ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 1, pp: (8-13), Month: January - March 2022, Available at: www.researchpublish.com

Study on the Enterprise security and management of hardwareBased-based secure USB Device

[1]INDRAJEET, [2]DR. HARSH KUMAR

[1]Research Scholar, Department of Computer Science, Himalayan Garhwal University, Uttrakhand, India -246169

[2]Associate Professor, Department of Computer Science, Himalayan Garhwal University, Uttrakhand, India -246169

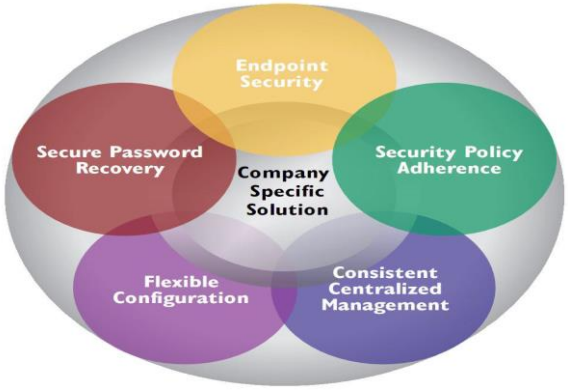
Abstract: **The secure drive was developed to improve the security of the conventional USB flash drive, which is vulnerable to leakages of internally stored data caused by extortion, loss, etc. However, it has been continuously reported that the secure USB flash drive, which protects data through the adoption of a wide range of security technologies in wide-ranging ways, cannot assure data security because of implementation and environmental vulnerabilities, eavesdropping, unlock commands, and reverse engineering. As such, there is growing demand for a more powerful secure USB flash drive to solve these fundamental problems. Therefore, this paper presents a secure USB mechanism that prevents leakages of authentication data and does not compare authentication data for smart human care services, which have been a fundamental problem of existing flash drives.**

Keywords: **secure drive, USB Flash.**

1. 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 Genesis. This paper examines Genesis's data encryption capabilities, compares the competing software and hardwarebased approaches, and analyzes their effectiveness against various threat models Genesis SecurDrive represent one of the most secure and easy-to-use solutions to the problem of physical USB device security. However, physical security of USB flash drives is only one issue IT managers face. With thousands of flash drives being used in an organization, managing the usage and policies of devices presents an equally significant challenge.

Common Concerns Among Enterprise Security Managers



Endpoint Security

The data on portable storage devices should ideally be protected from a myriad of known attacks, regardless of whether the device is being used correctly by its assigned owner or being tampered with by an intruder. The devices must also integrate easily with endpoint security software that authorizes which devices can be safely integrated with the existing network or PC.

Security Policy Adherence

Portable devices must reside under and support the organization's existing security policy umbrella. This means that data access must be controlled by the same password policies and external devices must be subject to the same on-the-wire security policies

Secure Device Recovery

Even if an enterprise's portable devices have been secured against a multitude of potential attacks, a forgotten password to a specific device could render the device inaccessible and result in loss of critical company information if there is not a secure means for device recovery. Examples also include accessing data on the device when an individual is no longer with the organization and changing the device owner's password for repurposing the device. Since forgotten passwords constitute upwards of 30% of all help desk requests5, data loss due to a forgotten password is a potentially significant problem for enterprise IT managers. However the ability to recover forgotten passwords carries its own set of security risks, and ensuring proper authentication, authorization and access are crucial. For example, even with military-grade device security, a disgruntled insider could gain access to the data on all of an organization's flash drives if the passwords are stored in a central database for administrators.

Flexible Configuration

How endpoint devices may be used needs to be subject to policies and processes unique to a specific organization. Security managers must be able to control what software can be used on specific devices, how that software is configured for use. Equally important, the IT organization must control who is allowed to administer which policies on which devices.

Consistent, Centralized Management

The flip side of flexible configuration is consistent management, and the two sides represent a balance of competing needs:

- The need to ensure that a minimum set of security standards can be established and automatically enforced across an entire group of portable devices.
- The need to allow flexible implementation to conform to the policy of a specific user group.

With multiple groups using portable devices throughout an organization (e.g. divisions, departments, teams), consistency of device policies becomes a critical concern. If a company has a seven character minimum for password length, then an enterprise administrator must be capable of enforcing that policy across all departments within their span of control. Another aspect of consistent management involves cost. Consistent management is ineffective if the cost of administration is too high to make it practical. With hundreds or thousands of devices in a given user group, device management must have a centralized control console. Provisioning cannot be practically handled by already overburdened IT staff. Simple, yet secure self-provisioning of devices by end users is a practical solution for this issue. IT administrators need to balance system configuration with ease-of use, cost, and consistent policy enforcement.

