



Current Issue



- ▶ ARCHIVE
- ▶ SUBSCRIBE
- ▶ RENEW
- ▶ ADVERTISERS

- ▶ ABOUT MCD
- ▶ PROFILES
- ▶ CIRCULATION
- ▶ CALENDAR
- ▶ RATE CARD
- ▶ CONTACT US

TXTLINX
CONNECTION
INSTANT PRODUCT
INFORMATION

MILCOTS
NEW
DISCUSSION FORUM
DIGEST
JOIN NOW!



FEATURE ARTICLE

Security Erase: When Data Destruction Becomes Top Priority

By Jhay Gregorios, BitMICRO Networks.
September / October 2005

It goes without saying that data security is a matter of utmost concern to the military. In fact, several government agencies were born out of the need for data in support of national defense. There's the Central Intelligence Agency, whose main job is to provide national security intelligence to senior US policymakers, and the National Reconnaissance Office, on which national and military leaders rely to provide warning of potential military aggression, monitor weapons of mass destruction programs, track terrorists, enforce arms control and environmental treaties, and assess the impact of natural and man-made disasters.

Several laws have also been enacted to regulate the handling of sensitive data within the government. Among these is the Espionage Act in the United States, which declares a penalty "punishable by a \$10,000 fine and 20 years in jail for a person to convey false reports or false statements with intent to interfere with the operation or success of the military or naval forces of the United States or to promote the success of its enemies"¹. Gathering information about an entity is as important as making sure classified information remains so. There is a high premium that goes with information mainly because it is power in itself, and whoever possesses more of it has an advantage.

Currently, almost all electronic information is stored in computer hard drives. Unfortunately, technological improvements, and the industry of hacking and information theft have also grown exponentially so that information can be easily retrieved even after it has been deleted. A higher level of security is needed especially for electronic data-gathering equipment that is used in penetrating enemy territories.

There are greater intricacies involved in data security as applied to the military. For a better understanding, it helps to look at how data security has been implemented in the past and what technological improvements are available to the military in purging sensitive information from IT equipment.



Figure 1: BitMICRO's E-Disk flash drive solid-state disk.

Data Security Back Then

The art and science of protecting data is an old craft. It has graced several hundred pages in history books. Each

entity has developed its own way of collecting, transferring, storing, and protecting data depending on its needs. In the 1940s, the military used codes to inhibit the enemies from getting any information about its location and plans of attack even if it intercepts a communication. During that time, the use of double agents was common. In England, operatives feed their handlers false information about attacks in their own territory to lead them to a false war ground.

In 1954, US military intelligence adopted a new concept of data collection by implementing its airborne reconnaissance program. This time, aircraft began to be employed to cover enemy areas and collect as much information as possible for use by ground operations and defense analysis, as well as to enhance the ability to conduct offensive attacks. Eventually, a Special Communications Center based in Germany and Japan was established to facilitate a direct and timely response to military commands and other organizations receiving intelligence support.

In 1970, the increasingly hostile threat against aircraft under the Airborne Reconnaissance Program focused national emphasis on reducing manned reconnaissance flights in high threat areas. It heralded the beginning of Unmanned Aerial Vehicles (UAVs), and has resulted in advances to unmanned aircraft technology. More and more types of UAVs are entering service, and billions of dollars are being funneled into improving the most successful UAVs and micro-UAVs. Nevertheless, any UAV can crash, necessitating continued improvements in storage security such as “security erase”, because these accidents increase the risk of placing sensitive information in enemy hands.

The Current Scenario

Data recoverability in storage devices such rotational hard disk drives and DRAM-based solid-state disks² (SSDs) is relatively easy even for novice computer experts, thanks to advanced utilities such as VirtualLab Data Recovery 3.7.9, Restorer2000, and Norton Unerase. Even if users delete their files (whether intentionally or accidentally), it reality only file directory information has been changed. Data pertaining to the “deleted” files can be recovered from “recycling” folders, since the actual bits of information that comprise the files have not necessarily been overwritten.

Similarly, DRAM-SSDs, which because they provide volatile storage are considered very safe, may suffer from hysteresis³ effects for some time after the power is cut off. Hysteresis has the effect of allowing the disk’s original contents to be recoverable through clever means.

These obstacles can be overcome when using a flash SSD equipped with an advanced security erase technology, a good example of which is BitMICRO’s securErase (Figure 1). Flash SSDs use memory chips that are non-volatile. When power is applied to an E-Disk SSD during securErase, the process “charges” cells of the flash memory to a default bit pattern of 1111s or FFFFs, overcoming hysteresis quantum energy potentials. Traces of data are not recoverable right after the securErase process.

The securErase utility automatically cycles every location to completely erase all traces of the disk data. Unlike a conventional disk on which each area must be accessed sequentially, the flash SSD is all electronic and does not use any moving parts. Embedded firmware makes it possible to address whole columns of memory chips at once, speeding up the erase process. As an example, it takes securErase approximately 33 s per 16 Gbyte memory board (using 2048 Mb flash chips) to complete the erase process when using a default pattern of 1111s or FFFFs. However, the data on the SSD that keeps track of erase/write cycles per each block of flash memory is preserved to maintain integrity of the storage device’s wear-leveling features.

The securErase technology meets the remanence⁴ security requirements of the U.S. Department of defense, National Security Agency, Air Force, Army, and Navy (NISPOM DoD 5220.22-M, NSA 130-2, Air Force AFSSI 5020, Army 380-19, NISPOMSUP and IRIG-106). Sanitization procedures accommodated by securErase are shown in **Table 1**.

Aside from regulatory compliance, flash solid-state disks hold other advantages over hard disks with regard to security erase during combat scenarios. Erasure and reformatting of hard disks takes minutes. In addition, deleting files from a mechanical disk does not actually erase the data, as only the file allocation table (FAT) is being updated while the data remains on the disk. To erase disk data beyond recovery, each storage element must be cycled repeatedly five or six times, which takes a considerable amount of time.

securErase may be initiated via software (i.e., E-Disk Analyzer, low-level ATA or SCSI command, etc.) or through hardware (i.e., units with PowerGuard or specially-configured units without PowerGuard). Flash memory is designed to erase and program bits in bulk (hence the term “flash”), speeding up the security erase process.

The adoption of security erase technologies will become more widespread as military and business organizations realize the importance of protecting data. Information can make the difference between success and failure in the battlefield. As post 9/11 governments ramp up homeland security and intensify intelligence activities, secure erasure will become a major technology issue in storage research and development.

About the Author

Jhay Gregorios is the engineering manager and a 9-year veteran at BitMICRO Networks Inc. He is a graduate of the University of Florida College of Engineering with concentrations on biomedical engineering, business administration, and physics. He may be contacted at jhay.gregorios@bitmicro.com.

Notes

1. Wikipedia (http://en.wikipedia.org/wiki/Espionage_Act)
2. Wikipedia (http://en.wikipedia.org/wiki/Solid_state_disk)
3. Hysteresis is a property of systems (usually physical systems) that do not instantly follow the forces applied to them, but react slowly, or do not return completely to their original state. That is, they are systems whose states depend on their immediate history.
4. Remanence is the magnetization left behind in a medium after an external magnetic field is removed.

