Comments on an Advanced Dynamic ID-Based Authentication Scheme for Cloud Computing

Ding Wang[1,2], Ying Mei[1], Chun-guang Ma[2], and Zhen-shan Cui[2]

[1] Department of Training, Automobile Sergeant Institute of PLA, Bengbu, China
[2] Harbin Engineering University, Harbin City 150001, China
wangdingg@mail.nankai.edu.cn

Abstract. The design of secure remote user authentication schemes for mobile devices in Cloud Computing is still an open and quite challenging problem, though many such schemes have been published lately. Recently, Chen et al. pointed out that Yang and Chang's ID-based authentication scheme based on elliptic curve cryptography (ECC) is vulnerable to various attacks, and then presented an improved password based authentication scheme using ECC to overcome the drawbacks. Based on heuristic security analysis, Chen et al. claimed that their scheme is more secure and can withstand all related attacks. In this paper, however, we show that Chen et al.'s scheme cannot achieve the claimed security goals and report its flaws: (1) It is vulnerable to offline password guessing attack; (2) It fails to preserve user anonymity; (3) It is prone to key compromise impersonation attack; (4) It suffers from the clock synchronization problem. The cryptanalysis demonstrates that the scheme under study is unfit for practical use in Cloud Computing environment.

Keywords: Dynamic ID, Authentication protocol, Elliptic curve cryptography, Cryptanalysis, Cloud Computing.

1 Introduction

With the advent of the Cloud Computing era, various services are provided on cloud to allow mobile users to manage their businesses, store data and use cloud services without investing in new infrastructure. Generally, the cloud infrastructure provides various kinds of services in a distributed environment, while sharing resources and the storage of data in a remote data center. Without knowledge of, expertise in, or control over the cloud infrastructure, mobile users can access data or request services anytime and anywhere, and thus it is of great concern to protect the users and the systems' privacy and security from malicious adversaries [16]. Accordingly, user authentication becomes an important security mechanism for remote systems to assure the legitimacy of the communication participants by acquisition of corroborative evidence.

In 2009, Yang and Chang [15] presented an identity-based remote user authentication scheme for mobile users based on ECC. Although the Yang-Chang's scheme preserves advantages of both the elliptic curve and identity-based cryptosystems, and is efficient than most of the previous schemes, in 2011, Islam et

F.L. Wang et al. (Eds.): WISM 2012, LNCS 7529, pp. 249–256, 2012.

al. [6] showed that the Yang-Chang's scheme suffers from clock synchronization problem, known session-specific temporary information attack, no provision of user anonymity and forward secrecy. Almost at the same time, Chen et al. [3] also identified two other security flaws, i.e. insider attack and impersonation attack, in Yang-Chang's scheme. To remedy these security flaws, Chen et al. further proposed an advanced password based authentication scheme using ECC. The authors claimed that their improved scheme provides mutual authentication and is free from all known cryptographic attacks, such as replay attack, impersonation attack and known session-specific temporary information attack, and is suitable for Cloud Computing environment.

In this paper, however, we will show that, although Chen et al.'s scheme is superior to the previous solutions for implementation on mobile devices, we find their scheme cannot achieve the claimed security: their scheme is vulnerable to offline password guessing attack, and key compromise impersonation attack, and suffers from clock synchronization problem. In addition, their scheme fails to preserve user anonymity, which is an important objective in their scheme.

The remainder of this paper is organized as follows: in Section 2, we review Chen et al.'s scheme. Section 3 describes the weaknesses of Chen et al.'s scheme. Section 4 concludes the paper.

2 Review of Chen et al.'s Scheme

In this section, we examine the identity-based remote user authentication scheme for mobile users based on ECC proposed by Chen et al. [3] in 2011. Chen et al.'s scheme, summarized in Fig.1, consists of three phases: the system initialization phase, the registration phase, the authentication and session key agreement phase. For ease of presentation, we employ some intuitive abbreviations and notations listed in Table 1. We will follow the original notations in Chen et al.'s scheme as closely as possible.

