Workshop on Cryptology and Information Security

Cryptanalysis and improvement of an improved Identity-Based key exchange protocol

Yu-Mim Tseng[1], Jinn-Ke Jan[2], Ching-Hung Wang[3]

1. Department of Information Management, Nan-Kai College
No. 568, Jungjeng Rd., Tsautuen Jen, Nantou, Taiwan542, R.O.C.
tym@nkc.edu.tw, (049)333489-861

2. Institute of Applied Mathematics, National Chung Hsing University
No. 250, Guoguang Rd., Nan Chiu, Taichung, Taiwan402, R.O.C.
jkjan@amath.nchu.edu.tw, (04)22858200

3. Institute of Applied Mathematics, National Chung Hsing University
No. 2, Lane 31, Dewei St., Wufeng Shiang, Taichung, Taiwan413, R.O.C.
g9053304@mail.nchu.edu.tw, 0922914975

Abstract

A key exchange protocol is used to establish a common session key for two specified entities. In the past, the security attributes of a key exchange protocol have been identified clearly and specified. For the key exchange protocol proposed latterly, these security goals are required to achieve. In 2000, Saeednia proposed an identity-based key exchange protocol, which is a modification of Gunther's protocol. Recently, Xie et al. proposed a slight modification of Saeednia's protocol in order to reduce the computation cost. However, we find that their modification made no service of key compromise impersonation, one concrete security goal. Moreover, we modify Saeednia 's protocol in another way to reduce the computation cost and keep it resistant to the key compromise impersonation attack.

Keywords: Cryptanalysis, Key exchange, Identity- based, Authentication

Contact author: Ching-Hung Wang[3]

Cryptanalysis and improvement of an improved Identity-Based key exchange protocol

Yu-Mim Tseng[1], Jinn-Ke Jan[2], Ching-Hung Wang[2]

1. Department of Information Management, Nan-Kai College

tym@nkc.edu.tw

2. Institute of Applied Mathematics, National Chung Hsing University

jkjan@amath.nchu.edu.tw, g9053304@mail.nchu.edu.tw

Abstract

A key exchange protocol is used to establish a common session key for two specified entities. In the past, the security attributes of a key exchange protocol have been identified clearly and specified. For the key exchange protocol proposed latterly, these security goals are required to achieve. In 2000, Saeednia proposed an identity-based key exchange protocol, which is a modification of Gunther's protocol. Recently, Xie et al. proposed a slight modification of Saeednia's protocol in order to reduce the computation cost. However, we find that their modification made no service of key compromise impersonation, one concrete security goal. Moreover, we modify Saeednia's protocol in another way to reduce the computation cost and keep it resistant to the key compromise impersonation attack.

Keywords: Cryptanalysis, Key exchange, Identity- based, Authentication

1. Introduction

In key exchange protocol, both entities contribute some information, which is used to derive the shared session key based on the Diffie-Hellman problem [1]. Over the years, numerous protocols have been proposed. However, many of these protocols have been found to be flawed subsequently, and then these are to be modified to resist the new attacks. After a series of attacks and modifications, only those surviving protocols were believed to resist all known attacks and were deemed secure for usage. It is heuristic for these protocols to evolve with this "attack-response" methodology, and their security attributes are typically unclear or not completely specified. People have no guarantee that the protocol still secure when a new attack appears since the lack of specified definition of security.

In the past, some desired security attributes have been identified for an authenticated key agreement protocol [2,3]. In general, the importance of providing these security properties will be dependent on the application. These security attributes include key authentication, known-key security, perfect forward secrecy, key-compromise impersonation and unknown key-share attacks. The descriptions about these security attributes are presented in the next section. According to these positive definitions of security goals, we now could determine whether a protocol is secure directly without a series of attacks and modifications. These goals are vital items to be considered while designing a protocol. Generally, protocols proposed recently have been required to achieve these security goals to make sure that it is really secure.

According to technical categories of authentication approach, key agreement protocols may be classified into some categories including ordinary public-key-based protocols, identity-based protocols and password-based protocols. The protocol we will discuss in this paper is the identity-based key exchange protocol. An identity-based key exchange protocol is a protocol that uses user's identity to achieve user authentication and key exchange. After Gunther's identity-based key exchange protocol being proposed [4], Saeednia [5] proposed a modification of Gunther's protocol in 2000. Recently, Xie et al. [6] proposed a slight modification of Saeednia's protocol in order to reduce the computation cost further. However, it could be found that their protocol does not meet one concrete security goal, key-compromise impersonation, due to this modification.

In the remainder of this paper, we summarize the desirable security attributes of a key exchange protocol in the next section. Section 3 gives the brief review of both the Saeednia's and the Xie et al.'s protocols, along with the security analysis on the Xie et al.'s protocol. In Section 4, we propose a slight modification on the Saeednia's protocol in another way to reduce the computation cost and keep it resistant to the key compromise impersonation attack. Finally, the conclusions are presented in Section 5.

