Cryptanalysis of Password Authentication Scheme Using Smart Cards

Sattar J Aboud
Department of Information Technology
Iraqi Council of Representative

Abid T. Al Ajeeli
Department of Information Technology
Iraqi Council of Representatives

Abstract

In this paper, we review two password schemes that use a smart card. The schemes verify the logon password without a password file. Both schemes are based on the idea of integer factoring and discrete logarithm problem. Also, we describe some schemes that indicated that there are two security problems in these password-typed smart card schemes: impersonation and offline password guessing attack. Then, we analyze the protection defenseless of the schemes. Assume that the hacker manages to calculate the modular exponentiation on both sides of the password schemes, with intercepted retrieve request, the hacker can create new access request with a successful entry into the remote server.

Keywords*: Password scheme, smart card, impersonate attack, offline guessing attack.*

1. Introduction

In the conventional password scheme, every user should register a pair of user identification id and password w with the computer server C so that it is employed for later login. Then, after finishing the registration in computer server C, the user id and the password w are stored inside the password file. However, if a hacker gets access to the computer server C, he can easily obtain the secret information of a user. So, to improve and fix the shortcomings of the scheme many authors suggested improvements [1, 2, 3] in order to defend a password obtained by the hackers. The improvements are as follow:

1. During the use of secure one-way hash function password w protection can be attained and saved within the password file.
2. Use the public-key cryptography to send the passwords by the encrypted methods in order to obstruct the hackers from easily obtaining the password w. Even if the hacker knows the inside of a password file, he cannot definitely obtain the password w. Because the hacker cannot obtain the private key, just the accepted receiver can decrypt the received encrypted message.

However, these improved password schemes also have some difficulties:

1. Hackers can use the one-way hash function to secure his password w as well as to attach it to the password file.
2. If several users enter the linked network, the password file should be expanded too, so the organization of the password file and the loading for servers will become difficult.
3. Hackers can prevent the authorized user from altering password.

By using the above security, in 1996 Wang and Chang suggested a password scheme that is embedded in a smart card. It lets the user choose by picking a password through registration. Also, the computer server C does not need a password file before authenticating the retrieve message. This scheme combined the signature suggested by Elgamal [4] with a signature using identity from Shamir scheme [5]. In the field of security scheme, it was using the polynomial factoring and the discrete logarithm problem and protected the repetitive trail attack.

In 2001, Chan and Chang [6] indicated that the Wang and Chang scheme cannot stop repetitive trial attacks, when the hacker reported the operative logged on documents besides forging a timestamp On the subsequently login to the system, the hacker can then resend before login to the system for service.

In 2008, Yoon et al. [7] examined the Wang and Chang scheme. It was reported that with the continuation of forged attack and offline guessing forged attack that result from the lack of factual identity authentication for the user, the hacker can obtain the timestamp and after that he can easily login by pretending to be an accepted user. In the password guessing attack, the hacker can estimate the password and verify until the authentication is successful in the timeframe chosen by the polynomial, then the hacker can obtain the accepted user password.

In 2010, Al Sakib Khan Pathan [8] analyzed the Wang and Chang scheme He showed that the scheme which so far have been thought to be intractable is still flawed, in spite of their later improvements.

The rest of the paper is organized as follows: we first review the Shen et al. scheme in Section 2, and present our impersonation attacks against the scheme. In Section 3, we study Wang and Chang scheme and establish a protection embrasure instead. When the hacker can implement the modular exponentiation in both sides of the authentication formulas and in intercepting the login request, then the hacker can create new logon request and successfully login to the computer server C Finally, the conclusion is given in Section 4.

2. Review of Shen et al. Scheme

The Shen et al. password scheme [9] includes three phases: registration, login, and authentication. We now review each phase as follows.

