# Tactical Drives – SSDs and Security

***Protecting Mission Critical Sensitive Data***

By: Martin Cardenas

## Overview

As cyber security concerns grow, the DoD is placing more emphasis on protecting data in motion and data at rest.

While data in motion primarily deals with hardening systems and preventing them from being hacked while operational, data at rest deals exclusively with encrypting data stored on non-volatile media and erasing or sanitizing that data when necessary.

GMS systems rely on a myriad of non-volatile media types ranging from 2.5-inch rotating hard drives (HDDs) to multiple form factors of solid state disks (SSDs) that use flash memory technology.

## Introduction

This paper deals with the complementary topics of mechanisms for securing drives using passwords and encryption techniques and sanitizing or erasing those drives when necessary to declassify a system.

We'll start with the encryption process (what it is and why it's necessary), proceed to different types of encryption strategies (hardware vs. software), and follow into various encryption standards, both commercial and defense.

Let's begin.

***Protecting sensitive data is not optional.***

## Why Encryption

Data is central to our personal lives as it is for many businesses, governments, and militaries. Data is the world's most important asset -- and yet, it is the most vulnerable!

Our digital word demands that we protect sensitive information from hackers and other cyber threats.

## What is Encryption

Encryption is a technology that conceals data through a complex mathematical algorithm to transform the plaintext (readable) data into ciphertext (unreadable) data.

The key to this operation (no pun intended) is the cryptographic encryption key. The encryption algorithm uses this key to transform the data into unreadable ciphertext. If this ciphertext data were to be compromised, or intercepted, it would be impossible to interpret.

The encryption key is then required in the reverse operation to unscramble the data back into readable form.

Today's drives implement a block encryption algorithm defined by the Advanced Encryption Standard (AES). More on this later.

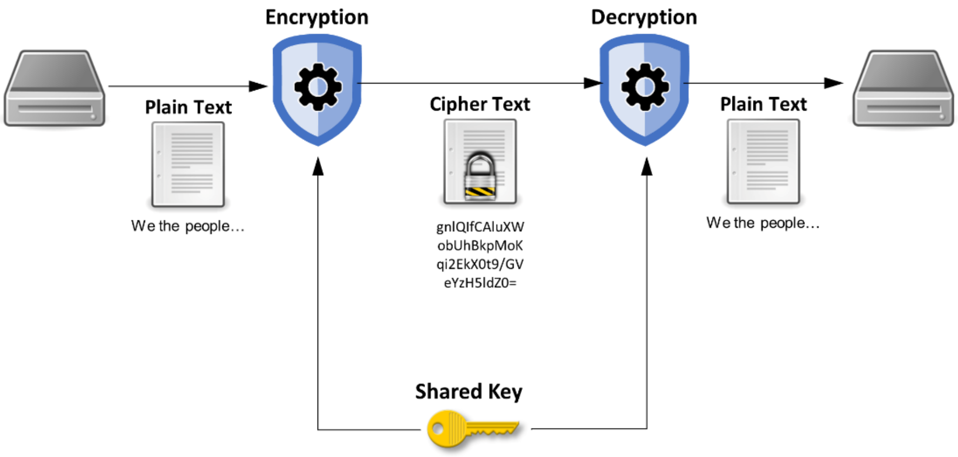


**Figure 1. Data Encryption and Decryption Process**

## Software vs. Hardware Encryption

The encryption process can be performed either in software or in hardware.

Software Encryption

Software encryption is performed by an application or program. This encryption typically relies on passwords as the encryption key to authenticate users.

It is extremely popular because it is affordable and easily accessible. Free options exist for many popular operating system platforms, for example BitLocker™ for Windows®, FileVault® for Apple®, and Linux Unified Key Setup (LUX) for Linux®, to name a few.

Software encrypting is very cost effective because it works with existing hardware, i.e., purchasing additional hardware is not required.

The drawback to software encryption, however, is that the encryption process is performed by the host CPU, thereby impacting system performance as precious system resources diverted to that process. Fortunately, modern computers are boasting more powerful processors than ever, so only a small dip in performance may be noticeable when encryption is at play.

