these apps, which focus on the protection of the system, not the user. They automatically detect malware on mobile devices and give users a short feedback of the result of a malware search. If a malware is detected the app recommended to the user to remove the detected malware. Some apps offer additional information or guidance to users. Application scenarios, where users remotely control other coupled systems with the mobile device and therefore other risks may threaten the user are not in focus of current mobile malware warning developers. Future warnings of security apps on mobile devices have to be improved with the increasing distribution of IoT devices, which could remotely controlled with mobile devices. This thesis introduce a warning design which focus on such application scenarios and which is adaptable for specific user-groups.

## 4.1. Malware warning design study of current mobile Android security apps

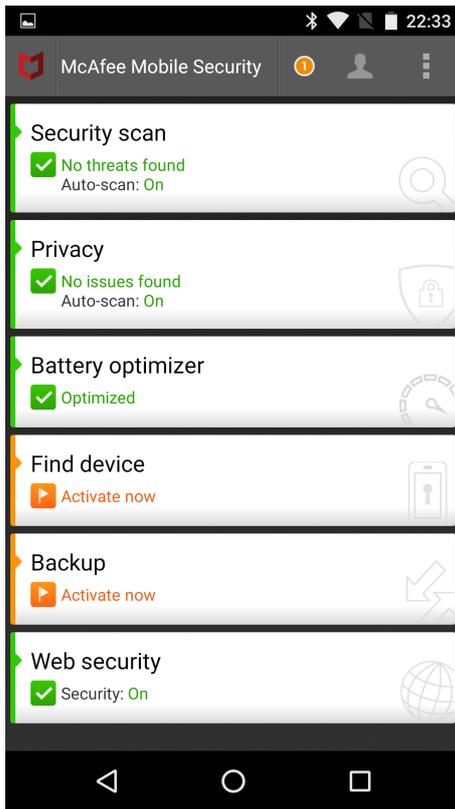


Figure 4.2: Screenshot of McAfee

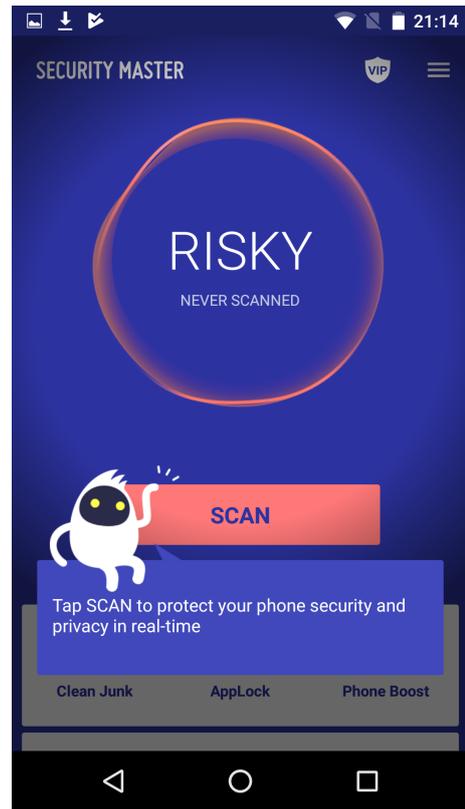


Figure 4.3: Screenshot of Cheetah guide

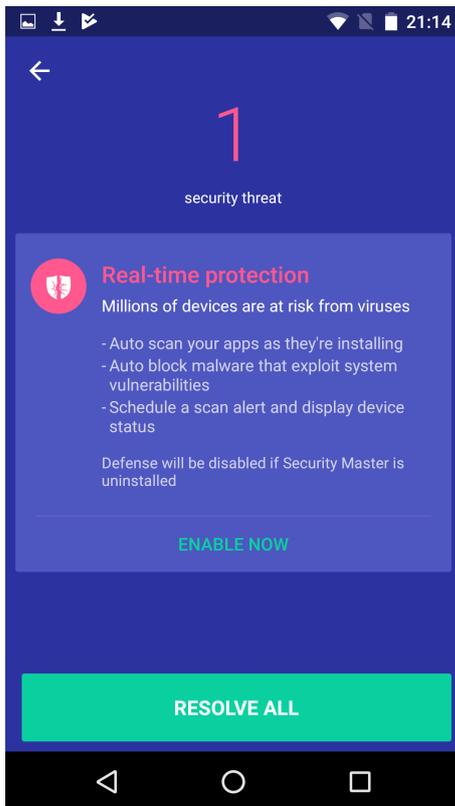


Figure 4.4: Screenshot of Cheetah guidance information

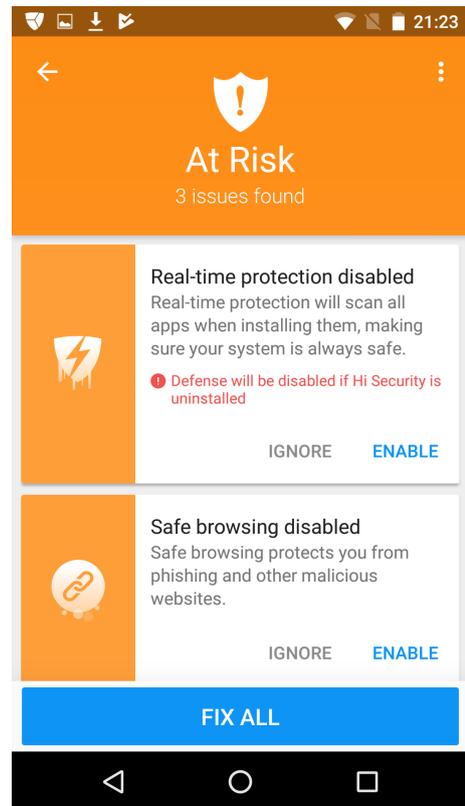


Figure 4.5: Screenshot of Psafe guidance information

## 4.2 Personal risks of mobile malware attacks

This section introduces a model, which maps malware attacks against mobile devices and coupled systems to personal risks of users. This model is a basis for the new warning approach in section 4.3. It is related to research objective 2 (section 1.3).

### RO2: Research of personal consequences of malware attacks to users of mobile devices.

In the literature the term 'risk' of a threat is defined as product of 'occurrence probability of a damaging event and severity of potential damage, caused by that event' [Eck08]. The risk is heavily dependent on the attacker model. This thesis focus on automated attacks via malware. The term 'personal'<sup>61</sup> should symbolise, that risks could impact persons. In the context of this thesis these are users of the mobile device. The term **personal risk** is defined in this thesis as: 'Malware triggered damaging impacts to human users of mobile devices and their coupled systems, including users' personal requirements, such as privacy, finances, personal and environmental safety, personal reputation, and availability of their personal equipment.'

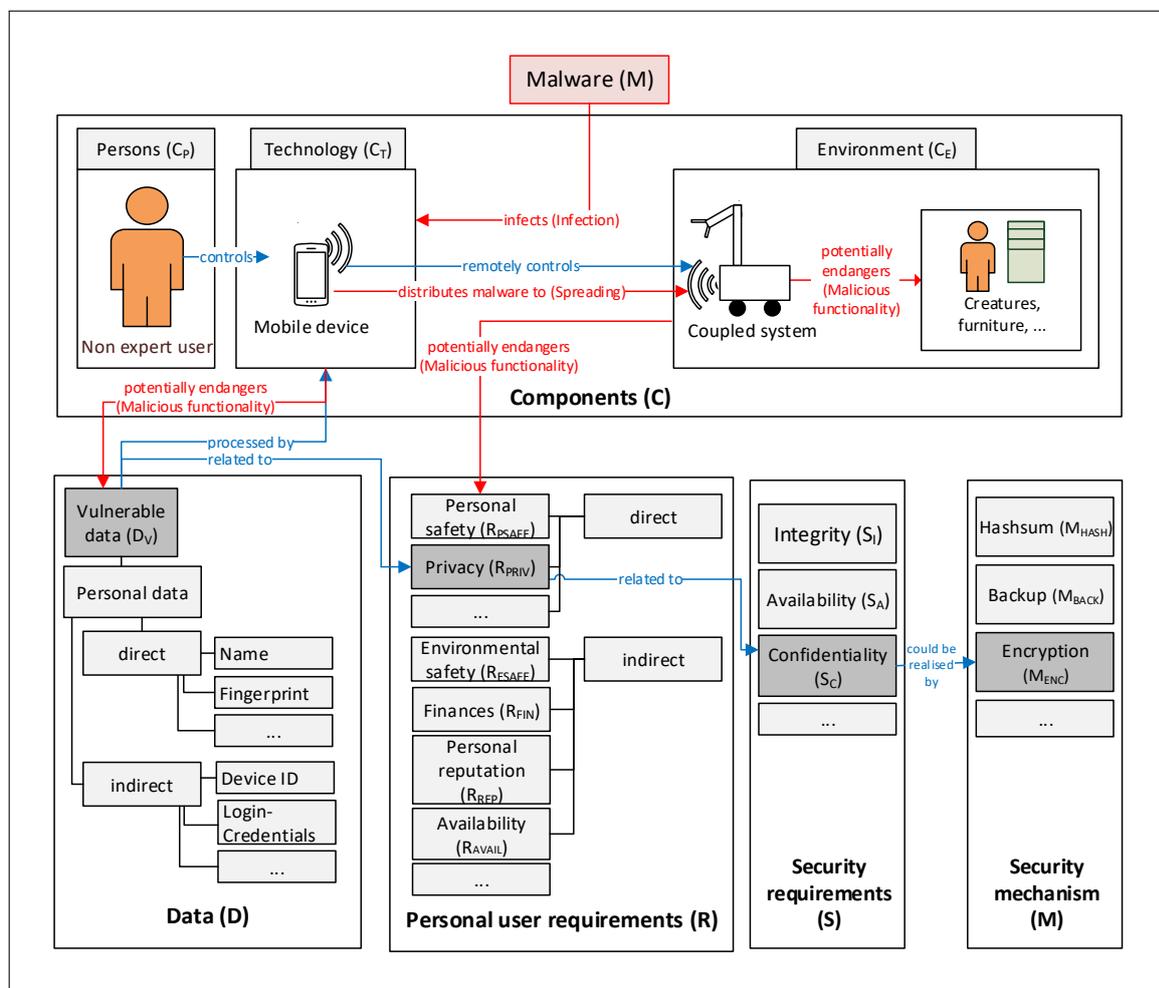


Figure 4.6: Overview of the personal risk model (based on [FDOF10] and [Bec09])  
(Note: red arrows: malware impacts, blue arrows: relations)

<sup>61</sup>The adjective term 'personal' is defined by the Cambridge dictionary as: 'relating or belonging to a single or particular person rather than to a group or an organisation', 'private or relating to someone's private life', and 'relating to your body or appearance' (Cambridge Dictionary, adjective 'personal', <https://dictionary.cambridge.org/dictionary/english/personal>, accessed: 27.11.17)

The **personal risk model** in figure 4.6 is inspired by two models. The first is an own metadata model for a secure data-management on embedded systems [FDOF10]. The second model is a classification of mobile malware activities by Becher [Bec09], introduced in section 2.3.2. In this thesis both models are used to model influences of malware attacks against mobile devices which potentially effect personal requirements of human users.

The **metadata model** is based on different submodels, examples are models for components, data on components, security and safety requirements per component and data. The personal risk model adapts and uses these submodels to describe personal risk of users of malware infected mobile devices and their coupled systems. The *component* model defines three classes ( $C$ ): technology ( $C_T$ ), persons ( $C_P$ ), and the environment ( $C_E$ ).  $C_T$  defines the technical components of the embedded system, roughly divided into soft- and hardware. Technical components in the context of this thesis are mobile devices, such as smartphones and tablets. The component *persons* ( $C_P$ ) includes single persons or group of persons, who interact with the component technology ( $C_T$ ). The component *environment* ( $C_E$ ) symbolises subjects and objects of the personal environment of users of mobile devices. Examples are unintended creatures (humans, animals), and technical systems, which could be coupled and remotely controlled by the mobile device or communicate with it. This thesis views on mobile systems, such as embedded systems and cyber-physical systems, e.g. mobile robots or cars.

For every single technical component in the metadata model the stored data, communicated data between components, and operations on data are modeled. The *data* ( $D$ ) in the metadata model are classified dependent on their intended use. This thesis focuses on personal risks of users, therefore 'vulnerable data' ( $C_V$ ) are defined as 'personal data'. Two categories are discriminated related to the General Data Protection Regulation [GDP16]. Whereas, 'direct' personal data (e.g. name, fingerprint) could be direct related to a person, 'indirect' personal data (e.g. device ID, login-credentials) could be indirect related to a person.

### **Personal user requirements:**

As introduced in section 2.3.2, Becher distinguished between three mobile malware impacts: monetary damage, data damage and hidden damage [Bec09]. Additionally to classical malware impacts on users privacy, this thesis focuses personal impacts, which occur if mobile devices are used as single devices or they are coupled with other systems, e.g. CPS. In comparison to Becher, the malware impacts in this personal risk model are related to user requirements, because it's a user-centred warning approach. On basis of Becher's mobile malware impacts an own description of *personal user requirements* is created. Mobile malware could impact personal user requirements directly and indirectly. *Direct personal requirements* are mobile device user requirements which are directly related to users ( $C_P$ ) health or life. *Indirect personal requirements* are indirectly related to users life, e.g. user's finances.

### Examples of **direct personal requirements**:

- *Privacy* ( $R_{PRIV}$ ): That is a user security requirement related to her personal data and information stored and communicated by the used mobile device ( $C_T$ ). Privacy-related malware attacks are related to personal data of the user (vulnerable data,  $D_V$ ), such as unauthorised usage of passwords/login credentials for online-banking. Another example are spying of privacy-related information by making audio or video recordings of the user and her environment. Other examples are unauthorised tracking of users locations of the mobile device using local GPS signals. Becher [Bec09] categorised these malware impacts as 'hidden damage', because these are often not visible for users.
- *Personal safety/Health* ( $R_{PSAFE}$ ): If mobile devices are coupled with other systems, such as CPS, mobile malware could be spread to it and malware activities on these systems could lead to malfunctions, which could endanger users personal safety and users life and limb. Beside the user itself also other persons (e.g. family members, friends, guests) could be in danger. Although, to date such attacks are not observed in reality, researchers show in prove-of-concept studies, that these attacks are realisable. Examples are attacks against mobile robots [VLG15] and modern cars<sup>62</sup> [HD14].

### Examples of **indirect personal requirements**:

- *Environmental safety* ( $R_{ESAFE}$ ): Beside their own safety users are also interested in the safety of their private environment, including their animals, and objects (e.g. personal belongings such as furniture, technology). Mobile malware could spread from mobile devices to remote controlled systems (section 2.3.2 'Mobile malware portability') and could cause system malfunctions. So amongst the mobile user also her environment could be in danger. Environmental damages could also lead to financial damages ( $R_{FIN}$ ) and damages of personal safety of other creatures ( $R_{PSAFE}$ ).
- *Finances* ( $R_{FIN}$ ): Another user requirement are finances. Becher described malware impacts on finances as 'monetary damage' [Bec09]. Current attack examples are ransomware attacks, which press money of users by encryption of their private data. Other examples are online-banking attacks, misusing of premium SMS or premium phone numbers, and attacks, which effect a higher device power consumption.
- *Personal reputation* ( $R_{REP}$ ): The publication of sensitive personal data, which is gathered by mobile malware, could be endanger the personal reputation of a person. Examples are sensible photos, video or audio recordings.
- *Availability* ( $R_{AVAIL}$ ): Another user requirement could be availability of the mobile device and their coupled systems. In cases the availability of devices is decreased, users have to wait till they could further use the mobile service. Exemplary attacks are denial-of-service (DoS) attacks. Exemplary malfunctions are the blocking of user interfaces or disabling of the device/system booting. These attacks also could have monetary effects ( $R_{FIN}$ ).

---

<sup>62</sup>Wired, Andy Greenberg, 'Hackers remotely kill a Jeep on the highway with me in it', <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>, accessed: 10.10.16

Another component in the metadata model are **security requirements** per data and component. The three classical security aims are confidentiality, integrity and availability. Security requirements are realised by security measures (see section 2.2).

Personal user requirements are direct or indirect related to security requirements. For example the personal requirement of privacy is related to the security requirement confidentiality. Both, privacy and confidentiality could be protected through encryption of personal data on the mobile device, which restricts the personal data access. Additionally, access protected personal data are less vulnerable to spied out by mobile malware, which may have indirectly positive effects on users' finances.

### **Malware activity phases:**

This thesis introduces a malware warning concept for mobile devices and coupled systems. Two application scenarios are distinguished: first, the *single usage of a mobile device*, and second, the *remote control* of a coupled system by a mobile device. Therefore, two main impact scenarios of malware attacks are classified. In the *first impact scenario*, malware attacks against a single mobile device are focused. They are referred to as '**first level impacts**', because the mobile device is the first target of the malware attack. Hoppe et al. called these impacts 'functional implications' [HKD09]. The *second impact scenario* describes malware attack impacts, which have their seeds in a malware infection of a mobile device which is coupled with another system for remote control. They are referred to as '**second level impacts**'. Hoppe et al. called these impacts 'structural implications' [HKD09]. The malware on the mobile device could spread to the coupled system, which could have manifold impacts to the system security and safety as well as to mobile device user's requirements. One example is the infection of a flying robot, shown in [SFH<sup>+</sup>12] for a quadcopter. The malware infected coupled system could also be spread malware to other coupled systems. These impact scenarios are referred to as '**third level impacts**', which are also 'structural implications' following the definition of Hoppe et al. [HKD09].

This thesis introduces a malware warning concept for mobile devices and coupled systems. Two application scenarios are distinguished: first, the *single usage of a mobile device*, and second, the *remote control* of a coupled system by a mobile device. Therefore, two main impact scenarios of malware attacks are classified. In the *first impact scenario*, malware attacks against a single mobile device are focused. They are referred to as '**first level impacts**', because the mobile device is the first target of the malware attack. Hoppe et al. called these impacts 'functional implications' [HKD09]. The *second impact scenario* describes malware attack impacts, which have their seeds in a malware infection of a mobile device which is coupled with another system for remote control. They are referred to as '**second level impacts**'. Hoppe et al. called these impacts 'structural implications' [HKD09]. The malware on the mobile device could spread to the coupled system, which could have manifold impacts to the system security and safety as well as to mobile device user's requirements. One example is the infection of a flying robot, shown in [SFH<sup>+</sup>12] for a quadcopter. The malware infected coupled system could also be spread malware to other coupled systems. These impact scenarios are referred to as '**third level impacts**', which are also 'structural implications' following the definition of Hoppe et al. [HKD09].

### First level impacts:

Becher [Bec09] distinguished between three phases of malware activities on mobile devices: infection, malicious functionality, and spreading. In the *infection* phase users may be influenced by their interaction with the mobile device if malware is installed or not, excluding infection ways without user interaction (e.g. worms). *Malicious features* of mobile malware may have direct impacts (e.g. privacy, personal safety) and indirect impacts to users of mobile devices (e.g. damages on finances, personal reputation, availability). The *spreading* of malware is possible over various channels, e.g. wireless communication, email, or phone network.

Table 4.2 introduces examples of 'first level impacts' on mobile devices and maps the malware impacts to personal risks of mobile device users. The first column are exemplary malware activities, which are based on Becher's [Bec09] classification of malware. It is assumed that these activities are detectable by current mobile anti-malware and intrusion detection applications. The last three columns are potential risks related to malware activities divided into *general short-term risks for the mobile device*, *direct* and *indirect personal risks* for mobile device users.

## 4.2. Personal risks of mobile malware attacks

Exemplary malware activities	Potential risks		
	General short-term risks for device	Direct personal risks	Indirect personal risks
<b>Infection of mobile device (first level impacts)</b>			
Infection without or with user-interaction (e.g. click on downloaded executable files, links of fraudulent e-mails and online links)	Malicious functions	Spying of personal information (Privacy, $R_{PRIV}$ )	DoS and remote control of system by an attacker (Availability, $R_{AVAIL}$ )
Infection over tethered or wireless communication links (e.g. Bluetooth, WLAN, NFC)	Spying of mobile device information for future criminal activities (e.g. malware spreading)	Spying of personal information (e.g. IMEI, device name) (Privacy, $R_{PRIV}$ )	DoS and remote control of system by an attacker (Availability, $R_{AVAIL}$ )
<b>Malicious function on mobile device (first level impacts)</b>			
Activation with startup of operational system (e.g. registry entries), Unintentional program call	Malicious malware activities	-	-
Placement as file on storage media (RAM, Flash, removable media)	Longterm placement, further spreading	-	-
Unauthorised eavesdropping of data	Disclosure of device data	Disclosure of personal data (Privacy, $R_{PRIV}$ )	Harm to persons reputation ( $R_{REP}$ ) and finances ( $R_{FIN}$ ) in case of data disclosure
Active communication (e.g. login trail, communication from the Internet, of other device)	Remote control of malware by attacker	Disclosure of personal data (Privacy, $R_{PRIV}$ ), Injury of user (Personal safety, $R_{PSAFE}$ )	DoS and malfunction of coupled systems (Sec/Safe), damage of objects and injury of other humans (Environmental safety, $R_{ESAFE}$ )
Passive communication (e.g. to the Internet)	Downloads of undesired software/modules	Disclosure of personal data (Privacy, $R_{PRIV}$ )	Malware spreading and infection of coupled systems (Sec/Safe)
Anomalous strong program activity (e.g. communication, processing)	Decreased availability of used system, Waste of energy	-	Availability ( $R_{AVAIL}$ ), Financial losses ( $R_{FIN}$ )
Unauthorised sending of personal data to the Internet	Unauthorised disclosure of personal data	Disclosure of personal data (Privacy, $R_{PRIV}$ )	Harm to persons reputation ( $R_{REP}$ ), finances ( $R_{FIN}$ )
Manipulation of device functions (e.g. calibration data, private sec. settings)	Decreased availability of used system	Manipulation of personal data (Privacy, $R_{PRIV}$ )	Financial losses ( $R_{FIN}$ ), Availability ( $R_{AVAIL}$ )
Denial of service (DoS) attacks (e.g. TCP flooding)	Decreased availability of used system	-	Financial losses ( $R_{FIN}$ ), Availability ( $R_{AVAIL}$ )

Table 4.2: Generic translation of examples of malware activities on mobile devices (first level impacts) to **personal risks** of mobile device users, (Note: '-': potentially no impact)

**Second and third level impacts:**

Table 4.3 introduces examples of 'second and third level impacts' of malware on mobile devices and maps the malware impacts to personal risks of mobile device users. The examples in table 4.3 are also found in some publications. As introduced in section 3.3 Vuong et al. developed and researched an intrusion detection system for mobile robots to detect several attacks. They described the effects of exemplary attacks in [VLG15]. Furthermore, results of own research activities in the field of industrial production are referred to in the table [DKF+10, FMG+11]

Exemplary malware activities	Potential risks		
	General short-term risks for device	Direct personal risks	Indirect personal risks
<b>Spreading to coupled systems (second level impacts)</b>			
<i>Spreading without or with user-interaction</i> (e.g. download and forward of malware infected executable files (e.g. e-mail attachments, patches, removable media files))	Malware infection and further spreading	-	Infection of coupled systems (Environmental safety, $R_{ESAFE}$ )
<b>Infection of coupled system (second level impacts)</b>			
Infection without user-interaction	Malicious functions	Spying of personal information (Privacy, $R_{PRIV}$ )	DoS and remote control of system by an attacker (Availability, $R_{AVAIL}$ )
Infection over tethered or wireless communication links (e.g. Bluetooth, WLAN, NFC)	Spying of coupled system information (e.g. IP, MAC, CPU name) for future criminal activities (e.g. malware spreading)	Spying of personal information (Privacy, $R_{PRIV}$ )	DoS and remote control of system by an attacker (Availability, $R_{AVAIL}$ )
<b>Malicious functions on coupled system (second level impact)</b>			
Manipulation of coupled systems' functions (e.g. robot control programs [DKF+10, FMG+11], calibration data [DKF+10], robot navigation map)	Misuse of coupled systems	Injury of user (Personal safety, $R_{PSAFE}$ )	Unexpected functionality, damage of objects and injury of other humans (Environmental safety, $R_{ESAFE}$ )
Active communication (e.g. login trail, communication from the Internet, of other device)	Remote control of malware by an attacker	Disclosure of personal data (Privacy, $R_{PRIV}$ ), Injury of user (Personal safety, $R_{PSAFE}$ )	DoS and remote control of system by an attacker (Availability, $R_{AVAIL}$ ), Damage of objects and injury of other humans (Environmental safety, $R_{ESAFE}$ ), Financial losses ( $R_{FIN}$ ), Malware spreading and infection of coupled systems (Sec/Safe)

## 4.2. Personal risks of mobile malware attacks

Passive communication (e.g. to the Internet)	Downloads of undesired software/modules	Disclosure of personal data (Privacy, $R_{PRIV}$ )	Remote control of system by an attacker (Availability, $R_{AVAIL}$ ), Financial losses ( $R_{FIN}$ ), Malware spreading and infection of coupled systems (Sec/Safe)
Anomalous strong program activity (e.g. communication, processing)	Decreased availability of used system, Waste of energy	-	Availability ( $R_{AVAIL}$ ), Financial losses ( $R_{FIN}$ )
Start of additional program modules	Misuse of the system	Disclosure of personal data (Privacy, $R_{PRIV}$ )	Remote control of system by an attacker (Availability, $R_{AVAIL}$ ), Financial losses ( $R_{FIN}$ )
Unauthorised sending of data to the Internet	Unauthorised disclosure of data	Disclosure of personal data (Privacy, $R_{PRIV}$ )	Harm to persons reputation ( $R_{REP}$ ), finances ( $R_{FIN}$ )
Denial of service (DoS) of coupled systems (e.g. TCP flooding)	Decreased availability of used system	-	Unexpected functionality (e.g. mobile robot: 'inconsistent stops' [VLG15]) (Environmental safety, $R_{ESAFE}$ ), Availability ( $R_{AVAIL}$ ), Charging (Finances, $R_{FIN}$ )
Disrupt of network communication (e.g. communication)	Decreased availability of used system	-	Unexpected functionality (e.g. mobile robot: 'frequent consistent stops' [VLG15]) (Environmental safety, $R_{ESAFE}$ ), Availability ( $R_{AVAIL}$ )
Injection of control commands to coupled system for manipulation	Decreased availability of used system	Injury of user (Personal safety, $R_{PSAFE}$ )	Unexpected functionality (e.g. mobile robot: 'frequent consistent jittering' [VLG15]) (Environmental safety, $R_{ESAFE}$ ), Availability ( $R_{AVAIL}$ )
<b>Spreading to other systems (third level impacts)</b>			
<i>Spreading without user-interaction</i>	Malware infection and further spreading	-	Infection of other systems (Environmental safety, $R_{ESAFE}$ )

Table 4.3: Generic translation of malware activity example on coupled systems of mobile devices (second and third level impacts) to **personal risks** of mobile device users  
(Note: '-': potentially no impact)

### 4.3 General warning design concept

---

This section introduces the design concept for the general user-centered effective malware warning approach for mobile devices. It is related to research objective 3 (section 1.3).

**RO3: Design of a general user-group specific effective malware warning concept for mobile devices.**

#### **General assumptions:**

For the creation of the warning concept are two assumptions made: first, the *user controls the system*, and second, the user is a *non-expert*.

**User controls the system:** The warning approach assumes that the user has the full control over the system (see research field and scenarios in section 1.1). The user has to be informed by the system about all system changes, e.g. app update, malware detection. On basis of this information the user has to decide what to do, e.g. update installation or cancel of update installation, malware remove or ignoring of remove.

**Non-expert user:** The user is a 'Joe public' user. In comparison to an expert user she has no specific knowledge (e.g. about computer technology, security, safety) and has no specific programming skills.

Figure 4.7 shows the composition of the general new warning design concept, which is a combination of state-of-the-art concepts and methods and own ideas. The new warning approach is determined by two main aspects: first, *user-group specific characteristics* (section 4.3.1) and second, *mobile device specific characteristics* (section 4.3.2). These both aspects also influence the both other elements of the warning approach, the *effective warning design* (section 4.3.3) and the usage of *multimodal feedback* (section 4.3.4).

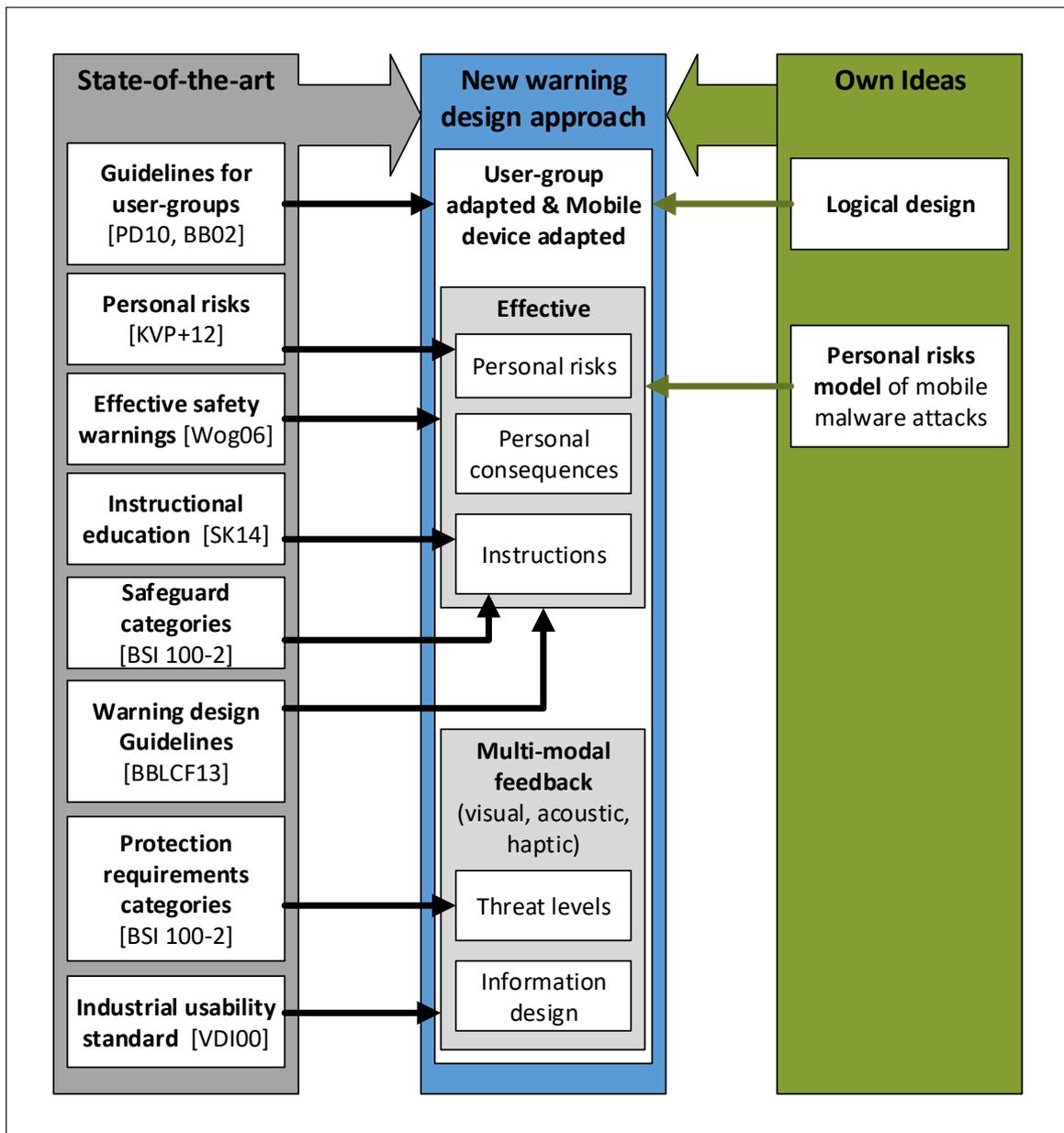


Figure 4.7: Major components of the warning design concept published in this thesis

### 4.3.1 User-group specific warning design

---

The focus lay on the protection of mobile device users not on a protection of the system. So the new warning design is highly depended on characteristics of the user-group (e.g. literacy, fine-motor skills). The warning design covers *warning content* (e.g. textual descriptions) and *warning layout* (e.g. arrangement of warning dialog elements), which have to be adapted to specific user-group needs.

#### **User-group definitions:**

The new warning design is highly depended on the user-group. On basis of the differentiation of user-groups in section 2.5.3 different user-groups and application cases are differentiated. The general warning approach is created for a generic user, which is defined as standard case.

#### **Standard case: Generic user:**

The generic user is an *adult* (aged 18 years or older), has *standard literacy* (e.g. could read and comprehend simple texts), has no mental handicaps (e.g. no dyslexia) and has no physical handicaps (e.g. no deafness, no blindness, no colour blindness). The user is familiar with the European culture (e.g. European colour coding, where red symbolises danger, green symbolises safety).

On basis of the definition of the generic user other variations and extensions of the standard case are defined. **Variations** are differences of single characteristics ('*individual variations*') or multiple user characteristics ('*class-specific variations*') in comparison to the generic user. *Individual variations* only differ in one specific user characteristic, e.g. vision or hearing. Exemplary user-groups are blind or deaf persons. *Class-specific variations* differ in multiple user characteristics, which are specific to one user-group, e.g. literacy and mental development. Exemplary user-groups are children or senior citizen. **Individual extensions** of the generic user are users with advanced capabilities in comparison to the generic user, e.g. knowledge of the system. Exemplary user-groups are experts, e.g. operators of complex systems, such as pilots, operators of nuclear power plants or chemical plants.

Beside the definition of the warning design for a generic user the design for the user-group **primary-children** as class-specific variation to the standard case is created (section 4.3.6). Both user-group specific warning designs are realised as test cases and evaluated with a user-study (chapter 5). The other variations and extensions of the standard case are discussed for future work research in chapter 7.

### 4.3.2 Adaption to mobile device characteristics

---

The warning design is also depended on and adapted to characteristics of the mobile device. The main restriction for the usage of multimodal warnings on mobile devices is the limited user interface [BFH<sup>+</sup>11]. The limitation of the user interface could considerable differ between different mobile devices, which could vary in size (e.g. screens) and technical equipment (e.g. quality of loudspeaker). Therefore, the warning appearance has to be well-considered (e.g. single page warning vs. pull-out warning contents).

The usage of multimodel feedback information could be limited by different configurations of the mobile device [Men11]. So four different **profiles** have to take into account: *first profile*, both sound and vibration are activated, *second profile*, only vibration is activated, *third profile*, only sound is activated, and *fourth profile*, nor sound or vibration are activated.

### 4.3.3 Effective warning design

---

The warning design approach based on the effective design approach for static safety warnings of Wogalter [Wog06b]. Wogalter's approach informs users about current risks, instructions, consequences of not complying instructions. The new warning approach adapts Wogalter's warning concept to raise warning effectiveness of active malware warnings on mobile devices. The warning literature recommends the using of personal risks to improve warning effectiveness (e.g. [KPV<sup>+</sup>12, HHWS14, MMHE17]). The new warning concept realises this recommendation by including *personal risk* and *personal consequences* of malware attacks into the warnings. Therefore, an own *personal risk model* was introduced in section 4.2.

Amongst personal information also **instructions** are included into the warnings. Instructions are an established method in the education, which are based on findings of the educational psychology [SK14]. Instructional design approaches offer the learner a structured expertise. In the warning approach instructions are used to give non-expert users a support to minimise or impede their personal consequences of malware attacks against mobile devices. The instruction design is derived from the *safeguard classes* of BSI standard [BSI08], which are grouped into safeguards for infrastructure, organisation, personnel, hard- and software, and communication and contingency planning. Only two types of instructions in the new warning approach are used to ease the understanding of non-expert users. That are instructions for technical security mechanisms and organisational security measures for mobile device users. Whereas *technical security mechanisms* are realised through the technical system itself, *organisational measures* include management and organisational aspects of the mobile device security. Examples of technical security mechanisms are check system with an anti-virus application, system switch off, or non-installation of an application. Examples of *organisational measures* are the contact of technical support or technology-savvy friend.

### 4.3.4 Multimodal feedback

---

Current security warning approaches mainly based on visual information (see related work in chapter 3) and only a few malware warnings uses a combination of visual and acoustic information (see Android app study in section 4.1). But industrial usability standards and guidelines (e.g. [VDI00, WHW09, KNB<sup>+</sup>09]) recommend the combination of sensory information to support human-machine interaction scenarios. So *multimodal feedback* is used to attract users attention to warnings and to ease the warning comprehension. That means warnings are designed as a combination of sensory information using visual, acoustic, and haptic information. Here the most used human senses in human-computer-interaction (visual, acoustic, haptic) [KNB<sup>+</sup>09] are included into the design concept. Approaches which are related to other senses, like smell or taste (e.g. electric nose [GB94, GO04]) are not included in this concept. Because this concept is designed for most used human-machine interfaces.

The combination of the three information types to one design is called 'logical design' [Bol98]. Table 4.4 illustrate the **general logical multimodal warning design**, which is divided into visual, acoustic and haptic design<sup>63</sup> [Bol98].

The general logical design is determined by **two main criteria**, first, the *threat scale* and second, the *information design*.

---

<sup>63</sup>Haptic information could be divided into tactile (sense of touch) and vestibular-kinaesthetic information (sense of motion). Here it would not be differentiated between these two sensory perceptions [KNB<sup>+</sup>09].

Criteria	Visual design	Acoustic design	Haptic design
Threat scale	<i>Colour coding</i> based on traffic lights and industrial standard [VDI00]	<i>Warning signal</i> (length, height, repeats)	<i>Vibration</i> (strength, duration, repeats)
	<i>Symbols/icons</i> from known domains (e.g. desktop IT-systems, road traffic)		
Information design	<i>Symbols/icons</i> from known domains (e.g. desktop IT-systems, road traffic)	<i>Speech output</i> (clear and slowly)	-
	<i>Text</i> (short, clearly, readable, large fonts, no technical terms)		

Table 4.4: General logical **multimodal feedback** design for a **generic user**  
(Note: -: not used)

**Threat scale:**

A threat scale is used to differentiate specific risk levels. A specific *risk level* is used, to warn users for specific personal risks and potential consequences of the current malware attack. Risk levels are differentiated by their combination of visual, acoustic and haptic design criteria. The definition of risk levels is inspired by the protection requirement categories of BSI [BSI08], which are defined on basis of specific damage scenarios (e.g. physical injury, financial losses). Because users are in focus of the warning approach the damage scenarios are related to users *personal requirements*, which are defined in section 4.2. Only four risk levels (including one normal state) are used to simplify the risk communication with non-expert users:

**Risk level 0 (normal operation):** The verification of a security application on the mobile device or coupled system is arrived to the conclusion that the usage of the mobile device or coupled system is *free of personal risks*.

**Risk level 1 (low):** The impact of any damage to personal requirements of users of mobile devices (including coupled systems) is *limited and calculable*.

**Risk level 2 (high):** The impact of any damage to personal requirements of users of mobile devices (including coupled systems) may be *considerable*.

**Risk level 3 (very high):** The impact of any damage to personal requirements of users of mobile devices (including coupled systems) may be of *catastrophic proportions*.

### 4.3. General warning design concept

Table 4.5 illustrates the three upper risk levels and their relation to the personal requirements of users. The visual design of risk levels also includes the usage of *differently coloured symbols or icons*, which are already used in mobile security applications (section 4.1). Examples are a red shield with an exclamation mark for the highest risk level, yellow triangle with an exclamation mark for middle risk level, and a green shield with a checkmark for no risk. This design criteria partly follows guideline 6 'consistent layout' of Bauer et al. [BBLCF13], which recommends only one icon which symbolises the risk severity. Amongst a coloured icon risk levels are also realised by acoustic and haptic information (table 4.4). Depending on the risk level acoustic signals differ in length, height, and repeats, and haptic feedback differ in strength, duration, and repeats.

Violation of personal requirements	Risk level 1	Risk level 2	Risk level 3
Violation of privacy ( $R_{PRIV}$ )	There is a low risk, that data or information of persons are affected (e.g. indirect data, such as access time to system).	There is a high risk, that data or information of persons are affected (e.g. indirect data)	There is a very high risk, that data or information of persons are affected (e.g. direct data, such video or audio live recordings of persons).
Violation of personal safety/health ( $R_{PSAFE}$ )	There is a low risk of injury.	There is a high risk of injury, but no danger to life and limb of persons.	There is a very high risk of serious injuries of persons, which endanger life and limb of persons.
Violation of environmental safety ( $R_{RSAFE}$ )	There is a low risk of violation.	There is a high risk of environmental violations.	There is a very high risk of serious violations of the environment (e.g. animals, objects).
Financial losses ( $R_{FIN}$ )	There is a low risk of financial losses.	There is a high risk of financial losses.	There is a very high risk of heavy financial losses.
Violation of personal reputation ( $R_{REP}$ )	Low risk of violation of personal reputation.	High risk of violation of personal reputation.	Very high risk of violation of personal reputation.
Availability ( $R_{AVAIL}$ )	The availability of the system is lightly affected, so small delays for users could occur.	The availability of the system is highly affected, so high delays for users could occur.	The availability of the system is very highly affected, so very high delays for users could occur.

Table 4.5: Definition of **risk levels** on basis of violation of personal requirements of the **generic user**

#### Information design:

Amongst the realisation of the threat scale also the warning information itself based on visual and acoustic information (table 4.4). The recommendations of warning research is included into the information design. Visual information are texts and icons, which could increase warning comprehension, if they used as combination (e.g. [Dew99, AM07]).

**Texts** describe personal risks, personal consequences, and offer users instructions and additional information to understand the current threat situation. *Simple and non-technical* texts ease the warning comprehension (e.g. [BBLCF13, SEA+09, BLCDK10, EMC+10, Har13]). So simple texts have low readability grades. Furthermore, text should be represented in *reasonable font size* (in respect to the display size), clearly readable, and displayed on a *uniformly coloured background* with high contrast. *Serif-free fonts* are recommended for this approach, because they are better to read on displays [JOA03]. Furthermore, texts should be as *brief* as possible (e.g. [BBLCF13, BVOP+09]). Felt et al. [FAR+15] mentioned that this is a challenging task to describe a threat in detail with a single short paragraph. So a trade-off between text brevity and warning comprehension has to take into account. Warning researcher also recommend to use a *specific risk description*, which has to be inform users about consequences of the risk if the warning is ignored in a *specific, explicit, and comprehensively* manner (e.g. [BBLCF13, BLCDK10, ES13]). This is realised by using information about personal risks and personal consequences. Additionally to symbols and icons a *speech output* could support the understanding of texts.

**Symbols and icons** are an additional part to texts, which should support the comprehension of textual descriptions. Examples are icons, e.g. shields, combined with specific symbols, e.g. biological virus, to symbolise a threat of malware infection of a mobile device [FKD11].

### 4.3.5 Generic warning layout

The above described four requirements of the new warning approach determines its layout. On basis of warning literature recommendations and own observations in warning user studies Bauer et al. suggest a **warning layout** [BBLCF13] (figure 2.4). In this thesis Bauer's approach is adapted to be useful for requirements of the new warning approach. Table 4.6 gives an overview of used aspects of Bauers guidelines and adapted items.

No.	Label of guideline	Examples of subcategories	New warning design
1	Comprehensively description of risk	Risk	Risk (malware activity)
		Consequences	Personal consequences (personal risks of malware activity)
		Instructions	
2	Concise and accurate content	User-group specific information	
3	Options	Two or more options	Options to switch to other views
4	Contextual information	Additional information	
5	Auditing information	Access changes	
6	Consistent layout	No close button, one icon, shade screen, primary text	
		Secondary text, question above option	Usage of warning views

Table 4.6: Warning design concept: Included and adapted parts of the warning design guidelines of Bauer et al. [BBLCF13] (Note: No.= Number of guideline)

The new warning design is mainly determined by *user-group specific* and *mobile device specific* characteristics. Bauer et al. do not make these difference.

*Mobile device specific* characteristics are realised with *option* buttons to switch to different warning views (*guideline 3*). The views are used to present different warning information (risks, consequences, instructions) and to switch to additional information (figure 4.8), which offers users *contextual information* (*guideline 4*) about the current malware threat. So the warning information is split to be adaptable to the limited display sizes of mobile devices (*guideline 6 - consistent warning layout*).

The *user-group specific warning design* follows *guideline 2*, which recommends *concise and accurate warning content*. In the warning approach these design recommendations are adapted to realise user-group adapted warnings (section 2.5.3). Furthermore, user-group specific warning design is also realised by follow *guideline 6 (consistent warning layout)*. In comparison to Bauer et al. different warning views are used. Additionally, user-specific characteristics are derived from general recommendations of human-machine interface guidelines for specific user groups which are currently the state-of-the-art (e.g. [PD10, BB02]).

*Warning effectiveness* is reached by a *comprehensive risk description* (*guideline 1*), including risks, consequences, and instructions (Wogalter [Wog06b]). The warning approach expands the risks and consequences aspects by using personal information based on a personal risk model (section 4.2). At which 'risk' is a specific malware activity (see tables 4.2 and 4.3). The 'personal consequences' symbolise consequences of users of malware attacks on mobile devices, which are related to personal user requirements (see figure 4.6). Additionally, the warning offers users instructions and additional information to support user's understanding of the current threat situation.

*Auditing information* (*guideline 5*) about access grants, access requests, and changes are related to user-group specific needs.

Figure 4.8 illustrates the **generic warning layout**, which includes:

1. A **main headline**, which indicates that following information belong to a *warning* or to *additional information*.
2. A single **icon**, which symbolises the *risk level* of the warning (section 4.3.4) or signals that additional information is displayed. The icon is always visible.
3. A **headline**, which summarises the following warning information for either personal risks, personal consequences, instructions, or additional contextual information. The headline is always visible.
4. A **description**, which displays warning information for either personal risks, personal consequences, instructions, or additional contextual information. This could be text as well as symbols and icons. The description is always visible.
5. A single **option** or **set of options**, whereby users could switch forward to other views of warning information (e.g. with 'Forward') or switch to read additional information (e.g. with 'More information') (figure 4.9). Only one option is offered if no additional information is presented or users switch from additional view to the main view.

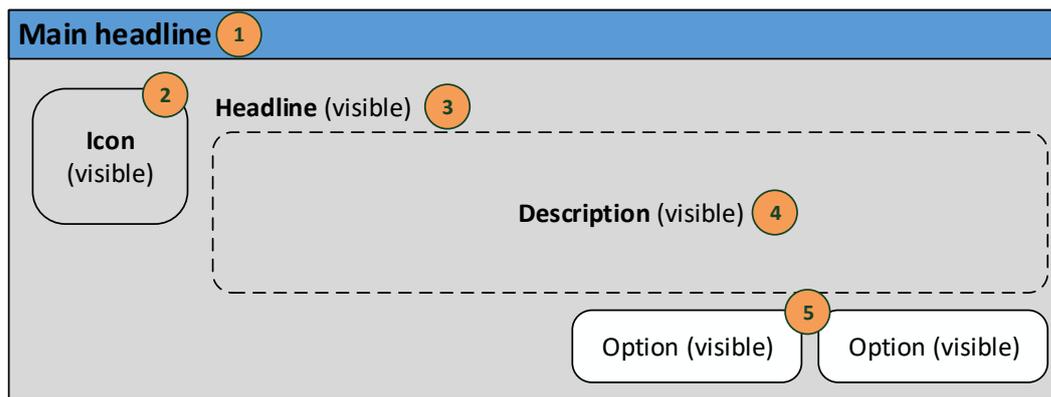


Figure 4.8: Generic warning design layout

The realisation of the warning design also depends on mobile device characteristics. Most tablets have larger displays to show warnings, in comparison to the most smartphones. Bauer et al. recommend the usage of warning information with one single main view and folding menus to show additional explanations. In the new warning design information (personal risk, personal consequences, instructions, additional information) is split into small pieces and presented successively by different warning views. Figure 4.9 shows an example of splitting information of the current risk and additional information in two different views. The information splitting is useful for mobile devices with limited displays, but it also serves to ease the comprehension of warning content for non-expert users.

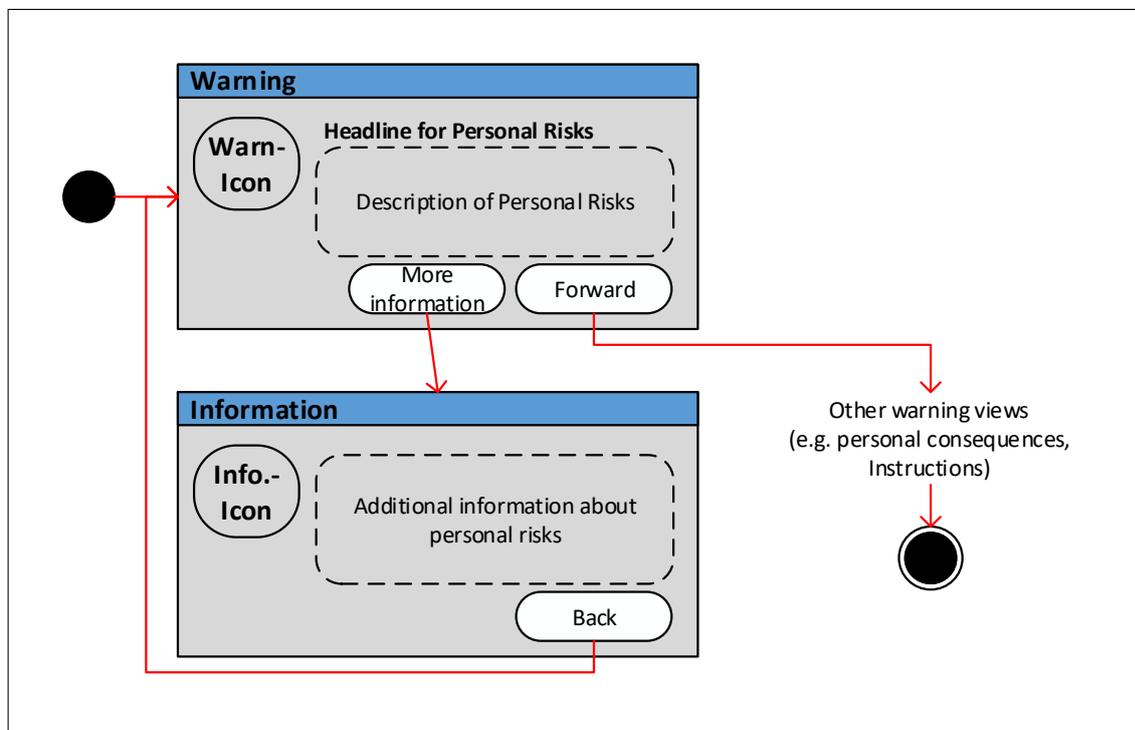


Figure 4.9: Example of different **warning views** represent as UML activity diagram

On basis of the introduced generic warning design approach two user-group specific warning design instances are considered, which are differ in design, user-group, and application scenario. The first warning instance is designed for a generic user (adult) in a remote-control-scenario of a domestic robot via a tablet (section 5.1). The second warning instance is prepared for a single usage scenario of a smartphone by primary-school children (section 5.2). In the following section the generic warning design for primary-school children is introduced.

