National Ilan University

Bulletin of College of Engineering
http://engineering.niu.edu.tw/main.php

國立宜蘭大學工程學刊第四期, 39-52 頁, 2008 年 2 月

Bulletin of College of Engineering, National Ilan University, NO. 4, P. 39-52, Feb. 2008

A Security Analysis of Two Remote User Authentication Schemes Using Bilinear Pairings

Hsin-Jen Wang [1] Shiow-Jyu Lin [1] Yean-Nong Yang [1] Shyi-Tsong Wu [2]

1. Lecturer, Department of Electronic Engineering, National Ilan University

2. Associate Professor, Department of Electronic Engineering, National Ilan University

ABSTRACT

In this paper, we indicate two pairing-based remote user authentication scheme are insecure. First, a proposed authentication scheme suffers from the impersonation attack. The malicious adversary intercepts valid information from the login request, modifies it, and is able to impersonate the legitimate user to pass the authentication. Secondly, we also point out another authentication scheme, using bilinear pairing and elliptic curve cryptography, will suffer from the off-line dictionary attack. Under the user selecting the same random number for two distinct login, the attacker could calculate out the private secret of the user, and impersonate to be the legitimate user to login the system.

Keywords: security analysis, password authentication, smart card, remote login, bilinear pairings.

National Ilan University

Bulletin of College of Engineering
http://engineering.niu.edu.tw/main.php

國立宜蘭大學工程學刊第四期, 39-52 頁, 2008 年 2 月

Bulletin of College of Engineering, National Ilan University, NO. 4, P. 39-52, Feb. 2008

兩個基於雙線性配對的遠端使用者身分鑑別方法之安全分析

王信仁[1]　林秀菊[1]　楊演農[1]　吳錫聰[2]

1. 國立宜蘭大學電子工程學系講師
2. 國立宜蘭大學電子工程學系副教授

摘要

本文指出兩個基於雙線性配對的遠端使用者身分鑑別方法是不安全的。首先，我們將敍述一個身分鑑別方法，並說明其將遭受偽裝攻擊，惡意敵手截取合法使用者的有效登入資料，加以修改，偽裝此合法使用者通過身分鑑別，並且成功登入遠端系統。其次，我們指出另一基於雙線性配對的遠端使用者身分鑑別方法將遭受離線攻擊，在截取同一使用者兩個不同的有效登入資料，但二者具同一由使用者選定的任意參數，攻擊者將能算出合法使用者的身分鑑別機密資料，最後達到成功偽裝此合法使用者的目的。

關鍵詞：安全分析、通行碼鑑別、智慧卡、遠端登入、雙線性配對

I. Introduction

Remote user authentication scheme are essential in networked system because they provide the mechanism allow the legitimate users to login the remote server. Lamport first proposed a remote authentication scheme with insecure communication [11]. The scheme can resist replaying attack, but it needs a password table to verify the legitimacy of the user. If the password table is stolen by the adversary, the system will be broken. From then on, many related remote user authentication schemes [2],[5],[12],[14],[17] have been presented. In 2000, Hwang and Li [10] proposed a new remote user authentication scheme. The remote system only keeps a secret key but the user password table to authenticate the legitimacy of the users. Chan and Chang [4] pointed out there is weakness in Hwang-Li's scheme. In 2003, Shen et al. proposed a modified version [13] against the Chan-Cheng's attack. However, Leung et al. [9] indicated the hole still exists.

In 2006, Wang and Chai proposed two secure remote user authentication schemes using smart cards [16]. The first one is a variation of Hwang-Li's scheme, and the second one is based on the bilinear pairings. We cryptanalyze the pairing-based remote user authentication schemes, and point out that Wang et al.'s pairing-based remote user authentication scheme is insecure. It suffers from the impersonation attack. The adversary is able to impersonate the legitimate user to pass the authentication, login the remote system, and obtain the rights of legal user.

Besides, in [6], the authors proposed a novel remote user authentication scheme using bilinear pairings, which allows a valid user to login to the remote system while prohibiting too many users' login with the same login-ID. However the scheme is insecure against forgery attack, replay attack and insider attack [15]. Jia et al. repair

the scheme and provide a new remote user scheme [8]. However, we will indicate this scheme is insecure. It will suffer from the off-line dictionary attack. Without the knowledge of password, the malicious attacker can impersonate to be the legitimate user successfully.

