May 25, 2004

HARDWARE WRITE BLOCK (HWB) SPECIFICATION VERSION 1.0 COMMENTS AND RESPONSES

NIST

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

1. Purpose

The specification for hardware write block requirements [http://www.cftt.nist.gov/HWB-posted.pdf] was posted on the Computer Forensics Tool Testing (CFTT) website in November 2003 and users were notified that it was available for review. This document summarizes the comments received and the responses to the comments. The changes are reflected in http://www.cftt.nist.gov/HWB-posted.pdf.

Comments are grouped according to common threads. The response follows each thread. In some cases, similar comments were omitted where it was clear that the response would address all of them.

Notes to the Reader:

- Comments are written in italic font.
- Responses are written in Roman font.
- Where comments referred explicitly to specification sections in the HWB version 1.0 specification, responses also refer those sections.
- Where necessary, responses will also mention new section numbers to alert readers to modifications in the specification.

2. Comments

2.1 Thread: Section 5, Item 5 – Scope – Non-hostile environment

It would be quite simple for a malicious program to permanently cause harm to a drive if it were built to match the current specification. As such, we would suggest that item 5 be dropped or changed to reflect this reality.

Response: Section 5, Item 5 – Scope – Non-hostile environment

The intent of this section was to communicate that the user of the device was not trying to circumvent the proper function of the HWB device. Several sections in the specification have been modified to more explicitly express this intention.

> **Purpose (Section 2):**
> **“**This document defines functional requirements for hardware write blocker (HWB) devices used in computer forensics investigations. It does not define requirements for protecting storage devices from misuse, either intentional or not intentional.”
>
> **Scope (Section 5, Item 5):**
> “Preventing misuse of the storage device is outside the scope of this document.”

2.2 Thread: Requirement to always allow non-modifying operations

We strongly disagree with the statement: “a HWB should not allow modifying commands to be transmitted to a storage device and should allow non-modifying commands to be transmitted a storage device”.

Response: Requirement to always allow non-modifying operations

The specification was modified to allow for flexibility in the design and implementation of HWB devices.

- **Previously**, the beginning of section 6 (Requirements) read: “a HWB should not allow modifying commands to be transmitted to a storage device and should allow non-modifying commands to be transmitted a storage device.”

- That statement **now** (currently at the beginning of section 7) reads: “a HWB should not allow modifying command operations to be transmitted to a storage device and should allow retrieval of all accessible data on the storage device.”

2.3 Thread: Section 6.1, RM-01: Mandatory Requirement 1

Microsoft Windows® and other operating systems issue a flurry of Identify Device commands to the drive. If no commands have been issued that could change the drive information, there is no point in bothering the drive for the info each time. Many of the Non-modifying commands fall into the category of commands for which a HWB may help protect the drive by responding on its behalf ...

In addition to having the HWB respond on behalf of the drive … The HWB may change the information in such a way as to make the Host system believe that a feature, such as SMART, is not supported.

Response: Section 6.1, RM-01: Mandatory Requirement 1

The specification was modified to allow for flexibility in the design and implementation of HWB devices.

An additional requirement was also introduced to ensure that all data is accessible on the protected storage device during the operation of a HWB.

Mandatory Requirements (Section 7.1):
"**HWB-RM-03** A HWB, after receiving an *information category operation* from the host, shall return a response to the host that shall not modify any access-significant information contained in the response."

Command Operation Categories (Section 6):
"**Information:** Any operation that requests data which is not stored on a storage device's medium and returns that data to the host"

Terminology (Section 4):
"**access-significant information:** Information contained within the response to an *information category operation* that is significant to locating and accessing data stored on the device. For example, the total number of sectors reported for a given storage device is significant to locating all data on the device."

2.4 Thread: Section 6.1, RM-02 Mandatory Requirement 2

HWB-RM-02: *A HWB shall allow non-modifying commands to be transmitted to a protected storage device.*
Disagree. Not all non-modifying commands should be passed to the drive. Passing all Non-modifying commands is not in the best interest of the drive. The less communication that there is between the HWB and the drive, the less chance there is for error. Therefore, in cases where the HWB may accurately respond on

behalf of the drive, it should be allowed to. Additionally, there are many cases where the command may require change in order to best protect the drive.