#### 4.3.6 Generic warning design for primary-school children

---

In this section the generic warning design approach for primary-school children as class-specific variation of the generic user is introduced and differences to the standard case are described.

##### **User-group specific warning design:**

Commonly, primary-school children are between 6 and 10 years old. It is assumed that these children have no mental/physical handicaps, a standard literacy, and are familiar with the European culture. As already mentioned in section 2.5.3 children - especially younger children - differ in their mental abilities (e.g. literacy) and physical abilities (e.g. control a computer mouse) in comparison to adults. Examples are their *thinking* in a world of fantasy and dream of magic, their *problems to read long and complicated texts* (where girls in comparison to boys tend to have better verbal skills), and their *low frustration tolerance* if they are overwhelmed with too much information. The warning design has to be adapted to childrens' characteristics.

##### **Adaption to mobile device characteristics:**

Already primary-school children use mobile devices, such as smartphones and tablets regularly [FPR17]. In this thesis it is assumed that parents wouldn't them allow to remotely control safety relevant systems, such as mobile domestic robots or cars. But there exist a lot of *toys*, which could be remotely controlled by apps installed on mobile devices of children. Examples are robot toys from manufacturers, such as robot kits of TinkerBots<sup>64</sup> or drones from Parrot<sup>65</sup>. Malware attacked and misdirected toys may also impact the safety of persons and integrity of creatures and objects in the environment, but to a more minor degree [SFH<sup>+</sup>12]. Because in comparison to other systems, these toys are build of light material and could only used in a limited range caused by low capacity of their batteries.

##### **Effective warning design:**

The warning design for the desired user-group is also includes information about risks, personal consequences, instructions, and additional information. These are realised in a child-friendly way. Recommended are more simple descriptions in comparison to the generic user-group. Information in *instructions* are separated into operations, which children could do alone (e.g. switch off the mobile device) and operations which have to realised by parents, or other adults (e.g. using an antivirus app, call the technical support).

---

<sup>64</sup>TinkerBots, <https://www.tinkerbots.de/en/about-us/control/>, accessed: 15.03.18

<sup>65</sup>Parrot, <https://www.parrot.com/global/drones/parrot-ardrone-20-elite-edition#parrot-ardrone-20-elite-edition>, accessed: 15.03.18

**Multimodal feedback** (according to [MTF<sup>+</sup>12]):

Table 4.7 illustrates the *general logical multimodal warning design* for children. The main difference to the generic user is the *visual design*, which is adapted to childhood experiences. Thus, the design should be imaginative, e.g. cartoon or comic characters could be used [FSRD13]. Reduced presentations for children in television are used in order to clarify the difference between reality and fiction. Those design criteria for digital media can also be used for security warnings on mobile devices. Derived from that, a *fantasy cartoon character* is used in the design scheme. A fantasy character in cartoon or comic style should be known by children from the television program and is thus based on the childrens world of experience.

**Threat scale** (according to [MTF<sup>+</sup>12]):

A threat scale is used to differentiate specific *risk levels* as combination of multimodal feedback information. The user-group specific risk levels are based on damage scenarios related to personal requirements of primary-school children. These differ in comparison to adults mainly in three aspects (table 4.5): financial losses, violation of personal safety/health, and violation of environmental safety. Children are not fully capable to contract. In cases of *financial losses* caused by children their parents or custodians are responsible. One example is the subscription of specific apps. But children also not responsible for consequences of malware-attacks, e.g. decryption of encrypted personal data by mobile ransomware. Children use mobile devices and could couple them with several toys. But the impact to persons (*personal safety/health*) and environment (*environmental safety*) of misdirected toys is limited because of their light building materials, and their limited range [SFH<sup>+</sup>12].

Risk levels are differentiated by their multimodal design. Visual differences are realised through colour-coding and usage of symbols or icons. Here, it would be important to use such colour-coding analogies and icons which are known to children, e.g. traffic lights. Other concepts, which lie beyond the experience of children (e.g. a speedometer) should not be used. The combination of visual information with acoustic and haptic signals should reinforce the effect of the security warning. *Guides* in cartoon style, so called 'cartoon characters' could help children to get access to abstract information. Risk levels for children could be also expressed by different colored cartoon characters.

**Information design** (according to [MTF<sup>+</sup>12]):

Information for primary-school children is visually represented as typography, symbols, icons, and cartoon characters. Attention should be paid to the fact that reading can be difficult for primary-school children. Thus, important information should be communicated directly and concretely in a short and child-friendly *text*. It is recommended for children to use symbols/i-cons in *comic style* to support the comprehension of texts in the warning. Other requirements to texts (e.g. serif-free fonts, readability) are similar to the generic user-group. Additional usage of speech output could facilitating the handling the textual information also for children.

In summary, the **logical design**, the combination of optical, acoustic and haptic designs, should guide childrens attention to the security warning messages and help them to understand the message content and its severity. The usage of multimedia signals can facilitate childrens handling with security warnings, but it is important not to distract them with too many media signals.

Criteria	Visual design	Acoustic design	Haptic design
Threat scale	<i>Colour coding</i> based on traffic lights	<i>Warning signal</i> (length, height, repeats)	<i>Vibration</i> (strength, duration, repeats)
	<i>Icons</i> in comic style from known domains (e.g. road traffic)		
	<i>Guide</i> as cartoon character		
Information design	<i>Symbols/icons</i> in comic style from known domains (e.g. road traffic)	<i>Speech output</i> (clear and slowly)	-
	<i>Text</i> (short, clearly, readable, large fonts, no technical terms)		

Table 4.7: General logical **multimodal feedback** design for user-group **children**  
(Note: -: not used)

The **generic warning layout for primary-school children** adapts the warning layout of the generic user (figure 4.8) to needs of primary-school children. One main difference amongst the child-friendly contents are the usage of a cartoon character guide instead of an icon to express specific risk levels.

## 4.4 Evaluation methodology and concept

This section introduces the evaluation methodology for this thesis, including the *general evaluation designs for the both test cases* (section 4.4.1), the *general evaluation methods and test metrics* (section 4.4.2), and the *evaluation concept* for the both test cases (section 4.4.3). This work is related to research objective 4 (section 1.3).

**RO4: Evaluation of the general user-group specific effective malware warning concept to measure the warning effectiveness.**

### 4.4.1 Generic design of both test cases

This section introduces the experimental design of the two different test cases (figure 4.10) of two instances of the generic warning approach (section 4.3). Furthermore, the *basic design aspects* and *quality criteria* of the tests are described, which based on state-of-the-art evaluation methods from usability and security warning research (section 2.6).

The new warning approach is determined by two main aspects, *user-group specific* characteristics and *mobile device specific* characteristics. These both aspects also influence the both other elements of the warning approach, the *effective* warning design and the usage of *multimodal feedback* information (see section 4.3). The two test cases differ in their realisation of the warning approach regarding these four mentioned influencing design aspects.

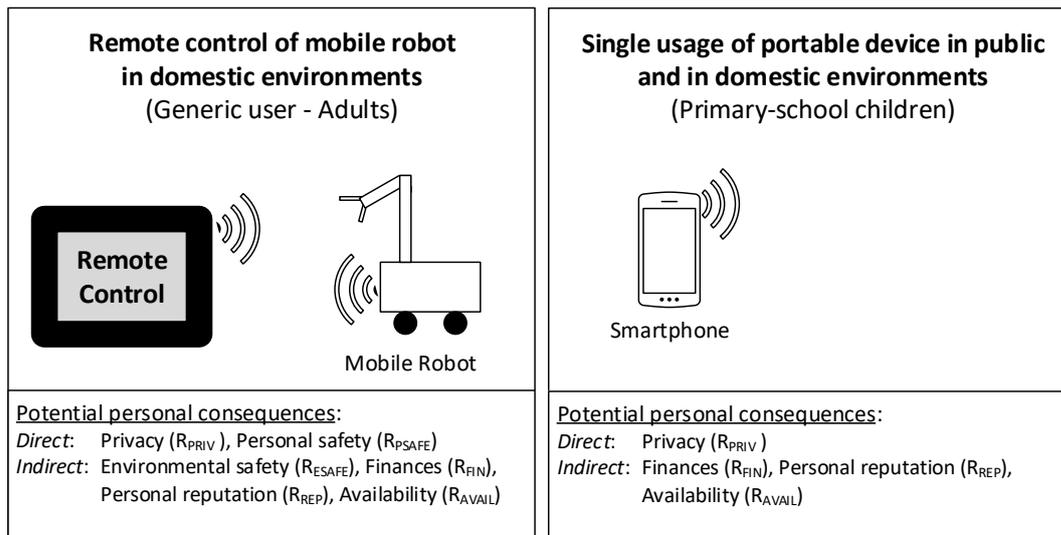


Figure 4.10: Test cases of two instances of the generic warning approach in this thesis

**Test cases:**

Every test case is a *specific adaption of the general warning approach* introduced in chapter 4.3. The warning is adapted to needs of specific *target user groups* (adults and primary-school children). All test persons are average users with no mental and no physical handicaps. Furthermore, they are all native German speakers with no specific previous knowledge of security, safety, and software development. The participants of both test cases differ in average age, previous technical experiences, possibility of remote control a to a mobile device coupled system and the level of severity of potential personal impacts of malware. Additionally, the test cases differ in their usage of a mobile device (tablet and smartphone). Figure 4.10 illustrates the test case specific *application scenarios*, where the test case specific warnings (see sections 5.1.1 and 5.2.1) are evaluated. The application scenarios differ in possibility of interaction of humans with mobile devices as remote control of a mobile device coupled system. The two test cases are briefly introduced. Detailed information about test case realisation is found in chapter 5.

**Test case 1:** *Human-robot-interaction of adults via tablet remote control in a domestic environment*

The application scenario is a remote control of a domestic mobile robot with a standard **tablet**. The test case simulate malware attacks of a mobile robot in a domestic environment. These attacks are classified as second level impacts on remote controlled systems in the personal risk model in section 4.2 (see figure 4.6 and table 4.3). The target user group are **adults** (defined as generic user). The test is realised in an office environment, where two domestic rooms (sitting room, kitchen) are simulated. Because giving participants a **primary task** is important to create a real scenario, the main task of the participants is the control of a mobile robot with a tablet.

The participants are divided into two groups: experimental and control group (between subjects test). Every group test a different variant of the warning approach (warnings with and without instructions). The display order of warnings is static and related to specific use-case scenarios (figure 5.11). A static order is used to simulate realistic warning scenarios for the test persons. The warning scenarios are related to specific user behaviour regarding the mobile robot. For example warning 4 'Unknown software autostart' is displayed if the test person want to install a chore app. The security warnings inform users about direct and indirect personal consequences of malware activities on the tablet and the mobile robot (see figure 4.10).

##### **Test case 2:** *Interaction of primary-school children with a smartphone*

The application scenario is a handling of a smartphone, which has no connection to another system. The single usage of the system reduces the potential malware related threat, the **primary-school children** are confronted with in the warnings. These attacks are classified as first level impacts on a mobile device (smartphone) in the personal risk model in section 4.2 (see figure 4.6 and table 4.2). The test is realised in a class-room environment, which the children are familiar with. So the fear of children should be decreased. The participants also get a primary task to create a real scenario. Their main task was to paint a picture in an app on their smartphone. All participants test the same warning variant (within subjects test). The security warnings inform children about direct and indirect personal consequences of malware activities on the tested smartphone (see figure 4.10).

##### **Basic test design aspects:**

The evaluation of the introduced warning approach is related to usability and security warning studies (see section 2.6.3).

**Independent variables** of the two test cases are *warning design* decisions for specific target user-groups, specific mobile devices, and specific application scenarios. Examples are design of warning information, icons, and location of buttons. Furthermore, the *experimental types* are independent variables. In test case 1 two test-groups are used, which evaluate a specific warning variant. The 'between subjects test' should evaluate whether instructions in warnings support warning effectiveness. In test case 2 one test-group evaluated one new warning design. The 'within subjects test' should find hints, if children who read warning information or additional background information are more adequately react to the warning in comparison to the others, who only clicked through the warnings.

Common **depended variables** of the two test cases are relating to the two aspects of *warning effectiveness* evaluated in this thesis. First aspect is the *comprehension* of warning information (personal risks and personal consequences). Test persons comprehend warning information, when they could explain the underlying risks and consequences of the malware attack. Second aspect is the adequate *reaction* after reading warning information and instructions. Test persons adequate react to the warning, when they are able to find adequate solutions to react to current malware threats.

Amongst above mentioned depended variables there are other ones. In *both test cases* the correlation between the warning design and the previous experiences of users with malware (test case 1) and mobile devices (test case 2) is evaluated, to find hints for which user group the new warning design is usable. Additionally, users' click-rates in warnings is logged and observed to get hints, if warning information is read. Furthermore, in *test case 1* the connection between the new warning design and the desire for external help is evaluated. The aim is to find indicators whether the new warning design better guides users through security risk decision processes in comparison to standard warnings.

### **Hypothesis:**

The evaluation with user studies should support the main *hypothesis*<sup>66</sup> of this thesis, that the use of personal information (personal risk, personal consequences), instructions and background information in warnings should increase effectiveness of the warning. Indicators for success are user's comprehension of warnings content and to find adequate solutions on basis of warning instructions. The hypothesis of both test cases describe, how the independent and dependent variables are connected to each other. Table 4.8 listed all hypothesis of both test cases.

### **Hypothesis for test case 1 (Adult-Robot-Interaction):**

**H1:** *Test group members with instructions (evaluation group, EG) will be more likely to rate usefulness of warnings higher than the control group (CG).*

In comparison to CG members EG members get information about solution possibilities of the current threat. Therefore, it is assumed that EG members will rate the usefulness of the warnings higher.

**H2:** *Evaluation group members will be more likely to desire less external help than the control group.*

The evaluation group (EG) is guided through situation-specific warning instructions. So EG members have more information what to do against the malware-related threat, in comparison to the control group (CG). Therefore it is assumed, that EG members do need less external help in comparison to the control group.

**H3:** *Evaluation group members will be more likely to rate comprehension of warnings higher than the control group.*

It is assumed, that EG members better comprehend the warnings in comparison to CG, because they are confronted with additional warning instructions.

**H4:** *Evaluation group members will be more likely to decide to heed the warning than the control group.*

It is assumed, that more EG members decide to follow the warnings in comparison to CG, because they are supported by additional warning instructions.

---

<sup>66</sup>Note: In this thesis no classical hypothesis testing [BS10] is realised, because of the small samples of test persons. The author has some 'ideas/assumptions' about the evaluation results, which are named 'hypothesis', but these are no classical hypothesis. These could be supported or not supported by the evaluation results.

ID	Hypothesis
<b>Test case 1 (Adult-Robot-Interaction)</b>	
H1	Test group members with instructions (evaluation group, EG) will be more likely to rate the usefulness of warnings higher than the control group (CG).
H2	Evaluation group members will be more likely to desire less external help than the control group.
H3	Evaluation group members will be more likely to rate the comprehension of warnings higher than the control group.
H4	Evaluation group members will be more likely to decide to heed the warning than the control group.
<b>Test case 2 (Child-Smartphone-Interaction)</b>	
H1	Children who read general warning information (without 'Why?' view) will be more likely to react adequately according to the warning instructions.
H2	Children who read additional information ('Why?' view) will be more likely to react adequately relating to the warning instructions.

Table 4.8: Hypothesis of both test cases

**Hypothesis for test case 2 (Child-Smartphone-Interaction):**

**H1:** *Children who read general warning information (without 'Why?' view) will be more likely to react adequately according to the warning instructions.*

General warning information provides information about the current risk and instructions to handle the risk. It is assumed that the children, who read this general information - without reading background information in the 'Why?' view - react more adequately according to the warning instructions in comparison to other test persons.

**H2:** *Children who read background information ('Why?' view) will be more likely to react adequately relating to the warning instructions.*

The 'Why?' view of the warning includes additional background information about the current malware-related risks, its damage potential to users and instructions to handle these risks. One exemplary risk is the malware infection of the smartphone with an update, which should not be installed. It's assumed that the children, who read these additional information, are more sensitised for the current threat and therefore react more adequately according to the warning instructions in comparison to other test persons.

**Study ethics:**

All gathered personal data (e.g. age, sex, opinions) of participants in both test cases are stored anonymised. But due to the small sample sizes no complete anonymisation could be guaranteed. Therefore, only aggregated information not the whole raw data set is published.

### 4.4.2 General evaluation methods and test metrics

---

This section introduces the chosen evaluation methods of the introduced user-centred warning approach based on fundamentals in section 2.6.3. According to Preim et al. [PD15] it is very important for user-centred approaches to realise *empirical studies* with representative users. Examples of empirical studies are tests of warning approaches where participants resolve specific tasks. Methods of usability tests are used to evaluate the warning effectiveness of the introduced approach. As introduced in section 2.6 usability studies measure quantitative and qualitative factors. *Qualitative factors*<sup>67</sup> are subjective values, such as test persons' opinions (self-reported metrics) and their behaviour (behavioural metrics). Exemplary methods to gain subjective values are questionnaires and observations. *Quantitative values* are objective values, such as interaction measures with warnings. One exemplary method is the logging of click events of warning buttons to estimate **click-through rates** of warnings. Click-through rates measure, how fast users' click through warnings and it could be estimated how much attention users pay to warnings. The logging of click events is used in combination with observations to estimate whether warning information is read by test persons.

The **test metrics** are related to the above described evaluation methods. In the following the common criteria of test metrics for both test cases are described.

Warning **comprehension** is evaluated with questionnaires and observations. *Questionnaires* are mainly designed with selection tasks (dichotomous tasks and multiple choice tasks) and rating tasks, because of their advantages of quick response of test persons and easy analysis. No middle category of rating tasks is used to get valuable results. Mostly verbal scales instead of numeric scales are used to ease the comprehension of responders. Exceptions are ratings with grades. High rated answers of test persons indicate that the warnings are adequate designed to specific needs of a test group. *Observations* include non-verbal behaviour of test persons, e.g. body language. For example wrinkly forehead and/or scratch of forehead indicates that test persons think about something. Furthermore, the method of thinking aloud is used. This information indicates whether test persons could adequately handle warning interaction or whether they have problems with it. For example the comment 'What should I do?' indicates the test person does not understand the warning information. A structured observation protocol is prepared to write down non-verbal behaviours and verbal comments of participants (sections 8.1.4 and 8.2.3). Additionally, test persons are asked to verbalise their potential ideas to solve the current problem, which they are warned for.

**Reaction/problem solving** is measured with questionnaires, observations, and logging of users' click events.

*Objective values* are measured with *logging of users' click events* on warning dialogue buttons. It should be evaluated whether warning information is **read** by users. *Estimation about reading of warning information* is based on time durations between one warning button click event to another, stored in log files and observations written in protocols. Measured time durations between two click events and observed reading activities of test persons are indicators for detailed reading of warning contents.

Table 4.9 summarises the chosen evaluation methods related to the dependent variables.

---

<sup>67</sup>Due to better analysis qualitative factors are stored as numerical values.

#### 4.4. Evaluation methodology and concept

Dependent variables	Evaluation methods for qualitative factors	Evaluation methods for quantitative factors
Comprehension	<i>Questionnaire</i> (mostly dichotomous selection tasks and rating tasks)	-
Reaction/problem solving	<i>Observations</i> (body language, thinking aloud)	<i>Log of click events</i>
Reading of warning information	<i>Observations</i> (body language, thinking aloud)	<i>Log of click events</i>

Table 4.9: Evaluation methods for qualitative and quantitative factors

#### 4.4.3 Evaluation concept

The following section describe the specific evaluation concept, including *evaluation methods* and *test metrics*, for the two specific test cases (section 4.4.1).

##### Test case 1: Adults

The aim of the test is to evaluate the warning effectiveness by measuring *comprehension* of warning information, influence of warning to *decision-making*, and *reaction* to warning instructions. The *comprehension of warnings* is measured with quantitative and qualitative evaluation methods. Indicators for reading or ignoring of warning information could be logged (logfile generation in figure 5.7) and also observed. **Logging** generates objective values. In this test case time stamps of click events on all warning buttons<sup>68</sup> are logged and compared with observations. The display order of warnings is static and related to specific use-case scenarios (figure 5.11). A static order is used to simulate realistic warning scenarios for the test persons. The warning scenarios are related to specific user behaviour regarding the mobile robot.

**Observations** are used to check whether participants read or ignore warning information. Additionally, the method of thinking aloud is used to evaluate whether test persons comprehend warning information, and how warnings provide participants to find own solutions for the current problem described in the warning. A structured protocol (figure 8.1.4 in appendix) is used to write down non-verbal user behaviour and verbal user comments.

An **online questionnaire** is prepared to get detailed qualitative values about test persons about all evaluation questions. Figures 8.3, 8.4, and 8.5 in appendix introduce the questionnaire. It is partitioned in six chapters related to six test specific evaluation questions (EQ, see table 4.10). Table 4.11 give an overview which depended variable relates to which test specific evaluation questions (EQ). The average is computed for results of EQ2 till EQ4 to compare the test results of both groups. Therefore, table 4.11 includes the ranges of average ratings for EQ2 till EQ4<sup>69</sup>. The average ranges for middle category are smaller, because of assumption of more ratings in this scale in comparison to low and high scale. Questions of EQ1, EQ5 and EQ6 are a combination of dichotomous selection tasks and rating tasks. According to test theory (section 2.6.3) these ratings should not be combined with each other, because the margins of the normal distribution are increased, which could falsify test results. Therefore the ratings for these questions are not averaged.

<sup>68</sup>Dialogue buttons for both groups - evaluation (EG) and control group (CG) - are 'Forward' and 'OK' buttons. The evaluation group (EG) had also the 'What can I do button?' button, because they had one more warning - the instruction information.

<sup>69</sup>For EQ2 - Knowledge the dichotomous selection tasks are ignored to summate the results.

Classification	Characteristics
<b>User study/survey</b>	
Environment	Office rooms in Faculty of Computer Science in Otto-von-Guericke-University of Magdeburg
Participants	23 test persons (7 men and 16 woman)
	all native German speakers
	Previous knowledge: different knowledge of malware and experiences for usage of Internet devices
Preparation	Introducing of testers, description as software evaluation
Execution	3 phases: 1) Introduction (5-10 min) 2) Operation of the robot remote control (20 min) 3) Online-Questionnaire (20-30 min, design criteria and comprehension of warning messages)
<b>Evaluation methods</b>	
Measurement of quantitative values	Logging of click events
Measurement of qualitative values	1) Observations (body language, thinking aloud, problem solving) 2) Online-Questionnaire
<b>Research questions</b>	
Previous experiences (EQ1)	<i>Questionnaire</i> (experiences with malware, using of mobile devices with Internet-connection, general Internet-usage)
Knowledge (EQ2)	<i>Questionnaire</i> (existence of malware for smartphones and tablets, responsibility of different groups and user activities for distribution of malware)
Usefulness of warnings (EQ3)	<i>Questionnaire, observations</i> (fun while handling the robot, helpfulness, uncertainty, and concern of warnings, additional help)
Comprehension of warnings (EQ4)	<i>Questionnaire, observations, logging</i> (rating of risk level, comprehension, influence of decisions and behavior by warnings)
Future of Internet of Things (EQ5)	<i>Questionnaire</i> (rating of likelihood of infection of IoT with malware, usage and future purchase of IoT devices)
Socio-demographic characteristics (EQ6)	<i>Questionnaire</i> (sex, age, profession)

Table 4.10: Evaluation environment and methods for *test case 1 (Adult-Robot-Interaction)*

Because of their simple response and analysis mainly selection tasks are used. Exceptions are socio-demographic characteristics of test persons, which are measured with *short essay tasks*. Two types of selection tasks are used, dichotomous selection tasks (yes/no requests) and rating tasks. One exemplary *dichotomous selection task* is related to previous experiences in Q11: 'Have you ever been a victim of a computer virus/Trojan horse or bothering software?'. 'Yes' indicates the test person had experiences with such malware. 'Yes' responds are rated with 2 points, 'no' responds with 1 point.

#### 4.4. Evaluation methodology and concept

Specific evaluation question	Dependent variables	Purpose	Average range (low, middle, high)
EQ1: Previous experiences (malware, Internet)	-	Result interpretation	-
EQ2: Knowledge (mobile malware and their distribution)	-		14-38, 38-60, 60-84
EQ3: Warning usefulness (helpfulness, uncertainty, concern, additional help)	-		8-22, 22-34, 34-48
EQ4: Warning comprehension (risk level)	-	Warning effectiveness	10-27, 27-43, 43-60
EQ4: Warning comprehension (comprehension)	Warning comprehension by target user-group		10-27, 27-43, 43-60
EQ4: Warning comprehension (decisions)	Influence of decision-making by warning design		10-27, 27-43, 43-60
EQ4: Warning comprehension (reaction)	Adequate reaction of target user-group to warning instructions (only for evaluation group)		10-27, 27-43, 43-60
EQ5: Future of Internet of Things (malware and usage)	-	Result interpretation	-
EQ6: Sociodemographic characteristics (sex, age, profession)	-		-

Table 4.11: Questionnaire: Relation of dependent variables to specific evaluation questions for test case 1

*Rating tasks* based on verbal scales to ease the interpretation of responders. Even rating categories are used to avoid neutral middle category. A unipolar scale with 6 categories is used, where high points indicates test persons' support of the evaluated item: 1-2: no/very less support, 3-4: less/rather support, 5-6: (highly) support of evaluated item. Examples are questions regarding the comprehension of warnings (Q43\_WMNo\_02 in figure 8.4). Rates of 5 and 6 mean, that single warnings were (very)<sup>70</sup> comprehensible for test persons.

Additionally, ratings of question categories to the six specific evaluation questions are summed. These *summed responds* are used to compare results of both test groups. High points for one test-group indicate that in average the test-group support the evaluated item. Examples are averaged rates for comprehension of all 10 evaluated warnings. Rates of 43-51 and 51-60 for one test-group indicate, that all warnings were in average (very) comprehensible to the test-group.

<sup>70</sup>The description is shortened to summarise two ratings. One example is '(very) comprehensible', which includes ratings of 'comprehensible' and 'very comprehensible'.

### Test case 2: Primary-school children

This section introduces the evaluation concept for smartphone warnings prototype for primary-school children based on the bachelor thesis of Wiebke Menzel [Men11] and a collective publication [MTF<sup>+</sup>12].

The aim was to evaluate the warning effectiveness by measuring the *comprehension* of warning information, and *reaction* to warning instructions. The *reaction* to warnings (EQ1) is measured with quantitative and qualitative evaluation methods. **Logging** is used to find indicators whether test persons read background information of the current warning. Therefore, user click events on the 'Why?' button are logged. The *display order of warnings* is dynamical to evaluate the importance of time and display order of warnings (EQ3). The test time is divided into 9 time slots, where 1 symbolises the test start and 9 the test end. The amount of displayed warnings depended on test person's reactions to previous warnings (section 5.2.1). Maximum 9 warnings are displayed in a variable order.

*Comprehension of warnings* (EQ1) is measured with *observations*, a post-test *questionnaire*, and *logging* of users' click events on the 'Why?' button. **Observations** of non-verbal user behaviour and verbal user comments are written down in a structured protocol (figure 8.2.3 in appendix). Here are notated, whether test persons read or ignore warning information. Furthermore, their thoughts about meaning of warning and their thoughts about their potential reaction to the warning are written down.

A **questionnaire** is used to answer the five specific evaluation questions (EQ1,2,4,5,6). The questionnaire is especially designed for primary-school children (figures 8.11 and 8.12 in appendix) to maintain test candidates concentration and to facilitate their processing. The design includes short questions with an appropriate font size, many images, and symbols. The test person is guided by a supervisor, which reads the questions out according to and enters the corresponding marks or answers to open question responses.

**Logging** of 'Why?' button click events is used to find indicators whether test persons read background information of the current warning.

Table 4.13 gives an overview, which of the five specific evaluation questions (EQ) in table 4.12<sup>71</sup> are related to the dependent variables. The ratings are not summated, because of the small amount of test persons, which hinders to separate the group into two test groups.

The respond tasks of the two questionnaires are a combination of *short essay tasks*, *rating tasks*, and *selection tasks* (dichotomous tasks, multiple choice tasks). As far as possible the same response options or scales are chosen to minimize cognitive overload of participating children. *Short essay tasks* are used to evaluate all four selective EQs. Test persons responds are coded with 0-2 points for assessment, in which 0 stands for a no answer, 1 for a wrong answer, and 2 for an adequate answer.

---

<sup>71</sup>EQ3: Influence of time and order of showing warnings to reaction is measured with logging and observations.

#### 4.4. Evaluation methodology and concept

Classification	Characteristics
<b>User study/survey</b>	
Environment	'Trilingual International Primary School' in Magdeburg (Germany) [DIG]
Participants	13 Children 8 to 9 years old (8 boys and 5 girls)
	all native German speakers
	Pre-knowledge: all familiar with desktop IT systems (school lessons supported with tablet PCs and a digital whiteboard)
Preparation	Letter of agreement and letter from the school administration to explain the evaluation
	Introducing of testers, description as user-interface evaluation (no mention of sec-warnings to prevent interference)
Execution	Three phases, normal school lessons length: 45 min 1) Introduction (5 min) 2) Operation of the prototype (15 min) 3) Questionnaire (15 min)
<b>Evaluation methods</b>	
Measurement of quantitative values	Logging of click events
Measurement of qualitative values	1) Observations (body language, thinking aloud) 2) Questionnaire (completed by supervisor)
<b>Research questions (EQ)</b>	
Comprehension of Warnings (EQ1)	Three instruments for measure: 1) Reaction: Observations, logging 2) Interpretation: Questionnaire 3) Usage of 'Why?'-button: logging
Warning Design (EQ2)	Questionnaire
Influence of time and order of showing warnings to reaction (EQ3)	Logfiles and written protocol
Previous experiences (EQ4)	Questionnaire (computer and mobile viruses; usage of computer, laptop, mobile phone)
Knowledge (EQ5)	Questionnaire (computer and mobile viruses; warnings)
Sociodemographic characteristics (EQ6)	Questionnaire (age, sex, mother tongue)

Table 4.12: Evaluation environment and methods for *test case 2 (Child-Smartphone-Interaction)*

*Rating tasks* are used to evaluate warning comprehension (EQ1) and warning design (EQ2). These tasks are realised with two different smiley scale types. A *3-item smiley scale*: is used for rating of warning design elements (2: slightly smiling face<sup>72</sup>: well designed, 0: neutral face<sup>73</sup>: no idea, 1: slightly frowning face<sup>74</sup>: bad designed). For example Q17: 'How do you like [red character icon] for 'very great danger'''. 'Slightly smiling face' means red character icon is very useful to symbolise very great danger. Additionally, a *5-item smiley scale*: is used only once to rate test stress level in Q1 (5: two slightly smiling faces: completely stressless,

<sup>72</sup>Unicode number for 'slightly smiling face', U+1F642

<sup>73</sup>Unicode number for 'neutral face', U+1F610

<sup>74</sup>Unicode number for 'slightly frowning face', U+1F641

## Chapter 4. Methodology and Concept

4: one slightly smiling face: stressless 3: neutral face: no idea, 2: two slightly frowning faces: stressful, 1: one slightly frowning face: very stressful). Furthermore, rating tasks with grades (1-6) are used to rate the general design of cartoon character (Q31) and warning messages (Q32) (1: very good, 2: good, 3: satisfied, 4: sufficient, 5: inadequate, 6: insufficient).

Amongst smiley scales also *asymmetric rating scales* are used to rate warning design (EQ2). One example is Q33 'How do you like the warning messages?'. Test persons responds are coded with 0-2 points for assessment, in which 0 stands for a neutral rating, 1 for a negative rating, and 2 for a positive rating.

*Selection tasks* are used for all other questions. *Dichotomous tasks* (yes/no answers) are used to rate test persons' previous experiences, knowledge regarding mobile malware, and comprehension of warning design (1:no, 2:yes). One example of rating of knowledge is Q12: 'Do you know computer viruses?'. 'Yes' is an indicator for test persons knowledge of computer viruses. One example of rating of previous experience is Q12.1: 'If yes, it is happened to you on a computer?'. 'Yes' indicates that the test person had personal experiences with computer viruses. One example of rating of warning comprehension is Q2: 'Did the cartoon character had different colours?'. 'Yes' indicates that the test person perceived the different colours of cartoon character.

Additionally, *multiple choice tasks* are used to evaluate the previous experiences (EQ4) of test candidates. For example in Q39: 'I have an own computer / laptop / mobile phones' multiple choices are possible.

Specific evaluation question	Dependent variables	Purpose	Assessment (points)
EQ1: Comprehension (interpretation)	Warning comprehension by target user-group	Warning effectiveness	0:no, 1:wrong, 2:adequate answer; 1:no, 2:yes
EQ2: Warning design	-	Result interpretation	1-6 grades; 0:neutral, 1:negative, 2:positive rating
EQ3: Influence of time and order of showing warnings to reaction	Adequate reaction of target user-group to warning	Warning effectiveness	-
EQ4: Previous experiences (Malware, computer usage)	-	Result interpretation	1:no, 2:yes
EQ5: Previous experiences (Malware, warnings)	-		1:no, 2:yes
EQ6: Sociodemographic characteristics (age, sex, mother tongue)	-		-

Table 4.13: Questionnaire: Relation of dependent variables to specific evaluation questions for test case 2

# 5

## Realisation of test cases

This chapter introduces the realisation and evaluation of the both test cases of the generic user-specific warning approach for specific application scenarios. This work is related to research objective 4 (section 1.3).

**RO4: Evaluation of the general user-group specific effective malware warning concept to measure the warning effectiveness.**

This chapter is partitioned into two parts. The first part in section 5.1 introduces the realisation of the warning test case for adults (generic user). As already described in section 4.4.1, the test case simulate malware attacks against a mobile robot in a domestic environment, which is controlled with a tablet. These attacks are classified as second level impacts on a remote controlled system in the personal risk model in section 4.2. In the second part of this chapter in section 5.2 the realisation of the warning test case for primary-school children is introduced. The test case simulate malware attacks of a smartphone, which is handled by primary-school children. These attacks are classified as *first level impact on a mobile device*.

### 5.1 Generic user - Mobile robot warnings

---

In this section the realisation of warnings for a specific mobile robot for adults (generic user) is described, which based on the scientific work of [Wul16]. For a better comprehension the test case introduced in section 4.4.1 is already briefly described. Test case 1 evaluates the **specific warning design** for a generic user-group, which is described in section 5.1.1.

Section 5.1.2 presents the **warning realisation** on a specific tablet. The application scenario is a remote control of a domestic mobile robot with a standard tablet. The test case simulate malware attacks against a mobile robot in a domestic environment. These attacks are classified as second level impacts on a remote controlled system in the personal risk model in section 4.2.

The test is realised in an office environment, where two domestic rooms (sitting room, kitchen) are simulated. Because giving participants a primary task is important to create a real scenario, the main task of the participants is the control of a mobile robot with a tablet. The **user-study** is presented in the last section 5.1.3.

### 5.1.1 Security Warnings

---

This section describes the user-group specific warning design for the generic user-group (adult) on basis of the generic warning approach in section 4.3.

#### **User-group specific warning design:**

The warnings are designed for a **generic user** (adult with no mental/physical handicaps, standard literacy, familiar with the European culture).

#### **Effective warning design:**

The warning information include the usage of risks, personal consequences, and instructions of potential malware activities on the mobile robot, which is remotely controlled with a tablet (second level impacts on a coupled system). The warning present no additional information (as shown in figure 4.9), because the evaluation of two warning variants (with and without instructions) are in focus of the evaluation.

#### **Multimodal feedback:**

The design includes the usage of *multimodal feedback*, a combination of visual and acoustic design elements. Haptic feedback (e.g. vibration) is not realised because the evaluation of two warning variants (with and without instructions) are in focus. Warnings are generated dynamically on the test *tablet*. The design of tested warnings differ depending on the threat scale which symbolise specific risk levels.

#### **Threat scale:**

The threat scale distinguishes between specific *risk levels*, which warn users for specific risks and potential personal consequences of the current malware attack on the robot. As table 5.1 show, risk levels are differentiated by their combination of visual, acoustic and haptic design criteria. The three risk levels of the generic design are adapted for the specific application scenario. Risk level 0 (normal operation) is not used, because it's the operational state of the robot, where no security threats disturb robots' activities. Instead one additional risk level is introduced, called risk level 3 'very high'. Risk level 2 and 3 differ in facility of impact of malware attacks to the robot and its environment. There are six warnings realised for risk level 1 'low' (warning 2 and 4-8, example in figure 5.2), two warnings designed for risk level 2 'high' (warning 9,10, example in figure 5.3), and two warnings realised for risk level 3 'very high' (warning 1,3, example in figure 5.3). In the following the three risk levels are defined.

**Risk level 1 (low):** represent a potential for a *small amount of personal risks* for users, which remotely control the mobile robot. For example an unknown communication from the Internet may impact the personal privacy of users (warning 8).

**Risk level 2 (high):** represent a potential for a *high amount of personal risks* for users, which remotely control the mobile robot. Warnings designed for risk level 2 warn about events were a *barrier hinder directly impact* of malware attack on the robot and its environment. Examples are constructional safety protection mechanism, such as bumper (warning 1) and needed user interaction of installing malware (warning 3). Both, warning 1 and 3, are implemented with a single alert signal.

**Risk level 3 (very high):** represent a potential for a *very high amount of personal risks* for users, which remotely control the mobile robot. Consequences of malware risks of that risk level are *not hindered by barriers* like safety measures or user interactions. In comparison to risk level 2 potential consequences are more directly related to users. That's why warnings 9 and 10 are realised with a permanent alert signal.

Table 5.2 summarises the warning design for all ten tested warnings including specific risk levels. Two different warning icons for risk levels<sup>7576</sup> and one icon for instructions are used<sup>77</sup>. Acoustical design is realised with free available alert signals<sup>78</sup>, which differ in length.

No	Risk level	Visual design	Acoustic design
1	Low	Corresponding text, yellow colour coding (Triangle icon with exclamation mark)	No alert signal
2	High	Corresponding text, red colour coding (Shield icon with stop hand symbol)	Single alert signal
3	Very high	Corresponding text, red colour coding (Shield icon with stop hand symbol)	Permanent alert signal

Table 5.1: Specific logical design of **risk levels** for test case 1

### Information design:

The information design based on textual information, which is short, clearly, readable, has large fonts, and less technical terms. For better comprehension the texts are combined with risk level icons (risk, consequences) and a single yellow light bulb icon (instructions). Amongst text and icons also buttons for user interaction are included into the warnings. The focus lay on evaluation of the two different warning variants so speech output is not realised. The contents of all 10 warnings, including risks, potential personal consequences of risk, and instructions, are summarised in table 5.3.

### Adaption to mobile device characteristics:

The used **tablet** (Asus Transformer Pad TF701T) has a midsize display (10.1 inch screen, 2560x1600 pixel resolution). In spite of the display size the warning information is split into small pieces and presented successively by different warning views to ease the comprehension of warning content for the desired user-group. Figure 5.1 shows an example of splitting information of the current risk, personal consequences and instructions in two different views for both test groups.

As mentioned before only visual and acoustic feedback information is used. Therefore the **third profile** is used, where the acoustical feedback (sound) of the tablet is activated.

<sup>75</sup>Tango Desktop Project, Dialog stop hand, <https://commons.wikimedia.org/wiki/File:Dialog-stop-hand.svg>, accessed: 29.06.17

<sup>76</sup>GNOME, Dialog warning, <https://commons.wikimedia.org/wiki/File:Gnome-dialog-warning.svg>, accessed: 29.06.17

<sup>77</sup>KSiOM, Dialog information on, [https://commons.wikimedia.org/wiki/File:Dialog-information\\_on.svg](https://commons.wikimedia.org/wiki/File:Dialog-information_on.svg), accessed: 29.06.17

<sup>78</sup>Sound Jay, Beep Sounds, <https://www.soundjay.com/button/sounds/beep-09.mp3>, accessed: 29.06.17

ID	Risk	RL	Warning	
			Visual	Acoustic
1	Unauthorised manipulation of robot map	2	red	1
2	Unauthorised login trial to robot	1	yellow	-
3	Unsignatured update	2	red	1
4	Unknown software autostart	1	yellow	-
5	Anomalous strong software activity	1	yellow	-
6	Unknown communication from the Internet	1	yellow	-
7	Communication trial of malware infected device	1	yellow	-
8	Unauthorised communication with the Internet	1	yellow	-
9	Unauthorised sending of pictures to the Internet	3	red	∞
10	Unauthorised sending of audio signals to the Internet	3	red	∞

Table 5.2: Logical warning design for test case 1  
 (Note: RL-Risk level, 1-low RL, 2-high RL, 3-very high RL  
 Acoustical: 1-Short, single alert signal, ∞-permanent alert signal)

**Warning layout:**

As already mentioned in section 4.4.1, in test case 1 two test groups are used. The warnings for both different groups of test persons differ. The first group - the experimental group (EG) - were shown detailed instructions in the warning in comparison to the second group - control group (CG), which has only the information about the security risk and potential consequences. Figure 5.1 illustrates the described differences between both test groups as UML activity diagram for warning 1. The other nine warnings differ in textual content, warning icon, and use of acoustical signal, which both symbolise the risk level (see table 5.3, p. 132). Warnings are visualised after test supervisor boots the robot computer and the test person activates robot driving. After the test person click the 'Forward' button the dialog with personal consequences for the user and its environment appears on the tablet. This dialogue only differ for both test groups in the 'OK' button for CG to finish the dialogue and 'What can you do?' button for EG to get instructions to handle the current threat for control group.

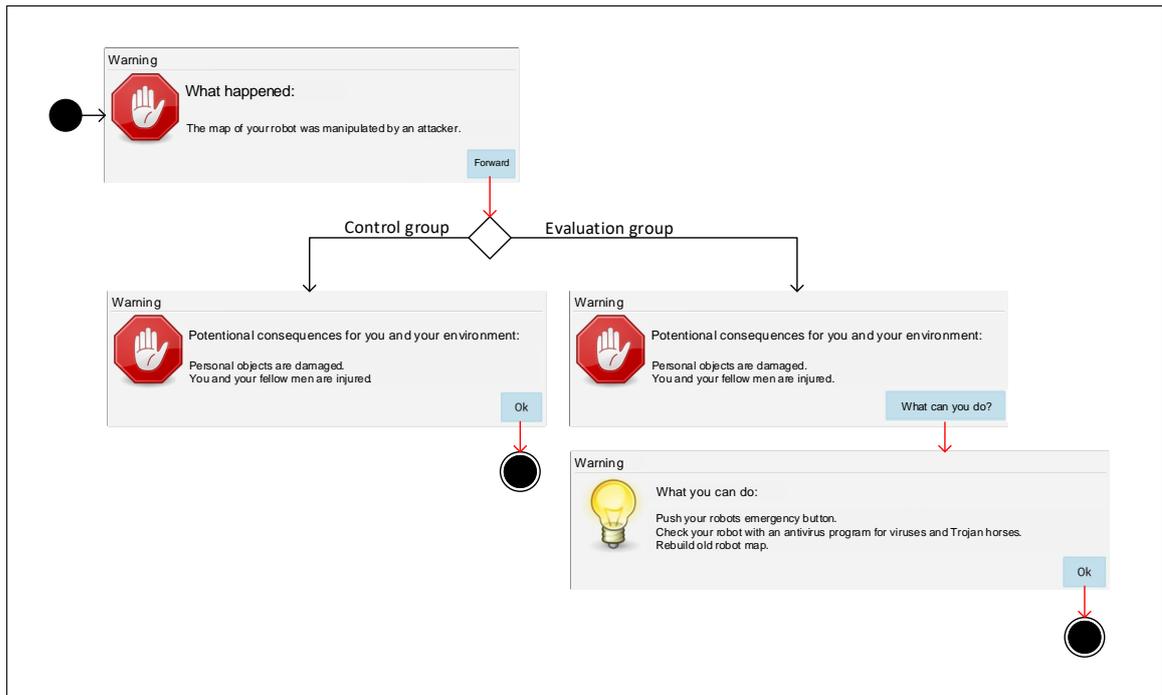


Figure 5.1: UML activity diagram for warning 1 (Unauthorised manipulation of robot map) for both test groups (Note: red arrows symbolise click on buttons)

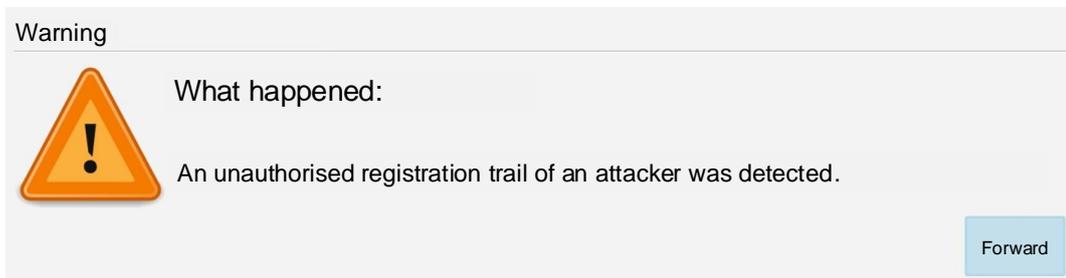


Figure 5.2: Risk level 'low': Warning 2

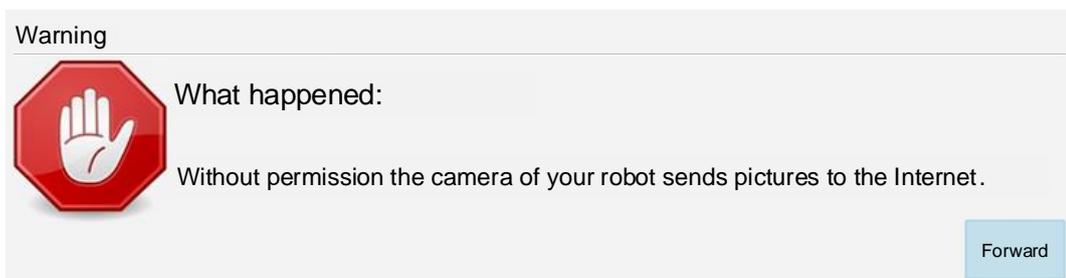


Figure 5.3: Risk level 'high': Warning 9

In the following, the multimodal design of every single warning of the ten evaluated warnings is described.

*Warning 1* warns for an unauthorised manipulation of robot map. The warning is designed with risk level 2 ('high'), because of a high risk for physical consequences to its environment. The consequences include high risk for injury of persons ( $R_{PSAFE}$ ) and damage of objects ( $R_{ESAFE}$ ). These malware impacts could be minimised by the functionality of robots bumper. Warning 1 is realised by red warning icon and single audio signal. Members of EG are instructed to push immediately robots emergency button, to check their robot with an antivirus program, and to rebuild old robot map.

*Warning 2* warns for an unauthorised login trial of an attacker to the robot. The warning is designed with risk level 1 ('low'), because it is assumed the login failed. So there is a low risk that the robot could be potentially controlled by an attacker ( $R_{AVAIL}$ ). The attacker could misuse her login to potentially get access to personal data ( $R_{PRIV}$ ), like camera video streams or audio signals from microphone. The risk level of warning 2 is symbolised by yellow warning icon. Additionally, malware threats to personal data (video and audio signals) are tested separately with warnings 9 and 10. EG gets instructions to separate their robot from the network, to check the network for unknown devices, and reconfigure the password of WLAN and their robot.

*Warning 3* warns for an unsigned software update for the robot, which is not created by original manufacturer. Risk level 2 ('high') is used, because of a high risk an attacker could potentially get access to personal data ( $R_{PRIV}$ ). Furthermore, the attacker could then control robot functions, which could affect robots' availability and functionality ( $R_{AVAIL}$ ), which could cause financial losses ( $R_{FIN}$ ). It is designed as warning of risk level 'high', because user interaction is needed for malware installation. The risk level of warning 3 is realised by red warning icon and single audio signal. Members of EG are instructed to do not install this update.

*Warning 4* warns for an autostart of unknown additional software. The warning is designed with Risk level 'low', because of a low risk an attacker could control the robot. The user is warned for potential negative effects on robots' availability and functionality ( $R_{AVAIL}$ ), which could cause financial losses ( $R_{FIN}$ ). The risk level of warning 4 is symbolised by yellow warning icon. EG are instructed to check the robot with an antivirus program or to switch off the robot and contact external services.

*Warning 5* warns for an anomalous strong software activity. Examples are mining of cryptic currency, like bitcoin<sup>79</sup>. Risk level 1 'low' is used, because of a low risk the robot potentially lose power, which could have effects on robots' availability ( $R_{AVAIL}$ ). The increased effort for robot recharge could cause financial losses ( $R_{FIN}$ ). The risk level of warning 5 is symbolised by yellow warning icon. Members of EG are instructed to check the robot with an antivirus program or to switch off the robot and contact external services.

---

<sup>79</sup>Wired, Robert McCillan, 'Watch Wired Get Rich Quick With Our Sleek Bitcoin Miner', [https://www.wired.com/2013/05/butterfly\\_live/](https://www.wired.com/2013/05/butterfly_live/), accessed: 23.06.17

*Warning 6* warns for an unknown communication with the robot from the Internet. This vulnerability could be caused by an open IP port (TCP or UDP) on the robot and a port forwarding from router to the robot. The warning is designed with risk level 1 'low', because of a low risk an attacker could potentially control the robot ( $R_{AVAIL}$ ) and install malware. The risk level of warning 6 is symbolised by yellow warning icon. EG are instructed to check their router configurations if their robot should be reachable from the Internet or contact external services.

*Warning 7* warns for communication with the robot by a malware infected device in internal network. Risk level 'low' is used, because of a low risk an attacker could potentially control the robot ( $R_{AVAIL}$ ) and install malware. The risk level of warning 7 is symbolised by yellow warning icon. Members of EG are instructed to check all their devices (like computer, tablets, mobile phones) in the internal network with an antivirus program.

*Warning 8* warns for unauthorised communication of robot with the Internet. The warning is designed with Risk level 'low', because of a low risk an attacker could potentially download undesired software, use it to control the robot ( $R_{AVAIL}$ ), and could potentially infect the robot and other devices in the network with malware. The risk level of warning 8 is symbolised by yellow warning icon. EG are instructed to separate robot from the network, check robot with an antivirus program or switch off the robot and contact external services.

*Warning 9* warns for unauthorised sending of pictures to the Internet by robot. Risk level 3 ('very high') is used, because of a high risk an attacker could potentially get access to personal pictures ( $R_{PRIV}$ ) and could publish these pictures on the Internet ( $R_{PRIV}, R_{REP}$ ). It is designed as warning of risk level 'very high', because malware risks are not hindered by system measures or user interaction activities. The risk level of warning 9 is realised by red warning icon and permanent audio signal. Members of EG are instructed to separate their robot immediately from the network, check their robot with an antivirus program or switch off their robot and contact external services.

