**Paper: Lessons from the Sony DRM Episode**

- Increased complexity ≠ increased security
- User experience matters
- Incentives matter
  - Music labels
    - Risk averse
    - Want to please users
  - DRM manufacturers
    - Risk tolerant
    - Want to please labels
  - User
    - License full rights
- Incentives of record label
  - Music DRM ineffective at preventing mass piracy
  - Prevent CD to CD copying
  - Limited distribution
  - Enables redundant setting
- Incentives of DRM manufacturers
  - Prevent copying
  - Build uninstall base
    - Increase value to customers
    - Control standards
    - Data harvesting
- Nobody cared about the users' interests
  - Fair user rights
  - System security
  - System reliability
  - System transparency
  - User privacy
- DRM manufacturers == malicious
  - SONY - negligible role
  - DRM users invaded user privacy
  - Harmed legal users
  - Illegal users attack
  - No prompt for user consent before uninstallation
  - Used GPL code as resource
  - Opened back door to user system
  - Restricted some legal \ rights of users
  - Violated other peoples' copyrights
- **Root kit**
  - Intended to hide malicious s/w running on computer
  - Anything could hide in this rootkit
  - Rootkit hid all files and processes whose names began with '$sys$'
  - Hunch that such a strategy was followed so that users think of it as a SYSTEM process rather than something malicious and external
  - Could have chosen something like '$sysxcp $' etc

- **Uninstall procedure**
  - Weak
  - Created directory with system services and user permissions
  - Final arguments use ActiveX
    - Install ActiveX control
    - Parameters to ActiveX control specific locations to download dll and then execute its code
    - ActiveX left on the user system with no set procedure to automatically uninstall it

- **Ultimate sufferer :: user**
  - Ends up paying for security breaches

- **Incentive misalignment**
  - Party A pays for security
  - Party B benefits

- **Security Feature**
  - Floods Amazon
  - Avoids being discovered
  - Set fake return addresses
    - Egress filter
    - Knows all machines on particular side of router have particular IP addresses

RESULT: Amazon saved but router overloaded

- **ATM use**
  - UK, USA
  - Users averse to using ATM
  - No human watch in ATM cubicle
  - Security through obscurity