Security Enhanced Anonymous Multi-Server Authenticated Key Agreement Scheme using Smart Card and Biometrics

Younsung Choi

College of Information and Communication Engineering,
Sungkyunkwan University, Suwon-si, Republic of Korea
yschoi@security.re.kr
http://www.security.re.kr

Abstract. Chuang and Chen propose an anonymous multi server authenticated key agreement scheme based on trust computing using smart card, password, and biometrics. Chuang and Chen say that this scheme not only supports multi-server but also achieves security requirements. but this scheme is vulnerable to masquerade attack, smart card attack, DoS attack and insufficient for perfect forward secrecy. To solve problems, this paper proposes security enhanced anonymous multi server authenticated key agreement scheme using smart card and biometrics.

Keywords: Key agreement scheme, Anonymous multi-server, Securty

1 Introduction

In Chuang and Chens paper, they propose an anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards, password, and biometrics. they say that proposed scheme not only is a lightweight authentication scheme which only uses the nonce and a hash function but also satisfies all of the following security properties: anonymity, absence of verification tables, mutual authentication, resistance to forgery attack, absence of clock synchronization problem, resistance to modification attacks, resistance to replay attacks, fast error detection, resistance to off-line guessing attacks, resistance to insider attacks, simple and secure password choice and modification, biometric template protection, and session key agreement.

But Chuang and Chen's Scheme has various security problems. this scheme is vulnerable to masquerade attack, smart card attack, DoS attack and Insufficient for perfect forward secrecy. To solve problems, this paper proposes security enhanced anonymous multi-server authenticated key agreement scheme using smart card and Biometrics.

The remainder of this paper is organized as follows. Section 2 introduces some related works. Section 3,4 describe and analyze Chuang and Chen's scheme in detail, Section 5 describe proposed scheme. and Section 6 analyzes the security, computation costs. Consequently, Section 7 summarizes conclusions.

2 Related Works

In this section, we research on anonymous multi server, security requirement and security requirement.

2.1 Anonymous User and Multi Server

The Anonymous user is used for public access the servers. Anonymous access is the most common web site access control method. Multi server provides various service to you using only once registration.

2.2 Security Requirement

Anonymous user and multi serve system must provide various security requirement as following.

(1) Simple and secure password choice and modification

(2) Single registration

(3) Anonymity

(4) Mutual authentication

(5) Integrity

(6) Session Key Agreement

(7) Perfect Forward Secrecy

2.3 Smart Card and Biometircs

Kocher et al. and Messerges et al. pointed out that confidential information stored in all exis- tent smart cards could be extracted by physi- cally monitoring its power consumption. So, if the user lost his smart card, all secrets in smart card may be revealed by attacker. so various scheme is vulnerable to off-line password attack. To solve this problem, Biometircs is sufficient solution. secret information combined passwords with biometrics cannot be guessed in polynomial time. And biometric is uniqueness in that everyone has a different biometric, and it is difficult for the users biometric to be stolen because only the user inputs his biometric into his own smart card.

3 Review on Chuang and Chen's Scheme

This section describe the notation and procedure of Chuang and Chen's Scheme.

x	: A secret value of the registraton center
RC	: The registration center
UID_i	: The identification of user i
SID_j	: The identification of server j
$AUID_i$	: The anonymous identification of user i
$ASID_j$	: The anonymous identification of server j
PW_i	: The password of user i
BIO_i	: The biometrics information of user i
$h()U$	: A secure one-way hash function
N_i	: A random number
PSK	: A secure pre-shared key among RC and authenticated servers
$\|$	: A string concatenation operation
$\oplus$	: A string XOR operation
$\underset{Secure}{\longleftrightarrow}$	: Messages through a secure channel
$\longleftrightarrow$	: Messages through a public channel

Table 1. Notation of Protocols

3.1 Notation

For convenience, the notations used throughout this paper are summarized in table 1.

