A Flexible Remote User Authentication Scheme Using Smart Cards

Cheng-Chi Lee[‡] Min-Shiang Hwang[†] Wei-Pang Yang[‡]
Department of Information Management, Chaoyang University of Technology[†]
168, Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.
Email: mshwang@mail.cyut.edu.tw
Department of Computer and Information Science, National Chiao-Tung University[‡]
1001 Ta Hsueh Road, Hsinchu 300, Taiwan, R.O.C.

Abstract

In 1999, Hwang and Li proposed a new user authentication scheme using s-mart cards. The scheme does not need any password or verification table. Later, Sun proposed an efficient remote use authentication scheme to improve the efficiency of the Hwang-Li scheme. However, these two schemes do not allow users to freely choose and change their passwords. In this article, we shall propose a simple and efficient remote user authentication scheme that allows users to freely choose and change their pass-words without significantly increasing the computation cost.
Keywords: Authentication, cryptography, password, security.

I Introduction

Recently, based on various techniques, many password authentication schemes using smart cards have been proposed by some researchers [1, 2, 3, 6, 9, 10]. These schemes can allow a legal user to login to remote server and the legal user will be granted access to the server's facilities. Based on ElGamal's cryptosystem [4], Chang and Liao proposed a remote password authentication scheme [1]. However, this scheme has a weakness that users cannot freely choose and change their passwords. Based on Chinese Remainder Theorem (CRT), Chang and Wu proposed a remote password authentication scheme [2]. Based on geometric Euclidean plane, Wu proposed a new remote login authentication scheme [10]. Its simplicity of geometry and the property allow users can freely choose their own passwords. However, this scheme is attacked by Hwang [5]. And in [3], Chien et al. proposed another attack to Wu's scheme and remedy his scheme.

Based on ElGamal's cryptosystem, Hwang and Li proposed a remote user authentication scheme using smart cards [6]. The scheme does not need any password and verification table for authentication. Later, Sun proposed an efficient remote use authentication scheme using smart cards [9]. He claimed that his scheme was much more efficient than Hwang and Li's scheme. However, in these two schemes, the users are not allowed to freely choose and change their passwords which can be a major drawback. Hence, in this paper, we shall propose a new scheme that allows users to freely choose and change their passwords without significantly increasing the computation cost.

This paper is organized as follows. We shall first review the Hwang-Li's scheme and the Sun's scheme in Section 2. Then, in Section 3, we shall propose a simple and efficient remote user authentication scheme. In Section 4, we analyze the security of our scheme. In Section 5, we show its efficiency. Finally, a brief conclusion will be given in Section 6.

II Literature Reviews

In this section, we briefly review the Hwang-Li's scheme [6] and the Sun's scheme [9]. Each of these two schemes is composed of three phases: the registration phase, the login phase, and the authentication phase.

2.1 The Hwang-Li's Scheme

Registration Phase:
The main task of this phase is to deliver a smart card to each registered user. When a user U_i wants to register with the server, U_i first submits his/her identity ID_i to the server. Then the server computes PW_i for U_i as follows:

$$PW_i = ID_i^{x_s} \bmod P. \tag{1}$$

Here x_s is a secret key for the server, and P is a large prime number of 1024 bits. Then the registration center stores PW_i, one-way function h, and P into the smart card. The smart card is delivered to the user by the registration center.

Login Phase:
To log in the system and access the resources, U_i first inserts his/her own smart card and keys in his/her (ID_i, PW_i). Afterwards, the smart card will perform the following tasks:

1. Randomly choose an integer r.
2. Calculate $C_1 = ID_i^r \bmod P$.
3. Calculate $t = h(T \oplus PW_i) \bmod (P-1)$, where T is the current date and time, and $\oplus$ denotes an exclusive operation.
4. Calculate $M = ID_i^t \bmod P$.
5. Calculate $C_2 = M(PW_i)^r \bmod P$.
6. Send the messages $C = (ID_i, C_1, C_2, T)$ to the server.

