Secure Control Protocols for USB Mass Storage Devices

Ankit Verma
M.Tech.(CS),
Department of Computer Science & Engg.
K.N.I.T. Sultanpur
UP, India

D. L. Gupta
Asso. Prof.,
Department of Computer Science & Engg.
K.N.I.T. Sultanpur
UP, India

Abstract **- USB based devices are very handy in nature due to their plug and play technology. With the advancement of technology their data carrying capacity is increasing day by day, which is imposing a threat of data theft. Presently most of the USB mass storage devices are not secured and therefore most of the companies restrict USB mass storage devices due to fear of confidential data loss. To avail the benefits of high speed data transmission and convenience of use, many research scholars suggested different secure protocols for establishing communication with USB mass storage devices. This study shows various features of existing secure control protocols for USB storage devices.**

Index Terms - Biometrics, Consumer Storage, Mass Storage Device, USB, Authentication, Key exchange.

I. INTRODUCTION

Now a days, data play an important role for the success of an organization. Lot of research is going on in the field of computer science and information technology for the capacity enhancement and ease of transferring large data with the help of Universal Serial Bus (USB). USB based mass storage devices are finding widespread use in various fields due to high speed of data transmission and convenience provided by plug and play technology. However, such features make USB devices vulnerable to data theft and malicious user may extract confidential information from the computer system using them.

Many organizations prohibit/restrict the use of USB mass storage devices due to potential threat of data leakage. Therefore it is required to device a methodology to make it secure without compromising convenience of use. This study shows various features of existing secure control protocols for USB storage devices.

Focus of most of the security protocol is to get secure session key after attaining mutual authentication between client system and authentication server. With the help of secured session, server provide file encryption/decryption key to the client system.

Authentication has a vital role in implementation of access control. Generally four forms of human authentication parameters are:

- Chosen identity (i.e. User ID or Name)
- What you can remember (i.e. Password)
- What you possess (i.e. USB device)
- Your unique identity (i.e. Biometric)

For better security of a system, authentication mechanisms many times involve more than one authentication parameter simultaneously, such schemes are known as multi-factor authentication schemes. For successful authentication user needs possess required information to satisfy all the authentication factors. Compared to only password based schemes, biometric keys have the following advantages [9]:

1) Biometric keys cannot be lost or forgotten;
2) Biometric keys are very difficult to copy or share;
3) Biometric keys are extremely hard to forge or distribute;
4) Biometric keys cannot be guessed easily.

II. REVIEW OF EXISTING SECURITY PROTOCOLS

Yang et al [1] proposed a Secure Control Protocol for USB Mass Storage Devices in 2010. In his proposed two-factor authentication protocol, user first achieve mutual authentication with an authentication server by supplying username and password for the plugged USB device. In order to use USB interface, User has to pass this authentication mechanism. After the user authentication, a session key is negotiated between user and the server, which is used to securely share symmetric key for encryption/decryption of files transmitted through USB interface.

Yang et al used Schnorr's digital signature scheme [15] for remote authentication purpose and Diffie-Hellman [6] key exchange for session key establishment. Proposed protocol is divided into two phases, namely Registration Phase and Verification & Data Encryption Phase. User needs to complete authentication mechanism every time before reading or writing of file stored on USB device.

Das [2] proposed analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards in 2011. His protocol was based on three factor authentication mechanism namely biometric, Password and user identity. To improve the input accuracy of noisy biometric system, das proposed to use biometric template pattern matching. His protocol consists of four phases, namely Registration phase, Login phase, Authentication phase and Password change phase. After plugging device into the client system, login phase of the protocol starts with biometric input from user. After successful biometric authentication, user inputs password. Protocol proceeds with stage wise clearance and finally do mutual authentication with remote server using random nonce. If successful, user is allowed to use device, otherwise session aborted and access denied.

Lee et al. [3] proposed a Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices in 2013. Two-factor authentication i.e. USB device and password based authentication provides better protection as compared to the earlier only password based authentication. However, if attacker got the physical device somehow then only one factor needs to be compromised to breach the security of this type of protocol.

