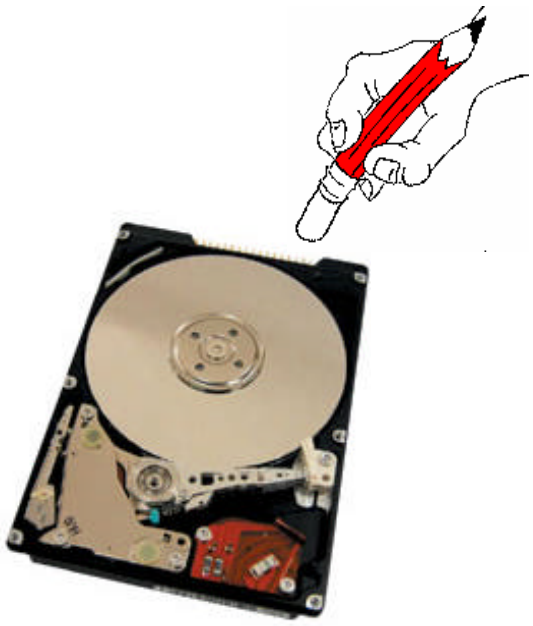
Secure Erase Newsletter



A Periodical Newsletter on Secure Erase and Data Recovery for Hard Disk Drives

September 2004, Volume 1a
(Revised)

Contents:

Interview with Gordon Hughes, Associate Director of CMRR, UCSD on the Secure Erase Initiative

Q: What is secure erase?

Secure erase is a means of erasing all data on a disk drive so the original user can be certain that it cannot be recovered, including data on reallocated blocks on the drive.

It's electronic data shredding, and allows a user to safely sell or donate an old drive.

Q: Why should people be interested in secure erase?

Because used drives are a source of data loss and data theft. When a disk drive leaves the physical control of its original user, his data is still on the drive and available to anyone. Even if the drive has been reformatted or its data has been protected, security systems can be overcome and the data recovered. The only way to ensure that data on a used drive can't be recovered is a securely erase.

Gartner Dataquest in 2002 projected that 150,000 hard disk drives were "retired." In 2003 Garfinkel and Shelat, from MIT reported in newspapers worldwide and in the IEEE

Journal of Security and Privacy[1] easy recovery of significant personal and confidential data from158 used hard disk drives that they bought at computer stores and on e-Bay. They found "significant personal information on 49, including medical correspondence, love letters, pornography, and information on 5,000 credit cards. One drive had bank account numbers from an ATM machine in Illinois. Prior reports found that Pennsylvania had sold computers with state employee information on them 2002 and in 1997 an Arizona pharmacy sold a computer containing 2,000 customer's prescriptions on it. Clearly the data on non-erased computers poses a significant threat to privacy!

Q: What is DoD 2550?

DoD document 2550.22M is the most widely quoted government document for erasure of classified data from computer storage devices. Issued in January 1995, it is now somewhat out of date. For erasure of Secret user data, it calls for all data locations ever accessible by users to be overwritten by '00', its binary complement 'FF', and a third random data pattern, which is read verified. Drives Physical destruction or magnetic degauss is required for Top Secret data or above, partly because of possible unerased data bands remaining between drive tracks and partly from risk of malicious software attacks. Such attacks can modify a block overwrite utility to report success but not actually overwrite. Block overwriting provides moderate erase security, but doesn't always erase an entire disk, doesn't erase reassigned (G-list) blocks, and does not always verify erasure. Block erase is also up to eight times slower than ATA Secure Erase.

Q: How do I do a "secure erase" on my drive before disposing of it?

There are several utility "block write" programs that can be purchased, such as Norton Wipe Info with Government Wipe, SCSI Toolbox's DataScrubber, Summit Computer Hard Disk Scrubber, Jetico Inc.'s BCWipe, LSoft Technologies Inc.'s KillDisk Pro, and Nortone.

CMRR offers a freeware downloadable utility as well as information on our secure erase work at http://cmrr.ucsd.edu (click on "Storage "Systems"). It uses the internal secure erase command available on most disk drives, which is fast and secure. Drives internally optimize the secure erase process, and are highly resistant to malicious attacks. Only a few specialized (and expensive) computer forensics companies are able to modify or bypass drive internal code.

The CMRR Secure Erase utility HDDerase.exe offers up to six choices of erasure methods, including DoD 5220 and fast in-drive erase. The utility can be run off a DOS floppy boot disk or a bootable CD-R. Its program erase options are: HDD SE, Fast Erase (password drive with 32-byte random string), and block overwrite (DoD 2550 triple; new CMRR single pass overwrite; and block overwrite with verify)

[1] S. Garfinkel, A. Shelat, "A Study of Disk Sanitization Practices," IEEE Security and Privacy, January-February 2003

The HDDerase.exe software checks to see if the Secure Feature Set is supported and whether the drive is locked or frozen. If it is locked it asks the user for the HDD password. Some computer BIOS chips prohibit SE, which allows only the block overwrite options.

