ENCRYPTION

The Perils of Using the Wrong Approach to USB Flash Drive Security

Only Hardware Ensures that Data Stays In and Malware Stays Out

January 9, 2008

IRONKEY
THE WORLD'S MOST SECURE FLASH DRIVE

350 million USB flash drives are in use worldwide.

The Perils of Using the Wrong Approach to USB Flash Drive Security

Only Hardware Ensures that Data Stays In and Malware Stays Out

A seemingly endless string of headlines trumpeting high-profile data breaches has helped to make organizations aware of the risk of data loss inherent in portable storage devices. In addition to the obvious requirement to secure the intellectual property and competitive business information stored on these devices, enterprises need to shelter themselves from the significant cost of noncompliance with new laws designed to safeguard personal data. Encryption not only protects this critical data but also offers safe harbor from the costly remediation and embarrassing public disclosures mandated by HIPAA, California's SB1386, and similar privacy laws.

86% of enterprises use USB flash drives to store and exchange data.

However, all encryption technologies are not created equal. In the face of growing threats that range from organized cybercrime operations to careless employees who lose drives or do not follow established security policies, enterprises should deploy the most effective encryption available. Since even the best encryption is useless if an attacker can guess the password or access the encryption keys, it is critical to select a solution that properly protects passwords and keys.

While software encryption programs, which are widely deployed to protect computer hard drives, provide an important layer of defense, they are vulnerable to decryption. This paper examines how the IronKey flash drive uses hardware-based encryption and key management within a highly secure framework—including a physically hardened enclosure and the US government's recommended mode of AES encryption—to eliminate physical and logical avenues of attack. It also details how the same hardware-based approach that delivers superior protection against critical data slipping out of the system also ensures that malicious code doesn't leak in.

52% of enterprises have lost confidential data through removable media such as USB drives in the past two years.

Vulnerabilities of Software Encryption

Brute Force Password Guessing

Most modern software encryption solutions employ AES for bulk data encryption, which is generally considered unbreakable. According to the US government, "it would take approximately 149 trillion years to crack a 128-bit AES key." Nonetheless, software encryption relies on a password. And cracking a password can take less than a second.

Even a casual hacker can download inexpensive password-guessing software that works by trying combinations of dictionary words or every possible combination of passwords until the correct one is found. Additionally, attackers can augment these brute force attacks by using rainbow tables. Rather than trying all the possible plaintexts one by one, this technique dramatically reduces the time required to crack a hashed password with a "time-memory trade-off technique" that essentially does all the cracking computations in advance and stores the results in a table.

“The number of publicly reported data breaches in the US rose by more than 40% in 2007.”
ITRC

More sophisticated password guessing machines—designed for use by law enforcement, but also readily available—can test more than 50,000 passwords per second. Worse yet, connecting these machines in parallel can enable an attacker to make 250,000 password guesses per second.

Some software implementations attempt to thwart brute force attacks by using a counter that tracks the number of failed login attempts. But a hacker can easily breach this defense with a memory rewind attack. All this requires is making a copy of the encrypted data and the encryption software's temporary files before beginning the attack, and then simply reinstating the original files after every password-guessing attempt. This vulnerability makes it impossible for the software implementation to prevent brute force password or key guessing attacks. Many hardware-based encryption systems are also vulnerable to these types of attacks if they store a counter in flash memory—the attacker simply rewinds the counter after a few attacks.

IronKey prevents this type of attack because the IronKey Cryptochip incorporates a hardware-based internal password counter that cannot be tampered with or reset. Furthermore, a hardened package and self-destruct capability ensure that no attacker can access the Crytochip in an operable state.

“In 2007, the average cost of a data breach was $6.3 million.”
Ponemon Institute

Parallel Offline Attacks

If the media is mountable as an encrypted volume, attackers also have another option. They can simply copy the encrypted data and work offline at their leisure. The attacker can replicate the encrypted data onto another machine or any number of machines linked in parallel and have them guess passwords or keys. Russian software maker Elcomsoft has recently upped the ante with a program that allows attackers to run NVIDIA high-speed accelerator cards—essentially small supercomputers available at a consumer price point—to guess millions of passwords per second.

Botnets further represent a potential new threat vector. Criminals have created many large botnets that hijack thousands or tens of thousands infected PCs. These computers are then unwittingly employed for spam, phishing, and password stealing. For example, in May 2008, the Srizbi botnet was discovered to be sending 60 billion spam messages per day. Another “zombie network,” the so-called Storm botnet, has access to more computing power than the world's top 10 supercomputers combined. Botnets such as these could also easily be used for distributed encryption password guessing attacks, and with a combined RAM capacity of between 1 and 10 Petabytes, they have the potential to store some rather enormous rainbow tables.

