RSA CONFERENCE 2007

Copy Protection Wars: Analyzing Retro and Modern Schemes

Nate Lawson
Cryptography Research, Inc.

Hackers & Threats II (1450)
February 6th, 2007

Which copy protection era are you?

Disk drive…?

2006

1996

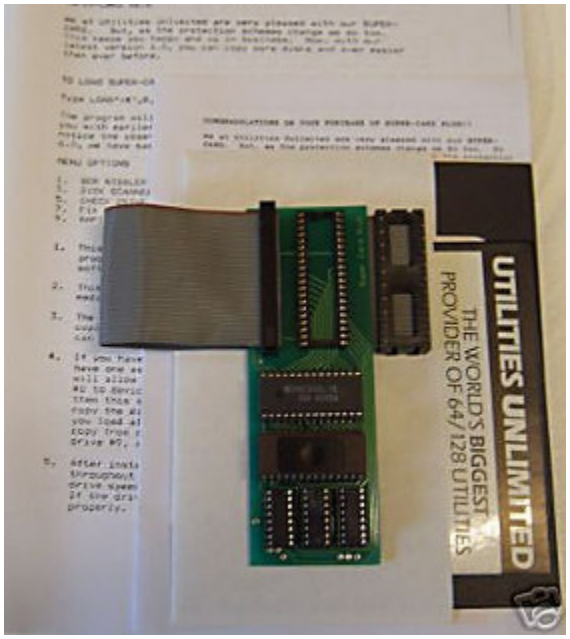
1986

Which copy protection era are you?

Modchip…?

2006
(Xbox360)

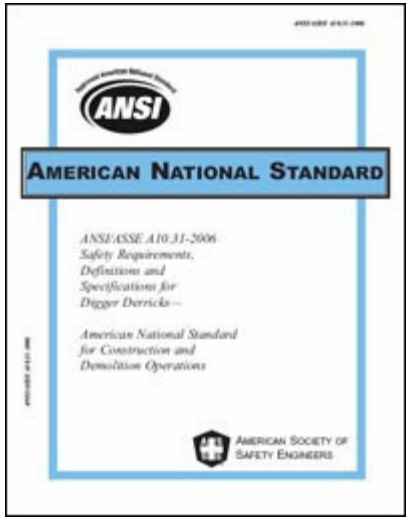
1996
(Sony PS1)



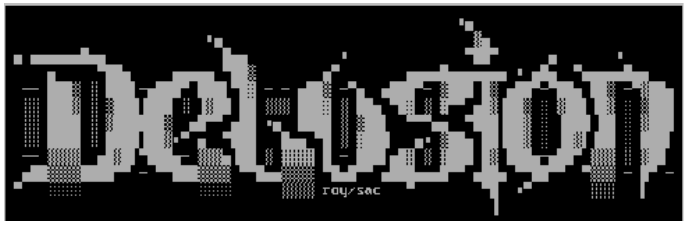
1986
(Commodore 1541 floppy)

Which copy protection era are you?

ANSI…?



2006



1996

1986

Which copy protection era are you?

Monitor…?

2006

1996

1986

Who am I?

- Co-designer of the Blu-ray disc content protection layer (Cryptography Research)
- Designer of ISS RealSecure network intrusion detection system
- FreeBSD committer since 2002
  - Author/maintainer of power management and ACPI kernel code, SCSI and USB
- Contributor to C64 Preservation Project
  - Software for imaging original floppies and replicating copy protection schemes bit-for-bit

Why does the past matter?

- Approaches are still the same as for C64
  - Killer tracks = LaserLock CD/DVD protection
  - Track-to-track alignment = Xbox1/360 sector skew checks
  - Custom GCR encoding = ECC tricks, weak sectors
- Many modern hackers linked to C64 scene
  - commodore4eva: Xbox360 drive firmware hacks
  - Michael Steil: Xbox1 MIST PCI hack

=

?

Legal support for retro-hacking

- Excluded from DMCA anti-circumvention clause
  - Library of Congress ruling (every 3 years)
- Copyright protection still applies so you must have original media
- Seek legal advice before circumventing any protection
  - I'm not your lawyer!

