

Secure Erase Q&A (CMRR at UCSD)

Q: What is secure erase?

A: The ANSI T-13 committee which oversees the ATA (also known as IDE) interface specification and the ANSI T-10 committee which governs the SCSI interface specification have incorporated into their standards a command feature known as **Secure Erase (SE)**. Secure erase is a positive easy-to-use data destroy command, amounting to “electronic data shredding.” It completely erases all possible user data areas by overwriting, including the so-called g-lists that contain data in reallocated disk sectors (sectors that the drive no longer uses because they have hard errors in them). SE is a simple addition to the existing “format drive” command present in computer operating systems and storage system software and adds no cost to hard disk drives. Since the Secure Erase command is carried out within a hard disk drive it doesn’t require any additional software to implement.

Q: Is secure erase approved for government security?

A: Secure erase has been approved by the U.S. National Institute for Standards and Technology (NIST), Computer Security Center¹. In general data erasure techniques when used alone are approved by NIST for lower security sanitization (less than secret) since the data can be recovered at least in theory. It should be noted though that a secure erased drive that is then physically destroyed would be extremely difficult if not impossible to recover data from. According to the NIST document Secure Erase as well as certain software utilities running in protected execution environments (e.g. running inside file system hardware like RAID arrays or inside secure computers) could be verified secure.

Q: Is any data left after a secure erase?

A: Investigations at CMRR at UCSD have shown that a single pass secure erase at lower frequencies results in no remaining data signals and a second erase reduces this signal only slightly more. The resulting data signal to noise ratio (SNR) at the magnetic drive head is below that required to recover data using a disk drive channel². The only recorded signal left in these experiments is a small amount of highly distorted track edge recording which is extremely difficult to recover data from even if the disk is removed from the drive and tested on a spin-stand.

Q: Is there a fast way to do secure erase?

A: an ATA disk drive user may want to do a "Fast Secure Erase" on a disk drive before disposing of it. ATA disk drives can have a user "password" that is used to access certain features of the disk drive. If a secure erase is started using a user "password" the disk drive must complete the secure erase before it accepting any other command. Even if SE is stopped before completion another user cannot acquire the drive and use the "password" to reactivate the disk drive. The SE must complete before the new user can access the drive.

¹ NIST Computer Security Resource Center, **Special Publication 800-88: Guidelines for Media Sanitization**, August 2006

² **Secure Erase of Disk Drive Data**, Gordon Hughes and Tom Coughlin, IDEMA Insight 2002, <http://www.tomcoughlin.com/techpapers.htm>

Secure Erase Q&A

(CMRR at UCSD)

Q: What is full disk encryption?

A: Recently 2.5-inch hard disk drives for laptop computer applications have been introduced that encrypt the recorded information within the hard disk drive—internal drive data encryption³. Such disk drives provide protection of the data on the disk drive should the laptop or drive be lost or stolen. Data encryption provides significant protection from forensic data recovery. Use of a key-based disk drive encryption technique opens the door to a new way to effectively “erase” the data of a hard disk drive by throwing away the encryption key.

Q: How can a user access full disk encryption

A: Full Disk Encryption (FDE) SE “secure erase,” (“FDE-SE”), is done by securely changing the internal drive encryption key to render encrypted user data on the disk⁴. This can be enabled via the Enhanced SE command in the existing ATA ANSI specs.

Q: What groups are behind full disk encryption?

A: An open industry standard for FDE is being worked on by the Trusted Computer Group (the Storage Working Group in trustedcomputinggroup.org). Drive members of the TCG include Seagate, HGST, Fujitsu and WD.

Q: What are the dangers of not sanitizing data?

A: If data is not eliminated beyond recovery on a disk drive that leaves the control of the original owner this data can and often does fall into the hands of others. Besides theft of computers and disk drives where data can be stolen data can often be recovered with little or no effort from discarded or sold disk drives. There are many reports of data being recovered from discarded disk drives⁵⁶. Each year hundreds of thousands of hard disk drives are retired. Some of these retired hard disk drives find their way back into the market and unless the data that they contain is eliminated securely it can be recovered.

