Comments on a novel user authentication and key agreement scheme

Jia-Lun Tsai

Department of Information Management

National Taiwan University of Science and Technology, Taipei 106, Taiwan

crousekimo@yahoo.com.tw

Abstract

In 2013, Sun et al. showed that the related works' authentication schemes proposed by [2-7] are vulnerable to an insider attack and fail to provide mutual authentication. These two attacks can be successfully plotted by an adversary, since the private key of the server can compute all the legal users' private keys. They then proposed a new remote user authentication and key agreement scheme for the mobile client-server environment. However, we find that their scheme is still vulnerable to insider attack (Sun et al.) and how to avoid such an insider attack on the client-server environment is still an open problem.

Keyword: user authentication, key agreement, client-server environment, insider attack, mutual authentication

1. Introduction

A remote user authentication scheme is a security mechanism for a network system which allows a remote user and a server to authenticate each other via an insecure network. Recently, with the wide popularity of mobile devices (e.g., smart phones), people can access many electronic transactions, such as online shopping, Internet banking, e-payment, e-voting and pay-TV anywhere anytime. However, since mobile

devices usually have limited energy resources and computing ability, with most remote user authentication schemes unsuitable for the mobile device environment due to the requirements of expensive computations and the burden of heavy certification.

In 2013, Sun et al. [1] found that the previous ID-based remote user authentication and key agreement schemes [2-7] are vulnerable to a weakness, i.e., the server can produce all users' private keys with its private key. Based on this weakness, these schemes are vulnerable to an insider attack proposed by them (Sun et al.) and cannot achieve mutual authentication. In addition, they discovered that some of these schemes do not provide user anonymity [2, 3, 7], perfect forward secrecy [2, 3], or leakage of session temporary secrets resistance [2, 3, 7]. To improve security, they also proposed a novel remote user authentication and key agreement scheme. In this study, we show that the authentication scheme proposed by Sun et al. cannot resist their proposed insider attack. Therefore, how to avoid insider attack on the client-server environment is still an open problem.

Table 1 Notations

Notation	Description
Q	a large prime number
G	a cyclic additive group of order q
P	the generator of G
ID_C, CID_C	the identity and the dynamic identity of a user C
s_C, x_C	the private key of a user C
PK_C, X_C	the public key of a user C
S	the private key and its corresponding public key of the server S
H_1, H_2, H_3, H_4	collision-free one-way hash functions
$[]_x$	the x-coordinate of a Point y

2. Review of Sun et al.'s authentication scheme

The authentication scheme proposed by Sun et al. [1] consists of three phases: system setup phase, client registration phase, and user authentication and key agreement phase. The notations are illustrated in Table I with the details of each phase described as follows.

***System setup phase*:** Let G be a cyclic additive group of order q, where P is the generator of G. Given a security parameter k, S selects a finite field F_p and we define an elliptic curve E: $y_2 \equiv x^3+ax+b \bmod p$ over F_p, where $a,b \in F_p$ and $p \geq 3,4a^3+27b^2$ 60 mod p. Next, S chooses a random number $s \in Z_q^*$ as the master private key, and then computes its corresponding master public key $P_{pub}=sP$. After that, S chooses four cryptographic hash functions H_1: $\{0,1\}^* \times G \rightarrow Z_q^*$, H_2: $\{0,1\}^* \times G_3 \rightarrow \{0,1\}^k$, H_3: $\{0,1\}^* \times G_4 \rightarrow \{0,1\}^k$ and H_4: $\{0,1\}^* \times G_5 \rightarrow \{0,1\}^k$. Finally, S publishes the system parameters $\{F_q, E, G, P, P_{pub}, H_1, H_2, H_3, H_4\}$ and keeps s as secret.

***Client registration phase*:** If a client C with a low-power computing device wants to register on the server S, he/she and the server S perform as follows.

Step1. C computes $X_C = x_C P$, and then sends (ID_C, X_C) to S via a secure channel, where $x_C \in Z_q^*$ is a secret random number.

Step2. Upon receiving (ID_C, X_C) from C, S computes $W_C = X_C + y_C P$ and $d_C = (H_1(ID_C, W_C)s - y_C) \bmod q$, and then sends (W_C, d_C) back to C via a secure channel, where $y_C \in Z_q^*$ *is a random number*.

Step3. C computes $s_C = (d_C - x_C) \bmod q$ and $PK_C = s_C P$, and then C sets (s_C, x_C) and (PK_C, X_C) as his/her private key and corresponding public key, respectively. Notice that the everyone that received W_C can compute $PK_C = H_1(ID_C, W_C)P_{pub} - W_C$.