3.2 Procedure of Chuang and Chen's Scheme

The application server sends the RC a join message if it would like to become an authorized server. Then, the RC replies with the key PSK to the server via the Internet Key Exchange Protocol version 2 (IKEv2). Afterwards, the authorized server uses this key (i.e., PSK) to facilitate the users authentication procedure. Every user needs to perform the user registration procedure with the registration center via a secure channel. Moreover, we assume that the authorized

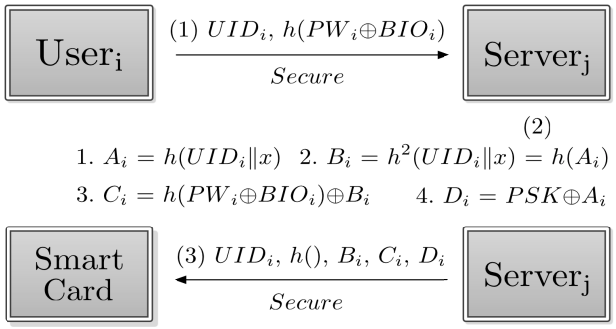

Fig. 1. Registration of Chuang and Chens scheme

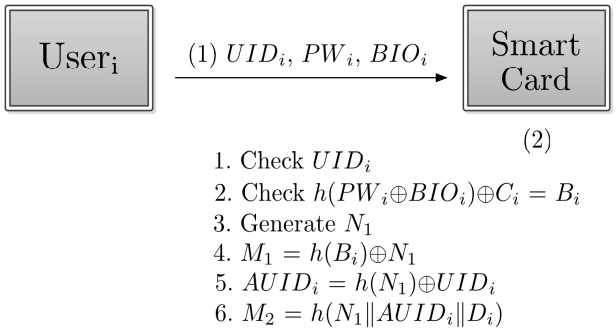

Fig. 2. Login of Chuang and Chens scheme

application servers are trusted according to the trust computing and that the PSK cannot be extracted from the RC and application servers. Fig. 1 depicts the user registration procedure. The steps of the procedure are described as follows. The login procedure is the first check point. The smart card detects an error event immediately if the user is not authorized to gain access (i.e., the user keys in the wrong identification, password, or biometrics information). Fig. 2 shows the steps of the login procedure. The smart card sends the server an authentication message after the user finishes the login procedure. Note that the smart card never uses the real identity to perform the authentication procedure. Fig. 3 shows the steps of the authentication procedure. This procedure is invoked whenever a user wants to change his password. In this procedure, the user can easily change his password without any assistance from the registration center. Fig. 4 illustrates the password change procedure, and the detailed steps are described as follows.

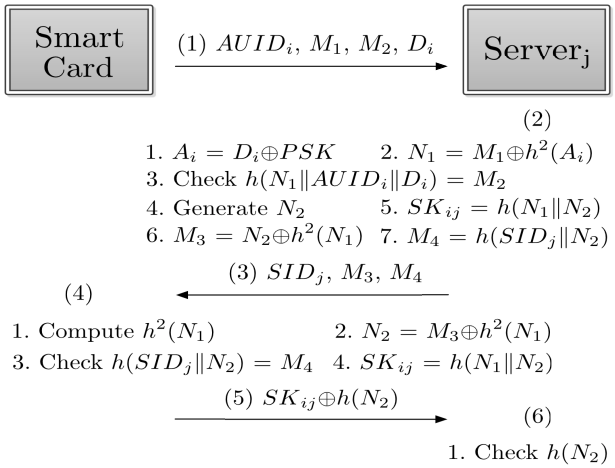

Fig. 3. Authentication of Chuang and Chens scheme

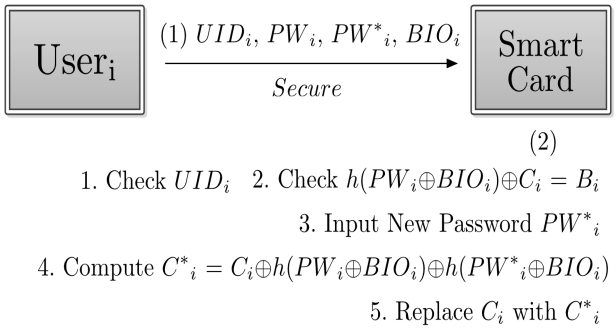

Fig. 4. Password change of Chuang and Chens scheme

4 Security Vulnerability of Chuang and Chen's Scheme

Chuang and Chen's Scheme has various security vulnerability. This scheme is vulnerable to masquerade attack, smart card attack, DoS and Insufficient for perfect forward secrecy.

