Cybersecurity Research:

Challenges and Course of Action

secUnity

supporting the security community

https://it-security-map.eu

SPONSORED BY THE

Federal Ministry of Education and Research

Cybersecurity Research: Challenges and Course of Action

secUnity-Roadmap on Cybersecurity Research

The European society faces numerous disruptive changes due to the progressing digitalisation. These changes have the potential to lead to a fair digitalised world if they are based on the ideal of digital sovereignty as a guiding principle at the citizen, economic and state levels. Research in cybersecurity creates the technological prerequisites for addressing the challenges of digitalisation in this spirit.

Researchers in academia and industry from all over Europe met in Darmstadt and Berlin to identify the main challenges of cybersecurity research. Irrespective of their scientific backgrounds, all authors agreed that effective security and privacy measures require a systematic and holistic approach which considers security and privacy from the ground up. They stressed that in addition to the proposed research agenda, it is necessary to improve education across the board. During the discussions, it became also clear that various important scientific questions remain open, and that only long-term research across all disciplines can solve these problems.

In the first chapter, we outline the major challenges in the fundamental research of the IT security fields in computer and engineering sciences. In the second chapter, we look at the cybersecurity challenges from the perspective of economic, legal and social sciences. In the last chapter, we analyse various examples of applications and technologies which combine the different research areas. Each section of the roadmap is dedicated to a specific challenge. The order of the sections is not intended to reflect their relative importance. For each challenge, we propose concrete next steps based on the state of the art in the scientific and industrial research landscape.

We hope to reach out to all interested parties who endeavour to strengthen cybersecurity and enhance digital sovereignty in Europe.

Thank you!

Jörn Müller-Quade
Spokesman of secUnity
On behalf of the authors

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

secUnity
supporting the security community

Authors

secUnity – Principal Investigators

Prof. Michael Backes, CISPA Helmholtz Center for Information Security, Chairman & Scientific Director

Prof. Peter Buxmann, TU Darmstadt, Chair of Information Systems, Software & Digital Business Group

Prof. Claudia Eckert, Fraunhofer AISEC, Director, and Technical University of Munich, Chair of IT Security

Prof. Thorsten Holz, RUB, Chair of Systems Security, HGI

Prof. Jörn Müller-Quade, KIT, Chair of Cryptography and IT Security, Spokesman of KASTEL

PD Dr. iur. Oliver Raabe, KIT, ZAR, Research Group Leader, Director FZI

Prof. Michael Waidner, Fraunhofer SIT, Director SIT, CEO National Research Center for Applied Cybersecurity CRISP

Invited Experts

Dr. Sébastien Bardin, CEA LIST, Software Safety and Security Laboratory, France

Prof. Hervé Debar, Télécom-SudParis, Head of Networks and Security Department, EUNITY, France

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

Prof. Sascha Fahl, RUB, Chair of Usable Security and Privacy, Germany

Prof. Sebastian Faust, TU Darmstadt, Chair of Applied Cryptography, Germany

Prof. Gloria Gonzalez Fuster, VUB, Law Science Technology & Society, Belgium

Prof. Stjepan Groš, Univ. of Zagreb, Head of Laboratory for Information Security and Privacy, Croatia

Dr. Joseph Hallett, Univ. of Bristol, CyBOK, Great Britain

Dr. Magnus Harlander, genua GmbH, Shareholder, Germany

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

Dr. Claude Kirchner, INRIA, France

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

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

Prof. Evangelos Markatos, Univ. of Crete, Head of the Distributed Computing Systems Laboratory, FORTH, Greece

Peter Möhring, Giesecke & Devrient, Managing Head of Security Network Munich, Germany

Prof. Reinhard Posch, TU Graz, Head of IAIK, Scientific Director of A-SIT, Austria

Steve Ritter, Federal Office for Information Security, Head of Section IT-Security and Law

Martin Schallbruch, ESMT Berlin, Deputy Director of Digital Society Institute (DSI), and Visiting Fellow at Hoover Institution, Stanford University

Dr. Matthias Schunter, Intel, Principal Engineer, Intel Labs, Germany

Prof. Melanie Volkamer, KIT, Chair of Security – Usability – Society, Germany

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

secUnity – Project Team

Adrian Engelbrecht, TU Darmstadt, Software & Digital Business Group, Research Associate
Andreas Fuchs, Fraunhofer SIT, Deputy Head of Dep. Cyber-Physical Systems Security
Dr. Willi Geiselmann, KIT, Inst. f. Theor. Informatics, Research Associate
Dr. Anna-Louise Grensing, KIT, Inst. f. Theor. Informatics, Project Coordinator secUnity
Margareta Heidt, TU Darmstadt, Software & Digital Business Group, Research Associate
Dr. Johann Heyszl, Fraunhofer AISEC, Head of Hardware Security Department
Dr. Matthias Hiller, Fraunhofer AISEC, Head of Physical Security Technologies Group
Lukas Jäger, Fraunhofer SIT, Research Associate
Claudia Kawohl, Saarland Univ., Information Security & Cryptography, Research Associate
Alexander Koch, KIT, Inst. f. Theor. Informatics, Research Associate
Annika Krämer, Saarland Univ., Information Security & Cryptography, Research Associate
Ninja Marnau, CISPA Helmholtz Center for Information Security, Senior Researcher
Kathrin Noack, KIT, Inst. f. Theor. Informatics, Project Coordinator secUnity
Dr. Roland Rieke, Fraunhofer SIT, Research Associate
Daniel Senf, Fraunhofer SIT, Research Associate
Markus Springer, Fraunhofer SIT, Research Associate
Anne Steinbrück, KIT, ZAR, Research Associate
Dr. Mario Strefler, KIT, Inst. f. Theor. Informatics, Project Coordinator KASTEL
Dennis Tatang, Ruhr University Bochum (RUB), Systems Security, Research Associate

Contents

A. Key Challenges

The advancements in digital technology affect and change the economic, industrial and social environment. They cover the entire value chain in IT starting at circuit level, through to services and analytics in the cloud. The rapid deployment of new technologies e.g., in the Internet of Things (IoT), and increased interconnectedness enable new opportunities. However, this also leads to new attack vectors and, in turn, challenges researchers across Europe.

The increasing pace and impact of cyber attacks show that current design principles have to be altered to enable security by design. This chapter highlights the key issues that span across traditional and emerging areas of cybersecurity research.

In the following sections, we outline the main challenges in each area and propose a course of action in three phases:

- ▷ Short-term goals should be achieved within 2 to 3 years.
- ▷ Mid-term goals should be achieved within 5 to 7 years.
- ▷ Long-term goals will take at least 10 years to be achieved.

1. Securing Cryptographic Systems against Emerging Attacks

> **Scenario:** *Cryptography is designed to protect threatened assets. Since the early days of crypto, advances on the design and attack sides have been leading to a constant evolution of technical devices. Since the late 1990s, not only the algorithms but also the devices executing the algorithms have been attacked more and more. Recent attacks on implementations have been extending these attacks from local attacks to instances that are running in the cloud [3], [2]. At some point in the future, the quantum computer will arise and question the fundamentals of how asymmetric cryptography is designed and implemented today.*

Today's cryptographic algorithms and procedures and their well-protected implementations can be considered to provide a reasonable level of security against state-of-the-art brute force attacks and physical attacks on hardened implementations in critical applications.

However, first hints of an upcoming age of quantum computing backed by new research results set at risk today's asymmetric cryptography. These risks remain fuzzy as long as the availability of practical quantum computers that can actually break today's cryptography is unclear. However, storing today's cryptographic key exchanges allows decrypting secret data later in the future. The European Quantum Technologies Roadmap [1] predicts that quantum computers might already be available in slightly more than a decade, hence this transition has to be initiated very soon in critical domains where data remains sensitive over a long time.

It is necessary to analyse the impact of new underlying primitives on performance characteristics, footprint, and the security assumptions of the protocols. Moreover, a first step towards quantum resilience can be hybrid systems where classical and post-quantum cryptography (PQC) algorithms are run in parallel and where an attacker has to break the trusted classical as well as the less scrutinised PQC algorithm in order to break the system. Research has to work on efficient and secure ways of composing classical as well as quantum-secure primitives without neglecting performance and efficiency goals.

Due to the unclear situation in PQC and its standardisation, it is anticipated that future secure systems have to support a wider range of cryptographic primitives and that more frequent updates and changes to the primitives and protocols can be expected. The ability to update, remove, or add cryptographic primitives is referred to as "cryptographic agility", and the design of crypto-agile systems poses several challenges. As a consequence, research is needed on more flexible platforms, more generic cryptographic accelerators and general strategies to manage the cryptographic ecosystems in long-term secure applications. This also includes methods for quantum-resilient firmware updates, which are the basis for a move to PQC on already deployed devices.

Similar to the technical advances in brute-force attacks, implementation attacks mature and new classes of attacks emerge that set the practical devices that compute cryptographic algorithms at risk. Over the last 20 years, side-channel and fault attacks developed from rather coarse approaches to a very high level of sophistication and maturity. Accordingly, the research community developed countermeasures to mitigate specific attacks or attack classes for hardened implementations [4].

Course of Action: Securing Cryptographic Systems against Emerging Attacks

---

Short-term goals:

- ▷ Development of post-quantum algorithms, mitigation techniques for cache-timing and other implementation attacks
- ▷ Design of resilient computer architectures

Mid-term goals:

- ▷ Standardisation and dissemination of post-quantum algorithms
- ▷ Implementation of the resilient architectures

Long-term goals:

- ▷ Commercial spread of the resilient architectures

In addition to existing work on classical algorithms, PQC implementations also have to be secured against side-channel, fault or invasive attacks for the roll-out on embedded devices, smart cards and travel documents. However, at the moment, PQC offers several highly different proposals (e.g., hash-based, code-based, lattice-based, MQ-based), and research on secure implementations requires further attention.

Besides, machine learning could be seen as one of the hot topics in side-channel analysis as it could lead to new and unexpected attacks. Moreover, it could simplify attacks and make them easier to carry out when using already existing massive computing infrastructures for machine learning, especially if combined with the recent advances in program analysis and automated reasoning for automatic vulnerability detection ("cyber-reasoning systems").

Recent attacks on computer architectures such as Spectre and Meltdown [3], [2] fundamentally question the way of efficient and secure computation on local devices, and especially in the cloud. Making the common case fast was the paramount goal in computer architecture, which cannot be pursued in this ultimate rigorousness anymore.

Further Reading

[1] A. Acín et al. "The European Quantum Technologies Roadmap". In: *ArXiv e-prints* (2017). arXiv: 1712.03773 [quant-ph].

[2] P. Kocher et al. "Spectre Attacks: Exploiting Speculative Execution". In: *ArXiv e-prints* (2018). accepted: S&P 2019. arXiv: 1801.01203.

[3] Moritz Lipp et al. "Meltdown". In: *ArXiv e-prints* (2018). accepted: 27th USENIX Security Symposium, Baltimore, MD, USA, August 15-17, 2018. arXiv: 1801.01207.

[4] Florian Unterstein et al. "High-Resolution EM Attacks Against Leakage-Resilient PRFs Explained – And An Improved Construction". In: *IACR Cryptology ePrint Archive* 2018 (2018). URL: http://eprint.iacr.org/2018/055.

2. Trustworthy Platforms

> **Scenario:** *A charge point operator, whose infrastructure includes charge points which are deployed for long periods of time in remote and often unsupervised environments, has to provide a secure and reliable charging infrastructure. Charge points have to reliably handle the authentication of customers and authorisation of charging sessions and must provide the operator and energy supplier with correct and unmanipulated metering values. The software running on these machines has to handle privacy related data of customers that needs to be protected at all costs and thus has to be protected from any form of manipulation. A trust anchor within the charge point can be used to achieve this and build a chain of trust.*

Modern IT systems depend increasingly on the results of dynamically distributed computing tasks. Each involved device plays a crucial role for the security and safety of the overall system. Not only may these devices be widely distributed and belong to different stakeholders, but they may be in the hands of a potential adversary. Examples range from embedded automotive control units to stolen laptops through to local network (managed switched) infrastructure components or even remote cloud data centres.

