Prof. Dr. Thorsten Holz _ Prof. Dr. (TU NN) Norbert Pohlmann
Prof. Dr. Eric Bodden _ Prof. Dr. Matthew Smith _ Dipl.-Wi.-Ing. Jörg Hoffmann

Human-Centered Systems Security

IT Security by People for People

universitätbonn
fir an der RWTH Aachen
PADERBORN UNIVERSITY The University for the Information Society
if(is) internet-sicherheit.
hgi Horst Görtz Institut für IT-Sicherheit

Imprint

Prof. Dr. Thorsten Holz
thorsten.holz@rub.de
Horst Görtz Institut für IT-Sicherheit (HGI)
Universitätsstraße 156, 44780 Bochum
https://www.hgi.rub.de

Prof. Dr. (TU NN) Norbert Pohlmann
pohlmann@internet-sicherheit.de
Institut für Internet-Sicherheit – if(is)
Neidenburger Straße 43, 45897 Gelsenkirchen
https://www.internet-sicherheit.de

Prof. Dr. Eric Bodden
Heinz Nixdorf Institut / Universität Paderborn / Fraunhofer IEM
Zukunftsmeile 1, 33102 Paderborn
https://blogs.uni-paderborn.de/sse

Prof. Dr. Matthew Smith
Universität Bonn / Institut für Informatik 4 / Fraunhofer FKIE
Friedrich-Ebert-Allee 144, 53113 Bonn
https://net.cs.uni-bonn.de

Dipl.-Wi.-Ing. Jörg Hoffmann
joerg.hoffmann@fir.rwth-aachen.de
Forschungsinstitut für Rationalisierung (FIR) e. V. an der RWTH Aachen
Campus-Boulevard 55, 52074 Aachen
http://www.fir.rwth-aachen.de

Design | Layout:
c74 gestaltung & design, Dortmund
Cornelia Robrahn | www.c74.org

1st edition
DRUCKZENTRUM Ruhr-Universität Bochum, Bochum
www.druckzentrum.ruhr-uni-bochum.de
80 copies

Picture credits:
Titelcollage: C. Robrahn, shutterstock: ProStockStudio, Bruce Rolff, kurhan; iStock: alengo, Yakobchuk; S. 3 oben: li: Horst Görtz Institut für IT-Sicherheit (HGI), mitte: if(is) – Institut für Internet-Sicherheit, re: Frauke Döll, S. 3 unten: li: Barbara Frommann Uni Bonn, re: Jörg Hoffmann; S. 4: shutterstock: iconspro, Bruce Rolff, kurhan; iStock: alengo, Yakobchuk; S. 5,7,8,13: C. Robrahn; U4: C. Robrahn, shutterstock: iconspro, Bruce Rolff, kurhan; iStock: alengo, Yakobchuk;

Sponsored by

Ministerium für Innovation, Wissenschaft und Forschung des Landes Nordrhein-Westfalen

nrw·uniTS
IT-SICHERHEIT NORDRHEIN-WESTFALEN

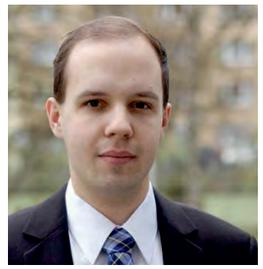
Authors

Prof. Dr. Thorsten Holz
Professor for Systems Security, Ruhr University Bochum (RUB), Horst Görtz Institute for IT-Security
thorsten.holz@rub.de

Prof. Dr. (TU NN) Norbert Pohlmann
Professor for Information Security and Director of the Institute for Internet Security – if(is), Westphalian University of Applied Sciences Gelsenkirchen
pohlmann@internet-sicherheit.de

Prof. Dr. Eric Bodden
Professor for Software Engineering at Heinz Nixdorf Institute, Paderborn University and Director for Software Engineering at Fraunhofer Research Institution for Mechatronic Systems Design (Fraunhofer IEM)
eric.bodden@uni-paderborn.de

Prof. Dr. Matthew Smith
Professor for Usable Security and Privacy, University of Bonn and Group Leader Usable Security and Privacy at Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE)
smith@cs.uni-bonn.de



Dipl.-Wi.-Ing. Jörg Hoffmann
Head of Research Unit IT Complexity Management within Department Information Management, FIR e. V. / RWTH Aachen University
joerg.hoffmann@fir.rwth-aachen.de

This research agenda was initiated by the „Round Table IT-Sicherheit NRW“ which was hosted by the Ministry for Innovation, Research and Science of the State of North-Rhine Westphalia. The research agenda has been supported by the ITS-cluster nrw.uniTS.

Information about this paper, its authors and the latest version can be found here:
www.it-sicherheit-nrw.de
As of 15 September 2016

Table of contents

Background | Purpose

Information technology is now a part of nearly all aspects of our daily lives. Whilst communication and entertainment have already been thoroughly transformed for end users by smartphones, tablets and smart TVs, other technological developments, such as smart homes, smart production and the smart grid, are on the cusp of refashioning major aspects of private and commercial life from the ground up. At the same time, the increased networking of industrial production by means of information and communications technologies poses a significant challenge *(Industry 4.0).* Economic expectations are high: these technologies will lead to the development of new business models and value chains and, at the same time, enable new service models that were previously unimaginable.