4.1 Vulnerable to Masquerade Attack

Chuang and Chen's Scheme is user vulnerable to masquerade attack. Fig. 5 describes the masquerade attack on Chuang and Chen's Scheme.

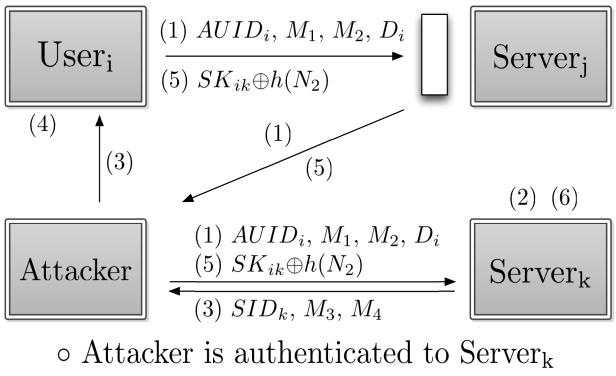

Fig. 5. Masquerade Attack

∘ Attacker Get(Still) User′s Smart Card
⇒ Exetracting the Information of Smart Card
(SPA, DSP... etc) ⇒ Get B_i

∘ Attacker Get M_1, M_3 in Public Channel
⇒ $N_1 = M_1 \oplus h(B_i)$
⇒ $N_2 = M_3 \oplus h^2(N_1)$
⇒ $SK_{ij} = h^2(N_1 \| N_2)$

∘ Attacker Know Session Key Between User i and Server j

Fig. 6. Smart Card Attack

4.2 Vulnerable to Smart Card Attack

Kocher et al. and Messerges et al. pointed out that confidential information stored in all exis- tent smart cards could be extracted by physi- cally monitoring its power consumption. So, if the user lost his smart card, all secrets in smart card may be revealed by attacker. So attacker can get user's smart card and exetracting the information of stolen smart card. using this, attacker can know session key between user and server. Fig. 6 describes the smart card attack on Chuang and Chen's Scheme.

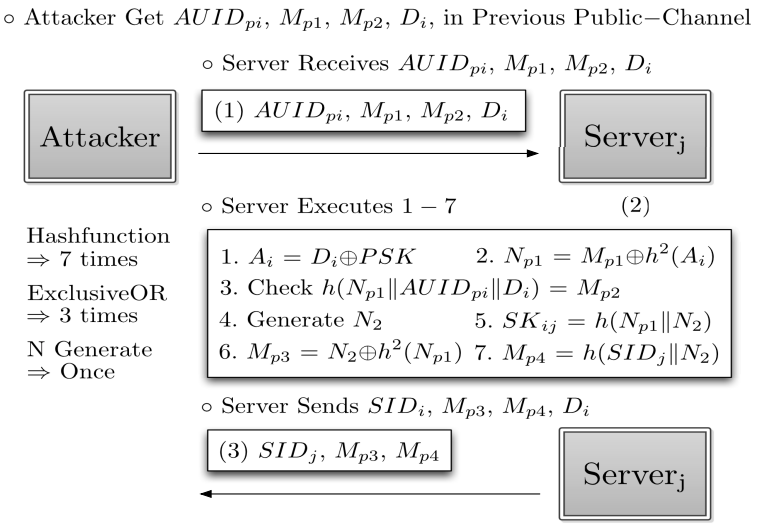

Fig. 7. DOS Attack

∘ Attacker Got M_{p1}, M_{p3} in Previous Public Channel
∘ Attacker Knows One of User′s LongTerm Secret : $h(B_i)$

⇒ Attacker Knows $h(B_i)$, M_{p1}, M_{p3}
⇒ $N_{p1} = M_{p1} \oplus h(B_i)$
⇒ $N_{p2} = M_{p3} \oplus h^2(N_{p1})$
⇒ $SK_{p-ij} = h^2(N_{p1} \| N_{p2})$

∘ Attacker Knows Previous Session Key Between User i and Server j

Fig. 8. Perfect Forward Secrecy

4.3 Vulnerable to DoS Attack

DoS attack is an attempt to make a machine or network resource unavailable to it's intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

4.4 Insufficient for Perfect Forward Secrecy

Perfect forward secrecy means that a session key derived from a set of long-term keys will not be compromised if one of the long-term keys is compromised in the future.