2.1 Registration Phase

Suppose that a server C has the RSA scheme, the steps of the initialization phase are as follows:

1. select randomly two large prime numbers p and q are equally likely.
2. find $n = p * q$.
3. compute $\theta(n) = (p-1)(q-1)$.
4. choose a random prime number e.
5. find the scheme private key by $e * d \equiv 1 \bmod \theta(n)$ with $\gcd(e, \theta(n)) = 1$.
6. determine the public by (e, n) and private key by (d, θ).
7. select a secure one-way hash function h [10].
8. select a generator a in both $GF(p)$, $GF(q)$

When a user A wants to register with the server C, he first submits his identity id and a chosen password w to a server C by a secure channel. Then, the server C should do the following:

1. find $s = id^{d} \bmod n$
2. find $h_i = a^{w*d} \bmod n$
3. find $ic = h(id \oplus d)$ such that $\oplus$ denotes an exclusive operation, and ic is the card identity.
4. write $(n, e, a, h, id, ic, s, h_i)$ into a smart card
5. Pass the smart card to the user A.

2.2 Login Phase

When the user A wants to login into the server C, he must do the following:

1. inserts his smart card ic into a card reader
2. enters his identity id and password w.
3. if both id and w are valid, the smart card ic does the following:

1. selects a random number r,
2. finds $x = a^{r*w} \bmod n$
3. finds $y = s * h_i^{r*h(ic*T_1)} \bmod n$ where a timestamp T_1 represents a current date and time if this login occurs.
4. sends login request message $m{=}(id,ic,x,y,n,e,a,T_1)$ to a server C.

2.3 Authentication Phase

After the server receives the message $m = (id, ic, x, y, n, e, a, T_1)$, he must checks the validity of this login request message as follows:

1. finds $ic \equiv h(id \oplus d)$
2. finds $y^{e} \equiv id * x^{h(ic,T_1)} \bmod n$
3. finds $T_2 - T_1 \leq T_3$

Such that T_2 represents the date and time if a server C received the request m, and T_3 is a predefined time interval to balance a reasonable transmission delay and potential replay attack. If any of the above verifications fails, the login request is rejected. Otherwise, a server C finds $R = h(ic, T_2)^{d} \bmod n$, and then sends back message $m^{-} = (R, T_2)$ to a user A. Upon receiving message m^{-}, a user A accepts a server C service if and only if both of the following checks hold:

1. $R^{e} \equiv h(ic, T_2) \bmod n$
2. $T_4 - T_2 \leq T_5$ where T_5 denotes the date and time if A received message m^{-}.

2.4 Cryptanalysis of the Scheme

Now we show that the Shen et al. authentication scheme [9] is indeed insecure by presenting an impersonation attack, The attack can be mounted if the RSA public key e is a small prime number. The Shen et al. scheme just requires the RSA public key e but does not specify the size of e. If one may implement a Shen et al. scheme by selecting a small prime number as a value of e, for example, $3,7,13$ etc. This is likely to happen due to two reasons:

1. Some standards for example $PKCS\#1$ [10], recommend using a small exponent e such as 3 to speed up the RSA signature verification;
2. Small exponent e can reduce the computing cost of smart cards used in the Shen et al. scheme as the authentication devices for users.

However, if a public e is truly set as a small prime number, the Shen et al. scheme is vulnerable to the following impersonation attacks:

1. The hacker intercepts a login request message $m = (id, ic, x, y, n, e, a, T_1)$ over the communication channel.

2. The hacker checks if $h(ic,T_1)$ is divisible by e or not. If not, it intercepts more login request messages. Otherwise, it continues.
3. Suppose $h(ic,T_1) = e*b$ for some integer $b \in Z$. Then, find $S = y * x^{-b} \bmod n$.
4. For any timestamp T_1^-, the hacker selects a random number, and computes x^- and y^- as follows: $x^- = r^e \bmod n$, and $y^- = S * r^{h(ic,T_1^-)} \bmod n$
5. The hacker can impersonate user A to access the server by sending out a forged login information message $m^-(id, ic, x^-, y^-, n, e, a, T_1^-)$.

