Some Practical Thoughts Concerning Active Disk Antiforensics

By

Travis Goodspeed

Presented At

The Digital Forensic Research Conference

DFRWS 2014 USA Denver, CO (Aug 3rd - 6th)

Some Practical Thoughts Concerning Active Disk Antiforensics and Other Entertaining Stories

Travis Goodspeed

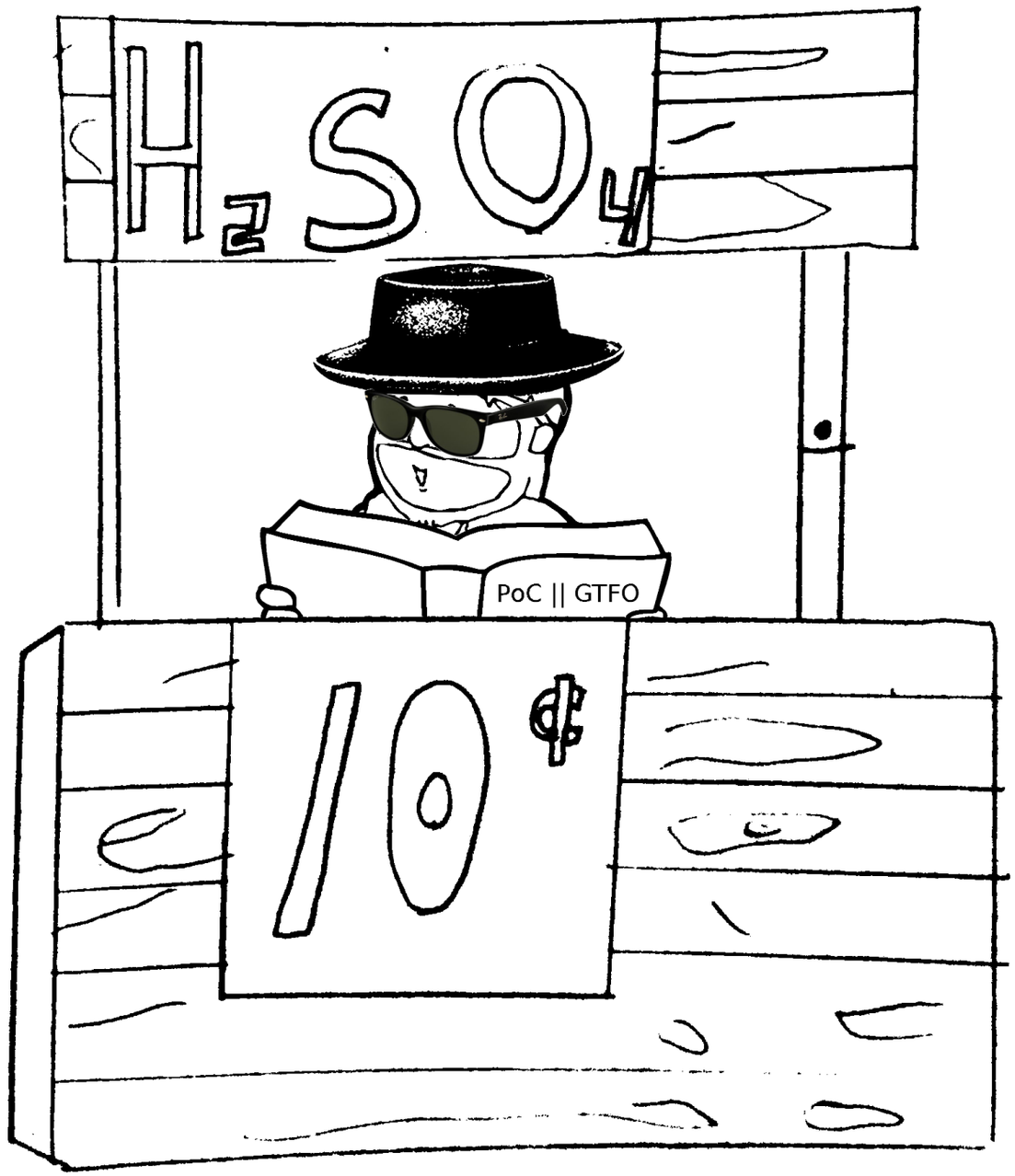
DFRWS 2014 USA
Denver, Colorado

Good Morning!

