DATA SECURITY IN SOLID STATE DISKS

Alan Fitzgerald
Chief Technology Officer
Adtron Corporation
Phoenix, AZ 85040

ABSTRACT
Solid state disk characteristics make them ideal for data collection in both harsh environments and secure telemetry application. In comparison to their magnetic counterparts, solid state disks are faster, more reliable, extremely durable and, with changing economies and geometries, more affordable and available in higher capacities than ever before.

This paper will discuss solid state disk storage, access controls, and data elimination in relation to various telemetry scenarios. The reader will be introduced to the operational considerations of solid state disk data security and the underlying technical concepts of how these are implemented.

KEY WORDS
Flash disk, solid state disk, secure erase

INTRODUCTION
Airborne data acquisition and rugged computing systems demand data storage devices with built-in features that ensure data security. An unprotected data storage device in these systems is vulnerable to virus attacks, network security assaults, enemy access to secret data, and potential misuse by trusted personnel. This paper delves into the qualities and characteristics of solid state disks in relation to data security issues with an emphasis on access control and data elimination.

Access control is not a new concept in the world of software applications, networking and web services. In embedded data storage applications, access control at the storage level is a relatively new and evolving concept. Physical and programmed dynamic protection of data is possible with the flexibility afforded by solid state storage.

Solid state flash disks allow fast elimination of data when a recording system is at risk of being compromised. The use of erase or sanitize operations quickly eliminates the data and leaves the flash disk reusable for recording. In a second or less, an electrical destruction function damages
the solid state memory to the point where the flash memory cannot be accessed and the flash disk cannot be reused. The operational environment dictates the use of the appropriate function.

The all electronic (no moving parts) characteristic of solid state disks make them ideal for data collection in harsh environments. In comparison to their magnetic counterparts, solid state disks deliver enhanced security, higher performance, greater reliability, significantly higher durability, greater packaging efficiency with more bits, less power, and lower weight per cubic centimeter. As a result of these benefits, many rugged computer systems incorporate flash disks instead of magnetic storage (tape or disk drives).

Figure 1 Flash Disk Capacity (based on industrial quality flash)
The capacity, price and performance charts illustrate the rapid change in high performance flash disk storage. These attributes have driven the aerospace industry to accept flash disks instead of hard disks in mission recording systems. With storage capacity demands growing, today a flash disk delivers one Terabyte (1TB) in a Mass Storage Unit (MSU) as small as 100mm H x 100mm
W x 200mm D, or 2,000 cubic centimeters, operates from -40 to +85 deg C, and requires only 20 Watts of operating power. These parameters make flash disks very attractive in already high density electronic systems, such as Unmanned Airborne Vehicles (UAV).

**DATA SECURITY FEATURES OF FLASH DISKS**

Data security features of flash disks include password or login access control, physical and commanded write protection, and rapid data elimination. When storing confidential, sensitive or secret data it is important to restrict access to the data, prevent accidental or unauthorized data overwriting, and in situations that risk system compromise, to eliminate or destroy the data.

Flash disks provide a range of data security features:

- Access control
  - Physical write protect
  - Password login
- Data elimination
  - Fast erase
  - Sanitize by multiple overwrites
  - Electrical damage

**ACCESS CONTROL**

It is common to have built-in access control in off-the-shelf hard disks which are programmed in-band (through the storage interface, e.g. SCSI, IDE or FC) for password or write protection. Flash disks offer the same access control methods through the storage interface with some offering a hardwired signal that enforces write protection regardless of the interface command.

Write protection is valuable to protect O/S boot images, read only mission data such as maps, and to protect against accidental overwrite during data analysis in the lab. To ensure boot image integrity, write protecting the boot disk prevents intentional and unintentional changes that can lead to system compromise and security breaches.

**WRITE PROTECT**

Two basic methods, commanded and physical, provide write protection of a solid state disk. Advantage and disadvantages apply to both methods. Write protection prevents unauthorized changes to operating system security features, alteration of program and data files, and system corruption due to errant system operation (software bugs). Through the use of the flash disk write protection feature, the integrity of the system does not have to depend on the write protection schemes of the operating system.
One implementation is to require the host computer to command the disk to block future write operations. In some systems, it is very convenient to allow the host to manage this function remotely as no user access to the flash disk is required and the user can execute it from software or a console. Because of the host ability to set or clear write protection it is not as fail safe as a physical jumper or switch on the disk.

The use of a physical write protection jumper or switch cannot be disabled by host command and therefore when set to write protect the disk is always protected until physically changed. With this method, remote attacks to the computer and write operations to the write protected disk will not alter the disk data.