Hardware Encryption

Hardware encryption uses devices that incorporate dedicated hardware controllers to specifically encrypt the data. Because of the dedicated hardware, host CPU performance is largely unaffected. Examples of such devices include Self-Encrypting Drives (SEDs). More on these to follow.

Unlike software-based encryption, which uses passwords for encryption keys, hardware encryption devices generate encryption/decryption keys to authenticate users so only authorized users have access to sensitive information.

The main downside to hardware encryption is the cost. Older drives would need to be replaced with newer drives that support hardware encryption.

## Self Encrypting Drives

Self encrypting drives (SEDs) are hard drives or solid state drives that are designed to automatically, and transparently, encrypt and decrypt data without user interaction. Data is automatically encrypted as it's being stored, then automatically decrypted as it's read. This mechanism is usually referred to as "security of data at rest".

The encryption algorithm process still functions as previously explained, and still needs an encryption key. But with an SED, the key is stored internally within the drive and is not exposed nor accessible to outside sources. It truly is a secret.

With SEDs, the key is known as a Data Encryption Key (DEK). The embedded controller on the SED uses the embedded DEK for the on-the-fly encryption and decryption as needed. Without this same key, the data is unreadable.

Note: the Secure Erase present on many SEDs takes advantage of one of the side effects of encryption. Encrypted data appears as random characters until the right key is used to read the data. So, to “erase” a disk, it is only necessary to simply change the encryption key. None of the old data will be readable, i.e. it is “erased”

Additionally, most SEDs support the TCG/Opal requirements, which specifies AES encryption. With AES-encrypted data and internal DEK management, SEDs are nearly impossible to crack.

A glaring caveat is that this situation does nothing to address physical access to a drive. For example, a malefactor could remove an SED, plug it in to another system, power it on, and immediately start accessing the data. This is because the DEK is always decrypted.

So why go to the trouble of encrypting, if the data can still be viewed by prying eyes? Thankfully, because most SEDs conform to the TCG Opal specification as previously stated, an additional security layer is available and must be enabled.

It involves another key, known as the Authentication Key (AK), which is used to decrypt the DEK. Setting up the AK automatically locks the SED when it is powered down.

Now, if someone were to take drive and insert it into another system, as in our hypothetical example, the AK will be requested during the boot process and must be validated before the contents of the drive can be accessed.

Because of the importance of the Authentication Key, users should go to great lengths to ensure keys are kept private and also to select keys that conform to time-tested guidelines for strong passwords.

## ATA Security

By now, you may be wondering about ATA Security. Most modern storage devices, from about 2000, support the ATA Security feature set.

ATA Security allows for a password on a drive. This is a basic security layer that provides locking access to a drive using the ATA password. The password is encrypted and can only be decrypted by an algorithm on the original drive. Once the password is set, drive access will be granted if the correct password is supplied.

**It is important to note that ATA Security grants access to the drive but does not encrypt the underlying data on the drive.**

ATA Security should only be considered for simple use-cases and is not recommended for more complicated security schemes.

## TCG/Opal 2.0

TCG stands for Trusted Computing Group. The Trusted Computing Group is an organization that develops open standards for trusted computing platforms.

The Opal Storage Specification is a set of specifications for features on data storage devices, such as disk drives, that enhance their security. The latest Opal standard is available in version 2.0. It requires encryption of stored data to prevent data access from an unauthorized person, even if they have physical possession of the drive.

SEDs which rely on the TCG Opal 2.0 standard are required to implement the double key mechanism described earlier, the Authentication Key (AK) and Data Encryption Key (DEK) and must implement AES encryption (AES is Advanced Encryption Standard – see below).

It is important to note that while most SEDs conform to the TCG Opal 2.0 standard, not all do. If in doubt, consult the appropriate documentation.

> “
> The **Federal Information Processing Standards** (**FIPS**) is a set of publicly announced standards that the National Institute of Standards and Technology (NIST) has developed for use in computer systems of non-military, American government agencies and contractors.
> ”

## AES Encryption and FIPS 197

We’ve made passing references to the AES encryption standard. Now let’s look at this a little closer.

Advanced Encryption Standard (AES) is a block cipher algorithm adopted by the US Government in 2001 and announced by the National Institute of Standards and Technology (NIST) as FIPS 197. It is the first, and only, publicly accessible cipher approved by the National Security Agency (NSA).