*Warning 10* warns for unauthorised sending of audio signals to the Internet by robot. The warning is designed with risk level 'very high', because of a high risk an attacker could potentially get access to personal conversations ( $R_{PRIV}$ ) and could publish these conversations on the Internet ( $R_{PRIV}, R_{REP}$ ). It is designed as warning of risk level 'very high', because malware risks are not prevented by system measures or user interactions. The risk level of warning 10 is realised by red warning icon and permanent audio signal. Members of EG are instructed to separate their robot immediately from the network, check their robot with an antivirus program or switch off their robot and contact external services.

No	Risk (malware activity)	Potential personal consequences (affected personal requirements)	Instructions (only for EG group)
1	The map of your robot was manipulated by an attacker.	Personal objects are damaged ( $R_{ESAFE}$ ). You and your fellow men are injured ( $R_{PSAFE}$ ).	Push your robots emergency button. Check your robot with an antivirus program for viruses and Trojan horses. Rebuild old robot map.
2	An unauthorised login trail of an attacker was detected.	Your robot could be controlled by an attacker ( $R_{AVAIL}$ ). The attacker could activate camera and microphone of your robot ( $R_{PRIV}$ ).	Separate your robot from network. Check your network for unknown devices. Change password of your WLAN and of your robot
3	The software update is not originated from manufacturer.	Your robot could refer your personal information and data to the attacker ( $R_{PRIV}$ ). Your robot could be controlled by an attacker ( $R_{AVAIL}$ ). Your robot is not usable anymore ( $R_{AVAIL}, R_{FIN}$ ).	In no case install this update. Only install original manufacturer updates.
4	An additional unknown software is launched on your robot.	Your robot could be controlled by an attacker ( $R_{AVAIL}$ ). Your robot is not usable anymore ( $R_{AVAIL}, R_{FIN}$ ).	Check your robot with antivirus program for viruses and Trojan horses. Or switch off your robot and contact a service technician.
5	A software shows an anomalous strong activity.	Your robot spend unusual plenty of power ( $R_{AVAIL}$ ). Your robot has to recharged more often and longer as usual ( $R_{FIN}$ ).	
6	Unknown communication with your robot from the Internet detected.	Your robot could be controlled by an attacker ( $R_{AVAIL}$ ). An attacker could install viruses and Trojan horses on your robot.	Check router if your robot should be reachable from the Internet. If not check router configurations or contact a service technician.
7	A virus infected device tries to communicate with your robot.		Check all your devices in the network (like computer, tablets, mobile phones) with antivirus program for viruses and Trojan horses.
8	Your robot communicated unauthorised with the Internet.	Your robot downloads undesired software from the Internet. Your robot could be controlled by an attacker ( $R_{AVAIL}$ ). Your robot infected other computer, tablets, mobile phones with viruses and Trojan horses	Separate your robot IMMEDIATLY from network. Check your robot with antivirus program for viruses and Trojan horses. Or switch off your robot and contact a service technician.
9	Without permission the camera of your robot sends pictures to the Internet.	The attacker owns your personal data and pictures ( $R_{PRIV}$ ). Your personal data and pictures could be published in the Internet ( $R_{PRIV}, R_{REP}$ ).	
10	Without permission the microphone of your robot sends audio signals to the Internet	The attacker owns your personal data and could monitor your conversations ( $R_{PRIV}$ ). Your personal data and conversations could be published in the Internet ( $R_{PRIV}, R_{REP}$ ).	

Table 5.3: Risk-Consequences-Instruction matrix for test case 1

### 5.1.2 Test program

The following two paragraphs are based on [Gie17].

The warning prototype is realised on a mobile robot platform *SCITOS G5* developed by German company MetraLabs GmbH<sup>80</sup>. It is used in industrial environments for environmental monitoring<sup>81</sup> as well as for business applications, like delivery services in restaurant and information of consumers in building supply stores<sup>82</sup>. Figure 5.4 shows the used robot platform, which is delivered by MetraLabs as research platform. A differential and an accumulator are placed behind the blue plastic case of the robot. The lower black rubber ring is a safety mechanism. It is a bumper, which could sense the contact with obstacles. Visible components are also two Wi-Fi antennas, a laser scanner coloured in yellow, and an embedded computational unit behind the aluminum frame. On the frame additional components for human-machine interaction could be installed, like touch screen display, a robot head or a grapppler. On the on-board PC runs an Ubuntu 12.04 LTS 64Bit<sup>83</sup> and MIRA middleware<sup>84</sup>. 'Middleware for Robotic Applications' (MIRA) is a platform comprehensive framework for robot applications. It is implemented in C++ and completely supported by the two operating systems Linux and Windows. In comparison to 'Robot Operating System'<sup>85</sup> (ROS) MIRA is build on a distributed communication structure and do not need a central server.



Figure 5.4: Mobile robot platform SCITOS G5 from MetraLabs  
(Photo: Tony Gieseler [Gie17])

A Android based *tablet* Asus Transformer Pad TF701T<sup>86</sup> is used for remote control of SCITOS G5 robot. In the user study the tablet was used without the delivered docking station because it has no function for robot remote control. The tablet has a 10,1 inch capacitive touch screen with a resolution of 2560x1600 pixel, which supports ten finger multi-touch functionality. Robot remote control with mobile devices, like smartphones and tablet have one two main advantages in comparison to the fixed installation of a robot control unit on top of robot frame.

<sup>80</sup>MetraLabs: Research in mobile robots, <http://www.metalabs.com/forschung>, accessed: 22.06.17

<sup>81</sup>MetraLabs: Industry turns mobile, <http://www.metalabs.com/en/industry-4-0>, accessed: 22.06.17

<sup>82</sup>MetraLabs: Inventory & Shopping Robots, <http://www.metalabs.com/shopping-rfid-robot>, accessed: 22.06.17

<sup>83</sup>Ubuntu Wiki: Releases, <https://wiki.ubuntu.com/Releases>, accessed: 22.06.17

<sup>84</sup>MIRA - middleware for robotic applications, <http://www.mira-project.org/joomla-mira/>, accessed: 22.06.17

<sup>85</sup>ROS - Robot Operating System, <http://www.ros.org/>, accessed: 22.06.17

<sup>86</sup>ASUS: The New ASUS Transformer Pad (TF701T), [https://www.asus.com/us/Tablets/The\\_New\\_ASUS\\_Transformer\\_PadTF701T/](https://www.asus.com/us/Tablets/The_New_ASUS_Transformer_PadTF701T/), accessed: 22.06.17

First, the robot could be controlled remotely by users without moving himself. Second, smartphones<sup>87</sup> and tablets<sup>88</sup> are often used in German households, users have less learning effort for GUI, because they seem to be familiar with control of devices via touchable screens. One main disadvantage of mobile remote control without intervisibility to the robot are safety aspects. One example are accidents of the robot with persons.

The warning prototype for mobile robot is implemented with Qt<sup>89</sup> version 5.6.2, a C++ based, cross-platform software development framework for GUI programming. Figure 5.5 shows an UML diagram, which shows the main functionality of the warning prototype. It is separated into program modules on user-side (tablet) and robot-side. On user-side the tablet is responsible for robot remote control and display of warnings. On robot-side the MIRA is responsible for communication of current robot coordinates to the communication server. The server realises the mapping of coordinates and commands between the GUI on users tablet and MIRA. Warnings are triggered by specific user activities on the tablet. There are two navigation modes: first, point target on robot map on GUI and click on start button on GUI; and second, click a task specific button, e.g. 'cupboard'. The first warning is activated four seconds after the test persons press initially the start button or task specific button. All following warnings are also displayed with a delay of four seconds after user activation occurs (figure 5.11 in section 5.1.3).

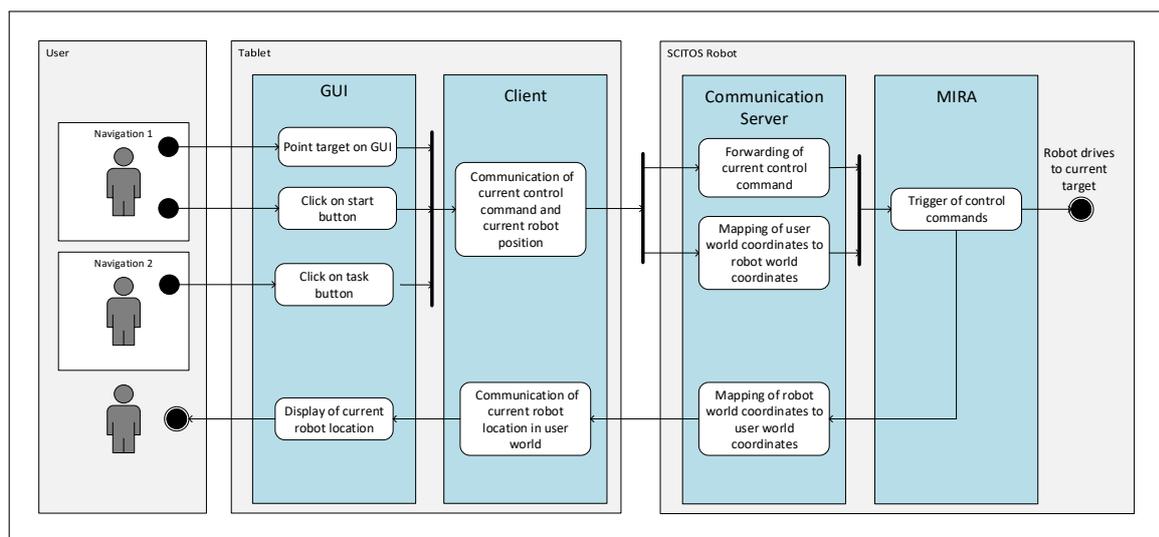


Figure 5.5: UML activity diagram for communication of drive command data between main prototype components

### Graphical user interface (GUI):

The GUI should ease the remote control of the robot by test persons. In the user study in section 5.1.3 test persons are introduced by test supervisor in ten different application scenarios for robot remote control with specific tasks (see figures 8.1 and 8.2 in appendix). For every of the application scenarios a specific GUI is implemented. Figure 5.6 show one example of the GUI for tasks regarding the cupboard. Exemplary tasks are taking things out of the cupboard, like dishes, and pick-up things from the cupboard, like coffee and cake. The outer right but-

<sup>87</sup>Statista: Number of smartphone users in Germany from 2013 to 2021 (in millions), Source: Statista DMO, <https://www.statista.com/statistics/467170/forecast-of-smartphone-users-in-germany/>, accessed: 22.06.17

<sup>88</sup>Statista: Number of tablet users in Germany from 2010 to 2020 (in millions), Source: eMarketer, <https://www.statista.com/statistics/462005/number-of-tablet-users-in-germany/>, accessed: 22.06.17

<sup>89</sup>Qt, <https://www.qt.io/>, accessed: 26.06.17

tons represent remote control ('Drive to target') and additional targets (e.g. 'Dish washer'). If robot reaches a target tasks are visualised left side of the outer right buttons. These buttons are for specific tasks for a specific target. With click on the 'Legend on' button names of targets in test environment are visualised left side in the GUI. If the user touches a specific button the corresponding robot control command is forwarded to the MIRA warning server wireless over TCP/IP (figure 5.5). The tablet is also used to generate warnings depending on user activities. Figure 5.11 shows the order of warning display during the test depending on specific application scenarios. Section 5.1.3 describes the test of the warning prototype in more detail.

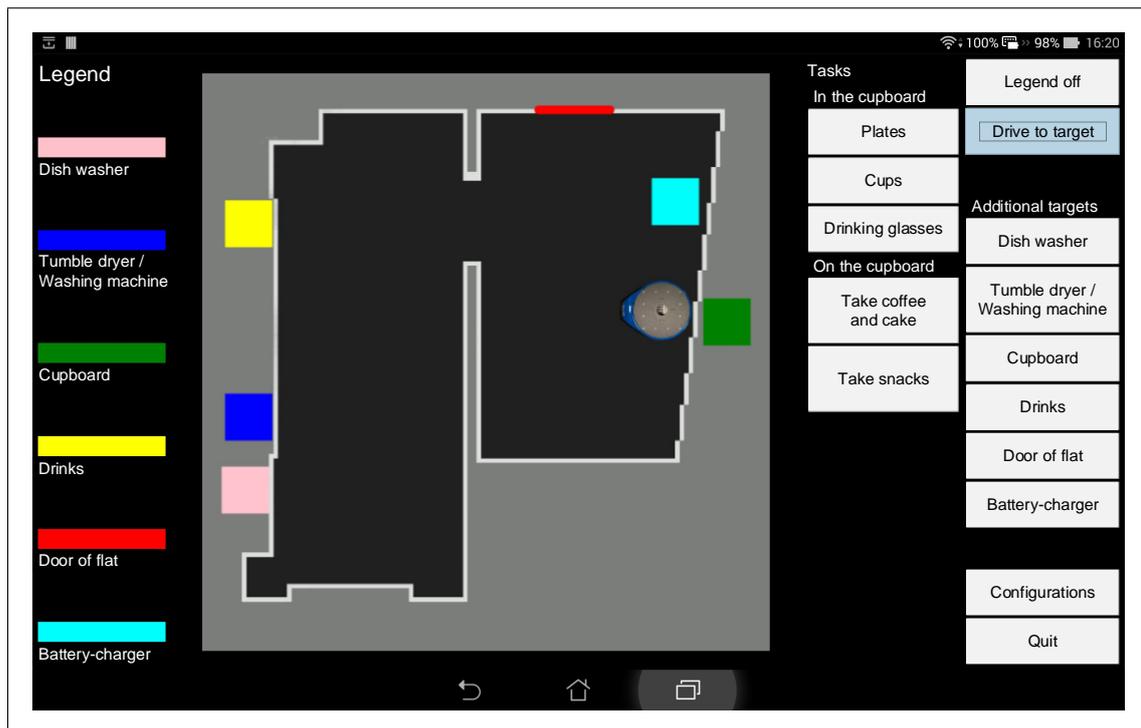


Figure 5.6: GUI screenshot of remote control via tablet  
Application scenario with cupboard - take dishes, coffee and cake, snacks (Legend on)

### Logfile:

As a technical evaluation tool a logfile is used. Figure 5.7 illustrates stored time stamps of users button clicking events for warnings with information for risk (both test groups: 'Forward' button), potential personal consequences (CG: 'OK', EG 'What can you do?' button), and instructions (only EG, 'OK' button). Red arrows in figure 5.7 symbolise that warnings are displayed immediately without delay, that are warnings for consequences of malware attacks after clicking 'Forward' button (both groups) and instructions after clicking 'What can you do?' button (only EG). On basis of these time stamps reading durations of warning contents are calculated. Figure 5.8 is an excerpt of a specific logfile of a test person of evaluation group. The first four lines of the logfile store registration information, as well as start time stamp, the length of test person's chosen password, TP - test person hours (exclusively for students of psychology), and ID to create a pseudonym for test person. The following lines of figure 5.8 show time stamps for display of warnings and clicking events on buttons by test persons.

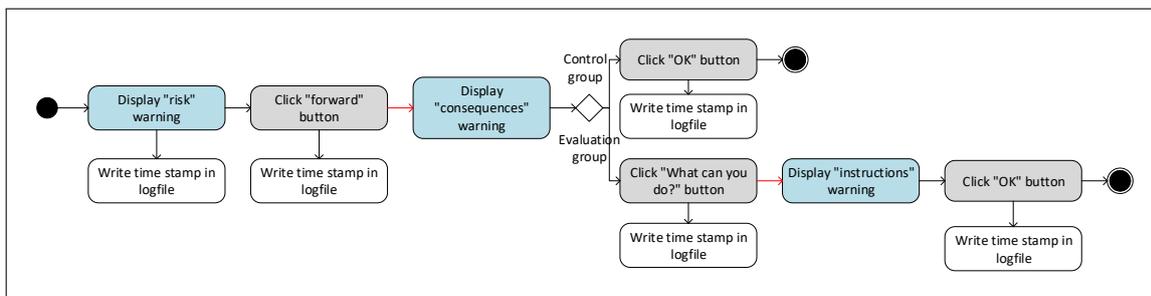


Figure 5.7: UML activity diagram for warning display and generation of logfile information  
 (Note: *blue shapes*: display of warning types,  
*grey shapes*: users click on buttons in warning,  
*white shapes*: write of logfile,  
*red arrows*: no delay to display next warning view  
*black arrows between blue & grey shapes*: time user reads warning information)

```

2016-12-14 15:07:37.929 Start
2016-12-14 15:09:07.503 Password length: 8
2016-12-14 15:09:07.504 TP-hours: no
2016-12-14 15:09:07.504 Test person ID: 12
2016-12-14 15:09:11.666 Warning 6: Incoming communication external
2016-12-14 15:09:16.183 Event button (Forward) clicked
2016-12-14 15:09:22.835 Consequences button (What can you do?) clicked
2016-12-14 15:09:32.875 Instructions button (OK) clicked
2016-12-14 15:10:17.154 Warning 4: Autostart
2016-12-14 15:10:20.695 Event button (Forward) clicked
2016-12-14 15:10:28.185 Consequences button (What can you do?) clicked
2016-12-14 15:11:13.675 Instructions button (OK) clicked
2016-12-14 15:13:26.667 Warning 7: Incoming communication internal
2016-12-14 15:13:33.204 Event button (Forward) clicked
2016-12-14 15:13:46.331 Consequences button (What can you do?) clicked
2016-12-14 15:13:51.804 Instructions button (OK) clicked
    
```

Figure 5.8: Exemplary excerpt from a logfile for a member of evaluation group

### 5.1.3 User study

In this section the evaluation environments and methods of **warning prototype for a mobile robot** for adults (generic user) is described. It mainly based on the scientific work of [Wul16], except the test environment and introduction, which based partly on [Gie17].

#### User Study:

The evaluation was realised as user study in the faculty of computer science of Otto-von-Guericke-University of Magdeburg<sup>90</sup>. The participating test persons were on average 29 years old. The test persons are separated into two groups in order to evaluate the advantage of the new warning design (section 4.3). The first group - the experimental group (EG) - were shown detailed instructions in the warning in comparison to the second group - control group (CG), which has only the information about the security risk and potential personal consequences. It participated 8 woman in both groups, 3 men in EG and 4 men in CG. Most of the candidates were students of non-technical course, 4 engineers, and 4 administrative clerks. All of the test persons were native German speakers. Most of the test persons had experiences with the Internet and use it several times a day. Most of test persons use mobile devices, like smartphones, and the half uses tablets. Furthermore, most of test persons had experiences

<sup>90</sup>Website Faculty of computer science of Otto-von-Guericke-University of Magdeburg, <http://www.inf.ovgu.de/inf/en/>, accessed: 26. June 2017

with malware attacks or know someone who had experiences in that topic. Half of test persons were already victims of malware attacks (section 6.1). The evaluation was realised with each single test person. The tester introduced themselves to the test person and described the test as evaluation of an app for robot remote control.

### Test environment:

Figure 5.9 shows the two neighbouring rooms of the faculty of computer science where the test was realised. The rooms were timely used as store room. They were ideal for testing because main door could be closed and both rooms are connected by a second entrance. So the test was realised with and without inter-visibility to the robot. During the test the participant stand with the tablet in the 'sitting room'. For all tasks related to the sitting room the robot was visible to the test person. For all tasks related to the kitchen the robot was not visible to the test candidate. These cases were all the same for each participant of each test group (EG,CG). Figure 5.9 shows a re-enacted test situation. The person on the figure represents the test person. During the test the supervisor stand beside the test person and observed his reactions and write the think aloud protocol.



Figure 5.9: Test environment of the mobile robot warnings prototype  
(Photo: Tony Gieseler)



Figure 5.10: Screenshot of test environment on tablet GUI  
(Note: Name of targets are annotated after screenshot. This information is displayed by switch on legend.)

### Test Realisation:

The test was realised on five consecutive days with 23 test persons in separated tests with single persons. The test was separated into *introduction* (5-10 minutes), *test* of the warning prototype (20 minutes) and *questionnaire* (20-30 minutes). Every test takes in average 45 minutes.

### Introduction:

Before the test begins, the test supervisor starts the robot as well as the tablet. Furthermore, the wireless connection between robot and tablet is initialised. After the technical preparation the test person was welcomed and invited to visit the both test rooms. The candidate should imagine a living room and a kitchen (figure 5.10). The imaginary test points in the kitchen (tumble dryer/ washing machine, dish washer, cupboard with drinks) and in the living room

(cupboard with coffee, cake and snacks, battery-charging station) are introduced to a single test person (see coloured line and squares in figure 5.10). Afterwards, the test person was introduced into the main functions of the mobile robot SCITOS G5 (figure 5.4). Afterwards, the test person insert registration information, including name of the robot, password, and if test person hours are needed (exclusively for students of psychology). Then the tablet GUI appears (figure 5.6 without menu 'Tasks'). Before the first task, the test person had some time to familiarise herself with the remote control.

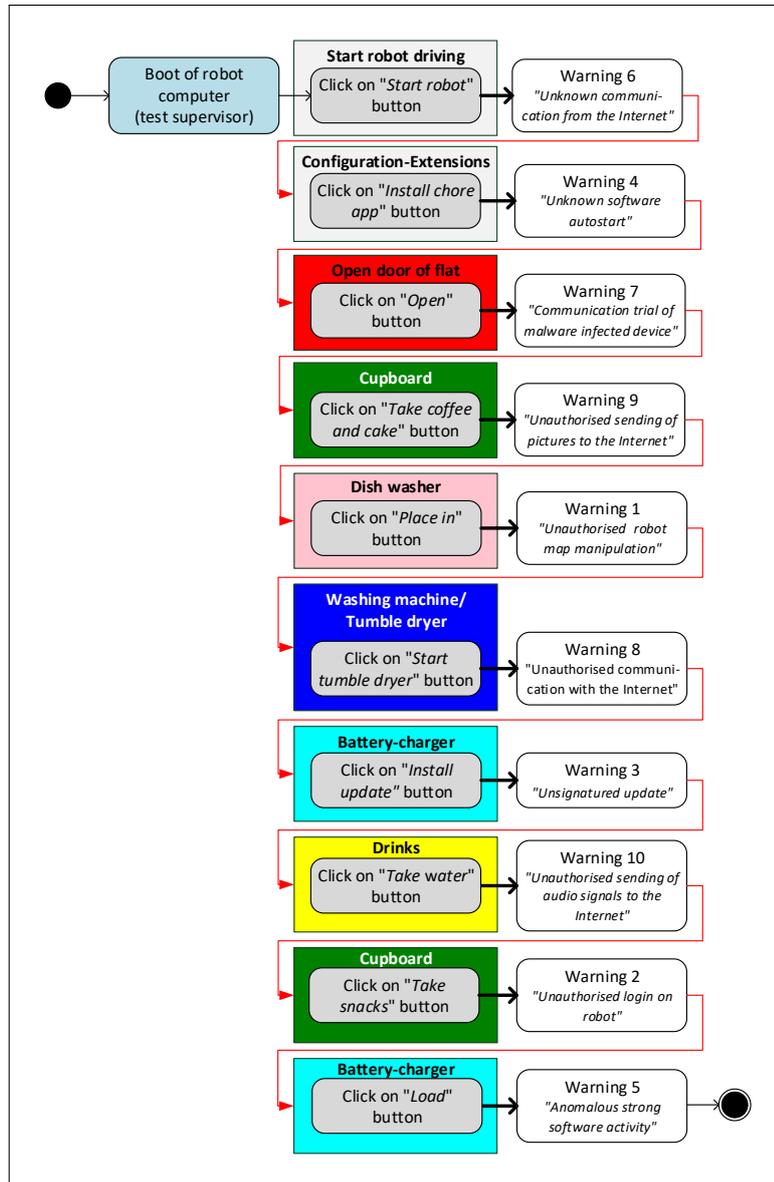


Figure 5.11: UML activity diagram for display of warnings  
 (Note: *thick black arrows*: four seconds delay to display next warning,  
*red arrows*: test supervisor explained next application scenario to test person)

**Test:**

After the introduction the test of the warning prototype began. The test was described to the test candidates as evaluation of an app for robot remote control. The test supervisor introduces two main application scenarios: first, relations are invited and test person shows functions of mobile robot and second, friends will come and the robot served them drinks and

snacks. Exemplary single tasks are launch the robot, install a chore app, and household tasks like fill in clothes in washing machine and start it. Detailed information of specific application scenarios and test persons tasks are visualised in appendix by figures 8.1 and 8.2. Related to this specific tasks warning messages appear on the tablet. This realises that test persons understand the relations between their activities and potential security or safety consequences to the robot and its environment. Figure 5.11 show the relation between tasks and display of warnings. The test supervisor observed all reactions of single test person and motivate her to think aloud. The non-verbal and verbal reactions are noted in a protocol for further analysis (section 8.1.4). The main test takes in average 20 minutes.

### **Questionnaire:**

After the main test an online questionnaire is filled in by the test person. It mainly includes questions regarding design criteria and comprehension of warning messages. Further questions concerned to previous experiences with the Internet and malware (EQ1), knowledge regarding malware activities (EQ2), usefulness of warning design (EQ3), comprehension of warning information (EQ4), future of Internet of Things (EQ6), and socio-demographic characteristics (EQ7). The full translated questionnaire is represented by figures 8.3, 8.4, and 8.5 in appendix. The original questionnaire in German is also added to the appendix to realise reproducibility for the evaluation (three pages, figure 8.6). The fill in of the online questionnaire takes in average 20 till 30 minutes. After that the test was finished.

## 5.2 Children - Smartphone warnings

---

In the following section the realisation of warnings for a smartphone for primary-school children is described, which based on [Men11] and [MTF+12]. For a better comprehension the test case, introduced in section 4.4.1, is already briefly described. Test case 2 evaluates the **specific warning design** for a primary-school children user-group, which is described in section 5.2.1.

Section 5.2.2 presents the **warning realisation** on a specific smartphone. The application scenario is a single handling of a smartphone by primary-school children. The test case simulate malware attacks against a smartphone. These attacks are classified as first level impacts on a mobile device in the personal risk model in section 4.2.

The main test is realised in a class-room, where the children are familiar with. Because giving participants a primary task is important to create a real scenario, the main task of the participants is the usage of a painting app on the test smartphone. The **user-study** is presented in the last section 5.2.3.

### 5.2.1 Security Warnings

---

This section describes the user-group specific warning design for the user-group primary-school children on basis of the generic warning approach in section 4.3.

#### **User-group specific warning design:**

The warnings are designed for **primary-school children** which are mostly between 6 and 10 years old. It is assumed that these children have no mental/physical handicaps, a standard literacy, and are familiar with the European culture. The warnings are adapted to the user-group specific needs (e.g. thinking in a world of fantasy and dream of magic, problems to read long and complicated texts).

### **Effective warning design:**

The warning design for the desired user-group includes information about risks and instructions. Furthermore, to support childrens' warning comprehension, additional information is presented. That are information about the risk (e.g. virus), personal consequences of the risk (e.g. spy of personal data), and instructions how to handle the risk (e.g. no update installation). The *instructions* are separated into operations, which children could do alone (e.g. switch off the smartphone) and operations which have to realised by parents (e.g. using an antivirus app).

### **Adaption to mobile device characteristics:**

The test case 2 is realised with a smartphone - iPhone 3G. The display is 3.5 inch large and has a resolution of 320 × 480 pixel. The warnings are implemented using the class UIAlertView, which creates standard warning messages on iOS. The include of pictures in warnings is not possible with UIAlertView. Therefore subviews are used to display the content of warnings, including pictures and text (see example of warning 2 in figure 5.13). The *first profile* of the smartphone is used where sound and vibration is activated. Scenarios with a reduced set of options in the logical design are reserved for future research (section 7).

### **Multimodal feedback:**

The tested warning design based on the *general logical multimodal feedback design* for primary-school children already illustrated in table 4.7. The main difference to the design of the general user are the usage of a imaginative cartoon character, which warn the children with speech bubbles (see information design). Furthermore, the design of tested warnings differ depending on the threat scale which symbolise specific risk levels.

### **Threat scale:**

A threat scale is used to differentiate specific *risk levels* as combination of multimodal feedback information. In test case 2 the participants use a smartphone (iPhone 3G) that is not connected to other systems for remote control (despite the Bluetooth connection to the control device in section 5.2.2 for triggering the display of warnings). Therefore, only *first level impacts* of malware attacks against childrens' smartphone are considered and second level impacts are suspended (see personal risk model, section 4.2).

The security threat scale distinguishes between different malware-related threats. A reduced number of risk levels to a minimum size is used to avert excessive demand of children. In the following the three risk levels are defined:

**Risk level 0 (normal operation):** represents a risk-less usage of the smartphone. This level should be a smartphone standard and should be shown after the anti-malware software verifies that no virus or security risk is present.

**Risk level 1 (high)**<sup>91</sup>: symbolises that the mobile device can still be used though it is threaten. This level should be signalled if the user wants to execute an action which would lead to security risks, e.g. a malicious update. The warning instruction is most important to prevent the infection of the smartphone.

---

<sup>91</sup>Risk level 1 in test case 2 equates to risk level 2 in table 4.5 in section 4.3.4.

**Risk level 2 (very high)**<sup>92</sup>: represents security risk(s) for the smartphone and its owner. For example, the smartphone could be infected by a malicious virus that spies out data (related to users' privacy  $R_{PRIV}$ ) or damages the device (related to users' requirement of device availability  $R_{AVAIL}$ ). The safest recommendation at this risk level would be for the children to turn off the mobile device and give it to their parents or other competent adults.

The different risk levels are *visual* represented by the cartoon characters mimic changes and its colour coding, which is defined in traffic colours (green, yellow, red). The *acoustic* feedback consists of a short standard warning sound [Sad]. Its intention is to emphasize that an event is a security warning and not a game. A wrong choice in this part of the design, e.g. a funny tone from a comic series, could lead to a too playful handling of the incident. Depending on the risk level, the sound is played once or twice when a warning is shown. The acoustic design is not used when the smartphone is switched to 'silent' mode. Furthermore, the risk levels are differentiated by their *haptic* feedback realised as vibrations (short or repeated). The vibration is not used when the smartphone's vibration is turned off (e.g. if the phone is switched to 'silent' mode).

Table 5.4 presents the logical design - combination of multimodal feedback information - for the three introduced risk levels. The combination differs depending on the different risk levels. Thus the possible combinations are selected based on the risk level so that the different levels are supported. The logical design of individual risk levels should be clearly distinguishable from each other. Furthermore, a possible overload by too many signals has to be avoided. Thus, the combination of sound and vibration is only used at the highest risk level 2.

No.	Risk level	Visual design	Acoustic design	Haptic design
0	Normal	Character: corresponding text, green colour coding, tick mark	no alert sound	no vibration
1	High	Character: corresponding text, yellow colour coding, emergency light	short, one time alert sound	no vibration
2	Very high	Character: corresponding text, red colour coding, emergency light	short, two time alert sound	short, one time vibration

Table 5.4: Specific logical design of **risk levels** for test case 2

Sound and vibration are realised according to the design in section 4.3.6 for every risk level. The class UIAlertView does not automatically play sounds during display of warnings. So the warning sound (basicsound.wav [Sad]) and vibration have to be implemented manually for every warning. That implies a minimal delay during the launch of warnings. This delay is not significant, because the warning does not appear immediately, because it has to be loaded, too. So the sound and vibration appear immediately in the first view.

<sup>92</sup>Risk level 2 in test case 2 equates to risk level 3 in table 4.5 in section 4.3.4.

If the smartphone's sound is turned off, the lack of the acoustic design component should be compensated by an additional vibration. Thus, there is an additional singular and short vibration in this case at risk level 1. At risk level 2 the missing sound would be compensated by two short vibrations. If the smartphone's vibration is turned off, the sound is still played two times at risk level 2. In case of disabling sound and vibration, the warning consists exclusively of the visual design.

### **Information design:**

The warnings are visually designed in a comic style, including an *imaginative character*, which should warn the child with speech bubbles. The speech bubbles have a uniform white background in order to increase the contrast. Furthermore, a font without serifs is used for simplifying reading on the small display. Moreover, we used two symbols in comic style, an emergency light and a green tick mark, for signalling the severity security threats. These symbols are shown in combination with the speech bubble. In order to complete the visual design of the warnings for their realisation, the standard alert style of the iOS (class UIAlert) is used and all components are inserted into an alert box scaled to fit the size of the iPhone display.

The warning is divided into **three views** (see figure 5.14) and there are several possibilities of interaction within the views of the security warning. The *first view* shows the character saying 'Caution'. The 'Next' button of the first view of the warning opens the second view of the warning. The *second view* informs users about the current risks and gives instructions how to handle the risk. On this second view a 'Why?' button opens an additional view of the warning in order to provide more detailed textual information for a better understanding of the warning. That are information about the risk, personal consequences, and instructions. Finally there is the 'OK' button of the second view for acknowledging and closing the warning (warnings 1,3,5) or to switch to the third view (warnings 3 and 4). The *third view* represents guiding information to handle securely, e.g. switch off Bluetooth. Because of the views, it is possible to lead children's attention to the warning. Thus the attention of the current usage scenario is better directed to the warning and additionally it is not feasible to close the warning on the first click. Instead, children are guided out of the current usage scenario through the first view and get more information after clicking 'Next' (the link to the second view). Additionally, it is also possible to integrate more information into the second view using the 'Why?' button and the third view.

### **Warning layout:**

The warnings are realised after the design in section 4.3.6. Table 5.5 introduces all of the warnings. There is one warning designed for risk level 0 (warning 1), three warnings designed for risk level 1 (warning 2 and 3), two warnings designed for risk level 2 (warnings 5 and 6) and three optional warnings (warnings 2b, 3b and 4b). The optional warnings are similar to warning 5 and displayed if participants do not react in a secure way (e.g. install a malware infected update despite a warning).

*Warning 1* (figure 5.12) is shown if the test person clicks on the update button 'Yellow background' in the game menu. The evaluation of the update is simulated. After that the message 'All is ok!' is displayed to show the update could be installed risk-less. The update stayed active if it is installed by the test person.

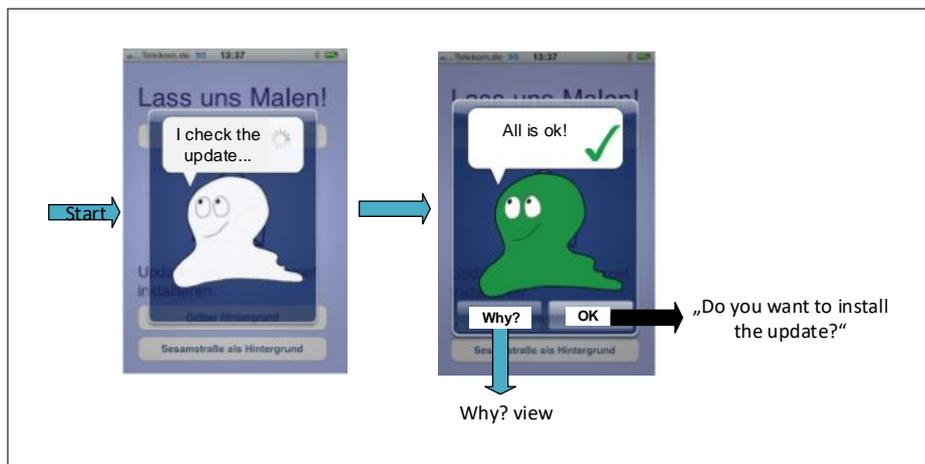


Figure 5.12: Warning 1: Update check with positive result  
(Note: The original warnings are designed in German, but translated for this thesis for better comprehension.)

*Warning 2* (figure 5.13) is displayed if the test person clicks on the update button 'Sesamstreet as background'. The simulated antivirus program shows a warning that the update is virus infected and should not be installed. The installation of the update is an inadequate reaction of the user. It is simulated that the antivirus program detects this case. The control program initiates the display of optional warning 2b, which is similar to warning 5 (figure 5.16). Warnings 3 till 6 and the optional warnings are displayed with help of the control program (described in section 5.2.2).

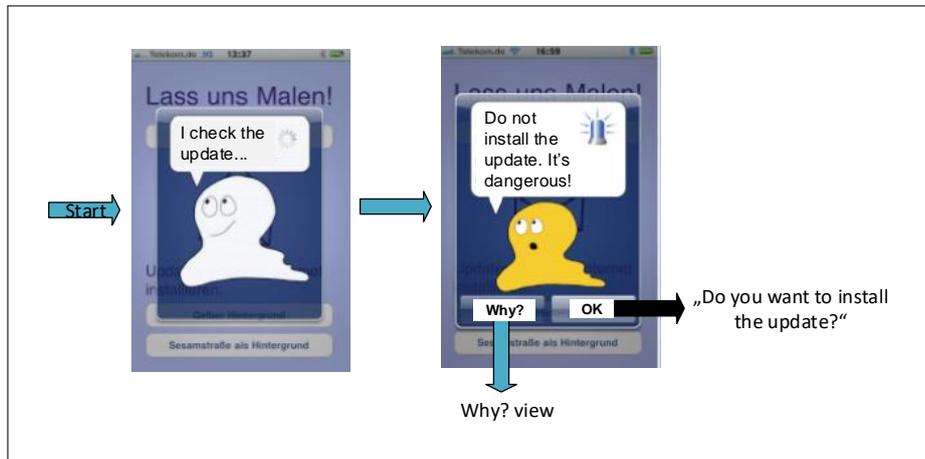


Figure 5.13: Warning 2: Update virus check with negative result

*Warning 3* (figure 5.14) warns for an attack via Bluetooth. The test person should defend the attack by deactivating Bluetooth itself or with help of the antivirus program. The third view is used as guidance for test person, the primary-school child, to deactivate Bluetooth. If the test person does not follow warning 3 and deactivates Bluetooth, optional warning 3b similar to warning 5 (figure 5.16) is displayed. That is a simulation of an virus on the iPhone.

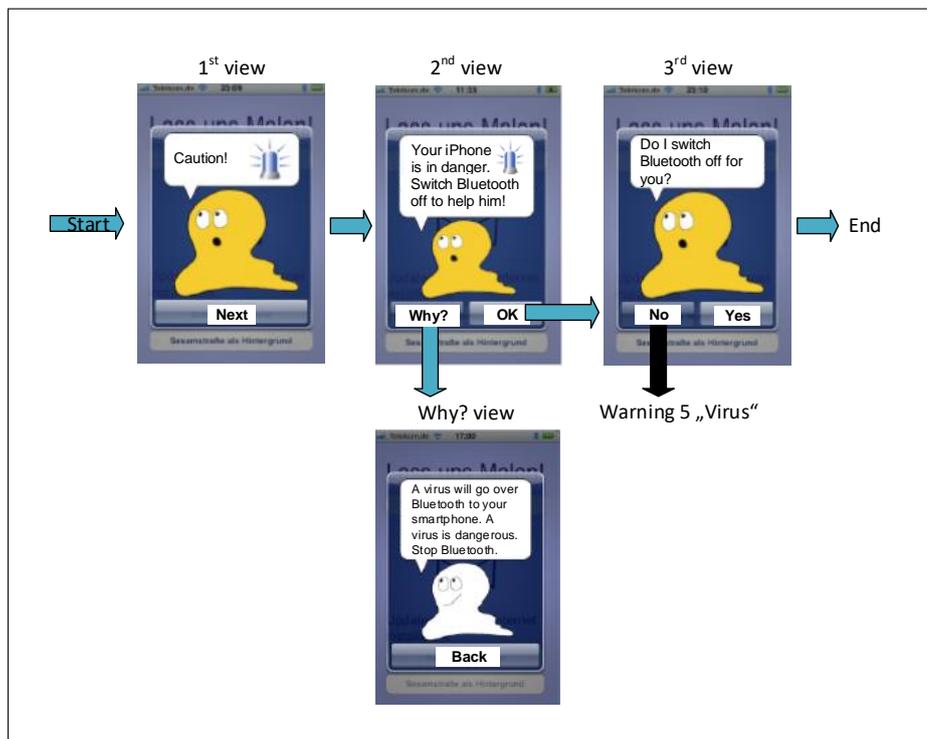


Figure 5.14: Warning 3: Attack via Bluetooth

*Warning 4* (figure 5.15) warns for a virus infected file, which was send to the iPhone. The test person should avoid to receive and store this files. The file could be blocked by the antivirus program. If the test person ignores this warning information, the iPhone is threatened by an infected file. So optional warning 4b (similar to warning 5 in figure 5.16) is displayed to indicate a iPhone virus infection.

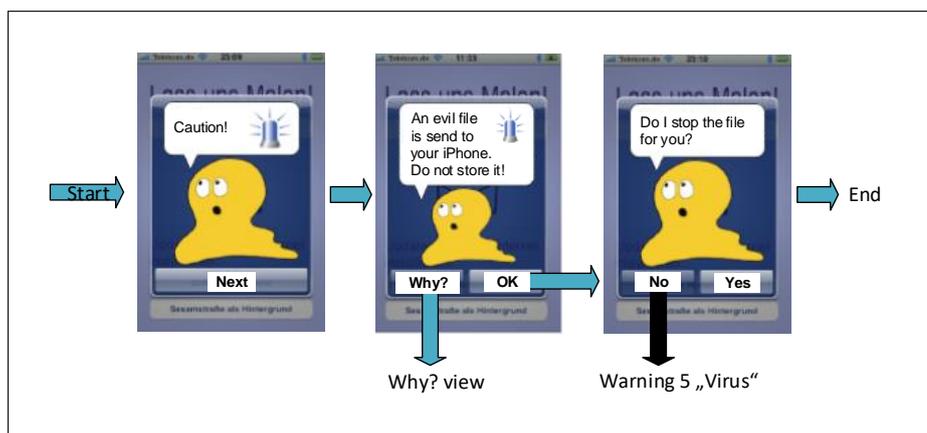


Figure 5.15: Warning 4: Sending a virus infected file to smartphone

*Warning 5* (figure 5.16) warns for a virus on the iPhone. Test persons are motivated to switch off the iPhone and give it to their parents.

*Warning 6* (figure 5.17) shows that the current used app is malware infected. Similar to warning 5 test persons should switch off the iPhone and should hand out to their parents.

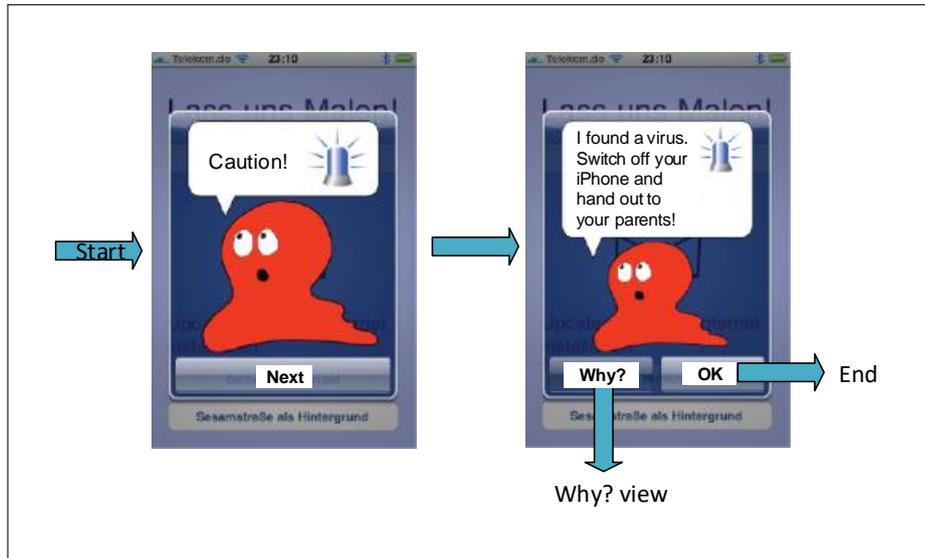


Figure 5.16: Warning 5: Smartphone is virus infected

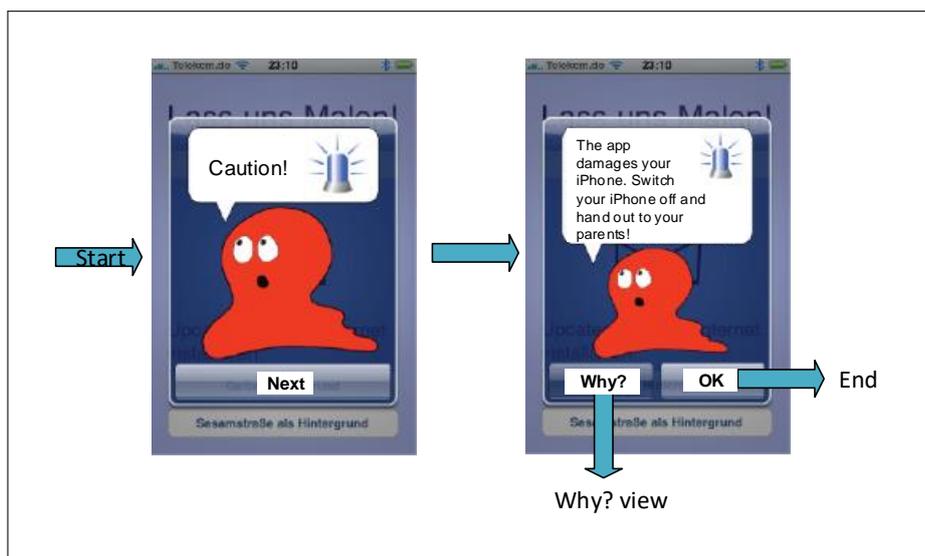


Figure 5.17: Warning 6: Current app is virus infected

For every warning a **'Why?' view** following the design approach in section 4.3.6 is implemented (example for warning 1 in figure 5.18). This symbolised additional information to the current threat. The single 'Why?' views are only differ in the text, which is displayed in a speech bubble. The last column in table 5.5 illustrates the single texts per warning in the 'Why?' view.



Figure 5.18: 'Why?' view of warning 1  
(Note: The other warnings are only differ in speech bubble texts, see. tab. 5.5)

## 5.2. Children - Smartphone warnings

No	Risk (malware activity)	RL	Instructions	Additional information (affected personal requirements in 'Why?' view)	Adequate reaction	Inadequate reaction
1	If update: Check has positive result	0	All is ok!	I have checked the update. It's no virus. You can install the update without danger.	Update installation	No update installation despite of a warning
2	If update: Check has negative result	1	Do not install the update! It's dangerous!	I have checked the update. It's a virus. It's dangerous, because it could spy you ( <i>R<sub>PRIV</sub></i> ).	No update installation	Update installation in spite of the warning
2b	Optional: Virus infected update installation despite a warning	see event no. 5				
3	Attack via Bluetooth	1	Your iPhone is in danger. Switch Bluetooth off to help him!	A virus will go over Bluetooth to your smartphone. A virus is dangerous. Stop Bluetooth.	Switch off Bluetooth manually or automatically	No switch off Bluetooth manually or automatically
3b	Optional: Virus infected update installation despite a warning	see event no. 5				
4	Sending a virus infected file to smartphone	1	An evil file with a virus is send to your iPhone. Do not store it!	An evil file with a virus is send to your iPhone. A virus is dangerous. Do not store the file!	No file storage	File storage in spite of the warning
4b	Optional: Virus infected update installation despite a warning	see event no. 5				
5	Smartphone is virus infected	2	I found a virus. Switch off your iPhone and hand out to your parents!	A virus can harm you ( <i>R<sub>PSAFE</sub></i> ) and damage your iPhone ( <i>R<sub>AVAIL</sub></i> ). Switch off your iPhone and stop the evil virus.	Phone switch off and hand out to parents	Further phone usage despite of a warning
6	Current used app is virus infected	2		The app is an evil virus. It sends your data to foreigners ( <i>R<sub>PRIV</sub></i> ). Switch off your iPhone and stop the evil virus.	Phone switch off and hand out to parents	Further phone usage despite of a warning

Table 5.5: Event matrix with Risks, Instructions, Additional information and reaction cases for test case 2

### 5.2.2 Test Program

---

The display of warnings is realised with two programs, which were running on two different iPhones (test phone, control phone). On the one hand, the main program displays the developed warnings. On the other hand, the control program which causes the warnings to be displayed in the main program via Bluetooth-based remote control. The test persons in the user study use the test device, an iPhone 3G<sup>93</sup>, with the main program. At the same time an assistant, who can observe the candidates but can not be seen by them, uses a second iPhone 4G<sup>94</sup> with the control program. Thus, it is possible to simulate an anti-malware program that displays security warnings to test persons.

The simulated context of the main program consists of a basic painting functionality, in order to give the candidates a task and an application context during the experiment. During the test the game runs on the iPhone 3G and the control program on the iPhone 4G. During the launch of the programs a Bluetooth connection is established between the two iPhones. This was implemented with the GameKit functionality for iOS operation systems.

#### **Main Program:**

The main program includes the paint game 'Lass uns Malen' [Sad], which realises the main task for test persons during the test. The paint game includes a menu (figure 5.19)<sup>95</sup>. to launch the game and two update buttons to install display backgrounds - a yellow background or picture of the Sesamstreet. The update buttons are needed to test different warning risk levels (section 4.3.6). During game launch the menu changes the view and test person can paint something into a white array, remove the painting or go back into the menu (figure 5.20).

The user has the full control over the system (see research field in section 1.1), so she has to be informed when a new update comes in and to agree with its installation. After installing the update 'Yellow background' the painting view changes. The test person could choose between a white and yellow background. The update 'Sesamstreet' includes a simulated computer virus. If the update is installed the malicious function of the virus is simulated with an incomprehensible error message (figure 5.21). The view of the paint game is not changed. After installing one of the both updates the responsible buttons are set in inactive mode with greyed out text. This should show the non-functionality of the buttons.

#### **Control Program:**

The control program initiates the display of warnings in the main program via a Bluetooth connection. Every warning has one button in the control program (figure 5.22). The program is separated into four parts, to give the assistant a good overview. That includes the group of warning, such as warning number 4 and optional warning number 4b. Optional warnings are warnings of the highest risk level, which are triggered through a previous wrong reaction of the test person. For example if an virus infected update was installed, a virus warning should follow.

---

<sup>93</sup>Apple: 'iPhone 3GS - Technical Specifications', <https://support.apple.com/kb/SP565>, accessed: 01. May 2017

<sup>94</sup>Apple: 'iPhone 4GS - Technical Specifications', <https://support.apple.com/kb/SP587>, accessed: 01. May 2017

<sup>95</sup>Note: The original warnings and game foreground are designed in German, but translated for this thesis for better comprehension.

