Key Challenges in IT Security Research

Discussion Paper for the Dialogue on IT Security

Rapid progress in the development and widespread use of IT systems is giving rise to a wide variety of new security issues. IT security providers need to come up with innovative solutions to keep pace with these developments. This paper identifies the eight most important challenges and the specific need for research they imply. Their order of appearance in this document is not intended to reflect their relative importance. We would also like to stress that a particular level of education is required across the board (university, dual education, technical college, etc.) in each of these areas. This paper does not cover options for improving education.

This paper has emerged from intensive discussions between the authors, who represent a broad variety of IT security stakeholders in academic research and industrial development. It also contains results of (roundtable) discussions in which the secUnity principal investigators participated. Therefore a lot of people not mentioned in this paper are involved and deserve credit. Version date: Decembre 2016

We invite everyone to join the dialogue and help identify the key challenges in IT security research. Please send your suggestions via E-mail or visit the discussion forum on our website:

kontakt@it-security-map.eu https://it-security-map.eu

Thank you!

secUnity
supporting the security community

Authors

Dr. Jochen Dinger, FIDUCIA & GAD IT AG, Head of IT Security Management – Banking Sector

Andreas Flach, Avira GmbH, Executive Vice President – Products & Services

Dr. Magnus Harlander, genua GmbH, Managing Director

Dr. Detlef Houdeau, Infineon AG, Senior Director Business Development

Volkmar Lotz, SAP Research, France, Head of Product Security Research

Dr. Wolfgang Klasen, Siemens AG, Head of Research Group Security for Embedded Systems

Axel Krein, Airbus Group, Senior Vice President Research & Technology

Univ.-Prof. Dipl.-Ing. Dr. techn. Reinhard Posch, TU Graz

Dr. Andreas Wespi, IBM Research Zürich, Head of IT-Security

Prof. Dr. Michael Backes, Saarland University, MPI for Software Systems, Director CISPA, secUnity PI

Prof. Dr. Peter Buxmann, TU Darmstadt, Chair of Software Business & Information Management, secUnity PI

Prof. Dr. Claudia Eckert, Fraunhofer AISEC, Director AISEC, secUnity PI

Prof. Dr. Thorsten Holz, RUB, Chair for Systems Security, secUnity PI

Prof. Dr. Jörn Müller-Quade, KIT, Chair for IT Security, Spokesman of KASTEL, secUnity PI

PD Dr. jur. Oliver Raabe, KIT, ZAR, Research Group Leader, Director FZI, secUnity PI

Prof. Dr. Michael Waidner, Fraunhofer SIT, Director SIT, Speaker of CRISP, secUnity PI

Contents

1 Security for Autonomous Systems

Self-driving cars, "intelligent" houses, and service robots are examples of new, autonomous systems. They are capable of learning, constantly evolving, and even take decisions in unforeseen situations, possibly with a critical impact on safety. During the design stage of self-learning systems, it is not completely known how the system will react later during actual use. Moreover, security and safety requirements may change. Since, however, certain guarantees are demanded (e.g. the behaviour of driver-assistance systems), safety-relevant, self-learning systems face a dilemma. This issue also involves legal questions in IT security and requires an "Ethics by Design" concept.

The design and use of autonomous systems creates new challenges for IT security which have to be addressed as quickly as possible. Mechanisms employed for sensing the external world are one potential target of attacks, since the system can be manipulated through this type of input. How can an autonomous system correctly assess the quality of data, and how can a self-learning system be protected against being simulated or taught false environments? The framework needed for autonomous systems therefore has to include IT security. Attacks are also made possible by external interfaces that provide otherwise quite desirable features — such as allowing executive authorities to stop a self-driving car by remote control.
In particular, for service robots and "intelligent" houses the creation and agreement on a reference architecture, despite the diversity of manufacturers, constitutes a first step towards obtaining a reliable model for studying the implications of autonomous systems that includes IT security.

The objective is to develop self-learning systems that meet the evolving security and safety requirements throughout their entire service life — not only at the very start of it. This requires basic research: Security levels need to be identified and defined for self-modifying systems (e.g. according to risk-based or probabilistic aspects). One possible consequence is to split a system into several independent autonomous subsystems which check each other to some extent. This requires the definition of hierarchies. To this end, it is first necessary to develop revisable systems and exchangeable software components for autonomous systems.