Without delving into specifics, AES is based on a design principle known as a substitution-permutation network. It uses 128-bit fixed data blocks with variable key sizes:

- 128-bits (AES-128): 3.4 x $10^{38}$ possible key combinations
- 192-bits (AES-192): 6.2 x $10^{57}$ possible key combinations
- 256-bits (AES-256): 1.1 x $10^{77}$ possible key combinations

Because of the astronomically large number of combinations involved, cracking an AES key is nearly impossible. For example, even with a modern computer with vast resources, cracking a 128-bit AES encryption key can take upwards of 36 quadrillion years!

In June 2003, the U.S. Government announced that AES encryption could be used to protect classified information as follows:

- SECRET: minimum of AES-128
- TOP SECRET: minimum of AES-192

## FIPS 140-2

Previously, it was shown that AES and FIPS 197 address the software algorithms required for data encryption.

On the other hand, FIPS 140-2 is the next, more advanced, level of certification. It's worth noting that FIPS 140-3 was announced in 2019 and is currently in the overlapping transition period to supersede FIPS 140-2.

In addition to certifying the AES algorithms (e.g., FIPS 197), FIPS 140-2 also involves a rigorous analysis of the product's physical properties.

FIPS 140-2 has four security levels, with higher levels offering more protective features.

- Level 1:
  Security level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module, such as at least one approved algorithm will be used. No specific physical security mechanisms are required for security level 1. An example of a Security Level 1 cryptographic module is a personal computer encryption board.
- Level 2:
  Security level 2 improves on the physical security of level 1 by requiring features that have evidence of tampering. This could be tamper-evident coating or seals that need to be broken to get physical access to the plaintext cryptographic keys and critical security parameters (CSP) within the module. This could also be locks on the covers of the module or doors that are pick resistant to help protect against physical access.
- Level 3:
  In addition to the tamper-evident physical security mechanisms required by level 2, level 3 attempts to stop an intruder from gaining access to the CSP within the module. The physical security mechanisms in level 3 may include strong enclosures and tamper detection that will delete all plaintext CSPs when the covers or doors to the module are opened.
- Level 4:
  Security Level 4 is the highest level of security. At this stage, the physical security provides complete protection around the cryptographic module with the intent of detecting all unauthorized attempts to the physical device. Unauthorized access to the cryptographic module from any direction has a very high probability of being detected and all plaintext CSPs will be deleted. At Security Level 4 a cryptographic module is required to have either special environmental protection features that will detect fluctuations and delete CSPs or to have rigorous environmental failure testing to provide assurance that the module will not be affected by fluctuations outside of the normal operating range. If the module is out of this range all CSP's will be deleted.

### FIPS 140-2: Validated or Compliant?

Devices that have been tested and have passed the rigorous NIST requirements are termed “FIPS 140-2 **Validated**”. Validated drives are also commonly called “certified” drives.

NIST maintains updated validation lists on its website (https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules).

The arduous process of getting a drive validated to FIPS-140-2 will be reflected in the drive’s price - a definite factor to consider - and may also mean that these drives may be slightly behind the technology curve due to the long validation process. FIPS 197 drives may also be validated (or certified), but that validation will only apply to the algorithm used by the drive and implemented by the drive’s controller logic.

A “compliant” device may contain certain components (e.g., the cryptographic module) that meet FIPS requirements but the drive, as a whole, has not been approved by NIST. Depending on the application, “compliant” devices may be an acceptable alternative to “validated” drives.

## CSfC – Commercial Solutions for Classified

Commercial Solutions for Classified (CSfC) is a strategy of the National Security Agency (NSA) to certify cybersecurity solutions that leverage commercially available solutions. Many government programs require CSfC solutions for securing data at rest for top secret information.

The NSA has developed, approved, and published solution-level specifications called Capability Packages (CPs) and, through the National Information Assurance Partnership (NIAP), works with technical communities to develop, maintain, and publish product-level security requirements.

The Data at Rest CP requirements ensure proper protection for classified data on a storage device.

A CSfC secure data-at-rest solution requires two independent layers of encryption. Typically, a combination of technologies is used, such as hardware (full disk encryption) and software (pre-boot authorization).

