Cryptanalysis on Tan-Zhu Remote Password Authentication Scheme¹

Chun-I Fan, Chien-Nan Wu, and Yung-Cheng Chan

Department of Computer Science and Engineering
National Sun Yat-sen University
Kaohsiung, Taiwan, R.O.C.
tel: +886-7-5252000 ext. 4346, fax: +886-7-5254301
e-mail: cifan@cse.nsysu.edu.tw

Abstract

In 1999, Tan and Zhu proposed a remote password authentication scheme that is the first remote login scheme using smart cards based on cross product of matrixes. The scheme is efficient and flexible as compared with other matrix-based remote authentication schemes. However, Chien, Jan, and Tseng have shown that an attacker can impersonate a legitimate user to login the system in the scheme. This paper will present another possible attack on Tan-Zhu scheme and it may also threaten the security of the scheme. If the format checking for the identities of users is not sufficient in the authentication phase of the protocol, the proposed attack will be valid such that attackers can forge valid authentication messages for the users who have not registered with the system yet and then successfully login the system.

Keywords: Remote password authentication, Cross product, Replay attacks, Smart cards

¹The result of this research was presented at the 15th National Information Security Conference, Kaohsiung, Taiwan, June 9-10, 2005.

This research was partially supported by the National Science Council of the R.O.C.(Taiwan) under grant NSC 94-2219-E-110-001.

1 Introduction

Due to security and cost efficiency, smart cards are usually adopted to store the secret information of users in many remote authentication protocols [1, 2, 7, 8]. By presenting the smart card and inputting the correct password, the cardholder can login the remote system or server. In a secure remote authentication scheme, none can login the system without the password, the card, or both. Basically, these protocols must rely on some robust cryptographic or mathematical foundations, such as discrete logarithms [6, 10] or quadratic residues [4], to guarantee their security. Tan and Zhu introduced the first remote password authentication scheme based on inner and cross products of matrixes [9]. In the protocol of [9], the system computes and records the secret information in each issued smart card via performing matrix multiplications and cross-product computations on some security parameters, and each user must also perform matrix inner-product computations to form her/his login request message. Through the normalization of matrixes defined in [9], the system can check if a login request message is valid without keeping a large verification table. Besides, the users can freely choose and change their own passwords in the protocol, and it is more efficient than Chang-Hwang scheme [3] that is also a matrix-based remote authentication scheme using smart cards. Although the authors of [9] have examined the security of their scheme, [5] has shown that the attackers can impersonate any registered user to login the system without being detected by the system in the scheme.

In addition, we find another weakness in Tan-Zhu scheme and it may also affect the security of the scheme. The proposed attack is based on the collusion of two registered users such that they can create valid login messages of unregistered users and then login the system successfully.

The rest of this paper is organized as follows. In Section 2, we briefly review Tan and Zhu's scheme [9]. Chien-Jan-Tseng attack [5] on Tan and Zhu's scheme is shown in Section 3. A new attack on Tan-Zhu scheme is presented in Section 4. Finally, a concluding remark is given in Section 5.

2 Review of Tan-Zhu Scheme

In this section we review Tan and Zhu's password authentication scheme [9]. The protocol consists of three phases, card initialization, login, and authentication phases. In the card initialization phase, a trusted card initialization center (CIC) issues a smart card to each user who has registered with CIC. In the login phase, the registered user attaches her/his card to the card reader and inputs her/his password, and then she/he forms and submits a login message to the system. After receiving the message, the system verifies whether it is correct or not in the authentication phase. If true, the system will accept the request; otherwise the system will reject it.