**PASSWORD LOGIN**

Like a network login, a disk login is required before any access is granted to the user. Typically the login process executes through the storage interface (in-band), via the SCSI or SATA controllers. An alternate method is through an auxiliary port such as RS232 or USB. This out-of-band process can be a more secure path because it does not involve the host computer which might track and store this activity.

Password login provides a first level deterrent if the disk drive falls into enemy hands. Because all of the data is intact, the unauthorized user must first defeat this front end barrier by hacking or by replacing the protected storage controller then access the media with an alternate method.

**DATA ELIMINATION**

A significant concern within the Defense industry is the possibility of sensitive data falling into the hands of an enemy. While in the extreme case a compromised data storage device yields information that could result in loss of lives and mission through enemy awareness of the focus and depth of ISR (Information, Surveillance and Reconnaissance) gathering capabilities.

Elimination of data when a recording system is at risk of compromise is performed by rapid clearing or sanitizing of data. After a Clear or Sanitize operation the solid state disk is reusable. A physical destroy function damages the solid state memory and the solid state disk is not reusable. The operational environment dictates the choice of the appropriate function.

- Clear
- Sanitize
- Destroy

**GOVERNMENT REQUIREMENTS FOR SECURE ERASE**

In the effort to create national standards for data security in embedded computer applications, many countries have established data erasure standards for hard disks and flash disks. The table shown below describes the standards established in the United States. While they have differences of application, in principle the requirements focus on three basic processes:
<table>
<thead>
<tr>
<th>Agency</th>
<th>Specification</th>
<th>Device</th>
<th>Clear</th>
<th>Sanitize</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoD</td>
<td>NISPOM 8-306 DoD 5220.22-M 1995 Original</td>
<td>FEPROM</td>
<td>Perform a full chip erase as per manufacturer’s data sheets</td>
<td>Overwrite all addressable locations with a single character then perform a full chip erase as per manufacturer’s data sheets.</td>
</tr>
<tr>
<td>DoD</td>
<td>DOD 5220.22-M NISPOM Supplement 1</td>
<td>FEPROM &amp; EEPROM</td>
<td>Not specified</td>
<td>Overwrite all locations with a character, its complement, then with a random character.</td>
</tr>
<tr>
<td>NSA</td>
<td>NSA 130-2</td>
<td>EEPROM</td>
<td>Same as sanitize operation.</td>
<td>Overwrite all locations with a pseudo-random pattern twice and then overwrite all locations with a known pattern.</td>
</tr>
<tr>
<td>Army</td>
<td>AR 380-19</td>
<td>FEPROM &amp; EEPROM</td>
<td>Perform a full chip erase as per manufacturer’s data sheets.</td>
<td>Overwrite all locations with a random character, a specified character, then its complement.</td>
</tr>
<tr>
<td>Navy</td>
<td>NAVSO P-5239-26</td>
<td>EEPROM</td>
<td>Erase per manufacturer’s specifications</td>
<td>Erase, program all locations with a random pattern, wait 2 minutes, erase, program all locations with another random pattern, verify the random pattern</td>
</tr>
<tr>
<td>AirForce</td>
<td>AFSSI-5020</td>
<td>FEPROM &amp; EEPROM</td>
<td>Erase, verify then overwrite all bit locations with arbitrary unclassified data</td>
<td>Erase, verify then overwrite all bit locations with arbitrary unclassified data. Declassify the media after observing the respective organizations verification and review procedures.</td>
</tr>
<tr>
<td>RCC-TG</td>
<td>IRIG 106-03</td>
<td>FEPROM &amp; EEPROM</td>
<td>Not specified</td>
<td>Erase; Write55h; Write AAh; Erase; Write single file containing string “SecureErase” repeated to fill all available space</td>
</tr>
</tbody>
</table>

**Table 1 Secure Erase Specifications**

**CLEAR - FAST ERASE**

This level of secure erase eliminates data in the flash memory erase state and performs this at very high speed. For example, high capacity single level cell (SLC) NAND flash chips erase typically in about 5 seconds and up to 20 seconds worst case. Some flash disks erase all of the chips in parallel, thus the longest erase time will be approximately twenty (20) seconds.

In terms of security levels, clearing data with this technique is not adequate for the highest level of protection. The concern here is the act of removing charge (erasing) from the flash cells during chip erase leaves remanence of the original data. Simply erasing data cells to a known logical level is not the same, in analog terms, as truly eliminating the memory value. Said another way, the erased charge level in a cell may vary after erasure depending if the prior state held a charge of a logical one or a zero. Analog “leftovers” of the original data levels after a simple erase may allow a sophisticated enemy to reconstruct the original data.
Sanitize, a method providing a higher level of security, discussed below, is designed to eliminate data remanence in flash memory. Even though Clear does not satisfy the highest and more stringent goals of Sanitize, Clear simply and rapidly eliminates flash disk data within a secure facility prior to redeployment.