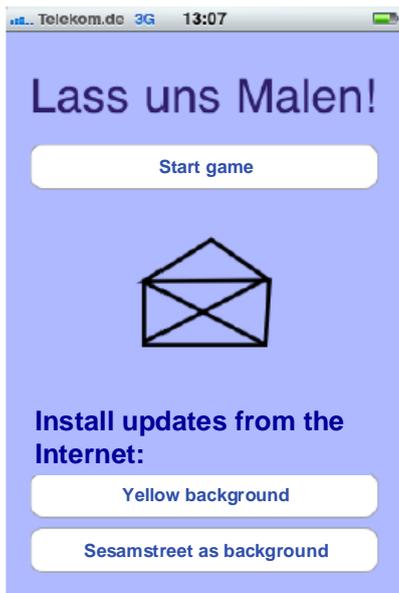


Figure 5.19: Game menu

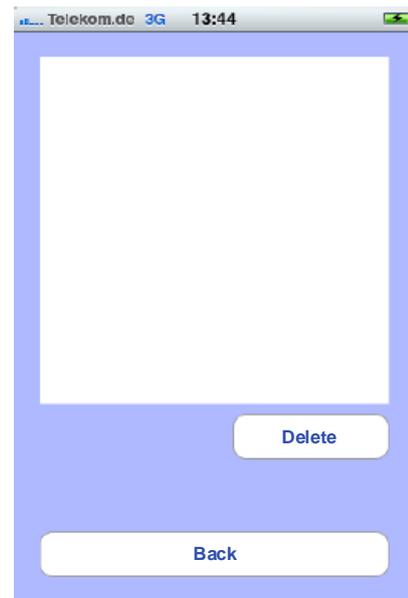


Figure 5.20: Game



Figure 5.21: Installed update 'Sesamstreet'

The order of warning groupings are irrelevant for the program procedure, because the assistant has to activate the warnings randomly. At the beginning the buttons of the optional warnings are inactive. The control program displays a warning when an optional warning has to be activated triggered by warning ignoring of the participant (figure 5.24). Additionally, the corresponding button is activated and highlighted with red text (figure 5.23). Furthermore, the successful display of a warning on the test iPhone is symbolised with an inactive button and grayed out text. During the presenting of one warning in the main menu, the display of additional warnings is blocked. In that case the additional pressed button stays in active mode.

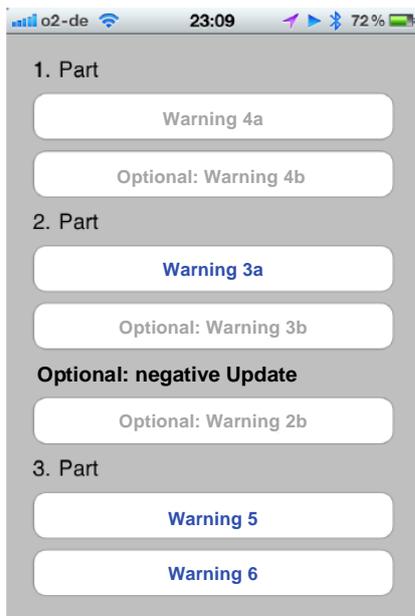


Figure 5.22: Control program after start

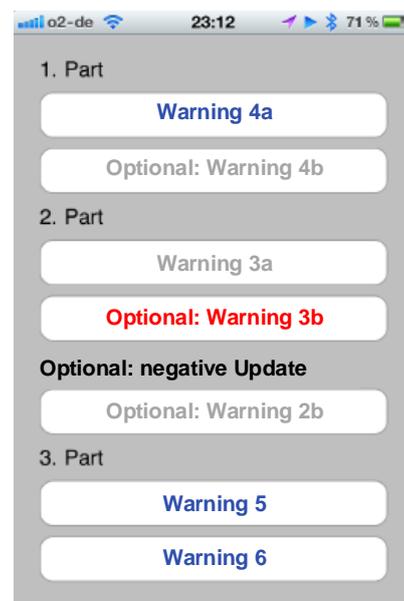


Figure 5.23: Optional warning: activated and highlighted with red text



Figure 5.24: Information for the assistant, that the participant ignores a warning and an optional warning has to be activated

### **Logfile:**

With click on the the iPhone's home key all programs are terminated. This function is also used for the developed programs. The terminating is triggered by click on the OK button in realised warnings. At once on the control device a logfile list in the .plist format is stored. The logfile in figure 5.25 includes date and time of start of the control program, and display and closing of warnings. On basis of the logfile the duration of warning display could be measured. Furthermore, adequate or inadequate reactions of test persons are stored, labelled by the name of the warnings and optional warnings.

The manually notation of the usage of the 'Why?' button by the assistant was very extensive. So after the first day of the user study the logfile was complemented by storing information about the usage of the 'Why?' button.

Property List	Class	Value
▼ Root	Array	14 ordered objects
0	String	15:47:08:21 start4a
1	String	15:47:57:70 end4a
2	String	15:49:18:71 start1
3	String	15:49:22:91 end1
4	String	15:50:05:42 start3a
5	String	15:50:09:92 end3a
6	String	15:52:04:53 start5
7	String	15:52:17:12 end5
8	String	15:53:39:53 start2a
9	String	15:54:30:34 end2a
10	String	15:54:45:24 start2b
11	String	15:54:50:11 end5
12	String	15:55:35:26 start6
13	String	15:55:40:41 end6

Figure 5.25: Excerpt of logfile: optional warning 2b is highlighted in red, logfile show that test person react inadequately to warning 2

### 5.2.3 User study

The following section presents the evaluation with a user study of the **smartphone warnings** realisation for primary-school children. The contents based on [MTF+12], except test environment and test realisation, which based on the bachelor thesis of Wiebke Menzel [Men11].

#### User Study:

The evaluation was carried out in a user study with a class of the 'Trilingual International Primary School' in Magdeburg (Germany) [DIG]. All participating children were 8 to 9 years old (all native German speakers). In the set of 13 evaluation candidates were 8 boys and 5 girls. All these children are familiar with desktop IT systems, because their school lessons of this class are supported with tablet PCs and a digital whiteboard. No child possessed an own smartphone, but 8 of the 13 participating children owned a mobile phone. Some of them used the smartphone of their parents. Only 4 children had used an iPhone before this user study. As a preparation a letter of agreement with an accompanying letter from the school administration were given to the parents to explain the evaluation. Furthermore, the testers introduced themselves to the class and described the evaluation as a user-interface evaluation. There was no mention of display warnings during the test in order to prevent interference.

#### Test environment:

Three different rooms are used for the user study: a class room, a free-time room of the participating class and one work room. The environment was known by the children and belongs to their daily routine. The greeting and introduction of the prototype take place in the class room or free-time room. In figure 5.26 the test situation is re-enacted. The child sat in the middle. On the left side of the child sat the investigator, which wrote the protocol. On the right side of the child sat the assistant, which simulated to take notes. In reality the assistant

operates the second iPhone with the control program to display the warnings on the child's iPhone. Video recordings were not used during the test [BB02]. Reasons are potential negative effects on the test results, because children tend to freeze or perform in front of a camera. Furthermore, a non-observed situation by cameras should create a natural atmosphere. The observations are noted by the investigator instead. The prototype on the child's smartphone generated a logfile about the candidate's handling. The questionnaire was filled in separately with each test person. It was realised with an additional assistant parallel to the beginning of the next test or in the class room or free-time room after the test.



Figure 5.26: Test environment of the smartphone warnings prototype (Photo: Wiebke Menzel)

### Test Realisation:

The test was realised on three consecutive days with 4 till 5 children in a separated test with one child. The test was separated into *introduction* (1-5 minutes), *test* of the warning prototype (15-20 min.) and *questionnaire* (20-35 minutes). The test should not continue more than a teaching lesson (ca. 45 min.) to not overstress the concentration of the children. Before a child was called by their teacher and entered the room, the both apps on both iPhones were launched and connected to each other. The iPhone, which was tested by the child was placed on the table visibly. The assistant hold the smartphone with the control program hidden.

### Introduction:

At the beginning the child was welcomed and the persons in the room were introduced to him/her. After the welcome the test was shortly explained to the test person. The child's role as assistant and helping person to evaluate the prototype was stressed to build trust, reduce fear of the child and to motivate the child to participate the test [JOA03]. The instructions were standardised to minimise effects of instruction variants.

### Test:

At the beginning of the test, the child was asked whether it had ever used an iPhone before. In the following, it was explained that the menu button of the iPhone was paste over to hinder a unintentional closing of the app. After the introduction the test of the prototype started. During the test the child was animated to think loudly. Generally, during the test the children speak very less. One reason could be the focus on the main task, the using of the iPhone

[NRN10]. The double-sided task, usage of the smartphone and thinking aloud at once seem to overload the children's cognitive resources. With the control app the warnings were displayed in randomised distance and order on the test device. A fixed order of warnings was avoided, because this could potentially influence the test results [HH09]. Furthermore, in the protocol the reactions of the child, the comments and pronounced thoughts of the children, respectively, were noted. After every test the both apps of the prototype were re-launched.

### **Questionnaire:**

After the test of the prototype the questionnaire was filled in together with the child (see translated questionnaire: figures 8.11 and 8.12, Original questionnaire: nine pages, 8.13). Amongst the think aloud protocol the questionnaire should clarify, whether the children comprehend the warnings. The questions were read to the child, and the answers of the child are written down or marked with a cross. The procedure was designed in a way to not overstress the concentration of the child and to answer additionally asks of the child during the fill-in process. The answering of the questionnaire took nearly 15 till 20 minutes. During the answering of the questionnaire the reasons of showing the warning was explained to the children. Based on this results, it should clarified, whether the warnings were designed children-friendly. Furthermore, the children were asked, which parts of the warning prototype had to be improved. After the filling of the questionnaire the test was finished.



# 6

## General Results and Discussion

This chapter presents the general results of the two evaluated warning instances for two different user-groups and mobile devices. Section 6.1 describes the results for test case 1, which simulates warnings for a *generic user* on a tablet, which warn about malware attacks against a mobile robot in a domestic environment. Section 6.2 presents the results for test case 2, which simulates warnings for *primary-school children* on a smartphone during its single usage. At the end of this chapter in section 6.3 the results of both test cases are compared with the human-in-the-loop security framework (HITL) model by Cranor [Cra08] to get ideas for further improvement. The chapter is related to research objective 5 (section 1.3).

**RO5: Investigation of influence of personal information and instructions in malware warnings on mobile devices on user's comprehension of warnings and support of users' adequate reaction.**

### 6.1 Generic user - Mobile robot warnings

---

This section describes the results for warnings designed for a generic user adults on a tablet for remote control of a mobile robot. The warnings should warn the user in their home about malware attacks against their mobile robot and the potential personal impacts on users. The test persons are separated into two groups to evaluate the advantage of the new warning design described in general in section 4.3 and test case specific in section 5.1.1. The first group - the experimental group (EG) - were shown detailed instructions in the warning in comparison to the second group - control group (CG), which had only the information about the security risk and potential consequences. Table 4.10 in chapter 4 summarises the evaluation environment and methods for the regarding test case.

**Six evaluation questions (EQ)** (see table 4.10 in chapter 4) are investigated with the user study course. EQ1 investigates *previous experiences* of test candidates, focused on general Internet usage, usage of mobile devices with Internet connection, and experiences with malware. With EQ2 detailed *knowledge* about malware is prompted. The focus lay on the knowledge about existence of malware for smartphones and tablets, and the responsibility of different groups and user activities for distribution of malware. EQ3 investigates the *usefulness* of warning design in general, including questions about fun during the robot usage, helpfulness, uncertainty and concern of warnings, and wish for additional help. With EQ4 detailed *comprehension* of warning information is prompted with focus on rating of danger, comprehension, influence of decision processes and behaviour (only EG) of participants with warnings. EQ5 investigate opinions of test persons regarding the *future of Internet of things*, including rating of likelihood of infection of IoT with malware, usage and future purchase of IoT devices.

With EQ6 *socio-demographic characteristics* are prompted, including sex, age, and profession. All evaluation questions are measured with the questionnaire, except questions EQ3 (usefulness) and 4 (comprehension), which includes additionally results from observations. The questionnaire consist of dichotomous tasks (yes/no questions) as well as rating tasks (scale: 1-min to 6-max). Answers which proof a specific evaluation question, like previous experiences, knowledge and the warning design are rated higher in comparison to other answers. So higher sum of points for the warning design (see table 4.11 in chapter 3) indicates a positive feedback from test candidates. One example is Q35 about wish of additional help: 'How well would have you helped, when you would have had a technical expert?'. When the test person answer 'very much' this is rated with 1, because the need of additional help indicates a lack in warning design. Otherwise when she answered with 'not at all' it is rated with 6, because she need no additional help, which is an indicator for a good warning design. Figures 8.3, 8.4, and 8.5 in the appendix present the questionnaire in more detail.

In the following the section is structured in three parts. At first, the *descriptive analysis* summarises the results of the evaluation via tables, statistical values and diagrams [BS10]. The second part, discusses the results of the *interference statistical analysis*. It is used to verify the hypothesis (first part of table 4.8) with the observations in reality [BS10]. The third part in section 6.1.3 discusses the *quality criteria and limitations* of the study.

### 6.1.1 Descriptive analysis

---

In this section the occurrence of test results for the six research questions are presented. If there are similar occurrences in percent, the results of separated test groups EG and CG are presented as mean value for both groups.

**Socio-demographic characteristics (EQ6)**<sup>96</sup>: Altogether 23 persons, 8 woman (both), 3 (EG) and 4 (CG) men participated the test. They were 29 years old in average. Most of the test persons were students (11 psychology, 1 cultural science, 1 brain science, 1 social work), 4 were engineers, 4 administrative clerks, and 1 person was a social worker. All of the test persons were native German speakers. Answers of EQ6 questions are not summated, because they are a combination of dichotomous selection and rating tasks, which should not be combined according to test theory (section 2.6.3).

**Previous experiences with malware and the Internet (EQ1)**: Nearly the half said (36% EG, 50% CG), that they were itself victims of malware. 70% know someone, who were a victim of malware attacks. Exemplary incidences were infections with malware and malfunction of computers, such as slowing of processes or restricted system accesses. Most of the test persons had *experiences with the Internet*. Most of them go online with a PC (96%), a smartphone (87%), and a tablet (52%). 9% use other devices with an Internet connection. Most of them (91%) go online several times a day. Only 9% use the Internet weekly or occasional. Answers of EQ1 questions are not summated, because they are a combination of dichotomous selection and rating tasks, which should not be combined according to test theory (section 2.6.3).

---

<sup>96</sup>Socio-demographic characteristics are prompted at the end of the questionnaire to avoid 'stereotype threat' influences on answers. That is defined by Myers [Mye15] as 'a self-confirming apprehension that one will be evaluated based on a negative stereotype'.

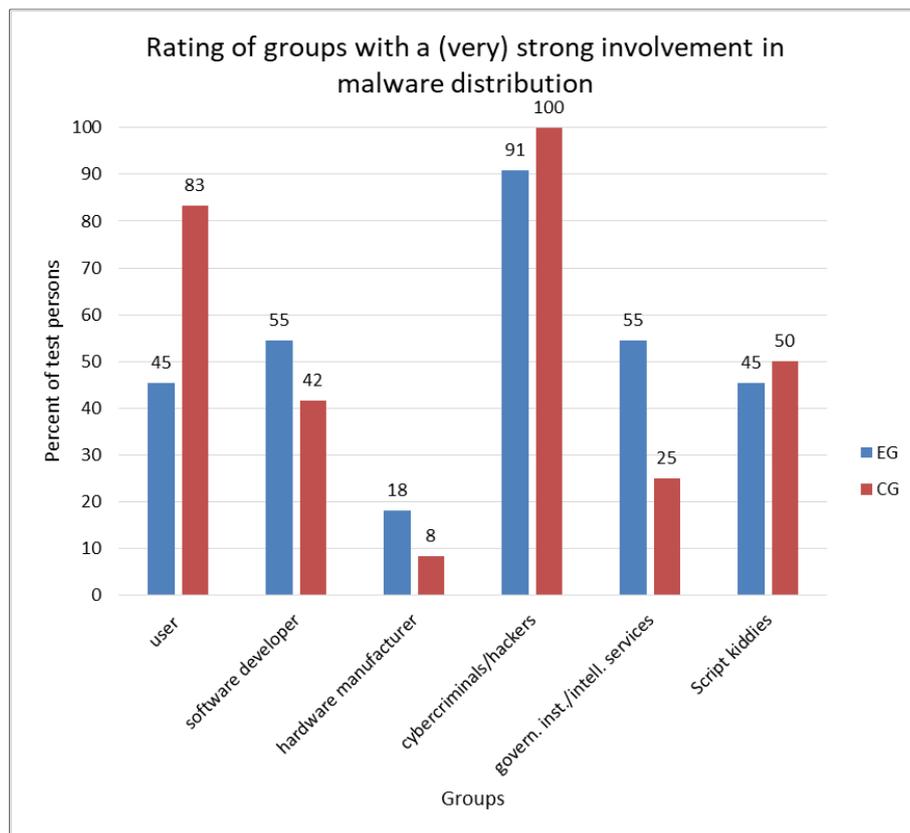


Figure 6.1: Rating results: Responsible groups with a (very) strong involvement in malware distribution

Note: Every test person rated the responsibility of all of six groups.

The figure shows amount of 'strong involvement' and 'very strong involvement' answers to question Q23 (questionnaire 8.3): 'In your opinion, how strong is the involvement of the following persons/groups in distributing computer viruses and Trojan horses?'

**Knowledge about mobile malware, responsibility user groups and user activities for malware distribution (EQ2):** all test persons knew about the *existence of malware implemented for smartphones and tablets*. Additionally, 70% knew that there exist *different classes of malware*, in which most knew the terms 'Virus' and 'Trojan'. Regarding the *responsibility of different groups for malware distribution* there were some differences comparing both test groups (Q23, figure 6.1)<sup>97</sup>. In the experimental group (EG) said 91% cyber-crimes/hacker, 55% software developer and governmental institutions/secret services, 45% users and script kiddies, and 18% hardware manufacturers have a (very)<sup>98</sup> strong involvement in malware distribution. In the control group (CG) said 100% cyber-crimes/hacker, 83% users, 50% script kiddies, 42% software developer, 25% governmental institutions/secret services, and 8% hardware manufacturers have a (very) strong involvement in malware distribution.

<sup>97</sup>The study was realised before the computer hardware vulnerabilities and Meltdown [LSG<sup>+</sup>18] and Spectre attacks [KGG<sup>+</sup>18] were published. This could be an explanation that participants made hardware manufacturers' less responsible for malware attacks as expected.

<sup>98</sup>The use of cramp symbolises two answers. For example '(very) strong' means, that test persons answered with 'strong' as well as with 'very strong'.

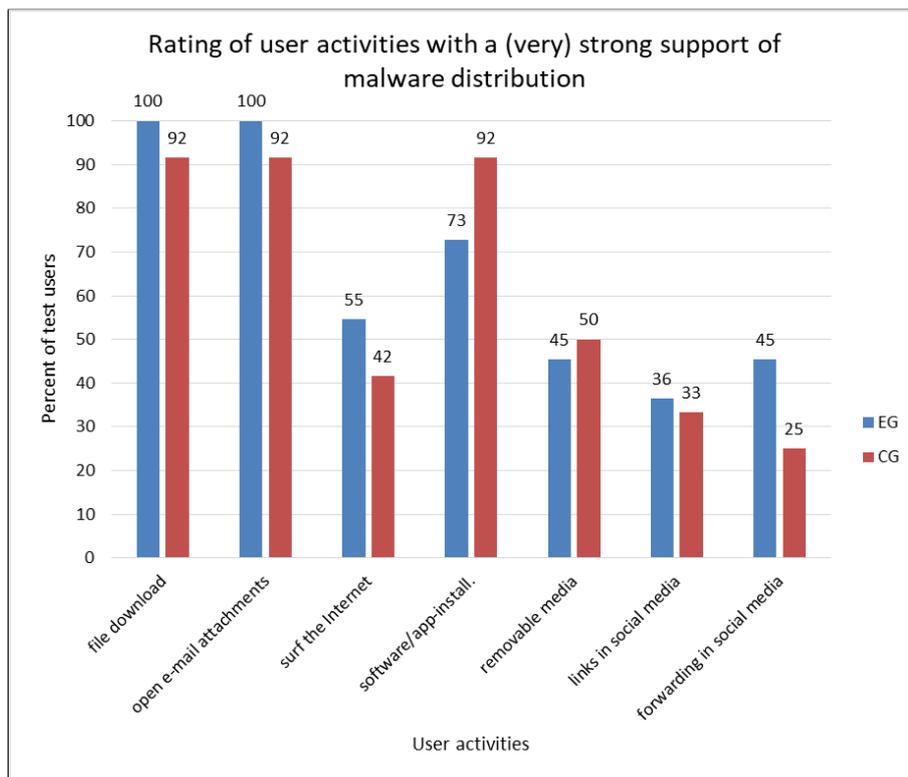


Figure 6.2: Rating results: Responsible user activities with a (very) strong support of malware distribution

(Note: Every test person rated the responsibility of all of seven user activities.

The figure shows amount of 'strong support' and 'very strong support' answers to question Q24 (questionnaire 8.3): 'In your opinion, how strong is the support of the following activities in distributing computer viruses and Trojan horses?')

Regarding the *support of malware distribution by different user activities* (Q24, figure 6.2) most of the test persons meant, that the download of files (96%), open an e-mail attachment (96%), and the installation of software and apps (EG: 75%, CG: 92%) are (very) strong support the distribution of malware. Nearly the half (48%) made surf the Internet, and usage of removable media, and one third (35%) made links and forwarding in social media responsible for malware distribution. Over the half (61%) said, that is (most) likely that networked domestic robots could be infected with malware.

Both groups achieved in average<sup>99</sup> 58 points, which symbolises according to table 4.11 a midrange result (38-60 points).

The average points for the 'knowledge' category has to be discussed, because the answers for Q23 and Q24 are not weighted regarding the correct answer. That means, if a test person answered with 'very strong' for all groups/user activities in both questions she would had achieved the maximum number in both questions. This has to be considered for questionnaire design in future tests.

<sup>99</sup>As illustrated in table 4.11 in chapter 4 the points of answers for every EQ are summated to get a better comparison between both test groups.

**Usefulness of warning design (EQ3):** over the half (63%) of EG and the half (50%) of CG said that they had (very) much *fun using the robot*. Nearly the half (45%) of EG and (58%) of CG rated the warning messages as (very) *helpful*. Over the half (55%) of EG and (67%) of CG were strongly *unsettled* by the warning messages. Over the half (54%) of EG were some (strongly) and over the half (66%) of CG were (very) strongly *concerned* by the warning messages. Regarding *additional help* over the half (55%) of EG and every fourth (25%) of CG wished support by a step-by-step instruction, every third (36%) of EG and most of the CG (67%) wished support by a technical-savvy friend or relation, most (64%) of EG and all (100%) of the CG wished support by a technical expert, only every fifth of EG (18%) and CG (17%) wanted support by a user guide.

According to answers in question category 'usefulness' (EQ3) EG members achieved in average 24 points, which means 'little useful' warnings. CG members achieved in average 21 points, which symbolises 'very little useful' warnings. That means the ratings for EG lay according to table 4.11 in a middle average range (22-34 points), whereas the ratings of CG members lay in the low average range (8-22 points).

**Comprehension of warnings (EQ4):** regarding the rating of the **risk level**<sup>100</sup> relating to a **specific warning icon** (Q41) most members (92%) of both test groups rated the red octagon icon with 'very high danger' (see icon in appendix on figure 8.4). The results for the yellow triangle symbol are more variant in both groups. They rated the symbol as follows: no-one of EG and 8% of CG with 'very high danger', 55% of EG and 33% of CG with 'high danger', 27% of EG and 33% of CG with 'some danger' and 18% of EG and 25% of CG with 'less danger'.

Regarding the **relation of risk level to combination of acoustical signal and vibration** (Q42) most of the test persons of both groups recognised a difference in the risk level. 82% of EG and all of CG classified the warning *without acoustical signal and without vibration* as 'some danger' or 'little danger'. 91% of EG and 83% of CG classified the warning *with acoustical signal and without vibration* as 'high danger'. Most of the test persons of both groups (82% of EG and 83% of CG) classified the warning message *with acoustical signal and with vibration* as 'very high danger'.

In question block Q43 all ten warning messages for the mobile robot are evaluated (see questionnaire in figure 8.4 in the appendix). Therefore, both test groups get three different questions per warning message: first, how they rate the **risk level** of the situation described by the warnings; second, user's **comprehension** of the warnings; third, influence of user's **decision making** by the warnings. Additionally, the EG get one more question, how their **actions** are influenced by the warnings instructions.

---

<sup>100</sup>In the questionnaire the term 'danger level' is used, so that users, who are non-security experts understand the question.

Figure 6.3 illustrates the **risk level** ratings of all warnings with 'very dangerous' by all participants. All other ratings are found in the appendix in table 8.1 for RL1 warnings, table 8.2 for RL2 warnings, and table 8.3 for RL3 warnings. Figure 6.3 shows in general that CG members' ratings and EG members' ratings are in most cases very different for each warning. Conspicuous are differences for warnings number 1, 3, and 8 with more than 20 points difference and low ratings for warning number 5. The first both warnings number 1 ('unauthorised manipulation of robot map') and 3 ('unsigned update') were designed with **risk level 2** (high, 'dangerous') symbolised with a red octagon icon and short and single alert signal. Warning number 8 ('unauthorised communication with the Internet') and 5 ('strong software activity') are designed with **risk level 1** (low, 'some dangerous') symbolised with a yellow icon and no alert signal.

Another conspicuousness in figure 6.3 are the ratings for warning 8 ('unauthorised communication of robot with Internet'). Most of the test persons (EG:73%, CG:58%) classified this warning with risk level 3 ('very dangerous') although it was designed as warning with risk level 1 ('some dangerous').

Also the ratings for warning 5 ('strong software activity') are conspicuous. Figure 8.10 in the appendix show that the results for both groups were nearly normal distributed. Both groups achieved in average 52 points for the question 'risk level' (Q43.WMNo.01), which means most participants rated the risk level of every warning with 'dangerous' (5.2 points).

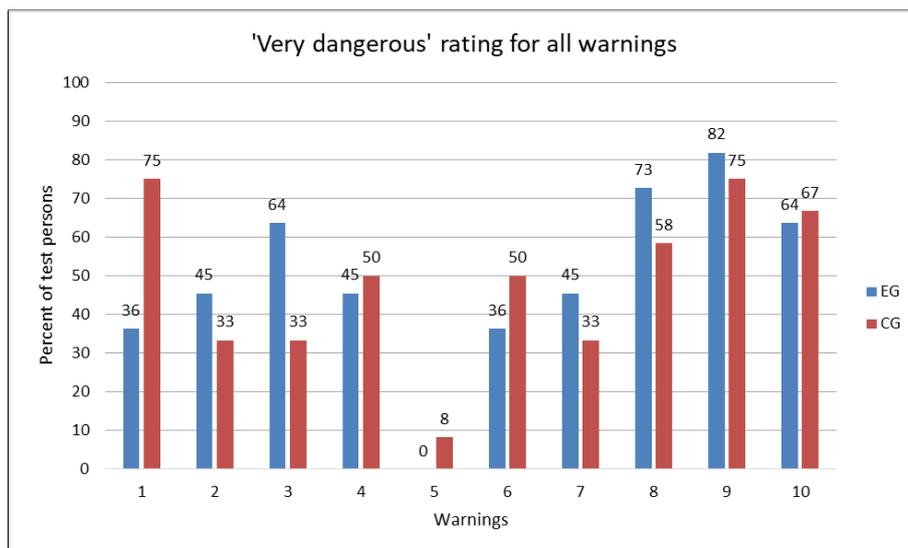


Figure 6.3: 'Very dangerous' risk level ratings for all warnings  
 (Note: The figure shows the amount of 'very dangerous' answers to question Q43.WMNo.01 (figure 8.4): 'How dangerous do you perceive the described situation in the warning?'.)

Figure 6.4 shows the 'very dangerous' risk level ratings for both groups for risk level 3 warnings (9 and 10). Warnings number 9 ('unauthorised sending of pictures to the Internet') and 10 ('unauthorised sending of audio signals to the Internet') are designed with the highest **risk level 3** (very high, 'very dangerous'), coded with a red octagon icon and permanent alert signal. The risk level ratings of both groups for risk level 3 warnings (9 and 10) are higher than risk level 2 warning ratings and similar in both test groups. So 82% of EG and 75% of CG classified warning 9, and 64% of EG and 67% of CG classified warning 10 as 'very high danger'.

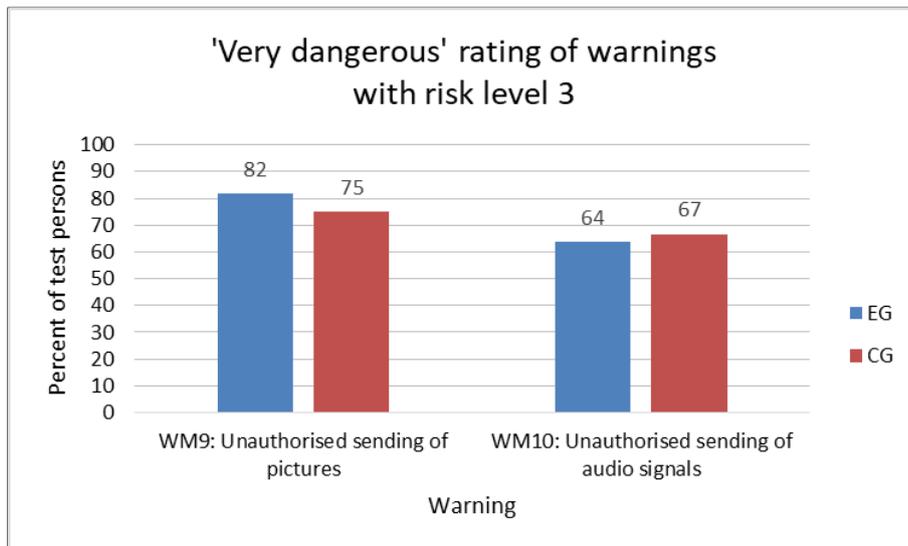


Figure 6.4: 'Very dangerous' risk level ratings for risk level 3 warnings (WM9,10)  
 (Note: The figure shows the amount of 'very dangerous' answers to question Q43\_WMNo.01 (figure 8.4): 'How dangerous do you perceive the described situation in the warning?'.)

Figure 6.5 shows the 'very dangerous' risk level ratings and figure 6.6 'dangerous' ratings for both groups for risk level 2 warnings (1 and 3). For this warnings there are very large differences of ratings between both test groups measured. As figure 6.5 shows 36% of EG and 75% of CG classified warning 1 and 64% of EG and 33% of CG classified warning 3 as 'very dangerous' warning. As figure 6.6 shows 36% of EG and 8% of CG classified warning 1 and 27% of EG and 58% of CG classified warning 3 as 'dangerous' warning similar to the warning design.

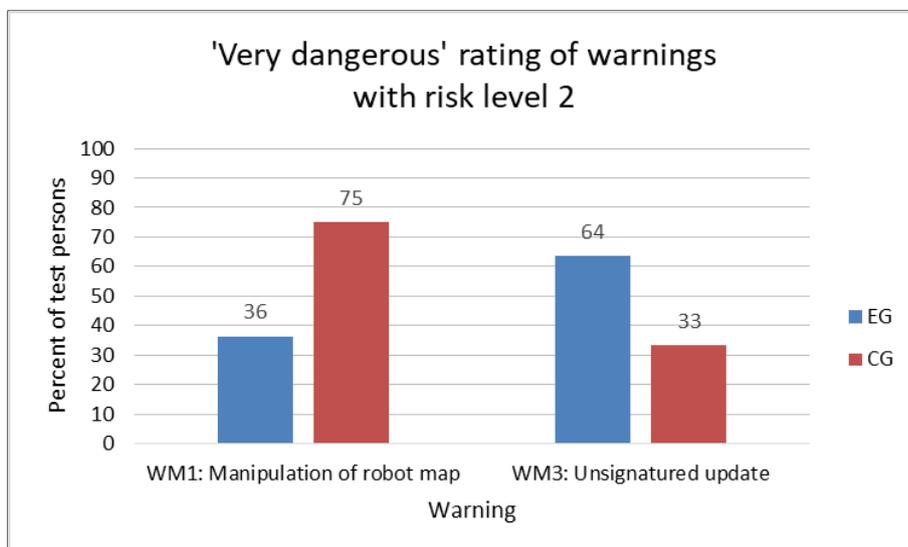


Figure 6.5: 'Very dangerous' risk level ratings for risk level 2 warnings (WM1,3)  
 (Note: The figure shows the amount of 'very dangerous' answers to question Q43\_WMNo.01 (figure 8.4): 'How dangerous do you perceive the described situation in the warning?'.)

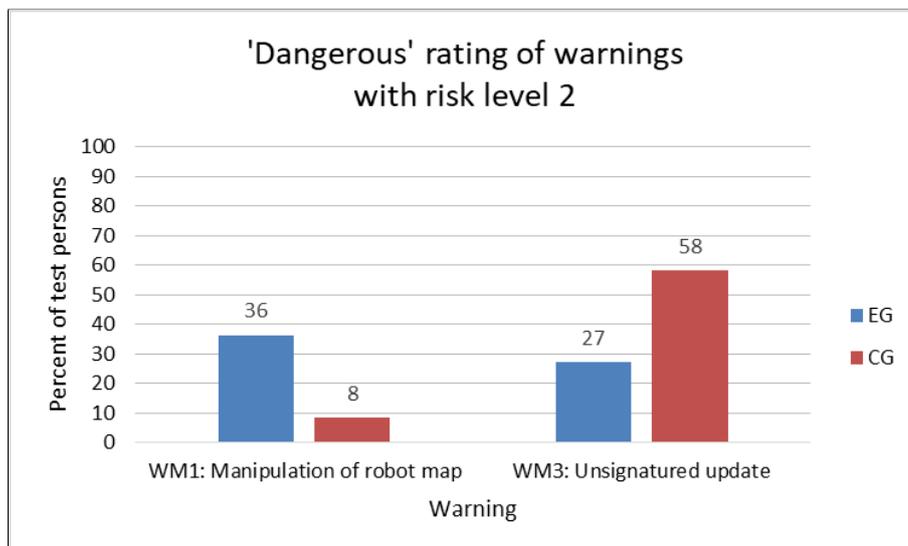


Figure 6.6: 'Dangerous' risk level ratings for risk level 2 warnings (WM1,3)  
 (Note: The figure shows the amount of 'very dangerous' answers to question Q43\_WMNo\_01 (figure 8.4): 'How dangerous do you perceive the described situation in the warning?'.)

The second question was how test persons rate the **comprehension** of the designed warnings (Q43\_WMNo\_02). Tables 8.4, 8.5, and 8.6 in the appendix show the comprehension ratings for all warnings of both test groups. As figure 6.7 shows more control group members rated each warning more often in comparison to the EG with 'very comprehensible'. The best rated warning messages were number 9 ('unauthorised sending of pictures to the Internet') and 10 ('unauthorised sending of audio signals to the Internet'). 73% of EG and 92% of CG rated the comprehension of warning 9, and 73% of EG and 83% of CG rated warning 10 with 'very comprehensible'. Additionally, minimum the half of test persons from CG rated warnings 1-4 ('unauthorised manipulation of robot map', 'unauthorised registration on robot', 'unsigned update', 'unknown software autostart'), and 8 ('unauthorised communication with the Internet') as 'very comprehensible'.

EG members achieved in average 52 points for question 'comprehension' (Q43\_WMNo\_02) and CG members 56, which means that all participants rated the warnings in average with 'very comprehensible'. That symbolises a higher average range (43-60 points) according to table 4.11.

The third question was how the test persons were influenced by warnings in their **decisions** (Q43\_WMNo\_03). Both groups achieved in average 53 points for question 'decisions', which means most participants said the warnings influenced their decisions 'very strongly'. That symbolises a higher average range (43-60 points) according to table 4.11.

Because of the additional instruction information in warnings the experimental group get one additional question (Q43\_WMNo\_04) than the CG members. They were asked how their **action** were influenced by the warning instructions. In average EG members achieved in average 52 points, which means that EG members' actions were 'very much' influenced by warning instructions. That symbolises a higher average range (43-60 points) according to table 4.11.

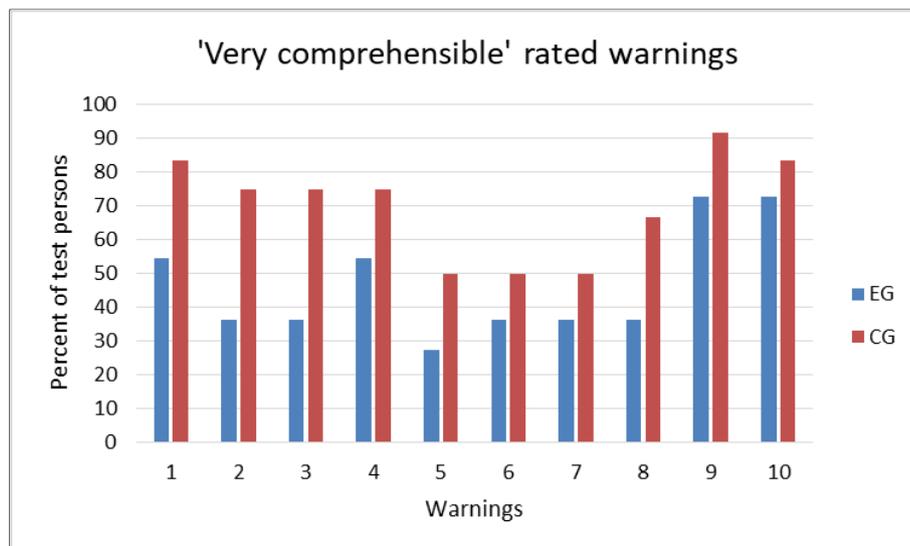


Figure 6.7: Test results: 'Very comprehensible' rating of all warnings of both test groups

**Future of Internet of Things (EQ5):** most test persons of both groups (83%) mentioned that it is (very) likely that *IoT devices could be infected with malware*. Every fifth (22%) affirmed currently to use an IoT device. Examples are smartphones, TVs, surveillance cameras, and fridges. Every third (31%) intended to *use smart IoT domestic devices in the near future*. Examples are thermostats, fridges, TVs, control of smart home, roller shutter, and stereo.

Answers of EQ5 questions are not averaged, because they are a combination of dichotomous selection and rating tasks, which should not be combined according to the test theory (section 2.6.3).

#### Observation and think aloud protocol:

The evaluation protocols show one *main difference* between both test groups. The EG members are more *able to find an adequate solution* without external help which solves the malware-related problem in comparison to the CG members. Most EG members at first tried to find a solution according to the warning instructions. As second solution they said they would have called a technical support. In comparison to EG members CG members did not find adequate solutions, they immediately wish to call the technical support and wanted to switch off the robot, respectively. It could be reasoned that EG members are better understand the underlying security problem on basis of the instructions.

#### Logfile analysis:

As introduced in section 5.1.2 users' click events on warning buttons are stored in a logfile (see procedure in figure 5.7). The click-through rates of participants for both test groups are measured for the two warning views (risk and personal consequences). These results are not accurate, because of the test case realisation, where sometimes the test person was in conversation with the tester, while the next warning was just presented. Nevertheless, figure 6.8 shows, that for EG members shorter click-through rates are measured. One reason for this difference could be the EG members' trust in the assumption that at the end of the warning a solution for the malware problem will be presented to them, and so they had clicked faster through the warnings than CG members without warning instructions.

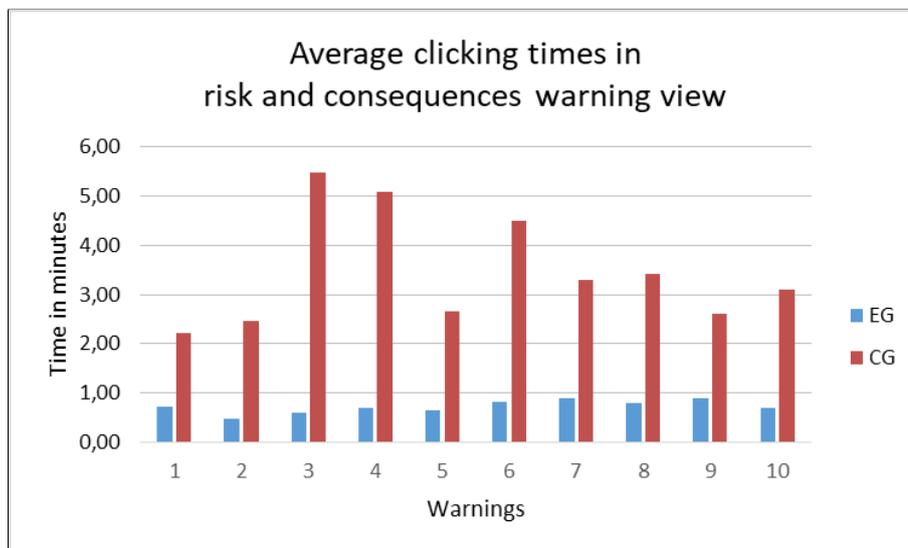


Figure 6.8: Average clicking times in risk and consequences warning view for all warnings and both test groups (EG,CG)

### 6.1.2 Inference statistical analysis and Discussion

The inference statistical analysis was realised with a SPSS program version 24. It used two different analysis types: first, the analysis of Cohen's effect size  $d$  after Bortz [BS10], and the two-sided correlation according to Pearson. Cohen's effect size is applicable for small sample sizes and is a reference for practical relevance of the test results [FEPS09]. If the standard deviation of the test results of both groups are not homogeneous the Cohen's  $d$  formula 2.2 is calculated with the formula 2.3 for joint variance after Bortz [FEPS09]. The second analysis - correlation according to Pearson - measures whether there is a linear dependency between two specific characteristics. The analysis of the *Cohen's effect size  $d$*  and the *two-sided correlation according to Pearson* produces some results (see table 8.8 in appendix), which are discussed in the following according to the four hypothesis introduced in section 4.4.1 (see first part of table 4.8). These results are complemented by the results for the six specific evaluation questions (EQ).

#### **H1: Evaluation group members (EG) will be more likely to rate usefulness of warnings higher than the control group (CG).**

This hypothesis *is* supported by the inference statistical analysis. EG members achieved higher results in average for the 'usefulness' category than CG members. After the skip of single extreme values in the results of both groups (see section 2.7) the mean values were corrected. The differences between both test group is supported by a 'strong' Cohen's effect size ( $d=0.895$ ). Additionally, other interesting correlations according to the warning **usefulness** (EQ3) are found. The evaluation of the **usefulness of warning design (EQ3)** resulted in a *correlation of usefulness of warnings and wish of external help*. Users in general (both test groups) who recognised warnings as 'little useful' and 'small useful' desired more external help. Four figures show the correlation of sum 'usefulness' with four answers of Q35 (see questionnaire in the appendix in figure 8.4). Figure 6.9 shows the correlation results for 'support by a step-by-step instructions' ( $r = 0.453; p < 0.05$ ), figure 6.10 for 'support by a technical-savvy friend/relation' ( $r = 0.618; p < 0.01$ ), figure 6.11 for 'support by a technical expert' ( $r = 0.471; p < 0.05$ ), and figure 6.12 for 'support by a user guide' ( $r = 0.463; p < 0.05$ ).

The above mentioned figures show on the:

- **X-axis:** the amount of participants, who *equally rated* the *first correlated item* (e.g. helpfulness of support by technical expert) symbolised with similar *colours*.
- **Y-axis:** the *second correlated item* expressed as *average* of all answers of all participants in a specific question category (e.g. usefulness of warnings).
- **Axis parallel to x-axis:** the *first correlated item* expressed as *average* of all answers of all participants for a specific question (e.g. helpfulness of support by technical expert) or in a specific question category (e.g. decision influence).
- **Horizontal lines:** separate results of the second correlated item on y-axis.
- **Vertical lines:** separate results of the first correlated item on x-axis.

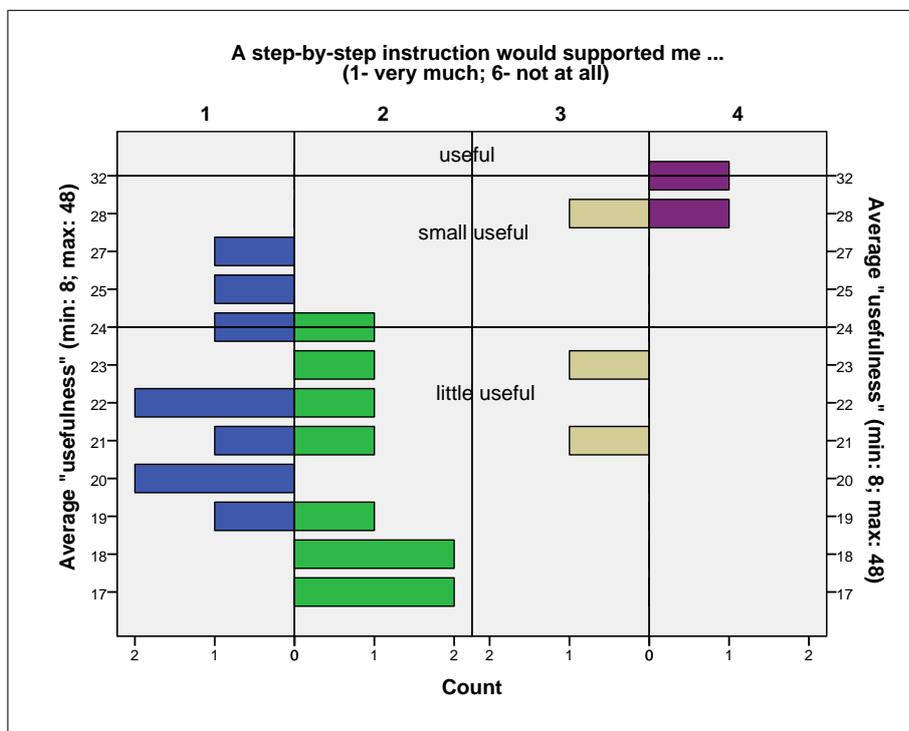


Figure 6.9: Test results: Correlation of average 'usefulness' and Rating of support by a step-by-step instruction

(Note: X-axis: amount of participants, who equally rated the support (grouped by colours);  
 Y-axis: average of all answers to question category 'usefulness' (EQ3),  
 Average range: 8-15:not at all, 15-22:very little useful, 22-28:little useful,  
 28-34:some useful, 34-41:useful, 41-48:very useful;  
 Axis parallel to x-axis: ratings of support by a step-by-step instruction:  
 1:very much, 2:much, 3:some, 4:little, 5:very little, 6:not at all)

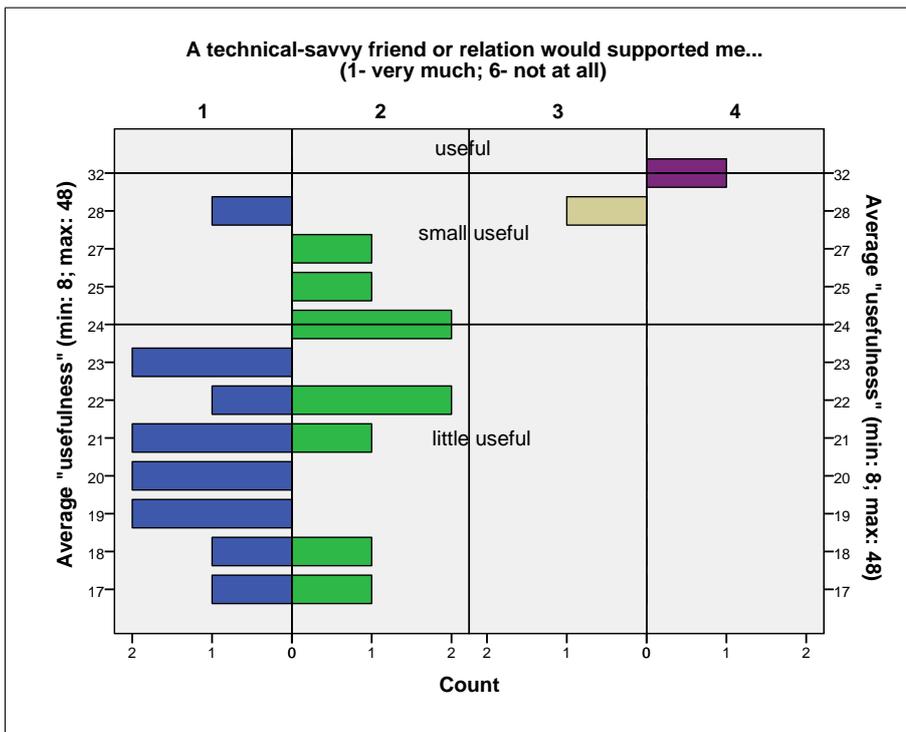


Figure 6.10: Test results: Correlation of average 'usefulness' and Rating of technical-savvy friend support (Note: X-axis: amount of participants, who equally rated the support (grouped by colours); Y-axis: average of all answers to question category 'usefulness' (EQ3), Average range: 8-15:not at all, 15-22:very little useful, 22-28:little useful, 28-34:some useful, 34-41:useful, 41-48:very useful; Axis parallel to x-axis: ratings of support by a technical-savvy friend: 1:very much, 2:much, 3:some, 4:little, 5:very little, 6:not at all)

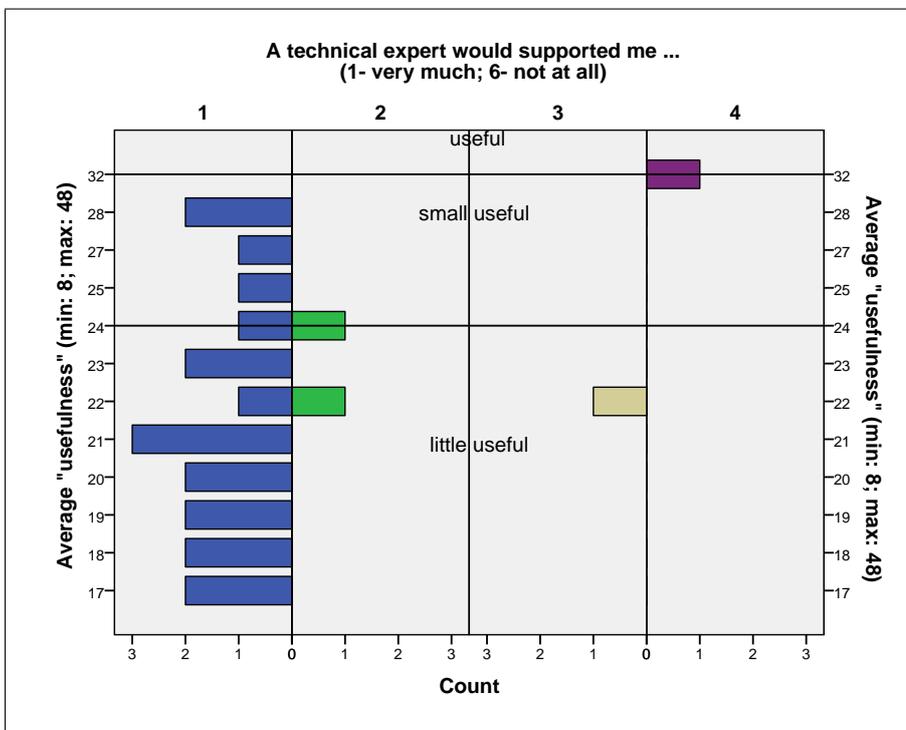


Figure 6.11: Test results: Correlation of average 'usefulness' and Rating of support of a technical expert (Note: X-axis: amount of participants, who equally rated the support (grouped by colours); Y-axis: average of all answers to question category 'usefulness' (EQ3), Average range: 8-15:not at all, 15-22:very little useful, 22-28:little useful, 28-34:some useful, 34-41:useful, 41-48:very useful; Axis parallel to x-axis: ratings of support by a technical expert: 1:very much, 2:much, 3:some, 4:little, 5:very little, 6:not at all)

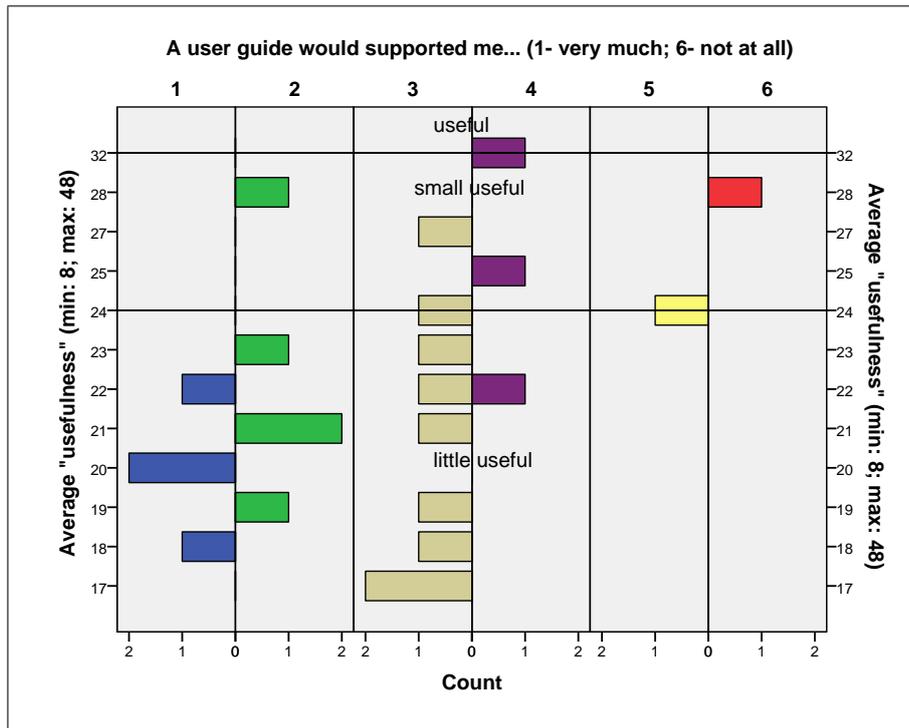


Figure 6.12: Test results: Correlation of average 'usefulness' and Rating of support by a user guide  
 (Note: X-axis: amount of participants, who equally rated the support (grouped by colours);  
 Y-axis: average of all answers to question category 'usefulness' (EQ3),  
 d Axis parallel to x-axis: ratings support by a user guide:  
 1:very much, 2:much, 3:some, 4:little, 5:very little, 6:not at all)

**H2: Evaluation group members (EG) will be more likely to desire less external help than the control group (CG).**

This hypothesis is *not* statistically supported by the analysis, but there are *indicators* which support H2. So a correlation of *test group and support of technical expert* was found ( $r = -0.425; p < 0.05$ ). As figure 6.13 shows, all members of CG rated the support of technical expert as 'very helpful'. In comparison, to CG the results for EG are more variant. Only 64% EG members rated the support of technical expert as 'very helpful'. Furthermore, more CG members (67%) than EG members (36%) wished support by a technical-savvy friend or relation. EG, the test group with more warning information, desired in average less additional support by a technical expert or technical-savvy friend in comparison to the control group. This should be an indicator that additional instructions in warnings help users with their problem solving, but the differences between both test groups are very little. So only 4 of 11 EG participants answered different to the 'very much' answer of 12 CG members. In the future, here are experiments with larger test groups needed to support H2. Surprisingly, more EG members (55%) than CG members (25%) rated a 'step-by-step instruction' as 'very helpful'. This is an indicator, that the current warning design with instructions has to be improved.