The long-standing concepts of perimeter-based security architectures with well-defined trust boundaries used in IT security up to now have long been outgrown by the reality of today's needs. Even on single devices, multiple (potentially untrusted) third-party applications are integrated and interact with each other. Such interactions occur inside smart phones as well as in virtualised cloud data centres and, in the future, will even be found in smart factories and other critical infrastructures.

To address these arising challenges, it is necessary to reliably assess the identity and integrity of each involved entity and to provide strong means for data secrecy and privacy. The solutions to be developed range from hardware-based trust anchors such as Trusted Platform Modules (TPM) to Device Identity Composition Engines (DICE) through to modern operating system isolation mechanisms and the design and integration of trustworthy applications and protocols. Trustworthy hardware anchors are currently developed by chip vendors that keep the design of their chips a trade secret. Therefore, a validation of the implementations' correctness is infeasible. A solution to this challenge lies in Open Source implementations of these techniques that allow a certain degree of control over chip designs and firmware implementations and strengthen the trustworthiness of the hardware anchors in this crucial aspect.

First of all, base integrations in platforms and local trust anchors are needed. The basic building blocks for trusted platforms are included in the form of TPM or DICE in hardware and software in the devices and are used for initial proprietary functions. In the medium term, integration with protocols and global management is required. The basis of interoperability between devices is to use standards. These must be redefined or extended to make integrity information usable and must be thoroughly verified in order to ensure that no flaw is introduced. In addition, trustworthy reference implementations and compliance suits need to be expanded to include the new features and must be thoroughly checked.

Course of Action: Trustworthy Platforms

Short-term goals:

- ▷ Use of trust anchors such as TPM or DICE in PC-clients, servers, embedded systems
- ▷ Trusted execution environments; e.g. microkernels and lightweight compartmentisation
- ▷ Software stack and middleware design and implementation

Mid-term goals:

- ▷ Protocol integration and development for trust establishment and configuration / identity assessment
- ▷ Trustworthy application design and system architecture specification

Long-term goals:

- ▷ Implementation of automated reference value recognition and validation as well as their integration into all common implementations
- ▷ Development of hardware trust anchors with Open Source hard- and firmware

A basic supply and scaling are planned for the long term. Integrity considerations of platforms will become the basic technology of all newly created devices and will be implemented as naturally as are access control or SSL/TLS. This requires the implementation of automated reference value recognition and validation as well as their integration into all common implementations.

Further Reading

[1] ENISA. *Infineon – NXP – STMicroelectronics – ENISA Common Position On Cybersecurity*. 2016. URL: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity (visited on 06/18/2018).

[2] Andreas Fuchs, Christoph Krauß, and Jürgen Repp. "ICT Systems Security and Privacy Protection: 31st IFIP TC 11 International Conference, SEC 2016". In: ed. by Jaap-Henk Hoepman and Stefan Katzenbeisser. Springer, 2016. Chap. Advanced Remote Firmware Upgrades Using TPM 2.0, pp. 276–289. DOI: 10.1007/978-3-319-33630-5_19.

[3] Andre Rein et al. "Trust Establishment in Cooperating Cyber-Physical Systems". In: *Security of Industrial Control Systems and Cyber Physical Systems, CyberICS 2015 and WOS-CPS 2015*. Ed. by Adrien Bécue et al. Vol. 9588. LNCS. Springer, 2016, pp. 31–47. DOI: 10.1007/978-3-319-40385-4_3.

3. Secure Lifecycle despite of Less Trustworthy Components

> **Scenario:** *In contrast to the rapid innovation cycles in IT, manufacturing environments and industrial infrastructures may exist for many years or even decades. Implementing a state-of-the-art control and communication architecture in a manufacturing line or critical infrastructure is rarely a greenfield project and typically requires a gradual transition from an existing structure to the new architecture with minimal downtime in between. Later on, the respective facility will be maintained and will be upgraded several times such that the security concept has to evolve together with the system's functionality. This also applies to prominent examples such as the World Mobile Network 5G or the European Navigation System GALILEO.*

Application domains such as Industry 4.0, the Internet of Things, autonomous vehicles or critical infrastructure all have in common that for most practical use cases, it is impossible to launch new stand-alone systems and architectures that do not interact with legacy components or infrastructures that cannot be changed e.g., due to accreditation. Therefore, designing, developing and operating secure systems requires designing a secure lifecycle that covers all stages of the lifetime of the system and its components [1]. Developing parameters and processes for risk assessment helps to evaluate the security of a system even under partial information.

Implementing a secure lifecycle requires skilled developers and also time so that the current skill gap can be closed to ensure widespread implementation. Technical competence has to be complemented with a wider awareness for cybersecurity. Dealing with innovative and creative attackers and assessing risks in a constantly changing environment also requires the system designers to follow innovations in several research and knowledge areas. Backup plans for reactions to attacks or breaches also help to limit their impact.

Integrating large numbers of heterogeneous components like microchips, embedded devices, operating systems, software libraries, applications, mobile devices and cloud services that are specified, developed and maintained independently requires special care and standardised processes. Functional and security updates improve the individual behaviour of components e.g., by firmware updates or by a controlled transitioning to new cryptographic primitives such as post-quantum algorithms. Going beyond the primitive, it is necessary to incorporate post-quantum cryptography in the protocols such as TLS, PACE, IPSEC, or EMV, that form the foundation of today's communication. However, the updates lead to a gradual change away from the system state that was initially specified and tested. This makes it hard to give security guarantees over longer time frames. Furthermore, individual components might not be maintained according to current best practices, or updates might be discontinued while deployed components remain productive. This might require a combination of virtualisation, isolation, compartmentalisation and modularisation. Usable tools for human involvement implement, analyse and support the lifecycle of a system. Open Source hardware and software are a great promise to design and maintain secure systems with the help of the community and increase their quality. However, they also open the potential for malicious manipulation and give attacks a large scalability if they are placed in popular code. Hence a thorough quality control is necessary.

Course of Action: Secure Lifecycle despite of Less Trustworthy Components

Short-term goals:

- ▷ Develop suitable and usable processes and tools to assess the security of systems and protect components
- ▷ Define standards for interoperability

Mid-term goals:

- ▷ Establish a secured infrastructure that was developed according to the developed methods
- ▷ Secure integration of components of different trustworthiness and legacy components
- ▷ Widen cybersecurity education to increase awareness and the number of available developers to design secure systems

Long-term goals:

- ▷ Fully hardened infrastructure with a secure lifecycle management

Clear liability trough the supply chain helps to enforce a secure lifecycle and also enables new businesses e.g., post-market certification to adapt to risks. A reasonable trade-off between certification effort and fast development cycles based on best practices allows to protect wider classes of applications and use cases. Central research questions here are: What certification processes are useful and manageable at the same time for different certification levels? Is it feasible to closer link security design and certification?

Lean and standardised protocols are another important aspect to set up and maintain a system securely. As a counterexample, hundreds of protocols are currently in place in the IoT world which inhibit interoperability and an easy assessment of the security of a product or a group of products. IoT devices used in industry, in smart homes, in automotive and in mobile medical devices pose different security requirements such that universal protocols have to be developed to enable a scalable security level.

A secure and scalable infrastructure provides the foundation for a secure system and allows a central component maintenance, security and privacy. The components connect to such infrastructure through trustworthy end points that manage the interaction between the components while allowing individual system configurations at the same time.

Migrating from legacy system architectures to state-of-the-art secured architectures while keeping components that are not secured at all or not secured anymore requires special care. Therefore, less trustworthy but also more vulnerable components have to be isolated to protect both, the system and the component [3].

Regarding the secure lifecycle, the methods and tools for development of software, and the remaining components have to be taken into account in addition [2]. This also includes the logistics in the distributed supply chain to design processes on how systems and software are introduced into the system and phased out again.

Further Reading

[1] Konstantin Böttinger et al. *Industrie 4.0 Security Guidelines Recommendations for actions*. 2016.

[2] Jörn Eichler and Roland Rieke. "Model-based Situational Security Analysis". In: *International Workshop on Models@run.time at the ACM/IEEE 14th International Conference on Model Driven Engineering Languages and Systems (MODELS 2011)*. Vol. 794. CEUR Workshop Proceedings. 2011, pp. 25–36. URL: http://ceur-ws.org/Vol-794/paper_1.pdf.

[3] Nisha Jacob et al. "How to Break Secure Boot on FPGA SoCs Through Malicious Hardware". In: *Cryptographic Hardware and Embedded Systems, CHES 2017*. 2017, pp. 425–442. DOI: 10.1007/978-3-319-66787-4_21.

4. Quantifying Security

> **Scenario:** *Every chief information security officer in a company faces the task of deciding how to achieve the best possible security with the limited available resources. It is, however, usually not clear what "better" or "best" means. Should he or she e.g., strengthen the use of formal tools to reduce the number of software flaws or invest in penetration testing?*

The desire to quantify IT security is not new. Heuristics are currently used in order to manage IT security and judge whether an organization maintains an adequate level of security. Because IT systems are complex, these heuristics mostly focus on the properties of the process that was used to construct a system rather than on the properties of the system itself.

An important unsolved problem is that of comparing the benefits of two different security measures when faced with a choice between them. In this case, inspecting the software construction process is not sufficient, as the question is not about the security of the software itself, but about its effects on a larger system. The long-term goal of quantifying security is enabling rational decision support. In order to prioritise security measures, there needs to be a way to make them comparable.

A simple example of quantifying security is the question "Is a piece of software more secure after a patch?" Even if the patch is correct and fixes a bug, it could in theory introduce a new one. Quantification also covers the comparison of different systems, of course.

The effort of quantifying security is related to but distinct from the "Science of Security" (SoS) effort, which aims to improve the scientific rigour of security research but is not necessarily focused on quantification. Quantification, on the other hand, greatly benefits from scientific rigour but should also be prepared to deal with aspects of IT security that are not yet available to a rigorous approach.

It should also be clarified that "security" should not be taken to mean immunity against all attacks. Security is always relative to attacker capabilities and security goals.

Efforts in the direction of quantification already exist and have been pursued in sub-fields of computer science and IT security for decades. A related effort, NSA's Science of Security (SoS) research initiative, is funded under the US Comprehensive National Cybersecurity Initiative (CNCI), which was started in 2008. Stand-alone metrics abound in the field of IT security. One prominent example is the Common Vulnerability Scoring System (CVSS). These metrics, however, make it clear that measuring alone is not sufficient. What is needed is an overarching effort to combine the results from single sub-fields into a big picture.

This effort will require a long-term collaboration of experts from different fields. Quantifying security is difficult even within one field, and combining different metrics with different histories is an intricate task. In addition, individual risk perception is not necessarily aligned with metrics, which has to be taken into account. Some goals might well prove to be impossible to achieve; it will almost certainly not be possible to describe the security of a system with a single number.

It is important to recognise the different advantages of the logical deductive approach that is restricted to a formal model, and the empirical inductive approach that is afflicted with uncertainty. One must consider the risk that is associated with models (which never fully reflect reality) and assumptions (which might prove to be false) and aim to quantify

Course of Action: Quantifying Security

Short-term goals:
- ▷ Develop ways to compare different versions of the same system in terms of security
- ▷ Compare advantages and limitations of different ways to quantify security
- ▷ Identify aspects of security that cannot be quantified

Mid-term goals:
- ▷ Develop a common language to talk about security quantification
- ▷ Identify sensible ways to quantify security in sub-fields of IT security
- ▷ Identify trade-offs between security measures
- ▷ Develop security metrics adapted to specific application areas

Long-term goals:
- ▷ Achieve security quantification of complex example systems
- ▷ Quantify security of real systems

the uncertainty inherent in the gap between the model and the real world. In addition, not everything can be quantified and researchers should be prepared to deal with this. The result will probably be a vector of measures and include unknown parameters that should be admitted as being unknown, such as the probability of an attack.

