Int. Computer Symposium, Dec. 15-17, 2004, Taipei, Taiwan.

Cryptanalysis of an anonymous user identification and key distribution scheme

Fuw-Yi Yang
Department of Electronics Engineering
Chien-kuo Technology University
E-mail:yangfy@ms7.hinet.net

Abstract-A scheme of anonymous user identification and key distribution was proposed by Wu and Hsu. This paper shows that their scheme is insecure to three attacks: a malicious responder can obtain the initiator's secret key, an adversary can impersonate a service provider, and an adversary can impersonate another legal user.

Keywords: Impersonation attack, identity protection, key agreement, user identification.

1. Introduction

The scheme of user authentication is used to distinguish an intruder from a legitimate user. Some of the early schemes authenticate users based on a password table [2]. The password table records the user's account and password for each registered user. As a user wants to login the system, he must enter his account and password. According to the content of the password table, the system can verify whether or not the user is a legal one.

Authentication using password table may cause problems. A user may deny having entered the system, because the user's password is stored inside the system and the user may argue that his password has been stolen. Therefore, the schemes that authenticate users by the pieces of secret data stored inside a smart card are explored, these schemes can be seen in [1, 4, 5]. By keeping the personal data in the smart card, rescues the system from maintaining the password table. Therefore, the mystery of stolen password is no longer a problem.

Wu and Hsu proposed an anonymous user identification and key distribution scheme in [3], henceforth called WH-scheme. The WH-scheme integrates the user authentication with key agreement, *i.e.*, a shared session key is generated after processing user authentication. Also, initiator's identity is transmitted in cipher. Thus no one listening on the channel can glean the identities of the initiators.

However the WH-scheme is insecure. This paper will propose three attacks to it. Assume that a user U_i sends a service request to a service provider P_j. The first attack shows that the service provider P_j is able to compute U_i's secret key. Knowing this secret key allows the provider impersonating the user U_i. By careful computing a user identity, an adversary can impersonate a pre-selected victim and launch the second and third attacks. These two attacks allow an adversary to impersonate either a service provider providing services or a user asking services.

2. Review of the WH-scheme

The WH-scheme consists of three entities: a Smart Card Producing Center (SCPC), service provider (access servers), and users. For easy interpretation, this scheme is divided into three phases: system initialization, key generation, and anonymous user identification.

System initialization: The SCPC randomly chooses two large prime numbers p and q, a collision-resistant hash function $f(.)$, two numbers e and d such that $e\ d = 1 \bmod \phi(N)$, and a random number g in the multiplicative group Z_N^*, where $N = p\ q$ and $\phi(N) = (p - 1)\ (q - 1)$. Then the SCPC publishes e, $f(.)$, g, and N.

Key generation (Registration): Both service provider P_i and user U_i register on the center SCPC and obtain a secret token

$$S_i = (ID_i)^d \bmod N, \tag{1}$$

where ID_i denotes the identity of service provider or user, *i.e.* P_i or U_i. In order to obtain services from the service provider P_i, user U_i also registers on service provider P_i. Unlike registering on the trusted center SCPC, P_i issues no token to U_i and uses an identity list to maintain the registered users.

Anonymous user identification: User U_i can request provider P_j to provide some services. Before granting U_i services, provider P_j should confirm that U_i is a legal user (registered user) without revealing user's identity to the public. The following steps demonstrate the details of user identification.

Step 1. User U_i submits a service request to P_j.

Step 2. Upon receiving this service request, P_j chooses a random number k, computes the quantity

$$z = g^k\ S_j \bmod N, \tag{2}$$

and sends z to challenge U_i.

Step 3. When receiving the challenge z, U_i chooses a random number t and computes the quantities

$$a = z^e\ /\ P_j \bmod N, \tag{3}$$

$$x = S_i\ f(a^t,\ T) \bmod N, \text{ and} \tag{4}$$

$$y = g^{et} \bmod N, \tag{5}$$

where T is the timestamp. Then U_i sends the response message (x, y, T) to P_j.

Step 4. Service provider P_j checks the timestamp T and verifies the response message by computing the quantity

$$ID = (x\ /\ f(y^k,\ T))^e \bmod N. \tag{6}$$

If the identity ID is in the identity list, P_j accepts user ID as an authorized user and grants her/him the requested services; otherwise, rejects the service request.

Subsequent to a successful user identification, user U_i uses (7) to compute the shared session key K_{ij} and service provider P_j uses (8) to compute the shared session key K_{ji}. Note that the quantities of K_{ij} and K_{ji} are identical.

$$K_{ij} = a^{tx} = (z^e\ /\ P_j)^{tx} = ((g^k\ S_j)^e\ /\ P_j)^{tx} = g^{ektx} \bmod N \tag{7}$$

$$K_{ji} = y^{kx} = (g^{et})^{kx} = g^{ektx} \bmod N = K_{ij} \tag{8}$$

Thus U_i and P_j uses the shared session key to decrypt/encrypt the exchanged data.

