Countering the Threat to the Digital Lifestyle

Encryption and USB Drives

8GB of Data
2,000 songs - or your company marketing strategies
2,500 vacation pictures - or your company employee records
4,000 e-books - or your personal diary

Super Talent Technology, Inc.
2077 N. Capitol Ave., San Jose, CA 95132 · Tel: (408)934-2560 · Fax: (408)719-5020
www.supertalent.com

The Need to Protect Digital Data

Before the widespread use of the Internet during the 1990's, only the military protected their digital data using encryption. But, as digital information became a bigger part of everyday life and in order to continue to protect privacy, encryption became more important to businesses, companies, and even to the average user. Electronics have invaded our everyday life at work and at home; we've gone from day planners to PDA's, from film cameras to digital cameras, and from rotary-dial phones to mobile phones.

Electronic devices make it easier to hold and pass around information. For example, a massive collection of data, such as a library, can be squeezed to fit an 8GB memory device. Today, people can even use their cell phones and media players to carry around songs, photos and files. But the most popular device to hold digital information for business users and end users alike is the USB Flash drive, otherwise known as the "thumb drive" or "pen drive."

The USB drive has the "ability to take vast amounts of information in a single go via an item which is commonly available, easy to conceal and even if discovered would arise little or no suspicion [1]." This constitutes a possible security risk since any type of information can be held in a USB drive. For example, "the personal information of 6,500 current and former University of Kentucky students, including names, grades, and Social Security numbers, was reported stolen May 26 after the theft of a professor's Flash drive [2]."

Flash memory manufacturer Sandisk analyzed thumb drive usage patterns and reported that portable drives can damage a company through the possibility of losing sensitive data. Figure 1 shows the Sandisk's survey results as a breakdown of the type of private information that professionals carry on a USB Flash drive [3].

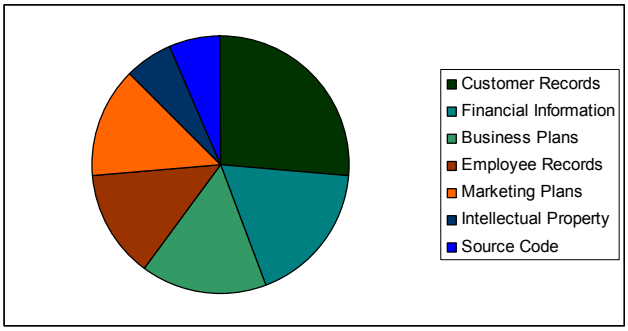

Figure 1: Flash drive usage categorization [3]

As illustrated in the graph, thumb drive users regularly carry confidential information for work purposes. If the USB drive is lost or stolen and the data is not protected, then companies can be hurt if sensitive information falls in the wrong hands [3].

Thus, a method needs to be implemented so that data can be kept restricted from people who are not supposed to have access. Data encryption provides the best method to protect confidential information.

What is Encryption?

Encryption is an algorithmic scheme in which data is converted into a format that has no resemblance to the original data. An *encryption key* provides instructions for how to encode the data. Figure 2 illustrates the basic encryption process.

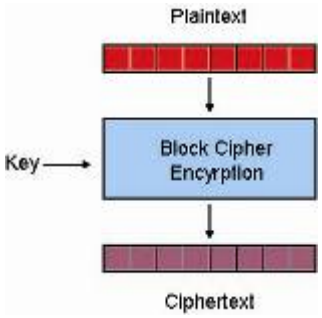

Figure 2: Encryption Process

The key must be re-used in order to transform the data back into the original readable format. This step is known as *decryption*. Both the sender and the receiver must possess the encryption key in order to perform the encryption and decryption process.

Why Encryption is Needed

Long before the advent of personal computers, or even electricity for that matter, there was a need to transform plain text messages into a format that only the intended receiver could read. For example, war-time spies who sent messages back to their home governments often needed to ensure that the enemy never intercepted these messages in order to preserve the sender's safety.

