Digitale Souveränität:

Sicherheit und Privatsphäre in der Digitalen Gesellschaft

Prof. Dr. Michael Waidner

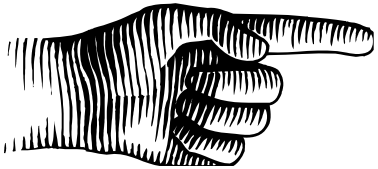
Technische Universität Darmstadt und
Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt

CASED

Future Internet Kongress
Frankfurt, 3. Dezember 2014

Fraunhofer
SIT

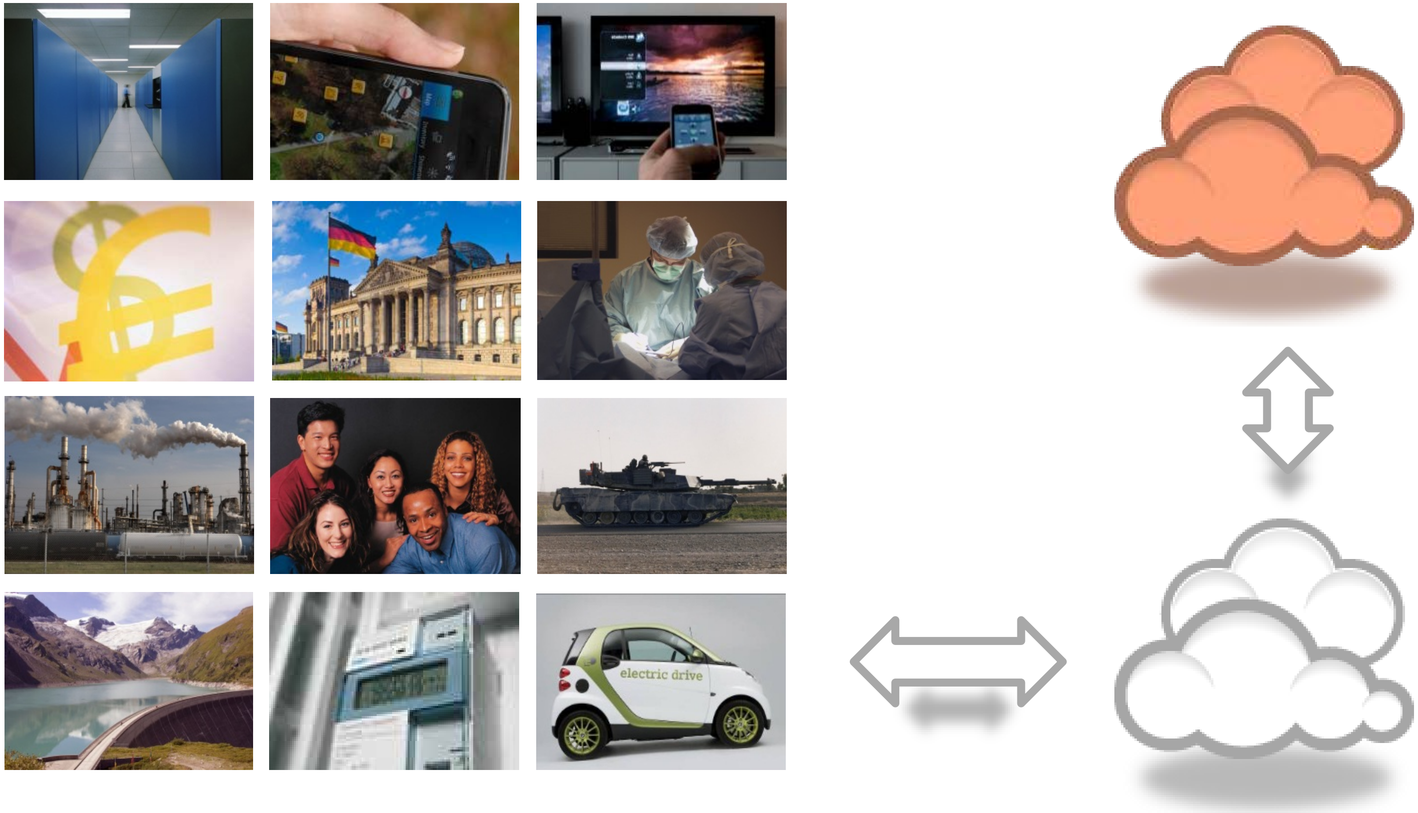
Agenda



- Digital Sovereignty: Objective and Reality
- Why is IT not Secure?
- What Needs to be Done?

»Digital Space« is Everywhere

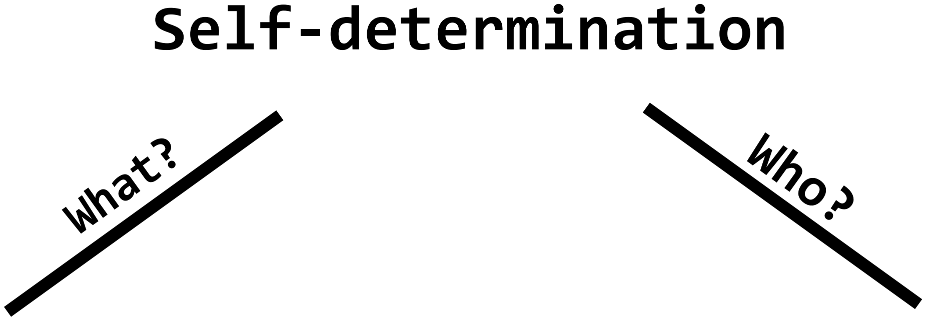
Connected, programmable, open and shared.
Generating massive amounts of data, often sensitive, mostly unstructured.



Every new technology, service, consumption, business model
creates new security and privacy challenges.

Digital Sovereignty: Objective

Self-determination in a digital world



1. »Gestaltbarkeit«: Ability to Shape the Digital World
2. Security
3. Privacy
4. Trust in the Quality of 1-3

- Citizen
- Enterprise
- Administration
- EU / States

Digital Sovereignty: Reality

Gestaltbarkeit	Limited
Security	Cybercrime, sabotage, espionage, individual surveillance, censorship
Privacy	Mass surveillance, profiling, data persistence, scoring, data analytics
Trust	Limited

Impact of Cybercrime and Espionage (Germany)