Q: What are the various ways to sanitize data and what does each approach do?

A: UCSD CMRR has established and tested protocols for software secure erase⁷. Their security levels vary between the levels just discussed. Four basic security levels are defined, Weak erase (deleting files), block erase (external overwrite), Normal secure erase (current SE implementation), and Enhanced secure erase (see below). Block and Normal secure erase are intended for elimination of user data up to the Confidential level, and Enhanced secure erase for higher levels. The Enhanced level has recently been implemented in drives by Seagate,

³ E.g. Seagate Momentus 5200 2.5-inch hard disk drive

⁴ G. Hughes, “Wise Drives”, IEEE Spectrum, August 2002

⁵ T. Coughlin, **Rumors of My Erasure Are Premature**, Coughlin Associates, http://www.tomcoughlin.com/Techpapers/Rumors_of_my_erasure,061803.pdf (2003)

⁶ J. Garfinkel, A. Shelat, **A Study of Disk Sanitization Practices**, IEEE Security and Privacy, Jan.-Feb. 2003.

⁷ G. Hughes, **CMRR Protocols for Disk Drive Secure Erase**, cmrr.ucsd.edu/Hughes/CmrrSecureEraseProtocols.pdf

Secure Erase Q&A (CMRR at UCSD)

Fujitsu and Hitachi. These four erasure protocols exist because users make a tradeoff between the erasure security level and the erasure time required.

Q: Some data sanitization technologies take a lot of time, is that a problem?

A: A high security protocol requiring custom software and up to days to accomplish will be avoided by most users, making it little used and therefore of limited practical value. For example, DoD 5220 calls for multiple block overwrites for Confidential data, which can take more than a day to complete in today's drives. So users make a tradeoff between the time required to eliminate their data and the risk that the next drive user will know and use recovery techniques to access weakly erased data. For all but top-secret information and when time is critical, users will often turn to erasure that takes minutes rather than hours or days. They will select a method giving them an acceptable level of security in a reasonable time window.

Q: Does physical destruction of hard disk drives make the data unrecoverable?

A: The disks from disk drives can be removed from the disk drives, broken up and even ground to very fine pieces to prevent the data from being recovered. However, even such physical destruction is not absolute if any remaining disk pieces are larger than a single record block in size, about 1/125" in today's drives (Note that as the linear and track density of magnetic recording increases the resulting recoverable pieces of disk must become ever smaller if all chances of data recovery after physical destruction alone are to be thwarted). Pieces of this size are found in bags of destroyed disk pieces studied at CMRR². Physical destruction nevertheless offers the highest level of data elimination (although it is more effective if the data is first overwritten since then there is almost no potential signal to recover) because recovering any actual user data requires overcoming almost a dozen independent recording technology hurdles.

Q: Do multiple overwrites work better than a single overwrite:

A: Many commercial software packages are available using some variation of DoD 5220, some going to as many as 35 overwrite passes. Unfortunately the multiple overwrite approach is not very much more effective than a single overwrite since it does not do much to the remaining track edges where most of the very low level distorted remnant data remains after an overwrite and it takes a lot more time (even with 3 overwrites it can take more than a day to erase a large capacity hard disk drive).

Q: What are legal requirements for data elimination/sanitization?

A: There are several laws and regulations that relate to data retention and data elimination or sanitization on data storage devices such as hard disk drives. Some of the US requirements are listed below:

- Health Information Portability and Accountability Act (HIPAA)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Gramm-Leach-Bliley Act (GLBA)
- California Senate Bill 1386
- Sarbanes-Oxley Act (SBA)

Secure Erase Q&A

(CMRR at UCSD)

- SEC Rule 17a

There are several approved methods for data sanitization to satisfy these legal requirements or to meet other sometimes even more stringent corporate or government secrecy requirements. Some of these techniques will physically destroy the disk drives or prevent their being used again. Secure encryption of user data from creation to destruction is approved by some of the regulatory compliance legislation to protect sensitive information.