Security at Large

Prof. Dr. Michael Waidner

Center for Research in Security and Privacy CRISP ● Fraunhofer SIT + TU Darmstadt

A CRISP Member

CRISP
Center for Research in Security and Privacy

ITeG Ringvorlesung
Kassel, 17. Januar 2018

Fraunhofer SIT

Fraunhofer Institute for Secure Information Technology

Leading Applied Cybersecurity Research Institute in Germany

Fraunhofer SIT

- **Security of IT-based Systems**
  - Security by Design & Security at Large
  - Analyses, experiments, measurements, tests, design, training
- **History**
  - **1961** »Deutsches Rechenzentrum«, **1992** cybersecurity, **2001** Fraunhofer
- **Statistics**
  - Budget of **12M€**, 1/3 government, 2/3 grants and contract research
  - **Darmstadt, Birlinghoven, Mittweida**: **180** employees in **9** departments
  - **Jerusalem** and **Singapore**

TECHNISCHE UNIVERSITÄT DARMSTADT

CRISP Center for Research in Security and Privacy

האוניברסיטה העברית בירושלים THE HEBREW UNIVERSITY OF JERUSALEM

NANYANG TECHNOLOGICAL UNIVERSITY

- **World-class industry-focused cybersecurity research**
  - Publications and awards
  - Patents/IP. designs, products & services, studies, tests, testimonies

CRISP
Center for Research in Security and Privacy

Center for Research in Security and Privacy

Largest center for cybersecurity research in Europe

TECHNISCHE UNIVERSITÄT DARMSTADT
CYSEC

Fraunhofer SIT
Fraunhofer IGD

Fraunhofer-Leistungszentrum Cybersicherheit

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

2008 founded and supported by Hessen, since 2011 by BMBF. 2015 named »CRISP«, since 2016 Fraunhofer-Leistungszentrum, will be turned into permanent institution in 2018.

450+ researchers from 40+ nations,

2000+ students

80+ Awards

50+ Distinguished Speakers

50+ Conferences

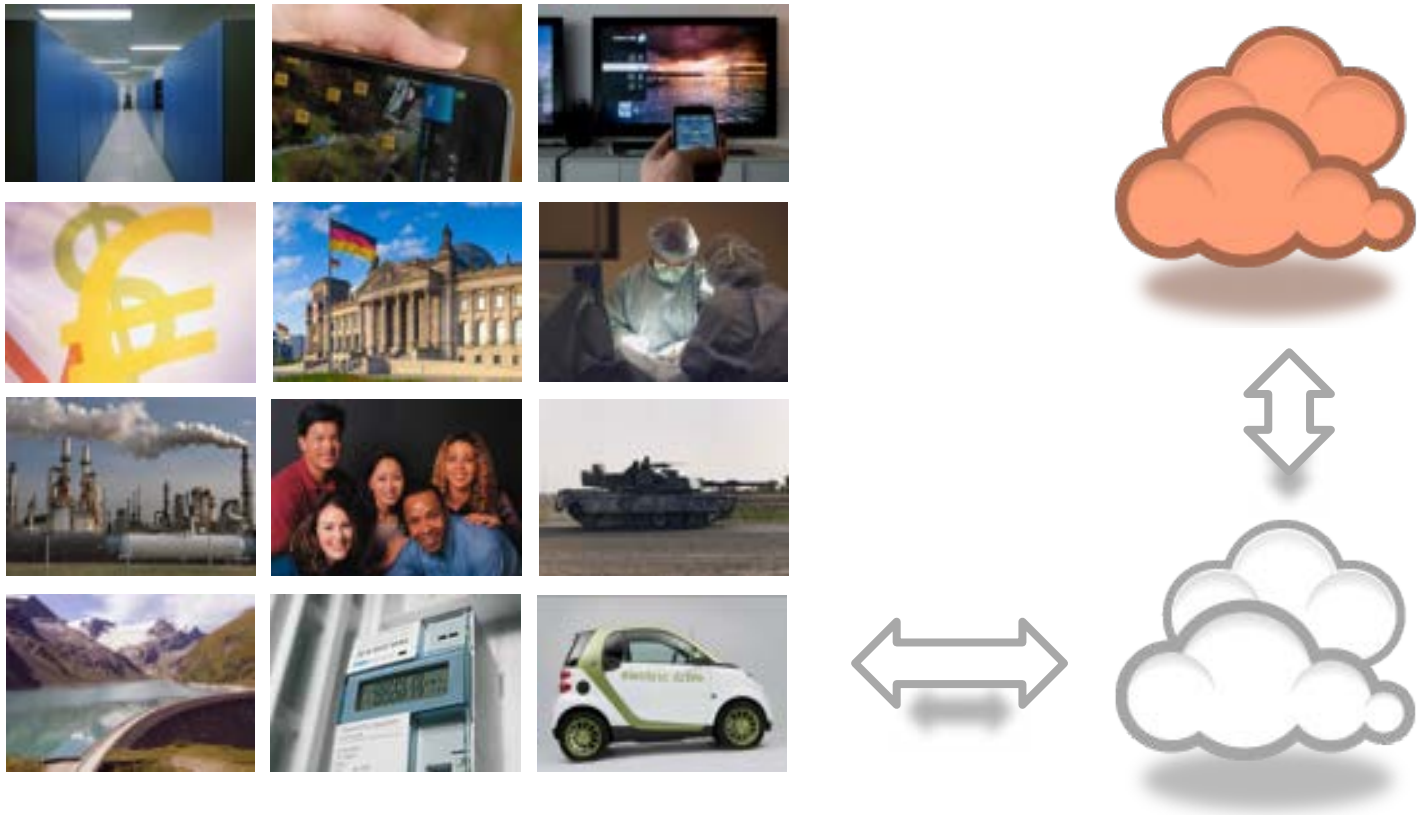
Bundesministerium für Bildung und Forschung

