Notes on "An Anonymous Multi-server Authenticated Key Agreement Scheme Based on Trust Computing Using Smart Card and Biometrics"

Yanjun Liu[1,2], Chin-Chen Chang[2,3] and Chin-Yu Sun[4]
(Corresponding author: Ching-Chun Chang)
School of Computer Science and Technology, Anhui University[1]
No. 111 Jiulong Rd., Hefei 230601, China
Department of Computer Science and Information Engineering, Asia University[2]
No. 500, Lioufeng Rd., Wufeng, Taichung 413, Taiwan
Department of Information Engineering and Computer Science, Feng Chia University[3]
No. 100 Wenhwa Rd., Seatwen, Taichung 407, Taiwan
Department of Computer Science, National Tsing-Hua University[4]
No. 101, Section 2, Kuang-Fu Road, Hsinchu, Hsinchu 30013, Taiwan
(Email: alan3c@gmail.com)
(Received Nov. 27, 2013; revised and accepted May 5 & July 25, 2014)

Abstract

Nowadays, multi-server remote user authentication schemes have been studied extensively in the literature. Recently, Chuang and Chen proposed a multi-server authentication scheme based on trust computing using smart cards and biometrics. Their scheme is more efficient and can achieve more security requirements than other related schemes. However, we found that Chuang and Chen's scheme can disclose private information shared between a legal user and an authorized server to another server. Moreover, loss of smart card attacks can be amounted and user anonymity cannot be achieved.

Keywords: Anonymity, authentication, disclosure of privacy, loss of smart card attack, multi-server

1 Introduction

Along with the rapid development of wireless communication technologies, more and more people can acquire different types of Internet service through their mobile devices effortlessly. Therefore, how to verify the validity of remote login users before they access the services has become a significant security problem in wireless networks. A remote user authentication scheme based on smart card [2, 3] and password is the most extensively used mechanism to solve the aforementioned security problem due to its simplicity and high efficiency.

Nowadays, the multi-server environment [1, 4, 5] has attracted increasing popularity such that a user may acquire services provided by multiple servers simultaneously. As a result, a practical remote user authentication scheme must take the multi-server environment into account to satisfy the requirement of single registration, that is, any user only needs to register at the registration center (RC) once without registering to each server. This can simplify the registration procedure and diminish computational burden of the RC's.

However, one of the shortcomings of conventional multi-server remote user authentication schemes is that if both the user's smart card and password are stolen, authentication schemes may be susceptible to some malicious attacks. To enhance the degree of security, Chuang and Chen [1] proposed a multi-server authentication scheme based on trust computing that integrates the user's unique biometrics (e.g., fingerprints and irises) with smart card and password. Their scheme is more efficient and can achieve more security requirements than other related schemes. Unfortunately, we found that Chuang and Chen's scheme suffered from some security weaknesses. More specifically, their scheme can disclose private information shared between a legal user and an authorized server to another server. It cannot withstand loss of smart card attacks and is not able to ensure user anonymity either. These security weaknesses will be demonstrated and analyzed in detail in the following section.

2 Comment on Chuang and Chen's Scheme

In this section, we first briefly review the multi-server authentication scheme proposed by Chuang and Chen [1], and then discuss its security weaknesses.

2.1 Review of Chuang and Chen's Scheme

Chuang and Chen's scheme [1] contains three types of entities, i.e., the user, the registration center (RC) and multiple servers. These entities perform three phases: 1) the registration phase; 2) the login and authentication phase; and 3) the password change phase. In the registration phase, servers and users must register at the RC respectively. Based on the concept of trust computing, all authorized servers constitute an alliance and trust each other. Each authorized server must register at the RC and share a common secret key PSK with the RC before providing services to users. Furthermore, Chuang and Chen's scheme assumes that the key PSK is impossible to be compromised and it will be used in the login and authentication phase later. On the other hand, each user only needs to register at the RC once without repeating registration to each server. After registration, the login and authentication phase is executed to achieve mutual authentication between the user and the server. In addition, users can select and update their passwords easily without depending on the RC. In the following, we give the detailed description of the user registration phase and the login and authentication phase in Chuang and Chen's scheme, and the notations used throughout the scheme are listed in Table 1.

Table 1: Notations list in Chuang and Chen's scheme

U_i	The user i
RC	The registration center
S_j	The authorized server j
ID_i	The identity of user U_i
PW_i	The password of user U_i
BIO_i	The biometrics information of user U_i
x	A secret value of RC
SID_j	The identity of authorized server S_j
N_i	A random number
$h(\cdot)$	A collision-free one-way hash function

2.1.1 The User Registration Phase

1) User U_i sends ID_i and $h(PW_i \oplus BIO_i)$ to the RC through a secure channel.

