Sensitive Information in a Wired World

CPSC 457/557, Fall 2013

Lecture 2, September 3, 2013

1:00-2:15 pm; AKW 400

http://zoo.cs.yale.edu/classes/cs457/fall13/

Basis of US Copyright Law

U.S. Constitution:

[Article I, Section 8]

"The Congress shall have Power…
[Clause 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…"

Note: The founding fathers did not feel the need to empower Congress to create physical property rights.

Examples of Exclusive Rights

- to reproduce the copyrighted work
- to prepare derivative works
- to distribute copies through sales, rental, lease, or lending
- to perform the copyrighted work publicly (applies, *e.g.*, to plays)
- to display the copyrighted work publicly (applies, *e.g.*, to sculpture)
- digital audio transmission

[These are paraphrases.]

Exception: “4-factors” test for “Fair Use”

- The purpose and character of the use, including whether such use is of a commercial nature or is for non-profit educational purposes
- The nature of the copyright work
- The amount and substantiality of the portion used in relation to the copyright work as a whole
- The effect of the use upon the potential market for or value of the copyrighted work

Exception: First-Sale Rule

- When a copyright owner sells a copy of a work, he relinquishes control over that copy but not over the work.
- The work cannot be reproduced by the purchaser, but the copy can be loaned, resold, or given to someone else.
- "Promotes progress" by enabling, *e.g.*
  - libraries
  - used book stores

General Structure of Copyright Law

- Copyright owners’ rights stated explicitly.
- General public has no explicitly stated rights, just exceptions to owners’ rights.
- Fair use is a *defense* against a charge of infringement.

This structure works fairly well for traditional media, particularly books.

Structure is Challenged by Digital Works

- Digital documents are fundamentally different:
  - Copies are perfect.
  - Copies can be made at zero cost.
  - Copying is not necessarily a good proxy for infringement.
- TPSs are imperfect:
  - A perfect TPS could moot fair use:
    no infringement, no charge, no defense.
  - But no TPS can be perfect in today's computers. General purpose PCs are programmable, and hence TPSs are circumventable (at least by experts).

Three Major “Enforcers” Support a Content-Distribution Business

- Copyright law

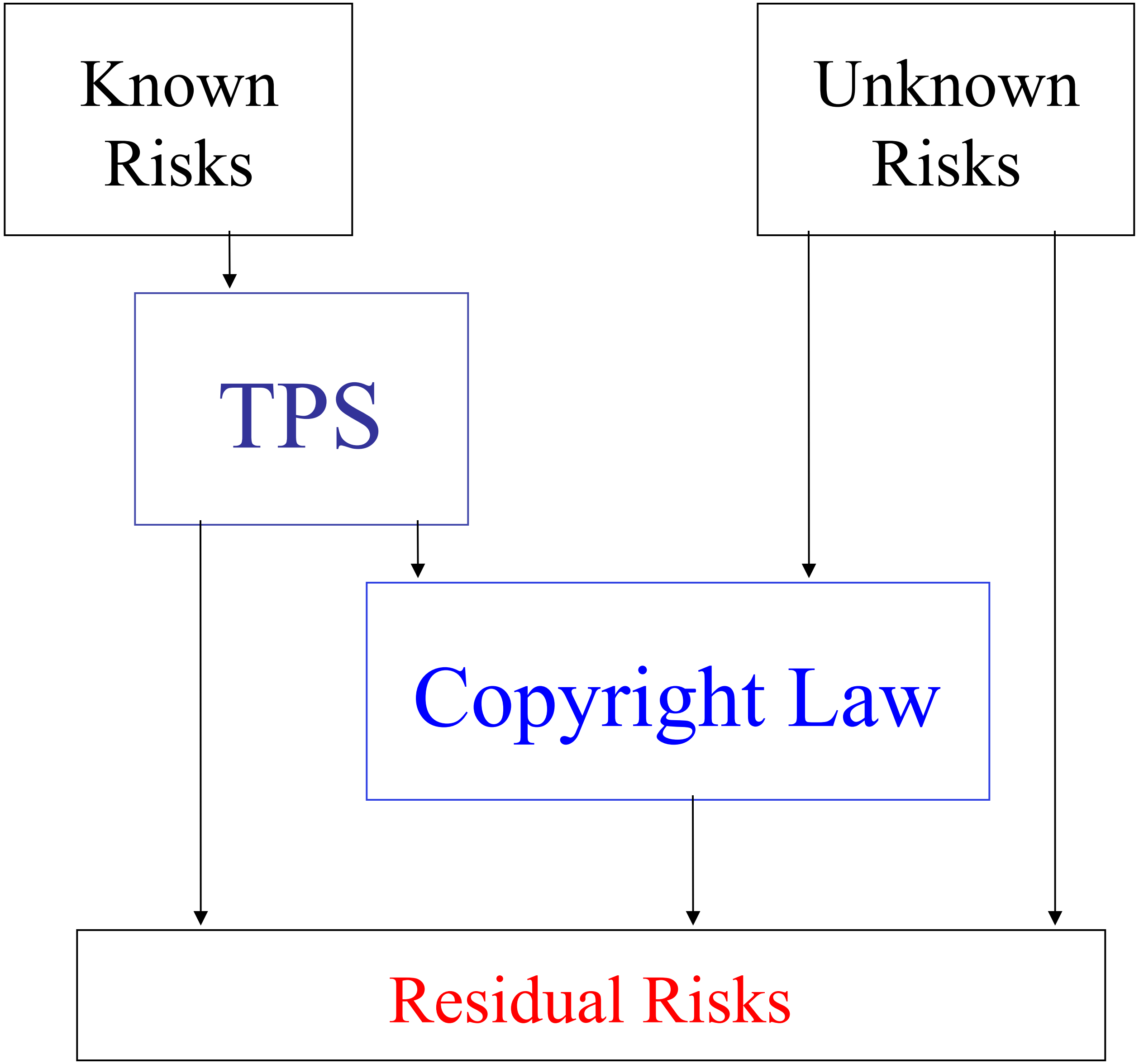
- Technical Protection System (TPS)

