ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A Review on Authentications based on Smartcards

Akhila Sreenivas K, Pretty Babu

P.G Scholar, Department of Computer Science, Sree Buddha College of Engineering, Alappuzha, India

Assistant Professor, Department of Computer Science, Sree Buddha College of Engineering, Alappuzha, India

ABSTRACT: Authentication is necessary for any secure transaction. Smart card based authentication mechanism are most popular because of the strong security and simplicity. This paper describes about various smartcard based authentication mechanisms.

KEYWORDS: Authentication, Password, Registration center, Smartcard, Service provider

I. INTRODUCTION

Authentications based on smart card provide an improvement on basic password operations. It is similar to taking cash from an ATM, where we have a bank card and a PIN number. A user's private key certificate information is stored on the smart card that helps to uniquely identify the user. The card will be automatically blocked after a number of unsuccessful PIN entries. A number of cryptographic operations on the card protects from malicious attacks. Those cryptographic operations are carried out by the processor. In many insecure transmission environments, such as internet and wireless channel, when a user wants to access the valuable resource from the server, typically, a user's identity and password are needed for the server to authenticate the validity of the user. Smartcard based authentication is one of the best known and simplest mechanisms for dealing with the transmission of secret data over insecure networks.

A smart card is a plastic card that contains user's data with a microchip. Cards must interface to a computer or terminal through a standard card reader. There are two types of smart cards. Contact smartcards and Contactless smart cards. Contact smart cards can be inserted into a smart card reader. They contain a small gold plate on the front. Electrical connectors in the smart card reader help to transfer data to and from the chip. Transactions in contact less smart cards are carried with the help of an antenna. They are also similar to plastic credit cards. It contains an electronic microchip and antenna for communication. These components allow the card to communicate with an antenna without a physical contact. Contactless cards provide transactions quickly.

Smart card based authentication scheme mainly consists of the following phases. They are the registration phase, login phase, verification phase and password change phase. The registration phase is activated when new user wants to register within the server. For the purpose of registration the user submits his or her details to the server. When the registration request from the user reached on the server side it calculates essential parameters by using the submitted information and finally issue smart card to the user by storing important parameters into the memory of smart card. The login phase and verification phase are used when a user wants to access resources from the server. In the login phase, user creates a login request and sends it to server for verification. Once the login request is received, server checks the validity of login request and the legitimacy of user. In password change phase user can change the password according to their needs.

II. LITERATURE REVIEW

Manik Lal, Saxena and Gulati proposed a remote user authentication mechanism [1] for smart cards. This technique allows the users to change and choose the passwords according to their needs without a verifier table. One way hash function provides better security to this approach. This method can resist all the attacks except the impersonate attack. Wang et' al proposed [2] an efficient and secure dynamic ID-based remote user mutual authentication mechanism with improved security. This scheme provides security for the changing of passwords independently by the users.

Li Yang, Jian-Feng Ma, and Qi Jiang proposed smart cards and passwords mutual authentication under trusted computing [3] consists of client and server side .This scheme contains a TPM chip and its function is to manage the server through wired network. Smart card user firstly registers with the server that containing TPM chip. TPM chip is an independent coprocessor performs encryption function, security function, storage function and also provides software and hardware support. Chang–Cheng's authentication mechanism uses one way hash function and exclusive OR operation for improving the performance of the system during multi server authentication process. Here the user performs the registration with registration center by giving the values of id, password and personal information as plain text so the insider of registration center can get id and password of the users. A password and smart card based user authentication mechanism for multi server environments involve hash function encryption process. In registration phase user computes hash value of id and password and also the user chooses a random number that improves the security. Service provider gives permission to users for accessing the resources.

Kwong chan [4] proposed a cryptanalysis for smart card authentication in multiserver environment. Tsai et'al proposed a scheme for smart cards with mutual authentication. In this scheme server's secret key is stored in the protected memory of server and its corresponding public key $Y=g^{x \bmod p}$ is stored in each user's smartcard. Here verification of the user's is done after the login request so it takes more time for password detection. Jiang et'al proposed [5] a user authentication with key agreement scheme can provide privacy to users. This remote authentication mechanism uses a public key based mechanism with low computational and communication cost.

