National Conference on Sustainable Engineering And Management (NCSEM24)
ISSN 2349-6002

Protecting Documents with a Secure Data Transfer Algorithm forUSB Mass Storage Devices

Geethu John[1], Monisha Prabhakaran.P[2]
[1]*IInd year, ME, Department of CSE, SIVAJI College of Engineering and Technology, Manivila*
[2]*Asst. Professor: Department of CSE, SIVAJI College of Engineering and Technology, Manivila*

Abstract-- ***The number of USB peripheral devices has increased significantly, and the Universal Serial Bus (USB) has emerged as the most widely used interface standard for hardware connections. Particularly, external USB storage devices are the most widely used products on the market. Unfortunately, many businesses have banned the use of USB devices to prevent sensitive data theft from computer systems via USB ports because USB allows for high-speed data transmission and is incredibly convenient to use. Nevertheless, this reduces the USB connection's convenience. Consequently, it has become crucial to figure out how to balance user convenience with a secure workplace. In order to circumvent this issue, we present in this paper a secure control algorithm that offers mutual authentication and key agreement between client and server***

Keywords: Key agreement, Mutual authentication, Storage device, Universal Serial Bus (USB)

1. INTRODUCTION

A USB port, which is now a standard feature of modern computer hardware due to its convenience and ease of connectivity, is one of the many new peripheral devices that can connect to a business computer terminal due to the rapid development of the computer and information industry in recent years. The ability to connect multiple devices, includinghard drives, flash drives, printers and keyboards, to a computer through a single interface is the primary benefit of the USB port . The modern society has witnessed a rapid increase in information or private data for individuals and companies doe to the advancements in computer science and technologies. As a result, in order to avoid numerous issues pertaining to the disclosure of the information ,advance planning has been necessary. Meanwhile, because of their accessibility and portability ,USB memories have become widely used as personal storage devices by governments, business and individuals. Because memories typically storea wide variety of crucial data, their portabilitycan occasionally lead to the loss, theft orhacking of vital information. As a result, numerous USB memories with security built in have been created

However, a series of analytical testsdemonstrate that the majority of commercial secure USB memories and their application software have significant vulnerabilities that expose critical data. The secure USB memories have their own user and device authentication protocol, but these vulnerabilities can make them easily compromised.

2. RESEARCH PROBLEM

The USB flash drive is a storage device with an integrated USB interface and NAND- type flash memory. Usually, it is lightweight, portable, compact and rewritable. However because of it's widespread usage, a number of security- related issues have arisen. Nevertheless, the majority of USB flash drives lack security features, making its simple for an attacker toaccess user data. Utilizing a USB exposes private company information to theft because it is highly convenient and fast transmission speeds. It is similar to passing data through an unguarded gate. For this reason, efficient management of these storage devices has grown to be a crucial concern for information security. Physical transmission of various computer peripherals between computers will remain chaotic if USB usage is outright prohibited. Confidential data loss is likely to occur if USB usage is not prohibited. Therefore, the most challenging USB management issues is striking a balanced between

the convenience of the USB port and its lack of security; private data must be protected, but access to USB devices must not be restricted. For this research, a middle ground must be found.

In order to effectively regulate file transmission via the USB port, we have *Problem definition:*
proposed a control algorithm in this paper that implements user authentication and key agreement. We have also suggested a system that will encrypt and decrypt the data before it is transmitted via USB inorder to add evenmore security.

To securely store the documents in a USB mass storage device, create and implement a two-layered secure data transfer algorithm.

