

Disk Drive Secure Erase for User Data

Summary: user data is left on disk drives removed from computers and storage systems, creating a data security vulnerability that few users are aware of. Complete eradication of user data off drives can be accomplished by running data erasure utilities such as the freeware “HDDerase” downloadable here, which offers four erasure options. Secure erase is implemented in all recent ATA drives tested by CMRR (greater than about 15-20 GB), but is optional and not yet implemented in SCSI drives tested. Secure Erasure takes ½-1 hour to complete. ATA drives also enable a “Fast Erase” in milliseconds, which may speed the acceptance of serial ATA drives in enterprise storage systems, in their competition with fiber channel/SCSI drives. Data encryption can also contribute an important level of security, but is vulnerable to cracking when done in computer software such as Windows.

Computer data storage devices are designed for maximum user data protection. This 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 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.

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

The elimination of unwanted data from a computer hard drive is not a simple task. Deleting a file merely removes its name from the directory structure while the data itself remains in the drive’s data storage sectors where it can be retrieved until the sectors are overwritten. Reformatting a hard drive clears the file directory and severs the links to file storage sectors, but the data can be recovered until the sectors are overwritten. Software utilities that overwrite individual data files (or an entire hard drive) are susceptible to error and require frequent modifications to accommodate new hardware and evolving computer operating systems. As a consequence, computer users, system administrators, security personnel and service providers can spend considerable time in an endless game of technology catch-up while trying to develop solutions for the above problems. As an example of vulnerability of traditional data security measures in the MIT study fifty-one of the 129 working drives in the had been reformatted, but 19 of them still contained recoverable data.

So what's a computer user or IT person supposed to do? Fortunately the common disk drive interface standards, ATA (also known as IDE) and SCSI

contain a 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 stops using for data because they have bit hard errors). SE is a simple addition to the existing “format drive” command currently present in computer operating systems and storage systems, and consequently adds little or no cost to drives. In addition security erase does not require any additional software to implement.

Encryption can provide an important level of user data security, but is vulnerable to cracking when done in computer software (by user application encryption or by Windows 2000 and XP O/S). Complete eradication of user data off drives offers an important additional security level, and can be accomplished in today’s drives with minimal erasure task overhead by using existing SE (commands in the SCSI and ATA standards. CMRR has run SE verification tests on over 35 drives, from 2 GB to today’s drives. We bought many of these test drives on eBay, and over 30% had previous user data. Secure erase is implemented in virtually all ATA drives but is optional in SCSI drives (and not yet implemented in any SCSI drives tested). This may give a competitive advantage for serial ATA drives in enterprise storage systems, in their competition with fiber channel/SCSI systems.

A full secure erase can be a lengthy process with today's high capacity disk drives, sometimes requiring more than an hour to complete. This time can be avoided by ATA disk drive **Fast Erase**, which locks a drive against data access until a new drive user completes a security erase of the former user's data. Fast erase is done by issuing a standard “set user password” 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 hardware-based security is higher than software-based 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 a drive power cycle is required to continue. When another user acquires the drive it will be locked against any data access commands until a secure erase command is issued and completed. The CMRR Freeware utility HDDerase can be downloaded to do this. This fast erase prevents access to data on discarded hard disk drives while allowing them to be available for resale, return to vendors, or donated. Full secure erase does have higher security against exotic data access attempts which bypass the ATA interface or disassemble drives. Nevertheless, fast erase is significantly effective.

Secure erase is required by the ATA Security Feature Set specification, although it is optional in SCSI. The new “serial ATA” drives will be able to advertise SE as a user feature, in their competition with SCSI and Fibre Channel drives for market share in low-end storage systems.