Cryptanalysis of a Markov Chain Based User Authentication Scheme

Ruhul Amin, G.P. Biswas
Indian School of Mines, Dhanbad
Department of Computer Science & Engineering
Email: amin_ruhul@live.com, gpbiswas@gmail.com

*

Abstract- Session key agreement protocol using smart card is extremely popular in client-server environment for secure communication. Remote user authentication protocol plays a crucial role in our daily life such as e-banking, bill-pay, online games, e-recharge, wireless sensor network, medical system, ubiquitous devices etc. Recently, Djellali et al. proposed a session key agreement protocol using smart card for ubiquitous devices. The main focus of this paper is to analyze security pitfalls of smart card and password based user authentication scheme. We have carefully reviewed Djellali et al.'s scheme and found that the same scheme suffers from several security weaknesses such as off-line password guessing attack, privileged insider attack. Moreover, we demonstrated that the Djellali et al.'s scheme does not provide proper security protection on the secret key of the server and presents inefficient password change phase.

Keywords: Security Attacks, Markov Chain, Authentication Protocol, Smart Card.

1 Introduction

Remote user authentication is the only mechanism employed by a server to confirm the legality of a user before he/she can access the resources or services provided by the server. Due to security concerns on the Internet which is insecure, the information transmitted between a legal user and a server should be protected from eavesdropping. In order to provide security protection of the transmitted information, a session key is generated after authenticating each other i.e. (user, server) of the system [2, 3]. Thereafter, the information are encrypted by the session key and transmitted over the internet as a cipher text.

Remote user authentication scheme was first proposed by the author Lamport [1] based on the hash function. later on, password with smart card based lots and lots of authentication protocols [2, 3, 4, 6, 7, 10, 11, 12, 15, 16, 19, 20, 26, 27, 28, 29] have been proposed. It has been observed that many schemes [8], [9], [17] suffer from smart card stolen attack resulting in off-line password guessing. In 2007, Wang et al. [18] illustrated that schemes [9, 21] cannot withstand forgery attack, off-line password guessing attack and denial of service attack, and presented solutions to fix the problems. In 2011, Awasthi et al. [22] pointed out that the Shen et al.'s [23] cannot withstand user impersonation attack, and also proposed an improve protocol.

[*] The most recent version of this document can be obtained from `http://www.iacr.org/docs/`

In 2012, Wang et al. [24] pointed out that the Yang et al.'s [25] and Hsieh-Leu's [8] schemes are insecure against smart card loss attack and proposed a robust scheme to thwart the problems of the smart card security breach. In 2013, Ruhul et al. [2] pointed out that the scheme [24] suffers from off-line identity-password guessing attack, user-server impersonation attack, and also proposed an improved protocol to fix the Wang et al.'s [24] problem.

2 Brief Review of Djellali et al. Scheme

This section reviews Djellali et al.'s scheme which consists of several phases such as setup phase, registration phase, login and authentication phase and password update phase. All the mentioned phases are presented in details as follows.

2.1 Setup Phase

In this phase, the server generates a transition probability matrix $P = M_{n \times n}$ corresponds to an irreducible and ergodic markov chain. The equation $\pi = \pi P$ can be computed in this phase for further use, where π is the stationary limit distribution. We will refer to reader regarding the concept of markov chain and it's uses in references [5].

2.2 Registration Phase

This phase executes for the new user who want to wish for accessing remote server. In order to complete this phase, the U_i and server perform the following operations which are as follows:

Step 1. The U_i primarily chooses desired identity ID_i and password PW_i and sends $\langle ID_i, hash(PW_i)\rangle$ to the server through secure channel after computing $hash(PW_i)$, where $hash()$ is the cryptographic one-way hash function.

Step 2. After receiving registration request, the server generates a random number y_i and computes $\pi = \pi P$, where π_{y_i} has been moved d digits number and erased the rest decimal places i.e. $\pi'_{y_i} = Shift_d(\pi_{y_i})$ and y_i lies between 1 to n. The server further computes $TID_i = hash(ID_i \parallel K_s)$ and $TPW_i = hash(PW_i) \oplus \pi'_{y_i}$, where K_s is the secret key of the server. Finally, the server issues a smart card containing $\langle TID_i, TPW_i, C_i, \pi'_{y_i}, hash()\rangle$ and sends it to the U_i securely.

