To: T13 Technical Committee
From: Rob Elliott (elliott@hp.com) and Jeff Wolford (jeff.wolford@hp.com), HP
Date: 16 April 2010
Subject: f10114r0 ACS-2 Remove SANITIZE FREEZE LOCK EXT

Revision history
Revision 0 (16 April 2010) First revision

Related documents
Revision 0 (16 April 2010) First revision

Revision 2 (16 April 2010) First revision

Revision 0 (16 April 2010) First revision

Overview
Using the Security feature set to purge drives (NIST SP800-800 terminology) presents numerous obstacles:

a) Many users do not want to use drive passwords. Passwords interfere with booting, recovery from sleep states, etc.

b) If the master password is set to a random value by rogue software, the drive becomes a brick (unusable for reads and writes forever);

c) Sending the SECURITY FREEZE LOCK command prevents rogue software from bricking drives, but also prevents running the SECURITY ERASE UNIT command;

d) BIOS and OS support for passwords and freeze lock is inconsistent and usually incomplete. They do not consistently send SECURITY FREEZE LOCK to all drives in all cases;

e) Drive preservation or (lack of) the frozen state through COMRESETs with and without SATA Software Settings Preservation enabled is inconsistent.

Users have struggled to figure out ways to bypass security freeze locks to get SECURITY ERASE UNIT to work - one example is http://cmrr.ucsd.edu/people/Hughes/HDEraseReadMe.txt:

Q: How can I bypass security freeze lock?

A: Three different ways can bypass a BIOS security freeze lock:
1. Most preferred method: If another computer is available, boot the drive from another computer. Since the freeze lock is entirely BIOS dependent, another computer's BIOS may not freeze lock the drive.

2. Second method: Switch the drive to another drive channel or another position on the channel, e.g. Switch drive from secondary master S0 to secondary slave S1 or vice versa. Some BIOSs do not send the Freeze Lock command to all channel master/slave positions.

3. Least preferred method: **There exists some danger to your drive in using this method, use at your own risk**. Shut down the computer system. Unplug the four-wire power cable of the hard drive while leaving the signal cable plugged in. To eliminate the danger of ESD, always ground yourself when removing the power cord. Power on the system and boot into DOS with a DOS boot disk. Once DOS has booted up and you are at a command line interface plug the power cord of the hard drive back in.
Run HDDerase.exe. The logic in this method is to prevent the drives detection in BIOS, which is when the freeze lock command is issued.

A proposal to allow SECURITY ERASE UNIT in the frozen state was rejected by T13 in June 2005.

The Sanitize Device feature set (new in ACS-2) should avoid all of these issues, but the final version of the proposal (e09197r4) ended up including a SANITIZE FREEZE LOCK EXT command and thus suffers from several of them.

SANITIZE FREEZE LOCK EXT should be removed before ATA-ACS2 is published (e.g., as a letter ballot comment resolution). Reasons include:

a) A sequence of WRITE commands can already erase all user data on the drive;
b) An SCT WRITE SAME command can already erase the entire drive in one command;
c) SCSI's FORMAT UNIT command has existed for many years without causing problems. If FORMAT UNIT is interrupted by a power cycle, the drive reports format corrupt after power on and requires another FORMAT UNIT command to complete the process - similar to how sanitize operations work;
d) T10 has directed that the SCSI version of Sanitize Device be implemented as enhancements to the FORMAT UNIT command, which has no facility for freeze lock;
e) An ATA device behind a SAT-3 SATL will not be able to receive freeze lock requests from applications since there will be no SCSI equivalent concept. In the Microsoft Windows operating system, for example, applications speaking to devices behind Storport drivers won't know anything about it. The SATL will still need to handle and report errors if the ATA device somehow reaches the frozen state;
f) The Sanitize Device CRYPTO SCRAMBLE EXT command will probably complete very quickly, so there is no guaranteed “oops” time to turn off power and save some of the contents;
g) BIOSes and OSes are certain to be inconsistent about sending SANITIZE FREEZE LOCK EXT and providing controls to do so or not do so, causing user confusion and consternation;
h) If BIOSes avoid sending SANITIZE FREEZE LOCK EXT, the user’s ability to purge the drive will still be at the mercy of inconsistent OS drivers;
i) SATA devices are likely to have inconsistent SATA Software Settings Preservation behavior. SATA 3.0 does not mention the Sanitize Frozen state, but does have some rules affecting Security Freeze Lock; implementations will probably differ on porting over those rules;
j) Rogue software could send SANITIZE FREEZE LOCK EXT to inconvenience the user (requiring a hardware reset to be able to purge the drive).

**Suggested changes to ACS-2**

Delete all references to SANITIZE FREEZE LOCK EXT and the Sanitize Frozen state, including:

a) Section 4.22 (Sanitize Device feature set) mentions of them
b) Section 4.22 Figure 15 (Sanitize Device State machine) state SD1 and associated text
c) Section 4.23.10 (Security feature set Security states) Table 10 (Security Command Actions) reference to the command
d) Section 7.43.1 (Sanitize Device) Table 49 reference to the command
e) Section 7.43.5 (SANITIZE FREEZE LOCK EXT)
f) Section 9.3 (Error Outputs) Table 157 reference to the command