Cryptanalysis of a smart card based secure password authentication scheme

Fuw-Yi Yang Wen-Hui Li
Department of Computer Science and Information Engineering,
Chaoyang University of Technology
yangfy@cyut.edu.tw s9627641@cyut.edu.tw

Abstract

Recently, Wang and Chang proposed a password authentication scheme is embedded in a smart card. This new verifier authenticates the login password key in without password table adoption. The safety aspects for this protocol were constructed on the basis of intensity factors and discrete logarithm. Nonetheless, in the year of 2008, Yoon et al. pointed out that there was a security loophole within the Wang and Chang's proposed, prone to two attacks like impersonation and offline password guessing. In this paper, we analyzed that the proposed from Wang and Chang did have security loopholes. Suppose an attacker proceeds to compute the Modular Exponentiation at both sides of the authentication programs, with intercepted logon information, the attacker can establish new logon information with a successful penetration into the server system.

Keywords: Password authentication, Smart card, Impersonate attack, Off-line password guessing attack.

1. Introduction

In the traditional password authentication scheme proposed, each user must register with a set of personal *ID* and password *PW* from the remote server so as to be used for later logon. And after the registration completion at server, user *ID* and password *PW* are saved within the authentication table. Nevertheless, if the attacker can penetrate inside the server, he can easily acquire the confidential information of the user. In order to enhance and correct the drawbacks of this proposed, many researches proposed enhancements [1] [2] so as to protect the passwords being acquired by the attackers. The enhancements are as follow: (1) Through the deployment of one-way hash function, *PW* protection can be achieved and stored inside the authentication table. (2) Employ the Public-Key Cryptosystems or Symmetric Cryptosystem to transmit the passwords via the encoded methods so as to impede the attackers from easily acquiring the *PW*. Even the attacker knows the contents of authentication table, he still cannot easily acquire the *PW*. Since the attacker cannot acquire the decoding key, only the preapproved recipient can decode the received encoded text. Nonetheless, these enhanced password authentication

scheme proposed still have a few problems: (1) Attackers can employ one-way hash function to protect his *PW* in addition to append it to the authentication table. (2) When many users log on the connected network, the authentication table must be expanded as well, therefore the management for the authentication table and the loading for servers would become complex. (3) Attackers can stop the legal user from changing password.

Based on the above security concerns for the password authentication scheme proposed, in the year of 1996, Wang and Chang proposed a password authentication scheme is embedded in a smart card. It allowed users with freedom in selecting passwords during registration. In addition, the server does not require authentication table prior authenticating the logon messages. This proposed united the signature proposed from Elgamal [4] and signature proposed based on identity from Shamir [5]. In the area of security protocol, it was based on the polynomial factoring and the discrete log solution and could protect the repetitive attack trials with timestamp.

In 2001, Chan and Chang [6] pointed out that the Wang and Chang proposed still could not prevent repetitive trial attacks, if the attacker recorded the effective logged on messages previously in addition to forge a timestamp, then on the next logon to the system, he could then retransmit prior to logon the system for service.

In 2008, Yoon et al. [7] analyzed the proposed from Wang and Chang, it was found with the existence of fake attack and offline password guessing attack. Fake attack, derived from the lack of true identity authentication for the user, all it takes is to have the attacker acquire the timestamp and then he can easily logon with pretending as the preapproved user. In the password guessing attack, the attacker can guess the password and confirm until the confirmation is successful within the timeframe allotted by the polynomial, then the attacker can acquire the preapproved user's password. In this paper, we analyzed Wang and Chang's proposed and found a safety loophole instead. If the attacker can execute the Modular Exponentiation at both sides of the authentication programs in addition to intercepting the logon information, then the attacker can establish new login information and successfully logon the server system.

2. Review of Wang-Chang's scheme

There are three phase in Wang-Chang's smart card based password authentication scheme: registration, login and verification phase. Assume the existence of a trusted key generation center (KGC) to issue personalized smart card to users when joining the system. Initially, the KGC sets up the following parameters:

- p, q, n : p and q are two large primes, and $n = pq$.
- e: a prime number, the system's public key.

- d: the system's secret key, such that $ed = 1 \bmod (p-1)(q-1)$.
- g: a primitive element in both GF(p) and GF(q).
- $f(\cdot)$: a one-way hash function pre-stored on smart card.

2.1 Registration phase

Suppose that a new user U_i registers with the system.

1. U_i submits his user identification ID_i and his preferred password PW_i to the KGC.
2. Upon receiving the registering request, the KGC selects a random number k_i, such that gcd(k_i, (p-1)(q-1))=1.
3. The KGC then computes $\alpha_i = g^{k_i} \bmod n$ and $h_i = \alpha_i^{b_i} \bmod n$, where b_i satisfies the relation.

$$ID_i = ePW_i + k_i b_i \bmod ((p-1)(q-1))$$

and U_i's secret key S_i by

$$S_i = (g^{ID_i})^d \bmod n$$

The number p, q, k_i, b_i, and d must be kept secret in the KGC. The KGC writes the other number (e, n, g, S_i, h_i) into the memory of a smart card and security issues the card to U_i. It is assumed that S_i and h_i cannot be read directly from the memory of the smart card, and k_i and b_i are kept secret by the KGC.

