Enhanced Three Factor Security Protocol for Storage Devices

T. Jenitha, S. Amutha, I. Shri Ram

Abstract--- The Universal Serial Bus (USB) is eshtabilised for connection, communication and power supply between peripherals, also acts as an extremely popular interface standard for computer peripheral connections and is widely used in consumer Mass Storage Devices (MSDs). Eventhough current consumer USB MSDs provide relatively high transmission speed and are convenient to carry, the use of USB MSDs has been prohibited in many commercial and everyday applications primarily due to security problems. Security protocols have been previously proposed and a recent approach for the USB MSDs is to utilize multi-factor authentication. This paper proposes significant enhancements to the three-factor control protocol such as user identity, password and one-time-password (OTP) being sent to the e-mail that now makes it secure under many types of attacks including the password guessing attack, denial-of-service attack, and the replay attack. The proposed solution is given with a rigorous security analysis and practical computational cost analysis to demonstrate the usefulness of this new security protocol for consumer USB MSD.

Keywords--- USB, MSD, Password guessing attack, ECC, OTP.

I. INTRODUCTION

Secondary storage refers to storage devices and media that are not constantly accessible by a computer system. Examples include external hard drives, portable flash drives, CDs, and DVDs. These devices and media must be either plugged in or inserted into a computer in order to be accessed by the system. Because secondary storage technology is not always connected to the computer, it is commonly used for backing up data. Mass Storage Devices (MSD) is primarily related to storage devices that provide consistent and permanent storage capacity. MSD is connected to the computer/server via a data transfer interface, such as SCSI, USB or even Ethernet (for storage area networks). Some of the common Mass Storage Devices include floppy disk drives, optical drives, hard disk drives, tape drives, external hard drives, RAID and USB storage devices. Currently, typical Mass Storage Device devices provide anywhere from a few gigabytes to terabytes of data. Internal Mass Storage Devices generally can't be removed, whereas external Mass Storage Devices can be easily removed, ported and plugged into another computer. The Universal Serial Bus (USB) is a ubiquitous interface standard being widely used for connecting storage to consumer devices. Because of its convenience and ease of connectivity, the Universal Serial Bus(USB) port has become an essential component of consumer electronics devices such as flash disks, keyboards, cell phones, chargers, speakers, and printers. However, the USB interface has the following three weaknesses when it is used for consumer storage devices: (1) anyone (e.g., an unauthorized user) could read or steal confidential information easily since the information is stored in plaintext format; and (2) an adversary could intercept attack the transmitted information since the transmit channel between the device and the computer is not secure. Therefore, despite their practicality, USB Mass Storage Devices (MSDs) have been prohibited in an enormous number of environments. To solve these problems, and extend the applications of USB consumer storage devices, an authentication protocol can be implemented to ensure secure communications between the device and the computer.

Removable storage media are finding widespread used to transfer or backup data, even as bootable devices in recent years. They have brought us great convenience, yet at the same time, information security problems have also come into being. They have always been fraught with risks, which including theft or loss of devices, theft or leakage of sensitive information. Some of access authentication schemes on removable storage media have been proposed as means to determine device trust.

Many protocols have been proposed for the secure authentication of USB devices. However all these protocols are not ideally suitable for USB Mass Storage Devices because their stored information can easily be read out or require significant local complex computations. Also these protocols were vulnerable to many types of attacks such as forge and replay attack. Various risk mitigation techniques and system protection strategies have been presented, such as encryption, disable auto-run, using anti-virus tools, log data, access authentication etc.

To solve these problems, a three-factor authentication protocol based on Elliptic Curve Cryptosystem (ECC) that requires the user identity, password and one-time-password (OTP) for authentication. A user is allowed access to the USB port only if he/she is an authenticated user.

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography is the same level of security provided by keys of smaller size.

