AFAUC – anti-forensics of storage devices by alternative use of communication channels

Harald Baier, Julian Knauer

Hochschule Darmstadt, CASED

IMF, 2014-05-12

Harald Baier

1. Doctoral degree from TU Darmstadt in the area of elliptic curve cryptography.
2. Principal Investigator within Center for Advanced Security Research Darmstadt (CASED)
3. Establishment of forensic courses within Hochschule Darmstadt.
4. Current working fields:
   - IT forensics.
   - Anomaly detection in high-traffic environments.
   - Security protocols for eMRTD.

Motivation

Foundations

General methodology

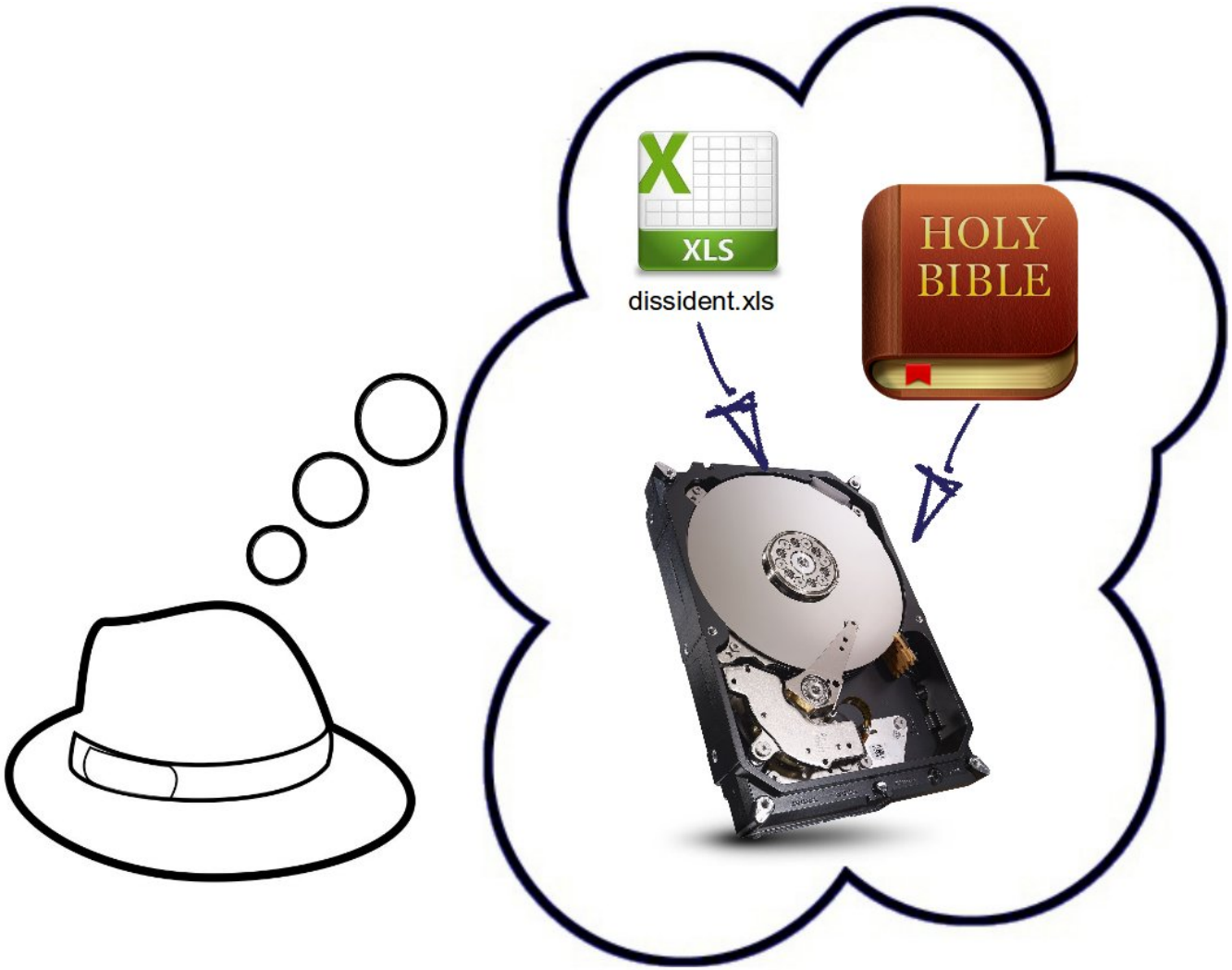
Sample access and reconfiguration

Evaluation

Conclusion and future work

Motivation

Use case: hide information in oppressive countries



Use case: detect dark activities

Key question: where to hide data?