In order to perform the protocol of [9], CIC (and the system) must prepare the necessary parameters for the protocol in advance. First, let p be a large prime and α be a primitive element in Galoid Field $\text{GF}(p)$. CIC (and the system) chooses a one-way hash function $f(\cdot)$ and a pseudorandom number generator $g(\cdot)$. It also randomly selects two three-dimensional row vectors $V_1 = (v_{11}, v_{12}, v_{13})$ with $v_{11} \neq 0$ and $V_2 = (v_{21}, v_{22}, v_{23})$ with $v_{21} \neq 0$ over $\text{GF}(p)$ such that V_1 and V_2 are linearly independent each other. CIC (and the system) keeps $\{g(\cdot), V_1\}$ secret and makes $\{p, \alpha, f(\cdot), V_2\}$ public. The cross product of two three-dimensional row vectors $M_1 = (m_{11}, m_{12}, m_{13})$ and $M_2 = (m_{21}, m_{22}, m_{23})$ over $\text{GF}(p)$ is defined as $(M_1 \times M_2)(\text{mod } p) = \left(\begin{vmatrix} m_{12} & m_{13} \\ m_{22} & m_{23} \end{vmatrix}, \begin{vmatrix} m_{11} & m_{13} \\ m_{21} & m_{23} \end{vmatrix}, \begin{vmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{vmatrix} \right)(\text{mod } p)$, and the normalization of vector $M = (m_1, m_2, m_3)$ over $\text{GF}(p)$ with $m_1 \neq 0$ is defined as $N(M) = (m_2 m_1^{-1}, m_3 m_1^{-1})(\text{mod } p)$. Upon the above definitions, the authors of [9] also introduced the theorem below.

Theorem 1: Let A be an $n \times 2$ matrix with $n \geq 2$ where any two row vectors in A form a nonsingular matrix and each row vector in A is nonzero. If

$$\begin{pmatrix} k_1 \\ k_2 \\ \vdots \\ k_n \end{pmatrix} = A \begin{pmatrix} V_1 \\ V_2 \end{pmatrix} (\text{mod } p), \text{ then } k_i \times W = c(V_1 \times V_2)(\text{mod } p), i = 1, 2, \dots, n$$

where c is a constant and $W = V_1$ or $W = V_2$.

From **Theorem 1**, the authors of [9] concluded the following result.

Corollary 1: If $N(k_i \times V_2)$, $N(k_j \times V_2)$, and $N(V_1 \times V_2)$ exist where $i, j \in \{1, 2, \dots, n\}$, then $N(k_i \times V_2) = N(k_j \times V_2) = N(V_1 \times V_2)$.

Finally, CIC (and the system) chooses A as defined in **Theorem 1** where n denotes the predicted number of users who will register with CIC. The details of the protocol are described as follows.

Phase I [Card Initialization]

If a new user u_i decides to register with CIC, she/he firstly chooses her/his own password PW_i and presents her/his identity $ID_i = (id_{i1}, id_{i2})$ and $f(PW_i)$ to CIC. Then CIC performs the following tasks:

Step 1: Select one two-dimensional row vector $A_i = (a_{i1}, a_{i2})$ with $a_{i1} \neq 0$ and $a_{i2} \neq 0$ from A where (a_{i1}, a_{i2}) has not been assigned to any other user. If there is not such a vector, CIC must find a two-dimensional row vector which is linearly independent to any row vector in A and appends it to A such that A becomes a $(n + 1) \times 2$ matrix, and then go to **Step 1** in **Phase I**.

Step 2: Compute

$$k_i = (a_{i1}, a_{i2}) \begin{pmatrix} V_1 \\ V_2 \end{pmatrix} \pmod{p} \text{ and}$$

$$PW1_i = N(k_i \times V_2) \begin{bmatrix} g(id_{i1}) \\ g(id_{i2}) \end{bmatrix} \oplus f(PW_i) \pmod{p}.$$

Step 3: Store $(PW1_i, k_i, f(\cdot))$ in a smart card and deliver the smart card to u_i on a secure channel.

Phase II [Login]

When user u_i is about to log into the system, she/he firstly attaches her/his own smart card to a terminal and inputs her/his password PW_i . Afterwards, the smart card performs the following tasks:

Step 1: Compute

$$PW2_i = PW1_i \oplus f(PW_i) \pmod{p} \text{ and}$$

$$PW3_i = \alpha^{N(k_i \times V_2) \bullet (f(PW2_i), f(T))} \pmod{p}$$

where $\bullet$ is the inner-product operator and T is the timestamp of the current time.