The goal of the effort of quantifying security is the ability to confidently estimate or in some cases even calculate a "Return on IT Security Invest" equivalent to the Return on Security Invest (ROSI) after quantifying the damage done by attacks and the cost of security measures.

Further Reading

[1] Cormac Herley and Paul C. van Oorschot. "SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit". In: *IEEE Symposium on Security and Privacy, SP 2017*. IEEE Computer Society, 2017, pp. 99–120. DOI: 10.1109/SP.2017.38.

[2] Marcus Pendleton et al. "A Survey on Systems Security Metrics". In: *ACM Comput. Surv.* 49.4 (2017), 62:1–62:35. DOI: 10.1145/3005714.

[3] Salvatore J. Stolfo, Steven M. Bellovin, and David Evans. "Measuring Security". In: *IEEE Security & Privacy* 9.3 (2011), pp. 60–65. DOI: 10.1109/MSP.2011.56.

5. IT Security and Data Protection for Machine Learning

> **Scenario:** *An attacker can manipulate road signs such that the automated interpretation of the signs by a machine learning system within an autonomous car will be wrong. For example, a stop sign with only minimal changes, such as a sticker, could be misinterpreted as a speed limit sign, potentially leading to accidents.*
> *A user regularly employs the language assistant on his or her smartphone to control smart home devices and also place orders in online shops. An attacker can trick the always-on language assistant, for example by embedding commands in inaudible noise. It may happen that orders are suddenly placed that were not initiated by the user.*

Machine learning (ML) will become an integral part of our daily lives with autonomous systems. Whether self-driving cars, home automation, decision procedures within companies, virtual assistants, or the Internet of Things—decisions are increasingly being made by ML-based systems independently using algorithms and thus having a direct impact on our physical environment and lives. Such ML systems are also self-learning and develop continuously over time in order to make increasingly autonomous decisions.

In the last few years, especially deep neural networks (DNN) and other machine learning algorithms have evolved into the state-of-the-art approach to automatic image analysis, speech recognition, and similar application domains. Their success is due to many factors, especially their ability to model large complex data sets to perform agnostic and also highly robust clustering and classification tasks. In practice, such approaches can cope with the complex environments that are typical of many scenarios such as autonomous driving or voice recognition systems. In addition, machine learning technologies might also be used for attacking computer systems in the future (e.g., an attacker could use ML algorithms to customise phishing e-mails to each individual victim).

With the development of these new autonomous systems and the resulting increased networking and automation of the individual components in recent years, taking a closer look at machine learning in the context of IT security and privacy is crucial. There are two sub-categories of IT security for machine learning that require specific focus: *Adversarial Machine Learning* and *Resilient Machine Learning*. Privacy aspects of machine learning can also be categorised into *Private Machine Learning* and *Transparent Machine Learning*, where the latter includes general notions of transparency, fairness, explainability, and related aspects of ML systems.

By Adversarial Machine Learning, we mean targeted attacks on machine learning algorithms themselves. Research has already shown that manipulated training material can lead to "mislearning" and an attacker can also exploit the learned model itself to trick it into misclassifying an input. This behaviour can lead to errors in the assignment of an input to an output, for example to the misinterpretation of a command or an image. According to this, a trained DNN is able to map an input x to an output y, but this mapping is not always correct. Furthermore, due to the high degree of non-linearity of this mapping function, it is not intelligible how the result is calculated. More importantly, this insufficient generalisation can lead to blind spots which may not be obvious to humans. As mentioned above, an attacker can utilise the incomplete generalisation of these systems to mislead the ML algorithm into misclassifying a given input. An example is to hide voice commands

Course of Action: IT Security and Data Protection for Machine Learning

Short-term goals:

- ▷ Formal definition of security in the context of machine learning
- ▷ Enhancing trustworthiness in machine learning
- ▷ Design of resilient computer architectures
- ▷ Creation of an environment for tests and testing of already trained machine learning systems to detect empirically exceptional cases and limits of the systems

Mid-term goals:

- ▷ Verifiable traceability and fairness of machine learning systems
- ▷ Accountability of machine learning in relation to the processed data
- ▷ Credibly communicate the results and trustworthiness of a machine learning system to the end user in a transparent and explainable way

Long-term goals:

- ▷ Policies that specify which algorithms should be used in which situations and what guarantees they must provide
- ▷ Implementation and control of the policies, ideally with a certification procedure
- ▷ Privacy-friendly machine learning

in audio signals in such a way that they are inaudible to humans but are recognised by automated speech recognition systems. As a result, an adversarial input can mislead the system, while tricking a user into understanding a completely different sentence. Similarly, image recognition systems can be tricked into assigning wrong labels to a given image, which is critical in many application scenarios (e.g., during autonomous driving).

An open research challenge is to obtain authenticity for ML systems such that they are immune against such manipulations. We need to develop mechanisms to improve the resilience of machine learning algorithms (Resilient Machine Learning), especially if we want to use them in the computer security context. Only if we can assure that the machine learning algorithms work correctly even under attack, we can utilise them for security-critical (and also safety-critical) tasks such as intrusion detection, malware analysis, or related scenarios. Moreover, we need to develop methods for assessing and improving the security of learning algorithms and devise methods to enhance explainability and transparency of machine learning systems such that human experts can better utilise them for detecting new and unexpected attacks. Such methods should provide a foundation for operating machine learning techniques under attack and thus render the detection of sophisticated threats possible.

Transparent Machine Learning is the effort to make machine learning algorithms more understandable, in particular, to create responsibilities concerning classified data and results. A user of an ML system should be able to understand and reconstruct how the system

arrived at a particular decision. Private Machine Learning encompasses the concept of data protection-friendly learning. A data trustworthiness assurance should be ensured through attestation mechanisms.

Investigating machine learning in the context of IT security is still a young discipline. For this reason, in a first step, a formal definition of "security" should be developed within the framework of machine learning, and requirements analyses should identify attributes that make up an IT security-compliant machine learning algorithm. In addition, reliable machine learning measures must be implemented so that the decisions and results of the trained systems are generally accepted. For this purpose, it makes sense to establish tests and a test environment of already trained machine learning systems to detect empirically exceptional cases and limitations to the systems. This would allow a systematic identification of attack vectors from different machine learning systems. Given that ML systems are typically very complex, such systematic testing would also uncover programming mistakes in the ML system itself.

New principles must be developed to check the traceability and fairness of machine learning systems. Especially fairness is crucial and hence we need to develop methods to avoid any kind of bias in such systems. This is the precondition for the accountability of machine learning to the processed data, results, and algorithms. In the medium term, this means that the results and the trustworthiness of a machine learning system must be convincingly communicated to the end users.

In the long term, new guidelines need to be introduced that specify which algorithms should be used in which situations and what guarantees they should provide. The implementation and control of these guarantees can be achieved only by the goals already mentioned. A certification procedure for ML systems needs to be developed. Data protection-friendly learning (*private learning*) in particular will be necessary for long-term goals, as the application of data analysis and machine learning must be ensured without impairing the rights and freedoms of individual users. This goal can only be achieved via a close collaboration between the IT security and machine learning communities.

Further Reading

[1] Nicholas Carlini and David Wagner. "Towards Evaluating the Robustness of Neural Networks". In: *IEEE Symposium on Security and Privacy, SP 2017*. IEEE Computer Society, 2017, pp. 39–57. DOI: 10.1109/SP.2017.49.

[2] Nicolas Papernot et al. "The Limitations of Deep Learning in Adversarial Settings". In: *IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2016, pp. 372–387. DOI: 10.1109/EuroSP.2016.36.

[3] Reza Shokri et al. "Membership Inference Attacks Against Machine Learning Models". In: *2017 IEEE Symposium on Security and Privacy, SP 2017*. IEEE Computer Society, 2017, pp. 3–18. DOI: 10.1109/SP.2017.41.

[4] Guoming Zhang et al. "DolphinAttack: Inaudible Voice Commands". In: *CCS 2017*. Ed. by Bhavani M. Thuraisingham et al. ACM, 2017, pp. 103–117. DOI: 10.1145/3133956.3134052.

6. Big Data Privacy

> **Scenario:** *Huge databases are created that record diverse sensitive medical and biological data. Examples are given by the International Cancer Genome Consortium (ICGC) or the Human Brain Project, which is the H2020 flagship project of the EU to support medical research in the area of neuroscience. In these projects, the protection of privacy has been given top priority. Specialised variants of multi-party computation were successfully used for comparing genomes to optimise medical therapies. We need well-elaborated procedures to guarantee privacy while evaluating sensitive big data.*

At present, the Internet can be seen as a huge data storage that collects personal and sensitive data about its users. For the latter, this leads to significant security and privacy risks due to the loss of control over their shared data. The increasing data volume and the concatenation of data enables the creation of personality profiles which can lead to discrimination against end users and might make them receptive to manipulative tailored messages (so-called "microtargeting"). Beyond that, even if data has been anonymised by state-of-the-art technologies, it might be accidentally re-identifiable. This risk of re-identification increases, especially if data from various sources such as different commercial or social online platforms or smart devices are brought together.

Medical studies provide another ecosystem operating on data. For the joint evaluation of multiple databases for a meta-study, differing privacy policies and probands' declarations of agreement have to be taken into account. Therefore, technologies such as multi-party computation (MPC), data anonymisation and processes such as separating databases are needed to ensure privacy-protecting, efficient, and fast analysis. In addition, machine learning algorithms that are used for automated analysis should be adapted to the processing of sensitive data.

In general, the development of methods and tools to enable secure and privacy-protecting data processing is one of the biggest challenges for ecosystems and applications operating on data. The success of digitalisation heavily depends on the ability of companies and operators of large-scale studies to gain the trust of their users or rather probands in their methods to suitably protect their privacy: Digital sovereignty is not possible without the citizens having control over their own data. The handling of personalised data and the optimisation of security and privacy in the area of information processing in diverse settings need improvement. Therefore, cryptographic schemes have to become more efficient and technologies such as machine learning have to be involved in the protection of privacy. In addition, binding standard procedures for big data processing have to be developed.

Anonymisation and Private Learning in Big Data

The most efficient way of protecting the privacy of users is to remove the personal references of data and anonymise it completely, so that the person in question is not identifiable anymore. For example, artificial intelligence is used in medical research to support tumor recognition via automatically analysing CT scans. In order to protect patients whose CT scans are used for pattern recognition (machine learning) from possible identification by third parties, the image data in the learning process must be sufficiently anonymised. But with

Course of Action: Big Data Privacy

Short-term goals:

- ▷ Extending and adapting existing concepts to anonymise data like k-anonymity, l-diversity, t-closeness and differential privacy for big data
- ▷ Use of trustworthy hardware security modules for small data volumes and increase in efficiency using trusted initialisers during the preprocessing phase of MPC protocols
- ▷ Implementation of MPC, secure against passive adversaries
- ▷ Standards for isolated computers in data centres (auditable security)

Mid-term goals:

- ▷ Development of new anonymisation methods
- ▷ Better insight and metrics of linkability, inference and re-identification risks
- ▷ Development of efficient MPC secure against active adversaries
- ▷ Efficient and feasible secure computation on encrypted data and efficient specialised protocols for concrete applications
- ▷ Comprehensive database for efficient PPA solutions

Long-term goals:

- ▷ Private learning and private modelling in order to allow value added without privacy risks
- ▷ Implementation of efficient MPC, secure against active adversaries
- ▷ Efficient and feasible computation methods on encrypted data using fully homomorphic encryption and usable indistinguishability obfuscation
- ▷ Establishing a standard procedure for efficient PPA with suitable privacy measure

the increasing amount of available data and the risk of linkability, effective anonymisation of personal data has become more complex and challenging. Existing anonymisation methods and techniques are not well suited for the specific challenges that big data poses, namely volume, velocity, and variety. Big data linkage could allow to draw conclusions in respect of individual identifiable users. In practice, there are many cases where allegedly fully anonymised data in fact have allowed re-identification.

