

Technical White Paper

July 17, 2003 www.TechPathways.com

Christopher L. T. Brown, CISSP

clbrown@techpathways.com

Analysis of the ATA Protected Area

Abstract

ATA Specifications added the “Protected Area” as a means for PC distributors to ship diagnostic utilities with PCs. Simply put, the ATA protected area is an area of the hard drive that is not reported to the system BIOS and operating system. Because the protected area is not normally seen, most disk forensics imaging tools will not image the area. Initially there was no great concern over the Protected Area by computer forensics analysts, largely because the feature was thought to be used only by PC distributors. There is now a growing level of interest and concern related to end user implementation of the Protected Area to hide data. The concern has been highlighted by the release of consumer marketed utilities to implement the Protected Area to hide user data.

One such utility is AREA51 created by StorageSoft, which has subsequently been purchased by Phoenix Technologies. Phoenix Technologies has temporarily taken Area51 off the market while they integrate the product with a larger suite of applications. This integrated suite of applications is expected to be released soon.

Note: ATA refers to an Advanced Technology Attachment device (AKA IDE drive) which conforms to the ATA standard.

Implementation

The ATA Protected Area is outlined in American National Standards Institute 346-2001 “Protected Area Runtime Interface Extension Services” (PARITES) and is supported on all drives that conform to ANSI NCITS 317-1998 (ATA/ATAPI 4).

Information about the protected area is not contained in the normally suspected places, such as, the Partition table, file allocation tables and boot record, making the area hard to detect unless

you are specifically looking for it. Protected Area information is contained in the Boot Engineering Extension Record (BEER). The BEER is a record that is stored on the native maximum address (last sector) of the device and contains non-volatile configuration information about the device. Commands outlined in the PARITES specification hide the BEER from the BIOS and operating system.

Once created, users can access the protected area only at boot time through a modified Master Boot Record (MBR), or a special boot disk.

Note: It is suspected BIOS manufacturers will add the ability to use a hot-key during the POST phase of booting the system allowing users to access the protected area.

Analysis

As you might expect, it would be easy to miss Protected Area implementation on a target system unless you were looking for it. Three methods for detection are:

1. The use of a modified MBR. Forensics examiners may be able to identify the use of the Protected Area by analyzing the MBR. Current versions of AREA51 modify the boot partition by changing the boot loader to include pointers to the protected area.
 - a. Identification of AREA51 is accomplished by examining the master bootstrap code at sector 0 offset 0. In this case the hex string for the first 4 offsets will be FA 33 C0 8E.
 - b. The copyright and version information for AREA51 can be found in Sector 1 offset 270. This section contains the ASCII text "Area51 boot selector".
 - c. The signature information above is still present on an imaged drive, but will be over written if a forensics workstation running Windows NT/2000 is allowed to write a signature to the disk. Computer forensics examiners should always employ some type of write-blocking on forensics workstations.
2. Another method to detect the use of the ATA Protected Area is by doing a little disk math. Consider the following scenario:

The examiner is about to image a disk which is labeled, or they know by other means has a CHS (Cylinder Head Sector) value of 16383/16/63. In this case to find out the total number of sectors which should be reported simply multiply (Cylinders x Heads x Sectors). In this case $16383 \times 16 \times 63 = 16,514,064$ total sectors. If the user started an image of the disk and noticed it only reported 4,192,965 sectors then they would be missing around 6 GB of data area depending on how many bytes were used in each sector. To establish the total disk size use total sectors x bytes (normally 512). In this case the disk should be 8.4 GB, but was reporting about 2 GB.

Note that this may not always be a good way to detect the Protected Area since the drive may be mislabeled.

3. Looking for a boot disk at the scene which may contain a utility for booting to a Protected Area. Any floppies labeled AREA51 should be suspect.

Once a system is identified as utilizing the Protected Area the forensics examiner is faced with the decision of how to proceed with evidence collection. At first glance standard drive imaging practices might seem reasonable, but there are obstacles to this approach. Imaging the Protected Area can only be accomplished by resetting the drive to report the native maximum sectors first. Hence, the examiner is faced with two options:

1. Reset the original evidence disk.
Or
2. Perform analysis directly on original evidence disk.

In the first choice the examiner could use a utility to cause the drive to report the native maximum sectors. Once this reset was accomplished, the examiner could follow standard imaging practices and computer forensics methodologies. The data formally located in the protected area will now be available in the imaged disk slack space. To reset the original evidence disk the examiner could use a tool such as:

- Technology Pathways provides a tool for removing the Protected Area with the ProDiscover™ DFT Application available at <http://www.TechPathways.com>.
- Mark Menz presented some Protected Area utilities during recent HTCIA conferences. Email markmenz@usa.net for more information.

In all cases where the examiner is intending to perform analysis on the original evidence disk they should ensure a hardware write blocking device is used. Two such devices are:

- NoWrite™ - IDE Write Blocker
<http://www.TechPathways.com>
- ACARD SCSI-to-IDE Write Blocking Bridge (AEC7720WP)
<http://www.microlandusa.com/>

<p>Caution: Always use great care when working directly with original evidence and ensure you have a backup image.</p>

Conclusion

The ATA Protected Area is a relatively new standard that requires increased attention due to it's availability to the public sector to hide data. While the Protected Area is fairly easy to detect with good attention to detail, detection may become more difficult as new products emerge utilizing the feature. Computer Forensics examiners should become knowledgeable of the ATA Protected Area and how to detect it. Labs are encouraged to implement procedures into their standard methodologies that encompass recovering data from the ATA Protected Area.