Solid-state drives meet military storage security requirements

By Gary Drossel

While many designers still utilize consumer-grade storage in military applications, these solutions offer sub-par security and insufficient reliability in the long-term compared to solid-state storage technologies developed for use in critical environments. Solid-state drives offer robust, customizable, and scalable security algorithms that, when combined with inherent environmental ruggedness, make solid-state drives ideal for military embedded systems.

A captain in the Dutch Air Force leaves a portable hard drive in his rental car. The contents: details of reconnaissance missions and security measures for the 1,200-man Dutch military presence in Afghanistan. The drive, which had no security encryption, is later found by two young men and copied onto a computer.

The data is later returned to the officer, but incidents such as this one demonstrate all too clearly the need for the security of military systems worldwide.

Designers must come to understand that the security requirements of military embedded systems are fundamentally different from those of consumer electronic devices. In contrast to consumer applications, military embedded systems require data to be rendered invalid and inaccessible when the storage device is improperly removed from the host system for which it was intended. The host system must maintain ultimate control over security algorithms to protect data and prevent IP theft. These algorithms can be as simple as ensuring that the correct storage product is in the host, or as intricate as tying the software IP and mission data directly to the storage device. Since the security algorithm is host-centric and not device-centric, the algorithm itself can be completely proprietary and therefore much more secure. This security platform – combined with mechanical scalability, low power consumption, and long product life cycle – makes solid-state drives very attractive to military embedded system designers.

Examining the considerations

Storage devices for military embedded systems must meet a daunting number of criteria in addition to protecting mission or application data and software intellectual property. Data integrity is paramount, and the drive itself must not be susceptible to corruption due to power disturbances. The equipment needs to be highly portable, so the technology must have low power consumption characteristics and must be small and light enough to fit seamlessly in a vehicle or aircraft, or be carried by an individual soldier. Such systems must be able to handle extreme environmental conditions such as shock, vibration, and altitude, and should tolerate a wide

Market concern	Hard drive	Solid-state drive	Flash card
Corruption due to power disturbances	Adequate	Requires enhanced protection circuitry	Poor
Product life cycle	Less than one year	Multiple years	Less than one year
Wear-out	Environmental and mechanical concerns	Very good – write/erase endurance exceeds 2 M cycles	Write/erase endurance less than 10 K cycles
Security	Possible password protection via ATA specifications. No sweep, scrub, or purge	High-end drives provide several security options such as password protection, sweep, scrub, and purge	Possible password protection via CompactFlash specifications. No sweep, scrub, or purge
Power consumption	> 2.5 W	> 2.5 W	< 1 W
Mechanical dimensions	2.5"	2.5"	CF

Table 1

range of temperatures. There is a need for a multiple-year product life cycle and high endurance rating to make sure the drives operate reliably for several years.

How different forms of storage stack up

With all these considerations, it is not surprising that storage products originally designed for the consumer electronics market do not in general meet the needs of military embedded systems. Table 1 illustrates the design trade-offs of traditional storage solutions for military embedded systems.

As the table shows, solid-state drives offer more advanced security options, better environmental performance, and longer product life cycles than hard disk drives, but designers must be careful when choosing these solutions. Traditional solid-state storage solutions designed to satisfy high capacity and advanced data security requirements have been mechanically confined to 2.5"or 3.5" hard drive form factors. This is not only because of the number of storage components – usually NAND flash – required to achieve the desired capacity, but also because of the physical size of the microprocessor and associated logic used to provide the host system interface and the solid-state memory management algorithms. These circuits have neither been able to scale to smaller form factors nor have they been able to achieve power consumption rates less than the typical 2.5 W of rotating hard drives.

Applications requiring smaller mechanical form factors such as CompactFlash or PC cards used in consumer applications present their own set of challenges. While these products offer relatively good environmental performance and consume little power – in general, less than 1 W – there are still concerns about product life cycles, endurance, and security capabilities.