Thus, the goal of research is to develop new anonymisation techniques which can reliably anonymise large and dynamic data sets. In the case of CT scans, a first step could be, for example, the removal of the bone structure on the scans so that the patient's face can no longer be calculated. At the same time, the optimal trade-off between data anonymisation and the data's validity and significance has to be balanced. Big data analysis has the potential for crucial societal benefits, for example in the case of mobility or health data. Therefore, in addition to data anonymisation, more research has to focus on alternative

privacy-enhancing approaches to machine learning such as private learning, private modelling or synthetic data.

Expanding Cryptographic Schemes for Secure Computation

The known methods for secure computation on sensitive data are multi-party computations (MCP) under different security assumptions, including garbled circuits, data anonymisation techniques and encryption techniques for databases which enable (limited) computations on encrypted data. With the help of "secure MPC" Yao's Millionaires' Problem can be solved, i.e. two parties can establish who is richer without revealing the actual value of their possessions to each other. Specialised variants of MPC were successfully used in big data scenarios.

These methods work well for small data volumes. In order to apply them to huge data volumes, it is necessary to turn attention to the scalability of the chosen method. Moreover, the speed or rather the loss of speed needs to be addressed. Hence, efficient protocols and variations of the methods mentioned before are required. Additionally, clever combinations of the methods and specialised protocols for precisely defined applications will build a promising starting point for effective and practicable secure computation on big data.

Approaches such as fully homomorphic encryption, indistinguishability obfuscation or functional encryption have to be deepened in the long-term to be used efficiently and feasibly for big data. Partial success can be reached with the help of homomorphic encryption as a component of specialised protocols in the mid-term. The theory of MPC, secure against passive adversaries, is already well-developed. In the short-term, feasible applications based on it can emerge. The efficiency of these can be increased if, during the preprocessing phase, trusted initialisers were used to perform computations which are independent of the actual input. This can be extended to specialised protocols for exactly defined applications. To handle verifiable computation on encrypted and/or authenticated data, we need to understand the theory of MPC, secure against active adversaries. This has to be adjusted to big data volumes. The implementation of executable and efficient procedures which are based on MPC, secure against active adversaries, remains a long-term goal.

Standard Procedures for Efficient Privacy Preserving Analytics

Social sciences perform statistical analyses of sensitive data. The researchers' fundamental interest lies in maintaining the privacy of personal data. First attempts at holistic approaches to private data handling are promising.

Privacy-preserving Analytics (PPA) comprises the handling of personalised, sensitive big data volumes, such that new insights can be generated without violating the privacy of individuals. An efficient PPA solution ideally includes all processes, hardware and software components as well as networks, which are involved in recording, storing, transferring, processing and outputting data, to guarantee the protection of privacy. Taking legal aspects and possible conglomerations of different data bases into account, the following question should be answered in the first place: "What and when should who know about whom?" Based on the answer, privacy measures to evaluate the quality of efficient PPA have to be developed in the short- and mid-terms.

Establishing binding standards for separating databases in data centres has already started and should be pursued (auditable security). Simultaneously, existing methods for

secure computations on sensitive data have to be adapted to the particularities of big data and complemented by new ones. At the same time, a comprehensive database has to be built displaying appropriate efficient PPA solutions to different applications. Mechanisms to estimate impacts of publishing sensitive data should be established and depicted ideally in the same database. The different privacy measures developed beforehand can be combined. Thus, within ten years, a technology and process standards can be developed, which allow private data analyses to run efficiently.

Further Reading

[1] Gilad Asharov et al. "Privacy-Preserving Search of Similar Patients in Genomic Data". In: *IACR Cryptology ePrint Archive* 2017 (2017), p. 144. URL: http://eprint.iacr.org/2017/144.

[2] Michael Backes et al. "Privacy in Epigenetics: Temporal Linkability of MicroRNA Expression Profiles". In: *USENIX Security 2016*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, 2016, pp. 1223–1240. URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/backes_epigenetics.

[3] ENISA. *Privacy and Data Protection by Design*. 2014. URL: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (visited on 06/19/2018).

[4] Rafael Tonicelli et al. "Information-theoretically secure oblivious polynomial evaluation in the commodity-based model". In: *Int. J. Inf. Sec.* 14.1 (2015), pp. 73–84. DOI: 10.1007/s10207-014-0247-8.

B. Interdisciplinary Challenges

Cybersecurity can only be achieved by the co-development of technological devices, applications, services, and methods. However, the systemic combination, interaction and final diffusion of such cybersecurity solutions also depend on a variety of factors beyond technology.

Cognitive and human-centred efforts increase usability by engaging all stakeholders – ranging from the end-user to developers, designers, administrators, and providers. Such a holistic approach should enhance digital awareness and lead to the development of fair business models which ultimately strengthens the European cybersecurity economy. Simultaneously, establishing and enforcing a coherent legal framework which incorporates procedural methods and metrics for a risk-adequate approach in data protection law is essential in the quest for cybersecurity and digital sovereignty.

In the following sections, we outline the main challenges in each area and propose a course of action in three phases:

- ▷ Short-term goals should be achieved within 2 to 3 years.
- ▷ Mid-term goals should be achieved within 5 to 7 years.
- ▷ Long-term goals will take at least 10 years to be achieved.

1. Measurable, Risk-adequate Security in Law

> **Scenario:** *1. In his smart home, a consumer who is highly interested in technology matters uses intelligent appliances such as smart speaker "Alexa" to control heating and power consumption. The consumer is concerned about his privacy and wonders whether in times of big data, he can control his personal information.*
> *2. An employer transfers premises to a smart environment, where each employee has a specific app to track working hours and the project status. During the implementation process, the question arises as to what steps need to be taken to imply the technical and legal requirements for systems of "self data protection".*

From a legal perspective, the terminology of *digital sovereignty* captures cybersecurity and data protection law having the function of ensuring and defending *individual rights*. At the same time, it refers to the development of a *sovereign European data economy* that includes protecting cross-border data flows and provides a supportive environment for the development of small and medium businesses that are producers applying the new source "data". These new producers need to be protected from attacks, misuse, and competitive distortion. The necessary *access and secret protection* for platforms and communication channels is already marginalised in particular through the transatlantic de facto-standardisation of substantial components. [1] Consequently, there is a need to integrate legal questions of cybersecurity and data protection law in present European law-making activities. [2]

In times of big data, the challenging tasks of an existing *incoherent legal structure* regarding complex ICT systems and the limited possibilities of influencing individual data flows need to be addressed by each of the actors in the system. [3] In addition cybersecurity and data protection law is increasingly dominated by *risk-adequate safeguards* rather than by precise legal proposals on how to design the legal mechanisms.

Thus, the cybersecurity regulations for risk predictions, particularly in the GDPR ("DPIA" and "Privacy by Design") and the European NIS Directive, are subject to systemisation and structuring. With this basis, the legally protected goods and contextual legal requirements (*"state of the art"*) with reference to the technical, organisational and procedural design can be identified in order to prevent sanctions. Furthermore, procedural mechanisms might be used to intervene in cases of high risk and allocate the responsibilities in such a manner that a win-win solution can be achieved. From an economic perspective, the challenge for the user to redesign and clarify the regulations for operationalisation in single aspects is also due to the uncertain legal structures and systems of the regulations. This reveals the urgent need for further research.

A possible solution might be to integrate the *transparency and measurability of the contextual risks as mechanisms of assessment* for the development of a *quantitative risk-metric* and implement them into the legal system as a contribution to legal certainty. The current substantive and procedural legal models build the basis for identifying convergences

[1] E.g., American platform providers are relatively dominant in the market.
[2] This is part of the ePrivacy Regulation.
[3] An example for such incoherent regulations is Article 14 (3) NIS Directive with regard to the German § 8 b (4) S.1 BSIG.

Course of Action: Measurable, Risk-adequate Security in Law

Short-term goals:

- ▷ Systemisation and classification of terms and definitions such as "risk" and "state of the art" in cybersecurity and data protection law
- ▷ Analysing the legal terms with taking the game theory approach into account
- ▷ Analysing the risk based approach in different legal fields

Mid-term goals:

- ▷ Establishing a convergent structure of existing legal rules and statutes in order to harmonise cybersecurity and data protection law
- ▷ Reviewing the technical standards in order to establish a coherent system for data protection and cybersecurity law
- ▷ Establishing methods and risk-metrics for cybersecurity and data protection law
- ▷ Developing a quantitative risk-metric

Long-term goals:

- ▷ Analysing the effects of the legal approaches by taking empirical studies into account
- ▷ Adjusting the legal approaches and risk-metric with regard to the current challenges faced by the stakeholders in cybersecurity and data protection law

and divergences regarding the risk concept. However, also *technical modelling of convergent normative complexes* of cybersecurity and data protection law should be subject to further research.

Further Reading

[1] Helmut Heil. "Datenschutz durch Selbstregulierung – Der europäische Ansatz". In: *Datenschutz und Datensicherheit* 25.3 (2001).

[2] Wolfgang Hoffmann-Riem. "Gesetz und Gesetzesvorbehalt im Umbruch: Zur Qualitäts-Gewährleistung durch Normen". In: *Archiv des öffentlichen Rechts* 130.1 (2005), pp. 5–70. DOI: 10.2307/44317328.

[3] Steve Ritter in: Schwartmann/Jaspers/Thüsing/Kugelmann. *Art. 32 DSGVO*. Kommentar DSGVO. Heidelberg: C.F. Müller, 2018.

[4] Anika Klafki. *Risiko und Recht*. Studien und Beiträge zum Öffentlichen Recht 29. Tübingen: Mohr Siebeck, 2017.

[5] Martin Schallbruch. "Die EU-Richtlinie über Netz- und Informationssicherheit: Anforderungen an digitale Dienste". In: *Computer und Recht* 32 (10 2016), pp. 663–670. DOI: 10.9785/cr-2016-1011.

2. Holistic Human-centred Security and Privacy Research

> **Scenario:** *Software developers usually are not security experts; nor are classical end users security experts. However, the tools they are supposed to use, such as crypto APIs for developers, security interventions and config interfaces, assume they are. Correspondingly, it is likely that any of them uses the provided tools in an insecure way.*

The history of information security and privacy has taught us that it takes more than technological innovation to develop functional and effective security and privacy mechanisms. Many aspects of information security and privacy depend on both technical and human factors. As a result, in the age of digitalisation, we see a persistent gap between theoretical security and actual security in the real world. The gap is mainly caused by strong and actually unrealistic assumptions of the users' knowledge and behaviour; while users range from

- ▷ classical end users in a private or business context (e.g., assuming they choose long complex text passwords and for each account a different one) to
- ▷ software developers (e.g., assuming they have a background in security and cryptography and know how to securely integrate crypto APIs) through to
- ▷ administrators (e.g., assuming they have time and the resources to spend on security interventions generated by various security tools like firewalls, and figure out the message, the risk level, and decide on the actions to be taken).

Human-centred cybersecurity and privacy research conventionally has been focusing on end users while involving studies on various authentication mechanisms including text and graphical passwords, security indicators and interventions like warning messages, permission dialogues and security and privacy policies. Recently, human-centred security and privacy researchers started investigating other actors such as software developers, system designers, and administrators.

Traditional *human factors in security and privacy* research areas are (independent of the addressed type of users):

- ▷ Identifying users' mental models,
- ▷ evaluating existing approaches regarding their effectiveness in supporting their users to make secure decisions,
- ▷ proposing improved or new approaches/extensions, and evaluating their effectiveness; approaches can be security/privacy mechanisms or security/privacy awareness measures.