2) The RC computes $A_i = h(ID_i \parallel x)$, $B_i = h(A_i)$, $C_i = h(PW_i \oplus BIO_i) \oplus B_i$, and $D_i = PSK \oplus A_i$.

3) The RC stores the parameters $\{ID_i, B_i, C_i, D_i, h(\cdot)\}$ on a new smart card and issues the smart card to user U_i over a secure channel.

2.1.2 The Login and Authentication Phase

1) User U_i inserts his/her smart card into a card reader and then inputs his/her ID_i and PW_i and scans his/her BIO_i at the sensor.

2) The smart card checks ID_i and then examines whether $h(PW_i \oplus BIO_i) \oplus C_i$ is equal to B_i or not. If the equation holds, the smart card generates a nonce N_1, and then computes $M_1 = h(B_i) \oplus N_1$, $AID_i = h(N_1) \oplus ID_i$, and $M_2 = h(N_1 \parallel AID_i \parallel D_i)$.

3) The smart card sends the authentication message $\{AID_i, M_1, M_2, D_i\}$ to server S_j.

4) Server S_j retrieves $A_i = D_i \oplus PSK$ and $N_1 = M_1 \oplus h^2(A_i)$. Then,$S_j$ computes and checks $h(N_1 \parallel AID_i \parallel D_i)? = M_2$. If it holds, the phase continues; otherwise,S_j terminates the phase. Next, S_j generates a nonce N_2 and constructs the session key $SK_{ij} = h(N_1 \parallel N_2)$. After that, S_j computes $M_3 = N_2 \oplus h^2(N_1)$ and $M_4 = h(SID_j \parallel N_2)$.

5) Server S_j sends the authentication reply message $\{SID_j, M_3, M_4\}$ to the smart card.

6) The smart card retrieves $N_2 = M_3 \oplus h^2(N_1)$ and checks whether $h(SID_j \parallel N_2)$ is equal to M_4 or not. If it holds, the smart card can generate the session key $SK_{ij} = h(N_1 \parallel N_2)$ and $M_5 = SK_{ij} \oplus h(N_2)$.

7) The smart card sends M_5 to server S_j.

8) Server S_j retrieves $h(N_2) = M_5 \oplus SK_{ij}$ and checks the validity of this value.

If the authentication is passed, the server and the user can mutually authenticate each other and establish a shared session key SK_{ij} for the subsequent secret communication. In Subsections 2.2 - 2.4, we will show the security weaknesses of this authentication scheme.

2.2 Disclosure of Privacy

In the multi-server environment, a user does not need to register to each server but only registers to the RC once [4, 5]. Moreover, Chuang and Chen assumed that their multi-server authentication scheme are based on trust computing, which means all authorized servers can trust and work in close collaboration with each other. Although authorized servers can be considered as an alliance in Chuang and Chen's scheme, it does not imply that one authorized server has the privilege to access the private information shared between a user and another authorized server. Unfortunately, we have found that the session key shared between a legal user and an authorized server can be disclosed to another authorized server. Under the

assumption that there are three entities, i.e., user U_i and servers S_A and S_B, and SK_{iA} is the session key shared between U_i and S_A, we demonstrate how S_B obtains SK_{iA} without detection by the following steps.

1) Server S_B registers at the RC and shares a secret key PSK with the RC.
2) S_B intercepts the messages M_1^A, D_i^A, and M_3^A that are transmitted between user U_i and server S_A through the public channel in the authentication.
3) S_B retrieves $A_i^A = D_i^A \oplus PSK$ and then uses M_1^A and A_i^A to compute $N_1^A = M_1^A \oplus h^2(A_i^A)$.
4) S_B uses M_3^A and N_1^A to obtain $N_2^A = M_3^A \oplus h^2(N_1^A)$.
5) With N_1^A and N_2^A in hand, S_B can immediately extract the session key $SK_{iA} = h(N_1^A \parallel N_2^A)$ shared between user U_i and server S_A.

2.3 Loss of Smart Card Attack

Here, we explain why Chuang and Chen's scheme is unable to withstand loss of smart card attacks. Assuming that an attacker Eve has stolen user U_i's smart card, Eve can extract all the secret information, i.e., ID_i, B_i, C_i, D_i, and $h(\cdot)$ preserved in the smart card and successfully launches the loss of smart card attack without knowing U_i's password PW_i and biometrics BIO_i as follows.