Good Morning!

- I hate keynotes.
  - Except those by FX and Dan Geer.
- I love Proofs of Concept.
  - Short, nifty tricks.
  - No grand theories, no unnecessary tables.

Did you know that you can just start a journal?



Did you know that you can just start a journal?

- A neighbor and I started a journal.
- No peer review, just a benevolent dictatorship.
    - Pastor Manul Laphroaig, Amateur Tyrant

International Journal of PoC || GTFO
Issue 0x00, a CFP with PoC

An epistle from the desk of Rt. Revd. Pastor Manul Laphroaig
pastor@phrack.org

August 5, 2013

Proceedings of the Society of PoC || GTFO
Issue 0x01, an Epistle to the 10th H2HC in São Paulo

From the writing desk, not the raven, of Rt. Revd. Preacherman Pastor Manul Laphroaig
pastor@phrack.org

Children's Bible Coloring Book of PoC || GTFO
Issue 0x02, an Epistle to the 30th CCC Congress in Hamburg

Composed by the Rt. Revd. Pastor Manul Laphroaig to put pwnage before politics.
pastor@phrack.org

December 28, 2013

AN ADDRESS
to the
SECRET SOCIETY
of
POC || GTFO
concerning
THE GOSPEL OF THE WEIRD MACHINES
and also
THE SMASHING OF IDOLS TO BITS AND BYTES
by the Rt. Revd. Dr.
PASTOR MANUL LAPHROAIG

pastor@phrack.org

TRACT
de la
SOCIÉTÉ SECRÈTE
de
POC || GTFO
sur
L'EVANGILE DES MACHINES ETRANGES
et autres
SUJETS TECHNIQUES
par le prédicateur

PASTEUR MANUL LAPHROAIG

pastor@phrack.org

PoC || GTFO;

