



The Natural Laws of Digital Content

Bruce Schneier

CTO, Counterpane Internet Security, Inc.
schneier@counterpane.com

**Digital Libraries: Digital Asset Management
Institute for Mathematics and its Applications
Minneapolis, MN—12 February 2001**



The Abstract Problem

- The owners of digital files would like to restrict how they are used by others
- Possible restrictions:
 - Copy protection: preventing a software owner from giving a copy of that software to someone else
 - Use limitation: allowing someone to buy a music or video file to play for a finite number of times—or for a finite period of time
 - Physical limitation: preventing someone from using a file on multiple devices
 - Copy prevention: allowing someone to view an image, but not save or copy it



The Abstract Solution

- There is none
- One of the fundamental differences between bits and atoms is that bits are infinitely and easily replaceable
- No amount of clever engineering can change this fact
- This is how the “physics” of bits works
- This is a natural law of digital content



Is There a Practical Solution?

- Enough about abstractions, we’re talking the real world here
- Is there a solution that is good enough?
- Is there a solution that works most of the time?
- Is there a solution that will allow content providers to remain in business?
- Is there a solution that allows content providers to manage their risks?



A Note About Terminology

- Digital file
 - Anything: software, text, graphics, audio, video
- Copy protection
 - Any form of use limitation—it does not matter
- User
 - Someone trying to use the digital file
- Attacker
 - The person trying to break the copy protection
 - Not meant as a pejorative
- Content owner
 - The business entity that owns the copyright on the digital file



Case Study #1: Software Copy Protection

- Since the Apple II, software manufacturers have attempted to prevent “sharing” of software
- Many software and hardware solutions have been implemented
- *All* have been broken by hackers
- Hackers do this for fun; hacked software is called “warez” and is traded
- Bragging rights go to the fastest hack, the cleanest hack, etc.



Case Study #2: Satellite TV Descramblers

- Since the mid-1980s, European satellite TV broadcasters have been at war with hackers
- Every satellite TV scrambling system has been broken
- Satellite TV “black boxes” are in widespread use
- When a new security system is put in place, it is broken within weeks



Case Study #3: CSS

- The DVD industry came up with the “Content Scrambling System” to protect DVDs from being copied
- In November 1999, Linux programmers developed the Windows tool DeCSS, which removed the copy protection
- Their motivation was to write a DVD viewer compatible with Linux, not to pirate DVDs
- The DVD industry has prosecuted some Web sites that link to DeCSS, but it is still easy to find a copy of the utility



Case Study #4: Steven King's eBook

- In March 2000, Steven King released an exclusively electronic book, *Riding the Bullet*
- The e-book was distributed by Glassbook as an encrypted PDF file
- Hacked versions of the book were available within days
- Some of those hacked versions were removed after cease-and-desist letters
- Today it is still possible to download a free copy of *Riding the Bullet*



Cast Study #5: SDMI

- The Secure Digital Music Initiative proposed a series of audio protection schemes
 - Most were based on watermarking
- All were broken within weeks, although the industry denies some of this
- Most breaks were done by students in a short amount of time with limited resources
 - A real break would be easier

Types of Attackers

- The average user
- The power user
- The hacker
- The professional pirate

Defenses Against the Average User

- Almost anything works against the average user
 - Disabling the “copy” button
 - Software that automatically enforces use limitations
 - A big red warning that says “don’t do that”
- The average user can barely install new software, and is terrified of anything different
- The average user will not be able to subvert a security measure



Defenses Against the Power User

- Power users know tricks that defeat weaker schemes:
 - Booting from a floppy
 - Reinstalling software from scratch
- Power users trade tricks amongst themselves:
 - Mailing lists, newsgroups, and Web sites
- A copy protection scheme has to be pretty good to survive a power user



Defenses Against the Hacker

- On a general-purpose computer, nothing works against a dedicated and skilled hacker:
 - Unlock codes, encryption, serial numbers, hardware devices, on-line verification, etc.
 - Copy protection, file encryption, and watermarking
- Secrecy does not work
- It is simply a matter of time
- A completely closed system is much more secure



Defenses Against the Professional Pirate

- This is an adversary who is willing to spend serious money to break the copy protection system
- These people not only clone software, but the manuals and the holograms as well
- These people clone Rolex watches and designer clothing
- No amount of hardware or software countermeasures can beat this guy



Defeating Copy Protection

- Every copy protection scheme ever invented has been defeated
 - It's just a matter of time
- At some point, the copy protection software needs to make a yes/no decision
 - Disable that decision point
- All you can do is disguise the decision point
- There is an underground of hackers who do this for fun, and then trade unprotected software programs



Defeating Digital File Encryption

- At some point, the digital file has to exist in unprotected form in memory
 - Copy the digital file at that point
- If there is a key, at some point that key has to exist inside the CPU
 - Copy the key at that point



Defeating Watermarking

- The idea behind watermarking is to somehow mark a digital file
 - The mark could identify the copyright holder
 - Software could refuse to copy software with a certain digital mark
 - Software could refuse to copy software without a certain digital mark
- Most watermarking schemes have been broken
 - The rest...are still intact because no one good has bothered trying
- This is *much* harder than people think



Traitor Tracing Schemes

- Some schemes attempt to identify the person who originally bought the digital object
 - Aim is to prosecute the person who violated the copyright
- The person who duplicates the file may not be the legitimate owner
- The legitimate owner may not be worth suing
- Many technical problems and privacy issues as well



Hardware vs. Software Security

- Most attacks work because the copy protection software resides on a general-purpose computer
- It is always possible to write software to defeat the copy protection scheme
- On a special-purpose hardware device, this is a much harder problem
 - CD players, DVD players, video game consoles, etc.



