Lessons from the Sony CD DRM Episode (05/08/2009)

General Points:
- Increased Complexity => Increased Security
- User Experience Matters

Incentives are different for the parties involved
- Music Label - Risk Tolerant
- DRM - Risk averse
- User - Wants to exercise full rights

Incentives/Goals of Record Label:
- prevent CD-CD copying
- limit illegal distribution
- enables redundant selling

Incentives/Goals of DRM Manufacturer
- have a huge installed base
- prevent copying
- increased value to customers
- control standards
- sell people information, data harvesting

Incentives of User
- Fair Use Rights
- Security cannot be compromises
- system reliability
- system transparency
- privacy

DRM Manufacturers mistakes
- invaded user privacy
- makes legal use difficult
- backdoor attempts are made easier now
- failed to obtain user consent
- violated other people copyrights
Rootkit-
- Patched a few system calls and filtered in the results
- Hide all files with $sys$
- Created directory with system service and open permission
- A malicious user can just sit on top of the root kit. It makes his job much easier

Final Uninstall was also defective
- Installs Active X control
- Parameter to Active X control specifies location to download all and then execute its code.
- Active X Control left on the system.
- Malicious Web Pages can use this Active X control later.

Incentive Misalignment
- Party A pays for security
- Party B benefits

Egress Filtering:
Target Machine--> Router -->Internet-->Amazon
We can perform egress filtering on the router so that packets leave only from known IP.
This way Amazon is saved but router is overloaded.

ATM principle
US
- Bank is liable
- Hence has reason to invest in security measures like hidden cams, data logging etc

UK
- Customer is liable
- No incentive for the bank to actually try to install extra security measures