J Comput Virol
DOI 10.1007/s11416-010-0149-x

ORIGINAL PAPER

Malware and steganography in hard disk firmware

Iain Sutherland · Gareth Davies · Andrew Blyth

Received: 20 December 2009 / Accepted: 22 November 2010

Abstract The hard disk drive remains the most commonly used form of storage media in both commercial and domestic computer systems. These drives can contain a vast range of data both of personal value and commercial significance. This paper focuses on two key areas; the potential for the drive operation to be impacted by malicious software and the possibility for the drive firmware to be manipulated to enable a form of steganography. Hard drive firmware is required for the correct operation of the disk drive in particular for dealing with errors arising due to natural wear as the drive ages. Where an area of the drive becomes unreliable due to wear and tear, the disk firmware which monitors the reliability of data access will copy the data from the failing area to a specially designated reserved area. The firmware remaps this data shift so the old data area and the original copy of the data are no longer accessible by the computer operating system. There are now a small number of commercially available devices, intended for data recovery, which can be used to modify the hard drive firmware components. This functionality can be used to conceal code on the disk drive, either as a form of steganography or to potentially include malicious code with the intention to infect or damage software or possibly system hardware. This paper discusses the potential problem generated by firmware being manipulated for malicious purposes.

I. Sutherland (✉) · G. Davies · A. Blyth
Faculty of Advanced Technology,
University of Glamorgan, CF37 1DL Wales, UK
e-mail: isutherl@glam.ac.uk

G. Davies
e-mail: gddavies@glam.ac.uk

A. Blyth
e-mail: ajcblyth@glam.ac.uk

1 Introduction

The most common form of storage media used in both the commercial and domestic environment is the hard disk drive. It is therefore unsurprising that this form of media forms a significant part of digital investigations. There are numerous papers discussing best practice in the collection and preservation of evidence from these devices. Most national police forces maintain a digital forensics capacity to address evidence of this nature e.g. *Institut de recherche criminelle de la gendarmerie nationale (IRCGN)* in France [1]. There are also a number of best practice procedures for law enforcement, an example from the UK is the Association of Chief Police Officers Guidelines [2]. These guidelines define best practice processes and procedures for the collection and general analysis of digital evidence and are relevant to the processing and analysis of hard disk media. However, in specific cases where a technically competent suspect has access to specific, commercially available hardware and software, there is the potential for the various hard disk drive firmware implementations to be manipulated. This may enable the user to conceal information on the drive and place this data beyond forensic recovery using standard data recovery tools and techniques. It may also enable the drive to be sabotaged by these tools and by possible future forms of malware, prohibiting forensic analysis. An investigator therefore requires some knowledge of the low level functioning of a hard disk and the tools that are available, to manipulate the firmware of a hard disk drive. In this paper we review the key aspects of hard disk drive architecture and design. We discuss the firmware and the functionality that support the normal

Published online: 11 January 2011

operation of the drive including the defect management processes focussed on maintaining drive reliability.

2 The hard disk

A hard disk drive is a complex device providing high volume non-volatile storage. A disk is composed of a number of elements including a voice coil, read / write heads, casing, mountings, a motor and a controller board. There are two commonly used form factors; the 3.5 inch used in desktop systems and 2.5 inch used in laptop computers although other form factors have been developed, one example is the 1 inch drives used in the older Apple iPods. Despite the variation in the form factor, the internal arrangement of the devices is similar; the data area consists of a stack of metal, ceramic or glass platters coated with a magnetic film. The current maximum storage capacity for user data on a disk drive is in the region of 2TB although 4TB versions are likely to be produced in 2011 [3]. Once a drive has been formatted and a file system written to the drive, the typical amount of storage is slightly less.

3 Data storage

Considering a single platter surface, a track can be defined as a rotation of the disk at a particular radius. For sets of surfaces, a set of tracks at the same radius is known as a cylinder. A separate head assembly is located on the armature for each disk surface. During use the position of the read / write heads is determined by location data embedded within the user data area. This location information is written to the drive at the point of manufacture. The sector is the smallest addressable unit on a drive. A specific sector can be located at one level of abstraction using a Logical Block Address (LBA). This method assigns a sequential address to each sector. To locate a sectors physical position on the hard drive this is converted to a physical location by referencing a specific Cylinder (C), Head (H) and Sector (S).

