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.
<table>
<thead>
<tr>
<th>Host/OS</th>
<th>Src</th>
<th>Count</th>
<th>Cmd</th>
</tr>
</thead>
<tbody>
<tr>
<td>FreeBSD5.2.1</td>
<td>Boot</td>
<td>196</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>FreeBSD5.2.1</td>
<td>Boot</td>
<td>1</td>
<td>30=WRITE W/ RETRY</td>
</tr>
<tr>
<td>FreeBSD5.2.1</td>
<td>Shutdown</td>
<td>104</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>RH7.1</td>
<td>Boot</td>
<td>759</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>RH7.1</td>
<td>Login</td>
<td>166</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>RH7.1</td>
<td>Shutdown</td>
<td>297</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>RH9PD.1</td>
<td>Boot</td>
<td>763</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>RH9PD.1</td>
<td>Login</td>
<td>186</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>RH9PD.1</td>
<td>Shutdown</td>
<td>402</td>
<td>CA=Write DMA</td>
</tr>
</tbody>
</table>
## Write Commands Issued by OS (MS)

<table>
<thead>
<tr>
<th>Host/OS</th>
<th>Src</th>
<th>Count</th>
<th>Cmd</th>
</tr>
</thead>
<tbody>
<tr>
<td>W98DS3</td>
<td>Boot</td>
<td>55</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>W98DS3</td>
<td>Boot</td>
<td>58</td>
<td>30=WRITE W/ RETRY</td>
</tr>
<tr>
<td>W98DS3</td>
<td>Login</td>
<td>22</td>
<td>30=WRITE W/ RETRY</td>
</tr>
<tr>
<td>W98DS3</td>
<td>Shutdown</td>
<td>76</td>
<td>30=WRITE W/ RETRY</td>
</tr>
<tr>
<td>W98dsbd</td>
<td>Boot</td>
<td>10</td>
<td>30=WRITE W/ RETRY</td>
</tr>
<tr>
<td>W98dsbd</td>
<td>Boot</td>
<td>48</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>Win2KPro</td>
<td>Boot</td>
<td>424</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>Win2KPro</td>
<td>Login</td>
<td>277</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>Win2KPro</td>
<td>Shutdown</td>
<td>269</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>Win98SE</td>
<td>Boot</td>
<td>65</td>
<td>30=WRITE W/ RETRY</td>
</tr>
<tr>
<td>Win98SE</td>
<td>Shutdown</td>
<td>90</td>
<td>30=WRITE W/ RETRY</td>
</tr>
<tr>
<td>WinNT4.0</td>
<td>Boot</td>
<td>452</td>
<td>C5=WRITE MULTIPLE</td>
</tr>
<tr>
<td>WinNT4.0</td>
<td>Login</td>
<td>520</td>
<td>C5=WRITE MULTIPLE</td>
</tr>
<tr>
<td>WinNT4.0</td>
<td>Shutdown</td>
<td>102</td>
<td>C5=WRITE MULTIPLE</td>
</tr>
<tr>
<td>WinXPPro</td>
<td>Boot</td>
<td>967</td>
<td>CA=Write DMA</td>
</tr>
<tr>
<td>WinXPPro</td>
<td>Shutdown</td>
<td>272</td>
<td>CA=Write DMA</td>
</tr>
</tbody>
</table>
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 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 Standards
susan.ballou@nist.gov