Table 1. Notations

Symbol	Description
U_A	the user A
S	remote server
ID_A	identity of user U_A
$\oplus$	the bitwise XOR operation
$\|$	the string concatenation operation
$h(\cdot)$	collision free one-way hash function
q_s	secret key of remote server S
$\mathcal{O}$	the point at infinity
$\mathcal{P}$	base point of the elliptic curve group of order n such that $n \cdot \mathcal{P} = \mathcal{O}$
Q_s	public key of remote server S, where $\mathcal{Q}_s = q_s \cdot \mathcal{P}$
$A \rightarrow B : M$	message M is transferred through a common channel from A to B
$A \Rightarrow B : M$	message M is transferred through a secure channel from A to B

2.1 The System Initialization Phase

Before the system begins, server S performs as follows:

Step S1. S chooses an elliptic curve equation $E_P(a, b)$ with order n.
Step S2. Selects a base point P with the order n over $E_P(a, b)$, where n is a large number for the security considerations. And then, S computes its private/public key pair (q_s, Q_s) where $Q_S = q_s \cdot P$
Step S3. Chooses three one-way hash functions $H_1(\cdot)$, $H_2(\cdot)$ and $H_3(\cdot)$, where $H_1(\cdot) : \{0,1\} \rightarrow G_p$, $H_2(\cdot) : \{0,1\} \rightarrow Z_P^*$ and $H_3(\cdot) : \{0,1\} \rightarrow Z_P^*$, where G_p denotes a cyclic addition group of P.
Step S4. Stores q_s as a private key and publishes message $\{E_p(a, b), P, H_1(\cdot), H_2(\cdot), H_3(\cdot), Q_s\}$.

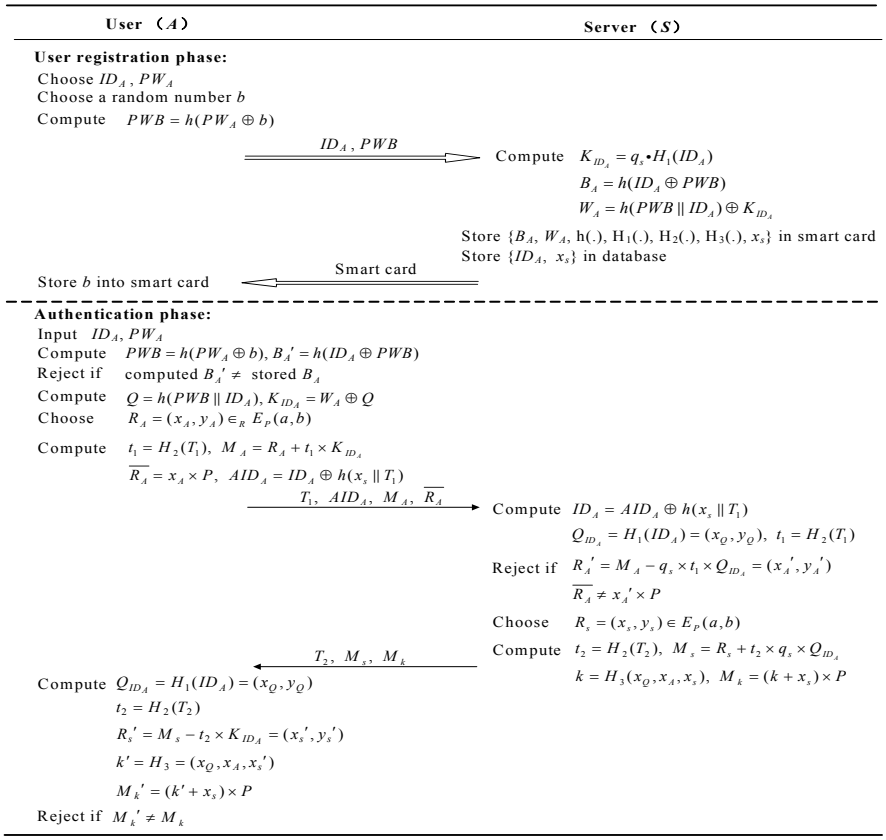

Fig. 1. Chen et al.'s remote authentication scheme for Cloud Computing

2.2 The Registration Phase

The registration phase involves the following operations:

Step R1. U_A chooses his/her ID_A and password PW_A and generates a random number b for calculating $PWB = h(PW_A \oplus b)$. Then, U_A submits ID_A and PWB to the server S.
Step R2. S computes $K_{IDA} = q_s \cdot H_1(ID_A) \in G_p$, where K_{ID_A} is U_A's authentication key.
Step R3. S computes $B_A = h(ID_A \oplus PWB)$ and $W_A = h(PWB \| ID_A) \oplus K_{IDA}$.
Step R4. S stores $\langle B_A, W_A, h(\cdot), H_1(.), H_2(.), H_3(.), x_s \rangle$ on a smart and sends the smart card to U_A over a secure channel (Here x_s is a secret key shared with users).
Step R5. Upon U_A receiving the smart card, U_A stores the random number b in the smart card. Note that now the smart card contains $\{B_A, W_A, h(\cdot), b, H_1(.), H_2(.), H_3(.), x_s\}$.
Step R6. U_A enters his/her ID_A and PW_A to verify whether $B_A = h(ID_A \oplus h(PW_A \oplus b))$. If it is hold, U_A accepts the smart card.