Exemptions:

2. Computer programs and video games distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive.

http://www.copyright.gov/1201/docs/2006_statement.html

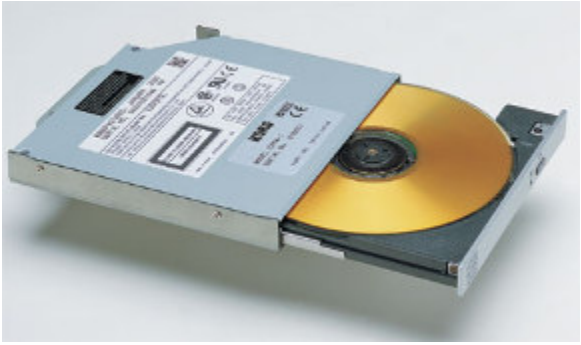
Definition: asymmetry

- Asymmetry
  - Property where forward operation is cheaper than reverse
  - Example:

Definition: copy protection

- Copy protection
  - Leveraging asymmetry between production and playback environment to increase *cost* of copying
  - If cost of copying > profit of copying, vendor wins!
    - Note: almost no systems meet this criteria

vs.



Definition: defender advantage

- Defender advantage
  - As first mover, defender sets the rules of the game
  - But defender must use advantage properly!

Asymmetry used for copy protection

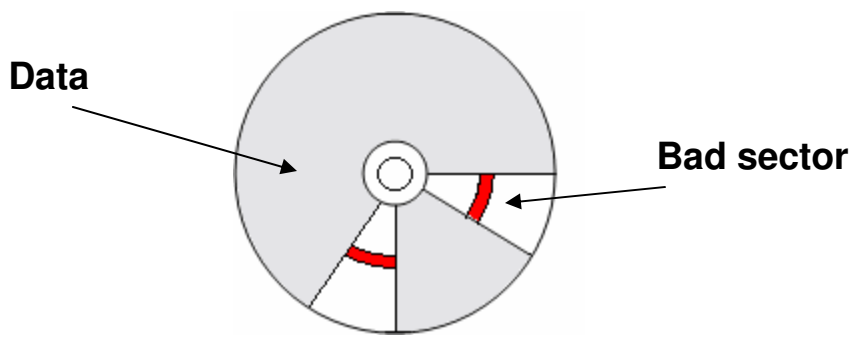
- Physical media
  - **Meta-data**: production equipment can create patterns on media user equipment cannot
  - **Cost**: pressing discs cheaper than burning recordable media
- Software
  - **Obscurity**: executing code easier than understanding it
  - **Self-checks**: creating integrity checks easier than finding them all
  - **Environment**: real hw/sw have behavior different from patched or emulated hw/sw
- Crypto
  - Encrypting data with a key easier than decrypting without it
    - Caveat: key is always somewhere in hw/sw attacker controls

Time for a remedial history lesson…

C64 Protection Methods

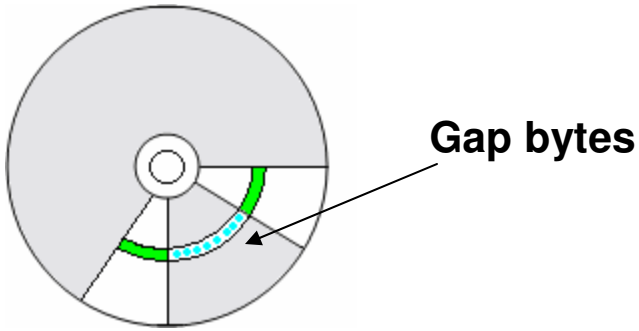
History: sector errors

- Checking sector errors (1983)
  - Asymmetry: firmware in drive cannot create sectors with errors
  - Protection: create bad sectors during mastering and check for them
  - Attack: create custom drive routine to detect and replicate error
- Modern use
  - Multi-session CD with TOC containing errors
  - Sony PS1/Suncomm/CactusShield/key2audio (“sharpie” hack)



