Chaos Function Based - Secure Deniable Authentication Protocol

[1]R.Gnanajeyaraman, [2]S.Sasidharan

[1&2]*Dept. of IT, Kongunadu College of Engineering & Technology, Thottiam, Trichy, Tamilnadu, India-621215*

[1]r.gnanajeyaraman@gmail.com,[2]sasi.it@gmail.com

Abstract - Deniability is defined as a privacy property which enables protocol principals to deny their involvement after they had taken part in a particular protocol run. This paper demonstrates that Yoon & Yoo's scheme is insecure to a Key-Compromise Impersonation (KCI) attack and Replay attack. Based on this, propose an Enhanced Scheme which preserves the authenticity, deniability and resistance against the KCI attack ing Chaos function f(x) = 4 * x * (1-x) and Replay attack ing Timestamp. This paper demonstrates that Yoon and Yoo's scheme "Secure Deniable Authentication Protocol Based on ElGamal Cryptography" is sceptible to KCI attack and replay attack. To mitigate this security breach, propose an improved deniable authentication protocol based on Chaos Function and ElGamal Cryptography. future work is to e this proposed Deniable Authentication Protocol for Micro Payment and Macro Payment in E-Commerce applications.

Keyword: Deniable, Authentication, ElGamal Cryptography, Chaos Function, KCI attack.

I. INTRODUCTION

The Deniable Authentication Protocol [1, 4, 5, 7-9] is a new technique of modern cryptography, compared with traditional authentication, it has two characteristics; first, a receiver can verify the sce of the message as in the traditional authentication protocol. Second, a receiver cannot prove the sce of the message to a third party. In 2005, Wang et al. [8] proposed an efficient deniable authentication protocol (WLT), which makes e of the inverse of the ElGamal cryptosystem. It requires less computational complexity and communication cost. In 2006, Shao et al. [7] hover, pointed out that the WLT protocol is insecure to a person-in the middle attack. That is in the whole process, the receiver cannot be aware of the existence of the adversary as ll as the modification of the messages. They have also proposed an improved deniable authentication protocol (SCL) based on ElGamal cryptography [3]. In 2008 Yoon and Yoo [9] pointed out that Shao et al.[7] scheme still suffers from person-in-the middle attack. They proposed one secure deniable authentication protocol based on ElGamal cryptography [3]. Hover, this paper points out that all the above schemes suffer from Key-Compromise Impersonation (KCI) attack [5] and replay attack. Once if the long-term secret key of any er is compromised, the total security of the communication will be compromised. Deniable Authentication Protocol is ed under certain circumstances such as electronic voting system, online shopping and negotiation over the internet. In these systems, security of communication plays a major role. In a distributed environment denial of service (DOS) attack is the most common one. Replay attack is one kind of DOS attack. In improved protocol achieve the resistance to KCI attack by ing chaos function. An algorithm ing one of the simplest chaotic function [6] f(x) =4*x*(1-x) is ed.

II. RELATED WORK

In the past several years, numero deniable authentication protocols have been proposed but many of them have also been proven to be vulnerable to vario cryptanalytic attacks [15-17]. The concept of deniable authentication protocol was initially introduced by Dwork et al. [18], which is based on the concurrent zero knowledge proof. Hover, this scheme requires a timing constraint. Not only that, the proof of knowledge is also time-consuming [1]. Another notable scheme which was developed by Aumann and Rabin [11, 12] is based on the intractability of the factoring problem, in which a set of public data is needed to authenticate one bit of a given message. Few years later, Deng et al. [1] have proposed two deniable authentication schemes based on Aumann and Rabin's scheme. The proposed scheme are based on the intractability of the factoring problem and the logarithm problem. Hover, in 2006, Zhu et al. [17] have successfully demonstrated the Man-in-the-Middle attack against Aumann and Rabin's scheme and this indirectly results in an insecure implementation of Deng et al., schemes. In 2003, Boyd and Mao [13] have proposed another deniable authenticated key establishment for Internet protocols based on elliptic curve cryptography. These schemes are believed to be able to solute the complexity of computation and appear to be more efficient than others but their vulnerability to KCI attack has been exploited by Chou et al. [] in 2005. Besides that, Fan et al. [4] have proposed a simple deniable authentication protocol based on Diffie-Hellman key distribution protocol in 2002. Unfortunately, in 2005, Yoon et al. [16] have pointed out that their protocol suffers from the intruder

masquerading attack and subsequently proposed their enhanced deniable authentication protocol based on Fan et al.'s scheme.