HESSEN Hessisches Ministerium für Wissenschaft und Kunst

Überblick

- Wie steht es um die Cybersicherheit in der „Digitalen Welt“
- Wieso sind IT-basierte Systeme angreifbar?
- Beispiele für Projekte zu „Security at Large“
- Was sollte passieren?

Everything is connected, programmable, open … and attacked



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

Prototypical Attacks

Economically or politically motivated, organized, targeted, automated

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)

German Steel Mill (2014)

Jeep Cherokee (2015)

XCodeGhost (2015)

German Bundestag (2015), US Democratcs National Committee (2016)

Various attempts to influence US Presidential Elections (2016)

Pegasus iOS Spyware (2016)

Yahoo: 3B (2013)
Equifax: 143M (2017)

WannaCry (2017)

Meltdown, Spectre (2017)

Vulnerabilities at all Layers, Slow Detection, High Risk

Mobile Apps (1)

- Over **81%** popular free apps communicate in the clear
- Over **73%** file viewer apps have security / privacy problems

Internet Infrastructure (1)

- Over **73%** DNS resolution platforms of enterprise networks are vulnerable
- Over **66%** of DNSSEC configurations are weak

Security Analytics (2)

- ∅ **99 days** to detect intrusions

Business Apps (1)

- Typically **100-1000** vulnerabilities / software

High Damages (3)

- Germany: **10*x B€**

Sources: (1) Fraunhofer SIT 2016;
(2) Mandiant 2017; (3) BITKOM 2016

Überblick

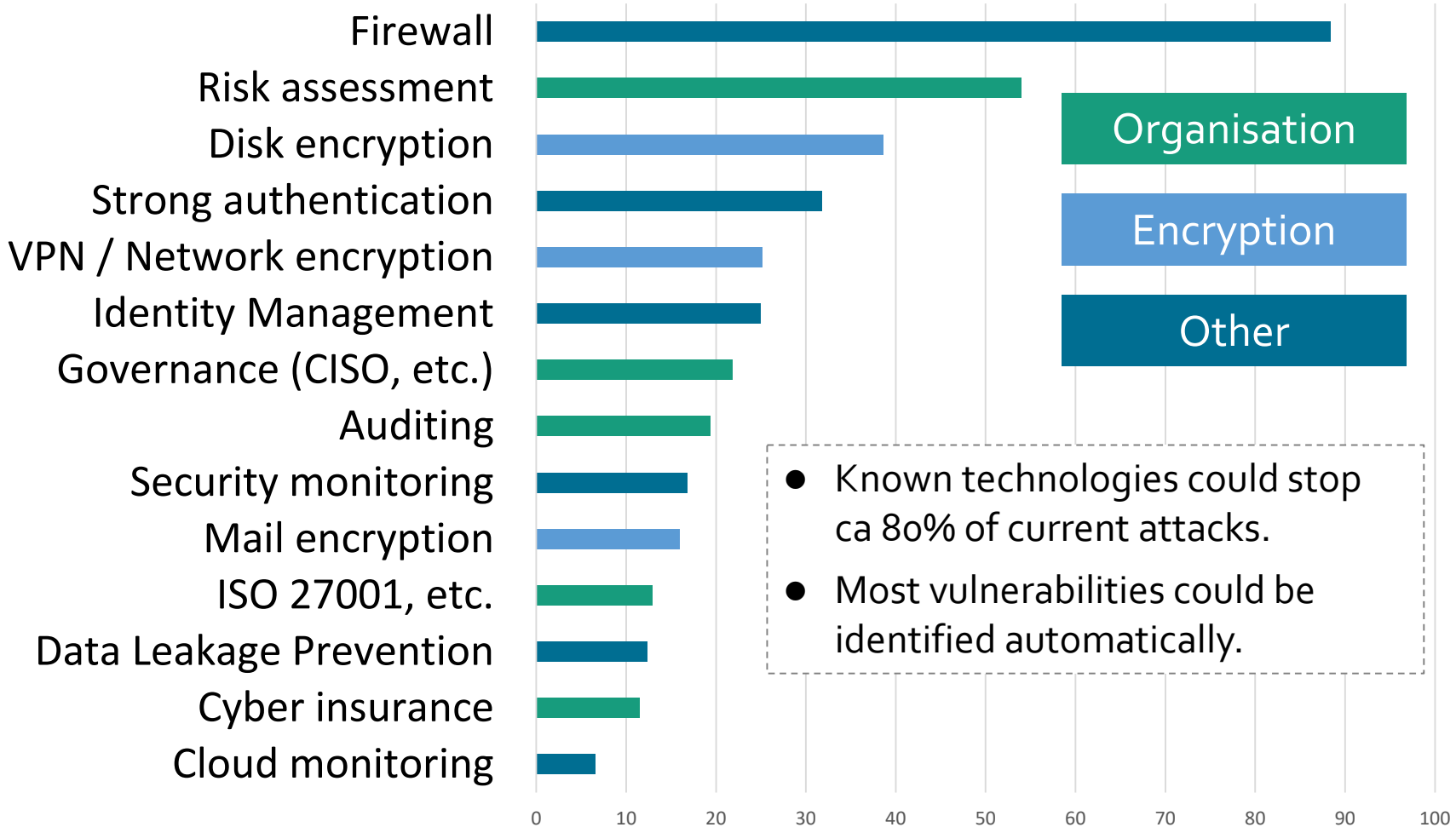
- Wie steht es um die Cybersicherheit in der „Digitalen Welt“
- Wieso sind IT-basierte Systeme angreifbar?
- Beispiele für Projekte zu „Security at Large“
- Was sollte passieren?