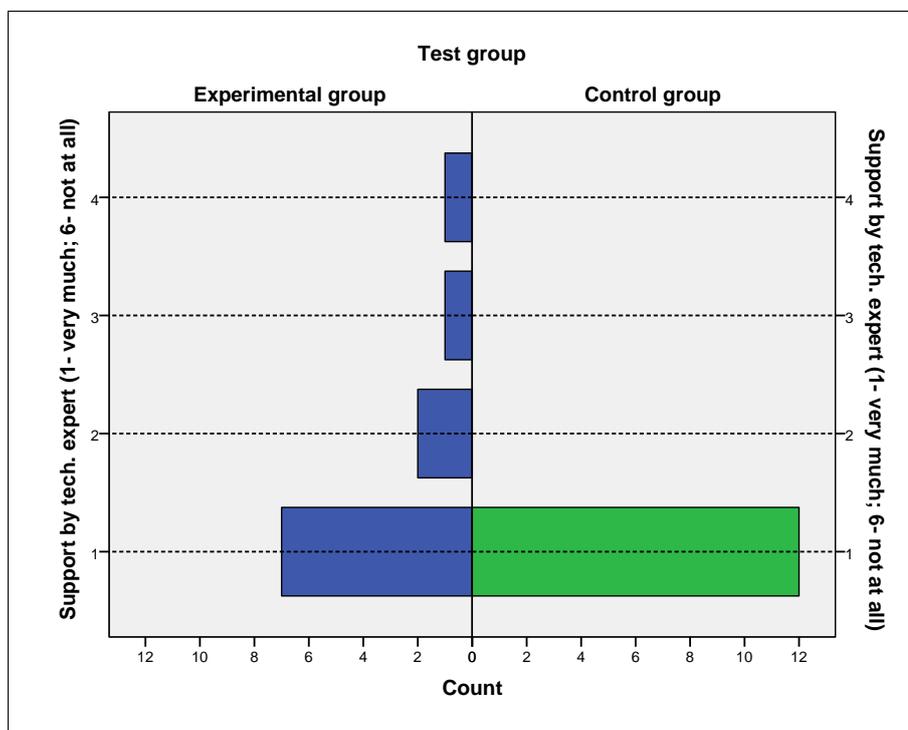


Figure 6.13: Test results: Correlation of group and support by a technical expert  
 (Note: X-axis: amount of participants in both test groups, who equally rated the support;

Y-axis: rating of support by a technical expert:  
 1:very much, 2:much, 3:some, 4:little, 5:very little, 6:not at all  
 Axis parallel to x-axis: both test groups (grouped by colours))

### **Touch of users' emotions (Concern and unsettlement by warnings (Q33,Q34)):**

In the test the participants of the both test groups are differently emotionally touched by the warnings. More members of CG (67%) than the EG (55%) said, that they were 'strongly unsettled' by the warnings (Q33). A more clear difference is found for the rating of concerning by warnings (Q34). 66% members of CG and only 36% members of EG were '(very) strongly concerned by the warnings. This could be an indicator that warnings with instructions could melt the fear of users of malware-related personal impacts, because they know what to do against it because they are instructed by the warnings. This new warning design could be a contribution to Angela Sasses' [Sas15] appeal for not scaring the user with security warnings. Nevertheless, this assumption is not supported by the inference statistical analysis.

### **Helpfulness of warnings (Q35):**

Surprisingly, more members of CG (58%) in comparison to the EG (45%) rated the warnings in general as '(very) helpful'. Potentially the complete warning design presented to the experimental group (including information about the risk, personal consequences, and instructions) is too complex. Nevertheless, this assumption is not supported by the inference statistical analysis and has to be evaluated in future experiments.

### **Usefulness of warnings (Average values):**

According to figure 6.14 surprisingly, younger test persons (all participants were aged between 19 and 57 years) rated the warnings in general as 'little useful' in comparison to elder participants ( $r = 0.500; p < 0.05$ ). Because of the small size of test persons (23 participants) and the high amount of younger participants (12 were under 25 years old) this result couldn't be generalised. It has to be evaluated in future tests whether the new warning design is better adapted to needs of users in a specific age range.

### **Risk level:**

Tables 8.1, 8.2, and 8.3 in the appendix show the risk level ratings for all warnings of both test groups. As already mentioned in the descriptive analysis sections most participants rated in average the risk level of the warnings with 52 points. That means they rate every warning in average with 5.2 points ('dangerous'). All warnings are designed with an average rate of 46 points<sup>101</sup>, which means an average rate for every single warning of 4.6 points ('some dangerous'). So the participants rate the risk level of the warnings higher as designed. This indicates that the warnings has to be improved to communicate the right risk level to non-expert users.

Conspicuous in figure 6.5 are the very different 'very dangerous' rating results for risk level 2 *warnings 1 and 3* (20 points difference between both test groups). Most of the CG members classified warning 1 and most of the EG members warning 3 with 'very dangerous', which equates to risk level 3. The high warning 1 ratings of CG members could be explained by the given warning information, which only includes the risk (robot map manipulation) and that personal objects and persons could be harmed. EG members instead were instructed what to do against the risk (robot stop, antivirus check, map rebuild). The high warning 3 ratings of EG members could have several reasons. It could be reasoned that the small design differences to risk level 3 warnings (duration of alert signal) were not perceived by the participants.

---

<sup>101</sup>Designed risk level for all warnings: 2x6 points for risk level 3 ('very dangerous') 2x5 points for risk level 2 ('dangerous'), 6x4 for risk level 1 ('some dangerous') = 12+10+24=46 points.

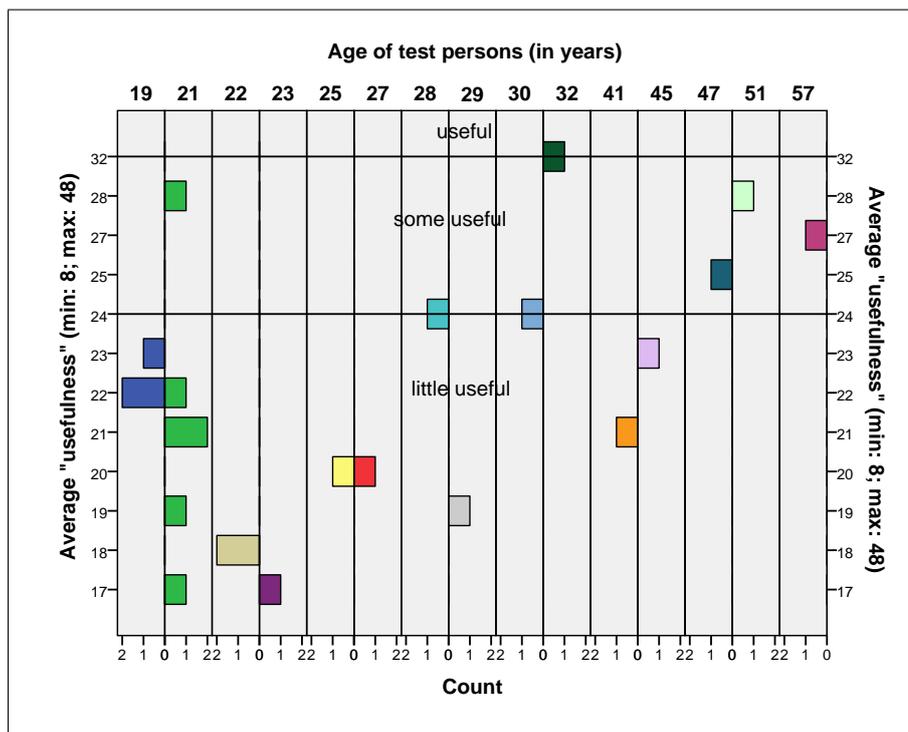


Figure 6.14: Test results: Correlation of average 'usefulness' and age  
 (Note: X-axis: amount of test persons in the same age (grouped by colours);  
 Y-axis: average of all answers to question category 'usefulness' (EQ3),  
 Average range: 8-15: not at all, 15-22: very little useful, 22-28: little useful,  
 28-34: some useful, 34-41: useful, 41-48: very useful;  
 Axis parallel to x-axis: age of test persons in years)

Just as well the display time after warning 8, which RL were also very high rated by EG members, could have been important for the rating. Another reason could be that the warning information for EG members (with instructions) were not so comprehensible (only 36% rated with 'very comprehensible'), so the warning were perceived as higher risk warning.

The adequate rating of warnings 9 and 10 by nearly all participants indicates, that the warning information and warning design are well selected.

Furthermore, participants rated warning 8 with a higher risk level as designed (RL 3 instead of RL1). Warning 8 is designed with risk level 1 (low), because the attacker (or a attacker tool such as a malware) could download undesired software to control the robot or infect other robot connected devices with malware. Therefore, warning 8 alert users for personal consequences, which includes the decreased availability of their robot ( $R_{AVAIL}$ ) and potential malware infection of other connected systems (see table 5.3 in section 4). As figure 5.11 in section 4 shows, warning 8 is presented right after two warnings with risk level 3 (WM9) and 2 (WM1). For test persons the risk description of warning 9 'Without permission the microphone of your robot sends audio signals to the Internet' seem to be similar to risk description of warning 8 'Your robot communicated unauthorised with the Internet'. So they rated warning 8 with a higher risk level as designed. In future, these interferences could be minimised by using a changing display order of warnings for all test persons. Furthermore, to picture the intended risk level, the textual information seem to be improved in future realisations to prevent personal imaginations and speculation about the intended background information.

In comparison to the other warnings the risk level of *warning 5* ('unusual software activity') was not clear by all test persons. The results were normal distributed. That could indicate, that users do not understand the communicated risk in the warning. Here the design of warnings has to be improved, so that the communicated risk level is clear.

Amongst the risk level design of the warnings itself also the **risk level design of the single both icons** are evaluated. The answers of test persons prove that the *red octagon icon* is well designed (see both icons in appendix on figure 8.4). Nearly all test persons relates the icon to the highest risk level. The high variant results for the yellow triangle as low risk level show, that not all users understand the meaning of the icon, so its design has to be improved. Test persons understand the combination of acoustical signal and vibration for a different risk level. Because the focus lay on evaluation of warning variant with instructions, only the multimedia combination of visual (warning icon) and acoustical design (alert signal) was realised in this test case. So the full warning design as combination of visual, acoustic and haptic information has to be implemented and evaluated in future tests. To get more concrete results a separate testing of warning design variants is needed in the future.

### **H3: Evaluation group members will be more likely to rate comprehension of warnings higher than the control group.**

This hypothesis is *not* statistically supported by the analysis. In the 'comprehension' category CG members achieved better results than EG members. There were no extreme values in the results of both groups to skip (see section 2.7) therefore no mean values to correct. The difference between both test groups is supported by a 'middle' Cohen's effect size ( $d=0.756$ ). Additionally, there are other interesting results according to warning **comprehension** (EQ4) are found. Tables 8.4, 8.5, and 8.6 in the appendix show the comprehension ratings for all warnings of both test groups.

As already mentioned in the descriptive analysis (section 6.1.1) some warnings are better rated regarding their 'comprehension' (see figure 6.7). Both groups rated warnings number 9 ('unauthorised sending of pictures to the Internet') and 10 ('unauthorised sending of audio signals to the Internet') as 'very comprehensible' (WM9: EG 73%, CG: 92%; WM10: EG 73%, CG 83%). One reason may be that test persons' understand, that sending of personal pictures and audio signals threaten their privacy directly. But also the design decision for both warnings may had impacted the rating. These warnings were designed with risk level 3 (very high risk), which foregrounded these warnings with a permanent audio alert in comparison to risk level 2 warnings, which only use a single alert.

Interestingly, more CG members than EG members also rated all other warnings as 'very comprehensible' (figure 6.7). These results of the descriptive analysis are surprising because the think aloud protocols and observations show, that most control group members are not able to find an adequate solution without additional help. This could be indicate that the presentation of risk and personal consequences in all warnings were well designed for CG members. Maybe the instructions for EG members presented after the risk and consequences information decrease warnings comprehension, which has to be researched in future experiments.

## Chapter 6. General Results and Discussion

The warnings in general include information about personal impacts of malware attacks. But in test case 1 only the comparison of warning with and without instructions are investigated. In future experiments state-of-the-art warnings have to be compared to the new warning approach to find indicators that personal risks seem to be a valuable warning approach according to the theory of De Keukelaere et al. and Kauer et al. [DKYT+09, KPV+12].

The interpretation of another result is difficult, because the conclusion is *contrary* to each other (figure 6.15). The test persons who counted specific warnings as 'very much comprehensible', said that the support of a technical expert is 'very helpful' ( $r = -0.478; p < 0.05$ ). These results were achieved for warning number 1 ('unauthorised manipulation of robot map'), 2 ('unauthorised login trial to robot'), 4 ('unknown software'), and 6 ('unknown communication from the Internet'). It could be interpreted that test persons are sensitised by the current warning for the current dangerous situation, but do not understand the complex interrelations. So they want help by a technical expert, who explained them the situation.

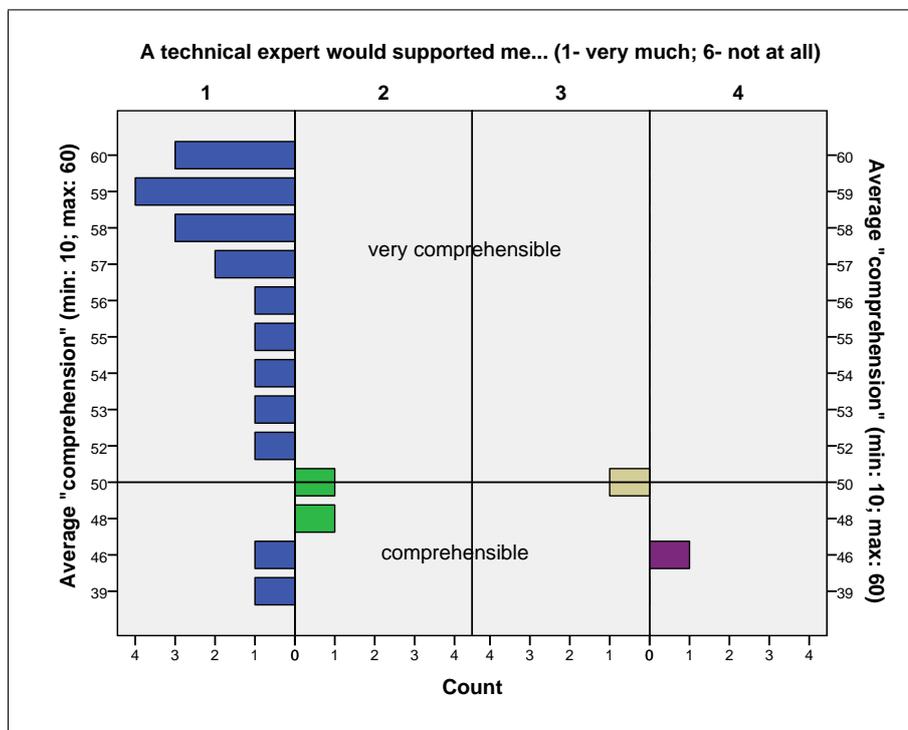


Figure 6.15: Test results: Correlation of average 'comprehension' and support by a technical expert

(Note: X-axis: amount of test persons, who equally rated support by a technical expert (grouped by colours);

Y-axis: averaged rating of 'comprehension' (EQ4) of all 10 warnings by one test person,

Average range: 10-19: not at all, 19-27: very little comprehensible,

27-35: little comprehensible, 35-43: some comprehensible,

43-51: comprehensible, 51-60: very comprehensible;

Axis parallel to x-axis: ratings of question 'How much do you were supported, when you would have had a technical expert':

1: very much, 2: much, 3: some, 4: little, 5: very little, 6: not at all)

**H4: Evaluation group members (EG) will be more likely to decide to heed the warning than the control group (CG).**

This hypothesis *is* statistically supported by the analysis. In the 'decision influence' category EG members achieved in average identical results to CG members (53 points). After skip of a single extreme value in the CG results (see section 2.7) the mean value of CG was 21 points. So the analysis regarding Cohen's effect size resulted in a 'strong' effect size ( $d=8.084$ ), which supported the hypothesis. Additionally, there are other interesting results according to the **decision** category (Q43\_WMNo\_03).

As figure 6.16 shows a correlation result between *decision influence and risk level of warnings* ( $r = 0.435; p < 0.05$ ). That means, the higher the test persons rated the danger, described in the warning, the rather they are compliant to decide after the warning recommendation. This seem to be an valuable approach for warning design in combination with user-group specific information. One challenge in warning design is to hold test persons by their high ratings and prevent habituation effects. One approach is the usage of so called 'polymorphic warnings', which change their appearance and reduce habituation effects in the brain [AKJ+15].

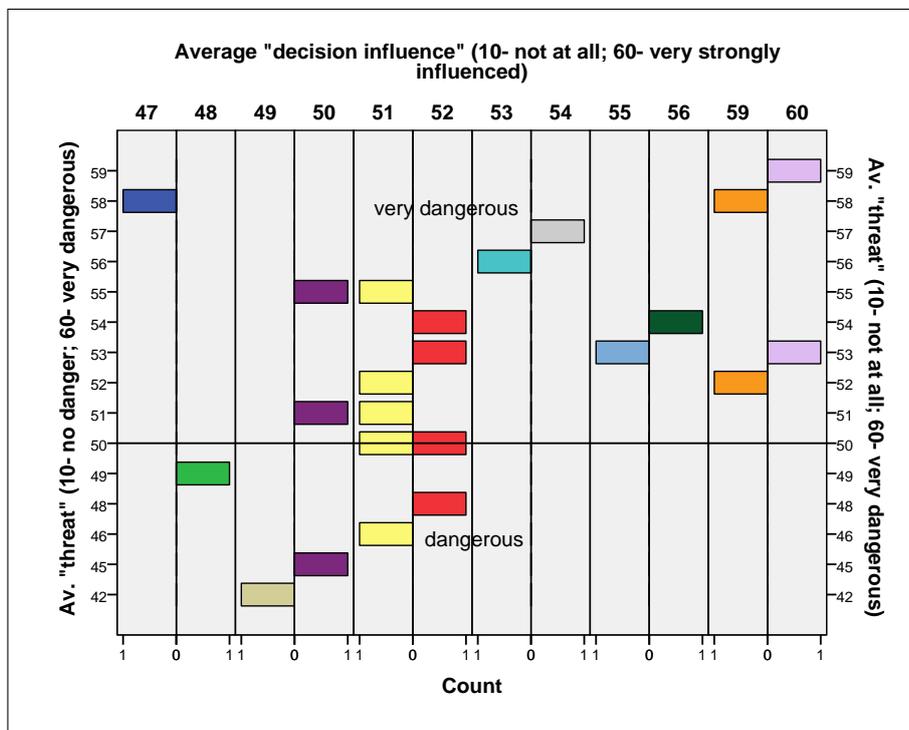


Figure 6.16: Test results: Correlation of average 'decision' and average 'risk level'  
 (Note: X-axis: amount of test persons, who equally rated decision influence (grouped by colours);  
 Y-axis: average of all 10 warnings by one test person to question 'danger' (Q43\_WMNo\_01),  
 Average range: 10-19: not at all, 19-27: very little dangerous, 27-35: little dangerous,  
 35-43: some dangerous, 43-51: dangerous, 51-60: very dangerous;  
 Axis parallel to x-axis: averaged 'decision influence' (Q43\_WMNo\_03)  
 rating of all 10 warnings by one test person,  
 Average range: 10-19: not at all, 19-27: very little influenced, 27-35: little influenced,  
 35-43: some influenced, 43-51: strongly influenced, 51-60: very strongly influenced

## Chapter 6. General Results and Discussion

As already mentioned in this section in 'Touch of users' emotions (Q33,Q34)', the study show, that warnings which touch users could influence their decisions. As figure 6.17 shows, for some warnings a correlation between users' *decision influence and concerning by warnings* is found ( $r = -0.435; p < 0.05$ ). The test persons who said that their decisions were '(very) strongly influenced by specific warnings were (very) (strongly) concerned by these warnings. These results were achieved for warning number 4 ('unknown software'), 5 ('unusual software activity'), and 6 ('unknown communication from the Internet'). That could be an indicator that users who are touched by warnings could benefit from clear warning information. The touch of users emotions seem to be an valuable approach for warning design.

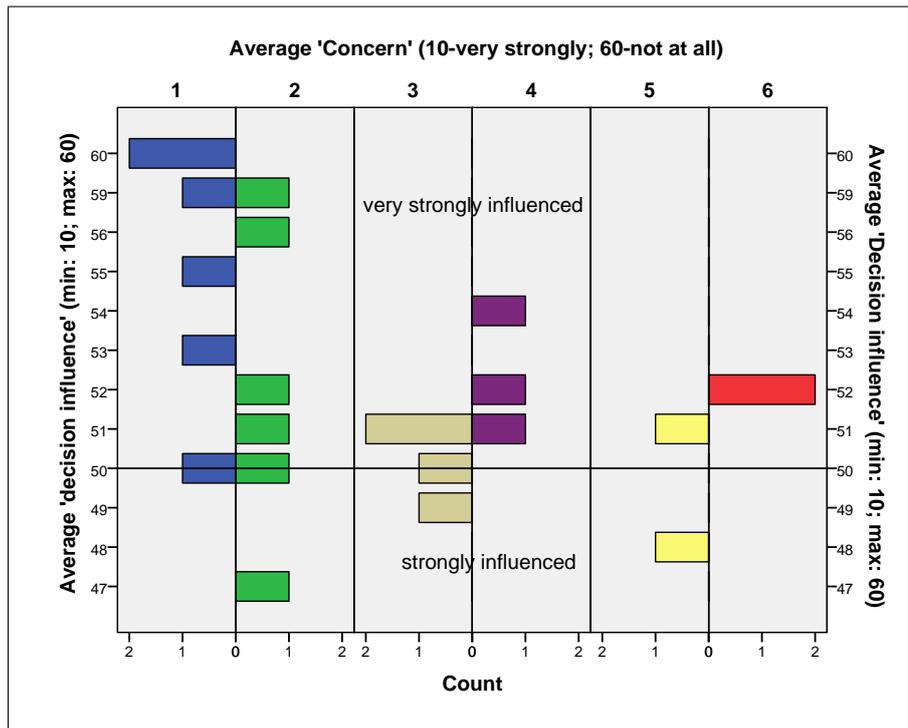


Figure 6.17: Test results: Correlation of average 'decision' and 'concern' (Q34)

(Note: X-axis: amount of test persons, who equally rated decision influence (grouped by colours);

Y-axis: average of all 10 warnings by one test person to question 'concern' (Q34),

Average range: 10-19: very strongly, 19-27: strongly, 27-35:some, 35-43:little, 43-51:very little, 51-60:not at all;

Axis parallel to x-axis: averaged 'decision influence' (Q43.WMNo.03) rating of all 10 warnings by one test person,

Average range: 10-19: not at all, 19-27: very little influenced, 27-35:little influenced, 35-43:some influenced, 43-51:strongly influenced, 51-60:very strongly influenced

The interpretation of another result is difficult, because the conclusion is *contrary* to each other (figure 6.18). The test persons who said the warnings influenced their *decision* intensively, said that the *support of a technical expert* is 'very helpful' ( $r = 0.414; p < 0.05$ ). Test users seem to understand that it is important to decide what the warning recommended, but to understand the complex relations they wish a technical expert. Future tests have to evaluate this correlation in more detail.

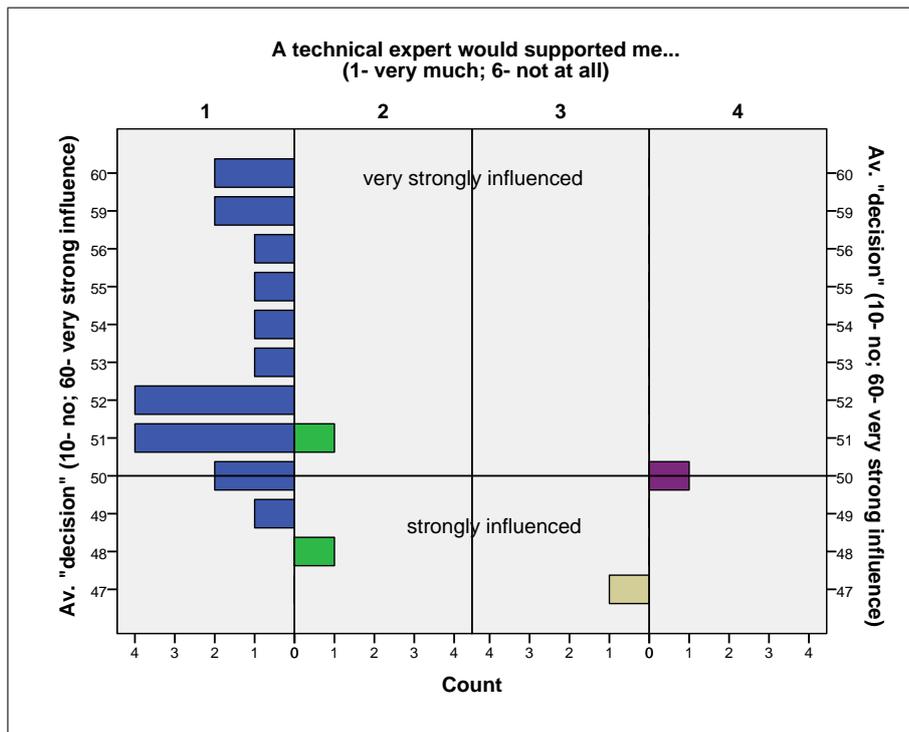


Figure 6.18: Test results: Correlation of average 'decision' and support by a technical expert

(Note: X-axis: amount of test persons, who equally rated support by a technical expert (grouped by colours);

Y-axis: averaged rating of 'decision' of all 10 warnings by one test person, Average range: 10-19:not at all, 19-27:very little comprehensible,

27-35:little comprehensible, 35-43:some comprehensible, 43-51:comprehensible, 51-60:very comprehensible;

Axis parallel to x-axis: ratings of question 'How much do you were supported, when you would have had a technical expert':

1:very much, 2:much, 3:some, 4:little, 5:very little, 6:not at all)

### Action influence (only EG):

Evaluation group members had one more question than CG members, because they had instructions in warnings. In question Q43.WMNo\_04 they were asked how their action was influenced by the warning instructions. As already mentioned in the descriptive analysis section EG members achieved in average 52 points, which means that EG members' actions were in average 'very strongly' influenced by the warnings. The inference statistical analysis found a correlation between decision and action for all warning messages except warning 8 ('unauthorised communication with the Internet') (see correlation values in table 8.7 in the appendix). That means that users decisions and reactions according to the warning are associated. This could be an indicator for well designed warnings, but it could have other reasons, too. When users interact with warnings they take short-time decisions (decide to heed/ignore the warning) and react shortly after, because the warning interrupt users' primary task. The correlation of users' decisions and actions seem to be a common relation in user-warning-interaction. Why decisions and actions do not correlate for warning 8 is speculative.

**Future of Internet of Things (EQ5):**

Regarding the question category EQ5 another interesting correlation is found ( $r = 0.564; p < 0.01$ ). Figure 6.19 shows that 6 of the 10 victims of a malware attack ('Previous experiences' EQ1) will be buy an IoT device in the near future. This result indicates, that the experience to be a victim of a malware attack seem users not to be afraid to buy an IoT device. Furthermore, they do not understand, that IoT devices are often cheap produced technical components, where security features are not implemented [RZL13] and graphical user interfaces for human-device-communication are not realised. These devices are valuable targets and simple to attack systems for cyber-criminals and their tools, such as malware. Most participants mentioned in the 'knowledge' category (EQ2) to knew about the existence of malware for mobile devices, networked robots, and other IoT devices, but they are not well sensitised for potential cyber-attacks against such devices. So in the future, users have to be more sensitised to these aspects.

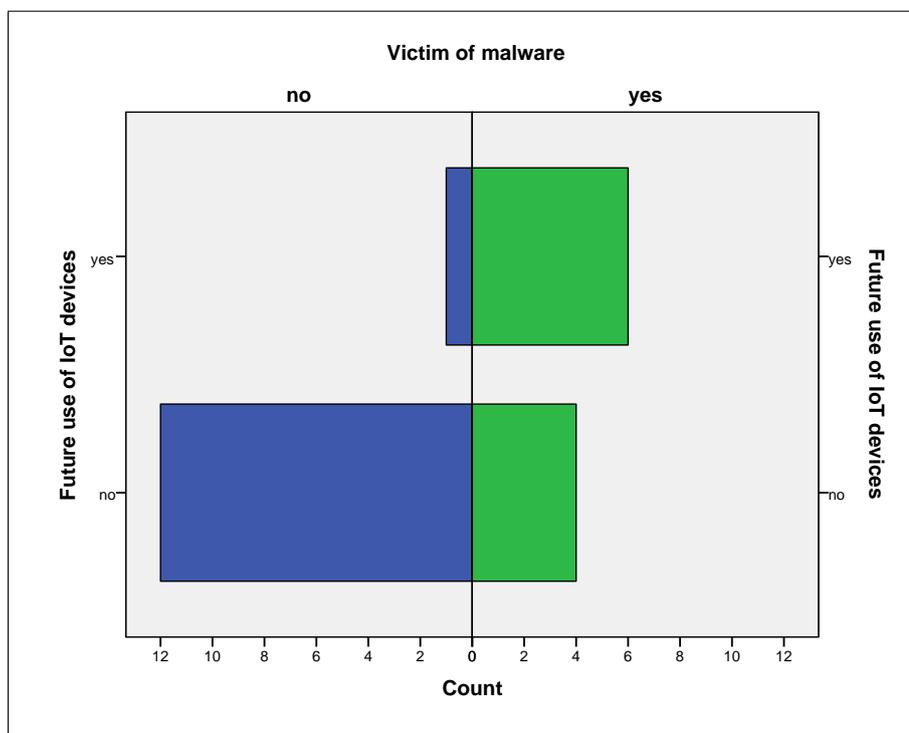


Figure 6.19: Test results: Correlation of 'victim of malware' and 'buy an IoT device in the near future'  
 (Note: X-axis: amount of test persons, who were a malware victim or not (grouped by colours);  
 Y-axis: rating of Q53 by one test person  
 'Do you plan in the near future to purchase such intelligent or smart devices?',  
 Axis parallel to x-axis: groups of malware victims and non victims)

### Knowledge (EQ2):

Nearly all members of EG and CG hold that cyber-criminals are very strongly involved in distributing malware. The opinions differ for the group 'user'. Only 45% of EG, but 83% CG think that users are responsible for malware distribution (figure 6.1). The belief of CG seem to be quite high, but correlate with the annual report of the BSI to information security in Germany 2016 [BSI17]. The report informed, that most malware is installed with help of users although malware (such as worms) exist, which need no user interaction for installation.

Most users of both test groups have an adequate awareness for specific user activities which are responsible to distribute malware (figure 6.2). So nearly all test users specified 'download of files' and 'open email attachments', which correlate with the BSI annual report 2016 [BSI17]. Participants underestimated user actions such as 'surf the Internet', where malware could get on users systems by so called Drive-by-Downloads, and 'click on links in social media' and 'forwarding in social media'. Here users need more education to raise their awareness to cyber-threats in the Internet.

### 6.1.3 Quality criteria and Limitations

---

The quality of the user studies validate how good, reliable, and reproducible the studies are. In the following the main quality criteria after Preim and Dachsel [PD15] and Krol et al. [KSPS16] and limitations for the user test are described.

The *plausibility* is reached by a clear definition of target groups and selection of test participants. It is payed attention to choose test persons, which are similar to real users, for example by avoidance of explicitly choosing technophiles.

The *internal validity* is minimised by following factors. Because of the *small amount of test persons* per group (11 and 12 persons) these results show only tendencies, which have to further investigated in future studies with larger test groups. Furthermore, most participants were *students* with an average of age 29 years. So these results could not be generalised for a hole population. During the user study a *static display order* of warning was used. The idea was to couple the display of warnings to specific tasks with the robot to make the warning plausible to the participants. To prevent side effects of habituation or transfer effects (e.g. similar rating of different designed warnings) a dynamic display order is recommended. Although priming of participants is avoided, due to limited resources (time and personal) all warning variants are tested in one single study. That means, all participants are confronted with all designed warnings (10 warnings). So participants will noticed, that the study has something to do with security warnings. In test case 1 only two warning variations (with and without instructions) and no other warning variations are tested (e.g. different texts, background colours, text and icon combinations). So the warning design could only evaluated in general, but no specific conclusions could be arrived from the influence of specific warning design elements to warning effectiveness. This has to be evaluated in future studies.

The *external validity or portability* of the test results for both test cases could not be guaranteed because of the small sample size of 23 participants. In the future, these test results have to be approved with larger test groups. Another limitation is the usage of laboratory equipment instead of equipment of participants. So participants were not confronted with real threats. The *reliability* of test results for larger amount of test persons and longer test durations have to be evaluated in the future.

### 6.2 Children - Smartphone warnings

---

The following section illustrates and discuss the results for warnings designed for primary-school children on a smartphone. This work based on the bachelor thesis of Wiebke Menzel [Men11] and a collective publication [MTF<sup>+</sup>12]. The warning messages should warn the primary-school children for malware attacks against their personal smartphones and personal threats regarding their privacy. The user test is realised with one test group to evaluate the advantage of the new warning design described in general in section 4.3.6 and test case specific in section 5.2.1. Table 4.12 in chapter 4 summarises the evaluation environment and methods for the regarding test case.

Six evaluation questions (EQ) are investigated within the user study (table 4.12): *comprehension of warnings* (EQ1), user-adequate *design* of warnings (EQ2), *influence of time and order of showing warnings to reaction* (EQ3), *previous experiences* (EQ4), knowledge (EQ5), and socio-demographics (EQ6). All evaluation questions are measured with the questionnaire, except question EQ1 and EQ3, which uses additionally information from logfiles and written protocols.

In the following the section is structured in three parts. At first, the *descriptive analysis* summarises the results of the evaluation via tables, statistical values and diagrams [BS10]. The second part, discusses the results of the *interference statistical analysis*. It is used to verify the hypothesis (second part of table 4.8) with the observations in reality [BS10]. The third part in section 6.2.3 discusses the *quality criteria and limitations* of the study.

#### 6.2.1 Descriptive analysis

---

In this section the frequency of test results for the four research questions are presented. In general, the children rated the stressfulness in average of the test on a scale from 1 ('very stressful') till 5 ('stressless') with 4,3 (Q1), which indicates that the test was not stressful.

**Socio-demographic characteristics (EQ6):** Overall, 13 pupil, 8 boys and 5 girls participated the test (Q37). They were 8 to 9 years old (Q36), and native German speakers (Q38). All these children were familiar with desktop IT systems, because their school lessons are supported with tablet PCs and a digital whiteboard.

**Previous experiences (EQ4):** 8 of 13 children said to possess and use an own mobile phone (e.g. Nokia, Sony, LG), 4 of 13 had an own PC and 1 an own laptop, 4 had no own devices (Q39/Q39.1). Most of them (12 of 13) used also their parents' computers, laptops or mobile phones (e.g. Blackberry, iPhone, Samsung) (Q40/Q40.1). Only some children said to be a victim of computer viruses (2 of 13, Q12.1) or a victim of mobile device viruses (1 of 13, Q13.1).

**Knowledge (EQ5):** 8 of 13 know that there exist computer viruses (Q12) and 7 of 13 know about the existence of mobile device viruses (Q13). Nearly all (12 of 13) know that warnings show that childrens' mobile phone is in danger (Q14).

**Comprehension of Warnings (EQ1):** The warning comprehension is measured with *observations*, a post-test *questionnaire*, and *logging* of users' click events. Adequate and inadequate *reactions* to warnings are captured within a protocol and the logfile. *Warning interpretation* is measured with a questionnaire, and the 'Why?' button usage is captured within the logfile.

### *Reaction of participants (Observations):*

The adequate and inadequate reaction to the warnings are interpreted as warning comprehension or incomprehension (see last columns of table 5.5). Figure 6.20 shows the adequate (green blocks) and inadequate reactions (red blocks) of all warnings according to the observations. The reactions could only be differentiated for warnings 1 to 4 ('update with virus', 'update without virus', 'Bluetooth attack', 'virus infected file'). According to the protocol for warnings 5 and 6 ('virus on phone', 'virus infected app') the reactions of the participants could not be reconstructed. Only the method of thinking aloud is used, but only some participants verbalise their thoughts loudly, which were not clearly in every case. Therefore, some values for reactions and thinking aloud for warning 5 and 6 are missing (blue values in figure 6.20).

**Warning 1:** the check of an update resulted in a recommendation of risk-less update installation. Most test persons (12 of 13) react adequately by update install in the first trial. One child did not install the update in the second trial.

**Warning 2:** the check of an update resulted in a recommendation of no update installation. As figure 6.20 shows that 10 times warning 2 was displayed participants react adequately by no update install and 9 participants with inadequate reaction of update install. 2 children react at first adequately and had then tried to install the update two times although the warning was displayed.

**Warning 3:** warns about an attack over Bluetooth. Most children (12 of 13) react adequately by deactivating Bluetooth.

**Warning 4:** warns about a virus infected file, which is sent to the smartphone. Most children (12 of 13) react adequately by blocking the infected file.

**Warning 5:** warns about a virus on the smartphone. Warning 5 was displayed 23 times. 6 times children react adequately by switch off the phone and hand out the phone to their parents, and 2 times children react inadequately. 13 values are missing because of small usage of the method of thinking aloud.

**Warning 6:** warns about a virus infected app. 4 children react adequately by switch off the phone and hand out the phone to their parents, and no child react inadequately. 9 values were missed because of the small usage of the method of thinking aloud.

### *Warning interpretation (Questionnaire):*

The reaction to warnings are aligned with the answers of every child in the questionnaire (Q6-11, 'Why this warning was displayed? What does it mean?'). The answers were freely verbalised by the children, which are interpreted by two independent experts and categorised in 'comprehended' or 'not comprehended'. Some answers were excluded from the analysis, those which were ambivalent and those which were interpreted by both experts differently. Figure 6.21 shows the results of the questionnaire regarding the warning comprehension. Most children understood warnings 1 ('update with virus'), 2 ('update without virus') and 4 ('virus infected file'). Nevertheless, warning 3 ('Bluetooth attack'), 4 ('virus on phone') and 6 ('virus infected app') were only comprehended by a minor amount of children.

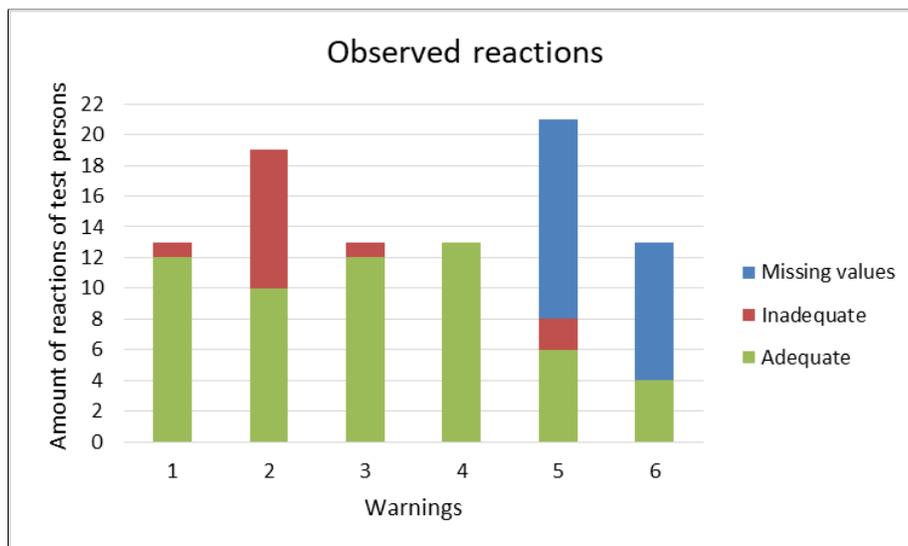


Figure 6.20: Test results: Reactions according to observations

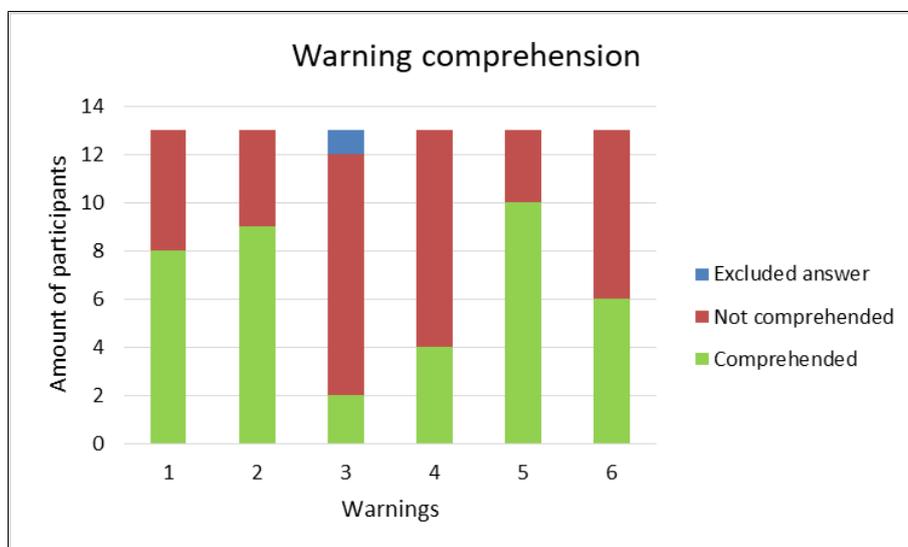


Figure 6.21: Test results: Warning comprehension

**'Why?' button usage (Logfile):**

The frequency of usage of the 'Why?' button could be an indicator, whether warnings were read and comprehended. A little usage of the 'Why?' button could indicate warnings are well designed or warnings are ignored by the test persons. Figure 6.22 shows a different frequency of use of the 'Why?' button per warning. Conspicuous is the small 'Why?' button use for warnings 1 (one time) and 6 (never). In all other warnings the 'Why?' button is clicked by the children between 4 and 7 times.

Most children could correctly identify the **meanings of the four colours** of the cartoon character (Q5), which symbolise a specific risk level. Figure 6.23 shows that all children identified correctly the risk level of the red colour, whereas the correct identification for other colours are different - white (9 of 13), green (8 of 13), yellow (9 of 13).

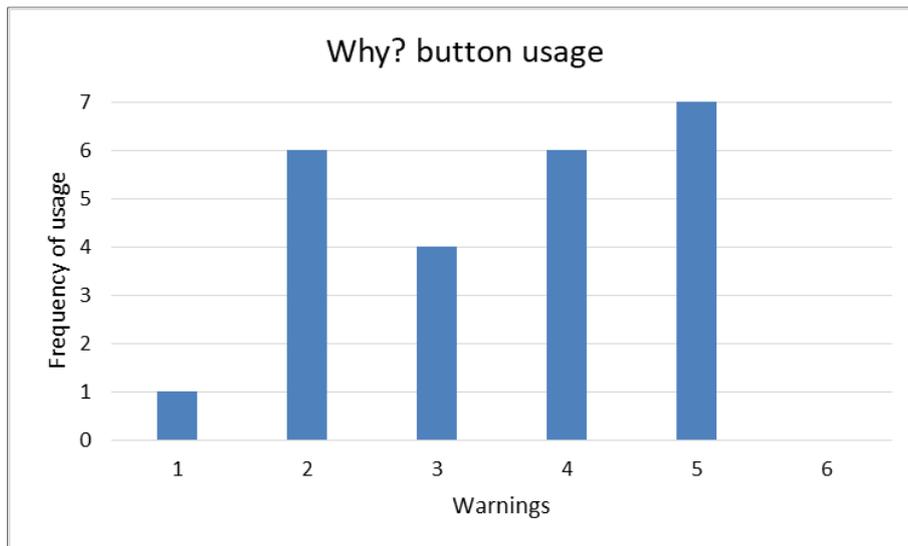


Figure 6.22: Test results: Frequency of 'Why?' button use per warning

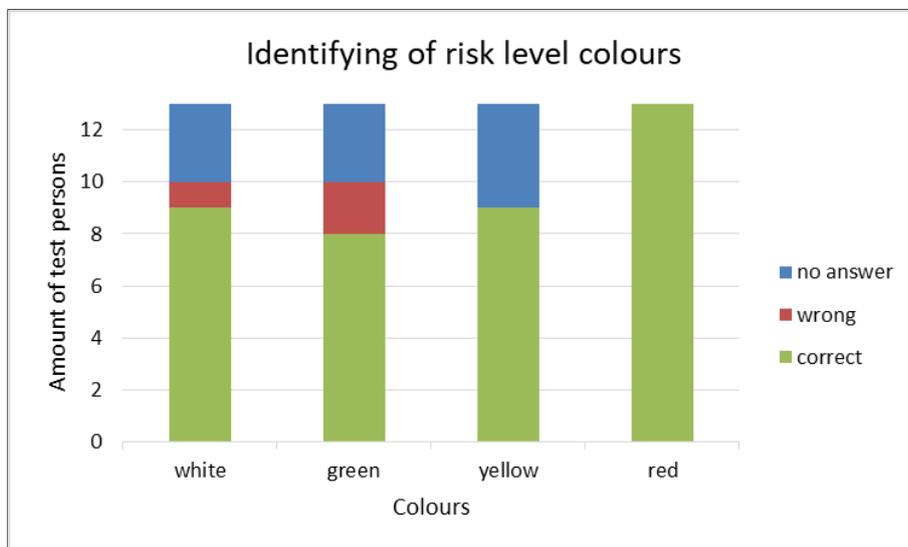


Figure 6.23: Test results: Identification of risk levels by colours

### Warning design (EQ2):

The warning design was evaluated with the questionnaire. Most children (9 of 13) rated the *warning* (Q32) and the *comic character* (Q31) on a scale from 1 (excellent) to 6 (insufficient) with excellent. 4 children rated the cartoon character with 'good', 3 the warnings with 'good' and 1 child the warnings as 'sufficient'. Most children (12 of 13) had the opinion that the frightened mimic of the cartoon character (Q21) was well chosen to symbolise the danger. 1 child rated with 'nor'. Most children (12 of 13) answered with 'yes' to both questions (Q19/Q20) in cases their phone is in danger - they would switch off their phone or give it to their parents. Furthermore, both icons 'green arrow' (Q22/23) and 'blue lamp' (Q24/25) are mostly rated with 'good'. Instead of one child, which did not recognise this icon nearly all children (12 of 13) understand why the 'green arrow' was shown and all rated it with 'good'. The ratings for the 'blue lamp' differ. 10 of 13 children understand why the 'blue lamp' was shown, 3 children did not understand it. Most children (10 of 13) rated the 'blue lamp' with 'good' and 3 children with 'neutral'.