A noteworthy historical example is the German military's use of the *Enigma* encryption machine during World War II. The Enigma machine was a mechanical

encryption key which used a complex arrangement of spools and wires to encode messages. The ability to send secure coded messages gave the German navy a strategic advantage. U-boats used Enigma machines to conceal messages containing convoy sightings and their periodic positions. Without the Enigma, these messages could not be kept secret since they were constantly intercepted by the Allies.

The British were finally able to decrypt the Enigma messages, changing the course of the war to the Allies' advantage during the Battle of the Atlantic. This example shows the importance of keeping your information secure. The Allies were able to decode the messages because the Enigma machine used an inadequately complex encryption method, and due to a parts of the encryption key being revealed through carelessness and, once, the capture of an Enigma machine from a German U-boat.

Modern encryption works by the same principles as the Enigma machine, though thankfully newer methods encrypt data so well that it cannot be decrypted without the key. To close or tighten the security gap inherent in portable USB Flash drives, we must use encryption. There are a variety of encryption types and methods of applying them. This whitepaper will discuss several USB drive data encryption strategies.

Encryption Schemes

There are three methods to encrypt digital data on USB drives: manual, semi-transparent and transparent.

Manual Encryption

With manual encryption, a user manually selects each file to encrypt or decrypt. Consequently, the user has to remember to run the encryption process for each file they want to protect. This method requires only basic encryption software on the user's computer. This method is the least safe because the user can forget to encrypt their files [4].

Semi-transparent Encryption

In semi-transparent encryption, encoding operations are done before or after access is made to confidential data. For example, a user can configure encryption software to decrypt their files when their computer boots up and encrypt them when the computer shuts down. A USB Flash drive might employ semi-transparent encryption by decrypting the drive's files when the drive is

connected to a computer, and then encrypting them before the user is allowed to disconnect the drive. This encryption method is less risky than the manual type of encryption since it is automatic; the user does not have to remember to encrypt their data [4].

Transparent Encryption

Completely automatic, transparent encryption is the most robust encryption scheme. Data is encrypted as it is written and, as a result, requires no interaction from the user. The theft or loss of a USB drive which uses transparent encryption does not mean that there is a loss of data, because the drive's data is always encrypted. Although this is the best type of encryption, it is also the most difficult type to implement in a USB drive because it is difficult to engineer into the drive architecture [4].

Transparent Encryption in USB Drives

To fill the need for secure portable storage, some USB Flash drive makers include transparent encryption in their products. Drive engineers can choose either software-based encryption or hardware-based encryption.

Software-based Encryption

In software-based encryption, the files that perform encryption are stored in a USB drive's Flash memory. As with typical unsecured USB drives, when the drive is plugged into a computer's USB port, it is immediately connected to the system. Because the encryption program is stored in a fully accessible part of the drive, hackers can locate the program in the USB drive's memory and compromise it. The encryption software itself cannot be protected any more than any other Windows program, or the operating system wouldn't be able to run it.

Another disadvantage of software-based encryption is that the password has the ability to be rewound, or "returned to a backed up state so that any password you may have created recently or after you had stored the files can be removed as if it had never been installed [5]."

An additional drawback of software-based encryption is that it uses the computer system's microprocessor to perform encryption and decryption.

Figure 3: Software-based Encryption Process [5]

The encryption process is slower than hardware encryption because bottlenecks occur when unencrypted data is processed into encrypted data due to the strain it puts on the processor. Bottleneck size increases as the amount of files to be encrypted increases [5].
Not only that, the price to have software-based encryption on the USB drive is higher than hardware-based encryption. This is because USB drive manufacturers have to pay for the software-based encryption's licensing and controller fees.

Hardware-based Encryption

Hardware-based encryption is more secure than software-based encryption. Encryption files are kept in a separate chip in the USB drive. When the USB drive is plugged into a computer, the user is required to give the correct password before it will connect to the system. If the drive is not connected to the computer system, hackers cannot hack your files. This encryption type allows users to set a password counter, which is the amount of time[s] to enter the correct password. If the incorrect password is given too many times, the drive will shut itself off and the data can never be retrieved [6].

Bottlenecks do not occur during hardware-based encryption because there is real time encryption processing. This makes hardware-based encryption faster than software-based encryption.

