Manipulation of hard drive firmware to conceal entire partitions

Huw Read a,b,*, Konstantinos Xynos a, Iain Sutherland a,b,c, Gareth Davies a,c,d,e, Tom Houiellebecq a, Frode Roarson a,b, Andrew Blyth a

a Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd, CF37 1DL, UK
b Noroff University College, Kristiansand, Norway
c Edith Cowan University, Perth, Australia
d Centre for Forensic Computing, Cranfield University, UK
e Longwood Centre for Cyber Security, Longwood University, Virginia, USA

A R T I C L E   I N F O

Article history:
Received 3 December 2012
Received in revised form 14 October 2013
Accepted 17 October 2013

Keywords:
Firmware
Hard drive
Manipulation
Data hiding
Xbox 360
Free space
ACPO

A B S T R A C T

Tools created by the computer hacking community to circumvent security protection on hard drives can have unintentional consequences for digital forensics. Tools originally developed to circumvent Microsoft’s Xbox 360 hard drive protection can be used, independently of the Xbox 360 system, to change the reported size/model of a hard drive enabling criminals to hide data from digital forensic software and hardware. The availability of such concealment methods raises the risk of evidence being overlooked, particularly as triage and on-scene inspections of digital media become more common. This paper presents two case studies demonstrating the process using Western Digital and Fujitsu branded drives. It outlines the difficulties faced by standard computer forensic analysis techniques in revealing the true nature of the drive and finally provides suggestions for extra checks to reveal this type of concealment.

© 2013 Elsevier Ltd. All rights reserved.

1. Introduction

Concealing data in hidden areas of a hard drive is not new; forensic investigators are able to use tools that detect if they are present. However, the emergence of new concealment methods that are not detected by forensic tools increases the risk of evidence being overlooked.

The modification of a hard drive layout to create a hidden volume is part of the recognised ATA standards (Technical Committee T13, 2012). Hard drive manufacturers have been creating partitions to store recovery partitions for years (IBM, 2012). A more advanced form of this method creates a “Host Protected Area” (HPA) using the ATA commands SET MAX ADDRESS and READ NATIVE MAX ADDRESS (Stevens, 2000). The resulting partition is hidden from an operating system to ensure it cannot be accidentally formatted. It is possible to identify the presence of an HPA with standard hard drive tools such as hdparm (Lord, 2012) and advanced recovery solutions such as DeepSpar and PC3000.

Manipulating the size of a storage device has also been attempted for more malicious reasons as been noted by Jitbit (2011). In this case a 128 MB USB stick was modified to appear as a 500 GB hard drive. When files are written to the “drive” and the 128 MB capacity is reached, the write process starts from the beginning of the drive overwriting existing content.
The possibility of manipulating a drive to enable the use of physical areas of a hard drive for steganography is also a concern. In Sutherland et al. (2009), the possibility for the application of steganography to a hard drive’s firmware is discussed. To date, the tools used to modify drive firmware have been of two types: 1) small programs in the form of software updates released by the manufacturers to update specific drives, and 2) larger tools suites, combinations of hardware and software designed for drive repair for data recovery purposes. These specialized data recovery tools (e.g., PC3000 by ACE laboratories and DeepSpar) are capable of modifying a range of different models from various manufacturers. These data recovery tools are expensive, although in recent years increased competition has reduced the prices of specialist equipment and technological advances have lead to improved functionality. These tools tend to require extensive training and detailed knowledge of the internal structure and operation of a hard drive.

One of the concerns highlighted in Sutherland et al. (2009) was that this type of tool would become more prevalent and less expensive. This appears to have been the case with the creation of small open source or freeware applications designed to alter firmware. This is also true of the gaming community where tools have been developed by hackers interested in either modifying or extending the functionality of their consoles. These tools, with supporting websites and online guides, have made basic techniques to modify firmware accessible to the average user (Free60 Project, 2013).

This paper demonstrates the process of altering a hard drive using freely available Xbox 360 hacking tools to hide a partition from detection by forensic software and hardware. Such concealment methods raise the risk of evidence being overlooked, particularly as triage and on-scene inspections of digital media become more common. Furthermore, when a hard drive appears to display the correct make, model and serial number, when examined using forensic tools, digital investigators could be lulled into a false sense of security causing them to overlook hidden data.

The rest of this paper is structured as follows. Section 2 demonstrates how a hard drive is prepared for use in an Xbox 360, Section 3 presents two case studies which demonstrate how partitions may be hidden to conceal data, Section 4 provides a review of techniques attempted to identify the hidden partitions, Section 5 provides suggestions for forensic investigators and Section 6 contains conclusions.