One of the most significant obstacles standing in the way of progress, however, is the existence – and increasing recognition – of real shortcomings in IT security. Despite years of intensive research and development on secure IT systems, the number of successful attacks, and their degree of severity, continues to increase with every passing year. An April 2015 study produced by the digital association Bitkom revealed that more than half (51 per cent) of all German companies have been victims of digital economic espionage, sabotage or data theft during the preceding two years, resulting in annual loses in Germany of around 51 billion euros. It is estimated that these damages will cost some 306 billion euros in coming years. Intensified digitisation and the implementation of other technological advances will only increase the vulnerability of deployed IT systems. How can this be explained, and how can we meet these threats head-on?

The authors of this research agenda have identified the *human factor* as one of the key problems when it comes to IT. Existing research initiatives in other federal states, for example, devote more attention to the secure development of hardware/software systems or to investigating the principles behind *security by design/privacy by design.* The question that has remained overwhelmingly unexamined thus far is how security mechanisms at all levels of the value chain can be designed such that relevant user groups can apply them more effectively. We believe that NRW possesses a unique strength as a location for top-quality research when it comes to this challenge. And it is an urgent one. Whilst research on IT security over the past several years has focused especially on innovative technological solutions, it is ultimately *people* who implement and utilise these solutions.

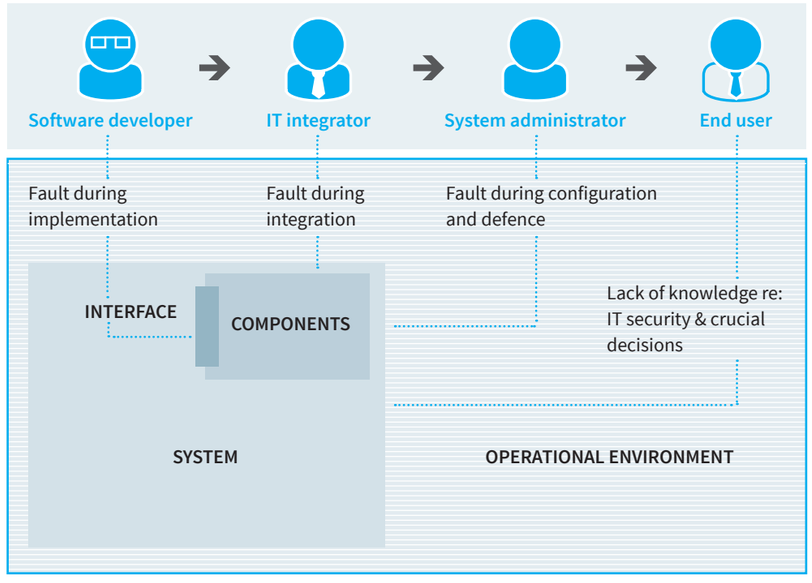


FIGURE 1: RELATIONSHIP BETWEEN INDIVIDUAL PARTIES AND POTENTIAL SECURITY PROBLEMS

It has become apparent, though, that people across all sections of the value chain are entirely overwhelmed by the security mechanisms with which they are entrusted (see Figure 1):

- **Software developers** do not have enough information to make reliable statements about the security of third-party components. In addition, they are often overwhelmed when working with important security interfaces (e.g. cryptographic libraries) and introduce faults. Similarly, a dearth

of modular security concepts makes it much more difficult to develop comprehensively secure software.

- **IT integrators** tend to be expert in their own application domains (e.g. the motor industry, mechanical engineering, public health or the chemical industry), but lack knowledge related to IT security and the integration of relevant mechanisms. Furthermore, some problems related to security are revealed only after the software has been used in a particular domain. What is needed are methods that can ensure proper adherence to all security requirements, even those that are domain-specific.
- **System administrators** must securely configure their systems and be able to reliably recognise – and counteract in an effective way – attacks on them. For the most part, though, they know far too little about both attacks and defence strategies. Their remit has, as a result, been expanded beyond classic IT functions to include the maintenance of complex IT systems in production facilities and products.
- **End users** work with IT systems in all aspects of their lives, both private and professional. They generally have absolutely no expertise in IT security, but they must nonetheless be protected from identity theft, data theft, data manipulation and other similar threats. End users face additional challenges in the form of security updates, error messages related to potential security problems, malware and other similar issues. They face an additional annoyance in the sheer number of passwords that are required, none of which may be written down or re-used. The demands placed on end users by current security strategies are simply unrealistic and, as a result, are often not met in practice. Business end users are divided into groups of normal users (e.g. industrial workers, craftsmen or office workers) and decision makers. Here, too, users must be made aware of the specific demands being made of them and trained in how to meet those demands. Managers are faced with the significant challenge of taking the appropriate decisions for their company when it comes to IT security. They need to know what rules to establish, which IT security projects should be promoted ahead of others, which risks to be aware of and how to avoid them. The overarching question is how to increase acceptance of IT security measures amongst users.