Authentication Phase:
After receiving the message C from U_i, the server verifies the login user as follows:

1. Check the validity of ID_i. If it is incorrect, then the server rejects the login user U_i.
2. Check the time interval between T and T', where T' is the moment when the server receives the message from U_i. If $(T' - T) \geq \Delta T$, then the server rejects U_i. The time interval ΔT denotes the expected legal time interval for transmission delay.
3. Calculate $PW_i = ID_i^{x_s} \bmod P$ and $t = h(T \oplus PW_i) \bmod (P-1)$. Then check the following equation:

$$C_2(C_1^{x_s})^{-1} \bmod P = ID_i^t \bmod P. \tag{2}$$

   If the above equation holds, the login user U_i is verified and is permitted to access the server.

In Hwang and Li's scheme, this scheme has much computation cost. It is inefficiency. Therefore, Sun proposed an efficient improvement of Hwang-Li scheme. The Sun's scheme is shown as the next subsection.

2.2 The Sun's Scheme

Registration Phase:
The registration phase in Sun's scheme is similar to that in the Hwang-Li scheme. However, there are two differences: One is Sun assumes that h is a one-way function with an output of 64 bits, and the other is

$$PW_i = h(ID_i, x_s). \tag{3}$$

Login Phase:
After a user keys in his/her ID_i and PW_i, the smart card will perform the following tasks:

1. Calculate $C_1 = h(T \oplus PW_i)$, where T is the current date and time by the input device.

2. Send the message $C = (ID_i, C_1, T)$ to the server.

Authentication Phase:
After receiving the message C from U_i, the server verifies the login user as follows:

1. Steps 1 and 2 are the same as those in the Hwang-Li's scheme.

2. Calculate $PW_i = h(ID_i, x_s)$ and $C_1' = h(T \oplus PW_i)$. Then compare C_1 with C_1'; if they match, the login user U_i is verified and is permitted access the server.

Since the Sun's scheme only uses one-way hash function, it reduces much more computation cost in Hwang-Li scheme. Therefore, this scheme is much more efficient than Hwang and Li's scheme. However, Hwang-Li scheme and Sun's scheme have the same weakness that the users are not allowed to freely choose and change their passwords. In this paper, we propose a new scheme to remedy it in the following section.

III Our Scheme

In this section, we shall depict our new simple, efficient remote user authentication scheme using smart cards. Unlike the Hwang-Li's scheme and Sun's scheme, our new scheme allows users to freely choose and change their passwords. In addition, the security is also based on one-way function, which is the same as Sun's scheme.
Registration Phase:
This phase is completed by the registration center, whose main task is to deliver a smart card to each registered user. When a user U_i wants to register with the server, U_i first chooses his/her own password PW_i and then computes $h(PW_i)$, where h is a one-way function with an output of 64 bits. The user U_i submits his/her ID_i and $h(PW_i)$ to the server. Then the server computes PW_{1i} for U_i as follows:

$$PW_{1i} = h(ID_i \oplus x_s) \oplus h(PW_i). \tag{4}$$

Here x_s is a secret key for the server; and $\oplus$ denotes an exclusive operation. Then, the registration center stores PW_{1i} and h into the smart card. Finally, the smart card is delivered to the user by the registration center.
Login Phase:
To log in the server and access the resources, U_i first inserts his/her own smart card and keys in his/her (ID_i, PW_i). Afterwards, the smart card will perform the following tasks:

1. Calculate PW_{2i} $(= PW_{1i} \oplus h(PW_i) = h(ID_i \oplus x_s))$.

2. Calculate $C_1 = h(PW_{2i} \oplus T)$, where T is the current date and time.

3. Send the message $C = (ID_i, C_1, T)$ to the server.

Note that, in order to reduce computational cost, $h(PW_i)$ can be pre-computed and stored in the smart card.

