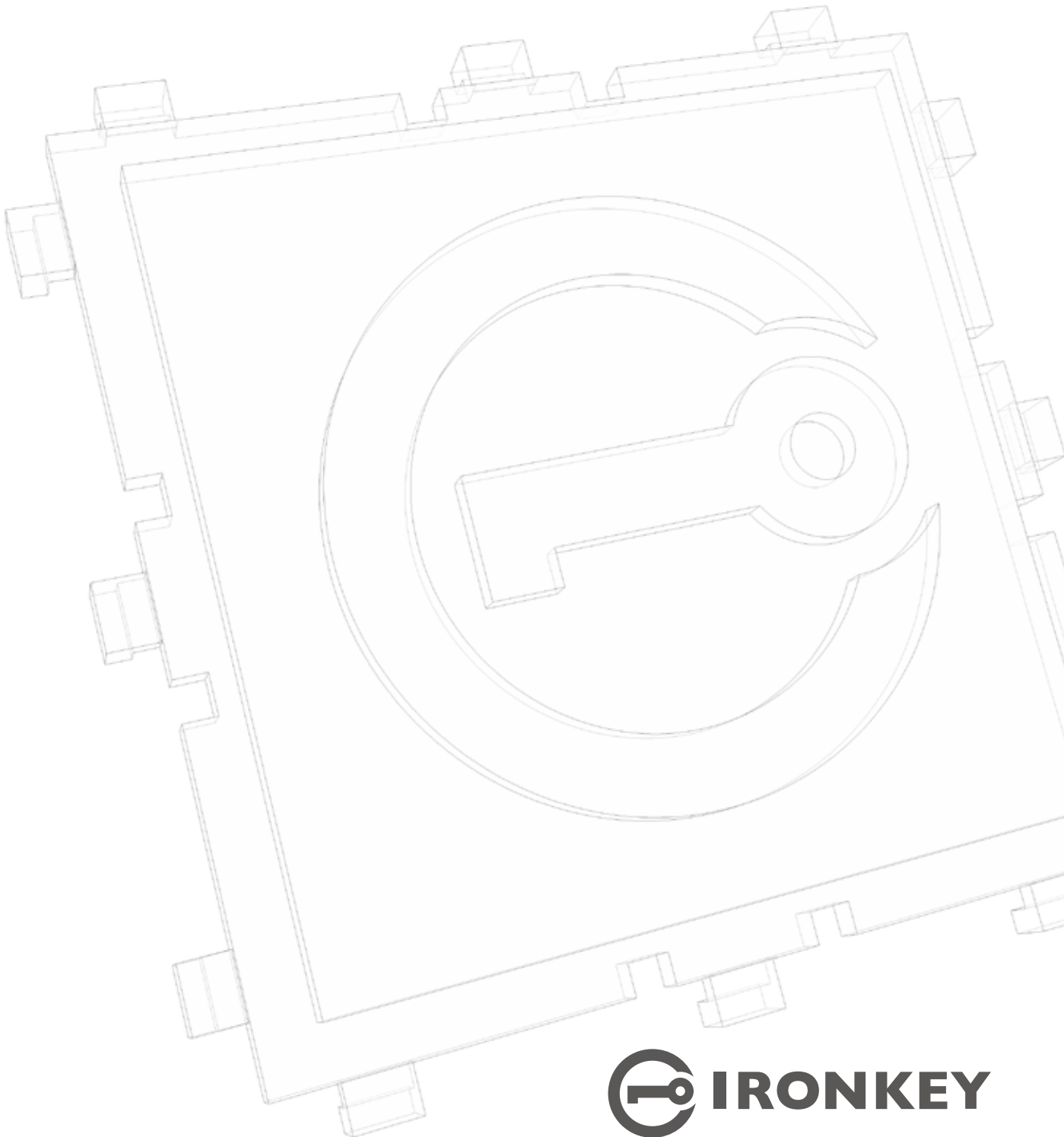


Benefits of Hardware-Based Encryption

An IronKey Whitepaper
February 2007



Introduction

Portable storage devices are a popular way to transport files between computers and to backup important information. However, the ubiquity of these devices heightens the security concerns of carrying confidential data. It is important to prevent confidential information from falling into the hands of unauthorized users should a device be lost or stolen. Encryption can be an effective way to protect the privacy of sensitive corporate and personal data.

