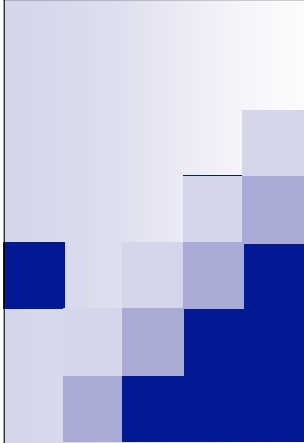




Z24: Digital Rights Management

Mark Handley



Intellectual Property Law

- “Intellectual property law cannot be patched, retrofitted, or expanded to contain digitized expression...*Information wants to be free.*”

John Perry Barlow

- Is he right?

[See “Information Rules, A Strategic Guide to the Network Economy”
by Carl Shapiro and Hal Varian]



Production and Distribution

- Digital technology lowers production costs
- Digital technology lowers distribution costs
- Examples
 - Tape recorder lowers production, but not distribution costs
 - AM radio broadcast lowers distribution costs, not reproduction costs



Make Lower Distribution Costs Work for You

- Information is an experience good
- Must give away some of your content in order to sell rest
- Can use product line/versioning
 - Easy to read, hard to print
- Historical Examples:
 - Libraries
 - Video rental as prelude to purchase
 - Growing the market



Demand for Repeat Views

- Give away all your content, but only once
- Music, books, video have different use patterns
- Children
 - Barney: free videos
 - Disney: sued daycare centers
- Adults



Illicit Copying

- Timely information: not a big problem
- Cheap information: not a big problem
- Negative feedback: the bigger you are, the easier to detect



Lessons

- Two challenges: cheap production, cheap distribution
- Cheap distribution: helps advertise by giving away samples
- Cheap distribution: good for bootleggers, but their need to advertise helps control them
- Copy protection that imposes costs on users is vulnerable to competitive forces



IANAL

*I am not a lawyer.
I'm probably wrong on legal issues.*



THE LAW

There are four basic types of Intellectual Property Law

Copyright

- Protects writing, music, video, etc against copying.
- Occurs by default.

Patent

- Protects ideas against duplication.
- Must be filed for.

Contract

- Does whatever the contract says.
- May not override your natural rights.

Trade Secret

- Protects against industrial espionage.



Fair Use Rights

■ US Law:

- ☐ Can copy a recording you own for personal use.
- ☐ Timeshifting.
- ☐ To play on a different device.

■ UK Law:

- ☐ No fair use provision.
- ☐ But in practice, not enforced for personal use.

DMCA

- Digital Millenium Copyright Act (US)
 - Makes it illegal to traffic in a device to defeat a copy protection mechanism.
- European Copyright Directive
 - Needs to be implemented in each nation individually
 - Has similar restrictions to the DMCA

For commentary, see:

- Ed Felton's blog: <http://www.freedom-to-tinker.com/>
- Electronic Frontier Foundation: <http://www.eff.org/>
- Foundation for Information Policy Research: <http://www.fipr.org/>

Copy Protection Mechanisms

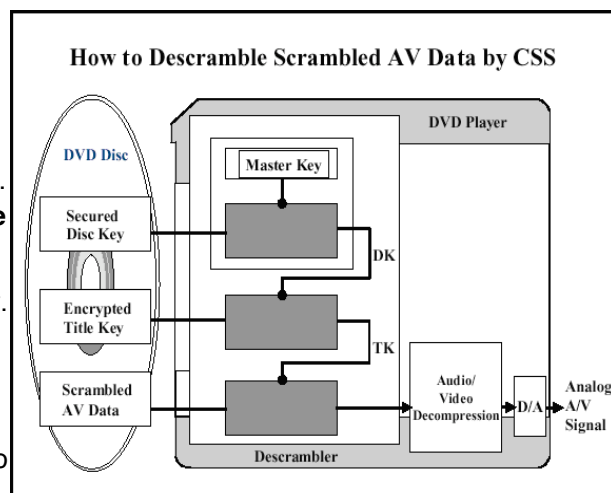
- An Audio CD only holds raw audio data and an index.
 - No copy protection.
- But CDs are also used to store data. The differences between audio players and data players can be exploited.
 - CD index can have *multiple versions* (for multi-session CDs).
Can have the first index correct and the next index corrupted.
Audio players only play the first.
 - Can make the CD “*autoplay*” in computers.
- These are hacks to deter casual copying.
 - They annoy customers!

