

Wagging the Dog

How Digital Rights Management needs are driving OS design

John P. Daigle

Department of Computer Science
Georgia State University

04.20.07

Outline

- 1 Introduction: What is DRM
- 2 Implementation
 - Traditional OS
 - DRM and Vista: Case Study
 - Trusted Computing Model
- 3 Do We Need DRM?

Outline

- 1 Introduction: What is DRM
- 2 Implementation
 - Traditional OS
 - DRM and Vista: Case Study
 - Trusted Computing Model
- 3 Do We Need DRM?

Definition and Purpose

What is DRM?

- Digital Rights Management
- Usually perceived as an extension of copyright law
- In this paper, a technology meant to prevent media “piracy”
- I.E., the goal of DRM is to make sure you cannot back up your music files

How is DRM implemented?

- Fairplay
- Macrovision

Requirements

- 1 The client cannot remove the encryption from the file and send it to a peer.
- 2 The client cannot 'clone' its DRM system to make it run on another host.
- 3 The client obeys the rules set out in the DRM license.
- 4 The client cannot separate the rules from the payload.

Outline

- 1 Introduction: What is DRM
- 2 **Implementation**
 - Traditional OS
 - DRM and Vista: Case Study
 - Trusted Computing Model
- 3 Do We Need DRM?

Strategies for DRM

Software Level

Apple's "Fairplay" is implemented at the level of the iTunes software, and nowhere else. Typical release/hack time is two weeks for software, 3 minutes per song. Fairplay cannot implement the 4 rules.

OS Level

Windows Vista has a large number of DRM components. Vista monitors and certifies:

- 1 All peripherals
- 2 All media

Windows Vista DRM has, according to one source, already been hacked.[1]

Limitations on a traditional OS

Case: Movie

What must be accomplished to protect a movie for two days of viewing?

Limitations on a traditional OS

Case: Movie

What must be accomplished to protect a movie for two days of viewing?

- ① Time Sensitive: Unalterable Datekeeping

Limitations on a traditional OS

Case: Movie

What must be accomplished to protect a movie for two days of viewing?

- 1 Time Sensitive:Unalterable Datekeeping
- 2 Protected Data:Encryption

Limitations on a traditional OS

Case: Movie

What must be accomplished to protect a movie for two days of viewing?

- 1 Time Sensitive:Unalterable Datekeeping
- 2 Protected Data:Encryption
- 3 Trusted Output:Monitor is not a recorder

Limitations on a traditional OS

Case: Movie

What must be accomplished to protect a movie for two days of viewing?

- 1 Time Sensitive:Unalterable Datekeeping
- 2 Protected Data:Encryption
- 3 Trusted Output:Monitor is not a recorder
- 4 Trusted Software:No decryption software running

Implementing the requirements

1 Maintain Time Sensitivity

- System clock must be guaranteed at boot time
- Content state must be constantly updated
- Otherwise: Content could be moved to or deployed to a virtual machine with a dishonest clock.

2 Encryption

- User cannot access the plaintext of the message. There must be sealed storage that the user does not have privileges to.
- Otherwise: they have the key. They have the decoder. They have the ciphertext and the plaintext. How long can your crypto last?

Implementing the requirements

1 Maintain Time Sensitivity

- System clock must be guaranteed at boot time
- Content state must be constantly updated
- Otherwise: Content could be moved to or deployed to a virtual machine with a dishonest clock.

2 Encryption

- User cannot access the plaintext of the message. There must be sealed storage that the user does not have privileges to.
- Otherwise: they have the key. They have the decoder. They have the ciphertext and the plaintext. How long can your crypto last?

Implementing the requirements

1 Maintain Time Sensitivity

- System clock must be guaranteed at boot time
- Content state must be constantly updated
- Otherwise: Content could be moved to or deployed to a virtual machine with a dishonest clock.

2 Encryption

- User cannot access the plaintext of the message. There must be sealed storage that the user does not have privileges to.
- Otherwise: they have the key. They have the decoder. They have the ciphertext and the plaintext. How long can your crypto last?

Implementing the requirements

1 Maintain Time Sensitivity

- System clock must be guaranteed at boot time
- Content state must be constantly updated
- Otherwise: Content could be moved to or deployed to a virtual machine with a dishonest clock.

2 Encryption

- User cannot access the plaintext of the message. There must be sealed storage that the user does not have privileges to.
- Otherwise: they have the key. They have the decoder. They have the ciphertext and the plaintext. How long can your crypto last?