Manuscript received February 01, 2019

T. Jenitha, Department of Computer Science and Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India. (e-mail: jenitha@mepcoeng.ac.in)

S. Amutha, Department of Computer Science and Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India. (e-mail: amuthavasan@mepcoeng.ac.in

I. Shri Ram, Department of Computer Science and Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India. (e-mail: ramshri14@gmail.com)

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

II. RELATED WORK

Removable storage media are finding widespread used to transfer or backup data, even as bootable devices in recent years. They have brought us great convenience, yet at the same time, information security problems have also come into being. Some of access authentication schemes on removable storage media have been proposed as means to determine device trust. Nowadays, the most widely used access authentication scheme of removable storage media is based on its unique identification. Properties that can uniquely identify it include the vendor ID (VID), product ID (PID) as well as Hardware Serial Number (HSN) and so forth.

Existing schemes such as Yang et al.'s scheme [4] and its revision by Chen et al[3] proposed a new authentication scheme based on the Schnorr protocol[9]. These schemes use an authentication server as a trusted third party, and they also use the Diffie-Hellman key exchange for the session's key agreement. The digital signature of the user's ID and password are generated in the registration phase by the authentication server. In the verification phase, the user must use her or his ID, password, and a corresponding digital signature to be authenticated by the authentication server. However, these schemes are vulnerable to insider attacks and server impersonation attacks, and they cannot provide key security and key freshness for the session key agreement.

Information security is currently a very important topic in computing. Traditional authentication methods based on passwords involve many security problems. In business applications, USB has three serious weaknesses. First, the information is not encrypted, making it possible for an unauthorised user to read confidential information from the USB. Second, the working environment is not secured that the staff can obtain the information from the USB when the computer got viruses. Third, the staff can steal data from the computers using the USB. These problems pose a serious threat to USB security in a business environment.

III. PROBLEM FORMULATION

Formulation for the problem of providing security to both the system files and the USB MSD is as follows: Our problem is to provide security to the USB port and the confidential files stored in the system. While current consumer USB MSDs provide relatively high transmission speed and are convenient to carry, the use of USB MSDs has been prohibited in many commercial and everyday environments primarily due to security concerns. Hence we propose a three factor authentication protocol for USB MSD to prevent the device from various types of attacks such as denial of service attack, password guessing attack and replay attack.

Any illegal user can gain access to your system in your absence by knowing your system password and steal confidential information by using their USB mass storage device. To avoid illegal users from gaining access to the USB port, a security protocol has to be designed that allows only authenticated users to use the port. This security is provided by the three factor authentication protocol. When a user wants to use the USB port, for the first time the user should register with the authentication server. Only one user can register with the authentication server thus preventing illegal users from gaining access to the USB port.

Anyone can steal the confidential information from the system by knowing the exact system password or by guessing the password. This is known as Password Guessing attack. Here a legitimate user access rights to a computer and network resources are compromised by identifying the user id/password combination of the legitimate user. To avoid this, the three factor authentication protocol is helpful.

When a user inserts the storage device into a client terminal, the authentication server asks for the identity, password and the one-time-password. The user inputs the password, identity and one-type-password being sent to the e-mail. Mutual authentication is then executed between user and authentication server. The authentication server checks if the details input by the user are matching with the details stored in the database. The authentication server then generates a session key if the user is successfully authenticated. With this key, user can store an encrypted file on the storage device.

When the user is successfully authenticated, a shared session key is generated between user and authentication server. Then, the session key will be used to encrypt the files transferred via the USB interface. When the user decrypts the files on the storage devices, the user must do the same authentication and generate the same session key for the original file. Every filename and user's identity will have a session key and different files or users' identity have different session keys. To ensure system security, the temporarily stored session key will be deleted after encrypting or decrypting the file.

The proposed protocol has the following three characteristics: (1) only authorized users can access the USB consumer storage devices; (2) files taken from the storage devices cannot be decrypted without the session key; and (3) other legal users cannot decrypt a legal classified file even if it is copied to their storage device. Therefore the original file is secure.

