Analysis of Two Types Deniable Authentication Protocols

Haibo Tian[1], Xiaofeng Chen[1], and Yong Ding[2]
(Corresponding author: Haibo Tian)

School of Information Science and Technology[1]
Sun Yat-Sun University, Guangzhou, Guangdong, 510275, China
School of Mathematics and Computational Science[2]
Guilin University of Electronic Technology Guilin, Guangxi 541004, China
(Email: tianhb@mail.sysu.edu.cn)
(Received May 10, 2008; revised and accepted Oct. 2, 2008)

Abstract

Deniability enables protocol participants to deny their involvement after they have taken part in a particular protocol run. In this paper, we present the security analysis of a class of interactive deniable authentication protocols and a noninteractive one. For interactive protocols, we focus on a serial of pairings based protocols proposed by Chou et al and repaired by Lim et al. We point out that their repaired protocols are still not secure under Key Compromise Impersonation (KCI) attack and give it an improvement. For noninteractive protocols, we point out that most current noninteractive deniable authentication protocols are not secure under KCI attack.

Keywords: Deniable authentication protocols, information security, interactive protocols, key compromise impersonation attack, noninteractive protocols

1 Introduction

Deniable authentication protocols allow a Sender to authenticate a message for a Receiver, in a way that the Receiver cannot convince a third party that such authentication (or any authentication) ever took place. Generally there are two kinds of such protocols, interactive protocols and noninteractive protocols.

1.1 Interactive Protocols

In the past several years, numerous interactive deniable authentication protocols have been proposed. A detail survey can be found in [7]. We here just state a list of literatures leading to our work. Fan et al. [3] proposed a simple deniable authentication protocol. Yoon et al. [13] pointed out that Fan et al.'s protocol suffered from the intruder masquerading attack and proposed an enhanced deniable authentication protocol. Cao et al. also [1] proposed an efficient ID-based deniable authentication protocol. Chou et al. [2] pointed out that Yoon et al.'s enhanced scheme and Cao et al.'s scheme were proven to be impractical and susceptible to Key Compromise Impersonation (KCI) attack and proposed another new deniable authentication protocol. Lim et al. [5, 6] pointed out that Chou's scheme was not secure under KCI attack and proposed an enhanced protocol. Lim et al. found out the security problem about their protocol in [5, 6] and gave out another enhancement [7]. We pointe out here that the last enhanced protocol is still not secure under KCI attack. This contradicts the claim in [7]. Also we give out an improvement method to avoid our attack.

You can see that KCI attack is heavily considered for interactive protocols. By KCI, we mean that the compromise of participant Bob's long-term private key should not enable the adversary to impersonate other participants to cheat Bob. KCI attack should be considered since it enables an attacker to cheat an honest participant Bob by impersonating another participant Alice who has a close relationship to Bob, such as Bob's secret lover, or supervisor.

1.2 Noninteractive Protocols

There are also some noninteractive deniable protocols. Shao [12] proposed an noninteractive deniable authentication protocol based on generalized ElGamal signature scheme. Lu and Cao proposed two protocols based on factoring [8] and on bilinear parings [9]. Lee et al. [4] pointed out that these three protocols had security flaws when a session secret was disclosed, i.e. the receiver could not identify the true source of a forged message. Lu and Cao have given out a group oriented deniable authentication protocol which claimed secure against session secret disclosure attack [10]. Also, Lu et al have constructed a new ID-Based deniable authentication protocol where a new construction method was employed [11].

We pointed out that most noninteractive protocols suffered from KCI attack since most such protocols took the advantage of long term secret keys. We note that the KCI resistance property is not a security goal of such noninteractive protocols. So what we point out here may be not qualify as an *attack*. But what we point out can restrict the application scenarios of such noninteractive protocols. Firstly, all participants' long term keys should have the same security level. Secondly, a method should be available for all participants to detect key disclosure.

The rest of this paper is organized as follows. The enhanced protocol of Lim et al.'s, our attack to their protocol, and our improvement are presented in Section 2. In Section 3, the noninteractive protocol of Lee et al.'s is reviewed and analyzed. Section 4 concludes the paper.

