PERGAMON

Mathematical and Computer Modelling 36 (2002) 103–107

MATHEMATICAL
AND
COMPUTER
MODELLING

www.elsevier.com/locate/mcm

A Simple Remote User Authentication Scheme

MIN-SHIANG HWANG
Department of Information Management
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng
Taichung County, Taiwan 413, R.O.C.
mshwang@cyut.edu.tw

CHENG-CHI LEE
Department of Computer and Information Science
National Chiao-Tung University
1001 Ta Hsueh Road
Hsinchu 300, Taiwan, R.O.C.
cclee@cis.nctu.edu.tw

YUAN-LIANG TANG
Department of Information Management
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng
Taichung County, Taiwan 413, R.O.C.

(Received January 2002; accepted February 2002)

Abstract—In this article, we propose a simple remote user authentication scheme using smart cards. This scheme has the following features. First, it does not require any password or verification tables. Second, it can withstand the message replay attack. Third, any legal users can arbitrarily choose and change their own passwords at will. And finally, the password of a user is not revealed to the server. In addition, the computational costs of this scheme are less than those of any previously proposed schemes. © 2002 Elsevier Science Ltd. All rights reserved.

Keywords—Authentication, Cryptography, Password table, Security.

1. INTRODUCTION

In a computer network, if a user wants to log in to a remote server, he/she must submit his/her personal identity (ID) and password (PW) to the server. Once the ID and the PW match the corresponding pairs stored in the server's verification table, the user will be granted access to the server's facilities. However, there is a threat in such a process, that is, a legal user could be impersonated by an intruder who intercepts these messages from the network and then log in to the server later using the intercepted information. Even if the PW is encrypted during

The authors wish to thank the 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. NSC90-2213-E-324-005.

PII: S0895-7177(02)00106-1

communication, such an impersonation attack is still possible. This kind of attack is called the replay attack.

To overcome this problem, Lamport proposed a password authentication scheme [1]. However, one of the shortcomings of his method is that a verification table should be stored in the server in order to verify the legitimacy of a user. If an intruder can somehow break into the server, the contents of the verification table can be easily modified. Thus, Lamport's scheme fails for the modification attack, although he has solved the replay attack problem. Researchers such as Chien *et al.* [2], Horng [3], and Jan and Chen [4] have recognized this problem and proposed solutions in which the verification table is no longer required in the server.

Recently, many password authentication schemes using smart cards have been proposed by some researchers [5–10]. In these methods, the smart card is used to authenticate a legitimate user. Therefore, there is no need to store the verification or password table, which, as a consequence, trivializes the modification attack problem. To the replay attack problem, on the other hand, a timestamp is used as a solution. In [6], Chang and Wu proposed a remote password authentication scheme with a smart card based on the Chinese remainder theorem (CRT). In 1995, Wu [9] proposed a new remote log in authentication scheme based on the geometric Euclidean plane. The merits of the later scheme are its simplicity of geometry and the property that users can freely choose their own passwords. However, the scheme is insecure as indicated in [11].

In 1990, Yamaguchi *et al.* proposed a simple but efficient authentication system, SPLICE/AS [12]. However, the scheme is vulnerable to the guessing attack [13]. An attacker can obtain the password, private-key, and public-key of the user. In 1994, Chang and Liao [5] proposed a remote password authentication scheme based on El Gamal's signature scheme. However, this method has a drawback that users cannot freely choose their own passwords. A similar problem also occurs in the scheme proposed by Hwang *et al.* [8]. In 1999, Yang and Shieh proposed two timestamp-based and nonce-based password authentication schemes with smart cards [10]. The features of their approach are

(1) the server does not need the password or verification tables to authenticate the users, and
(2) the users can select and change their passwords freely, however, the users' passwords are to be revealed to the server in Yang and Shieh' scheme.

In this paper, we propose a simple remote user authentication scheme using smart cards. Our scheme has the following characteristics:

- password or verification tables are not required in the server;
- the replay attack problem is completely solved;
- any legal users can select and change their password freely;
- the password is not revealed to the server.

Note that this scheme allows users to select and change their passwords without revealing them to the server. In other words, only the users know their passwords, and the server does not. In fact, the users can prove their legitimacy to the server without revealing the passwords. This concept is similar to the zero-knowledge proof [14].

