Digital Rights Management

John Manferdelli
University of Washington

DRM as Protection for copyrighted materials

- Digital objects are very easy and cheap to copy:
  - Music, Movies, Text, Executables.
  - Essentially no “friction” from duplication costs
- *How* to protect digital copyrighted content?
- *Should* content be protected?
  - 40 billion dollars a year in foreign trade for the US.
  - Should not conflict with “fair-use” doctrine.
  - What is fair use anyway?
- *Can* content be protected?
  - Persistent pirate will always succeed in copying.
  - Technology can potentially prevent small scale copying:
    “keeping honest people honest”

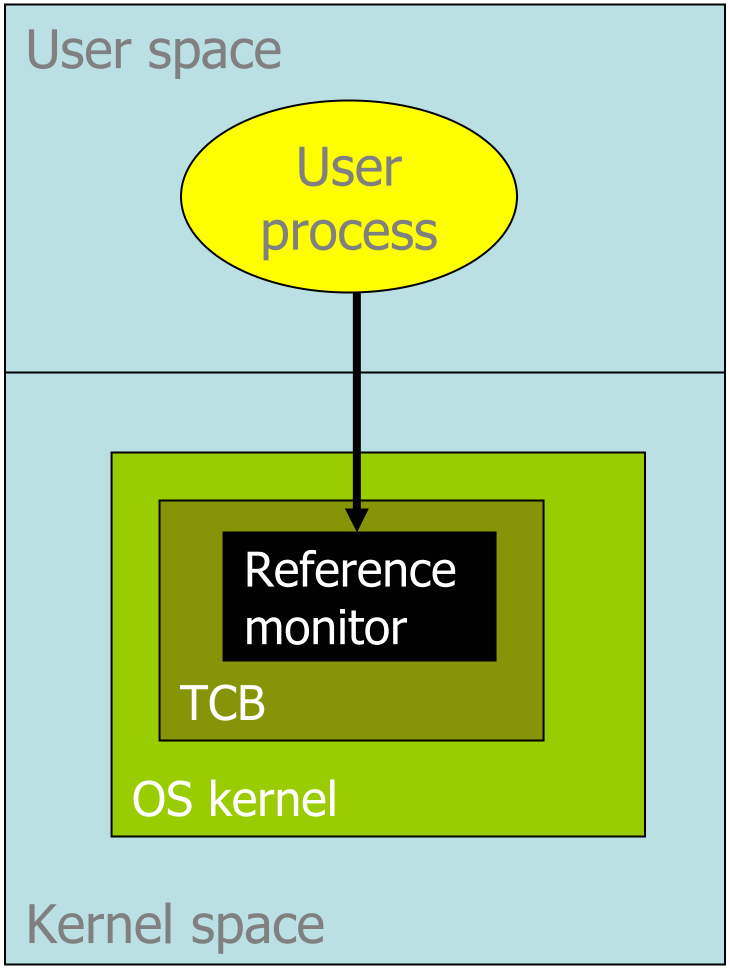
Slide from Dan Boneh

Computer Security and DRM

- *Computer Security* involves processes and technology that enable the enforcement of a *security policy* on a computer system. Security Policy specifies:
  - Isolation/Secure Execution and other “safety” properties
  - Access and use restrictions on resources imposed on *security principals* (think “users”) using the computer system (“Access Control”)
  - Availability and other “liveness” properties
- *Digital Right Management* (a.k.a – copyright/content protection) *involves* enforcement of a security policy affecting use of digitally encoded material specified by a content “owner” on computers not in the physical control of the content owner.

Kernelized Design

- Trusted Computing Base
  - Hardware and software for enforcing security rules
- Reference monitor
  - Part of TCB
  - All system calls go through reference monitor for security checking
  - Note implicit trust assumption: “owner” or “Admin” fully trusted and omnipotent
  - Additional assumption: no offline attack.



