Practical Aspects of Modern Cryptography

Winter 2011

Josh Benaloh
Brian LaMacchia

Agenda

- Guest lecture
- Final project presentation logistics
- The Politics of Crypto
  - Export Controls
  - Key Escrow
    - The Clipper Chip
  - Copyright and the DMCA
- Course evaluations

Agenda

- Guest lecture
- Final project presentation logistics
- The Politics of Crypto
  - Export Controls
  - Key Escrow
    - The Clipper Chip
  - Copyright and the DMCA
- Course evaluations

Final Project Presentations

- All sessions start at 6:30pm
- MSR Building 99 sessions will be in 99/1915

- Thursday evening, March 17, at UW 15
- Friday evening, March 18, at MSR 9
- Wednesday evening, March 16, at MSR 6
- Either Wednesday or Friday 5
  - If you selected this option (either Wed or Fri) *please come on Wednesday*

Agenda

- Guest lecture
- Final project presentation logistics
- The Politics of Crypto
  - Export Controls
  - Key Escrow
    - The Clipper Chip
  - Copyright and the DMCA
- Course evaluations

Why Talk About Crypto Politics?

- You can't really avoid the political aspects of crypto, especially if you're trying to ship a product that depends on good crypto
  - In the past, the regulations have been so complex & time consuming that companies had dedicated individuals/departments for dealing with regs.
- Often public pronouncements don't match reality
  - Just because a government body says "crypto is freely exportable" doesn't make it so

Caveats...

- I'm going to present a (mostly) U.S.-centric view of the issues
  - Each country deals differently with these issues, but the U.S. typically leads in this policy area
- These are national issues – nation-states are still important to the discussion
- Much of what we have learned about the history of export controls has come from FOIA requests
  - The government doesn't like to give answers...

Agenda

- Guest lecture
- Final project presentation logistics
- The Politics of Crypto
  - Export Controls
  - Key Escrow
    - The Clipper Chip
  - Copyright and the DMCA
- Course evaluations

Export Controls in the U.S.

- In the beginning, cryptographic hardware and software were considered “munitions” by the U.S. government.
  - Export of crypto was covered by the same set of regulations that covered the export of other munitions, like nuclear weapons, missiles, and the equipment that is used to make them
  - These regulations were known as ITAR (International Traffic in Arms Regulations).

Export Controls (cont.)

- Under ITAR, all exports of crypto required a license
  - If you were exporting “weak crypto” you could get a license.
    - “Strong crypto” couldn’t be exported at all.
    - “Crypto with a hole” couldn’t be exported either.
  - The distinction between “weak” and “strong” was generally based on bit-length of the secret key or public key modulus

Crypto Export/Import Controls

- The export of cryptography is currently restricted by the U.S. Bureau of Industry and Security (BIS, part of the US Department of Commerce)
  - Until January 2000, couldn't export symmetric ciphers using keys > 56 bits in length.
  - Jan 2000: Clinton administration rewrote the regulations
    - "ITAR" became "EAR", and the regulations got a bit "looser" but they still exist
    - You can (generally speaking) export "strong crypto" without a specific product license

Current Export Regulations

- "Monolithic applications" can export strong cryptography in binary form simply by sending the BIS a piece of e-mail
  - Example: secure e-mail client, web browser
- "Crypto libraries" can be exported under an "open source" exemption, if they qualify
  - Again, by sending BIS a piece of e-mail with a link to where the sources are posted
- "Crypto with a hole" in commercial products is still tightly controlled