The rest of the paper is organized as follows. In the next section, we shall describe our approach in detail. In Section 3, the proposed scheme will be analyzed with respect to its security, and finally, some brief conclusions will be given in Section 4.

2. THE PROPOSED SCHEME

Like other smart-card-based authentication schemes, our scheme is comprised of three phases: registration, log in, and authentication.

REGISTRATION PHASE. The registration process is accomplished by the registration center, whose main task is to release a smart card to the registering user. When a user U_i wants to register with the server, he/she first chooses a password PW_i, and then computes $f(\mathrm{PW}_i)$, where f is a one-way function which generates an integer of 1024 bits in length. U_i thus, submits his/her ID_i and $f(\mathrm{PW}_i)$ to the registration center. After receiving $(\mathrm{ID}_i, f(\mathrm{PW}_i))$, the center computes PW_{1i} for the U_i using the following equation:

$$\mathrm{PW}_{1i} = f(\mathrm{ID}_i \oplus x_s) \oplus f(\mathrm{PW}_i), \tag{1}$$

where x_s is the server's secret key and $\oplus$ denotes the exclusive operation. Then the registration center stores PW_{1i} and $f(\cdot)$ into the smart card. The smart card is then released to U_i.

LOG IN PHASE. To access a server, U_i first inserts his/her smart card and keys in his/her $(\mathrm{ID}_i, \mathrm{PW}_i)$ via a client device. Afterwards, the smart card performs the following computations.

1. Calculate $\mathrm{PW}_{2i}(= \mathrm{PW}_{1i} \oplus f(\mathrm{PW}_i) = f(\mathrm{ID}_i \oplus x_s))$.
2. Calculate $L = f(\mathrm{PW}_{2i} \oplus T)$, where T is the timestamp which is the current date and time.
3. Send the messages (ID_i, L, T) to the server.

Note that, in order to reduce the computational cost, $f(\mathrm{PW}_i)$ can be computed and stored in the smart card in advance.

AUTHENTICATION PHASE. Upon receiving the messages (ID_i, L, T) from U_i, the server verifies the user as follows.

1. Check the validity of ID_i. If it is incorrect, U_i is rejected.
2. Check the time interval between T and T', where the T' is the time when the server receives the messages from U_i. If $(T' - T) \geq \Delta T$, then the server rejects U_i. ΔT denotes the predetermined legal time interval of transmission delay.
3. Check the equality:

$$L = f(f(\mathrm{ID}_i \oplus x_s) \oplus T). \tag{2}$$

If it holds, U_i is authenticated and access to the server is granted.

If U_i wants to change his/her password, the following procedure is performed.

1. Calculate $\mathrm{PW}_{1i} \oplus f(\mathrm{PW}_i)(= f(\mathrm{ID}_i \oplus x_s))$.
2. Select a new password PW'_i and then calculate $f(\mathrm{PW}'_i)$.
3. Calculate $\mathrm{PW}'_{1i}(= f(\mathrm{ID}_i \oplus x_s) \oplus f(\mathrm{PW}'_i))$.
4. Store the PW'_{1i} into the smart card in place of PW_{1i}.

3. SECURITY ANALYSIS

Since the server's secret key x_s is protected by the one-way function $f(\cdot)$, it is computationally infeasible for the user to derive x_s. Even if the user loses the smart card, anyone who picks it up will still have to face the same problem.

The time-stamp T prevents the replay attack. With the time-stamp, the server is able to pinpoint an intruder who replays a message. To pass the authentication phase, the intruder must change T in order to satisfy $(T' - T) \geq \Delta T$. However, if T is changed, then Step 3 in the authentication phase cannot be passed unless L is also changed and x_s is known to the intruder, which does not seem possible at all.

In case the user loses his/her smart card, impersonation is also impossible. Since the intruder does not know the password PW_i of the smart card's owner, he/she cannot compute PW_{2i}. He/she will fail in the authentication phase. Even if the intruder (who picks the smart card up) has $\mathrm{PW}_1 i$, he/she still has difficulty deriving x_s and PW_i because both of them are protected by the one-way function.

4. CONCLUSIONS

In this article, we have proposed a simple remote user authentication scheme that is able to protect the system against both the modification attack and the replaying attacks. The system is further protected by not having to reveal the password to the server. In addition, the user has the freedom to choose and/or change the password arbitrarily.