* Business Model

Dual Doomsday Scenarios

Rights Holders and Distributors: TPSs don't suffice. Digital copying, modification, and distribution are uncontrollable. We need more legal and social sanctions.

Fair-Use Advocates and (Some) Consumers: TPSs work too well. Some rights holders now have *more* control than they do in the analog world. *Normal* use can often be monitored and controlled in the digital world.



Known Risks

Unknown Risks

TPS

Copyright Law

Residual Risks

A.Rubin & M. Reiter – used with permission

Best TPS is a Great Business Model

"The first line of defense against pirates is a sensible business model that combines pricing, ease of use, and legal prohibition in a way that minimizes the incentives for consumers to deal with pirates."

Lacy *et al.*, IEEE Symposium on Industrial Electronics, 1997.

Holy Grail: A Great Business Model for Internet Music Distribution

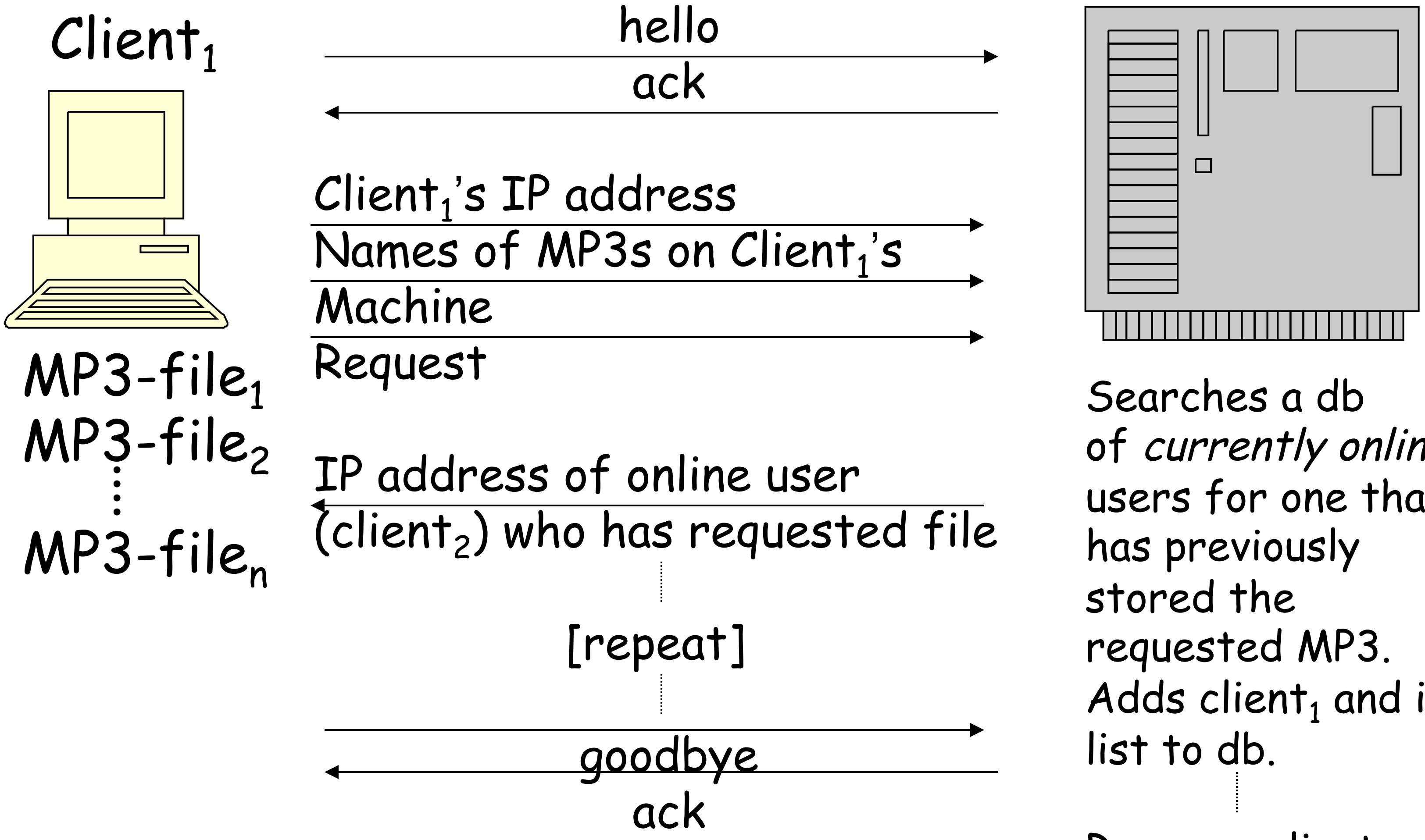