Implementing the requirements

1 Maintain Time Sensitivity

- System clock must be guaranteed at boot time
- Content state must be constantly updated
- Otherwise: Content could be moved to or deployed to a virtual machine with a dishonest clock.

2 Encryption

- User cannot access the plaintext of the message. There must be sealed storage that the user does not have privileges to.
- Otherwise: they have the key. They have the decoder. They have the ciphertext and the plaintext. How long can your crypto last?

Implementing the requirements

1 Maintain Time Sensitivity

- System clock must be guaranteed at boot time
- Content state must be constantly updated
- Otherwise: Content could be moved to or deployed to a virtual machine with a dishonest clock.

2 Encryption

- User cannot access the plaintext of the message. There must be sealed storage that the user does not have privileges to.
- Otherwise: they have the key. They have the decoder. They have the ciphertext and the plaintext. How long can your crypto last?

Implementing the requirements

1 Maintain Time Sensitivity

- System clock must be guaranteed at boot time
- Content state must be constantly updated
- Otherwise: Content could be moved to or deployed to a virtual machine with a dishonest clock.

2 Encryption

- User cannot access the plaintext of the message. There must be sealed storage that the user does not have privileges to.
- Otherwise: they have the key. They have the decoder. They have the ciphertext and the plaintext. How long can your crypto last?

Implementing the requirements

1 Trusted Drivers

- No unapproved devices can be allowed
- This means all video cards, monitors, and speakers must be “trusted” and constantly updated
- Otherwise, any output device could be a recorder instead of a display.

2 No changes to system

- System must be clean at boot, all trusted
- System must be constantly checked
- Otherwise, malicious program could be launched

Implementing the requirements

1 Trusted Drivers

- No unapproved devices can be allowed
- This means all video cards, monitors, and speakers must be “trusted” and constantly updated
- Otherwise, any output device could be a recorder instead of a display.

2 No changes to system

- System must be clean at boot, all trusted
- System must be constantly checked
- Otherwise, malicious program could be launched

Implementing the requirements

1 Trusted Drivers

- No unapproved devices can be allowed
- This means all video cards, monitors, and speakers must be “trusted” and constantly updated
- Otherwise, any output device could be a recorder instead of a display.

2 No changes to system

- System must be clean at boot, all trusted
- System must be constantly checked
- Otherwise, malicious program could be launched

Implementing the requirements

1 Trusted Drivers

- No unapproved devices can be allowed
- This means all video cards, monitors, and speakers must be “trusted” and constantly updated
- Otherwise, any output device could be a recorder instead of a display.

2 No changes to system

- System must be clean at boot, all trusted
- System must be constantly checked
- Otherwise, malicious program could be launched

Implementing the requirements

1 Trusted Drivers

- No unapproved devices can be allowed
- This means all video cards, monitors, and speakers must be “trusted” and constantly updated
- Otherwise, any output device could be a recorder instead of a display.

2 No changes to system

- System must be clean at boot, all trusted
- System must be constantly checked
- Otherwise, malicious program could be launched

Implementing the requirements

1 Trusted Drivers

- No unapproved devices can be allowed
- This means all video cards, monitors, and speakers must be “trusted” and constantly updated
- Otherwise, any output device could be a recorder instead of a display.

2 No changes to system

- System must be clean at boot, all trusted
- System must be constantly checked
- Otherwise, malicious program could be launched

Implementing the requirements

1 Trusted Drivers

- No unapproved devices can be allowed
- This means all video cards, monitors, and speakers must be “trusted” and constantly updated
- Otherwise, any output device could be a recorder instead of a display.

2 No changes to system

- System must be clean at boot, all trusted
- System must be constantly checked
- Otherwise, malicious program could be launched

Implementing the requirements

1 Trusted Drivers

- No unapproved devices can be allowed
- This means all video cards, monitors, and speakers must be “trusted” and constantly updated
- Otherwise, any output device could be a recorder instead of a display.

2 No changes to system

- System must be clean at boot, all trusted
- System must be constantly checked
- Otherwise, malicious program could be launched

Vista, the First DRM based OS

The Tech Spec

“It is recommended that a graphics manufacturer go beyond the strict letter of the specification and provide additional content-protection features, because this demonstrates their strong intent to protect premium content”

The Goal

The goal of Vista's content protection is to prevent you from viewing unauthorized HD content.