1. Location of hidden data:
   - Inspire yourself by well-known anti-forensic approaches.
2. Access channel:
   - Usual one as expected.
   - Usual one in an unexpected way.
   - Alternative channel.

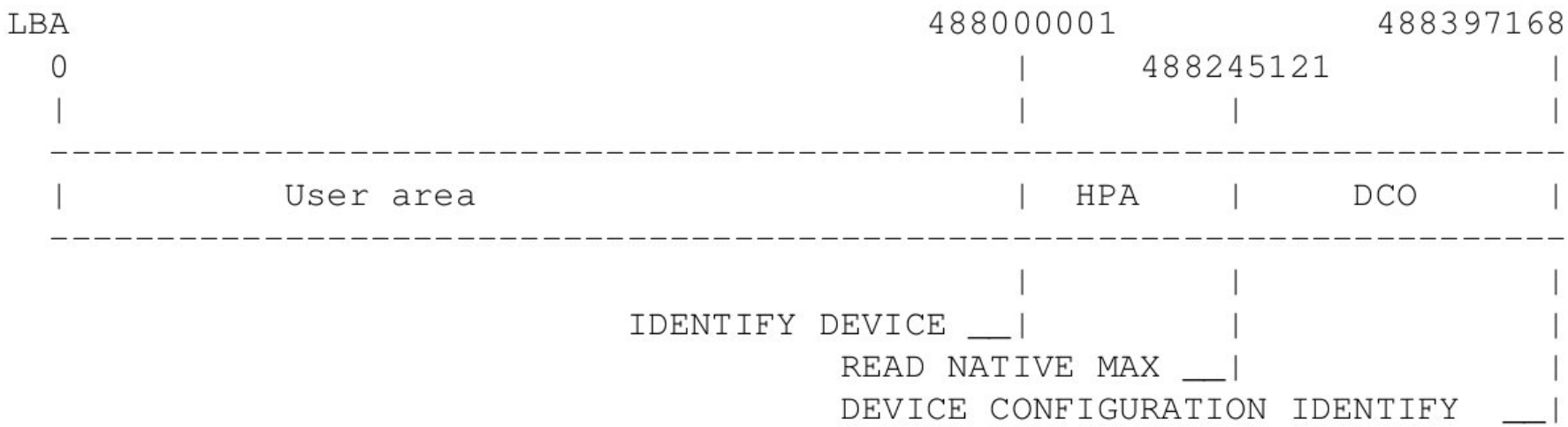
General anti forensic measures

1. Obfuscation techniques to prevent investigators to access content of data, e.g.,
   - Encryption.
   - Packers.
2. Hide data somewhere on the disc, e.g.,
   - Steganography.
   - Non-partioned area.
   - Slack space of the file system.
   - Journals.
   - Inode area of an extX file system.
   - ATA-standardised disc areas like HPA or DCO.

HPA and DCO

- HPA = Host/Hidden Protected Area
  - At the 'end' of the disc.
  - Not accessible using ordinary OS commands.
  - Possible aims: installation/recovery software of manufacturers including boot sector.
  - Detectable by boot messages, `hdparm` or using `disk_stat` from TSK.
- DCO = Device Configuration Overlay
  - Located 'behind' HPA.
  - Configure parameters of the disc including its native size.
  - Possible aim: the device looks smaller than it actually is (e.g., because a distributor sells 600 GiB HDDs instead of 1 TiB HDDs).