Therefore, an attack is successful if a forged login request message $m^- = (id, ic, x^-, y^-, n, e, a, T_1^-)$ can be delivered to a server C before $T_1^- \_ T_5$. This is not hard for the hacker, since this condition applies to each legal user as well. The only concern is a probability of $h(ic,T_1)$. Under an assumption that the outputs of hash function $h(.)$ are random numbers, it is easy to know $h(ic,T_1)$ for a random timestamp T_1 with probability of $1/e$. This implies that to successfully amount an attack, a hacker only needs to intercept a dozen of valid login messages on average if e is a prime less than 20.

Actually, $e = 65537 = 2^{16} + 1$ attack remains feasible in practice if a hacker eavesdrops thousands of valid login messages. However, note that if $|e| \geq 80$, it seems infeasible to amount this attack since each single run of the attacking algorithm with success probability only about 2^{-80}, a negligible quantity. This is the reason why we have to assume that e should be a small number in this attack.

3. Review of Wang and Chang Scheme

There are four phases in Wang and Chang smart card typed password scheme. These phases are: initialization phase, registration phase, login phase and verification phase. Suppose that the computer server C issues a tailored smart card to user once entering the system. Firstly, the computer server C sets up the initiation phase which is as follows:

3.1 Initialization Phase

By using RSA public key encryption scheme [10], the steps of the initialization phase are as follows:

1. select randomly two large prime numbers p and q are equally likely.
2. find $n = p*q$.
3. compute $\theta(n) = (p-1)(q-1)$.
4. choose a random prime number e which is the system public key.
5. find the system private key by $e*d \equiv 1 \bmod \theta(n)$ with $\gcd(e, \theta(n)) = 1$.
6. determine the public by (e,n) and private key by (d,θ).
7. select a secure one-way hash function h [11] resaved into smart card.
8. select a generator a in both $GF(p)$, $GF(q)$

3.2 Registration Phase

The steps of the registration phase are as follows:

Step 1: The user A

Assume that the new user A registers with the system. Then he should do the following:

1. select the identification id
2. select the password w
3. send identification id and password w to the computer server C.

Step 2: The Computer server C

The steps of the algorithm after receiving the registering information are as follows:

1. choose an arbitrary integer v where $\gcd(v, \theta(n)) = 1$.
2. find $z = a^v \bmod n$
3. compute $c = z^j \bmod n$, where j satisfies the formula $id = e*w + (v*j \bmod \theta(n))$.
4. compute $g = (a^{id})^d \bmod n$, where g is the private key of A
5. determine the private keys by (θ, v, j, d).
6. enter the values (e,n,a,g,c) in a smart card memory and issues the card to A.
7. suppose that g and c cannot be read directly from the memory of the smart card.
8. pass the smart card to the user A

3.3 Login Phase

The steps of the login phase are as follows:

Step 1: The user A

If the user needs to enter the system, he should do the following:

1. inserts the smart card into the reader
2. enters id and w from the screen.
3. generates an arbitrary integer u.

4. find $i = c * a^{e*u} \bmod n$.
5. obtains timestamp T .
6. finds $b = (g * a^{u-w})^{f(i*T)} \bmod n$, such that T is a present logon time used as a timestamp.
7. computes the logon information $m=(e,i,b,T)$
8. passes m to the computer server C .

3.4 Authentication Phase

The steps of the authentication phase are as follows:

Step 1: The Computer server C

If at time T^* the computer server C receives a message m from A . The following steps must be as follows:

1. insert the time T^* .
2. check if the time difference between T and T^* is in an allowed range. If not, the logon information is rejected.
3. verify if the formula $b^e \equiv i^{f(i*T)} \bmod n$. If yes the logon information is valid and accepted; else, the logon is rejected.
4. passes logon accepted or rejected to the user A .

3.5 Cryptanalysis of the Scheme

We analyzed Wang and Chang smart card typed password scheme. Some security defects were discovered in the scheme. When the hacker can implement the modular exponentiation in both sides of authentication formulas in addition to intercepting the login request, the hacker can then start a new logon request and successfully login to the computer server C . However, the attack will be as follows:

1. obtain from the authentication formula $b^e = i^{f(i_i,T)} \bmod n$.

   verify that $i = b = 1$ or $i = b = 0$ will satisfy the authentication formula.
2. perform the modular exponentiation in both sides of the authentication formulas:

   $b^{e*z} = i^{z*f(i,T)} \bmod n$,

   $(b^z)^e = (i^{f(i,T)})^z \bmod m$.