- **Cyber attacks considered serious threat by**
  74% of all enterprises[1], **85%** of all users[2]
  49% of all attacks are »opportunistic«[3]

- **Many got already hit by cyber attacks**
  38% of all users[1], **21%** with identity theft[2];
  30% of all enterprises with cyber crime [1],
  54% with industrial espionage, **>50%** through »hacking«[4]

- **Significant damages**
  40 **M€/a** in reported cases of computer fraud (reality likely **11x**)[5];
  40 **B€/a** (1,6% BIP) total cost of cyber crime[6],
  larger than total costs of car incidents)

Sources: (1) BITKOM 3/5 2014, (2) SCHUFA 9/2013, (3) IBM 3/2013, (4) Corporate Trust 7/2014, (5) BKA 8/2014, (6) Center for Strategic and International Studies 6/2014, (7) Bundesanstalt für Straßenwesen 8/2010

Prototypical Attacks

Targeted, organized, financially or politically motivated

Zeus Trojan and Botnet (2007)

Anonymous (2008)

Jérôme Kerviel vs.
Société Générale
(2008)

False Flag Operations:
"Iranian Cyber Army" vs.
"Baidu" Search Engine (2010)

DigiNotar (2011), RSA/Lockheed-Martin (2011),
Saudi Aramco (2012), EADS (2012), ...

Stuxnet (2010)

PRC Unit 61398, Shanghai (2013)

NSA / GCHQ Programs (2013/14)

Snowden Revelations on NSA/GCHQ Activities

PRISM

TEMPORA

TAO

BULLRUN

MYSTIC

MUSCULAR

HACIENDA

etc.

