THE Open GROUP

Boundaryless Information Flow™

Boundaryless Information Flow
Open Source in the Enterprise

September 8, 2003

Hilton London Paddington

London, UK

Digital Rights Management - The Implications of Open Source

Craig Heath, Symbian

Product Strategist - Core OS & Security

Open Source in the Enterprise - 08 Sep 2003

symbian

I Propose Not To Discuss:

- Whether intellectual property is a viable concept
  - …"information wants to be free"
- Whether consumers should be assumed to be honest
  - …"innocent until proven guilty"

- Premise: owners of intellectual property legitimately wish to police consumers' use of digital content to enforce limited rights

Trust Issues

- Content provider doesn't trust the user
  - …"reverse threat model"
- Content provider *does* trust the device manufacturer
  - …on-device agent to act in *their* interests
- To get the benefits of DRM, user must surrender some degree of control to the device manufacturer
  - …deliberately and voluntarily

Need Openness

- Openness to Independent Software Vendors
  - … Documented APIs
  - … ISVs would need to be “blessed” somehow
- Openness to Service Providers
  - … Interoperable protocols
  - … Open standards allow mix-and-match services and devices
- Openness to Content Providers
  - … Unconstrained content provision
  - … Should allow fair access to “independent labels”
- Openness to Consumers
  - … Coexistence with free content
  - … Willing cooperation, not coercion

Need Real Benefits To Users

- New pricing models
  - …e.g. OD2
    - £1 to burn a track to an unprotected CD
    - 10p to download a track to a single device for 1 year
    - 1p to listen to a track once
- Convenience
  - …iTunes (5 million tracks sold in 8 weeks)
    - more reliable, better presented, easier to use than peer-to-peer file sharing
- Respect “fair use”
  - …backup/restore, move between devices

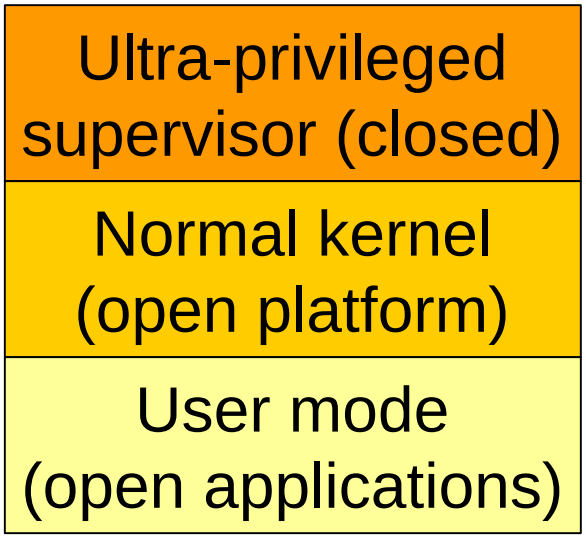
The End of “Security by Obscurity”

- Open source implies:
  - …No secret algorithms
  - …No secret APIs
  - …No compiled-in secret tokens
  - …No obfuscation of code
- Problem:
  - …How do you implement a *mandatory* security policy when a user can freely examine and modify the code?

Mandatory Security Policies - Part 1

- Add a new privilege level to the processor
  - … Intel - “LaGrande Technology”
  - … ARM - “TrustZone”

Very simplified:



Needs integrity checks to prevent tampering with supervisor

… Supervisor could grow very large

Mandatory Security Policies - Part 2

- Verification of run-time state
  - Trusted Computing Platform Alliance (TCPA)
    - (Palladium / NGSCB)
  - extended by Trusted Computing Group (TCG)
    - for mobile devices
- Hardware Trusted Platform Module
  - Allows “trusted” applications to use public key cryptography to authenticate themselves to content servers
  - Keys are only released if and when the system is in a known state (h/w and s/w integrity checks)

In Closing...

- Will open source DRM be implemented?
  - …There are open protocol/format standards
    - Open Mobile Alliance DLDRM
    - ISO MPEG-21
  - …The necessary hardware is on the way
    - LaGrande, TrustZone, TCPA/TCG
  - …But is there the will to do it?
    - Linus says he is OK with the idea of DRM on Linux
      - …but who will implement it?
    - Content providers may still worry about security
      - …can’t hide vulnerabilities in the mechanism