2.3 Mutual Authentication with Key Agreement Phase

When U_A wants to login to S, the following operations will be performed:

Step V1. U_A inserts the smart card into the card reader and enters his/her ID_A and PW_A.
Step V2. Smart card calculates $PWB = h(pw_A \oplus b)$ and $B'_A = h(ID_A \oplus PWB)$ and checks whether $B'_A = B_A$. If it holds, smart card calculates $Q = h(PWB \| ID_A)$ and $K_{IDA} = W_A \oplus Q$.
Step V3. After U_A obtaining his/her authentication key K_{IDA}, U_A (actually the smart cardchooses a random point $R_A = (x_A, y_A) \in E_{P(a,b)}$, where x_A and y_A are x and y coordinating point of R_A.
Step V4. U_A computes $t_1 = H_2(T_1)$, $M_A = R_A + t_1 \times K_{ID_A}$ and $\overline{R}_A = x_A \times P$ at the timestamp T_1.
Step V5. U_A computes $AID_A = ID_A \oplus h(x_s \| T_1)$ to obtain an anonymous ID.
Step V6. U_A sends message $m_1 = \{T_1, AID_A\ , M_A, \overline{R}_A\}$ to S.
Step V7. After receiving m_1, S performs the following operations to obtain $Q_{IDA} = (x_Q, y_Q)$ and $R'_A = (x'_A, y'_A)$ of U_A as follows:
$ID_A = AID_A \oplus h(x_s \| T_1)$;
$Q_{IDA} = H_1(ID_A)$;
$t_1 = H_2(T_1)$;
$R'_A = M_A - q_s \times t_1 \times Q_{IDA}$.
Step V8. S verifies whether $\overline{R}_A = x'_A \times P$. If it holds, U_A is authenticated by S.
Step V9. S chooses a random point $R_S = (x_S, y_S) \in E_p(a, b)$.
Step V10. S computes $t_2 = H_2(T_2)$,$M_S = R_S + t_2 \times q_S \times Q_{ID_A}$, session key $k = H_3(x_Q, x_A, x_S)$ and $M_k = (k + x_S) \times P$ at the timestamp T_2.

Step V11. S sends message $m_2 = \langle T_2, M_S, M_k \rangle$ to U_A.
Step V12. After receiving m_2,U_A performs the following computations to obtain $Q_{IDA} = (x_Q, y_Q)$ and $R'_s = (x'_s, y'_s)$ of S:
$Q_{IDA} = H_1(ID_A)$;
$t_2 = H_2(T_2)$;
$R'_S = M_S - t_2 \times K_{IDA}$.
Step V13. U_A computes $k' = H_3(x_Q, x_A, x'_S)$ and $M'_k = (k' + x'_s) \cdot P$ to verify whether $M'_k = M_k$. If it holds, S is authenticated by U_A.

Finally, U_A and S empoly k as a session key for securing subsequent data communications.

3 Cryptanalysis of Chen et al.'s Scheme

With superior properties over other related schemes and a long list of arguments of security features that their scheme possesses presented, Chen et al.'s scheme seems desirable at first glance. However, their security arguments are still specific-attack-scenario-based and without some degree of rigorousness, and thus it is not fully convincing. We find that Chen et al.'s scheme still fails to serve its purposes and demonstrate its security flaws in the following.

3.1 Offline Password Guessing Attack

Although tamper resistant smart card is assumed in many authentication schemes, but such an assumption is difficult and undesirable in practice. Many researchers have pointed out that the secret information stored in a smartcard can be breached by analyzing the leaked information [9] or by monitoring the power consumption [7,10]. In 2006, Yang et al. [14] pointed out that, previous schemes based on the tamper resistance assumption of the smart card are vulnerable to various types of attacks, such as user impersonation attacks, server masquerading attacks, and offline password guessing attacks, etc., once an adversary has obtained the secret information stored in a user's smart card and/or just some intermediate computational results in the smart card. Since then, researchers in this area began to pay attention to this issue and admired schemes based on non-tamper resistance assumption of the smart card is proposed, typical examples include [8, 12, 13]. Hence, in the following, we assume that the secret data stored in the smart card could be extracted out once the smart card is somehow obtained (stolen or picked up) by the adversary $\mathcal{A}$. Note that this assumption is widely assumed in the security analysis of such schemes [8, 11, 12, 14].

