A NEW REMOTE USER AUTHENTICATION SCHEME USING SMART CARDS

Min-Shiang Hwang [0]   Li-Hua Li

Department of Information Management
Chaoyang University of Technology
168, Gifeng E. Rd., Wufeng,
Taichung County, TAIWAN 413, R.O.C.
Fax: 886-4-3742337
Email: mshwang@mail.cyut.edu.tw
http://www.cyut.edu.tw/∼mshwang/

Abstract

In this article, we propose a new remote user authentication scheme using smart cards. The scheme is based on the ElGamal's public key cryptosystem. Our scheme does not require a system to maintain a password table for verifying the legitimacy of the login users. In addition, our scheme can withstand message replaying attack.

Index Terms: Authentication, cryptography, data security, password.

1 INTRODUCTION

In 1981, Lamport [5] proposed a remote password authentication scheme with insecure communication. His scheme can withstand replaying attacks, but it needs a password table for verifying the legitimacy of the login users. This scheme may cause problem if intruders can modify the passwords stored in the password table of the system. Later, Hwang et al. [2] proposed an authentication scheme using smart cards. Their scheme is based on the Shamir's ID-based signature scheme. In 1995, Wu proposed an efficient remote login authentication scheme [8] which is based on simple geometric properties on the Euclidean plane. Unfortunately, the scheme is weakness in the security [4].

In this article, we propose a new remote user authentication scheme using smart cards. The scheme is based on ElGamal public key cryptosystem [1, 3]. The new scheme not only can withstand against message replaying attacks but can perform remote user authentication without using a password table. Before describing the proposed scheme, we first briefly review the ElGamal public key scheme as follows.

2 ELGAMAL'S PUBLIC KEY CRYPTOSYSTEM

There are two public parameters, P and g, in the ElGamal public key cryptosystem. P is a large prime number and $(P-1)$ has a large prime factor; g is the primitive element in Galois field $GF(P)$ [6, 7]. Each user U_i has a secret key x_i ($x_i \in [1, P-2]$) and a public key y_i, where $y_i = g^{x_i} \bmod P$. If user A wants to send a message M to user B. User A selects a random number r ($r \in [1, P-1]$) and calculates

$$C_1 = g^r \bmod P. \tag{1}$$

User A then uses the public key y_b of user B and the random number r to encipher the message M as follows:

$$C_2 = M(y_b)^r \bmod P. \tag{2}$$

[0]Responsible for correspondence.

The order pair (C_1, C_2) is transmitted to user B and the random number r is kept secret by user A. User B can decipher (C_1, C_2) to get the plain-text M as follows:

$$M = C_2(C_1^{x_b})^{-1} \bmod P. \tag{3}$$

3 OUR SCHEME

The new remote user authentication scheme can be divided into three phases: the registration phase, the login phase, and the authentication phase. Before accessing a remote system, a new user should submit his/her identity to the system in the registration phase. The system (registration center) will give the new user a smart card and a password through a secure channel. When a legal user wants to login the computer system, he/she has to insert his/her smart card into the login device and keys in his/her identity and password.

Registration phase: Suppose that a new user U_i submits his ID_i to the system for registration. The system calculates the password PW_i for the user U_i as follows:

$$PW_i = ID_i^{x_s} \bmod P, \tag{4}$$

where x_s is a secret key maintained by the system. The registration center issues a smart card, which contains the public parameters (f, P), where f is a one-way function. The registration center is also delivered PW_i to the user through a secure channel. The smart cards possessed by all users will contain the same data and functions, i.e., (f, P).

Login phase: Upon login, U_i attaches his smart card to his input device. Then he keys in his ID_i and the password PW_i to the device. The smart card will perform the following operations:

1. Generate a random number r.
2. Compute $C_1 = ID_i^r \bmod P$.
3. Compute $t = f(T \oplus PW_i) \bmod (P - 1)$, where T is the current date and time of the input device. And $\oplus$ denotes an exclusive operation.
4. Compute $M = ID_i^t \bmod P$.
5. Compute $C_2 = M(PW_i)^r \bmod P$.
6. Send a message $C = (ID_i, C_1, C_2, T)$ to the remote system.