In addition, most drives and flash cards customarily designed for use in consumer applications do not provide security technology such as fast erase or purge that will prohibit data from falling into the wrong hands. In addition, their password protection algorithms may not be flexible enough to allow the host system to implement its desired algorithm.

The ideal solution for military applica-tions, therefore, is a mechanically scalable, low-power storage solution that is impervious to power disturbances, maintains a long product life cycle, prevents field failures due to wear-out, and provides access to low-level security *hooks* so the host can define its own security algorithm.

Security concerns worth consideration

Many military embedded applications require advanced security levels. Data recorders and wearable and field computers require features such as ultra-fast data erasure and sanitization, data zones with independent security parameters, and secure areas for designers to access and create their own encryption and decryption keys. These features protect application data and software IP from theft or from falling into the wrong hands as illustrated in the 2001 incident where a Navy surveillance plane collided with a Chinese jet and was forced to make an emergency landing in China.

Military-focused OEMs want to perform two key functions in their application to protect mission data and software IP. First, there is a need to ensure that the end user is utilizing a qualified storage device in the system. In some instances, perhaps for security, warranty, or service purposes, the OEM needs to know that the specific drive originally shipped with the equipment is indeed still in the system. This type of technology prevents a rogue storage device from entering a secured system. Without this technology, it is possible to place a similar product with the same part number from the same vendor into a system. That similar part number may contain incorrect or malicious data that may or may not be detected before it is too late. With the type of technology described here, the system would not even boot and the chances for errors (or worse) would be greatly diminished. Second, there is a need to tie mission data and software IP to the specific drive for which they were intended to prevent theft and ensure software integrity.

One possible method to accomplish this is for the drive to reserve a specific area that is only accessible to the OEM through a proprietary command. That area could store specific host system information so that when the drive boots up, the host reads the data in this secure area and looks to match that data with a host serial number or other identifier. If there is no match, the drive is inaccessible. That area could also store data that the host could use as the key to its proprietary encryption algorithm.

Preventing data from falling into the wrong hands

Data in a hard drive, a solid-state drive, or a flash card is stored in 512-byte increments called *sectors*. Each sector also has associated with it a 16-byte control block as illustrated in Figure 1. Control blocks store bad block information, error correction, and perhaps some proprietary monitoring information that must be maintained if the drive is to be reused.

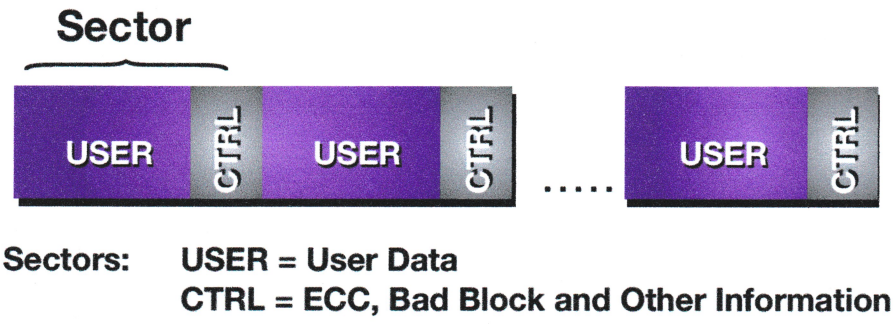

Figure 1

Data security features can be initiated via software through hardware initiation such as a switch connected directly to the storage device, a vendor-specific command structure, or through some combination of both. Consideration should be given to the specific implementation and the re-quired drive technology. Magnetic media such as hard disks and tape drives provide the lowest initial price per gigabyte at the expense of environmental performance, multi-year product life cycles, and the ability to quickly erase all data on the drive. It can take a matter of hours for large amounts of data to be scrubbed from magnetic media. Even then, the process needs to be repeated to prevent data *ghosts* or portions of data that remain on the drive that can be recovered with specialized equipment. The result is a very time-intensive process not at all well-suited to the quick-erase needs of military systems.