What's more, in Chen et al.'s scheme, a user is allowed to choose her own password at will during the registration phase; the user usually tends to select a password, *e.g.*, his home phone number or birthday, which can be easily remembered for his convenience. Hence, these easy-to-remember passwords, called weak passwords, have low entropy and thus are potentially vulnerable to offline password guessing attack.

Let us consider the following scenarios. In case the legitimate user U_A's smart card is in the possession of an adversary $\mathcal{A}$ and the parameters stored in it, like B_A, W_A, b and x_s, is revealed. Once the login request message $m_1 = \{T_1, AID_A, M_A, \overline{R}_A\}$ during any authentication process is intercepted by $\mathcal{A}$, an offline password guessing attack can be launched as follows:

Step 1. Computes the identity of U_A as $ID_A = AID_A \oplus h(x_s \parallel T_1)$, where AID_A, T_1 is intercepted and x_s is revealed from the smart card;
Step 2. Guesses the value of PW_A to be PW_A^* from a dictionary space $\mathcal{D}$;
Step 3. Computes $PWB^* = h(PW_A^* \oplus b)$, as b is revealed from the smart card;
Step 4. Computes $B_A^* = h(ID_A \oplus PWB^*)$;
Step 5. Verifies the correctness of PW_A^* by checking if the computed B_A^* is equal to the revealed B_A;
Step 6. Repeats Step 1, 2, 3, 4 and 5 of this procedure until the correct value of PW_A is found.

As the size of the password dictionary, i.e. $|\mathcal{D}|$, is very limited in practice, the above attack procedure can be completed in polynomial time. After guessing the correct value of PW_A, $\mathcal{A}$ can compute the valid authentication key $K_{ID_A} = W_A \oplus h(PWB \parallel ID_A) = W_A \oplus h(h(PW_A \oplus b) \parallel ID_A)$. With the correct K_{ID_A}, $\mathcal{A}$ can impersonate U_A to send a valid login request message $\{T_1, AID_A, M_A, \overline{R}_A\}$ to the service provider server S, and successfully masquerade as a legitimate user U_i to server S.

3.2 No Provision of User Anonymity

Let us consider the following scenarios. A malicious privileged user $\mathcal{A}$ having his own smart card or stolen card can gather information x_s from the obtained smart card as stated in Section 3.1, while x_s is shared among all the users. Then, $\mathcal{A}$ can compute ID_A corresponding to any user U_A as follows:

Step 1. Eavesdrops and intercepts a login request message $\{T_1, AID_C, M_C, \overline{R}_C\}$ of any user, without loss of generality, assume it is U_C, from the public communication channel;
Step 2. Computes $ID_C = AID_C \oplus h(x_s \parallel T_1)$, where x_s is revealed from the smart card and AID_C, T_1 is intercepted from the public channel as stated in Step 1;

It is obvious to see that user anonymity will be breached once the parameter x_s is extracted out. Hence, Chen et al.'s scheme fails to preserve user anonymity, which is the most essential security feature a dynamic identity-based authentication scheme is designed to support.

3.3 Key Compromise Impersonation Attack

Suppose the long-term secret key q_s of the server S is leaked out by accident or intentionally stolen by the adversary $\mathcal{A}$. Without loss of generality, we assume one

of U_A's previous login requests, say $\{T_1, AID_A\ , M_A, \overline{R}_A\}$, is intercepted by $\mathcal{A}$. Once the value of q_s is obtained, with the intercepted $\{T_1, AID_A\ , M_A, \overline{R}_A\}$, $\mathcal{A}$ can impersonate the legitimate user U_i since then through the following method:

Step 1. Guesses the value of ID_A to be ID_A^* from a dictionary space $\mathcal{D}_{ID}$;
Step 2. Computes $k_{ID_A}^* = q_s \cdot H_1(ID_A^*)$;
Step 3. Computes $t_1 = H_2(T_1)$;
Step 4. Computes $R_A^* = M_A - t_1 \times k_{ID_A}^* = (x_A^*, y_A^*)$;
Step 5. Computes $\overline{R}_A^* = x_A^* \times P$;
Step 6. Verifies the correctness of ID_A^* by checking if the computed $\overline{R}_A^*$ is equal to the intercepted $\overline{R}_A$;
Step 7. Repeats Step 1, 2, 3, 4, 5 and 6 of this procedure until the correct value of ID_A is found;
Step 8. Computes $K_{IDA} = q_s \cdot H_1(ID_A)$.

As the size of the identity dictionary, i.e. $|\mathcal{D}_{ID}|$, is often more limited than the password dictionary size $|\mathcal{D}|$ in practice, the above attack procedure can be completed in polynomial time. After guessing the correct value of K_{ID_A}, $\mathcal{A}$ can impersonate U_A since then. Hence, Chen et al.'s scheme cannot withstand key compromise impersonation attack.

