International Journal of Scientific Research in Computer Science, Engineering and Information Technology

© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Enhanced Three-Factor Security Protocol for Consumer USB Mass Storage Devices

Kirti Kamthe, Prtithviraj Chavan, Monika Jadhav, Kavita Phadatare

KJEI's Trinity Academy of Engineering, Pune, Maharashtra, India

ABSTRACT

USB stands for universal serial bus, it is very famous and accepted as bridge for connecting different computer systems and its peripherals. Generally, user uses USB as MSD (Mass Storage Device) as it is very convenient and easily connects to computer system. As it is very easy to connect means it has more drawbacks. USB can get attacked by different attacks such as replay attack, password guessing attack, denial of services attack. And for saving from these attacks we are proposing new technique called as three factor security protocol. From the previous papers we have learnt different techniques. From the first paper wireless communication authentication scheme with anonymity have been analyzed. Also security errors with sensible cards within three user authentication scheme based on password is learnt from another paper. After that Li-Hwang's has improved the user authentication scheme based on password and smart card. Jong-Hyouk Lee implemented work for HOTA (Handover Optimized Ticket Based Authentication) for enabling MN The implemented protocol is described with precise analysis of security with analysis of cost computation with practical. All this analysis explains importance of using USB-MSD to its users.

Keywords : Authentication, Mass Storage Device, USB.

I. INTRODUCTION

USB can get attacked by different attacks such as replay attack, password guessing attack, denial of services attack. And for saving from these attacks we are proposing new technique called as three factor security protocol. The implemented protocol is described with precise analysis of security with analysis of cost computation with practical. All this analysis explains importance of using Universal Serial Bus –Mass Storage Device to its users.

System requirements specification document is required to produce a detailed summary of our product of the software, its parameters and goals. This document describes the projects audience and its hardware interface and code necessities. It defines however our consumer, team and audience observe the product and its functionality.

Replay attack: Also known as playback attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as a part of masquerade attack by IP packet substitution.

Password guessing attack: Here a legitimate users access rights to a computer and network resources are compromised by identifying the user ID/password combination of the legitimate user.

Password guessing attack is of two types:

1.Brute force attack.
2.Dictionary attack.

Brute force attack: Consists of trying every possible code, combination or password until you find the correct one. This type of attack may take long time to complete. A complex password can make the time for identifying the password by brute force long.

Dictionary attack: It is another type of password guessing attack which uses a dictionary of common words to identify the user password.

CSEIT1722154 | Received :18 March 2017 | Accepted: 30 March 2017 | March-April-2017 [(2)2: 418-422]

Denial of services attack: In a computer, a Denial of services(DOS) attack is an attempt to make a machine or network resource unavailable to its intended user, such as to temporarily or indefinitely interrupt to the internet.

Dos is a typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate request from being fulfilled.

II. METHODS AND MATERIAL

A. Literature Survey

[1] Chia-Chun Wu et.al has been presented wireless communication authentication scheme with anonymity, therefore few security problems are incontestable. Here author have discussed some issues which was found in the proposed system so that they would find way to overcome these issues. These issues were related to the properties of anonymity and backward secrecy. It is very essential to recognize authenticated wireless users to avoid restricted use of resources. Also author have focused on characteristics of anonymity for protecting the user’s privacy. In this paper, every security problem is verified firstly and then proper solutions on it have been proposed. Here author have explained the different properties of backward secrecy as well as anonymity under the authentication strategy for wireless communication. The analysis has shown that the problems related to security within the previous schemes will be solved with very easy method.

[2] Kyung-Ah Shimhave detected security errors with sensible cards within three user authentication scheme based on password. The results of the work shows that no additional authentication schemes based on password with sensible cards should be made with such ad-hoc strategies. These ad-hoc strategies are the formal style methodology through demonstrable security approach. This approach would be utilized in future style. These approaches are very common technique for checking the validity of the login message and authenticate the user. The remote password authentication scheme in 1981 demonstrated the remote users over an insecure channel. From that time, number of authors has started proposing similar schemes for enhancing security, efficiency, and cost of the same approach. Authors have shown that 3 improved versions are still not secure against several active attacks. We tend to noticed security flaws within the 3 password-based remote user authentication schemes with sensible cards. We tend to didn't propose an improved version to beat the protection weaknesses since we can’t guarantee its security against all best-known attacks and unknown potential attacks with only heuristic security analysis. The formal design methodology with demonstrable security approach as in should be used in future design.

[3] Jong-Hyouk Lee ,Jean-Marie Bonninhave implemented HOTA (Handover Optimized Ticket Based Authentication) for enabling MN. This HOTA is utilized for reusing the credential provided by an AS (Authentication Server). After handover authentication is performed by MN on various networks. Latency of handover is minimizes by reusing the credentials and also makes very simple handover authentication procedure. Limitations of the system are mobility signaling occurred for each moment on MN. And another is MN doesn’t produces their own mobility signal.HOTA have been presented for managing the centralized mobility. Centralized mobility maintains and handles mobility context as well as routing status of registered MNs. This maintaining and handling is done by using LMA (local mobility anchor) of PMIPv6. But centralized management might be suffered from mobile internet traffic which is increasing fast. So for saving from this traffic distributed mobility management is standardizedat IETF within the architecture of flat mobile networks.Anchors of mobility have been distributed at high scalability level of an access network. Also while offering the better performance to end to end packet transmission no failure signals are provided. HOTA is implemented in some accessible networks, in future author had planned to extend HOTA into distributed mobility management.