2. Preparation of a hard drive – for Xbox 360

The modification of a hard drive to be used on the Xbox 360 requires the following:

- A bootable medium such as a floppy disk with an appropriate firmware modification tool e.g. HDDHackr (MODFREAKZ, 2009).
- A hard drive from a particular manufacturer – compatible models mentioned in Appendix A. For this experiment, a 120 GB Western Digital Scorpio SATA HDD (WD1200BEVS) was acquired with serial no. WX530734xxxx.
- (Optional) An Xbox 360 games console, to initialize and verify the drive in the native Xbox format.

The process required to set up a drive to work with an Xbox 360 is available online in a fairly comprehensive guide (InsaneNutter, 2009). Using a combination of the tools and firmware, a commercial off-the-shelf hard drive can be used in an Xbox 360, which is less expensive than an official Microsoft drive. If the intention is to use the drive in the Xbox 360 games console, an appropriately signed firmware sector must be obtained either online or from a current system.

As part of this “modding” process, Fig. 1, a backup of the original firmware configuration is also created, saved by default in the same location as the tool itself. A successful modification results in the drive being verified and accepted by an Xbox 360 console (Fig. 2).

It should be noted that although the modding process was developed for the Xbox 360 games console, it can be used to conceal data on a hard drive without an Xbox 360 system present, as detailed in the next section.

3. Preparation of the hard drive – for concealment purposes

The method presented in Section 2 was adapted by the authors for the purposes of concealing data from forensic software and hardware. Two case studies will be presented, demonstrating how those without specialist knowledge of the hard drive can easily hide data from a forensic investigator (ACFO, n.d).

3.1. Case study 1: a hidden partition on an external drive

There are many different connection formats that offer interoperability with external devices, for example eSATA, USB, Firewire, Thunderbolt etc. In order to modify the firmware with the tools used in this paper the hard drive made use of an eSATA interface to the PC. HDDHackr scans for devices connected to SATA connections on the computer.

Following a method for preparation similar to Section 2 above, the hard drive underwent the following modification albeit without the involvement of an Xbox 360 system:

- The firmware is reset to its original settings, 120 GB Western Digital.
- Using a zeroing tool (dd under a Linux LiveCD) the drive is blanked.
- HDDHackr is used to change the firmware to a 20 GB Fujitsu.
- The 20 GB partition is formatted as NTFS on a Windows XP system.
- A copy of the Master Boot Record (MBR), representing this single partition layout is kept on a floppy disk, mbrutil.exe by Powerquest (now Symantec) was used.
- HDDHackr is used to change the firmware to a 120 GB Western Digital.
- The unallocated space (i.e., 100 GB) is formatted as NTFS and becomes the partition which can be later hidden.
This can then be used for any required purpose, such as a storage device etc.

- Another copy of the MBR, representing this now dual-partition layout, is kept on a floppy disk.

To hide the 100 GB partition, HDDHackr was used to flash the 20 GB Fujitsu firmware and mbrutil.exe was used to apply the single partition MBR to the drive. The drive now appears in the host operating system as a 20 GB Fujitsu NTFS drive. This is true of Windows, Mac OSX and Linux.

To restore the 100 GB partition, HDDHackr was used to flash the original firmware and mbrutil.exe was used to apply the dual partition MBR to the drive. The drive now appears in the host operating system as a 120 GB Western Digital drive containing two partitions, a 20 GB and a previously undetectable 100 GB.

3.2. Case study 2: a hidden operating system

Given the large number of forensic artifacts that can be obtained from light usage of a desktop operating system, it is very difficult to successfully conceal all user activity. Concealing the existence of a 2nd operating system might be preferable, if this were possible to achieve and required less effort than maintaining a ‘clean’ system. Usage of LiveCD systems makes data retention difficult to hide. Forensic best practice procedures require that other media (e.g. memory sticks, CDs etc.) is retrieved. Concealing operating systems inside virtual machines has also been addressed as many forensic tools have built-in support for analyzing virtual hard drive formats. This case study demonstrates how it is possible to hide a second operating system in a hidden area of the drive.