addressed to the

INHABITANTS

of

EARTH

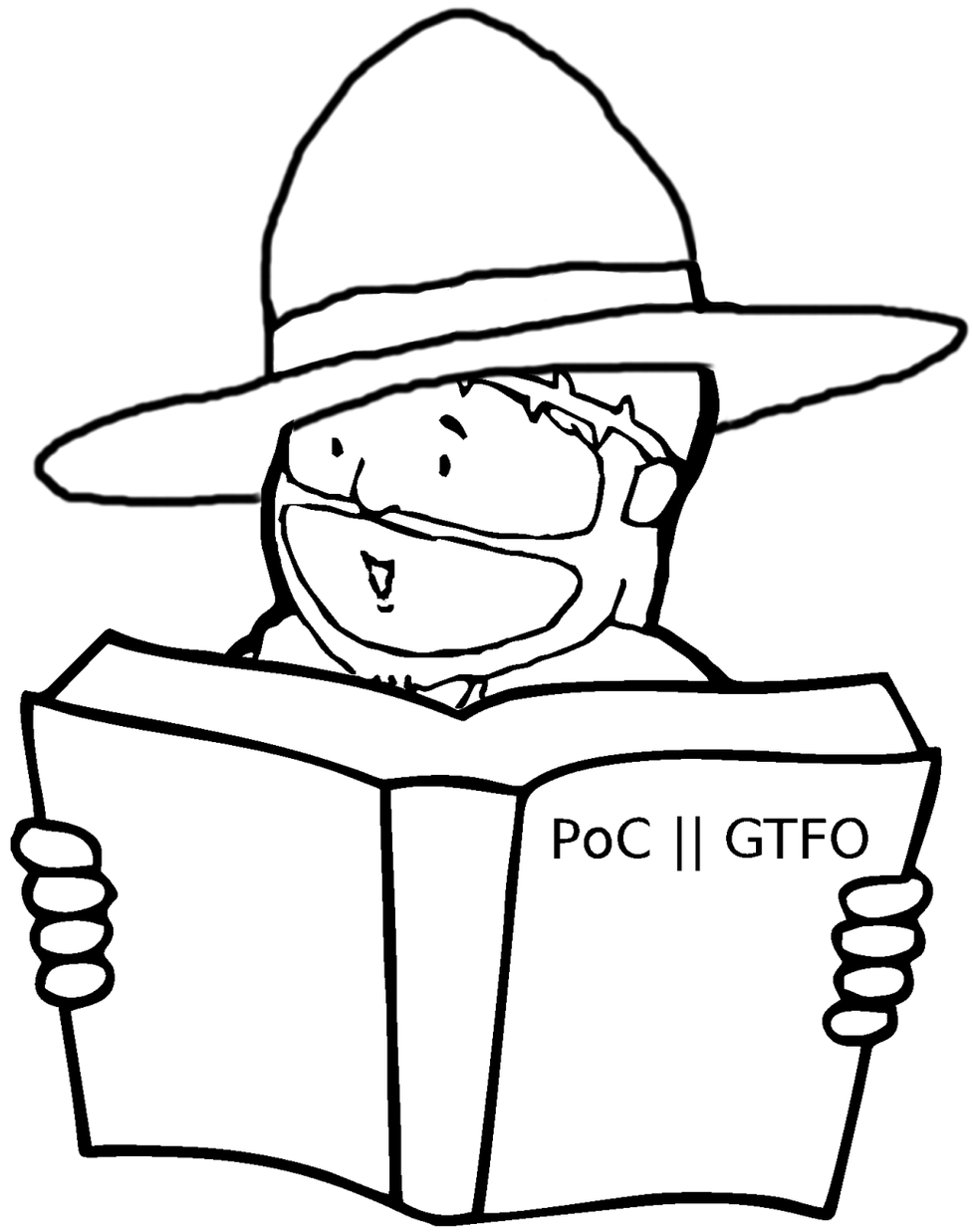
on the following and other

INTERESTING SUBJECTS

written for the edification of

ALL GOOD NEIGHBORS

Let’s hear some stories!



Proofs of Concept are

Proofs by Construction

Active Disk Antiforensics
PoC||GTFO 0:2

Active Disk Antiforensics

- You think of a disk as a block device.
    - Blocks are written, then read back intact.
    - Sometimes they are damaged.
- A disk is really a server.
    - Host makes requests by SCSI or ATA.
    - Software in the disk responds.


Demotivation.us
novate.ru


novate.ru

iPod is a Computer

- Low-end ARM with hardware MP3 decoding.
- Custom operating systems
  - iPod Linux, Rockbox
- Disk Mode is implemented in software.
  - C code translates USB Mass Storage to ATA.

iPod is a Computer

iPod Disk Layout

- First sector is MBR.
- Then comes the iPod Firmware.
- Finally, there is a FAT32 or HFS+ partition for music.

iPod Disk Layout

This is *NEVER* legitimately read by the host!

- First sector is MBR.
- Then comes the iPod Firmware.
- Finally, there is a FAT32 or HFS+ partition for music.

Fingerprinting a Host OS

- Windows
  Reads the Master Boot Record (MBR) 9 times.

- FreeBSD
  Speaks some antique SCSI requests.

- OpenBSD
  Doesn’t delay on SCSI errors.

- Linux
  Varies by automounter.

Fingerprinting Disk Imaging

- tar -cf mnt.tar /mnt
  Follows the filesystem structures,
  never reading empty space,
  or deleted files, or orphaned inodes.

- dd if=/dev/sdc of=forensics.img
  This reads from the beginning to the end,
  in order, as large blocks, without reading ahead,
  and without following filesystem or partition structs.

So let's make a trap!

- Pick an unused sector early in the disk.
- The sector must be one that is *NEVER* read.
- If this sector is read anyways,
  - Erase all future sectors.
  - Reply with legitimate-looking garbage.