Authentication phase: After receiving the authentication message C, the system authenticate the login user using the following steps. Suppose that the system receives the message C sent from the user U_i at T', where T' is the current date and time of the system.

1. Test the validity of ID_i. If the format of ID_i is incorrect, then the system rejects the login request.
2. Test the time interval between T and T'. If $(T' - T) \geq \Delta T$, where ΔT denotes the expected legal time interval for transmission delay, then the system rejects the login request.
3. If $C_2(C_1^{x_s})^{-1} \bmod P = (ID_i)^{f(T \oplus PW_i)}$, then the system accepts the login request. Otherwise, it rejects the login request.

4 SECURITY ANALYSIS

Because the scheme is based on the ElGamal public key scheme, it is very difficult for the user U_i to compute the secret key of the system from the equation $PW_i = (ID_i)^{x_s} \bmod P$. Also it is difficult for an intruder to obtain the system generated random number r directly from the equation $C_1 = (ID_i)^r \bmod P$ of step 2 in the login phase. The difficulty relies on the complexity of computing discrete logarithms over finite fields [1].

In order to pass the test of step 2 in the authentication phase, the intruder must change T into a new time T^* such that $(T'' - T^*) \leq \Delta T$ where T'' is the time when the system receives the illegal login message. Once T is changed, the test of step 3 in the authentication phase is failure unless either t or C_2 has been changed accordingly. Therefore, the proposed scheme is secure to withstand the replaying attack.

5 CONCLUSION

We have proposed a remote user authentication scheme without using a password file or a verification table. Our scheme can withstand the attack of replaying a previously intercepted login request message. The security of the scheme relies on the difficulty of computing discrete logarithms over finite fields.

ACKNOWLEDGEMENTS

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC86-2621-E-324-001-T.

References

[1] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory 31 (1985) 469–472.

[2] T. Hwang, Y. Chen, and C.S. Laih, Non-interactive password authentications without password tables, IEEE Region 10 Conference on Computer and Communication Systems, IEEE Computer Society, 1990 pp. 429–431.

[3] M.S. Hwang, A remote password authentication scheme based on the digital signature method, International Journal Of Computer Mathematics 70 (1999) 657-666.

[4] M.S. Hwang, Cryptanalysis of a remote login authentication scheme, Computer Communications 22 (8) (1999) 742-744.

[5] L. Lamport, Password authentication with insecure communication, Communications of ACM 24 (1981) 770–772.

[6] H.E. Rose, A course in number theory, Clarendon Press, Oxford, (1988).

[7] M. R. Schroeder, Number theory in science and communication, 2'nd edition, Springer-Verlag, (1985).

[8] T.C. Wu, Remote login authentication scheme based on a geometric approach, Computer Communications 18 (12) (1995) 959–963.

BIOGRAPHICAL SKETCHES

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 is currently the Associate Professor and Head of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. Dr. Hwang's current research interests include database and data security, cryptography, image compression, and mobile communications.

Li-Hua Li received her M.S. and Doctoral degree of Computer Science from the University of Alabama in 1991 and 1995, respectively. Her working experience includes working as a research assistant in the Flight Test Department of Aeronautical Industrial Development Center (AIDC) which is a research center of Chung-Shan Institute of Science and Technology (CSIST) under the National Defense Department from 1986 to 1989, the head of the Information Management (IM) Department of Chaoyang University of Technoloty (CYUT) from Aug. 1997 to July 1999 , and the associate professor of the IM Department of CYUT from 1995 to present. The research areas of Dr. Li include fuzzy applications, especially in the areas of fuzzy decision making and fuzzy expert systems, neural network application, and the security topics in electronic commerce.