Security, Privacy and the Future Internet

Prof. Dr. Michael Waidner
Outline

- Future Internet
- Security and Privacy
- Security and Privacy by Design
Internet of People, Data, Services, Things, ... and Crime & War

Cloud-delivered IT & Business Services

Globally interconnected cyber-physical system

Online Social Networks

Cloud-delivered Crime & War

© Fraunhofer-Gesellschaft 2011
Overall, Security is Becoming More *Difficult*

- Future Internet is the ideal target: everybody, everything is online
- Professionalization and industrialization of cybercrime and cyberwar
- Network of people and user-generated content
  - Privacy (in public spaces …)
  - Intellectual property
  - Filtering illegal and dangerous content
  - Withstanding censorship
But Security may Also *Benefit* from the Future Internet

- **Better security through standards, automation, services**
  - Cloud will lower costs for good and well-managed security and privacy
  - Today, poor service management (governance, change, patch) is key source of insecurity!

- **Global scale, global economy may enable global standards**
  - Trust and identity infrastructures
  - Privacy and information sharing
  - Assurance, auditing, forensics
Outline

- Future Internet
- Security and Privacy
- Security and Privacy by Design
A Slightly More Technical View: Security Problems

- New technologies, new threat vectors
  - Massive resource sharing in clouds
  - Mobile and ambient as new access channel
  - Cyber-physical convergence
  - Global connectivity without global identity

- Old principles don’t apply anymore
  - Perimeter security vs. service decomposition
  - Trusted base vs. *everything* in the cloud
  - Managed endpoint security vs. consumerization
  - ...
Some Security Research Challenges

- Research pipe full of untested results
  - Crypto, trusted computing, provenance, sticky policies, automated checking, ...

- More applied research
  - Security for legacy systems, networks, ...
  - Unexpected intrusions, abuses, insiders
  - Accountability with privacy
  - Forensics with privacy
  - Quantification of risks and security

- Create a network to fight a network
  - Cross-org sharing of security information

- Commons nature of security
Privacy in the Future Internet

- Privacy is difficult to define
  - What is the €-value of your personal information?
  - What is privacy in a public space like an OSN?
  - Tradeoffs are always individual

- Status
  - **Purpose Binding**: responsible data management – mostly mature
  - **Data minimization**: crypto and data management – no practical experience
  - **Context binding**: not even well defined
  - **Sustainable informational self-determination**: no good solutions
Some Privacy Research Challenges

- **What is privacy in ...**
  - OSN, location, ambient, mobile, cloud, smart grids, ...
  - Mental models for usability

- **Research pipe full of untested results**

- **Standardization**
  - Portable id, pseudonyms, options, expiration dates, ...
  - Globally practical trust and identity framework

- **More applied research**
  - Privacy *despite accountability*
  - Privacy *despite forensics*
  - Computing with encrypted data

- **Commons nature of privacy**
Outline

- Future Internet
- Security and Privacy
- Security and Privacy by Design
Building a Secure System

- Huge body of engineering knowledge
- Many articles, books, courses, degrees, tools, ...
- So, in theory, this should be doable
Building a Secure System

State of the art in the software industry

But # of vulnerabilities is still going up

A more detailed look shows:
- Same errors again and again
- IT people lack skills
- Current processes and tools are too complex for humans

Source: Microsoft Secure Development Lifecycle

Source: IBM X-Force, 2011
Which one is Better: “by design” or “by patching”

<table>
<thead>
<tr>
<th>Security and Privacy by Design</th>
<th>Security and Privacy by Patching</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overall: economic</strong></td>
<td><strong>Overall: expensive</strong></td>
</tr>
<tr>
<td>▪ High initial costs</td>
<td>▪ Low initial costs</td>
</tr>
<tr>
<td>▪ Low recurring costs</td>
<td>▪ High recurring costs</td>
</tr>
<tr>
<td><strong>Avoids damage</strong></td>
<td><strong>Damage might be irreversible:</strong></td>
</tr>
<tr>
<td></td>
<td>▪ Life and health</td>
</tr>
<tr>
<td></td>
<td>▪ Critical infrastructure</td>
</tr>
<tr>
<td></td>
<td>▪ Privacy, reputation, confidentiality</td>
</tr>
</tbody>
</table>

**NIST 2010:**
- 80% of development costs spent on finding and fixing errors

**IBM 2010:** Fixing a single defect during ... costs:
- Coding: $80
- Build: $240
- QA/Test: $960
- Post release: $7’600 + reputational costs

European Center for Security and Privacy by Design (EC-SPRIDE)
Projected start: October 1st, 2011
What needs to be done

Challenges

- Consistent models throughout all phases
- Patterns for requirements analysis
- Model-driven security (design, test)
- Static and dynamic analysis
- Usability: end users, developers, admins
- Ready to use building blocks
- Demonstrable and quantifiable improvements in security
- Applied to interesting cases: cloud computing, embedded, ...
- Education for ordinary developers
Outline

- Future Internet
- Security and Privacy
- Security and Privacy by Design