Cryptanalysis of the Mutual Authentication and Key Agreement Protocol with Smart Cards for Wireless Communications

Shu-Fen Chiou[1], Hsieh-Tsen Pan[2], Eko Fajar Cahyadi[2,3], and Min-Shiang Hwang[2,4]

(Corresponding author: Min-Shiang Hwang)

Department of Information Management, National Taichung University of Science and Technology, Taiwan[1]

Department of Computer Science & Information Engineering, Asia University, Taichung, Taiwan[2]

Department of Telecommunication Engineering, Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia[3]

Department of Medical Research, China Medical University Hospital, China Medical University, Taiwan[4]

(Email: mshwang@asia.edu.tw)

(Received Aug. 21, 2018; revised and accepted Dec. 5, 2018)

Abstract

Recently, Guo *et al.* proposed a secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications. There are two main contributions of their scheme: confidentiality of the session key and updating the password efficiently. They claimed that their scheme could withstand various known types of attacks: user anonymity, withstanding the insider attacks, the replay attacks, and the offline dictionary attacks. However, we find some weaknesses of their scheme in this article. We show that their scheme is vulnerable to on-line password guessing with smart cards under stolen attacks and the denial of service attacks.

Keywords: Formal Proof; Key Agreement; Password; Smart Card; User Authentication

1 Introduction

The most widely applied to verify the legitimate users in wireless communications is the user authentication schemes [5, 9, 13, 17, 22, 26]. Many user authentication schemes are designed to verify the users for single server environment [2, 8, 18, 21]. However, more and more remote users need more services in various clouds or different servers. In other word, the remore users in internet and wireless communications will be operated in a multi-servers or multi-clouds [4,11,16]. In the conventional user authentication schemes, the remote users not only need to login to various cloud servers with repetitive registration, but also need to remember the various remote user ID (identity) and password pairs [3, 6, 10, 12].

In 2012, Ramasamy *et al.* proposed a remote user authentication scheme for smart cards [20]. However, Thandra *et al.* showed that their scheme is insecure [23]. In 2016, Thandra *et al.* also proposed a secure and efficient user authentication scheme [23]. However, Pan *et al.* shown that their scheme is vulnerable to denial of service, online and offline password guessing, and user impersonation attacks [19]. In 2016, Wei *et al.* proposed a user authentication scheme [25]. However, Tsai *et al.* also shown that their scheme is vulnerable to password guessing, denial of service, and privileged insider attacks [24]. In 2017, Liu *et al.* thus proposed an efficient and secure user authentication scheme with smart cards [15]. However, Liu *et al.* shown that their scheme was also vulnerable to the replaying attacks [14].

Recently, Guo *et al.* proposed a secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications [7]. There are two main contributions of their scheme: confidentiality of the session key and updating the password efficiently. They claimed that their scheme could withstand various known types of attacks: user anonymity, withstanding the insider attack, the replay attacks, the offline dictionary attacks. However, we find some weaknesses of their scheme in this article. We show that their scheme is vulnerable to on-line password guessing with smart cards under stolen attacks and the denial of service attacks.

The rest of this paper is organized as follows. In Section 2, we briefly review Guo *et al.*'s mutual authentication and key agreement protocol. In Section 3, we analyze and show that some security flaws exist in Guo *et al.*'s user authentication scheme. Finally, we present our conclusions in Section 4.

2 Review of Guo *et al.*'s Scheme

In this section, we briefly review Guo *et al.*'s mutual authentication and key agreement protocol with smart cards for wireless communications [7]. There are four participants in Guo *et al.*'s mutual authentication and key agreement protocol: Users ($U_i, i = 1, 2, \cdots, m$ for short); Card reader (CR for short); Base stations (BS for short) and cluster head ($CH_j, j = 1, 2, \cdots, n$ for short). The scheme consists of four phases, namely, the registration phase, the login phase, the authentication phase, and the password change phase.

2.1 The Registration Phase

In the registration phase, the base station BS makes a smart card for a new user (U_i). The registration phase is executed as follows:

1) The new user U_i firstly chooses a random number y_i, his/her identity ID_i and password pw_i.