DVD Copy Protection

- Content Scrambling Scheme (CSS)
- Region Encoding

CSS

- (1) Read encrypted **disk key** from the DVD
- (2) Uses its **player key** (master key) to decrypt the disk key.
- (3) Read encrypted **title key** for the file to be played. Each file has its own title key.
- (4) Use decrypted disk key to decrypt the title key.
- (5) Finally, use the decrypted title key to descramble the actual content.



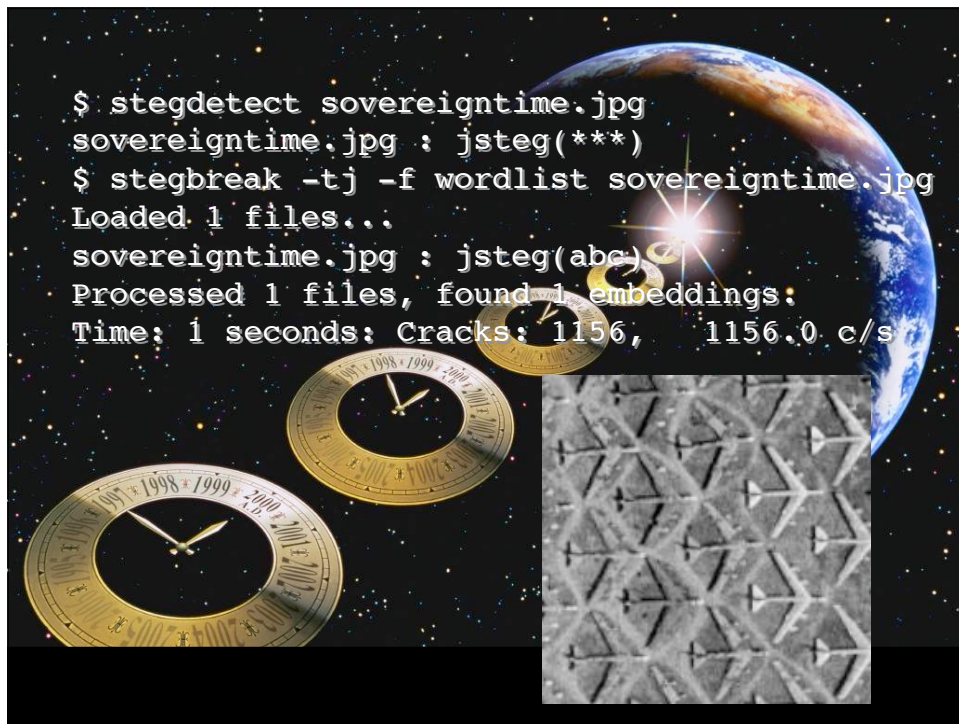
CSS Weaknesses

- The data encryption is only 40 bits.
- A master key needs to be embedded in every player.
 - The use multiple master keys to protect against leakage, but how do you revoke a key?
 - Theoretically impossible to disguise a key in a software player.
 - Can only make it hard to find.

DECSS

- Jon Lech Johansen in Norway managed to extract the Master Key from the Xing software player.
- Wrote DECSS
- Massive damage control attempt by the DVD Copy Control Association
 - DMCA, Trade Secret Law
- Basically failed.