The rest of the paper is organized as follows. The basic concepts of bilinear pairings are introduced in Section II. We then review Wang-Chai's first authentication scheme and present a cryptanalysis of the scheme in Section III and Section IV. In Section V, we introduce Jia et al.'s remote user authentication scheme and make a cryptanalysis for the scheme in Section VI. Finally, we draw our conclusion in Section VII.

II. Bilinear Pairings

We briefly describe the basic definition and properties of the bilinear pairing in this section. Let G_1 be an additive group of prime order q and G_2 be a multiplicative group of the same order q. We assume that the discrete logarithm problem (DLP) in both G_1 and G_2 are hard. Typically, G_1 will be a subgroup of the group of points on an elliptic curve over a finite field, and G_2 will be a subgroup of the group of the multiplicative group of a related finite field. Let $\hat{e}$ is the bilinear map from $G_1 \times G_1$ to G_2 on the elliptic curve and satisfies the following conditions:

Bilinear: $\hat{e}(P_1+P_2, Q) = \hat{e}(P_1, Q)\cdot\hat{e}(P_2, Q)$, $\hat{e}(P, Q_1+Q_2) = \hat{e}(P, Q_1)\cdot\hat{e}(P, Q_2)$ and $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, P_1, P_2, Q \in G_1$ and $a, b \in Z_q^*$.

Non-degenerate: There exists a point $P \in G_1$ such that $\hat{e}(P, P) \neq 1$.

Computability: There is an efficient algorithm to compute $\hat{e}(P, Q) \in G_2$ for all $P, Q \in G_1$.

We note that the Weil or Tate pairing associated with supersingular elliptic curves can be modified to create such bilinear maps [1], [7].

III. Review of Wang-Chai's pairing-based remote user authentication scheme

Remote user authentication is an important issue for practical wired and wireless access control applications, such as Internet banking, online shopping, and resource sharing. Remote user authentication schemes guarantee only the legal users have the right to access the resource provided by the remote servers. In this section, we will introduce Wang-Chai's second user remote authentication scheme [16]. The scheme is based on the pairings, and the knowledge proof of user's password and time stamps are used to construct the authentication mechanism. The remote system keeps a secret for computing the user passwords and does not need to maintain password verification table for verifying legal user. This pairing-based remote user authentication scheme is divided into registration phase, login phase and authentication phase. We briefly describe the procedures of the scheme as follows.

Registration Phase

In Registration Phase, the remote server first prepares some parameters for the system. The notations are listed as follows:

q	a secure large prime
G_1	a cyclic additive group of order q
G_2	a cyclic multiplicative group of order q
P	a specific point in G_1
$\hat{e}$	bilinear map from $G_1 \times G_1$ to G_2
x_s	the secret key owned by the remote server
$H(.)$	$\{0,1\}^* \rightarrow G_1$, a secure one-way *MapToPoin*t hash function

When a new user U_i submits his identity ID_i to the remote server for registration, the remote server first checks its validity and then computes the password PW_i as follows:

$$PW_i = x_s \cdot H(ID_i)$$

Then the server stores the public parameters $\{q, G_1, P\}$ to a smart card. Finally, the server issues the smart card and PW_i to the user U_i via a secure channel.

Login Phase

When U_i wants to login to the remote server, he inserts his smart card into the terminal, and keys in his ID_i and PW_i. Then the smart card will perform the following steps:

1. Select a random number $r \in [1,\ldots, p\text{-}1]$.
2. Compute $C_1 = r \cdot P$.
3. Pick up the current date and time T of the login device.
4. Compute $C_2 = \frac{1}{T + r} \cdot PW_i$.
5. Send the message $C = \{C_1, C_2, T, ID_i\}$ to the remote server.

Authentication Phase

Suppose that the remote server receives the message C at T', where T' is the current date and time of the system. Then the following operations are performed to facilitate the authentication.

1. Check the validity of the identity ID_i, if the format is incorrect, the login request will be rejected.
2. Check the time interval between T and T'. if $(T' - T) \geq \Delta T$, where ΔT is the expected legal time interval for transmission delay, the system will reject the

login request.