**SANITIZE – MULTIPLE OVERWRITE**

There are many different specifications for Sanitize, of which all are defined with the common goal to eliminate flash cell charge data remanence. By repeatedly overwriting every block of flash memory with alternating or random patterns the original data pattern is entirely removed from the flash cell.

Prior to writing data to flash memory, an erase cycle is performed automatically. So for every overwrite pattern written during Sanitize, an erase operation is performed to the flash memory. The sequence below illustrates the IRIG 106-03 Sanitize operation:

1. Erase and write 0x55 to flash blocks
2. Erase and write 0xAA to flash blocks
3. Erase and write the string “SecureErase” to flash blocks
4. Repeat steps 1-3 to all unused/spare and bad blocks

Sanitize presents a special concern to flash disk users and requires certification by flash disk manufacturers that bad blocks have been sanitized. Flash disk defect management techniques ensure data integrity by taking blocks with data errors out of service. Prior to being marked as bad, these blocks may have held user data and to achieve the Sanitize data security goal these blocks must be included in the Sanitize operation.

The time to complete a Sanitize operation is relative to the general performance of the flash memory and the architecture of the flash disk. The Adtron ArrayPro™ architecture in Adtron flash disks achieves Sanitize rates that approach 100MB/s in high capacity flash disks. At this internal data rate, a 10GByte flash disk can be Sanitized with three overwrites at an effective rate of 33MB/s or just over five (5) minutes. The time performance for the Sanitize function varies based on the specific Sanitize operation and specific architecture within the flash disk.

**DESTROY - PHYSICAL DAMAGE**

Destroy operations are expected to physically damage the storage media so it cannot be used to retrieve data. Terms generally associated with destroy are pulverize and incinerate. These can be accomplished in some environments, but not easily in airborne systems.

In an all electronic storage device like a flash disk, it is possible to cripple the circuits by application of an electrical over-voltage to the flash media. Speed of execution is the main advantage to using an electrical method to damage the media. Typically an over-voltage can be developed and delivered in tens of milliseconds. Depending on the flash disk capacity, a number
of cycles may be required, thus lengthening the overall time to about one second for large capacity, 128GByte, flash disks.

In applications where speed to disable the flash memory is critical this method completely disables access to the data through both the interface and the device level. As an example, the time it takes for a low flying aircraft to land after being damaged could be significantly less than the time sanitize or clear. While this technique does not absolutely eliminate flash cell content, it does make data recovery outside of the realm of the sophisticated scientific laboratory impossible.

ENSURING SECURE ERASE INITIATION AND COMPLETION

Any of the methods discussed can be initiated by software command or hardware signal (button pressed). Features of armed and disarmed for secure erase are very useful to eliminate false triggers. Once armed, the data elimination process activates by the action of the computer, or autonomously by a discrete signal.

To be a robust secure erase implementation all data elimination schemes must be irreversible such that it does not stop once started. Once initiated the process continues to completion and during the process no data access is permitted. This ensures that data cannot be retrieved even if the operation did not complete before losing power.

Power cycles during erase are of concern to the system architects as a damaged aircraft may cause intermittent system power. If power is lost, when the power is restored the erase operation must continues and cannot be defeated or disabled until completed.

It is possible to add a backup power system to supplement the aircraft power. In the design of these supplemental power sources it is critical to maintain the same level of aircraft quality and reliability offered by the flash disk. The use of low reliability, consumer grade super capacitors for energy storage does not represent good design practice in airborne systems depending on secure erase for data security.

DATA ENCRYPTION

Data encryption may serve as an alternate data protection scheme to those listed above. Instead of erasing data, the data could be simply safeguarded. Encryption engines can be co-located within a flash disk to encode and decode the data in real time during a disk write and read transfer. For example, DES and Triple DES engines can be tailor fit into the ASICs and FPGAs found in many flash disks.
Airborne, ship board and ground based rugged computer systems incorporate flash disks for the enhanced functionality of durability, performance and capacity. In addition to these benefits are the advanced security features provided by flash disks. By safeguarding data through access control and data elimination techniques, flash disks provide a full range of data security features.

Flash disks from Adtron Corporation incorporate the data security features of Write Protect, Password Login, Clear, Erase and Destroy mentioned in this article. Additionally the Adtron ArrayPro™ architecture supports the addition of internal data encryption. Adtron FlashPaks™ can be seen at [www.adtron.com](http://www.adtron.com) and the secure erase functions offered by Adtron EraSure™ can be seen at [www.adtron.com/expertise/datasecurity.html](http://www.adtron.com/expertise/datasecurity.html).