Turning a Computer into Specialized Hardware

- Some current proposals involve extending the copy protection to the output device:
 - Computer monitor, speakers, etc.
- This mimics the properties of special-purpose hardware
 - The digital file does not exist in unencrypted form in the computer
- This does not work for executable software, only digital media
- You can always redigitize the analog output



The Current Industry Strategy

- They know that nothing can stop the professional pirate
- They sometimes believe that they can stop the hacker
- Their goal is to make casual copying more difficult than purchasing a second original:
 - Protect their content against the average and power user



Why the Internet Is Different

- To a first approximation, security on the Internet is just like the real world
- There are, however, three major differences:
 - Automation
 - Action at a distance
 - Technique propagation
- These are the other natural laws of digital content



How Automation Affects the Solution

- Automation allows attacks to flow backwards from the more skilled to the less skilled
- A skilled attacker can encapsulate his attack in software
- A skilled attacker can disable the prevention software, and make the digital file available without restriction
- A defense is not good enough if it is secure against the *average* attacker; it must be secure against the *most skilled* attacker



Industry Reaction: Use the Legal System

- The Digital Millennium Copyright Act has made circumventing copy protection schemes illegal
- Content providers have used the courts to go after those who write hacking tools
- Content providers have used the courts to go after those who distribute hacking tools



How Action at a Distance Affects the Solution

- Difficulty of tracing and prosecuting attacker
 - Sometimes you don't know who wrote a particular hacker tool
- Jurisdiction shopping
 - Sometimes, you can't prosecute someone who wrote a hacking tool
 - Some tool Web sites are beyond your legal reach



Industry Reaction: Enlist the World

- Lobby for anti-circumvention laws in as many countries as possible
- Try to make U.S. laws apply to the world
- This is very difficult:
 - There are 192 countries in the world, and nearly all of them are connected to the Internet



How Technique Propagation Affects the Solution

- Tools spread on hacker newsgroups, bulletin boards, mailing lists
- Only the first needs skill; the rest can use software
- Security schemes are necessarily *fragile*



Industry Reaction: Broaden the Counterattack

- Transfer liabilities to third parties
- Make it illegal to download programs that circumvent copy protection technologies
- Require all digital content to be registered
- Make unprotected recording and playback equipment illegal
- These are not all happening right now, but are inevitable next steps in this process.



The End Result: Failure

- All digital copy protection schemes can be broken; it's simply a matter of when someone skilled enough gets around to it
- Automatic software tools to facilitate this breaking will be generally available, it's simply a matter of searching for them
- Pirated digital content will be available, it's simply a matter of indexing it
- Eventually, average users will have access.

Real Solutions?

- Don't fight the natural laws of digital content
- Don't try to fundamentally change how computer networks work
- Look for business models that work on the Internet

Historical Examples

- Advertiser funding
 - Television and radio
 - Commercials or product placement
- Government funding
 - National Endowment for the Arts
- Public funding
 - Civic art projects, community theater, public television
- Patronage
 - Theater, opera, symphony, public television

Historical Examples (cont.)

- Charge for timeliness
 - Stock data
- Charge for relationship
 - Tech support
- Charge for ancillary paperwork
 - CDs, records, some software
- Charge for interaction
 - Give away tapes, sell performances
 - Give away performances, sell consulting

The Street Performer Protocol

- “Electronic Commerce and the Street Performer Protocol,” J. Kelsey and B. Schneier, *The Third USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1998
- Provide a vehicle to aggregate patronage funding for creative works
- Work is made available for free once a threshold is achieved
- Works better for established artists than unknowns, but so do the conventional product marketing systems

- Commerce in the real world is based on the scarcity model:
 - Produce copies of something and charge for the each copy
- This model goes against the natural laws of digital content
 - Enforcement of this model leads to failure
- Smarter business models are based on the unlimited distribution model
 - Charge for the action or the relationship, not for copies of bits

- Copyright can survive this, just as it has survived the VCR, the photocopy machine, computers, etc.
- The world will not end, although some existing business models might



Two Useful Resources from Bruce Schneier

Secrets and Lies: Digital Security in a Networked World
John Wiley & Sons, 2000

<http://www.counterpane.com/sandl.html>

Crypto-Gram

free monthly e-mail newsletter

<http://www.counterpane.com/crypto-gram.html>



Counterpane™
Internet Security

www.counterpane.com

3031 Tisch Way, 100 Plaza East
San Jose, CA. P:408.260.7500 F:408.556.0889

Counterpane™ is a registered trademark of Counterpane.
© Copyright Counterpane Internet Security. All rights reserved.