In addition, in 2005, Cao et al. [14] have proposed an efficient ID-based deniable authentication protocol which enables a dynamic shared secret to be derived as a session key. Unfortunately, in 2006, Yoon et al.'s enhanced scheme and Cao et al.'s scheme are proven to be impractical and sceptible to KCI attack respectively by Chou et al. [15]. Moreover, Chou et al. have proposed another new deniable authentication protocol [15] and they have claimed that their proposed protocol has achieved strong deniability as ll as authenticity with great resistance against KCI attack. In 2007, Meng-Hui Lim et al. [5] have proved that Chou et al.'s scheme provides inadequate resistance against KCI attack. In 2008, Eun-Jun Yoon et al. [9] has proposed one deniable authentication protocol which is based on Elgamal Cryptography.

III. KCI Attack On Yoon And Yoo's Scheme

The list of terms and their definitions ed in Yoon and Yoo's scheme [9] and scheme are given in Table1.

TABLE 1

Terms	Meanings
S	Sender
R	Receiver
p	Prime Number
g	Primitive Root
x_s	Sender's private key
y_s	Sender's Public key
x_r	Receiver's private key
y_r	Receiver's Public key
DH	Shared key
a	Random number a € Zp
H()	One way hash function
||	Concatenation Symbol
M	Message to send
rk_i	Random session key generated by chaotic function
T	Timestamp

In this section, will depict how Yoon and Yoo's [9] scheme can be intruded by 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 E, has the knowledge of sender's private key xs and he intends to launch the KCI attack against sender by pretending receiver to communicate with sender.

Step 1: Adversary E chooses a random number a' and computes DH by ing the equation DH = y_r^{xs} mod p and A' and C1'. Then, he initiates the communication by sending A' and C1'.

Step 2: After receiving A', C1', sender thought that receiver is trying to communicate with him. He verifies the received value from receiver, if the verification is successful, sender truly believes that he is communicating with receiver although he is in fact communicating with adversary E. Hence, KCI attack is successful.

Step 3: Sender chooses the message M and it computes C2 and C3.

As know that, Deniable Authentication Protocol is ed in sensitive area like Electronic Voting System, Online shopping, negotiation over the Internet in which security of communication is more important. But demonstrated that Yoon and Yoo's Scheme is insecure against KCI attack.

IV. Enhanced Scheme

As have noticed in the previo section, Yoon and Yoo's [9] Scheme has fallen into the KCI attack mainly due to their failure in concealing the value of C1 and C2 when x_s (x_r) is exposed. Once the adversary has obtained x_s (x_r), he is able to derive all the subsequent parameters as ll as the message. In other words, the values of C1 and C2 should be obscured even if x_s or x_r has been compromised so as to resist the KCI attack. For this purpose, e a Chaotic function [6] f(x) = 4 * x * (1-x) for calculating the random key and communicate Chaotic function and their parameters through telephone and other parameters through network. So, assumption is Intruder have no idea to tap the message through network and telephone lines at the same time. Partial listening (tapping) of information either through telephone or network should not allow the Adversary to launch the KCI attack.

A. Chaos Function

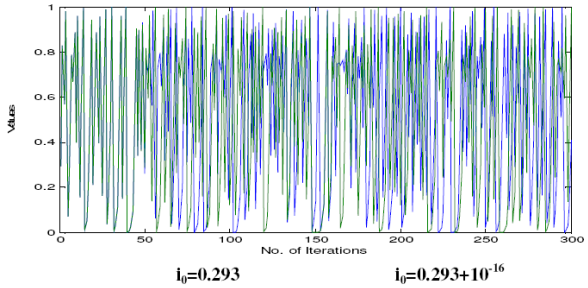
Chaotic functions [6] which re first studied in the 1960's show numero interesting properties. The iterative values generated from such functions are completely random in nature although limited beten bounds. However, the most fascinating aspect of these functions is their extreme sensitiveness to initial condition. A slight difference in the Initial Starting value i.e., i_0 leads to substantial difference in the obtained iterative values. This is tabulated in Table 2.

TABLE 2

Error in the Starting Value	Iteration number after which the difference in values > 0.0625
1 E -02	5

1 E-05	14
1 E-10	26
1 E-16	49

The divergence of obtained Chaos values for jt a small disturbance in initial starting value can be seen much more clearly in Figure 1.



i_0=0.293 i_0=0.293+10^{-16}

Figure 1: Iterative values obtained for two different starts

1. Generating Values from Chaos Function

The chaotic function which have considered is f(x) = 4 * x * (1-x). To generate the values from this chaotic function the following three factors have to be first decided.