Authentication Phase:

Upon receiving the message C from U_i, the server verifies the login user as follows:

1. Check the validity of ID_i. If it is incorrect, then the server rejects the login user U_i.

2. Check the time interval between T and T', where T' is the time when the server receives the message from U_i. If $(T' - T) \geq \Delta T$, then the server rejects U_i. Here, ΔT denotes the expected legal time interval for transmission delay.

3. Check the equation

$$C_1 = h(h(ID_i \oplus x_s) \oplus T). \tag{5}$$

   If the above equation holds, the login user U_i is verified and is permitted access the server.

If the remote user wants to change his/her password, he/she only has to perform the procedures below:

1. Calculate $PW_{1i} \oplus h(PW_i) = h(ID_i \oplus x_s)$.

2. Select his/her new password PW_i' and then calculate $h(PW_i')$.

3. Calculate $PW_{1i}'(= h(ID_i \oplus x_s) \oplus h(PW_i'))$.

4. Store PW_{1i}' into his/her smart card in place of PW_{1i}.

In our scheme, we only use one-way hash function. It also reduces much more computation cost in Hwang-Li scheme. Furthermore, our new scheme allows users to freely choose and change their passwords to remedy the weakness of Hwang-Li and Sun's scheme.

IV Security Analysis

In this section, we analyze the security of our scheme as follows.

1. Due to the fact that the one-way function is computationally difficult to invert, it is extremely hare for the user U_i to derive the secret key x_s of the server from Equation (4). Even if the smart card of the U_i is picked up by an intruder, it is also difficult for the intruder to derive the x_s.

2. No one can forge a valid $C = (ID_i, C_1, T)$ because $C_1(= h(PW_{2i} \oplus T))$ can only be derived from PW_i and x_s.

3. The added time-stamp T prevents the replay attack. With the time-stamp, the system can check the correct time frame and prevent an intruder from replaying messages. To pass the authentication phase, an intruder must somehow change his/her T to match the requirement $(T' - T) \geq \Delta T$. However, if T is changed, Step 3 in the authentication phase cannot be passed unless C_1 has also been changed and x_s is know to the intruder, both of which seem out of the question.

4. In cases where a smart card is lost, no one can impersonate the smart card owner to login the server. The intruder will not know the user's password PW_i, and therefore he/she cannot compute PW_{2i}. The intruder cannot pass the authentication phase successfully. In addition, if an intruder (who picks up the smart card) only knows PW_{1i}; he/she still cannot derive x_s and PW_i.

In our scheme, we suppose the one-way function is secure. This function, $h : x \to y$, has the four properties [7, 8]. First, The function h can take a message of arbitrary-length input and produce a message digest of a fixed-length output. Second, since the function h is one-way, it is easy to compute $h(x) = y$ when given x. However, given y, it is hard to compute $h^{-1}(y) = x$. Third, The function h, given x, it is computationally infeasible to find $x' \neq x$ such that $h(x') = h(x)$. Fourth, The function h, it is computationally infeasible to find any two pair x and x' such that $x' \neq x$ and $h(x') = h(x)$.

V Efficiency

In this section, we compare Hwang-Li's scheme, Sun's scheme, and our scheme in terms of efficiency. In Hwang-Li's scheme, the security is based on the discrete logarithm problem, and P is as large as 1024 bits to make the puzzle unbreakable. In Sun's scheme and our scheme, on the other hand, the security is based on the one-way function with an output of 64 bits.

In Table 1, we list the efficiency comparison of Hwang-Li's scheme, Sun's scheme, and our scheme. It can be seen that Sun's scheme and our scheme are more efficient than Hwang-Li's scheme. And our scheme consumes one more hashing than Sun's scheme, computationally speaking, in the registration phase. However, our scheme can support users to freely choose and change their passwords.