3. Check

$$\hat{e}(T\cdot P+C_1, C_2) = \hat{e}(P, x_s H(ID_i))$$

If it holds, the system will accept the login request. Otherwise, the request will be rejected. Since

$$\hat{e}(T\cdot P+C_1, C_2)$$

$$= \hat{e}((T+r)\cdot P, \frac{1}{T+r}\cdot PW_i)$$

$$= \hat{e}(P, PW_i)^{(T+r)\frac{1}{T+r}}$$

$$= \hat{e}(P, PW_i)$$

$$= \hat{e}(P, x_s H(ID_i))$$

IV. Security analysis of Wang-Chai's second scheme

Wang-Chai's pairing-based remote user authentication scheme suffers from the impersonation attack. In this scheme, the user U_i is authenticated if the login request message $C = \{C_1, C_2, T, ID_i\}$ satisfies $\hat{e}(T\cdot P+C_1, C_2) = \hat{e}(P, x_s H(ID_i))$. Due to the difficulty of Elliptic Curve Discrete Logarithm Problem, the computation is difficult for the user U_i to compute the secret key x_s from the equation $PW_i = x_s\cdot H(ID_i)$ so that he can compute another user U_j's valid password via $PW_j = x_s\cdot H(ID_j)$. In addition, it is extreme difficult for the adversary to compute the password of a legitimate user PW_i and the remote server secret key x_s from the login request $\{C_1, C_2, T, ID_i\}$.

However, by another approach, to pass the authentication, the adversary does not need to crack the password PW_i and the system secret key x_s. Eavesdropping a valid authentication message $C = \{C_1, C_2, T, ID_i\}$, the adversary can use the valid message of a legitimate user and impersonate the user to login the remote system. He sends a

modified authentication message $C' = \{C_1', C_2, t, ID_i\}$ to the remote system, where

$$C_1' = C_1 + T \cdot P - t \cdot P$$

and the t is the current date and time while the illegitimate user logins. The modified authentication message C' will satisfy the authentication equation $\hat{e}(t \cdot P + C_1', C_2) = \hat{e}(P, x_s H(ID_i))$, and the adversary will login the remote system successfully. It is because that

$$\hat{e}(t \cdot P + C_1', C_2)$$

$$= \hat{e}(t \cdot P + C_1 + T \cdot P - t \cdot P, \frac{1}{T+r} \cdot PW_i)$$

$$= \hat{e}(r \cdot P + T \cdot P, \frac{1}{T+r} \cdot PW_i)$$

$$= \hat{e}((T+r) \cdot P, \frac{1}{T+r} \cdot PW_i)$$

$$= \hat{e}(P, PW_i)^{(T+r)\frac{1}{T+r}}$$

$$= \hat{e}(P, x_s H(ID_i))$$

Finally, the illegitimate user is able to pass the authentication phase and gains the authority of the legitimate user.

In addition, the scheme is not user-friendly. It has the disadvantage that the password of the user is assigned by the system. The lengthy assigned password does not satisfy the user's requirement and is also against the habit of the user. If the password of user can be chosen and changed by the user himself, the system would be more user-friendly.

V. Review of Jia et al.'s remote user authentication scheme

In this section, we introduce and cryptanalyze Jia et al.'s remote user authentication scheme [8]. Jia et al.'s scheme allows the valid user to login the remote system, and time stamps used to assure the freshness of the login request message. The scheme is based on bilinear pairings and ECC, and claimed that the replay attacks and the forgery attacks can be blocked. The main of the scheme includes setup phase, registration phase, and authentication phase. Firstly, we review the scheme as follows.

Initialization Phase

The remote server (RS) selects a private key s and computes his public key Pub_{RS} as

$$Pub_{RS} = sP$$

Then the server publishes the parameters $\{G_1, G_2, \hat{e}, q, P, Pub_{RS}, H(\cdot)\}$ and keeps s secret, where $H(\cdot)$: $\{0,1\}^* \rightarrow G_1$, is a public one-way hash function.

Registration Phase

The user wants to be a legitimate one must register with the remote server before he can get any service from the server. If user U_i wants to register with the remote server he executes the following steps:

1. U_i submits his identity ID_i and password PW_i to the RS.
2. On receiving the registration request, the RS computes:

$$\text{Re}g_{IDi} = sH(ID_i)+H(PW_i)$$

3. RS personalizes a smart card with the parameters: $\{ID_i, \text{Re}g_{IDi}, H(\cdot), P, Pub_{RS}\}$

and distributes the smart card to U_i over a secure channel.