2) U_i computes $pwr_i = h(pw_i \parallel y_i)$ and sends $\{ID_i, pwr_i\}$ to the base station BS through a secure channel.

3) After getting message $\{ID_i, pwr_i\}$ from the user U_i, base station computes $X_i = h(ID_i \parallel s) \oplus pwr_i$ and $B_i = h(h(ID_i \parallel s) \parallel pwr_i)$.

4) The base station issues a smart card for user U_i by storing $\{X_i, B_i, h(\cdot)\}$ into the memory of the smart card.

5) After getting his/her smart card, user U_i stores y_i into the memory of the smart card.

2.2 The Login Phase

In this phase, the user (U_i) wants to login to the base station BS_j for obtaining some services; the user (U_i) firstly attaches his/her smart card to a device reader and inputs his/her identity ID'_i and password PW'_i. The login phase is executed in the following:

1) Then card reader computes

$$\begin{aligned} pwr'_i &= h(pw_i \parallel y_i), \\ Y'_i &= X_i \oplus pwr'_i, \\ B'_i &= h(Y'_i \parallel pwr'_i), \end{aligned}$$

and checks whether computed B'_i equals stored B_i. If true, proceed to next, otherwise 'rejects' user U_i, then, user U_i chooses ID_{CH_j} and submits it to the card reader.

2) The card reader further chooses a random number N_1 and computes

$$\begin{aligned} P_i &= h(Y'_i \parallel ID_{CH_j} \parallel N_1 \parallel pwr'_i) \\ R_i &= N_1 \oplus pwr'_i, \end{aligned}$$

and sends $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ to the base station.

2.3 The Authentication Phase

Upon receiving the authentication request message $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ from user U_i, the base station BS executes this authentication phase in the following:

1) The base station computes

$$\begin{aligned} Y_i^* &= h(ID_i \parallel s), \\ pwr_i^* &= Y_i^* \oplus X_i, \\ N_1^* &= pwr_i^* \oplus R_i \\ P_i^* &= h(Y_i^* \parallel ID_{CH_j} \parallel N_1^* \parallel pwr_i^*). \end{aligned}$$

2) BS checks whether computed P_i^* equals sending P_i or not. If it holds good, base station further chooses a random number N_2 and computes

$$\begin{aligned} Z_i &= pwr_i^* \oplus N_2, \\ D_i &= h(Y_i^* \parallel N_2 \parallel ID_{CH_j} \parallel ID_i \parallel N_1^*). \end{aligned}$$

3) BS sends $\{ID_i, ID_{CH_j}, Z_i, D_i\}$ to the user U_i. Again base station computes

$$\begin{aligned} N_3 &= N_2 \oplus N_1^*, \\ V_i &= h(ID_{CH_j} \parallel S_{CH_j}), \\ E_i &= V_i \oplus N_3, \\ A_i &= h(Y_i^* \parallel N_3 \parallel pwr_i^*), \\ L_i &= A_i \oplus V_i \\ G_i &= h(S_{CH_j} \parallel N_3 \parallel A_i \parallel ID_i \parallel ID_{CH_j}) \end{aligned}$$

4) BS sends $\{E_i, L_i, G_i, ID_i, ID_{CH_j}\}$ to the cluster head CH_j. After that, the following computations are performed:

   a. After getting reply message $\{ID_i, ID_{CH_j}, Z_i, D_i\}$ from base station, the card reader computes $N'_2 = Z_i \oplus pwr'_i$, $D'_i = h(Y'_i \parallel N'_2 \parallel ID_{CH_j} \parallel ID_i \parallel N_1)$ and checks whether computed D'_i equals sending D_i or not. If it holds good, then computes $N'_3 = N_1 \oplus N'_2$, $A'_i = h(Y'_i \parallel N'_3 \parallel pwr'_i)$ and session key $SK = h(ID_i \parallel ID_{CH_j} \parallel N'_3 \parallel A'_i)$.