## Chapter 6. General Results and Discussion

The cartoon character was **colored** differently to symbolise different **risk levels** (Q2/Q2.1). All children remembered this aspect, but as figure 6.24 shows the children remembered different colours. Interestingly, all children remembered the colour *red*, but only 5 (38%) remembered the colour *yellow*. Also circa only half of the children (46%) remembered the colour *green*, which was used as risk level 0. 11 children (85%) remembered the *white* character and 4 children (31%) the *blue* character. Furthermore, the ratings of the cartoon character also differ (Q15-Q18.1). Most children rated the colours with 'good' or 'neutral'. The *green* colour was rated by 11 children (85%) with 'good' and 2 children with 'neutral'. The *yellow* colour was rated by 8 children (62%) with 'neutral', 4 children (31%) with 'good' and 1 child with 'bad'. Instead of yellow 5 children (38%) had better chosen the colour red. The *red* colour was rated by 10 children (77%) with 'good', 2 children with 'neutral', and 1 child did not understand the difference between red and yellow. The *white* colour was rated by 10 children (77%) with 'good' and 3 children with 'neutral'. Instead of white 2 children had better chosen the colour orange, 1 child yellow, and 1 child light-blue.

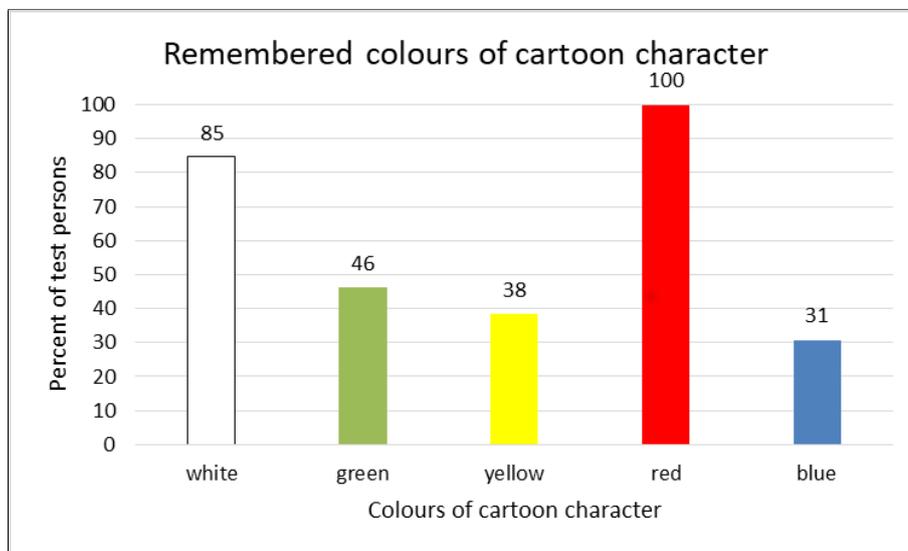


Figure 6.24: Test results: Remembered colours of cartoon character

Most children (10 of 13) said they read the **text** and 3 said they read the text partly (Q26). Most children (9 of 13) said only to understand the text partly, and only 4 mentioned they understand the text (Q27). All children rated the font size (Q28) and most children (11 of 13) the **text** length (Q29) as suitable. Most children (7 of 13) rated the used words as 'easy', 3 children with 'very easy', and 3 children with 'difficult' (Q30). Nevertheless, some had in the test comprehension problems with English terms, like 'update' or 'Bluetooth'.

In general, most children (10 of 13) rated the warning messages (Q33) with 'totally right', 'helpful' (10 of 13), 'funny' (9 of 13), and 'sweet nor nerved' (8 of 13). Only a small group of children rated the warnings with 'too colourful' (3 of 13), 'annoying' (1 of 13), 'helpful nor annoying' (3 of 13), 'funny nor babyish' (4 of 13), 'nerved' (1 of 13) and 'sweet' (4 of 13).

The children also are asked for **own ideas for improvement** (Q34) and circa half of the children (6 of 13) gave comments. They recommended to warn immediately for the danger, do not use heavy words (e.g. usage of term 'danger' instead of 'virus', usage of 'attention'), and use a smiley with colours green, yellow, orange and dark red. Some children (5 of 13) created a **name** for the cartoon character (Q35): 'Dirigent' (engl. conductor), 'Klaro', 'Alien', 'Schleimi', and 'Monsttis'.

The participants recognised the **acoustical signal and vibration** different (Q3 and Q4). Most children (9 of 13) said that they heard 'always' the alarm signal, only 3 'sometimes' and only 1 'never'. In comparison to the acoustical signal only 4 children recognised 'always', 5 'sometimes' and 4 'never' the vibration. Most children rated the **acoustical signal and vibration** in the warning messages on a 3-level smiley scale with 'good' or 'neutral' (Q3.1 and Q4.1). The alert signal was rated by 8 participants with 'neutral' and 3 children with 'good'. The vibration was rated worse than the alert signal. 4 children rated the vibration with 'good' and 4 children with 'neutral'. However, some children were frightened by the vibration during the test, which was observed by a little wince of childrens' body.

**Influence of time and order of showing warnings to reaction (EQ3):**

The reading of a warning was estimated with two measures: first, logging of the time span how long the warning was open, and second, the written protocol, where a assumption over the reading was notated. With these both values an approximated time value is estimated, which indicates a reading or ignoring of a warning. Therefore, the classification 'read of a warning' is an approximation. In the following, the influence on reading behaviour of participants by the timely order of warning display is investigated. The time of the test is separated into time slots, where slot 1 symbolises the test begin and slot 9 the test termination. Altogether, minimum 6 warnings and maximum 9 warnings were displayed. In which the amount of displayed warnings is depending on the repeated display of warning 1, warning 2 and the inadequate reactions of participants, which trigger the display of warnings. Slot 9 was only reached once, therefore it is less meaningful in comparison to the other slots. As figure 6.25 shows the longer the test takes, the more decreases the time for reading the warning.

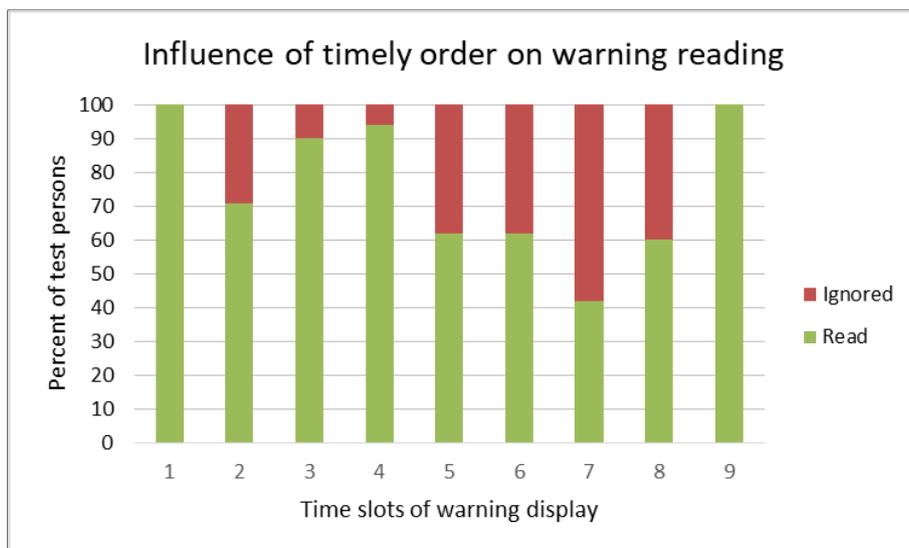


Figure 6.25: Test results: Influence of timely order on warning reading

As figure 6.26 shows that also the use of the 'Why?' button also decreased during the test.

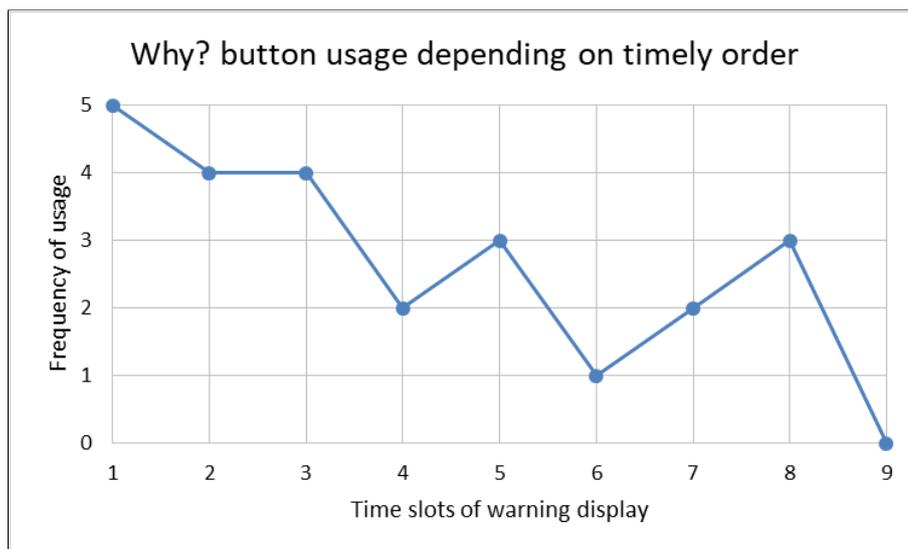


Figure 6.26: Test results: Frequency of 'Why?' button use depending on timely order of warning display

### 6.2.2 Interference statistical analysis and discussion

---

It was realised by using SPSS (version 16). The one-sided correlation according to Pearson is used to analyse the significance of the test results. Following study results are analysed with Pearson's one-sided correlation: *estimation of warning reading* (protocol and logfile), *usage of the 'Why?' button* (logfile), *adequate and inadequate reaction* (protocol and logfile), and *interpretation of warnings by children* (questionnaire). In respect to the small sample size group (13 participants) those results represent the strongest effects, more effects are expected in empirical studies with increased sample sizes. The correlation results are discussed in the following according to the two hypothesis introduced in section 4.4.1 (see second part of table 4.8). These results are complemented by the results for the six evaluation questions (EQ).

#### **H1: Children who use the 'Why?' button will be more likely to react adequately according to the warning instructions.**

This hypothesis *is* supported by the interference statistical analysis, but only for warning 2 ('malware infected update'). Warning 2 showed a significant correlation between the usage of the 'why?' button and the *reaction* to the security threat ( $r = 0.675; p < 0.01$ ). The correlation represents a strong effect with a probability of 1% for a random result. Warning 2 warned after a check against an installation of an update. In 10 cases (53%) warning 2 was displayed the participants react adequately (no update installation) and in 9 cases inadequately by installing the update (47%). Most of the children, who used the 'Why?' button (4 of 5) also react adequately, and most who did not use it react inadequately (7 of 8). This indicates that the usage of the 'Why?' button triggers an adequate reaction to children. Nevertheless, this is only a single result for one warning for a small sample test group and therefore this result could not be generalised for the user-group primary-school children.

**H2: Children who read background information ('Why?' view) will be more likely to react adequately relating to the warning instructions.**

This hypothesis *is* supported by the interference statistical analysis, but only for warning 3 ('Bluetooth attack'). Warning 3 showed a significant correlation between *reading* the warning and the *reaction* to the security threat ( $r = 0.527; p < 0.03$ ). All children (10 of 13), who read the warning react adequately, too. This is an indicator that reading background information could trigger the right reaction of children. Nevertheless, this is only a single result for one warning for a small sample test group and therefore this result could not be generalised for the primary-school children in general.

**Comprehension of Warnings (EQ1):**

The warning comprehension is composite of three parameters: first, adequate and inadequate *reaction* to the warning (protocol and logfile), second, childrens' warning *interpretation* (questionnaire), and third, the '*Why?*' *button usage* (logfile). Table 6.1 illustrates the results of the three parameters to find indicators for warning comprehension.

The results of **warning 1** ('update with virus') indicate, that this warning is comprehensible designed for the target user-group. The correlation of  $r = -0.365; p < 0.11$  represents a middle effect with a probability of 11% for a random result. So the small usage of the 'Why?' button (once) and adequate warning interpretation by most participants (8 of 13 comprehended) supports the theory that warning 1 is well designed.

Warning number	Adequate reaction per trail	Interpretation	Frequency of 'Why?' button use	Correlation
1	12 of 13 (92%)	8 of 13 comprehended (62%)	1	$r = -0.365; p < 0.11$ (Interpretation and 'Why?' button usage)
2	10 of 19 (53%)	9 of 13 comprehended (69%)	6 (includes one double usage)	$r = 0.675; p < 0.01$ (Reaction and 'Why?' button usage)
3	12 of 13 (92%)	10 of 12 (1*) not comprehended (83%)	4	$r = 0.527; p < 0.03$ (Reaction and warning read)
4	13 of 13 (100%)	4 of 13 comprehended (31%)	6	-
5	6 of 23 [13] (35%)	10 of 13 comprehended (77%)	7 (includes two double usages)	-
6	4 of 13 [9] (31%)	6 of 13 comprehended (46%)	0	-

Table 6.1: Warning comprehension results according to three parameters (Reaction, interpretation, 'Why?' button usage) and Correlation results after Pearson (Note: \*: excluded result; -: no result; [x]: lack of x values)

Conspicuous is the *discrepancy between the warning interpretation and reaction to warnings*. One example is **warning 2** for installation of an infected update. Most of the children (9 of 13) interpreted the warning 2 correctly, but half of the children react inadequate, they installed the infected update. The right interpretation and wrong reaction to warning 2 could be reasoned by less comprehension of the warning message and other parameters. Potentially causes of inadequate reactions of test persons could be the uncertainty of children, the request character of the update warning and a less awareness to the security of their smartphones.

Other examples with a discrepancy between the warning interpretation and reaction to warnings are **warning 3** for a Bluetooth attack (adequate reaction is deactivating of Bluetooth) and **warning 4** of sending an infected file to the smartphone (adequate reaction is the blocking of this file). Most of the children (Bluetooth warning: 92%, Infected file warning: 100%) react adequate. However the interpretation of the questionnaire and protocols of method of thinking aloud resulted that most children do not understand warnings 3 and 4. The children react intuitively right or on basis of the instruction information in the warning though they misinterpreted the sense of the warnings. In the future the design of these warnings has to be improved to increase the warning comprehension of children.

The comprehension of **warning 5** ('virus on phone') could not clearly estimated, because of the absent of the results (13 data sets) for the test persons' reactions. However the answers in the questionnaire indicate, that children comprehended the underlying meaning of warning 5. The 7 usages of the 'Why' button could indicate, that the children used additional information to increase their comprehension.

For **warning 6** ('virus infected app') half of the children interpreted the warning correctly or had an idea of the warning importance. Conspicuous is that the 'Why?' button is not used for warning 6. The analysis of the answers in the questionnaire indicate that the results of warning 6 are influenced by other factors, such as test time (slot) and display order of the warning (see discussion to EQ3).

### **Warning design (EQ2):**

In general the results of the questionnaire showed that the children rated the warnings and the comic character as adequately designed. Although, most children remembered only the red coloured cartoon character the children *remembered the first meaning of a warning in combination with the colour of character*. This result could be used in further warning realisations, so different characters could be used for different warning messages with different risk levels.

The questionnaire show that most children rated the *text, font size and text length* as suitable. Nevertheless, foreign and technical terms should be avoided, such as 'update' or 'Bluetooth', and terms, such as 'danger' and 'attention' should be preferred. An idea for improvement could be the personalisation of the character by giving it a name. Future studies could evaluate whether children react differently to warnings if they build a personal bound to the warning guide. Children recognised the usage of the *acoustical signals and vibrations* differently. The alarm signal was rated better than the vibration. Some children were frightened by the vibration. Future tests should evaluate how the previous experiences of children with smartphones influence children's positive and negative reactions to multimodal warnings.

**Influence of time and order of showing warnings to reaction (EQ3):**

The analysis of the log files of the warning display time span and the written observation protocol showed a decreasing reading time during the test. This is an indication for habituation effects, which are normal reactions, when the human brain is confronted with similar stimuli, such as warnings [AVK<sup>+</sup>14]. Also the usage of the 'Why?' button decreased during the test. *Habituation effects* could also be the reason for the lack of usage of warning 6 (see figure 6.26), but also a systematic design error. The warnings should be displayed in a randomly order. The analysis of the display position uncovers that warning 6 was always displayed after warning 5 (excluded of warning 2b, 3b and 4b). Furthermore as figure 6.27 shows warning 6 was displayed in general at a later test phase. This error could have influenced the results for warning 6 and is considered in the analysis.

Another reason could be habituation effects, because warning 5 and 6 are similar designed (risk level 2). Probably most participants do not read warning 6 (10 of 13) in comparison to warning 5 (11 of 13 read). The frequently usage of the 'Why?' button in warning 5 (7 times) and lack usage in warning 6 could be also reasoned by habituation effects.

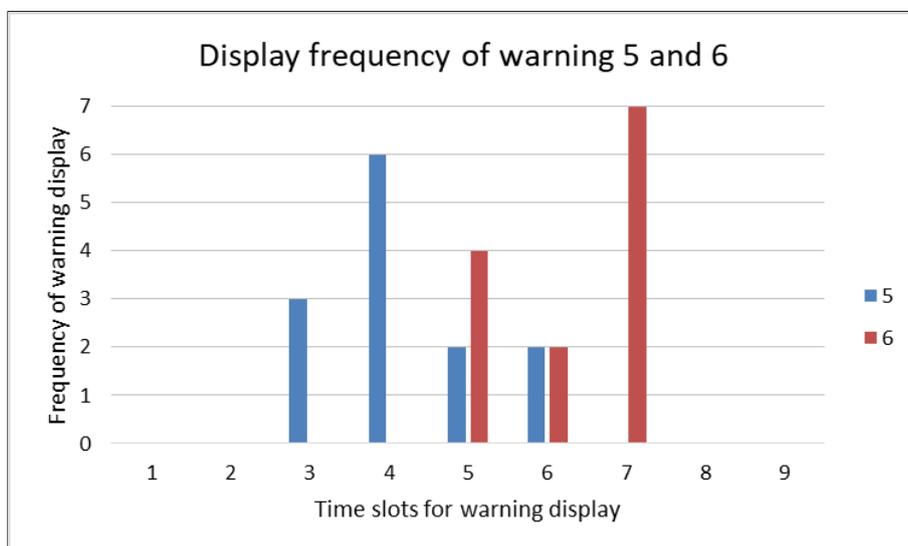


Figure 6.27: Test results: Frequency of display of warning 5 ('virus on phone') and 6 ('virus infected app') regarding the time slot

**Previous experiences (EQ4) and knowledge (EQ5):**

The most children answered to possess and use an own mobile device (8 of 13) or use their parents' computers, laptops or mobile phones (12 of 13). Only 2 children were a victim of computer viruses and 1 was a victim of mobile device virus. Nevertheless, half of the children answered in the questionnaire to know about the existence of computer viruses and mobile device viruses. The answers are surprising, because some warnings about viruses were not comprehended by the children. The answered could be reasoned by a priming effect, because in the test the warnings include the term 'virus'. This could be influenced the answer to this question. Furthermore, it is assumed that a so called 'Rosenthal effect' [BD06] occurred. That is a result in an investigator-test person relationship, where the test persons give social and situational desirable answers to the investigator. For example a child expressed that it find the warnings annoying, but the child did not indicate this in the questionnaire (Q33: 'How do you like the warning messages?'), although a checkbox with 'annoying' exist.

### 6.2.3 Quality criteria and Limitations

---

The quality of the user studies validate how good, reliable, and reproducible the studies are. In the following the main quality criteria after Preim and Dachsel [PD15] and Krol et al. [KSPS16] and limitations for the user test are described.

If target groups and selection of test participants are clear described a *plausibility*. It is paid attention to choose test persons, which are similar to real users. So primary-school children were chosen aged between 8 to 9 years.

The *internal validity* is minimised by following factors: the *small sample size* of 13 participants, the focus on children between *8 and 9 years* and children who were *familiar with desktop IT systems* used during their school lessons. So the study results are not generalisable for the user-group primary-school children and show only tendencies. Future studies with a wide variety of participants and larger test groups have to show, whether the results are generalisable. The priming of participants is tried to avoid. That means, the participants in the test cases are not tell about the real aim of the user study to obtain internal validity. Due to limited resources (time and personal) all warning variants are tested in one single study. That means, all participants are confronted with all designed warnings (6 warnings). So participants will noticed, that the study has something to do with security warnings.

In the study only one warning variation and no other warning variations are tested (e.g. different texts, background colours, text and icon/cartoon character combinations). So the warning design could only be evaluated in general, but no specific conclusions could be arrived from the influence of specific warning design elements to warning effectiveness. This has to be evaluated in future studies.

The *external validity or portability* of the test results for both test cases could not be guaranteed because of the small sample size of 13 participants. In the future, these test results have to be approved with larger test groups. Another limitation is the usage of laboratory equipment (iPhone) instead of equipment of the children. So they are not confronted with real threats.

The *reliability* of test results for larger amount of test persons and longer test durations have to be evaluated in the future.

## 6.3 Discussion with HITL framework

The following section discusses the results of the above described evaluations of the both warning test cases. The HITL framework of Cranor [Cra08] the so called 'human-in-the-loop security framework', which is a basis to evaluate security applications, is used to compare both warning test cases and find indicators for improvements (section 2.4). Table 6.2 presents the results of the comparison.

Component	Mobile Robot Warnings for Adults	Smartphone Warnings for Children
<b>Task identification</b>	Security warnings from anti-malware applications rely on users, which have full system control (e.g. because of transparency issues, see section 1.1). They decide to follow warning instructions or ignore the warning to return to their primary task.	
<b>Task automation</b>	In this thesis warning scenarios are described, where the user has full control over the system. Some decisions could be automatised within the configuration of the anti-malware application, but caused by the full control approach users have to be involved during the configuration. One example is the blocking of unauthorised access to person-related data. Because users are control the system, they have to be informed or warned in cases their personal requirements are impacted (e.g. privacy, personal safety).	
<b>Failure identification</b>		
<i>Communication:</i>	Warning	Warning
<i>Communication Impediments:</i>		
Environmental Stimuli	Warnings from other apps relating to user's primary task and different environmental influences could impediment the communication of warnings.	
Interference	Warning messages of anti-virus applications could be prohibit by malware influences [Sri07, ACS10].	
<i>Personal Variables:</i>		
Demographics and personal characteristics	Participants consist of two groups of 11-12 people, were in average 29 years old, mostly woman and students, and all native German speakers. The test results indicate that younger test persons rated the warnings 'little useful' in comparison to elder participants.	Participants were 13 primary-school children, 8-9 years old, mostly boys, and all native German speakers.

## Chapter 6. General Results and Discussion

Component	Mobile Robot Warnings for Adults	Smartphone Warnings for Children
Knowledge and experience	Test persons had different knowledge and experiences of and with malware attacks. Most participants mentioned to know about malware for mobile devices, networked robots, and other IoT devices, but they are not well sensitised for potential cyber-attacks against such devices.	Test persons were all familiar with desktop IT systems, but less sensible to security threats of smartphones.
<i>Intentions:</i>		
Attitudes and beliefs	All participants pay attention to the warnings, but after the 10th warning within 30 minutes, warnings were often sensed as annoying.	All participants pay attention to the warnings, but some sensed warnings as very annoying.
Motivation	Some participants were not motivated to read the warning information carefully.	Reading time of warnings decreases during the test, because of habituation effects and focus on the main task (paint a picture).
<i>Capabilities:</i>	The test results indicate that the test group with instructions need less additional help than participants without instructions.	Additional information help children participants to solve malware problems. But not all tasks relating to security attack could be solved by children alone, because these are too complex for them, e.g. remove of malware. Additional help by (technical-savvy) peers and/or parents is useful.
<i>Communication Delivery:</i>		
Attention switch	Noticing of warning is not significant, because test persons were partly in conversation with the tester, while the next warning was just presented.	All warnings were noticed, but reading time of warnings decreases during the test. Children often focus their main task (paint a picture).
Attention maintenance	Participants, which was motivated also read warning texts carefully.	

### 6.3. Discussion with HITL framework

Component	Mobile Robot Warnings for Adults	Smartphone Warnings for Children
<i>Communication Processing:</i>		
Comprehension	The test results show, that the test group with warning instructions rated the warnings as less comprehensible than participants without instructions. The study also show, that comprehensible warnings are no substitution for additional help. The comprehension of some participants were in some cases negative influenced by warning information: 'I'm overloaded with this information!'.  Future: Training of applying of warnings in practice is needed.	Some warnings are misinterpreted, but children participants react to them intuitively in the right way. Some children remembered the first meaning of a security warning in combination with the colour of the cartoon character.
Knowledge acquisition	Future: Training of applying of warnings in practice is needed.	
<i>Application:</i>		
Knowledge retention and knowledge transfer	The knowledge is not applicable, because these are first warning prototypes.	
<i>Behaviour:</i>	Participants with instruction information are more likely to heed the warning than test persons without instructions. Furthermore, participants, who rated a higher risk level are more compliant to decide after the warning recommendation than other participants. Additionally, the study show that warnings with instructions could melt the fear of users of malware-related personal impacts, because they know what to do against it because they are instructed by the warnings. Users decisions and reactions according to the warning are associated. This indicates well-designed warnings or are common human-warning interaction schemes, where short-time decisions (decide to heed/ignore the warning) and reactions are taken.	The user study show for 3 of 6 warnings that reading background information and warning information supports the adequate reaction of users.

Component	Mobile Robot Warnings for Adults	Smartphone Warnings for Children
Failure mitigation	The user study uncovers no system design failures or human errors, because not the security application but warnings of a security program are evaluated.	
	Additional information realised as instructions could decrease warning comprehension, but could increase adequate reaction to warnings of users, which remote control a mobile domestic robot over a tablet. Additional warning information has to be carefully used, because it could be irritating for users. Future studies have to research the sophisticated usage of additional warning information to increase their effectiveness.	The study course shows that additional information as background information and reading the content of warnings on smartphones could support the effectiveness of warning messages as adequate reaction of infantile users. Future studies have to research sophisticated usage of additional information for children, including usage of different characters for different types of warning messages.

Table 6.2: Results of both warning test cases evaluated with HITL framework (according to [Cra08])

**Summary:**

The comparison of the both prototypes with HITL show following tendencies, which have to be evaluated in future studies with larger test-groups:

- Demographic factors may play a role in warning perception and warning comprehension. So the most younger participants in test case 1 ('mobile robot warnings') rated the 'warning usefulness' as 'less useful' than elder participants. Most children in test case 2 do not comprehend the warnings, but react intuitively in the right way. Some children remembered the first meaning of a security warning in combination with the colour of the cartoon character.
- Reading additional information in security warnings (instructions and background information) could support the adequate reaction of users.
- Instruction information in security warnings could decrease the wish of users for additional help and could support their problem solving.
- Instruction information in security warnings could increase the heed of the warning by users.
- The perception of a high risk level by users could increase their compliance to decide after the warning recommendation.
- Instructions in warnings could melt the fear of users of malware-related personal impacts.

#### Main lacks:

- Effects of *habituation* and *focus on the main task* were observed in both user studies. Some test persons were annoyed by warnings and therefore they were less motivated to read the warning messages carefully.
- The *attention switch* to warnings in the adults study is not relevant, because of the test situation where the tester talks to the participants.
- *Not all users are capable* to handle malware related situations only by reading warning information. Especially children have to be supported by (technical-savvy) peers and/or parents to solve complex malware problems. But it has to be also evaluated whether security decisions in domestic environments are solvable by **non-security experts**.
- Additional warning information have to be well designed, because it *could negative influence user's comprehension*.
- The effects of *knowledge acquisition* and *application* of warning messages of the both prototypes has to be evaluated in future studies.
- Warning information is *no substitute for training, and external help*. It should be evaluated, whether a specific user-group is able to comprehend and process the recommended warning instructions or whether training and additional help is needed.
- Participants showed a less awareness for security threats on mobile devices and IoT devices although they knew about mobile malware.



# 7

## Summary, conclusions, related and future work

In this chapter in section 7.1 the results of this thesis are summarised and conclusions are drawn. Furthermore, in section 7.2 selected topics of own research work related to this thesis topic are sketched and in section 7.3 ideas for the future work are described.

### 7.1 Summary and conclusions

---

In this thesis a new effective malware warning approach for mobile devices is introduced, which considers potential security and safety implications to users of mobile devices. It is based on recommendations of safety [Wog06b] and security warning research (e.g. [BBLCF13]) and own ideas. The answers to the research questions of section 1.2 can be briefly summarised:

**Research question 1 (RQ1):** '*Design of current mobile malware warnings*'. The investigations showed lacks of current mobile malware warnings regarding information of mobile devices users of personal-related risks. It's a motivation for the introduced new warning approach.

**Research question 2 (RQ2):** '*Potential personal consequences of malware attacks to users of mobile devices*'. A new *personal risk model* is introduced to design a new user-centered warning approach, which informs users about direct and indirect personal risks of malware incidents.

**Research question 3 (RQ3):** '*Design of an effective malware warning concept*'. Due to the lack of an existing *literature review* an own research of existing warning approaches is realised in chapter 3. On basis of recommendations of the first comprehensive literature review for security warnings and the *personal risk model* a new malware warning approach for mobile devices is introduced in section 4.3. The new warning approach is realised as test cases for two user-groups (adults, primary-school children) and two specific application scenarios (adults - remote control of a domestic robot, children - single smartphone usage) (section 5).

**Research question 4 (RQ4):** '*Evaluation of malware warning effectiveness*'. On basis of state-of-the-art evaluation methods from usability and security warning research a evaluation methodology and concept for the new warning approach is introduced. It is used to measure the effectiveness of the introduced approach, which includes users' adequate warning comprehension and solution finding to adequately react to current malware threats. The results of the evaluation of the two warning test cases show tendencies, that the warning effectiveness can be increased using the new warning approach. Because of the small sample sizes (adults: 23, children: 13 participants) and testing of the whole warning design in one single user-study session future studies are needed.

In the following the **conclusions** of this research work are summarised.

Today, there exist no adequate user-centred malware warnings on mobile devices, because these applications focus the protection of the system not the user. Furthermore, the research field of security warning research is relatively new. Most warning research results are published after the year 2009 and often focus browser warnings (e.g. malware, SSL). The new approach in this thesis want to fill this research gap by introducing user-centred warnings, including information about personal risks, consequences, and instructions to handle malware attacks. The results in section 6 show, that demographic factors may play a role in warning perception and warning comprehension. Furthermore, it is shown that reading additional information in security warnings (instructions and background information) could support the adequate reaction of users. The results also show, that the perception of a high risk level by users could increase their compliance to decide after the warning recommendation. Furthermore, tendencies are found, that warning instructions could decrease the wish of users for additional help, could support their problem solving, could increase the heed of the warning by users, and could melt the fear of users of malware-related personal impacts.

The results of the evaluation of the both warning instances disclose also some '**lacks**' of the warning design and test realisation. Habituation effects are observed because user-study participants are confronted with a set of similar designed warnings. The results also show, that tests have to be well prepared to prevent failures during test realisation, which influence the test results. For example in the adults test the measured time stamps of user warning interactions were not useful, because the tester sometimes already talks to the participants, while the system starts automatically time logging. The test results also show that additional warning information (e.g. instructions) have to be well designed, because it could be negative influence user's comprehension. It could be also concluded that in some cases warning information is no substitution for training and external help, because lay users often do not comprehend complex interrelations of malware attacks and are unable to handle malware related situations only by reading warning information.

## 7.2 Selected topics of own related research work

---

Amongst the introduced research of security warnings for mobile devices for non-experts other research related to this topic is done. The main fields of research were the *risk communication in the industrial field*, raising and evaluation of *security awareness*, design of *online security guides*, and *security evaluations of embedded systems*.

**Risk communication in the industrial field:** Amongst the security warning in non-professional environments warnings in professional environments are researched. One example is the generic description of **attack scenarios of the Conficker worm in a production engineering environment** [DKF<sup>+</sup>10]. In this article the formalisation methodology for malware of Kiltz et al. [KLD06] is used to describe characteristics of the worm Conficker variant C. It is used to analyse oncoming threats to modern production engineering systems. Based on the Conficker worm formalism and a component model of an exemplary production scenario (the automatic chamfering of great gears with an industrial robot) an exemplary methodology is introduced. The methodology is demonstrated to analyse malware threats to component related security aspects and to compare the criticality of different malware instances for a special

## 7.2. Selected topics of own related research work

production system. On the basis of this methodology potential threats to the security of software and hardware components of the exemplary production scenario are shown (figure 7.1). Furthermore, this methodology could also be used to illustrate security threats and protection concepts with virtual techniques to help software engineers to program secure software. The threats are illustrated by the means of *four exemplary scenarios*: the impeding of production processes, the eavesdropping of information, the manipulation of information, and the inducing safety-relevant impact to persons (e.g. operators) or objects (e.g. a work-piece).

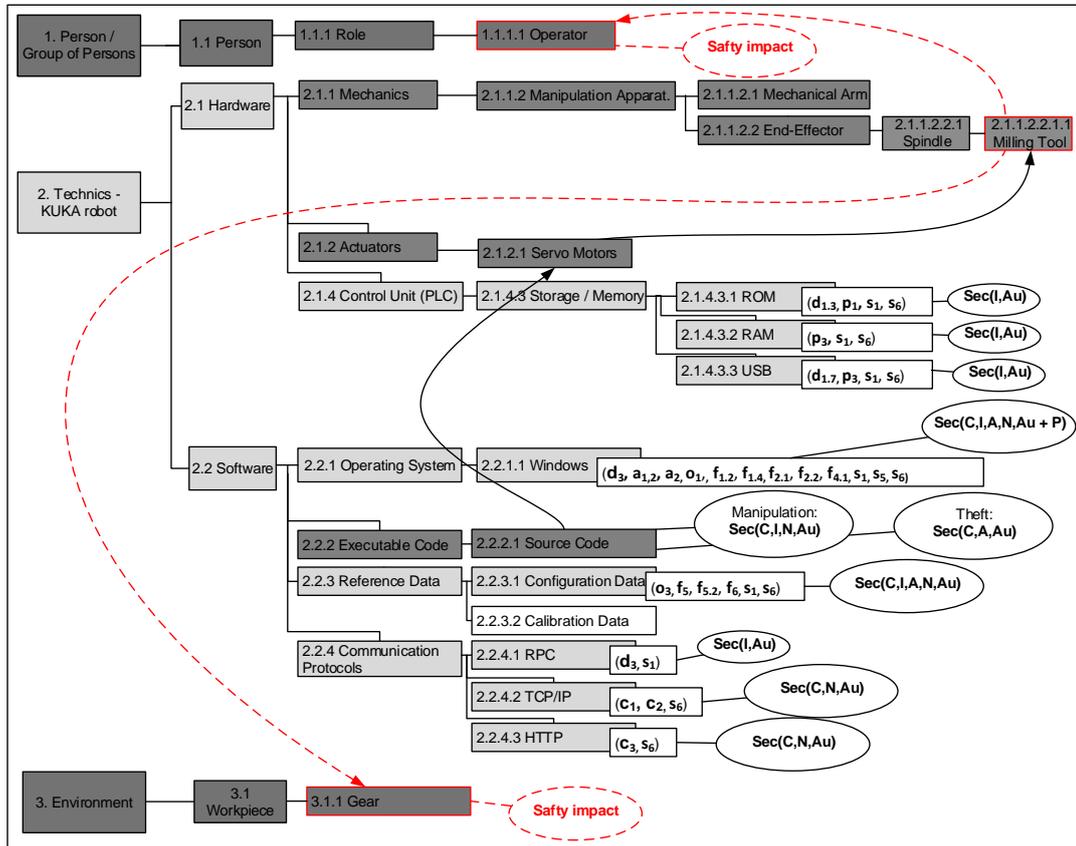


Figure 7.1: Potential security and safety implications of a Conficker worm infection to an industrial robot: An exemplary annotated component model for the robot controlled automated machining of a work piece

(Note: *in light grey*: components potentially influenced directly by primary malicious functionality of the worm, *in dark grey*: components potentially influenced by structural implications of the malicious worm functionality, *in rectangles*: the formalised properties of a potential worm, *in ovals*: the security/safety aspects of components threatened by the worm's malicious functionality, *broken lines*: the potentially safety impact to components)

Another example is the **warning design and evaluation for the human-robot-interaction** in the industrial field [FKD11]. In this document a multimodal security warning design approach for automated production scenarios with industrial robots is introduced. This first approach is based on and adapts design principles of common security programs and a German VDI standard for safety warnings design [VDI00]. It was focused on direct human-to-robot interaction scenarios, e.g. the online-programming of industrial robots, because of their potential indirect safety impacts, which could be caused by malware infection of a robots control computer. Ten different designed multimodal security warnings are created, composed of visual and acoustical information. The visual information of warnings is transported via a traffic light

metaphor (symbolising three different threat levels), different warn icons (symbolising properties of malicious codes) and instructions icons to programmers or operators and additional textual information. Figures 7.2 and figure 7.3 illustrate two different warning risk levels of the three designed risk levels of the warning approach. With an acknowledgement button in the middle of the warning, the programmer's confirmation of the reception of the warning is verified. Additionally, three different acoustical signals also indicate the threat level of the warning. Furthermore, an evaluation is presented, which uses concepts known from usability testing (method of loud thinking, questionnaire, time measurement). The aim is to evaluate general design criteria of the developed security warnings and tendency of user perception for further advancement of our warnings design.

The ten designed warnings were presented in a pilot study to ten participants<sup>102</sup> in an office environment. The participants had an average age of 27 years, different gender and professions. The tests was carried out in an office environment, where the test persons sit on a standard office chair in front of a standard laptop, where one key is defined as emergency button. Additionally, a standard office telephone is provided in cases of emergency to call the responsible supervisor.

The results show that the different warning icons are *different comprehended* by the test persons. There are a significant differences between the recognition of *round instruction icons* 'call supervisor' and 'push emergency button & call supervisor' and *triangle malware property icons*. The round instruction icons were better comprehended by the participants. One reason for the good results could be the focus of test persons on a correct reaction, including operation of the emergency button. Furthermore, it could be concluded that the additional information of the current malware property seem to overburden operators comprehension. Potential countermeasures against this lack are the simplification of warning information, the adaption of warning information to specific roles (e.g. operator, administrator), the sensitisation of operators to cyber-threats, and their education of warning interpretation. The test results also show that the choosing of warning icons, which meaning is different in other application contexts is difficult for warning cause identification with a new meaning (example symbol of 'radio activity' choosing for damage warnings). Here are future evaluations of single warning icons useful [WSLZ06].

Furthermore, the reaction to warnings are analysed. Measured were the clicking time stamps of the acknowledgement button in the warning and the dummy emergency button on the test laptop. The results show, that most test persons react adequate regarding pushing the emergency button. Nevertheless, only less the half of test persons clicked the acknowledgement button, which indicate a bad design or placement of this warning element. However, the test results could not be generalised because of the small sample size of test persons (10) and the lack of realistic data, because a laboratory study was realised. In the future the research of security warnings in industrial fields has be realised in realistic industrial environments with more test persons.

---

<sup>102</sup>As a rule of thumb in usability evaluation, four of ten persons detect the most serious problems in an evaluation [Nie94].

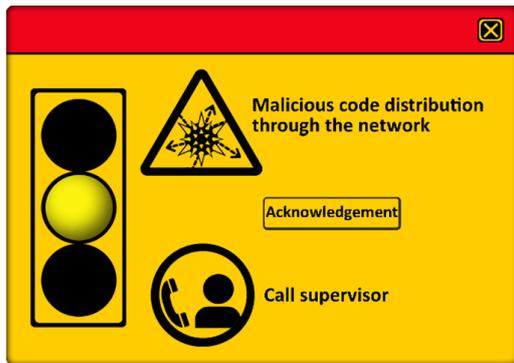


Figure 7.2: Exemplary warning for threat level 'low'

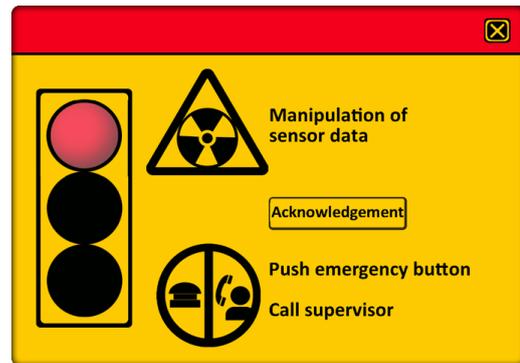


Figure 7.3: Exemplary warning for threat level 'high'

On basis of the metamodel [FDOF10] an **uniform risk communication approach for distributed IT environments** is published, which combines safety and security aspects [FN14]. It is motivated by the trend to compose real time systems with standard IT known from conventional office domains results in heterogeneous technical environments. Examples are modern industrial process automation networks. It is a challenging task, because of potential impacts of security incidents to the system safety. For example, robot control units could be manipulated by malware. The term 'risk communication' is introduced, to describe alarm communication in human-machine interaction scenarios. User adapted risk communication between humans and industrial automation systems, including domestic robotics, can prevent hazards and/or threats to the entire system safety and security. In this paper a selection of current safety and security risk communication standards and recommendations are compared using selected evaluation criteria. This paper focuses on alarm system standards in the industrial process automation domain and intrusion detection systems known from conventional desktop IT domain. A series of DIN standards and recommendations, which are available free of charge from approved industrial and computer security organisations, are reviewed. Current risk communication standards and recommendations offer domain-specific solutions, but are not sufficient to fulfil safety and security requirements of distributed IT environments with safety and security properties. Therefore a new model based approach is introduced. There are still gaps concerning joint (unified) safety and security analysis, development and maintenance/operation. Therefore, further safety and security standards and approaches used in general in industrial context should be taken into account in the future, e.g. IEC 61508 (Functional Safety)<sup>103</sup> or ISO 13482 (Safety requirements for personal care robots) [ISO14] and security standards, such as ISO 15408 (Common Criteria) [ISO07] or the ISO 2700x series (Security Management)<sup>104</sup>. In the future, the generic approach for risk communication in heterogeneous systems has to be specified and evaluated with practical implementations on selected heterogeneous systems, e.g. service robots.

**Security awareness raising and evaluation:** In [FMG+11] an exemplary VR prototype is introduced to sensitise production engineers to security risks in manufacturing engineering. With the increasing use of standard IT technologies in automated production systems, similar security vulnerabilities and threads known from the desktop IT domain are also introduced in manufacturing engineering. These vulnerabilities could be misused for different attacks employing malware. Derived attacks can be hazardous to production system safety, for example objects and/or people in the vicinity of functioning industrial robots might be in danger.

<sup>103</sup><http://www.iec.ch/functionalsafety/>, accessed: 01.05.2018

<sup>104</sup><http://www.27000.org/>, accessed: 01.05.2018

Usually, users are given oral instructions on relevant safety information. Often this is not sufficiently to explain the complexity of security attack scenarios, which could cause safety issues. In this article the use of a VR simulation environment as a better visualisation of potential security risks in the production domain is proposed, e.g. the manipulation of robot control programs via malware. To outline the idea an exemplary scenario in a VR simulation, the automated chamfering of large gears with an industrial robot, is used. In the future, the VR simulation has to be annotated with multimedia security warnings to better facilitate the users' comprehension of the potential security and safety risks.

[KHFD12] introduces an **investigation of the security awareness of teens/children regarding specific websites**. This results should be the basis for the design of online security guides for children. Therefore, in the first step, websites of categories chat, social networks, search engines, lifestyle, TV and video were selected. Then these design websites were analysed by means of usability, transparency of security, children-like contents. Furthermore, the three goals, protection of privacy, passwords, and Internet behaviour and their realisation are analysed and rated by a three security experts. In the next step, 18 children of a sixth class in a secondary school were confronted with a questionnaire of 10 questions regarding Internet usage and sense of security while using the Internet. The study show that there are children-specific website, but sometimes they are not known. Another lack are the offer of security related topics for children, especially for the protection of childrens' privacy. Here videos or games are suitable e-learning concepts for children. Furthermore, an uniform icon is recommended, which symbolises the security of a specific website. Children have to be supported to learn the adequate usage of the Internet and they have to be sensitised what happens to their data in the Internet. In the future the approach of natural metaphors (e.g. for the nursery) will be used to realise children-friendly online contents and guides.

On basis of the findings in [KHFD12] a **game prototype for children** for e-learning of IT security threats is published in [FSRD13]. In this paper an e-learning game prototype for primary-school children (aged between 7 and 9 years) is introduced. The game teaches children about IT security threats, which they may encounter while they using the Internet. The game is separated into three mini games: virus infection of the computer, inviting somebody in social networks, and chatting with strangers. The game design used metaphors and based on standard guidelines of infantile learning environments (e.g. paradigm of simplicity, multidimensional stimuli, characters). Furthermore, the results of a user study of 36 primary school children show, that the metaphors for exemplary IT security threats partially support childrens' way of playful learning. In the future, the prototype will be extended by additional metaphors.

**Online security guides:** On basis of the findings in [KHFD12] and [FSRD13] a first concept approach for **security types** are introduced in [FBV<sup>+</sup>13]. The approach is based on the theory of 'security mentalities' for criminal risks [Kli08] and is adapted for the security awareness of children and teens. The approach is based on a large questionnaire study with 157 pupil of a grammar school aged between 10 and 15 years. The results of the questionnaire regarding security awareness of children (e.g. publish of private data) are used to classify three specific security types. Members of security type 1 are most younger children (10-13 years) of both sexes, which have less technical previous experiences than members of the both other security types. They said to do not offer any personal data in the Internet and wish more help by their parents and their school. Members of security type 3 are mostly older children (12-14 years)

and more boys as girls. They have the most experiences with IT and the Internet in comparison to the members of the both other security types. Although, they seem to be sensitised for online security threats, they publish more personal information in the Internet (e.g. address, telephone number) than children of the other security type classes. Most of them want to have more information about secure Internet use by their parents. Children of security type class 2 are from all age classes (10-15 years) and are more girls. This class symbolises an average between the both other security type classes. In the future the security type approach should be used for security awareness measures, such as warnings and online security guides.

On basis of the findings in [KHFD12] and [FSRD13] a first prototype of an **security guide for primary-school children** using the Internet is published in [FTKD14]. Already primary-school children (aged between 6 and 10 years) using the Internet regularly and are confronted with security threats they could not handle. The introduced concept and prototype of a security guide should sensitise the children for security threats in the Internet and should offer them a security mechanism to handle these threats. The prototype is realised as Firefox add-on, detects and identifies the online activities regarding a specific website type (community site, online login, e-mail, chat, search engine, password entering, file download). The security guide uses multimodal design criteria, e.g. visual and acoustical warning information, comic character, and an information view to feedback the current threat situation. To test the prototype guide and to realise privacy requirements a virtual test environment is implemented including three websites: registration, e-mail, and chat. The prototype was evaluated with a long-term user-study in a primary-school with 12 children, where participants get website specific tasks. The evaluation goal was to prove a learning effect and the usability of the guide. The tests could not significantly support learning effects, but the usability and optical design of the guide was rated with good. In the future, the assumed learning effects are proved with further tests with larger participant sizes. Furthermore, it is planned to improve the security guide, implement and test it on different devices for different application scenarios (e.g. security-safety-warnings).

**Security evaluations:** Another relevant research topic are security evaluations of embedded systems to evaluate potential threats, which have to be prevented, detected or warned to users. One example is the security evaluation of the AR.Drone, a **quadrocopter**. In [SFH<sup>+</sup>12] a security threat analysis and an exemplary attack to track persons were introduced. The security analysis is based on the BSI standard procedure for an IT baseline security protection. The article illustrates an approach of a security threat analysis of the quadrocopter AR.Drone, a toy for augmented reality (AR) games. The technical properties of the drone can be misused for attacks, which may relate to security and/or privacy aspects. The aim is to sensitise for the possibility of misuses and the motivation for an implementation of improved security mechanisms of the quadrocopter. It is primarily focused on obvious security vulnerabilities (e.g. communication over unencrypted WLAN, usage of UDP, live video streaming via unencrypted WLAN to the control device) of this quadrocopter. In three exemplary scenarios it could be practically verified that the security vulnerabilities can be misused by unauthorised persons for several attacks: high-jacking of the drone, eavesdropping of the AR.Drone's unprotected video streams, and the tracking of persons. Amongst other aspects, the current research focuses on the realisation of the attack of tracking persons and objects with the drone. Besides the realisation of attacks, the potential of this particular drone for a 'safe-landing' function as well as potential security enhancements are evaluated. Additionally, in the future it is planned to investigate an automatic tracking of persons or objects without the need of human interactions.

### 7.3 Possible directions for future work

---

This section sketched the future work of the introduced new warning approach. In section 7.3.1 the *improvements* of the new warning approach and in section 7.3.2 the application of parts of the warning concept to other research fields are described.

#### 7.3.1 Future improvements

---

This section briefly describes possible improvements of the introduced approach, based on the test results in section 6. That are mainly the improvement of the *warning design* and the *test design* for evaluation.

##### **Improvement of warning design:**

**Personal user requirements:** In this thesis a selection of potential user requirements are introduced which could be effected by malware attacks on mobile devices. The requirements could be better differentiated. One example is 'privacy'. In future, further aims of data privacy (e.g. integrity, unlinkability, transparency) could be included into the warning concept.

**Instruction information design:** Additional warning information have to be well designed, because it could negative influence user's comprehension. That includes the design of instruction information. The test results for the adults warning instance show, that more than the half of participants with instruction information rated step-by-step-instructions as very helpful. Amongst the step-by-step instructions other information could be useful, such as links to detailed online information, and contact information for external help. Furthermore, it should be investigated if a group specific instruction design increases warning effectiveness. One example are instructions for elderly people [Har94]. Amongst the improvement of the warning instruction design also its *theoretical basis* could be improved. The instruction information in section 4.3.3 based on recommendations from a BSI standard [BSI08]. That are instructions for technical security mechanisms and organisational security measures for mobile device users. In the future an **instruction model** could a be better basis to create instruction information in warnings. One example are information from security awareness research of Bitton et al. [BFS+18], whose introduce a taxonomy of mobile users' security awareness. Their taxonomy based on three psychological dimensions of users: attitude, knowledge and behaviour. The behaviour information about preventive or confronting behaviour of mobile devices users could be used for a warning instruction model. Furthermore, previous research results of mental models of non-expert users could be included into the instruction model. Examples are **metaphors** of the physical world and criminal mental models for risk-communication [Was10, ALC07].