Hal Varian (quoted in C. Mann's 2000 "Heavenly Jukebox" article): "Maybe Coke will find a way integrate itself directly into the shows. Or they'll release the music free on the Internet, except that it will be wrapped in a commercial." What's the difference if the Spice Girls are marketed by Coca-Cola or by Virgin Records, soon to be a subdivision of AOL-Time Warner?

2000 Sales by RIAA members: $15B
2000 Coca-Cola Net Operating Income: $20.5B

Discussion Point

That was 13 years ago. Is Internet music distribution now a solved problem?

Napster Client-Server Interaction



Client$_1$

hello

ack

Client$_1$'s IP address

Names of MP3s on Client$_1$'s Machine

Request

IP address of online user (client$_2$) who has requested file

[repeat]

goodbye

ack

MP3-file$_1$
MP3-file$_2$
⋮
MP3-file$_n$

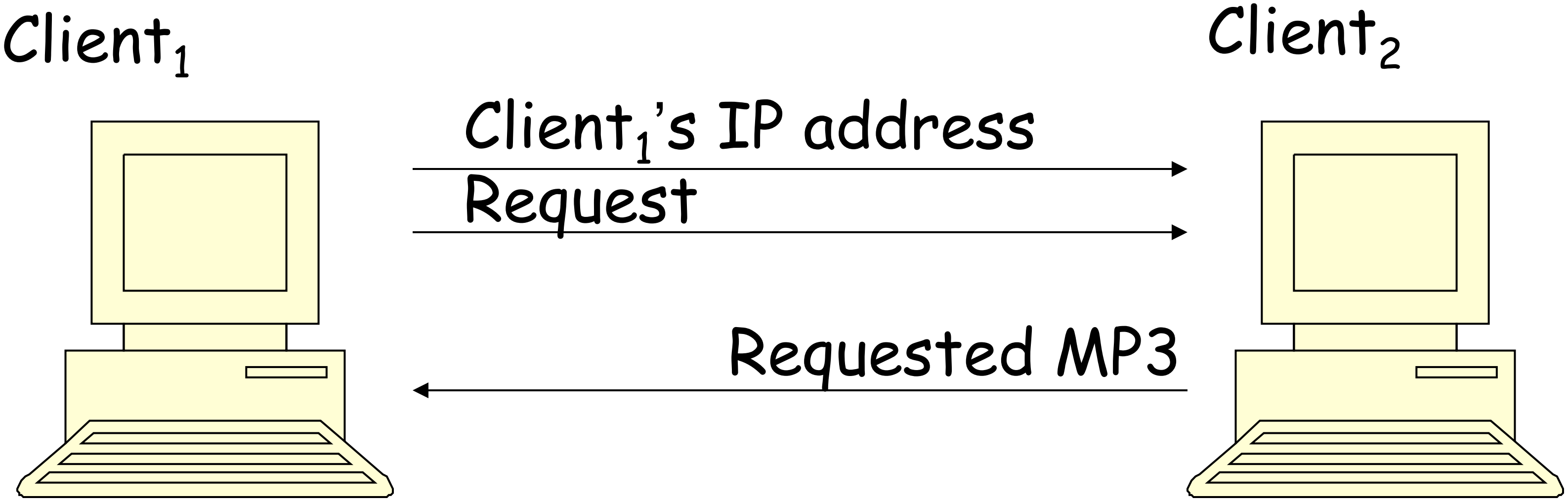
Searches a db of *currently online* users for one that has previously stored the requested MP3. Adds client$_1$ and its list to db.

