Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2015) 23: 80 – 84
© TÜBİTAK
doi:10.3906/elk-1212-152

Design of a novel USB cryptobridge device

Orhan ŞENGÜL[*]
R&D Department, TÜBİTAK Space Technologies Research Institute (UZAY), Ankara, Turkey

Received: 26.12.2012 • **Accepted:** 12.02.2013 • **Published Online:** 12.01.2015 • **Printed:** 09.02.2015

Abstract: Information technologies have emerging use of portable drives. Hence, the readability and security of the content is at great risk in the event that it is lost or stolen. An effective solution to this issue is the use of removable disks in encrypted form. In this paper, a novel USB device that has cryptobridge capability is proposed.

Key words: Universal serial bus, cryptobridge, USB encryption, hard drive

1. Introduction

Presently, the security problem in the data transfer process is of significant importance. Since coding and encrypting keys are applied on main systems like computers and tablets, this causes serious security gaps. While the protected data cost per gigabyte is excessive, disk capacity becomes an important security feature and a limitation for users. Some products used for security features are turned on and the disk can be hacked or data can be lost [1–4].

The information technology sector has increasing use of portable drives. The readability of the content is at great risk in the event that it is lost or stolen. The most reasonable solution to this issue is the use of a removable disk in encrypted form. Software products are developed especially for operating systems. The software for one operating system does not work properly for a different one. Some products encrypt only files and set up a file system on the hard disk. However, systems cannot use this file system. Each system cannot go to the same specification product on the market, between host systems running on different operating systems, because the security is unable to use a shared disk [5].

Encoding of the information can be performed after transferring it to a computer. There is no security product like an encryption device on the market where the main system is not a computer. It is not feasible to produce security software for unrecognized, rarely used, or outdated operating systems. There is still a need for low-cost secure portable disks. Success of the encryption process requires particular attention to safety procedures, like the protection of the encryption key, the encryption process, the copying of encrypted and unencrypted files mixed together, disk transfer, and the deletion of residues. The importance of the information to be hidden can make these challenges bearable. These difficulties lead to procedural mistakes [6–8]. In particular, a rush for encryptions causes cessation of work, which may result in serious security vulnerabilities. In this work, a novel USB device with the capability of a cryptobridge is proposed as a security procedure applicable to portable devices. The USBK cryptobridge is an on-the-fly encryption device featuring 2 USB ports that establish and maintain an encrypted link between the host system and the backend disk. It is

[*]Correspondence: drorhansengul@gmail.com

equipped with a USB type A receptacle for attaching the backend disk and a USB type A plug for attaching to the host system.

2. Design and functionality

This paper presents the design and evaluating processes of a USBK cryptobridge that is fabricated to secure the content inside of a portable data device in the event that it is lost or stolen. The most reasonable solution in these cases is the use of a removable disk in encrypted form. The USBK cryptobridge is a disk encryption product with which the users have the ability to encrypt/decrypt all of the data transmitted between the host system and a backend disk. Since the main feature is encrypting/decrypting the transmitted data from/to the disk, users are not restricted by limited disk space; on the contrary, they have the ability to use it with any USB flash and USB external hard drives that can be plugged into the cryptobridge. Figure 1 depicts the generic usage of the cryptobridge.

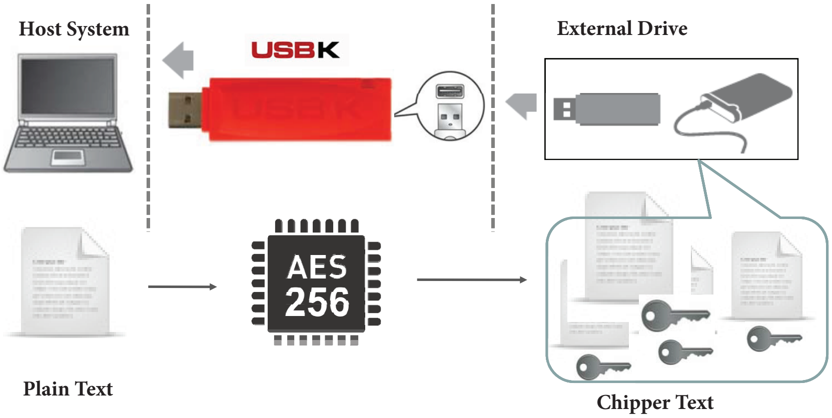

Figure 1. Generic usage of the cryptobridge.