Step 2: Construct the login request message $R = (PW3_i, T, ID_i)$ and transmit

it to the system.

Phase III [Authentication]

After receiving the login request message R , the system performs the following tasks to authenticate the request:

Step 1: Verify whether the format of ID_i is correct or not. If false, the system will reject the request.

Step 2: Suppose that T^* represents the time on which R is received. Verify whether the transmission time (i.e., $T^* - T$) is within the legal tolerant interval ΔT or not. If $(T^* - T) > \Delta T$, then the request will be rejected.

Step 3: Compute

$$Q = N(V_1 \times V_2) \begin{bmatrix} g(id_{i1}) \\ g(id_{i2}) \end{bmatrix} \pmod{p} \text{ and} \\ Z = \alpha^{N(V_1 \times V_2) \bullet (f(Q), f(T))} \pmod{p}.$$

If $PW3_i = Z$, then the system will accept the login request; otherwise the system will reject it.

3 Chien-Jan-Tseng Attack on Tan-Zhu Scheme

In [5], Chien, Jan, and Tseng proposed an attack on Tan-Zhu scheme. The attack is described below.

Let user j have registered with CIC, where her/his card contains $(PW1_j, k_j, f(\cdot))$.

Since V_2 is public, user j can derive that $N(k_j \times V_2) = (a, b)$ where a and b are integers. From **Corollary 1**, $N(k_i \times V_2) = N(k_j \times V_2) = N(V_1 \times V_2) = (a, b)$.

To impersonate user i , who has registered with CIC, to login the system, user j intercepts the login message $R = (PW3_i, T, ID_i)$ of user i and then computes $PW3'_i = PW3_i * \alpha^{-b*f(T)} * \alpha^{b*f(T')} \pmod{p}$

and submits $R' = (PW3'_i, T', ID_i)$ to the system where T' is the timestamp of the current time. Thus, the system will accept the login request message R' because that

$$\begin{aligned} &PW3'_i \\ &= PW3_i * \alpha^{-b*f(T)} * \alpha^{b*f(T')} \\ &= \alpha^{N(k_i \times V_2) \bullet (f(PW2_i), f(T))} * \alpha^{-b*f(T)} * \alpha^{b*f(T')} \end{aligned}$$

$$\begin{aligned}
&= \alpha^{(a,b) \bullet (f(PW2_i), f(T))} * \alpha^{-b * f(T)} * \alpha^{b * f(T')} \\
&= \alpha^{a * f(PW2_i) + b * f(T)} * \alpha^{-b * f(T)} * \alpha^{b * f(T')} \\
&= \alpha^{a * f(PW2_i) + b * f(T')} \\
&= \alpha^{(a,b) \bullet (f(PW2_i), f(T'))} \\
&= \alpha^{N(V_1 \times V_2) \bullet (f(Q), f(T'))} \pmod{p}.
\end{aligned}$$

Therefore, the request message $R' = (PW3'_i, T', ID_i)$ can pass the verification process and thus user j successfully impersonates user i to login the system.

4 Another Attack on Tan-Zhu Scheme

In this section, we present a new attack on Tan-Zhu scheme. The details are described as follows.

Let user i with identity $ID_i = (x, y)$ and user j with identity $ID_j = (y, x)$ have registered with CIC where $x \neq y$. Hence, user i and user j , respectively, have obtained $(PW1_i, k_i, f(\cdot))$ and $(PW1_j, k_j, f(\cdot))$, respectively, from CIC. By **Corollary 1**, let $N(k_i \times V_2) = N(k_j \times V_2) = N(V_1 \times V_2) = (a, b)$ where a and b are integers. Thus, we have that

$$a * g(x) + b * g(y) = PW1_i \oplus f(PW_i) \pmod{p} \text{ and}$$

$$a * g(y) + b * g(x) = PW1_j \oplus f(PW_j) \pmod{p}.$$

Solving the above two congruences, we can obtain

$$g(x) = \frac{a * (PW1_i \oplus f(PW_i)) - b * (PW1_j \oplus f(PW_j))}{a^2 - b^2} \pmod{p} \text{ and}$$

$$g(y) = \frac{b * (PW1_i \oplus f(PW_i)) - a * (PW1_j \oplus f(PW_j))}{b^2 - a^2} \pmod{p}.$$