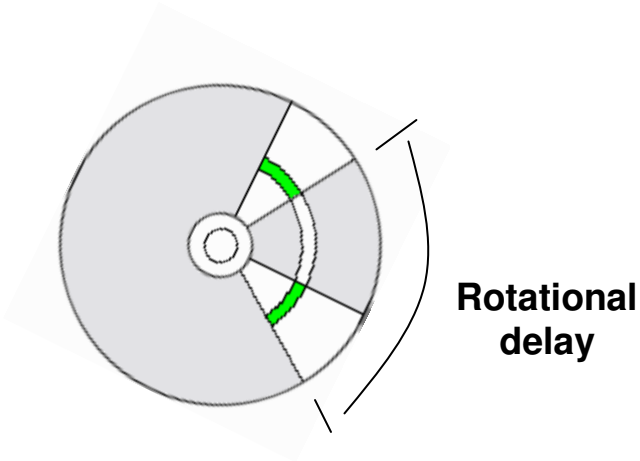
History: gap bytes

- Checking gap bytes (1985)
  - Asymmetry
    - Drive head requires time to switch from reading to writing
    - Drive finds where it is by reading header data
  - Protection: store pattern in gap between sectors and check for it
  - Attack: solder on more drive RAM or parallel cable so entire track can be written at once
- Modern use
  - Store key in sub-channel data that is used to decrypt exe (SafeDisc)



History: track alignment

- Track-to-track alignment (1986)
  - Asymmetry: “soft sector” locator method means overall physical layout unknown
  - Protection: seek from track to track and immediately check first data found
  - Attack
    - Write entire track at once (addl. RAM or parallel cable)
    - Custom drive routine to recreate alignment of original
- Modern use
  - CD Cops PC game protection
  - Xbox1/360 security sector alignment



Who watches the watcher?

- If you were listening, you said…
  - "All the above schemes can be subverted if code not intact."
- Self-checks, obfuscation, crypto, environment checks…
  - Would be another whole talk
  - Asymmetries
    - Difficult for human to understand arbitrary code
    - Protection can occur anywhere within the code
    - Nearly all methods of observing/modifying code execution cause observable side effects
      - Profound impact on detecting modern virtualization techniques