Unlike software-based encryption, a properly implemented hardware-based encryption system prevents such attacks by not mounting the device onto a PC until the correct password has been entered. This prevents an unauthorized user from copying the contents of the drive to a host PC for replication. IronKey drives are designed to prevent these types of attacks by not mounting the media until the correct password has been entered and authenticated in hardware.

Even when the encrypted volume cannot be mounted, some hardware devices could still be vulnerable to a parallel offline attack. In the case of most hardware encrypted flash drives, if the attacker could disassemble the device, remove the flash memory chips, and install them onto a custom circuit board, it would be possible to copy the contents of the memory chips. IronKey makes this type of attack virtually impossible by embedding the chips in a special epoxy potting compound and a tamper-proof casing. These measures make it extremely difficult to get the memory chips off the printed circuit board without destroying them in the process.

An IronKey flash drive is more secure than a typical personal computer.

Malicious Code Vulnerabilities

In addition to the perils posed by unauthorized users gaining access to critical data, conventional USB flash drives can allow viruses, worms and other malicious code to penetrate the IT system. And today's enterprises and government agencies must guard against potential threats ranging from cyber-vigilantes to hostile governments. This is why the IronKey solution—which was funded in part by the US Department of Homeland Security—has from the outset included an array of defenses against these types of attacks. The same hardware-based approach to encryption that protects critical data from unauthorized access also makes an IronKey drive a trusted platform for mobile data. In fact, because authentication is performed in hardware using unique digital certificates, an IronKey flash drive is more secure than a typical personal computer.

The IronKey secure mobile data solution allows organizations to gain the productivity benefits enabled by employees using USB drives while providing an unrivalled set of malware protections that includes:

IronKey devices will not function without secure and digitally signed and verified firmware and software.

Malware-protected software and firmware updates — IronKey devices can be updated remotely via a secure update service. All firmware and software is validated by industry leading 2048-bit RSA digital signatures, preventing the installation of malicious software or firmware onto IronKey devices.

Secure manufacturing processes — Unlike many computer hardware products that are manufactured in offshore, uncontrolled factory environments, all IronKey devices are designed and assembled in the USA, which dramatically reduces that risk of hostile factories implanting malware onto silicon or memory chips during the manufacturing process.

Secure provisioning and quality assurance processes — IronKey devices will not function without secure and digitally signed and verified firmware and software. These software and firmware images are developed, security scanned, anti-malware scanned, and digitally signed at IronKey premises in the USA. All IronKey devices are inoperable until they are loaded with verified and scanned software and firmware from IronKey headquarters. This provides a security validation that is unmatched in the industry, ensuring that IronKey devices have not been tampered with in the manufacturing or supply chain process.

Real-time anti-malware scanning — IronKey is integrating best-of-breed anti-malware scanning technology to prevent malware residing on untrusted computers from infecting IronKey secure storage devices, and then spreading into corporate and government networks. IronKey has numerous patent-pending technology innovations that leverage the power of the onboard crypto-processor to enable anti-malware protection in the hardware on the IronKey device to protect data and networks—without requiring the installation and operation of software or drivers on host computers.

Top-tier US-based ASIC security processor design team — IronKey's continued innovation in the areas of intelligent security processors on very small form-factor portable storage devices—particularly USB flash drives or memory sticks—allows IronKey to deliver the world's most secure flash drive with intelligent on board anti-malware and anti-crimeware technology. IronKey has a top-tier ASIC security processor design team that develops the world's most secure, intelligent security processors for secure storage and authentication. The integration of intelligent security processors into standard USB flash drive formats provides affordable, easy-to-use, and effective protection against data loss, data leakage, and malware for enterprise and government customers.

IronKey stores all encryption keys onboard the hardened drive.

Attacks on Encryption Keys Stored in RAM

Like passwords, encryption keys represent another weak link encryption solutions. Software-based encryption programs store the decryption keys in RAM, and even after power-down they stay in RAM for several minutes. Cooling the RAM chips can preserve the data for much longer. If an attacker gains access to a computer recently after it was powered off—or if the user put it to sleep—the encryption keys can be recovered and the attacker will have access to the entire contents of the device. This so-called "cold boot" attack was recently documented in a study by researchers at Princeton University, who used a widely available aerosol computer cleaning spray to cool the RAM chips of a PC running hard disk encryption software.