2. Security goals

Clearly the fundamental goal of any key exchange protocol is to establish a common session key which may be used to achieve some encryption subsequently. In the other word, it depends on the security of the key exchange protocol that whether the encryption secure. Fortunately, the notion of provable security makes several concrete security attributes and goals to be identified as desirable. Now, there are informal descriptions for these security attributes in the remainder of this section. The reader may refer to [2] in detail.

Fundamental security goals

・**implicit key authentication**

Suppose that two honest entity, A and B, want to execute a key exchange protocol to establish a common session key. If entity A is assured that no other entity except the identified entity B can learn this session key, then the key exchange protocol is said to provide implicit key authentication of B to A.

・**explicit key authentication**

Please note that the definition of implicit key authentication does not imply that A is assured of B actually possessing the key. Therefore, if entity A is assured that the entity B has actually computed the agreed session key, we say the key exchange protocol provide explicit key confirmation of A to B. Additionally, a protocol provides implicit key confirmation if A is only assured that B can compute the agreed session key in the future, but not really possess the key presently. And then, if a key exchange protocol provides both implicit key authentication and implicit or explicit key confirmation, we say it provides explicit key authentication of B to A.

Other desirable security attributes

・**known-key security**

In each run of a key exchange protocol, A and B should produce a unique session key. When an adversary has learned some other session key produced by previous runs, a protocol should still achieve the goal to limit exposure in the event of session key compromise. In the other word, one can not learn a session key from the other session keys.

・**forward secrecy**

It means that if one’s long-term private key is disclosed to some adversaries, they can not learn the previous session key. So this security goal makes the secrecy of previous session key not affected, even if the long-term private key loss. A further distinction is that a single entity’s private key is compromised or the private keys of both participating entity are compromised. The former is called half forward secrecy, and the latter is called full forward secrecy.

・**key-compromise impersonation**

It is clearly and inevitably that f A’s long-term private key is disclosed, an adversary who knows this value can easily impersonate A to the other entities. However, one question is that whether the adversary is able to impersonate other entities to A in some conditions. Therefore this goal is to make sure that the loss of A’s long-term private key does not enable the adversary to impersonate the other entities to A.

· **unknown key-share**

It means that when entity B to believe mistakenly the key is shared with some entity C≠A, and entity A correctly believes the key is shared with entity B. That is, entity B cannot be forced to share a key with entity A without B' s knowledge.

3. Review of two protocols

3.1 Saeednia' s identity-based key exchange protocol

An identity-based key exchange protocol can be regard as a variation of public-based key exchange protocol due to the generalization of identity-based cryptosystem. It employs user' s identity to achieve user authentication and key exchange purposes. Each new user needs only to visit a key authentication center (KAC) once and is from then on able to exchange authenticated keys with each other.

The Saeednia' s key exchange protocol is briefly reviewed as follow. The KAC chooses a large prime p and a large prime factor q of p -1. Let a be an element of order q in Z_p^*. Then, the KAC possess a one way function $f(\;)$ and a key pair (x,y), in which the private key $x \in Z_q$ is a random number and $y = a^x (\bmod p)$ is a public key, and publishes a, p, $y = a^x (\bmod p)$ and $f(\;)$.

For each user, the KAC first compute $I = f(ID)$, where ID is the string that may include the name, birthday or physical description corresponding to the user's identity. Next step the KAC computes $r = a^k (\bmod p)$ as the user' s public key and $s = Ik + xr (\bmod q)$ as the user' s private key, in which $k \in Z_q$ is a random number. The description of the protocol is presented as follows.

[Protocol]

$$\begin{array}{llcl}
 & \text{A} & & \text{B} \\
\text{Step1:} & t \in_R Z_q & & t' \in_R Z_q \\
 & u = a^t \bmod p & & u' = a^{t'} \bmod p \\
 & & \xrightarrow{u,r,ID} & \\
 & & \xleftarrow{u',r',ID'} & \\
\text{Setp2:} & I' = f(ID') & & I = f(ID) \\
 & Z = (u')^s & & Z = (u)^{s'} \\
 & Z' = (r'^{I'} y^{r'})^t & & Z' = (r^I y^r)^{t'} \\
 & K = ZZ'(u')^t & & K = ZZ'(u)^{t'}
\end{array}$$

It is clear that this protocol provides the service of key-compromise impersonation and forward secrecy. Since the $K = ZZ'(u')^t = ZZ'(u)^{t'} (= ZZ'a^{tt'})$, even the adversary C learn the private key of entity A, he is unable to impersonate other entities to A. On the other hand, if the long term private keys are disclosed, the adversary still can not compute the previous session key since the no ideal about $a^{tt'}$.

3.2 Xie et al.'s improvement on Saeednia's key exchange protocol

Recently, Xie et al.'s proposed a modification of Saeednia's key exchange protocol, in which the computation cost can be further reduced. As same as Saeednia's protocol, the KAC possess a one way function $f(\ )$ and a key pair (x, y), and then generates a pair (r, s) of public key and private key for each user.