Reasons for Insecurity of Information Technology

1. Lack of risk awareness
2. Insiders
3. Social Engineering
4. Negative incentive through cost pressure
5. Limited market success of known technology*
6. Low software quality*
7. No support for secure integration
8. Insufficient usability
9. Time to market

Limited Market Success of Known Technology

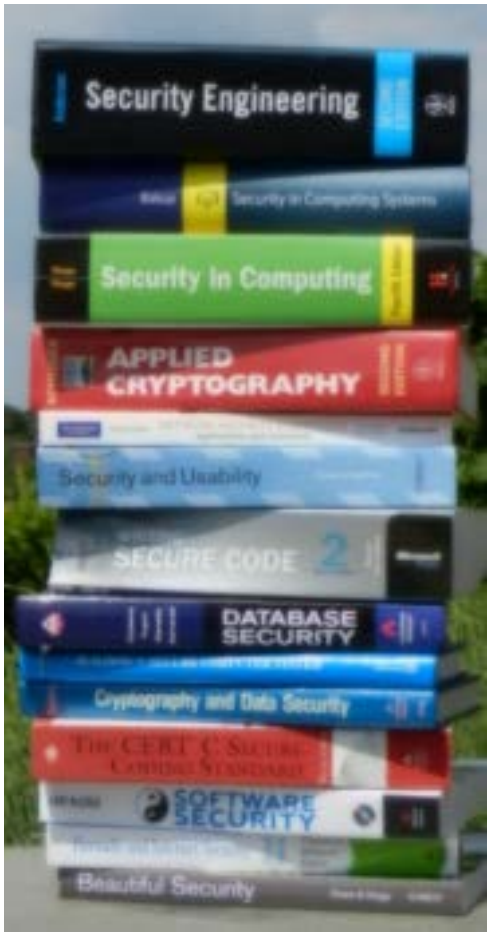
Percentages of companies in Germany



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

Low Software Quality