- **Mass surveillance** of Internet and mobile networks
- **Wiretapping** of selected individuals, including Chanceller Merkel
- Suspicion of support for **industrial espionage**
- Circular trading to **evade national law**
- **Direct access** auf cables satellites, Internet backbone, cloud providers in the USA/UK and likely also in EU/Germany
- **Manipulation** of central infrastructures (SSL PKIs, DNS, BGP)
- **Manipulation of supply chain** (»Tailored Access Operations«)
- **Systematic backdoors** in NIST standards, in specific products
- **Collection of vulnerabilities** in products

Commercial Data Collection (Examples)

facebook

android

Google

amazon

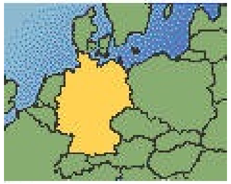
IBM |

VISA

MasterCard
Worldwide

doubleclick
by Google

Google Ads



vodafone

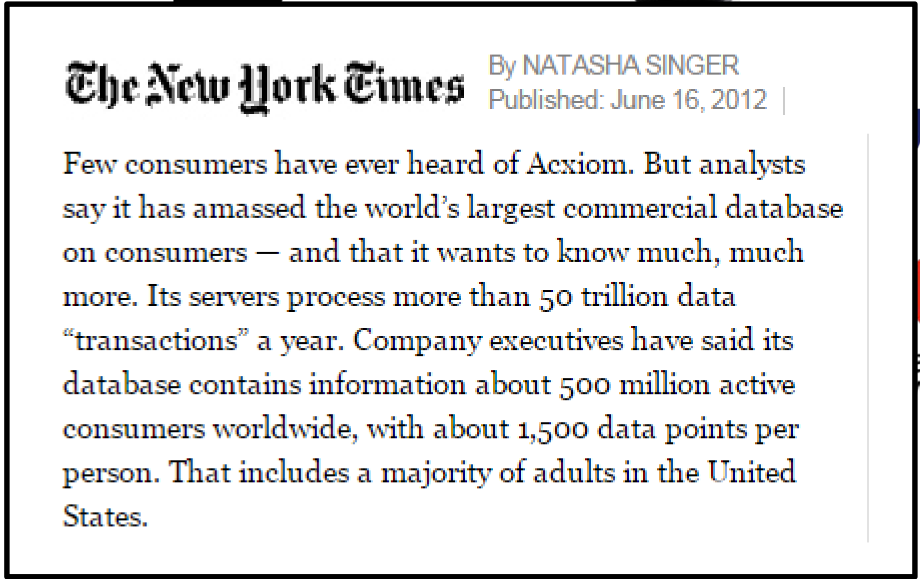
T · ·

PayPal

acxiom™

Source: Company web site

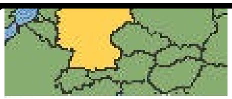
Commercial Data Collection (Examples)



The New York Times

By NATASHA SINGER
Published: June 16, 2012 |

Few consumers have ever heard of Acxiom. But analysts say it has amassed the world's largest commercial database on consumers — and that it wants to know much, much more. Its servers process more than 50 trillion data "transactions" a year. Company executives have said its database contains information about 500 million active consumers worldwide, with about 1,500 data points per person. That includes a majority of adults in the United States.