The cryptobridge is also not dependent on any operating system on the host system that the encrypted data will be transmitted from. The cryptobridge communicates with the host system using a small computer system interface (SCSI). The cryptobridge supports predefined vendor-specific SCSI commands. An application on the host system can be used as an interface between the user and the SCSI. This type of communication between the host system and cryptobridge provides independence from the operating system. The cryptobridge supports cryptographic operation according to the supported AES key size. Users can either generate a 128-bit or 256-bit AES key.

The cryptobridge is an integrated system that enables users to protect their data after the transmission to a backend disk. Upon the initialization and activation of the target of evaluation, the authorized user can transfer data by encrypting it with a 128-bit or 256-bit AES transfer key to a formatted backend disk. The authorized user can also perform the decryption operation for the encrypted files in a backend disk. The user can configure the security functions and user security attributes of the cryptobridge only if it is deactivated. Appropriate user authentication is performed during the configuration. Figure 2 presents the functional hardware units of the proposed cryptobridge. The superiority of the proposed cryptobridge, other than its novelty, comes from its unlimited capacity, as there is no restriction on the quantity and size of the USB drives that can be attached to the USBK; compatibility with a wide range of hosts, including oscilloscopes, electrocardiograms, and tablets; independence of the operating system; and no need to require an installation driver of software on the host.

Other products on the market (Enigma, Cipher USB, Aegis Secure Key) have full compatibility problems with some platforms and do not offer in-place encryption for the existing content. The cryptobridge offers a low-cost solution with a nationalized algorithm for military and governmental applications.

The software- and hardware-based solutions dedicated to data security problems are discussed in the next 2 subsections. The encryption methods and operating systems are then described. Finally, the peripheral proposed solution and security procedures are mentioned.

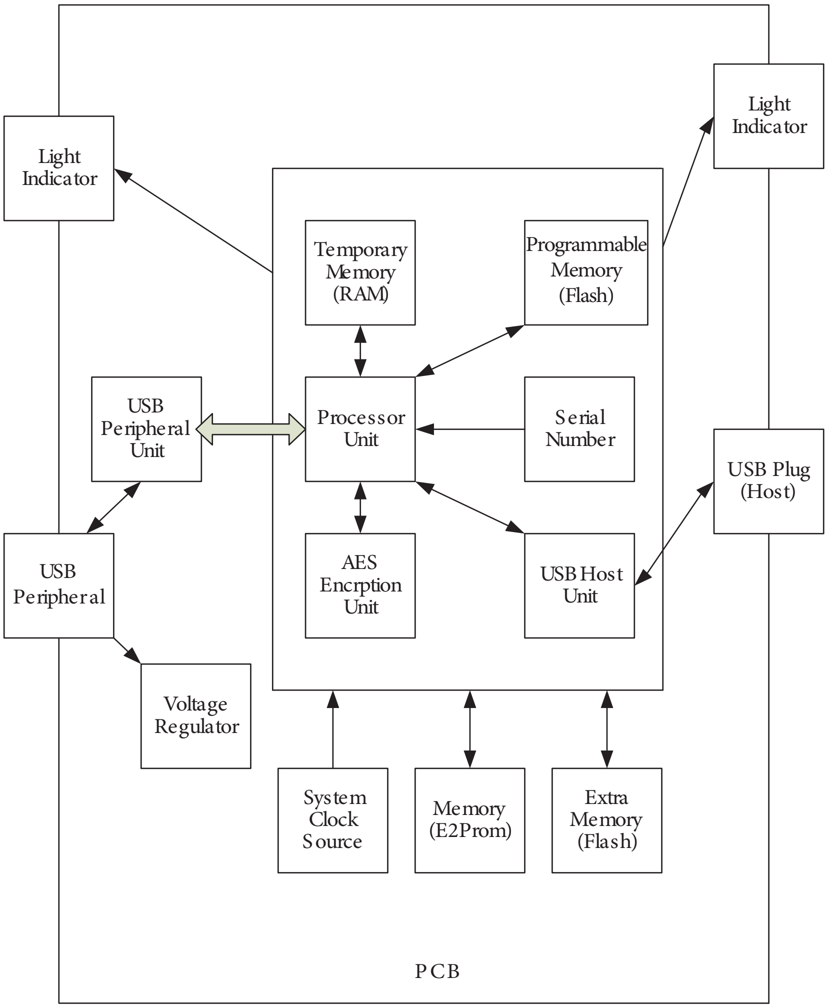

Figure 2. Functional hardware units.

2.1. Software-based solutions

In these solutions, the most critical computing software is keeping the encryption key. The following methods can be applied to realize this:

- Use a separate portable USB disk to save the encryption key.
- Use the disk of a computer and store them in an encrypted file.