3. Cryptanalysis of the WH-scheme

The first attack: *Service provider can obtain user's secret token (secret key)*

Upon receiving a response message (x, y, T) from U_i, the service provider can compute the user's secret token S_i by implementing (4) and (5). The details are shown in (9).

$$S_i = x\ /\ f(a^t,\ T) = x\ /\ f(g^{ekt},\ T) = x\ /\ f(y^k,\ T) = S_i\ f(a^t,\ T)\ /\ f(g^{ekt},\ T) \bmod N \tag{9}$$

The secret token S_i is essentially a secret key issued from the SCPC to user U_i. Thus anyone knows the secret token S_i can impersonate user U_i.

The second attack: *Impersonate service provider P_j*

Assume that an adversary U_v has registered on the center SCPC and obtain a secret token

$$S_v = (ID_v)^d = (g^{ev}P_j)^d \ mod\ N, \tag{10}$$

where $U_v = g^{ev}P_j$ is the registered identity, e is SCPC's public key, and v is a random number chosen by the adversary U_v. Then the adversary U_v can impersonate the service provider P_j. A scenario of impersonation is as follows.

Step 1. User U_i submits a service request to P_j. However, this request is intercepted by the adversary U_v.

Step 2. Upon intercepting the service request emitted from U_i, the adversary U_v chooses a random number k, computes the quantity $z = g^k\, S_v\ mod\ N$ and sends z to challenge U_i.

Step 3. When receiving the challenge z, U_i chooses a random number t and computes the quantities $a = z^e / P_j\ mod\ N$, $x = S_i\, f(a^t, T)\ mod\ N$, $y = g^{et}\ mod\ N$, and sends the response message (x, y, T) to P_j. Also U_i uses (7) to compute the shared session key K_{ij}. The result is shown in (11).

$$K_{ij} = a^{tx} = (z^e / P_j)^{tx} = ([g^k(g^{ev}P_j)^d]^e / P_j)^{tx} = g^{ektx + evtx}\ mod\ N \tag{11}$$

Step 4. Once again, the adversary U_v intercepts the response message emitted from U_i and uses (12) to compute the shared session key K_{ji}.

$$K_{ji} = (y\ g^{ev})^{kx} = (g^{et}\ g^{ev})^{kx} = g^{ektx + evtx}\ mod\ N = K_{ij} \tag{12}$$

As can be seen in (11) and (12), the adversary U_v and user U_i does share the same session key. This result may cause problem. As an example, if user U_i initiates the protocol to deposit an electronic fund to P_i's account, the deposit will eventually be made to the adversary U_v's account.

The third attack: *Impersonate user U_i*

Assume that an adversary U_v has registered on the center SCPC and obtain a secret token

$$S_v = (ID_v)^d = (U_i / g^{ev})^d \ mod\ N, \tag{13}$$

where $U_v = U_i / g^{ev}$ is the registered identity, e is SCPC's public key, and v is a random number chosen by the adversary. Then the adversary U_v can impersonate the user U_i. A scenario of impersonation is as follows.

Step 1. Adversary U_v submits a service request to P_j.

Step 2. Upon receiving the service request, P_j chooses a random number k, computes the quantity $z = g^k\, S_v\ mod\ N$ and sends z to challenge U_v.

Step 3. When receiving the challenge z, U_v chooses a random number t, computes the quantities $a = z^e / P_j\ mod\ N$,

$$x = g^v\ S_v\ f(a^t, T)\ mod\ N, \text{ and} \tag{14}$$

$y = g^{et}\ mod\ N$, and sends the response message (x, y, T) to P_j.

Step 4. Service provider P_j checks the timestamp T and verifies the response message by computing the quantity

$$ID = (x / f(y^k, T))^e = [g^v\ (U_i / g^{ev})^d\ f(g^{ekt}, T)) / f(g^{ekt}, T)]^e = U_i\ mod\ N. \tag{15}$$

The adversary U_v and service provider use (7) and (8) to compute their session key.

As can be seen in (7) and (8), the adversary U_v and user U_i does share the same session key. This result may also cause problem. As an example, if the services provided by P_i are pay per access, user U_i will receive bill for accessing the services.

4. Conclusion

The paper has shown three attacks to the WH-scheme. By implementing a response message, the responder can solve for the initiator's secret key. Using a pre-computed identity to register on SCPC, an adversary is able to impersonate service provider or user.

Acknowledgement

This research was partially supported by National Science Council, Taiwan, R.O.C. under the contract number: NSC 93-2218-E-270-007.

References

1. C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," IEE Proceedings-E 1991; 138(3): 165-168.
2. L. Lamport, "Password authentication with insecure communication," Communications of ACM 1981; 24: 120-125.
3. T. S. Wu and C. L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks," Computers & Security 2004; 23:120-125.
4. S. J. Wang, "Yet another log-in authentication using n-dimensional construction based on circle property," IEEE Transactions on Consumer Electronics 2003; 49(2): 337-341.
5. T. C. Wu, "Remote login authentication scheme based on a geometric approach," Computer Communications 1995; 18(2): 959-963.