There are areas of the drive that are not available for user data storage, some of these additional regions are addressable by the operating system and are reserved for different purposes. The Host Protected Area (HPA) provides storage for diagnostics and other utilities required by the PC manufacturer [4]. The existence of an HPA can be detected by the difference in values provided by the command READ_NATIVE_MAX_ ADDRESS, which indicates the total number of sectors on the disk the value provided by the IDENTIFY_DEVICE command which provides total sectors a user can access on the drive. A Device Configuration Overlay (DCO) is used by manufacturers to configure drive sizes and may exist in addition to a Host Protected Area [5]. If a DCO is present on the device this can be detected by the difference in values returned from the following two commands; READ_NATIVE_MAX_ADDRESS and DEVICE_CONFIGURATION_IDENTIFY. Carrier [4] provides a comprehensive review of the concepts relating to HPA and DCO.

4 Hard drive firmware functionality

In addition to those areas of a drive not addressable by a user there are also areas of the drive that are not addressable by the host computer's operating system and contain firmware used to control the normal operation of the disk. Manufacturers implement the firmware operations in different ways, however, typically this firmware is located on both the PCB and on the platters of the disk. The initial portion of code located on disk controller PCB, is used to load firmware resident on the drive platters. (See Fig. 1). It should be noted that in some cases in multi-platter drives the firmware may be duplicated across the platters.

The firmware controls the correct internal operation of the hard drive, allowing it to interact with the host computer (i.e. the operating system). During the initial startup the controller board loads the firmware from the disk platters. The firmware then performs a number of checks to ensure correct operation of the drive, the disk then presents itself in a ready state enabling the host computer to load any operating system stored on the disk. When the hard drive is powered down after use, it is the firmware which executes a shutdown sequence to ensure the hard drive powers down correctly to a safe state.

During normal operation, firmware provides a number of functions: SMART Monitoring (Self-Monitoring, Analysis, and Reporting Technology), which monitor a number of manufacturer dependent criteria to ensure the drive is operating within certain parameters. Attributes include, amongst others; read error, seek error, uptime and device temperature. The firmware is also responsible for monitoring defect control. The error management firmware contains a catalogue of defects present at the point of manufacture. These flaws are recorded in the disk firmware. Further flaws are recorded as the drive wears due to use.

Monitoring defect control is an important firmware function. This process is transparently handled by the hard disk and occurs 'beneath' the operating system. Any flaws identified on the drive during production are recorded in the disk firmware as the 'P' (primary, production or permanent) list. As the disk ages and as a result of wear & tear other sectors fail and this is recorded within the firmware area in the 'G' (growth) list [6,7]. Reads and writes are automatically redirected (remapped) to spare sectors within the Reserved Area (see Fig. 2). The sectors recorded in the P-list and G-list are automatically bypassed by the drive electronics.

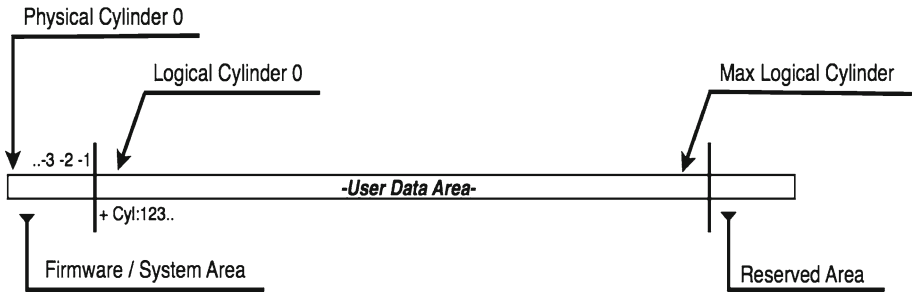

Fig. 1 Data storage locations (single platter)