Disk Imaging my iPod

```
//These sectors are for 2048-byte sectors.
//Multiply by 4 for devices with 512-byte sectors.
if(cur_cmd.sector>=10000 && cur_cmd.sector<48000)
  tamperdetected=true;
```

Terminal

File Edit View Search Terminal Help

```
0555c000  4e 65 76 65 72 20 67 6f  6e 6e 61 20 6c 65 74 20  |Never gonna let |
0555c010  79 6f 75 20 64 6f 77 6e  2e 00 ff ff ff ff ff ff  |you down.....|
0555c020  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
0556c000  4e 65 76 65 72 20 67 6f  6e 6e 61 20 67 69 76 65  |Never gonna give|
0556c010  20 79 6f 75 20 75 70 2e  00 ff ff ff ff ff ff ff  | you up.....|
0556c020  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
0557a000  4e 65 76 65 72 20 67 6f  6e 6e 61 20 6c 65 74 20  |Never gonna let |
0557a010  79 6f 75 20 64 6f 77 6e  2e 00 ff ff ff ff ff ff  |you down.....|
0557a020  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
0558a000  4e 65 76 65 72 20 67 6f  6e 6e 61 20 67 69 76 65  |Never gonna give|
0558a010  20 79 6f 75 20 75 70 2e  00 ff ff ff ff ff ff ff  | you up.....|
0558a020  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
05598000  4e 65 76 65 72 20 67 6f  6e 6e 61 20 6c 65 74 20  |Never gonna let |
05598010  79 6f 75 20 64 6f 77 6e  2e 00 ff ff ff ff ff ff  |you down.....|
05598020  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
```

Beyond a PoC

- My iPod is well and good as a PoC, but
  - There's a disk recover mode.
  - The disk can be read directly.
  - Who carries an iPod in 2014?
- So let's weaponize this.

