A Strategy for Testing Hardware Write Block Devices

By

James Lyle

A Strategy for Testing Hardware Write Block Devices

James R Lyle

National Institute of Standards and Technology

DISCLAIMER

Certain trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

Project Sponsors

- NIST/OLES (Program management)
- National Institute of Justice (Major funding)
- FBI (Additional funding)
- Department of Defense, DCCI (Equipment and support)
- Homeland Security (Technical input)
- State & Local agencies (Technical input)
- Internal Revenue, IRS (Technical input)

HWB Protection Goals

- Prevent any change to data
- Allow access to entire user area
- Preserve the configuration of the drive
- May change a drive configuration – e.g., To access HPA or DCO

Prohibit Change by …

- Prohibit changes by a malicious program
- Prohibit accidental change (blunder)
- Prohibit change by operating system
- Prohibit damage to a drive
- Prohibit any changes to a hard drive

Write Block Strategies

- Block unsafe commands, allow everything else
  - + Always can read, even if new command introduced
  - - Allows newly introduced write commands

- Allow safe commands, block everything else
  - + Writes always blocked
  - - Cannot use newly introduced read commands

Need to Know What's Happening

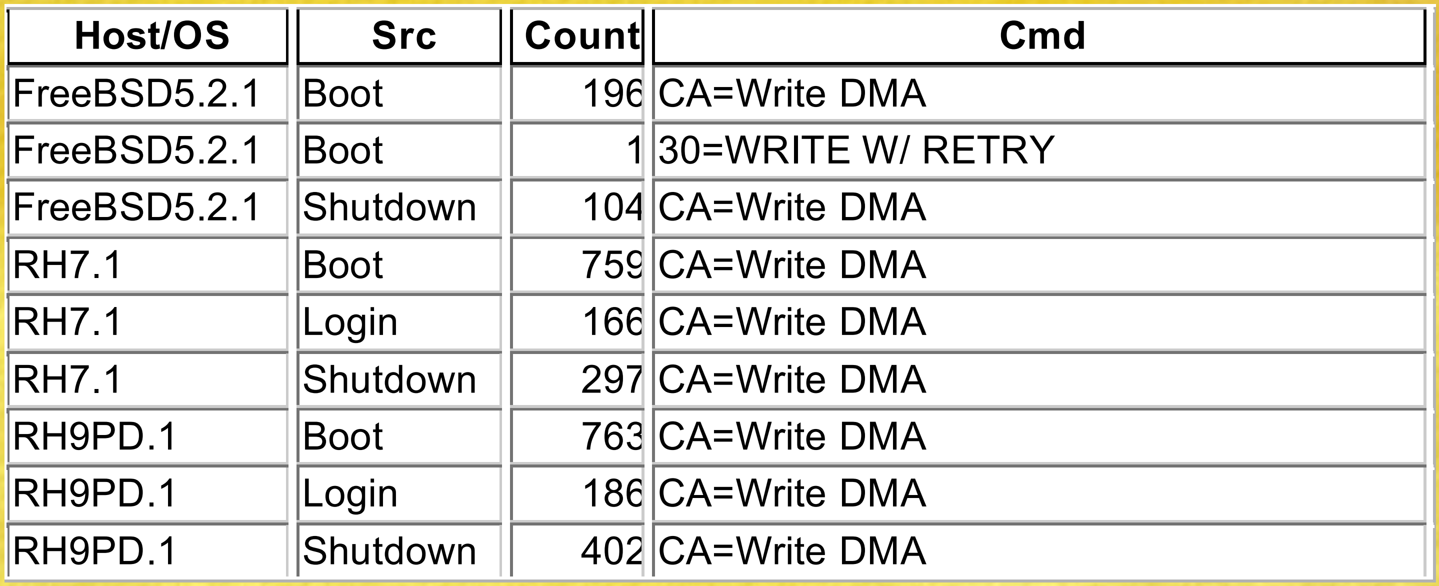
Need to Know

- Know what cmd sent to blocker by host
- Know what cmd sent to drive by blocker

How to know

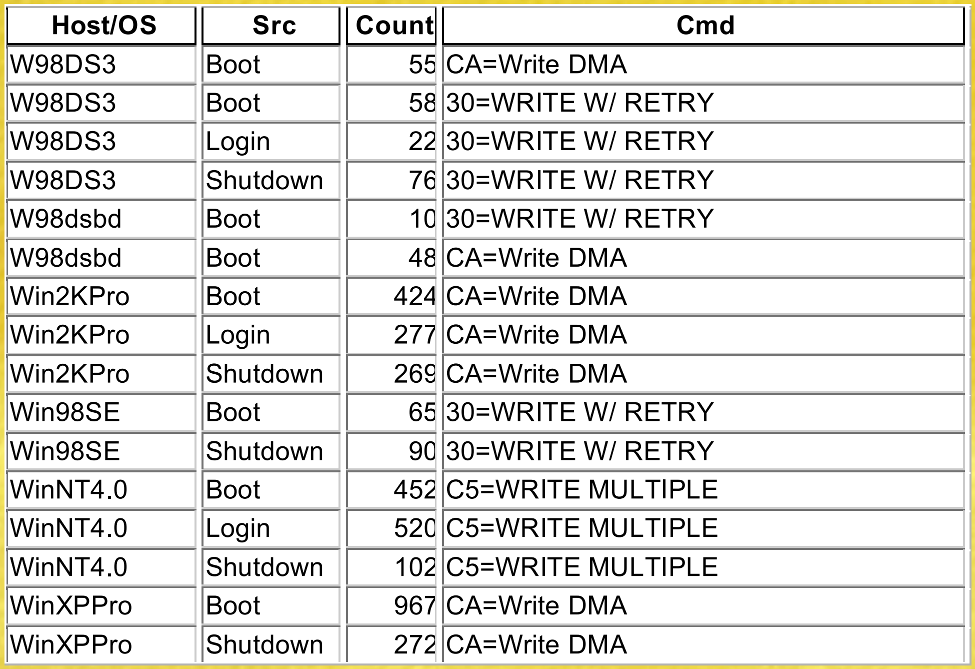
- Hardware bus monitor
- Send specific command
- Look for effect of known command

Write Cmds Used by …



Host/OS	Src	Count	Cmd
FreeBSD5.2.1	Boot	196	CA=Write DMA
FreeBSD5.2.1	Boot	1	30=WRITE W/ RETRY
FreeBSD5.2.1	Shutdown	104	CA=Write DMA
RH7.1	Boot	759	CA=Write DMA
RH7.1	Login	166	CA=Write DMA
RH7.1	Shutdown	297	CA=Write DMA
RH9PD.1	Boot	763	CA=Write DMA
RH9PD.1	Login	186	CA=Write DMA
RH9PD.1	Shutdown	402	CA=Write DMA

Write CMDs Used by Win OS



Host/OS	Src	Count	Cmd
W98DS3	Boot	55	CA=Write DMA
W98DS3	Boot	58	30=WRITE W/ RETRY
W98DS3	Login	22	30=WRITE W/ RETRY
W98DS3	Shutdown	76	30=WRITE W/ RETRY
W98dsbd	Boot	10	30=WRITE W/ RETRY
W98dsbd	Boot	48	CA=Write DMA
