Trusted Computing and OS Architectures

Dirk Kuhlmann
Trusted Systems Lab, HPL Bristol

Trust

- A social phenomenon
  - technology cannot create it
  - technology can only support its creation
- Trust in technology
  - Why do you trust your computer?
- What kind of information must be revealed between parties in order to create trust between them?

Trusted Computing

- Many things to many people
  - Here: focus on boot integrity and attestation
  - OS features to support TC
  - “Open Trusted Computing”
- Public Debate still ongoing
  - Much relaxed, though …
  - Actively encouraged by governmental entities
- Major driving force
  - Necessary alternative for Open Source
  - New CPUs support virtualization

Current Issues concerning TPs

- Implications for Free/Libre/Open Source Software
  - Security attestation is orthogonal to FLOSS licenses
  - Growing importance of FLOSS in commercial sector
- Flexibility vs. Security? Very difficult problem.

§ 12 GPL

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING **WILL ANY[ONE]** … **BE LIABLE TO YOU FOR DAMAGES** … ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (**INCLUDING** BUT NOT LIMITED TO **LOSS OF DATA** OR **DATA BEING RENDERED INACCURATE** OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES …)

TC and Communication Contracts

- Present
  - TCP/IP and authentication are entrance ticket
  - User authentication says little about exposure to risk
- Future
  - Active (counter–)measures
  - Scan for vulnerabilities before admission to the network
  - List of known vulnerabilities becomes ever longer
  - Validation of patch levels to shorten challenge-response

Preliminary work

- Securing Linux
  - Hardened versions (SE Linux, HP TLX, RSBAC …)
- Combining Linux with TC
  - E.g. Bear/Enforcer
  - Investigations both in HP and IBM Labs
  - Feasible, but large Trusted Computing Base
    - 120 – 500 files to be checked
    - SE Linux: difficult policy definition and configuration
    - Implications: reduce TCB size
- Candidate: OS sandboxing / virtualization

Driving Forces

- Virtualization for Servers
  - Important element for managed services
  - Utility computing: new management model
    - Customer ‘owns’ OS instance
  - Pronounced for GRID sceanrios
- 3G Mobile
  - Combination of PDA and Phone network endpoint
    - Programmable
    - Prospect: simultaneous DoS attacks on phone and data networks

Architecture Elements

- Attest system boot integrity
- Attest integrity maintenance
- Hosted OS instances
  - Subjected to Information Flow policies
  - Enforcement outside control of instance (proxy?)
- Virtualized TPM module per hosted instance
  - But also non-interferable by host system!
  - Interesting challenge for memory management
- Must work across multiple types of platforms

Approach

- Involvement of TCG board member organizations
- European activity
  - Most advanced public discussion
- Start from existing GPL’ed solutions with user and developer communities
  - Candidates: L4, Xen
- Synchronize with emerging activities
  - TCG working groups
  - Industry specification on Open Virtualization?
- (L)GPL, no enforcement of existing IP
  - Dual licensing?

Risks

- Changes in GPL v3?
  - First drafts differentiate between corporate and private use of TC
  - Simplified notions of ‘control’ and ‘ownership’
    - Control must cover the option of credibly giving it up!
  - Could make useful applications impossible
    - E.g. Trusted peer-to-peer storage (Wiki)
  - Stallman vs.Torvalds?
    - Different opinions on compatibility of TC and OSS
- Can this scale?
  - If not, “everyone for himself” is the best we can get

Q & A