In light of the issues mentioned above, it is no surprise that the *human factor* has been the *weakest link* in the majority of successful attacks over the past several years. People have regularly played a significant part in creating the pertinent security vulnerabilities, whatever their precise role. Information technology is man-made, and it can only be as secure as the people who created it, people who must also understand the relevant security concepts. The aim of research must therefore be the development of security concepts, methods and technologies that require relevant users, wherever they may be on the value chain, to take only those decisions they are qualified to take. The research agenda presented here aligns its recommendations with this aim and outlines various areas that will benefit from research, taking into account all user groups and the challenges specific to them.

Needs assessment

Before the problems outlined above can be effectively addressed, *usability* must be systematically improved at all levels of IT security. This includes a better understanding of and accounting for the human factor in technical systems. The following examples will illustrate some of the challenges involved in this:

- An examination into how and why software developers introduce faults is needed, as is the research and development of tools to support them in creating and testing (secure) software. Automated inspection for security vulnerabilities is one major challenge. Tools that can automate the identification of potential faults must be designed and evaluated with an eye to usability.
- We must also consider how and why IT integrators introduce faults and survey the various tools and processes that will enable them to deploy secure software in their respective domains. There is also a need for research into how security solutions can be reliably integrated into existing infrastructures.
- An examination is necessary into how and why system administrators introduce faults in their respective application areas, and powerful but still usable tools must be developed to make the secure configuration of systems possible and to optimally support the administrator in meeting the challenges of IT security. When it comes to recognising and defending against attacks, more research is needed into how software can generate findings and overviews that provide direct and practical information that system administrators can use to take preventative measures, thereby limiting potential damages.
- End users require IT solutions that are tailored to their needs and easy to use and understand. The ultimate aim is the creation of security solutions that are as transparent as possible for users and which allow for sound intervention by the end user when necessary. In addition, these solutions must work in both private and business contexts, especially since existing boundaries between the two have become more blurred. End users require secure IT solutions and must understand how these are used not only for machines on the shop floor, on work computers and in business information systems, but on their smartphones and on social networks as well. In this context of growing digitisation, business decision makers must have guidelines, quantification aids and best practices available to them to be able to take the right decisions regarding secure, company-specific IT practices.

Figure 2 illustrates the interaction between various actors. Each relationship in which something is "created" or "configured" represents an action in which an original fault can be produced; the actors who "use" the components face grave challenges in correcting these faults, if they can be corrected at all. When an actor "uses" an element, its faults are brought along with it, and its use also creates the possibility of introducing new faults. Additional actors who "use" these components in subsequent steps again face significant difficulties in correcting these faults, if they can be rectified at all. What this tells us is that actors such as developers and cryptographers play a much more important role in IT security than do end users, and their errors can have much more profound effects. The red-green shading in the figure reflects this differentiated weighting. We thus consider research focused on providing assistance to these actors in their efforts to build secure and usable systems to be the most significant in terms of need.