… and now for something completely different

- Superficially anyway
- Trust Model Changes
  - Admin is not “root of trust” for all actions
  - Model is naturally distributed
- Persistent Rights
  - Off-line
  - Granular and Flexible
- Cryptographic protection
- Software runs in Trusted Environment.
  - Software is the Security Principal
  - Lampson, Abadi, Wobber model

Key Elements of DRM

- Licensing
  - The process of packaging and delivering protected bits with un-forgeable terms of usage (“digital license”) useable only by authenticated user/environment
- Enforcement
  - The process of insuring that the use of the digital work adheres to enumerated use, privacy and operating restrictions stated in a digital license

Encryption and Rules

- Content is encrypted
  - *Therefore unusable with the right to decrypt the content*
- Content license specifies rights (“capabilities”) – cannot be forged
  - *Specifies authentication information, environment (application, OS, etc.)*
  - *Specifies usage/access control rules*
  - *Contains the “sealed” key for the content. Key can be sealed by any licensor (using a public key) but can only be “unsealed” within an isolated, trusted environment (by a private key only known in that trusted environment)*

```
Content License 938473

Machine 02345 Running
Program 1 (with hash 0x7af33)
Can view Document 3332 on 2002-20-01
Sealed Key: 0x445635

Signed Boeing
```

Enforcement

At initialization, Trusted Program says:

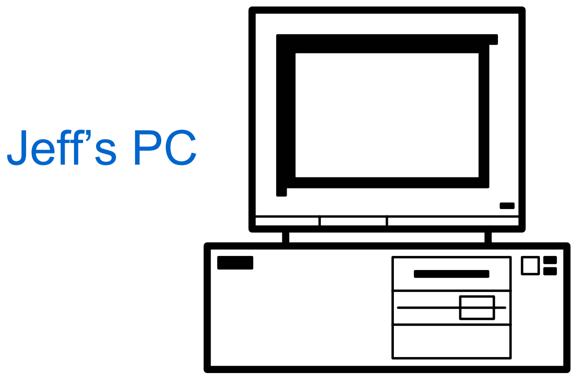
1. Isolate me
2. Authenticate me

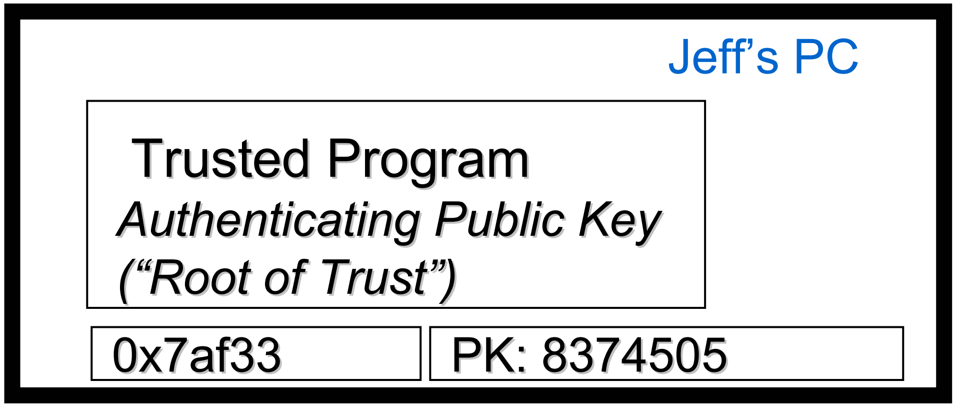
After Initialization completes successfully, Jeff’s PC

1. Makes Private key available for use

When consuming content, Trusted Program:

1. Retrieves license and encrypted content file
2. Authenticates license by checking digital signature
3. Checks rule compliance
4. Uses private key to unseal the content key
5. Decrypts and uses content within Trusted Program




Jeff’s PC

Trusted Program
Authenticating Public Key
(“Root of Trust”)