Device Monitoring I

- HD can only be output through HDCP connectors
 - Therefore perhaps one card supports HD content under Vista
 - DVI-D, 15-pin D-Sub, S-Video, and component video connectors cannot be trusted and will not carry HD content
- Some content will merely be degraded, not shut off altogether
- Vista has an error for “Resolution Too High”
- Content cannot be fed back into the machine
 - voice applications (skype, etc) require this for echo cancellation
 - VOIP performance degrades under Vista
- Drivers cycles slow down
 - Devices must be specified more carefully, no unified drivers
 - All drivers must be signed by Microsoft.

Device Monitoring II

- Currently, very few drivers are signed by Microsoft
- Worldwide signature revocation for leaky devices
- “tilt bits”: small problems restart graphics subsystem
- All device traffic must be encrypted: heavy CPU usage
- Experts agree that all of this is useless.[7]

What *will* work?

Least Privilege

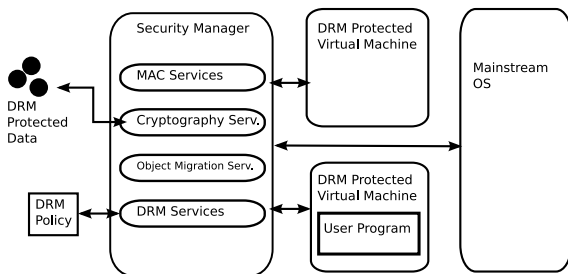
The system must be able to assign to each process only those permissions that are actually needed, and no more, to guarantee security.

Trusted Computing

The system can be trusted to implement a security model. This means changing access from user centered to process centered, Mandatory Access Control model. A MAC OS

- Several Levels of Security
- Defined at the CPU
- Same input/output limitations

3 Layer Approach



- Solves the access problem, as the user cannot access the plaintext or the cyphertext
- Does not solve the functional problems that we saw with Vista

Outline

- 1 Introduction: What is DRM
- 2 Implementation
 - Traditional OS
 - DRM and Vista: Case Study
 - Trusted Computing Model
- 3 Do We Need DRM?

Effectiveness

Can non-MAC DRM be effective in combatting piracy?

No. Easy software, physical, and hardware hacks will beat *any* DRM scheme. The reason is that there has to be a way for the consumer to view the media, thus creating the lever for reverse engineering the cryptography scheme or hardware.[7]

What does standard DRM accomplish

DRM makes it marginally more difficult for non-technical people to re-purpose media for personal use, or to trade media with their friends.

Is this a desirable outcome?

?

Ethical Problems With DRM

- 1 No Backups, must buy things twice
- 2 Inhibits Fair Use
- 3 Stifles creativity:the “clearing” problem
- 4 Increases Hardware/Software Costs
- 5 Places more control with larger companies: prohibition of non-secure content
- 6 Requires more laws, limits free speech, destroys America
- 7 Inevitably takes control of machines away from consumers

For Further Reading I



P. Gutmann.

A cost analysis of windows vista content protection.
Web site, University of Auckland, Private Bag 92019
Auckland, New Zealand, April 2007.



S. Bekker.

Trojan found piggybacking sony drm rootkit.
ENT, November 2005.



L. J. Camp.

Drm: doesn't really mean digital copyright management.
In *CCS '02: Proceedings of the 9th ACM conference on
Computer and communications security*, pages 78–87,
New York, NY, USA, 2002. ACM Press.

For Further Reading II



A. Cooper and A. Martin.

Towards an open, trusted digital rights management platform.

In DRM '06: Proceedings of the ACM workshop on Digital rights management, pages 79–88, New York, NY, USA, 2006. ACM Press.



T. Gal, H. M. Singer, and L. Popkin.

The ip war: apocalypse or revolution?

In DRM '03: Proceedings of the 3rd ACM workshop on Digital rights management, pages 39–46, New York, NY, USA, 2003. ACM Press.

For Further Reading III



D. Monniaux and J.-B. Soufron.

Drm as a dangerous alternative to copyright licences.

UPGRADE: The European Journal for the Informatics Professional, VII(3), June 2006.



J. F. Reid and W. J. Caelli.

Drm, trusted computing and operating system architecture.

In *ACSW Frontiers '05: Proceedings of the 2005 Australasian workshop on Grid computing and e-research*, pages 127–136, Darlinghurst, Australia, Australia, 2005. Australian Computer Society, Inc.