Sample disc layout



1. Three different maximum Logical Block Addresses (LBA):
   - `lastUserLBA` $= 488,000,000$ (set by `SET MAX ADDRESS`)
   - `nativeMaxLBA` $= 488,245,120$ (set by `DEVICE CONFIGURATION SET`)
   - `realMaxLBA` $= 488,397,168$ (invariant (?))

Identifying HPA using hdparm

```
$ hdparm -N /dev/sda
     /dev/sda:
        max sectors = 488000001/488245121, HPA is enabled
```

```
$ man hdparm
[REMOVED]
 -N      Get/set  max  visible  number of sectors, also known as the Host
         Protected Area setting.  Without a parameter,  -N  displays  the
         current  setting,  which  is  reported  as two values: the first
         gives the current max sectors setting, and the second shows  the
         native  (real)  hardware  limit  for  the  disk.  The difference
         between these two values indicates how many sectors of the  disk
         are currently hidden from the operating system, in the form of a
         Host Protected Area (HPA).
```

Identifying DCO using hdparm

```
$ hdparm --dco-identify /dev/sda
    /dev/sda:
    DCO Revision: 0x0002
    The following features can be selectively disabled via DCO:
        Transfer modes:
             udma0 udma1 udma2 udma3 udma4 udma5 udma6
        Real max sectors: 488397168
        ATA command/feature sets:
    [REMOVED]
```

```
$ man hdparm
[REMOVED]
--dco-identify
       Query and dump information regarding drive configuration set-
       tings which can be disabled by the vendor or OEM installer.
       These settings show capabilities of the drive which might be
       disabled by the vendor for "enhanced compatibility". When dis-
       abled, they are otherwise hidden and will not show in the -I
       identify output.
```

Knowledge about HPA / DCO

1. Knowledge about the existence of an HPA or a DCO is not widespread under computer scientists.
2. However, well-known in the computer forensics community.
   - Part of any investigation.
   - IT forensic guideline from the German Federal Office for Information Security:

     Completeness of the image: Reserved areas of mass storage media (e.g., HPA and DCO) must be detected reliably and deactivated during acquisition to get a complete image.
3. Many tools available to acquire the whole drive until `realMaxLBA`.

Basic idea: special case ATA devices

Create non-standardised data area similar to HPA / DCO.

1. We are inspired by both hidden data areas and side channel attacks from cryptography.
2. Key questions:
   - 2.1 Is it possible to manipulate `realMaxLBA`?
   - 2.2 Is there an alternative interface to the firmware than the ATA one?
   - 2.3 If yes, how to access the maintenance area?

$\Longrightarrow$ AFAUC – anti-forensics of storage devices by alternative use of communication channels

Key steps (1/2)

1. Identify communication channel to access storage device:
   - Further interfaces than bulk data interface?
   - Wired or wireless?
   - Paradigm: 'abuse' it for unintended use.
   - Notation side channel vs. alternative use of a communication channel.
2. Connect to the interface and find out basic communication parameters:
   - Role of pins, voltage.
   - Data structures, baud rate.

Key steps (2/2)

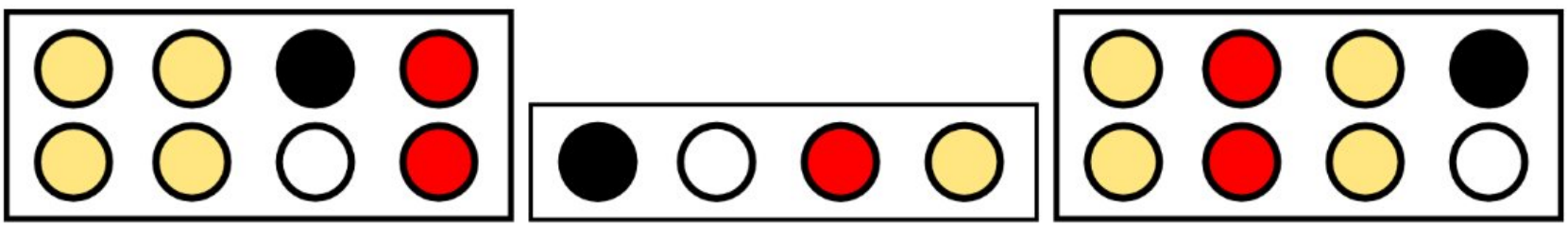
3. After successful connection: reverse engineer interface commands to change configuration.
   - Sample sources: manuals, manufacturer's web site, Internet forums, ...
   - Pitfalls: checksums, backup copies, encryption.
4. Adapt non-digital information, e.g., HDD identification plate.
5. Self-evaluate your manipulation using common IT forensic tools.

