Technical Proposal on ATA Secure Erase

Gordon Hughes+ and Tom Coughlin*
+CMRR, University of California San Diego
*Coughlin Associates

Introduction and Summary

Secure erase "SE" is defined in the ATA specification and implemented in all recent disk drives (greater than 15-20 GB), tested by the Center for Magnetic Recording Research at UCSD. All such drives tested at CMRR perform normal Security Erase, not the optional Enhanced Security Erase command. SE is part of the Security Feature Set, called Security Erase. Secure erase execution is currently denied by a drive if the Freeze Lock ATA command has been invoked, which is done during boot-up by many computer BIOS chips. SE is on the ATA Freeze Lock Abort Command List. This prevents malicious attacks via the SE command, but it also prevents a legitimate SE. A malicious attack can erase user data by block writes, as Norton Wipe Info and other erase utilities demonstrate. These software utilities are themselves attackable and thus provide only moderate erase security. The drive SE command is eight times faster than block writing in CMRR tests and will not report success if any user logical address is not erased. But under Freeze Lock, a user cannot securely erase his data when releasing a drive from his physical control. Even the CMRR Freeware DOS utility cannot run because the BIOS boots first.

This proposal discusses methods to allow a legitimate security erase command to be issued by an operating system or by an erase utility. One method is to provide attack protection via the existing ATA password system, by modifying the ATA specification to allow SE to be enabled under Freeze Lock if a User password has been set at Maximum security. This would allow a user to set such a password via BIOS Setup, and to then run a SE utility or use an O/S SE command.

However, operating systems can provide attack security and should be able to execute a secure erase command without a drive User Password set.. The password method above does not appear to allow this, because an O/S issued Set Password command is aborted under a BIOS-issued Freeze Lock state. One possible solution is for computer manufacturers to chose not to have a BIOS-issued Freeze Lock, and to handle SE security internally (such as via Trusted Computer Group methods). Another method discussed below uses the Master Password feature for O/S SE.

The current ATA specification for Normal Erase mode states that the SECURITY ERASE UNIT command shall write binary zeroes to all user data areas. This level of erasure is excellent for fast erasure of user data, but is not literally the triple write in Federal document DoD 5220. This document permits erasure of Secret user data, if all data locations ever accessible by users are overwritten by '00', by '11', then by random data patterns and verified. CMRR argues that Normal ATA SE erasure security is equal to DoD 5220, because drives recent enough to have the Security Feature Set also have bit randomizers in their PRML read channels. The write verify function is accomplished via drive write fault detection. The fast speed of ATA SE and its in-drive security against malicious attack gives it higher security than block write software utilities doing DoD 5220 triple writes. They can take days to complete, leading to Government concerns that many users will abort before completion.

Additional modifications are proposed to the present optional ***Enhanced*** Security Erase command, to give it the highest level of erasure security in Federal document 5220.22M.

Proposed Modification to the ATA Specification on Security Freeze

Allow SECURITY ERASE and its SECURITY ERASE PREPARE COMMAND to be executable in SECURITY FREEZE LOCK, if issued via a secure password. This can be accomplished by removing SE from the abort command list (Table 10), if the security system has been enabled by setting a User password at Maximum Security, or if a Master password is set and a SE command is issued with the correct Master password. Specifically, in Table 10 Security mode command actions:

- Change SECURITY ERASE PREPARE and SECURITY ERASE from ABORTED to EXECUTABLE in Frozen state, if the Security System is enabled at Maximum Security or the Master password is supplied.

Note that the SECURITY ERASE UNIT command (8.44) presently requires a Master password, or a User password if one is set (Table 48). The malicious attack issue arises if no User password has been set. Enabling SE via the Master password allows computer manufacturers to give their customers convenient SE ability, without the need to use BIOS Setup to set a User password. A unique Master password could be set into a drive during computer assembly, and used for a SE command under O/S security (for example, by a Windows Administrator).

Proposed Modifications to the ATA Specification on *Extended* Security Erase

Currently, the ATA specification states: *"When Enhanced Erase mode is specified, the device shall write predetermined data patterns to all user data areas. In Enhanced Erase mode, all previously written user data shall be overwritten, including sectors that are no longer in use due to reallocation. This command shall disable the device Lock mode, however, the Master password shall still be stored internally within the device and may be reactivated later when a new User password is set.*

To allow secure erase of the most sensitive user data, minimum mandatory properties of a Enhanced Secure Erasure algorithm should be defined. CMRR specifies a minimum of two random data writes of all physical user sectors offset off-track opposite to each other (including attempts to write reassigned sectors). The number of physical sectors not successfully written should be reported, and whether any reassigned sectors could not be written. The in-drive SE command verifies that each block is written, an equivalent level of security to the DoD 5220 requirement to read verify of the final data write. This enhanced SE would take twice as long to complete as Normal SE, but still be far faster than DoD 5220 triple block writes with verify.

