International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Analysis of Password based Multi-server Authentication Schemes

Swati Nema[1], Anamika Soni[2]

[1]Department of CSE, Patel College of Science & Technology, Bhopal, India

[2]Department of CSE, Patel College of Science & Technology, Bhopal, India

Abstract: ***As of today, numerous researchers have explored the issue of secure and efficient smart card based authentication scheme for these variety of application areas. This article explores the background research on the single server smart card authentication schemes as well as multi-server smart card authentication schemes and its associated research gaps. This article gives comparative analysis of major smart card authentication schemes for single server as well as multi-server environment in terms of security features provided and the computational complexity. This effort assists the researchers to work in different directions towards design and development of secure and efficient smart card authentication scheme.***

Keywords: Authentication, Denial-of-Service attack, insider attack, perfect forward secrecy, smart card, user anonymity.

1. Introduction

In order to authenticate the legitimate users, password based security mechanisms have been widely used in many remote login systems. In conventional password authentication schemes, every user has an identity (ID) that is public and a password (PW) that is private. At the time of login, if the submitted password matches the one stored in the verification table then server authenticates the corresponding user. The result may be that one can easily get the exact the password if somehow access the verification table stored in the server.

One of the famous solutions to counter this drawback is to encode all the passwords by making use of one way hash function and then store the digest in the verification table stored in the server [26]. Another alternate is to store the password in encrypted form which cannot be easily derived from an attacker even if an attacker knows the content of the verification table. However, it consumes more memory space to store the encrypted password. In both the approaches, size of the verification table increases as the number of users increases. Moreover, the main problem related to single factor (password) authentication is the ease of breaking the system which result the entire system to fail.

As a single layer of password protection merely is not enough, it has given rise to the concept of two factor authentication as an option to boost protection. It is provided by the utilization of password and user's registered phone or email to receive the dynamic one-time password (OTP). Though, sending this OTP through SMS text message is not safe as it is also sent in plain text form. Further, we have to rely on the mobile network also. In order to counter these problems and limitations, password based smart card authentication scheme has been proposed as a replacement for OTP.

Smart card is a tamper resistant integrated circuit card with memory and processor capable of performing computations [7]. Data are stored in the chip's memory and can be accessed to execute and complete various processing applications. Authentication scheme which treats smart card as a base is free from maintaining a verification table in order to validate the legal user. Further, it increases the security by providing two factor authentication as a replacement for simple password based authentication.

Following are the three stages of smart card authentication scheme.

- **Registration phase**. Once the registration request has been received from the user, server calculates the necessary parameters, keeps these parameters into smart card memory and distributes the smart card to the user.
- **Login phase**. The login phase and authentication phase are invoked at the time when user is going to login into the server. In the login phase, the smart card creates the login request using the inputted credentials of user and the necessary parameters stored in the smart card memory.
- **Authentication phase**. After receiving the login request, server checks the validity of the login request by using its own secret key in order to authenticate the requested user.

The rest of the paper is organized as follows. Section 2 explores major contributions in the field of single server as well as multi-server smart card authentication. A comparison of these smart card authentication schemes is investigated in section 3. Finally, section 4 concludes the paper.

2. Noteworthy Contribution

There is a substantial body of work devoted to the topic of remote user authentication dating as back as the late 1980's and continuing through today to protect the information from unauthorized user [14, 11]. Encouraged by Lamport's scheme [26], Haller proposed the prominent S/KEY one time password for an Internet draft RFC 1760 [12, 24]. Though, few researchers have proved that the security of the S/KEY scheme can be breached by server spoofing attacks, replay attacks and password guessing attacks [20, 16, 2]. Then after, SAS and OSPA protocols are suggested by Sandirigama et al. [4] and Lin et al. [1] respectively.

However, Chen and Ku found that the SAS and OSPA protocols can be breached by two stolen verifier attacks [19]. In order to protect identified security attacks on the verification tables, smart card password authentication scheme has been suggested.

In a single server environment, only a single server is responsible for providing services to all the authorized remote users. In this perspective, Hwang and Li [10] presented a remote user smart card authentication scheme which stands on ElGamal's cryptosystem. The authors declared that their scheme vanish the role of verification table and it defies replay attack. Nevertheless, it has been demonstrated that Hwang-Li's scheme is prone to impersonation attack [13].