Assume that user i colludes with user j . They can forge a pseudo identity $ID_x = (x, x)$ and then form and submit the login request message $(PW3_x, T, ID_x)$ to the system where

$$PW3_x = \alpha^{N(k_i \times V_2) \bullet (f(PW2_x), f(T))} \pmod{p},$$

$$PW2_x = N(k_i \times V_2) \begin{bmatrix} g(x) \\ g(x) \end{bmatrix} \pmod{p},$$

and T is the timestamp of the current time.

At **Step 1** in **Phase III** of Tan-Zhu protocol, the system must check the format of the identity of each login user. However, Tan and Zhu did not

definitely define the content of the identity checking in their protocol. If all of the checking procedures the system has to perform are just to verify whether each received identity is a two-dimensional vector or not, the login request message $(PW3_x, T, ID_x)$ will be accepted by the system because

$$PW3_x = \alpha^{N(V_1 \times V_2) \bullet \left(f \left(N(V_1 \times V_2) \begin{bmatrix} g(x) \\ g(x) \end{bmatrix} \pmod{p} \right), f(T) \right)} \pmod{p}.$$

Similarly, they can also form a valid login request message $(PW3_y, T, ID_y)$ of the unregistered user with identity $ID_y = (y, y)$ and then successfully login the system where

$$PW3_y = \alpha^{N(k_i \times V_2) \bullet (f(PW2_y), f(T))} \pmod{p},$$

$$PW2_y = N(k_i \times V_2) \begin{bmatrix} g(y) \\ g(y) \end{bmatrix} \pmod{p},$$

and T is the timestamp of the current time.

5 Conclusions

In this paper, we have proposed another possible attack on Tan-Zhu remote password authentication scheme. If the format checking for the identity of each login user is not strict enough in Tan-Zhu scheme, the attack will work without $g(\cdot)$ which is kept secret by CIC and the system in the scheme.

References

- [1] C.C. Chang and T.C. Wu, "Remote password authentication with smart card," *IEE Proceeding – Computers and Digital Techniques*, Vol. 138, No. 3, pp. 165-168, 1991.
- [2] C.C. Chang and C.S. Lai, "Correspondence for remote password authentication with smart cards," *IEE Proceeding – Computers and Digital Techniques*, Vol. 139, No. 4, pp. 372, 1992.

- [3] C.C. Chang and S.J. Hwang, "Using smart card to authenticate remote password," *Computers & Mathematics with Applications*, Vol. 26, No. 7, pp. 19-27, 1993.
- [4] C.C. Chang, S.M. Tsu, and C.Y. Chen, "Remote scheme for password authentication based on theory of quadratic residues," *Computer Communications*, Vol. 18, No. 12, pp. 936-942, 1995.
- [5] H.Y. Chien, J.K. Jan, and Y.M. Tseng, "Impersonation attack on Tan-Zhu's remote login scheme," *Electronics Letters*, Vol. 36, No. 14, pp. 1202-1203, 2000.
- [6] M.S. Hwang and L.H. Li, "A new remote user authentication scheme using smart card," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp. 28-30, 2000.
- [7] W.S. Juang, "Efficient password authenticated key agreement using smart cards," *Computers & Security*, Vol. 23, No. 2, pp. 167-173, 2004.
- [8] H.M. Sun, "An efficient remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 4, pp. 958-961, 2000.
- [9] K. Tan and H. Zhu, "Remote password authentication scheme based on cross-product," *Computer Communications*, Vol. 22, No. 4, pp. 390-393, 1999.
- [10] S.J. Wang and J.F. Chang, "Smart card based secure password authentication scheme," *Computers & Security*, Vol. 15, No. 3, pp. 231-237, 1996.

Received: November 5, 2005