Seemingly stable number of new vulnerabilities

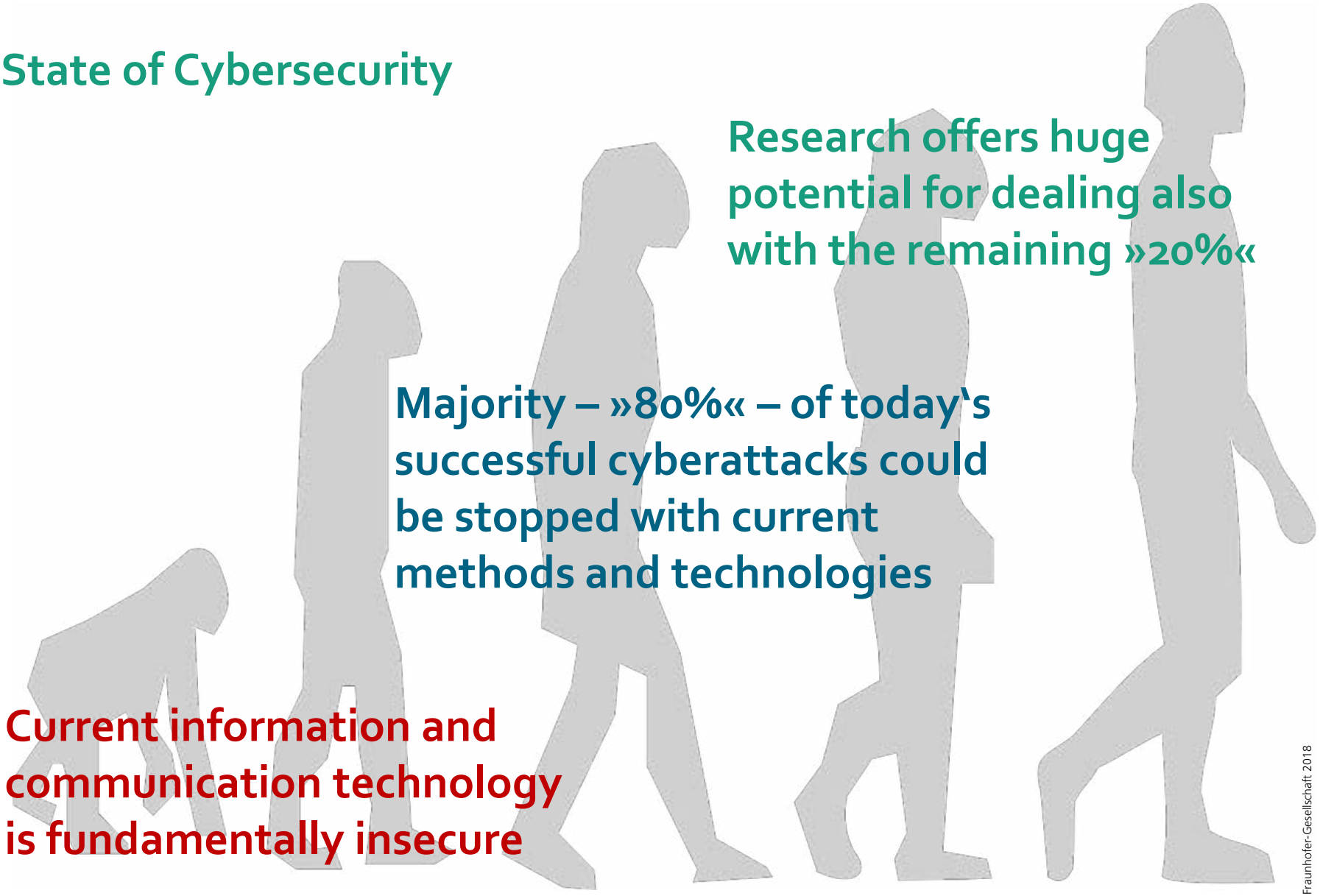


Includes some Android

100-1000 vulnerabilities in large software.
Slow adoption of »Security & Privacy by Design«

Source (# of Disclosures): IBM X-Force Threat Intelligence Report 2016 (© 2017)

State of Cybersecurity



Research offers huge potential for dealing also with the remaining »20%«

Majority – »80%« – of today's successful cyberattacks could be stopped with current methods and technologies

