Survey of Enhanced Three-factor Security Protocol for Consumer USB Mass Storage Devices

Ranjana A.Vhankade
Department of Information Technology, Walchand College of Engineering, Sangli, Maharashtra, India

B.S.Shetty
Department of Information Technology, Walchand College of Engineering, Sangli, Maharashtra, India

Abstract- This study proposes a three-factor control protocol for universal serial bus (USB) device on an Advance Encryption Standard(AES) algorithm. USB or plug-n-play device is a universal interface used in an large number of devices. It has become the most popular interface standard for CPU connections. However, since USB provides very convenient to carry , many workplace ,high transmission speed, and commercial establishments have prohibited their employees from using USB devices. This provision is an important way to prevent privacy data leaks via USB devices, as USB connections is deficient in security management. Therefore , use a three-factor control protocol to make sure the security of storage device(USB) connections. The proposed three-factor control authentication protocol combines username, password of user and unique id of USB device for authentication of device to provide high security on the USB mutual authentication. To provide secure and efficient transmission between and the USB server and the user, the proposed protocol adopts AES (Advance Encryption standard) algorithm to encrypt data and user can not decrypt data without USB device authentication. Compared to other encryption methods, the proposed three-factor authentication protocol uses much key sizes. As a further benefit, this protocol reduces the smart card computational cost and provides an efficient transmission for USB devices. security AES is more secure and faster compared to the other algorithm and as memory usage of other algorithm[1] is higher AES has more efficiency than other algorithm. This new scheme improves the security, efficiency and usability of the authentication process. More studies on USB are needed.

Keywords – Data Confidentiality ,USB device unique id ,encryption,AES,removable media

I. INTRODUCTION

Rapid technological advancements in computing have led to the invention of more and more computer products. Universal serial bus (USB) is a popular standard that has been widely adopted in storage devices. USB has become an important component in current computer-connected devices due to its convenience and ease of connectivity. USB has the advantages of high data processing speed, plug-and-play, hot swapping and self-power supplying to peripherals. USB connections allow a wide range of different electronic devices to connect to computers, including keyboards, cell phones, chargers, speakers, printers and various electronic devices. 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 unauthorized 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. To solve the above-mentioned problems, we need a more secure authentication protocol for USB storage devices. Most early authentication protocols are password-based. These protocols are relatively easy to implement, but they have many weaknesses. For example, dictionary attacks can crack and steal passwords in a short time. Owing to these problems, the users need a more secure authentication protocol like user password and USB device authentication. The password authentication based on smart cards is also called two-factor authentication [2], meaning that the users must own the smart card to certify the passwords. The smart card-based password authentication provides stronger security guarantees than the earlier password-based

authentication. However, this authentication method is problematic if the two factors are compromised; the attacker can successfully obtain the password and any user data stored in the smart card. Three-factor authentication can help avoid this problem and enhance system security. Owing to the singularity, biometric authentication protocol is ideal for user authentication, and addresses the weakness of password and smart card methods. The users can use their own biometric characteristics, such as fingerprint [3], voiceprint and iris scan. Biometric characteristic identification systems offer reliable authentication because biometric characteristics cannot be copied, stolen or easily lost. Although there are many advantages in using biometrics, this approach still has some shortcomings. For example, biometric characteristics cannot be easily changed or replaced. For these reasons, there is a demand for a more secure protocol like three-factor authentication. The three-factor authentication method in this paper uses a username, password and unique id of device for device authentication/verification. The authentication is based on the characteristics of all three factors. Without device authentication(unique id of device) user can not encrypt the file or decrypt the file. The advantages of this three factor protocol is device authentication that are not applied in previous three-factor protocol. By using device authentication the system become most secure compared to previous protocols.