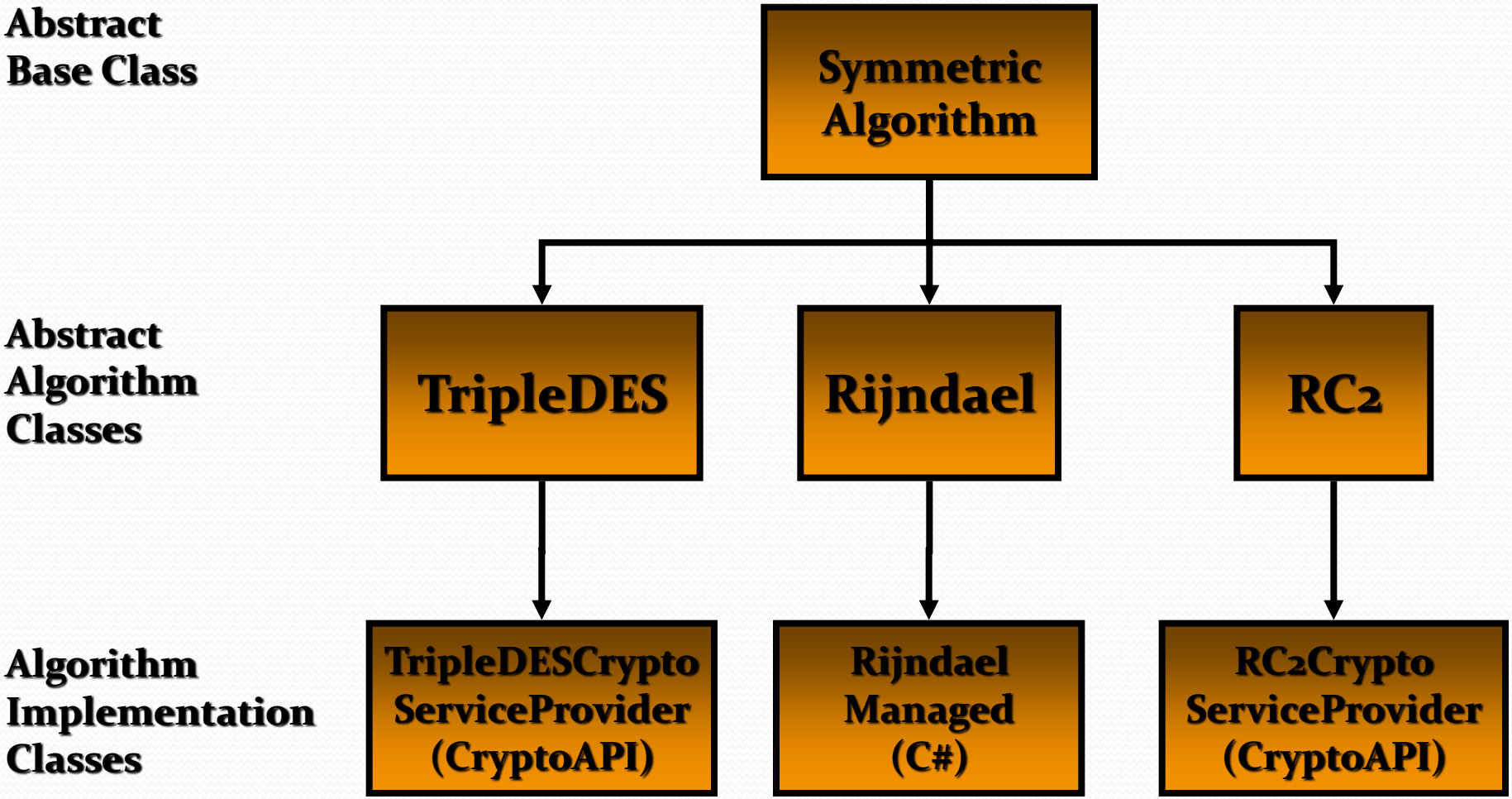
Example: Windows 7

- Windows XP ships with “strong crypto” baked in & enabled
  - RSA to 4096 bits, TripleDES, etc.
- Windows XP is exportable because it’s a “monolithic application”
- CryptoAPI, the Win32 crypto library that was designed to support plug-able “cryptographic service providers” is not freely exportable
  - If you want to plug into CryptoAPI, you need a license...

The Regs are Still Ambiguous

- In the .NET Framework, we have a class library for cryptography…
- It took BIS 18 months to tell us what the rules were regarding export of our class library…

.NET FX Crypto Object Model



The Regs are Still Ambiguous

- In the .NET Framework, we have a class library for cryptography…
- It took BIS 18 months to tell us what the rules were regarding export of our class library…
- We could open up & let people subclass the bottom abstract classes (like RSA) without a license
- Opening up AsymmetricAlgorithm was not allowed without an explicit license
- Solution? Open source the code!

Agenda

- Guest lecture
- Final project presentation logistics
- The Politics of Crypto
  - Export Controls
  - Key Escrow
    - The Clipper Chip
  - Copyright and the DMCA
- Course evaluations

Key Escrow

- The general topic of “key escrow” is about archiving copies of private keys with third parties.
  - This is also sometimes called “key archival”
  - When the government is the archive, this is GAK (Government Access to Keys)
- There are legitimate cases where you might need a key escrow scheme
  - Stored data recovery in case of accident/loss/termination of employment

Key Escrow

- There are no legitimate cases (at least from a commercial perspective) for archival of secret session keys.
  - If the data didn't get transmitted correctly during the session, send it again
- Governments care about session encryption key recovery
  - Want to preserve their wiretapping capabilities
- Government spent a lot of time trying to convince businesses that the needs of stored data recovery & session key recovery were the same

Digital Telephony

- In the U.S., the digitization of the nation's telephone system was seen by law enforcement as a threat to their ability to conduct wiretaps
  - In the analog world, you just go tap a pair of wires
  - In the digital world, you need to sift out the right bits from the optical fiber.
    - Even if you find the bits, they could be encrypted!