Three-factor authentication schemes can handle such situations in a better way. In Lee et al protocol, third factor is biometric authentication apart from device and password. Biometric parameters cannot be stolen or copied easily hence provide better and reliable authentication as compared to other authentication mechanism.

The proposed protocol uses three-factor authentication and elliptic curve cryptosystem (ECC) [8] to encrypt the files inside USB device. As compared to traditional public key cryptography system, the ECC can perform better and can provide similar security using a smaller key size .Proposed protocol is divided into three phases, namely Registration Phase, Verification and Data Encryption Phase and last, Key agreement phase.

In this protocol, user inserts his USB device into client system and inputs the personal biometrics along with user ID and Password. After successful authentication, a session key is established using ECC between user system and authentication server. This session key is then used to encrypt the symmetric key which will actually be used for file encryption/decryption in USB device. Due to the absence of modular exponentiation operations, computational cost of proposed protocol is significantly less than the Yang et al. [1] protocol; however it is more secured because of three factor authentication mechanisms.

He et al. [4] introduces enhanced Three-factor Security Protocol for Consumer USB Mass Storage Devices in 2014. Proposed protocol claims to eliminate the existing shortcomings of three factor authentication protocol. As we know that biometric characteristic of every person vary from time to time hence it is possible that legitimate user may face denial of service for his valid request if his biometric is directly used for authentication. To overcome this biometric variation issue, He et al proposed concept of fuzzy extractor [7] which caters delta change in biometric characteristic, thereby avoiding denial of service.

The computational cost of given protocol is slightly higher than Lee et al's [3] protocol due to fuzzy extractor operations, but He et al. claims that their protocol can withstand many known attacks like Password guessing attack, DoS attack, Replay attack, Stolen-verifier attack, Impersonation attack, Mutual authentication and Man-in-the-middle attack.

Jiping et al. [5] introduces an Improved Biometric-Based User Authentication Scheme for Client Server System in 2014. This protocol claims to overcome the design flaws in existing Das's scheme [2] with additional improvements such as security aspect and mutual authentication. To improve the verification of noisy biometric system it includes tolerance mechanism, so that minor variation in biometric characteristics should not halt the system. It also incorporated transmission delay mechanism between client server communication to withstand various known attacks like Man-in-the-middle attack and Replay attack. Similar to Das [2] protocol, this protocol also consists of four phases, namely Registration phase, Login phase, Authentication phase and Password change phase.

After plugging device into the client system, login phase of the protocol starts with biometric input from user. After successful biometric authentication, user inputs password. Protocol proceeds with stage wise clearance and finally do mutual authentication with remote server using random nonce. If successful, user is allowed to use device, otherwise session aborted and access denied. Jiping et al. claims that their protocol can withstand many known attacks like Denial-of-Service Attack, Stolen-Verifier Attack, Many Logged-In Users Attack, Guessing Attack, ReplayAttack, User Impersonation Attack, Server Masquerading Attack, Insider Attack, Mutual Authentication and Man-in-the-Middle Attack.

Wei et al [14] proposed a secure control protocol for universal serial bus mass storage devices in 2015. In this protocol there is nothing stored inside USB device to locally verify the authenticity, instead everything is validated through server, although this may create additional communication overhead but security can be assured.

Verification is based on Diffie–Hellman [6] key exchange to generate a secured session key between server and client. Time-stamping is used to ascertain freshness of data. Symmetric encryption/decryption key is shared using session key and all files are encrypted and secured with this key. Without following proper authentication mechanism, user cannot access USB device data.

Giri et al. [13] proposed Efficient Biometric and Password Based Mutual Authentication for Consumer USB Mass Storage Devices in 2015. It consist of five phases namely registration phase, login phase, authentication and session key agreement phase, data retrieval phase and password update phase. During registration phase, some parameters are stored into USB device which are used for local authentication purpose later.

Data inside USB device is stored after encrypting it using shared session key. Data identity and session key also saved inside USB device after encryption using biometrically derived random string and user ID.

During data retrieval phase, firstly data identity and session key is retrieved from USB device then using decrypted session key remaining data is obtained. Giri et al. claims that their protocol can withstand many known attacks like replay attack, forgery attack, off-line password guessing attack.