Defining the level of security

When evaluating security options, it is important to identify the impact to your business associated with the information you are protecting and the threats from which you are protecting them. Remember, too that security is a moving target and the threats continue to escalate to both the data and the device itself. As revealed at black Hat 2014, BadUSB is the first USB malware designed to attack the device itself instead of attacking the data on the device. The attack changes the firmware that controls the behavior of the USB hardware, allowing the USB device to become a host that can subsequently infect other computers and USB devices.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 1, pp: (8-13), Month: January - March 2022, Available at: www.researchpublish.com

Compliance Vs. Security

Secure, more secure, and most secure

Security levels for storage devices can be described as "secure," "more secure," and "most secure. To understand the level of security your organization needs, you first must take inventory of your reasons for implementing a secure data strategy. You must also always evaluate the need to move beyond compliance. IT managers frequently cite one of three primary drivers:

We need to be compliant with data security Requirements:

When compelled to implement a data security strategy, organizations frequently fail to see a direct relationship between adding security and achieving improved efficiencies across their operations. Their goal is to simply be secure enough that if a breach occurs, they can show that they followed "industry standard and best practice," thus avoiding the cost of fines from government oversight bodies. In other words, the organization needs to get a passing grade in a security audit but does not see any pressing reason for security investments outside of this objective.

Our workforce deals with information that is highly sensitive and cannot fall into the wrong hands:

In this case, a loss of critical proprietary or confidential information could have severe or even catastrophic consequences to a business; organizations tend to choose a security level that keeps the data secure from even the most aggressive and well-capitalized hackers, such as foreign governments and identity theft cartels.

The storage device must survive the harshest of environments while being secure and accessible for long periods of time:

Most organizations don't subject their data devices to challenging physical conditions. But for those that do– including government, military, first responders, and hospital workers in sterilized environments – keeping data secure is a matter of more than data security. It can be a matter of national security or public safety. Understanding your needs and the potential impact that exposures may have on your organization or business will help pinpoint your tolerance for data breaches. The greater the potential damage, the greater the need for the highest levels of security.

Understanding What keeps data safe

It's one thing to pinpoint why you need security. It's another to understand the options available to you to help you meet those needs. This requires digging into the technology, architecture, physical composition, and management of storage devices. The more you know, the more it becomes clear why some solutions protect data more persistently than others, and why those solutions can cost more.

Encryption and Authentication:

These are the common denominators for all systems regardless of the security level.

Encryption: transforms the data on the storage device so that an intruder cannot decipher the information.

Authentication controls access to the information by requiring users to provide passwords or biometric identification (such as a fingerprint). Some devices require multiple forms of authentication.

Encryption comes in many forms and different algorithms, but all are designed around a fundamental premise: To create an algorithm with so many permutations that it would take thousands of years to solve them, even when using the most

advanced current computing power. To ensure that this is true, current encryption algorithms use long encryption (or crypto) keys that make them exponentially more difficult to crack than shorter ones.

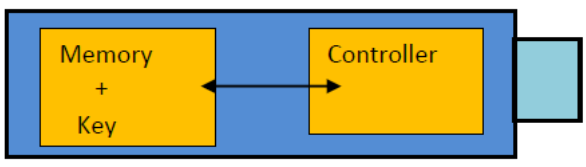


Figure 1: Drives that store encryption keys in the clear make it easier for hackers to read the key and steal the data stored on the device.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 1, pp: (8-13), Month: January - March 2022, Available at: www.researchpublish.com

Hardware design:

The way a device's security is implemented is just as important as the encryption technology utilized within it. Some devices store the crypto key in clear readable text in the flash memory itself, while others store the crypto key on a separate secure cryptographic module.

Readable clear text in the flash:

This means the crypto key is stored in the flash memory or hard drive built into the device, which makes it easier to read by people trying to get to the stored data. Many devices that meet the FIPS 140-2 Level 2 security standard store their crypto key in this manner, or they obfuscate it using a key derived from the password. In either case, the key is usually stored in the same memory area as the rest of the data. It is a lower-cost approach that offers less protection than devices with a cryptographic module. (See Figure 1.)