II. LITERATURE SURVEY

Removable media has the benefits of usage from any system and without any installation it is widely preferred among people for migration of data. But due to security breaches removable devices are restricted in many organizations as data can easily be stolen through USB MSD devices hence to protect the sensitive data many techniques have been used which are as follows

1) Smartcard as a second authentication factor:

In Yang et al. technique[2], when the user inputs the plug-n-play device required username, password and smart card authentication for confidentiality purpose. Then legitimate user is been given to open the encrypted files. The smart card responds with the equivalent verification value and thus eligibility to decrypt files on plug-n-play device is been gained by the user.. This mechanism also prevents forgery attack as device id is also been recorded. The password authentication based on smart cards is also called two-factor authentication [2] meaning that the users must own the smart card to certify the passwords. The smart card-based password authentication provides stronger security guarantees than the earlier password-based authentication. However, this authentication method is problematic if the two factors are compromised; the attacker can successfully obtain the password and any user data stored in the smart card.

The author constructed a two-factor control protocol with functionalities of mutual authentication and key agreement for USB storage device. In their scheme, a successful authentication requires a user to provide the correct password and storage device simultaneously. However, their scheme needs excess modular exponentiation operations, and thus is not efficient enough.To prevent the disclosure of data stored in the computer and storage devices via USB port, author proposed a control protocol that provides user authentication and key agreement.

Now demonstrate that Yang et al.'s [2] protocol suffers from impersonation attack when a user's USB storage device is lost, and thus fails to achieve two-factor authentication as they claimed. This kind of attack(Impersonation attack with disclosed password), indicates that Yang et al.'s protocol fails to achieve the basic security requirement of two-factor control protocol for USB storage device, namely, when the password is disclosed, the protocol is insecure. Furthermore, the reason that why Yang et al.'s control protocol cannot resist the above attack is that the private data stored in the storage device is not involved in the verification and data encryption phase**.**

2) Providing authentication using Diffie-Hellman key exchange agreement:

Mohamed Hamdy Eldefrawy [3] have proposed a secure and effective control protocol for USB ports. The protocol employs a remote authentication server to verify authorized users and use the key of Diffie-Hellmen technique to protect the privacy of a file transmitted to a storage device. We have further proved that our protocol can resist some general attacks. In terms of protocol communication costs, achieving mutual verification requires only two rounds of communication sessions. Therefore, the proposed protocol provides an efficient control protocol for USB MSD which is both secure and effective.

For key agreement author used Whitfield Diffie and Martin Hellman proposed the key exchange agreement in 1976. The purpose of the Diffie-Hellman key exchange is for both sides to get the same session key by sharing some secret information via exponential and modular computation when the both sides try to communicate. Subsequently, the key can be used for encrypting a message for transmission.

3) *Providing authentication using ECC technique*

Modular exponentiation operations, and thus is not efficient enough. To obtain a more efficient and secure control protocol for USB storage device, Lee et al. [4] introduced a three-factor authentication scheme by combining biometric, password and storage device. Compared with Yang et al.'s protocol, Lee et al.'s scheme involves an additional class of authentication factor (i.e. biometric) to enhance security of the protocol, and exploits an elliptic curve cryptosystem (ECC) and exclusive-or (XOR) operations to increase efficiency of the protocol.

USB control protocol is not efficient for transmission. Yang et al.'s protocol uses too much exponentiation in the transmission process. This reduces the speed of system transmission and wastes time in calculations, so that it cannot transmit efficiently.

The three-factor (password, smart card and biometrics) control protocol for USB devices using an elliptic curve cryptosystem (ECC) [5][6]. In the this scheme, any user who wants to pass as a system user must provide smart card, password and biometrics to achieve mutual authentication with an authentication server (AS). Without authentication, the system will deny user access to the USB port. After completing the mutual authentication, the user and the server system negotiate a common session key to encrypt and decrypt files transmitted through the USB port. The process described above protects the transmission of data to USB devices using system encryption. Next, we brief the ECC as follows.

An elliptic curve E over a prime finite field F_p is defined by an equation of the form $y^2 = x^3 + ax + b$, where a and b are arbitrary constants and $4a^3 + 27b^2 \neq 0$. G is a cyclic additive group under the point addition. The security of ECC is based on the following two problems. Given P, Q∈G, the discrete logarithm problem (DLP) is intractable to find a such that Q = aP. Given $a \times P$, $b \times P \in G$.