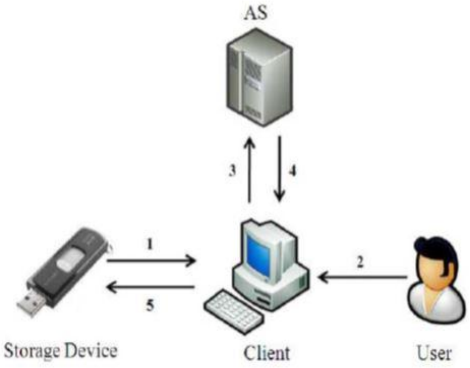
IV. PROPOSED WORK

In our work we provide additional security to the USB device by using multi factor authentication. In our work we propose a three factor security protocol for storage devices that keeps the device secure from many types of attacks such as man-in-the middle attack, password guessing attack, denial-of-service attack and replay attack. The proposed solution is presented with a rigorous security analysis and practical computational cost analysis to demonstrate the usefulness of this new security protocol for consumer USB MSDs.

Existing systems use various cryptographic algorithms for the key generation which involve huge cost and computational complications. The proposed protocol uses Elliptic Curve Cryptosystem (ECC) for key generation. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Also the keys generated by ECC are smaller compared to other cryptographic algorithms. Compared with the traditional public key cryptosystem, the ECC can provide better performance because it can achieve the same security level using a smaller key size. For example, the 160-bit ECC and 1024-bit from the popular Rivest– Shamir–Adleman (RSA) cryptosystem have the same level of security. Hence the cost needed to implement the proposed is less compared to that of the existing system.

In this paper, an enhanced three-factor security protocol is introduced that removes the shortcomings of past three-factor security protocols. The three factor authentication protocols include user identity, password and a one-time-password being sent to the e-mail id that the user provides during the registration phase. Hence the system is more secure from various types of attacks.

The proposed system consists of various modules. When the user inserts the USB device the AS detects the device and displays the port in which the device has been plugged in. The AS then checks if the user has already registered or if the user is a new user. If the user is a new user, then the AS provides the user with the registration form. The user inputs some basic details such user identity, password and the e-mail id to which the one-time-password should be sent. Only one user can register with the AS. Hence no other illegal user can gain access to the USB port by registering as authenticated user. If the user has already registered with the AS, then the AS displays the login page. The user inputs the user identity, password. If the user is authenticated, then it sends the OTP to e-mail id. If the user is authenticated, then the user gains access to the USB port. Finally the AS provides the user with the option for encryption.



A. Detection of USB device

When the USB device has been plugged in the port, the authentication server detects the device and displays the port in which the USB device has been plugged in. When the device has been detected the authentication server checks if the user has already registered or new user.

B. Disable the ports

When the server detects that the USB MSD has been plugged, the AS disables all the ports to prevent the user from copying the files from the PC to the USB device.

C. Matching with authentication server

The user inputs the username, password and the OTP being sent to the email in the login phase. The authentication server then compares the details input by the user with the details already stored in the database. If the details are matched then the AS grants permission to the user to access the USB port. Else the AS doesn’t consider the user as valid and denies access to the USB port.

D. Enable the ports

If the user is valid, then the authentication server then enables all the ports. Only if the ports are enabled, the user can transfer files to the USB MSD.

E. Encryption of Files

The files stored in the USB storage device are in text format and hence any illegal user can access the files stored in the USB device. To avoid this, the authentication server asks the user, if the file should be encrypted. If the user prefers file encryption, then the file is encrypted and transferred to the USB storage device. Else the original file is transferred to the storage device.

V. RESULTS AND DISCUSSION

In our system, initially the AS checks whether the user is already registered or not. If new user the AS displays the registration page else if already registered it displays the login page. When the user logins, the AS sends the OTP to the e-mail id to complete the login process. Then it asks the user to choose the file to be sent to the USB storage device. It also provides option for the user to select whether the file should be encrypted. If the user prefers file encryption, then it encrypts the file using ECC and transfers to the USB MSD, else it transfers the original file to the device.