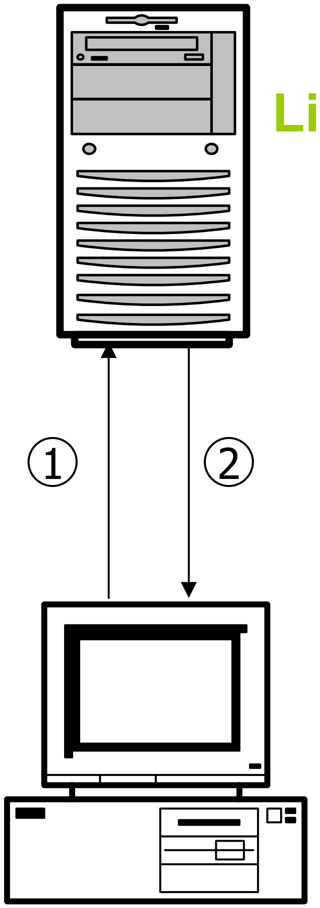
0x7af33

PK: 8374505

Obtaining Rights and Permissions

1) Request
I want document 2346.
Here’s my Machine License to show you can trust my machine

```
Machine License 83874

Machine 02345 Running
Program 1 (with hash 0x7af33)
Has access to a private key
Whose public key is 0x2231

Signed Microsoft
```



License Server

Jeff’s PC

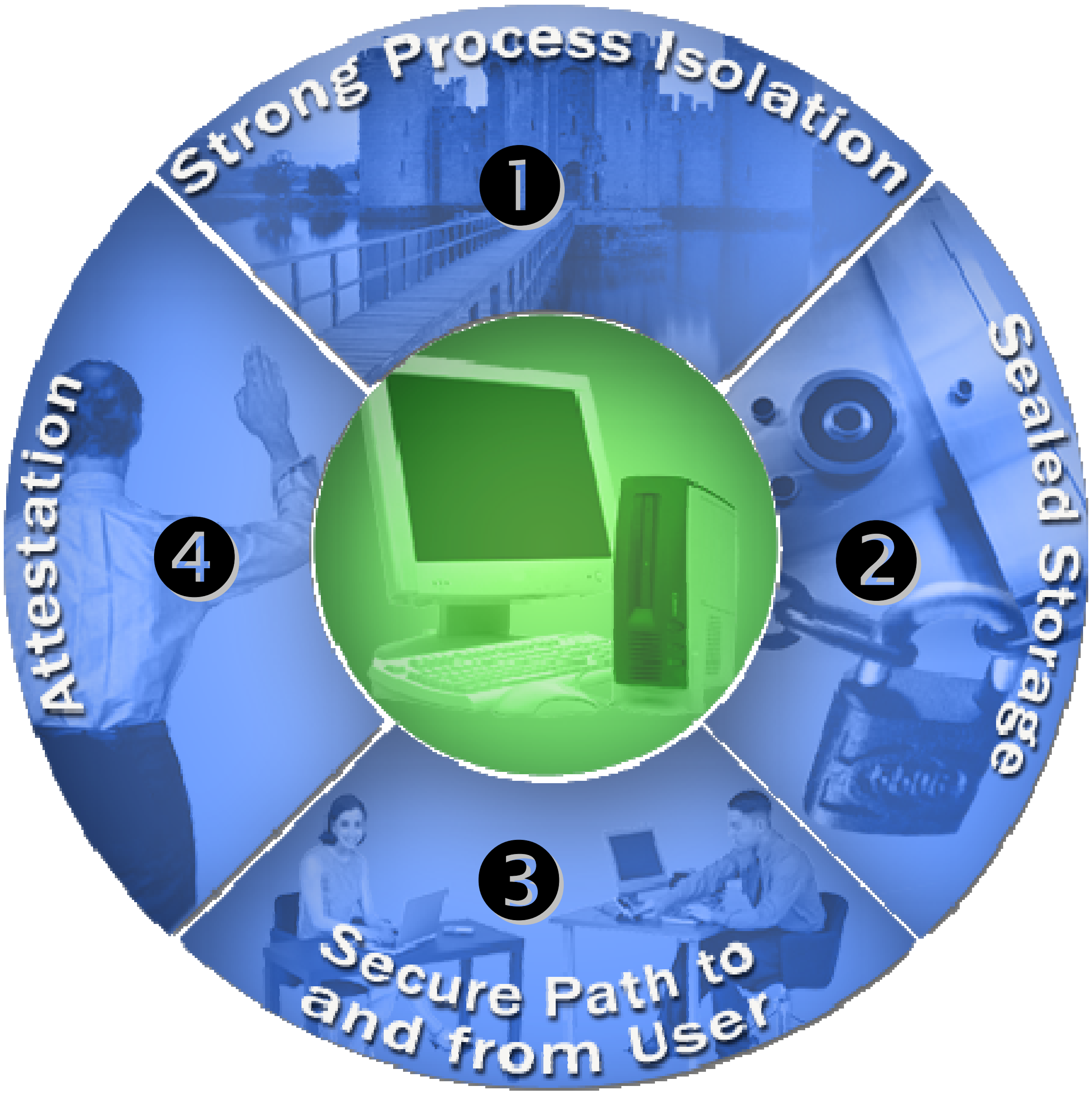
2) Response
Here’s your license

```
Content License 938473

Machine 02345 Running
Program 1 (with hash 0x7af33)
Can view Document 3332
on 2002-20-01
Sealed Key: 0x445635

Signed Boeing
```

