ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(37), DOI: 10.17485/ijst/2016/v9i37/102546, October 2016* ISSN (Online) : 0974-5645

Secure USB Authentication on Distributed Cloud Computing Environments

Sunghyuck Hong*

Division of Information and Communication, BaekseokUniversity, Cheonan, Chungnam, 33065 Korea; sunghyuck.hong@gmail.com

Abstract

Objectives: Authentication is the first step of secure communication. Especially, cloud environment is a critical issue for user authentication because cloud storages have a lot of user credentials. **Methods/Statistical Analysis**: To solve this problem, security USB is released currently, especially in the public sector, use a mandatory system of security USB memory in the enterprise has been applied. However, information for user authentication or be stored in plain text in a specific area of the USB memory, vulnerabilities that can be authenticated bypassed by user interaction is found. **Findings:** Cloud storage services are getting popular and it must be secured. Otherwise, personal privacy could be compromised. Once username and password are compromised, valuable information will be in jeopardy. USB memory is small, cheap and the capacity ratio of price as a portable storage medium to provide a large capacity, it has secured already many users. Further, due to the small size, often lost or stolen accident, flows out the data in the USB memory, social problems such as major technology leakage of effluent and industrial personal information has occurred. **Improvements/ Applications**: To solve the vulnerability of such user's authentication, by using the structure properties of the hash function and encryption algorithm and the storage medium presents a secure user's authentication methods.

Keywords: Access Control, USB, User Behavior, Secure Authentication

1. Introduction

The certification is the process of determining whether someone or just things that people are reported (or just those things). Authentication of the public network or the Internet, including the individual, is through the use of a password to log usually. The person who knows the password is considered to be one reliable user. All users initially register a password of their choice on and after each use continued, the user must use a password that is not forgotten in the previous report. However, the weakness of this system is in critical transactions, such as money exchange is involved, passwords are often stolen or may be known or accidentally or be forgotten[1–3]. Currently, USB memory is getting smaller and smaller. However, the storage size of USB is getting bigger and bigger. USB memory is stolen or copied by immoral employees to sell company's valuable information. Therefore, secure USB must be used for protecting technical information. Secure USB memory is user authentication information for user authentication mainly used in the method of storing a particular area. The user using this increased value is stored when plain text password has been exposed or malicious user. Since the operation has been found in possible authentication bypass vulnerability. This paper addresses a vulnerability in the user authentication of such secure USB structured of a hash function and encryption algorithm and a USB memory by using the character, I propose a secure user authentication methods[3]. A conventional USB storage configuration is as shown in Figure 1. According to[1], the process we have to verify whether who the (certification) is an important way to protect the online information of the individual. E-mail confirmation, so that access to online shopping or bank account, in order to obtain our personal information, you need to use a safe way for us to prove who you are. In order to prove yourself, you have three ways. In other words, such as passwords, that we know, like a passport, what we have, as of the fingerprint, there is only thing that we have. These methods are, there

* *Author for correspondence*

are advantages and disadvantages, respectively. The most common method of authentication, such as passwords and use of the fact that we know in Table 1.

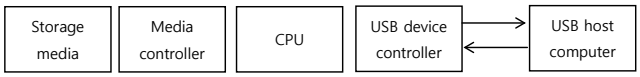

Figure 1. Conventional USB configuration.

1.1 Password-based Authentication

We are using almost everyday password in everyday life. The purpose of the password is what we prove who you are. The password is one of the examples of the things that we know. The risk of password has, you can guess the other person is the password, to disguise the identity and access to the password, you can have access to all the information that is protected by a password. So, for an attacker to hard to guess, please tell me how to protect your password as the strong password. Password the problem is that soon become obsolete. As new technology is developed, using the same technology as the key input value collector, cyber attack, you can guess collection to test more easily password. It is easy for strong authentication but requires a more secure manner. Fortunately, the method has been used a lot, called the recent two-step authentication. To protect us, as much as possible, it is strongly recommended that you use this method[4–8].

