22-Sep-2011

CS 557 Presentation
Why DRMs don't work

Lessons from the Sony CD DRM Episode

J. Alex Halderman and Edward W. Felten

Debayan Gupta
(All Wrongs Revenged)

Case Study: XCP and MediaMax

(so, we will be focusing on audio CD DRMs)

- How and why they were made
- How they worked
- How to get around them
- Problems
- Lessons

Conclusions

- The design of DRM systems is driven by the incentives of the content distributor and the DRM vendor (which may not always be identical). "user", "copyright law", "artist"
- DRM can expose users to significant security and privacy risks (especially DRM vendors).
- The better the DRM is at "controlling" users, the worse are the security holes it causes.
- CD DRM systems are almost entirely useless.
- DRMs don't really follow copyright law (they don't even try) – they follow only the "rules" dictated by the label's and the vendor's business models.
- The stakes are high.

We think it unlikely that future CD DRM systems will do better.

DRM Incentives

- Label
  - Can't stop p2p (needs only 1 "evil" file)
  - Stopping local copying might increase sales.
    - Stopping, say, copying to iPod may create new revenue, but it reduces the original value of the CD (to the user)
    - Strategic Decision: control use, or increase original value ?
  - Can make money by monetizing platform (ads, statistics)
  - "Using DRM to enforce copyright law exactly as written is almost certainly not the record label's profit-maximizing strategy."
- Vendor
  - (usually) higher risk tolerance than label
  - vendor can leverage the installed platform to make money in ways the record label can't.
  - Wants BIG BASE.

DRM Requirements

- Must play on CD players
- Must be unreadable to computer programs (other than the vendor's own software)
- Should "prevent copying"
- Compatibility & Updates
- Should not be "annoying"

Methods

- Active Protection
  - Once the DRM is installed, every time a new CD is inserted, the software check to see whether it is protected by the DRM. If so, the active protection software will interfere with accesses to the disc, except those originating from the vendor's own music player application.
- Temporary (pre-active) protection
  - Runs before active protection is installed (more on this later)
- Passive Protection
  - If you can't convince them, confuse them!

Installation

- Autorun
  - Windows
  - Shift, Felt-tip pen, Antivirus, procexp, etc.
- Temporary protection (before active protection is installed)
  - Could install automatically, but legal (Computer Fraud and Abuse Act) and ethical (!) issues
  - EULA

Temporary Protection

- XCP
  - Monitors system for “blacklisted” processes
  - 30 second timer if found
  - **Solution**: Kill process, or lock drive
- MediaMax
  - Installs Active protection before EULA (exe/dll)
  - Copies sbcphid.sys to the Windows drivers directory, sets it up as a service in the registry, and runs it.
  - Manual to Auto: update bug (no time limit!)
  - Files not removed even if EULA is declined

Misleading Text

- MediaMax EULA

Passive Protection

- Confuse computers without confusing CD players
- Multisession Trick
  - “Advanced” Software: Nero
  - Non Windows platforms
  - Good ol’ Felt-tip marker

What should active protection do?

- **Uniqueness**
  - Identify protected discs without triggering the copy protection on unprotected ones.
- **Detectability**
  - Reliably and quickly detect the feature in protected discs
- **Indelibility**
  - Can’t remove without degrading audio quality (copies will still have DRM).
- **Unforgeability**
  - Only the vendor should be able to create protected discs.

What did the “active protection” try to do?

- Tried to recognize the disc
  - Steganography (e.g. MediaMax watermark)
    - Relied on unpublished method for protection
    - Didn’t work. <- deletable, forgeable, etc.
    - “Rosetta Stone”: Velvet Revolver’s *Contraband*, 3 versions:
      - U.S. release protected by MediaMax
      - European release (passive scheme developed by Macrovision)
      - Japanese release with no copy protection.
    - XCP: marker in data track (simple mechanism ☺)
- Upon recognizing a disc as “protected by my DRM”, monitor and interfere with disc access
  - corrupt the audio returned by the drive (random jitter, white noise, etc.)
- Sent usage information back to the vendor/label

How to get around active protection

- Proprietary media players with backdoors
  - Can burn a limited number of backups (no further generations of copying)
  - Can rip, but still DRM protected format
- Attacks
  - Rollback
  - Edit file that keeps track of backups (primitive encryption)
  - Sony provided a workaround!! (burn WMA)
  - Can simply deactivate MediaMax service
  - Can delete XCP files

XCP + iPod

- XCP copied open source software to add an iPod compatibility feature.
- Inactive, but fully functional

Security Concerns: MediaMax

- Lax Permissions (%programfiles%\Common Files\SunnCommShared)
  - Change permissions back, you say?
- Even if user declines EULA, files remain
  - dll “attack”: how MediaMax checks its files
  - Users who decline an EULA usually assume that nothing has been installed on their computer
- Sony Patch
  - Checks the dll file

Security Concerns: XCP

- Installs a rootkit
  - Hides everything starting with **sys**
  - Modifies OS without permission
  - Unstable

Uninstallation

- Customized uninstallers
  - Worked only on one computer
  - Used ActiveX controllers to download file!
  - Didn’t remove “Remove” (MediaMax)
  - Similar problem in XCP

CAM (Consumer Anger Management)

- ***Audio*** CD
- Deliberate risks (it was hard to pass off a rootkit as an “implementation error”)
- Reluctant (and incompetent*) uninstallation

*couldn’t find a better word

Hopefully, there’s enough time left for discussion.