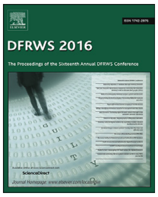
Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin



Forensic limbo: Towards subverting hard disk firmware bootkits

Michael Gruhn

Department of Computer Science, Friedrich-Alexander University of Erlangen-Nuremberg, Martensstr. 3, 91058 Erlangen, Germany

ARTICLE INFO

Article history:
Received 17 July 2016
Received in revised form
19 August 2017
Accepted 10 October 2017
Available online xxx

Keywords:
Anti-forensics
Hard disk firmware rootkit
Hard disk firmware bootkit

ABSTRACT

We discuss the problem posed by malicious hard disk firmware towards forensic data acquisition. To this end, we analyzed the Western Digital WD3200AAKX model series (16 different drives) in depth and outline methods for detection and subversion of current state of the art bootkits possibly located in these particular hard disks' EEPROMs. We further extend our analysis to a total of 23 different hard drive models (16 HDDs and 7 SSDs) from 10 different vendors and provide a theoretical discussion on how hard disk rootkits residing in the firmware overlays and/or modules stored in the special storage area on a HDD called the Service Area could be detected. To this end, we outline the various debug interfacing possibilities of the various hard disk drives and how they can be used to perform a live analysis of the hard disk controller, such as dumping its memory over JTAG or UART, or how to access the Service Area via vendor specific commands over SATA.

Introduction

In digital forensics data is analyzed. In order to analyze data, it must, however, first be acquired. Because many times forensic investigations, of, e.g., industrial espionage, involve rootkit compromises, this paper addresses persistent data acquisition from potentially rootkit subverted hard drives. This is a task that has not been addressed by the current state of the art in forensic hard drive forensics. Current literature on hard drive forensics always recommends making a copy of the original source drive, while using a write blocker to prevent changes to the original source drive. The current state of the art also recommends the acquisition of the usually hidden HPA and DCO sections. For a non-compromised hard drive, those measures work fine. However, they are not enough to ensure that evidence is not destroyed, lost or never found when the analyzed hard drive has been compromised by a firmware rootkit.

Hence, in this paper, we first give a short overview of what effect a firmware rootkit can have on an investigation. We then demonstrate how firmware bootkits can be detected and we outline several possibilities how even deep firmware rootkits can be detected. We will use a Western Digital WD3200AAKX as running example throughout this paper.

HDD anatomy

A modern HDD is not just a block device but rather a whole computer system in itself. The symbolic picture in Fig. 1 on the following page shows the anatomy of a hard disk drive (HDD). It is loosely based on the Western Digital WD3200AAKX drive. The picture shows the HDD and selected components in the middle. The components are: the disk, also known as the platter; the read and write head; and the PCB containing the processor, RAM, EEPROM, etc. The figure further points out three topics of interest: persistent storage areas, interfacing possibilities, and anti-forensic threats. These are detailed in the next two sections. The first section outlines the persistent storage areas and their associated anti-forensic threats. The second section outlines the interfacing and verification possibilities.

Persistent storage areas and anti-forensic threats

While the main purpose of a HDD is to provide persistent storage, the HDD itself has also storage areas it can use, which may not be accessible by a normal user of the HDD. The following areas are pointed out in Fig. 1 on the next page:

Mask ROM. The mask ROM is integrated into the processor on the HDD's PCB. Because it is programmed by the integrated circuit manufacturer during the manufacturing process directly via the photo*mask* in the photolithography process, it is read-only and can not be modified. It contains code that allows the processor to

E-mail address: michael.gruhn@cs.fau.de.

https://doi.org/10.1016/j.diin.2017.10.003
1742-2876/© 2017 Elsevier Ltd. All rights reserved.