2 Security in Spite of Untrustworthy Components

Looking at upcoming use cases like Industry 4.0, the Internet of Things, or autonomous vehicles, highly connected embedded systems will collect and process information, and perform critical control tasks. They are mainly found in the operations domain, and not in IT, which changes the usability criteria in practice. Embedded systems are increasingly assembled from independent system components (such as microchips, operating systems, software libraries, applications, but also cloud services) which were developed for a wide span of applications.

For example, applying updates or upgrades during ongoing operations causes a strong dynamics and adds to complexity, since system characteristics and, consequently, security characteristics may change over time. In addition, the heterogeneity of the systems is increased by the large number of involved manufacturers and the use of several generations of legacy components, for some of which the manufacturers no longer provide updates. The piecemeal, and sometimes uncontrolled improvement of individual functions and components is another source of hazard. However, forbidding operators from updating software libraries, is not a viable solution either. Therefore, suitable methods and tools for system engineering need to be developed. These should be non-intrusive in order to avoid creating new potential targets.

The challenge is to design key components adequately to ensure the security characteristics for the operation of an embedded system over its entire lifetime. New system architectures must enable a dynamic, gradual adaptation of security concepts and controls in response to changing security and safety requirements. Furthermore, the development methods and system architectures to be explored should allow secure integration of untrustworthy or unchangeable system parts — even if those parts might have weaknesses. It must be possible to evaluate the current security levels in spite of such "dark spots" in the system. Finding a suitable IT security metric is essential for assessing/rating the overall system and its components (see also Issue 3).

3 Security Commensurate with Risk

“There is no such thing as 100% security.” This truism also applies to IT security and data protection. Consequently in practice one would not ask, whether a system is secure, but how secure it is. In other words, it is of interest to measure and assess security. Thus it is sought to achieve adequate security rather than security per se. This approach dominates security management, data protection management, risk management and legislation. The General Data Protection Regulation (GDPR), effective in 2018, includes a risk-based approach, which is unknown within the legislation on the protection of human dignity. Additionally, the NIS Directive of the European Union, which was adopted in 2016, regulates issues on cybersecurity in critical infrastructures and reflects the basis for security and data protection as market-relevant characteristic of IT products and services. This approach is indispensable in order to enable a manufacturer or an operator to gain a competitive advantage due to a high level of security and data protection.

There is a need for scientific methods with regard to qualitative and quantitative modelling, measuring and evaluating security and data protection in realistic systems. The first issues to be clarified are the types of incidents (e.g. attacks or successful attacks) to be taken into account and the relevant metric to use. This implies the need to develop well-founded, dynamic risk models. Due to the high complexity of real systems and their cybersecurity threats, significant support for empirical research on this subject is matter of high interest. This also includes the development of methods in order to eliminate any risks based on shared data by effectively anonymising data provided by e.g. the public health sector, banks, or insurance companies.
Research on risk balanced security must be interdisciplinary, i.e. based on cooperation between computer scientists, economists, and legal experts. Risks only arise in the context of the socio-technical system. Security arises through interactions between people and business, technology and law. A well-informed and closely coordinated approach involving technical design, the legal principles and economic evaluation is therefore essential. Can we develop technical measures and legal requirements that allow us to evaluate the chain of trust comprising the actors and components of a complex product? (See also Issue 5.)

This research aims to provide measurable security and legal compliance for IT systems and services, which can be in the long-term matter of proof based on their measurability and adaptability. One possible approach for a potential metric could focus on quantifying/classifying damages and potential damage. However, the need remains to find completely new approaches in order to discover and establish a commonly accepted IT security metric.

4 Privacy for Big Data

Big Data analytics create new challenges for privacy protection techniques that have been effective in the past. Aggregation, segregation, anonymisation, and pseudonymisation lose their protective effect when pieces of information originating from diverse sources — whilst not attributable to specific persons per se — are dynamically combined. A similar problem emerges when data is streamed (e.g. from sensors). The risk of profiles being created and supported with location data and the implied violation of privacy is increasingly becoming a critical issue. In particular, anonymisation concepts need to be reappraised according to scientific standards and redeveloped to meet these new challenges. The objective in the context of real systems is to establish an acceptable balance between usability and the risk of re-identification.