**Risk level design:** The test results in this thesis show that most participants rate the risk level of the warnings higher as designed. Furthermore, differences between design and interpretation of risk levels could be explained by priming effects, inaccurate warning design, and wrong mental models of participants of the malware attack. In the future, priming effects in test realisation should be prevented. Furthermore, textual information should be improved to prevent personal imaginations and speculation about the risk level of the current situation. The changing of the mental model of users regarding function of malware attacks could not be realised by using warnings. Here education of users is necessary to sensitise users for malware attacks and correct their mental models.

**Multimodal warning design:** The both tested warning instances in this thesis were a realisation of a specific profile as combination of visual, acoustic and haptic information. For example for test case 1 only visual and acoustic feedback information is used. In the future all different profiles of feedback information have to be tested to show their relevance for warning perception of users.

**Polymorphic warning design:** The evaluation of the two warning variants in this thesis show that after the repeating display of similar designed warnings test persons tend to ignore these warnings. To fight these habituation effects variations of the warnings should be designed and tested. The concepts of polymorphic warnings introduced by Brustoloni and Villamarín-Salomón [BVS07] and Jenkins et al. [JKB<sup>+</sup>18] have to be adapted for the warning approach in this thesis.

**Touch of users emotions:** The study results for the adult warning instance show the higher users perceived the danger level, the rather they are compliant to decide after the warning. The touch of users emotions seem to be a valuable approach for warning design, which confirmed the research results of [HPB09]. This concept has to be proved by larger studies in the future.

**Alternatives in methodology and concept:** In the future, the introduced general effective security warning design approach has to be adapted to additionally user groups, different mobile devices and coupled systems as addressed in this thesis. Possible research directions are warning design adaptations to specific user groups, such as visual-disabled and hearing-impaired people. Additionally, the introduced warning concept could be adapted for future systems, such as IoT devices, which have often no classical user interfaces. Here speech outputs could be used to warn users for potential personal impacts of cyber-attacks.

#### **Improvement of test design:**

**Larger sample sizes:** Amongst the warning design also the test design could be improved. As already mentioned in sections 6.1.3 and 6.2.3 the test results could not be generalised to the whole population, because of the small sample sizes (adults: 23, children: 13 participants). Therefore, in the future tests with **larger sample sizes** have to be realised. **Field tests:** The both warning instances in this thesis are tested under laboratory conditions. To get realistic results in the future field studies are needed. **More test cases:** In this thesis two test cases of the new warning approach are realised. To estimate the effect of warning design elements to the warning effectiveness different profiles of complex instructions, risk level combinations, and multimodal feedback combinations have to be investigated. Furthermore, **long-term studies:** are needed to measure the long-term effects of warning effectiveness, such as *knowledge retention and knowledge transfer* of warnings.

**Pre-separation of novice and experts users:** are recommended in warning science literature (e.g. [BLCD<sup>+</sup>11, AF13]), because both groups differ in their previous knowledge of computers, security risks, and risk handling strategies. In the future, test candidates are assigned into one of the both groups by their answers to a previous questionnaire. So their test results could be better interpreted on basis of this pre-selection.

**Investigation of demographic factors:** Warning researchers assume that demographic factors have an impact of user behaviour regarding warnings (e.g. Akhawe and Felt [AF13]). The results for the adult warning instance indicate also supports this theory of demographic differences of warning perception. In the future this theory has to be investigated in more detail.

**Using novel evaluation methods:** The both warning instances are tested with classical usability evaluation methods, e.g. questionnaires, observations, method of thinking aloud and logging of user click events. Other warning researchers using new evaluation methods of the cognitive neuroscience technology (e.g. B.B. Anderson et al. [AVK<sup>+</sup>14, AVK<sup>+</sup>16, NSK<sup>+</sup>14]), such as EEG and fmRT. In comparison to classical usability evaluation methods, neuro-science methods directly measure the warning processing in the human brain. The main disadvantage using neuroscience methods are the potential influence to study result validity, because these methods are used in laboratory studies and users could be distracted by technical equipment they have to wear.

**Single testing of design elements:** In both test cases in this thesis the whole warning design (test case 2) and one warning variation (test case 1) are tested. Single warning design elements have to be tested in the future to get more specific information about the influence of single warning design elements to the warning effectiveness. Furthermore, these warning variations have to be compared with state-of-the-art warnings. Examples are variations of text elements, text combinations, icons, background colours, illustrations of the current risk, and other languages. Furthermore, the design of specific icons could be evaluated. One example are icon sets to express privacy statements [Han08].

**Using 'real risks':** Warning researcher recommended to confront users with real risks to get portable test results [KMS12]. In the future, real risk could be 'simulated' if participants use their own technology equipment or login credentials.

### 7.3.2 Future research

---

This section briefly describes, examples of future research on basis of the introduced warning approach.

**Human-information-processing:** The *literature review* of security warnings in chapter 3 disclosed unexplored further research topics related to human-information-processing. One research field is the impact of *warning impediments* to users attention to warnings. Users attention could be distracted for example by their primary task, and environmental stimuli. For example results from field studies for the new improved warning approach could be compared laboratory study results to find improvements.

Another research topic is the *application* of warning, including knowledge retention and knowledge transfer. This affects application scenarios in which users mainly control the system. So the users have to decide whether the warning is applicable to the current situation. Here long-time studies are needed to measure the effects of knowledge retention and knowledge transfer in warning processing.

Furthermore, the *behaviour* of users could be researched in more detail. It could be investigated, how *warning interaction failures* of users impact the warning effectiveness. Especially, Norman's 'gulf of execution' (inability to complete an action successfully) and 'gulf of evaluation' (inability to determine if the action is correctly carried out) have to be investigated.

**Personal risks to increase warning comprehension:** The introduced warning approach includes personal risks as basis of an effective warning design. It is based on the recommendation of Kauer et al. [KPV<sup>+</sup>12] to choose personal risks in warnings to improve warning comprehension. Future research should investigate, how the personal information in warnings has to be designed to be more effective. In this context the introduced 'personal risk model' could be the basis for information coding in warnings.

**Improvement of other security warning types:** In this thesis a malware warning approach is introduced. Malware attacks potentially could impact all security aspects of a system (see section 2.5.1). That distinguishes malware warnings from other warning types, such as browser SSL warnings, browser phishing warnings, firewall warnings, and spyware warnings. The concept of using personal risks, consequences and instructions in warnings could also improve the effectiveness of other warning types. Main advantages are the sensitizing of users for personal risks of cyber-attacks and the potential improvement of problem solving of users by warning instructions.

**Habituation effects of specific security warning types:** The research of current warning literature in section 3 revealed another future research topic. Akhawe and Felt [AF13] receive in their non-representative studies with malware, SSL, and phishing browser warnings less habituation effects for malware warnings (see section 3.2). Future study results have to prove whether these results could be supported.

**Individualised security warnings:** In section 3.1.1 exemplary research work for individualised warnings is sketched (e.g. [DKYT<sup>+</sup>09, BV14, KPV<sup>+</sup>12, HHWS14, MMHE17]). These warnings could be improved by communicating *personal risks* and give users *instructions* how to handle security risks. Furthermore, on basis of the individual security awareness of a user-specific designed warnings and instructions depending on user's security awareness could be displayed. The individual security awareness could be measured for example by using a taxonomy of mobile users' security awareness [BFS<sup>+</sup>18].

**Warning design for exemplary non-professional application scenarios:** Parts of the introduced warning approach could also be used in other non-professional application scenarios. Two examples are warnings in modern automotive systems and IoT devices. The usage of warnings in **automotive systems** has to be well prepared [KNB<sup>+</sup>09], because these systems have specific technological and safety requirements. The usage of multimodal warnings could disturb the driver potentially cause an accident. Therefore, the introduced warning approach could be used to display the driver detailed warning information when the automotive system stops, e.g. textual instructions how to handle the current risk. The small dashboard displays are not usable for such textual information, but modern head-up displays (HUD) are a potential alternative.

Another application example for the introduced approach are **IoT** devices, such as smart home devices. Most of them do not have classical user interfaces, such as displays. So warning information has to be adapted, e.g. instructions could be given as speech output.

**Warning design for exemplary professional application scenarios:** As already mentioned in section 7.2 the introduced warning approach could be used in professional human-machine-interaction scenarios, such as with industrial robots, airplanes and other complex systems. The user-groups are experts, which are in contrast to lay users educated and trained for their specific tasks. The new warning approach could be used for risk communication on basis of interrelations of security impacts to safety functions. Furthermore, the instruction concept could be used as basis for expert education, training, and practices.

Another research field are the adaption of Meyer's concepts and methods [[Mey01](#), [Mey04](#)] for dynamic safety warnings in complex systems for non-expert users in non-professional application scenarios, because Meyer's models assume experienced operators. Examples are the research of the 'compliance' and 'reliance' of non-experts and the usage of an economic cost-benefit analysis to improve the design of the introduced warning approach.

**Warning design for different user-groups:** The warning approach could be also adapted for other user-groups, such as further mentioned *experts* with specific capabilities. However, also other user-groups could benefit from the warnings with personal information and instructions, for example user-groups with *limited capabilities* (e.g. hearing, vision). During the adaption process it has to be weighed up if warning effectiveness is influenced by adaption decisions (e.g. removing of visual warning information), and countermeasures to keep warning effectiveness have to take into account (e.g. replace of visual warning information by acoustic signals). Another interesting research direction could be the adaption of the warning approach to different *organisational roles* (e.g. students, professors), *individual differences/personality types* (e.g. extraverts, introverts), and *cultural differences* (e.g. Asian vs. European users).

# 8

## Appendix

This chapter presents all necessary contents for the user studies, including evaluation documents, questionnaires and important results.

## 8.1 Adults - Mobile robot warnings

---

### 8.1.1 Application scenarios

---

**Application scenarios – Mobile Robot Warning Messages**

Version: February 2017

**Introduction of robot and main scenarios:**

- New robot for chore, have to be tested
- Later: Parents or good friend/relation will come for coffee and cake (already placed on the cupboard)
- Show guests what robot is able to do (e.g. do the chores, wash and dry clothes)
- Later in the evening: friends will come

**1) Launch the robot:**

- First: launch the robot (tester)
- Insert some data (Start-GUI): Name of robot, password, test person hours
- **Launch the robot** (test person)

**2) Chore app:**

- If robot could do his chores, we need an extension:
- Configurations -> Extensions -> **Install chore app**

**3) Household:**

- Parents or good friend/relation will come for coffee and cake
- Show guests what robot is able to do (get coffee and cake)
- Before coffee: Put clothes in washing machine
- After coffee: Put washed clothes in tumble dryer

**3a) Washing machine**

- Robot should only fill in clothes, because it is already charged with clothes
- Task: Drive robot to washing machine -> Fill in -> Launch

**3b) Door of flat**

- The bell ringed, parents or good friend/relation are arrived
- Robot opens the door
- Task: Drive robot to door -> **Open** -> Close

**3c) Coffee and cake**

- Eat cake and drink coffee with parents or good friend/relations
- Task: Drive robot to cupboard -> **Pick-up coffee and cake** -> Deliver

**3d) Clear away used dishes**

- Ready with eating and drinking, clear away used dishes
- Robot is already charged with used dishes
- Task: Drive robot to dish washer -> **Place in used dishes** -> Start dish washer

Figure 8.1: Application scenarios for test of test case 1 (scenario 1-3d)

### 3e) Tumble dryer

- Washing machine is ready
- Robot has to put wet clothes in the tumble dryer
- Task: Drive robot to washing machine -> Empty washing machine -> Fill in wet clothes in tumble dryer -> **Start tumble dryer**

### 3f) Update

- Robot is a new device, which needs a software update
- Therefore, robot has to drive to battery-charging station.
- Task: Drive robot to battery-charging station -> **Install update**

### 4) TV-/Ladies-/Mens' night:

- You have friend invited for a nice evening. They are still arrived.
- You are already sit on the sofa.
- Robot has to bring something to drink, one friend wants only **water**
- After that you all want to have something for nibbling.
- Task: Drive robot to drinks -> Take bottle of **water** (-> other drinks) -> Deliver
- Task: Drive robot to cupboard -> **Take snacks** -> Deliver

### 5) Load robots batteries:

- The evening with friends is over. All guests are away. The chore is done. Only the robot has to drive to battery-charging station to load its batteries.
- Task: Drive robot to battery-charging station -> **Load robot**

Figure 8.2: Application scenarios for test of test case 1 (scenario 3e-5)

### 8.1.2 Questionnaire

**Questionnaire – Mobile Robot Warning**

Version: February 2017

**[EQ1] Previous experiences:**

**Q11:** Have you ever been a victim of a computer virus/Trojan horse or bothering software?  
1 - no / 2 – yes, which kind of disturbance + comment

**Q12:** Have a friend of you ever been a victim of a computer virus/Trojan horse or bothering software? 1 - no / 2 – yes, which kind of disturbance + comment

**Q13:** Which devices you use for the Internet?  
1 – computer / 2 – tablet / 3 – smartphone / 4 – other devices

**Q14:** How oft you use the Internet?  
6 – several times a day / 5 – once a day / 4 – several times a week / 3 – once a week / 2 – occasional / 1 – rare till never

**[EQ2] Knowledge:**

**Q21)** Do you know that there are computer viruses and Trojan horses for smartphones and tablet PCs? 1 - no / 2 – yes

**Q22)** Do you know that there are different classes of malicious codes (e.g. computer viruses and Trojan horses)?  
1 - no / 2 – yes, which malicious codes you know and which malicious functions they have? + comment

**Q23)** In your opinion, how strong is the involvement of the following persons/groups in distributing computer viruses and Trojan horses? (*User, Software developer, Hardware manufacturer, Cyber-criminals/hackers, Governmental institutions/intelligence services, Script kiddies (teenaged computer-hackers)*)  
1 – no involvement / 2 – very little involvement / 3 – little involvement / 4 – some involvement / 5 – strong involvement / 6 – very strong involvement

**Q24)** In your opinion, how strong is the support of the following activities in distributing computer viruses and Trojan horses? (*File download, Open an e-mail attachment, Surf the Internet, Installation of software/apps, Usage of removable media (e.g. USB flash drive, burned CD/DVD), Links in social media (Facebook, Twitter, WhatsApp, etc.), Forwarding in social media (Facebook, Twitter, WhatsApp, etc.)*)  
1 – no support / 2 – very little support / 3 – little support / 4 – some support / 5 – strong support / 6 – very strong support

**Q25)** In your opinion, how likely is the infection of networked domestic robots (e.g. vacuum cleaner, lawn mower or toy robot) with computer viruses and Trojan horses?  
1 – very unlikely / 2 – unlikely / 3 – somewhat unlikely / 4 – somewhat likely / 5 – likely / 6 – very likely

Figure 8.3: Questionnaire for test case 1 (EQ1-2)  
(Note: Text in bold angled brackets are added after the test for better readability)

**[EQ3] Usefulness of warnings:**

**Q31)** How much fun do you had using our robot?

1 – no / 2 – very little / 3 – little / 4 – some / 5 – much / 6 – very much

**Q32)** How helpful do you find the warning?

1 – not helpful / 2 – very little helpful / 3 – little helpful / 4 – some helpful / 5 – helpful / 6 – very helpful

**Q33)** How much do you were unsettled by the warning?

6 – not unsettled / 5 – very little unsettled / 4 – some unsettled / 3 – little strongly unsettled / 2 – strongly unsettled / 1 – very strongly unsettled

**Q34)** How much do you were concerned by the warning?

6 – not at all / 5 – very little / 4 – little / 3 – some / 2 – strongly / 1 – very strongly

**Q35)** How much do you were supported, when you...

... *would have had a step-by-step instruction?*

... *would have had a technical-savvy friend or relation?*

... *would have had a technical expert?*

... *would have read a user guide?*

6 – not at all / 5 – very little / 4 – little / 3 – some / 2 – much / 1 – very much

**[EQ4] Comprehension of warnings:**

**Q41)** Which danger level do you relate to these two icons?



1 – no danger / 2 – very little danger / 3 – little danger / 4 – some danger / 5 – high danger / 6 – very high danger

**Q42)** Which danger level do you classify following warning?

Warning WITHOUT sound and WITHOUT vibration,

Warning WITH sound and WITHOUT vibration,

Warning WITH sound and WITH vibration

1 – no danger / 2 – very little danger / 3 – little danger / 4 – some danger / 5 – high danger / 6 – very high danger

**Q43)** In the experiment you saw following warning.

[Notes:

Warning 1 – 10 are visualised previous the following questions.

WMNo = Warning number

WMNo\_04: Only for the evaluation group]

**Q43\_WMNo\_01)** How dangerous do you perceived the described situation in the warning?

1 – not at all / 2 – very little dangerous / 3 – little dangerous / 4 – some dangerous / 5 – dangerous / 6 – very dangerous

**Q43\_WMNo\_02)** How comprehensible was the warning for you?

Figure 8.4: Questionnaire for test case 1 (EQ3-4)

(Note: Text in bold angled brackets are added after the test for better readability)

1 – not at all / 2 – very little comprehensible / 3 – little comprehensible / 4 – some comprehensible / 5 – comprehensible / 6 – very comprehensible

**Q43\_WMNo\_03**) How strong do the warning influenced your decision?

1 – not at all / 2 – very little influenced / 3 – little influenced / 4 – some influenced / 5 – strongly influenced / 6 – very strongly influenced

**Q43\_WMNo\_04**) How much do you follow the warning instructions during your action?

1 – not at all / 2 – very little / 3 – little / 4 – some / 5 – much / 6 – very much

**[EQ5] Future of Internet of Things:**

**Q51)** In your opinion, how likely is the infection of IoT devices by computer viruses and Trojan horses?

1 – very unlikely / 2 – unlikely / 3 – somewhat unlikely / 4 – somewhat likely / 5 – likely / 6 – very likely

**Q52)** Do you already use such ‘intelligent’ or ‘smart’ devices?

1 - no / 2 – yes, which kind of devices + comment

**Q53)** Do you plan in the near future to purchase such ‘intelligent’ or ‘smart’ devices?

1 - no / 2 – yes, which kind of devices + comment

**[EQ6] Socio-demography:**

**Q61:** Education and profession

*Apprenticed trade, field of study, profession*

**Q62:** Sex

1 – female, 2 - male

**Q63:** Age

**Q64:** Identification number of test person

Figure 8.5: Questionnaire for test case 1 (EQ4-6)  
(Note: Text in bold angled brackets are added after the test for better readability)

## 8.1.3 Original Questionnaire

**Online-Fragebogen (Mobile Roboter Warnmeldungen)**  
Version: Februar 2017

Evaluierung einer App zur Navigation eines Serviceroboters

Bei dem Versuch ging es nicht um die Benutzerfreundlichkeit der Anwendung, sondern um die Warnmeldungen. Die Warnmeldungen werden durch das unterschiedliche Verhalten der Schadprogramme ausgelöst. Solche Schadprogramme können Viren, oder auch Trojaner sein. Je nach Verhalten des Schadprogramms und potenzieller Gefahr wurden unterschiedliche Warnungen eingeblendet.  
Diese Umfrage enthält 63 Fragen.

**[EQ1] Vorerfahrung:**

**Q11:** Wurden Sie schon einmal Opfer eines Virus/Trojaners oder einer störenden/nervenden Software? 1 - nein / 2 - ja, welche Art der Störung + Kommentar

**Q12:** Wurde ein Bekannter schon einmal Opfer eines Virus/Trojaners oder einer störenden/nervenden Software? 1 - nein / 2 - ja, welche Art der Störung + Kommentar

**Q13:** Mit welchen Geräten gehen Sie ins Internet?  
1 - PC / 2 - Tablet / 3 - Handy / 4 - andere Geräte

**Q14:** Wie oft nutzen Sie das Internet?  
6 - mehrmals täglich / 5 - einmal täglich / 4 - mehrmals wöchentlich / 3 - einmal wöchentlich / 2 - gelegentlich / 1 - selten bis nie

**[EQ2] Wissen:**

**Q21)** Haben Sie gewusst, dass es auch Viren und Trojaner für Handys und Tablet-PCs gibt?  
1 - nein / 2 - ja

**Q22)** Wissen Sie, dass es unterschiedliche Arten von Schadprogramme (z.B. Viren und Trojaner) gibt?  
1 - nein / 2 - ja, welche Schadprogramme kennen Sie bzw. welche Funktionen können diese aufweisen? + Kommentar

**Q23)** Wie stark sind Ihrer Meinung nach folgende Personen/Gruppen daran beteiligt, dass sich Viren und Trojaner verbreiten? (*Nutzer, Hersteller von Software, Hersteller von Hardware, Cyber-Kriminelle/Hacker, Staatliche Institutionen/Geheimdienste, Script Kiddies (jugendliche Computer-hacker)*)  
1 - nicht beteiligt / 2 - sehr wenig beteiligt / 3 - wenig beteiligt / 4 - weniger stark beteiligt / 5 - stark beteiligt / 6 - sehr stark beteiligt

**Q24)** Wie stark unterstützen Ihrer Meinung nach folgende Aktivitäten die Verbreitung von Viren und Trojanern? (*Download von Dateien, Öffnen eines Mail-Anhanges, Surfen im Internet, Installation von Software/Apps, Benutzen von Wechseldatenträgern (z.B. USB-Stick, gebrannte CDs/DVDs), Verlinken in sozialen Medien (Facebook, Twitter, WhatsApp, usw.), Weiterleiten in sozialen Medien (Facebook, Twitter, WhatsApp, usw.)*)  
1 - unterstützt nicht / 2 - unterstützt sehr wenig / 3 - unterstützt wenig / 4 - unterstützt weniger stark / 5 - unterstützt stark / 6 - unterstützt sehr stark

**Q25)** Für wie wahrscheinlich halten Sie es, dass vernetzte Haushaltsroboter (z.B. Staubsauger, Rasenmäher oder Spielzeugroboter) mit Viren und Trojanern infiziert werden könnten?  
1 - sehr unwahrscheinlich / 2 - unwahrscheinlich / 3 - eher unwahrscheinlich / 4 - wenig wahrscheinlich / 5 - wahrscheinlich / 6 - sehr wahrscheinlich

Figure 8.6: Original questionnaire for **test case 1 (adult-robot-interaction)** - page 1/3  
(Based on research work of Marcus Wulfänger [Wul16].)

### [EQ3] Nützlichkeit der Warnmeldungen:

**Q31)** Wieviel Spaß hat Ihnen der Umgang mit dem Roboter gemacht?

1 – keinen / 2 – sehr wenig / 3 – wenig / 4 – etwas / 5 – viel / 6 – sehr viel

**Q32)** Wie hilfreich fanden Sie die Warnmeldungen?

1 – nicht hilfreich / 2 – sehr wenig hilfreich / 3 – wenig hilfreich / 4 – eher hilfreich / 5 – hilfreich / 6 – sehr hilfreich

**Q33)** Wie sehr haben Sie die Warnmeldungen verunsichert?

6 – nicht verunsichert / 5 – sehr wenig verunsichert / 4 – wenig verunsichert / 3 – weniger stark verunsichert / 2 – stark verunsichert / 1 – sehr stark verunsichert

**Q34)** Wie sehr haben die Warnmeldungen Sie beunruhigt?

6 – gar nicht / 5 – sehr wenig / 4 – wenig / 3 – weniger stark / 2 – stark / 1 – sehr stark

**Q35)** Wie sehr hätte es Ihnen geholfen, wenn Sie ...

... eine Schritt-für-Schritt-Anleitung gehabt hätten?

... einen technisch versierten Freund, Bekannten oder Verwandten gehabt hätten?

... einen Fachmann gehabt hätten?

... ein Benutzerhandbuch verwendet hätten?

6 – gar nicht / 5 – sehr wenig / 4 – wenig / 3 – mäßig / 2 – viel / 1 – sehr viel

### [EQ4] Verständnis der Warnmeldungen:

**Q41)** Welche Gefahrenstufe würden Sie den unterschiedlichen Symbolen zuordnen?



1 – keine Gefahr / 2 – sehr geringe Gefahr / 3 – geringe Gefahr / 4 – weniger hohe Gefahr / 5 – hohe Gefahr / 6 – sehr hohe Gefahr

**Q42)** Wie würden Sie die Gefahrenstufe der Warnmeldungen einstufen?

Warnmeldung OHNE Ton und OHNE Vibration,

Warnmeldung MIT Ton und OHNE Vibration,

Warnmeldung MIT Ton und MIT Vibration.

1 – keine Gefahr / 2 – sehr geringe Gefahr / 3 – geringe Gefahr / 4 – weniger hohe Gefahr / 5 – hohe Gefahr / 6 – sehr hohe Gefahr

**Q43)** Im Versuch haben sie folgende Warnmeldung gesehen.

[Hinweis: Warnmeldung 1 – 10 wurden vor den folgenden Fragen den Probanden angezeigt.

WMNo = Warnmeldungsnummer

WMNo\_04: Nur für die Evaluationsgruppe.]

**Q43\_WMNo\_01)** Wie gefährlich empfinden Sie die in der Warnmeldung beschriebenen Situation?

1 – nicht gefährlich / 2 – sehr wenig gefährlich / 3 – wenig gefährlich / 4 – mäßig gefährlich / 5 – gefährlich / 6 – sehr gefährlich

**Q43\_WMNo\_02)** Wie verständlich war die Warnmeldung?

1 – nicht verständlich / 2 – sehr wenig verständlich / 3 – wenig verständlich / 4 – mäßig verständlich / 5 – verständlich / 6 – sehr verständlich

**Q43\_WMNo\_03)** Wie sehr hat Sie die Warnmeldung in Ihrer Entscheidung beeinflusst?

1 – nicht beeinflusst / 2 – sehr wenig beeinflusst / 3 – wenig beeinflusst / 4 – weniger stark beeinflusst / 5 – stark beeinflusst / 6 – sehr stark beeinflusst

Figure 8.7: Original questionnaire for **test case 1 (adult-robot-interaction)** - page 2/3  
(Based on research work of Marcus Wulfänger [Wul16].)

**Q43\_WMNo\_04)** Wie sehr haben Sie den Hinweis der Warnmeldung in Ihrem Handeln berücksichtigt?

1 – gar nicht / 2 – sehr wenig / 3 – wenig / 4 – weniger stark / 5 – stark / 6 – sehr stark

**[EQ5] Zukunft:**

Immer mehr Geräte werden intelligenter und sollen den Alltag erleichtern. Solche Geräte werden auch als "Internet der Dinge", kurz IoT (für Internet of Things) bezeichnet. Diese Geräte können dann z.B. mit dem Smartphone oder dem Internet kommunizieren und darüber gesteuert werden. "Intelligente" oder "smarte" Geräte können Thermostate, Lautsprecher (Amazons Echo), Licht und Rollladensteuerungen, oder auch Fernsehgeräte und Überwachungskameras, oder auch Kühlschränke sein.

**Q51)** Für wie wahrscheinlich halten Sie es, dass derartige Geräte ebenfalls von Viren und Trojaner befallen werden können?

1 – sehr unwahrscheinlich / 2 – unwahrscheinlich / 3 – eher unwahrscheinlich / 4 – wenig wahrscheinlich / 5 – wahrscheinlich / 6 – sehr wahrscheinlich

**Q52)** Nutzen Sie bereits solche "intelligenten" oder "smarten" Geräte?

1 - nein / 2 – ja, welche Geräte + Kommentar

**Q53)** Beabsichtigen Sie sich in naher Zukunft solche "intelligente" oder "smarte" Geräte zuzulegen?

1 - nein / 2 – ja, welche Geräte + Kommentar

**[EQ6] Sozio-Demographie:**

**Q61:** Ausbildung und Beruf

*Ausbildungsberuf, Studienfach, Beruf*

**Q62:** Geschlecht

1 – weiblich, 2 – männlich

**Q63:** Alter

**Q64:** Probandennummer

Vielen Dank für die Beantwortung des Fragebogens.

Figure 8.8: Original questionnaire for **test case 1 (adult-robot-interaction)** - page 3/3  
(Based on research work of Marcus Wulfänger [Wul16].)

8.1.4 Structured observation protocol

In the protocol verbal and nonverbal participant behaviour was notated (section 2.6).

Participant number: \_\_\_\_\_

Warning no.: \_\_\_\_\_  
 ignored

Problem comprehension (Degree):  
\_\_\_\_\_  
\_\_\_\_\_

Own solution:  
\_\_\_\_\_  
\_\_\_\_\_

Consequences:  
\_\_\_\_\_  
\_\_\_\_\_

Figure 8.9: Structured observation protocol for test case 1

8.1.5 Results

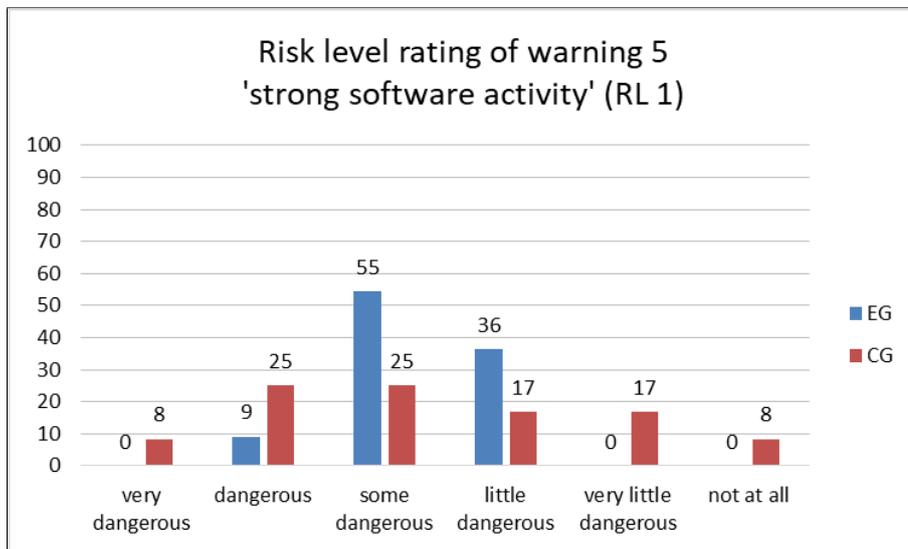


Figure 8.10: Rating results of risk level of warning 5  
(Note: X-axis: answers to question Q43.WMNo\_01  
'How dangerous do you perceived the described situation in the warning?'  
Ratings: 6:very dangerous, 5:dangerous, 4:some dangerous,  
3:little dangerous, 2:very little dangerous, 1:not at all)

## 8.1. Adults - Mobile robot warnings

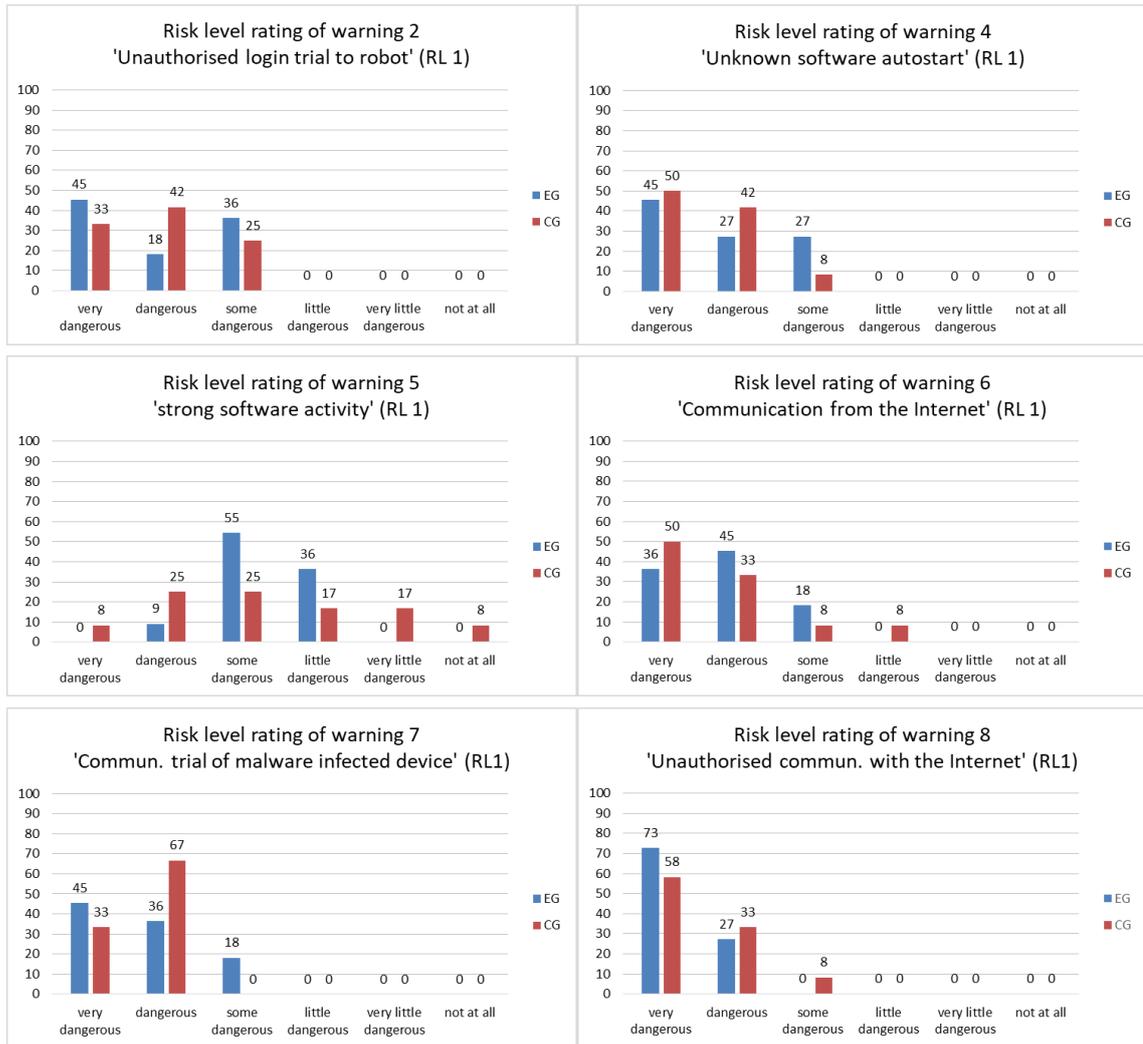


Table 8.1: Risk level ratings for warnings with risk level 1

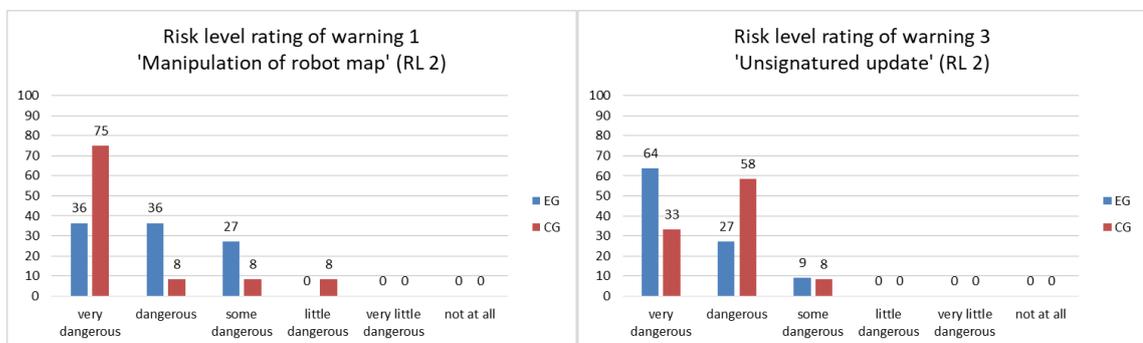


Table 8.2: Risk level ratings for warnings with risk level 2

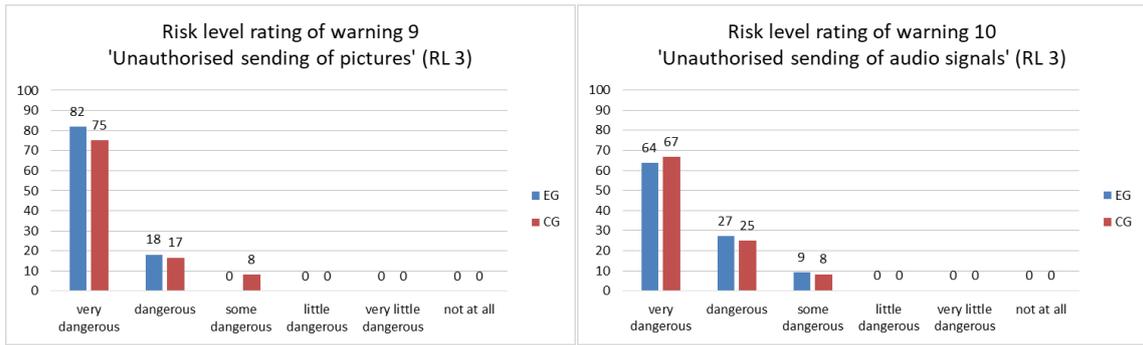


Table 8.3: Risk level ratings for warnings with risk level 3

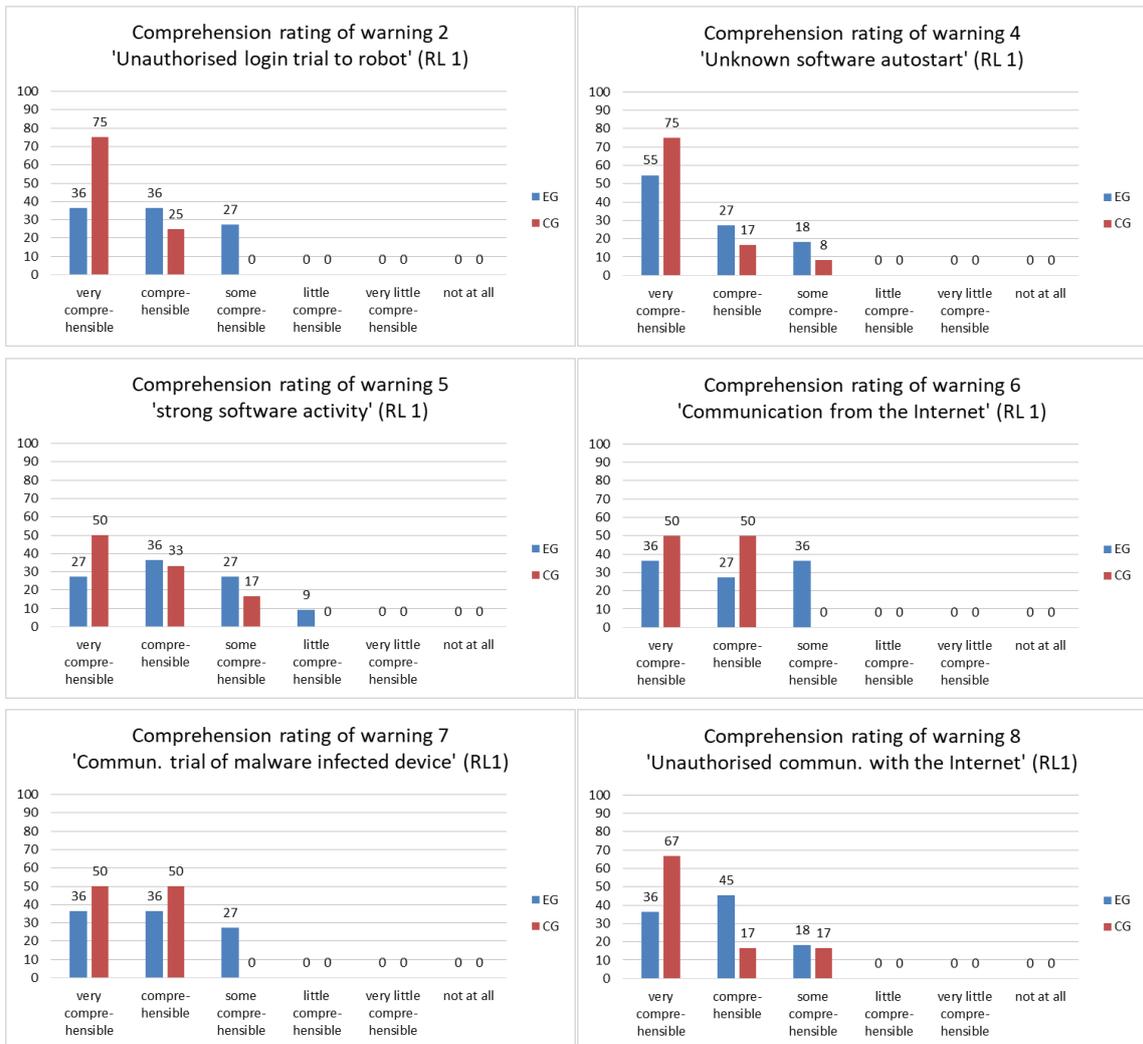


Table 8.4: Comprehension ratings for warnings with risk level 1

## 8.1. Adults - Mobile robot warnings

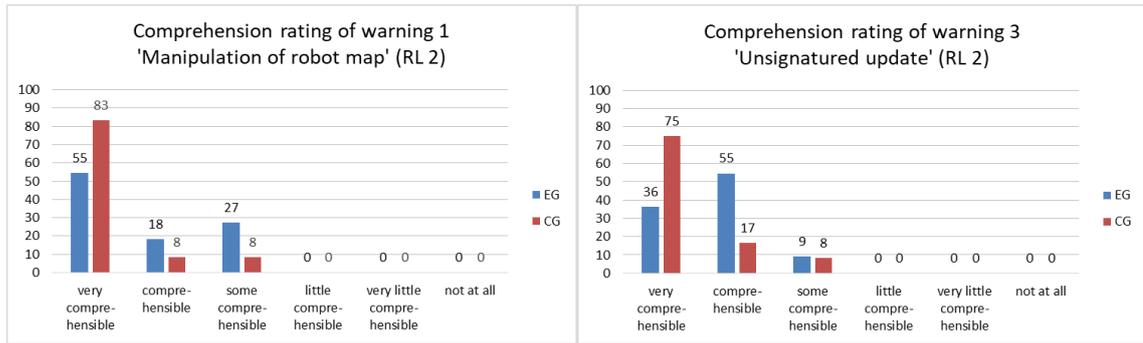


Table 8.5: Comprehension ratings for warnings with risk level 2

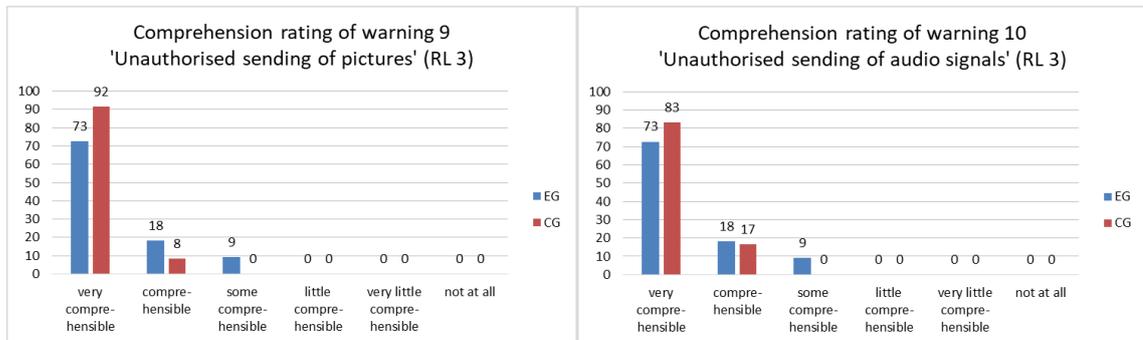


Table 8.6: Comprehension ratings for warnings with risk level 3

Warning number	Result	Two-sided significance	Significance niveau
1	.8	.003	.01
2	.823	.002	.01
3	.633	.036	.05
4	.722	.012	.05
5	.866	.001	.01
6	.667	.025	.05
7	.796	.003	.01
8	.449	.166	.166
9	.828	.002	.01
10	.904	.000	.01

Table 8.7: Two-sided correlation results according to Pearson for decision vs. reaction (EG)

Item 1	Item 2	Figure	Result	Two-sided significance	Significance niveau
Average Usefulness	Step-by-step. (Q36)	6.9	.453	.03	.05
	Tech. friend (Q36)	6.10	.618	.002	.01
	Tech. expert (Q36)	6.11	.471	.023	.05
	User guide (Q36)	6.12	.463	.026	.05
	Age (Q63)	6.14	.500	.015	.05
Test group	Tech. expert (Q36)	6.13	-.425	.043	.05
Average Comprehension	Tech. expert (Q36)	6.15	-.478	.021	.05
Average Decision	Risk level (Q43.WMNo_01)	6.16	.435	.038	.05
	Concern (Q34)	6.17	-.435	.038	.05
	Tech. expert (Q36)	6.18	-.414	.049	.05
Victim of malware (Q11)	Future IoT usage (Q53)	6.19	.564	.005	.01

Table 8.8: Two-sided correlation results according to Pearson

Item	Group	Sample size	Mean value	Standard deviation	Cohen's d	Confidence Interval (95%)
<b>Strong effects (&gt;  0.8 )</b>						
Average 'Usefulness' (8-48 points)	EG	10*	22.80	3.293	0.895	-0.003 - 1.793
	CG	11*	20.27	2.328		
Average 'Decision influence' (10-60 p.)	EG	11	52.91	4.527	8.084	4.505 - 11.663
	CG	11*	21.09	3.239		
<b>Middle effects (between  0.5  and  0.8 )</b>						
Average 'Comprehension' (10-60 p.)	EG	11	52.36	6.546	0.756	-1.603 - 0.091
	CG	12	56.42	4.010		

Table 8.9: Strong and middle effects after Cohen's d analysis  
 Comparison of experimental group (EG) and control group (CG)  
 (Note: \*: skipped single extreme values; Formula for threshold: mean value + 2\*standard deviation)

## 8.2 Children - Smartphone warnings

### 8.2.1 Questionnaire

**Questionnaire**  
(Design and evaluation of security multimedia warnings for children's smartphones)  
Version: October 2011

**In general:**

1. *How stressful was the test for you?* smiley scale 5-1 (5: stressless till 1: very stressful)

**[EQ1: Comprehension, EQ2: Warning design]**  
**During the game warning messages were displayed. There was a cartoon character which spoke to you with help of speech bubbles.**

2. *Did the cartoon character had different colours?* yes/no  
2.1 *If yes, which colours?* [comment]

**Acoustical signals and vibration in the warning messages?**

3. *Did you heard a tone?* always / sometimes / never  
3.1 *If yes, how do you like the tone?* smiley scale 3-1 (3: super till 1: bad)  
4. *Did the mobile phone vibrate?* always / sometimes / never  
4.1 *If yes, how do you like the vibration?* smiley scale 3-1 (3: super till 1: bad)

**[EQ1: Comprehension]**  
**The cartoon character in the warning messages was coloured in white, green, yellow and red.**

5. *What meanings do the colours have?*  
White: [comment]  
Green: [comment]  
Yellow: [comment]  
Red: [comment]

6.-11. These warning messages were displayed. Why they were displayed? What they mean?  
(Note: Showing warning message 1-6)  
*Why?* [comment]  
*Meaning?* [comment]

**[EQ4: Previous experiences, EQ5: Knowledge]**  
**In the experiment it was not about the game. It was about the warning messages. The warning messages should warn you for danger. Danger are for example computer viruses.**

12. *Do you know computer viruses?* yes/no  
12.1 *If yes, it is happened to you on a computer?* yes/no  
13. *Do you know, that there are computer viruses for mobile phones?* yes/no  
13.1 *If yes, it is happened to you on a mobile phone?* yes/no  
14. *Do you understand, that warning messages show if your mobile phone is in danger?* yes/no

**[EQ2: Warning design]**  
**The cartoon character in the warning messages was coloured different to show you if the iPhone was in danger.**  
smiley scale 3-1 (3: super till 1: bad)

15. *How do you like [green cartoon character icon] for "no danger"?*  
15.1 *If [bad icon], which colour is better?* [comment]  
16. *How do you like [yellow cartoon character icon] for "danger"?*  
16.1 *If [bad icon], which colour is better?* [comment]  
17. *How do you like [red cartoon character icon] for "very great danger"?*  
17.1 *If [bad icon], which colour is better?* [comment]  
18. *How do you like [white cartoon character icon] for "neutral"?*  
18.1 *If [bad icon], which colour is better?* [comment]  
19. *Your iPhone is in danger. Would you switch it off?* yes / no / no idea  
20. *Your iPhone is in danger. Do you give it to your parents?* yes / no / no idea

**(Yellow cartoon character icon) and (red cartoon character icon) look frightened.**

21. *Does it show the danger well?* yes / no / no idea

Figure 8.11: Translated questionnaire for **test case 2 (child-smartphone-interaction)** (EQ1,2,4)  
(Note: Text in bold angled brackets are added after the test for better readability. Based on questionnaire in section 8.2.2 as part of bachelor thesis of Wiebke Menzel [Men11].)

**[EQ1: Comprehension, EQ2: Warning design]**

**This green arrow [green arrow icon] should show that everything is ok.**

22. *Do you understand why the green arrow was shown?* yes / no

23. *How do you like the green arrow for "Everything is ok"?* smiley scale 3-1 (3: super till 1: bad)

**This blue lamp [blue lamp icon] should show in a dangerous situation that the message is very important.**

24. *Do you understand why the blue lamp was shown?* yes/no

25. *How do you like the blue lamp for an important message?* smiley scale 3-1 (3: super till 1: bad)

**This cartoon character is speaking to you in speech bubbles. The text is in the speech bubble.**

26. *Did you read the text?* yes / partly / no

27. *Do you understand the text?* yes / partly / no

28. *How do you like the font size?* to great / totally right / to small

29. *How do you like the text?* to short / totally right / too long

30. *All in all there are rather... very easy words / easy words / difficult words / very difficult words*

**[EQ2: Warning design]**

**Grade the warning message.**

**1 – very good, 2 – good, 3 – satisfied, 4 – sufficient, 5 – inadequate, 6 - insufficient**

31. *Cartoon character* (grade 1 - 6)

32. *Warning message* (grade 1 - 6)

**33. How do you like the warning messages? (one cross per row)**

less colourful / totally right / too colourful

helpful / annoying / nor

funny / babyish / nor

sweet / nerved / nor

[comments]

**We need your help!**

**34. How we can improve the warning messages? Do you have an idea how it can be warned for computer viruses on mobile phones? Write and draw what you come to mind!**

[Place for ideas]

**35. Our cartoon character needs a name. Can you help us!**

[Cartoon character with speech bubble with space for a comment.]

**[EQ6: Sociodemographic characteristics]**

**Questions about you**

36. *I'm ... years old.*

37. *I'm a... boy / girl*

38. *My mother tongue is... German / Others [comment]*

**[EQ4: Previous experiences]**

**No or several crosses possible.**

39. *I have an own... computer / laptop / mobile phone.*

39.1 *What kind of mobile phone do you have?* [comment]

40. *I use the... computer / laptop / mobile phone of my parents.*

40.1 *What kind of mobile phone is it?* [comment]

Figure 8.12: Translated questionnaire for **test case 2 (child-smartphone-interaction)** (EQ1,2,4,5)  
(Note: Text in bold angled brackets are added after the test for better readability. Based on questionnaire in section 8.2.2 as part of bachelor thesis of Wiebke Menzel [Men11].)