Future research needs a more systematic and holistic approach to make more contributions that are both effective and deployable in the real world (e.g., because the constraints of the addressed user groups are considered and the corresponding user groups can be reached). We need a better understanding of interdependencies between different user groups, the expectations of different user groups, and we have to focus more on supporting those who design and develop security-/privacy-critical systems. This needs to be done at all levels e.g.,

- ▷ system designers need to be supported in considering human security/privacy aspects from the very beginning (to enable them to apply a human-centred security and

privacy by design approach) in an effective and efficient way; e.g., efficient in the sense that knowledge from past research is provided to them in an adequate way and is integrated in corresponding tools,

- ▷ software developers need to be supported in properly integrating crypto APIs, security concepts and protocols, as well as in properly designing security indicators and security interventions (e.g., by integrating corresponding checks, feedback, and decision support in the tools they use for development); properly in this context means considering the cultural background of the actual end users,
- ▷ security professionals (e.g., CISOs), i.e. those responsible for the security of infrastructures, need to be supported in developing and implementing security policies including awareness measures which are accepted and can be respected by the employees.

Furthermore, research needs to find a balance between focusing on established security- and privacy-critical systems and more recently deployed ones such as Internet of Things, blockchain, or autonomous cars/car2car communication.

Additionally, future research needs to tackle methodological challenges: In the context of end-user research, past research was mainly based on data collected from service providers such as Amazon Mechanical Turk. Similarly, in the context of developers or administrators, research was mainly based on studies with computer science students. Significantly more research is needed to shed light on the fundamental question as to when participants recruited through service providers (such as Amazon MTurk) and computer science students are appropriate subjects to study, and what needs to be considered.

Previous work often focused on first-contact evaluations or short-term field studies of security and privacy tools and mechanisms. However, to prevent a replication crisis as known from other scientific disciplines, our community needs to push the need for more in-depth replication studies.

Finally, it is important that scientists researching human factors in security and privacy interchange their results with standardisation bodies (in particular ISO 27001) and governmental agencies (such as the NIST and the BSI in Germany) to make sure their requirements are aligned with well-established research results.

Further Reading

[1] Yasemin Acar, Sascha Fahl, and Michelle L Mazurek. “You are not your developer, either: A research agenda for usable security and privacy research beyond end users”. In: *Cybersecurity Development (SecDev)*. IEEE Computer Society, 2016, pp. 3–8. DOI: 10.1109/SecDev.2016.013.

[2] Yasemin Acar et al. “You get where you’re looking for: The impact of information sources on code security”. In: *IEEE Symposium on Security and Privacy (SP) 2016*. IEEE Computer Society, 2016, pp. 289–305. DOI: 10.1109/SP.2016.25.

[3] Anne Adams and Martina Angela Sasse. “Users are not the enemy”. In: *Communications of the ACM* 42.12 (1999), pp. 40–46. DOI: 10.1145/322796.322806.

[4] Matthew Green and Matthew Smith. “Developers are Not the Enemy!: The Need for Usable Security APIs”. In: *IEEE Security and Privacy* 14.5 (2016), pp. 40–46. DOI: 10.1109/MSP.2016.111.

Course of Action: Holistic Human-centred Security and Privacy Research

Short-term goals:

- ▷ Identifying relevant problem areas and tools to help end users, software developers and administrators to increase information security and privacy
- ▷ Developing and validating generalised theories and frameworks

Mid-term goals:

- ▷ Establishing best practices for conducting replication studies
- ▷ Establishing best practices for conducting field studies
- ▷ Establishing best practices for conducting studies with various user groups in particular with engineers and administrators

Long-term goals:

- ▷ Merging lines of research covering all involved actors for a holistic approach
- ▷ Contributing to standardisation activities.

[5] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. "Why Doesn't Jane Protect Her Privacy?" In: *Privacy Enhancing Technologies PETS 2014*. 2014, pp. 244–262. DOI: 10.1007/978-3-319-08506-7_13.

[6] Bruce Schneier. "The Psychology of Security". In: *AFRICACRYPT 2008*. 2008, pp. 50–79. DOI: 10.1007/978-3-540-68164-9_5.

[7] Melanie Volkamer and Karen Renaud. "Mental Models – General Introduction and Review of Their Application to Human-Centred Security". In: *Number Theory and Cryptography*. 2013, pp. 255–280. DOI: 10.1007/978-3-642-42001-6_18.

3. Digital Business Models for a Fair Economy and Society

> **Scenario:** *A start-up that develops a time management app would like to support their users while also generating revenue. In this regard, they are faced with determining the adequate level of security and privacy. Should they implement a two-factor authentication process that requires a biometric approach, for example a fingerprint, in addition to a password or PIN? Or would that be too time-consuming and privacy-sensitive? They also wonder how much user data should be collected and stored in order to develop and enhance their app or to pave the way for additional complementary products and services while not intruding too much into their users' privacy.*

The ever-increasing digitalisation and the ubiquity of internet-based services continue to disrupt the industry, daily life of the individual, and the society as a whole. Despite the numerous benefits and chances, these changes also entail an increasing vulnerability which prompts concerns by enterprises, public organisations, and end-users. Against this backdrop, the question arises as to how Europe can contribute and potentially harness the concept of digital sovereignty.

In addition to raising awareness among users of digital technologies through better communication, providers of digital goods or services could and should have a share in increasing security and privacy and should realise their potential as an enabler for their business. This requires not only the emergence of (new) providers of innovative and user-friendly IT security and privacy solutions that are based on the newest research findings but also addresses (existing) providers of digital services who base their business models on the utilisation of user data. Focusing on a high degree of usability and distributing control over data across stakeholders is the key to achieving data sovereignty.

The analysis along with the design of business models and the desired data sovereignty require an interdisciplinary approach, i.e. an interdisciplinary cooperation between disciplines such as computer science, economics, law, and the humanities. Such a cooperation could be organised within a new European interdisciplinary centre where economic stakeholders, i.e. both provider and user organisations, as well as private EU citizens are involved. An essential part of such a joint approach should comprise empirical studies that address the complex questions brought forward by all involved stakeholders through international comparative studies. Results of these studies along with their publications should not be reserved for scientific outlets but also diffused through citizen-oriented forums and thus contribute to raising awareness for potential security and privacy threats while enhancing the data sovereignty of all involved stakeholders. Additionally, findings and insights derived through these studies could serve as a basis for the development of new business models or technologies. By way of example, the joint development of privacy-enhancing technologies for services could help preserve the privacy of user data, thus contributing to data sovereignty while enabling implementing enterprises to generate revenue through using user data. This is a concept that could be applied in other contexts such as big data, machine learning, the Internet of Things, or the Internet of Vehicles.

However, when analysing and designing these new business models, it is essential to know the ropes of the digital economy and thus consider the particular properties of digital goods and services and the characteristics of software and digital markets. From a macroeconomic

Course of Action: Digital Business Models for a Fair Economy and Society

Short-term goals:

- ▷ Conception of first interdisciplinary empirical studies on data sovereignty and fair business models

Mid-term goals:

- ▷ Development and installation of an interdisciplinary research centre
- ▷ International comparative studies across EU countries on data sovereignty and fair business models
- ▷ Roundtables with all involved stakeholders (industry, scientist, and citizens)

Long-term goals:

- ▷ Exertion of influence on the design of data-driven, fair business models
- ▷ Guarantee of enhanced data sovereignty for EU citizens

perspective, it is further necessary to determine whether or how investment incentives or state regulations can encourage the development of a new range of products and services, in particular for small and medium-sized enterprises and start-ups in the EU.

Methods and Principles of Fair Business Models

Empirical findings – both from quantitative and qualitative studies (e.g., through the use of Delphi methods, expert interviews, focus groups) – could additionally serve as the groundwork for the definition and basic principles of fairness and the subsequent development of fair data-driven business models. Fairness in this context does not only refer to transparency during the extraction and processing of data but also comprises adequate pricing models and the identification of tensions between the different values held by stakeholders. Therefore, it must be examined whether the extensive collection of data might violate the privacy of citizens or whether it provides a basis for unfair pricing models that take advantage of potential dependencies that could become apparent through, for example, the analysis of an individual's surfing behaviour. This will also require investigations of data analyses through machine learning algorithms, of whether these can be performed without compromising the individual's rights and freedom and of how the analyses and resulting judgments comply with general ethical rules. These investigations should ideally lead to the identification of the kind of ethical behaviour that should be promoted unanimously across the European Union and in guidelines regarding the fair usage of (open) data.

Overall, a strong IT security and privacy industry that includes successful providers and start-ups building on data-driven (and fair) business models could help strengthen the competitive position of German and European providers compared to their US counterparts. The odds are in favour of these domestic providers as users in Europe, and in Germany

in particular, exhibit a more pronounced willingness to pay for IT security and privacy compared to other countries or continents.

Further Reading

[1] Robert E Crossler and Clay Posey. "Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem". In: *Journal of the Association for Information Systems* 18.7 (2017), p. 487. URL: http://aisel.aisnet.org/jais/vol18/iss7/2.

[2] Nicole Eling et al. "Investigating Users' Reaction to Fine-Grained Data Requests: A Market Experiment". In: *Hawaii International Conference on System Sciences (HICSS) 2016*. Ed. by Tung X. Bui and Ralph H. Sprague Jr. IEEE Computer Society, 2016, pp. 3666–3675. DOI: 10.1109/HICSS.2016.458.

[3] Adrian Engelbrecht, Jin Gerlach, and Thomas Widjaja. "Understanding the Anatomy of Data-Driven Business Models-towards an Empirical Taxonomy". In: *European Conference on Information Systems (ECIS) 2016*. 2016. URL: http://aisel.aisnet.org/ecis2016%5C_rp/128.

[4] Jens Grossklags and Alessandro Acquisti. "When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information". In: *Workshop on the Economics of Information Security (WEIS)*. 2007. URL: http://weis2007.econinfosec.org/papers/66.pdf.

[5] Rabea Sonnenschein, André Loske, and Peter Buxmann. "Which IT Security Investments Will Pay Off for Suppliers? Using the Kano Model to Determine Customers' Willingness to Pay". In: *Hawaii International Conference on System Sciences (HICSS) 2016*. Ed. by Tung X. Bui and Ralph H. Sprague Jr. IEEE Computer Society, 2016, pp. 5672–5681. DOI: 10.1109/HICSS.2016.701.

C. Technologies and Applications

Problems in reality are complex and require the combined effort of different research areas. Cybersecurity is an enabling factor for new ecosystems such as, inter alia, the Internet of Vehicles and blockchain-driven applications.

These ecosystems and other technologies offered by digitalisation and applied in everyday life need to be made transparent to end users, for example the Internet and its many facets from its infrastructure through to content-driven applications. Moreover, the development of user-centric privacy tools and remotely un-hackable PCs for private use could increase the digital sovereignty of individuals.

privacy by offering users technical means to understand and judge relevant decisions in their daily online activities.

Remotely Un-hackable PC . . . . . p. 47
Once a programme or part of a PC has been attacked externally e.g., via its Internet connection, all other systems of the PC are usually threatened as well. The objective is therefore to develop a "remotely un-hackable PC", whose components have no or only a strictly controlled influence on each other, such that the overall system remains protected while retaining remote access. At the same time this PC needs to be user-friendly and the developed concepts need to allow for future developments such as intelligent personal assistants.

IT Security for Autonomous Driving . . . . . p. 49
IT security and data protection are enabling factors for the newly emerging Internet of Vehicles. Autonomous driving requires both a strong interconnectedness of vehicles and an opening to external information sources and services, which increases the attack surface. Therefore, a trusted platform for autonomous vehicles must be created, as well as a process framework considering security, and in particular crypto agility in the development and entire lifecycle of vehicles.