3. RELATED WORK

Few publications provide a thorough security analysis of USB storage devices.[1] The protocol utilizes the Diffie-Hellmen key technique to protect the privacy of a file transferred to a storage device and employs a remote authentication server to confirm thelegitimacy of users. They have also demonstrated the protocol's resistance toa few common attacks. Realizing mutual authentication just takes two communication sessions in terms of protocol communication costs. This protocol, therefore, offers a secure and efficient control protocol for USB storage devices. Numerous theoretical and practical attacks pertaining to the mechanical, electrical, and software aspects of USB keys are described in [6],[9] research along with various attacks on USB devices. These attacks are not limited to USB keys; they could be developed further and applied to otherproducts. Users should weigh the advantages and security risks of each tool before recommending and integrating it into their infrastructure because the current generation of USB hardware tokens on the market has flaws. Onlyafter the weaknesses have been found can some of these flaws be fixed. Before deploying a solution, hardware designers– especially those of the security product category- should have a thoroughunderstanding of the threat model specific to their product. Research papers [2],[10],which describe various authentication protocols for three different types of commercial secure USB memories, have proposed various users authentication methods in order to address the vulnerabilities mentioned in [6[,[9]. Despite the fact that these products made an effort to be secure, there are still many vulnerabilities that could be exploited in variety of potential attacks due to incomplete software and dedicated authentication protocols. Private information is exposed when using a USB flash drive without any security measures. To make up for the issue, a new USB flash drive with supportfor security features was created. Theauthors of this paper examine the vulnerabilities in six well-known secure USB flash drives and show how a password can be revealed during communication between a PC and a secure flash drive. We also demonstrate the secure flash drive's S/W bug and data recovery vulnerability. After examining the weaknesses of secure USB flash drives, research in [6] indicates that. Fourweaknesses in the products were discovered by the authors. The first is the communication between the security program and secure USB flash drive thatexposes the password. The second is thatthe data on the secure USB flash drive can be recovered by an unauthorized user after formatting. The third is a security program's S/W bug. Hardware design without packaging is the final one. We offer a number of solutions, including theuse of hash functions, wiping technology,and secure coding techniques, to addressthese issues.

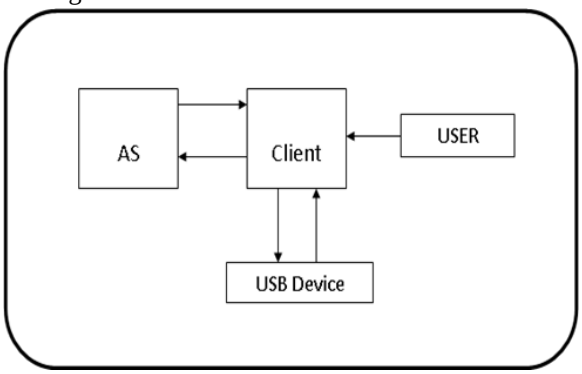
In conclusion, the necessary system for comprehensive data protection as suggested in [2] comprises remote user authentication [3] and Diffie-Hellmen key exchange [7]. Security from general attacks is also provide by the research in [2]. However, a few vulnerabilities that might be discovered. A control algorithm that offers user authentication[10], key agreement [7], and other features is required to successfully stop information theft via USB storage devices. Hence,few suggested a data

4. MATERIALS AND METHODS / OUR APPROACH

Any file transfer through a USB interfaceis prohibited in order to manage a USBstorage device, unless the user firstcompletes a valid authentication process.To ensure legality, a user wishing to senda file to a storage device via a USBinterface needs to enter their user nameand password. After that, the USBStorage device is accessible to the user. During the authentication process, asession key will be generated by both theuser

and the authentication server. Thiskey is then used to encrypt all files thatare transferred to the storage devicethrough the USB interface. The USB
This protocol has the following three characteristics: encryption/decryption algorithm as an extra layer of protection[11]. Theenvironment is now efficient in addition to being safe to this security addition. storage device has encrypted all of the files on it.USB access will be blocked following the encryption and transmission of the files until the next successful verification. The original file can only be obtained by users who successfully complete the verification process and obtain the agreement key is established for each filename and user identity. Furthermore, after the file is encrypted or decrypted, the system will remove the agreement key that was momentarily saved on the user's end, guaranteeing key independence and system security.

1. Only users verified to be legal can access the USB storage device.
2. Even if a confidential file on a storage drive is stolen, the file cannot be decrypted without a key.
3. Even if a legal file owner wants to malevolently store confidential data on a storage device and distribute it to another person, the owner cannot obtain the corresponding agreement key for decryption as long as the authentication server suspends this user account. Consequently, the originalfile is secure.