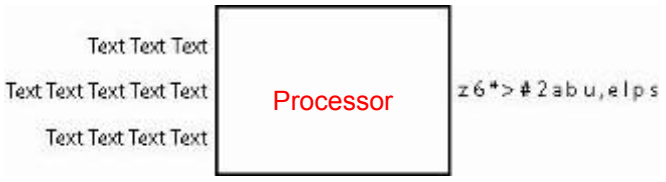

Figure 4: Hardware-based Encryption [5]

Instead of the computer's CPU processing the encryption, the USB drive has dedicated hardware to perform the encryption. Thus, your computer still performs similarly to an unencrypted computer [11].

There are other features that can be added to hardware-based encryption. An example is *Smart Chips*. Smart Chips do not allow the Flash memory chips to be removed from a USB drive. If the Flash chips are removed, the data is automatically deleted [7].

Another feature is *Locking & Deletion*, which "runs off a separate chip that deletes and re-writes over the data so it cannot be restored [7]." This situation happens when the wrong password is given too often.

Although hardware-based encryption is cheaper and safer than software-based encryption, not all USB drive controllers can support this method. Thus, software-based encryption is still widely used.

Deciding which encryption method is best for a user is dependent upon the user's application. Each approach has its own benefits and drawbacks in relation to cost, support and implementation.

How Secure is Modern Encryption?

AES, an acronym for "advanced encryption standard," is the standard for encryption today. The US government states that "AES is a National Institute of Standards and Technology (NIST) specification for the encryption of electronic data. It is expected to become the accepted means of encryption digital information, including financial, telecommunications and government data [8]." It has been said that this encryption method will be sufficient to protect data for the next 20 to 30 years [8].

AES Basics

AES is an iterative, symmetric-key block cipher that can use keys of 3 different sizes. AES encrypts and decrypts data in blocks of 128 bits. The following shows the strength of each of the three cipher keys.

Key Size: **128-bit** = 10 x (3.4×10^{38}) possible 128-bit keys

Key Size: **192-bit** = 12 x (6.2×10^{57}) possible 192-bit keys

Key Size: **256-bit** = 14 x (1.1×10^{77}) possible 256-bit keys

"The cipher is specified in terms of repetitions of processing steps that are applied to make up rounds of keyed transformation between the input plain-text

and the final output cipher text. A set of reverse rounds are applied to transform cipher-text back into the original plain-text using the same encryption key [9]." Increasing key sizes not only scrambles the data better but also increases the complexity of the cipher algorithm.

Both software- and hardware-based encryption employ AES. AES improves on earlier encryption methods by providing faster encryption and increased security due to its larger key size. Furthermore, AES is easy to implement and takes up little memory on the USB drive.

To give a sense of how secure AES is, if a machine can crack 2^{55} keys/second, then it will take 149 trillion years to crack the 128-bit AES key. The universe is less than 20 billion years old [10].

1. Device Wall from Centennial Software, *The Threat of Lifestyle Computing in the Enterprise*, February 2005 Issue 1.1
2. Swartz, Jon, *Small drives cause big problems*, August 16, 2006, USA Today
3. SanDisk, *SanDisk Survey Shows Organizations at Risk from Unsecured USB Flash Drives*, April 9, 2008, Press Room Press Releases
4. http://services.devadvisers.net/cryprite/042ETYPE.HTM, *Three Types of Encryption*
5. Via, *Why Hardware Encryption is Better Than Software Encryption*, http://services.devadvisers.net/cryprite/042ETYPE.HTM
6. encryptedusb.net, *Software Vs. Hardware Based USB Encryption*, April 5, 2008
7. encryptedusb.net, *Hardware Based USB Encryption*, April 5, 2008
8. McCaffrey, James, *Keep Your Data Secure with the New Advanced Encryption Standard*, 2008
9. Wikipedia, *Advanced Encryption Standard*,
10. Dyke, Jim & Francis, Trevor, *Commerce Secretary Announces New Standard for Global Information Security*, NIST News Release, December 4, 2001
11. J.D Hietala, *Hardware versus Software*, September 2007, A SANS Whitepaper