1.2 Software-based Key Authentication

In order for users of Internet banking and telephone banking smart to take advantage of services such as account transfer and financial product registration, unless the electronic signature to an electronic document in the user's private key, the effect will occur. Create a secret key with the public key-based systems, electronic signature generation information, so you must be only to those who have been authenticated the electronic signature generation information from accredited certification body, to use it in both Internet banking and smart telephone banking in is used to copy the certification certificate and private key for. For general users, certification certificate and private key, not only not a file format in contact with the general, because it is located in the general folder you do not have access, their official certificate and a secret that has been made in the file it is difficult to identify the key[9–13]. Be copied to this smartphone feels more difficult. In the financial company, in order to make me overcome the difficulty and inconvenience of these users, it is willing to offer a public certificate of copy services for the smart telephone banking[14–19].

1.3 Security Requirements

In this section, USB security for user authentication on technology security requirements is showed and attempts to analyze. Authentication is confirmed whether the user is a legitimate user and the process by which a user and the user information registered in advance authentication by contrast to the information you enter could prove the user. For user authentication must meet the following security requirements[20–22]:

- Camouflage: The user does not justify the camouflage as a legitimate user if you receive a certification.
- Forging and Modulation: When forged or modulate the message for the authentication information.
- Exposure: The exposure value authentication information to any other third party authentication values if you use.

2. Proposed Methods

User environment of a computer network as in the past, simply information Telephone banking not only to take advantage of search and e-commerce[23–27]. It has been expanded to the same commercial field. As a result, the online of trespassing network security block so that it can

Table 1. Types of authentication

Authenticatio Element	Password-based Authentication	Software-base Authentication	Hardware-base Authentication	Biometric-based Authentication
Authenticator	Password	Certificate	Secure Card	Biometric information
Authentication Mechanism	Password Validation Software	Certificate Validation Software	Card Validation Software	Biometric Recognition Device
Environment	Client-Server	Web-based Client-Server / Multicast	Client-Server	Client-Server

not access the self-critical information. The importance of it is emphasized to the outside of the intruder that is not allowed. Information and shall flow out, outside of the intruder of security data. It shall not be possible to manipulate the content[28–31]. The computer is composed of hardware and software, an error in one of the two parts is generated, a problem throughout the computer occurs. To avoid these problems, we are using the simulation and testing techniques. However, testing techniques, the only all possible testing techniques a drawback that it is impossible to check the operation of the execution, it is difficult to ensure the high level of reliability. Thus, shaping verification methods have been proposed based on mathematical accuracy to ensure the reliability of the problems with the computer system. In this paper, using the NuSMV, to shape the Needham- Shroeder protocol.

Model checking (Model checking), from among the verification method, which is a typical validation technique. This is automatically formatted verification technology the accuracy of the finite state machine. Finite state the operation of the system. Specify in the form of a machine, to express if the characteristic If you are not satisfied by that system in temporal logic, such as the CTL and LTL. In the subsequent representation properties it is specified in the finite state machine system, a method for inspecting whether satisfied in all cases. Through these Moderuchi Ekkingu technique, a very complex system, such as hardware and communication protocols can be shaped successfully validated[32–37].

2.1 Hardware Method

In the case of hardware system, especially wearing the different hardware chip to USB memory, to perform such as authentication and data encryption of the useras follows:

- Low in another storage area that is built authentication value for user authentication Run the method of the chapter. This is a malicious user to random access less likely it offers stability.
- Difficult to hardware implementation.
- Increase of another device according to production costs for security.
- There exists the possibility of user authentication bypass the authentication chip removed in some of the product.

2.2 Software Method

If the software system, by operating the security program in the USB memory, using the program, features are as follows in the method of performing an authentication and encryption of the user:

- The password stored in a specific area of the USB memory damage and counterfeiting of objection for user authentication, the possibility of forgery.
- In some of the product, there is a security vulnerability due to password clear text save for user authentication.
- To prevent the exposure of the plaintext password, but to save the hash value, it can be authenticated bypassed by counterfeit or forged.
- To reduce production costs as compared with the hardware method, easy to implement.
- In this research, I use the software user authentication, by using the structural features of the hash function and encryption algorithm of the existing memory proposes a more secure user authentication.

2.3 Storage Location for Authentication Value

Authentication is carried out in a way that controls the user authentication value previously saved with the password entered by the user, the location of the authentication value, not must the place where the general user is not easy to publish. Therefore, in this paper and access on a sector basis in the USB memory, using a method of storing user authentication value in reserved areas not used by the file system. Using the method as described above, it will not be able to normal operation the user authentication value. Movement of files, there is no risk that the authentication value may be damaged from the normal tasks such as Delete. Notationis shown in Table 2. The secure credentials stored using a hashing algorithm and encryption algorithm and protocol are as follows:

Step 1: Users to XOR the production number of the user authentication password and products set to generate a key for encryption.