AFAUC is dual use

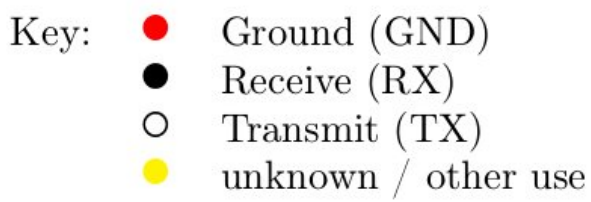
Our sample disc

Diagnostic interface

1. Manufacturers use it for maintenance:
   - Hardly documented.
   - Provides serial interface to the Micro Controller Unit (MCU) of the HDD.
2. Sample layouts:

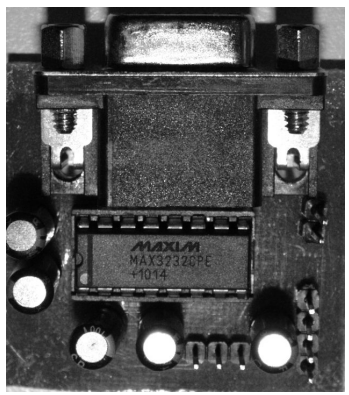


(a) Seagate PATA (b) Seagate SATA (c) Samsung SATA

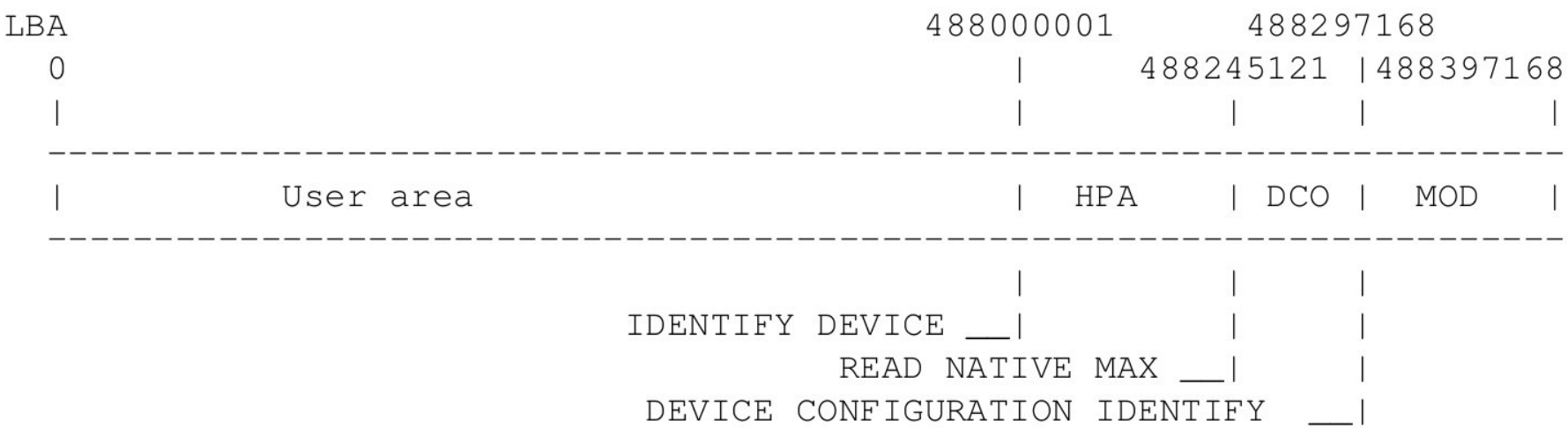


Our host environment

1. An 'old' PC providing a serial interface :-).
2. Linux, `hdparm`.
3. `minicom` as terminal emulator.
4. RS232 transceiver