VI. CONCLUSION

Thus the three-factor authentication protocol based on Elliptic Curve Cryptosystem for USB consumer storage devices has been shown to have significant advantages. But, there were still existing security vulnerability issues needed to be solved, specifically the password guessing attack, the Denial of service attack and the replay attack. The proposed protocol has been presented and rigorously analyzed in terms of security and computational cost. As shown, the proposed protocol is robust against conceivable attacks while at the same time having the same computational cost compared to the literature. The work is ideal to be embedded in the firmware of consumer based USB Mass Storage Devices thus relieving the user of extra security burdens and enabling the devices to be confidently used in the knowledge that the data stored is secure.

REFERENCES

1. Debiao He, Neeraj Kumar, Jong-Hyouk Lee, Senior Member, IEEE, and R. Simon Sherratt, Fellow, IEEE, “Enhanced Three-factor Security Protocol for Consumer USB Mass Storage Devices”, IEEE Transactions on Consumer Electronics, Vol. 60, No. 1, February 2014.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

3. B. Chen, C. Qin, and L. Yu, "A Secure Access Authentication Scheme for Removable Storage Media," Journal of Information & Computational Science, Binary Information Press, vol. 9, no. 15, pp.4353-4363, Nov. 2012.
4. C. Lee, C. Chen, and P. Wu, "Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices," IET Computers & Digital Techniques, vol. 7, no. 1, pp. 48-55, Jan. 2013.
5. F. Y. Yang, T. D. Wu, and S. H. Chiu, "A secure control protocol for USB mass storage devices," IEEE Trans. Consumer Electron., vol. 56, no. 4, pp. 2339-2343, Nov. 2010.
6. Mohamed Hamdy Eldefrawy, Muhammad Khurram Khan, Hassan Elkamchouchi, "The Use of Two Authentication Factors to Enhance the Security of Mass Storage Devices", 11th International Conference on Information Technology: New Generations, 2014.
7. M.H. Eldefrawy, M.K. Khan, K. Alghathbar, T.H. Kim, and H.Elkamchouchi, "Mobile one-time passwords: two-factor authentication using mobile phones," Security and Communication Networks, vol. 5, pp. 508-516, 2012.
8. Alzarouni. M.: 'The reality of risks from consented use of USB devices", Proc. 4th Australian Information Security Conf., pp. 312–317, 2006.
9. Yang, G., Wong, D.S., Wang, H., Deng, X.: 'Two-factor mutual authentication based on smart cards and passwords', J. Computer. System.Science , vol. 74, pp. 1160–1172, 2008.
10. Lauter, K.: 'The advantages of elliptic curve cryptography for wireless security', IEEE Wirel. Commun., pp. 1536–1284, 2006.
11. Schneier, B.: 'Applied cryptography, protocols, algorithms, and source code', Wiley, 2nd edn, 1996.
12. M. N. Rani, A. Kaushik, and M. Kumar, "A Review Based Study of Key Exchange Algorithms," International Journal of Recent Trends in Mathematics & Computing, vol. 1, 2013.
13. C. Wu, W. Lee, and W. J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," IEEE Communications Letters, vol. 12, no. 10, pp. 722-723, Oct. 2008.
14. D. Hankerson, S. Vanstone, and A. Menezes, "Guide to elliptic curve cryptography", Lecture Notes in Computer Science, 2004.
15. W. Yuan, L. Hu, H. Li, and J. Chu, "An Efficient Password-based Group Key Exchange Protocol Using Secret Sharing," Appl. Math, vol. 7, pp. 145-150, 2013.
16. Suratose Tritilanunt, Napat Thanyamanorot, Nattawut Ritdecha, "A Secure Authentication Protocol using HOTP on USB Storage Devices", Information Science, Electronics and Electrical Engineering(ISEEE), International Conference, vol. 3, pp. 1908-1912, 2014.