SILICON SYSTEMS
The *Future* of Storage...Today™

Advanced Storage Technology

WHITE PAPER

SILICONDRIVE SECURE™

SILICONSYSTEMS, INC.
26940 Aliso Viejo Parkway
Aliso Viejo, CA 92656
Phone: 949.900.9400
Fax: 949.900.9500
http://www.siliconsystems.com

May 2006

INTRODUCTION

SiliconDrive Secure™ combines all the high-performance, high-reliability, and multi-year product lifecycle benefits of the standard SiliconDrive with a comprehensive suite of patented and patent-pending technologies that provide multiple security options to safeguard application data and software IP in embedded systems. Combined with SiliconSystems' patented PowerArmor™ and SiSMART™ technologies, SiliconDrive Secure provides the most secure, robust, and scalable storage platform for the most demanding embedded applications.

Applications requiring advanced levels of security, such as data recorders, wearable and field computers, medical monitoring and diagnostic equipment, POS systems, and voting machines are able to activate features such as ultra-fast data erasure and sanitization, data zones with independent security parameters, and secure areas for OEMs to access and create their own encryption/decryption keys. SiliconDrive Secure protects application data and software IP from theft, falling into the wrong hands from deployments in high-risk areas, corruption, and accidental or malicious overwrites.

BACKGROUND

Historically, embedded devices have had limited security options available because of the engineering obstacles of designing robust security features into the small mechanical footprints required for embedded systems. Challenges such as storage components, processing power, and battery life, as well as time-to-market and overall cost concerns, have limited many security features from being implemented in hard drives and traditional flash cards.

The security industry has focused on portable storage devices for the consumer electronics industry, where the basic premise is that users want the security algorithm to travel with the storage device—for example, a USB thumb drive. This allows the user to protect and use the data on any system, whether it is an office PC, home computer, Internet kiosk, or other public computer. Software applications and user data are encrypted and password-protected using industry-defined security protocols, which become targets for Internet hackers.

Enterprise System OEMs operate under a different premise. Data must be rendered unreadable if the storage devices are removed from the systems for which they were intended. Highly visible security breaches such as a flash card with sensitive military documents being found in a bazaar in Bagram, Afghanistan have become more prevalent as more and more embedded devices handle sensitive data.

In the Enterprise System OEM market, 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 application data directly to the storage device.

SILICONDRIVE SECURE

SiliconDrive Secure is a comprehensive solution that overcomes the design challenges and performance trade-offs in hard drives and traditional flash cards to deliver an unprecedented level of embedded storage system security. The low-power, highly scalable storage solution enables designers to easily integrate security to guard against critical data from falling into the wrong hands and software IP theft. SiliconDrive Secure integrates a suite of low-level, SiliconSystems-specific commands that can be used by the host to create a completely proprietary, highly configurable security algorithm.

SiliconDrive Secure increases storage system flexibility, while decreasing cost by eliminating the need for storing information on multiple platforms based on security requirements. Benefits to OEMs include IP theft prevention, new market opportunities, and being able to capture untapped revenue streams and enhanced product differentiation.

BENEFITS

Application Data and Software IP Theft Prevention

SiliconSystems' customers want to perform two key functions in their application to protect application data and software IP. First, there is a need to ensure that the end customer is using a qualified storage device in the system. In some instances, perhaps for warranty or service purposes, the OEM needs to know that the specific SiliconDrive Secure originally shipped with the equipment is indeed still in the system. Second is the need to tie specific application data and software IP to the specific SiliconDrive Secure for which it is intended to prevent theft and ensure software integrity.

SiKey™

SiKey™ ties application data and software IP to a specific SiliconDrive Secure so that the host system can verify the drive and create unique encryption keys to prevent theft. With SiKey, any application that ties storage to the host system, such as companies that routinely ship software IP upgrades, can select the right level of advanced security to prevent theft.

> ***Example:*** A voicemail system provider sells software upgrades to either increase the number of users, or provide some type of system level improvement. The upgrade is shipped on SiliconDrive Secure as a "kit." The voicemail system provider wants to ensure that the software is tied only to that specific SiliconDrive Secure so that even if the software is copied onto another device, it does not work properly in the host system.