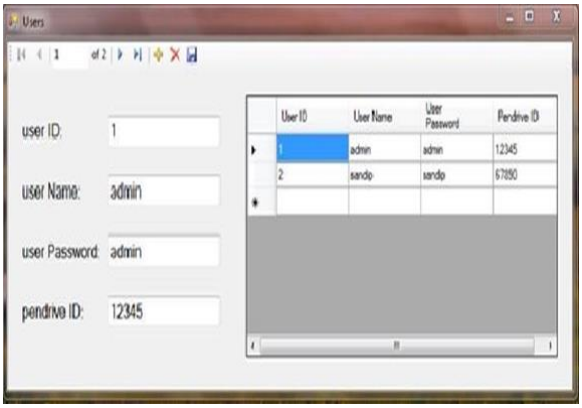
Above is the system environment which includes client server pair, user and USB device. System will work according to following procedure,

1. Insert a USB device.
2. User will provide user ID and password.
3. Achieve mutual authentication with AS.
4. Acquire a key from AS for encryption.
5. Save an encrypted file in USB device.

Even before accessing USB device user need to undergo the process of registration.Where, user needs to provide User ID and password. This set of ID and password will then communicated with authentication server (AS). Server will generate the mapping between ID – Password and USB device so; the process of registration for same USB devices will be avoided in future.In this registration phase different hash functions are used to provide better security.
Once the registration of the device is done itis ready to use for data transfer. While, doingso system will again undergo the process ofverification. After verifying the authenticity of the user authentication server will generate a session key. This session key is generated using user name as well as the IDof the USB device so; the session key will bedifferent for different files and/ or Users. The same key further used in the process of encryption and decryption. USB device stores the data in encrypted format. So it is very difficult to access the data in USB device without a session key. In order to generate a session key one has to undergo the process of verification. Further, advanceencryption system (AES) is used to encrypt/ Decrypt the data to be transferred to and from USB. This AES will provide morecomplexity to the protocol which is essential to avoid brute force attacks. Following are the different phases discussed further in detail.

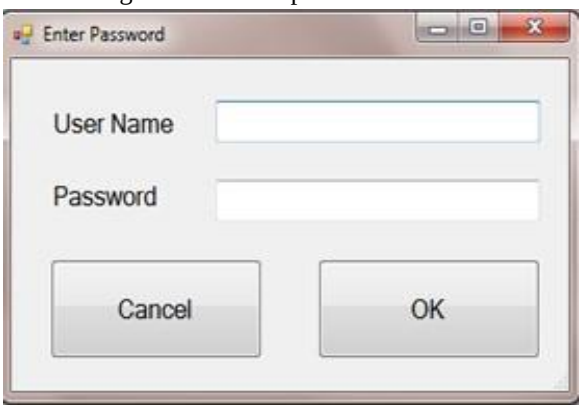
4.1. Registration Phase

In this phase user needs to pass throughregistration before using the system. User needs to register user ID and password in theauthentication server. To manage a USBstorage device effectively, any file via the USB interface is restricted unless a user firstpasses a legal authentication procedure. Following is the window where new user is registered.



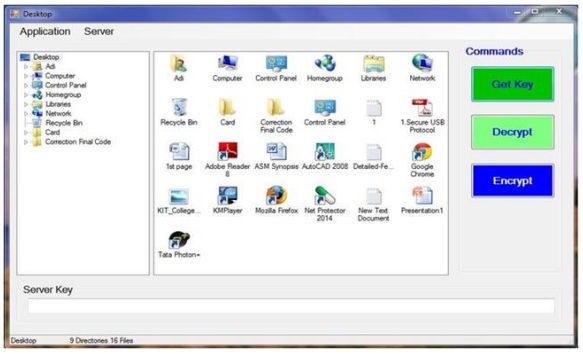
4.2. Verification and Key Exchange Phase

In verification process authentication server will verify that legality of the user. A user wanting to transmit a file to a storage devicevia USB interface must input username and password. Then, the user is able to access the USB storage device. After completing the registration phase, and when accessing the USB storage device, the user needs to achieve mutual authentication with theauthentication server using the id and the password.



4.3. Data Encryption / Decryption Phase

In this phase the session key generated in earlier phase is used to encrypt or decrypt the data to be transmitted via USB port.



Thus, all files stored on the USB devices areencrypted. After all files are encrypted and transmitted, USB access will restrict until the next successful verification. If user wants to decrypt the file on USB storage device later, they must pass the same

4.4. Client – Server Communication

The system environment is implemented using Client – Server communication. User has access to only client where as administrator has access to server. Client – Server communication also helps to monitor the entire process. Design of Client – Server verification procedure to obtain the same session key in order to acquire original file. This session key will be different for each user ID. To encrypt / decrypt the files, we use AES (Advanced encryption system) algorithm communication form includes server IP address which will help client to connect to server. Also TCP port has to mention. Prerequisite of implementing client – server communication is to check both are in samenetwork or connected to each other via web.

