Hiding Data in Hard-Drive's Service Areas

Ariel Berkman <ariel@recover.co.il>
Recover Information Technologies LTD
http://www.recover.co.il

February 14, 2013

Contents

1 Introduction

In this paper we will demonstrate how spinning hard-drives' service areas[1] can be used to hide data from the operating-system (or any software using the standard OS's API or the standard ATA commands to access the hard-drive). These reserved areas are used by hard-drive vendors to store modules that in

[1]Sometimes referred to as "Reserved area", "System Area", "Negative sectors", "Firmware area", "Microcode Area", etc.

turn operate the drive, and in a sense, together with the ROM, serve as the hard-drive's internal storage and OS. By sending Vendor Specific Commands (VSCs) directly to the hard-drive, one can manipulate these areas to read and write data that are otherwise inaccessible. This should not be confused with DCO[2] or HPA[3] which can be easily detected, removed and accessed via standard ATA commands.

2 Service Areas and Service Area Modules

A service area is a logical area on the hard-drive (residing on the platters) set aside by hard-drive vendors for internally managing the drive. These areas are outside the hard-drive's Logical Block Address (LBA) space and as such are inaccessible via the standard ATA commands. As the complexity of hard-drives grow, so does the software and data required to manage that complexity, and correspondingly, the need for larger service areas. The service area contains both code and data modules such as defect management modules, SMART data modules, self-test modules and much more. Due to their importance, there are usually two copies of these modules, such that if one copy gets damaged or corrupted, the drive could continue to operate.

Since these modules are responsible for the operability of the drive, corruption of these modules could result in a drive failure. Professional data-recovery labs have been using, since the inception of the field, data-recovery tools (e.g., Ace Laboratory's[4] PC3000) to access these service areas and repair, when possible, the critically damaged modules.

In order to access the service area, Programmable IO must be used to send VSCs directly to the hard-drive's IO port. These commands are unique to the hard-drive vendor and are not publicly disclosed. Hard-drive vendors often release tools for manipulating hard-drive's functionality; these tools use VSCs to modify certain elements of the drive. One such example is Western-Digital's *wdidle3.exe*[5] (and its open source counterpart *idle3-tools*[6]) which changes the way the hard-drive's built-in activity timer operate. Another

[2]http://en.wikipedia.org/wiki/Device_configuration_overlay
[3]http://en.wikipedia.org/wiki/Host_Protected_Area
[4]http://www.acelaboratory.com/
[5]http://support.wdc.com/product/download.asp?groupid=609&sid=113
[6]http://idle3-tools.sourceforge.net/

example is the *hddhackr*[7] tool which modifies the service area modules in charge of the hard-drive identification information.

3 Service Area Sizes

Service area size and service area module sizes vary significantly across hard-drive vendors, families, capacities and firmware versions. For example, a WD2500KS-00MJB0 drive (Western-Digital, Hawk family, 250GB, Firmware version 02AEC) has two copies of its service area modules (on platter surfaces mapped to heads 0 and 1), each around 6MB in size. The reserved-area size on each surface is approximately 23MB (720 sectors-per-track x 64 tracks). Furthermore, since this drive has 6 surfaces (heads 0 through 5) and the service area modules copies are on surfaces mapped to heads 0 and 1, the corresponding areas on surfaces mapped to heads 2 through 5 are reserved, but not in use by the drive. As such the total reserved area size on such drives is approximately 141MB, of which 12MB is in use.

In comparison, a WD10EACS-00ZJB0 drive (Western-Digital, Hulk family, 1TB) has two copies of its service area modules, each approximately 26MB. The reserved-area size on each surface is approximately 56MB (1280 sectors-per-track x 86 tracks). This drive has 8 surfaces (heads 0 through 7) and the service area modules copies are on surfaces mapped to heads 0 and 1. The rest of the reserved area is not in use. As such, the total reserved area sizes on such drives is approximately 450MB, of which 52MB is in use.

4 Other Reserved Areas

In addition to areas reserved for service area modules, other forms of ATA-inaccessible locations that require VSCs might be available:

- The hard-drive's flash chip is used for boot-strapping the drive. While usually very small (around 1MB), could contain some available space.
- Unused tracks past the hard-drive's LBA.
- Some hard-drives have disabled head(s) which map to a whole surface. By sending VSCs, one could theoretically enable that head, use that

[7] http://www.google.com/search?q=hddhackr

entire unused surface to store data and then disable the head to render that data inaccessible.

