International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 6 Issue 12|| December 2017 || PP.09-12

Remote User Authentication Schemes: A Review

Narendra Singh Panwar[*], Dr. Manmohan Singh Rauthan[#], Dr. Amit Agarwal[$]
[*]*Department of Computer Science & Engineering,*
Uttarakhand Technical University, [#]*Department of Computer Science & Engineering,*
HNB Garhwal University,
[$]*Department of Computer Science & Engineering, University of Petroleum &Energy Studies, Dehradun,*

Abstract: *To secure the resources or information from illegitimate users various kinds of authentication schemes have been designed and developed. Some of these schemes are vulnerable to a variety of attacks. In last decade authentication schemes based on smart card has been proposed to withstand the possible attacks on verification table. Smart card provides a convenient storage and processing capability to the users. It is widely used for a range of applications such as remote user authentication, ID verification and access control.The present study gives recent developments in the area of smart card based authentication schemes and their comparative analysis. It also presents security requirements to the design and development of best authentication scheme. We have taken various authentication schemes as sample for efficiency comparisons and provide comparison results based on various operation used in respective schemes. This paper identified various security requirements which are must require in strong and efficient authentication schemes: Authentication schemes built on presented security requirements can be applied for online health care system, telecare system, Medicare system etc. for patient health care data privacy.*

Keywords: *remote user, authentication, security, smartcard.*

Date of Submission: 15-11-2017 Date of acceptance: 28-11-2017

I. Introduction

Remote user authentication (RUA) is a technique to securely authenticate remote users over insecure network. Authentication schemes are used before the user make use of the remote services through computer networks. A remote server is used to verify legitimacy of the users prior to access the resources from remote server. The RUA schemes are one of the critical security primitives due to the Internet's openness and lack of security concern in the Internet activities. In a networked system, when a user legitimate user requests a remote server's service, he/she must pass a user authentication process. Through this user authentication process, the server can determine either the user can make use of the provided services or not. When a user uses a service in a remote server, then the communication between the user and the server must be kept secret. They must use a session key for protecting their communications. Smart Cards are extraordinarily useful as crypto devices. A primary reason for this is that they have the quite unique ability of being capable of generating and protecting a private signing key which can never leave the card. In this paper we have carried out a comprehensive survey on some of the distinguished smart card based remote user authentication schemes.

A remote user authentication scheme with a password table was proposed and claimed that the proposed scheme is secure even though an malicious attacker has intercepted the message between a user and a remote system[1][2]. In a network environment, a remote server provide services to all the legitimate remote users. During the last decade several user authentication schemes developed with smart cards have been proposed[3-10][38-39]. Further it has been claimed that to avoid the risk of exposing the information in the secret password file of a system to illegitimate users, one should store the scrambled values f(PW) in the file for every password PW, where f is a "one-way" function, i.e. a function that is easy to evaluate but very hard to invert[11]. It has the advantage that the password files need.

A remote user authentication scheme based on ElGamal's cryptosystem was proposed[12]. It was claimed that the scheme does not maintain any verification table and it is secure against replay attack. However, it is vulnerable to impersonation attack[13]. Further improvement were given by[14]which was also cryptanalyzed[15]. An enhanced authentication scheme was proposed to withstand impersonation attack in which login request variables are computed from S_{ID} instead of ID[16]. Additional improvement was proposed in which S_{ID} is computed instead of ID, its login request contents are ($S_{ID} \| C_{ID}$, C_1, C_2, T_1), where $C_{ID} = C_K(S_{ID})$. An ID based scheme using RSA cryptosystem has been proposed[17]. However, it exhibit impersonation attack[13]. Further improvement has been proposed[14] which has all the merits of the previous scheme with an added trait of mutual authentication. It has been found that the scheme does not resist impersonation attack[18]. In 2004, Das et *al.*[19]proposed a dynamic ID-based remote user authentication scheme to prevent the risk of

ID-theft and to resist against the impersonation attack. Das et *al.* scheme was crypt-analyzed and it is demonstrated that an attacker can login onto the remote server with his chosen random password[16].

A user friendly authentication scheme using one way hash function was propose[20]. It was proved that the scheme is weak against impersonation attack and then further improvement was also proposed[21]. It was pointed out that the scheme is vulnerable to guessing attack, forgery attack; to overcome these weaknesses, an improved scheme was also proposed[22]. However, due to the symmetric structure of communicating messages, this scheme does not resist reflection attack and parallel session attack. In 2009, Id-based authentication with key agreement schemes for mobile devices communication on elliptic curve cryptosystem based on pairing free, certificate less were discussed to overcome various attacks.