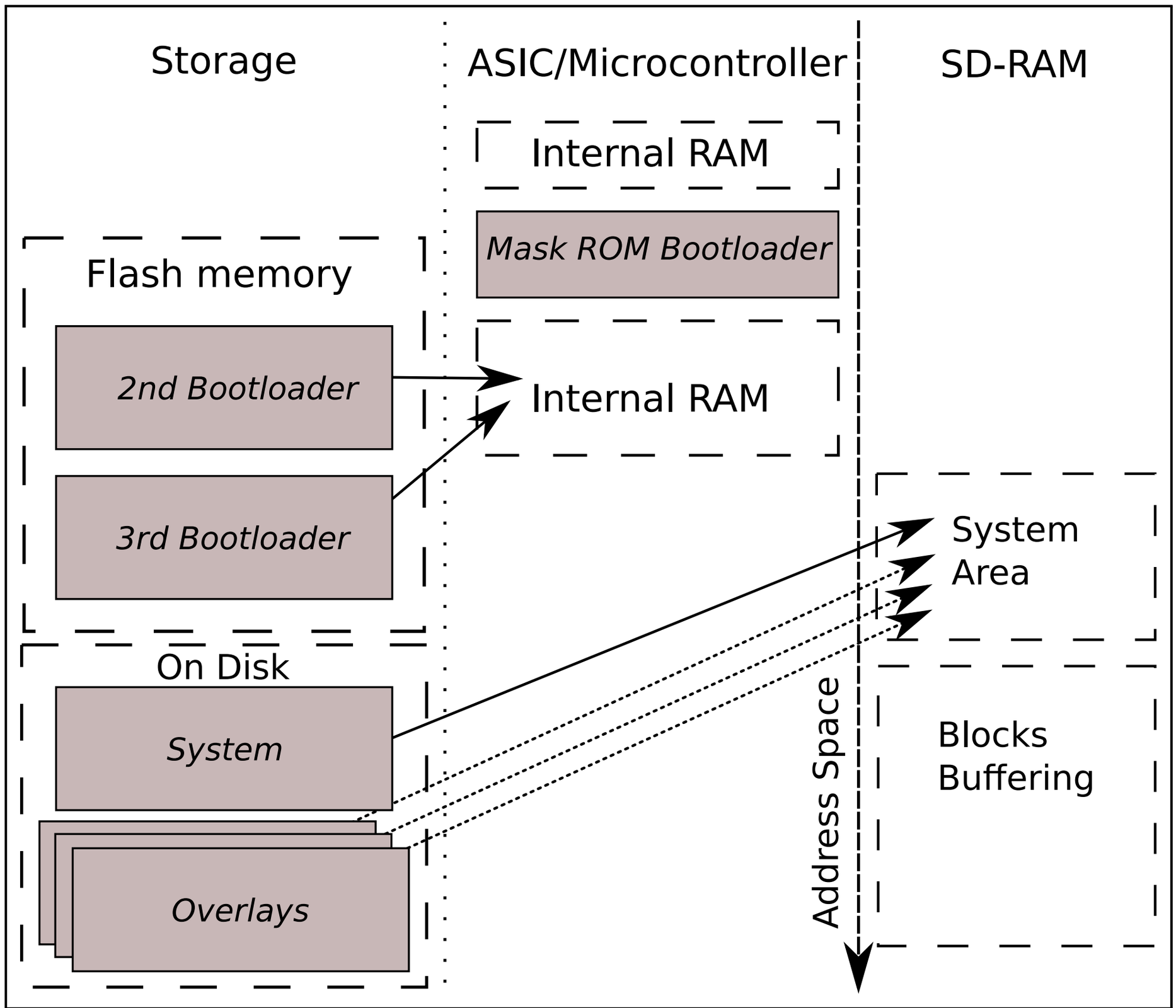
Beyond a PoC

- So let's patch the firmware of a real disk.
- And let's make it more malicious.

Implementation and Implications of a Stealth Hard-Drive Backdoor

Jonas Zaddach[†*] Anil Kurmus[‡*] Davide Balzarotti[†] Erik-Oliver Blass[§] Aurélien Francillon[†]
Travis Goodspeed[¶] Moitrayee Gupta[‖] Ioannis Koltsidas[‡]

