New (?) IT-Security

Prof. Dr. Michael Waidner
Fraunhofer SIT (Director) & TU Darmstadt (Professor)
Center for Research in Security and Privacy CRISP (Speaker),

The Digital Society Conference 2016
Fraunhofer Institute for Secure Information Technology
Leading Applied Cybersecurity Research Institute in Germany

- **Security of IT-based Systems**
  - Security by Design & Security at Large
  - Analyses, experiments, measurements, tests, design
  - Training and education

- **History**
  - Founded **1961** as »Deutsches Rechenzentrum«, since **1973** GMD, since **1992** focus on cyber, since **2001** Fraunhofer Society

- **Statistics**
  - Budget of **11M€**, 1/3 government, 2/3 grants and contract research
  - **Darmstadt** and **Birlinghoven**: **170** employees in **9** departments
  - **Jerusalem**: Project Center at HUJI
  - Partner in **CRISP**

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

- Empirics
- Causes
- Challenges
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


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

Stuxnet (2010)  PRC Unit 61398, Shanghai (2013), NSA/GCHQ Programs (2013/14)


Yahoo lost 500M passwords (2016)  DARPA Cyber Grand Challenge (2016)
Vulnerabilities at all Layers, Slow Detection, High Risk

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

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

Security Analytics
- ∅ 146 days to detect intrusions

High Damages
- Germany: 10*x B€

Sources: (1) Fraunhofer SIT 2016; (2) Mandiant 2016; (3) BITKOM 2016
Limited market success of known technology
Percentages of companies in Germany

- Firewall
- Risk assessment
- Disk encryption
- Strong authentication
- VPN / Network encryption
- Identity Management
- Governance (CISO, etc.)
- Auditing
- Security monitoring
- Mail encryption
- ISO 27001, etc.
- Data Leakage Prevention
- Cyber insurance
- Cloud monitoring

Organisation
Encryption
Other

- Known technologies could stop ca 80% of current attacks.
- Most vulnerabilities could be identified automatically.

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

- Empirics
- Causes
- Challenges
Causes for Insecurity

1. Quality
   - Design and implementation errors
   - Poor usability

2. Human factor
   - Poor usability
   - Social engineering
   - Insiders

3. Integration & deployment problems
   - No empirical understanding of existing systems
   - Integration of legacy systems

3. Dependencies
   - Trojan functionality in hw/sw
   - Supply chain security

4. Market factors
   - Invisibility of security as market differentiator
   - Negative incentive through cost pressure
   - Limited market success of known technology*

5. Visibility and reaction
   - No cross-organizational visibility
   - Slow detection and slow reaction
   - Challenge ahead: Autonomous systems

*Note: The asterisk indicates a specific technology or approach related to market factors.
Outline

- Empirics
- Causes
- Challenges
What are the Challenges?

1. Quality
   - Design and implementation errors
   - Poor usability
   - Security by Design

2. Human factor
   - Poor usability
   - Social engineering
   - Insiders
   - Usable Security

3. Integration & deployment problems
   - No empirical understanding of existing systems
   - Integration of legacy systems
   - Security at Large
   - Empirical Cybersecurity
   - Risk-adequate security

3. Dependencies
   - Trojan functionality in hw/sw
   - Supply chain security
   - High assurance

4. Market factors
   - Invisibility of security as market differentiator
   - Negative incentive through cost pressure
   - Regulation
   - Limited market success of known technology*

5. Visibility and reaction
   - No cross-organizational visibility
   - Slow detection and slow reaction
   - Challenge ahead: Autonomous systems
   - Cognitive Security
Security by Design: Test tools for Internet-based infrastructures and apps

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

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

1. Platz
Usable Security: Volksverschlüsselung®

1. VV generates keys & triggers certification

2. VV detects apps & provisions keys

3. VV synchronizes keys between devices
Security at Large: Key Projects

**INDUSTRIAL DATA SPACE ASSOCIATION**

Data Sovereignty through standards:\(^{(1)}\)
Industrial Data Space (Fraunhofer, IDS Association)
http://www.industrialdataspace.org/

**iuno**

National Reference Project for Cybersecurity in Industrie 4.0:\(^{(1)}\)
Reference Architectures, Mechanisms and Tool Box
http://www.iuno-projekt.de/

**Volksverschlüsselung**

Easy to use end-to-end Encryption:
Volksverschlüsselung (Fraunhofer SIT, Telekom)
http://www.volksverschluesselung.de

**CRISP**

Center for Research in Security and Privacy

- Secure Web Applications:
  Security analysis of Javascript
- Secure Internet Infrastructures:
  Measurements and evolutionary, i.e., practical Improvements

(1) Supported by: Bundesministerium für Bildung und Forschung
(2) Supported by: Hessisches Ministerium für Wissenschaft und Kunst
Vielen Dank!

Thank you very much!

Merci beaucoup!

Thank you very much!

Dank je well!

شكرا لك

Vielen Dank!

Vielen Dank!