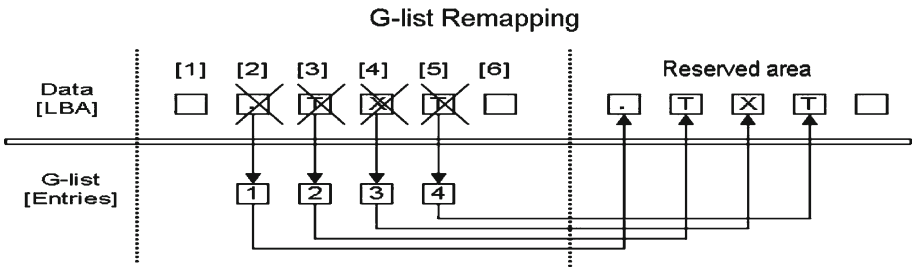

Fig. 2 Data reallocation example

5 Steganography using firmware

One aspect of this paper is the possibility of the defect control system being manipulated to enable data to be concealed on the hard disk drive. This possibility was tested as part of the following experiment: A 3.5" Fujitsu Hard Disk Drive (Model MPA3035AT) was populated with a Windows XP, NTFS file system and a variety of mixed data files commonly located on a hard disk drive. The NTFS file system was selected, as this is one of the most common file systems found on hard disks although it should be noted that in terms of the experiment the file system is not significant. The proposed method of steganography operates 'beneath' the file system and can be applied to any almost data in a physical sector on the drive. A randomly selected text file was chosen and edited to include a distinctive keyword. This was to enable the file to be searched for using standard commercial forensic tools. In the case of an investigation the investigator would have a reasonable expectation to locate this keyword either on the original drive or in a forensically sound copy.

The particular model of the Fujitsu disk selected for this experiment supports two error lists in the firmware; one firmware list relating to production defects and another list relating to failing tracks on the drive. The majority of modern hard disk drives support this particular error handling function in some form. A specialist firmware analysis and repair tool from ACE laboratory [8] was used to access and view the drive contents in order to locate the physical location (sector) for the text file. This tool can modify drive firmware including error lists to effect repairs on malfunctioning drives. The firmware error list on the Fujitsu hard disk drive relating to defective tracks (T-list) was modified using the data recovery tool to include an additional entry in the error list relating to the physical location of the modified text file.

The disk was rebooted and mounted. The Windows Operating System could no longer access the physical location (hidden data area) nor the data residing at that location. The drive firmware system would not permit access to this location and as the remapping process normally associated with a failing sector had not occurred, the data was not accessible. This was also confirmed via external hex editors (Winhex) [9]. What is more, after taking a forensic image of the drive the specific keyword added to the file was not present in any searches performed on the drive using forensic tools. The data was inaccessible by the disk drive and the computer operating system. The data can therefore be concealed on the disk beyond the reach of most commercial digital forensics tools.

The firmware recovery tool was used to edit the error list returning it to its original state removing the previously added entry. The data area and text file containing the keyword was accessible on the drive. It should be noted that due to the error handling functionality being present on the vast majority of modern drives this behaviour would be repeated on most drives to varying degrees in terms of the volume of data that could be contained in these sectors.

6 Malicious modificaton of firmware

The use of firmware tools for steganography purposes is fairly straightforward as outlined in the section above. A malicious user with a higher level of technical competency may be able to modify firmware to embed malware on the drive to prevent the correct operation of the drive.

Disk firmware provides low level control of the drive. During a forensic invesigation or when configuring a secure system it is trusted and assumed to be operating correctly when supplied from the manufacturer. Malware engineered to target hard disk firmware could in theory prevent access to the data contained on the drive even with sophisticated data recovery tools and donor parts. This could be due to the malware targeting disk specific critical subsystems contained in the firmware, damaging the drive logically, in certain cases beyond repair. There may also be a number of possible ways to damage the drive by either preventing firmware from operating normally or by modifying it to compromise the drives operation. Possible methods include disabling SMART systems, corrupting physical to logical translation tables, altering the current to the read/write heads to damage the circuitry or more difficult, but more destructive, would be to reduce the motor speed abruptly to destroy the air bearing causing a head crash and damage to the disk platter. This kind of exploit would be developed and targeted at particular disks and systems and would act as a sophisticated method of sabotage that could render the drive contents irrecoverable.

7 Forensic impact

Currently there are limited number tools available tools to perform repair or modifications on firmware. The available free/shareware tools available to access usually disk model/serial number [10]. The commercially available tools provide a finer degree of control, and access to a broader set of the disks features. There are currently two main systems available for data recovery and firmware modification and repair. A complete suit for UDMA is supplied from ACE Laboratories in Russia and costs approximately $10,000 for the UDMA toolset although a more comprehensive tool suite with the ability to extract data and work with some solid-state devices is available. An alternative device is offered from China (Salvation Data) [11] and can be obtained via resellers in Europe for approximately $450 per disk manufacturer. Either of these tools would enable a competent user to manipulate firmware to conceal data or code.

Firmware manipulation can have a significant impact on the forensic process. Data that has been hidden using firmware steganography techniques will not appear for analysis in a traditional forensic image. In the event of malware targeting and corrupting the firmware, this can potentially prevent the acquisition of a forensic image from the hard disk drive. In the case of determining if the disk firmware has been tampered with or modified, the investigator would need to establish the provenance of the firmware. This is a challenging process, as the firmware implementation not only varies between manufacturers but also between the various models of the disk drives. There are also portions of code unique to individual disk drives.