In the following sections, we outline the main challenges in each area and propose a course of action in three phases:

- ▷ Short-term goals should be achieved within 2 to 3 years.
- ▷ Mid-term goals should be achieved within 5 to 7 years.
- ▷ Long-term goals will take at least 10 years to be achieved.

1. Safeguarding Key Services of the Internet

> **Scenario:** *Attacks on the Internet infrastructure have serious consequences. In 2013, a security incident happened that was aimed at the name resolution via the Domain Name System. With this attack, a group of hackers were able to redirect all visitors of Google's Malaysian domains to their own website. Misconfigurations within the core Internet infrastructure can also result in severe consequences, as was shown by an incident in 2017. A configuration issue within the routing infrastructure spread over the US and affected several Internet service providers, which lead to wide spread Internet outages.*

The Internet is the biggest and most complex communication network and, as such, the largest IT infrastructure worldwide. We have long been so dependent on the functioning of modern Internet technology that an attack on critical infrastructures, much like an attack on electricity or water supplies, can be life-threatening. For a universal use of Internet technology, the secure and stable operation of central protocols, services and applications is indispensable. The goal is to secure services that make up the Internet infrastructure so that the Internet communication is reliable, confidential and of integrity. These properties can be put at risk by undetected configuration errors or by adversaries of different qualities, like single perpetrators or groups of hackers, even with governmental affiliations.

Examples of such services are routing and name resolution functions in the Internet as well as key infrastructures, which enable e.g., end-to-end encryption.

Some solutions are already available today, but are not widely used. This results in an attack surface of rather unknown size. Further complicating matters, trends like the Internet of Things (IoT) steadily increase the amount of poorly managed and yet Internet-connected devices. Large-scale analyses of Internet-connected devices and services are necessary to identify vulnerabilities and to mitigate any risk they introduce. This is achieved by further spreading the neglected security features, also in the services of the core Internet infrastructure, and to establish a recommended level of security. This issue mainly concerns the developers of the related software as well as the operators of key services, which use the software. It is necessary to create incentives for both parties, which should serve at the beginning as unique selling point, but should then be established as required feature for software solutions and key services.

Detection and prevention of attacks on the Internet infrastructure and of misconfigurations of the corresponding services are to advance. First, it is necessary to analyse the distribution of secure protocol alternatives in the backbone infrastructure of the Internet and to detect configuration errors. In the medium term, technical measures must be developed to detect and prevent configuration errors at an early stage, to identify attempts to attack and to distinguish them from configuration errors. The long-term goal is to secure the backbone infrastructure of the Internet and to globally implement secure protocols for the Internet infrastructure.

Course of Action: Safeguarding Key Services of the Internet

Short-term goals:

- ▷ Analysis of adoption of security extensions for crucial protocols of the Internet infrastructure
- ▷ Identification of misconfigurations

Mid-term goals:

- ▷ Research for creating new technologies to detect and prevent misconfigurations
- ▷ Identification of attack pattern and distinction from misconfigurations
- ▷ Creation of incentives to incorporate security technologies in key services and their software

Long-term goals:

- ▷ Securing the key services of the Internet
- ▷ Global introduction and usage of secure protocols for the services of the Internet
- ▷ Establish security technologies as required feature for key services and their software

Further Reading

[1] Avichai Cohen et al. "Are We There Yet? On RPKI's Deployment and Security". In: *Network and Distributed Systems Security Symposium, NDSS 2017*. 2017. URL: https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/are-we-there-yet-rpkis-deployment-and-security/.

[2] Amit Klein, Haya Shulman, and Michael Waidner. "Counting in the Dark: Caches Discovery and Enumeration in the Internet". In: *IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017*. IEEE Computer Society, 2017, pp. 367–378. DOI: 10.1109/DSN.2017.63.

[3] Amit Klein, Haya Shulman, and Michael Waidner. "Internet-Wide Study of DNS Cache Injections". In: *IEEE International Conference on Computer Communications, INFOCOM 2017*. IEEE, 2017, pp. 1–9. DOI: 10.1109/INFOCOM.2017.8057202.

[4] C. Lévy-Bencheton et al. *Threat Landscape and Good Practice Guide for Internet Infrastructure*. Tech. rep. ENISA, 2015. DOI: 10.2824/34387.

[5] Haya Shulman and Michael Waidner. "One Key to Sign Them All Considered Vulnerable: Evaluation of DNSSEC in the Internet". In: *USENIX Symposium on Networked Systems Design and Implementation, NSDI 2017*. USENIX Association, 2017, pp. 131–144. URL: https://www.usenix.org/conference/nsdi17/technical-sessions/presentation/shulman.

2. Security of Blockchain Technology

> **Scenario:** *The Bitcoin protocol was presented in a white paper in 2008 and implemented in programme code in 2009. It is the first successful example of a decentralised cryptocurrency. It is also the first example of the new blockchain technology. Blockchains are also used for smart contracts, for example in the case of special travel insurances, where smart contracts are executed automatically in the case of flight-delays.*

Blockchain technology can be shortly described as being a "decentralised, tamper-proof and consensual data repository in distributed networks" (see e.g., German Federal Office for Information Security (BSI)). However, many challenges need to be addressed to make blockchain technology ready for mass adoption. As a prerequisite for the competent use of blockchains, the risks for the participants have to be assessed. In order to evaluate the security of the diverse proposals for the use of blockchain technology – or, more generally, of the so-called distributed ledger systems – interdisciplinary fundamental research is necessary.

First and foremost, cryptographic research in the field of this technology should be fostered with the aim of building a theoretical foundation. There are already promising approaches towards appropriate security models for existing blockchains. However, modelling in a more restrictive cryptographic sense is complicated by the economic assumptions reflecting the participants' behaviour. Therefore, aspects of game theory have to be incorporated. In the mid- to long-terms, interdisciplinary efforts should be able to provide precise risk assessments and security evaluations.

In addition, scalability of blockchain technology is a major challenge. The Proof-of-Work used by common blockchain protocols such as the Bitcoin cryptocurrency consumes an enormous amount of energy. Still, a concept that ensures reaching consensus in an open environment where everybody can join the network is essential. Therefore, alternatives to Proof-of-Work such as Proof-of-Stake or Proof-of-Space should be evaluated and considered within the security models. The replacement of a protocol component interferes with former security assumptions, thus concepts to integrate modified security assumptions should be developed.

Another important long-term goal for improving scalability is to develop second layer off-chain protocols. In these protocols, the massive bulk of transactions is kept off-chain thereby significantly improving transaction throughput and decreasing latency of transaction processing. As the design of secure off-chain protocols – in particular for the off-chain execution of smart contracts – is complex, sound cryptographic models are needed to ensure high standards of security.

In the mid-term, an analysis of different applications and a comparison with other established solutions without blockchains should be performed. The diverse applications can be systematically evaluated and labelled with recommendations and security assessments. Here, the use of blockchains to improve cryptographic systems should be distinguished from direct applications of blockchain technology e.g., shared databases for participants who do not trust each other. In the first case, the aim is to decentralise cryptographic schemes whose security relies on trustworthy entities. In the second case, especially applications integrating smart contracts should be considered.

Course of Action: Security of Blockchain Technology

Short-term goals:
- ▷ Extraction of and agreement on provable security properties of blockchains
- ▷ Evaluation of the advantages and disadvantages of alternatives to Proof-of-Work
- ▷ Concepts for and feasibility studies on digital alternatives for usual options known from centrally controlled currencies

Mid-term goals:
- ▷ Cryptographically valid, standardised security evaluation of blockchain systems
- ▷ Enhancing efficiency and scalability
- ▷ Development of hardware components to enable un-hackable wallets
- ▷ Methods for rollback of transactions
- ▷ Authentication or identity concepts with "revocable anonymity"

Long-term goals:
- ▷ Long-term security, i.e. methods to integrate modified security assumptions and to replace protocol components
- ▷ Design and analysis of secure off-chain protocols
- ▷ Establishment of a standardised formal intermediate language to design smart contracts

We suggest a strong European participation in the IEEE campaign proposed in November 2017 in the white paper entitled "Reinforcing the Links of the Blockchain" to create an interdisciplinary, unbiased haven with members from economy, industry and research.

Competent Handling of Cryptocurrencies and Smart Contracts

In order to recommend a cryptocurrency as a valid alternative to approved centrally controlled currencies, it has to pass security tests comprising matters of exchange, rollbacks, secured personal wallets and secure pseudonymous payment that simultaneously allow for traceability to identify money laundering.

First of all, suitable concepts for the digital alternatives to usual options known from hard money have to be designed. A subsequent feasibility study will identify the concepts to be elaborated. Here, those concepts should be preferred which are assumed to be secure according to security models for blockchains established so far. In the long term, usability aspects should be incorporated.

Furthermore, comprehensive state-supported protection concepts against cryptocurrency hacks, especially against hacker attacks (of all kinds) on the ownership of crypto money, should be pursued. In doing so, no central entity should be established, but decentralisation

should be stabilised by protecting the weak spots at individual levels e.g., by un-hackable hardware wallets.

Simultaneously, it has to be elaborated how stakeholders from a governmental and business perspective can apply the legal mechanisms against illegally acquired or traded crypto money. In addition, the question arises as to how a modern regulatory system can solve the challenges to the rule of law. Are there technical alternatives to hardfork in case of unintended or illegal transactions? At this point, the interface between the digital and physical worlds is problematic, especially if one has to deal with money laundering, export and trading bans or monetary flows of criminal organisations. Is it even possible to combine authentication or identity concepts with so-called revocable anonymity?

There is demand for comprehensible smart contracts. Is it possible to develop in the mid term a formal intermediate language which generates a code based on a sequence of actions to be automatised, and thus drafts a smart contract which can be formally verified and understood by non-experts? What kind of legal and technical possibilities besides rollbacks exist in the case of incorrect execution or a dispute? From a legal point of view, the question arises as to how the content of the smart contract and the details of the applied algorithm can be translated into a comprehensible format. Based on this, it can be argued that an increased use of smart contracts can have an institutional dimension, also called software as institution, if the automatic enforcement of rights induces a possible control over behaviour or social interaction.

Further Reading

[1] BSI. *Blockchain sicher gestalten – Eckpunkte des BSI*. 2018. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Eckpunktepapier.pdf (visited on 06/19/2018).

[2] IEEE Future Directions. *White Paper – Reinforcing the Links of the Blockchain*. 2017. URL: https://blockchain.ieee.org/images/files/pdf/ieee-future-directions-blockchain-white-paper.pdf (visited on 06/19/2018).

[3] Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. "The Bitcoin Backbone Protocol with Chains of Variable Difficulty". In: *CRYPTO 2017*. 2017, pp. 291–323. DOI: 10.1007/978-3-319-63688-7_10.

[4] Markus Kaulartz. "Smart Dispute Resolution". In: *DSRI 2017*. 2017, p. 599.

[5] Markus Kaulartz and Jörn Heckmann. "Smart Contracts – Anwendungen der Blockchain-Technologie". In: *CR 2016*. 2016, p. 618.

[6] Arvind Narayanan and Jeremy Clark. "Bitcoin's academic pedigree". In: *Commun. ACM* 60.12 (2017), pp. 36–45. DOI: 10.1145/3132259.

[7] Orwat et al. *Software als Institution, Informatik Spektrum 2010,* p. 626.