Through the use of the SiKey technology and a SiliconSystems-specific command, the host can read two unique pieces of data that can be used for validation. The first data string identifies the product as being SiliconDrive Secure. The second identifies the specific SiliconDrive Secure. The host system can then use that data to create encryption/decryption keys for software IP and application data. While this method does not provide copy protection, it does inhibit the use of the particular software on any system other than the original host.

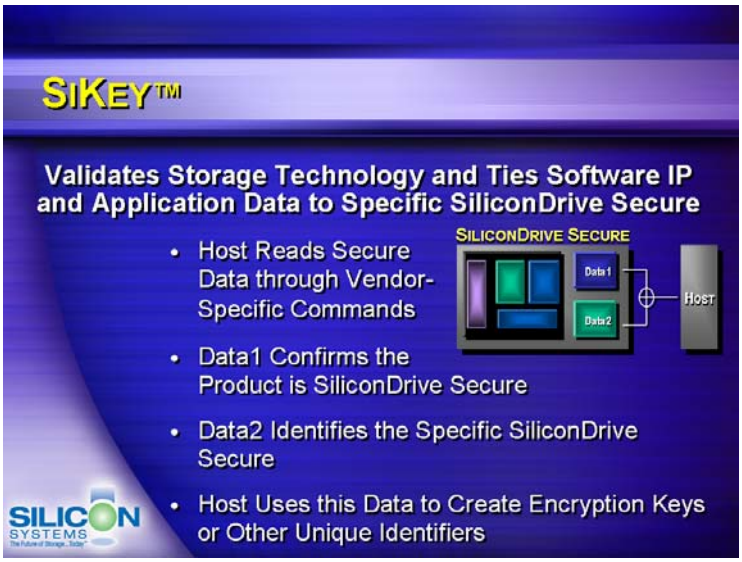

Figure 1: SiKey

Confidential Data Protection

Applications requiring advanced levels of data security in high-risk environments such as data recorders, wearable and field computers, medical monitoring and diagnostic equipment, POS systems, and voting machines can employ SiliconSystems' patent-pending SiSweep™, SiScrub™, and SiPurge™, which rapidly and completely remove data from SiliconDrive Secure and prevent sensitive data from falling into the wrong hands.

These data security features can be initiated in two ways:

- Via software through a two-level command structure that greatly decreases the probability of initiating the functions inadvertently.
- Through an optional hardware initiation, like a switch or a push-button.

Hardware versions of SiSweep, SiScrub, and SiPurge will be available in Q3, 2006.

SiSweep™

As illustrated in Figure 2, the SiSweep function completely erases *all* data fields in SiliconDrive Secure. As a result, all user data, master boot records (MBR), and file allocation tables (FAT) are destroyed. While the actual recovery procedure is highly application-dependent, a functional equivalent of the following process is required to recover or re-use SiliconDrive Secure after the SiSweep command has been executed.

1. FDISK. This command re-creates the MBR and partition information.
2. FORMAT.
3. RE-LOAD. This command reloads the operating system and application data.