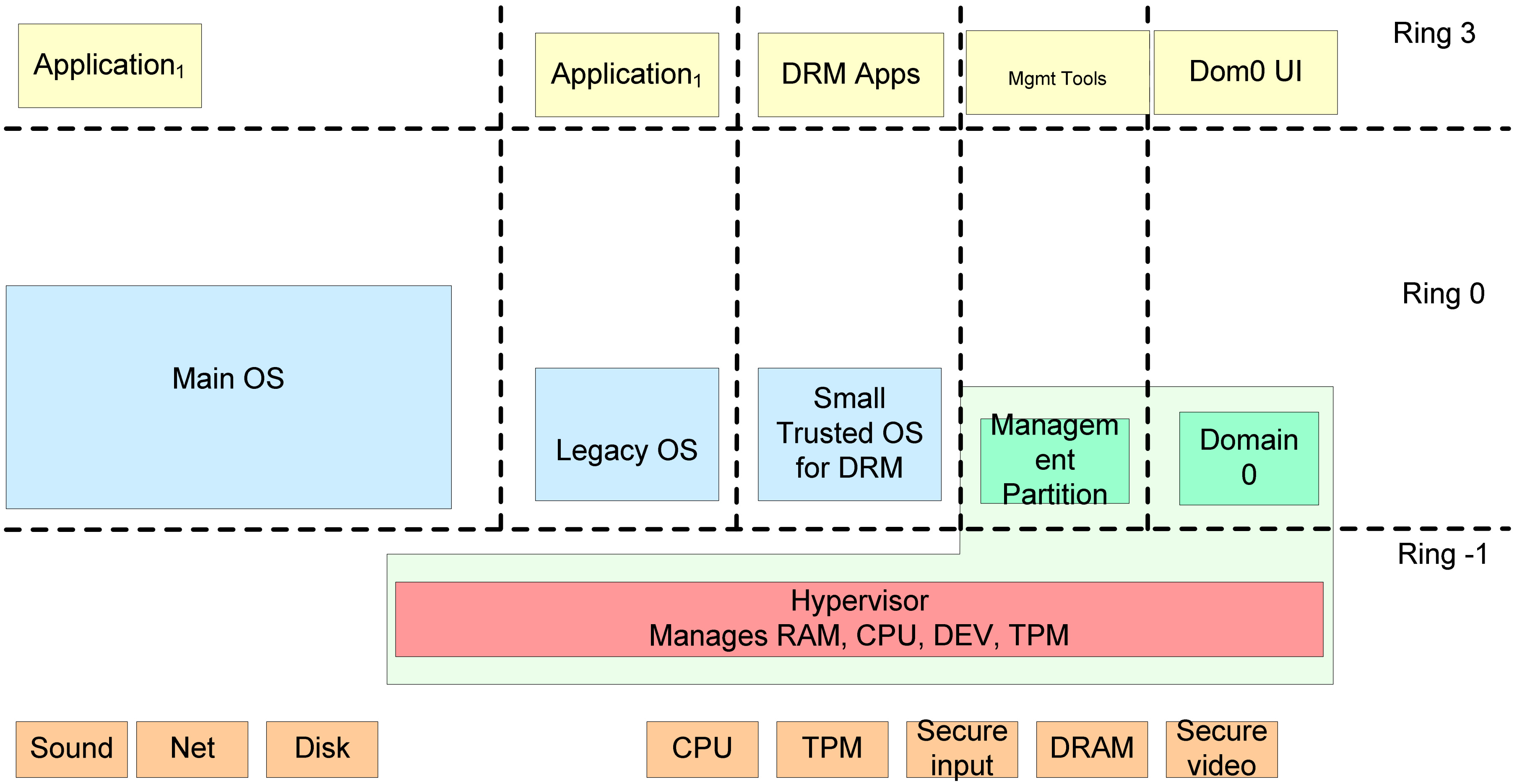
Customer benefits

- Licenses can be used offline
- Simple management of authorization (no central authority)
- Very simple and flexible distribution (a server can distribute to “any” client)

Key Hardware Components



A Hypervisor?



XrML Expressions

Each “rights expression” may specify a combination of rules such as:

- **what rights are available,**
- **for whom,**
- **for how many times,**
- **within what time period,**
- **under what access conditions,**
- **for what fees,**
- **within which territory, and**
- **with what obligations,**
- **Etc.**

“Small” Rights Management

- Protecting Personal Information
- Protecting personal Health and Financial information
- Protecting individual communication
- Protecting Corporate information

Scenarios for Small Rights Management

Web Content	• Secure database-backed content • Intranet portals • Backward compatibility for earlier apps
Protected Information	• Who can access sensitive plans • Level of access: print, edit, save, etc. • Length of access period
Do-Not-Forward Email	• Keep mail off internalmemos.com • Secure Executive-level mail • Consistent application of expiry rules
Centralized Policy Control	• Centralized logging of license requests • Centralized templates to express policy • Offline and online scenarios

“Big” Rights Management

- Mass Market Content
  - Books
  - Audio
  - Video
  - Software
- Much more flexible use and better content management
  - But there are “Fair Use” concerns which can be mitigated … maybe

Scenarios for Big Rights Management

Pay per view movies

- Premium releases
- Price discrimination

Web distributed songs

- I hear it. I want it. I get it.