   b. After receiving message $\{E_i, L_i, G_i, ID_i, ID_{CH_j}\}$ from base station, cluster head CH_j computes $V_i^\star = h(ID_{CH_j} \parallel S_{CH_j})$, $N_3^\star = V_i^\star \oplus E_i$, $A_i^\star = L_i \oplus V_i^\star$ and $G_i^\star = h(S_{CH_j} \parallel N_3^\star \parallel A_i^\star \parallel ID_i \parallel ID_{CH_j})$ and checks weather computed $G_i^\star$ equals sending G_i or not. If true, then it computes session key $SK = h(ID_i \parallel ID_{CH_j} \parallel N_3^\star \parallel A_i^\star)$.

   Now, both parties (user U_i and cluster head CH_j) agree with common shared session key SK and can communicate securely to each other by a shared secret session key SK in future.

3 Cryptanalysis of Guo *et al.*'s Scheme

In this section, we will analyze Guo *et al.*'s mutual authentication and key agreement protocol with smart cards for wireless communications [7]. Guo *et al.* claimed that their scheme resisted different possible attacks, including smart card stolen attacks, impersonation attacks, privileged insider attacks, replay attacks, off-line password guessing attacks, theft attacks, session key recovery attacks, denial of service attacks, and cluster head capture attacks. In this section, we show that Guo *et al.*'s user authentication scheme is vulnerable to off-line password guessing with smart cards under stolen attacks.

3.1 Off-line Password Guessing with Smart Cards under Stolen Attacks

Guo *et al.* claimed that an attacker is hard to derive user's password PW_i if the attacker gets the user's smart card and a login message $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ between the user U_i and base station BS. In this section, we will show that Guo *et al.*'s scheme is vulnerable to off-line password guessing with smart cards under stolen attacks.

The attacker is able to intercept from the public channel. Thus, the attacker obtains a login message $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ between the user U_i and base station BS. The attacker may guess the user's password PW_i as follows:

1) The attacker guesses the user's password PW'.

2) The smart card computes pwr'_i as follows:

$$pwr'_i = h(PW'||y_i),$$

here y_i is obtained from the smart card.

3) The smart card computes Y'_i and N'_1 as follows:

$$\begin{aligned} Y'_i &= X_i \oplus pwr'_i, \\ N'_1 &= R_i \oplus pwr'_i. \end{aligned}$$

Here, X_i and R_i are intercepted from the last login message between the smart card and the base station.

4) The attacker computes P'_i as follows:

$$P'_i = h(Y'_i||ID_{CH_j}||N'_1||pwr'_i).$$

Next the attacker checks if P'_i is or not equal to P_i; here P_i is intercepted from the last login message between the smart card and the base station. If it's hold, the guessed password is correct, otherwise, the attacker guess other password and checks it again as the above steps.

The attacker could repeat the above step to re-guess the other password. If it is true, this implies that the guessing password PW'_i is correct. Therefore, Guo *et al.*'s user authentication scheme is vulnerable to the off-line password guessing with smart cards under stolen attacks.

3.2 The improvement of Guo *et al.*'s Scheme

The main weakness of Guo *et al.*'s user authentication scheme is that the attacker could repeat to guess the password with smart card. To improve the weakness of Guo *et al.*'s scheme, the smart card in this scheme should set up the timer. If the user input the incorrect password 3 times, the smart card must initiate the registration of the user.

4 Conclusion

In this article, we have reviewed Guo *et al.*'s mutual authentication and key agreement protocol with smart cards for wireless communications [7] and cryptanalyzing its security. Because the user password chosen is easy to remember, we showed that Guo *et al.*'s user authentication scheme cannot withstand the off-line password guessing with smart cards under stolen attacks. We also propose an improvement of Guo *et al.*'s Scheme in this article.

Acknowledgment

This research was partially supported by the Ministry of Science and Technology, Taiwan (ROC), under contract no.: MOST 104-2221-E-468-004 and MOST 105-2410-H-468-009. MOST 106-2221-E-468-002.