2.2 Login phase

1. User U_i wishes to enter the network; he must first insert his smart card into a reader, then key in his ID_i and PW_i into a terminal.
2. The smart card generates a random number r_i and computes

$$x_i = h_i g^{er_i} \bmod n$$

and

$$y_i = (S_i g^{r_i - PW_i})^{f(x_i, T)} \bmod n$$

where T is the current login time used as a timestamp.

3. The login request $M = \{e, x_i, y_i, T\}$ is then sent to the remote host.

2.3 Authentication phase

When at time T^* the host computer receives a message M from U_i, the time T^* is first recorded.

1. The remote host first verifies if the time difference between T and T^* is within a legal range. If not, the login request is rejected.
2. The remote host then checks whether the following equation holds:

$$y_i^e \stackrel{?}{=} x_i^{f(x_i, T)} \bmod n$$

The equation holds the login request is valid and accepted; otherwise, the login request is rejected.

3. Cryptanalysis of Wang-Chang's scheme

We analyze Wang-Chang's smart card

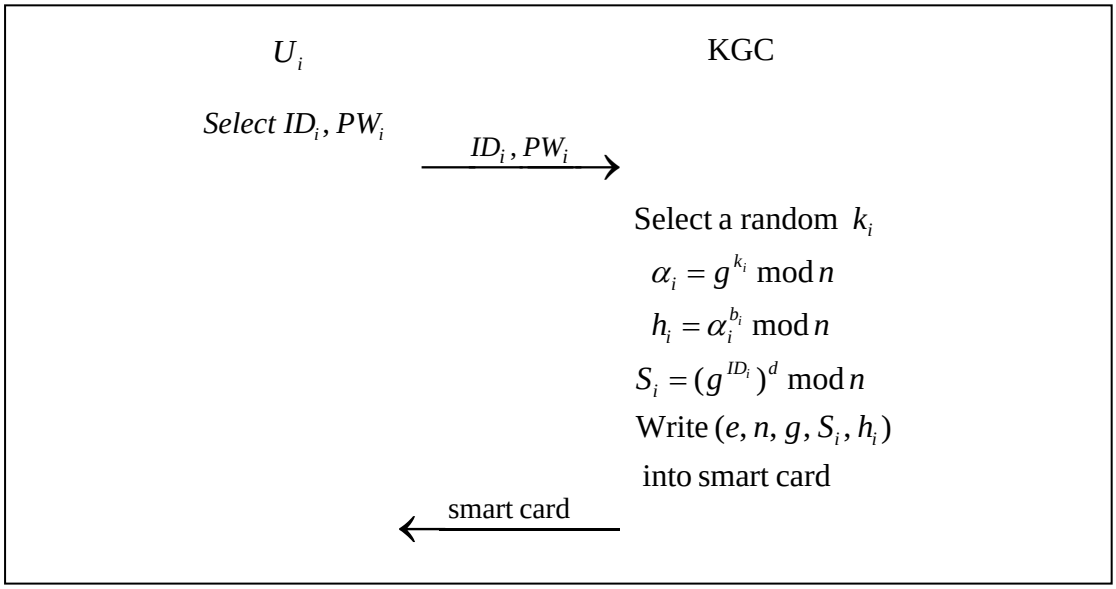

Fig. 1. Registration phase of Wang-Chang's scheme

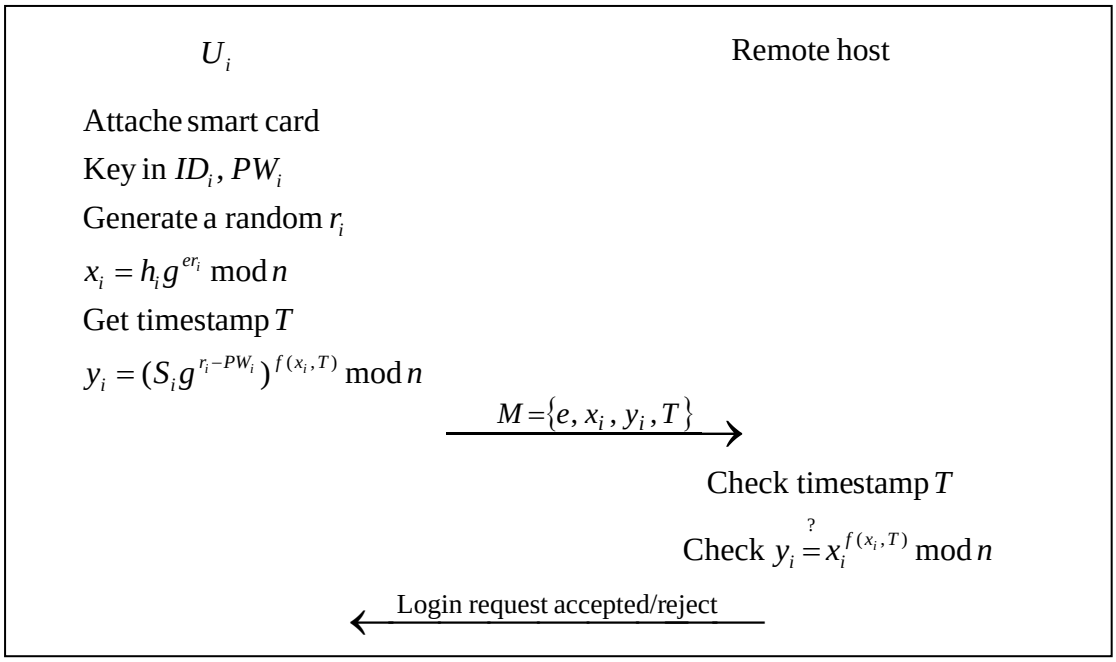

Fig. 2. Login and authentication phase of Wang-Chang's scheme

based password authentication scheme, it was found with security loophole as well. If the attacker can execute the Modular Exponentiation at both sides of the authentication programs in addition to intercepting the logon information, then the attacker can establish new login information and successfully logon the server system. And the attack simulation is as follow:

1. Derive from the authentication equation:

$$y_i^e = x_i^{f(x_i, T)} \bmod n$$

Proved that $x_i = y_i = 1$ or $x_i = y_i = 0$, will always satisfy the authentication equation.

2. Execute the Modular Exponentiation at both sides of the authentication programs:

$$y_i^{e \cdot a} = x_i^{a \cdot f(x_i, T)} \bmod n$$
$$(y_i^a)^e = (x_i^{f(x_i, T)})^a \bmod n$$

Therefore after intercepting the logon information $\{e, x_i, y_i, T\}$ then new logon information can be established $\{e, x_i', y_i', T'\}$ as follow:

(1) T' is the logon timestamp.

(2) $x_i' = x_i^{f(x_i, T)} \bmod n$

(3) $a = f(x_i', T')$

(4) $y_i' = y_i^a \bmod n$

Then the new logon information $\{e, x_i', y_i', T'\}$ can be registered inside the server system.

Proof:

$$(y_i^a)^e = (x_i^{f(x_i, T)})^a \bmod n$$