In 2010, Lee et *al*.[23] have analyzed the security of the smart card based user authentication scheme proposed by Lee et *al*.[21]. Their security analysis showed that Lee et *al*.[21] scheme does not achieve its main security goal of the two-factor security. To demonstrate this, they have shown that the scheme is vulnerable to an off-line dictionary attack in which an attacker, who has obtained the secret values stored in the user's smart card, can easily find out its password. Besides reporting the security problem, they showed what really is causing the problem and how to fix it and proposed the scheme which improves on Lee et al.[21]scheme. In 2011, Khan et *al*.[24] showed that Wang et *al*.[25] cannot provide user anonymity because of the transmission of ID and proposed an improved dynamic ID-based remote user authentication scheme, which can provide user anonymity, mutual authentication, and session key establishment, and resist against several attacks, such as stolen-verifier, insider, DOS, replay, and parallel session attacks. Further Jenq et *al*.[26] show that Lee et *al*.[23] scheme is still vulnerable to password guessing attack, server spoofing attack and masquerade attack. Author compare the scheme with Lee et *al*.[23] to prove that the computation cost, security and efficiency of the proposed scheme are well suitable for practical applications in a distributed system.

In 2015, efficient and secure authenticated key agreement protocol based on elliptic curve cryptosystem for user anonymity, for UMTS network, grid network has been discussed. Novel mutual authentication scheme for session initiation protocol based on elliptic curve cryptography implemented for controlling communication on the internet was proposed by [27]and [28].Recently S Hong[29] proposes the use of a Media Access Control (MAC) as a security tool in the beginning of authentication stage and claimed that it contributes to secure the group member authentication while the MAC spoofing problem is avoided and the secure user authentication can be assured as the MAC-based authentication is being used. User authentication scheme for IoT has been proposed by Rafida et *al.* [30]. It was claimed that low communication overhead is required by the proposed scheme because the size of the message for authentication between user and server is too short and fulfill the properties of Zero Knowledge proof, provides solutions against various threats in network. Table 1 shows the comparison of computational cost of various authentication schemes.

II. Conclusion

A handful of user authentication schemes using biometrics and smart card have been studied in this article. It has been analyzed that the authentication and security of the schemes have been enhanced with more and more research.For security purpose, the servers are also designed not to store the password and verification tables or the biometric records in it. In order to build a strong authentication system, both the user and the server should be involved in mutual authentication and should also be properly synchronized. An ideal biometric based smart card authentication scheme is also resistant to impersonation attack, replay attack, stolen smart card attacks, server spoofing attacks, insider attacks, password guessing attacks, man-in-the-middle attacks and denial of service attacks and should conform to the perfect forward secrecy.

Table 1: Comparison of computational cost of eminent smart card based user authentication schemes

Authentication Schemes	**Registration phase**		**Login phase**		**Authentication phase**	
	User end	Server end	User end	Server end	User end	Server end
[31]	-	1⊕	1H +3⊕	-	-	1H + 3⊕
[14]	-	1⊕	1H +3⊕	-	-	1H + 3⊕
[16]	-	1⊕	1H +3⊕	-	-	1H + 3⊕
[32]	-	1⊕	1H +3⊕	-	-	1H + 3⊕
[33]	-	1H	IH	-	-	2H
[34]	-	1H	2H	-	2H	4H
[35]	4H	3H	8H	-	2H	6H
[36]	IH	2H	4H	-	1H	3H
[14]	-	1H + 2⊕	1H + 2⊕	-	1H + 1⊕	3H + 3⊕
[20]	-	2H + 1⊕	2H + 1⊕	-	-	1H
[23]	-	2H + 1⊕	2H + 1⊕	-	-	2H
[22]	-	3H + 1⊕	4H + 1⊕	-	1H	3H
[19]	-	2H	4H	-	-	3H
[25]	1H	1H	4H	-	1H	4H
[37]	-	2H	2H	-	1H	3H

Notation used in Table 1: ⊕: Exclusive OR operation, H: Hash function, U: User's end, S: Remote Server's end.

References

[1]. Lamport L. Password authentication with insecure communication. Commun ACM. 1981;24(11):770-772. doi:10.1145/358790.358797.

[2]. Lennon RE, Matyas SM, Meyer CH. Cryptographic authentication of time-invariant quantities. Commun IEEE Trans. 1981;29(6):773-777.

