Open Source Security Analysis
Evaluating security of Open Source Vs. Closed Source operating systems

Paulo Teixeira
Daniel Reuxes
Carlos Benito


Agenda

Scope
Concepts
DRM client architecture & POF (points of failure)
Threats:
  - breaking OS (robustness)
  - changing OS (modifying)
  - Open-source
  - Closed-source
  - Conclusions

Scope of this presentation
- Hardware threats (PC as unsecure platform...)
- Operating system features that might be considered threats: one process reads other processes’ memory
- DRM client will try to minimize the profit of breaking the DRM system, maximizing the security mechanisms
- Starting from that (unperfect) level of security: does closed-source OS provide better security?

Concepts
- Free software
- Open source
- Shared source
- Closed source
Operating System threats I (robustness)

- Unsecure OS:
  - Malicious user exploit OS flaw (buffer overflow, ...) in order to access to multimedia content when he does not has permission to do so
- OS security depends on:
  - Solid development
  - Architecture strengths: microkernel / monolithic, user mode / kernel mode, ...
  - Fast bugs detection
  - Bug reporting
  - Quick issue of patches

Operating System threats II (modification)

- Change OS source code in order to make a system call to have a different behavior as original planned
- Only feasible in open-source
Modifying the (open-source) Operating System

- **Easy to change**
  - Kernel available
  - good tools (IDE, compilers, documentation,...)
  - complex structure

- **Hard to disseminate:**
  - source patch: depends on version, need to recompile
  - entire binary kernel: large set of files (kernel, modules, dependencies,...), very dependent of different hardware configurations

Closed source

- **security by obscurity**

  - Kerckhoffs principle

  - very hard to change the operating system

  - DVD example

Open source

- **Good examples:**
  - protocols (TCP/IP stack)
  - programs (Apache, sendmail, BIND,...)

  - Security for the user or applications are assured:
    - trapsdoors could be detected
    - will not be dependent of "one" company

DRM Security Risk Weighting

- Risk of someone breaks it
- Consequences of that break

  - Global Profit of having the system
Conclusions

- No technical evidence that open-source OS is unsecure (from DRM point-of-view)
- Industry trend toward open-source
- Lack of certification for open-source software (drivers, OS, ...); maybe through vendors or an independent organization
- Open-source is not by nature more insecure than Closed Source

Questions?

Paulo.Trezentos@adetti.iscte.pt