## 8.2.2 Original Questionnaire

**Fragebogen**

**Hilf uns es besser zu machen!**

Versuchs-Nummer: \_\_\_\_\_ Datum: \_\_\_\_\_

**Allgemein**

1. Wie anstrengend fandest du den Versuch?  
 ((😊): "nicht anstrengend" bis (😞): "sehr anstrengend")

**Während des Spiels wurden Warnmeldungen angezeigt. Bei den Warnmeldungen gab es eine Figur, die über eine Sprechblase mit dir gesprochen hat.**

2. Hatte die Figur unterschiedliche Farben?  Ja  Nein

2.1 Wenn ja, welche? \_\_\_\_\_

**Ton und Vibration bei den Warnmeldungen?**

3. Hast du einen Ton gehört?

3.1 Wenn ja, wie fandest du den Ton?

Immer  Manchmal  Nie

😊  😐  😞

4. Hat das Handy vibriert?

4.1 Wenn ja, wie fandest du die Vibration?

Immer  Manchmal  Nie

😊  😐  😞

Figure 8.13: Original questionnaire for **test case 2 (child-smartphone-interaction)** - page 1/9  
 (Based on bachelor thesis of Wiebke Menzel [Men11].)

Fragebogen

**Hilf uns es besser zu machen!**

---

**Die Figur in den Warnmeldungen war weiß, grün, gelb und rot.**



5. Was bedeuten die Farben?

weiß: \_\_\_\_\_

grün: \_\_\_\_\_

gelb: \_\_\_\_\_

rot: \_\_\_\_\_

---

Figure 8.14: Original questionnaire for **test case 2 (child-smartphone-interaction)** - page 2/9  
(Based on bachelor thesis of Wiebke Menzel [Men11].)

Fragebogen

Hilf uns es besser zu machen!

Diese Warnmeldungen wurden angezeigt. Warum wurden sie angezeigt? Was bedeuten sie?



6.

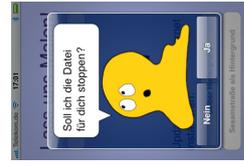
7.

Warum? \_\_\_\_\_

Bedeutung? \_\_\_\_\_

Warum? \_\_\_\_\_

Bedeutung? \_\_\_\_\_



8.

Warum? \_\_\_\_\_

Bedeutung? \_\_\_\_\_

Warum? \_\_\_\_\_

Bedeutung? \_\_\_\_\_

Figure 8.15: Original questionnaire for test case 2 (child-smartphone-interaction) - page 3/9 (Based on bachelor thesis of Wiebke Menzel [Men11].)

**Fragebogen**

**Hilf uns es besser zu machen!**

9.   

Warum? \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 Bedeutung? \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

10.   

11.  

Warum? \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 Bedeutung? \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

Figure 8.16: Original questionnaire for **test case 2 (child-smartphone-interaction)** - page 4/9  
 (Based on bachelor thesis of Wiebke Menzel [Men11].)

**Fragebogen**

**Hilf uns es besser zu machen!**

---

**Bei dem Versuch ging es nicht um ein Spiel. Es ging um die Warnmeldungen. Die Warnmeldungen sollten dich vor Gefahren warnen. Gefahren sind zum Beispiel Computer-Viren.**

12. Weißt du was Computer-Viren sind?  Ja  Nein

12.1 Wenn ja, ist dir das bei einem Computern schon passiert?  Ja  Nein

13. Weißt du, dass es Computer-Viren bei Handys gibt?  Ja  Nein

13.1 Wenn ja, ist dir das bei einem Handy schon passiert?  Ja  Nein

14. Hast du verstanden, dass die Warnmeldungen Gefahren für das Handy zeigen?  Ja  Nein

**Die Figur in den Warnmeldungen hat unterschiedliche Farben um dir zu zeigen, ob das iPhone in Gefahr ist.**

15. Wie findest du  für „Keine Gefahr“?      

15.1 Wenn , welche Farbe ist besser? \_\_\_\_\_

16. Wie findest du  für „Gefahr“?      

16.1 Wenn , welche Farbe ist besser? \_\_\_\_\_

---

Figure 8.17: Original questionnaire for **test case 2 (child-smartphone-interaction)** - page 5/9  
(Based on bachelor thesis of Wiebke Menzel [Men11].)

**Fragebogen**

**Hilf uns es besser zu machen!**

---

17. Wie findest du  für „Sehr große Gefahr“?      

17.1 Wenn , welche Farbe ist besser? \_\_\_\_\_

18. Wie findest du  für „neutral“?      

18.1 Wenn , welche Farbe ist besser? \_\_\_\_\_

19. Dein iPhone ist in Gefahr. Schaltest du es aus?  Ja  Nein  keine Ahnung

20. Dein iPhone ist in Gefahr. Gibst du es deinen Eltern?  Ja  Nein  keine Ahnung

 **und**  **sehen erschrocken aus.**

21. Zeigt das die Gefahr gut?  Ja  Nein  keine Ahnung

**Dieses grüne Häckchen  soll zeigen, dass alles in Ordnung ist.**

22. Hast du verstanden, warum es gezeigt wird?  Ja  Nein  

23. Wie findest du das grüne Häckchen für „Alles ist in Ordnung“?      

---

Figure 8.18: Original questionnaire for **test case 2 (child-smartphone-interaction)** - page 6/9  
 (Based on bachelor thesis of Wiebke Menzel [Men11].)

**Fragebogen**

**Hilf uns es besser zu machen!**

---

**Dieses Blaublicht**  soll bei Gefahr zeigen, dass die Nachricht sehr wichtig ist.

24. Hast du verstanden, warum es gezeigt wird?  Ja  Nein

25. Wie findest du das Blaublicht für eine wichtige Nachricht?      

**Die Figur spricht in den Warmmeldungen mit dir. Der Text steht in einer Sprechblase.**

26. Hast du den Text gelesen?  Ja  teilweise  Nein

27. Hast du den Text verstanden?  Ja  teilweise  Nein

27. Wie findest du die Schriftgröße?  zu groß  genau richtig  zu klein

28. Wie findest du den Text?  zu kurz  genau richtig  zu lang

29. Insgesamt gibt es eher...  sehr leichte Wörter  leichte Wörter  schwere Wörter  sehr schwere Wörter

**Gib der Warmmeldung eine Note.**

1=sehr gut    2=gut    3=befriedigend    4=ausreichend    5=mangelhaft    6=ungenügend

30. Figur  1  2  3  4  5  6

31. Warmmeldung  1  2  3  4  5  6

Figure 8.19: Original questionnaire for **test case 2 (child-smartphone-interaction)** - page 7/9  
(Based on bachelor thesis of Wiebke Menzel [Men11].)

**Fragebogen**

**Hilf uns es besser zu machen!**

---

**32. Wie gefallen dir die Warmmeldungen? (je Zeile ein Kreuz)**

<input type="radio"/> wenig bunt	<input type="radio"/> genau richtig	<input type="radio"/> zu bunt
<input type="radio"/> hilfreich	<input type="radio"/> störend	<input type="radio"/> weder noch
<input type="radio"/> lustig	<input type="radio"/> kindisch	<input type="radio"/> weder noch
<input type="radio"/> süß	<input type="radio"/> nervig	<input type="radio"/> weder noch
<input type="radio"/>	_____	_____
<input type="radio"/>	_____	_____

**Wir brauchen deine Hilfe!**

Wie können die Warmmeldungen besser werden? Hast du eine Idee wie man vor Computer-Viren auf Handys warnen kann?  
Schreibe und male was dir dazu einfällt!

---

Figure 8.20: Original questionnaire for **test case 2 (child-smartphone-interaction)** - page 8/9  
(Based on bachelor thesis of Wiebke Menzel [Men11].)

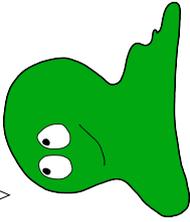
**Fragebogen**

**Hilf uns es besser zu machen!**

---

Unserer Figur fehlt noch ein Name. Kannst du ihr helfen?

Gib mir einen Namen: \_\_\_\_\_



**Fragen zu Dir**

Ich bin \_\_\_\_\_ Jahre alt.

Ich bin ein  Junge  Mädchen.

Meine Muttersprache ist  Deutsch  Andere: \_\_\_\_\_.

**Kein oder mehrere Kreuze möglich.**

Ich habe einen eigenen/ ein eigenes  Computer,  Laptop,  Handy. Was für ein Handy hast du? \_\_\_\_\_

Ich benutze den/ das  Computer,  Laptop,  Handy von meinen Eltern. Was für ein Handy ist es? \_\_\_\_\_

---

**Vielen Dank für deine Hilfe!**

Figure 8.21: Original questionnaire for **test case 2 (child-smartphone-interaction)** - page 9/9  
 (Based on bachelor thesis of Wiebke Menzel [Men11].)

8.2.3 Structured observation protocol

---

In the protocol verbal and nonverbal participant behaviour was notated (section 2.6).

Test number:	Date, time:	Page:
Event no.: _____		
Reaction:	further: _____	
<input type="checkbox"/> read through	_____	
<input type="checkbox"/> very fast (without read through)	_____	
clicked		
Comment:		
_____		
_____		
_____		
_____		
_____		
What you think? What you believe this could mean?/What's your opinion? What you would do?		

Figure 8.22: Structured observation protocol for test case 2

# 9

## Bibliography



# Bibliography

- [ACS10] Abraham, S. and Chengalur-Smith, I., *An overview of social engineering malware: Trends, tactics, and implications*, in: *Technology in Society*, vol. 32(3):(2010) 183–196. 191
- [AF13] Akhawe, D. and Felt, A.P., *Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness.*, in: *USENIX security symposium*, vol. 13 (2013). 6, 46, 47, 68, 70, 72, 75, 76, 77, 79, 80, 85, 205, 206, 207
- [AFRC14] Almuhimedi, H., Felt, A.P., Reeder, R.W., and Consolvo, S., *Your reputation precedes you: History, reputation, and the chrome malware warning*, in: *Symposium on Usable Privacy and Security (SOUPS)*, vol. 4, p. 2 (2014). 6, 46, 68, 76, 84
- [AKJ<sup>+</sup>15] Anderson, B.B., Kirwan, C.B., Jenkins, J.L., Eargle, D., Howard, S., and Vance, A., *How polymorphic warnings reduce habituation in the brain: Insights from an fMRI study*, in: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 2883–2892, ACM (2015). 47, 76, 175
- [ALC07] Asgharpour, F., Liu, D., and Camp, L.J., *Mental models of security risks*, in: *International Conference on Financial Cryptography and Data Security*, pp. 367–377, Springer (2007). 204
- [AM07] Amer, T. and Maris, J.M.B., *Signal words and signal icons in application control and information technology exception messageshazard matching and habituation effects*, in: *Journal of Information Systems*, vol. 21(2):(2007) 1–25. 81, 109
- [Ang17] Angrishi, K., *Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets*, in: *Computing Research Repository (CoRR)*, vol. abs/1702.03681, URL <http://arxiv.org/abs/1702.03681>. 14
- [AT13] Albert, W. and Tullis, T., *Measuring the user experience: collecting, analyzing, and presenting usability metrics*, Newnes (2013). 53, 56, 60
- [AVK<sup>+</sup>14] Anderson, B., Vance, T., Kirwan, B., Eargle, D., and Howard, S., *Users arent (necessarily) lazy: using neurois to explain habituation to security warnings*, in: *Thirty Fifth International Conference on Information Systems, Auckland 2014*. 19, 47, 70, 76, 82, 189, 206
- [AVK<sup>+</sup>16] Anderson, B.B., Vance, A., Kirwan, C.B., Eargle, D., and Jenkins, J.L., *How users perceive and respond to security messages: a NeuroIS research agenda and empirical study*, in: *European Journal of Information Systems*, vol. 25(4):(2016) 364–390. 76, 206
- [BB02] Bruckman, A. and Bandlow, A., *HCI for Kids*, in: J. Jacko and A. Sears, eds., *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications*, Lawrence Erlbaum and Associates (2002). 61, 111, 154
- [BB05] Barendregt, W. and Bekker, M., *Extended guidelines for usability (and fun) testing with children*, in: *Proceedings of SIGCHI. nl Conference* (2005). 61

## BIBLIOGRAPHY

---

- [BBLCF13] Bauer, L., Bravo-Lillo, C., Cranor, L.F., and Fragkaki, E., *Warning Design Guidelines*, Tech. Rep., Carnegie Mellon University, Pittsburgh, PA 15213 (2013), URL [http://www.cylab.cmu.edu/research/techreports/2013/tr\\_cylab13002.html](http://www.cylab.cmu.edu/research/techreports/2013/tr_cylab13002.html). 13, 47, 48, 49, 68, 78, 88, 109, 110, 197
- [BD06] Bortz, J. and Döring, N., *Forschungsmethoden und Evaluation*, Springer, Berlin, Heidelberg (2006), ISBN 978-3-540-33305-0, doi:10.1007/978-3-540-33306-7. 189
- [Bec09] Becher, M., *Security of smartphones at the dawn of their ubiquitousness*, Ph.D. thesis, Universität Mannheim (2009). 9, 30, 33, 35, 96, 97, 98, 100
- [Ber12] Berk, L.E., *Child Development*, Pearson, 9 edn. (2012), ISBN 978-0205149766. 51
- [BFH<sup>+</sup>11] Becher, M., Freiling, F.C., Hoffmann, J., Holz, T., Uellenbeck, S., and Wolf, C., *Mobile security catching up? revealing the nuts and bolts of the security of mobile devices*, in: *Security and Privacy (SP), 2011 IEEE Symposium on*, pp. 96–111, IEEE (2011). 26, 106
- [BFS<sup>+</sup>18] Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., and Shabtai, A., *Taxonomy of mobile users' security awareness*, in: *Computers & Security*, vol. 73:(2018) 266–293. 4, 204, 207
- [Bis02] Bishop, M., *Computer Security: Art and Science*, Addison-Wesley (2002). 28
- [BLCD<sup>+</sup>11] Bravo-Lillo, C., Cranor, L.F., Downs, J., Komanduri, S., and Sleeper, M., *Improving computer security dialogs*, in: *IFIP Conference on Human-Computer Interaction*, pp. 18–35, Springer (2011). 6, 68, 72, 73, 75, 83, 205
- [BLCDK10] Bravo-Lillo, C., Cranor, L.F., Downs, J.S., and Komanduri, S., *Bridging the gap in computer security warnings: A mental model approach*, in: *IEEE Security & Privacy*, vol. 9:(2010) 18–26, doi:10.1109/msp.2010.198. 37, 38, 47, 70, 72, 73, 75, 76, 77, 110
- [BLKC<sup>+</sup>13] Bravo-Lillo, C., Komanduri, S., Cranor, L.F., Reeder, R.W., Sleeper, M., Downs, J., and Schechter, S., *Your attention please: designing security-decision UIs to make genuine risks harder to ignore*, in: *Proceedings of the Ninth Symposium on Usable Privacy and Security*, p. 6, ACM (2013). 68, 79
- [BMS99] Byrnes, J.P., Miller, D.C., and Schafer, W.D., *Gender differences in risk taking: A meta-analysis.*, in: *Psychological bulletin*, vol. 125(3):(1999) 367. 72
- [Bol98] Boles, D., *Vorlesungsskript Multimedia-Systeme* (1998), URL <http://www.boles.de/teaching/mm/buch/node66.html>. 107
- [Bre13] Breznitz, S., *Cry wolf: The psychology of false alarms*, Psychology Press (2013). 76
- [BS10] Bortz, J. and Schuster, C., *Statistik für Human- und Sozialwissenschaftler*, Springer Medizin, Heidelberg, 7 edn. (2010), ISBN 978-3-642-12769-4. 13, 52, 55, 58, 65, 118, 158, 166, 180

- [BSI06] BSI, *Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen*, Tech. Rep., Bundesamt für Sicherheit in der Informationstechnik (2006). 25, 26, 30
- [BSI08] BSI, *BSI Standard 100-2: IT-Grundschutz Methodology*, Bundesamt für Sicherheit in der Informationstechnik (2008), URL [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard\\_100-2\\_e\\_pdf.pdf?\\_\\_blob=publicationFile&v=1](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile&v=1). 13, 28, 88, 107, 108, 204
- [BSI17] BSI, *Die Lage der IT-Sicherheit in Deutschland 2016*, Bundesamt für Sicherheit in der Informationstechnik (2017), URL [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?\\_\\_blob=publicationFile&v=5](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5). 18, 179
- [BSW09] Beutement, A., Sasse, M.A., and Wonham, M., *The compliance budget: managing security behaviour in organisations*, in: *Proceedings of the 2008 New Security Paradigms Workshop*, pp. 47–58, ACM (2009). 71
- [BV13] Bartsch, S. and Volkamer, M., *Effectively Communicate Risks for Diverse Users: A Mental-Models Approach for Individualized Security Interventions*, in: *RiskKom-Workshop, INFORMATIK 2013*, pp. 1971–1984, Gesellschaft für Informatik (2013). 2, 15, 68, 72, 73
- [BV14] Bartsch, S. and Volkamer, M., *Expert Knowledge for Contextualized Warnings*, Tech. Rep. (2014). 15, 68, 72, 74, 207
- [BVOP<sup>+</sup>09] Biddle, R., Van Oorschot, P.C., Patrick, A.S., Sobey, J., and Whalen, T., *Browser interfaces and extended validation SSL certificates: an empirical study*, in: *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 19–30, ACM (2009). 110
- [BVS07] Brustoloni, J.C. and Villamarín-Salomón, R., *Improving security decisions with polymorphic and audited dialogs*, in: *Proceedings of the 3rd symposium on Usable privacy and security*, pp. 76–85, ACM (2007). 2, 68, 77, 205
- [BVTK13] Bartsch, S., Volkamer, M., Theuerling, H., and Karayumak, F., *Contextualized web warnings, and how they cause distrust*, in: *International Conference on Trust and Trustworthy Computing*, pp. 205–222, Springer (2013). 68, 72, 73
- [Cam09] Camp, L.J., *Mental models of privacy and security*, in: *IEEE Technology and society magazine*, vol. 28(3):(2009) 37–46, doi:10.1109/mts.2009.934142. 69
- [CDC06] Cameron, K.A., Dejoy, D.M., and Cameron, K.A., *The persuasive functions of warnings: Theory and models*, in: *Handbook of warnings*, Lawrence Erlbaum Associates (2006). 40
- [CG05] Cranor, L.F. and Garfinkel, S., *Security and usability: designing secure systems that people can use*, " O'Reilly Media, Inc." (2005). 30
- [Coh77] Cohen, J., *Statistical power analysis for the behavioral sciences (revised ed.)*, Academic Press, New York (1977). 66

## BIBLIOGRAPHY

---

- [Cra08] Cranor, L.F., *A Framework for Reasoning About the Human in the Loop*, in: *Proceedings of the 1st Conference on Usability, Psychology, and Security*, UP-SEC'08, pp. 1:1–1:15, USENIX Association, Berkeley, CA, USA (2008), URL <http://dl.acm.org/citation.cfm?id=1387649.1387650>. 3, 12, 20, 37, 38, 41, 43, 44, 45, 69, 70, 71, 75, 81, 157, 191, 194
- [Dew99] Dewar, R., *Design and evaluation of public information symbols*, in: *Visual information for everyday use: Design and research perspectives*, pp. 285–303. 109
- [DHC06] Downs, J.S., Holbrook, M.B., and Cranor, L.F., *Decision strategies and susceptibility to phishing*, in: *Proceedings of the second symposium on Usable privacy and security*, pp. 79–90, ACM (2006). 47, 77
- [DIG] DIG, *Dreisprachige Internationale Grundschule Magdeburg*, URL <http://www.gs-dig.bildung-lsa.de/>. 125, 153
- [DKF<sup>+</sup>10] Dittmann, J., Karpuschewski, B., Fruth, J., Petzel, M., and Münder, R., *An Exemplary Attack Scenario: Threats to Production Engineering Inspired by the Conficker Worm*, in: *Proceedings of the First International Workshop on Digital Engineering*, IWDE '10, pp. 25–32, ACM, New York, NY, USA (2010), ISBN 978-1-60558-992-3, doi:10.1145/1837154.1837158, URL <http://doi.acm.org/10.1145/1837154.1837158>. 31, 102, 198
- [DKYT<sup>+</sup>09] De Keukelaere, F., Yoshihama, S., Trent, S., Zhang, Y., Luo, L., and Zurko, M.E., *Adaptive security dialogs for improved security behavior of users*, in: *IFIP Conference on Human-Computer Interaction*, pp. 510–523, Springer (2009). 2, 15, 17, 68, 72, 73, 174, 207
- [ECH08] Egelman, S., Cranor, L.F., and Hong, J., *You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings*, in: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pp. 1065–1074, ACM, New York, NY, USA (2008), ISBN 978-1-60558-011-1, doi:10.1145/1357054.1357219, URL <http://doi.acm.org/10.1145/1357054.1357219>. 47, 68, 71, 76, 77, 80
- [Eck08] Eckert, C., *IT-Sicherheit: Konzepte-Verfahren-Protokolle*, Oldenbourg Wissenschaftsverlag GmbH, 5. edn. (2008). 28, 46, 96
- [Ege09] Egelman, S., *Trust me: Design patterns for constructing trustworthy trust indicators*, Ph.D. thesis (2009). 47
- [EMC<sup>+</sup>10] Egelman, S., Molnar, D., Christin, N., Acquisti, A., Herley, C., and Krishnamurthi, S., *Please Continue to Hold An empirical study on user tolerance of security delays* (2010). 77, 82, 110
- [EOM09] Enck, W., Ongtang, M., and McDaniel, P., *On lightweight mobile phone application certification*, in: *Proceedings of the 16th ACM conference on Computer and communications security*, pp. 235–245, ACM (2009). 36

- [EPS08] Edwards, W.K., Poole, E.S., and Stoll, J., *Security Automation Considered Harmful?*, in: *Proceedings of the 2007 Workshop on New Security Paradigms*, NSPW '07, pp. 33–42, ACM, New York, NY, USA (2008), ISBN 978-1-60558-080-7, doi:10.1145/1600176.1600182, URL <http://doi.acm.org/10.1145/1600176.1600182>. 43
- [ES80] Ericsson, K.A. and Simon, H.A., *Verbal reports as data.*, in: *Psychological review*, vol. 87(3):(1980) 215. 53, 60
- [ES13] Egelman, S. and Schechter, S., *The importance of being earnest [in security warnings]*, in: *International Conference on Financial Cryptography and Data Security*, pp. 52–59, Springer (2013). 68, 80, 110
- [FAR<sup>+</sup>15] Felt, A.P., Ainslie, A., Reeder, R.W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., and Grimes, J., *Improving SSL warnings: Comprehension and adherence*, in: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 2893–2902, ACM (2015). 68, 70, 77, 79, 110
- [FBV<sup>+</sup>13] Fruth, J., Beskau, M., Volk, M., Meyer, A., Richter, R., and Dittmann, J., *Erster Konzeptansatz von Sicherheitstypen: Sicherheitsbewusstsein von Kindern und Jugendlichen im Umgang mit dem Internet*, in: *Informatik 2013, 43. Jahrestagung der Gesellschaft für Informatik, Workshop "Risikokommunikation im Kontext von IT-Sicherheit"*, pp. 2000–2014, Koblenz (2013). 202
- [FDOF10] Fruth, J., Dittmann, J., Ortmeier, F., and Feigenspan, J., *Metadaten-Modell für ein sicheres eingebettetes Datenmanagement*, in: P. Horster, ed., *DACH Security 2010*, pp. 359–370, Syssec (2010), ISBN 978-3-00-031441-4. 9, 96, 97, 201
- [FEF<sup>+</sup>12] Felt, A.P., Egelman, S., Finifter, M., Akhawe, D., Wagner, D. et al., *How to Ask for Permission*, in: *HotSec* (2012). 81
- [FEPS09] Fröhlich, M., Emrich, E., Pieter, A., and Stark, R., *Outcome effects and effects sizes in sport sciences*, in: *International Journal of Sports Science and Engineering*, vol. 3(3):(2009) 175–179. 66, 166
- [FKD11] Fruth, J., Krätzer, C., and Dittmann, J., *Design and Evaluation of Multi-Media Security Warnings for the Interaction between Humans and Industrial Robots*, in: *SPIE 7878, Intelligent Robots and Computer Vision XXVIII: Algorithms and Techniques, 78780K, 2011*, San Francisco Airport, CA, USA (2011), doi:10.1117/12.872846. 110, 199
- [FMD11] Fruth, J., Merkel, R., and Dittmann, J., *Security warnings for children's smart phones: A first design approach*, in: B. De Decker, J. Lapon, V. Naessens, and A. Uhl, eds., *12th Joint IFIP TC6 and TC11 Conference on "Communications and Multimedia Security" (CMS'2011), Lecture Notes in Computer Science*, vol. 7025, pp. 241–243, Springer, Berlin, Heidelberg (2011), ISBN 3-642-24711-3, doi:10.1007/978-3-642-24712-5\_24. 51
- [FMG<sup>+</sup>11] Fruth, J., Münder, R., Gruschinski, H., Dittmann, J., Karpuschewski, B., and Findeisen, R., *Sensitising to security risks in manufacturing engineering - an exemplary VR prototype*, in: *2nd International Workshop on Digital Engineering 2011*, pp. 39–44, Magdeburg (2011). 102, 201

## BIBLIOGRAPHY

---

- [FN14] Fruth, J. and Nett, E., *Uniform Approach of Risk Communication in Distributed IT Environments Combining Safety and Security Aspects*, in: O.F. Bondavalli A. Ceccarelli A., ed., *Computer Safety, Reliability, and Security - SAFECOMP 2014, 1st International workshop on the Integration of Safety and Security Engineering (ISSE14)*, pp. 298–300, Springer, Cham, Florence, Italy (2014), ISBN 978-3-319-10556-7, doi:10.1007/978-3-319-10557-4\_32. 2, 201
- [FPR17] Feierabend, S., Plankenhorn, T., and Rathgeb, T., *KIM-Studie 2017*, Medienpädagogischer Forschungverbund Südwest, Stuttgart (2017). 113
- [FSK13] Fedler, R., Schütte, J., and Kulicke, M., *On the effectiveness of malware protection on android*, in: Fraunhofer AISEC, vol. 45. 26, 35
- [FSRD13] Fruth, J., Schulze, C., Rohde, M., and Dittmann, J., *E-learning of IT Security Threats: a Game Prototype for Children*, in: B. De Decker, J. Dittmann, C. Kraetzer, and C. Vielhauer, eds., *14th Joint IFIP TC6 and TC11 Conference on "Communications and Multimedia Security" (CMS'2013), Lecture Notes in Computer Science*, vol. 8099, pp. 162–172, Springer, Berlin, Heidelberg (2013), ISBN 978-3-642-40778-9, doi:10.1007/978-3-642-40779-6\_14. 51, 114, 202, 203
- [FTKD14] Fruth, J., Thimm, M., Kuhlmann, S., and Dittmann, J., *Ein erster Prototyp - Sicherheitsguide für Grundschul Kinder beim Umgang mit dem Internet*, in: *Informatik 2014, Big Data - Komplexität meistern, 44. Jahrestagung der Gesellschaft für Informatik*, pp. 2081–2092, Stuttgart (2014). 203
- [GB94] Gardner, J.W. and Bartlett, P.N., *A brief history of electronic noses*, in: *Sensors and Actuators B: Chemical*, vol. 18(1-3):(1994) 210–211. 107
- [GDG<sup>+</sup>05] Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., and Konstan, J., *Stopping spyware at the gate: a user study of privacy, notice and spyware*, in: *Proceedings of the 2005 symposium on Usable privacy and security*, pp. 43–52, ACM (2005). 81
- [GDP16] GDPR, *General Data Protection Regulation*, European Parliament & Council (2016), URL <https://gdpr-info.eu/>. 4, 28, 97
- [GHH<sup>+</sup>18] Guo, Y., Hu, X., Hu, B., Cheng, J., Zhou, M., and Kwok, R.Y., *Mobile cyber physical systems: current challenges and future networking applications*, in: *IEEE Access*, vol. 6:(2018) 12.360–12.368. 27
- [Gie17] Gieseler, T., *Entwicklung einer Fernsteuerung eines Roboters über ein Android Tablet*, in: Bachelorarbeit, Informatik, Otto-von-Guericke-Universität Magdeburg, April (2017). 135, 138
- [GO04] Gutierrez-Osuna, R., *Olfactory interaction*, in: *In Berkshire encyclopedia of human-computer interaction*, Great Barrington, MA: Berkshire Publishing, pp. 507–511. 107
- [Gus98] Gustafsdod, P.E., *Gender Differences in risk perception: Theoretical and methodological erspectives*, in: *Risk analysis*, vol. 18(6):(1998) 805–811. 72

- [Han08] Hansen, M., *Marrying transparency tools with user-controlled identity management*, in: *The Future of Identity in the Information Society*, pp. 199–220, Springer (2008). 206
- [Har94] Hartley, J., *Designing instructional text for older readers: A literature review*, in: *British journal of educational technology*, vol. 25(3):(1994) 172–188. 204
- [Har13] Hartley, J., *Designing instructional text*, Routledge (2013). 110
- [HBRF06] Hancock, H.E., Bowles, C., Rogers, W., and Fisk, A., *Comprehension and retention of warning information*, in: *Handbook of Warnings*. Lawrence Erlbaum Associates, Mahwah, NJ, pp. 267–277. 39
- [HD14] Hoppe, T. and Dittmann, J., *Prävention, Detektion und Reaktion gegen drei Ausprägungsformen automotiver Malware*, Phd thesis, Magdeburg (2014). 14, 68, 88, 98
- [Her09] Herley, C., *So long, and no thanks for the externalities: the rational rejection of security advice by users*, in: *Proceedings of the 2009 workshop on New security paradigms workshop*, pp. 133–144, ACM (2009). 70, 72, 76, 81
- [HH09] Häder, M. and Häder, S., *Telefonbefragungen über das Mobilfunknetz*, in: Verlag für Sozialwissenschaften, München. 155
- [HHT03] Höysniemi, J., Hämäläinen, P., and Turkki, L., *Using peer tutoring in evaluating the usability of a physically interactive computer game with children*, in: *Interacting with computers*, vol. 15(2):(2003) 203–225. 63
- [HHWS14] Harbach, M., Hettig, M., Weber, S., and Smith, M., *Using personal examples to improve risk communication for security & privacy decisions*, in: *Proceedings of the SIGCHI conference on human factors in computing systems*, pp. 2647–2656, ACM (2014). 12, 68, 72, 74, 83, 107, 207
- [HKD09] Hoppe, T., Kiltz, S., and Dittmann, J., *Automotive IT-Security as a Challenge: Basic Attacks from the Black Box Perspective on the Example of Privacy Threats*, in: B. Buth, G. Rabe, and T. Seyfarth, eds., *Computer Safety, Reliability, and Security: 28th International Conference, SAFECOMP 2009, Hamburg, Germany, September 15-18, 2009*, pp. 145–158, Springer, Berlin, Heidelberg (2009), ISBN 978-3-642-04468-7, doi:10.1007/978-3-642-04468-7\_13, URL [https://doi.org/10.1007/978-3-642-04468-7\\_13](https://doi.org/10.1007/978-3-642-04468-7_13). 2, 14, 29, 35, 99
- [HPB09] Helisch, M., Pokoyski, D., and Beyer, M., *Security Awareness - Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*, Vieweg + Teubner, Wiesbaden (2009), ISBN 9783834806680. 18, 205
- [HRA97] Hanna, L., Ridsen, K., and Alexander, K., *Guidelines for usability testing with children*, in: *interactions*, vol. 4(5):(1997) 9–14. 61, 64
- [HYG+13] Han, J., Yan, Q., Gao, D., Zhou, J., and Deng, R.H., *Comparing mobile privacy protection through cross-platform applications*, in: . 33
- [HZGH+10] Hoffmeyer-Zlotnik, J.H.P., Glemser, A., Heckel, C., von der Heyde, C., Quitt, H., Hanefeld, U., Herter-Eschweiler, R., and Mohr, S., *Demographische Standards*, in: Statistisches Bundesamt: Statistik und Wissenschaft, vol. 5. 56

## BIBLIOGRAPHY

---

- [ISO07] ISO/IEC, *ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation* (2007). 201
- [ISO14] ISO, *ISO 13482: Robots and robotic devices – Safety requirements for personal care robots* (2014). 201
- [JKB<sup>+</sup>18] Jenkins, J., Kirwan, B., Bjornn, D., Anderson, B.B., and Vance, A., *How People Habituate to Mobile Security Warnings in Daily Life: A Longitudinal Field Study*, Tech. Rep., Brigham Young University (2018), URL <http://www.cl.cam.ac.uk/~rja14/shb17/vance2.pdf>. 2, 68, 70, 77, 83, 205
- [JOA03] Jürgens, S., Oberquelle, H., and Aufenanger, S., *Evaluation von world-wide-web basierten Benutzungsschnittstellen für Kinder*, in: Diplomarbeit, Fachbereich Informatik, Universität Hamburg, 2003. 110, 154
- [Kas08] Kaspersky, E., *Malware*, München: Hanser (2008). 31, 36
- [Kas17] Kaspersky Lab, *Kaspersky Security Bulletin: Kaspersky Lab Threat Predictions for 2018*, Tech. Rep., Kaspersky Lab (2017). 31
- [KGG<sup>+</sup>18] Kocher, P., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T., Schwarz, M., and Yarom, Y., *Spectre Attacks: Exploiting Speculative Execution*, in: arXiv preprint arXiv:1801.01203. 159
- [KHFD12] Kuhlmann, S., Hoppe, T., Fruth, J., and Dittmann, J., *Voruntersuchungen und erste Ergebnisse zur Webseitengestaltung für die Situationsbewusste Unterstützung von Kindern in IT-Sicherheitsfragen*, in: *Informatik 2012, 42. Jahrestagung der Gesellschaft für Informatik*, Braunschweig (2012). 202, 203
- [KLD06] Kiltz, S., Lang, A., and Dittmann, J., *Klassifizierung der Eigenschaften von Trojanischen Pferden*, in: P. Horster, ed., *DACH Security 2006 - IT Security & IT Management*, pp. 351–361, Syssec (2006). 31, 33, 35, 198
- [Kli08] Klimke, D., *Wach- & Schließgesellschaft Deutschland: Sicherheitsmentalitäten der Spätmoderne*, Springer-Verlag (2008). 202
- [KMS12] Krol, K., Moroz, M., and Sasse, M.A., *Don't work. Can't work? Why it's time to rethink security warnings*, in: *7th International conference on risk and security of internet and systems (CRiSIS)*, pp. 1–8, IEEE (2012). 68, 69, 72, 76, 78, 82, 206
- [KNB<sup>+</sup>09] Knapp, A., Neumann, M., Brockmann, M., Walz, R., and Winkle, T., *Code of Practice for the Design and Evaluation of ADAS*, in: Preventive and Active Safety Applications, eSafety for road and air transport, European Commission Integrated Project, Response, vol. 3. 12, 15, 107, 207
- [KPV<sup>+</sup>12] Kauer, M., Pfeiffer, T., Volkamer, M., Theuerling, H., and Bruder, R., *It is not about the design it is about the content! Making warnings more efficient by communicating risks appropriately*, in: N. Suri and M. Waidner, eds., *Sicherheit, LNI*, vol. 195, pp. 187–198, GI (2012), ISBN 978-3-88579-289-5. 3, 12, 15, 17, 68, 72, 74, 75, 88, 107, 174, 207

- [KSPS16] Krol, K., Spring, J.M., Parkin, S., and Sasse, M.A., *Towards robust experimental design for user studies in security and privacy*, in: *LASER Workshop 2016*, IEEE, IEEE (2016). 52, 55, 88, 179, 190
- [KSS08] Kim, H., Smith, J., and Shin, K.G., *Detecting energy-greedy anomalies and mobile malware variants*, in: *Proceedings of the 6th international conference on Mobile systems, applications, and services*, pp. 239–252, ACM (2008). 36
- [KW06] Kalsher, M.J. and Williams, K.J., *Behavioral Compliance: Theory, Methodology, and Results*, pp. 313–331, Lawrence Erlbaum Associates, Mahwah, NY (2006). 40
- [LE11] Liebal, J. and Exner, M., *Usability fuer Kids*, Vieweg+Teubner Verlag, Springer Fachmedien Wiesbaden GmbH (2011). 61, 62, 64
- [Lik32] Likert, R., *A technique for the measurement of attitudes.*, in: *Archives of psychology*. 58
- [LKK09] Lee, J.s., Kim, T.H., and Kim, J., *Energy-efficient run-time detection of malware-infected executables and dynamic libraries on mobile devices*, in: *Future Dependable Distributed Systems, 2009 Software Technologies for*, pp. 143–149, IEEE (2009). 36
- [Lou15] Loukas, G., *Cyber-Physical Attacks*, Elsevier (2015). 1, 2, 14, 27, 29
- [LSG<sup>+</sup>18] Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., Kocher, P., Genkin, D., Yarom, Y., and Hamburg, M., *Meltdown*, in: *arXiv preprint arXiv:1801.01207*. 159
- [LYZC09] Liu, L., Yan, G., Zhang, X., and Chen, S., *VirusMeter: Preventing Your Cellphone from Spies.*, in: *RAID*, vol. 5758, pp. 244–264, Springer (2009). 36
- [MA14] Modic, D. and Anderson, R., *Reading this may harm your computer: The psychology of malware warnings*, in: *Computers in Human Behavior*, vol. 41:(2014) 71–79. 6, 68, 72, 76, 84
- [May99] Mayhew, D.J., *The usability engineering lifecycle*, in: *CHI'99 Extended Abstracts on Human Factors in Computing Systems*, pp. 147–148, ACM (1999). 49, 50
- [MBG07] Maly, J., Burmester, M., and Görner, C., *Usability Testing mit Vorschulkindern*, in: *Usability Professionals*, p. 25. 61
- [Men11] Menzel, W., *Designansatz und Evaluation von Securitywarnungen für Smartphones*, in: *Bachelorarbeit, Informatik, Otto-von-Guericke-Universität Magdeburg*, Okt. (2011). 106, 124, 141, 153, 180, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233
- [Mey01] Meyer, J., *Effects of warning validity and proximity on responses to warnings*, in: *Human factors*, vol. 43(4):(2001) 563–572. 45, 68, 86, 87, 208
- [Mey04] Meyer, J., *Conceptual issues in the study of dynamic hazard warnings*, in: *Human factors*, vol. 46(2):(2004) 196–204. 68, 87, 208

## BIBLIOGRAPHY

---

- [Mil11] Miller, C., *Mobile attacks and defense*, in: IEEE Security & Privacy, vol. 9(4):(2011) 68–70. 33
- [MK07] Moosbrugger, H. and Kelava, A., *Testtheorie und Fragebogenkonstruktion*, Springer (2007). 56, 57, 58, 59
- [MMHE17] Malkin, N., Mathur, A., Harbach, M., and Egelman, S., *Personalized security messaging: Nudges for compliance with browser warnings*, in: *2nd European Workshop on Usable Security. Internet Society* (2017). 12, 68, 72, 74, 107, 207
- [MN99] Mock, M. and Nett, E., *Real-time communication in autonomous robot systems*, in: *The Fourth International Symposium on Autonomous Decentralized Systems, March 21-23, 1999, Tokyo, Japan*, pp. 34–41, The Society, Los Alamitos, Calif (1999), ISBN 0-7695-0137-0, doi:10.1109/ISADS.1999.838363. 1
- [MTF<sup>+</sup>12] Menzel, W., Tuchscheerer, S., Fruth, J., Krätzer, C., and Dittmann, J., *Design and evaluation of security multimedia warnings for children's smartphones*, in: R. Creutzburg, D. Akopian, C.G.M. Snoek, N. Sebe, and L. Kennedy, eds., *SPIE 8304, Multimedia on Mobile Devices 2012; and Multimedia Content Access: Algorithms and Systems VI*, vol. 8304, p. 83040B, Burlingame, Calif., USA (2012). 51, 114, 124, 141, 153, 180
- [Mye15] Myers, D.G., *Exploring social psychology*, McGraw-Hill New York, 7 edn. (2015). 158
- [NFHD11] Neubüser, C., Fruth, J., Hoppe, T., and Dittmann, J., *Wechselwirkungsmodell der Safety und Security*, in: *D-A-CH Security 2011: Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven*, pp. 67–78, Horster, Patrick, Prof. Dr. (2011), ISBN 978-3-00-034960-7. 14, 29
- [Nie] Nielsen, J., *Usability Inspection Methods. CHI'94. Boston, Massachusetts. April, 1994*. 52
- [Nie94] Nielsen, J., *Usability Engineering*, Morgan Kaufmann, New Edition edn. (1994). 61, 200
- [Nie10] Nielsen, J., *Children's Websites: Usability Issues in Designing for Kids* (2010), URL <http://www.nngroup.com/articles/childrens-websites-usability-issues/>. 51
- [Nok17] Nokia, *Threat Intelligence Report*, Tech. Rep. (2017), URL <https://resources.ext.nokia.com/asset/201621>. 31
- [Nor88] Norman, A.D., *The Design of Everyday Things*, Basic Books (1988). 41, 42
- [Nor02] Norman, D., *The Design of Everyday Things*, Perseus Books, Reprint edn. (2002). 82
- [NRN10] Niemann, J., Reissland, J., and Neumann, A., *Mobile Dienste im Fahrzeug: Gestaltung von Sprachausgaben zur Reduzierung visueller Ablenkung*, in: *Mensch & Computer 2010: Interaktive Kulturen, Interdisziplinäre Fachtagung*, 12.-15. September 2010, Duisburg, Germany, pp. 301–310. 155

- [NS03] Nett, E. and Schemmer, S., *Reliable Real-Time Communication in Cooperative Mobile Applications*, in: IEEE Trans. Comput., vol. 52(2):(2003) 166–180, ISSN 0018-9340, doi:10.1109/TC.2003.1176984, URL <http://dx.doi.org/10.1109/TC.2003.1176984>. 1
- [NSK<sup>+</sup>14] Neupane, A., Saxena, N., Kuruvilla, K., Georgescu, M., and Kana, R.K., *Neural Signatures of User-Centered Security: An fMRI Study of Phishing, and Malware Warnings.*, in: NDSS (2014). 76, 206
- [PD10] Preim, B. and Dachzelt, R., *Interaktive Systeme - Band 1: Grundlagen, Graphical User Interfaces, Informationsvisualisierung*, eXamen.press, 2 edn. (2010). 3, 49, 52, 88, 111
- [PD15] Preim, B. and Dachzelt, R., *Interaktive Systeme - Band 2: User Interface Engineering, 3D-Interaktion, Natural User Interfaces*, eXamen.press, 2 edn. (2015). 52, 53, 54, 55, 56, 120, 179, 190
- [Pia70] Piaget, J., *Science of education and the psychology of the child. Trans. D. Colman.*, in: . 62
- [PR97] Parasuraman, R. and Riley, V., *Humans and automation: Use, misuse, disuse, abuse*, in: Human factors, vol. 39(2):(1997) 230–253. 86
- [Ram12] Ramu, S., *Mobile malware evolution, detection and defense*, in: EECE 571B, term survey paper. 27, 36
- [RBG14] Reinfelder, L., Benenson, Z., and Gassmann, F., *Differences between Android and iPhone users in their security and privacy awareness*, in: *International Conference on Trust, Privacy and Security in Digital Business*, pp. 156–167, Springer (2014). 33, 36
- [Rea90] Reason, J., *Human Error*, Cambridge University Press (1990). 41, 42
- [RHH<sup>+</sup>11] Raja, F., Hawkey, K., Hsu, S., Wang, K.L., and Beznosov, K., *Promoting a physical security mental model for personal firewall warnings*, in: *CHI'11 Extended Abstracts on Human Factors in Computing Systems*, pp. 1585–1590, ACM (2011). 81
- [RZL13] Roman, R., Zhou, J., and Lopez, J., *On the features and challenges of security and privacy in distributed internet of things*, in: *Computer Networks*, vol. 57(10):(2013) 2266–2279. 178
- [Sad] Sadun, E., *Sourcecode to "Das große iPhone Entwicklerbuch: Rezepte für Anwendungsprogrammierung mit dem iPhone SDK"*, URL <https://github.com/erica/iphone-3.0-cookbook-/tree/master/C10-Alerts/13-Sound%20Alerts%20And%20Vibrations>, last access: 31.03.17. 143, 150
- [Sas15] Sasse, A., *Scaring and bullying people into security won't work*, in: *IEEE Security & Privacy*, vol. 13(3):(2015) 80–83. 69, 70, 72, 171
- [SBO15] Silic, M., Barlow, J., and Ormond, D., *Warning! A comprehensive model of the effects of digital information security warning messages*, Tech. Rep., Cooperation of University of St Gallen/ZSEM, California State University, and Creighton University (2015). 6, 68, 85

## BIBLIOGRAPHY

---

- [SBW01] Sasse, M.A., Brostoff, S., and Weirich, D., *Transforming the weakest linka human/computer interaction approach to usable and effective security*, in: BT technology journal, vol. 19(3):(2001) 122–131. 71
- [Sch00] Schneier, B., *Secrets and Lies: Digital Security in a Networked World*, John Wiley and Sons (2000). 37
- [SDOF07] Schechter, S.E., Dhamija, R., Ozment, A., and Fischer, I., *The emperor's new security indicators*, in: *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pp. 51–65, IEEE (2007). 45, 55, 82
- [SEA<sup>+</sup>09] Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., and Cranor, L.F., *Crying Wolf: An Empirical Study of SSL Warning Effectiveness*, in: *Proceedings of the 18th Conference on USENIX Security Symposium, SSYM'09*, pp. 399–416, USENIX Association, Berkeley, CA, USA (2009), URL <http://dl.acm.org/citation.cfm?id=1855768.1855793>. 68, 76, 77, 79, 110
- [SFH<sup>+</sup>12] Samland, F., Fruth, J., Hildebrandt, M., Hoppe, T., and Dittmann, J., *AR.Drone: security threat analysis and exemplary attack to track persons*, in: *SPIE 8301, Intelligent Robots and Computer Vision XXIX: Algorithms and Techniques, 83010G*, vol. 8301, p. 83010G (2012), doi:10.1117/12.902990, URL <http://dx.doi.org/10.1117/12.902990>. 99, 113, 114, 203
- [SH12] Sikorski, M. and Honig, A., *Practical malware analysis: the hands-on guide to dissecting malicious software*, no starch press (2012). 36
- [SK14] Seidel, T. and Krapp, A., *Pädagogische Psychologie. 6., vollständig überarbeitete Auflage* (2014). 3, 88, 107
- [Sri07] Srinivasan, R., *Protecting anti-virus software under viral attacks*, Master's thesis, Arizona State University (2007). 191
- [Sto96] Storey, N., *Safety-Critical Computer Systems*, Addison Wesley Longman Limited (1996). 29
- [Sym17] Symantec, *Internet Security Threat Report* (2017), URL <https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf>. 1
- [SZ04] Skoudis, E. and Zeltser, L., *Malware: Fighting malicious code*, Prentice Hall Professional (2004). 31, 32, 35
- [Szo05] Szor, P., *The art of computer virus research and defense*, Pearson Education (2005). 31
- [TDHK10] Tuchscheerer, S., Dittmann, J., Hoppe, T., and Krems, J., *Theoretical analysis of security warnings in vehicles and design challenges for the evaluation of security warnings in virtual environments*, in: *First International Workshop on Digital Engineering (IWDE 2010)*, pp. 33–37, Magdeburg (2010). 4, 68, 87
- [VDI00] VDI, *VDI-Standard: User-friendly design of useware (VDI/VDE 3850-1)*, VDI/VDE (2000). 12, 15, 88, 94, 107, 108, 199

- [VKBVL03] Van Kesteren, I.E., Bekker, M.M., Vermeeren, A.P., and Lloyd, P.A., *Assessing usability evaluation methods on their effectiveness to elicit verbal comments from children subjects*, in: *Proceedings of the 2003 conference on Interaction design and children*, pp. 41–49, ACM (2003). 62, 63
- [VLG15] Vuong, T.P., Loukas, G., and Gan, D., *Performance evaluation of cyber-physical intrusion detection on a robotic vehicle*, in: *IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM)*, pp. 2106–2113, IEEE (2015). 88, 98, 102, 103
- [Was10] Wash, R., *Folk models of home computer security*, in: *Proceedings of the Sixth Symposium on Usable Privacy and Security*, p. 11, ACM (2010). 204
- [WGF<sup>+</sup>87] Wogalter, M.S., Godfrey, S.S., Fontenelle, G.A., Desaulniers, D.R., Rothstein, P.R., and Laughery, K.R., *Effectiveness of warnings*, in: *Human Factors*, vol. 29(5):(1987) 599–612. 2
- [WHW09] Winner, H., Hakuli, S., and Wolf, G., *Handbuch Fahrerassistenzsysteme*, Vieweg + Teubner, Wiesbaden (2009). 12, 15, 107
- [Wog06a] Wogalter, M.S., *Communication-Human-Information Processing (C-HIP) Model*, in: Wogalter, M. S., ed., *Handbook of Warnings*, CRC Press, pp. 51–61. 70, 80, 85
- [Wog06b] Wogalter, M.S., *Handbook of Warnings (Human Factors and Ergonomics)*, CRC Press (2006), ISBN 9780805847246. 2, 3, 12, 37, 68, 86, 88, 107, 111, 197
- [Wog06c] Wogalter, M.S., *Purpose and Scope of Warnings*, in: Wogalter, M. S., ed., *Handbook of Warnings*, CRC Press, pp. 3–9. 38, 44
- [WSLZ06] Wogalter, M.S., Silver, C.N., Leonard, D.S., and Zaikina, H., *Warning symbols*, in: In Wogalter, M. S., ed., *Handbook of Warnings*, CRC Press, pp. 159–176. 200
- [Wul16] Wulfänger, M., *“Concept, implementation and evaluation of a security warning approach for cyber-physical effects on users of mobile robots”*, in: Research work, Otto-von-Guericke-University Magdeburg, Institute for Intelligent Cooperating Systems, Working group “Real time systems and communication”, Prof. Edgar Nett, Jana Fruth. 127, 138, 215, 216, 217
- [XSJ<sup>+</sup>16] Xu, M., Song, C., Ji, Y., Shih, M.W., Lu, K., Zheng, C., Duan, R., Jang, Y., Lee, B., Qian, C. et al., *Toward engineering a secure android ecosystem: A survey of existing techniques*, in: *ACM Computing Surveys (CSUR)*, vol. 49(2):(2016) 38. 33, 34
- [YGI11] Yang, L., Ganapathy, V., and Iftode, L., *Enhancing mobile malware detection with social collaboration*, in: *Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on*, pp. 572–576, IEEE (2011). 36