Attempts were recently made by military contractors and research institutions to improve erasure time by exposing drives to extremely high-powered magnets – a process also known as *degaussing*. Researchers made custom neodymium iron-boron magnets and special pole pieces made of cobalt alloys and used them to erase hard drive data.

Erasure time was reduced from several hours to several minutes, but other problems presented themselves. For one, the magnets weighed about 125 pounds, causing severe limitations in most field applications and virtually eliminating possible use in mobile computers. The mechanics of the magnets proved to be a challenge as well. Mechanisms had to be fabricated that would push the drives past the magnets, further adding to the weight consideration. Users had to physically pull drives out of their enclosures to pass them through the magnetic field. This added more steps to the data removal and greatly impacted the amount of time required to erase the data.

Later improvements on the magnet expos-ure process have brought the weight down to as little as six pounds, still a consideration for wearable computers but better for vehicle and aircraft mounted equipment. There is still the necessity of pulling the drives from their enclosures to place into the mechanism by hand, which can significantly slow the overall process.

Other methods of eliminating data are still under consideration. In recent years, exposing drives to heat-generating ther-mal material has been explored. Repeated tests of this method, however, have not been promising. Evidence has shown that despite the damage a thermal reaction can inflict, amounts of data on drives could still be recovered.

The act of physically crushing or shredding a drive to prevent future use and data access is another alternative, but one that carries with it certain drawbacks. For one, even badly mutilated drives can still yield useful amounts of data. Another factor is the machinery necessary to destroy the drives, which can be very heavy. As with using heavy magnets, the extra steps of removing the drives from their enclosures and inserting them into the machinery for destruction make this more awkward.

The solid-state difference

Because the physics of solid-state drives are significantly different from those of their magnetic counterparts, so is the way solid-state drives write and erase data. Figure 2 illustrates a typical floating gate cell in a nonvolatile storage component. Charge on the floating gate allows the threshold voltage to be electrically manipulated to levels that represent a logical 0 or 1. The process of erasing and writing revolves around tunnel release and tunnel injection of electrons onto the floating gate. These processes allow no possibility of ghost images on the device after an erase, so no scrubbing technology is required. In fact, the erase process itself is a form of data scrubbing since the operation consists of writing "00"s then "FF"s.

In addition to the type of media, the system designer must determine whether or not the drive should be reusable or rendered unrecoverable after executing the fast erase – or *sweep*. He should also determine what needs to happen with any data that may be in non-user-addressable areas like bad blocks or spares. Standard ATA commands will not be able to address these areas. The designer may also want to implement a multiple-step command sequence to ensure the erase is not initiated erroneously.

Consideration should also be given to providing enough power to complete the erase, but this may not always be possible. In such an event, intelligence must be built into the drive so that an incomplete sweep operation will finish the next time the power is applied – independent of the host system. The designer must also model the time required to fully erase the drive based on the criticality of the data. Table 2 and Figure 3 illustrate the benefits of proprietary commands that can be used to provide a fast erase mechanism versus using standard ATA commands.

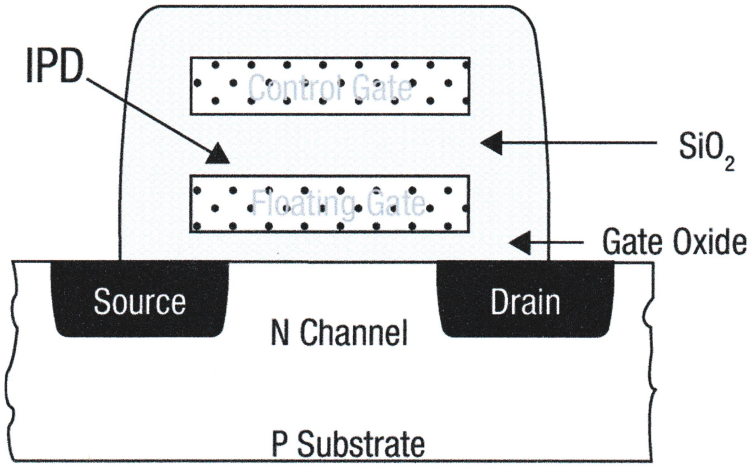

Figure 2

Table 2 contrasts the time it would take to fully erase a storage product by using advanced storage technology (for example, a vendor-specific command) and using standard ATA commands. These benchmark times show that data can be erased significantly faster if advanced security technology (such as fast erase or sweep) is used.