Chien, Jan and Tseng, developed [6] an efficient and practical solution to remote authentication on smart card. It can provide mutual authentication between user and server without a verification table. Another advantage of this approach is that users can freely change password. Communication and computational cost is also very low. Chen, Kuo, and Wuu used [7] a strong and efficient smart card based remote user password authentication scheme. They proposed an improved and efficient password authentication mechanism. This approach can handle the secret information with a key agreement phase by mutual authentication. It can provide security to stolen smart card attack.

Hwang and Li proposed [8] another remote user authentication scheme using password based on El Gamal's public key encryption process. This scheme can check the legitimacy of user without any verification table. Another advantage is that it can overcome message replay attack. Yoon, & Yoo develop [9] a robust biometrics based multi server authentication mechanism on smart card based on elliptic curve cryptosystem. This scheme minimizes the complexity of hash operations. Biometric technique allows strong user authentication operation. It provides better security, reliability and efficiency and suitable to use in distributed multi server network environment.

Sood, Sarje, Kuldip proposed [10] secure and efficient dynamic identity based authentication protocol for multi server environment. It contains two servers one is the service provider server and other is the control server. Service provider server is open for clients for getting the services during their registration, login and password change phase. This scheme uses one way hash functions and EXOR operations. This scheme can change the user's password securely without the help from server. Xiong Li et 'al proposed [11] an enhanced smart card based remote user password authentication approach that can ensure forward secrecy and also it can detect the wrong password given by the user during their login phase. This scheme is user friendly and the user can change or update the password without making any communication to server system.

III. Conclusion

Authentications based on smart card provide an improvement on basic password operations. Smart card based authentication mechanism are most popular because of the strong security and simplicity. The survey shows various smart card based authentication mechanism. In this survey have looked on various papers of authentication mechanism based on smart cards and each of the paper has its own advantages and limitations. Therefore it is necessary to design a secure and efficient smart card based authentication mechanism.

References

1. Das, M. L.,Saxana, A., & Gulati, V. P. (2004). A dynamic]ID-based remote user authentication scheme, IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 629-631..
2. Wang, Y.Y., Liu J.Y., Xiao,F.X., & Dan J., (2009). A more efficient and secure dynamic ID-based remote user authentication scheme, Computer Communications, vol. 32, no. 4, pp. 583-585.

3. Li Yang, Jian-Feng Ma, and Qi Jiang, Mutual Authentication Scheme with SmartCards and Password under Trusted Computing, International Journal of Network Security, Vol.14, No.3, PP. 156-163.
4. C. K. Chan, and L. M. Chang, Cryptanalysis of a remote user authentication scheme using smart cards, IEEE Trans. on Consumer Electron., vol. 46, no. 4, pp. 992-993, Nov. 2000
5. Jiang, P., Wen, Q., Li,W., Jin Z., and Zhang, H. (2013). Ananonymous user authentication with key agreement scheme without pairings for multiserver architecture using SCPKs. The Scientific World Journal, vol. 2013, Article ID 419592, 8 pages
6. H. Chien, J. Jan, and Y. Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card," Computers and Security,Vol. 21, No. 4, pp. 372-375, 2002
7. Chen BL, Kuo WC, Wuu LC (2012). Robust smart-card-based remote user password authentication scheme, International Journal of Communication Systems
8. M. Hwang and L. Li, A New Remote User Authentication Scheme Using Smart Cards, IEEE Transactions on Consumer Electronics,Vol. 46, No. 1, pp. 28-30, February, 2000
9. Yoon, E.-J., & Yoo, K.-Y. (2010). Robust biometrics-based multi-server authentication with key agreement scheme for smart cards onelliptic curve cryptosystem. Journal of Supercomputing, 1–21.
10. Sandeep K. Sood, Anil K. Sarje, Kuldip Singh (2011)."A secure dynamic identity based authentication protocol for multi-server architecture," Journal of Network and Computer Applications , pp. 609-618.
11. Xiong Li, Jianwei Niu, Muhammad Khurram Khan, Junguo Liao (2013). An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications, pp. 1365-1371