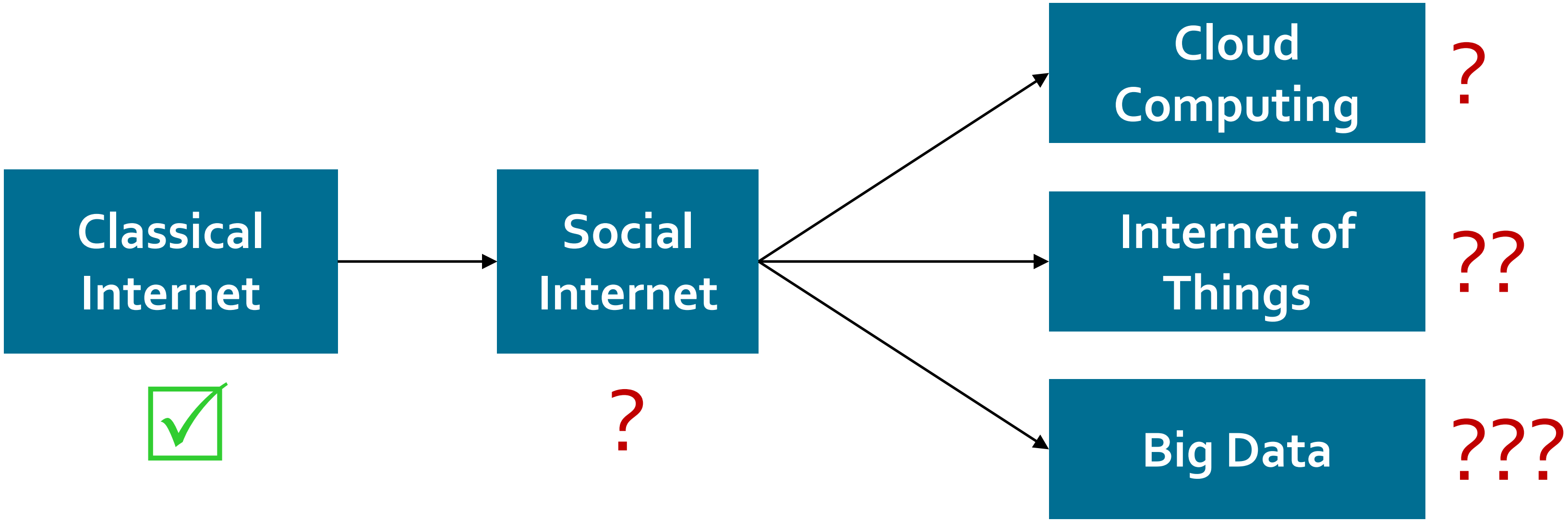
Source: Company web site

What is at Risk?

- **Informational Self-Determination:**
  - Individual: being observed / sense of being observed
  - Industry, government, society: influence over public / individual opinion + loss of control over data collections
- **Discrimination: Transparent citizens, enterprises**
- **Risk through centralized data silos**
  - Access by foreign services (e.g., as in PRISM)
  - Access by criminals (e.g., malware via ads, prep social engineering via online social networks)

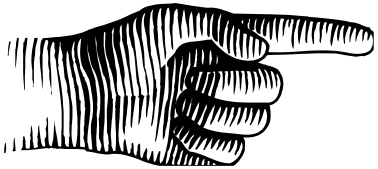
Research Challenges for Countering Loss of Privacy

Established technology concepts – data minimization, anonymity & pseudonymity, transparency & control – don’t work well in »new« environments



Agenda

- Digital Sovereignty: Objective and Reality



- Why is IT not Secure?
- What Needs to be Done?

