actices Principles

Susan Landau
Senior Staff Engineer
Sun Microsystems Inc.

Sun microsystems
We make the net work.

[redacted]

Sun microsystems

TCG technology seeks to provide:

- Security
- Privacy
- Interoperability
  respecting laws and regulations in
  an international market

A (very brief) History of TCG

- 1999: Compaq, HP, IBM, Intel, Microsoft; goals include: multi-platform security standard secure storage of crypto keys enabling remote authentication
- Reformed in 2003 as the Trusted Computing Group (TCG); Sun and Sony join as "promoter" members. www.trustedcomputinggroup.org

Sun microsystems

Issues with TCG Technology

- Public concerns about copyright, fair use, data portability, open source, privacy, interoperability ...
- Who owns *my* computer anyway?

TCG Best Practices

- Chartered as a special committee to develop "Best Practice Guidelines" for various domains (server, PCs, mobile devices, etc.)
- First effort: TCG Design, Implementation, and Usage Principles (.95 draft)

[redacted]

Sun microsystems

Best Practices Principles Document

- Purpose: to articulate the underlying design principles so as to (i) clarify choices, (ii) guide developers to purpose of TCG technologies
- Audience: users and developers of TCG technology
- Enforcement mechanisms

[redacted]

Sun microsystems

Fundamental TCG Principle: Separation between Owner vs. User

- Owner: the owner of a system. It is the owner of the system that sets the security policy for the system.
- User: individual currently making use of the system.

Sun microsystems

TCG Best Practices Principles

- Security
- Privacy
- Interoperability
- Portability of data
- Controllability
- Ease of use

[redacted]

Sun microsystems

Security

- TCG-compliant components should achieve protection of secured data and should reliably report the system's security properties. The reporting mechanism should be fully under the owner's control.

[redacted]

Sun microsystems

Privacy

- TCG-compliant components should be designed and implemented with privacy in mind and adhere to the letter and spirit of all relevant guidelines, laws, and regulations. This includes, but is not limited to, the OECD Guidelines, the Fair Information Practices, and the European Union Data Protection

[redacted]

Sun microsystems

Privacy

- Notice
- Choice
- Purpose Limitation
- Security
- Data Quality
- Access
- Proportionality

[redacted]

Sun microsystems

Interoperability

- Implementations and deployments of TCG specifications should facilitate interoperability. Furthermore, implementations and deployments of TCG specifications should certainly not introduce any new interoperability obstacles.

[redacted]

Sun microsystems

Portability of Data

- Deployment should support established principles and practices of data ownership.

[redacted]

Sun microsystems

Controllability

- Each owner should have effective choice and control over the use and operation of TCG-specified capabilities that belong to them; **their participation must be opt-in. Subsequently any user can reliably disable the functionality in a way that does not violate the owner's security policy.**

[redacted]

Sun microsystems

Controllability II: Concerns

- "Bundling" is a misuse of TCG technology.
- Use of market clout to force use of TCG technology is a misuse of TCG technology.
- Use of coercion to force use of TCG technology is a misuse of TCG technology.

Ease of Use

- The non-technical TCG user should find the TCG-specified capabilities comprehensible and usable.

[redacted]

Sun microsystems

What will it take to work?

- A combination of forces: industry, government, private groups.

[redacted]

Sun microsystems

What do we need from you?

- Comments:
  https://www.trustedcomputinggroup.org/downloads/TCG_Principles_DraftD.v95.pdf