Besides all the above merits, we call our scheme "simple" because it requires much fewer computations than other schemes as in [2,8,4,10]. Table 1 gives brief comparisons among various methods in registration, log in , authentication, and change password phases. In registration and authentication phases, our scheme requires $2(T(f)+T(\oplus))$ operations. In log in and change password phases, our scheme requires $T(f)+2T(\oplus)$ operations. It is obvious that our scheme is the most efficient one.

Table 1. Comparisons of computation costs.

	Registration	Log In	Authentication	Change Password

Our Scheme	2T(f)
	2T($\oplus$)
		1T(f)
		2T($\oplus$)
			2T(f)
			2T($\oplus$)
				T(f)
				2T($\oplus$)

Chien-Jan-Tseng Scheme [2]	3T(f)
	2T(M)
	2T(D)
	2T(A)
		2T(f)
		1T($\oplus$)
		2T(D)
		1T(A)
			3T(f)
			2T(M)
			1T($\oplus$)
				Not Supported

Hwang-Li Scheme [8]	1T(ME)	1T(f)
		3T(ME)
		1T($\oplus$)
		1T(MM)
			1T(f)
			2T(ME)
			1T(MM)
			1T($\oplus$)
				Not Supported

Yang-Shieh Scheme [10]	3T(ME)
	2T(MM)
		1T(f)
		2T(ME)
		3T(MM)
			1T(f)
			1T(M)
			2T(E)
				1T(ME)
				1T(MM)

Jan-Chen Scheme [4]	1T(f)
	1T(ME)
	1T(SE)
		1T(f)
		3T(ME)
		2T($\oplus$)
		1T(MM)
		1T(SE)
			2T(ME)
			1T(MM)
			2T(SE)
			2T($\oplus$)
				Not Supported

Wu Scheme [9]	3T(f)
	2T(M)
	2T(D)
	1T(A)
		2T(f)
		2T(D)
		2T(A)
			3T(f)
			2T(M)
			1T(A)
				Not Supported

T(): Computation Time; MM: Modular Multiplication; ME: Modular Exponentiation; f: One-way Function; M: Multiplication; D: Division; A: Addition operation; $\oplus$: Exclusive-OR operation; SE: Symmetric Encryption; E: Exponentiation.

REFERENCES

1. L. Lamport, Password authentication with insecure communication, *Communications of the ACM* **24**, 770–772, (November 1981).
2. H.-Y. Chien, J.-K. Jan and Y.-M. Tseng, A modified remote log in authentication scheme based on geometric approach, *Journal of System and Software* **55**, 287–290, (2001).
3. G. Horng, Password authentication without using password table, *Information Processing Letters* **55**, 247–250, (1995).
4. J.K. Jan and Y.Y. Chen, 'Paramita wisdom' password authentication scheme without verification tables, *The Journal of Systems and Software* **42**, 45–57, (1998).
5. C.C. Chang and W.Y. Liao, A remote password authentication scheme based upon El Gamal's signature scheme, *Computer & Security* **13** (2), 137–144, (1994).
6. C.C. Chang and T.C. Wu, Remote password authentication with smart cards, *IEEE Proceedings* **138**, 165–168, (May 1991).

7. M.-S. Hwang, A remote password authentication scheme based on the digital signature method, *International Journal of Computer Mathematics* **70**, 657–666, (1999).
8. M.-S. Hwang and L.H. Li, A new remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics* **46** (1), 28–30, (2000).
9. T.C. Wu, Remote log in authentication scheme based on a geometric approach, *Computer Communications* **18** (12), 959–963, (1995).
10. W.H. Yang and S.P. Shieh, Password authentication schemes with smart cards, *Computers & Security* **18** (8), 727–733, (1999).
11. M.-S. Hwang, Cryptanalysis of remote log in authentication scheme, *Computer Communications* **22** (8), 742–744, (1999).
12. S. Yamaguchi, K. Okayama and H. Miyahara, Design and implementation of an authentication system in WIDE Internet environment, In *Proceedings of IEEE Region Conference on Computer and Communication System*, (1990).
13. M.-S. Hwang, C.-C. Lee and Y.-L. Tang, An improvement of SPLICE/AS in WIDE against guessing attack, *International Journal of Informatica* **12** (2), 297–302, (2001).
14. O. Goldreich, *Modern Cryptography, Probabilistic Proofs and Pseudo-Randomness*, Springer Verlag, (1999).