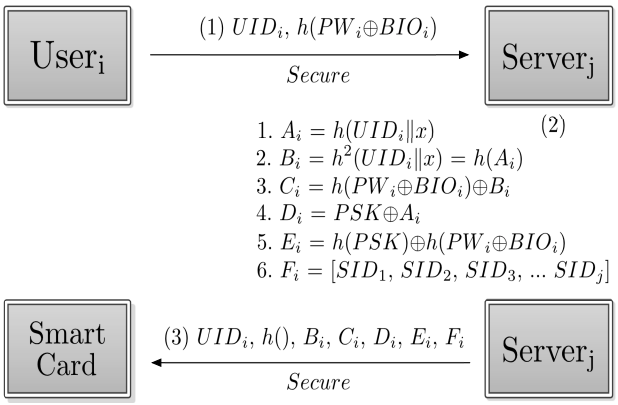

Fig. 9. Proposed scheme's Registration procedure

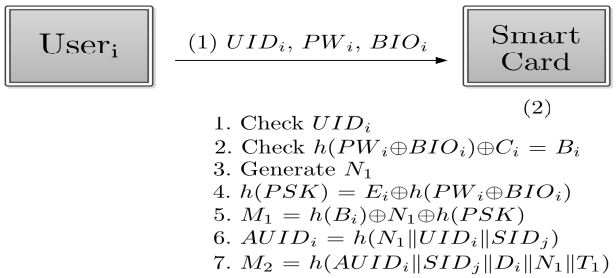

Fig. 10. Proposed scheme's Login procedure

5 Proposed Scheme

To solve security problems, this paper proposes security enhanced anonymous multi-server authenticated key agreement scheme using smart card and Biometrics.

5.1 Registration

The registration procedure of proposed scheme is described in Fig. 9.

5.2 Login and Authentication

The login procedure of proposed scheme is described in Fig. 10.
The authentication procedure of proposed scheme is described in Fig. 11.

5.3 Password Change

The password change procedure of proposed scheme is described in Fig. 12.

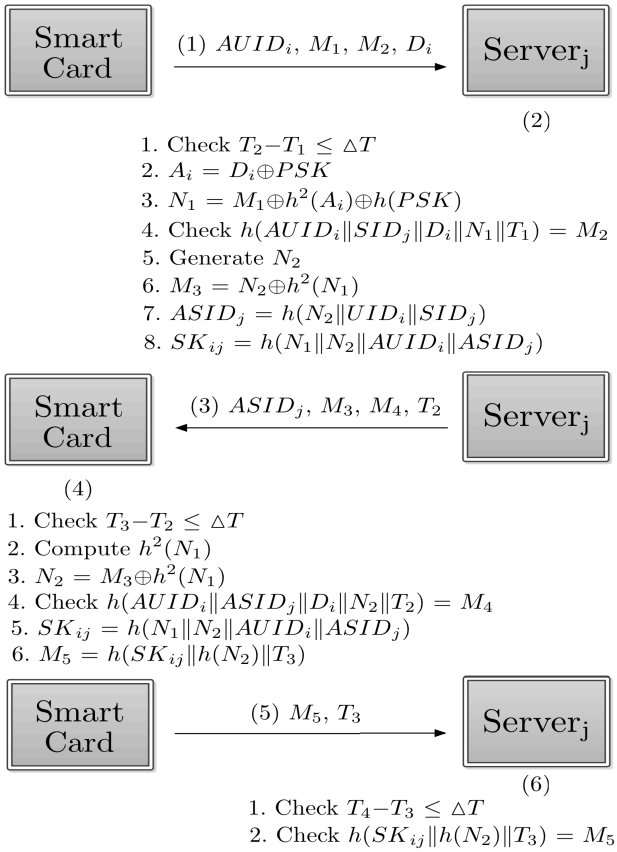

Fig. 11. Proposed scheme's Authentication procedure

6 Analysis on Proposed Scheme

This section analyzes the security and computational cost of proposed scheme.