In order to preserve the user anonymity, Das et al. [15] suggested a new concept of dynamic ID. The authors claimed that their scheme provides the facility for the users to select and alter their passwords liberally. Moreover, it defies ID theft, replay attack, forgery attack, insider attack, stolen verifier attack and guessing attack. Unfortunately, Liao et al. [5] proved that Das et al.'s scheme does not resist guessing attacks and fails to achieve mutual authentication. Further, password can be exposed. In order to handle these issues, they proposed an enhanced scheme to raise the security of Das et al.'s scheme. Additionally, the proposed scheme is also effficient and not only achieve their advantages but also enhances their security by withstanding the weaknesses.

Later on, Xie et al. [6] found that Liao et al.'s scheme is not safe against the identified attacks. To conquer their security pitfalls, they enhanced Liao et al.'s scheme by means of one way hash function. The authors declared that their enhanced and improved scheme defies the impersonate attack. Moreover, it can also provide security against the stolen attack. Song [17] proposed a new smart card authentication scheme. Song stated that the proposed scheme can defy the existing potential attacks. Moreover, it achieves mutual authentication and shared session key. Unfortunately, it is shown that Song's scheme is vulnerable to DoS attack. In addition, server interaction is required during password change phase that is also prone to DoS attack.

However, if a user wishes to access several network services, he or she has to register with different servers and maintain different corresponding user IDs and PWs. To conquer this complexity, numerous schemes have been proposed. These authentication schemes eliminate the necessity of separately registering with each server. In this context, Li et al. [3] proposed multi-server authentication scheme. The authors claimed that their scheme provides the facility for the users to select the passwords liberally. This scheme allows users to get service from multiple servers without separately registering with each server. In this scheme, the users only keep in mind user identity and password numbers to log in to different servers. Users can liberally choose their password. Also, the system is not essential to keep a verification table and can resist the replay attack.
However, Lin et al. [18] found that Li et al.'s scheme takes long time on training neural networks. It has a merit that the system can administer user's privileges by using the service period. As soon as the service period of a user expires, the service for that user will be halted by the central authority. Even though, it has been proved that Lin et al.'s scheme is unsafe against masquerade attack.

Juang [9] presented nonce based smart card authentication scheme and claimed that the scheme has merits include: (1) users has to register with the registration centre only once and there is no need to register with the servers. (2) the scheme eliminates use of verification table; (3) users can freely choose its own passwords; (4) efficient as the communication and computation cost is very low; (5) session key establishment and mutual authentication is achieved; (6) it uses nonce to avoid serious time-synchronization problem.

Unfortunately, it is weak in opposition to insider attack and does not provide forward secrecy [25]. Moreover, Liao and Wang [8] found that Juang's scheme [9] fails to update user's password without the help of registration center. Further, it does not provide any mechanism to verify the identity and password at the time of login phase. Also, it fails to resist online guessing attack. To overcome these problems, they proposed their scheme based on cryptographic one way hash function to improve efficiency.

Hsiang and Shih [27] located that Liao-Wang's scheme [8] is susceptible to masquerade attack, registration center spoofing attack, privileged insider attack and server spoofing attack. Their enhanced and improved scheme inherits all the merits and advantages of Liao-Wang's scheme. Sood et al. [21] illustrates that Hsiang-Shih's scheme [27] is uncovered with stolen smart card attack, replay attack and impersonation attack. To get rid of these security flaws, the authors suggested an enhanced smart card authentication scheme for multi-server scenario.

Wang and Ma [22] presented smart card based secured and efficient multi- server authentication scheme by making use of Elliptic Curve Discrete Logarithm Problem (ECDLP). But, it is inadequate to offer safety against impersonation attack, server spoofing attack, offline password guessing attack and privileged insider attack. Chen et al. [23] proposed their scheme by means of one way hash function. Their proposed scheme not only assembles all the security requirements but also provides security against all the well-known attacks. To address the problem of verification table at the server, this scheme makes use of RC during authentication phase to achieve successful mutual authentication between user and the server. Server always requests to RC to generate session key shared by users. However, involvement of RC during verification makes it inefficient practically.

