BLOCKMASTER
Security Through Innovation

7 Major Weaknesses with Software Encryption of USB Flash Drives

1. Software Encryption (AES256) Is as Weak as the Password.

A six-character password guarding a soft-encrypted USB flash drive takes half an hour to break on your average home PC! To make good use of AES-256 strong encryption technology, a secret key of adequate length is needed. "Adequate" here means 50 characters, using numbers and letters. Since this is software-based encryption, the only key is the user's password. Few users can remember a key of such length. But by using just an eight-character password of letters, numbers, and even special characters, the user is only availing himself of an infinitesimal (0.00000000000000000000000000000000000000000000000000000000000025%) portion of the encryption security available, as expressed in the formula (3*10^15/2^256). In contrast, a hardware encryption device such as a SafeStick generates its key within its embedded system on the flash drive itself, and applies 100% of the available encryption power, no matter the password length or complexity. SafeStick's encryption is as strong as the algorithm itself, not as weak as the password chosen by the user.
The use of software to encrypt desktop hard drives is commonplace and should be encouraged, but when it comes to encrypting USB flash drives, only hardwarebased encryption makes sense.

2. Software Encryption Is Open to Quick and Easy Attacks.

Anyone who has access to the software-encrypted USB Flash Drive for as little as one minute can copy the softencrypted files (often one big file container). The copy can then be attacked without the user ever knowing it. Software to do this is readily available for download. In hacker lingo, this is called parallel offline attack.

3. Software Encryption Is Expensive and Time-Consuming.

All desktop software can be expensive to support, but softencryption software products for USB flash drives are susceptible to problems, since they are used in different environments every day and can easily be infected or break. Software encryption almost always results in big problems down the road.

4. Software Encryption Can Easily Lead to Information Exposure and Data Corruption.

To adequately protect data, it should be stored on highquality flash drives with wear leveling. That's because cheaper drives with no wear leveling will break down over time and corrupt data. It is an accident waiting to happen sooner than later. But for security reasons it is not recommended to use wear leveling in combination with software-encryption.
From soft-encryption leader TrueCrypt.org:
This [use of wear-leveling usb flash devices] may have various security implications. For instance, when you change a volume password/keyfile(s), the volume header is, under normal conditions, overwritten with a reencrypted version of the header. However, when the volume resides on a device that utilizes a wear-leveling mechanism, TrueCrypt cannot ensure that the older header is really overwritten. If an adversary found the old volume header (which was to be overwritten) on the device, he could use it to mount the volume using an old compromised password (and/or using compromised keyfiles that were necessary to mount the volume before the volume header was re-encrypted). Due to security reasons, we recommend that TrueCrypt volumes are not stored on devices (or in file systems) that utilize a wearleveling mechanism.

The risk of data corruption on soft-encrypted data containers is also much higher than for the normal file system. Recovery of corrupted data is an expensive undertaking.

5. Software Encryption Can Be Tampered With.

It is easy to change the way a software encryption product functions. The Internet is loaded with devious applications set up by opportunistic, criminally minded people waiting to infect your encryption product. Once they've succeeded, you'll be running their altered code and you may never even know it.

6. Software Encryption Is Slow.

Since software encryption depends on the host computer for its operation, it is usually very slow, operating at 5%-15% of the speed of most hardware encryption devices. Software encryption is nevertheless a resource drain and can leave other programs running sluggishly or render them completely unresponsive.

7. Software Encryption Can Be Disabled, Deleted and Misleading.

Encryption is intended to keep stored data secure at all times. But when physically transporting a storage device from point A to point B, it can be well outside of the corporate network and the corporation's physical protection plan. The encryption software can be deleted (unintentionally or maliciously) and then stored data will be unprotected. A novice user might believe he is protected and take risks he might not take otherwise. Without hardware encryption, the corporation can suffer enormous, even catastrophic, loss of information and public goodwill.