Properly implemented hardware-based encryption solutions such as IronKey do not store the encryption keys in RAM, and thus are not vulnerable to cold boot attacks. IronKey stores all encryption keys onboard the hardened drive.

IronKey users can use other people's PCs without leaving a software footprint behind.

The Need to Install Drivers

Another shortcoming of most encrypted flash drive solutions is the need to install drivers (or special client software) on the host PC before files can be copied onto or off the drive. This approach also means that to use another person's computer the flash drive user must install drivers onto that machine as well. Furthermore, it usually limits the types of computers on which these devices can be used, which typically eliminates Macintosh and Linux machines. And it exposes these other PCs to risks from incompatible drivers, driver bugs, and malicious code installation—not to mention malware could also copy software encryption keys.

In IronKey devices, the onboard hardware handles all the encryption functions, eliminating the need to install any software on the PC. IronKey users can use other people's PCs without leaving a software footprint behind.

Risk of Using the Improper AES Encryption Mode

Whether the encrypted flash drive uses hardware or software to perform the encryption, it is important that it implement the encryption algorithm in the recommended mode. In other words, it is possible that the device is FIPS 140-2 Level 2 validated, yet uses the wrong mode of encryption.

The easiest AES encryption mode to implement is Electronic Codebook (ECB). However, this approach encrypts identical blocks of plaintext into identical ciphertext blocks. This method does not provide serious confidentiality for files.

In AES Cipher-Block Chaining (CBC), each ciphertext block is dependent on all plaintext blocks processed before it. This provides a much greater degree of security, but it is much harder to implement in a high-speed hardware approach, especially when using NAND flash memory.

To ensure the highest security, IronKey uses AES 128-bit in CBC mode, and with encryption keys generated by a hardware-based random number generator within the protected Cryptochip. As a result, the IronKey cryptographic module is certified as FIPS 140-2 validated at Level 2 by the US National Institute of Standards and Technology and by the Canadian Government's Communications Security Establishment.

IronKey provides always-on data protection.

Summary

An increasingly mobile workforce depends on USB flash drives as indispensable tools. However, in an environment of increasing security risks and stricter regulations, security professionals must find ways to protect the data stored on these devices without limiting the productivity benefits they provide. With their small form factors, flash drives are easily lost or stolen. But because they can carry everything from legally protected consumer data to critical IP to national secrets, the price of allowing unauthorized access to files is too high to pay. The mobile nature of these devices also means that, without the proper protections, they can open avenues of attack via worms, viruses and other malicious code.

Consequently, organizations are looking for the most secure way to protect data stored on flash drives. In the event a drive is lost or stolen, encryption not only protects critical data from unauthorized access but also provides safe harbor from the disclosure requirements of some privacy laws. Nonetheless, encryption solutions are only as secure as the encryption keys and passwords. Because software-based products store passwords and encryption keys in RAM they are vulnerable to brute-force password guessing, parallel offline, and cold boot attacks.

Many vendors of hardware encryption also do not understand that AES has several different modes, and it is possible to be FIPS 140-2 Level 2 validated, yet use the wrong mode of encryption.

Unlike software-based solutions, IronKey drives generate and store strong, random encryption keys in hardware, and all data stored on an IronKey drive is encrypted with the only mode of AES data encryption recommended by NIST. A hardened physical enclosure and anti-tampering measures also protect the encryption chip and flash memory. This hardware approach provides superior data protection by preventing password guessing as well as attacks that attempt to reset the password counter or steal encryption keys from memory.

Additionally, IronKey devices prevent parallel offline attacks because the media does not mount until the correct password has been verified in hardware. This and other hardware-based defenses further protect against malware and crimeware infecting an organization's PCs or network.

This superior protection is also "always on," and careless users or malware cannot disable it. Additionally, IronKey hardware encryption not only runs faster than any software-based encryption system but also improves security and ease-of-use by eliminating the need to install drivers on the host computer.

CONTACT US:

www.ironkey.com
sales@ironkey.com

5150 El Camino Real, Suite C31
Los Altos, CA 94022 USA

T 650 492 4055
F 650 967 4650

1. *Making a Faster Cryptanalytic Time-Memory Trade-Off (Philippe Oechslin)*
2. *Lest We Remember: Cold Boot Attacks on Encryption April 2, 2008. Princeton, EFF, Wind River Systems*