6. RESULTS

As stated in the problem definition in Chapter 1, we are able to offer USB devices two layers of security following algorithm execution. We will talk bout the algorithm's outcomes in this part. Encrypting and decrypting files that are tobe stored on a USB device is essentially the function of this algorithm. Text and image files are the two types of files we take into account when creating thealgorithm. Each kind of file is handled by the algorithm's execution will be coveredin the following sections.

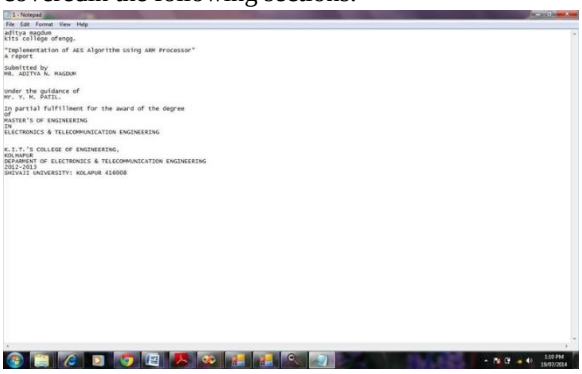


Fig. File before Encryption

Above figure shows a file (.txt) before encryption. The path of this file is selected on client and encryption is performed. Result of encryption is shown in fig. below which is a cipher text as we use the AES algorithm for encryption.

Fig. File after Encryption

7.CONCLUSION AND FURTHER WORK

We have presented a safe and effective control algorithm in this paper to giveUSB devices two layers of security.Further analysis enables us to demonstrate that this algorithm is resistant to a few common attacks. Realizing mutual authentication just takes twocommunication session in terms of

ACKNOWLEDGMENTS

It gives me immense pleasure to acknowledge and thank many people who contributed in various ways for the successful completion of this paper. Words are inadequate to express my feelings whilerecording my deep sense of gratitude and protocol; communication costs. Consequently, the proposed protocol offers a secure and efficient control mechanism for USB storage devices. We used visual Studio to design thisalgorithm. It is also possible to create hardware that works with the algorithm this paper proposes respect to my guide Dr. Y. M. PATIL. The work presented in this paper could not havebeen accomplished without his inspiring guidance, constructive criticism and sustained encouragement.

REFERENCES

[1] Fuw-Yi Yang, Tzung-Da Wu, and Su-Hui Chiu, “A Secure Control Protocol for USB Mass Storage Devices”, IEEE Transactions on Consumer Electronics, Vol. 56, No. 4, November 2010.

[2] Kyungroul Lee, Hyeungjun Yeuk. “Safe Authentication Protocol for Secure USB Memories”, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 1, number: 1, pp. 46-55, December 2010.

[3] Hyun sook Rhee, Jeong ok kwon, and Dong Hoon lee, “A remote user authentication scheme without using smart cards,” computer standards & interfaces, Vol.31, No.1, pp. 6-13, 2009.

[4] Kangbin Yim, “A fix to the HCI specification to evade ID and password exposure by USB sniff,”Proceedings of APIC-IST 2008, pp.191-194, December 2008.

[5] Tzung-her chen, wei-bin lee, “a New method for using hash function to solve remote user authentication,” Computer & Electrical Engineering, Vol.34, No.1, pp. 53-62, 2008.

[6] Hanjae Jeong, “Vulnerability Analysis of Secure USB Flash Drives,” Journal of the KIISC, vol. 17, No. 6, pp.99-118, December 2007.

[7] W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Transactions on InformationTheory, Vol. 22, No. 6, pp. 644-654,1976.

[8] C. P. Schnorr, “Efficient identification and signatures for smart cards,” Journal of Cryptology,Vol. 4, pp. 161-174, 1991.

[9] Kingpin @stake, Inc.196 Broadway, Cambridge, MA 02139, USA “Attacks on and Countermeasures for USB Hardware Token Devices”.

[10] Zhaohui Wang, Ryan Johnson, Angelos Stavrou “Attestation & Authentication for USBCommunications”.

[11] Aseem Jagadev, Vivek Senapati “ADVANCED ENCRYPTION STANDARD (AES)IMPLEMENTATION”, may 2009.