Cybersecurity Research: Challenges and Course of Action

secUnity

supporting the security community

Roadmap

Roland Rieke, St. Petersburg 10.10.2019
Slides based on work of the secUnity team

secUnity-Roadmap on Cybersecurity Research

Target Groups:

- Informed and invested political stakeholders in cybersecurity in the EU and its member states
- Stakeholders from research and development (industry and academia) in cybersecurity in the EU

Objective:

- Identify the challenges for IT Security and accordingly IT security research
- Target-setting for civilian IT Security Research in the short, mid- and long-term

Release:

- 5th Feb 2019 in Brussels in cooperation with the Representation of the State of Hessen to the EU
- Online: it-security-map.eu/de/roadmap/secunity-roadmap/
- DOI: 10.5445/IR/1000090060 (open access)

The project secUnity was funded by the German Federal Ministry of Education and Research.

Content

A. Key Challenges

1. Securing Cryptographic Systems against Emerging Attacks
2. Trustworthy Platforms
3. Secure Lifecycle Despite of Less Trustworthy Components
4. Quantifying Security
5. IT Security and Data Protection for Machine Learning
6. Big Data Privacy

B. Interdisciplinary Challenges

1. Measurable, Risk-adequate Security in Law
2. Holistic Human-centred Security and Privacy Research
3. Digital Business Models for a Fair Economy and Society

C. Technologies and Applications

1. Safeguarding Key Services of the Internet
2. Security of Blockchain Technology
3. Accountability and Transparency for Information Quality
4. User-centric privacy tools
5. Remotely Un-hackable PC
6. IT Security for Autonomous Driving

Cybersecurity Research:
Challenges and Course of Action

secUnity
supporting the security community

Chapter A: Key Challenges

A1. Securing Cryptographic Systems against Emerging Attacks

Scenario:

- Cryptography is designed to protect threatened assets.
- 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.
- At some point in the future, the *quantum computer* will arise and question the fundamentals of how asymmetric cryptography is designed and implemented today.

A1. Securing Cryptographic Systems against Emerging Attacks

Problem: variety of brute-force and physical attacks on critical applications

Required: transition to PQC (hybrid systems) and implement PQC secure against side-channel, fault or invasive attacks

Required: research on „crypto-agile“ systems, i.e. flexible platforms, generic cryptographic accelerators

Problem: new attacks with a) machine learning and b) on computer architecture (Spectre …)

Required: new paradigm for „Making the common case fast“

A1. Course of Action

Short-term	• Development of post-quantum algorithms, mitigation techniques for cache-timing and other implementation attacks • Design of resilient computer architectures
Mid-term	• Standardization and Dissemination of post-quantum algorithms • Implementation of the resilient architectures
Long-term	• Commercial spread of the resilient architectures

A2. 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 charging infrastructure.
- Charge points have to reliably handle the authentication of customers and authorization of charging sessions and must provide the operator and energy supplier with correct and unmanipulated metering values.

A2. Trustworthy Platforms

Scenario:

- 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 (e.g. hardware security module HSM) within the charge point can be used to achieve this and build a chain of trust.

A2. Trustworthy Platforms

Problem: dynamically distributed computing tasks on devices controlled by adversaries and interactions with untrusted applications

Outdated: perimeter-based security architectures

Required: reliable identity and integrity assessment and modern concepts for data secrecy and privacy via

- Hardware-based trust anchors (e.g. TPM)
- Device Identity Composition Engine (DICE)
- Isolation mechanisms
- Design and integration of trustworthy protocols and applications

A2. Course of Action

Short-term	• Use of trust anchors such as TPM or DICE in PC-clients, servers, embedded systems • Trusted execution environments; e.g. microkernels and lightweight compartmentization • Software stack and middleware design and implementation
Mid-term	• Protocol integration and development for trust establishment and configuration / identity assessment • Trustworthy application design and system architecture specification
Long-term	• Implementation of automated reference value recognition and validation as well as their integration into all common implementations of the policies • Development of hardware trust anchors with Open Source hard- and firmware

A3. 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.
- 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.
- The facility will be maintained and 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.

