

Adetti «Creating Knowledge...» technology | research | development | knowledge

## Open Source Security Analysis


Evaluating security of Open Source Vs. Closed Source operating systems



Paulo Trenzatos  
Daniel Neves  
Carlos Serrão

ICEIS 2003 - Angers - France, 23-26 April 2003

Adetti «Creating Knowledge...» technology | research | development | knowledge



## Agenda

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

Open Source Security Analysis

Adetti Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática

Adetti «Creating Knowledge...» technology | research | development | knowledge




## Scope of this presentation

- **Hardware threats** (PC as unsecure platform...)
- **Operating system features** that might be considered threats: one process reads other process' 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?*

Open Source Security Analysis

Adetti Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática

Adetti «Creating Knowledge...» technology | research | development | knowledge

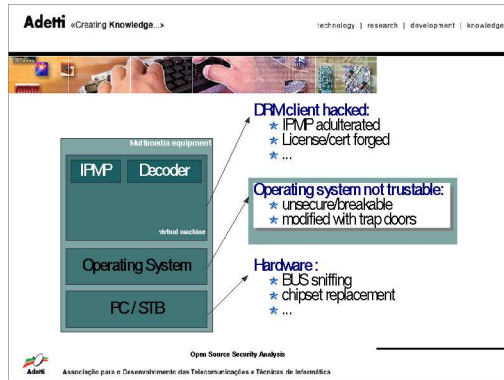


## Concepts

- Free software
- Open source
- Shared source
- Closed source

Open Source Security Analysis

Adetti Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática



- Adetti «Creating Knowledge...» technology | research | development | knowledge
- ### 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
- Open Source Security Analysis  
Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática

Adetti «Creating Knowledge...» technology | research | development | knowledge


### Operating system robustness

	Open Source	Closed Source
Fast bugs detection	Good	Good
Bug reporting	Good	Poor
Quick issue of patches	Good	Medium
Solid development	Good	Good
Good architectural design	Medium	Medium

Open Source Security Analysis  
Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática

- Adetti «Creating Knowledge...» technology | research | development | knowledge
- ### 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
- Open Source Security Analysis  
Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática

Adetti «Creating Knowledge...» technology | research | development | knowledge




### 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

Open Source Security Analysis

Adetti Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática

Adetti «Creating Knowledge...» technology | research | development | knowledge




### Open source

- Good examples:
  - protocols (TCP/IP stack)
  - programs (Apache, sendmail, BIND,...)
- Security for the user or applications are assured:
  - trapdoors could be detected
  - will not be dependent of "one" company

Open Source Security Analysis

Adetti Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática

Adetti «Creating Knowledge...» technology | research | development | knowledge




### Closed source

- security by obscurity
- Kerckhoffs principle
- very hard to change the operating system
- DVD example

Open Source Security Analysis

Adetti Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática

Adetti «Creating Knowledge...» technology | research | development | knowledge



### DRM Security Risk Weighting

$$\text{Risk} = \frac{\text{Risk of someone breaks it} \cdot \text{Consequences of that break}}{\text{Global Profit of having the system}}$$

Open Source Security Analysis

Adetti Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática



## 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](mailto:Paulo.Trezentos@adetti.iscte.pt)