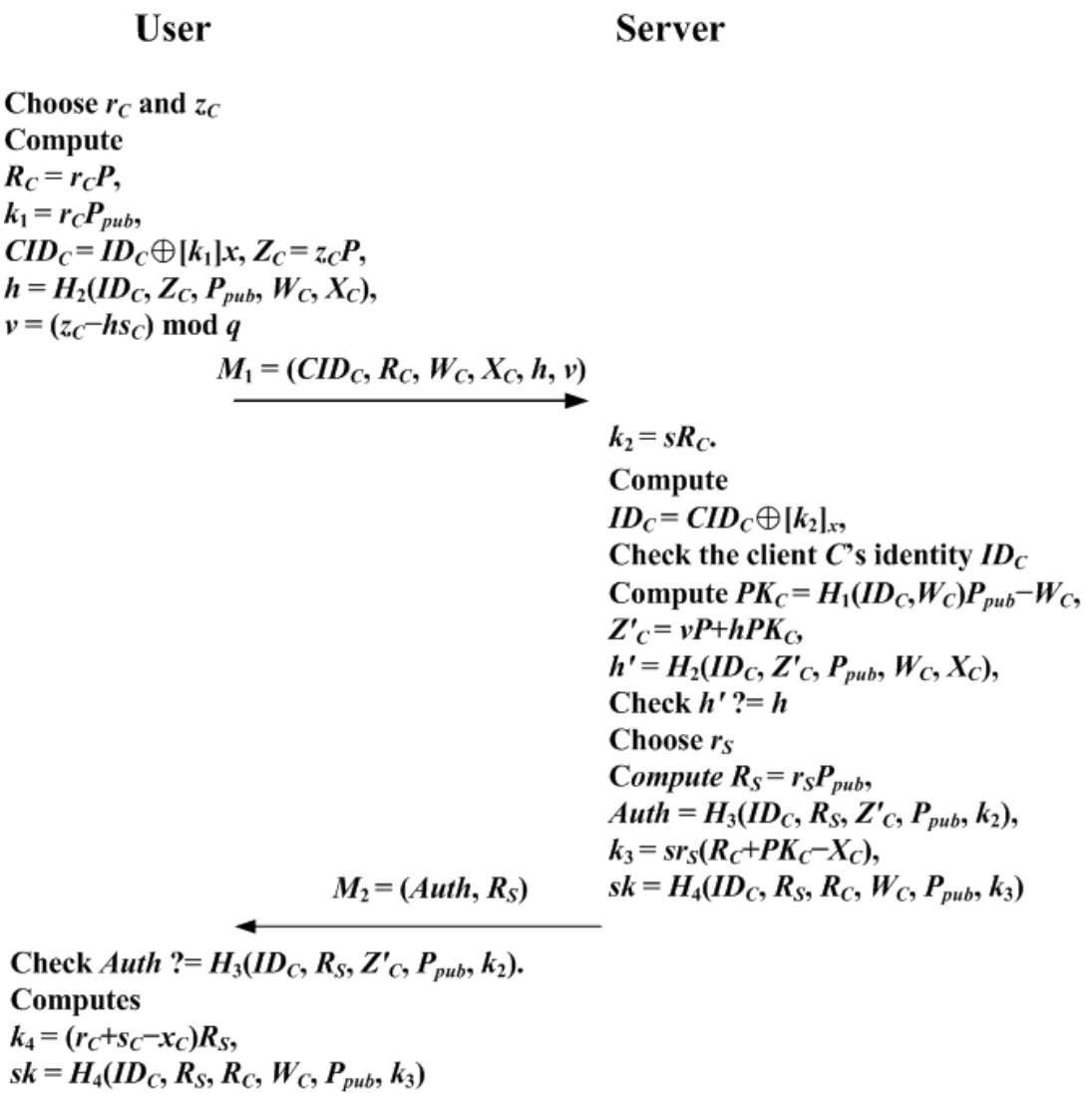

Fig. 1 User authentication and key agreement phase of the authentication scheme proposed by Sun et al.

***User authentication and key agreement phase*:** If a client C with a low-power computing device wants to access the server S, he/she and the server S perform the following steps. The phase is depicted in Fig. 1.

Step1. C computes $R_C = r_C P$, $k_1 = r_C P_{pub}$, $CID_C = ID_C \oplus [k_1]_x$, $Z_C = z_C P$, $h = H_2(ID_C, Z_C, P_{pub}, W_C, X_C)$, and $v = (z_C - hs_C) \bmod q$, where $r_C, z_C \in Z_q^*$ are two random numbers. Next, C sends $M_1 = (CID_C, R_C, W_C, X_C, h, v)$ to S.

Step2. Upon receiving M_1 from C, S computes $k_2 = sR_C$. Next, S retrieves C's

identity ID_C by computing $ID_C = CID_C \oplus [k_2]_x$, and then checks C's identity ID_C. If ID_C is valid, S continues to the following steps. Otherwise, S rejects C's login request.