[3]. N. Panwar, M. S. Rauthan and A. Agarwal, "A comparative analysis and improvement of smart card based authentication scheme," IEEE 2016 Ninth International Conference on Contemporary Computing (IC3), Noida, 2016, pp. 1-4., doi: 10.1109/IC3.2016.7880250

[4]. Yassin AA, Jin H, Ibrahim A, Zou D. by Using Smart Card. In: WISM 2012. Springer-Verlag; 2012:314-323.

[5]. Moon J, Choi Y, Jung J, Won D. An Improvement of Robust Biometrics-Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards. Shi Y, ed. PLoS One. 2015;10(12):e0145263. doi:10.1371/journal.pone.0145263.

[6]. Nimbhorkar S, Malik L. Comparative Analysis of Authenticated Key Agreement Protocols Based on Elliptic Curve Cryptography. ProcediaComput Sci. 2016;78(December 2015):824-830. doi:10.1016/j.procs.2016.02.065.

[7]. Li C-T, Weng C-Y, Lee C-C, Wang C-C. Secure User Authentication and User Anonymity Scheme based on Quadratic Residues for the Integrated EPRIS. ProcediaComput Sci. 2015;52:21-28. doi:10.1016/j.procs.2015.05.008.

[8]. Alizadeh M, Zamani M, Baharun S, et *al*. Cryptanalysis and Improvement of "A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks." Choo K-KR, ed. PLoS One. 2015;10(11):e0142716. doi:10.1371/journal.pone.0142716.

[9]. Ramesh S. A Secured and Improved Dynamic ID based Remote User Authentication Scheme using Smart Card and Hash Function for Distributed Systems. IJCSE. 2014;6(08):305-320.

[10]. Pippal RS, Jaidhar CD, Tapaswi S. Enhanced time-bound ticket-based mutual authentication scheme for cloud computing. In: Informatica (Slovenia). Vol 37. ; 2013:149-156.

[11]. G.M.J P, Leeuwen J van. Authentication : A Concise Survey. ComputSecur. 1986;5:243-250. doi:0167~4048/86.

[12]. Li C-T, Hwang M-S. An efficient biometrics-based remote user authentication scheme using smart cards. J NetwComput Appl. 2010;33(1):1-5. doi:10.1016/j.jnca.2009.08.001.

[13]. Chi-Kwong C, Cheng LM. Cryptanalysis of a remote user authentication scheme using smart cards. IEEE Trans Consum Electron. 2000;46(4):992-993.

[14]. Shen J-J, Lin C-W, Hwang M-S. A modified remote user authentication scheme using smart cards. IEEE Trans Consum Electron. 2003;49(2):414-416. doi:10.1109/TCE.2003.1209534.

[15]. Leung K-C, Cheng LM, Fong AS, Chan C-K. Cryptanalysis of a modified remote user authentication scheme using smart cards. IEEE Trans Consum Electron. 2003;49(4):1243-1245. doi:10.1109/TCE.2003.1261224.

[16]. Awasthi AK, Lal S. An enhanced remote user authentication scheme using smart cards. IEEE Trans Consum Electron. 2004;50(2):583-586. doi:10.1109/TCE.2004.1309430.

[17]. Yang WH, Shieh SP. Password authentication schemes with smart cards. ComputSecur. 1999;18(8):727-733. doi:10.1016/S0167-4048(99)80136-9.

[18]. Lu Y, Li L, Yang X, Yang Y. Robust Biometrics Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards. Du W-B, ed. PLoS One. 2015;10(5):e0126323. doi:10.1371/journal.pone.0126323.

[19]. Das ML, Gulati VP, Saxena A. A dynamic id-based remote user authentication scheme. IEEE Trans Consum Electron. 2004;50(2):629-631. doi:10.1109/TCE.2004.1309441.

[20]. Wu S-T, Chieu B-C. Shyi-Tsong Wu and Bin-Chang Chieu - A User Friendly Remote Authentication with Smart Cards: A User Friendly Remote Authentication Scheme with Smart Cards. ComputSecur. 2003;22(6):547-550. doi:10.1016/S0167-4048(03)00616-3.

[21]. Lee, Narn-Yih; Chiu Y-C. Improved remote authentication scheme with smart card. Comput Stand Interfaces. 2005;27(2):177-180.