2 Lim et al.'s Enhanced Protocol

2.1 Preliminary

Let G_1 be a cyclic additive group of a large prime order, q and G_2 be a cyclic multiplicative group of the same order, q. Let $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing with the following properties:

1) Bilinearity: $e(aP, bQ) = e(P, Q)ab = e(abP, Q)$ for any $P, Q \in G_1$, $a, b \in \mathbb{Z}_q^*$.

2) Non-degeneracy: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.

3) Computability: There is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G_1$.

A bilinear map which satisfies all three properties above is considered as admissible bilinear. It is noted that the Weil and Tate pairings associated with the supersingular elliptic curves or abelian varieties, can be modified to create such bilinear maps.

Bilinear Diffie-Hellman Problem (BDHP):
Let G_1, G_2, P and e be as above with order q being prime. Given $\langle P, aP, bP, cP\rangle$ with $a, b, c \in \mathbb{Z}_q^*$, compute $e(P, P)^{abc} \in G_2$. An algorithm α is deemed to have an advantage ϵ in solving the BDHP in (G_1, G_2, e) based on the random choices of $a, b, c \in \mathbb{Z}_q^*$ and the internal random operation of α if

$$Pr[\alpha(\langle P, aP, bP, cP\rangle) = e(P, P)^{abc}] \geq \epsilon.$$

Throughout this paper, we assume that BDHP is a hard computational problem such that there is no polynomial time algorithm to solve BDHP with nonnegligible probability.

2.2 Lim et al.'s Enhanced Deniable Authentication Protocol

Suppose that two communication parties, Alice and Bob wish to communicate with each other. The Private Key Generator (PKG) *uniformly* picks a master key $s \in \mathbb{Z}_q^*$ and sets

$$P_{pub} = sP.$$

The PKG then publishes $\{G_1, G_2, e, P, P_{pub}, q, H_1, H_2, H_3\}$. G_1, G_2, e, P and q are defined as above subsection. $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : G_2 \rightarrow \{0,1\}^q$ and $H_3 : \{0,1\}^* \rightarrow \{0,1\}^*$ are one way collision-free cryptographic hash functions. For a given string $ID \in \{0,1\}^*$, the PKG computes the public key,

$$Q_{ID} = H_1(ID),$$

and the private key,

$$S_{ID} = sQ_{ID},$$

where s is the master key. Alice and Bob's public/private key pairs are denoted as Q_A/S_A and Q_B/S_B respectively. We describe Lim et al.'s protocol as follows:

Step 1. Alice uniformly chooses a random number, $r_A \in \mathbb{Z}_q^*$, computes

$$u = r_A Q_A, \text{ and } w = r_A^{-1} P, \quad (1)$$

and then sends (ID_A, u, w) to Bob.

Step 2. After receiving (ID_A, u, w), Bob checks whether

$$e(w, u) = e(P, Q_A). \quad (2)$$

If it does not, Bob terminates the session. Otherwise, Bob uniformly chooses a random number, $r_B \in \mathbb{Z}_q^*$ and calculates

$$v = r_B Q_B \quad (3)$$
$$h_B = H_2(e(u, r_B S_B)) \quad (4)$$
$$f = h_B \oplus r_B, \quad (5)$$

and sends (ID_B, f, v) to Alice.

Step 3. After receiving (ID_B, f, v), Alice computes

$$h_A = H_2(e(v, r_A S_A)) \quad (6)$$
$$r_B = h_A \oplus f. \quad (7)$$

Then, Alice computes $r_B Q_B$ and checks whether

$$r_B Q_B = v. \quad (8)$$

Alice terminates the session if the verification fails. Otherwise, she calculates X_A, Y_A, and the session key K_A as follows:

$$X_A = H_2(x_A), \text{ where } x_A = e(r_B Q_B, P_{pub}) \quad (9)$$
$$Y_A = H_2(y_A), \text{ where } y_A = e(r_B S_A, P) \quad (10)$$
$$K_A = kdf(e(S_A, Q_B)^{X_A Y_A} || u || w || f || v), \quad (11)$$

where $kdf(\cdot)$ is a key derivation function with arbitrary bits input and fixed m bits output, where m is

a security parameter. For the concatenation operator typically takes two bit strings as arguments, the integers appeared in the Assignment (11) and following assignments including the operator should be treated as bit strings using some type converting function.