Detecting this form of misuse is potentially difficult. The investigator would need to evaluate the drive against a comparable disk and perhaps use key firmware modules, from the donor drive to verify the firmware is valid or to use donor hardware components to repair the original drive. This would however leave the problem of the error lists, which are unique to the drive although it is possible to clear some of the error lists present on the drive whilst still retaining user data. The major problem lies in the ability to obtain and verify the error lists. The error lists and certain portions of the data contained in the firmware / system area are unique and disk model specific and therefore cannot be compared to another version of the disk.

8 Forensic best practice

These types of malicious techniques have the potential to impact upon forensic best practice and information security. The possibility of firmware modification emphasises the importance of retaining the original hard disk drive. It can be argued that the analysis of firmware for evidence of tampering is not appropriate in most investigations. This is due to the fact it is difficult and timing consuming (and therefore expensive) it would be unwarranted in most cases. Rather the investigator would need to consider the possibility of firmware tampering if there is evidence to suggest this may have occurred. This may be indicated by a combination of the suspect's technical expertise, the presence of certain hardware and software tools at the scene and suspected incomplete or missing evidential material. Where there are grounds for suspecting that a suspect may have modified drive firmware, then there are a number of actions proposed as best practice in this type of case that have been suggested by the authors [12].

9 Summary and conclusions

We have highlighted the concern that there is a potential for data to be concealed in a drive by manipulating the drive firmware. There is also the possibility for firmware to be modified for malicious purposes. There are a number of potential problems relating to the forensic analysis of malicious hard disk firmware modification. Even with the correct tools it can be very difficult to find or reverse this type of modification. Hardware and software costs supporting this type of analysis are significant. The correct training is not widely available and is expensive. While this remains unlikely to impact the vast majority of forensic cases, the increasing availability of the data recovery tools used to carry out this work makes it a possible area for future concern.

10 Future work

This paper has focused on highlighting the concern that firmware can be manipulated either to conceal data on the drive or to disrupt the drives correct operation. Future work will consist of a number of avenues: Assessing some of the potential routes for the introduction and execution of malware intended to disrupt firmware. Determining forensically sound best practice to detect modification to disk firmware.

Acknowledgments The authors would like to thank the members of the Information Security Research Group (IRSG) in particular Mr Nick Pringle.

References

1. Gendarmerie Nationale.: http://www.gendarmerie.interieur.gouv.fr. Accessed 10 April 2010
2. ACPO: Association of Chief Police Officers Good Practice Guide for Computer based Electronic Evidence, Version 4.0. http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf. Accessed 9 April 2010 (2008)
3. Hitachi Website.: http://www.hitachi.com/New/cnews/071015a.html. Accessed 12 April 2010
4. Carrier, B.: Forensic File System Analysis. Addison Wesley, Reading (2005)
5. Gupta, M.R., Hoeschele, M.D., Marcus, K., Rogers, M.K.: Hidden disk areas: HPA and DCO. Int. J. Digit. Evidence, Fall 2006, vol. **5**, Issue 1 (2006)
6. Blyth, A.J.C., Sutherland, I, Pringle, N.: Tools and techniques for steganography and data insertion onto computer hard-drives. In: 8th Annual Program Manager's Anti-Tamper Workshop. Sponsored by US DoD Anti-Tamper Executive Agent SAF/AQL and Department of the Army, Redstone Arsenal, Huntsville (2008)
7. Sutherland, I., Davies, G., Pringle, P., Blyth, A.J.C.: The impact of hard disk firmware steganography on computer forensics. In: The 2009 ADFSL Conference on Digital Forensics, Security and Law, May 20–22, Champlain College, Burlington (2009)
8. Ace Laboratories Website.: http://www.acelaboratory.com. Accessed 14 October 2010
9. Winhex Website.: http://www.winhex.com/winhex. Accessed 14 October 2010
10. Browsedata: HDD firmware serial number source code 1.01 free download. http://www.softlow.com/windows/development-tools/debugging/shareware/hdd-firmware-serial-number-source-code.html. Accessed 11 March 2009 (2004)
11. Salvationdata Website.: http://www.salvationdata.com. Accessed 14 October 2010
12. Davies, G., Sutherland, I.: Hard disk storage: firmware manipulation and forensic impact and current best practice. The 2010 ADFSL Conference on Digital Forensics, Security and Law, May 19–21, 2010, St. Paul (2010)