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)

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

Creating a Specification

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

Writing the Specification

- Specification for a single forensic function
- Describe technical background, define terms.
- Identify core requirements all tools must meet.
- Identify requirements for optional features related to the function being specified.

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

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 assertion

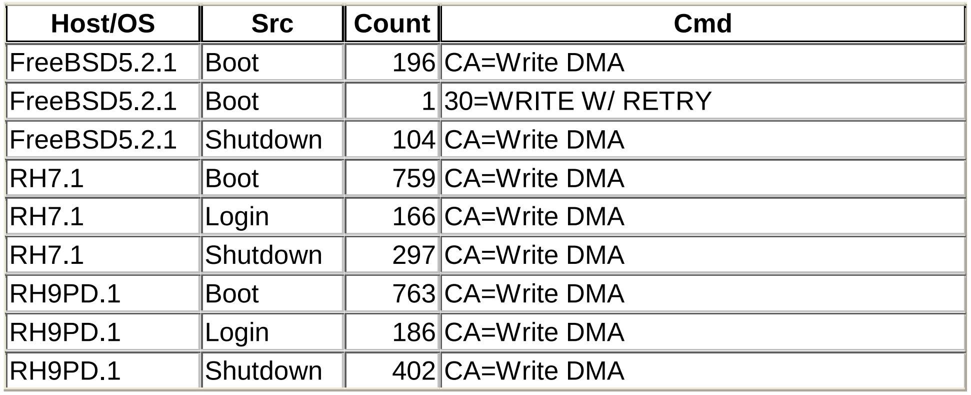
Develop Test Harness

- 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

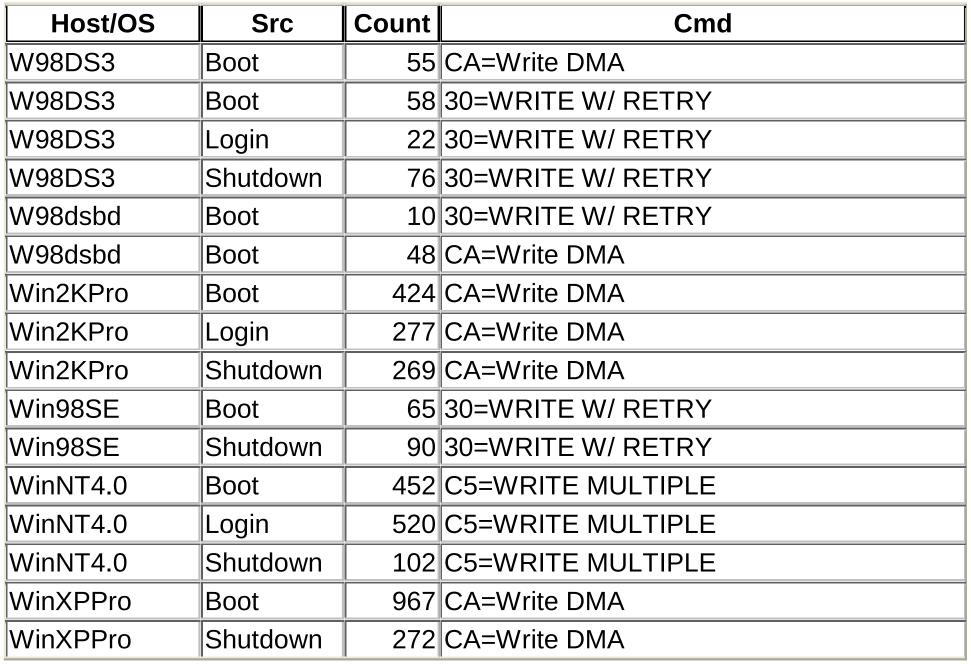
- The device forwards the command to the hard drive.
- The blocking device substitutes a different command
- The device simulates the command
- If a command is blocked, the device may return either *success* or *failure* back to the host
- Present the drive as a read-only device
- May issue commands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

Write Commands Issued by OS (Unix)



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 Commands Issued by OS (MS)



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

Notable Blocker Behaviors

- allow the volatile SET MAX ADDRESS, block if non-volatile
- cached the results IDENTIFY DEVICE
- substituted READ DMA for READ MULTIPLE
- allowed FORMAT TRACK
- Depending on OS version, might no 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 Standards
susan.ballou@nist.gov