Capacity	Vendor-specific commands (in seconds)	Standard ATA commands (in seconds)
32 MB	3.4	5.2
64 MB	5.9	10.4
128 MB	2.8	20.7
256 MB	3.3	41.4
512 MB	4.9	82.9 (1.38 minutes)
1 GB	5.9	166.5 (2.77 minutes)
2 GB	6.8	333.5 (5.55 minutes)
4 GB	8.3	671.5 (11.19 minutes)
8 GB	13.8	1343.9 (2239 minutes)
16 GB	14.7	2621.7 (43.69 minutes)

Table 2

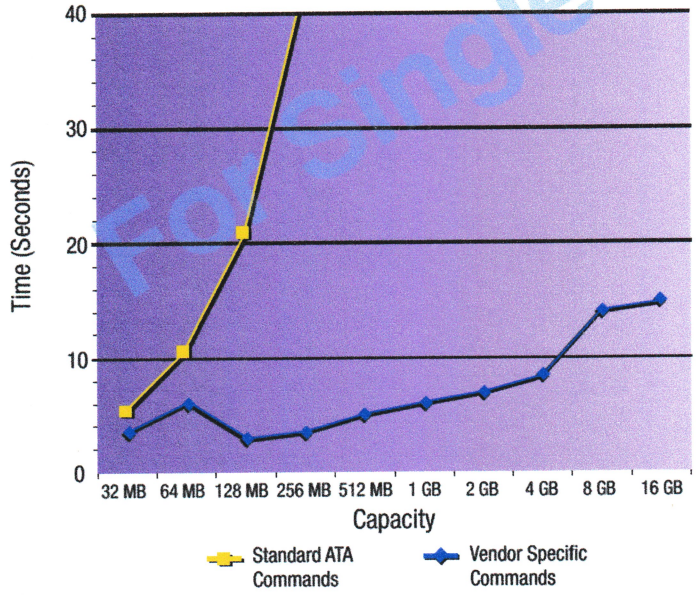

Figure 3

It is also important to understand how the drive implements the fast erase feature. Some require the entire contents of the drive to be erased. Others can sweep only the most critical or classified data by implementing advanced zoning technology. Use of this technology allows the system designer to be able to partition the drive into different zones with different security parameters. One zone could hold standard operating systems or nonclassified data files. A second zone could be a read-only lookup table, and a third zone could store classified data. Designers then have the flexibility to only sweep that zone with the classified data. Depending on the size of the classified partition versus the size of the drive, erase times could be cut by more than half.

The future of storage

New technology is continually evolving to meet the stringent security demands of military embedded systems. The overwhelming success of solid-state drives in the consumer electronics sector will continue to motivate traditional hard drive users to seek lower-power, more portable, more rugged solutions. Storage vendors targeting the military embedded system space will continue to leverage the economies of scale this success has brought. However, they must provide robust, host-centric security methodologies to enable OEMs to define their own security algorithms, and they must provide the engineering and technical support required to ensure a smooth implementation of storage into more complex military and embedded systems.

Gary Drossel, *VP of Product Planning, joined SiliconSystems in 2004 and is responsible for managing technical marketing and application engineering for SiliconSystems' complete product line. A 16-year embedded computing industry veteran with a wealth of knowledge concerning solid-state storage technology, he has also played a leading role in developing the company's marketing strategy, including product roll-out and customer introduction. Gary received a BS degree in Electrical and Computer Engineering from the University of Wisconsin.*

SiliconSystems, Inc.
26940 Aliso Viejo Parkway
Aliso Viejo, CA 92656
949-900-9400
gdrossel@siliconsystems.com
www.siliconsystems.com