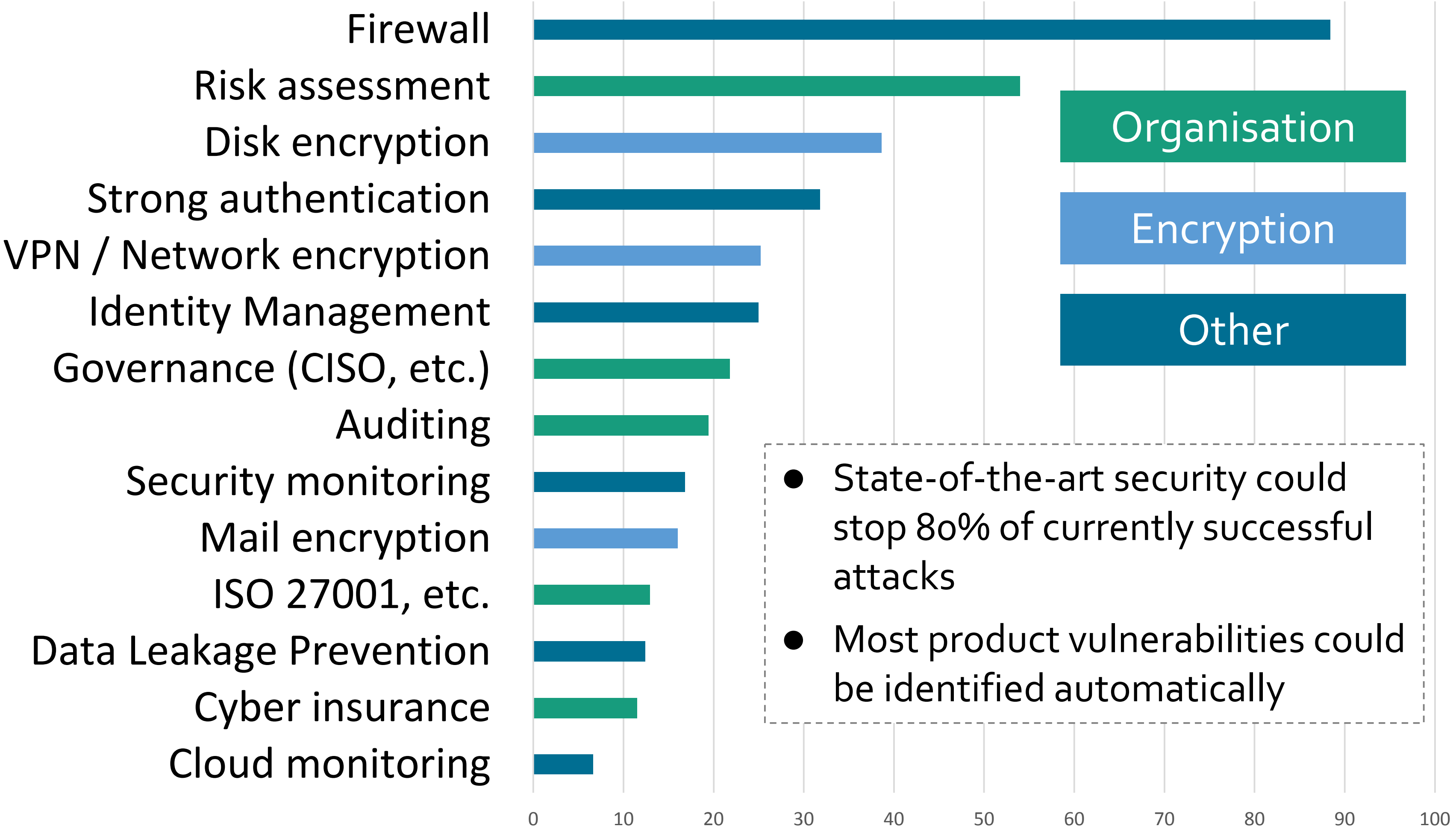
Why is Information Technology not Secure?

Several fundamental problems

- Insiders
- Usability
- Long Innovation Cycles
- Slow Adoption of Security Best Practices
- Software Quality

Why is Information Technology not Secure?