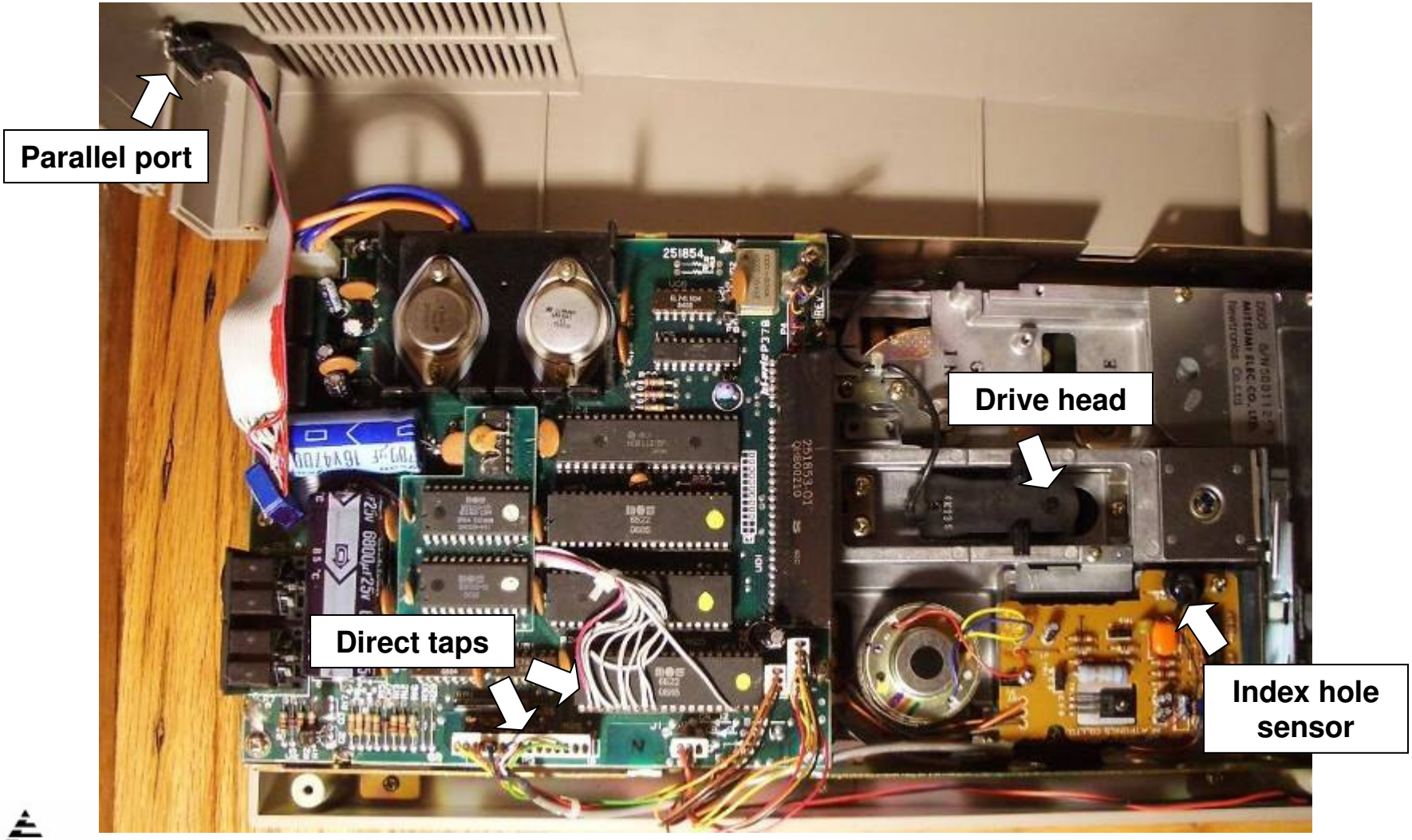
And now the main event…

C64 vs. Xbox 360

C64 drive interface

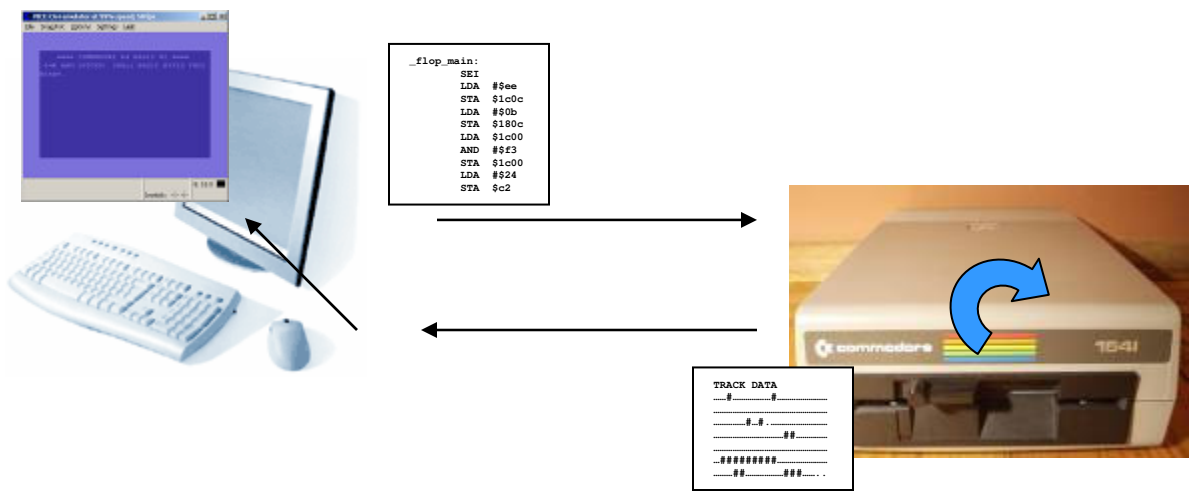
- Serial I/O port provides command/response channel
- Parallel I/O port added to tap data directly