Suppose that m_A is the message that Alice would like to send together with her ID. She computes

$$g_A = H_3(ID_B||m_A||x_A||y_A||K_A), \quad (12)$$

and sends (g_A, m_A) to Bob.

Step 4. After receiving (g_A, m_A), Bob calculates X_B, Y_B and the session key K_B as follows:

$$X_B = H(x_B), \text{ where } x_B = e(r_B S_B, P) \quad (13)$$
$$Y_B = H(y_B), \text{ where } y_B = e(r_B Q_A, P_{pub}) \quad (14)$$
$$K_B = kdf(e(Q_A, S_B)^{X_B Y_B}||u||w||f||v). \quad (15)$$

At last, he computes

$$g_B = H(ID_B||m_A||x_B||y_B||K_B), \quad (16)$$

and checks whether $g_A = g_B$. If it does (does not), Bob accepts (rejects) the session key.

2.3 Our Attack

In this section, we will depict how Lim et al.'s scheme can be intruded by using KCI Attack. In fact, this attack is deemed successful only if the adversary manages to masquerade as another protocol principal to communicate with the victim after the victim's private key has been compromised.

Assume that an adversary, Eve has the knowledge of Bob's private key S_B and he intends to launch the KCI attack against Bob by pretending Alice to communicate with him. Hence, Eve is able to carry out his attack as follows:

Step 1. Eve uniformly chooses a random number, $r_E \in \mathbb{Z}_q^*$, computes

$$u = r_E P \text{ and } w = r_E^{-1} Q_A,$$

and then by using the ID of Alice, ID_A, sends (ID_A, u, w) to Bob.

Note that the replacement of $r_A Q_A$ by $r_E P$ and the permutation of u and w are crucial for the attack. With such a replacement and permutation, Eve can compute h_A, y_A without Alice's long term private key.

Step 2. After receiving (ID_A, u, w), Bob checks u and w according to Equation (2). Note that the G_1 is a cyclic additive group of a large prime order q such that $e(P, Q) = e(Q, P)$. So Bob will think that Alice is trying to communicate with him. Then, he chooses a random number, $r_B \in \mathbb{Z}_q^*$ and calculates v from Equation (3), h_B from Equation (4) and f from Equation (5). After that, he sends (ID_B, f, v) to Alice.

Step 3. After intercepting (ID_B, f, v), Eve computes h_A, r_B, X_A, Y_A, K_A and g_A. As Alice's secret key S_A is unknown, Eve is unable to compute pairings which involve S_A. However, Eve can compute

$$h_A = H(e(r_E P_{pub}, v))$$
$$y_A = e(r_B Q_A, P_{pub})$$
$$K_A = kdf(e(Q_A, S_B)^{X_A Y_A}||u||w||f||v),$$

instead of Equations (6), (10), and (11). Eve computes other values by using Equations (7), (9) and (12). Here the message Eve to Bob is still denoted by m_A.

Note that the involvement of Bob's long term private key for computing K_A just concretes the KCI attack.

Step 4. After receiving (g_A, m_A), Bob calculates X_B, Y_B, the session key K_B and g_B by using Equations (13), (14), (15) and (16) respectively. Since g_A and g_B are always equal, Bob will eventually accept the session key and truly believes that he is communicating with Alice although he is in fact communicating with Eve. Hence, our KCI attack is successful.

2.4 Improvement

The improvement involves small modifications of the enhancement protocol in [7].

Step 1. Equation (1) is replaced by the following Equation (17).

$$u = r_A Q_A, w = r_A^{-1} Q_B. \quad (17)$$

Step 2. Equations (2) and (3) are replaced by Equations (18) and (19) respectively.

$$e(w, u) = e(Q_A, Q_B) \quad (18)$$
$$v = r_B w. \quad (19)$$

Step 3. Equations (6) and (8) are replaced by Equations (20) and (21) respectively.

$$h_A = H(e(v, r_A S_A)^{r_A}) \quad (20)$$
$$r_B r_A^{-1} Q_B = v. \quad (21)$$

All other equations are unchanged. The improvement protocol remains deniable due to the Lemma 3 of [7]. The resistance about key replicating attack can be argued similar with Lemma 2 in [7]. For KCI attack, if the private key of Alice is compromised, Eve cannot impersonate Bob since the mandate of value v. if the private key of Bob is compromised, Eve cannot impersonate Alice since the mandate of value u. Note that the value w is embedded in the computation of the value v such that the permutation attack can not work. For time computation, the improved protocol needs a bit more time for the replacement of Equation (6) by Equation (20). In fact, one more exponentiation computation time is needed.