The Clipper Chip

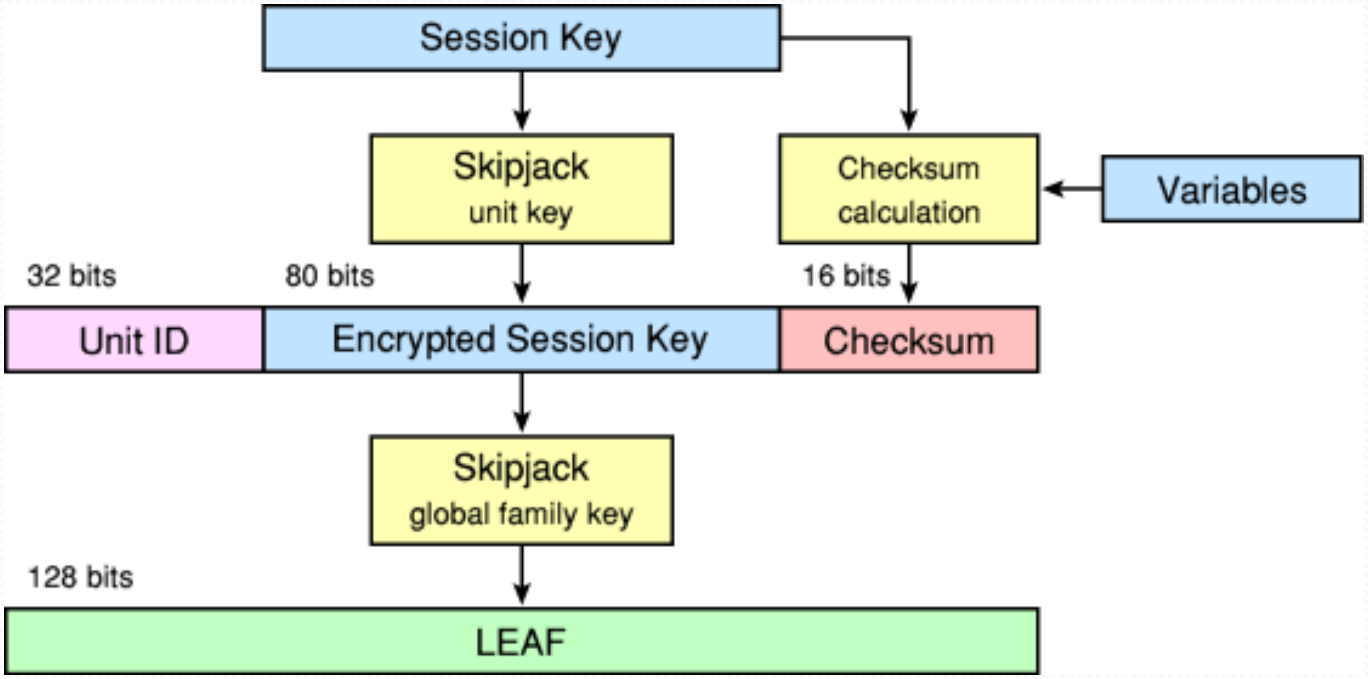
- US Government attempt to “stimulate” the market for “voluntary” key escrow equipment
  - Contracted w/ AT&T to produce “Clipper phones” for government use
  - Phones would also be available for non-government use
  - Encryption keys could be accessed through the “Law Enforcement Access Field” (LEAF) in the protocol

How Clipper Worked

- Clipper was implemented in a tamper-resistant hardware device (a single chip)
  - Each chip was numbered and had a separate per-chip secret that was also held by a "trusted agency" (read: US Gov't)
- Per-session keys were encrypted with a Clipper family key and the per-chip key, and sent along as part of the data stream
- Someone listening in on the conversation would see enough information to identify the chip used to encrypt, find the per-chip key, and recover the session key

How Clipper Worked (2)