While software encryption programs can help protect data and provide a good first line of defense, they are vulnerable to a number of decryption attacks. Hardware-based encryption offers a stronger defense against the same threat models, and is now available on a new generation of portable data security and authentication devices from IronKey. This paper examines IronKey's data encryption capabilities, compares the competing software and hardware-based approaches, and analyzes their effectiveness against various threat models.

Encryption Algorithms

Typically a government approved strong encryption algorithm such as AES is used for both hardware and software-based encryption. Since 128-bit key lengths will protect data from brute force decryption attacks for the foreseeable future, IronKey devices implement standard, government-approved AES CBC-mode 128-bit encryption. This encryption is implemented in hardware and can not be tampered with or disabled.

Encryption Key Strength

Software encryption algorithms use a password as the encryption key to scramble data. This exposes inherent weaknesses in the security, as the encryption strength is entirely dependent on the strength, or unguessability, of the password. Some software products attempt to require users to have passwords that are not easily guessed, but this makes it difficult for people to remember their passwords. These approaches encourage users to have a password with both upper and lower case letters, as well as numbers in the password (e.g. "myPa\$\$wor3!"). Having an uncommon password may delay an attacker from guessing the encryption key; however, computers can quickly process algorithms that will guess all possible password combinations ("brute force" attack). Another problem with software-based approaches is that the passwords may be of limited length. Typically, user passwords are 4-8 characters long. This means that the encryption key is easy to guess and is subject to brute force attacks. An AES 128-bit encryption algorithm requires a password that is 16 characters long, but this would be even more difficult for a user to create and remember.

Hardware-based encryption can suffer from the same weaknesses if the password is used as the encryption key. The IronKey architecture removes this vulnerability by using randomly generated long and strong encryption keys. These 128-bit long keys are generated by a FIPS 140-2 compliant True Random Number Generator in the cryptographic processor. The user's password is used to unlock the encryption key, which is then used to decrypt or encrypt data.

Brute Force Attacks

Software implementations, and even some hardware-based encryption systems, are vulnerable to brute force password guessing or key guessing attacks. An attacker can plug the USB flash drive into a computer and have a program guess hundreds of passwords or keys a second.

Some software implementations may try to defend against brute force attacks by maintaining a counter that tracks the number of times an incorrect password was entered. This can be easily defeated by a memory rewind attack. To do this, the attacker makes a copy of the encrypted data and the encryption software's temporary files before beginning the brute force attack. The attacker simply re-instates the original files after every password-guessing attempt. This 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 the flash memory. The attacker simply re-winds the counter after every attack.

The IronKey Cryptochip uses government-approved AES CBC-mode 128-bit encryption.

The IronKey Cryptochip generates strong 128-bit long random keys that are unlocked by the user's password.

The IronKey Cryptochip utilizes an internal password counter that cannot be tampered with or reset.

The IronKey Cryptochip is permanently set in a solid metaling filled with a tamper-resistant potting material.

IronKey devices do not require any software installations or device drivers to work.

IronKey's hardware encryption is always on and cannot be disabled or tampered with.

IronKey devices use a separate cryptographic processor with its own internal password guessing counter. This counter is not stored in the flash memory, so it is not vulnerable to memory rewind attacks. This cryptographic processor is hardened against power attacks, bus sniffing, etc. It is impossible to physically tamper with or reset the counter. Once the counter has reached a pre-defined limit, the encryption keys are destroyed by the processor, and the stored encrypted files are permanently inaccessible.

Parallel Offline Attacks

Software encryption algorithms on USB flash drives store the encrypted data as a file on the flash drive. This file can be copied off the drive by an attacker onto their machine. This gives the attacker the ability to implement massively distributed password guessing attacks by replicating the data onto many machines and having them guess passwords or keys in parallel.

The www.distributed.net organization has been operating parallel offline attacks as research projects for many years. Today, malicious attackers can scale up this approach and put tens of thousands of computers to work guessing passwords. It is not uncommon to find botnets ("roBOT NETworks") of hijacked PCs ("zombies") on the Internet for rent. For a small fee, an attacker could potentially have 10,000 to 100,000 PCs cracking a password or key in parallel.

A properly implemented hardware-based encryption device can help prevent such attacks by not mounting the device onto a PC until the correct password has been entered. Thus an unauthorized user cannot copy the contents of the drive onto a PC for replication to a botnet. Some hardware devices could still be vulnerable to a parallel offline attack if the attacker can disassemble the device, remove the flash memory chips, and install them onto a device of his own manufacture. This could allow the attacker to copy the contents of the memory chips onto his PC for replication to a botnet. IronKey devices make this kind of attack very difficult due to their tamper-resistant casing and board-level potting. This process makes it extremely difficult to get the memory chips off the printed circuit board without destroying them in the process.