Slow Adoption of Security Best Practices in Industry

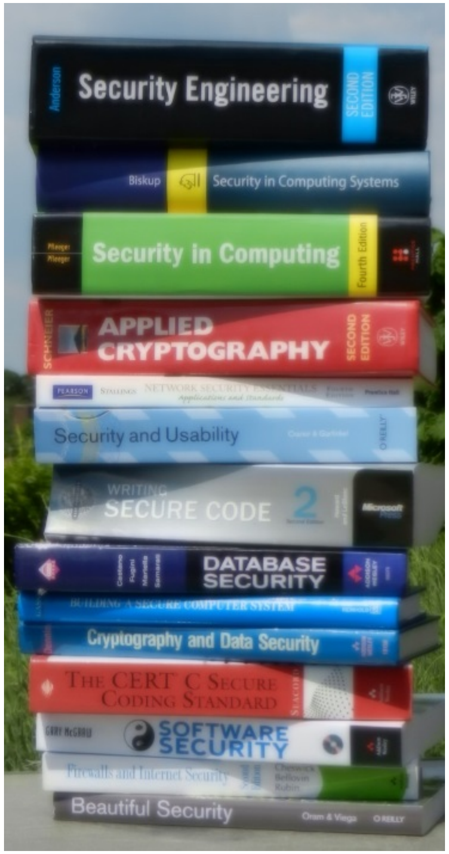


- State-of-the-art security could stop 80% of currently successful attacks
- Most product vulnerabilities could be identified automatically

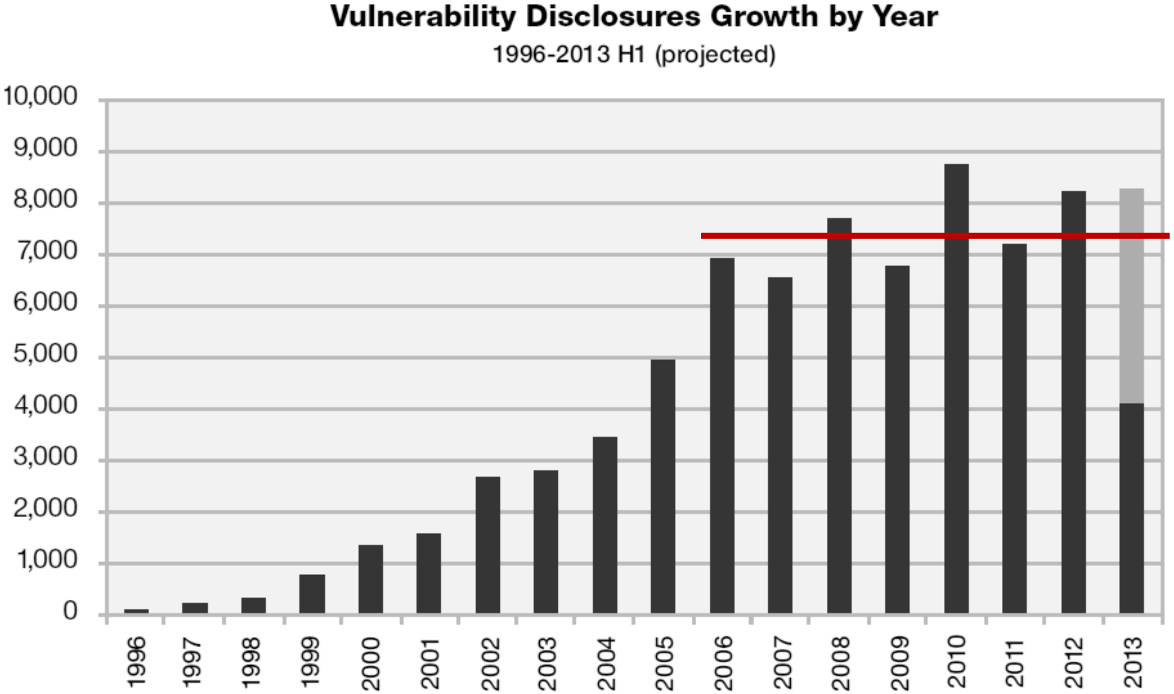
Source: Studie Industriespionage 2014; Corporate Trust, 30. Juli 2014 (Grafiken 24, 27, 29)

Why is Information Technology not Secure?