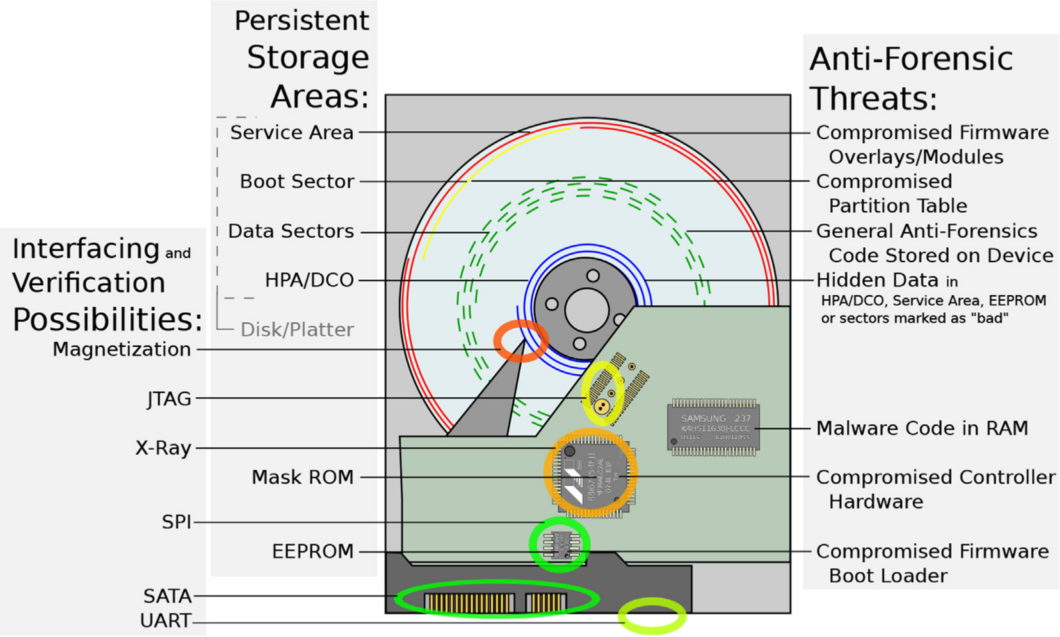

Persistent Storage Areas:
Service Area
Boot Sector
Data Sectors
HPA/DCO
Disk/Platter
Mask ROM
EEPROM
Interfacing and Verification Possibilities:
Magnetization
JTAG
X-Ray
SPI
SATA
UART
Anti-Forensic Threats:
Compromised Firmware Overlays/Modules
Compromised Partition Table
General Anti-Forensics Code Stored on Device
Hidden Data in HPA/DCO, Service Area, EEPROM or sectors marked as "bad"
Malware Code in RAM
Compromised Controller Hardware
Compromised Firmware Boot Loader

Fig. 1. HDD anatomy: storage areas, interfacing possibilities and anti-forensic threats.

boot and load the firmware boot loader code from the EEPROM into RAM.

EEPROM. The EEPROM contains the boot loader of the firmware. The boot loader bootstraps the system to the point where it can read from the platter. At this point, it will start loading more firmware from the platter. The EEPROM can also be read and written by software via the HDDs SATA connection. This way firmware code can be modified, e.g., to perform legitimate firmware upgrades. This results in the anti-forensic threats associated with a compromised firmware boot loader, also known as a bootkit. It is important to note that this firmware bootkit does not interfere with the boot process of the operating system installed on the HDD, but rather the boot process of the HDD itself. Besides compromising the firmware, the EEPROM could be used as hidden data storage.

Service Area. The Service Area is a hidden area on the platter that, unlike the HPA or DCO, can not be used by a normal user. This area is used to store further firmware components called overlays or modules, which are loaded into RAM by the boot loader. On some HDD's some overlays are only loaded on demand and swap other overlays out of RAM. While this area is reserved for usage by the firmware, there are vendor specific commands (VSCs) with which this area can be accessed via the SATA interface. This allows an attacker to modify firmware as well as hide data. After the Service Area begins the regular storage area of the HDD platter — often known as the User Area. However, in Fig. 1 we additionally point out different aspects of the User Area, because these different sections of the User Area can be used in different ways to facilitate anti-forensics. But to the hard drive, the User Area is treated as one single storage area.

Boot sector. The Boot Sector is the first thing loaded by a BIOS when booting from the HDD. Because a professional forensic investigator will not boot from the device, any malware infections, such as bootkits in the boot sector, will not immediately impact his work, unless, of course, the malware is the subject of his investigation.

The Boot Sector usually also contains the partition table, which can be malicious. In CVE-2016-5011, we have shown that it is possible to cause a denial of service (DoS) against various Linux systems with a specially crafted DOS/MBR partition table, that uses an extend partition loop (Wundram et al., 2013), i.e., an extended partition within the DOS/MBR partition table will point back to the DOS/MBR itself causing infinite recursion in the library libblkid when parsing the partition table. Another such example uses GPT partitioning. It can cause a DoS against Windows 7 by setting the number of partition table entries to zero in the GPT header, which will result in the so-called Blue Screen of Death due to an implementation error which causes a division by zero within the kernel. So even by merely connecting a HDD with such a compromised partition table to a vulnerable system can impact the forensic investigator's work negatively.

Data sectors. The Data Sectors are all sectors that a regular user of the HDD has access to. This is where, e.g., the file system resides, the files within it, etc. Regular anti-forensic measures, typically, reside here, e.g., directory loop attacks (Wundram et al., 2013) or XSS code injection into forensic reports that are generated as HTML files (Wundram et al., 2013).

HPA/DCO. Last but not least the HDD can contain the so-called Host Protected Area (HPA) and/or a Device Configuration Overlay (DCO). Both are hidden from the user. The HPA can be used to store installation files used for system recovery, while the DCO can be used to control over-provisioning of the HDD. Access to both the HPA and DCO can be acquired via ATA commands (Gupta et al., 2006). Both areas are well known to forensic investigators, hence, they lost their value as data hiding spot for criminals.

Interfacing and verification possibilities

Fig. 1 also shows the various interfacing and verification possibilities we found provided by the analyzed hard drives. We will outline most of them in more detail throughout this paper. Hence, here we only give a brief outline of each.

Magnetization. The first idea to verify the data on the HDD platter seems to be to read the magnetization directly from the platter. While this may have worked on older hard disk drives, newer disk

Please cite this article in press as: Gruhn, M., Forensic limbo: Towards subverting hard disk firmware bootkits, Digital Investigation (2017), https://doi.org/10.1016/j.diin.2017.10.003