Current information and communication technology is fundamentally insecure

Source image (CC): https://opentextbc.ca/abealf5/chapter/chapter-1/

Security at Large: Security for large, real IT-based systems

»Ad-hoc Security«
Reactive

»Security & Privacy by Design«
Proactive,
attack resilience

»Security & Privacy at Large«
Systematic Security
for big, real-life systems

CRISP
Center for Research
in Security and Privacy

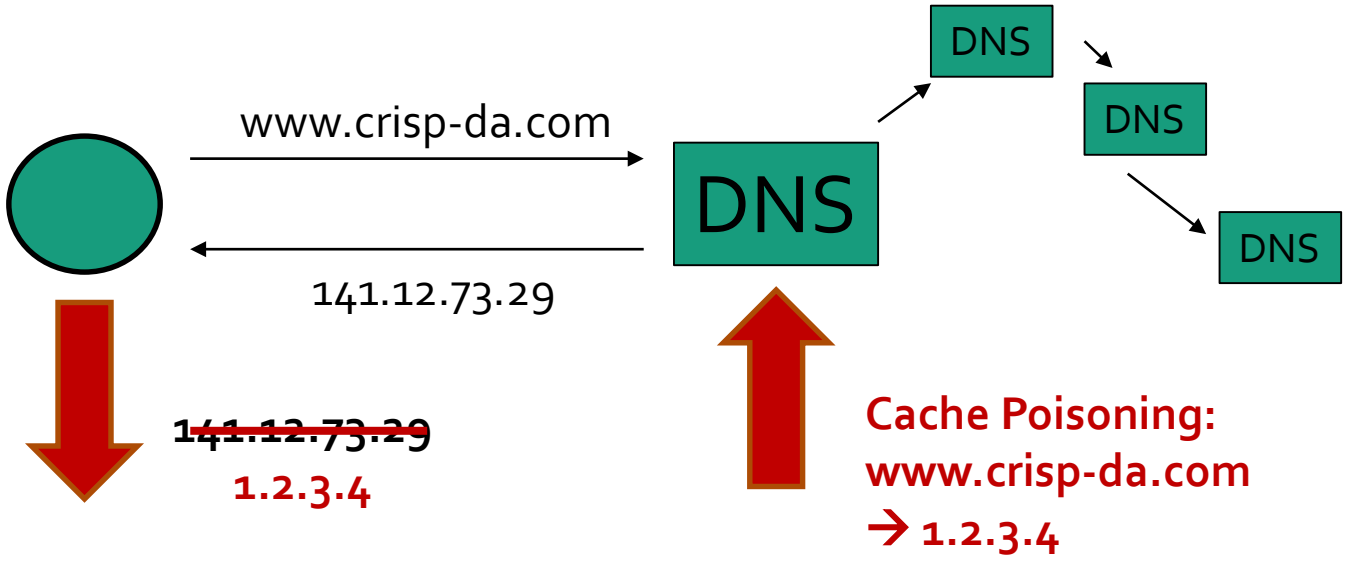
Überblick

- Wie steht es um die Cybersicherheit in der „Digitalen Welt“
- Wieso sind IT-basierte Systeme angreifbar?

- Beispiele für Projekte zu „Security at Large“
- Was sollte passieren?

Projekt »Mechanical Pentester«

Nicht-invasives, agentenloses Werkzeug zur large-scale Erfassung, Analyse und Verbesserung der Sicherheit Internet-basierter Infrastrukturen – Beispiel »Domain Name Service«

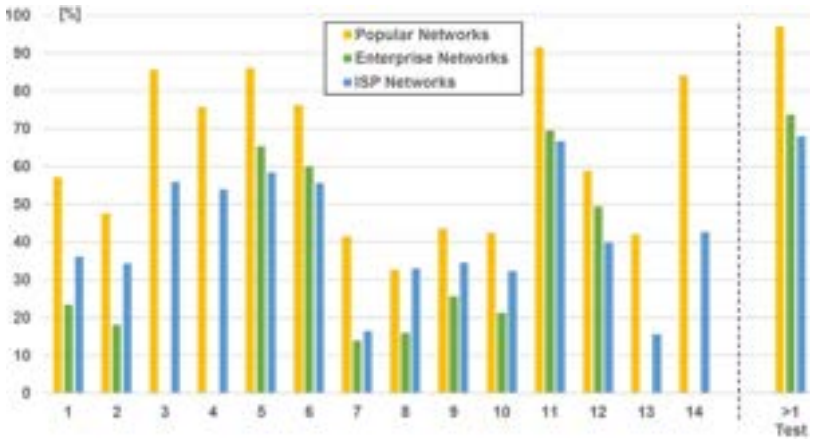


Cache Poisoning wird verwendet z.B. für:

- Falsche Web-Anwendungen: Passwort-Klau
- Abfangen von E-Mails: falsche Bestätigungen
- Beispielsweise durch NSA (ref. Snownden), aber auch andere Dienste und kriminelle Organisationen

Domain Name System (DNS) Study

Analysis of networks: majority is vulnerable, across the world



Survey of types of networks (popular, enterprise, ISP)