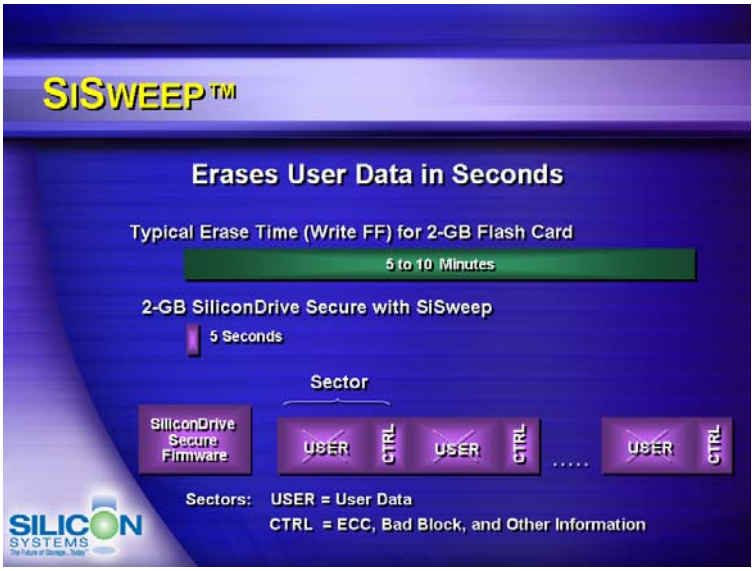

Figure 2: SiSweep

Figure 3 below and Table 1 on the next page illustrate the benefit of SiSweep as an alternative to using standard ATA commands to erase/overwrite SiliconDrive Secure. For a 16-GB SiliconDrive Secure, sweep time is reduced from just under *44 minutes* to just under *15 seconds.* Figure 4 on the next page shows that the effective data sweep rate of SiliconDrive Secure can exceed 1 GB per second (GBps).

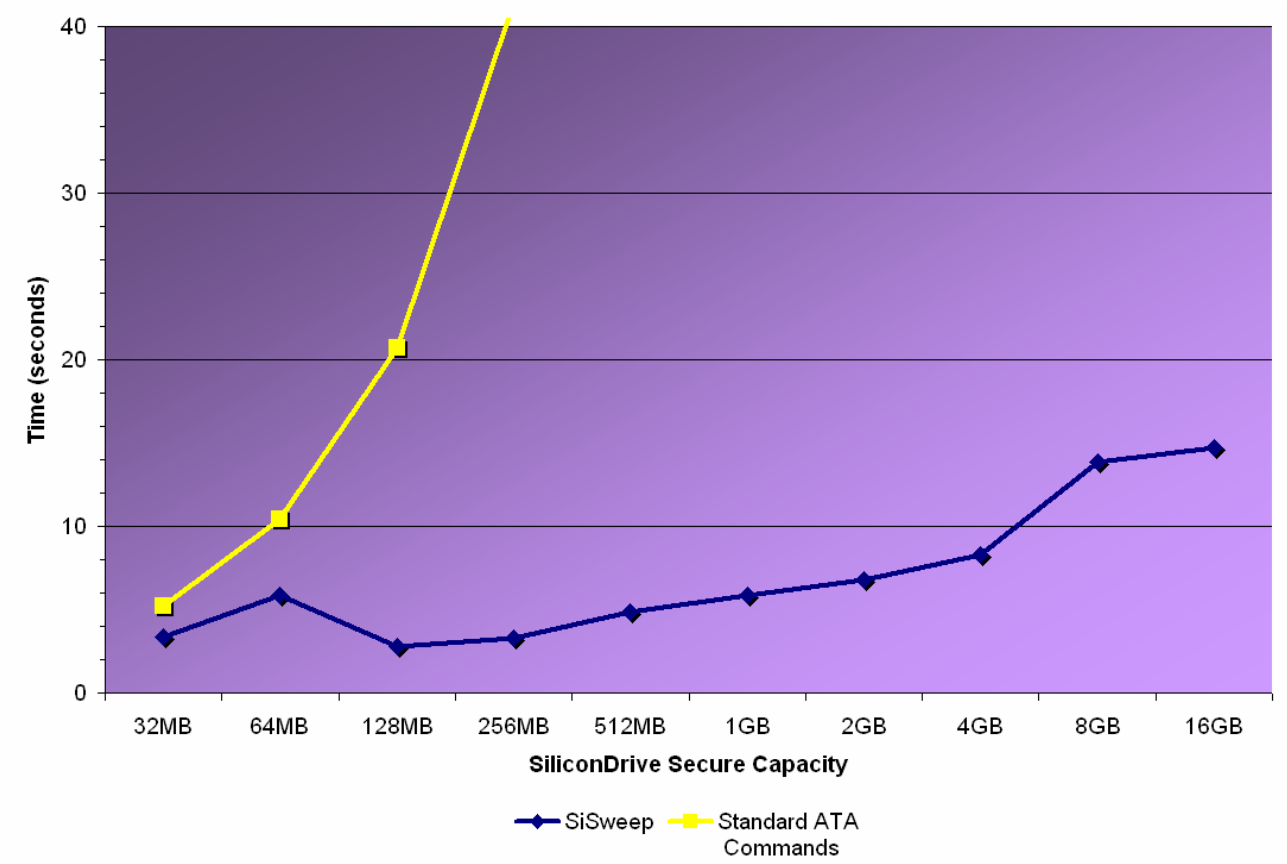

Figure 3: SiSweep Speed Benefit

Capacity	SiSweep	Standard ATA Commands
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 GB	5.9	166.5
2 GB	6.8	333.5
4 GB	8.3	671.5
8 GB	13.8	1343.9
16 GB	14.7	2621.7