Software Quality: Constant Number of New Vulnerabilities



Security Engineering
Security in Computing Systems
Security in Computing
APPLIED CRYPTOGRAPHY
NETWORK SECURITY ESSENTIALS
Security and Usability
WRITING SECURE CODE 2
DATABASE SECURITY
BUILDING A SECURE COMPUTER SYSTEM
Cryptography and Data Security
THE CERT C SECURE CODING STANDARD
SOFTWARE SECURITY
Firewalls and Internet Security
Beautiful Security



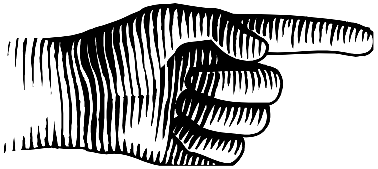
100-1000 vulnerabilities in software products

Slow adoption of "Security & Privacy by Design"

Source (Disclosures): IBM X-Force 2013 Mid-Year Trend and Risk Report, September 2013

Agenda

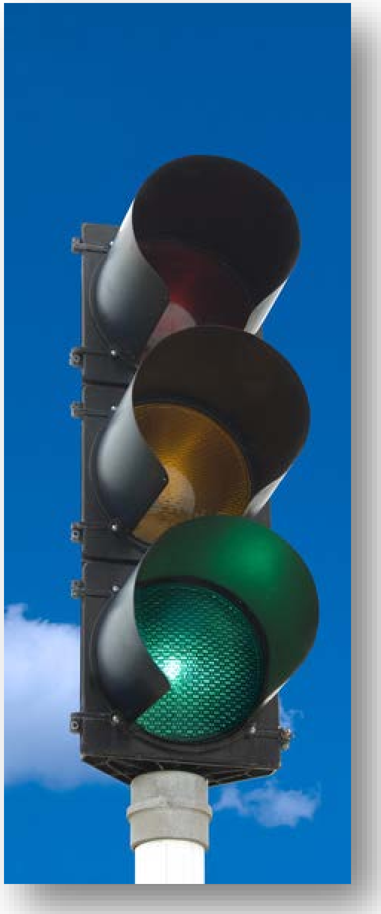
- Digital Sovereignty: Objective and Reality
- Why is IT not Secure?



- What Needs to be Done?

Society and Citizens

Make »Europe online« a trustworthy and secure place



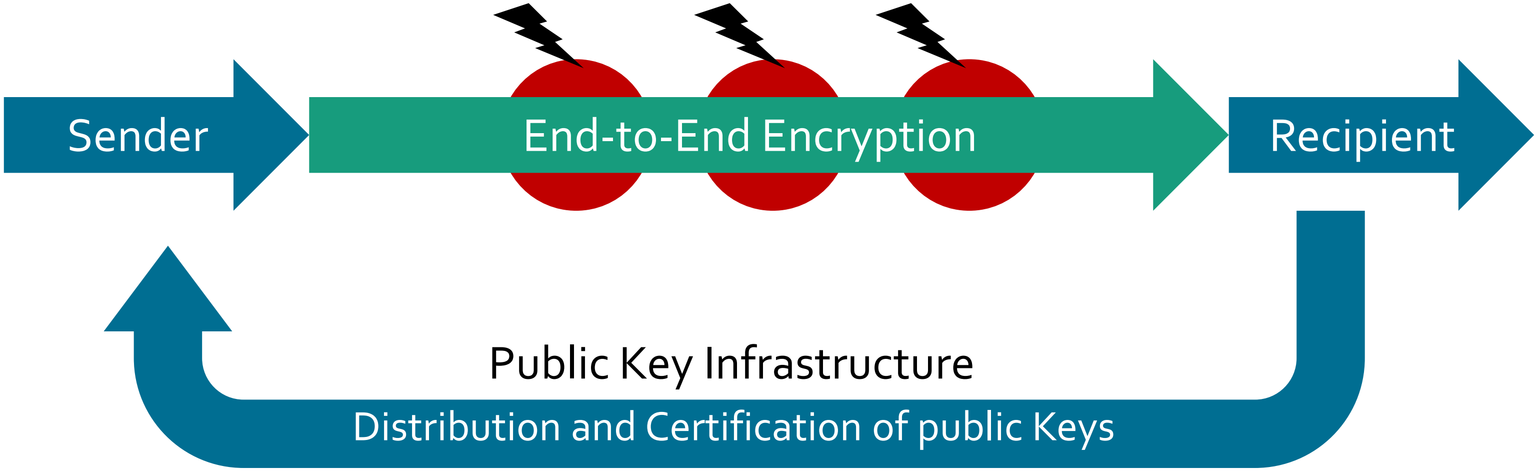
- Selecting, configuring and using security features, products and services is difficult:
  Broaden scope and capabilities of consumer advisors