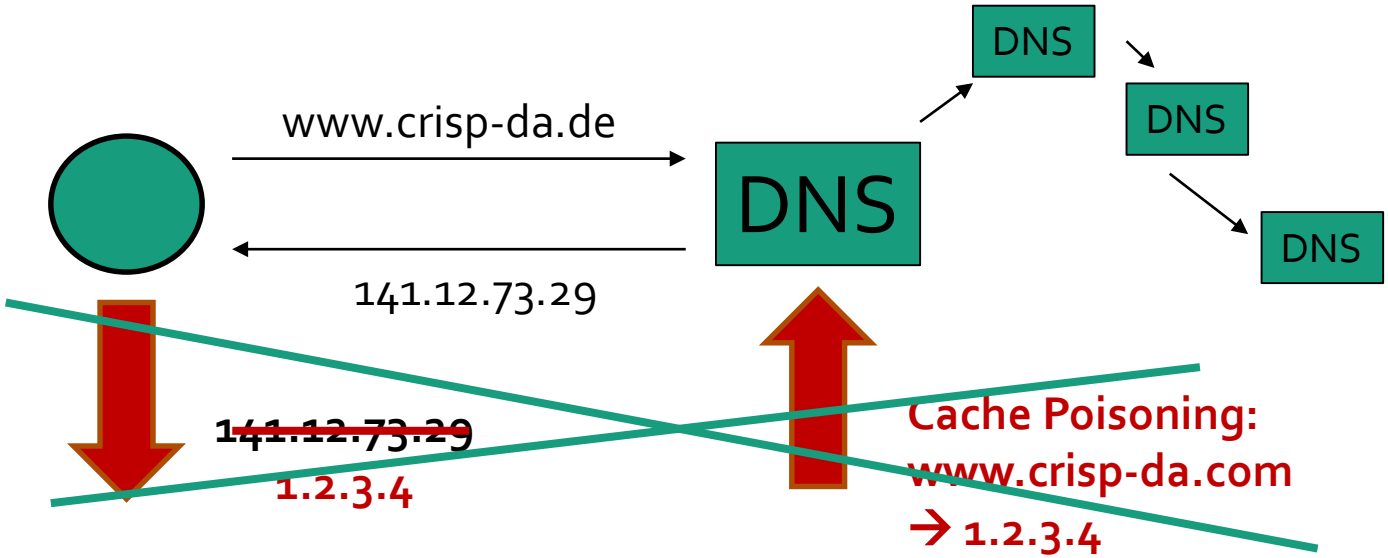
Survey of countries

Survey of products

	Name											
1	ns0	no	yes	yes	no	yes	yes	yes	yes	no	yes	no
2	ns0-auth	no	yes	yes	no	yes	no	no	no	no	no	no
3	ns	yes	yes	yes	no	yes	yes	yes	yes	no	yes	no
4	ns-auth	yes	yes	yes	no	yes	no	no	no	no	no	no
5	ns2	yes	yes	yes	no	yes	yes	yes	yes	no	yes	no
6	ns2-auth	yes	yes	yes	no	yes	no	no	no	no	no	no
7	ns	no	no	no	no	yes	yes	yes	yes	no	yes	no
8	v3-auth	no	no	yes	no	yes	no	no	no	no	no	no
9	v3-2	no	no	yes	no	yes	yes	yes	yes	no	yes	no
10	v3-3	no	no	yes	no	yes	yes	yes	yes	no	no	no
11	v3-4	yes	yes	yes	no	yes	yes	yes	yes	no	yes	yes
12	w-dname	yes	yes	no	no	no	no	yes	yes	no	no	yes
13	w7	no	no	no	no	yes	yes	yes	yes	no	yes	no
14	w8	yes	yes	no	no	yes	yes	yes	yes	no	yes	no
15	dname	yes	yes	no	no	no	no	yes	yes	no	no	yes
16	ak3	yes	yes	no	no	yes	yes	yes	yes	yes	yes	no
17	w11	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
18	w11dn	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes

»Signing« DNS with DNSSEC can avoid cache poisoning

But our analysis shows: 2/3 of DNSSEC keys are weak, due to misconfiguration



www.crisp-da.de → 141.12.73.29

Signiert:

Summary: Deployed DNS/DNSSEC Solutions are Vulnerable

More than 73% of the DNS servers operating for company networks are vulnerable

- Amit Klein, Haya Shulman, Michael Waidner:
  Internet Study of Injection Vulnerabilities in DNS;
  IEEE International Conference on Computer Communications (INFOCOM),
  Atlanta, USA, May 2017.

More than 66% of the used DNSSEC keys are weak

- Tianxiang Dai, Haya Shulman, Michael Waidner:
  DNSSEC Misconfigurations in Popular Domains;
  International Conference on Cryptology and Network Security (CANS),
  Milan, Italy, November 2016; LNCS 10052, Springer-Verlag, Berlin 2016.
- Matan Ben Yossef, Gal Beniamini, Haya Shulman, Michael Waidner:
  Factoring DNSSEC: Internet-Wide Study of Vulnerabilities in Signed Domains;
  14th USENIX Symposium on Networked Systems Design and Implementation (NSDI),
  Boston, USA, March 2017.

Weitere Test Werkzeuge

- **Code Inspect:** Halbautomatische Analyse von ByteCode
- **Harvester:** Erkennung verschleierter Internet-Kommunikation
- **Appicaptor:** Test-Framework für Massentests von iOS/Android Apps

Code Inspect

1. Platz

6. Deutscher IT-Sicherheitspreis 2016

- **Mechanical Pentester:** Werkzeug zur Analyse und Verbesserung von Internet-basierten Infrastrukturen

IETF

Projekt »Volksverschlüsselung«

- **Ende-zu-Ende Verschlüsselung**
  - Verhindert Massenüberwachung
  - Wird von allen populären Mail-Clients unterstützt und ist leicht nutzbar
  - Wird aber trotzdem kaum verwendet

