An Improved Deniable Authentication Protocol

Chia-Chen Lin,† and Chin-Chen Chang ††,

Providence University, Feng Chia University, Taiwan, R. O. C.

Summary
In 2002, Fan et al. proposed a deniable authentication protocol based on the Deffie-Hellman key agreement protocol. They claimed that their proposed protocol is deniable, can authenticate the source of a given message, and resists the person-in-the middle (PIM) attack. However, their proposed protocol can not support the sender to authenticate his receiver's identity, which may cause some security flaws. Meanwhile, their proposed protocol suffers lacking of efficiency when two parties are engaged in constant exchanges of messages. Therefore, we propose an improved deniable authentication protocol, which not only has same properties as Fan et al.'s scheme has, but also provides mutual authentication between the sender and the receiver which can rectify the potential security problem under Fan et al.'s. In addition, our proposed protocol proves to be more efficient than Fan et al.'s under the case that the sender and the receiver are engaged in constant exchanges of messages.

Key words:
Deniable authentication, mutual authentication, PIM attack.

Introduction

There are numerous occasions on the Internet where authentication protocols are required to identify participants. Although traditional authentication protocols did help receivers identify sources of a given message, they further revealed the identity of the message sender. This may cause problems on many occasions, especially on those where the identification of the message sender should not be revealed, for example, electronic elections and on-line auctions. During the electronic elections, for example, if the message sender is known to the receivers, the sender may be biased toward a certain candidate knowing that the sender may be sanctioned socially, economically, or even physically by the receiver or after his/her name goes public. In order to conquer this potential problem, a new authentication protocol, called 'deniable authentication protocol' has been proposed [1, 2, 3, 4]. This protocol purports to alleviate the problem that may caused by the traditional authentication protocol. In this protocol, the message receiver can still identify the source of a given message, but he/she is unable to prove this source to a third party. However, the problem described above has not really been solved, and the denial authentication protocols are far from perfection in this problem.

Manuscript received November 5, 2006.
Manuscript revised November 25, 2006.

In 2002, Fan et al. applied the Deffie-Hellman algorithm [4] to propose a deniable authentication protocol. Their protocol does not need a public directory that is required by Dwork et al.'s [1] and Auman and Rabin's [2]. Since Fan et al.'s scheme does not support the message sender to verify whether the partial secret message, which is used to produce the session key, is generated by the original receiver or anyone else. Once the receiver seeks to conspire with the third party for their own benefits, the third party can be relegated to generate the partial secret message. On the other hand, the sender will not be able to see the difference. Under this circumstance, the generated session key is only shared by the sender and the third party, and the original receiver is not involved. Therefore, the original receiver can prove the source of receiving message to the third party. Namely, there seems to be a case of wicked problem-solving, the problem purported to be solved by the Fan et al.'s is indeed solved. However, new problems emerge following the resolution of the old.

In this letter, we propose an improved deniable authentication protocol. The authentication is deniable, no trusted third party is required, and any attack initiated by the person-in-the middle (PIM) can be resisted. In addition, it will not cause the problem which can be seen in Fan et al.'s as depicted above. The remaining text of this letter is organized as follows. Section 2 introduces and discusses Fan et al.'s protocol [4]. Section 3 introduces our proposed protocol. The security analysis and discussions will be presented in Section 4, followed by the conclusions in Section 5.

2. Fan et al.'s Deniable Authentication Protocol

In 2002, Fan et al. presented their deniable authentication protocol based on Deffie-Hellman Algorithm [4]. Three participants are required to execute their protocol: a sender, a receiver and an inquisitor INQ. The sender has a certificate issued by a certification authority (CA). The certificate contains the sender's public key (*PK*), and the signature of CA for this certificate. The receiver not only obtains the sender's public key, but also can verify it. The sender's secret key (*SK*) is kept secret by the sender him/herself. In this authentication protocol, both the sender and the receiver will use two public prime numbers

g and *n*, as did the original Deffie-Hellman protocol. Assume that A wants to send a message *M* to B. The detailed description of Fan et al.'s protocol is as follow:

Step 1: A chooses a random large number *x* and computes $X = g^x \bmod n$, $X' = E_{SK_A}(X)$, and then sends X' to B.