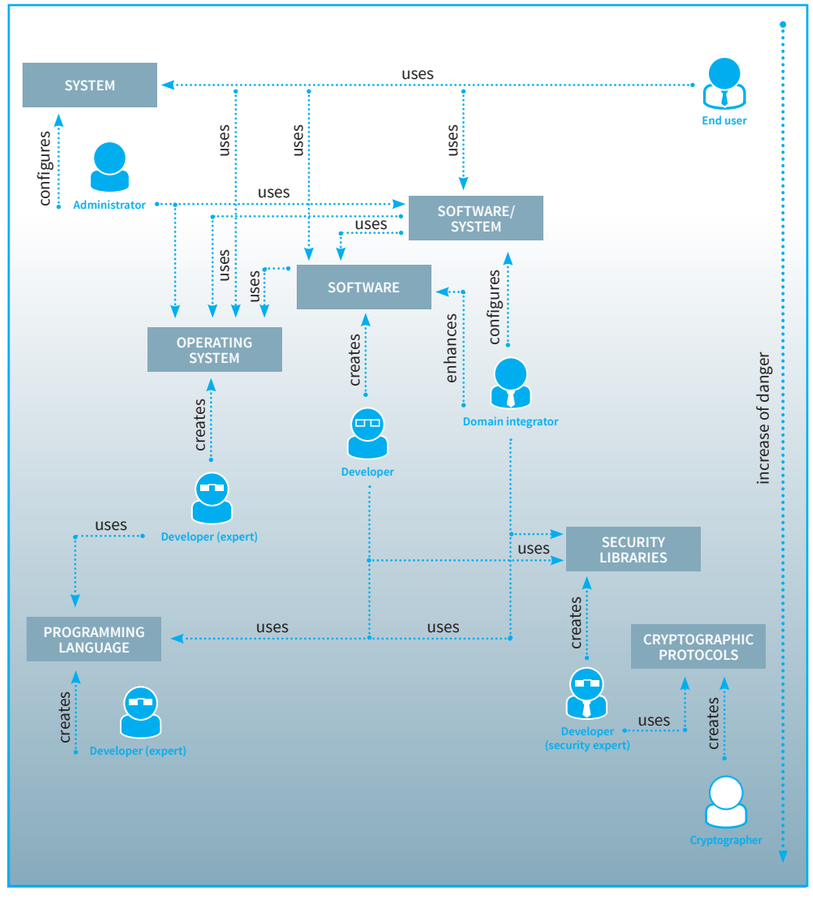
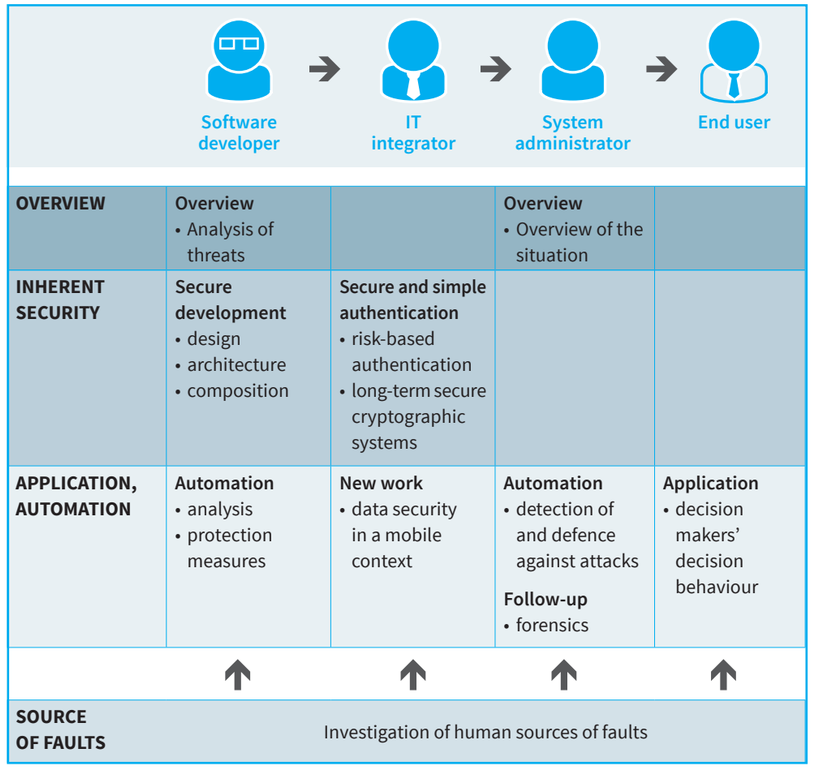


FIGURE 2:
INTERACTION AMONG VARIOUS ACTORS AND THEIR RELATIONSHIPS

Future Research Needs

FIGURE 3:
SUMMARY OF RESEARCH NEEDS RELATED TO *HUMAN-CENTRED SYSTEMS SECURITY*



The needs assessment has identified four areas in which future research is necessary and which will be outlined below. Relevant time frames are provided for each. Figure 3 provides an overview of the research needs and summarises the pertinent challenges. This assessment of future research needs is a supplement to the challenges outlined in the policy paper 'IT Security for NRW 4.0: Embracing the digital age – securely' and provides additional information about challenges in each respective area.

Software developers are the first link in IT systems' value chains. They create new software products, typically through the application of a number of existing third-party software components, which means they must be prepared to solve a complex set of problems. The crucial challenge in supporting software developers is to find a way to systematically ease the assessment and solution of the variety of problems they currently tend to encounter. The following challenges deserve particular consideration. Attention must be given to the human factor from all angles. It is with this in mind that user studies are conducted to evaluate empirically the methods under investigation:

- **Effective, reproducible analysis of threats:**
  The first step in building a secure IT system is the systematic survey of possible threats to the system. You can only protect something if you know what it is you are protecting against. To avoid missing or misjudging threats, it is important to support software architects in this work.

Methods and tools should therefore be developed that will enable reproducible analyses of threats (ideally by regular software developers). (~5 years)

- **Investigating human sources of faults in software development:**
  Faults created by developers are critical for the security of the entire ecosystem. To support developers in creating secure software, we must determine which faults arise for which reasons. A thorough examination of these reasons in particular, such as the human factor, has yet to be conducted. User studies must also be undertaken to chart the mental models and behaviours of developers. The insights gained from these studies can be used in subsequent research initiatives to eliminate these sources of faults. (5 years)
- **Secure design methodologies:**
  Software development not only involves a variety of technologies, it is also driven by a number of different human actors. In this process, the desire to create secure software is pitted against other factors, including a short time-to-market, competitive pressures, and shifting demands and technologies. The goal behind systematic design methodologies is to confront all of these factors in a controlled manner in order to discover pareto-optimal solutions. Research is also required into how to optimally increase the security of software systems even when certain factors, like those named above, serve to counteract this goal. (~5 years)
- **Secure software and system architecture:**
  Whilst many vulnerabilities exist on the level of source code, an equal number arise at the level of software architecture as a result of a flawed understanding of security concepts and the safeguards in parts of the architecture. Researchers should investigate how existing analyses of threats may provide clues on how to develop architectural structures that can deploy defence mechanisms to counteract these threats in a demonstrably secure way (assuming that these concepts have been implemented securely themselves). In this way, security requirements may be monitored and honed across a number of levels. (5 years, EFRE)
- **Secure composition:**
  Research is needed into how third-party components can be integrated securely into an existing software system. Amongst other things, interaction protocols – both required and optional – between the software as a whole and its components should be investigated and simplified when possible. A particularly important application of this research will likely be the creation of usable interfaces and protocols for the use of cryptographic processes (1-3 years, MIWF).
- **Automated analysis of software codes and models:**
  To optimally limit the costs related to the elimination of security vulnerabilities, it is essential that these vulnerabilities be discovered as early as possible in the value chain. The study of automated analyses of software artefacts and models, which should be able to identify software vulnerabilities with as little manual intervention from the software developer as possible, is a key component in this initiative.