After intercepting the login request (e,i,b,T) , the new login request can be created (e',i,b',T') as follows:

1. T' is the login timestamp.
2. $i' = i^{f(i,T)} \bmod n$
3. $z = f(i',T')$
4. $b' = b^z \bmod n$

Then the new login request (e,i',b',T') can be requested inside the computer server C .

Correction:

$(b^z)^e = (i^{f(i,T)^z} \bmod n$

$= (i^{f(i,T)^z} = (((a^{e*w+v\ *j)^d} * a^{r-w)^z})^z)^{e*f(i,T)} \bmod n$

$= (((a^{e*w} * a^{v\ *j})^d * a^{u-w})^z)^{e*f(i,T)} \bmod n$

$= (((a^{v*j})^d * a^u)^z)^{e*f(i,T)} \bmod n$

$= (a^{v*j} * a^{e*u})^{z*f(i,T)} \bmod n$

$= (h\ * a^{e*u})^{z*f(i,T)} \bmod n$

According to the above correction, we can say that implementing the modular exponentiation in both sides of the authentication formulas, the computer server C can authenticate its request and takes in as accepted. However, if a hacker login with appropriate request he can create new logon request as well as logon to the computer server C .

4. Conclusions

We indicated that there is a security leak at Wang and Chang scheme which is that the hacker can implement modular exponentiation in both sides of authentication formulas, also after intercepting the login request, he can create a new login request and successfully logon to the computer server C . Therefore, Wang and Chang scheme cannot give sufficient security and is not appropriate for practical achievement of the scheme.

5. References

[1] Evans A., Kantrowitz W., and Weiss E., (1974) ‘A User Authentication System Not Requiring Secrecy in the Computer’, Communications of the ACM, 17, pp. 437-442.

[2] Lennon R., Matyas S., and Meyer C., (1981) ‘Cryptographic Authentication of Time-invariant Quantities’, IEEE Transactions on Communications, COM-29, 6, pp. 773-777.

[3] Wang and S., and Chan J., (1996) ‘Smart Card Based Secure Password Authentication Scheme’, Computers and Security, Volume 15, No. 3, pp. 231-237.

[4] Elgamal T, (1985) ‘A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms’, IEEE Transactions on Information Theory, Volume IT-31, No. 4, pp. 469-472.

[5] Shamir A., (1985) ‘Identity-Based Cryptosystems and Signature Schemes’, Proceeding of CRYPTO’84, Lecture Notes in Computer Science, Volume 196, Springer, Berlin, pp. 47-53.

[6] Chan C., and Cheng L., (2001) ‘Remarks on Wang-Chang’s Password Authentication Scheme’, Electronics Letters, Volume 37, No. 1, pp. 22-23.

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

[8] Al-Sakib Khan Pathan**,** (2010) 'A Review and Cryptanalysis of Similar Timestamp Based Password Authentication Schemes Using Smart Cards', International Journal of Communication Networks and Information Security (IJCNIS), Volume 2, No. 1, April 2010.

[9] [11] J.J. Shen, C.W. Lin, and M.S. Hwang (2003) 'Security enhancement for the timestampbased password authentication scheme using smart cards' Computers & Security, vol. 22, no. 7, pp. 591-595.

[10] [12] PKCS (2001) 'Public key cryptography standards, PKCS #1' v2.1, RSA Cryptography Standard, Draft 2,www.rsasecurity.com/rsalabs/pkcs/

[11] Rivest R., Shamir A., and Adleman L., (1978) 'A Method For Obtaining Digital Signature and Public-key Cryptosystems', Communication of ACM, Volume 21, No. 2, pp. 120-126.

[12] FIPS PUB 180-2, (2004) 'Secure Hash Standard, National Institute of Standards and Technology', US Department of Commerce.