[4] C-C Lee, C-T Chen, P-H Wu, T-Y Chenexplains the combine biometric authentication through password and smart card for providing high security for authentication of mutual UBS. The proposed method allows ECC for information encoding for secure and proficient transmission between user and USB server. The proposed method utilizes smaller key size than any other strategies. As an additional profit, this protocol decreases the process of smart card price calculation. And also it gives a capable transmission for USB

devices. This new scheme progresses the safety, effectiveness and usefulness of the authentication method. A lot of studies on USB are required. Different authentication schemes supported biometrics offer high security and singularity; however biometric identification has some imperfect options similarly. The planned protocol utilizes smaller key sizes to extend the speed of computation of transmission. As compared with the initial protocol, the planned protocol has higher process efficiency and needed lower memory.

[5] Firstly A.K. Dashas studied the recently planned technique of Li-Hwang's biometric-based remote user authentication scheme through the smart cards; then showed that the Li-Hwang's methodology had some design errors in their implementation. This method is improved more for avoidingthose errors in their implementation. The author has proved that the proposed method gives high authentication through biometric password as compared to Li-Hwang's scheme and different related schemes as well. Users are not able to give non repudiation while using method of remote user authentication with password and cryptographic key. Because the cryptographic key can be forgotten, shared to other user or might be lost and so that it is impossible to identify authenticated user.

[6] Remote user authentication scheme is a procedure which allows a server to authenticate a remote user through insecure channel. Recently, Yoon, Ryu and Yoo made an enhancement based on Ku–Chen's remote user authentication scheme by using smart cards. The scheme has the merits of providing mutual authentication, no verification table, freely choosing password, involving only few hashing operations and parallel session attack resistance. In this paper, author pointed out security flaws of Yoon–Ryu–Yoo's protocols against masquerading attack, off-line password guessing attacks and parallel session attack. An improvement to enhance Yoon–Ryu–Yoo's security scheme is proposed. Author founded that masquerading attack and password guess attack were existed. As solutions to these drawbacks, this paper presented an efficient scheme. The proposed scheme not only inherits the merits of their scheme but also enhances the security of their scheme. Author presented a cryptanalysis of Yoon–Ryu–Yoo's scheme by showing that their scheme is vulnerable to parallel session attack, masquerading attack and password guess attack. The proposed work is an enhancement to Yoon–Ryu–Yoo's scheme.

[7] In this paper, security flaws in three password-based remote user authentication schemes with smart cards are pointed out. These results demonstrate that no more password-based authentication schemes with smart cards should be constructed with such ad-hoc methods, i.e., the formal design methodology with provable security approach should be employed in future design. We did not propose an improved version to overcome the security weaknesses since we cannot guarantee its security against all known attacks and unknown potential attacks with only heuristic security analysis. Also, our results demonstrate that no more password-based remote user authentication schemes with smart cards should be constructed with such ad-hoc methods, i.e., the formal design methodology with provable security approach.

[8]In this paper, author proposed an enhanced multimodal personal authentication system for mobile device security. The proposed approach combines information obtained from face, teeth and voice modalities for increasing performance. For integrating these three modalities, author utilizes various fusion techniques such as the weighted-summation rule, K-NN, Fisher and Gaussian classifiers. Author then evaluated the authentication performance of the proposed system. The performance is evaluated on a database consisting of 1000 biometric traits. These traits were correspondent to the face, teeth and voice modalities of 50 persons. That is 20 biometric traits per individual, in which these biometric traits are collected through smart phone simultaneously.The traits, face, teeth and voice can be captured by mobile phone having camera and microphone. This is the big advantages of the proposed system. Thus, in practical applications, fake attempting to use the device can be dissatisfied. Especially, for integrating the face, teeth and voice modalities at a fusion stage author utilized several fusion techniques such as the weighted-summation rule, K-nearest neighbor (KNN), Fisher and Gaussian classifiers. After that, author evaluated the authentication performance of the proposed system.From the experimental results, we confirmed that the proposed multimodal personal authentication approach worked well. It will significantly improved authentication performance over the methods that uses a single modality and/or the fused methods of two

modalities.The proposed system is widely divided into two categories: first is image-based authentication using face and teeth modalities, and second is voice-based authentication. Image-based authentication is subdivided into face-based and teeth-based authentication. These modules are managed according to similar authentication procedures.That is, image-based authentication is includes following sequential steps: image acquisition, region detection, and the authentication phase based on the EHMM algorithm. These stages are equivalently applied to face and teeth authentication. However, the number of EHMM states is somewhat different for each procedure. In order to model the face, author composed the state structure of EHMM using five super-states with three, five, five, five and three embedded-states, respectively. Each super-state represents the vertical face features such as forehead, eyes, nose, teeth and chin in the face image. And each embedded state in the super-state represents the horizontal local features. Also, the teeth image is modeled using three super-states and embedded-states of three, five and three in each super-state like that previous system. To obtain the adequate face subject, author utilized a pre-processing procedure, i.e., rotated-angle compensation, of previous system.