On a chip:

More secure systems keep the data encryption key out of the main device memory and store it on a separate cryptographic module, commonly used in smart cards. The chip is shielded in a tamper-resistant environment. Devices that meet the more stringent FIPS 140-2 Level 3 security standard store their encryption key on a cryptographic module in this manner. (*See Figure 2.)*

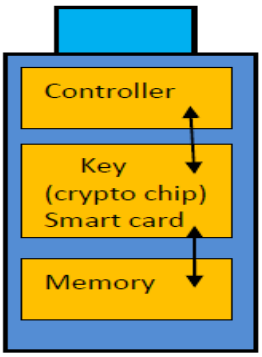


Figure 2: Drives that store encryption keys in a separate tamper resistant Crypto chip module are significantly more difficult to compromise. They tend to feature unique defenses, such as a metal mesh cladding and self-destruct function in case of physical attacks.

The Benefits of a the Managed Security Service

The SecurDrive: Enterprise Edition allow administrators to manage their devices without having to install and integrate complex enterprise software. The benefits of device management as a service include:

Easy to Trial and Deploy

There is no complex enterprise software to purchase and install. SecurDrive: Enterprise Edition's device management is straightforward to pilot, test and rollout.

Scalability

SecurDrive: Enterprise Edition scales as your organization grows and changes. It is equally well suited for large enterprises as it is for small and medium businesses

Reduced Cost of Ownership

Genesis IT staff ensures that the service is online 24x7**. They are constantly managing network performance and availability. The team also manages service upgrades and the rollout of new features. All of this reduces the burden of IT administrators and the total cost of ownership of the managed solution.

The Security Architecture of the Enterprise Managed Service

The SecurDrive: Enterprise Edition has been designed from the ground up with security in mind:

Network Security of the Service

SecurDrive enterprise services have been designed by security architects with a background in managing the security of banking and payment systems. Best practices are used in firewalls, IPS, event monitoring and cryptographic key management. All access to the systems is through two-factor authenticated encrypted communications.

Hardware Cryptographic Authentication of Devices to the Service

All user and administrator SecurDrive devices authenticate themselves to the management service with on-board hardware encryption. This allows the service to ensure that administrators and users are authenticated and have the appropriate permissions.

Encryption of All Communications with the Service

All communications with the service are encrypted and strongly authenticated to mitigate spoofing, man-in-the-middle, phishing and pharming threats.

Anti-Phishing Technology

User and administrator accounts have the latest anti-phishing technologies to authenticate users, including two-factor cryptographic mutual authentication, shared secret images, shared secret questions and device fingerprinting.

Cryptographic Architecture of Secure Device Recovery

Unlike "backdoor password" systems, the Securdrive device key recovery system uses strong public-key cryptography to encrypt and recover device passwords.

2. CONCLUSION

The security experts at Genesis have gone to extreme lengths to ensure that the SecurDrive: Enterprise Edition meets the common security, deployment, and usability/maintenance needs of IT managers demand, while maintaining the overall security of the SecurDrive enterprise services at the same unmatched level as the SecurDrive hardware. 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.

SecurDrive 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. SecurDrive devices provide fast, strong, and always-on encryption that mitigates the security concerns of transporting confidential data.

REFERENCES

[1] Unworth, Joseph. "Forecast: USB Flash Drives, Worldwide, 2001-2011", Boston: Gartner/Dataquest, October 2007.

[2] Pointsec as quoted in *Outlaw News*, June 13, 2005.

[3] 2006 CSI/FBI Computer Crime and Security Survey, *http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf*

[4] Ponemon Institute, 2006 Cost of Data Breach Study, *http://www.computerworld.com/pdfs/PGP_Annual_Study_PF.pdf*

[5] Marianne McGee, "The Top Reason Users Call the IT Help Desk", InformationWeek, March 1, 2007, *http://www.informationweek.com/news/showArticle.jhtml?articleID=197700628*. Also ContactCenterWorld, January 15, 2003.

[6] Bruce Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, 2nd Ed, 1996, John Wiley & Sons, Inc.

[7] FIPS PUB 140-2 Federal Information Processing Standards Publication – Security Requirements for Cryptographic Mod- ules,http://csrc.nist.gov/publications/fips/fips1402/fips1402.pdf

[8] FIPS PUB 197 Federal Information Processing Standards Publication – Announcing the Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[9] Joan Daemen, Vincent Rijmen, The Design of Rijndael: AES – The Advanced Encryption Standard, 2002, Springer-Verlag Berlin Heidelberg.

[10] 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

[11] Bellare, Mihir. "Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements." Springer Berlin Heidelberg, 2000. Page 1

[12] https://security.berkeley.edu/content/data-encryption-transit-guideline

[13] Robert Richardson, 2008 CSI Computer Crime and Security Survey at 19.i.cmpnet.com

[14] Fiber Optic Networks Vulnerable to Attack, Information Security Magazine, November 15, 2006, Sandra Kay Miller