A New Session Key Agreement Scheme Using Smart Cards

Jongkook Lee[0] , Jongsoo Jang
Security Gateway Research Team, Information Security Division,
Electronics and Telecommunications Research Institute
{ljk63466[0], jsjang} @etri.re.kr

스마트 카드를 이용한 새로운 세션 키 생성 방법

이종국[0], 장종수
한국전자통신연구원 정보보호연구본부 보안게이트웨이팀

Abstract

This paper proposes a new session key agreement scheme which is based on Station-to-station protocol, or STS shortly. We extend key agreement model of STS, to take into account smart cards. Besides, we modify STS to withstand message replaying attack. Security analysis shows our scheme is still secure.

1. Introduction

Securities of cryptosystems are mainly dependent on secret keys, which are used to encrypt or decrypt message or data. Accordingly, the secret key of cryptosystem is able to be kept safely, that cryptosystem may be guaranteed its security. The secret keys are essential to both secret key and public key cryptosystems, and how to share secret keys is not a trivial problem in both cryptosystems. To share a secret key, key distribution protocol or key agreement protocol is available. In those protocols, our scheme take into account Diffie-Hellman Key Exchange, which the first and best known key agreement and based on computationally infeasible problem, discrete logarithm problem[1][2][3][4]. However, this protocol can be attacked by impersonation and substitution[1][3]. STS[1][3], which is an extension of Diffie-Hellman Key Exchange, can overcome these attacks, but can' t still withstand message replaying attack. Accordingly, we extend STS to think over smart cards and change the format of signature included in certificate of STS to make proposed scheme withstand message replaying attack. Security analysis proves proposed scheme is still secure against intruder-in-the-middle attack, which consists of substitution and impersonation, and message replaying attack.

2. Notations and Assumptions

In this letter, U and V are users who participate in key agreement, and W is an active adversary who can do intruder-in-the-middle attack and message replaying attack. Both U and V have a signature scheme with verification algorithm ver_U, ver_V and signing algorithm sig_U, sig_V. Trusted Authority, or TA shortly, that is responsible for verifying the identities of users, also have a signature scheme with public verification algorithm ver_{TA} and signing algorithm sig_{TA}. p is a prime number and α is a primitive element in Z_p^*. p and α are publicly known to everyone in the network. ID(U) and ID(V) is identification information of user U and V. User U and V also have certificates C(U) and C(V). And, we assume that a pseudo random number generator, or PRNG shortly, exists and is available in each user' s smart card.

3. A New Session Key Agreement Scheme

In our scheme, each user' s smart card deals with generating a random number and making his certificate. So, to take into account using smart cards, followings are taken. One thing is that p and α are stored on, and PRNG is also in smart card. This means that all elements required to do key agreement are only in smart cards, and if anyone who want to share a session key must insert his smart card into the card reader. Another is each user' s signature is

signed in his own smart card using given timestamp. Detailed description of our scheme is showed in Fig. 1. Parts to be given attention to, are step 4, 6, 7, 8. Step 4 and 7 are related to each user' s signing signature, and step 6 and 8 have relation to checking validity of received message and verifying received signature and certificate. ΔT used in step 6 and 8, are predefined value as expected legal time interval for transmission delay, signing a signature and making a certificate. As shown in Fig. 1, needed computations in our scheme are equal to those of STS. However, by adding timestamps, we make our scheme more secure without loss of additional time waste. Whenever session key agreement is needed, our scheme can be used. Moreover, our scheme can replace STS which is already used in many places, with same time and strengthened security.

4. Security Analysis

Smart card is known for its tamper-resistance. That is, data which is inside of card can' t be accessed by any trial to access without valid authentication given by card. By this facts, all works, like generating random numbers, signing signatures, and make certificates, which are done in card, can be secure and protected. So, without loss of generality, security analysis focus on only scheme itself. Because p and α are public, if W can get random numbers, au or av, then our scheme may be attacked. However, W can' t get au or av directly from α^{au} mod p and α^{au} mod p, because this equation relies on the complexity of computing, discrete logarithm problem[3]. W can' t attack our scheme by substitution and impersonation, because certificates are used to authenticate each communicants U and V. This is showed in Fig. 2 in detail. Once W impersonate U and V, and substitute α^{au} and α^{av}, the signatures must be changed accordingly. This failure is caused by W' s ignorance about signing algorithm of U and V. To withstand message replaying attack, similar underlying principle is applied in signing user's signatures. As shown in step 4 and 7, U and V insert current system time into their signatures which is used in step 6 and 8 to test validity of message. In order to pass step 6, W has to change the value of T_1 into a new time T_1' such that $(T_2 - T_1') \le \Delta T$. Once W changes T1, the test of step 6 is failed naturally, unless the signature has been changed accordingly. However, it is impossible that W makes a new and valid signature which is according to changed value, T_1' , because W doesn' t know the signing algorithm of U and V. The same checking is used in step 8.