Removes client$_1$ and its list from db

Noteworthy Features

- Proprietary protocol and db search.
- No MP3 files stored on server.
- Don’t *need* usernames. Could have made the service anonymous.
- No need to save IP addresses between sessions. Many are assigned dynamically.
- <u>Discussion point:</u> Are anonymity and memorylessness threats or opportunities for business?

Napster Client-Client (P2P) Interaction



Client$_1$

Client$_2$

Client$_1$'s IP address

Request

Requested MP3

Note: This part uses "standard Internet protocols," *e.g.*, FTP

Napster History

- 1987: MP3 format developed by Karlheinz Brandenburg of Fraunhofer Gesellschaft. “CD ripping” now feasible.
- 1999: Shawn Fanning develops Napster, believing he has “bypassed” copyright law. Napster has >25M users in its first year.
- Dec., 1999: RIAA sues Napster for “contributory and vicarious” copyright infringement.
- April, 2000: Metallica sues Napster, Yale, Indiana Univ., and USC. (Yale bans the use of Napster within a week.)

Napster History (2)

- July, 2000: US District Judge Patel grants RIAA's request for an injunction. The injunction is temporarily stayed soon thereafter.
- October, 2000: Napster announces a partnership with Bertlesmann AG (one of the "major labels" in the industry whose trade association is suing it!).
- January, 2001: Napster and Bertlesmann say that they will roll out a "subscription service" by "early summer" and will use "DRM technology."

Napster History (3)

- February, 2001: Ninth Circuit upholds lower court's findings that Napster is guilty of contributory and vicarious infringement.
- Summer, 2001: Napster and Bertlesmann fail to roll out subscription service.
- September, 2001: Napster reaches a settlement with music publishers (but not with RIAA record labels). However, CNET.com reports the number of users has "dropped from tens of millions…to almost zero."

Napster, R.I.P.

Digital Video Disks (DVDs)

- Developed by movie studios and consumer electronics companies in 1995.
- Compatible with CDs. Same size and thickness as CDs. Up to 25 times the storage capacity as CDs.
- TPS for DVDs includes
  - CSS encryption (“content scrambling system”)
  - R/W’able copy-control marks (*e.g.,* “copy freely,” “one copy,” “no copies”)
  - Macrovision analog copy protection
  - Other ingredients

Studios' Overall IP-Management Strategy

- Use TPS to "keep honest people honest."
- Assume (temporarily) that lack of bandwidth will prevent large-scale Internet distribution of movies.
- → Use courts aggressively to punish (alleged) violators of existing copyright laws and *lobby heavily* for new laws that favor rights holders.

Digital Millennium Copyright Act (1998)

- Illegal, except under narrowly defined special circumstances, **to circumvent effective technological protection measures**
- Illegal to distribute **circumvention tools**
- Gives content owners a property right in TPS as well as the content that the TPS protects. In SAT terms, circumvention is to infringement as breaking and entering is to burglary.