[22]. Hölbl M, Welzer T, Brumen B. Improvement of the Peyravian--Jeffries's user authentication protocol and password change protocol. ComputCommun. 2008;31(10):1945-1951.

[23]. Lee Y, Yang H, Won D. Attacking and Improving on Lee and Chiu ' s Authentication Scheme Using Smart Cards. In: Kwak J, Deng RH, Won Y, Wang G, eds. Information Security, Practice and Experience. Berlin, Heidelberg: Springer Berlin Heidelberg; 2010:377-385. doi:10.1007/978-3-642-12827-1_27.

[24]. Ying M, Guowei L, Laomo Z. A Novel Remote Authentication Scheme Based-On Password for Anonymous Users. In: IBI 2011. Springer-Verlag; 2012:187-194.

[25]. Liao Y-P, Wang S-S. A secure dynamic ID based remote user authentication scheme for multi-server environment. Comput Stand Interfaces. 2009;31(1):24-29. doi:10.1016/j.csi.2007.10.007.

[26]. Leu J-S, Hsieh W-B. Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards. InfSecur IET. 2014;8(2):104-113.

[27]. Saxena N, Thomas J, Chaudhari NS. ES-AKA: An Efficient and Secure Authentication and Key Agreement Protocol for UMTS Networks. WirelPersCommun. 2015;84(3):1981-2012.

[28]. Juan Z, Fangmin D. The authentication and key agreement protocol based on ecc for wireless communications. In: Management and Service Science, 2009. MASS'09. International Conference on. ; 2009:1-4.

[29]. Hong S. Multi-factor User Authentication on Group Communication. Indian J Sci Technol. 2015;8(15). doi:10.17485/ijst/2015/v8i15/72941.

[30]. RafidhaRehiman KA, Veni S. A Secure Authentication Infrastructure for IoT Enabled Smart Mobile Devices – An Initial Prototype. Indian J Sci Technol. 2016;9(9). doi:10.17485/ijst/2016/v9i9/86791.

[31]. Tsai CS, Lee CC, Hwang MS. Password authentication schemes: Current status and key issues. In: International Journal of Network Security. Vol 3. IEEE; 2006:101-115. doi:10.1109/ICM2CS.2009.5397977.

[32]. Kumar M. Security Analysis of a Remote User Authentication Scheme with Smart Cards. 2005:- - .

[33]. Sun H-M. An efficient remote use authentication scheme using smart cards. IEEE Trans Consum Electron. 2000;46(4):958-961. doi:10.1109/30.920446.

[34]. Lee S-W, Kim H-S, Yoo K-Y. Improvement of Chien et al.'s remote user authentication scheme using smart cards. Comput Stand Interfaces. 2005;27(2):- - . doi:http://dx.doi.org/10.1016/j.csi.2004.02.002.

[35]. Sood SK, Sarje AK, Singh K. Secure Dynamic Identity-Based Remote User Authentication Scheme. In: ICDCIT 2010. Vol 5966 LNCS. ; 2010:224-235. doi:10.1007/978-3-642-11659-9_25.
[36]. Pu Q, Wang J, Zhao R. Strong authentication scheme for telecare medicine information systems. In: Journal of Medical Systems. Vol 36. ; 2012:2609-2619. doi:10.1007/s10916-011-9735-9.
[37]. Wang D, Ma C, Gu D, Cui Z. Cryptanalysis of Two Dynamic ID-Based Remote User Authentication Schemes for Multi-server Architecture. In: Xu L, Bertino E, Mu Y, eds. Network and System Security: 6th International Conference, NSS 2012, Wuyishan, Fujian, China. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012:462-475. doi:10.1007/978-3-642-34601-9_35.
[38]. N. Panwar, M. S. Rauthan and A. Agarwal, "Cryptanalysis of smart card and biometric-hash based authentication scheme," 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, 2016, pp. 831-834, doi: 10.1109/NGCT.2016.7877525
[39]. N. Panwar, M. S. Rauthan and A. Agarwal, "Privacy of Patient Information: Implementation and Security Analysis of a Secure Three Tier Patient Information System Based on QR Code," IEEE 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), Ghaziabad, 2016, pp. 232-234, doi: 10.1109/ICMETE.2016.130

International Journal of Engineering Science Invention(IJESI) is UGC approved Journal with Sl. No. 3822, Journal no. 43302.

Narendra Singh Panwar "Remote User Authentication Schemes: A Review." International Journal of Engineering Science Invention(IJESI), vol. 6, no. 12, 2017, pp. 09-12.