Security Evaluation

(of)

A Moving Target

Dieter Gollmann

Institute for
Security in Distributed Applications

Hamburg University of Technology, Germany

Dieter Gollmann

- PhD on a topic in cryptography, 1984
- Research on cryptographic algorithms & protocols, foundations of computer security
- Course director, MSc in Information Security, Royal Holloway, University of London, 1992 – 1997
- Microsoft Research Cambridge, 1998 – 2003
- Chair for Security in Distributed Applications, Hamburg University of Technology, Germany, since September 2003
- Visiting professor with the Information Security Group, Royal Holloway, adjunct professor, Technical University of Denmark, visiting professor, School of Software, Tsinghua University.
- I have not actively participated in security evaluation, but have been following this field for the past 25 years.

Starting Point

- IT is today old enough to have its own history.
- Security concepts have developed and must be understood in their historical context.
- This also applies to security evaluation.
- To predict how security evaluation might evolve and where new challenges have to be faced, I will put security evaluation into its historical context.

Evaluating Evaluation

- My history of IT security & security evaluation will refer to the following dimensions:
  - Product – system/infrastructure: Is the focus on stand-alone products or on operational systems?
  - Layer of IT system: Are controls implemented in the core of an IT system or in the applications?
  - Technical – management: Are we evaluating a technical component or a management process?
  - Policy: How much variety is there in security policies?

Epochs of IT

- *1930s: People as "computers"*
- *1940s: First electronic computers*
- *1950s: Start of an industry*
- *1960s: Software comes into its own*
- 1970s: Age of the mainframe
- 1980s: Age of the PC
- 1990s: Age of the Internet
- 2000s: Age of e-commerce

1970s: Mainframes – Data Crunchers

- Technology: Winchester disk (IBM) 35-70 megabytes memory.
- Application: Data crunching in large organisations and government departments.
- Protection of classified data in the defence sector dominates security research and development.
- Security controls in the system core: Operating systems, database management systems
- Security policies: Discretionary and mandatory access control, multi-level security.

1980s: PCs – Office Workers

- Technology: Personal Computer, GUI, mouse, …
- Application: Word processors, spreadsheets, i.e. office work.
- Liberation from control by the IT department.
- Single-user machines processing unclassified data: No need for multi-user security or for multi-level security.
- Risk analysis ⇒ no need for computer security.
- Security evaluation: Orange Book (TCSEC, 1983/85): Driven by the defence applications of the 1970s.

1990s: Internet – Surfers Paradise?

- Technology: Internet, commercially used, Web 1.0.
- Applications: Web surfing, email, entertainment, …
- The single-user machine that had lost its defences in the previous decade is now exposed to the "hostile" Internet.
- No control on who can send what to a machine on the Internet.
- Buffer overrun attacks:
  - Aleph One (1996): Smashing the Stack for Fun and Profit
- "Add-on" security controls: Firewalls, SSL, browser sandbox as reference monitor, …

1990s: Security Evaluation

- Orange book policies superseded by commercial policies, e.g. role-based access control, relating to the business applications that emerged in the 1980s.
- Orange Book evaluation perceived as too rigid to meet commercial requirements.
- Security evaluation: ITSEC (1991/98) for flexible support of a greater variety of security policies and assurance requirements.
- Security controls in the core & in add-on components.
- Common Criteria approved at the end of this decade.

2000s: E-commerce

- Technology: Web services, Web 2.0, wireless communications (WLAN), PKI??
- B2C applications: Amazon, eBay, (budget) airlines, on-line stores, electronic banking, Google, managing program committees for conferences.
- SSL/TLS for secure sessions.
- Software security: Some progress, but the problems are shifting from the operating systems to the applications (SQL injection, cross-site scripting).
- Security controls moving to the application layer: Web pages start to perform security checks.

2000s: Security Evaluation

- Common Criteria: Focus on technical controls in the core and in add-on components:
  - Certified product list: Access Control Devices and Systems, Boundary Protection Devices and Systems, Data Protection, Databases, Detection Devices and Systems, ICs, Smart Cards and Smart Card related Devices and Systems, Operating Systems, Other Devices and Systems, Products for Digital Signatures.
- Compliance: Focus on best practices in security and in management:
  - Baseline protection, Cobit, ISO 27000, ITIL, SOX, …
- Who is evaluating the applications?

Evaluating Security – Status Quo

- We have considerable experience in evaluating security components, and a growing list of evaluated products.
- However, security problems can arise in parts of the system that don't appear security critical at first sight, written by developers with no security expertise.
- We have some experience in managing security in security aware organisations, and audit teams with expertise in evaluating the status of an organisation.
- However, can end users manage their end systems?

Evaluating Security – The Future?

- The target is moving to the application layer.
  - In terms of IT: SQL injection, XSS, XSRF, JavaScript Hijacking all exploit flaws in application software.
  - In terms of organisation: How to manage security (components).
- Applications are heavily customized.
- We need a rapid and adaptable methodology for evaluating application software.
- When moving to the application layer, security is moving closer to the end user.
- Security evaluation has to consider unsophisticated end users when assessing usability.

Thank you very much