Q: Do all drives support secure erase?

CMRR tested many ATA interface drives, from a few hundred megabyte capacity to hundreds of gigabytes. We found that All ATA drives less then 3-4 years old (more than 15-20 GBytes) support secure erase. No SCSI drives tested support secure erase.

Q: Why do ATA drives support secure erase, but not SCSI drives?

The theft vulnerability of notebook and laptop computers led drive makers to put a security system into the standardized specifications for ATA drives. This system allows users to set a password on their notebook drives. Secure Erase is a mandatory part of this ATA security system. The T-10 SCSI specification committee also put an (optional) secure erase command into their specification. SCSI and Fibre Channel drives are often used in array configurations where the data is striped across multiple disk drives and perhaps for this reason SCSI customers haven't asked their drive suppliers to include secure erase. CMRR disagrees with this analysis however. In transaction processing systems, user data records can be smaller than one disk sector so un-erased information on SCSI and Fibre Channel disk drives can pose a threat to privacy and security of data on returned and used drives. System designers do pay considerable attention to user data security in high-end enterprise systems, but perhaps not beyond the point where drives are physically removed..

Q: How many times must a drive overwrite data to erase it to the point that it cannot be recovered?

Experimental testing at CMRR on drives with secure erase demonstrates that a single verified write pass with a random data pattern makes all original data unrecoverable (see the resources on the CMRR website). Drives randomize user data before magnetically recording, so the zeros data pattern in the ATA specification meets DoD 5220. This random write takes place on all drive user data sectors as well as re-allocated sectors (the G-list sectors), in order to ensure that no user data "echoes" remain on disk (such as O/S page files, crash recovery files, or free space from deleted or modified files). For higher erasure security, Enhanced secure erase (see below) is superior to multiple pass erase. External block erase passes cannot erase track edges and data between tracks, as Enhanced SE can.

Q: What is fast erase?

Fast erase implements the secure erase command with a random 256-bit drive password invoked. The power is turned off the drive after secure erase begins. This takes only milliseconds. The next time that power is turned on the drive will either be locked against

any user data access, or until it completes the secure erase. Thus after initiating a fast erase the drive can be sold or transferred and the data on the drive can be assured of being relatively secure. (however see the Vogon story below). The drive can be reused, after the new user allows a SE to complete. The CMRR SE utility can be used for this.

Q: What is Enhanced Secure Erase?

For maximum erasure security for user data having high sensitivity requirements established by law, off-track writing is necessary. This can only be done by incorporating the operation into disk drive internal designs. The existing "Enhanced security erase" command presently in the ATA specification could be used (it is not implemented in today's drives). Some of the magnetic recording issues involved are that random data overwriting is most resistant to exotic recovery technologies,[2] but a low frequency overwriting data pattern erases more thoroughly than random data. Low frequency creates a broader erase field that more effectively writes over entire tracks and their possible erasure bands between tracks. DoD 5220 attempted to cover this by requiring a data zeros overwrite. But this is no longer valid because modern disk drives randomize user data before magnetic recording. User data zeros become random patterns on disk. To keep the benefits of random data overwrite but also positively erase track edges, CMRR requires a minimum of two random data writes of all user record ever accessible, offtrack in opposite directions. The two random writes provide the erasure level security of a low frequency write, and writing offtrack also erases possible track edge data.

The CMRR minimum requirement for Enhanced secure erase is a two pass random overwrite performed with the write heads slightly offset to the sides of the data tracks during each writing pass, by 5-10% of the track width.. Drives have long had offtrack capability, but only controllable internally. Each offtrack erase pass requires the same time as the existing Normal secure erase, which can take up to an hour. Experimental CMRR testing shows complete erasure by the existing Normal SE process[2], and that offtrack magnetization is random noise not requiring track-offset erase passes. CMRR has therefore qualified Normal secure erase with security level of equivalent to DoD 5220 triple pass overwrite, and with significantly higher malicious attack security.

Enhanced secure erase is proposed to qualify for Federal Government erasure requirements for data above secret and CMRR is currently working to prove this.

Q: Can secure erase be made a part of Microsoft Windows, Unix/Linux, and Apple Macintosh operating systems, to be more convenient for the public?

Making the Secure Erase utility available at CMRR is intended to encourage more widespread SE use and its incorporation into popular operating systems. We have written articles in journals and magazines and encourage additional publicity. CMRR is also working with Microsoft, the ANSI T-13 committee and other standards bodies to make it easier for people to access and use the secure erase commends.