Win2KPro	Boot	424	CA=Write DMA
Win2KPro	Login	277	CA=Write DMA
Win2KPro	Shutdown	269	CA=Write DMA
Win98SE	Boot	65	30=WRITE W/ RETRY
Win98SE	Shutdown	90	30=WRITE W/ RETRY
WinNT4.0	Boot	452	C5=WRITE MULTIPLE
WinNT4.0	Login	520	C5=WRITE MULTIPLE
WinNT4.0	Shutdown	102	C5=WRITE MULTIPLE
WinXPPro	Boot	967	CA=Write DMA
WinXPPro	Shutdown	272	CA=Write DMA

Creating a Specification

- Specification (informal) vs Standard (Formal ISO process)
- NIST does research: tools, vendors, users
- NIST drafts initial specification
- Post specification on web for public comment
- Resolve comments, post final version

Requirements

- **HWB-RM-01** A HWB shall not, after receiving an *operation of any category* from the host nor at any time during its operation, transmit any *modifying category operation* to a protected storage device.
- **HWB-RM-02** A HWB, after receiving a *read category operation* from the host, shall return the data requested by the read operation.
- **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.
- **HWB-RM-04** Any error condition reported by the storage device to the HWB shall be reported to the host.

Develop Test Assertions

- Each test assertion should be a single testable statement (or condition)
- Pre-condition: establish conditions for the test
- Action: the operation under test
- Post-condition: measurement of the results after the operation

Test Assertions

HWB-AM-01. The HWB shall not transmit any modifying category operation to the protected storage device.

HWB-AM-02. If the host sends a read category operation to the HWB and no error is returned from the protected storage device to the HWB, then the data addressed by the original read operation is returned to the host.

HWB-AM-03. If the host sends an information category operation to the HWB and if there is no error on the protected storage device, then any returned access-significant information is returned to the host without modification.

HWB-AM-04. If the host sends an operation to the HWB and if the operation results in an unresolved error on the protected storage device, then the HWB shall return an error status code to the host.