1. The starting value for the iteration (i_0).
2. The number of iterations after which the first value can be picked for generating keys.
3. The number of iterations to be maintained beten 2 picked values thereafter.

For example,
Start Value – 0.293
First iteration to be considered – 119
Number of iterations for separation – 27
This will provide the set of values.

2. Generation of random session key from chaotic values

It is proposed that the values yielded by the Chaos function are converted to Binary fractions whose first 16 bits are taken and their decimal equivalent will be ed as the random session key.
$rk_i = (b_0\text{-}b_{15}$ of chaotic values$)_{10}$ 1<= i <n.

B. Proposed Deniable Authentication Protocol

This section proposes an improved Deniable Authentication Protocol to solve the security problems mentioned in Section 3. There are f steps in the proposed protocol as follows.

Step 1: The Receiver R first computes Diffie-Hellman value DH= y_s^{xr} mod p by ing Sender's Public key y_s and his/her own private key x_r. Then R chooses a Random number a € Zp * and computes A=g^a mod p and C1=H (A || DH || rk), and finally sends A and C1 to the Sender S while keeping 'a' secret.

Step 2: After receiving A and C1 from R, S computes Diffie-Hellman value DH = y_r^{xs} mod p by ing Receiver's Public key y_r and his/her own private key x_s. S checks

C1=H (A || DH || rk).

If this equation holds, then S authenticates R; otherwise, values are rejected. When S wants to send a message M to R, he/she computes
C2=A^{xs} M. rk mod p, C4 = H (rk || T) and C3=H (M || rk).
S finally sends (C2, C3, C4, T) to R. Further communications will be continued by varying timestamp alone without varying random key in order to reduce the computational complexity.

Step 3: R first checks C4=H (rk || T). If this equation holds, step 4 will be processed. Otherwise request is rejected.
Step 4: R gets the message M by M = C2 mod p and checks C3=H (M || rk). If this equation holds, then R accepts the message M; otherwise message is rejected.

V. PROPOSED PROTOCOL

Security Analysis

In this section, will scrutinize enhanced DAP ing Chaos function in order to ensure that the security requirements for a Deniable Authentication Protocol are satisfied.

Lemma 1: Enhanced Protocol is Deniable

Proof: Once (C2, C3, C4) is received and verified, Receiver can easily identify the sce of the message M, since the message is integrated with Sender's private key and random key. After verification Receiver R can be assured that the message originated from Sender S. If receiver R intends to expose the message Sender's identity to a third party, Sender S would be able to repudiate as he/she would argue that receiver R could also generate (C2, C3, C4) by ing Sender's public key, random number and random key. Hence the deniability property is satisfied.

Lemma 2: The proposed protocol provides Mutual Authentication

Proof: In Step 2, Sender S checks C1 = H (A || DH || rk) to authenticate the Receiver R. In Step 3, the Receiver R also checks C4= H (rk || T) to authenticate the Sender S.

Lemma 3: The enhanced protocol is able to resist the KCI attack.

Proof: The resistance of the enhanced protocol towards KCI attack is analyzed by considering the following 2 scenarios.

a. Receiver's Private Key x_r, has been compromised.
Initially, the Receiver R (Adversary E) chooses a random number a', computes A' and computes C1' = H (A' || DH || rk') and sends it to Sender S. ?

Sender S first checks C1=H (A'|| DH || rk). If this equation does not hold, Sender S terminates the session.

b. Sender's Private Key x_s, has been compromised.

Initially, the Receiver R chooses a random number a, computes A and C1 = H (A || DH || rk) and sends it to S. Adversary (E) intercepts (A, C1) and he omits the C1 computation. He is not able to compute C1 and checks the received value, becae he doesn't know the rk value. Adversary E chooses a Message M' and a random key rk' and computes C2', C4' and C3' as follows.

$$C2' = A^{xs}. M. rk' \bmod p$$
$$C4' = H(rk' || T)$$
$$C3' = H (M' || rk')$$

Receiver R checks the C4 value. If it is invalid, Receiver R confirms that there is an intruder and terminates further communication.

Lemma 4: The enhanced protocol is able to resist the Replay attack.

Proof: In the proposed protocol, Time stamp T and Random Key rk is included in constructing the parameter C4 and sends the quadruple(C2,C3, C4,T) to Receiver R. R first computes C4 value. If it is invalid, R rejects the message. By this way replay attack is avoided.

Lemma 5: The enhanced protocol withstands the Person-in the Middle attack.