ÅKeyŅČ_ĀÁ ČE

Step 2: For password control, the user stores the hash value of the encryption key previously set.

Sec_Area[H[Key]]

Step 3: Add a flag to the security zone information, to save the no value of peripheral meaning of encrypted inareserved area together.

$Sec\_Area[E_{Key}[A|F|S\_INF|A]]$

Table 2. Notation

P_ID	**Product identity**
PW	Secure USB Authentication password
S_INF	Security Area
Key	Secret key for encryption
A	To make expose with random meaningless value
R	Random number
F	Special code in secure area
E[]	Encryption function
D[]	Decryption function
H[]	Hash function
Sec_Area	Store in USB memory area

2.4 Authentication Method

Protocol authentication method is as:

Step 1: The user to generate a key for decryption and XOR production a numeric number of the password and the product that you entered.

åKeyŋČ_ĀÁ ČE

Step 2: Hashes the encryption key that you set in the destination is compared with the stored value.

H[Key]' = H[Key]

Step 3: If the password is correct, to decrypt the passphrase that contains the information of the security zone that is stored in a reserved area of the value of the key that you just created.

$D_{Key}[E_{Key}[A|F|S\_INF|A]'] = A|F|S\_INF|A$

Step 4: To extract the flag in decrypted value, stored in a random position, to find the information in the security zone and to provide a security zone.

2.5 Analysis

The proposed scheme, depending on the security requirements, perform analysis, such as it can do:

- Camouflage: Because to use the user authentication using a password is very little possibility of identity impersonation.
- Forgery and Falsification: Because even if a counterfeit and modulation user authentication values, it is impossible to decrypt the encrypted value of the security zone, which provides stability.
- Exposure: To encrypt the information storage and security zone for the user authentication value using the hash function, the authentication information is not published.

3. Conclusion

Therefore, once user name and password are compromised, valuable information will be in jeopardy. In this study, we studied the measures for secure user authentication in the USB security system. Core security USB system, in order to guarantee the reliability of user authentication in the user authentication, it is necessary to continue research. Further, through a combination of a software system and the hardware system, it is expected to be necessary to develop USB security system to provide a more powerful and complete security services. Therefore, we proposed secure USB based user authentication in a cloud environment to increase the security level.

4. Acknowledgement

2016 Baekseok Research Fund supports this research.

5. References

1. Evans W. Jr, Weiss KE. A user authentication scheme is not requiring secrecy in the computer. Communication of the Association for Computing Machinery. 1974 Aug; 17(8):437–42.
2. Yi X, Shenzhen Y. Anomaly detection based on web users' browsing behaviors. Journal of Software. 2007; 18(4):967–77.
3. Mather T, Kumaraswamy S, Shahid L. Cloud security and privacy: An enterprise perspective on risks and compliance (Theory in Practice). 1st ed. O'Reilly Media; 2009 Oct.
4. Bae K, Yim K. Analysis of an intrinsic vulnerability on keyboard security. Journal of the Kandersteg International Scout Centre. 2008 Jun; 18(3):89–95.
5. Shiralizadeh A, Hatamlou A, Massari M. Presenting a new data security solution in cloud computing. Journal of Scientific Research and Development. 2015; 2(2):30–6.
6. Lee K, Bae K, Yim K. Hardware approach to solving password exposure problem through keyboard sniff. World Academy of Science, Engineering and Technology. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering. 2009; 3(8):1501–3.
7. O'Gorman L. Comparing passwords, tokens and biometrics for user authentication. Proceedings of the IEEE. 2003 Dec; 91(12):2021–40.
8. Jung T, Yim K. Countermeasures to the vulnerability of the keyboard hardware. Journal of the Korea Information Security and Cryptology. 2008; 18(4):187–94.