Response: Section 6.1, RM-02: Mandatory Requirement 2

The specification was modified to allow for flexibility in the design and implementation of HWB devices. The first three mandatory requirements reflect this philosophy.

2.5 Thread: Section 6.1, RM-03 Mandatory Requirement 3

HWB-RM-03: *A non-modifying command that enters the HWB shall be equivalent to the command that exits the HWB.*
Disagree. Controlling the drive is the domain of the HWB. As such, it there may be times where the drive cannot be properly protected if a Non-modifying command is allowed to go through unchanged. An example would be the Set Max Address command. If the Host System requests a permanent change to the Max Address, the HWB may substitute the command to make the change temporary.

Response: Section 6.1, RM-03: Mandatory Requirement 3

The specification was modified to allow for flexibility in the design and implementation of HWB devices. The first three mandatory requirements reflect this philosophy.

2.6 Thread: Section 6.1, RM-04 Mandatory Requirement 4

HWB-RM-04: *The response that is transmitted from the protected storage device to the HWB shall be equivalent to what is transmitted from the HWB to the computer.*
Disagree. We believe that this is an oversimplification, and is not in the best interest of the drive ...

Response: Section 6.1, RM-04: Mandatory Requirement 4

This requirement has been removed from the specification. The specification was modified to allow flexibility in the design and implementation of HWB devices as well as flexibility in the choice of methods for interacting with the storage device.

2.7 Thread: Section 6.2, RO-01 Optional Requirement 1

…we believe that the analyst is best protected by having no user configurable options on the device.

HWB-RO-01: *A HWB shall provide the capability to have a storage device either protected or not protected.*
Strongly disagree. A forensics device should not have any settings that would allow the user to change its state.

Response: Section 6.2, RO-01: Optional Requirement 1

This optional requirement has been removed from the specification.

2.8 Thread: Section 6.2, RO-02 Optional Requirement 2

HWB-RO-02: *A HWB shall provide the capability to protect a storage device's firmware.*
Unnecessary. In the Addendum, the download microcode command is declared modifying, and therefore must be blocked.

Response: Section 6.2, RO-02: Optional Requirement 2

This optional requirement has been removed from the specification.

2.9 Thread: Section 6.2, RO-04 Optional Requirement 4

HWB-RO-04: *A HWB shall provide the capability to indicate a failed response for blocked commands.*
Problematic. When a write command is blocked under an operating system, such as Windows, and the response code is fail, Windows becomes unpredictable ...

Response: Section 6.2, RO-04: Optional Requirement 4

This optional requirement has been removed from the specification.

2.10 Thread: Addendum – Example ATA Command Listing

re: The command set description found on page 8 ...where are the 48 bit lba cmds (EXT) ? The document does not specify what range of ATA stds(eg:ata-3,ata-4,ata-5, ata-6, ata-7). I know that the ATA-7 (pre-lim specs were thinking about DCO modify cmds...)

Response: Addendum – Example ATA Command Listing

Only command examples were included in the specification. To increase clarity, a single command operation for each category is now listed in the specification. The full command operation lists will be detailed in the HWB test plan.

2.11 Thread: Optional Warning – Appearance of writing when protected

*Scenario: I have been given a hard disk to analysis and believe it might contain a virus). I connect this hard disk to [a HWB device] … I boot my analysis system up with the protected disk connected via the HWB and run a virus scan against a partition's) on the protected disk. The anti virus program finds multiple viruses and attempts/appears to clean them, although it really is not because the disk is protected by the HWB. I guess **what I am pondering is if there should be some kind of notification that indicates that although the system appears to be writing to the drive, the HWB is actually protecting the disk from being written to.** This is more of an issue with the actual system itself and not the HWB but none the less is a common occurrence… it just seems as if an optional requirement (not sure what) might be added to address this.*

Response: Optional Warning – Appearance of writing when protected

Such a requirement is out of scope for this specification.