FSEM 1111 Computer Security – from a Free Software Perspective

Christian Grothoff
christian@grothoff.org

http://grothoff.org/christian/

Standards

- A *standard* is a technical specification defining certain aspects of a product
- A product follows a standard if it complies with the aspects defined in the standard
- Standardization is the process of creating and establishing standards

What can a standard specify?

- Physical aspects of a product (lead free)
- Production process (organically grown)
- Usability categories (safe for babies)
- Disposal process (recyclable)

Common Standards

- Power supply (voltage and frequency)
- Shape of plugs, calbes (Garden Hose, SATA)
- Paper sizes (US letter, DIN A4)

Kinds of Standards

- "de facto" standards are followed "for convenience"
- "de jure" standards are followed "for legal reasons"

Computer Standards

- Processors (x86)
- Network Protocols (IP, TCP, HTTP)
- Programming Languages
- APIs (System V, POSIX, W32, DX9)
- File Formats (PDF, HTML, XML)

Benefits of Standardization

Benefits of Standardization

- Enable interoperability
- Improve ability of customers to compare products
- Enable predictable operation (which in return, enables operations at a larger scale)
- Reduce Vendor lock-in by improving interchangability of products

Problems with Standards

Problems with Standards

- Standards reduce product diversity
- Standards can inhibit progress (towards better products violating existing standards)
- Compliance with standards is difficult to enforce
- Some standards require licensing, reducing competition by raising the barrier to enter markets
- Standards may conflict with social, cultural or legislative expectations and requirements
- Proliferation of standards reduces their effectiveness

The Standardization Process: ISO

1. Need for a standard expressed as a work item to ISO, including definition of the technical scope
2. Countries negotiate detailed specifications
3. Formal approval of the draft (75% majority)

$\Rightarrow$ Periodic review and update of standard

The Standardization Process: IETF

1. Internet community develops specification (Internet Draft)
2. IESG recommends draft for publication as RFC
3. Specification is published as part of the RFC series
4. RFC 2026 defines the requirements for RFCs

The Standardization Process: Free Software

- Standardization by market share (`apache`, `gcc`)
- Standardization by community members, driven by technical needs (LSB, POSIX)
- Adaptation of existing standards (PDF)
- Participation in standard development (ODF)

Standards and Security

+ Quality Assurances

+ Standards include good security practices

o Standards reduce diversity (fewer problems, but impact of remaining problems more significant)

- Flawed but widely-used standards are hard to eliminate (UPNP)

Important Security Standards

- AES – symmetric encryption
- SHA – cryptographic hash function
- HTTPS & X.509 – "secure" HTTP
- SSH – remote login protocol

Questions

?