Step 3. After obtaining the smart card, the U_i computes $C_i = hash(K_s) \oplus y_i$ and embeds $\langle C_i \rangle$ into the smart card memory and completes the registration process.

2.3 Login and Authentication Phase

In order to get server's services, the registered user has to login into the system by providing user's confidential information. The main focus of this phase is to achieve mutual authentication and session key agreement between the user and server. The login and authentication mechanisms work as follows.

Step 1. The U_i first connects his/her smart card to the card reader and then provides password PW_i^*. Then, the smart card reader computes $TPW_i^* = hash(PW_i^*) \oplus \pi'_{y_i}$ and checks the condition $TPW_i^* =?TPW_i$. If the condition does not hold, the login request is rejected; otherwise, generates two random nonces $\langle x, a\rangle$ and computes $X_i = TPW_i^* \oplus x$, $A_i = TID_i \oplus a$ and $L_i = A_i \oplus \pi'_{y_i}$. The server then encrypts $E_{A_i}(TID_i, TPW_i, \pi'_{y_i}, X_i)$ using the key A_i and sends login request message $M_1 = \langle L_i, E_{A_i}(TID_i, TPW_i, \pi^{'}_{y_i}, X_i), C_i\rangle$ to the server through open channel.

Step 2. After obtaining the login message, the server computes $y_i = C_i \oplus h(K_s)$, $\pi = \pi P$, $\pi^{''} = Shift_d(\pi_{y_i})$, $A_i = L_i \oplus \pi^{''}_{y_i}$ and decrypts $E_{A_i}(TID_i, TPW_i, \pi^{'}_{y_i}, X_i)$ using the computed A_i. Therefore, the server gets $\langle TID_i, TPW_i, \pi^{'}_{y_i}, X_i\rangle$ after completing decryption procedure. The server then verifies whether the condition $\pi^{'} = \pi^{''}$ matches or not. If the condition does not hold, immediately rejects the login request; otherwise, computes $x = TPW_i \oplus X_i$, $Z = z \oplus \pi^{'}_{y_i}$, where z is the random nonce. The server then constructs authenticated session key $AK_s = x.z$ of the protocol and encrypts $E_{A_i}(Z)$ using the parameter A_i. Finally, the server sends $M_2 = \langle E_{A_i}(Z)\rangle$ to the U_i through open channel.

Step 2. After receiving the message, the U_i decrypts $E_{A_i}(Z)$ using A_i and computes $z = Z \oplus \pi_{y_i}$, $AK_s = x.z$, where AK_s is the authenticated session key.

2.4 Password Change Phase

During updating the old password in Djellali et al.'s scheme, the user provides old and new password PW_i and PW_i^* respectively. Then, the smart card reader computes $TPW_i^* = TPW_i \oplus h(PW_i) \oplus h(PW_i^*)$ and replaces TPW_i with the computed TPW_i^* in the smart card memory.

3 Security Attacks and Weaknesses in scheme [5]

We have assume that the threat model mentioned in reference [19] are widely accepted and realistic. In this section, we have demonstrated that the Djellali et al.'s scheme is not secure against several security attacks. In addition, we have presented design flaws in the password change phase. The security pitfalls of the scheme [5] are discussed below.

3.1 Off-line Password Guessing Attack

If we assume that the Djellali et al.'s scheme has implemented for ubiquitous devices, then the same protocol is not suitable owing to off-line password guessing attack. According to the protocol description of the scheme [5], the attacker can easily guess the legal user's password in off-line mode.

Step 1. It is our valid assumption that the attacker has got legal user's smart card and extracted all the confidential information by monitoring power consumption [13, 14]. Therefore, the attacker knows $\langle TID_i, TPW_i, C_i, \pi^{'}_{y_i}, hash()\rangle$, where $TPW_i = hash(PW_i) \oplus \pi^{'}_{y_i}$.