Some of the reserved bits in IDENTIFY Word 128 could be used to specify the version of enhanced SE supported; the SE command 'na' byte outputs in section 6.44.5 could be used to report the number of non-defective physical sectors not successfully written; and whether any reassigned sectors could not be written[1] There are also reserved bits in word 128 that could be used to specify a Enhanced SE version number. Table 38 and the text above it specifies the mandatory use of SE and User & Master passwords, and the optional Enhanced SE.

Suggestions:

- Also modify the Identify Device command to indicate drives that support SE under Freeze Lock with User or Master Password
- Consider identification flexibility to specify new SE algorithms and SE Extended command options to specify the algorithm desired.
- Extend error reporting on SE so that unerased sectors are reported and optionally ignored. This may be negotiated with the HDD during the SE, or it may be an aspect of the algorithm chosen.
- Enable operating systems such as Windows and Linux to issue SE and SE extended commands, just as they can now execute block erase algorithms
- As a goal, be able to SE the C drive the O/S is running on.
- Allow Microsoft Windows Setup to be able to SE drives.

Security Implications of Specification Changes to Allow the Secure Erase Command

CMRR believes that security against malicious attacks with Secure Erase are better than with current block erase technology. It is easy to overwrite blocks on a disk drive, but the in-drive secure erase command can be restricted to O/S protected use via ATA passwords, as described above.

An Existing Secure Erase Utility - The CMRR Secure Erase Freeware Utility

User data erasure can presently be accomplished by running data erasure utilities such as the freeware “HDDerase” from CMRR at UCSD (http://cmrr.ucsd.edu/ click on “Storage Systems”). It offers five offers several erasure options. If the drive SE command is aborted by a BIOS Freeze Lock, the utility offers single random and 5220 block write erase.

A full secure erase can require more than an hour to complete with today's high capacity disk drives.. This time can be avoided by at a lower erasure security level by ***Fast Erase***, which locks a drive against data access until a new drive user completes a secure erase of the former user's data. Fast erase is done by issuing a standard “set user password" command to a ATA drive, with a randomly selected 256-bit user password and setting drive security to ”Maximum” This command completes in milliseconds, leaving the drive locked with a secure password. Note that such hardware-based password security is higher than software-based passwords because each drive Unlock command takes a random number of milliseconds of disk revolution delay to verify, and only 3-5 Unlock attempts are allowed before the drive locks itself against additional attempts. When a new user acquires the Locked drive no data access commands will be accepted until a secure erase command is issued and completed. The CMRR Freeware utility HDDerase offers this option. Fast erase prevents access to data on discarded hard disk drives while allowing

[1] ATA7 6.17.65 & IDENTIFY Table 16 Word 128 show the IDENTIFY bit that specifies whether Security is supported (in which case SE support is mandatory) and the bit that specifies if Enhanced SE is supported. The SE command Normal Outputs in 6.44.5 has several unused 'na' bytes.

them to be available for resale, return to vendors, or donated. Full secure erase does have higher security than Fast Erase against exotic computer forensic attacks which bypass the ATA interface, or transfer the drive firmware from an non-passworded drive, or disassemble drives. Nevertheless, Fast Erase is far better than the common situation of no user erase at all..

Five drive erase choices are provided in the UCSD freeware utility:
1) Secure Erase Unit: the ATA internal drive Secure Erase command.

- The highest level of Secure Erase.
- Can take 10-60 minutes depending on drive capacity and rpm.
- Program reports estimated time to complete secure erase
- Program reports whether Secure Erase successfully completes.

2) Multi-pass. Passes of three overwrites by zeros, ones and random data.

- Performs "DoD 5220" erase, a lower security level
  - see section *Revising DoD 5220 for modern disk drives*
- Can take eight times as long as Secure Erase, for each triple pass and verify
- User is prompted to enter number of triple passes desired.

3) Fast Erase. Puts a random 256-bit password on drive in milliseconds,

- locks the drive against future data access until next drive user executes a Secure Erase command which completes successfully.
- Has an intermediate level of erasure security.
- CMRR utility can be later used to Secure Erase the drive and leave it unlocked.

4) Single-pass overwrite. New fast DoD erase candidate for modern drives.

- Overwrites all data on the drive with random data bits.
- Similar level of erasure security as multi-pass overwrite (option # 2) but executes 3X faster.

5) Multi-pass overwrites with final random data write verify.

The CMRR program tests whether the drive is new enough to support the ATA Security Feature set, which allows method 1) and method 3), and notifies the user if Secure Erase is not supported by the selected drive (this may be the case for ATA drives more than several years old, generally < 10-15 GB). It detects and warns if BIOS has issued Freeze Lock. Method 2) has universal applicability but has the longest execution time and provides less security.

