Impuls:
Zum Stand der IT-Sicherheitsforschung

Prof. Dr. Michael Waidner
Outline

- Future of IT and IT Security
- Four Promising Examples for Innovative Security Solutions
- Some Remarks on Security and Privacy Research in Germany
Future of Information Technology

GROWING RISK: IT is growing in design and operational complexity, and in overall criticality.

- Global, Open Internet of People and Things
  - People-centric online services, user generated content
  - Fully instrumented and interconnected physical world

- Global Marketplace for IT Services
  - Only end-points and some mission-critical functions provided in-house
  - Cloud of clouds
  - Standardized and automated, integrated end-to-end

- “Big Data” and Analytics
  - Broad information sharing across organizations and people

- “BYOD” and Consumerization
  - Personal mobile devices as primary way of accessing “the Cloud”
Future of Information Security **Attacks**

**EVOLUTION OF THREATS:** From Spam and DDOS to well-orchestrated, targeted Advanced Persistent Threats

**Major Approaches for Cyberattackers**

- Spreading malware through compromised web servers and drive-by exploits
- Attacks targeted at specific groups or people
  - Social engineering and emails with infected attachments
  - Attacks spanning multiple organizations (e.g., Stuxnet, RSA/Lockheed)
- Botnet-based distributed denial of service attacks
- Identity theft via spam and drive-by exploits

Source: BSI
Future of Information Security *Problems*

**NO CHANGES IN SECURITY:**

Well-known challenges

**Top structural problems stay the same**

- Security & privacy 2nd class considerations
- Poor designs, coding and admin errors lead to vulnerabilities
- Poor usability: engineers, admins and users are overburdened and under-motivated
- Human nature: curiosity, desire for efficiency and trust go against security
- Security context, identities and security events often lost between systems
- Poor lifecycle and change management, in particular for security objects (rights, id’s, ...)
- Insufficient visibility into security posture, location and state of data and IT
- Insufficient early warning, detection and forensic capabilities

© Fraunhofer-Gesellschaft 2012
Future of Information Security Solutions

SECURITY AND PRIVACY BY DESIGN: Most efficient and effective approach to security

Fixing vulnerabilities is more expensive than avoiding them

Average costs per defect (in USD)
Source: IBM 2009

- Code: 80 USD
- Build: 240 USD
- QA: 960 USD
- Deployed: 7600 USD
Outline

- Future of IT and IT security
- Four Promising Examples for Innovative Security Solutions
- Some Remarks on Security and Privacy Research in Germany
Four Promising Examples for Innovative Security Solutions

2. Bring Your Own Device: Virtual Security Domains
3. Privacy: Transparency
4. Security by Design: Model-driven Security
1. Cloud Computing: Gateways

**Applied research**

**Gateway / Cloud Broker**

- Unified access to multiple clouds
- Simplifies workload portability
- Improves security
  - Matching compliance requirements
  - Gateway encryption
  - Auditing, billing and metering, ...
  - Gateways can be local or shared

- Example: OmniCloud

*Fundamental research*

- Computes $\text{enc}(F(\text{data}))$ without the ability to decrypt $\text{enc}(\text{data})$.

- One of several cryptographic patterns for extending trust and confidence into the Cloud

- Various theoretical, very few practical results exist.

- Hot and promising area for basic and applied research.
2. Bring Your Own Device: Virtual Security Domains

Virtual Security Domains
- Isolate domains, e.g., “private” from “business”
- BYOD without reducing usability and appeal
- Various approaches
  - Always: root of trust, secure OS, trusted hw
  - Isolation can be done at several layers
- Device only one part of the solution
  - Infrastructure: VPN, TNC, app certification, ...
  - Mobile device management
  - App security

Example: BizzTrust for Android
3. Privacy: Transparency

**Personal Information Sharing Advisor and Dash Board**

- Unified account and profile management (“privacy dashboard”)
- User-centric identity management (incl. pseudonyms)
- Safety and security checking of partners and policies
- Personal privacy firewall, data leakage protection
- Awareness through displaying hypothetical €-values
- Advice on how to design and manage personal online image
- ...

---

**Trusted Identity & Profile Holder**

**Social Network 1**

**Social Network 2**
4. Security by Design: Model-driven Security

Idea

✓

Human-friendly description

Automate

Implementation

Examples:

- Security policies
- Security mechanisms (in software engineering)
- Compilers for cryptographic protocols
  - Secure function evaluation
  - Hardware constraints
Outline

- Future of IT and IT security
- Four Promising Examples for Innovative Security Solutions
- Some Remarks on Security and Privacy Research in Germany
Security and Privacy Research in Germany

Several strong security and privacy research institutes and groups
- CASED Darmstadt; CISPA Saarbrücken; ECSPRIDE Darmstadt; Fraunhofer Bonn, Darmstadt, Karlsruhe, München; HGI Bochum; KASTEL Karlsruhe; ...
- Several individual groups and researchers

Global context for German IT industry
- Strong positions: e.g., embedded IT, business software, services, privacy & trust
- Depends on global supply chain for base hardware and software

Domestic D/EU market offers strong position in setting standards

Suggests research focus on
- Strong positions (embedded IT, business software, ...)
- Standards: interoperability, integration, assurance, ...
- Engineering: security by design, trust from untrusted components
Gap between Theory and Practice of IT Security

There is 10+ years gap between academic and industrial state of the art in IT security.

- Partly standard problem of research
- Partly because of “commons nature” of IT security and privacy
Prof. Dr. Michael Waidner
michael.waidner@sit.fraunhofer.de

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Rheinstraße 75
64295 Darmstadt
www.sit.fraunhofer.de

Technische Universität Darmstadt
Fachbereich Informatik, Lehrstuhl Sicherheit in der IT (SIT)
Mornewegstraße 30
64289 Darmstadt
www.cased.de
www.ecspride.de
www.sit.tu-darmstadt.de