Particular attention must also be paid to the presentation of the findings of these analyses since software developers must be able to correctly understand and interpret them. (1-5 years, MIWF/EFRE)

- **Protective mechanisms for software systems:**
  Developers may do their best to prevent vulnerabilities in their software, but it is human nature to make mistakes. This is why additional protective mechanisms are necessary to catch these types of faults and vulnerabilities. Research is needed to identify ways in which software systems can be made more secure against attack through automated means of hardening, including, for example, preventing exploitation of existing vulnerabilities. (1-3 years, EFRE/MIWF)

There are moreover a significant number of security demands related to **IT integrators.** As mentioned above, they tend to be extremely knowledgeable in their own areas but lack expertise when it comes to IT security. Thus, methods must be investigated and/or designed to ensure compliance with domain-specific security requirements. In concrete terms, there is a particular need for **identity management that is secure and easy to use,** which is a basic prerequisite for any secure system. In addition, **usable cryptographic processes that are secure over the long term** are required since cryptography is a fundamental building block for secure systems. The following thematic groups merit study:

- **Investigation into human sources of error in IT integration:**
  Faults created by IT integrators are critical for integrated systems. We need to identify which faults are introduced for which reasons if we are to support IT integrators effectively in the integration of software. Insufficient attention has been paid to studying these reasons, namely, the human factor. This would necessarily include user studies to map the mental models and behaviours of IT integrators. The findings of these studies would form the basis for subsequent research into how to eliminate these sources of the problem and develop suitable methods for supporting IT integrators. (5 years, MIWF/EFRE)
- **Risk-based means of authentication:**
  User authentication, the verification of a person's identity, is a central component in the design of many IT systems. Processes involving passwords or general knowledge-based methods are widespread, but have a number of disadvantages: passwords are easily forgotten by users; they generally have low entropy and are therefore easy to guess; they are prone to phishing attacks; and the use of a single password across a number of services can lead to a 'cascade effect', when

an attack on one service can compromise the security of a number of services. In *risk-based authentication,* log-in attempts are divided into 'unsuspicious' and 'suspicious' activities on the basis of available information.

Available information includes, for example, the IP address used and the resulting determination of the user's location, information about the software being used and installed extensions, and the time and frequency of the log-in attempts, amongst others. The process is completely invisible to the user. It can be implemented, on the one hand, to add extra security to password-based authentication and, on the other, to serve as the basis for a password-free authentication in those cases where classification is precise enough. A scientific study should improve the processes' reliability and, at the same time, increase the number of companies that will be in a position to utilise risk-based authentication and thereby enhance their users' comfort and security. (1-3 years, EFRE/MIWF)

- **Security concepts for new work environments:**
  IT systems pervade large swaths of today's work environments. This pervasiveness merits study, and new security concepts need developing if necessary security-related goals are to be met in these work environments. Mobile devices are a pertinent example in this case. These tend to be employed in diverse contexts, which results in one single device containing data, particularly access data, related to all of these diverse contexts. These data should be separated out and secured in an effective manner. (1-5 years, EFRE)
- **Effective, functional cryptographic systems that are secure over the long term:**
  All of the classic cryptographic processes currently in use are secure because solving the diverse number-theoretical problems associated with them is extremely difficult using modern computers. Quantum computers follow quantum mechanical laws and can solve the above-mentioned problems very quickly (i.e. any classic type of cryptography can be broken with the help of quantum computers). It remains unclear whether and when we will be able to build quantum computers, but leading international researchers estimate that it will be within the next 10-20 years. No practical prospects for efficient asymmetrical cryptography that would be post-quantum secure, i.e. secure in the face of quantum computers, currently exist. In the past several years, lattice-based systems have become increasingly promising, but they still lack efficiency. The currently existing alternatives are slower than traditional processes by several orders of magnitude. Over the next several years, we will require a good deal of basic mathematical research that will improve the theory behind lattice-based cryptography. This is absolutely necessary in creating secure and, at the same time, efficient cryptographic processes. (1-10 years, MIWF/DFG)