Authentication Phase

The authentication phase includes user's login and RS's verification. When user U_i wants to login to the RS, two steps must be followed:

1. U_i inserts the smart card into the terminal and inputs his identity ID_i and his password PW_i. If ID_i and PW_i are identical to those stored in the smart card, the smart card performs the next step.

2. The smart card computes

$$DID_i = T \cdot \mathrm{Re}g_{IDi}$$

$$V_i = T \cdot H(PW_i)$$

where T is user system's timestamp. Then the smart card will choose a random integer k and encrypt DID_i and V_i via

$$C_1 = kP$$

$$C_2 = (DID_i - V_i) + kPub_{RS}$$

After that the terminal can send the login request $\{ID_i, C_1, C_2, T\}$ to the remote server over public channel.

On the receiving the login request $\{ID_i, C_1, C_2, T\}$, RS performs the following steps to verify the login request:

1. Verify the validity of time interval between the RS's timestamp T' and T. If $(T' - T) < \Delta T$ then RS go to step 2, otherwise it rejects. Here ΔT denotes the time delay that is tolerable by both user and RS.

2. Check to see whether

$$\hat{e}(C_2 - sC_1, P) = \hat{e}(H(ID_i), Pub_{RS})^T$$

If it holds, RS accepts the login request, otherwise rejects. The deduction is described as follows.

$$\hat{e}(C_2 - sC_1, P)$$

$$= \hat{e}((DID_i - V_i) + kPub_{RS} - sC_1, P)$$

$$= \hat{e}((T \cdot \mathrm{Reg}_{IDi} - T \cdot H(PW_i)) + ksP - skP, P)$$

$$= \hat{e}(T(sH(ID_i) + H(PW_i) - T \cdot H(PW_i)), P)$$

$$= \hat{e}(TsH(ID_i), P)$$

$$= \hat{e}(H(ID_i), P)^{Ts}$$

$$= \hat{e}(H(ID_i), sP)^T$$

$$= \hat{e}(H(ID_i), Pub_{RS})^T$$

VI. Security analysis of Jia et al.'s remote user authentication scheme

In this section, the trick of attacker for Jia et al.'s remote user authentication scheme is introduced. In [8], user U_i computes C_1, C_2 and sends $\{ID_i, C_1, C_2, T\}$ to the RS for login request. The wired or wireless login request message $\{ID_i, C_1, C_2, T\}$ transmitted over public insecure communication channel might be eavesdropped, further analyzed by some software tools, and stored in the database of computing devices for future need. And the attacker can compute private secret of user U_i after got two U_i's different valid login request messages but both with the same C_1, i.e., $\{ID_i, C_1, C_2, T\}$ and $\{ID_i, C_1, C_2', T'\}$, where $C_1 = kP$ and k is a random number. Although to obtain the $\{ID_i, C_1, C_2, T\}$ and the $\{ID_i, C_1, C_2', T'\}$ is a probability

problem. However, it is possible after long term of data mining and analysis. The adversary could calculate out the private secret of U_i, $sH(ID_i)$, by the two intercepted login message $\{ID_i, C_1, C_2, T\}$ and $\{ID_i, C_1, C_2', T'\}$ via

$$sH(ID_i) = (T' - T)^{-1} \cdot (C_2' - C_2)$$

It is because that

$$(C_2' - C_2)$$

$$= (DID_i' - V_i') - (DID_i - V_i)$$

$$= (T' \cdot \mathrm{Reg}_{IDi} - T' \cdot H(PW_i)) - (T \cdot \mathrm{Reg}_{IDi} - T \cdot H(PW_i))$$

$$= (T' - T) \cdot (\mathrm{Reg}_{IDi} - H(PW_i))$$

$$= (T' - T) \cdot (sH(ID_i) + H(PW_i) - H(PW_i))$$

$$= (T' - T) \cdot sH(ID_i)$$

So,

$$sH(ID_i) = (T' - T)^{-1} \cdot (C_2' - C_2)$$

The calculation of $(T' - T)^{-1}$ is an easy work under the order q.

After the calculation of $sH(ID_i)$, the malicious attacker can always impersonate to be the user U_i without the knowledge of password PW_i. He first selects a random integer k^*, and calculates $C_1^* = k^*P$ as well as $C_2^* = T^*(sH(ID_i)) + k^*Pub_{RS}$, here T^* is the valid current system's timestamp, and $sH(ID_i)$ had been calculated. Then he sends the login request $\{ID_i, C_1^*, C_2^*, T^*\}$ to the RS. It will pass the authentication since that $\hat{e}(C_2^* - sC_1^*, P) = \hat{e}(H(ID_i), Pub_{RS})^{T^*}$.