B. Algorithm's to be used

1. Gray Scale Algorithm
2. AES Algorithm (Advanced Encryption Standard)
3. OTP Algorithm(One Time Password)

Gray Scale Algorithm

Input :- Color Image Output:-Gray Scale Image

1. Get the red, green, and blue values of a pixel.
2. Use fancy math to turn those numbers into a single gray value.
3. Replace the original red, green, and blue values with the new gray value.

AES Algorithm(Advanced Encryption Standard)

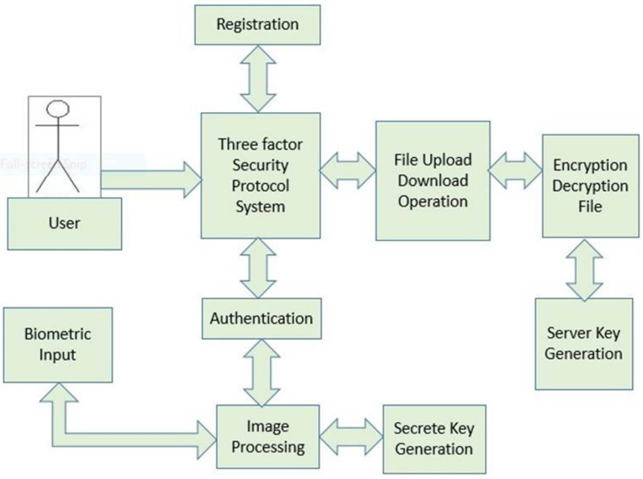
1. First derive the different round keys from cipher key.
2. Initialize the state array with block data or plaintext.
3. Start with initial state array by adding round key.
4. Perform the process of state manipulation in nine round

By above process we get the final encrypted text or cipher text.

OTP Algorithm(One Time Password)

1. During authorization, besides a users login and password, a user will be asked for a one-time password that he/she will have to enter in the form after generating it with one of our tokens.
2. The one-time password is sent through the API to Protectimus.
3. In real-time mode, the ??? and the user are verified, and your application instantly receives a positive or a negative response.
4. Your application responds to the authentication attempt based on the response received.

System Architecture



III. CONCLUSION

The three factor security protocol for consumer USB storage devices is suggested with some significant advantages but in the proposed work presented in the given pa- per shows existing issues of security liability which required being fix specially Daniel of service attack, guessing of password and replay attack. The proposed work explains the enhanced three factor security protocol to fix the weaknesses from previous papers. The projected security protocol have been predicted and severely analyzed in terms of security and computational cost with respect to another existing protocol.

.

IV. FUTURE SCOPE

In future we will try to check the DOS attack and also need to work more security issues related to password guessing attack and replay attack.

V. REFERENCES

[1]. Chia-Chun Wu, Wei-Bin Lee, Woei-JiunnTsaur, “A Secure Authentication Scheme with Anonymity for Wireless Communications”, IEEE COMMUNICATIONS LETTERS, VOL. 12, NO. 10, OCTOBER 2008

[2]. Kyung-Ah Shim, “Security Flaws in Three Password-Based Remote User Authentication Schemes with Smart Cards”, Cryptologia, 36:62–69, 2012 Copyright # Taylor & Francis Group, LLC ISSN: 0161-1194 print DOI: 10.1080/01611194.2011.606352

[3]. Jong-Hyouk Lee, Jean-Marie Bonnin, “HOTA: Handover optimized ticket-based authentication in network-based mobility management”, Information Sciences 230 (2013) 64–77

[4]. C-C Lee, C-T Chen, P-H Wu, T-Y Chen, “Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices”, IET Computer Digital Techniques 2013, Vol. 7 Iss 1, pp. 48–55 doi: 10.1049/iet-cdt.2012.0073

[5]. A.K. Das, “Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards”, IET Information Security 2011 Vol 5, Iss 3, pp. 145–151 145 doi: 10.1049/iet-ifs.2010.0125

[6]. Han-Cheng Hsiang a,b,*, Wei-Kuan Shih,” Weaknesses and improvements of the Yoon–Ryu–Yoo remote user authentication scheme using smart cards”, 2008 Published by Elsevier B.V. doi:10.1016/j.comcom.2008.11.019

[7]. Dong-Ju Kim, Kwang-Woo Chung, and Kwang-SeokHong,“Person Authentication using Face, Teeth and Voice Modalities for Mobile Device Security”, Electronic version published 12/30/10.