9. Kaur R, King S. Analysis of security algorithms in cloud computing. International Journal of Application or Innovation in Engineering and Management. 2014 Mar; 3(3):171–6.
10. Lockdown: A safe and practical environment for security applications. 2009. Available from: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1004&context=cylab
11. Padmapriya A, Subhasri P. Cloud computing, reverse Caesar cipher algorithm to increase data security. International Journal of Engineering Trends and Technology. 2013 Apr; 4(4):1067–71.
12. Li W, Ping L. Trust model to enhance security and interoperability of cloud environment. Springer Berlin Heidelberg: Cloud Computing; 2009 Dec. p. 69–79.
13. Arockiam L, Monikandan S. Data security and privacy in cloud storage using hybrid symmetric encryption algorithm. International Journal of Advanced Researching Computer and Communication Engineering. 2013 Aug; 2(8):3064–70.
14. Millan GL, Perez MG, Perez GM, Skarmeta AFG. PKI-based trust management in inter-domain scenarios. Computers and Security. 2010 Mar; 29(2):278–90.
15. Kingpin. Attacks on and counter measures for USB hardware token devices. Proceedings of the Fifth Nordic Workshop on Secure IT Systems Encouraging Co-operation; Reykjavik, Iceland. 2000 Oct. p. 35–57.
16. Electronics Computer Technology (ICECT) 2011 3rd International Conference on Kanniyakumari. 2011. Available from: http://toc.proceedings.com/12007webtoc.pdf
17. William S. Cryptography and network security, Principles and practices. 6th ed. Prentice Hall; 2013 Mar.
18. Hwang SJ, Park KH. A keyboard security method based on a sub-classing. Journal of Korea Multimedia Society. 2011; 14(1):15–23.
19. Shakeeba SK, Tuteja RR. Security in cloud computing using cryptographic algorithms. International Journal of Innovative Research in Computer and Communication Engineering. 2015 Jan; 3(1):148–54.
20. Research on trust model of PKI. 2011. Available from: https://www.researchgate.net/publication/232639129_Research_on_trust_model_of_PKI
21. Data encryption and decryption algorithms using key rotations for data security in the cloud system. 2014. Available from: http://ieeexplore.ieee.org/document/6884895/
22. Chen D, Zhao H. Data security and privacy protection issues in cloud computing. IEEE Proceedings of International Conference on Computer Science and Electronics Engineering; 2012. p. 647–51.
23. Purdy GB. A high-security log-in procedure. Communications of Association for Computing Machinery. 1974 Aug; 17(8):442–5.
24. Kwon K, Ahn SJ, Chung JW. Network security management using ARP spoofing. Springer Berlin Heidelberg; 2004 May. p. 142–9.
25. Haller NM. The S/Key one-time password system. Proceeding Internet Society Symposium on Network and Distributed System Security; 1944. p. 151–7.
26. Arockiam L, Monikandan S. Arocrypt: A confidentiality technique for securing enterprise's data in the cloud. IJET. 2015 Feb-Mar; 7(1):245–53.
27. A new noise mingling approach to protecting the authentication password. 2010. Available from: http://ieeexplore.ieee.org/document/5447494/?reload=true&arnumber=5447494
28. Jeong H. Vulnerability analysis of secure USB flash drives. IEEE International Workshop on Memory Technology, Design and Testing; 2007. p. 61–4.
29. Yim K. A fix to the HCI specification to evade ID and password exposure by USB sniff. Proceedings of APIC-IST 2008; 2008 Dec. p. 191–4.
30. Mitchell CJ, Chen L. Comments on the S/KEY user authentication scheme. ACM Operating Syst Rev. 1996 Oct; 30(4):12–6.
31. Trusted framework for health information exchange. 2013. Available from: https://www.healthit.gov/sites/default/files/trustframeworkfinal.pdf
32. Zhang N, Shi Q, Merabti M. Anonymous public-key certificates for anonymous and fair document exchange. IEEE Proceedings-Communications. 2000 Dec; 147(6):345–50.
33. Abbasi G, Muftic S. Cryptonet, security management protocols. DNCOCO'10 Proceedings of the 9th WSEAS International Conference on Data Networks, Communications, Computers; 2010. p. 15–20.
34. Yu J, Wang G, Mu Y, Gao W. An efficient generic framework for three-factor authentication with provably secure instantiation. IEEE Transactions on Information Forensics and Security. 2014 Dec; 9(12):2302–13.
35. Pansa D, Chomsiri T. Security web improving by using dynamic password authentication. International Conference on Network and Electronics Engineering. 2011; 11:32–6.
36. Hong S. Multi-factor user authentication on group communication. Indian Journal of Science and Technology. 2015 Jul; 8(15):1–6.
37. Hong S. Hybrid routing algorithm on mesh network based on traffic records. Indian Journal of Science and Technology. 2015 Apr; 8(S7):327–31.