3. Accountability and Transparency for Information Quality

> **Scenario:** *In the 2018 Brazilian presidential race, several companies used the messenger service WhatsApp to spread discrediting misinformation about one of the candidates by sending messages to hundreds of millions of users. This current example of attempted election manipulation shows the scope that targeted political propaganda has reached. The use of a private messenger service makes it even more difficult for the individual to detect misinformation since it is often passed on by people the user trusts.*

As more and more people are using the Internet as their main method of communication and source of information, the accountability and transparency of this information and its sources have become a crucial issue. The vast amount of information that is provided and shared on the Internet makes it difficult for the individual users to differentiate between trustworthy and fake or misleading information. Furthermore, the origin and authors of the information are often unknown and, as a consequence, can rarely be held accountable for untrue and discrediting statements. This has paved the way for the emergence of digital disinformation campaigns in recent years. Social media platforms in particular – such as Facebook, Twitter, and YouTube – have made negative headlines as being used by private groups or foreign state actors to purposefully distribute misleading information to influence public discourse and democratic elections. In the U.S. presidential election campaign of 2016, the UK Brexit Referendum, and the most recent German, French and Brazilian parliament elections fake user accounts on social media, often operated by so-called social bots, were used to deliberately spread false information and tried to manipulate political opinion. Even though it is not yet clear to what extent voters were actually influenced, it has become evident that these deliberate attacks on democratic discourse and elections are an increasing threat as digital disinformation campaigns and computational propaganda on the Internet are becoming technically easier.

Online social platforms use algorithms to predict what users want to see in order to promote engagement and generate revenue on the platform. Based on a user's preferences, clicks and likes, algorithms filter and prioritise the content the user sees. As users interact and engage more with content that triggers an emotional response or confirms existing bias, this type of content is prioritised by the platforms and being shown and recommended to more users. This algorithmic prioritisation of content can potentially isolate different user groups within echo chambers and contribute to political polarisation.

As a consequence of the ever-increasing user profiling by the social platforms, the user is particularly susceptible to so-called microtargeting, which allows to address and advertise to highly tailored groups of users, who share certain interests or demographics, for example for political purposes. Distinguishing between trustworthy factual and false information is a challenge for the user, especially when that information is shared by people that he or she trusts or prioritised by the platform that he or she uses on a daily basis.

In the near future, advancements in machine learning research will exacerbate the problem, making it possible to create false but deceptively realistic images, audio tracks and videos (so-called deepfakes), which will likely be utilised for computational propaganda.

Course of Action: Accountability and Transparency for Information Quality

Short-term goals:

- ▷ Assessment of the actual impact of targeted misinformation
- ▷ Assessment of the legal framework with regards to the freedom of expression and the use of micro-targeting and propaganda
- ▷ Assessment of societal agreement with regards to the use of micro-targeting and propaganda as means of democratic discourse
- ▷ User awareness for micro-targeting and digital disinformation campaigns

Mid-term goals:

- ▷ Assessment of means and methods for automated detection and backtracing of false information
- ▷ Assessment of the need and options for regulation of accountability and transparency of information on a national, European and global scale

Long-term goals:

- ▷ Automated analysis of the trustworthiness of information and sources
- ▷ Creation of usable end-user tools for information trustworthiness

To adequately address the issue of digital disinformation and propaganda campaigns on the Internet, an interdisciplinary research approach has to be taken, which combines technological, legal and social aspects.

As a first step, the actual impact of microtargeting and digital disinformation has to be examined to establish a common base for further research. As a second step, the awareness of these mechanisms has to be raised among the users.

From a legal perspective, the line between permitted free expression of opinion, e.g., exaggeration and aggravation, and deliberate disinformation and propaganda has to be clearly identified. The extent to which microtargeting and propaganda are accepted by society and legitimately contribute to public and political discourse also has to be evaluated. Based on that evaluation, it must be determined whether additional regulation for platforms and actors is necessary and which instruments could be enforceable, both on a national and international level.

In addition to social and legal research, computer science methods for an automated detection and backtracing of digital disinformation campaigns and social bot activity have to be investigated. Automated recognition of disinformation is hardly possible on the basis of content, since current algorithms do not understand semantics such as half-truths, exaggerations or irony. But recognition might be possible for specific domains or on the basis of behaviour or distribution patterns. The goal is to be able to automatically analyse the trustworthiness of information or sources. In the long term, end users must be provided with effective tools to assess the truthfulness of information, why they see this information and the trustworthiness of sources.

Further Reading

[1] Marco Bastos and Dan Mercea. "The public accountability of social platforms: lessons from a study on bots and trolls in the Brexit campaign". In: *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 376.2128 (2018). ISSN: 1364-503X. DOI: 10.1098/rsta.2018.0003. URL: http://rsta.royalsocietypublishing.org/content/376/2128/20180003.

[2] Philip N. Howard, Samuel Woolley, and Ryan Calo. "Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration". In: *Journal of Information Technology & Politics* 15.2 (2018), pp. 81–93. DOI: 10.1080/19331681.2018.1448735.

[3] T. Hwang and Atlantic Council of the United States. Dinu Patriciu Eurasia Center. *Digital Disinformation: A Primer*. Atlantic Council, 2017. URL: https://books.google.de/books?id=E2mvswEACAAJ.

[4] Harri Jalonen et al. "Understanding the Trolling Phenomenon: The Automated Detection of Bots and Cyborgs in the Social Media". In: *Journal of Information Warfare* 15 (Dec. 2016), pp. 100–111.

[5] Dhiraj Murthy et al. "Automation, Algorithms, and Politics| Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital". In: *International Journal of Communication* 10 (2016). ISSN: 1932-8036. URL: https://ijoc.org/index.php/ijoc/article/view/6271.

[6] Onur Varol et al. "Online Human-Bot Interactions: Detection, Estimation, and Characterization". In: (2017). URL: https://aaai.org/ocs/index.php/ICWSM/ICWSM17/paper/view/15587.

4. User-centric Privacy Tools

> **Scenario:** *In the event that a user wants to upload a post or message to the Internet, a user-centric tool could be an app which locally calculates possible correlations and inferences of the text or photo from already published data about the user. The aim of the app would be to warn the user before publication, if, on the basis of information already known, he or she would reveal more than the post says on its own e.g., use of identical user name, phrasing, metadata to the user's prior post on a health advice forum.*

From a mere communication network, the Internet has rapidly evolved into a global platform for social networking, entertainment, education, trade, and political activism, used by more than two billion users. Users have matured from mere consumers of information to content publishers and interactive participants in blogs, tweets, social networks, and other online communities.

In this context, assuring online privacy of individual end-users has become a formidable and largely unsolved problem. Personal information is being widely dispersed in the Web. Social networks, in particular, have become a focal point for collecting data from billions of people. Users are therefore often overwhelmed by the complexity of online data accessibility and dissemination in an ever-growing technical landscape. Today, it is almost impossible for regular users to understand the privacy implications entailed, like the spreading of private posts within their network, or the reality and possible effects of linking information across multiple sites and platforms. Yet, users are offered little to no support for comprehending their privacy exposure, and struggle with privacy settings that are technically motivated and notoriously difficult to handle. Furthermore, there is the complicating factor that potential risks often only arise over the course of several years due to the increasing volume of data about a particular person on the Internet (so-called digital footprints), which makes it all the more difficult for individuals to trace the links. Often data comes into play which the user has forgotten that he or she had already disclosed at an earlier point in time. As a result, the user loses more and more control over his or her own data.

It is therefore not sufficient, if IT security research only addresses the operator side. While it is necessary to establish privacy-by-design standards and best practices for privacy engineering as a key engineering focus for developers, in addition, users themselves must be empowered. The individual users must be provided with the necessary information and, above all, suitable and manageable tools to enable them to understand the risks and, based on this, to control and thus protect their data. To this end, existing technologies are to be analysed for existing usage barriers in order to develop new user-centric tools in the long term. At the same time, privacy risks must be better understood in order to inform users. Therefore, a unified approach to privacy understanding and control has to be taken. Also, for the information and tools to be usable, manageable and meaningful, interdisciplinary efforts in the field of usability, human-computer interaction and psychology research must be intensified.

Overall, the aim is to provide the interested user with information in a suitable way as well as easy-to-use tools to effectively protect his or her privacy.

Course of Action: User-centric Privacy Tools

Short-term goals:

- ▷ Analysis of areas, in which tools of self-data-protection are useful and necessary
- ▷ Analysis of existing tools to find potential barriers of usage
- ▷ Further improvement and development of user-focused privacy tools

Mid-term goals:

- ▷ Usability research of user-centric privacy tools, in particular analysis of how users perceive information and how risks for data protection can be communicated
- ▷ Training courses and material to raise awareness of privacy risks
- ▷ Standards and best practices for privacy engineering

Long-term goals:

- ▷ Development of usable new tools which support user-decisions by providing information and by technically enforcing them

Further Reading

[1] Michael Backes et al. "On Profile Linkability despite Anonymity in Social Media Systems". In: *ACM Workshop on Privacy in the Electronic Society (WPES) 2016*. 2016. URL: https://publications.cispa.saarland/769/.

[2] Jinyuan Jia and Neil Zhenqiang Gong. "AttriGuard: A Practical Defense Against Attribute Inference Attacks via Adversarial Machine Learning". In: *USENIX Security 2018*. Baltimore, MD: USENIX Association, 2018, pp. 513–529. ISBN: 978-1-931971-46-1. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/jia-jinyuan.

[3] Yang Zhang et al. "Tagvisor: A Privacy Advisor for Sharing Hashtags". In: *Proceedings of the Web Conference 2018 (WWW)*. ACM, 2018. URL: https://publications.cispa.saarland/1443/.

5. Remotely Un-hackable PC

> **Scenario:** *The "Secure Inter-Network Architecture" (SINA), which was co-developed by the BSI, is used for governmental computers of normal to high security levels. Other solutions for highly secured computers exist. What has to be done to make them usable for home applications?*

The components of a remotely un-hackable system ideally have no influence on each other or are bound to strict protocols controlling the interaction. Thus, even if one programme gets compromised, all other programmes will remain unaffected. The objective is to develop a remotely un-hackable personal computer (RUPC) for private use. Thus, it is a manageable example of a trustworthy platform. The main focus of the RUPC development is on usability.

A first (technical) step towards the RUPC is the deployment of trustworthy hardware security modules, an "un-hackable" kernel and a hardened operating system. As a starting point for RUPC development, already existing components can be used. In this case, the obstacle is to ensure the secure usage despite unknown source code or hardware architecture for example. Suitable (preferably Open Source) solutions have to be selected and further developed, following state-of-the-art practices of safe and secure programming, such as systematic programme analysis and testing, compiler-based code hardening or even (if needed) formal verification of selected key components. In parallel, requirements for usability are to be formulated and tested. As a second step, such a PC should be extended by common browsers and office packages that run without any restrictions to their usability. In the mid term, a full-featured, user-friendly RUPC should be built.

During this approach, it is important to develop the RUPC in such a way that its security properties are also compatible with new concepts of user interaction such as the further development of intelligent personal assistants (IPA). The long-term challenge is to incorporate functionalities for inter-connectedness and exchange between different

Course of Action: Remotely Un-hackable PC

Short-term goals:

- ▷ Deployment of trustworthy hardware security modules, hardened kernel and hardened operating system
- ▷ Specification of usability requirements

Mid-term goals:

- ▷ RUPC extended by common browser and office packages
- ▷ Usability tests

Long-term goals:

- ▷ Full-featured, user-friendly RUPC
- ▷ AI based usability, remotely un-hackable intelligent personal assistant

programmes and data. Thus, the balancing act between security features such as data protection, separation of data, etc. and the request for transparency has to be managed.

Further Reading

[1] ENISA. *Hardware Threat Landscape and Good Practice Guide*. 2017. URL: https://www.enisa.europa.eu/publications/hardware-threat-landscape (visited on 06/19/2018).

[2] Joanna Rutkowska and Rafal Wojtczuk. *Qubes OS Architechture*. Version 0.3. 2010. URL: https://www.invisiblethingslab.com/resources/2014/Software_compartmentalization_vs_physical_separation.pdf (visited on 06/22/2018).