Inside a Seagate Disk

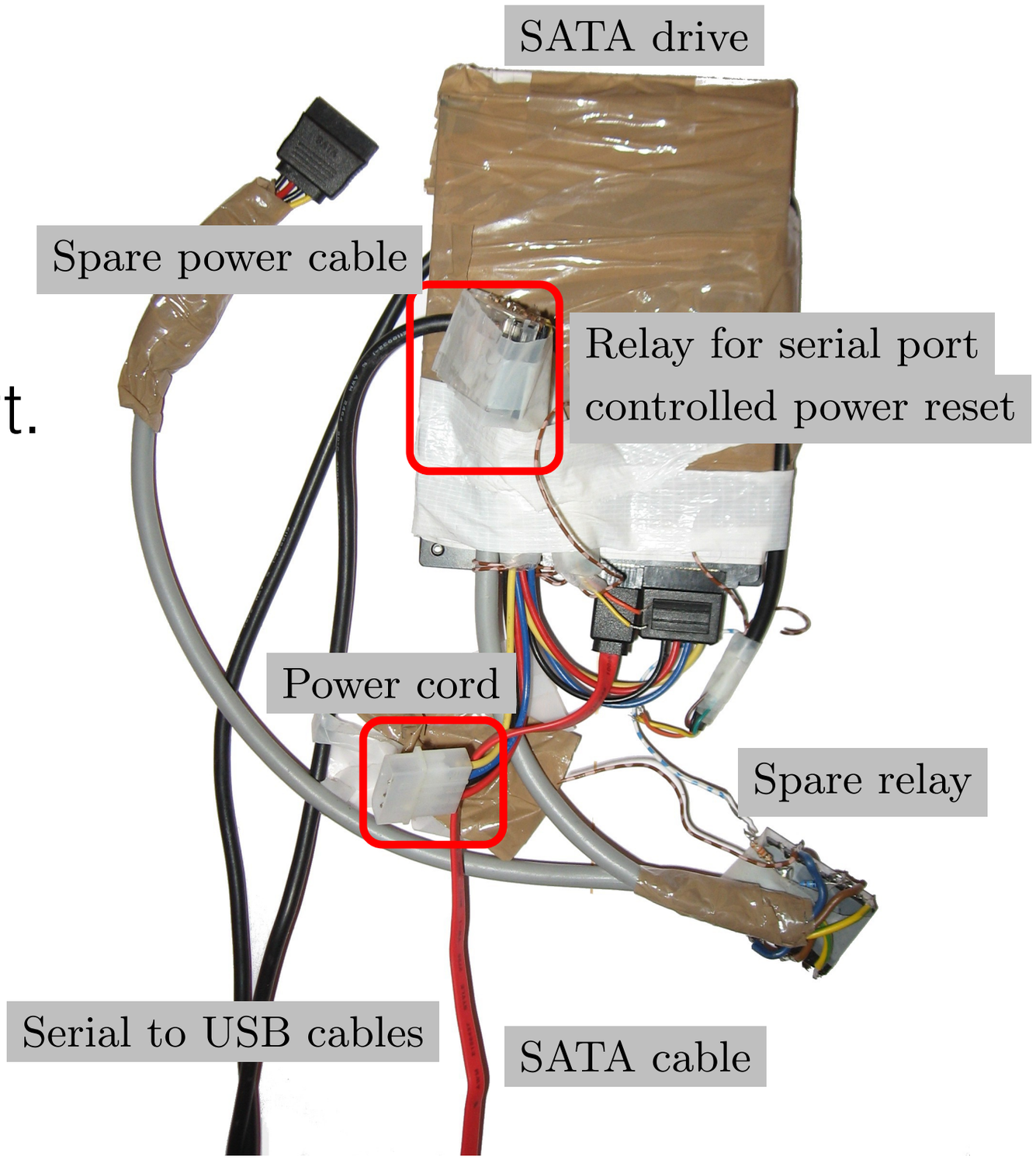


We Needed a Devkit

- Reversing is Hard Work
  - 10 man-months for this project.
    - Lots of mistaken assumptions, instabilities.
- Debuggers are great!
  - But Seagate kills JTAG. :(

We Needed a Devkit

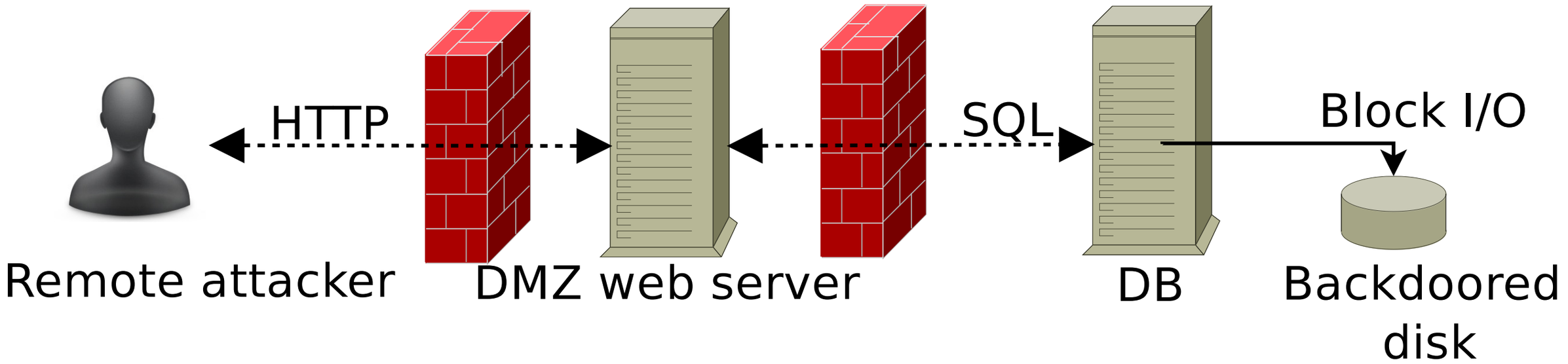
- GDB Stub is easy to port.
  - UART as comms.
- Need external reboots.