3. Comparison of Major Smart Card based Authentication Schemes

This section provides a comparison result for multi sever smart card based authentication schemes. Table I shows comparative results in terms of security attacks and Table II explores comparative analysis for various smart card authentication schemes under multi-server environment in

terms of computational complexity. Meaning of notations used in the tables is defined as follows:

- F1 indicates that the scheme is free from maintaining verification table,
- F2 means that user is permitted to decide the password,
- F3 means that user is allowable to modify the password,
- F4 indicates that the proposed scheme is liberated from participation of RC or server throughout password change phase,
- F5 means that the scheme affords mutual authentication,
- F6 means that the scheme affords early wrong password detection,
- F7 means that the scheme affords mutual authentication without support of RC,
- F8 means that the scheme offers session key agreement,
- F9 means that the scheme defies user impersonation attack,
- F10 means that the scheme defies server spoofing attack,
- F11 means that the scheme defies replay attack,
- F12 means that the scheme defies password guessing attack,
- F13 means that the scheme defies reflection attack,
- F14 means that the scheme defies parallel session attack and
- F15 means that the scheme defies known session key attack.
- H means One Way Hash Function
- En means Symmetric Encryption
- De means Symmetric Decryption
- ECCPM means Elliptic Curve Cryptography Point Multiplication
- EX means Exponentiation

This study has surveyed most of contact smart card based authentication schemes found in the literature. Despite the existence of a broad body of work focused on smart card based authentication schemes, there is still considerable room for improvement as none of the schemes can satisfy all the security requirements and withstand all the identified attacks.

Table 1: Comparison of Multi-server Smart Card based Authentication Schemes in terms of Security Features and Attacks

Security Features	*Juang [9]*	*Liao-Wang [8]*	*Hsiang-Shih [27]*	*Sood et al. [21]*	*Wang-Ma [22]*	*Chen et al. [23]*
F1	No	Yes	Yes	No	No	Yes
F2	Yes	Yes	Yes	Yes	Yes	Yes
F3	No	Yes	Yes	Yes	Yes	Yes
F4	Yes	Yes	Yes	Yes	No	Yes
F5	Yes	Yes	Yes	Yes	Yes	Yes
F6	No	Yes	Yes	Yes	No	No
F7	Yes	Yes	No	No	Yes	No
F8	Yes	Yes	Yes	Yes	Yes	Yes
F9	Yes	No	No	Yes	No	Yes
F10	Yes	No	No	Yes	No	Yes
F11	Yes	Yes	No	Yes	Yes	Yes
F12	Yes	Yes	No	Yes	Yes	Yes
F13	Yes	Yes	Yes	Yes	Yes	Yes
F14	Yes	Yes	Yes	Yes	Yes	Yes
F15	Yes	Yes	Yes	Yes	Yes	Yes

Table 2: Comparison of Multi-server Smart Card based Authentication Schemes in terms of Computational Complexity

Schemes	*Registration Phase*	*Login and Authentication Phase*	*Total*
Juang [9]	3H + 1En	5H + 3En + 4De	8H + 4En + 4De
Liao-Wang [8]	5H	16H	21H
Hsiang-Shih [27]	7H	23H	30H
Sood et al. [21]	5H	25H	30H
Wang-Ma [22]	2H + 2ECCPM	11H + 4 ECCPM	13H + 6ECCPM
Chen et al. [23]	3H	11H + 4EX	14H + 3EX

References

[1] L. Lamport, “Password authentication with insecure communication,” Communications of theB. Wang and M. Ma, “A smart card based efficient and secured multi-server authentication scheme," Wireless Personal Communications, vol. 68, 2013, pp. 361-378.

[2] C. J. Mitchell and L. Chen, “Comments on the S/KEY user authentication scheme,” ACM Operating Systems Review, vol. 30, pp. 12–16, Oct. 1996.

[3] C. K. Chan and L. M. Cheng, “Cryptanalysis of a remote user authentication scheme using smart cards,” IEEE Transactions on Consumer Electronics, vol. 46, no. 4, 2000, pp. 992-993.