- 128-bit LEAF contains session key encrypted with family and per-chip keys



- Image courtesy http://www.cryptomuseum.com/crypto/usa/clipper.htm

Clipper in Operation

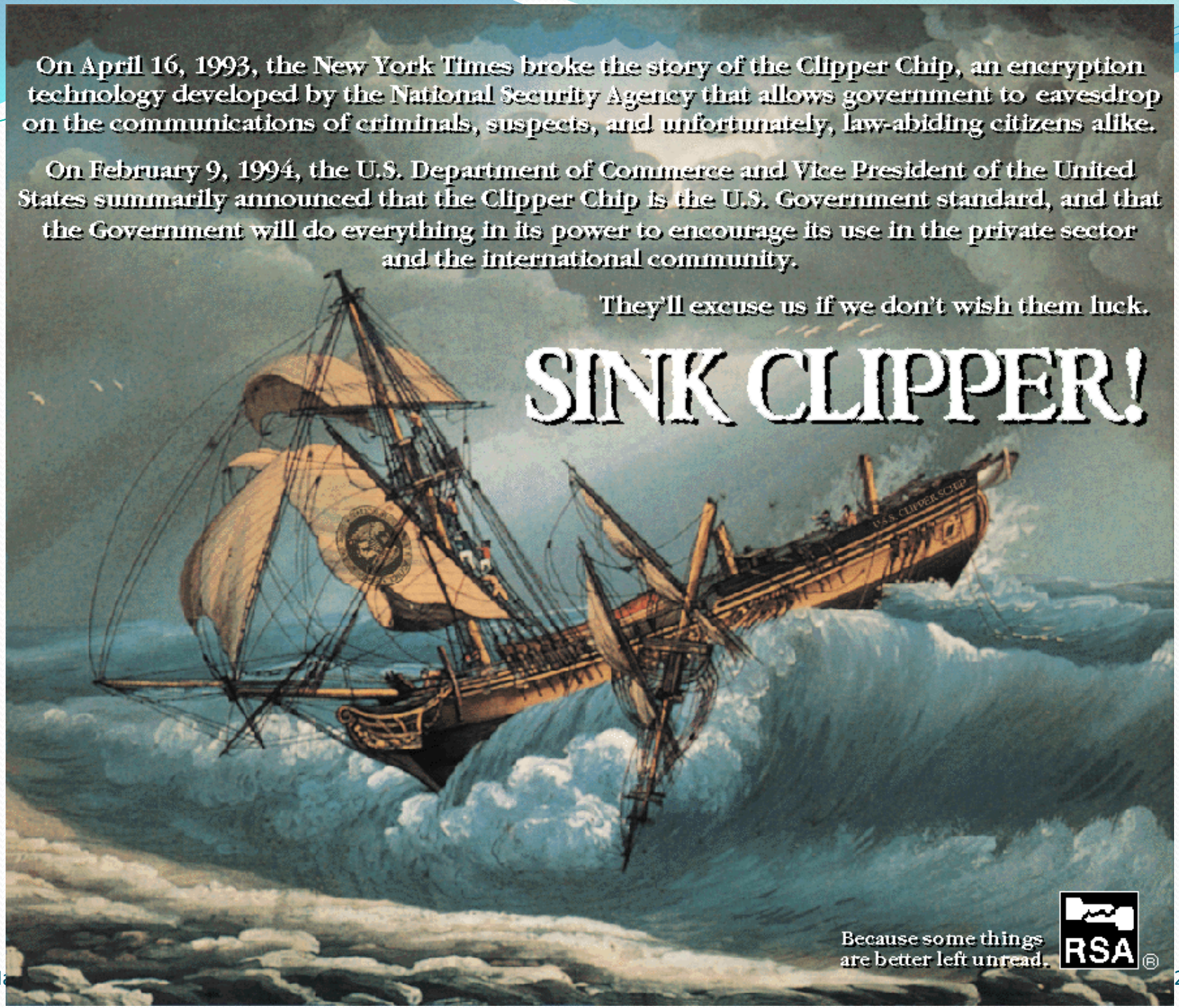
- Other party & third-party decrypt LEAF with the family key
- Both parties check the checksum to detect bogus LEAF
  - Bogus LEAF ➔ chip turns off, refuses to decrypt
- Third party looks up chip key in DB to decrypt session key

Clipper Weaknesses

- The 80-bit session key was too small
- The symmetric cipher (SKIPJACK) was classified; no public scrutiny
  - Later, a “panel of outside experts” was allowed to look at it for a day
  - Even later, after Clipper failed, SKIPJACK was declassified
- 16-bit checksum could be defeated (Blaze ’94)
- ChipID tagged every single communication