A3. Secure Lifecycle Despite of Less Trustworthy Components

Required: coverage of all stages of the system‘s and its components‘ lifetime including legacy components, e.g. firmware updates, transition to PQC

Opportunities and challenges with open source soft- and hardware

Required: standards for integration of diff. components and protocols (esp. for IoT)

Foundation for secure systems:

- Secure and scalable infrastructures with trustworthy end points and isolation mechanisms
- Secure lifecycle management (software and subsystems)

A3. Course of Action

Short-term	• Develop suitable methods and tools to assess the security of systems and protect components
Mid-term	• Establish a secured infrastructure that was developed according the developed methods • Secure integration of components of different trustworthiness
Long-term	• Fully hardened infrastructure with a secure lifecycle management

A4. 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?

A4. Quantifying Security

Current situation: only heuristics available to judge a system’s security

Required: development of security metrics to

- Compare the security of two system versions (e.g. before and after a patch)
- Compare the benefit of different security measures (prioritization)

Difficult Problem! No single number will quantify security of a system.

Required: combination of measures from different sub fields of cybersecurity

- Furthering improved scientific rigor and a common language
- Combining logical, deductive approach and the empirical, deductive one
- Clarifying what aspects cannot be quantified

"Security" will never mean immunity against all attacks! …

A4. Course of Action

Short-term	• 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	• 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	• Achieve security quantification of complex example systems • Quantify security of real systems

A5. 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.
- E.g. 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.

A5. IT Security and Data Protection for Machine Learning

Problem: more highly developed ML/DNN in daily life; cyber attacks via ML

IT security for ML, i.e. adversarial and resilient ML

- Understand flaws on ML (e.g., mislearning, blind spots, insufficient generalization) by targeted attacks
- Improve resilience of ML (esp. for security appl. such as intrusion detection, malware analysis) by new methods and enhancing explainability and transparency

Privacy for ML, i.e. transparent and private ML

- Create responsibilities concerning classified data and results
- Develop data protection-friendly learning, attestation mechanisms

Required: definition "security for ML", evaluation of trained ML systems, concepts for traceability and fairness

A5. Course of Action

Short-term	• Formal definition of security in the context of ML • Enhancing trustworthiness in ML • Design of resilient computer architectures • Creation of an environment for tests and testing of already trained ML systems to detect empirically exceptional cases and limits of the systems
Mid-term	• Verifiable traceability and fairness of ML systems • Accountability of ML in relation to the processed data • Credibly communicate the results and trustworthiness of a ML system to the end user
Long-term	• Policies that specify which algorithms should be used in which situations and what guarantees they must provide • Implementation and control of the policies • Privacy-friendly ML and Private Modelling to allow value added without privacy risks

A6. Big Data Privacy

Scenario:

- Huge databases are created that record diverse sensitive medical and biological data.
- E.g. by the International Cancer Genome Consortium 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.
- Specialized variants of multi-party computation were successfully used for comparing genomes to optimize medical therapies.
- We need well-elaborated procedures to guarantee privacy while evaluating sensitive big data.

A6. Big Data Privacy

Problems: microtargeting, re-identification, revealing sensitive data, linkability

Anonymisation and Private Learning in Big Data:

- Adapt anonymisation methods to Big Data, i.e. address volume, velocity, and variety
- Enhance privacy, e.g., Private Learning, Private Modelling or synthetic data

Expanding Cryptographic Schemes for Secure Computation:

- Improve scalability and adapt methods such as MPC, data anonymisation, and computation on encrypted data to Big Data

Standard Procedures for Efficient Privacy-Preserving Analytics:

- Develop holistic approach for handling personalised, sensitive Big Data
- Include all processes, hardware and software, and networks for recording, storing, transferring, processing, and outputting data to guarantee protection of privacy
- Auditable security

A6. Course of Action

Short-term	• Extending and adapting (…) k-anonymity, l-diversity, t-closeness and Differential Privacy for Big Data • Use of trustworthy hardware security modules (… and) trusted initializer during preprocessing phase (…) • Implementation of MPC, secure against passive adversaries • Standards for isolated computers in data centres (auditable security)
Mid-term	• Development of new anonymization 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 (…) • Comprehensive database for efficient PPA solutions
Long-term	• Private Learning and Private Modelling in order to allow value added without privacy risks • Implementation of efficient MPC, secure against active adversaries • (…) fully homomorphic encryption and usable indistinguishability obfuscation • Establishing a standard procedure efficient PPA with suitable privacy measure

Cybersecurity Research:
Challenges and Course of Action

secUnity
supporting the security community

Chapter B: Interdisciplinary Challenges

B1. Measurable, Risk-adequate Security in Law

Scenario:

1. In his smart home, a consumer uses intelligent appliances such as smart speaker “Alexa” to control heating and power consumption. She is concerned about her privacy and wonders whether in times of big data, she can control her 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. The question arises as to what steps need to be taken to imply the technical and legal requirements for systems of “self data protection”.