- **Problem 1:** Erfordert Erzeugung und Installation von Schlüsseln

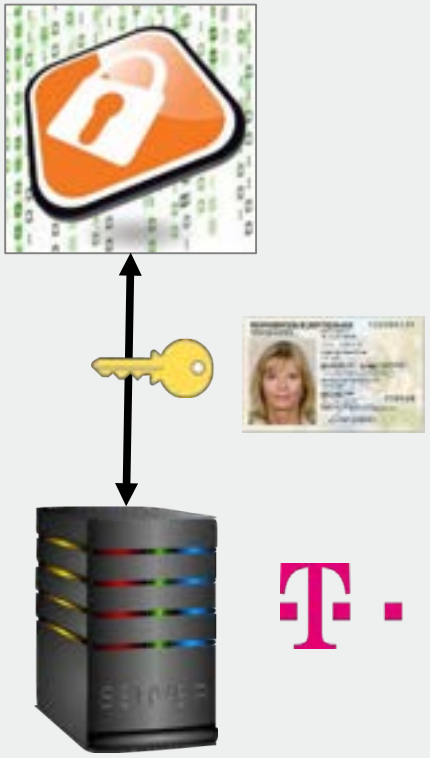
VV Software

- **Problem 2:** Erfordert eine Infrastruktur, um die Schlüssel der Kommunikationspartner zu finden

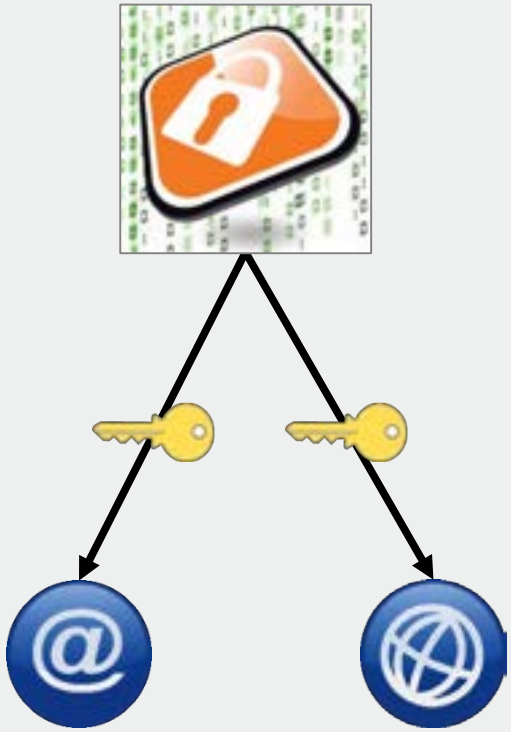
VV PKI

Usable Security: Volksverschlüsselung®

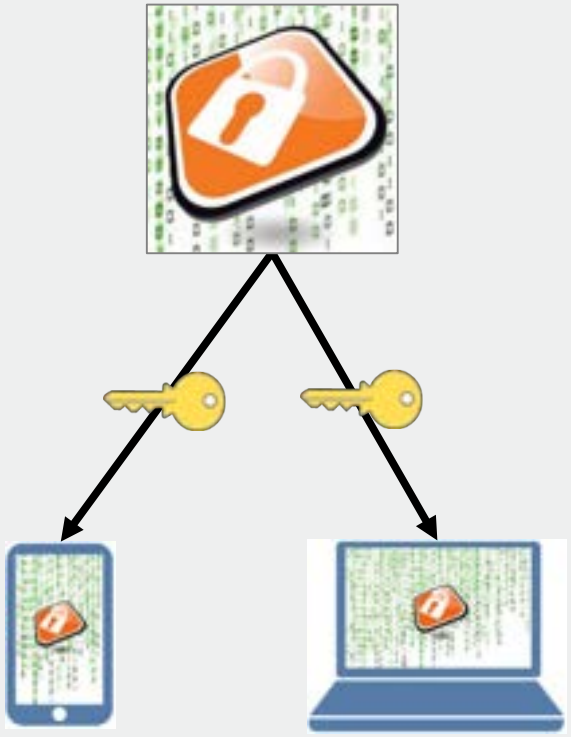
1.VV generates keys & triggers certification