Opposition to Clipper

- Opposition to Clipper was widespread
  - The US Gov't proposed it as the federal Escrowed Encryption Standard and pushed it through NIST into FIPS-185 in Feb '94
  - During the public comment period, 300 comments received, only 2 supported it
- No one bought Clipper
  - AT&T shut down its product line, offered leftover phones to employees to get rid of them
- Oddly, the proposal probably did more to galvanize the strong-crypto community than anything else


On April 16, 1993, the New York Times broke the story of the Clipper Chip, an encryption technology developed by the National Security Agency that allows government to eavesdrop on the communications of criminals, suspects, and unfortunately, law-abiding citizens alike.
On February 9, 1994, the U.S. Department of Commerce and Vice President of the United States summarily announced that the Clipper Chip is the U.S. Government standard, and that the Government will do everything in its power to encourage its use in the private sector and the international community.
They'll excuse us if we don't wish them luck.
SINK CLIPPER!
U.S. CLIPPER SCHIP
Because some things are better left unread.
RSA ®

Agenda

- Guest lecture
- Final project presentation logistics
- The Politics of Crypto
  - Export Controls
  - Key Escrow
    - The Clipper Chip
  - Copyright and the DMCA
- Course evaluations

Copyright

- More recently, cryptography has become an issue in the area of copyright.
- Why?
- The rise of digital rights management (DRM) systems, all of which are based on strong crypto.
  - Break the crypto, break the DRM…

Copyright & DRM

- Digital Rights Management (DRM) technologies limit access to digital intellectual property.
  - Example: A DRM-protected e-book might let you loan it only once, and then for only a two-week period
  - Example: A DRM-protected streaming audio player could charge you based on bandwidth & content.
- Major issues:
  - How restrictive can a DRM be?
  - How restrictive should a DRM be?
  - How do DRMs interact with “fair use” and other copyright rights reserved to the public?

Digital Millennium Copyright Act (DMCA)

- Characterized by proponents as a “small, technical” change to US copyright law
  - In reality, made major, sweeping provisions to the rules regarding digital content
- Incorporated into U.S. law at 17 USC 1201 et. sec.
  - “No person shall circumvent a technological measure that effectively controls access to a work protected under [copyright]…”

Anti-Circumvention Measures

- The DMCA made it a crime to circumvent a “technological measure that effectively controls access to a work”
  - “A technological measure ‘effectively controls access to a work’ if the measure, in the ordinary course of its operation, requires the application of information…with the authority of the copyright owner, to gain access to the work.
- Limited exemptions for
  - Encryption research
  - Reverse-engineering computer programs for interoperability.

DMCA cases/issues (1)

- DeCSS
  - DVDs are encrypted. In order to play a DVD, a licensed DVD play must first authenticate to the DVD disk.
  - DeCSS is a program that removes/bypasses the encryption, allowing the DVD to be played on an “unlicensed” player, such as a Linux box.
  - MPAA sued, claiming DCMA violations
  - Upheld in NY

DMCA cases/issues (2)

- *Blizzard v. BNetD*
  - Reverse-engineering of client-server protocol to allow third-party servers
- *Felten v. RIAA*
  - The SDMI challenge
- Macrovision v. 321 Studios
  MGM v. 321 Studios
  - DVD copying software
- *US v. ElcomSoft and Sklyarov*
  - Criminal prosecution for distribution of ElcomSoft's "Advanced eBook Processor"
- *Lexmark v. Static Control*
  - Laser toner cartridges
- *Chamberlain v. Skylink*
  - Garage door remote controllers

DMCA Exemptions (2010 round)

- As part of the DMCA, every three years the Librarian of Congress is charged with investigating whether any classes of works should be exempted from the anti-circumvention provisions.
  - The Registrar of Copyrights conducts a rulemaking procedure & solicits input from the public. The result is a series of recommendations to the Librarian

DMCA Exemptions (2010 round)

- The results of the most recent round of exemption rulemaking was announced last July. Six classes of works were exempted. In short they are:
- Extraction of clips from CSS-protected DVDs for
  - Educational uses by college and university professors and by college and university film and media studies students
  - Documentary filmmaking;
  - Noncommercial videos
- Cellphone "jailbreaking" (two types: access to MO & third-part apps)
- Testing, investigating, security research on video games on personal computers
- Dongle-protected computer programs where the dongles are obsolete or malfunction.
- eBooks that have access controls that prevent screen readers/read-aloud functions.

- See http://www.loc.gov/today/pr/2010/10-169.html for details

Agenda

- Guest lecture
- Final project presentation logistics
- The Politics of Crypto
  - Export Controls
  - Key Escrow
    - The Clipper Chip
  - Copyright and the DMCA
- Course evaluations