Step 2. Now, the attacker chooses a password PW_i^d from the dictionary $|D|$ and computes $TPW_i^d = hash(PW_i^d \parallel \pi^{'}_{y_i})$, where $\pi^{'}_{y_i}$ is known to the attacker. The attacker checks the condition $TPW_i^d =?TPW_i$. If the condition holds, the attacker successfully gets legal user's password; otherwise, continue step2 until the correct password is obtained. Thus, the attacker can guess legal user's password from the smart card information.

3.2 Insecurity on Server's Secret Key

In Djellali et al.'s scheme, one smart card parameter is computed as $C_i = hash(K_s) \oplus y_i$, where K_s is the secret key of the server and y_i is the random number generated by the user. Throughout the protocol, the random number y_i is used as a confidential information. It is clear from the equation $C_i = hash(K_s) \oplus y_i$ that the legal user can easily compute $hash(K_s) = C_i \oplus y_i$ and may it announce as a public parameter. Therefore, the attacker can easily compute y_i using the smart card information. Therefore, the protocol proposed by [5] has not provided security on the secret key of the server.

3.3 Privileged Insider Attack

In this attack model, the insider person tries to find the user's password and if gets it, either insider person or attacker can launch insider attack. During the registration procedure of the scheme[5], the user sends $hash(PW_i)$ to the server. It is clear that the server can easily guess the legal user's password using the procedure mentioned in section 3.1. Therefore, the scheme [5] is not secure against insider attack.

3.4 Design Flaws in the Password Update Phase

During updating the password, we found that the smart card never checks the old information of the user. Therefore, this phase may suffer from serious weaknesses. We assume that the legal user has provided wrong old password $PW_i^w \neq PW_i$ and new correct password PW_i^* during updating. Now, the smart card computes $TPW_i^* = TPW_i \oplus h(PW_i^w) \oplus h(PW_i^*)$ which is not equivalent to $TPW_i = hash(PW_i^*) \oplus \pi_{y_i}^{'}$. Therefore, the legal user would not be authenticated due to wrong password. It is noted that the parameter TPW_i^* is reliant on the old and new password of the user.

4 Conclusion and Future Research

In this paper, we have analyzed security pitfalls such as off-line password guessing attack, insider attack, insecurity on secret key and inefficient password change phase etc. of the recently published Djellali et al.'s scheme user authentication and privacy preserving for ubiquitous devices. Therefore, this protocol is not suitable for real-time implementation. For implementation it, the protocol needs improvement in terms of security attacks. In future, the protocol should be enhanced based on the markov chain principle.

References

[1] L. Lamport, Password authentication with insecure communication, Communications of the ACM, vol. 24, no. 11, pp. 770-772, 1993.

[2] R. Amin, T. Maitra, S. P. Rana (2013), An Improvement of Wang. et al.'s Remote User Authentication Scheme against Smart Card Security Breach, International Journal of Computer Applications (0975 - 8887) Volume 75 - No. 13.

[3] R. Amin, G.P. Biswas, A Novel User Authentication and Key Agreement Protocol for Accessing Multi-Medical Server Usable in TMIS. Journal of Medical Systems, vol. 39(3), pp. 1-17. (2015).

[4] R. Amin, G.P. Biswas, Design and Analysis of Bilinear Pairing Based Mutual Authentication and Key Agreement Protocol Usable in Multi-server Environment, Wireless Personal Communications, 10.1007/s11277-015-2616-7, (2015).

[5] Djellali, B., Belarbi, K., Chouarfia, A. and Lorenz, P. (2015), User authentication scheme preserving anonymity for ubiquitous devices. Security Comm. Networks, doi: 10.1002/sec.1238.

[6] R. Amin, G.P. Biswas, Remote Access Control Mechanism Using Rabin Public Key Cryptosystem, Information Systems Design and Intelligent Applications(Springer), 525-533, 10.1007/978-81-322-2250-7_52, (2015).

[7] R. Amin, G.P. Biswas, Anonymity preserving secure hash function based authentication scheme for consumer USB mass storage device, Computer, Communication, Control and Information Technology (C3IT), 2015 Third International Conference on, pp. 1-6, 10.1109/C3IT.2015.7060190, (2015).

[8] W. Hsieh, J. Leu, Exploiting hash functions to intensify the remote user authentication scheme, Computers & Security, vol. 31, no. 6, pp. 791-798, 2012.