6. IT Security for Autonomous Driving

> **Scenario:** *With 100 million lines of code, a modern vehicle is one of the most complex electronic systems ever built. Users want to improve driving safety by networking the vehicle with the environment in order to get traffic information and automatic assistance when driving. An indispensable assumption, however, is that the vehicle cannot be controlled illegitimately from outside.*

If vehicles are to take over tasks which, up to now, have been the responsibility of the driver, an increasing automation and networking of these vehicles with each other and with the infrastructure are necessary. Not only are new vehicle systems being created, but also a new ecosystem, the Internet of Vehicles (IoV). The external threat surface increases with the number of interfaces and the interconnectedness. The successful manipulation of one car can have an impact on the swarm behaviour of all other vehicles. At the same time, the demands on data protection are increasing as a consequence of the collection and processing of data for the autonomous management of complex driving situations. For the security of vehicles in general and in particular for autonomous driving, almost all known security issues are important – a combination of systems is the major challenge.

Vehicle Security Architecture

The development of a trusted platform for autonomous vehicles should be based on the conception of a vehicle-wide security architecture.

- ▷ Protect and measure the code integrity of controllers and monitor their behaviour
- ▷ Instantiate "secure identities" in the vehicle as sources of confidence for further security measures
- ▷ Trusted in-vehicle data transmission and storage based on input from standardisation activities such as AUTOSAR
- ▷ Trustworthy communication with external entities taking into account the data protection interests of the occupants
- ▷ Develop learning methods for adaption of attack classifiers and selection of an appropriate response
- ▷ Develop formal methods and test methods to demonstrate the required level of autonomous vehicle security

Security by Design and Crypto Agility

The integration of security consideration into the development process should enforce, in particular, security requirements management for the entire lifecycle of the product, even after the start of production.

It is expected that autonomous driving would be based on AI technologies in many areas, like intelligent navigation in metropolitan areas, or image recognition of the traffic and others. Such AI systems must be designed robustly against attackers; "security by design" for AI needs new guidelines.

Course of Action: IT Security for Autonomous Driving

Short-term goals:
- ▷ Prevent attacks on the assistance systems by security measures already in the design
- ▷ Vehicles with secure identities and trust anchors
- ▷ Self-monitoring, attack detection and safe fallback mode

Mid-term goals:
- ▷ Self-learning and self-adaption for in-vehicle intrusions detection and mitigation systems

Long-term goals:
- ▷ Automated countermeasures

Particular attention is paid to the aspect of cryptography. Vehicles must be safe for a very long period of 20-30 years (from the beginning of the development of a new series of vehicles until scrapping of the last vehicle in that series). The security of cryptographic processes can be expected to erode during that time, and the number of minimum security parameters will be increasing. In the worst case, entire procedures will have to be replaced. In particular, the introduction of new methods, for example in the field of post-quantum cryptography (PQC), may require the exchange of procedures and protocols during the life of a vehicle series. Therefore, cryptographic processes have to be implemented agilely from the beginning, so that they can be easily updated or exchanged if necessary even in an extremely heterogeneous vehicle network.

First of all, it is important to provide IT security for partial automation, which means that the system monitors the driving environment, and driver assistance systems help with vehicle operation. Attacks on the assistance systems must be prevented by security measures already during the design. Therefore, vehicles have secure identities and trust anchors. The system must continue to monitor itself, detect attacks, warn the driver and, if necessary, place the controller in a safe fallback mode. In the medium term, IT security has to provide for conditional automation. The system gradually assumes autonomous control, with the expectation that the driver reacts when required. Autonomous systems have to learn by themselves and adapt the behaviour to new situations and new insights during the operational phase. Systems for detecting and mitigating the effects of attacks also need to learn and adapt. In the long-term, IT security has to cope with high/full automation. Fully autonomous driving also requires fully automated countermeasures in the event of attacks.

Further Reading

[1] ENISA. *Cyber Security and Resilience of smart cars.* Tech. rep. 2016. DOI: 10.2824/87614.

[2] Ruben Niederhagen and Michael Waidner. *Practical Post-Quantum Cryptography*. Tech. rep. Fraunhofer SIT, 2017. URL: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Practical.PostQuantum.Cryptography_WP_FraunhoferSIT.pdf.

[3] Roland Rieke et al. "Behavior Analysis for Safety and Security in Automotive Systems". In: *Parallel, Distributed and Network-Based Processing (PDP), 2017*. IEEE Computer Society, 2017, pp. 381–385. DOI: 10.1109/PDP.2017.67.

[4] SAE International. *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. Tech. rep. J3061. 2016. URL: http://standards.sae.org/wip/j3061/.

[5] Daniel Zelle et al. "On Using TLS to Secure In-Vehicle Networks". In: *International Conference on Availability, Reliability and Security, 2017*. 2017, 67:1–67:10. DOI: 10.1145/3098954.3105824.

Further Reading

We recommend the following projects and position papers of our colleagues from all over Europe. In addition to our roadmap, these provide a multi-faceted perspective on the cybersecurity agenda by the different stakeholders in Europe.

[1] The CANVAS-Project - Constructing an Alliance for Value-driven Cybersecurity. URL: https://canvas-project.eu.

[2] The CyBOK-Project - The Cybersecurity Body of Knowledge. URL: https://cybok.org.

[3] The EUNITY-Project - Cybersecurity and Privacy Dialogue between Europe and Japan. URL: https://eunity-project.eu.

[4] ECSO - European Cyber Security Organisation. *Strategic Research and Innovation Agenda*. 2017. URL: https://www.ecs-org.eu/documents/publications/59e615c9dd8f1.pdf.

[5] ENISA - European Union Agency for Network and Information Security. *Looking into the crystal ball: A report on emerging technologies and security challenges*. 2017. URL: https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball/.

[6] ENISA - European Union Agency for Network and Information Security. *Threat Landscape Report 2017*. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

[7] Jean-Gabriel Ganascia, Eric Germain, and Claude Kirchner. *Sovereignty in the Digital Age – Keeping control over our choices and values*. 2018. URL: http://cerna-ethics-allistene.org/digitalAssets/55/55817_Sovereignty_CERNA_2018.pdf.

[8] JRC - Joint Research Centre, European Commission. *European Cybersecurity Centres of Expertise Map – Definitions and Taxonomy*. 2018. URL: http://publications.jrc.ec.europa.eu/repository/handle/JRC111441.

[9] SAM - European Commission's Scientific Advice Mechanism. *Cybersecurity in the European Digital Single Market*. 2017. URL: https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf.

[10] Jörn Müller-Quade, Ralf Reussner, and Jürgen Beyerer. *Karlsruher Thesen zur Digitalen Souveränität Europas*. 2017. URL: https://www.iosb.fraunhofer.de/servlet/is/78237/.

[11] syssec. *The Red Book: A Roadmap for Systems Security Research*. 2013. URL: http://www.red-book.eu/m/documents/syssec_red_book.pdf.

[12] Volker Wittphal, ed. *Digitale Souveränität: Bürger – Unternehmen – Staat*. iit-Themenband. Springer Vieweg, Berlin, Heidelberg, 2017. DOI: 10.1007/978-3-662-55796-9.

secUnity Partners

CISPA - Helmholtz Center for Information Security
https://cispa.saarland

CRISP – National Research Center for Applied Cybersecurity
https://crisp-da.de

KASTEL - Competence Center for Applied Security Technology
https://kastel.kit.edu

Fraunhofer Institute for Applied and Integrated Security (AISEC)
https://aisec.fraunhofer.de

Fraunhofer Institute for Secure Information Technology (SIT)
https://sit.fraunhofer.de

Karlsruhe Institute of Technology (KIT)
Research Group Cryptography and IT Security
https://kit.edu

Karlsruhe Institute of Technology (KIT)
Zentrum für Angewandte Rechtswissenschaft (ZAR)
https://kit.edu

Ruhr-Universität Bochum
Research Group Systems Security
https://rub.de

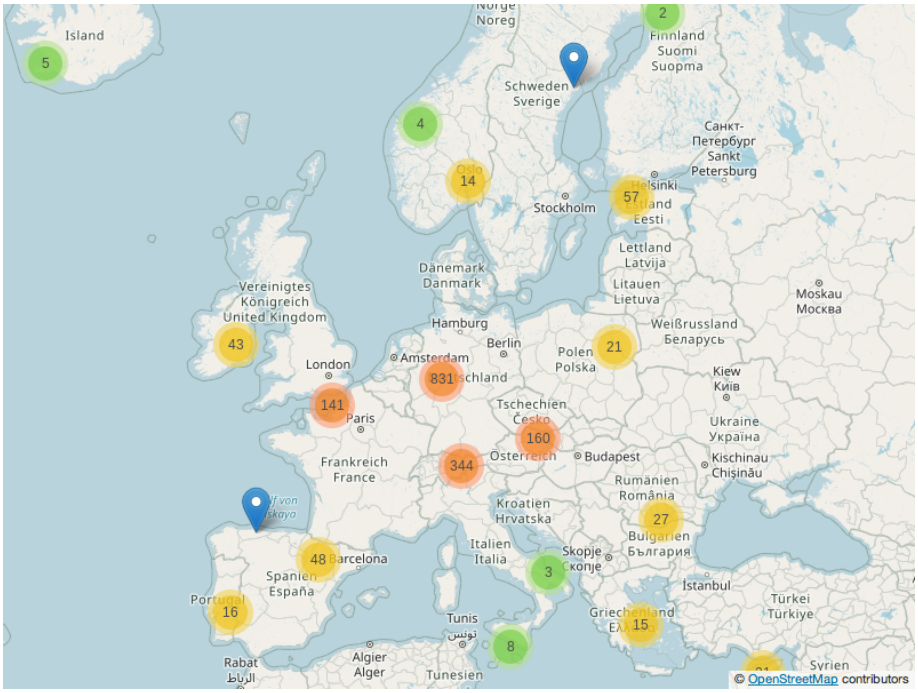
Technische Universität Darmstadt
Research Group Software & Digital Business
https://www.tu-darmstadt.de

About secUnity

The secUnity project is funded by the German Federal Ministry of Education and Research (BMBF) to support IT security research in Germany and Europe since its launch in 2016. The joint interdisciplinary project pools the expertise for European IT security research and policy of the secUnity partners. Its main objective is to support sustainable interdisciplinary networking in cybersecurity research by fostering a dialogue to obtain a vision and roadmap of long-term cybersecurity research policy for Europe.

The roadmapping process is one of the central objectives of the project and involved dozens of European experts. Many distinguished scientists from academic and industrial research contributed as co-authors of the final roadmap document.

IT Security Map



Map data © OpenStreetMap contributors

The IT Security Map contains a comprehensive overview of over 1,700 European stakeholders, ranging from all fields and areas of cybersecurity: from education, research and development institutions up to small, medium and large enterprises offering technical, economical and legal expertise in the fields of cyber and data security. All entries are sorted by an underlying, specifically developed taxonomy and can be searched by tags.

The survey of the stakeholders was initially performed solely by the project team, but is now growing with new participants continuously joining the platform through a manually verified online form. In this way, every stakeholder in cybersecurity in Europe is welcome to join the IT Security Map.

Contact:

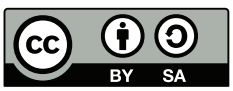
Karlsruhe Institute of Technology (KIT)
Institute of Theoretical Informatics
Jörn Müller-Quade
Am Fasanengarten 5
76131 Karlsruhe
Germany
E-Mail: contact@it-security-map.eu
URL: it-security-map.eu

Cite as:

Jörn Müller-Quade (ed.)
Cybersecurity Research: Challenges and Course of Action
by secUnity – supporting the security community, 2019
DOI: 10.5445/IR/1000090060

Legal notice:

This publication represents the views and interpretations of the authors. Third-party sources are quoted as appropriate. secUnity and the authors are not responsible for the content of the external sources including external websites referenced in this publication.
The project secUnity is funded by the German Federal Ministry of Education and Research.



SPONSORED BY THE

Federal Ministry
of Education
and Research

secUnity

supporting the security community

https://it-security-map.eu