B1. Measurable, Risk-adequate Security in Law

Digital sovereignty also finds its legal basis in cybersecurity law and data protection law regarding the guarantee and protection of rights ➔ rights of actors such as individuals, enterprises and (state-) institutions.

The sovereign European data economy includes data as a protective good particularly in cases of cross-border data flow. Problem: Still there is limited influence on the data flows.

Legal challenge 1: Incoherent legal structure; complex ICT-systems ➔ Need of a coherent legal frame work.

Legal challenge 2: Establishing a procedural method for a risk-adequate approach in data protection law balancing the different needs of protection.

B1. Course of Action

Short-term	• Systemization and classification of terms and definitions such as “Risk” and “State of the Art” in cybersecurity and data protection law
Mid-term	• Establishing a convergent structure of existing legal rules and statutes
Long-term	• Developing a quantitative risk-metric

B2. 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 configuration interfaces, assume they are.
- Correspondingly, it is likely that any of them uses the provided tools in an insecure way.

B2. Holistic Human-centred Security and Privacy Research

Problem: Gap between theoretical and actual security caused by unrealistic assumptions (e.g. on end users assuming good password choice)

New focus on software developers, system designers and administrators (instead of end user)

Required: Holistic and systematic approach for design of security/privacy critical systems (in contrast to traditional research)

Methodological challenges: selection of probands and in-depth replication study

B2. Course of Action

Short-term	• Identifying relevant problem areas and tools to help end users, software developers and administrators to increase information security and privacy • Developing and validating generalized theories and frameworks
Mid-term	• 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	• Merging lines of research covering all involved actors for a holistic approach • Contributing to standardisation activities

B3. 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.

B3. Digital Business Models for a fair Economy and Society

Current situation: Radical change of economy, everyday life, and society due to increasing digitalization and omnipresence of internet-based services

Problem: Ever-increasing vulnerability and simultaneous lack of awareness regarding privacy and security (among providers and users)

Problem: Increasing (data) inequality and imbalance of risks and benefits and simultaneous lack of governmental support and incentives

Problem: Necessity for adequate and FAIR technological, socio-economic, legal, etc. imperatives and business models for the age of digitalisation to ensure a strong European IT (security) economy

B3. Course of Action

Short-term	• Development of usable new tools which support user-decisions by providing information and by technically enforcing them
Mid-term	• Development and installation of an interdisciplinary research centre • Internat. comparative studies across EU countries on data sovereignty and fair business models • Roundtables with all involved stakeholders (industry, scientist, and citizens)
Long-term	• Exertion of influence on the design of data-driven, fair business models • Guarantee of enhanced data sovereignty for EU citizens

Cybersecurity Research:
Challenges and Course of Action

secUnity
supporting the security community

Chapter C: Technologies and Applications

C1. 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 in the routing infrastructure spread over the US affected several Internet service providers, leading to wide spread Internet outages.

C1. Safeguarding Key Services of the Internet

Problem: Internet as critical infrastructure

Required: secure and stable operation of central protocols, services and applications for reliable, integer and confidential internet communication

Problem: security extensions are associated with a higher resource consumption such as computational capacity, higher bandwidth, higher costs

Required: sophisticated measures to spread the neglected security features in the core Internet infrastructure

C1. Course of action

Short-term	• Analysis of adoption of security extensions for crucial protocols of the Internet infrastructure • Identification of misconfigurations
Mid-term	• Research for creating new technologies to detect and prevent misconfigurations • Identification of attack pattern and distinction from misconfigurations
Long-term	• Securing the Internet infrastructure • Global introduction and usage of secure protocols for the backbone of the Internet

C2. Security of Blockchain Technology

Scenario:

- The Bitcoin protocol was presented in a white paper in 2008 and implemented in 2009.
- It is the first successful example of a decentralized 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.

