B2 An Alternate Methodology for Validating Hardware Write Block Devices

Benjamin R. Livelsberger, MS, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8970, Gaithersburg, MD 20899-8970*

The goal of this presentation is to show how the Computer Forensics Tool Testing (CFTT) project at National Institute of Standards and Technology has developed an alternate methodology for validating Hardware Write Block (HWB) devices. After attending this presentation, attendees will be familiar with this methodology and the benefits it offers.

This presentation will impact the forensic science community by showing how the current methods used to validate HWBs have an inherent weakness. This presentation will have the impact of educating the community to the nature of this weakness and to introduce an alternate NIST-developed method that seeks to account for it.

Before being used in an investigation, the correct functioning of a forensic tool must first be established. For Hardware Write Block tools this involves testing: (1) that the HWB allows informational and read commands to be passed to the drive and their responses to be returned to a host computer; and, (2) that it blocks modifying commands from reaching the protected drive.

The current commonly used method for validating a HWB involves using forensics tools and/or common operating system utilities and operations to attempt to read and write to a protected drive. There is a weakness inherent in this approach, namely that it only tests a small subset of the commands that could be used to read from or write to a drive. For example, testing a HWB's ability to block modifying commands by attempting a file copy operation to a protected ATA drive using an operating system that implements the WRITE DMA EXT command for ATA devices will only test the hardware write block's ability to block the WRITE DMA EXT command; it will not test whether the HWB blocks the WRITE SECTORS EXT or WRITE MULTIPLE EXT commands. In this scenario, a malfunctioning HWB that incorrectly allows the WRITE MULTIPLE EXT command to be passed to protected drives will not be identified as faulty. A more thorough approach, one that tests the HWB's behavior with a broader range of commands than those implemented by a given operating system is desirable.

The Computer Forensics Tool Testing (CFTT) project has developed an alternate methodology for validating HWBs. With this methodology, testing is not limited by the subset of commands implemented by the operating system being used. HWBs are instead tested with all read and write commands as defined in ATA specs 4-8 and SCSI Block Commands-2 and as implemented by an extended version of the ATAraw Linux library written by Kyle Sanders and Simson Garfinkel of the Naval Post Graduate School. Three Linux programs were written to implement the CFTT methodology. These programs tie into the ATAraw library to send ATA or SCSI commands to devices via the Linux SCSI Generic driver. The three programs are:

try_read sends all defined SCSI or ATA read commands to a drive;
try_write sends all defined SCSI or ATA write commands to a drive, and;
write_verify measures whether any hard drive sectors have been successfully written to.

Using these programs, a HWB tool may be validated in the following manner:

1. For each hard drive interface supported by the HWB, initialize a drive with known content.
2. Calculate a before reference hash for each drive.
3. For each permutation of host-to-blocker and blocker-to-drive interfaces execute the try_read and try_write programs.
4. Calculate an after reference hash for each drive.
5. Use write_verify and a comparison of the reference hashes to measure whether any sectors on the test drives have changed.

Digital Forensics, Hardware Write Block, Tool Validation

 ** Presenting Author*