3 Noninteractive Deniable Authentication Protocols

3.1 Lee et al.'s Protocol

There is an authority who selects two large prime numbers p, ranging in size from 1024 to 2048 bits, and q with a bit size of 160, where $q|p-1$, an element g of order q in GF(p) and a collision-free hash function $H(\cdot)$ with an output of q bits. The secret key of the sender S is $X_S \in \{1, 2, \ldots, q\}$ and $Y_S = g^{X_S} \bmod p$ is the corresponding public key. Similarly, (X_R, Y_R) is the key pair of the receiver R, where $X_R \in \{1, 2, \ldots, q\}$ and $Y_R = g^{X_R} \bmod p$. The symbol "||" is the concatenation operator of strings. S will execute the following steps to deniably authenticate a message M to R:

1) Choose a random integer $t \in \{1, 2, \ldots, q\}$.

2) Compute

$$\begin{aligned} r &= g^t \bmod p, \\ \delta &= H(M)X_S + tr \bmod q, \end{aligned}$$

where $H(M)$ is treated as an integer here assuming there is some type converting function.

$$\begin{aligned} k &= (Y_R)^{\delta} \bmod p, \\ MAC &= H(k||M). \end{aligned} \tag{22}$$

3) Send (r, MAC) with M to R.

After receiving (r, MAC) and M from S, R will execute the following steps:

1) Compute

$$k' = (Y_S^{H(M)} r^r)^{X_R} \bmod p, \tag{23}$$

where $H(M)$ is again treated as an integer.

2) Verify whether $H(k'||M) = MAC$. If the equation holds, R accepts; otherwise, R rejects it.

3.2 KCI Attack Scenario

Suppose that the long term private key of receiver R has been compromised. An adversary now can select any message M, and a random element r in GF(p). Now the adversary can use any sender's public key Y_S and the receiver's private key X_R to calculate a valid k' by using Equation (23). With a valid k', the adversary can certainly compute a valid MAC further by using Equation (22). Since everything is dedicatedly computed for the receiver's verification procedure, the message M will be accepted as from a valid sender S. So everyone can pretend to be the receiver's supervisor to direct the poor receiver to do some bad things.

The attack has practical effects on application scenarios. Firstly, all participants' long term keys should have the same security level. Considering military applications, the key security level of a commander is usually much higher than a common soldier. If the commander has commanded the soldier once and the soldier's long term key is compromised, anyone can impersonate the commander to give new commands to the soldier. Secondly, there should be a method for all participants to detect key disclosure in time. Let's continue to say the above military application. If the soldier has such a method to detect her/his key disclosure in time. He can take measures to obtain a new long term key such that no one can easily cheat her/him before her/his new key is disclosed.

We have to say such kind of KCI attack can be applied to most noninteractive deniable authentication protocol in [4, 8, 9, 10, 12]. Considering the practical effects on application scenarios, new methods to construct noninteractive deniable protocols are really needed. We have seen one method in [11] where a PKG is used. In their construction, a receiver can not reconstruct its received message. But the receiver can construct another valid message to pass the verification procedure. In such a way, the deniable property holds up to the PKG.

4 Conclusions

For interactive protocols, this paper pointed out that Lim et al.'s last enhanced protocol is still unsatisfactory and gave it an improvement. For noninteractive protocols, this paper pointed out most noninteractive protocols are not secure under KCI attack and discussed some practical effects of the KCI attack.