Table 1: Comparison among Hwang-Li's scheme, Sun's scheme, and our scheme

	Hwang-Li's Scheme	Sun's Scheme	Our Scheme
Length of Password	1024 bits	64 bits	64 bits
Length of Transmitting in Login Phase*	2048 bits	64 bits	64 bits
Computations in Registration Phase	1 T_{Exp}	1 T_H	2 T_H
Computations in Login Phase	3 T_{Exp} +1 T_H	1 T_H	1 T_H
Computations in Authentication Phase	3 T_{Exp} +1 T_H	2 T_H	2 T_H
Computations in Change Password Phase	Not supported	Not supported	2 T_H
Public Information in Smart Card	(h, P)	h	h

*The non-cryptographic parameters ID_i and T are excluded from reckoning;
T_{Exp} denotes a time to compute an exponential operation;
T_H denotes a time to compute a one-way hash function.

VI Conclusions

In this article, we have proposed a simple and efficient remote user authentication scheme. Compared with our scheme, the Hwang-Li's scheme and Sun's scheme are not practical enough because they do not allow users to freely choose and change their passwords. The proposed scheme has succeeded in allowing a user to freely change and choose his/her password without significantly increasing the computation cost.

ACKNOWLEDGEMENTS

Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC90-2213-E-324-005.

References

[1] C. C. Chang and W. Y. Liao, "A remote password authentication scheme based upon ElGamal's signature scheme," *Compuper & Security*, vol. 13, no. 2, pp. 137–144, 1994.

[2] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 138, pp. 165–168, May 1991.

[3] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng, "A modified remote login authentication scheme based on geometric approach," *The Journal of System and Software*, vol. 55, pp. 287–290, 2001.

[4] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469–472, July 1985.

[5] Min-Shiang Hwang, "Cryptanalysis of remote login authentication scheme," *Computer Communications*, vol. 22, no. 8, pp. 742–744, 1999.

[6] Min-Shiang Hwang and 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.

[7] R. C. Merkle, "One-way hash functions and DES," in *Advances in Cryptology, CRYPTO'89*, pp. 428–446, Lecture Notes in Computer Science, Vol. 435, 1989.

[8] M. Naor and M. Yung, "Universal one-way hash functions and their cryptographic applications," in *Proc. of the 21st STOC*, pp. 33–43, 1989.

[9] Hung-Min Sun, "An efficient remote use authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 958–961, 2000.

[10] T. C. Wu, "Remote login authentication scheme based on a geometric approash," *Computer Communications*, vol. 18, no. 12, pp. 959–963, 1995.

BIOGRAPHY

Cheng-Chi Lee received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999 and in 2001. He is currently pursuing his Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, Republic of China. His current research interests include information security, cryptography, and mobile communications.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from

1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.

Wei-Pang Yang was born on May 17, 1950 in Hualien, Taiwan, Republic of China. He received the B.S. degree in mathematics from National Taiwan Normal University in 1974, and the M.S. and Ph.D. degrees from the National Chiao Tung University in 1979 and 1984, respectively, both in computer engineering.

Since August 1979, he has been on the faculty of the Department of Computer Science and Information Engineering at National Chiao Tung University, Hsinchu, Taiwan. In the academic year 1985-1986, he was awarded the National Postdoctoral Research Fellowship and was a visiting scholar at Harvard University. From 1986 to 1987, he was the Director of the Computer Center of National Chiao Tung University. In August 1988, he joined the Department of Computer and Information Science at National Chiao Tung University, and acted as the Head of the Department for one year. Then he went to IBM Almaden Research Center in San Jose, California for another one year as visiting scientist. From 1990 to 1992, he was the Head of the Department of Computer and Information Science again. His research interests include database theory, database security, object-oriented database, image database, and Chinese database retrieval systems.

Dr. Yang is a senior member of IEEE, and a member of ACM. He was the winner of the 1988, and 1992 AceR Long Term Award for Outstanding M.S. Thesis Supervision, 1993 AceR Long Term Award for Outstanding Ph. D. Dissertation Supervision, and the winner of 1990 Outstanding Paper Award of the Computer Society of the Republic of China. He also obtained the Outstanding Research Award of National Science Council of the Republic of China.