[4] C. L. Lin, H. M. Sun, and T. Hwang, "Attacks and solutions on strong-password authentication," IEICE Transactions on Communications, vol. E84-B, pp. 2622–2627, September 2001.
[5] C. M. Chen and W. C. Ku, "Stolen-verifier attack on two new strong-password authentication protocols," IEICE Transactions on Communications, vol. E85-B, pp. 2519–2521, November 2002.
[6] Cheng Hsiang and Wei-Kuan Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment", Computer Standards & Interfaces, vol. 31, no. 6, 2009, pp. 1118-1123.
[7] I.C. Lin, M.S. Hwang and L.H. Li, "A new remote user authentication scheme for multi-server architecture", Future Generation Computer Systems, vol. 19, no. 1, 2003, pp. 13-22.
[8] I-En Liao, Cheng-Chi Lee and Min-Shiang Hwang, "Security enhancement for a dynamic ID-based remote user authentication scheme", International Conference on Next Generation Web Services Practices, 2005.
[9] J. M. Timothy and G. B. Scott, "Smart cards: The developer's toolkit," Prentice Hall, 2002.
[10] K. S. Booth, "Authentication of signatures using public key encryption," Communications of the ACM, vol. 24, no. 11, 1981, pp. 772-774.
[11] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, 1981, pp. 770-772.
[12] L. Li, I. Lin and M. Hwang, "A Remote Password Authentication Scheme for Multi-server Architecture Using Neural Networks," IEEE Transactions on Neural Networks, vol. 12, no. 6, 2001, pp. 1498-1504.
[13] M. Sandirigama, A. Shimizu, and M. T. Noda, "Simple and secure password authentication protocol (SAS)," IEICE Transactions on Communications, vol. E83-B, pp. 1363–1365, June 2000.
[14] M.S. Hwang and L.H. Li, "A new remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 46, no. 1, 2000, pp. 28-30.
[15] Manik Lal Das, Ashutosh Saxena, and Ved P. Gulati, "A dynamic ID-based remote user authentication scheme", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, 2004, pp. 629-631.
[16] N. Haller, "The S/KEY one-time password system," in Proceedings of Internet Society Symposium on Network and Distributed System Security, 1994, pp. 151–158.
[17] N. Haller, "The S/KEY one-time password system," RFC1760, Feb. 1995.
[18] Qi Xie, Ji-Lin Wang, De-Ren Chen and Xiu-Yuan Yu, "A novel user authentication scheme using smart cards", International Conference on Computer Science and Software Engineering, 2008, pp. 834-836.
[19] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," Communications of the ACM, vol. 21, no. 12, 1978, pp. 993-999.
[20] R. Song, "Advanced smart card based password authentication protocol," Computer Standards & Interfaces, vol. 32, no. 5-6, 2010, pp. 321-325.
[21] S. M. Yen and K. H. Liao, "Shared authentication token secure against replay and weak key attacks," Information Processing Letters, vol. 62, pp. 77–80, 1997.
[22] Sandeep K. Sood, Anil K. Sarje and Kuldip Singh, "A secure dynamic identity based authentication protocol for multi-server architecture", Journal of Network and Computer Applications, vol. 34, no. 2, 2011, pp. 609-618.
[23] T. C. Yeh, H. Y. Shen, and J. J. Hwang, "A secure one-time password authentication scheme using smart cards," IEICE Trans. on Communications, vol. E85-B, pp. 2515–2518, Nov. 2002.
[24] T. Y. Chen, C. C. Lee, M. S. Hwang, J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," Journal of Supercomputing, Vol. 66, 2013, pp. 1008-1032.
[25] W.S. Juang, "Efficient multi-server password authenticated key agreement using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, no. 1, 2004, pp. 251-255.
[26] Wei-Chi Ku, Hsiu-Mei Chuang, Min-Hung Chiang and Kuo-Tsai Chang, "Weaknesses of a multi-server password authenticated key agreement scheme", 2005 National computer Symposium, pp. 1-5.
[27] Y.P. Liao and S.S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment", Computer Standards & Interfaces, vol. 31, no. 1, 2009, pp. 24-29.