Driver Installation Risks & Portability Issues

Software-based encryption packages typically require the installation of USB disk drivers onto the PCs operating system before files can be copied onto or off the device. This also means that in order to use the device on other people's PCs, you must install the driver software on those devices as well. This exposes these other PCs to risks from incompatible drivers, driver bugs, and malicious code installation. Furthermore, it usually limits the types of computers on which these devices can be used. Macintosh and Linux users are typically out of luck.

IronKey devices with onboard hardware-based encryption do not require any software to be installed on the PC. This means the encryption is independent of which operating system you have and can be used on other people's PCs without leaving a software footprint behind.

Vulnerability to Malicious Code & Disabling Encryption

Software-based encryption is only as secure as the PC that it is run on. Malicious code could alter the software or drivers and modify or disable the encryption. IronKey's hardware-based encryption does not have this vulnerability.

Additionally, software-based encryption is only effective when it is turned on. If the encryption software is disabled or the user forgets to turn it on for some reason, data can be stored on the flash drive in an unencrypted way. This type of security risk is not acceptable in many enterprise or personal environments. By contrast, IronKey's hardware-based encryption is always on. It cannot be turned off on purpose or accidentally. All data written to an IronKey device will be strongly encrypted.

IronKey digitally signs all updates, ensuring the authenticity of firmware upgrades.

IronKey devices are optimized for high-speed data transfer, reading up to 30MBps and writing up to 20MBps.

Find more information about IronKey online at: www.ironkey.com

IronKey, Inc.
5150 El Camino Real, Suite C31
Los Altos, CA 94022 USA
+1 (650) 492-4055

Additional Security Features

IronKey's hardware-encrypted devices can also perform security and cryptographic functions that would not be practical or secure in a software package. Hardware-based encryption processors are used for authentication of users and of software updates and installations. Software implementations can generally not be used for this, as the cryptographic keys are stored in the PC's memory during execution, and are vulnerable to all manner of malicious code.

Security Updates

It is fairly common for software and firmware to be updated by the manufacturer on a periodic basis. It is convenient for users to download these updates over the Internet. IronKey devices verify the authenticity of these updates by checking digital signatures before installing the firmware upgrades. This checking is done in hardware, thus preventing malicious code from being executed on the device. Software implementations can check signatures of update files; however, the signature checking could be compromised and modified by malicious software on the PC.

Speed

In addition to much better security, hardware-based encryption has other benefits for users. Software based encryption typically runs much more slowly than hardware-based encryption. IronKey devices are specially optimized for high-speed data transfer, performing at the top of their class by reading data at up to 30 megabytes per second and writing data up to 20 megabytes per second (numbers generated from Intel's Iometer performance measurement tool).

Conclusion

Hardware-based encryption, when implemented in a secure manner, is demonstrably superior to software-based encryption. That being said, hardware-based encryption products can also vary in the level of protection they provide against brute force rewind attacks, offline parallel attacks, or other cryptanalysis attacks.

IronKey devices address the threat models described in this whitepaper. Password brute force guessing is prevented, and a variety of two-factor authentication protocols are provided. The physical security features of the devices protect against disassembly, rewind attacks and offline parallel attacks. IronKey devices provide fast, strong, and always-on encryption that mitigates the security concerns of transporting confidential data.

References

- Bruce Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, 2nd Ed, 1996, John Wiley & Sons, Inc.
- Definition of Brute Force Attack, Wikipedia, http://en.wikipedia.org/wiki/Brute_force_attack
- FIPS PUB 140-2 Federal Information Processing Standards Publication – Security Requirements for Cryptographic Modules, <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- FIPS PUB 197 Federal Information Processing Standards Publication – Announcing the Advanced Encryption Standard (AES). <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- Joan Daemen, Vincent Rijmen, The Design of Rijndael: AES – The Advanced Encryption Standard, 2002, Springer-Verlag Berlin Heidelberg.
- Niels Ferguson, Bruce Schneier, Practical Cryptography, 2003, John Wiley & Sons.
- Secure Encryption Challenged by Internet-Linked Computers, Oct. 22, 1997, <http://distributed.net/pressroom/56-PR.html>