Step3. S computes $PK_C = H_1(ID_C, W_C)P_{pub} - W_C$, $Z'_C = vP + hPK_C$ and $h' = H_2(ID_C, Z'_C, P_{pub}, W_C, X_C)$, and then checks whether h' is the same as h. If they are not the same, S rejects C's login request. Otherwise, S computes $R_S = r_S P_{pub}$, $Auth = H_3(ID_C, R_S, Z'_C, P_{pub}, k_2)$, $k_3 = sr_S(R_C + PK_C - X_C)$ and $sk = H_4(ID_C, R_S, R_C, W_C, P_{pub}, k_3)$, where $r_S \in Z_q^*$ is a random number. After that, S sends $M_2 = (Auth, R_S)$ to C.

Step4. Upon receiving M_2 from S, C checks whether $Auth$ is the same as $H_3(ID_C, R_S, Z'_C, P_{pub}, k_2)$. If they are the same, then C computes $k_4 = (r_C + s_C - x_C)R_S$ and $sk = H_4(ID_C, R_S, R_C, W_C, P_{pub}, k_3)$.

3. Weaknesses on the authentication scheme of Sun et al.

This section shows that the authentication scheme proposed by Sun et al. is still vulnerable to their insider attack, since the server in their scheme cannot check the validity of the user partial public key. Details of the attack are described as follows.

Assume that a privileged insider of the server has the master private key s of the server. The privileged insider then chooses a random number $x''_C \in Z_q^*$, and then computes $X''_C = x''_C P$, $W''_C = X''_C + y''_C P$ and $d''_C = (H_1(ID_C, W''_C)s - y''_C) \bmod q$. Next, the privileged insider computes $s''_C = (d''_C - x''_C) \bmod q$ and $PK''_C = s''_C P$, and then C computes $R''_C = r''_C P$, $k''_1 = r''_C P_{pub}$, $CID''_C = ID_C \oplus [k''_1]_{x''}$, $Z''_C = z''_C P$, $h'' = H_2(ID_C, Z''_C, P_{pub}, W''_C, X''_C)$, and $v'' = (z''_C - h''s''_C) \bmod q$, where $r''_C, z''_C \in Z_q^*$ are two random numbers. Next, the privileged insider sends $M_1 = (CID''_C, R''_C, W''_C, X''_C, h'', v'')$ to the server S. Since the server S cannot check whether $PK''_C = H_1(ID_C, W''_C)P_{pub} - W''_C$ is

forged by the privileged insider, the server S will use the forged public key (PK''_C, X''_C) to authenticate the privileged insider, so S computes $PK''_C = H_1(ID_C, W''_C)P_{pub} - W''_C$, $Z'''_C = v''P + h''PK_C$ and $h''' = H_2(ID_C, Z'''_C, P_{pub}, W''_C, X''_C)$. Obviously, the computed h''' *is* the same as the received h''. Hence, the privileged insider can masquerade as any legal user to access S if he/she learns the master private key s.

From the above attack, we can find that the insider attack proposed by Sun et al. cannot be avoided, since the server cannot check whether the partial public key is forged. The reader may think that the server can store the public keys of the users into its database to overcome this weakness. However, if a privileged insider can steal the server's private key from the server, he/she also can modify or learn the public keys of all users from the database of the server. Hence, how to avoid their insider attack on the client-server environment is still an open problem.

4. Conclusion

In this paper, we show that the authentication scheme proposed by Sun et al. is still vulnerable to the insider attack proposed by them (Sun et al.). Hence, how to avoid such an insider attack on the client-server environment is still an open problem.

Reference

[1] H. Sun, Q. Wen, H. Zhang and Z. Jin, A novel remote user authentication and key agreement scheme for mobile client-server environment, Appl. Math. Inf. Sci. 7(4), 1365-1374 (2013).

[2] T. Wu and Y. Tseng, An efficient client authentication and key agreement protocol for mobile client-server environment, Computer Networks 54, 1520-1530 (2010).

[3] D. He, An efficient remote user authentication and key agreement protocol for mobile client-server environment from pairings, Ad Hoc Networks 10(6),

1009-1016 (2012).

[4] J. Yang and C. Chang, An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Computers & Security 28(3-4), 138-143 (2009).

[5] E. Yoon and K. Yoo, Robust ID-based remote mutual authentication with key agreement scheme for mobile devices on ecc, IEEE International Conference on Computational Science and Engineering, 633-640 (2009).

[6] S. Islam and G. Biswas, A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Journal of Systems and Software 84(11), 1892-1898 (2011).

[12] T. Truong, M. Tran and A. Duong, Improvement of the more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on ECC, The 26th Conference on Advanced Information Networking and Applications Workshops, 698-703 (2012).

[7] D. He, J. Chen and J. Hu, An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security, Information fusion 13(3), 223-230 (2012).