Notes:

- If Secure Erase command execution is interrupted before completion, drive will be left in locked state. In order to access the drive the user must run the utility program again after reboot to successfully execute Security Erase and unlock the drive for a new use.
- After Fast Erase, HDDErase.exe can be run to Secure Erase drive and leave it unlocked and empty.
- The Windows Disk Management system program can be used to partition and format an erased disk for reuse.
- A Secure Erase must wipe the entire drive - otherwise user data could be left on O/S page files and in slack or free space.
- Maximum drive capacity for multi-pass overwrites is 2 Terabytes.
- The utility will only run from a DOS floppy or CD-R, not from a Virus.

Block overwrite erase: revising DoD 5220 for modern disk drives

The Federal Government National Industrial Security program (DoD 5220.22-M, January 1995) authorizes hard disk drives to be erased by ‘writing all addressable locations with a character, its complement, then a random character.” This block write overwrite is authorized up to Secret data, but not Top Secret.

The in-drive secure erase command has significantly higher security than any block overwrite method such as DoD 2550. The block writes have to be executed by software programs, which are more vulnerable to cracking and spoofing than disk drive hardware SE, which will simply not report a successful SE if any user accessible block is not properly erased.

Moreover, disk recording technology has changed from the simple peak detect read channels used when 5220 was written. Modern drives (capacities over one gigabyte) use partial response read channels, with bit scramblers that randomize all user bit patterns before they are magnetically recorded on disks. Writing a character, then its complement, then a random character (as 5220 instructs) today just writes three random characters. Although three writes could conceivably be more secure than one or two, technology testing done at CMRR shows that the most secure erase is with two passes, each written ***offtrack*** in opposite directions (see “Secure Erase of Disk Drive Data” IDEMA Insight Magazine, Spring 2002). This is not possible by block write software, but can be implemented by drive designers, using the existing ATA enhanced secure erase command.

Background information on the need for Secure Erase

Computer data storage devices are designed for maximum user data protection. Such protection includes protection against accidental erasure, using “recycle” folders and unerase commands. Drives use elaborate error detection and correction techniques to never return *incorrect* user data. All this means that unrecoverable file erasure is an abnormal situation.

Consequently, user data usually remains stored on disk drives when they are discarded from PCs or from large enterprise systems, transferred to another user, or returned off lease. Even if users “delete” their files, they can be recovered from “recycling” folders or by special programs such as Norton Unerase (since the actual bits of information that comprise the files have not been overwritten, only the file directory has been changed).

Data left on disk drives can fall into the hands of others. Beyond theft of computer disk drives, data can be easily recovered from discarded or sold disk drives. There is a long history of personal information turning up on used hard drives, raising concerns about privacy and identity theft.

Gartner Dataquest estimates that 150,000 hard drives were "retired" in 2002. Many of these drives are thrown away, but a significant percentage find their way back onto the market.

In 2003 two students at MIT (Simson Garfinkel and Abhi Shelat) reported in newspapers worldwide and in the journal IEEE Security & Privacy, that they bought 158 used hard drives at secondhand computer stores and on eBay. 129 of these drives were functional. 69 of these still had recoverable files on them and 49 contained "significant personal information" including medical correspondence, love letters, pornography and 5,000 credit card numbers. One even had a year's worth of transactions with account numbers from a cash machine in Illinois. In 2002 Pennsylvania sold used computers containing information about state employees. In 1997, a Nevada woman bought a used computer and found it contained prescription records for 2,000 customers of an Arizona pharmacy.

The need for SE eradication of user data arises in:

Mainframes and storage networks

- When a user releases storage, a drive transfers to a new user or storage server, is removed for maintenance, or returned from lease.
- Storage devices are re-configured for other uses or users, for instance in expiring leased data storage facilities at an SSP or data center
- A RAID drive backs up data to a hot spare

Individual user PCs and workstations

- A computer (and hard drive) is replaced by a newer machine and the older machine is discarded or sold (often by computer stores via eBay).
- A project is completed and the data must be purged to protect “need to know” or to prepare the drives for new users or applications.
- When a user departs an organization and either leaves sensitive/personal data on the computer or may take the computer (and the organization’s data) with them.
- When a drive is to be returned to a drive manufacturer or a drive repair facility after a drive failure or near failure (for instance upon a SMART drive replacement after imminent failure is determined.
- Data on a drive must be erased to protect digital content from unauthorized access
- A virus has been detected and all possible traces of the offending code must be eliminated.
- An extreme virus or hacker attack where it is desirable to completely erase the data on some disks and reinstall back-up data

Consumer Electronics Applications

- Digital content owners may wish to use Secure Erase to thoroughly erase accessed content after the contracted period
- It may be desirable to use secure erase to eliminate unlicensed content