Acknowledgments

This work is supported by National Natural Science Foundation of China under Grant No. 60773202, 60803135, also by Guangdong Natural Science Foundation under Grant No. 8451027501001508 and Sun Yat-Sen university under Grant No. 35000-2910025,35000-3171912. The authors are grateful to the anonymous reviewers for valuable comments. While the authors are grateful to Dr. Fangguo Zhang and Dr. Bodian Wei for helpful discussions.

References

[1] T. J. Cao, D. D. Lin, and R. Xue, "An efficient ID-based deniable authentication protocol from pairings," *Advanced Information Networking and Applications, 19th International Conference on*, vol. 1, pp. 388-391, Taipei, Taiwan 2005.

[2] J. S. Chou, Y. L. Chen, and J. C. Huang, "A ID-based deniable authentication protocol on pairings," *Cryptology ePrint Archive: Report*, 335, 2006.

[3] L. Fan, C. X. Xu, and J. H. Li, "Deniable authentication protocol based on Diffie-Hellman algorithm," *Electronics Letters*, vol. 38. no. 4, pp. 705-706. 2002.
[4] W. B. Lee, C. C. Wu, and W. J. Tsaur, "A novel deniable authentication protocol using generalized ElGamal signature scheme," *Information Sciences*, vol. 177, pp. 1376-1381. 2007. http://www.sciencedirect.com.
[5] M. Lim, S. Lee, Y. Park, and H. Lee, "An enhanced ID-based deniable authentication protocol on pairings," *Cryptology ePrint Archive: Report*, 113, 2007.
[6] M. Lim, S. Lee, Y. Park, and H. Lee, "An enhanced ID-Based deniable authentication protocol on pairings," *ICCSA (2)*, LNCS 4706, pp. 1008-1017, Springer-Verlag, 2007.
[7] M. Lim, S. Lee, and H. Lee, "Cryptanalysis on improved chou et al.'s ID-Based deniable authentication protocol," *International Conference on Information Science and Security*, pp. 87-93, 2008.
[8] R. Lu, and Z. Cao, "Non-interactive deniable authentication protocol based on factoring," *Computer Standards & Interfaces*, vol. 27, no. 4, pp. 401-405. 2005.
[9] R. Lu, and Z. Cao, "A new deniable authentication protocol from bilinear pairings," *Applied Mathematics and Computation*, vol. 168, no. 2, pp. 954-961. 2005.
[10] R. Lu, and Z. Cao, "Group oriented Identity-Based deniable authentication protocol from the bilinear pairings," *International Journal of Network Security*, vol. 5, no. 3, pp. 283-287, Nov. 2007.
[11] R. Lu, Z. Cao, and S. Wang etc, "A new ID-based deniable authentication protocol," *Informatica*, vol. 18, no. 1, pp. 67-78, 2007.
[12] Z. Shao, "Efficient deniable authentication protocol based on generalized ElGamal signature scheme," *Computer Standards & Interfaces*, vol. 26, no. 5, pp. 449-454. 2004.
[13] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Improvement of Fan et al.'s deniable authentication protocol based on Diffie-Hellman algorithm," *Applied Mathematics and Computation*, vol. 167, no.1, pp. 274-280. 2005.

Hai-Bo Tian obtained a Ph.D. degree in cryptography from Xidian University and is currently working in School of Information Science and Technology, Sun Yat-Sen University. He also joined the Guangdong Key Laboratory of Information Security Technology. He is a member of China Computer Federation. His research interests include cryptography and network security. His major research is in the area of key establishment protocols, public key encryption schemes, privacy protection etc.

Xiao-Feng Chen is an associate professor in the Department of Computer Science at Sun Yan-Sen University, Guangzhou, China. He obtained his Ph.D. degree in cryptography from School of Communication Engineering, Xidian University in 2003. He was a post-doc fellow in International Research Center for Information Security (IRIS), Information and Communications University (ICU), Korea from 2003 to 2004. His main research interests include public key cryptography and E-commerce security.

Yong Ding was born in Chongqing China in June 1975. He graduated with a B.S degree from Dept. of Mathematics, Sichuan University, China, in 1998. He received M.S degree and PhD degree in Xidian University,China, in 2003 and 2005, respectively. He is currently an associate Professor in School of Mathematics and Computational Science, Guilin University of Electronic Technology. His research interests are cryptography and network security.