- Lower manufacturing costs
- More variety?

Ring tones

- Most popular use of DRM
- I don’t get it

E-Books

- Library/archive
- Roaming
- “Active” content

Watermarking

- Durable, imperceptible marking of content. Each “mark” is one bit of information.
  - Robust watermarking – watermark is hard to removed (using Stirmark, etc)
  - Approach taken by SDMI, Digimarc, Verence.
  - A failure, generally speaking
- Watermarking is content specific
  - Text- custom spacing, custom fonts, deliberate errors
  - Music – Changes to Fourier transformed components
  - Picture – Slight changes to Fourier transformed image
  - Video
- Watermarking bandwidth is also content specific

How a watermarking system protection systems work

- One bit of information (The “protected bit”) signals to player (IE, RealPlayer, Windows Media Player, DVD Player) that content is protected and requires a license.
  - Sometimes additional bits encoded identifying content
- Player refuses to play content without a license

- Can you think how to defeat this?
  - Hint: Don’t ask, don’t tell, don’t enforce

DRM Systems in the News

- SDMI
- Windows Media Player
- Real DRM
- Apple DRM
- IRM
- CSS
- Macrovision
- LexMark
- Xbox
- Sony Playstation

Technical Issues in Mechanisms

- Break Once Break Everywhere
- Degree of isolation
  - Transducer Problem
  - I/O
- Privacy and Interoperability
- Flexibility (transfer, etc)
  - Multiple devices
  - Multiple users
  - Migration
- User Control/Backup

Social and Policy Issues

- “Fair Use”
- Monopoly “Lock-in”
- Erosion of copyright in favor of “contracts”
- Archive
- DMCA and hacking
- “Information wants to be free”
- Consumer expectations
- Draconian licensing policies

An Analog Attack …