Table 1: Data Sweep Times in Seconds

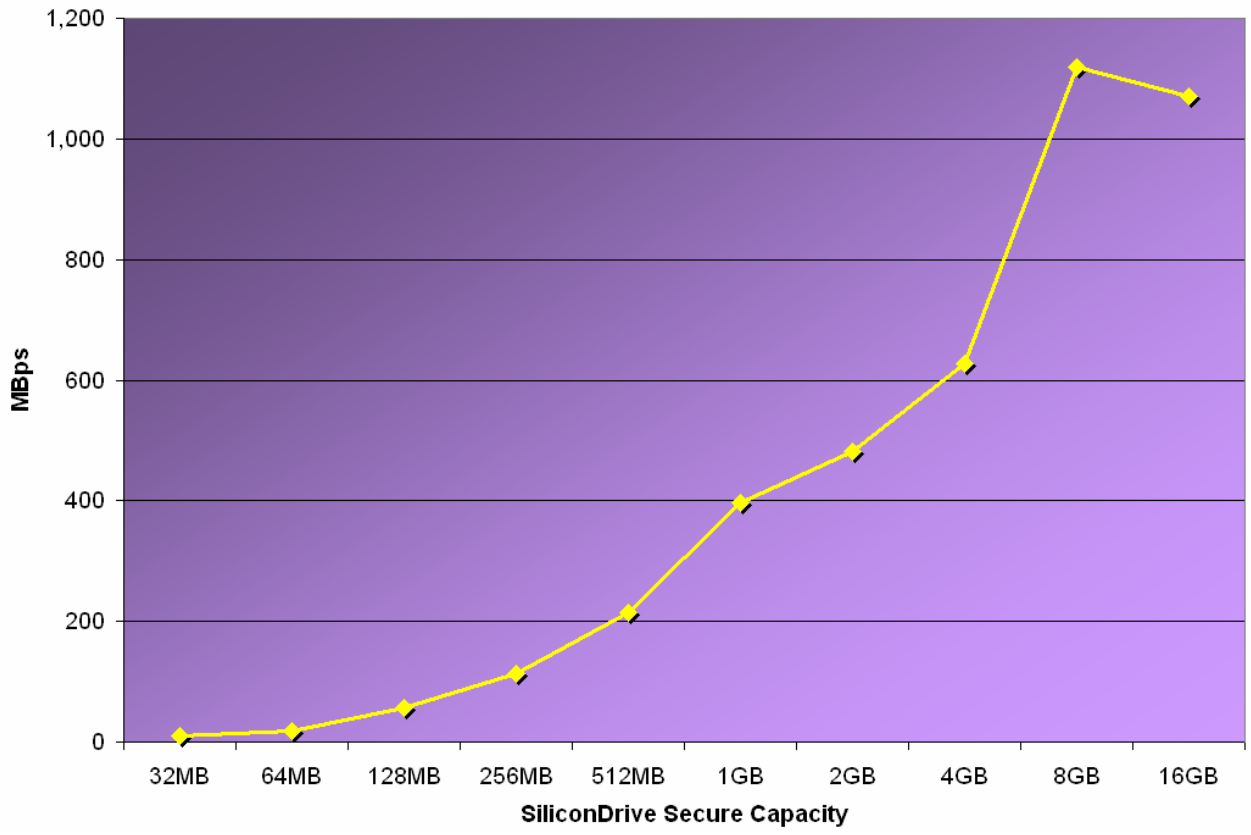

Figure 4: SiSweep Effective Data Rate

SiPurge™

SiPurge takes SiSweep one step further by not only eliminating all user data, MBRs, and FATs, but also by erasing control blocks and SiliconDrive Secure firmware, as shown in Figure 5. SiPurge is a non-recoverable operation, which means SiliconDrive Secure cannot be re-used after this command is executed.

