Digital Rights Management

CS 166: Introduction to Computer Systems Security
Digital Rights Management (DRM) is a term used for systems that restrict the use of digital media. DRM defends against the illegal altering, sharing, copying, printing, viewing of digital media. Copyright owners claim DRM is needed to prevent revenue lost from illegal distribution of their copyrighted material.
Early U.S. Copyright History

• US Constitution, Article 1, Section 8
  – “To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries”

• Copyright Act of 1790
  – "the author and authors of any map, chart, book or books already printed within these United States, being a citizen or citizens thereof....shall have the sole right and liberty of printing, reprinting, publishing and vending"
  – Citizens could patent books, charts, or maps for a period of 14 years – Could renew for another 14 years if you were alive
  – Non-citizens and works form other countries not protected
Copyright Act of 1976

- Could copyright literary works, musical works, dramatic works, choreographic works, graphical works, motion pictures, and sound recordings (architectural works added in 1990)
- Copyright holders had exclusive right to reproduce, create derivative works of the original, sell, lease, or rent copies to the public, perform publicly, display publicly
- Could hold copyright for 28 years with a possible 28 year extension
- Rights of copyright holders are limited slightly by sections 107 through section 118 – Often referred to as Fair Use
Fair Use Doctrine

• When reproducing a particular work is considered fair use
  – Criticism, comment, news reporting, teaching, scholarship, research

• Four factors for determining fair use [17 U.S.C. § 106]
  1. The purpose and character of the use, including whether such use is for commercial nature or is for nonprofit educational purposes;
  2. The nature of the copyrighted work;
  3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
  4. The effect of use upon the potential market for or value of the copyrighted work
Sony vs. Universal Studios

• In the 1970s, Sony invented Betamax, a video tape recording format similar to VHS
• Could be used to record copyrighted broadcasts
• At the same time, some movie studios created Discovision which was a large disk that would disintegrate after a few plays
• In 1976 Universal Studios and Disney sued Sony for all the lost profits and tried to ban the use of Video Tape Recorders (VTR)
• District Court for the Central District of California rejected the claim on the basis that noncommercial use of VTRs was considered fair use
• Court of Appeals for the Ninth Circuit reversed the ruling and held Sony liable for aiding in copyright infringement
Sony vs. Universal Studios (cont.)

• In 1984, the Supreme Court revisited the issue of whether selling VTRs to the public aids in copyright infringement.

• It ruled that “the sale of the VTR’s to the general public does not constitute contributory infringement of copyrights”
  – Most copyright holders who license their work for public broadcast would not mind having their broadcasts recorded on a Betamax tape by viewers.
  – Betamax was ruled that it fell under the Fair Use clause.

• Landmark case often referred to in subsequent lawsuits.
Digital Millennium Copyright Act (DMCA)

- Illegal to circumvent anti-piracy measures built into software
- Unlawful to create, sell, or distribute devices that illegally copy software
- Legal to crack copyright protection to conduct encryption research, assess product interoperability, and test computer security systems
- Exceptions to nonprofit libraries, archives, and educational institutions in some cases
- ISPs are not held accountable for transmitting information resulting from their customers infringements
- Service providers are required to remove material when found
Dmitry Skylarov (Elcomsoft)
• Wrote software to remove encryption from PDF documents (legal in Russia)
• Arrested in the US and jailed for DMCA violations
• Eventually Elcomsoft sued and Skylarov released
• Elcomsoft found not guilty of DMCA violations

Edward Felten (Princeton)
• Secure Digital Music Initiative (SDMI) invited researchers to break watermark technology
• Felten and his team succeeded and wrote paper for conference
• SDMI and RIAA threatened legal action
• Felten sued RIAA and SDMI
• SDMI and RIAA withdrew threat
• Felten eventually presented paper
Copy Protection Methods

• Dongle
  – Pluggable hardware device that contains a secret value required to run the software

• Product key
  – Required to be entered by installation software
  – Online check for duplicate use
  – Hardware and OS fingerprinting to bind license to machine

• Phone activation
  – Human-to-human interaction servers as deterrent
A controller distributes protected content to a collection of devices

The devices share a common symmetric key with the controller

Each content item is encrypted with the shared key and broadcast to all the devices

Some devices (traitors) are cloned or used to illegally copy and distribute protected content

Problems:
- Identifying traitors
- Revoking traitors
Logical Key Hierarchy

- Balanced binary tree of symmetric encryption keys
- Devices associated with leaves, each holding the keys on the path to the root
- Content encrypted with the key of a node $v$ can be decrypted by all the devices in the subtree of $v$
Revocation of a Device

- If a device needs to be revoked, the keys known to this device must be changed and the new keys must be distributed.
- The distribution of new keys can be done with a logarithmic number of encrypted broadcast messages.
Encrypted Broadcasts

- Content hierarchy with various subscription packages
- Each content item is encrypted with a single symmetric key before broadcasting
- Subscriber authorized to view item must have the key to decrypt the item
- Single key per node allows computation of keys of descendant nodes
- Key distribution problem
What We Have Learned

• Legal framework and historical perspective on copyright
• DMCA and implications on DRM research
• Restricting software installation and execution
• Device revocation
• Encrypted broadcasts