References

[1] R. Amin, "Cryptanalysis and Efficient Dynamic ID Based Remote User Authentication Scheme in Multi-server Environment Using Smart Card", *International Journal of Network Security*, Vol. 18, No. 1, pp. 172-181, 2016.

[2] N. Anwar, I. Riadi, A. Luthfi, " Forensic SIM Card Cloning Using Authentication Algorithm", *International Journal of Electronics and Information Engineering*, Vol. 4, No. 2, pp. 71-81, 2016.

[3] C. C. Chang, W. Y. Hsueh, T. F. Cheng, "An Advanced Anonymous and Biometrics-based Multi-server Authentication Scheme Using Smart Cards", *International Journal of Network Security*, Vol. 18, No. 6, pp. 1010-1021, 2016.

[4] 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", *The Journal of Supercomputing*, Vol. 66, No. 2, pp. 1008-1032, 2013.

[5] T. Y. Chang, W. P. Yang, M. S. Hwang, "Simple authenticated key agreement and protected password change protocol", *Computers & Mathematics with Applications*, vol. 49, pp. 703–714, 2005.

[6] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's Improvement on a Password Authentication Scheme for Multi-server Environments",

International Journal of Network Security, Vol. 16, No. 4, pp. 318-321, 2014.

[7] C. Guo, C. C. Chang, S. C. Chang, "A secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications", *International Journal of Network Security*, Vol. 20, No. 2, pp. 323-331, 2018.

[8] M. S. Hwang, L. H. Li, "A New Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp. 28-30, 2000.

[9] C. C. Lee, M. S. Hwang, I. E. Liao, "Security Enhancement on a New Authentication Scheme with Anonymity For Wireless Environments", *IEEE Transactions on Industrial Electronics*, Vol. 53, No. 5, pp. 1683-1687, 2006.

[10] L. H. Li, I. C. Lin, M. S. Hwang, "A Remote Password Authentication Scheme for Multi-server Architecture Using Neural Networks", *IEEE Transactions on Neural Networks*, Vol. 12, pp. 1498-1504, 2001.

[11] I. C. Lin, M. S. Hwang, L. H. Li, "A New Remote User Authentication Scheme for Multi-Server Architecture", *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13-22, 2003.

[12] C. H. Ling, W. Y. Chao, S. M. Chen, and M. S. Hwang, "Cryptanalysis of Dynamic Identity Based on a Remote User Authentication Scheme for a Multi-server Environment", in *2015 International Conference on Advances in Mechanical Engineering and Industrial Informatics (AMEII 2015)*, Zhengzhou, April 11-12, 2015, Advances in Engineering Research, vol. 15, pp. 981-986, Atlantis Press, 2015.

[13] C. W. Liu, C. Y. Tsai, and M. S. Hwang, "Cryptanalysis of an Efficient and Secure Smart Card Based Password Authentication Scheme", *Recent Developments in Intelligent Systems and Interactive Applications*, Lecture Notes in Computer Science, Springer, 2017.

[14] C. W. Liu, C. Y. Tsai, and M. S. Hwang, "Cryptanalysis of an Efficient and Secure Smart Card Based Password Authentication Scheme", *Recent Developments in Intelligent Systems and Interactive Applications*, Lecture Notes in Computer Science, Springer, 2017.

[15] Y. Liu, C. C. Chang, S. C. Chang, "An Efficient and Secure Smart Card Based Password Authentication Scheme", *International Journal of Network Security*, Vol. 19, No. 1, pp. 1-10, 2017.

[16] Y. Liu, C. C. Chang, C. Y. Sun, "Notes on An Anonymous Multi-server Authenticated Key Agreement Scheme Based on Trust Computing Using Smart Card and Biometrics", *International Journal of Network Security*, Vol. 18, No. 5, pp. 997-1000, 2016.

[17] J. W. Lo, J. Z. Lee, M. S. Hwang, Y. P. Chu, "An Advanced Password Authenticated Key Exchange Protocol for Imbalanced Wireless Networks", *Journal of Internet Technology*, Vol. 11, No. 7, pp. 997-1004, 2010.