5 Data Hiding and Sanitation

The common notion in data sanitation is that data sanitation software tools, when properly used, will completely purge all data on the hard-drive. However, this does *not* apply to the aforementioned reserved areas, regardless of the employed data destruction method (e.g. single pass, multiple passes with random data, nulls, etc.).

It's important to emphasize that the only way data can be written to reserved areas is by using the hard-drive's VSCs. For that reason, it's very unlikely that data would, for example, be accidentally copied or leaked[8] to these areas. It is however possible, although non-trivial to accomplish, that a software designed for that purpose, would be able to copy data to reserved areas such that they would not be sanitized despite any software sanitation efforts.

Furthermore, software designed to manipulate the reserved areas - via the drive's VSCs - could use the reserved areas as a "hiding" place. Not only that these areas can't be sanitized (via standard tools), they cannot be accessed via anti-virus software, computer forensics tools, etc.

6 Proof of Concept

In order to demonstrate the ability to hide data in the service area, we've developed a proof-of-concept designed to work on Western-Digital 250GB Hawk hard-drives (available for download at http://www.recover.co.il/SA-cover/SA-cover-poc.c). These drives have 6 surfaces, each with 64 tracks (with 720 sectors-per-track) reserved for service area. The first two surfaces contain copies of the service area modules and are therefore not used in the POC (despite the unallocated areas which can also be used). The POC can read and write a file of upto 94MB to the reserved area (4 x 64 x 720 x 512

[8] An exception to this is when a hard-drive decides to re-allocate a suspected bad-sector, and re-maps that logical address to a new sector, leaving the original sector inaccessible to the user. However, the risk is minor due to the small amount of reserved sectors for this purpose and the inability to control when and where it will take place.

bytes). The code *can* result in data loss, or hard-drive failure, therefore *use it at your own risk!*

In this example we demonstrate how the POC can be used to hide data that will not be sanitized (or accessible) using standard tools:

- Generate a random file (94MB in size) and compute its MD5 hash value.
- Write the file to the service area.
- Sanitize the drive by dd-ing /dev/zero onto the "entire" drive (the block device of the relevant hard-drive). Our understanding is that a complete, successful single pass of nulls (or any other byte) would suffice for the data to be rendered unrecoverable.
- Read the service area content and calculate its MD5 value to see the random data file is intact.

```
root@Shafan1:~/SA# dd if=/dev/urandom count=184320 > random-file ; md5sum random-file
184320+0 records in
184320+0 records out
94371840 bytes (94 MB) copied, 12.8187 s, 7.4 MB/s
0baca7245e1efa160512a6217c13a7b0  random-file

root@Shafan1:~/SA# ./SA-cover-poc -p 0x0170 -w ./random-file
using port address: 0x0170

Model: WDC WD2500KS-00MJB0
S/N:      WD-WCANK5391702
F/W Ver:        02.01C03
LBA24:268435455    LBA48:488397168

Service area sectors-per-track (720)
Service area tracks (64)
Num of heads(6)
Unused reversed space (94371840 bytes)
writing head(2) track(-1)
writing head(2) track(-2)
writing head(2) track(-3)
....
writing head(5) track(-62)
writing head(5) track(-63)
writing head(5) track(-64)
```

```
root@Shafan1:~# dd if=/dev/zero of=/dev/sdb bs=1M
dd: writing '/dev/sdb': No space left on device
238476+0 records in
238475+0 records out
250059350016 bytes (250 GB) copied, 4732.86 s, 52.8 MB/s

root@Shafan1:~/SA# ./SA-cover-poc -p 0x0170 -r after-dding-dev-zero
using port address: 0x0170

Model: WDC WD2500KS-00MJB0
S/N:      WD-WCANK5391702
F/W Ver:        02.01C03
LBA24:268435455    LBA48:488397168

Service area sectors-per-track (720)
Service area tracks (64)
Num of heads(6)
Unused reversed space (94371840 bytes)
reading head(2) track(-1)
reading head(2) track(-2)
....
reading head(5) track(-62)
reading head(5) track(-63)
reading head(5) track(-64)

root@Shafan1:~/SA# md5sum after-dding-dev-zero
0baca7245e1efa160512a6217c13a7b0  after-dding-dev-zero
```

7 Summary

Spinning hard-drives contain reserved areas with non-negligible sizes that are used by hard-drive vendors to store service area modules. These areas can only be accessed and manipulated via VSCs (Vendor Specific Commands). By using VSCs, one can store data in these areas such that it would be effectively hidden to the OS and other tools using standard ATA commands.