Examples of Allowed Circumventions

- Nonprofits may circumvent to "shop."
- Law enforcement and intelligence agencies
- Reverse engineering to achieve interoperability
- "**Encryption research**." The "researcher" has to "make a **good faith effort** to obtain authorization."
- Protection of "personally identifying information"

Techies' Objection to DMCA

- What is an "**effective** technological protection measure?"
  - If a skilled hacker can break it, is it "**effective**"?
  - If an average computer-literate person can break it, *but few do*, is it "**effective**"?
- Weakens incentives for content owners to pay for good IP-management technology.
- Shifts costs from content owners to society at large by shifting responsibility from TPSs to courts and police.
- **Exceptions for R&D are vague**.

DMCA vs. Copyright Violations

Questions:

- What does the DMCA actually do to existing copyright law?
- What happens to fair use?
- Are there differences between **violations of copyright law** and **violations of the DMCA**?

DeCSS Violates DMCA

- DeCSS is software that reads CSS-scrambled video from a DVD and writes unscrambled MPEG-2 video.
- In effect, DeCSS **circumvents** the TPS for DVDs.
  - **Question:** Is CSS an ***effective*** copy-protection mechanism?

DeCSS Violates DMCA (2)

- Magazine that published the DeCSS algorithm got sued.
  - **Question:** Is this different from "a reputable journal" publishing **research**?
- **Question:** Is DeCSS different from a regular DVD player?
- **Questions:** Does DeCSS fit under any of the DMCA exceptions? Where is the **copyright violation**?

AEBPR (Adobe eBook Processor) Violates DMCA

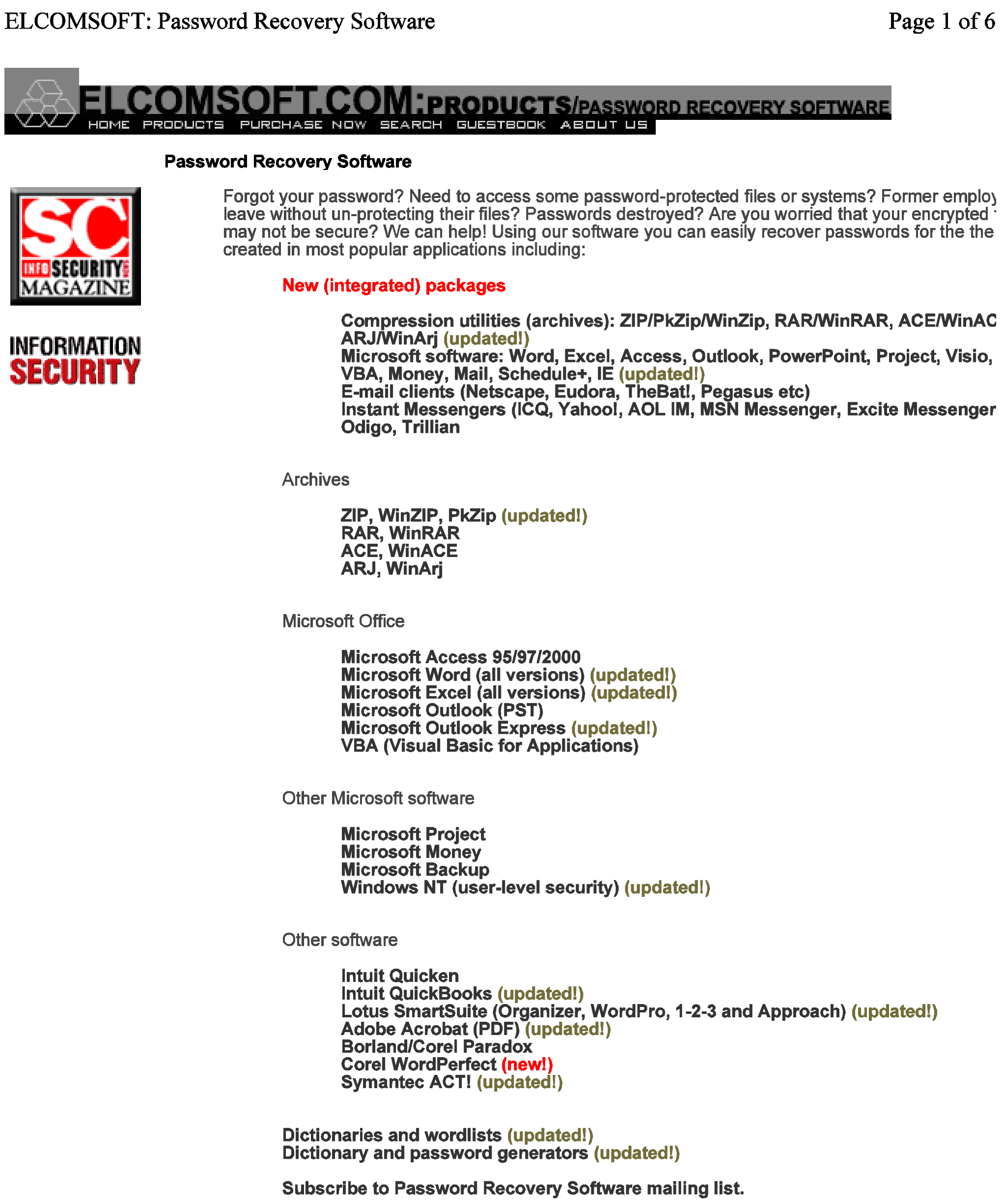
- Adobe established one format for electronic books: the "Adobe **eBook**."
- To use eBooks, purchase and download them, and view them using a special reader (Adobe eBook client).
- The eBook format contains provisions for publisher controls on:
  - Text-to-speech processing
  - Copying to another device or making a backup
  - Translating between formats