The method for creating a hidden operating system largely follows the preparation method mentioned above with a few observations:

- The hard drive was only connected to a PC, and not to an XBox 360 system.
- After the drive is shrunk to 20 GB using the HDDHackr tool, Windows XP is installed using the default partition information, i.e. the full capacity of the drive (20 GB).
- Using one of numerous DOS-based master boot record (MBR) backup tools, a copy of the MBR was stored on a floppy disk. This experiment made use of the utility mbrutil.exe by PowerQuest (now Symantec).
- Using HDDHackr, the drive is restored to 120 GB and a second copy of Windows XP was installed in the unallocated space (i.e., 100 GB, which becomes the second partition).
- Using the same MBR backup tool as before, an updated copy of the MBR was stored alongside the original.

At this point, a dual-boot Windows XP system is created. To conceal the secondary Windows XP operating system, the following steps may be taken:

- Using HDDHackr, flash the hard drive firmware back to 20 GB. N.B. If the primary Windows XP operating system is booted immediately after this point, it will crash with a blue screen of death. This happens because as Windows boots it reads the MBR partition information and if the location of the 2nd partition is still present but the drive is set to 20 GB the operating system fails in its attempt to access a non-existent location. This is why it is important to have a DOS-based bootable floppy or usb stick with the HDDHackr and MBR backup tools as the primary Windows will not boot.
- Restore the original MBR from the floppy disk (e.g., mbrutil.exe)

This will let the primary Windows XP to boot normally. For further clandestine activity, one may remove the second operating system entry from the boot loader. Since Windows XP is being used the boot.ini file may be modified.

Further to the method described above, the following should be observed. Before any changes were made to the 120 GB drive, it was zeroed out using the tool dd running on a LiveCD Linux distribution. To confirm the changes made to the drive, FTK Imager was used to make an image of the 20 GB drive after the primary Windows XP was installed. A second image of the primary Windows XP partition was again taken after the secondary Windows XP was installed and the drive size reduced to 20 GB. The two images were compared to identify any differences that may assist the forensic examiner. The main observable differences were to the MBR offset 0x1CE (the starting location of the 2nd partition) as seen in Fig. 3 and to the boot.ini file.
4. Drive analysis using forensic tools

4.1. Initial investigation

A number of experiments were carried out to determine if any software or hardware forensic analysis could reveal the true nature of this apparent 20 GB Fujitsu drive.

Initially, FTK Imager (v3.1.1) by AccessData was used to assess the drive. During the acquisition process, the drive was reported as a 20 GB Fujitsu; a raw acquisition resulted in a 20 GB image.

The presence of a Device Configuration Overlay (DCO) or Host Protected Area (HPA) was then checked to determine if the hidden area was identifiable. Using the open source hdparm tool and the method described in Carrier (2004), neither a DCO nor an HPA was found.

Commercial forensics equipment by DeepSpar Data Recovery Systems has a number of advanced auto-analysis features to identify anything unusual. Upon connecting the drive to the DeepSpar device, DeepSpar reported the drive was a 20 GB Fujitsu. DeepSpar did not report anything unusual on the drive and again confirmed that neither a DCO nor HPA was found.

Another equipment manufacturer is AceLaboratory which produce an advanced data recovery solution called PC3000. This device can manipulate the hard drive at a firmware level, and is especially slanted for data recovery when analyzing "...a hard disk which spins erratically, or [when] the heads are making clicking noises, or [when] maybe everything seems fine but the disk is just not recognized by the PC or any other tool" (PC3000, 2013).

PC3000 accessed the drive using its automatic detection functions. It tests the structure of firmware by querying ROM based values to determine the correct family of drive which then helps identify the correct firmware-level command set to use.

PC3000 identified the drive as a 20 GB Fujitsu (Fig. 4), and reported it was fully operational and the synchronization routines performed without fault. Upon trying the auto-detected Fujitsu command set on the drive, commands then failed to run successfully. Although this is an indication that something is wrong, the explanation is far more likely to be corrupt firmware rather than anything malicious.

4.2. Further investigation

A number of further experiments were conducted to determine if any indicators of the true nature of the drive could be found.

The first method involved checking if the LBA Maximum setting had a different value to the original drive configuration. The drive did not have this value set. It is possible to forcibly set the LBA Maximum value on a drive, however this risks damaging the drive. As the true size of the hard drive was known in this case it was set to the correct value, which allowed some tools to read past the 20 GB limit set by HDDHackr. If this procedure is carried out incorrectly, it could cause the drive heads to crash by trying to read an area outside the true capacity of the drive.