## GMS and Tactical Drives

With years of experience in rugged embedded computers, GMS is keenly aware of the importance of securing mission critical data.

GMS has partnered with top-grade SSD manufacturers to ensure data security at the highest level and is committed to providing the right SSD solution for each customer’s needs.

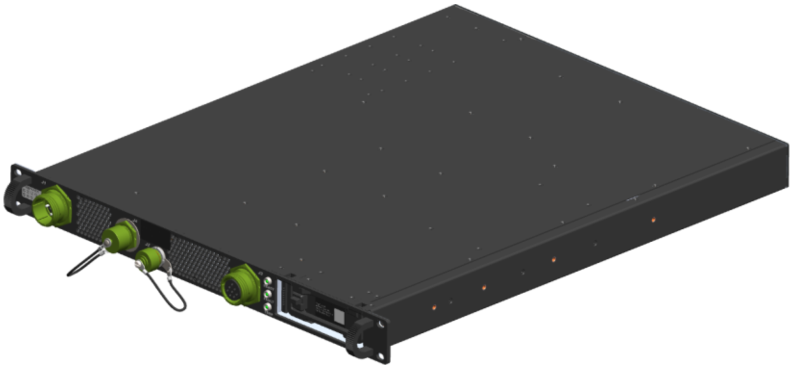
Capitalizing on these relationships with drive manufacturers, GMS has been able to introduce several products that incorporate FIPS 140-2 validated storage and is evaluating CSfC-certified drive options.

## Representative GMS Products with SSDs

**2.5" SATA Docking Station**

**SB1102-XV**
**Two removable nDrives™**
**(ruggedized sealed mSATA)**

**S1202-XVE**
**Removable 2.5" drive**
**(NVME/SATA)**



**TITAN CSSU**
**Removable canister**
**Eight 2.5" drives (NVMe)**

**SD1202-17**
**Removable nDrive™**
**(ruggedized sealed mSATA)**

**X9 SPIDER STORAGE**
**Removable canister**
**four 2.5" drives (NVMe/SATA) or eight M.2 2280**

## SSD Usage in GMS Products

| Form Factor | Interface | | | Certifications | |
|---|---|---|---|---|---|
| | SATA | NVMe | SAS | FIPS 140-2 | CSfC |
| mSATA | ■ | | | | |
| M.2 2230 | | ■ | | | |
| M.2 2242 | ■ | | | | |
| M.2 2280 | ■ | ■ | | ■ | |
| 2.5” | ■ | ■ | ■ | ■ | ■ |

**Note:**
Various GMS products implement custom pin configurations on the SSDs to allow external hardware control of the Secure Erase and Write Protect functions (Part of GMS’s .SecureDNA™)

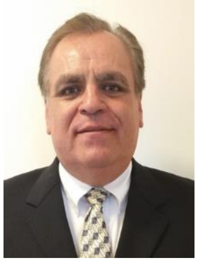
# Tactical Drives – SSDs and Security

*Protecting Mission Critical Sensitive Data*

By: Martin Cardenas

## Reference GMS Documents:

| | |
|---|---|
| 003-0004: | Application Brief: SecureDNA™ |
| 003-0009: | White Paper: SSDs Demystified |



Martin Cardenas is a Product Marketing Engineer at General Micro Systems. He transitioned to this position after a nearly 30-year career as a Software Engineer, primarily in the aerospace and defense sectors. He holds a Bachelor's Degree in Electrical and Computer Engineering.

**About General Micro Systems:**

General Micro Systems (GMS) is the industry expert in highest-density, modular, compute-intensive, and rugged small form-factor embedded computing systems, servers, and switches. These powerful systems are ideal for demanding C4ISR defense, aerospace, medical, industrial, and energy exploration applications. GMS is an IEC, AS9100, and MIL-SPEC supplier with infrastructure and operations for long-life, spec-controlled, and configuration-managed programs. Designed from the ground up to provide the highest performance and functionality in the harshest environments on the planet, the company's highly customizable products include GMS Rugged DNA™ with patented RuggedCool™ cooling technology. GMS is also the leader in deployable high-end Intel® processors and a proud Intel partner since 1986. For more information, visit www.gms4sbc.com.

For Sales inquiries, please contact: (909) 980-4863 option 1 (Eastern Time).