Step 1. U gets a random number au using PRNG, where $0 \le au \le p-2$.

Step 2. U computes α^{au} mod p and sends this value to V.

Step 3. V gets a random number av using PRNG, where $0 \le av \le p-2$.

Step 4. V computes α^{av} mod p. Then V computes $K = (\alpha^{au})^{av}$ mod p and $y_v = sig_v(\alpha^{av}, \alpha^{au}, T_1)$, where T_1 is current date and time of V' s system.

Step 5. V sends (C(V), α^{av}, y_v, T_1) to U.

Step 6. U computes $K = (\alpha^{au})^{av}$ mod p. U verifies y_v using ver_v and U verifies C(V) using ver_{TA}. And check $T_2 - T_1 \le \Delta T$, where T_2 is current date and time of U' s system and ΔT is expected legal time interval in our scheme.

Step 7. U computes $y_u = sig_u(\alpha^{au}, \alpha^{av}, T_3)$ and sends (C(U), y_u, T_3) to V, where T_3 is current date and time of U' s system.

Step 8. V verifies y_u using ver_u and verifies C(U) using ver_{TA}. And check $T_4 - T_3 \le \Delta T$, where T_4 is current date and time of V' s system and ΔT is expected legal time interval in our scheme.

Prerequisite

C(U) = (ID(U), ver_u, sig_{TA}(ID(U), ver_u)),

C(V) = (ID(V), ver_v, sig_{TA}(ID(U), ver_v))

Fig. 1 A new session key agreement scheme

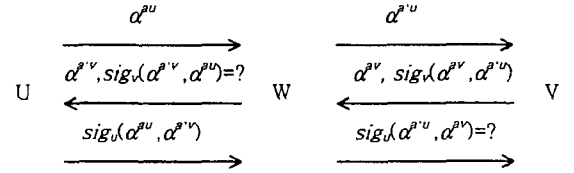

Fig. 2 Failure in impersonation and substitution

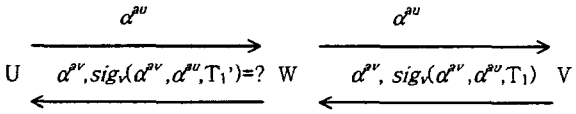

Fig. 3 Failure in message replaying attack

Therefore, our scheme is secure to withstand message replaying attack. Fig. 3 shows that W can' t attack our scheme by message replaying attack. Finally, all elements are protected by smart card' s infrastructure, all computation is computationally infeasible to W, and our scheme is still secure against impersonation, substitution and message replaying attack.

5. Conclusions

This letter has presented a new session key agreement scheme, which is based on STS, using smart cards. Because of certificates, original STS is secure to withstand the impersonation and substitution. In addition to, our scheme has timestamps in signers' signatures and certificates, to be secure to withstand message replaying attack. Security analysis shows that our scheme is still secure to endure impersonation, substitution and message replaying attack. Moreover, smart card' s infrastructure guarantee that no authenticated access to data in smart card is permitted. Our scheme relies on the difficulty of computing discrete logarithm problem over finite fields, and can be secure. Future work will involve investigation of the PRNG which is appropriate for smart cards, and reinforcement of authentication. And our scheme can be tied up with other authentication scheme or smart card authentication system with proven security power.

References

1. Douglas R. Stinson: Cryptography Theory and Practice, CRC Press, 1995.
2. Bruce Schneier: Applied Cryptography, second edition, John Wiley & Sons, Inc., 1996.
3. Alfred J. Menezes: handbook of Applied Cryptography, CRC Press, 1997.
4. William Stallings: Cryptography and Network Security, second edition, Prentice Hall, 1999.