$$\begin{aligned} \Rightarrow (x_i^{f(x_i, T)})^a &= (((g^{ePW_i + k_i b_i})^d \cdot g^{r_i - PW})^a)^{e \cdot f(x_i, T)} \bmod n \\ &= (((g^{ePW} \cdot g^{k_i b_i})^d \cdot g^{r_i - PW})^a)^{e \cdot f(x_i, T)} \bmod n \\ &= (((g^{k_i b_i})^d \cdot g^{r_i})^a)^{e \cdot f(x_i, T)} \bmod n \\ &= (g^{k_i b_i} \cdot g^{er_i})^{a \cdot f(x_i, T)} \bmod n \\ &= (h_i \cdot g^{er_i})^{a \cdot f(x_i, T)} \bmod n \end{aligned}$$

From the above proof, we can learn that executing the Modular Exponentiation at both sides of the authentication programs, the remote server can authenticate its information and takes in as preapproved; hence, as long as the attacker logs on with proper information he can establish new login information as well as login the server system.

4. Conclusion

We pointed out a security loophole at Wang-Chang proposed, which is that the attacker can execute Modular Exponentiation at both sides of the authentication programs, in addition that after intercepting the logon information, he can establish new logon information and successfully log into the server system. Thus, Wang-Chang proposed cannot provide adequate security and is not suitable for practical implementation of the proposed.

References

[1] A. Jr Evans, W. Kantrowitz and E. Weiss, A user authentication system not requiring secrecy in the computer, ***Communications of the ACM***, 17(1974) 437-442.

[2] R.E. Lennon, S.M. Matyas and C.H. Meyer, Cryptographic authentication of time-invariant quantities, ***IEEE Transactions on Communications***, COM-29, 6 (1981) 773-777.

[3] S.J. Wang and J.F, Chan, "Smart card based secure password authentication scheme", ***Computers and Security***, Vol. 15, No. 3, 1996, pp. 231-237.

[4] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", ***IEEE Transactions on Information Theory***. Vol. IT-31, No. 4, 1985, pp. 469-472.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes", ***in: Proc. CRYPTO '84, Lecture Notes in Computer Science***, Vol. 196, Springer, Berlin, 1985, pp. 47-53.

[6] C.K. Chan and L.M. Cheng, "Remarks on Wang-Chang's password

authentication scheme", ***Electronics Letters***, Vol. 37, No. 1, 2001, pp. 22-23.

[7] Eun-Jun Yoon and Kee-Young Yoo, "Breaking a Smart Card based Secure Password Authentication Scheme", ***International Conference on Information Security and Assurance***, 2008, pp. 83-86.