C2. Security of Blockchain Technology

Problem: not ready for mass adoption

Required: cryptographic research for theoretical foundation such as security models (incorporating game theory)

Major challenge: scalability of blockchain technology

- Replacement of Proof-of-Work by Proof-of-Stake, Proof-of-Space, etc.
- Sound crypto models and second layer off-chain protocols

Required: analysis and database of existing blockchains

Competent Handling of Crypto Currencies and Smart Contracts

- Concepts for digital alternatives for e.g. rollback… followed by feasibility studies
- Legal mechanisms against illegally acquired or traded crypto money
- Institutional dimension of smart contract (software as institution)

C2. Course of Action

Short-term	• 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 (…) centrally controlled currencies
Mid-term	• Cryptographically valid, standardised security evaluation of blockchain systems • Enhancing efficiency and scalability • Methods for rollback of transactions • Authentication or identity concepts with “revocable anonymity”
Long-term	• Long-term security, i.e. methods (…) to replace protocol components • Design and analysis of secure off-chain protocols • Establishment of a standardised formal intermediate language to design smart contracts

C3. 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 candidate 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.
- A private messenger service makes it more difficult for the individual to detect misinformation since it is often passed on by people the user trusts.

C3. Accountability and Transparency for Information Quality

Current situation: Internet main source of information, but often unknown origin of information or authors on e.g. social media platforms

Problem: ever-increasing user profiling by social platforms using prioritisation algorithms (echo chambers)

Problem: emergence of digital disinformation campaings due to technically advancements (social bots, ML & deep fakes)

Required: interdisciplinary effort on social, legal and technological level

- Social: determine actual impact of microtargeting and digital disinformation, raise awareness
- Legal: define line between permitted free expression of opinion and deliberate disinformation
- Technological: automated recognition of disinformation (based on e.g. distribution patterns)

C3. Course of Action

Short-term	• 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 microtargeting and propaganda as means of democratic discourse • User awareness for microtargeting and digital disinformation campaigns
Mid-term	• 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	• Automated analysis of the trustworthiness of information and sources • Creation of usable end-user tools for information trustworthiness

C4. User-centric Privacy Tools

Scenario:

- When 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, 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.

C4. User-centric Privacy Tools

Problem: non-transparent and unpredictable background processes of linking individual data, hence poor individual risk assessment

Problem: “digital footprints”, loss of control over individual data

Required: better understanding of privacy risks

Required: suitable and manageable tools for users enabling them to

- Understand the risk
- Control the users’ data (based on understanding provided by the tool)
- Effectively protect users’ privacy

C4. Course of Action

Short-term	• 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	• 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 for privacy engineering
Long-term	• Development of usable new tools which support user-decisions by providing information and by technically enforcing them

C5. Remotely unhackable PC

Scenario:

- The “Secure Inter-Network Architecture” (SINA), 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?

C5. Remotely unhackable PC

Required: Remotely unhackable PC for private use, i.e.

- Rule interactions between different components by strict protocols
- Focus on usability (during all development steps)

Suggest development of RUPC - starting from trustworthy hardware security modules, to systematic programme analysis, to office packages and common browsers …

Extension to intelligent personal assistants, AI

C5. Course of Action

Short-term	• Deployment of trustworthy hardware security modules, hardened kernel and operation system • Specification of usability requirements
Mid-term	• RUPC extended by common browser and office packages • Usability tests
Long-term	• Full-featured, user-friendly RUPC • AI-based usability, remotely un-hackable intelligent personal assistant

C6. 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.

C6. IT Security for Autonomous Driving

Problems for the new ecosystem Internet of Vehicles: increasing complexity, individual vs. swarm behaviour, adequate data protection

Vehicle Security Architecture: Build basis of trusted platform for autonomous vehicles

Security by Design and Crypto Agility:

Enforce security requirements management for the entire lifecycle

Design all involved AI-technologies (e.g., intelligent navigation, image recognition) robust against attackers

Secure crypto for 20-30 years via, e.g. an exchange management for protocols and procedures for vehicles and IoV (PQC)

C6. Course of Action

Short-term	• 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	• Self-learning and self-adaption for in-vehicle intrusions detection and mitigation systems
Long-term	• Automated countermeasures

Cybersecurity Research: Challenges and Course of Action

secUnity

supporting the security community

Thank you!