2.VV detects apps & provisions keys

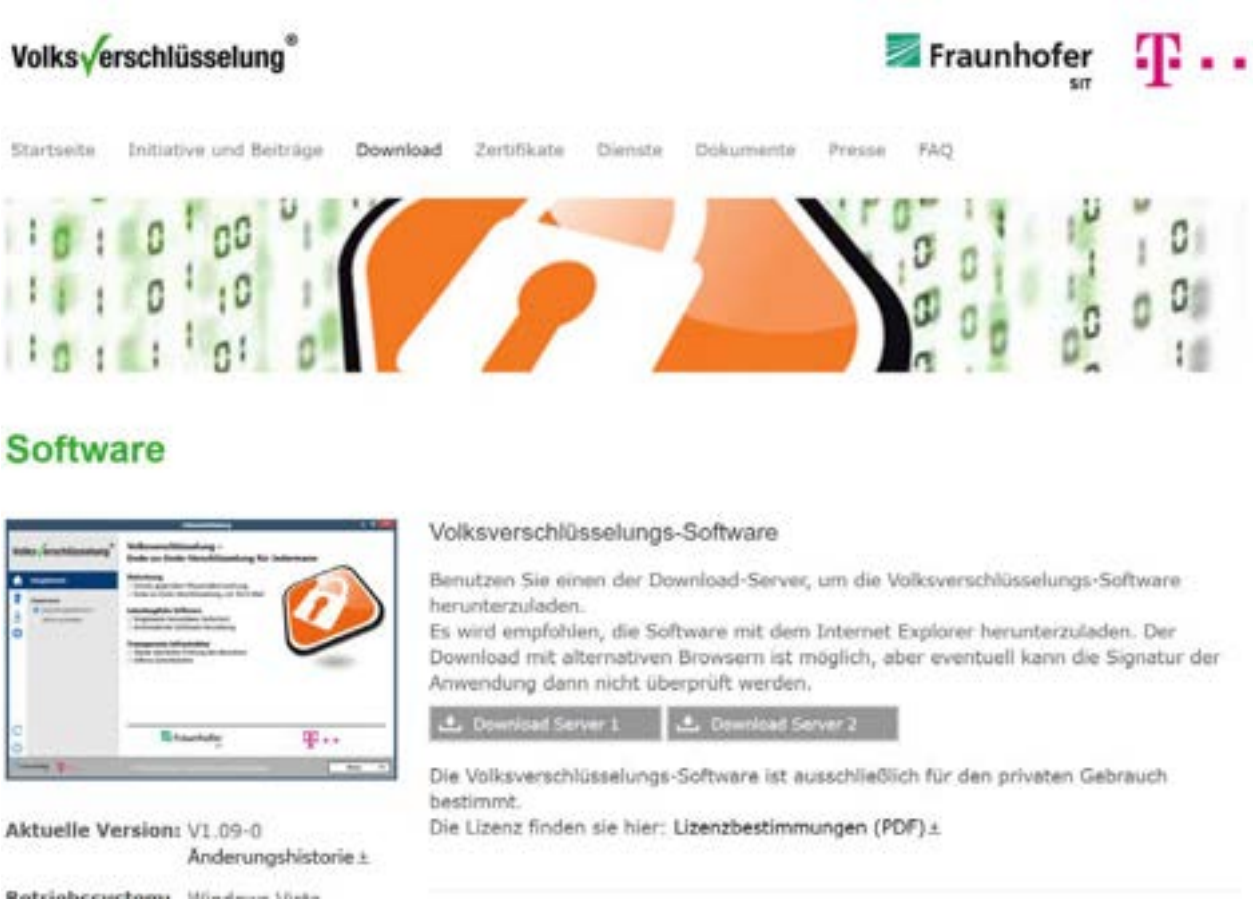


3.VV synchronizes keys between devices



Volksverschlüsselungs-Software

→ https://volksverschluesselung.sit.fraunhofer.de



Überblick

- Wie steht es um die Cybersicherheit in der „Digitalen Welt“
- Wieso sind IT-basierte Systeme angreifbar?
- Beispiele für Projekte zu „Security at Large“
- Was sollte passieren?

Was sollte passieren?

Positionspapier der drei Zentren CISPA, CRISP und KASTEL, Februar 2017

1. Strategisches Ziel »Digitale Souveränität«
2. Mindeststandards und Produkthaftung
3. Cybersicherheitsinfrastrukturen
4. Stärkung von Grundrechten
5. Aus- und Weiterbildung
6. Cybersicherheitsforschung
7. Innovationsrahmen für Cybersicherheit

https://www.kompetenz-it-sicherheit.de/positionspapier-cybersicherheit/

Was sollte passieren?

Langfristig: Grundsätzliche Verbesserungen von Cybersicherheit

- Security at Large
- Security by Design
- Empirische Cybersicherheit
- Autonome Cybersicherheit
- Post-quantum Kyptographie
- Messbarkeit von Sicherheit
- Beweisbare bzw. zuverlässig vorhersagbare Sicherheit

https://it-security-map.eu/en/roadmap/discussion-paper/

תודה רבה!

çok teşekkürler

Merci beaucoup!

谢谢

Thank you very much!

Dank je wel!

Vielen Dank!

Muchas gracias

ありがとうございます

Dziękuję!

zor spas

شكرا لك

Grazie mille!

Prof. Dr. Michael Waidner

Fraunhofer-Institut für
Sichere Informationstechnologie SIT

Institutsleiter

www.sit.fraunhofer.de

Technische Universität Darmstadt

FB Informatik, Lehrstuhl SIT

www.sit.tu-darmstadt.de

Rheinstraße 75, 64295 Darmstadt
michael.waidner@sit.fraunhofer.de
+49 6151 869 250 (Büro)
+49 170 929 8243 (Mobil)