Favoured modified disc layout



1. Keep `lastUserLBA` and `nativeMaxLBA` unaltered.
2. `realMaxLBA` $\leftarrow$ `realMaxLBA` $-100,000$.

Relevant Samsung diagnostic commands

Command	Parameter	Description
`RM`	ModuleIndex	Read Module: reads the module with ModuleIndex from the service area into the device memory.
`MW`	Offset DataWord [DataWord...]	Memory Write: modify the contents of the memory by writing one or multiple DataWord beginning at Offset.
`WM`	ModuleIndex	Write Module: writes the memory buffer back to the service area as module ModuleIndex.

CONFIG module before manipulation

```
ENG> RM 6
W:005B00 434F 4E46 4947 2020 0000 0000 0000 0004
W:005B08 0000 0001 0002 0003 0000 0001 0002 0003
W:005B10 3FFF 0010 003F 5970 1D1C 0000 0000 0000
W:005B18 2459 005B 65B4 01D2 7242 0349 7D93 04BE
[...]
```

1. 434F 4E46 4947 2020 == CONFIG__
2. We search for realMaxLBA:

$$488397168 = 0x1D1C5970$$

CONFIG module before manipulation

```
ENG> RM 6
W:005B00 434F 4E46 4947 2020 0000 0000 0000 0004
W:005B08 0000 0001 0002 0003 0000 0001 0002 0003
W:005B10 3FFF 0010 003F 5970 1D1C 0000 0000 0000
W:005B18 2459 005B 65B4 01D2 7242 0349 7D93 04BE
[...]
```

1. `434F 4E46 4947 2020` == `CONFIG__`
2. `realMaxLBA` at offset `W:005B13`:

$$488397168 = 0x1D1C5970$$

Modification of the CONFIG module

1. Determine modified realMaxLBA:

$$488297168 = 0x1D1AD2D0$$

2. Translate it to little-endian words D2D0 and 1D1A.
3. Write two words at offset W:005B13:

   MW 5B13 D2D01D1A

4. Make the changes permanent:

   WM 6.

Evaluation

Evaluation tools and persons

1. Different tools:
   - `dd`.
   - `hdparm`.
   - ACE Laboratory PC-3000 UDMA suite.
   - Tableau TD1 Forensic Duplicator.
2. Two IT forensic departments to apply their *common* process modell to acquire the HDD dump:
   - Law enforcement.
   - IT forensic department of an audit firm.
3. Only consider digital information, e.g., do not process HDD label.

Basic functional tests: Preparation

- Disable HPA and DCO.
- Write a file of length 512 bytes into the final HDD block.
- File contains the ASCII control pattern

  Do you detect our AFAUC anti-forensic approach?
- Modify `CONFIG` module of the HDD as described before.

Basic functional tests

1. HDD dump using `dd`:
   - Acquire disc data: `dd if=/dev/sda of=dump.dd`
   - Control pattern not found in dump `dump.dd`.
2. Read out `realMaxLBA` using `hdparm`:

```
$ hdparm --dco-identify /dev/sda
    /dev/sda:
    [REMOVED]
        Real max sectors: 488297168
    [REMOVED]
```

Evaluation using PC-3000 UDMA

1. German law enforcement agency.
2. PC-3000 connects to S-ATA interface of the HDD.
3. Hidden data partition is **not** revealed.
4. However, PC-3000 can access 3 backup copies of the modules: all backup copies contain the original `realMaxLBA`.

Evaluation using TD1

Performed by a German IT forensic department.

Conclusion and future work

Take home messages

1. Always keep anti-forensic measures in mind.
2. Be aware of alternative use of interfaces.
3. Skilled people can generate hidden HDD partitions 'for free'.
4. AFAUC is dual use.

Future work

1. Terminology: side channel vs. interface for unintended use vs. interface for alternative use
2. Manipulation of backup copies of the modules.
3. Reverse engineer non-standardised ATA commands as used by manufacturers and PC-3000.
4. Wireless interfaces (e.g., SD card).

Conclusion and future work

Questions?

Source: www.dilbert.com/strips/