Future research and development of technical solutions in the field of privacy-preserving data processing will be a key enabler for utilising big data analytics for the benefit of society as a whole (e.g. in medical research). Citizens will be inclined to consent to processing of their data for the purpose of analysis only if concepts and technical solutions can be developed to ensure usability as well as reliable privacy protection safeguards. This calls for models and technical solutions that make communication structures and reutilisation automatisms and results behind collected data more transparent and easier to understand. These may also be demonstrated with media-savvy example studies (e.g. car sharing).

Jurisprudence must establish a foundation for a new kind of data privacy. First of all, this involves interdisciplinary cooperation in developing a threat analysis framework that also models the implications of data disclosure. Who can know what — when — and about whom must be redefined from a legal perspective. The next step will be the technical implementation of these requirements. Differences across Europe regarding ownership rights to data (e.g. in the field of health data) must be taken into account.

In the years ahead, researchers will have to develop a comprehensive scientific and technical basis for the protection of privacy within the context of a digital society. First of all, basic research efforts must be made to gain an understanding of the implications of data collation for the privacy of individuals. This makes it possible to take the second step, developing technologies to facilitate efficient protection.

These efforts can only be accomplished through interdisciplinary collaboration and they must address the following key points: Techniques for accurate privacy assessment; techniques for improved enforcement of privacy protection; methods for demonstrating to users in a comprehensible way the implications of revealing their data; development of privacy-friendly business models combining the interests of users and vendors better than currently.

5 Economic Aspects of IT Security

In addition to the further development of existing security solutions and the creation of new ones, it is also essential that persons as well as organizations should be aware of the existence of threats to security and privacy – and, ideally, behave competently and safely online. The latter is important because many citizens claim to be concerned about the violation of their privacy, especially since the revelations by former intelligence service employee Edward Snowden, but nonetheless fail to act accordingly. This discrepancy between intention and action is also called the privacy paradox. A similar paradox can be observed in many companies. Efforts to educate the public and to create awareness of digital carelessness therefore need to be greatly intensified. This applies, in particular, to imparting knowledge to young people, who are often careless with regard to how they handle their data. New concepts are needed, such as the concept of "proactive/preventive security".

An important task in organizations and companies consists of establishing efficient risk management. This risk management also includes business models supporting decisions on whether to make specific investments in IT security. This requires identifying critical parts of the system and mapping business decision processes in order to develop appropriate prioritization aids. These models should also provide specific decision-making aids based on the criticality of the decision and the corresponding industry. This is important, for instance, when we are considering critical infrastructures – e.g., in the energy or communications sector. There is still a lack of good models for measurable and quantifiable IT security which needs to be filled by further research.

Apart from raising and increasing awareness among individuals, companies, and organizations, IT security providers can and should also contribute to improving security and privacy on the net. A holistic assessment system for IT security would be necessary for company-internal decision making. The objective is to develop innovative and user-friendly IT security based on the latest insights from security research and commensurate with the requirements of users and organizations and their willingness to make expenditures. From a macroeconomic perspective, it should be considered whether and to what extent it would make sense to offer investment incentives and other support for developing new offers for vendors in Germany and Europe – particularly for small and medium-sized companies and start-ups. This also includes promoting cooperation between start-ups and academic institutions or supporting spinoffs from academic research centers for IT security.

Security could become a USP (unique selling proposition) for vendors in Europe and Germany. Since the topics of security and privacy will become increasingly important in the future, boosting the IT security economy by these means could help to enhance the competitiveness of Germany and Europe in the worldwide competition for dominance in the digital economy.

6 Behaviour-related and Human Aspects of IT Security

Security mechanisms on any level of the value chain must be designed to allow the relevant group of persons to apply them effectively. The problems are urgent, for whilst IT security research in recent years has mainly provided new technological solutions, it is, after all, humans who utilise and apply those solutions. However, it is apparent on all levels of the value chains that people today are unable to cope with the security mechanisms entrusted to them. Software designers, for example, cannot make well-informed statements on security-related matters concerning third-party components; they are, moreover, often out of their depth regarding the use of important security interfaces (e.g. crypto libraries) and make mistakes. Furthermore, the lack of modular security concepts impedes them from creating secure software encompassing entire systems. System administrators must be able to ensure the security of systems by means of configuration and to reliably detect attacks and counter them effectively. In most cases, however, they know far too little about attacks or defence strategies. At the same time, their area of responsibility has evolved from traditional IT operations to managing complex IT systems in manufacturing facilities and products. As a result, it is no wonder that, due to the problems described above, in most of the successful attacks in recent years, it has been the human factor as the weakest link in the chain that has played a significant role in generating the relevant security gaps. Information technology is shaped by humans and can only be secure to the same degree as the people shaping it understand its safety concepts.