Given the complexity of current systems, the development of completely secure systems remains an impossibility. There is thus a demand for **reactive security** that can respond to security breaches in an efficient and timely manner. If we are to implement comprehensive threat management, there are three interconnecting thematic areas that demand attention: *prevention, detection and reaction.* The human factor plays a significant role here as well. **System administrators** in particular must be in a position to be able to securely configure systems and to reliably recognise attacks. Moreover, an efficient strategy for defending against attacks is needed so as to be able to react quickly to any violations of the target. In practice, however, administrators are overwhelmingly under-informed regarding attacks and about defensive strategies, which is why research initiatives geared towards supporting this user group are a necessary precursor to designing a usable threat management strategy. The following thematic areas illustrate specific concrete needs:

- **Investigation into human sources of error in IT administration:**
  Administrators' errors are critical for the systems themselves and for all of a system's users. To effectively support administrators in their software administration responsibilities, research is needed on which errors are created for which reasons. Insufficient attention has been paid to studying these reasons, again namely the human factor. This would necessarily include user studies to map the mental models and behaviours of system administrators. The findings of these studies would form the basis for subsequent research into eliminating these sources of the problem. (5 years, MIWF/EFRE)
- **Automated prevention and detection of and defence against attacks:**
  Research into how software tools can simplify system administrators' work is required. The three aspects of threat management must be taken into account. In terms of preventing threats, research is needed into how we can set up an automated, secure configuration and safeguarding of computer systems. A reliable, automated and precise detection of threats is required, on both the network level and on the level of end systems, in order to promptly uncover security incidents. An automated reaction to attacks is also highly desirable, since this would allow for a swift response to any security incident. Methods should be developed in all three areas to support system administrators in their work through the use of automated processes and in improving their reactions to an increasing number of incidents. (1-10 years, EFRE/MIWF)
- **Reliable generation of overviews of the IT situation:**
  The level of IT security within IT networks (company networks, government networks, the Internet, etc.) depends on a number of factors and is therefore difficult for system administrators to assess. As a result, this user group needs the means to quickly and easily acquire an overview of the current state of the system. Appropriate, people-centred methods and tools for the reliable generation of overviews of IT security need to be developed and tested in practice. We would also like to see the establishment of a cyber-situation room in NRW, which would be charged with creating communications overviews of the situation to be distributed to public bodies in local authorities, government departments and companies when allowable from a security standpoint. This would provide answers to questions about the state of IT systems in our connected infrastructures and help to clarify what is needed as a response.

This would also allow for anonymous comparison and improve the collective level of security over the medium and long terms. (1-3 years, EFRE)

- **Automated support for incident response/recovery and forensic analysis:**
  To facilitate the efficient response to security incidents, it will be necessary to develop people-centred forensic tools for the clarification of incidents after the fact in order to more effectively and quickly explain what occurred during attacks. Study is needed on how to gather and assess information in a manner that will allow it to be used as evidence in court. Attention must also be paid to questions of scalability and data protection. Research targeted towards developing novel and effective means of responding to security incidents, such as the automated reconfiguration of systems or network settings, is equally essential. (1-5 years, EFRE)

End users merit attention similar to that which has been given to software developers, IT integrators and system administrators. They deploy the developed systems, use IT security mechanisms to varying degrees and are therefore consumers in relation to all of the groups previously discussed. **Specifications for implementing aspects of IT security** in terms of development, implementation and administration can be discerned through study of the behaviours of various user groups. We can thereby similarly define recommendations for action regarding measures that aim to raise awareness.

- **User studies into sources of faults introduced by end users:**
  End users are users of components, software and systems. As such, they make errors, from the careless handling of data because they do not understand the associated risks to the circumvention of implemented security functions because they believe these to impede their work or because they are engaged in deliberate sabotage. An investigation into these errors in a variety of commercial and private applications is therefore necessary in order to identify the sources of these errors and to develop solutions targeted towards the above-mentioned measures. These should take all relevant user groups into account (e.g. industrial works, tradesmen, office workers and decision makers). (5 years, MIWF/EFRE)
- **Decision-making behaviour regarding IT security on the part of decision makers:**
  Decisions about security measures in industrial contexts are influenced not only by end users themselves, but also by the company's organisational and decision-making structures. Faults are also introduced here that can have a negative impact on IT security. It is necessary to examine who takes decisions, why these decisions are taken and what criteria are involved. A summary of these sources of errors is useful in the overall conceptualisation of the envisaged measures and serves to aggregate the findings in a way that is useful for industrial practice. (1-5 years, MIWF/EFRE)

Existing funding measures

The federal government published its Research Framework Programme on IT security in March 2015 under the title 'Safe, secure and empowered in the digital world'. It brings together for the first time research activities related to IT security across a number of different agencies and supports the development of secure, innovative IT solutions with a focus on practical (basic) research. The framework programme will receive around 180 million euros from the Federal Ministry of Education and Research (BMBF) through 2020. The programme has four key research focuses:
(1) new high-tech technologies for IT security,
(2) secure and trustworthy ICT systems,
(3) fields of application for IT security and
(4) privacy and the protection of data.
No priority is given to the human factor, nor is it explicitly addressed. Nonetheless, there are clear points of contact between it and the research challenges outlined in this document.