[9] W. C. Ku, S. M. Chen, Weakness and improvement of an efficient password based remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 204-207, 2004.

[10] R. Amin, Cryptanalysis and An Efficient Secure ID-Based Remote User Authentication Scheme Using Smart Card, International Journal of Computer Applications, vol. 75, no. 13, pp. 43-48, (2013).

[11] D. Giri, T. Maitra, R. Amin, P.D. Srivastava, An Efficient and Robust RSA-Based Remote User Authentication for Telecare Medical Information Systems. Journal of Medical Systems, doi=10.1007/s10916-014-0145-7.

[12] R. Amin, T. Maitra, D. Giri(2013)," An Improvement of Wang. et al.'s Remote User Authentication Scheme against Smart Card Security Breach", International Journal of Computer Applications (0975 - 8887) Volume 69 - No. 22, PP. (1-6).

[13] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis", *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'99)*, LNCS vol. 1666, pp. 388-397, (1999).

[14] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart card security under the threat of power analysis attacks", *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541-552, (2002).

[15] R. Amin, G.P. Biswas, A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity. Journal of Medical Systems, vol. 39(8), pp. 1-19. (2015).

[16] R. Amin, G.P. Biswas, An Improved RSA Based User Authentication and Session Key Agreement Protocol Usable in TMIS. Journal of Medical Systems, DOI: 10.1007/s10916-015-0262-y, (2015).

[17] S. Kumari, M. K. Khan, X. Li, An improved remote user authentication scheme with key agreement, Computers and Electrical Engineering, vol. 40, pp. 1997-2012, 2014.

[18] X. M. Wang, W. F. Zhang, J. S. Zhang, M. K. Khan, Cryptanalysis and improvement on two efficient remote user authentication scheme using cards, Computer Standards & Interface vol. 29, no. 5, pp. 507-512, 2007.

[19] R. Amin, G.P. Biswas, A Secure Light Weight Scheme for User Authentication and Key Agreement in Multi-gateway Based Wireless Sensor Networks. Ad Hoc Networks, doi:10.1016/j.adhoc.2015.05.020, (2015).

[20] R. Amin, G.P. Biswas, Cryptanalysis and Design of a Three-Party Authenticated Key Exchange Protocol Using Smart Card. Arabian Journal for Science and Engineering, doi:10.1007/s13369-015-1743-5, PP. 1-15, (2015).

[21] E. J. Yoon, E. K. Ryu, K. Y. Yoo, Further improvement of an efficient password based remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 612-614, 2004.

[22] A. K. Awasthi, K. Srivastava, R. C. Mittal, An improved timestamp-based remote user authentication scheme, Computer and Electrical Engineering, vol 37, no. 6, pp, 869-874, 2011.

[23] J. J. Shen, C. W. Lin, M. S. Hwang, Security enhancement for the timestamp-based password authentication scheme using smart cards, Compuers & Security, vol. 22, no. 7, pp. 591-595.

[24] D. Wang, C-G. Ma, Q-M. Zhang, S. Zhao, Secure Password-based Remote User Authentication Scheme against Smart Card Security Breach, Journal of Networks, vol. 8, no. 1, pp. 148-155, 2013.

[25] G. M. Yang, D. S. Wong, H. X. Wang, X. T. Deng, Two-factor mutual authentication based on smart cards and passwords, Journal of Computer and System Sciences, vol. 74, no. 7, pp 1160-1172, 2008.

[26] S. H. Islam, G. P. Biswas, A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Journal of Systems and Software, vol. 84, no. 11, pp. 1892-1898, 2011.

[27] S. H. Islam, G. P. Biswas, Design of Improved Password Authentication and Update Scheme based on Elliptic Curve Cryptography, Mathematical and Computer Modelling, vol. 57, no. 11-12, pp. 2703-2717, 2013.

[28] S. H. Islam, Design and analysis of an improved smartcard based remote user password authentication scheme, International Journal of Communication Systems, 2014. DOI:10.1002/dac.2793.

[29] S. H. Islam, M. K. Khan, Cryptanalysis and Improvement of Authentication and Key Agreement Protocols for Telecare Medicine Information Systems, Journal of Medical Systems, vol. 38, no. 10, pp. 1-16, 2014.