[Protocol]

$$\begin{array}{llcl}
 & \text{A} & & \text{B} \\
\text{Step1:} & t \in_R Z_q & & t' \in_R Z_q \\
 & u = a^t \bmod p & & u' = a^{t'} \bmod p \\
 & & \xrightarrow{u,r,ID} & \\
 & & \xleftarrow{u',r',ID'} & \\
\text{Setp2:} & I' = f(ID') & & I = f(ID) \\
 & Z = (u')^t & & Z = (u)^{t'} \\
 & Z' = (r'^{I'} y^{r'})^s & & Z' = (r^I y^r)^{s'} \\
 & K = ZZ' & & K = ZZ'
\end{array}$$

[Cryptanalysis]

This modification reduces the computation cost of one modular multiplication and one modular exponentiation. Besides, it is desirable that the modification still keeps the protocol providing forward secrecy.

However, this protocol does not achieve the attribute of key-compromise impersonation. This attribute is to make sure that the loss of A' s long-term private key does not enable the adversary to impersonate the other entities to A. According to the identity-based key exchange protocol, an adversary can learn the value of r, u and ID of any entity easily. He is enable to impersonate real owner of r, u and ID, but he is unable to compute the common session key until he know the long-term private key s. Now note that if A' s long-term private key s is compromised to an adversary C, and C also learn the u', r' and ID' of B. Then C can not only impersonate B to A but also compute the common session key shared with A because of

$Z' = (r^I y^r)^{s'} = a^{ss'} (= a^{s's} = (r'^{I'} y^{r'})^s)$. Thus C can compute $Z' = (r'^{I'} y^{r'})^s$ easily and derive the session key further without the knowledge of B's long-term private key s'.

4. Our slight Improvement

We also make a slight modification on saeednia's protocol to reduce the computation in the other way and will not cause damage to original security. The most difference between two protocols is the generation of the user's private key s. The KAC still possess a key pair (x, y), and then generates a pair (r, s) of public key and private key for each user. But now the KAC uses a hash function $h(\ )$ instead of the one way function $f(\ )$, and computes $s = k + xh(ID, r)$ as the user's private key.

[Protocol]

$$
\begin{array}{llcl}
 & \quad A & & \quad B \\
\text{Step1:} & t \in_R Z_q & & t' \in_R Z_q \\
 & u = a^t \bmod p & & u' = a^{t'} \bmod p \\
 & & \xrightarrow{u,r,ID} & \\
 & & \xleftarrow{u',r',ID'} & \\
\text{Setp2:} & Z = (u')^s & & Z = (u)^{s'} \\
 & Z' = (r' y^{h(ID',r')})^t & & Z' = (ry^{h(ID,r)})^{t'} \\
 & K = ZZ'(u')^t & & K = ZZ'(u)^{t'}
\end{array}
$$

According to the protocol, the computation cost of Z' is reduced from $(r^I y^r)^t$ to $(ry^{h(ID,r)})^t$ and the computation $I = f(ID)$ is not needed any more. Note that since the hash function will make the value smaller, the value of $h(ID, r)$ is smaller than the value of r. Hence, a modular exponentiation is reduced, and we make the degree of the modular exponentiation of y lower, simultaneously.

Besides, it is clear that this protocol still provides the forward secrecy and key-compromise impersonation because the computation of the session key is the same in our protocol and Saeednia's protocol. Therefore, the proposed protocol is secure as Saeednia's protocol against various attacks.

5. Conclusions

We have shown that Xie et al.'s modification really reduces the computation cost much, but they missed the security attribute of key-compromise impersonation. Meanwhile, we have also proposed another slight modification to reduce the computation cost, and the modification preserves the security attributes.

Reference

[1] Diffie, W., Hellman, M.E., New directions in cryptography. IEEE Transactions on Information Theory IT-22 (6), 1976, 644-654.

[2] S. Blake-Wilson and A. Menezes, Authenticated Diffie-Hellman key agreement protocols, In Fifth Annual Workshop on Selected Areas in Cryptography (SAC '98), Lecture Notes in Computer Science, (Springer-Verlag, 1999), 339-361.

[3] Diffie, W., Van Oorschot, P.C., Wiener, M.J., Authentication and authenticated key exchanges. Designs, Codes and Cryptography, 2, 1992, 107-125.

[4] C. Gunther, An identity-based key-exchange protocol, Advances in Cryptology (Proc. Eurocrypt' 89), Lecture Notes in Computer Science, 434, (Springer-Verlag, 1990), 29-37.

[5] S. Saeednia, Improvement of Gunther' s identity-based key exchange protocol, Electronics Letters, 36, (18), 2000, 1535-1536.

[6] Bin-Can Xie, Hong-Min Sun, Zong-Li Huang and Chen-Tang Lin, An improvement of Saeednia's identity-based key exchange protocol, Information Security Conference 2002, pp. 41-43.