In addition to federal funding, federal states have taken numerous steps and made investments towards meeting the significant demand for research related to IT security. A number of initiatives have been launched, such as the Hessian state government's 'Commitment to Security Valley'. The centre of excellence, located in Darmstadt, is well positioned and has 34 million euros available to it for research through June 2018. Other federal states, including Bavaria, Saarland, Berlin and Baden-Württemberg, have recognised the importance of the IT security industry and IT security research and have invested millions in research initiatives. In Baden-Württemberg, for example, work has begun to transform 'Karlsruhe into the leading location for IT entrepreneurs by 2020'. Chapter four of the policy paper 'IT Security for NRW 4.0: Embracing the digital age – securely' provides an overview of current funding initiatives in other federal states. This assessment of current funding in other states clearly demonstrates that NRW needs to introduce appropriate measures to focus and expand its existing expertise in IT security.

On the European level, IT security is no longer represented as a discrete research topic in Horizon2020; the entire programme gives only marginal consideration to the subject. Some attention is given to certain topics related to IT security within the context of the 'Secure Societies' work programme, but the emphasis is instead on the implementation of prototypes, tests and demonstrators based on existing technologies. Research is often not prominently represented in these calls for bids. A public-private partnership between the European Cyber Security Organisation (ECSO) – which represents industry, users, public authorities, SMEs and associations related to cyber security – and the EU includes an agreement on a cooperative initiative related to cyber security. This partnership's overarching aim is to support the EU in fulfilling the goals set out in Horizon2020, the European Cyber Security Strategy and the Digital Single Market Strategy. Relevant aspects include, for example, funding market development, jobs, investments, development, pilots, trustworthy solutions, services and processes, awareness and more related to the field of cyber security.

The EU has dedicated 450 million euros from the Horizon2020 programme to support these activities for the period 2017-2020.

The Research Agenda in NRW

The following section provides more detail on NRW's research agenda for IT security, which aims to support the themes outlined above related to *Human-Centred Systems Security.* This research agenda provides potential measures that would contribute to the aim of expanding support for research on secure and reliable IT systems. We consider several time frames for these activities: 1-3 years, around 5 years and a longer-term time frame of around 10 years. We provide recommendations on how the identified research themes might receive support from existing funding schemes (e.g. EFRE, DFG, BMBF) and identify topics that deserve support on the basis of their significance, urgency and their contribution to the further definition of the MIWF's focus. Figure 4 provides an overview of the research themes in this section within the relevant time frame.

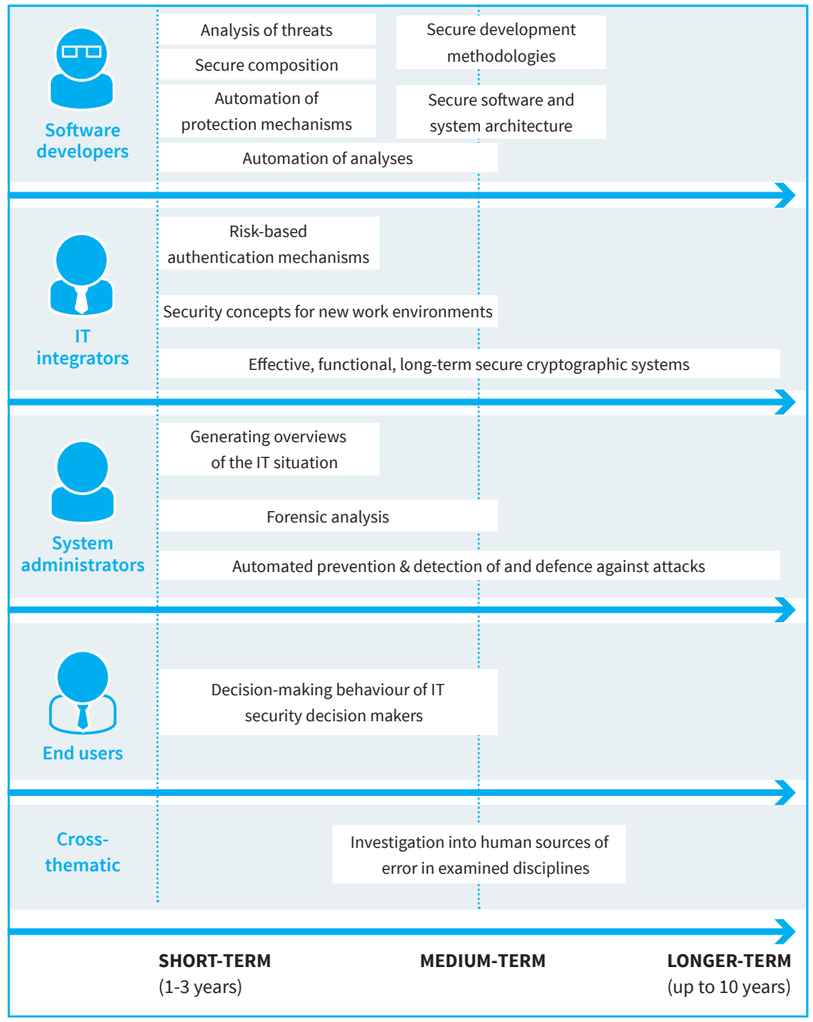


FIGURE 4: RESEARCH CHALLENGES ORGANISED BY SHORT, MEDIUM AND LONG-TERM TIME FRAMES

Short-term challenges

There is a general need for investigations into human sources of error amongst various actor groups, which requires additional studies to better understand the research need itself.