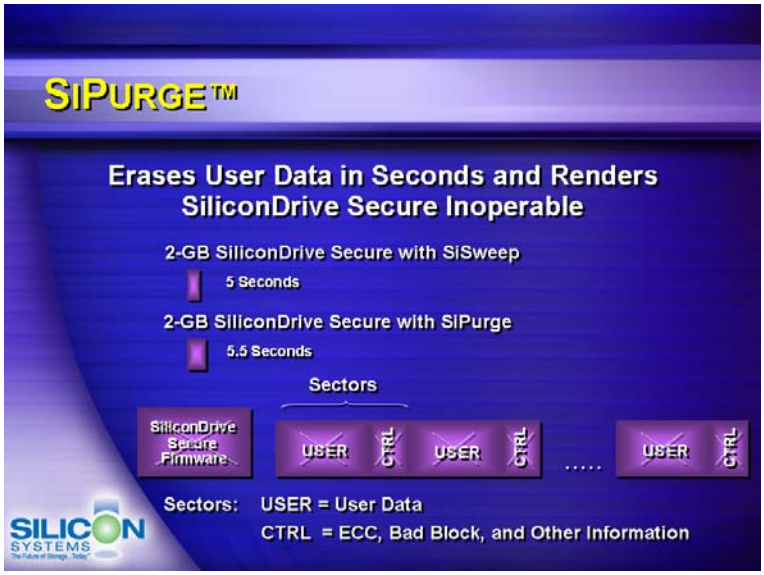

Figure 5: SiPurge

SiScrub™

SiScrub is a command created to allow SiliconDrive Secure to be used as a drop-in replacement for magnetic hard drives in applications that require multiple write/erase cycles before the drive is deemed "sanitized" or "scrubbed." It is generally well-known that ghost images can still reside on the magnetic media of hard drives, even after an erase. Writing and erasing multiple times eliminates this issue. In solid-state drives, an "erase" is actually a write of all zeros followed by a write of all FFs, which in itself is a "scrubbing" methodology. SiScrub, therefore, is not technically required to completely sanitize SiliconDrive Secure, but it may still be needed if the end customers do not want to re-write their requirements based on the move to solid-state.

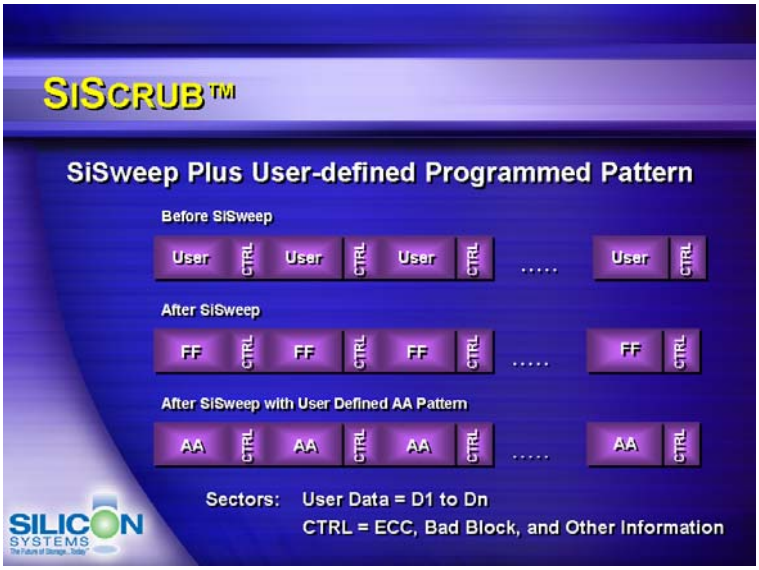

Figure 6: SiScrub

Access Control and Permissions Selection

SiliconDrive Secure integrates a set of proprietary commands that allow the host system to set, change, or delete a unique password that locks and unlocks the data space of SiliconDrive Secure. These features have been found to be highly effective in safeguarding against illegal spying or piracy of sensitive information.

SiSecure™

SiSecure™ enables the user to block unauthorized access to an entire drive by establishing a required password for read/write access.