C64 drive interface



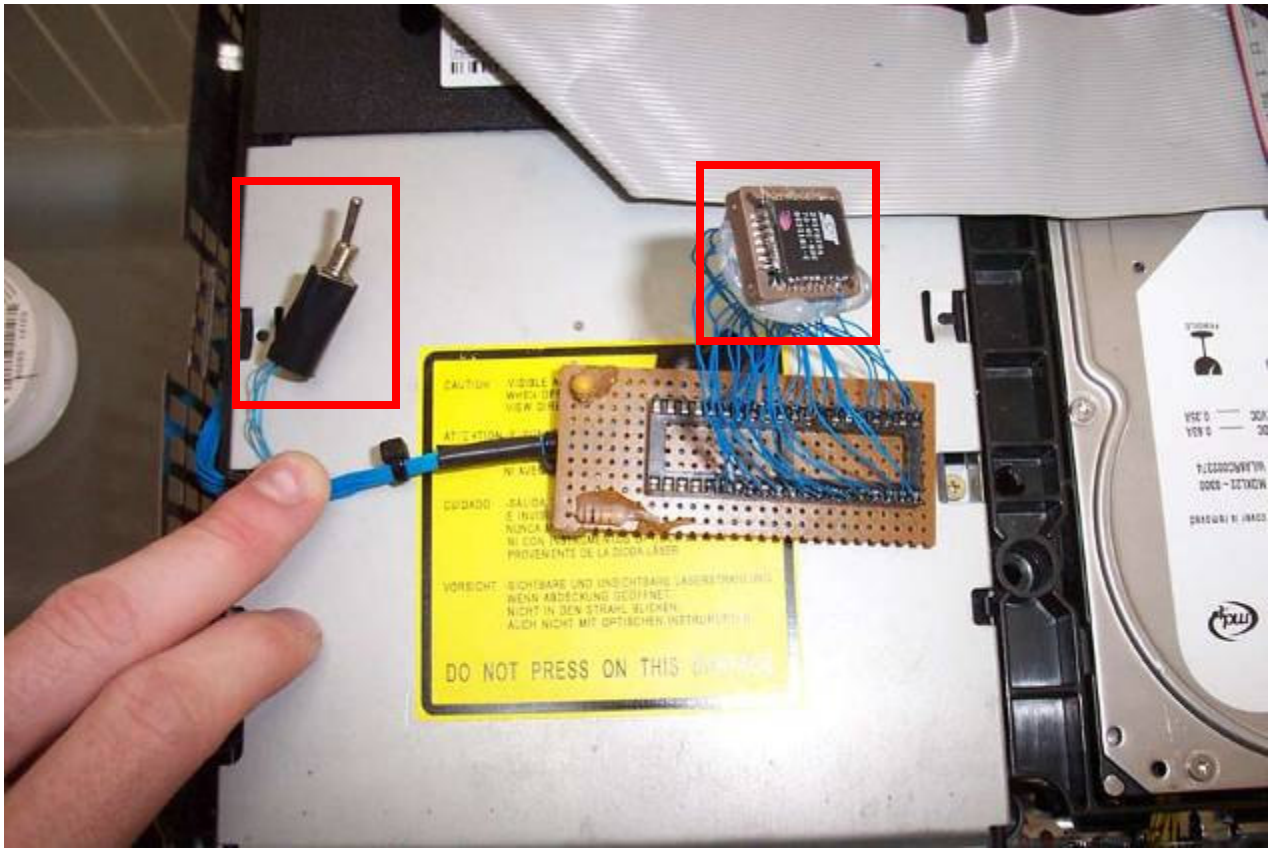
Demo: C64 disk imaging process

- PC writes to drive RAM directly via serial port
- Custom code reads raw track data
- PC scans raw bytes from parallel port
- PC loads disk image into emulator for analysis