With an eye to supporting software developers, we have identified an immediate need for research on
(1) the secure composition of software artefacts,
(2) protective mechanisms for software systems and
(3) the automated analysis of software code and models. When it comes to supporting IT integrators, there is a need for
(4) security concepts for new work environments, particularly in the context of mobile applications. Administrators require support in the form of
(5) methods for automating the prevention and detection of and defence against attacks and
(6) the reliable generation of overviews of the IT situation. In the case of end users, there is a need for
(7) user studies into the sources of errors introduced by a variety of user groups and
(8) support for decision makers in companies located in NRW as they take relevant, company-specific decisions.

All of these topics urgently demand practical solutions. At the same time, research has progressed to such a degree that we can expect these solutions to materialise in the coming years.

Recommendations for initial model projects
If the above-outlined initiatives are to be implemented in a timely manner, NRW should offer support to a number of model projects. On the one hand, these projects aim to connect the most important actors in the state who are relevant to this research agenda and ensure they are on the same page. At the same time, these projects are meant to position these actors to be able to undertake additional work that addresses other aspects of the agenda and, when possible, to secure other funding for this. The research areas *Automated software analysis and Simple, usable cryptography* are perhaps best suited for these model initiatives.

Automated software analysis
The number of critical vulnerabilities found in software grows each year and there is little prospect of being able to counteract this manually. Supporting software developers in finding and avoiding these vulnerabilities is absolutely necessary. There are already a number of technical approaches that exist for searching software for security vulnerabilities, though these are not user friendly and they return a high number of false positives, which tends to seriously limit their usefulness in practice. This project brings together expertise from several locations in NRW to study techniques for automating software analysis that can be customised for human users. Researchers at a number of locations in NRW have already laid the groundwork for this effort. The *DREAM++ Decompiler,* for example, is the first malware decompiler, a tool for analysing malware, tailored for human users. In fact, DREAM++ won the *Distinguished Paper Award* at the NDSS Symposium 2015. Researchers in NRW have already developed a variety of techniques for discovering software vulnerabilities in PHP applications, Android apps or Java applications, but automated and usable analyses of software artefacts and models are still very much needed.

Simple, usable cryptography
Security vulnerabilities uncovered in the past several years, including BEAST, BREACH, CRIME, FREAK, Heartbleed and Logjam, have shown very clearly that it is not only end users who face problems when it comes to security technologies' usability. Security experts and developers in particular also make mistakes. In the above mentioned cases, software developers introduced faults whilst implementing security-critical cryptographic protocols, unwittingly introducing dangerous vulnerabilities. There is a significant demand for support from developers and usable cryptography. A joint project in this area would have the potential to network a number of locations that are important for work on IT security. There has always been a research focus on cryptography in Bochum, but there are experts on cryptographic systems in other institutions too, such as in Paderborn, where this focus is currently being expanded. Other research teams in NRW are working on methods for secure software development with a focus on the secure use of cryptographic interfaces. Research on the human factor and usable security is being conducted in Bonn. Combining expertise from several locations will facilitate research on the usability of cryptographic systems and the development of *usable* cryptography. In this way, expertise in cryptography, software development and usable security will fuse to create a new regional powerhouse in the area of *usable cryptography.*

Medium-term challenges

The following issues should not be considered less important than the themes addressed above; given the current state of scientific knowledge, only longer-term research will produce results that can be applied to these challenges. Amongst these, the most prominent is research on a more systematic and reproducible form of threat analysis. Practical usage scenarios are a key component in this work, which is why close cooperation with private industry is recommended, particularly with companies active in software and/or system development. The systematic study of human sources of error in software development is thematically related to the above, as is research on secure design methods and secure software and system architectures, which aim to prevent these errors. Basic research is needed, but this should proceed in close consultation with partner companies. This kind of collaboration is of course necessary in studies on security concepts for new work environments, but other partner companies must in this case assume a more prominent place: those that use or integrate IT systems instead of producing them. Collaboration with these partners will allow for research into human sources of error in the secure integration and administration of systems. Basic research is necessary for the development of effective and functional cryptographic systems that are secure over the long term. Research into automated support for incident response/recovery and forensic analysis should be undertaken in conjunction with companies from the IT security industry, but also with companies that administer and are responsible for monitoring those IT systems.

The key focus here is ensuring maximum coverage of the supply chain.

Longer-term challenges

Some of the identified research directions will obviously require longer time frames, particularly because many of the relevant fundamentals require additional study. This includes, for example, the themes of
(1) effective, reproducible threat analyses,
(2) secure software and system architectures and
(3) the automated prevention and detection of and defence against attacks.

Attention should be paid to these challenges as this research agenda is implemented to ensure that no one loses sight of the long-term challenges that will remain.