AEBPR Violates DMCA (2)

- ElcomSoft, a Russian company, created **AEBPR**, the **eBook Processor**.
  - AEBPR translates eBooks to Adobe PDF.
  - Software available for purchase on ElcomSoft's website and through a U.S. firm, RegNow (used for handling payments).
- Dimitri Sklyarov, one of the designers, presented his methods at DEF CON, a conference in the U.S.

ElcomSoft's Product Webpage

http://www.elcomsoft.com/prs.html


ELCOMSOFT.COM:PRODUCTS/PASSWORD RECOVERY SOFTWARE
HOME PRODUCTS PURCHASE NOW SEARCH GUESTBOOK ABOUT US
SC INFOSECURITY MAGAZINE
INFORMATION SECURITY

ELCOMSOFT: Password Recovery Software Page 1 of 6

Password Recovery Software

Forgot your password? Need to access some password-protected files or systems? Former employ leave without un-protecting their files? Passwords destroyed? Are you worried that your encrypted may not be secure? We can help! Using our software you can easily recover passwords for the the created in most popular applications including:

New (integrated) packages

Compression utilities (archives): ZIP/PkZip/WinZip, RAR/WinRAR, ACE/WinAC ARJ/WinArj **(updated!)**
Microsoft software: Word, Excel, Access, Outlook, PowerPoint, Project, Visio, VBA, Money, Mail, Schedule+, IE **(updated!)**
E-mail clients (Netscape, Eudora, TheBat!, Pegasus etc)
Instant Messengers (ICQ, Yahoo!, AOL IM, MSN Messenger, Excite Messenger Odigo, Trillian

Archives

ZIP, WinZIP, PkZip (updated!)
RAR, WinRAR
ACE, WinACE
ARJ, WinArj

Microsoft Office

Microsoft Access 95/97/2000
Microsoft Word (all versions) (updated!)
Microsoft Excel (all versions) (updated!)
Microsoft Outlook (PST)
Microsoft Outlook Express (updated!)
VBA (Visual Basic for Applications)

Other Microsoft software

Microsoft Project
Microsoft Money
Microsoft Backup
Windows NT (user-level security) (updated!)

Other software

Intuit Quicken
Intuit QuickBooks (updated!)
Lotus SmartSuite (Organizer, WordPro, 1-2-3 and Approach) (updated!)
Adobe Acrobat (PDF) (updated!)
Borland/Corel Paradox
Corel WordPerfect (new!)
Symantec ACT! (updated!)

Dictionaries and wordlists (updated!)
Dictionary and password generators (updated!)

Subscribe to Password Recovery Software mailing list.

AEBPR Violates DMCA (3)

- Sklyarov was arrested for **violating the DMCA** by circumventing Adobe's protection built into the eBook format.
- **Question:** Does it matter that Sklyarov was working for a company?
- **Question:** Does it matter that the company is Russian and that its software is legal in Russia?

AEBPR Violates DMCA (4)

- **Question:** Does the software simply allow "fair use" that was prevented by Adobe's format? (Does that even matter?)
  - People can make backups of eBooks they bought and don't want to lose.
  - People can transfer copies to their laptop or handheld.
  - People with visual impairments can have the computer read the eBook.
- **Other Questions:** Is AEBPR a product of research? Is the eBook TPS **effective**?