4) *Providing authentication using Biometrics of user*

In this technique, the biometric keys are used which have the advantages like it cannot be guessed easily, it cannot be forgotten or lost, extremely hard to copy or distribute and very difficult to copy or share. Authentication Server (AS) is used to manage security for a USB device. AS restricts the data transfer over USB MSD interface unless the user passes the AS's verification. If the user wishes to transfer the data he/she is required to input username, password and biometric characteristic to verify legitimacy [3].

Furthermore, by making use of a fuzzy extractor, author proposed an enhanced three-factor security protocol for consumer USB mass storage devices. Unfortunately, the security of their protocol is based on a strong and irrational assumption that the private information (i.e. biometric key) generated by a user's biometric is very difficult to copy or share. In fact, such assumption violates the security definition for three-factor authentication scheme[9,12]. As presented in Section 4, we will show that He et al.'s protocol fails to achieve three-factor authentication, and is not an efficient and practical two-factor control protocol for USB mass storage devices. When user wants to be the valid user of AS, he/she needs to input biometric characteristic, through a biometric device and provide password and identity. This input values are used for the authentication/verification procedure. When user is successfully authenticated, a shared session key is generated between AS and users. Then, the session key will be used to encrypt the files transferred via the USB interface. When the user decrypts the files on the USB MSD device user must follow the same procedure and generate the session key for the original file. The advantage of this is, it is robust against conceivable attacks but there is a still existing security vulnerability problems that is needed to be solved like the DoS attack and replay attack.

This protocol requires the fuzzy extractor that can be created from universal error-correcting codes or hash functions requiring only lightweight operations [7]. It is here implicit that the time for executing a fuzzy extractor is mostly same as that for executing an ECC(elliptic curve point) multiplication. Note that the ECC(elliptic curve point) multiplication as per computing the cost is considered as time-consuming and a complicated operation among the cryptographic operations.

V. DISSCUSSION

This paper shows that two stages and three stages secure control protocol by using ECC and biometric device have only user authentication not have device authentication. In proposed protocol we improve USB control using a three-factor method based on unique id of USB device. By using unique id we can do device verification from authentication server to system become most secure. The proposed protocol uses AES algorithm to increase the computing speed of transmission. Compared with the other protocol, the proposed protocol has better computational efficiency and lower memory requirements

AKNOWLEDMENT

Authors express our sincere thanks to all the authors, whose papers in the area of storage device security techniques has to be published in various conference proceedings and journals.

REFERENCES

[1] Jivani et al., International Journal of Advanced Research in Computer Science and Software Engineering 5(4),April- 2015, Volume 5, Issue 4, 2015.

[2] Yang, G., Wong, D.S., Wang, H., Deng, X.: "Two-factor mutual authentication based on smart cards and passwords", J. Comput. Syst.Sci., 2008, 74, (7), pp. 1160–1172.

[3] M. Hamdy Eldeframy, M. Khurram Khan1 and Hassan Elkamchouchi, "The Use of Two Authentication Factors to Enhance the Security of Mass Storage Devices", IEEE 11th International Conference on Information Technology: New Generations, 2014.

[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] Hankerson, D.Menezes, A.Vanstone, S.: "Guide to elliptic curve cryptography" (Springer, 2004) 19 Schneier, B.:'Applied cryptography,protocols,algorithms,and source code'(Wiley,1996,2nd edn.)

[6] Lauter, K.: "The advantages of elliptic curve cryptography for wireless security", IEEE Wirel. Commun. Mag., 2004, 4, (20),pp. 1536–1284.

[7] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," in Proc. 2004 Int.Conf. Theory and Applications of Cryptographic Techniques, Interlaken,

Switzerland, in Lecture Notes in Computer Science, pp. 523-540, 2004.

[8] 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.

[9] Pointcheval, D., Zimmer, S.: "Multi-factor authenticated key exchange". Proc. Sixth Int. Conf. Applied Cryptography and Network Security, Beijing, China, June 2008, pp. 277–295.

[10] Huang, X., Xiang, Y., Chonka, A., et al.: "A generic framework for three-factor authentication: preserving security and privacy in distributed systems", IEEE Trans. Parallel Distrib., 2011, 22, (8), pp. 1390–1397.