6.1 Security Analysis

Proposed scheme is more secure than Chuang and Chen's Scheme on masquerade attack, smart card attack, DoS and perfect forward secrecy. And proposed scheme is satisfied with anonymity, no verification table, mutual authentication, resistance to replay attacks, session key agreemen, resistance to modification attacks, resistance to forgery attacks, resistance to off-line password guessing attacks, simple and secure password choice and modification, resistance to insider attacks.

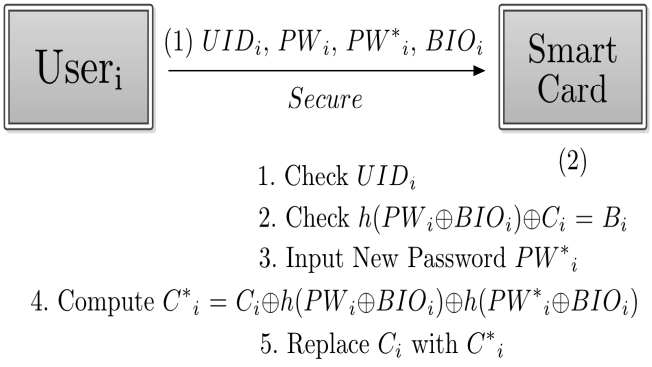

Fig. 12. Proposed scheme's Password change procedure

6.2 Computational Cost Analysis

In performance, proposed protocol is similar to Chuang and Chen's Scheme. Chuang and Chen's Scheme has a little less computational cost but it is vulnerable to various attack. Proposed scheme has a little more computational cost but it is more secure. So, proposed protocol solves the security problems with similar computaional cost.

7 Conclusions

Chuang and Chen's Scheme has various security problems. this scheme is vulnerable to masquerade attack, smart card attack, DoS attack and Insufficient for perfect forward secrecy. To solve problems, this paper proposes security enhanced anonymous multi-server authenticated key agreement scheme using smart card and Biometrics.

8 Future Works

This paper shows the various security problem of Chuang and Chen's Scheme and proposes the security enhanced anonymous multi-server authenticated key agreement scheme. This paper will add-modify details of proposed scheme. And security / computational cost analysis of Chuang and Chen and proposed scheme will be added.

References

1. Chuang, Ming-Chin, and Meng Chang Chen. "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics." Expert Systems with Applications 41.4 (2014): 1411-1418.

2. Yeh, KuoHui, Nai-Wei Lo, and Yingjiu Li. "Cryptanalysis of HsiangShih's authentication scheme for multiserver architecture." International Journal of Communication Systems 24.7 (2011): 829-836.
3. Yoon, EunJun, and KeeYoung Yoo. "Cryptanalysis of a simple threeparty password-based key exchange protocol." International Journal of Communication systems 24.4 (2011): 532-542.
4. Junghyun Nam, Kim-Kwang Raymond Choo, Moonseong Kim, Juryon Paik and Dongho Won, "Dictionary Attacks against Password-Based Authenticated Three-Party Key Exchange Protocols", KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, Volume 7, NO. 12, December 2013, pp.3244-3260.
5. Junghyun Nam, Minkyu Park, Sangchul Han, Juryon Paik, and Dongho Won, "Scalable Group Key Exchange for Securing Distributed Operating Systems", Journal of Information Science and Engineering (IF : 0.175), Volume 28, No. 5, September 2012, pp.829-857.
6. P. Kocher, J. Jaffe, and B. Jun, Differen- tial power analysis, in Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 99), vol. 1666 of Lecture Notes in Computer Science, pp. 388397, 1999.
7. T. S. Messerges, E. A. Dabbish, and R. H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Transactions on Computers, vol. 51, no. 5, pp. 541552, 2002.