TABLE I
SECURITY COMPARISONS AMONG RELATED PROTOCOLS

Attack Vulnerability / Feature	Yang et al. [1]	Das [2]	Lee et al. [3]	He et al. [4]	Jiping et al. [5]	Wei et al [14]	Giri et al. [13]
Stolen-verifier attack	N	N	Y	N	N	N	N
Impersonation attack	Y	N	Y	N	N	N	N
Replay attack	N	N	N	N	N	N	N
Mutual authentication	Y	Y	Y	Y	Y	Y	Y
Session key agreement	Y	Y	Y	Y	Y	Y	Y
Forward secrecy	Y	Y	Y	Y	Y	Y	Y
Multi-factor authentication	N	Y	Y	Y	Y	Y	Y
Fuzzy extractor	N	N	N	Y	Y	N	Y
Denial-of-service attack	N	Y	Y	N	N	N	N
Off-line password guessing attack	N	N	Y	N	N	N	N

III. CONCLUSION AND FUTURE WORK

This paper presents various client/server based secure control protocols for Universal Serial Bus (USB) mass storage devices. The survey has shown that how different protocols withstand in front of various known attacks like stolen-verifier, man-in-the-middle attack, replay attack, impersonation attack, Password guessing attack and establish mutual authentication with remote authentication server. Proposed protocols commonly uses generic cryptographic functions like one way hash function, XOR operation, symmetric encryption/decryption, fuzzy extractor operation etc.

Security protocols in future can become de-facto standard for USB mass storage devices. These protocols can be embedded into the firmware of consumer mass storage devices to provide secured access and better authentication. Better security will create confidence among users for data protection.

REFERENCES

[1] 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.

[2] A. K.Das, “Analysis and improvement on an efficient biometric based remote user authentication scheme using smart cards,” IET Information Security, vol. 5, no. 3, pp. 145–151, 2011.

[3] 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.

[4] D. He, N. Kumar, J.-H. Lee, and R. S. Sherratt, “Enhanced three-factor security protocol for consumer USB mass storage devices,” IEEE Trans. Consumer Electron., vol. 60, no. 1, pp. 30-37, Feb. 2014.

[5] L. Jiping, D. Yaoming, X. Zenggang, and L. Shouyin, “An improved biometric-based user authentication scheme for c/s system,” Int. J. Distributed Sensor Networks. Article ID 275341, pp. 1-9, April 2014.

[6] W. Diffie, and M.E. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theor. vol. 22, no. 6, pp. 644-654, Nov 1976.

[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] D. Hankerson, S. Vanstone, and A. Menezes, “Guide to elliptic curve cryptography,” Lecture Notes in Computer Science, 2004.

[9] C. -T. Li, and M. -S. Hwang, “An efficient biometrics-based remote user authentication scheme using smart cards,” Journal of Network and Computer Applications, Elsevier, vol. 33, no. 1, pp. 1-5, Jan. 2010.

[10] D. -J. Kim, K. -W. Chung, and K. -S. Hong, "Person authentication using face, teeth and voice modalities for mobile device security", IEEE Trans. Consumer Electron, vol. 56, no. 4, pp. 2678-2685, Nov. 2010.

[11] K. -A. Shim, “Security flaws in three password-based remote user authentication schemes with smart cards,” Cryptologia, Taylor and Francis, vol. 36, no. 1, pp. 62-69, Jan. 2012.

[12] D.-J. Kim, and K.-S. Hong, “Multimodal biometric authentication using teeth image and voice in mobile environment,” IEEE Trans. Consumer Electron., vol. 54, no. 4, pp. 1790-1797, Nov. 2008.

[13] D. Giri, R. S. Sherratt, T. Maitra, and R. Amin, “Efficient Biometric and Password Based Mutual Authentication for Consumer USB Mass Storage Devices,” IEEE Trans. Consumer Electron., vol. 61, no. 4, pp. 491-499, Nov. 2015.

[14] J. Wei, W. Liu, X. Hu, “Secure control protocol for universal serial bus mass storage devices,” IET Comput. Digit. Tech., 2015, Vol. 9, Iss. 6, pp. 321–327, Apr. 2015.

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