

Lessons learnt from SONY CD DRM Episode:

1) Increased complexity does not mean increased security (Economy of Mechanism)

2) User Experience matters (Psychological acceptability)

3) Incentives Matter:

Incentives vary depending on the party. Design decisions are influenced by incentives.

-- Music Labels

-- Risk averse as reputation is at stake

-- They want to please users.

-- DRM Vendors

-- More risk tolerant as they are small companies trying to acquire more market share.

-- They want to please labels.

-- Users

-- Would like to exercise full rights

-- Perhaps abuse the rights :)

Incentives of Music Labels:

Music DRM is ineffective at preventing mass piracy. But attempts can be made to:

-- Reduce piracy or make it harder

-- Preventing CD-to-CD copy

-- Limited Distribution

-- Enable redundant selling (Same user may have to buy multiple cds for home, car etc)

Incentives of DRM Manufacturers:

-- Prevent copying

-- Build Install base to build credentials

-- Increase value to customers

-- Control DRM standards

-- Data Harvesting (Make illegal use of end user information for profits)

User Incentives:

-- Fair usage rights

-- System's security

-- System Reliability

-- System transparency

-- Privacy

-- Abuse the rights

4) DRM Manufacturer Sins:

From the whole episode, it appears that DRM vendors were the culprits:

-- Invaded user privacy

-- Harmed legal users

- Opened back doors to user's systems
 - For example, XCP installed rootkits which hid all files and processes whose name began with \$sys\$. They also created a directory with system services and open permissions. This created a serious security hole in the user's system.
- Failed to obtain user consent before installing software on systems
- Voilated other people's copyrights
- Restricted some legal rights of users
- Initial system did not have uninstall procedure at all. After public uproar, they finally provided an uninstall procedure which aimed at making the uninstall itself difficult:
 - First approach they used was providing a cumbersome procedure for uninstalling the software which took many days.
 - The second approach involved installing Active X controls on the system to uninstall their software. So active x control remains on system forever! Also, it opened new avenues for security breach:
 - Parameters to Active X control specified location to download a dll and then execute its code.
 - Via this framework, any other malicious code can be downloaded and installed and run on the system.

5) The Paper did not talk about the incentives misalignment between users and DRM vendors.

6) Incentive Misalignment:

- Party A pays for security (Good DRM code by DRM vendors)
- Party B benefits (user benefits as his system is secure)

Examples:

Egress Filtering:

Infected/Malicious Machine <---> ISP's Router <---> Internet <---> Amazon.com server

In the above scenario, the machine floods amazon with packets having fake return addresses and launches DOS on Amazon. To avoid this, the intermediate routers have Egress filtering in place so that information flow outbound from one network to another can be restricted. Thus,

- Router does the job
- Amazon.com benefits

Online Banking and ATM usage:

- In US, banks are responsible for frauds
 - So US banks took all measures to enhance security
- In UK, users are liable for any fraud
 - Banks did not care about security, there were cases of insider frauds.
- All this due to incentive misalignment!
- **Reference:** <http://axion.physics.ubc.ca/atm.html>