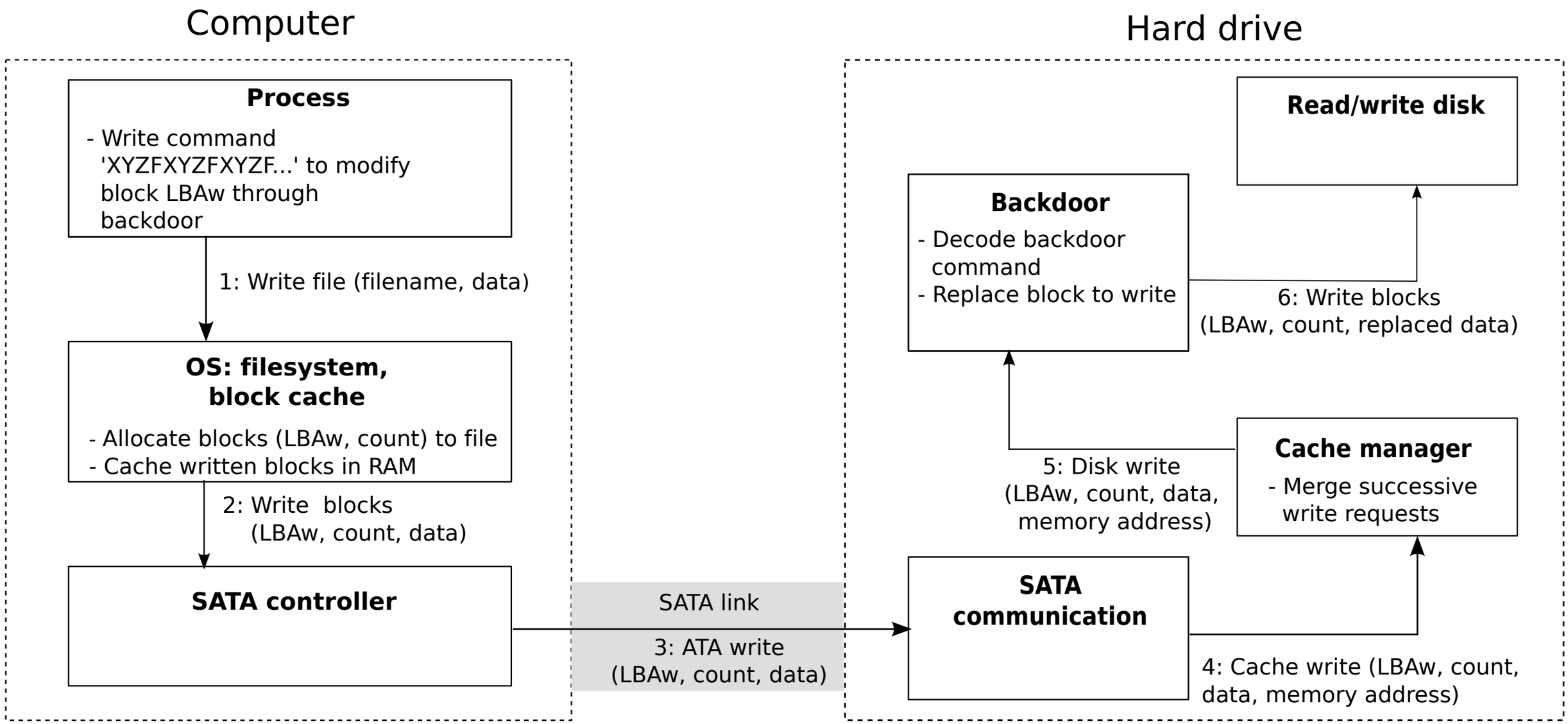
Better than Antiforensics

- Not only can I fingerprint the host, but
  I can also do a discrete, remote comms channel.
  - HTML5 Local Storage
  - Cookies
  - SQL Database Contents

Backdoored Disk



Discrete Comms Channel



End Result

- Attacker can remotely mount Defender's disk.
- There is no malware running on the X86 CPU.
- Installation takes seconds.

Other Platforms

- Sprites Mods on Western Digital Disks
  - Uses JTAG instead of GDB Stub
    - Begins to boot Linux on the disk!
- Flowswitch Tools for Phison Firmware
  - Python scripts for Thumbdrive Firmware

So how do we catch this?

- Single, Known Implementation
  - Exploit a bug!
- Multiple, Unknown Implementations
  - Read chips from the raw?
  - How much of a backlog would you like?

Reading Chips in the Raw

- Lots of labwork.

- Which devices do you spend extra time on?

So how do we catch this?

Go now in peace.

- Read your scripture.
  - PoC||GTFO, Phrack, conference proceedings!
- Preach the good news!
  - Conference talks, soap box.
  - ``Hey, want to learn a cool trick?''

Credits

- Unpublished Experiments with Dan Kaminsky
- Antiforensics iPod, PoC||GTFO 0:2
    - Travis Goodspeed
- Implementation and Implications of a Stealth Hard-Drive Backdoor, ACSAC 2013
    - Zaddach, Kurmus, Balzarotti, Blas, Francillon, Goodspeed, Gupta, Koltsidas
- International Journal of PoC||GTFO