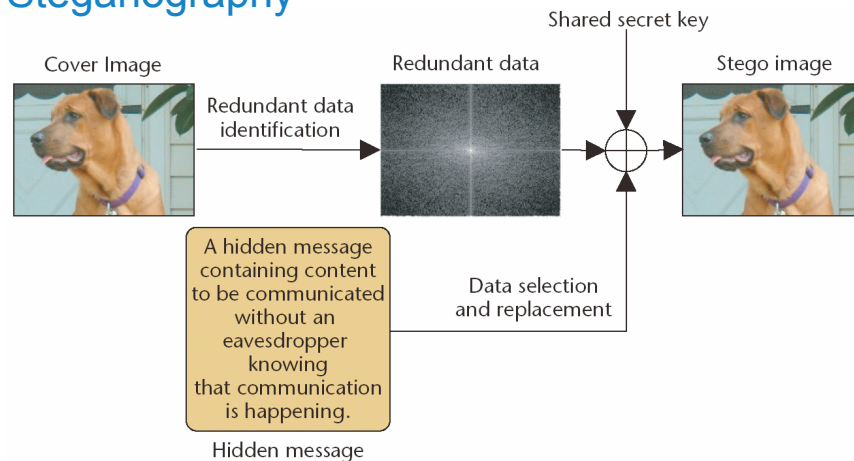




Steganography

- Steganography is the science of hiding data in otherwise plain text or images.
 - The previous image hides data inside inside JPEG images.
- Data can be hidden in pretty much all forms of multimedia data - anywhere the user won't notice.
 - E.g., replace the least-significant bits of each sample in a CD audio file, and no-one will hear the difference.

Steganography

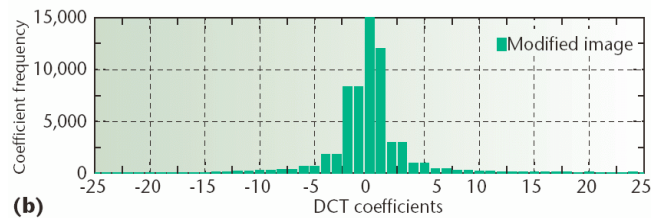
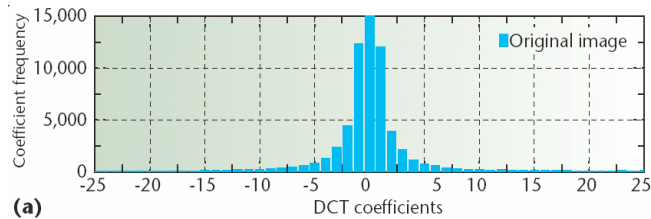


Hide and Seek: An Introduction to Steganography - Niels Provos and Peter Honeyman, *IEEE Security & Privacy Magazine*, May/June 2003

jsteg

- The JPEG encoding procedure divides an image into 8x8 blocks of pixels in the YCbCr colorspace.
 - A discrete cosine transform (DCT) is done on each block.
 - The resulting frequency coefficients are scaled to remove the ones which a human would not normally detect.
- If steganographic data is being loaded into the JPEG image, the loading occurs after this step.
 - The lowest-order bits of all non-zero frequency coefficients are replaced with successive bits from the source file to be hidden.
- These modified coefficients are sent to the Huffman coder.

Steganalysis



Graphs show frequency sequential changes to the least significant bit of the DCT coefficients.

- ☐ Randomizing the LSB tends to equalize adjacent coefficients.

Watermarking

- Like steganography, the aim is to hide information.
 - ☐ The goal is to be able to tell which original a copy of the data was made from.
 - ☐ Just need to hide a unique number for each copy.
 - ☐ Perhaps hide a signal to compliant media devices “this is copyright”, so they won’t copy it.
- Unlike steganography, the goal is to make the ID impossible to remove without destroying the data.
 - ☐ Does the copier know the ID is there?
 - ☐ The problem of collusion.
 - ☐ The problem of transcoding.



SDMI Challenge

- **Secure Digital Music Initiative**, a group whose goal is to "protect the playing, storing, and distributing of digital music"
- In 2000, open invite to people to attempt to crack technologies they were considering for use in their system.
 - Ed Felton and students at Princeton analyzed the watermarked clips, and successfully modified them so that the watermarks could no longer be detected, while maintaining a level of audio quality satisfactory to SDMI.
 - Got threatened with the DMCA when they tried to publish their results (SDMI backed down).



"Trusted Computing"

- The big problem is that the content providers can't trust the media players (if they're on general purpose computers).
- "Trusted Computing" platforms aim to solve this.
 - The hardware contains authentication mechanisms so it will only run a trusted OS.
 - The trusted OS will validate and certify trusted applications.
 - Content providers can then safely provide their content to the trusted applications, safe in the knowledge their data can't be copied.



Copy via analog?

- Can still copy through analog recording.
 - ☐ If you only do this once, the quality degradation is minimal.
- Aim is to have secure interfaces from PC to disk, from PC to display, from PC to speakers.
 - ☐ Impossible to tap without re-recording (with a microphone or camera).
- The death of the general-purpose PC?
- **Do you want to live in such a world?**