SECURITY FRAMEWORK OF HARD DISK DRIVE

Khanob.thongkhome
Somsak Choomchuay

PROBLEM STATEMENT

The risks to organizations of losing confidential data stored on hard drives in PCs and servers cannot be ignored. Utilizing password security to protect data on hard drives is better than relying on BIOS or operating system passwords, but it is not strong enough for most organizations. Hard drive password security can be easily defeated by an attacker, either through a service or by obtaining password-cracking tools from any number of sources. Because hard drive password systems do not encrypt the actual data, a broken password routine allows full access to the data on the drive. This means that hard-drive ATA password security alone is not secure enough for protecting anything but casual data. For most organizations, obtaining adequate protection of sensitive data on their hard drives requires encrypting that data. Software-based full drive encryption systems are one solution, but the next generation of encrypting hard drives have important advantages over the software-only solutions and will certainly be of value to any organization with high-value or regulated information.

Since the first FDE(Full disk encryption) hard disk drive was announced by HDD manufacturing to support customer for against unauthorized access to information stored on laptop PCs, even if they are lost or stolen. It is more powered by many HDD manufacturing, a groundbreaking security platform that couple strong, fully automated hardware-based full disk encryption with leading security-based software applications to deliver centralized encryption management, multifactor user authentication and other capabilities that help lock down personal computer and data center storage. All of them are used AES (Advanced Encryption Standard) encryption algorithm that was qualified by NAS (National Security Agency) and NIST (National Institute of Standard and Technology).AES is a symmetric block cipher that can process data block of 128 bits, using cipher keys with lengths of 128, 192 and 256 bits (Depend on HDD manufacturing).

There is some confusion around the market for FDE products. Are 128 or 256 bits key length clearly sufficient to address all commercial and non top secret government application?. Are more energy should be focused on solution-level deployment issue when put encryption engine to the rest?. How is it operation speed?., etc. To answer that question, It's necessary to define "better". Given that we are studying and focusing in technical details about FDE to establish FDE hard disk drive hardware prototype for deeply study it properties and finding the way to improve some weakness of FDE hard disk drive to meet customer requirement.

What is FDE drive?.

FDE(Full disk encryption) drive is a disk drive with security processor on board, encrypting the data on the fly. FDE did not require any special support from the OS. The drive is fully autonomous. All it needs is a BIOS supporting ATA Security commands. The security ASIC chip on the drive generates a unique AES key to encrypt all data. When the drive is not locked, the key is always released by the security processor and data is transparently encrypted on writes and decrypted on reads. Hence it works just like normal drive, you can write / read anything to it. The only difference is, what is actually written to the drive platters, is AES-encrypted. When you lock the drive (by setting a password in BIOS), the password you set is a wrapper for the key. The security chip on the drive releases the key only when you enter the right password at boot time. Easy and transparent. Buy an FDE drive, install whatever you need on it (the OS and your programs and data) and when you are happy, just set the BIOS password. The data has already been encrypted, and by setting the password you are taking control of the encryption key.

Today the FDE drives are the most secure option to protect your data on a hard drive. And they are the least troublesome option at the same time. From the user's perspective, the overhead is very low - just to enter a password at boot time. No extra software, installation, maintenance, special partitioning needed... Almost plug and play. Plus there is one extra benefit. When you want to wipe the drive, instead of reformatting it, just drop the encryption key. The data left on the drive will be just a noise from that point.

FDE Key Advantages.

- Protects data and enables companies to be in compliance with an increasing number of regulations
- Easy to implement and manage, as encryption is always on
- No impact on system performance, unlike software encryption
- Only drive accepted by the National Security Agency (NSA) to protect classified, mission-critical and national security information
- Works with multiple security software applications to provide greater functionality
- Adopted by global companies and government agencies with the highest standards of security protection