Step 2: B chooses a random large integer *y* and computes $Y = g^y \bmod n$ then he sends *Y* to A.

Step 3: B decrypts X' and gets $X = E_{PK_B}(X')$, and then B computes $k = X^y \bmod n$.

Step 4: A computes $k' = Y^x \bmod n$. Since $k = g^{xy} = k'$, now A and B share a session key *k*.

Step 5: A computes $D = H(k, M)$, and then A sends both *D* and *M* to B.

Step 6: After B receives the message, B computes $D' = H(k, M)$ and compares it with *D*. If they are equivalent, B accepts *M*; otherwise, rejects it.

In Fan et al.'s protocol, a sender not only needs to present his/her certificate but also needs to use his/her secret key to encrypt the partial secret message (shown in Step 1), which is used to generate a session key for both the sender and the receiver. The sender's secret key is only known by him/herself, a third party can not successfully cheat a receiver, and thus a potential PIM attack can be resisted in Fan et al.'s protocol. However, Fan et al. can only successfully prevent a third party from cheating the receiver. Their protocol does not provide a mechanism for mutual authentication. If there is a third party (called C) who performs Step 2 in Fan et al.'s protocol, and then sends Y to B. Then, B passes Y to A. A will not be able to see the difference. And hence, the generated session key will be known by A and C, rather than by A and B. After A uses the session key to send a message to B, B can simply pass it to C, and then, C can easily adopt Fan et al.'s protocol to authenticate the source of this received message. Under this circumstance, the deniable property guaranteed by Fan et al.'s protocol is violated. In order to rectify this problem, we propose a new deniable authentication protocol, which supports mutual authentication between the sender and the receiver and maintains crucial characteristics of deniable authentication. That is to say, the authentication is deniable, no trusted third party is required, and any attack initiated by the person-in-the middle (PIM) can be resisted.

3. Our Proposed Protocol

Our deniable authentication protocol requires three roles: the inquisitor INQ, the sender, and the receiver. Our protocol supports constant exchanges of messages between the sender and the receiver following the two parties' identities being authenticated. INQ then perches on the link between the sender and the receiver, intercepts the communication messages between them and then injects a message of his/her own.

In our protocol, the sender has a certificate issued by the certificate authority (CA). The certificate contains the sender's public key and signed by CA. Once the receiver gets the sender's certificate, he/she can verify the validity of the certificate and then he/she will obtain the sender's public key. The sender's secret key is kept secret by the sender him/herself. Assume that A wants to send a message M to B. Our proposed protocol is as follows:

Step 1: A randomly generates a session key k. Then, A uses his own secret key to compute $X = E_{SK_A}(k, T)$, *T* means the timestamp. Finally, A uses B's public key to encrypt X, and sends the encrypted message and his certificate to B.

Step 2: After receiving the above messages, B uses his secret key to decrypt the encrypted message. Then, B retrieves A's public key to decrypt X and to get k and T . Finally, B checks whether T is valid or not.

Step 3: If T is valid, B records k and computes $\bar{k} = H(k)$ and $Y = E_{SK_B}(\bar{k})$. Finally, B sends Y and B's certificate to A.

Step 4: After receiving the above message, A first verifies the validity of B's certificate. Then, A retrieves the public key from B's certificate to decrypt Y and to get $\bar{k}'$. If $\bar{k}' = H(k)$, A is convinced that the transmitter is B and performs Step 5; otherwise, A terminates the communication.

Step 5: A uses the session key k to compute D=H(k, M), H() is a collision-free hash function and sends both M and D to B.

Step 6: B computes $D' = H(k, M')$. If $D' = D$, B accepts M; otherwise, B rejects it.

4. Protocol Analyses

This section demonstrates that our proposed protocol is deniable, resists PIM attack, and provides both mutual authentication and efficiency. In addition, the receiver can not prove the source of a given message to a third party.

Property 1: The proposed protocol provides mutual authentication.
As described in Steps 1 to 4 in Section 3, while the sender A sends a session key to the receiver B, he needs to use his secret key to sign a session key, then sends both the signed session key and his certificate to B. B can verify the validity of A's certificate, then he can retrieve A's public key to verify the signed session key. Therefore, B can authenticate the source of a given message. In addition, our proposed protocol also requires B to sign the received session key using his secret key, and sends both the signed session key and B's certificate back to A. Since both A and B need to use their secret keys to encrypt the session key, they can authenticate each other's identities and sources of the messages. The mutual authentication is achieved in our proposed protocol.