VII. Conclusion

In this paper, we have presented cryptanalysis for both Wang-Chai's pairing-based remote user authentication scheme, and Jia et al.'s remote user authentication scheme. Wang-Chai's proposed scheme is not user-friendly, and suffers from the impersonation attack. After intercepting a valid login request, the adversary modifies it, and resubmits the modified request. Finally the illegal user will obtain the right of legitimacy. Besides, we also point out that Jia et al.'s pairing-based remote user authentication scheme is insecure. It suffers from the off-line dictionary attack. The adversary could calculate out the private secret of legitimate user, and impersonate to be the legitimate user to login the remote system successfully.

References

[1] Dan Boneh, Matthew Franklin, "Identity-Based Encryption from the Weil Pairing," Advances in Cryptology – CRYPTO 2001, Springer- Verlag, pp. 312-229, 2001.

[2] C. C. Chang and S. J. Hwang, "Using smart cards to authenticate remote passwords," Computers and Mathematical Applications, vol.26, no.7, pp.19-27, 1993.

[3] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards,"IEE Proceeding-E, vol.138, no.3, pp.165-168, 1993.

[4] C.K. Chan and L.M. Cheng, "Cryptanalysis of a remote user authentication scheme using smear cards", IEEE Trans. Consumer Electronics, vol.46, no.4, pp.992-993, 2000.

[5] Hung-Yu Chien, Jinn-Ke Jan and Yuh-Min Tseng, "An efficient and practical solution to remote authentication: smart card," Computer & Security, vol.21, no.4, pp.372-375, 2002.

[6] M.L. Das, A Saxena, V.P. Gulati, and D.B. Phatak, " A novel remote user authentication scheme using bilinear pairing," Computers & Security, Vol.25, No.3, pp.184-189, 2006.

[7] Steven D. Galbraith, Keith Harrison and David Soldera, "Implementing the Tate Pairing", Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS-V, Sydney, Australia, pp. 324-337, July 7-12, 2002.

[8] Zhongtian Jia, Yuan Zhang, Hua Shao, Yongzheng Lin, and Jin Wang, "A remote authentication scheme using bilinear pairings and ECC," in Proceedings

of the Sixth International Conference on Intelligent System Design and Application (ISDA'06), Vol.2, pp.1091-1094, 2006.

[9] K.C. Leung, L.M. Cheng, A.S. Fong, and C.K. Chan," Cryptanalysis of a modified remote user authentication scheme using smart cards', IEEE Trans. on Consumer Electronics, vol.49, no.4, pp.1243-1245, 2003.

[10] Min-Shiang Hwang and Li-Hua Li, "A new remote user authentication scheme using cards," IEEE Trans. on Consumer Electronics, vol.46, no.1, pp.28-30, 2000.

[11] L.Lamport, "Password authentication with insecure communication," Communications of ACM, vol.24, pp.770-772, 1981.

[12] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang, "A flexible remote authentication scheme using smart cards," ACM Operating Systems Review, vol.36, no.3, pp. 46-52, 2002.

[13] J.J. Shen, C.W. Lin, and M.S. Hwang, "A modified remote user authentication scheme using smart cards", IEEE Trans. Consum. Electron. vol.49, no 2, pp. 414 - 416, 2003.

[14] Hung-Min Sun, "An efficient remote use authentication scheme using smart card," IEEE trans. on Consumer Electronics, vol.46, November, pp.958-961, 2000.

[15] G. Thulasi, M.L. Das and A. Saxena, "Cryptanalysis of recently proposed remote user authentication schemes," http://eprint.iacr.org/2006/028.pdf.

[16] Xue-Guang Wang, and Zhen-Chuan Chai, "Two secure remote user authentication schemes using smart cards", Proceedings of Fifth International Conference on Machine Learning and Cybernetics, pp. 2653-2658, Dalian,13-16 August 2006.

[17] Shyi-Tsong Wu and Bin-Chang Chieu, "A note on a user friendly remote authentication scheme with smart cards," IEICE Trans. Fundamentals, vol. E87-A, no.8, pp.2180-2181, 2004.