3.4 Clock Synchronization Problem

It is widely accepted that, remote user authentication schemes employing timestamp may still suffer from replay attacks as the transmission delay is unpredictable in real networks [5]. In addition, clock synchronization is difficult and expensive in existing network environment, especially in wireless networks [4] and distributed networks [1]. Hence, these schemes employing timestamp mechanism to resist replay attacks is not suitable for mobile applications [2, 6]. In Chen et al.'s scheme, this principle is violated.

4 Conclusion

In this paper, we have shown that Chen et al.'s scheme suffers from the offline password guessing, no provision of user anonymity and key compromise impersonation attack. In addition, their scheme suffers from the clock synchronization problem. In conclusion, Although Chen et al.'s scheme possesses many attractive features, it, in fact, does not provide all of the security properties that they claimed and only radical revisions of the protocol can possibly eliminate the identified pitfalls.

Acknowledgments. This research was in part supported by the National Natural Science Foundation of China (NSFC No. 61170241 and No. 61073042).

References

1. Baldoni, R., Corsaro, A., Querzoni, L., Scipioni, S., Piergiovanni, S.: Coupling-based internal clock synchronization for large-scale dynamic distributed systems. IEEE Transactions on Parallel and Distributed Systems 21(5), 607–619 (2010)
2. Chang, C.C., Lee, C.Y.: A secure single sign-on mechanism for distributed computer networks. IEEE Transactions on Industrial Electronics 59(1), 629–637 (2012)
3. Chen, T., Yeh, H., Shih, W.: An advanced ecc dynamic id-based remote mutual authentication scheme for cloud computing. In: Proceedings of the 2011 Fifth FTRA International Conference on Multimedia and Ubiquitous Engineering, pp. 155–159. IEEE Computer Society (2011)
4. Giridhar, A., Kumar, P.: Distributed clock synchronization over wireless networks: Algorithms and analysis. In: 2006 45th IEEE Conference on Decision and Control, pp. 4915–4920. IEEE (2006)
5. Gong, L.: A security risk of depending on synchronized clocks. ACM SIGOPS Operating Systems Review 26(1), 49–53 (1992)
6. Islam, S.H., Biswas, G.: 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)
7. Kasper, T., Oswald, D., Paar, C.: Side-Channel Analysis of Cryptographic RFIDs with Analog Demodulation. In: Juels, A., Paar, C. (eds.) RFIDSec 2011. LNCS, vol. 7055, pp. 61–77. Springer, Heidelberg (2012)
8. Ma, C.-G., Wang, D., Zhang, Q.-M.: Cryptanalysis and Improvement of Sood et al.'s Dynamic ID-Based Authentication Scheme. In: Ramanujam, R., Ramaswamy, S. (eds.) ICDCIT 2012. LNCS, vol. 7154, pp. 141–152. Springer, Heidelberg (2012)
9. Mangard, S., Oswald, E., Standaert, F.X.: One for all-all for one: unifying standard differential power analysis attacks. IET Information Security 5(2), 100–110 (2011)
10. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Examining smart-card security under the threat of power analysis attacks. IEEE Transactions on Computers 51(5), 541–552 (2002)
11. Wang, D., Ma, C.G.: On the security of an improved password authentication scheme based on ecc. Cryptology ePrint Archive, Report 2012/190 (2012), `http://eprint.iacr.org/2012/190.pdf`
12. Wang, D., Ma, C.-G., Wu, P.: Secure Password-Based Remote User Authentication Scheme with Non-tamper Resistant Smart Cards. In: Cuppens-Boulahia, N., Cuppens, F., Garcia-Alfaro, J. (eds.) DBSec 2012. LNCS, vol. 7371, pp. 114–121. Springer, Heidelberg (2012)
13. Xu, J., Zhu, W., Feng, D.: An improved smart card based password authentication scheme with provable security. Computer Standards & Interfaces 31(4), 723–728 (2009)
14. Yang, G., Wong, D.S., Wang, H., Deng, X.: Formal Analysis and Systematic Construction of Two-Factor Authentication Scheme (Short Paper). In: Ning, P., Qing, S., Li, N. (eds.) ICICS 2006. LNCS, vol. 4307, pp. 82–91. Springer, Heidelberg (2006)
15. Yang, J., Chang, C.: 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)
16. Yu, H., Powell, N., Stembridge, D., Yuan, X.: Cloud computing and security challenges. In: Proceedings of the 50th Annual Southeast Regional Conference, pp. 298–302. ACM (2012)