Using PC3000 and the true make/model of the drive (Western Digital), the family and firmware revision was set manually overriding the tool’s auto-detection function (described in 4.1). At this point, the discrepancy between the correct firmware revision and the modified version on the drive could be seen. Furthermore, an examination of the drive’s surface area showed that only the first 20 GB was readable, from LBA 0 up to the drives reported upper LBA (20 GB). Any attempt to read past the reported maximum LBA was not permitted at this point by PC3000. This is not a limitation of the tool but rather the tool using the reported LBA values. After modifying the LBA Maximum value manually (120 GB), PC3000 was able to read data past the 20 GB limit. It should be stressed this process could only be performed as the true nature of the drive was already known in this experiment.

A comparison of firmware revision values from the overwritten firmware and the ROM’s second copy did show an inconsistency on the drive. However, this could just mean a corruption on either copy rather than an attempt of deliberate tampering.
5. Suggestions for the digital forensic analyst

Considering the two scenarios presented in Section 3, any post-acquisition analysis would not reveal the presence of a hidden partition so long as the owner had been careful. To the unwary, a hard drive that spins up and is recognized by the operating system and can be imaged with forensic tools is enough. Therefore, effort to find such a modification should be made at the beginning of a forensic investigation.

The authors propose a modification to current custom and practice in the imaging process with the following observations:

1. Validate that the size reported by the analysis platform is the same as that on the drive sticker. A 20 GB drive on a drive reporting to be a 120 GB is a giveaway; but what if the LBA is altered to provide a smaller hidden area? Given the long standing misuse of terms like kilobyte to indicate 1024 bytes and megabyte to indicate 1024 kilobytes leading to the differences in size reported by operating systems of a hard drive; a few missing gigabytes will likely go unnoticed even by someone who is looking for size inconsistencies.

2. Check for evidence of deliberate alteration, wear, removal or replacement of the hard drive label. This may be an attempt to try and provide a false alibi of the reported size of the drive.

3. Look at the physical drive (Fig. 5) in order to examine its exterior chassis and any possible parameters that may indicate drive construction: The PC3000 data recovery tool has a catalogue of the different types of drive including a photographic record of the top label and PCB underside. Even if the label is damaged or missing, identification of the drive through its casing/PCB construction may be possible.

4. Keep track of which hard drives are likely candidates for alteration, and therefore need to be checked more thoroughly. For example, the tools used in this paper only work with a specific set of Western Digital drives.

5. When firmware is altered, a backup is normally provided. Is there any evidence to suggest a backup of the firmware exists? If so, the question why remains. In the preparation detailed in Section 3, the backup firmware is required to reveal the hidden partitions.

6. Check for evidence of so-called “modding” tools. Even if the seized computer’s hard drive hasn’t been modified, this may still indicate an ability to tamper with another system, such as a games console.

7. Check and validate the reported firmware version from multiple areas of the drive.

8. Check the reported and actual LBA size for inconsistencies.

6. Conclusions

The analysis conducted in this paper raises some serious questions about the degree to which forensic investigators can identify a drive. The fact that it is possible to have a hard drive report a different make, model and capacity to a number of advanced digital forensic tools by using free applications downloaded from the Internet demonstrates
how important it is to be aware that such tampering can easily take place. If in the unlikely event that a criminal is devious enough to alter a drive’s firmware and remove its label this would make analysing the drive a very frustrating and cumbersome exercise.

The authors advise that analysts are made aware of the drives that can be manipulated to contain the firmware of the offending drives. If tampering is suspected then further checks must be performed to verify the drive. This paper also presented verification methods to assist the forensic analyst when undertaking an investigation.

The experiments performed in this paper made use of a 120 GB Western Digital. At the time of writing, 750 GB Scorpio Black models (about £70) could in theory be flashed with the 20 GB Xbox 360 firmware providing up to 730 GB of concealed information in a standard NTFS formatted partition.

The paper has demonstrated that it is possible to use freely available tools to modify the firmware on a hard drive, without requiring any specialist forensic knowledge, to conceal information from all advanced digital forensic tools tested. To an unsuspecting forensic analyst the true nature of the drive is undetectable even when using more advanced data recovery tools which require extensive training.

Acknowledgements

The authors would like to thank the individuals that make up the Information Security Research Group (ISRG) at the University of South Wales, and particular thanks to Mr. Mathew Evans for his suggestions and support.

Appendix A. HDDHackr compatible hard drives

- Western Digital Scorpio Series BEVS/BEAS (All Sizes)
- Western Digital Scorpio Blue Series BEVS/BEVT/BPVT (All Sizes)
- Western Digital Scorpio Black Series BEKT/BJKT (All Sizes)
- Western Digital VelociRaptor Series (All Sizes)
- Western Digital AV-25 Series BUDT (All Sizes)

As of HDDHackr v1.3, all Western Digital Scorpio drives are supported.

References