HWB-AM-05. The action that a HWB device takes for any commands not assigned to the modifying, read or information categories is defined by the vendor.

Measuring HWB Conformity to Test Assertions

- Detailed -- HWB behavior observed (by hardware monitor) for all commands (defined, undefined, etc)
- Indirect -- All commands with an observable effect
- Observational -- Commands issued by common tools observed by hardware monitor
- Operational -- Pre-test & post-test hash used to detect change to protected drive

Develop Test Cases

- A test case is an execution of the tool under test
- Each test case should be focused on a specific test objective
- Each test case evaluates a set of test assertions

Write Protect Cases

- **HWB-01** Identify commands blocked by the HWB. This case uses a protocol analyzer and a general command generator.
- **HWB-02** Identify modifying commands blocked by the HWB. This case uses a write command generator to try to write a unique message to a unique location for each defined write command.
- **HWB-03** Identify commands blocked by the HWB while attempting to modify a protected drive with forensic tools. This case uses a protocol analyzer to record the commands generated and blocked by attempting to write to a drive with either a forensic tool or an operating system command.
- **HWB-04** Attempt to modify a protected drive with forensic tools. This case attempts to write to a drive with either a forensic tool or an operating system command. Any modifications to the protected drive are detected by comparing a pre-test hash of the drive to a post-test hash of the drive.

Read Tests

- **HWB-05** Identify read commands allowed by the HWB. A read command generator is used to try to read known data from a drive using each defined read command.
- **HWB-06** Identify read and information commands used by forensic tools and allowed by the HWB. Use a forensic tool to read an entire drive with a protocol analyzer recording the actual commands generated by the forensic tool.
- **HWB-07** Read a protected drive with forensic tools. Use a forensic tool to read an entire drive.

Info & Error Tests

- **HWB-08** Identify access significant information unmodified by the HWB. Use a tool to generate a request for drive size and verify that the correct size is reported.
- **HWB-09** Determine if an error on the protected drive is returned to the host. Generate an error at the drive by attempting to read a sector beyond the end of the drive.

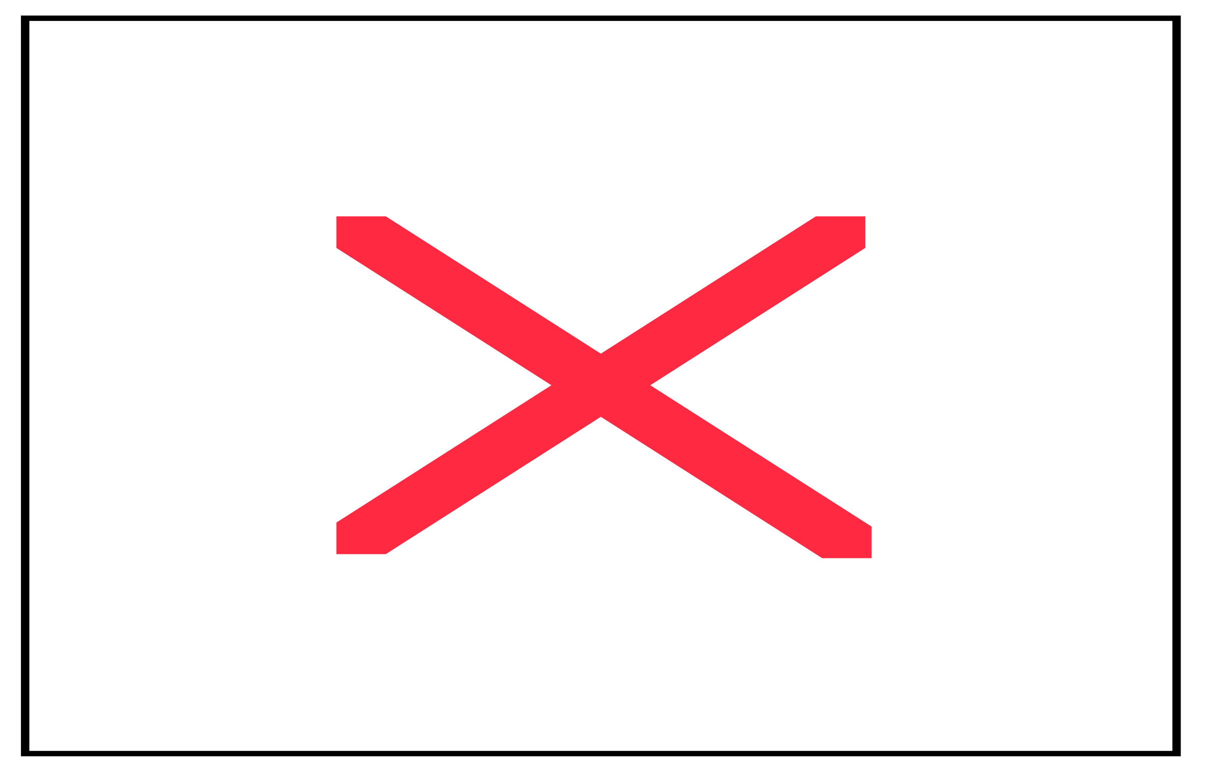
Develop Test Harness

- A set of tools or procedures to measure the results of each test assertion
- Must be under strict version control
- Must measure the right parameter (validated)
- Must measure the parameter correctly (verified)