- The quality of security and privacy must be made visible:
  EU-level criteria, test and certifications

- Confidentiality of communications requires availability of technologies and infrastructures
  - Support cross-EU infrastructure and tools for (**end-to-end) encryption for citizens and enterprises**
  - Mandate (cloud, …) service provides to always offer an option **supporting state-of-the-art security and privacy**

Mechanism of Choice: End-to-End Encryption

For Email, Chat, VOiP, ... Cloud: »Volksverschlüsselung«


Sender
End-to-End Encryption
Recipient
Public Key Infrastructure
Distribution and Certification of public Keys

BUNDESREPUBLIK DEUTSCHLAND T22000129
PERSONALAUSWEIS
MUSTERMANN
GEB. GABLER
ERIKA
12.08.1964 DEUTSCH
BERLIN
31.10.2020 938568

Challenges: Secure standards & implementation, usability, scalability

Industry and Government

Make the EU a leader in cybersecurity preparedness and trustworthy ICT

- **Necessary level of security and privacy must be turned from »competitive disadvantage« into »cost of doing business«**
  - Mandatory minimum standards
  - Encourage sharing of information within sectors
- **Security and Privacy by Design**
  - Encourage adoption of SPbD principle
  - Investment in standards, processes, tools
  - Enterprise encryption, and other best practices
- **Trustworthy ICT requires international cooperation**
  - Security testing / verification of any component
  - Secure integration of (even untrusted) components
- **Create a single market for security & privacy products**

Verschlüsselung im Unternehmen

Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

SIT TECHNICAL REPORTS

VERTRAULICHKEITSSCHUTZ DURCH VERSCHLÜSSELUNG

STRATEGIEN UND LÖSUNGEN FÜR UNTERNEHMEN

12/2014

FRAUNHOFER-VERLAG

Vertraulichkeitsschutz durch Verschlüsselung

Bericht, Dezember 2014

https://www.sit.fraunhofer.de/reports

Research

European research agenda for security and privacy

- **Security and Privacy**
  - Must be ***part of*** any project using / creating ICT
  - Must be a ***first class*** topic of the EU research agenda
- **Accelerate innovation cycles in cybersecurity**
  - Regular ICT: 1-5 years
  - Security: >10 years
- **Strong »Centers of Excellence« critical for success**
  - Research requires a critical mass of expertise

Grand Challenges in Security and Privacy

- IT products without (unknown) vulnerabilities
- Secure integration (composition) at large
- Detecting Trojans in IT products
- Enforcement of digital rights and provenance across domains
- Verifiable trust in remote platforms and their services
- Measuring, improving, and understandably explaining privacy in the digital world
- Security against bad (insider fraud) and lazy (social engineering) people
- Autonomous security and security management
- Usable security (including id's)
- Malware resistant computing platform
- Provably secure and efficient crypto
- Internet-scale trusted identities and key exchange
- Societal agreement on privacy and social networks, big data, pervasive computing, …

Prof. Dr. Michael Waidner

**Fraunhofer Institute for
Secure Information Technology SIT**

Director

www.sit.fraunhofer.de

Technische Universität Darmstadt

Computer Science, Professor
CASED & EC SPRIDE, Director

www.sit.tu-darmstadt.de

Rheinstrasse 75, 64295 Darmstadt
michael.waidner@sit.fraunhofer.de
+49 6151 869 250 (Office)
+49 170 929 8243 (Cell)