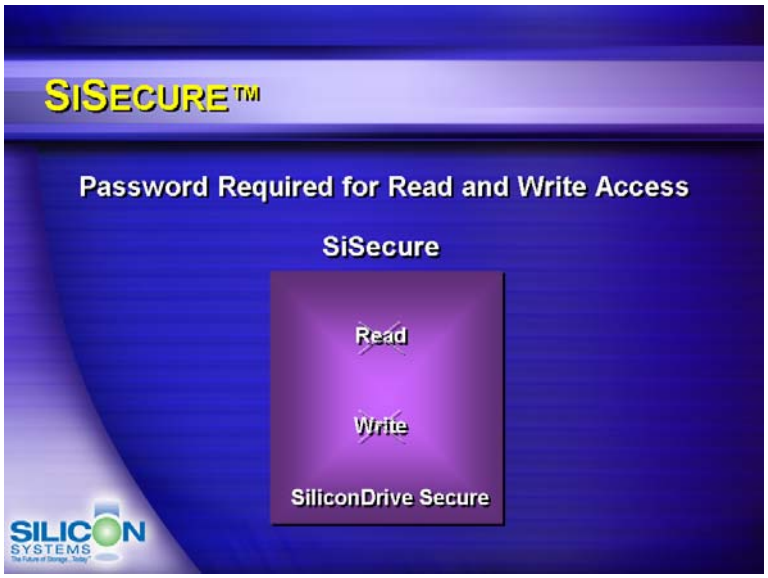

Figure 7: SiSecure

SiProtect™

SiProtect™ employs software write protection for read-only access to prevent accidental overwrites or data tampering.

Figure 8: SiProtect

Multiple Security Zone Creation

SiliconSystems' patent-pending SiSecure, SiProtect, and SiSweep are security technologies which, when used by themselves, allow the user to adjust the security parameters of the entire SiliconDrive Secure.

SiZone™

SiZone™ allows the design engineer to define up to five independent security zones with different security parameters for ultimate protection and flexibility. This is especially important in applications such as wearable computers or industrial PCs, where application program information, sensitive documents, and classified data can be stored independently with unique security parameters.

> ***Example:*** A gaming OEM manufactures video poker machines that use SiliconDrive Secure as the storage technology. The machine has three different storage requirements—one to store and manage specific validation codes required by regulatory agencies, a second to store the game and its associated graphics images, and a third to provide player tracking statistics for casino marketing programs. Previously, the OEM needed three different storage products to accomplish this task—a secure EPROM for the validation codes, a CD-ROM for read-only access to the game itself, and a flash card for player tracking. All three requirements can now be satisfied by one SiliconDrive Secure—with zone one implementing SiSecure to provide restricted access to the validation codes, zone two implementing SiProtect to provide read-only access to the game, and zone three to allow full read and write access to monitor player tracking.

SiZone is enacted by a series of SiliconSystems-specific commands that enable the user to:

- Define up to five zones
- Define and change the following for each zone:
  - Beginning and ending logical block addresses
  - Password (though the use of the SiSecure/SiProtect command)
  - Security:
    - Unprotected = full read and write access
    - SiProtect = read-only access
    - SiSecure = no access without password
    - SiSweep = ultra-fast data erasure

SiliconDrive Secure Technologies

SiKey	Ties SiliconDrive Secure to a specific host and/or software IP
SiZone	Data zones with different security parameters
SiSweep	Ultra-fast data erasure
SiScrub	Ultra-fast data erasure followed by a programmed pattern
SiPurge	Non-recoverable data erasure
SiProtect	Software write protection for read-only access
SiSecure	Password required for read/write access

Each zone can be configured with any combination of SiSweep, SiSecure, and SiProtect, or the zone can have full read/write operation, providing the ultimate in protection and flexibility.

SiliconDrive Secure includes the following SiliconSystems' base technologies:

- PowerArmor, which eliminates drive corruption.
- SiSMART, which calculates remaining useful life.

Related Information

All SiliconSystems' security technologies are easy to implement and integrate into the host application software. User-defined security applications can be created around these custom commands with complete flexibility as to what specific technologies are implemented in the final application. Application notes detailing the exact implementation of the proprietary SiliconDrive Secure commands are available under the NDA from a SiliconSystems' Field Application Engineer.