White paper

Self Encrypting Drives

Overview

Table of contents

Overview of Self Encrypting Drives

What is a Self Encrypting Drive (SED)?

A Self Encrypting Drive (SED) is a hard disk or a solid state drive that provides hardware-based data encryption. All data that is committed to the media is encrypted with either a 128-bit or 256-bit key. Because all encryption is handled in hardware, there is a great performance benefit to using SED over software based encryption. When using Software based encryption, all of the data written and read from the drive must be encrypted and decrypted by the system processor. This extra processing work can lead to noticeable performance degradation. With hardware encryption using an SED, there is not a noticeable change in performance.

All SED devices have the ability to create a Data Encryption Key (DEK.) The DEK is used to encrypt all of the data on the drive when written, and to decrypt the data when read. The DEK is generated by the drive, and is stored in an encrypted format in multiple locations on the drive itself. By default the SED device is unlocked, and the DEK is used to encrypt and decrypt writes and reads to the media. It is not until the drive is provisioned and locked that the data is fully secured. Provisioning a drive entails creating an Authentication Key (AK) that is used in conjunction with the DEK to read and write data to the SED.

Another benefit of using SED is the device can be securely erased in a matter of seconds, as opposed to several hours using traditional drive wipe methods. The SED can be instructed to change the DEK, rendering all data on the drive destroyed. The data remains in an inaccessible encrypted format that can no longer be accessed.

All SED devices sold by HP comply with the OPAL specification. The Trusted Computing Group created the OPAL specification. More information on the OPAL specification can be found on the Trusted Computing Group website: http://www.trustedcomputinggroup.org/

Provisioning and Locking an SED

As stated above, in order to fully secure the data on an SED, the drive must be at a minimum locked, and should be properly provisioned. Provisioning an SED requires SED management software. The management software guides the user through creating an Authentication Key (AK). The AK is used at power on to decrypt the DEK. If the correct AK is not provided, the drive remains in a locked state. Only after decrypting the DEK can data be written to or read from the SED. This provides what is called “data at rest” security. The information on the media is always encrypted.

ATA Drive Lock (HP BIOS)

Drive Lock is a part of the ATA standard, and restricts access to the SED unless the correct password is entered during POST to unlock the drive. Using ATA Drive Lock doesn’t require any additional software. In addition, when using ATA Drive Lock, an AK is not created on the SED. This means that the DEK is not encrypted, and is considered less secure. If possible, the drive should be properly provisioned as described in the next section.

The specific procedure to enable ATA drive lock can be found in the Workstations Maintenance and Service Guide. This guide can be found for all platforms at the HP Workstations Business Support Center website: http://www.hp.com/go/workstationsupport/

SED Management Software

SED Management software helps with the administration of SED in your specific environment. These tools offer features like security compliance, data protection policies, reporting, data recovery, and an interface which simplifies management. HP offers an SED management software solution as a part of HP ProtectTools.

There are also many third party software packages available for SED management. Available management features vary by manufacturer. A list of TCG OPAL approved vendors can be found on the Trusted Computing Group Website: http://www.trustedcomputinggroup.org/

HP ProtectTools

HP ProtectTools is included with all HP workstations that ship with an SED. To provision the SED, use the following procedure:

- Install HP ProtectTools Security Manager / Credential Manager
- Install Drive Encryption for HP ProtectTools
- After rebooting, the HP ProtectTools Security Manager Setup dialog will appear
- Click on the 'Next' Button to proceed with the setup process
- Input your Windows Password, then click 'Next'
- Provide input to setup your SpareKey, then click 'Next'
  - This process is optional and can be skipped
- The next screen allows you to enable Windows Logon Security and/or Drive Encryption
  - If you only want to enable Drive Encryption, you do not have to enable Windows Logon Security
  - For the purposes of this document, it is assumed that Windows Logon Security is enabled
- Select both Windows Logon Security and Drive Encryption, then click 'Next'
- Select the drive you would like encrypted, then click 'Next'
  - There is an available option in this dialog box to 'Disable Sleep Mode for Added Security'
  - For the purposes of this document, it is assumed that sleep mode is not disabled
- Reboot the system when prompted

SED Setup and Boot Process

During the provisioning process of the SED using HP ProtectTools Drive Encryption Services, the following steps are followed:

- Password (AK) is established.
- Shadow Master Boot Record created on SED.
  - This allows the use of a pre-boot OS to allow the entering of the password (AK) to unlock the drive, enabling access to the data stored on the device.

After completing the setup process for the SED, the boot flow of the Workstation is as follows:

- System BIOS attempts to read Master Boot Record of the SED.
- System BIOS is redirected and loads the pre-boot OS.
- The user authenticates by entering the password defined during the setup process.
- If authentication is successful, the pre-boot OS passes control to the original MBR and the OS on the SED loads.
- If authentication is not successful, the machine is unable to boot.

Supported Configurations of SED in HP Workstations

SED devices can be configured as both boot and data devices within HP workstations. Multiple SED can be provisioned within one HP workstation as standalone drives. As the DEK for each drive is unique, the DEK and AK hash will be unique for each drive, despite using the same AK for multiple SED devices.

Configurations not supported in HP Workstations:

- RAID configurations with SED devices are not allowed
- Flash Cache SSD modules used with the Intel SRT software are not supported with the use of an SED HDD. The Intel SRT software configurations requires that the cache module and the HDD be configured in a RAID array, thus it cannot support an SED device.

Learn more at
hp.com/

Sign up for updates
hp.com/go/getupdated

Additional Resources
www.hp.com/go/whitepapers

Solutions Guide for Data-At-Rest in PDF found at Trusted Computing Group website.