1) Without U_i's correct parameter N_1, Eve must choose a random number N_1^* and generates $M_1^* = h(B_i) \oplus N_1^*$, $AID_i^* = h(N_1^*) \oplus ID_i$, and $M_2^* = h(N_1^* \parallel AID_i^* \parallel D_i)$ by himself/herself.
2) Eve impersonates U_i to send $\{AID_i^*, M_1^*, M_2^*, D_i\}$ to server S_j.
3) S_j retrieves $A_i = D_i \oplus PSK$ and $N_1^* = M_1^* \oplus h^2(A_i)$. Then, S_j checks whether $h(N_1^* \parallel AID_i^* \parallel D_i)$ is equal to M_2^*. If it holds, S_j continues the procedure.
4) S_j generates a nonce N_2 and constructs the session key $SK_{Ej} = h(N_1^* \parallel N_2)$. Afterwards, S_j computes $M_3^* = N_2 \oplus h^2(N_1^*)$ and $M_4 = h(SID_j \parallel N_2)$.
5) S_j sends $\{SID_j, M_3^*, M_4\}$ to Eve.
6) Eve retrieves $N_2 = M_3^* \oplus h^2(N_1^*)$ and checks whether $h(SID_j \parallel N_2)$ is equal to M_4. If it holds, Eve computes the session key $SK_{Ej} = h(N_1^* \parallel N_2)$ and $M_5^* = SK_{Ej} \oplus h(N_2)$.
7) Eve sends M_5^* to S_j.
8) S_j retrieves $h(N_2) = M_5^* \oplus SK_{Ej}$ and checks the validity of this value.

Based on the above analysis, it indicates that when the smart card is stolen, the server can be convinced that attacker Eve is a legal user and they will establish a common session key. Therefore, loss of smart card attacks can be amounted in Chuang and Chen's scheme.

2.4 User Anonymity

Chuang and Chen claimed that their scheme can ensure the user anonymity such that an attacker has no way to obtain the original identity of a user. This is because the user's identity is concealed in AID_i as $AID_i = h(N_1) \oplus ID_i$ and the random number N_1 selected by user U_i is not revealed. However, the following scenario shows that attacker Eve can determine the original identity of a user.

1) Attacker Eve intercepts the messages AID_i, M_2, and D_i.
2) Since $M_2 = h(N_1 \parallel AID_i \parallel D_i)$, Eve can easily find out the correct value of N_1 via M_2, AID_i, and D_i by launching an off-line guessing attack.
3) Eve computes $ID_i = AID_i \oplus h(N_1)$.

Therefore, we can conclude that Chuang and Chen's scheme cannot achieve user anonymity.

2.5 Conclusions

In this paper, we pointed out the security weaknesses in the multi-server authentication scheme based on trust computing proposed by Chuang and Chen. Although their scheme combines the user's biometrics with smart card and password to enhance the security, it still suffers from three security problems, i.e., 1) the disclosure of the session key shared between a legal user and an authorized server; 2) it cannot withstand loss of smart card attacks; and 3) it cannot guarantee user anonymity.

References

[1] M. C. Chuang, and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," *Expert Systems with Applications*, vol. 41, no.4, pp. 1411–1418, 2014.
[2] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," *Computer Communications*, vol. 34, no. 3, pp. 367–374, 2011.
[3] C. T. Li, and C. C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications," *Mathematical and Computer Modelling*,vol. 55, no. 1, pp. 35–44, 2012.
[4] 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, pp. 13–22, 2003.
[5] W. J. Tsaur, J. H. Li, and W. B. Lee, "An efficient and secure multi-server authentication scheme with key agreement," *Journal of Systems and Software*, vol. 85, no. 4, pp. 876–882, 2012.

Yanjun Liu received her B.S. degree in 2005, in School of Computer Science and Technology from Anhui University, Hefei, China. She received her Ph.D. degree in 2010, in School of Computer Science and Technology from University of Science and Technology of China, Hefei, China. She is currently serving in Anhui University. Meanwhile, she is a postdoctor at Asia University, Taichung, Taiwan. Her current research interests include information security and computer cryptography.

Chin-Yu Sun received the MS degree in Department of Information Engineering and Computer Science from Feng Chia University, Taichung, Taiwan in 2013. He is currently pursuing his Ph.D. degree in computer science from National Tsing Hua University, Hsinchu, Taiwan. He current research interests include information security, cryptography, wireless communications, mobile communications, and cloud computing.

Chin-Chen Chang received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Taiwan. He was the head of, and a professor in, the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the dean of the College of Engineering at the same university. From August 1995 to October 1997, he was the provost at the National Chung Cheng University. From September 1996 to October 1997, Dr. Chang was the Acting President at the National Chung Cheng University. From July 1998 to June 2000, he was the director of Advisory Office of the Ministry of Education of the R.O.C. Since February 2005, he has been a Chair Professor of Feng Chia University. He is currently a Fellow of IEEE and a Fellow of IEE, UK. He also published several hundred papers in Information Sciences. In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, image compression and data structures.