---

[2] G. Hughes, T. Coughlin, "Secure Erase of Disk Drive Data" IDEMA Insight Magazine, Spring 2002

Secure Erase Improvement Being Considered by ANSI Standards Committee

In April 2004 Dr. Gordon Hughes from CMRR, accompanied by Thomas Coughlin of Coughlin Associates attended the ANSI T-13 Committee meeting in San Jose. This committee creates standards for the ATA interface specification for personal computer storage connections as well as lower performance enterprise applications and consumer devices.

Gordon presented a proposal to the T-13 committee to remove secure erase from the Freeze Lock abort command list so that it can be implemented by secure erase utilities, by Windows, and by Unix/Linux. He requested that Table 10 in the current Version 6 specification on Security mode command actions should be changed.

- Change SECURITY ERASE PREPARE from ABORTED to EXECUTABLE, in Frozen state
- Change SECURITY ERASE from ABORTED to EXECUTABLE, in Frozen state

He pointed out that virus security with this approach will be the same as with block write secure erase (such as can be implemented today).

He also discussed a higher security alternative, that T13 make both commands executable only if a drive had an active user password set. After discussing the HDDerase.exe utility available as freeware from CMRR, Gordon described the differences between block erase as described in government document DoD 2550 and Secure Erase. Unlike block level erase Secure Erase also overwrites reassigned blocks and can be up to eight times faster (per CMRR tests). In addition the enhanced SE command qualifies for Federal Government secret data classification erasure.

CMRR tested 35 ATA and SCSI drives of various vintage for Secure Erase support. All recent ATA drives support secure erase (> 15 GB drives). In addition all four x86 system board ports and all command combos successfully secure erase. Fast erase was successful, using a power interrupt that leaves a drive locked until secure erase is completed. Interestingly, no SCSI drives tested implemented secure erase (optional in the T10 specification). We believe that all SATA drives will support Secure Erase. Gordon went on to show cases where significant amounts of private data has been reported recovered from used disk drives.

As a result of this presentation and subsequent discussions with Microsoft, Intel and other T13 member companies representatives a proposal is being created to modify the ATA version 8 so that Secure Erase can be implemented with all complying BIOS and operating systems. This effort is expected to take over a year to complete.

Update of DoD 5220 document for modern drives

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 internal

drive erasure is excellent and quick, although it does not precisely follow the existing government standard DoD 5220. CMRR verification testing shows that the erasure security is equivalent to DoD 5220 overwrite, because drives having the command also randomize user bits before storing on magnetic media. They verify the block writes via their internal write fault detection hardware, avoiding a separate read verify pass. This speeds execution time, increasing user willingness to secure erase drives. An in-drive command has higher security from malicious software attack. All computer software is vulnerable to attack, but hardware erase "hides" behind the standardized drive interface, rejecting any nonstandard commands. It is about eight time faster than the three block writes plus verify of DoD 5220. CMRR testing shows that multiple pass block overwrite utilities which attempt to meet DoD 5220 can take days to execute, in a drive that can internally Secure Erase itself in 30 minutes.

Vogon Breaks UCSD Fast Erase

CMRR challenged data recovery companies to break the Fast Erase protocol developed at UCSD. In Fast Erase the erase process is initiated by setting a random 256-bit user drive password at maximum security level. When power is reapplied to the drive the only command it will accept is a Secure Erase which must proceed until it completes for the drive to be reusable. Since this leaves user data on the drive until the Secure Erase completes, CMRR wanted to find out if advanced data recovery companies might be able to break the Fast Erase random password and recover data from the drive without erasure.

Vogon International accepted this challenge. CMRR sent them two identical 80 GB 2.5-inch laptop drives, one unlocked for their testing and the other with unique stored data locked with a random 256-bit password. The unique data was generated, recorded and stored on a computer not connected to any network. Within a few days, Vogon returned correct binary files of the unique data sectors.

CMRR contacted the drive manufacturer, who stated that their ATA security system had been improved over the years after such attacks, and that their entire data reading and password checking process was now inside a single read channel chip on this drive, which should have been very difficult to crack. So how was cracking done? Perhaps through "back door access" which stem from a drive manufacturer's needs to test and repair his drives, and to update his drive firmware (internal operating system). When a drive manufacturer receives a user drive for repair, he typically reloads the original factory firmware, thus erasing any user password that might block access. ATA and SCSI specs provide "Vendor Specific Commands" for such purposes, so possibly the firmware from the non-passworded drive was read out and reloaded onto the passworded drive. That would allow reading the unique data CMRR stored, but not the (now erased) password – and that password was in fact not read.

For More Information and For Subscriptions

This newsletter is provided free by CMRR at UCSD. To subscribe please fill out the form at http://cmrr.ucsd.edu/hughes/subpgset.htm. email: gfhughes@ucsd.edu.