Proof: In the Proposed protocol to do a Person-in the Middle attack, Adversary mt impersonate like S with R and R with S. For this purpose the attacker is required to know Axs or ysa and rk. This is equivalent to solving discrete logarithmic problem and solving chaos function. Therefore the proposed protocol withstands the Person-in the Middle attack.

VI. Conclusion And Future Work

This paper demonstrates that Yoon and Yoo's scheme "Secure Deniable Authentication Protocol Based on ElGamal Cryptography" is sceptible to KCI attack and replay attack. To mitigate this security breach, propose an improved deniable authentication protocol based on Chaos Function and ElGamal Cryptography. future work is to e this proposed Deniable Authentication Protocol for Micro Payment and Macro Payment in E-Commerce applications.

References

[1] X. Deng, C. H. Lee, and H. Zhu, "Deniable Authentication Protocols",IEEE Proc., Comput. Digit. Tech., Vol. 148(2), pp.101-104, 2001.

[2] W. Diffie, and M. E. Hellman, "New directions in cryptography", IEEE Trans. Inf.Theory, Vol. 10(6), pp. 644-654, 1976.

[3] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms", IEEE Trans Information Theory, Volume 31,pp.469-472,1985.

[4] L. Fan, C. X. Xu, and J. H. Li, "Deniable Authentication Protocol Based on Diffie-Hellman algorithm", Electron. Lett., Volume 38(14),pp.705-706,2002.

[5] Meng-Hui Lim, Sanggon Lee, Youngho Park and Hoonjae Lee,"An Enhanced ID-based Deniable Authentication Protocol on Pairings", in Computational Science and its Applications – ICCSA 2007, Vol. 4706, pp.1008-1017, 2007.

[6] Dr. Ranjan Bose and Amitabha Banerjee, " Implementing Symmetric Cryptography ing Chaos Functions", Electrical Engineering Department, Indian Institute of Technology, New Delhi.

[7] J. Shao, Z. Cao, and R. Lu., "An improved Deniable Authentication Protocol", in Networks, Volume 48, pp. 179-181, 2006.

[8] Y. Wang, J. Li and L. Tie. "A simple protocol for deniable authentication based on ElGamal cryptography", in Networks, Vol. 45, pp. 193-194, 2005.

[9] Eun-Jun Yoon and Kee-Young Yoo, "Secure Deniable Authentication Protocol Based on ElGamal Cryptography", in Information Security and Assurance, 2008, ISA 2008 International conference, IEEE, pp. 36-39.

[10] E. J. Yoon, and K. Y. Yoo, "Security analysis of Hsieh-Sun's deniable authentication protocol", in International Conference on Hybrid Information Technology(ICHIT 06), Vol. 2, pp. 45-48, Nov. 2006.

[11] Yonatan Aumann, Michael O. Rabin, "Authentication, Enhanced Security and Error Correcting Codes" (Extended Abstract). CRYPTO 1998, 299-303.

[12] Yonatan Aumann, Michael O. Rabin, "Efficient Deniable Authentication of Long Messages", Inf. Conf. on Theoretical Computer Science in hon of Professor Manuel Blum's 60th birthday, 1998.

[13] C. Boyd, W. Mao, K.G. Paterson, "Deniable authenticated key establishment for Internet Protocols", 11th international workshop on security protocols, Cambridge (UK), April 2003.

[14] T. J. Cao, D. D. Lin and R. Xue, "An Efficient ID-based Deniable Authentication Protocol from pairings", Proceedings of the 19th international conference on Advanced Information Networking and Applications (AINA '05).

[15] J. S. Chou, Y. L. Chen and M. D. Yang, "awakens of the Boyd-Mao Deniable Authenticated key Establishment for Internet Protocols", Cryptology ePrint Archive: Report, (451) (2005).

[16] E. J. Yoon, E. K. Ryu, K. Y. Yoo, "Improvement of Fan et al.'s Deniable Authentication Protocol based on Diffie-Hellman Algorithm" ,Applied Mathematics and Computation, Vol. 167 (1), Augtn 2005, pp. 274-280.

[17] Robert W. Zhu, Duncan S. Wong, and Chan H. Lee, "Cryptanalysis of a suite of Deniable Authentication Protocols", IEEE Communication Letters , Vol. 10, No. 6, June 2006, pp. 504-506.

[18] C. Dwork, M. Naor, A. Sahai, "Concurrent Zero-Knowledge", Proc. 0th ACM STOC '98, Dallas TX, A, 1998, pp. 409-418.

[19] J. S. Chou, Y. L. Chen and J. C. Huang, "A ID-Based Deniable Authentication Protocol on Pairings", Cryptology ePrint Archive: Report, (335) (2006).
[20] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.