Self-Encrypting Drives and Commercial Solutions for Classified

The Self-Encrypting Drive, or SED, is a storage device that adds data security. The device, typically a solid-state drive or hard-disk drive, transparently encrypts all data written to the device and then decrypts it when data is retrieved from the device. In addition, it provides a locking mechanism that prevents unauthorized access to some, or all the data stored on the device.

SEDs are primarily storage devices with added capabilities for data protection. These SEDs roughly consist of:

1. Large amounts of non-volatile memory media, the backend of the storage device where all user data is stored.
2. A dedicated controller chip implementing all critical high-speed capabilities of the storage device, including a Full Disk Encryption (FDE) engine. It provides at-interface speed data encryption, typically using XTS-AES-256 cryptography.
3. A security subsystem managing device security specific tasks such as key management, device secure boot, and data access controls. Additionally, it exposes an interface through which the SED can be managed by its host system.

A SED provides data confidentiality through data access controls and instant secure erase functionality. It depends on encrypting all data stored on the device's media using a strong (symmetric key) encryption algorithm and high-quality encryption keys[*)]. Typically, SEDs have their encryption functionality enabled at factory time, implying that any data written to media has or is always encrypted.

Instant Secure Erase, also known as Cryptographic Ease, destroys a SED's existing encryption keys and generates new ones. All data encrypted with the destroyed key is no longer recoverable: the key is not available to decrypt any data. Additionally, when data is retrieved from the storage device the data is decrypted using the new key, resulting in an additional level of data scrambling. Destruction and generation of keys is typically done in about two seconds or less. This is significantly faster than overwriting all the device's media one or multiple times with random data, which can take hours or even days for hard disk drives.

The device's data access controls are enforced by the SED's security subsystem. Based on Trusted Computing Group's Storage specifications, the security subsystem exposes a protocol interface through which the host system can set access control policies. The device can be provisioned to support multiple data partitions each with their own encryption keys and access control credentials. Additionally, user and administrator accounts are selectively enabled or disabled. By authenticating with the proper credential, the host system can enable or disable data access by locking or unlocking one or more data partitions. Alongside data access controls, the security subsystem interface also supports management of other security sensitive device capabilities, such as enabling or disabling certain device level debug capabilities.

[*)] The topics of correct implementation of cryptographic symmetric key algorithms and the generation of high-quality keys with appropriate levels of entropy is outside the scope of this document. That said, these items are extremely critical to maintaining the data's confidentiality.

Commercial Solutions for Classified

There is an increasing need to secure data in Edge deployments. The Edge - in this case - is broadly defined as any computer system that is not installed within a data center protected by guards, guns, and gates. A subset of the Edge is the Tactical Edge: that part of the Edge physically located in contested areas or locations. Commercial Solutions for Classified (CSfC) approved solutions are increasingly targeted for Tactical Edge deployments where controlled or classified data is used.

CSfC is an NSA program that supports the deployment of commercial-of-the-shelf security solutions to protect data on national security systems. These solutions typically implement a layered approach using approved components from different manufacturers as defined in one of the CSfC approved Capability Packages (CPs). The CP most applicable to SEDs is the Data-at-Rest Capabilities Package. It requires two layers of data encryption using approved solutions and components. This layered approach of encryption, also known as Dual-DAR, lowers the risk of unauthorized disclosure in the event of a security failure in one of the components. The added requirement that different technologies and different component vendors are deployed significantly lowers the probability of both layers failing at the same time.

Any components used in a CSfC Dual-DAR solution must be on the CSfC “Hardware Full Drive Encryption” approved products list. Any listed product must pass an extensive review, successfully obtain a Common Criteria evaluation, and comply with CSfC specific protection profile selection criteria (where applicable). The relevant Protection Profile for Common Criteria evaluations of SEDs is the “collaborative Protection Profile for Full Drive Encryption - Encryption Engine Version 2.0 + Errata 20190201”. A unique property of the collaborative Protection Profile for Full Drive Encryption is that the evaluation is split between an Encryption Engine (EE) and Authorization Acquisition (AA) part. In most systems where the EE is implemented by a SED, the AA runs as software on the host system in which the SED is deployed. It provides an authentication and authorization mechanism for managing SED data access controls.

Software that implements a Common Criteria evaluated AA for SEDs is also known as Pre-Boot Authentication (PBA) software. It consists of a stripped-down operating system combined with a cryptographic library and functionality that implements multiple capabilities. These include configuration of users and user roles, user authentication with one or more factors (e.g., using a hardware token), logging and auditing, data access management, and crypto erase. The PBA is loaded in a special read-only partition of the SED and is executed during the system’s boot process. The user authenticates and unlocks data partitions, allowing the system to boot into its main operating system. In most cases the PBA is included as part of a larger software package that provides additional capabilities once the system is fully operational.

To meet CSfC’s dual-DAR requirements involves deploying an additional data confidentiality layer besides the one provided by the SED. In these scenarios the outer layer of the Dual-DAR solutions implements SEDs with an approved PBA, while the inner layer uses hardware and/or software components that encrypt individual files or file system volumes. The combined outer and inner layers provide the baseline of a CSfC Dual-DAR solution for data-at-rest security.