Software and vulnerabilities

Robert Sloan, March 2010

Software: Purity and Transparency

- "*Transparency*" = software disclosing all functions to end users. (E.g., no "Easter eggs").
- *Purity:* (stronger) = software doing only what you expect, not having any functions foreign/irrelevant to stated purpose and utility.
  - Impure (usually also opaque)
    - Sony CD copy protection software (the infamous rootkit)
    - Comcast injection of reset packets
    - Microsoft Live OneCare in 2007 changing user settings to re-enable Windows services disabled on purpose. (Documented, albeit obscurely)
  - Opaque:
    - Anti-cheating Warden snooping your computer in World of Warcraft

Most Vulnerabilities limited set of sources

- Security issues arise heavily from small group of programs
  - Windows
  - Flash players
  - Adobe PDF readers/writers
  - Web Browsers (3–4?), Microsoft Office, Email Clients (3–5?), Media players (5), Backup
  - Security: Anti-virus and firewall
  - Server-side stuff (including *all* server OS!)