[18] E. O. Osei, J. B. Hayfron-Acquah, "Cloud Computing Login Authentication Redesign", *International Journal of Electronics and Information Engineering*, Vol. 1, No. 1, pp. 1-8, 2014.

[19] C. S. Pan, C. Y. Tsai, S. C. Tsaur, M. S. Hwang, "Cryptanalysis of an efficient password authentication scheme", *2016 3rd International Conference on Systems and Informatics (ICSAI 2016)*, 2016.

[20] R. Ramasamy and A. P. Muniyandi, "An Efficient Password Authentication Scheme for Smart Card", *International Journal of Network Security*, Vol. 14, No. 3, pp. 180-186, 2012.

[21] J. J. Shen, C. W. Lin, M. S. Hwang, "A Modified Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, Vol. 49, No. 2, pp. 414-416, 2003.

[22] M. Stanek, "Weaknesses of Password Authentication Scheme Based on Geometric Hashing", *International Journal of Network Security*, Vol. 18, No. 4, pp. 798-801, 2016.

[23] P. K. Thandra, J. Rajan, and S. A. V. S. Murty, "Cryptanalysis of an Efficient Password Authentication Scheme", *International Journal of Network Security*, Vol. 18, No. 2, pp. 362-368, 2016.

[24] C. Y. Tsai, C. S. Pan, and M. S. Hwang, "An Improved Password Authentication Scheme for Smart Card", *Recent Developments in Intelligent Systems and Interactive Applications*, Lecture Notes in Computer Science, Springer, 2017.

[25] J. Wei, W. Liu, X. Hu, "Secure and Efficient Smart Card Based Remote User Password Authentication Scheme", *International Journal of Network Security*, Vol. 18, No. 4, pp. 782-792, 2016.

[26] H. Zhu, Y. Zhang, and Y. Zhang, "A Provably Password Authenticated Key Exchange Scheme Based on Chaotic Maps in Different Realm", *International Journal of Network Security*, Vol. 18, No. 4, pp. 688-698, 2016.

Biography

Shu-Fen Chiou received a B.B.A degree in Information Management from National Taichung Institute of Technology, Taichung, Taiwan, ROC, in 2004; She studied M.S. degree in Computer Science and Engineering from National Chung Hsing University for one year, and she started to pursue the Ph.D. degree. She received a Ph. D. from Computer Science and Engineering from National Chung Hsing University in 2012. She is currently an assistant professor of department of Information Management, National Taichung University of Science and Technology. Her current research interests include information security, network security, data hiding, text mining and big data analysis.

Hsien-Tsen Pan received B.S. in Business Administration From Soochow University Taipei Taiwan in

1999; M.S in Information Engineering, Asia University Taichung Taiwan 2015; Doctoral Program of Information Engineering, Asia University Taichung Taiwan from 2015 till now. From 2011 to 2014, he was the manager in Enterprise Service Chunghwa Telecom South Branch Taichung Taiwan. From 2014 to 2017, he was the operation manager in Medium division Taiwan Ricoh Co., Ltd. Taichung Taiwan From 2017 Sep 20 he is the Apple MDM Server Service VP in Get Technology Co.Ltd. Taipei Taiwan.

Eko Fajar Cahyadi is currently pursuing a Ph.D. degree in the Department of Computer Science and Information Engineering at Asia University, Taiwan. He receives the B. Eng. and M. Sc. degree in electrical engineering from Institut Sains dan Teknologi Akprind Yogyakarta in 2009, and Institut Teknologi Bandung in 2013, respectively. His research interest includes wireless network security, optical fiber communication, and teletraffic engineering.

Min-Shiang Hwang received M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988; and Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan in 1995. He was a professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2009. He was also a visiting professor with University of California (UC), Riverside and UC. Davis (USA) during 2009-2010. He was a distinguished professor of Department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). Dr. Hwang was a dean of College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with Department of Computer Science and Information Engineering, AU. His current research interests include information security, electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.