Property 2: The proposed protocol is deniable.
As mentioned in Section 3, before the sender A uses a session key to transmit his secret message to the receiver B. Our proposed protocol requires B to sign the session key, and send both the signed session key and his certificate back. Therefore, A can make sure two things: one is the identity of his communication party is B, and the other is that B also knows the session key. Since not only A knows the session key but also B does, once B uses the session key to forge a message and to claim it is generated by A, A can deny this allegation. It follows that the proposed protocol is deniable.

Property 3: The proposed protocol is efficient.
In our protocol, participants can mutually authenticate each other according to Steps 1 to 4. After the sender A sends a message to the receiver B, if B wants to send another message to A, B can use the same session key continuously instead of initiating another new session key. Therefore, our proposed protocol is efficient for two participants to send messages to each other continuously.

Property 4: The proposed protocol resists PIM attack.
In our proposed protocol, participants have to authenticate each other before they transmit messages. The authentication approach is participants have to encrypt session keys using their own secret keys, and then send the sign session keys and their certificates to each other. An intruder can not act as a sender or a receiver without being discovered. Therefore, the PIM attack is neutralized.

Property 5: The receiver can not prove the source of a given message to a third party.
In Fan et al.'s protocol, this property can not be achieved, when there is a third party called C, who performs Step 2 and the receiver B passes it to A for C. Then, the session key will be only known by A and C rather than by A and B. After B receives the messages M and D, he can only pass them to C. B can successfully prove the source of the message M to C according to Step 6 of Fan et al.'s protocol.

5. Conclusions

In 2002, Fan et al. proposed a deniable authentication protocol. However, their protocol remains some security flaws which could compromise the deniable authentication properties. In addition, their protocol suffers lacking of efficiency when two participants are engaged in constant exchanges of messages. In this letter, we propose another approach to satisfy the deniable authentication requirements. According to the properties shown above, it is obvious that our proposed protocol supporting mutual authentication, is deniable, secure, and efficient. Thus, it is a substantial improvement over Fan et al.'s.

References

[1] Dwork, C. Nair, M., and Sahai, A., "Concurrent Zero-knowledge," *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, May 1998, Dallas,, Texas, USA, pp. 409-418.
[2] Aumann, Y. and Rabin, M., "Efficient Deniable Authentication of Long Message," *Proceedings of International Conference on Theoretical Computer Science*, in Honour of Professor Manuel Blum's 60th Birthday, April 1998, Hong Kong, China.
[3] Deng, X., Lee, C.-H., and Zhu, H., "Deniable Authentication Protocols," *IEE Proceedings of Computers and Digital Techniques*, Vol. 148, March 2001, pp. 101-104.
[4] Fan, L., Xu, C.-X., and Li, J.-H., "Deniable Authentication Protocol Based on Deffie-Hellman Algorithm," *IEE Electronics Letters*, Vol. 38, No. 4, July 2002, pp. 705-706.

Chia-Chen Lin received her B.S. degree in information management in 1992 from the Tamkang University, Taipei, Taiwan. She received both her M.S. degree in information management in 1994 and Ph.D. degree in information management in 1998 from the National Chiao Tung University, Hsinchu, Taiwan. Dr. Lin is currently an associate professor of the Department of Computer Science and Information Management, Providence University, Sha-Lu, Taiwan. Her research interests include image and signal processing, image hiding, mobile agent, and electronic commerce security.

Chin-Chen Chang received his BS degree in applied mathematics in 1977 and the MS degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980-1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University. From 1983-1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From August 1989 to July 1992, he was the head of, and a professor in, the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the dean of the college of Engineering at the same university. From August 1995 to October 1997, he was the provost at the National Chung Cheng University. From September 1996 to October 1997, Dr. Chang was the Acting President at the National Chung Cheng University. From July 1998 to June 2000, he was the director of Advisory Office of the Ministry of Education of the R.O.C. From 2002 to 2005, he was a Chair Professor of National Chung Cheng University. Since February 2005, he has been a Chair Professor of Feng Chia University. In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, image compression and data structures.