These problems cannot be addressed effectively unless usability is systematically improved at all levels of IT security. For this purpose, the human factor within technical systems needs to be better understood and taken into account in order to increase system resilience to operator errors. The role and the rights of the person concerned also need to be considered. Research must therefore aim to develop security concepts, methods, and technologies that, at all levels of the value chain, only require decisions from persons that they are qualified to make. Can we develop technical and legal measures providing for a market-adequate evaluation and certification of the chain of trust comprising the actors and components of a complex product? (See also Issue 3)

7 Security of Cryptographic Systems against Powerful Attacks

Cryptographic procedures currently regarded as secure can be threatened by new forms of attacks as well as resource-heavy bruteforce attacks. Threats posed by quantum computers and side-channel attacks are already being discussed. The research on quantum computers is receiving significant support all over the world, including in the EU. If a breakthrough should be achieved, most encryption and signature procedures will no longer be safe. The investigation and development of new types of cryptographic algorithms resilient to quantum attacks is therefore indispensable for any future IT infrastructure and must be advanced further. The first implementations and countermeasures in this area should be studied and expanded. Quantum technology can also be used to protect confidentiality. Various standardisation committees (such as NIST), have already recognised the issue and called for the development of a new, efficient generation of public-key cryptography that will resist quantum computers. This is all the more important in order to ensure a timely transition. Particular attention should be given to the cryptographic protection of archives — for the long or short term.
Furthermore, it has been shown that cryptography can be bypassed using side channels in software and hardware and must therefore be designed with an adequate level of security. Cryptanalysis is currently carried out using expensive laser technology, but also with simple, readily-available devices for, e.g., power consumption analysis. Protection is by now quite effective against the means of attack that have become cheaper and cheaper within the past 15 years. However, attacks using newly developed, expensive measuring and laser technologies require constant attention.

In order to achieve long-term security, this research aims at developing mechanisms (algorithms, software, and hardware) which will still be secure against future attacks (e.g. by quantum computers or side channels). In the interest of the long-term adequacy of implemented security measures, progress expected for the next few years has to be taken into account now.

8 Detection and Reaction

There is no such thing as 100% prevention. As a consequence, networks and IT systems should not be operated without elaborate mechanisms for detection, reaction, and recovery. For detection, methods from machine learning are being investigated and are considered a promising approach. This approach was also taken up by DARPA in 2016: The objective of their Cyber Grand Challenge was to find and eliminate safety gaps in software automatically for the first time, using unmanned Cyber Reasoning Systems. Several successful teams came up with innovative solutions for this difficult problem. These efforts are bringing a new quality to IT safety, as previously any search for such security gaps had to be performed "manually". These techniques also facilitate a quicker response to attacks.
Automated attacks create a new type of continuous threat that leaves conventional anti-virus software defenceless. Moreover, even manual attacks have become so frequent that they urgently require new solutions and countermeasures. Research should therefore focus not only on finding security gaps, but also on the real-time detection of unknown attacks ("intrusion detection") and on effective countermeasures.

The promising recent progress in the domains of artificial intelligence and machine learning ("deep learning") allows for an innovative research approach for automated protection against security gaps and a large variety of attack types.
An intermediate step on the way to fully automated solutions is the development of semi-automated alarm systems for networks. In this context, machine learning can support decision-making through attack assessment and can already suggest response options. The opportunities offered by machine learning systems have yet to be further studied and expanded in order to facilitate automatically and autonomously responding alarm systems in the future.

The aim is to develop automatic defence systems that are able to detect and eliminate safety gaps quickly and reliably. One of the challenges is to teach the machine learning system to differentiate between attack and normal operation reliably for its entire service life. In particular, situations where attackers try to train the machine learning system have to be identified in time and reflected in new security rules. Since attackers themselves can, of course, use self-learning systems against other self-learning systems/classifiers, machine learning should also be protected against this possibility.

We invite everyone to join the dialogue and help identify the key challenges in IT security research. Please send your suggestions via E-mail or visit the discussion forum on our website:

kontakt@it-security-map.eu https://it-security-map.eu

Thank you!

secUnity
supporting the security community