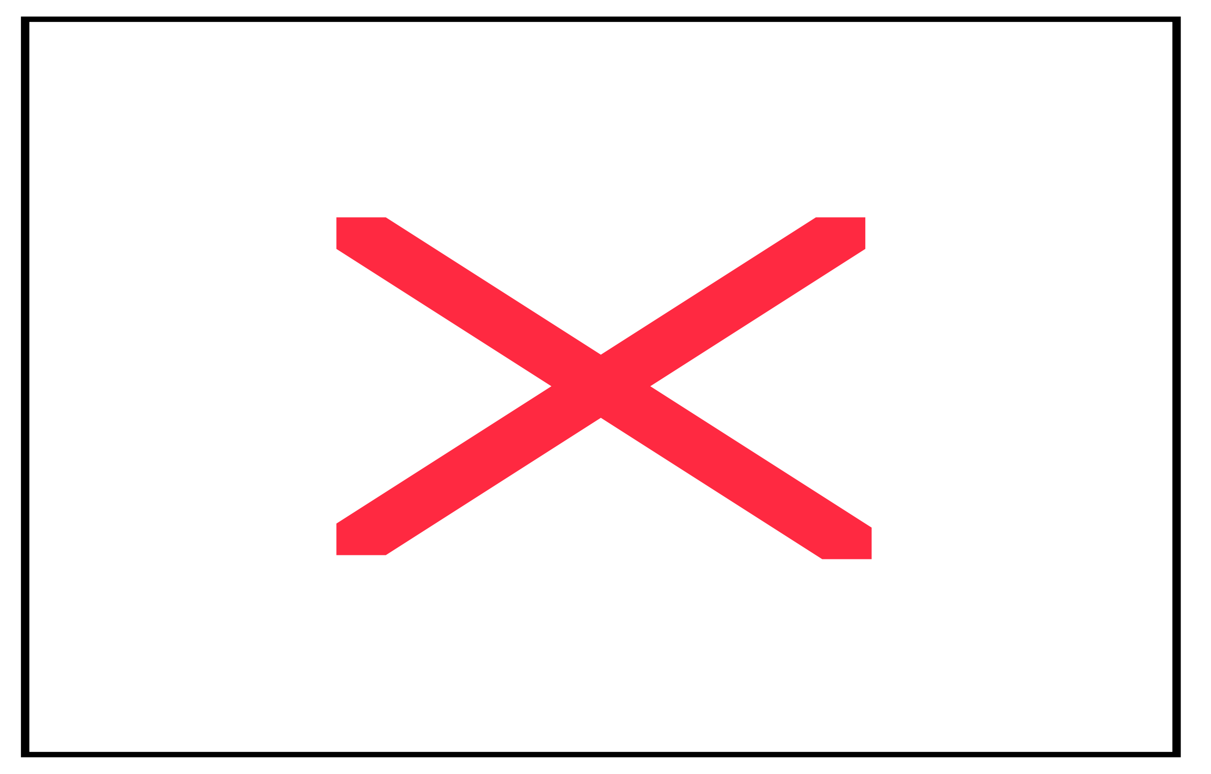
Blocking Device Actions

- The device forwards the command to the hard drive.
- The blocking device substitutes a different command
- The device simulates the command
- If a command is blocked, the device may return either *success* or *failure* back to the host
- Present the drive as a read-only device
- May issue commands without a command from the host

Write Commands Issued by OS (Unix)



Write Commands Issued by OS (MS)



Notable Blocker Behaviors

- Allow the volatile SET MAX ADDRESS, block if non-volatile
- Cache the results IDENTIFY DEVICE
- Substitute READ DMA for READ MULTIPLE
- Allow FORMAT TRACK
- Depending on OS version, user might not be able to preview NTFS partition

Contacts

Jim Lyle
www.cftt.nist.gov
cftt@nist.gov

Doug White
www.nsrl.nist.gov
nsrl@nist.gov

Barbara Guttman
bguttman@nist.gov

Sue Ballou, Office of Law Enforcement Stds
susan.ballou@nist.gov