This solution may entail special software, such as software that can be part of the operating system.

2.2. Hardware-based solution

A portable piece of hardware on the disk does the encryption. Both the AES key and the encrypted password files are saved on the disk. Users are required to choose the key size and encryption keys accordingly. Encrypted data stored in the backend disk cannot be decrypted without using the correct encryption keys. The use of the disk by entering the password of a user identifies itself with the OPEN command to open the disk. The CLOSE command exits the functionality of the disk after the end of usage. After 3 wrong password attempts, the USBK erases all of the encrypted keys and password and returns back to the default.

2.3. Encryption method

AES is an encryption method that is commonly applied and has a low amount of weaknesses. A huge amount of confidential information can be stored by AES. The American National Institute of Standards and Technology AES is declared to be an appropriate method [9]. Portable drives are safe enough to protect the information stored.

2.4. Operating systems

Each file system is not supported on all operating systems, as there is no platform for joint work between systems. Commercially produced products are available only for a specific operating system.

2.5. Proposed solution

The proposed USBK cryptobridge is a portable drive with a USB port that can be inserted between the host system and backend disk [10]. It can introduce itself to the host system as a device that can communicate in MSD-SCSI protocol. The information that is encrypted using the user-defined key toward the disk out of the computer correctly deciphers the information. A device overcomes these problems by using the encryption key after verifying and storing. This device can also handle a huge amount of data, like video files, and avoids the crushing caused by processing the load and the generated heat during operation.

A random encryption key is assigned after the password is set. A user with such a device keeps the encryption key as not accessible. Hence, sufficient security to protect the data can be provided. Information kept on the disks remains encrypted at all times to provide maximum security. This paper proposes a system in which user can keep as much information as possible in encrypted form. Since the proposed device offers low-cost data security, the overall cost for the encrypted data is decreased dramatically. The cryptobridge encrypts the information passing through it sector by sector.

2.6. Easy security procedure

Protection of the encryption password and encryption process is done by the cryptobridge. Encryption is done when the data flows between the host system and the disk at the time (on-the-fly). The normal procedure of using portable drives is plug/use/unplug. In this paper, a system procedure is proposed to operate as plug/activation/use/unplug. There is no difference except the password entry for the user.

3. Conclusion

In summary, a novel USB device that has cryptobridge capability is demonstrated. The certification and security tests of the device are held by the TÜBİTAK Common Criteria Test Center (OKTEM). By utilizing this system, the user will keep as much information as possible in encrypted form. Thus, the cost per gigabyte of encrypted data is reduced. Moreover, there are several security features that make the proposed device safer to use. The problem of security in data transfer with a low data cost per gigabyte is a hot topic for novel devices. Therefore, the proposed device is a secure and low-cost solution for these problems.

References

[1] T. Liu, H. Zhu, "An ID-based multi-server authentication with key agreement scheme without verification table on elliptic curve cryptosystem", International Conference on Computational Aspects of Social Networks Proceedings, pp. 61–64, 2010.

[2] M. Matsui, "Cryptography in embedded environments", IEEE 13th International Symposium on Consumer Electronics, pp. 16–17, 2009.

[3] C.L. Chen, "A secure and traceable E-DRM system based on mobile device", Expert Systems with Applications, Vol. 35, pp. 878–886, 2008.

[4] C. Hessel, "Passive protection against security compromise or possible insecurity when information/communications devices are lost", IEEE Military Communications Conference, Vol. 2, pp. 758–760, 2003.

[5] Y. Zhou, S. Guo, "SPA-based security evaluation of RSA implementation in Internet banking USB token", International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp. 499–503, 2011.

[6] A. Falcone, R. Focardi, "Formal analysis of key integrity in PKCS#11", Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security, Joint Workshop, pp. 77–94, 2010 .

[7] L. Han, J. Liu, D. Zhang, Z. Han, X. Wei, "A portable TPM scheme for general-purpose trusted computing based on EFI", International Conference on Multimedia Information Networking and Security, Vol. 1, pp. 140–143, 2009.

[8] G. Lomako, I.P. Park, S. Johnson, D. Braun, K. Guo, "Cryptographic consumer electronic devices file systems performance", IEEE Consumer Communications and Networking Conference , Vol. 2, pp. 1303–1304, 2006.

[9] AES Technical Standard, available at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[10] Turkish Standards Institution Common Criteria Certification Scheme: USBK Cryptobridge v 2.0 for Model A101 and Model A103, available at http://www.commoncriteriaportal.org/products/.