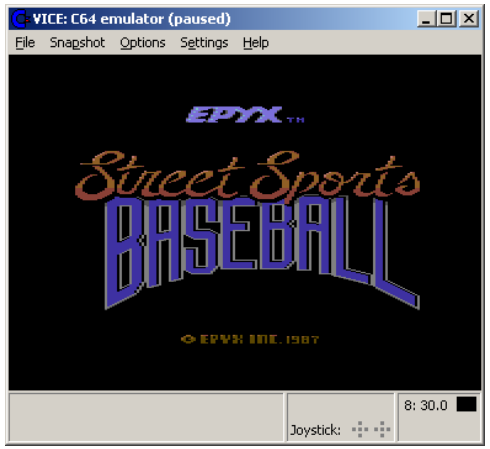
Xbox360 drive hardware hack

- Desolder flash chip and dump/replace using socket
- Disassemble firmware (MN103 microcontroller)



Demo: cracking C64 disk in emulator

- Disk image fails to boot in emulator
- Watch command channel in emulated drive
- Identify protection sequence in drive
  - Vorpal (Epyx): checks gap bytes
- Subvert protection check by patching drive RAM



Xbox 360 drive software hack

- Unlocking drive (mode B)
  - Send a sequence of ATA commands
  - Ground pin on SATA connector while powering up
- Accessing firmware
  - Read/write a few bytes in drive RAM using cmd 0xE7
  - Upload and execute custom trampoline code
  - Read/write entire drive RAM using custom code

```
// Hitachi read memory command (Kevin East - 7thSon)
cgc.cmd[0] = 0xE7;
cgc.cmd[1] = 0x48;
cgc.cmd[2] = 0x49;
cgc.cmd[3] = 0x54;
cgc.cmd[4] = 0x01;
cgc.cmd[6] = (unsigned char)((addr & 0xFF000000) >> 24);
cgc.cmd[7] = (unsigned char)((addr & 0x00FF0000) >> 16);
cgc.cmd[8] = (unsigned char)((addr & 0x0000FF00) >> 8);
cgc.cmd[9] = (unsigned char)(addr & 0x000000FF);
```

Xbox 360
Security Analysis

Xbox 360 status

- Drive totally compromised
  - Fully custom firmware in use
  - Copies run from DVD-R media
- Host completely uncompromised
  - No Linux, user-created games, etc.
  - All crypto keys and kernel code still secret
- Current hacks good enough to support copied games
  - Attacker winning this battle
- Much still unknown about overall security
  - Advantage: defender, but how well will they use this?

Challenge/response scheme

1. Drive reads security sector from lead-out
2. Drive sends encrypted data to host
3. Host decrypts table
4. Host chooses various challenges and sends to drive
   - Type 0: static value from DRT table
   - Type 1, 3: measurements of length of security sectors
   - Type 5, 7: skew between sector locations on disc
   - Type E0: account of all previous challenges seen
5. Drive calculates response and replies
6. Host checks if response matches value decrypted from table

Challenge/response attack analysis

- Security sector stored in lead-out
  - Asymmetry: stock firmware won't read this data for the user
  - Attack: read drive memory after it reads lead-out
- C/R table is encrypted
  - Asymmetry: only Xbox has key to decrypt table
  - Attack: none yet, but table can be sent to host without decrypting
- Responses to challenges derived from physical media
  - Asymmetry: real media has strict physical layout, recorded won't
  - Attack: query drive from PC while real media in drive, replay values from patched firmware

Repairing the hole

- Attackers only have a tenuous hold on drive and no host compromise
- Examining asymmetries gives new defenses
  - Asymmetry: real media analysis will be slightly different each time
    - Defense: check that responses vary appropriately between challenges of the same type
  - Asymmetry: patched firmware can't disable loader methods
    - Defense: use same debug commands to load disc-specific hashing code into drive, check for patched firmware
  - Asymmetry: response table must be somewhere on copied media
    - Defense: look for SS.bin file via host or code loading into drive

Conclusion

- Asymmetry is a useful concept for analyzing schemes
  - Defender only has to increase cost of attack enough (effort/$) to force attackers to look elsewhere
  - Defender starts with inherent advantage but must use it properly
- A lot can be learned from the past
  - Attacks and defenses still same as 1986!
  - Retro-hacking is fun, cheap, and informative

Copies of the slides or comments?

Nate Lawson
nate@root.org
http://root.org/