INFORMATICA, 2005, Vol. 16, No. 1, 37–44

Cryptanalysis of the Modified Remote Login Authentication Scheme Based on a Geometric Approach

Chin-Chen CHANG
Department of Computer Science and Information Engineering
National Chung Cheng University
160, San-Hsing, Min-Hsiung, Chiayi 621, Taiwan
e-mail: ccc@cs.ccu.edu.tw

Iuon-Chang LIN
Department of Management Information System
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan
e-mail: iclin@cs.kuas.edu.tw

Received: November 2001

Abstract. In 1995, Wu proposed a remote login authentication scheme based on geometric approach. However, Chien, Jan and Tseng presented a cryptanalysis of Wu's scheme to show that it is not secure. Moreover, they proposed a modified version of Wu's scheme. This paper presents there is a serious weakness in this modified remote login authentication scheme. We show that an illegal user can easily forge a valid login request in the modified version proposed previously.

Key words: cryptography, remote login.

1. Introduction

In 1995, Wu (Wu, 1995) proposed a remote password authentication scheme based on geometric approach. The advantages of this scheme are that (1) modular exponential operations are not required by the system and users, (2) the system does not need to maintain password table and/or verification table, (3) the user can choose his own password freely, and (4) the scheme can withstand the replaying attack.

However, Wu's scheme is not secure. In 1999, Hwang (Hwang, 1999) proposed a cryptanalysis to show that an illegal user can forge a valid login request from the eavesdropped login requests. Recently, Chien, Jan and Tseng (Chien *et al.*, 2001) also proposed a different approach to break Wu's system. An attacker can easily derive a secret point for a legal user from two eavesdropped login requests, and then the attacker has the ability to impersonate the legal user and issue a valid login request. Furthermore, they also proposed a modified version of Wu's scheme, which not only can withstand the attacks of theirs and Hwang's, but also keep the efficiency.

In this paper, we show that Chien, Jan and Tseng's modified scheme is still not secure. The rest of this paper is organized as follows. In Section 2, we shall briefly review Wu's scheme and Chien, Jan and Tseng's attack and their improved scheme. In Section 3, we shall present an approach to break their improved scheme. Finally, some conclusions are made in the last section.

2. Previous Works

Remote login authentication scheme is a critical issue in the computer and network systems. Many efficient methods (Chang and Wu, 1991; Chang *et al.*, 1995; Liaw, 1995) have been developed to verify the legitimacy of each login user. Recently, Chien, Jan and Tseng (Chien *et al.*, 2001) pointed out that Wu's remote login authentication scheme is not secure and they proposed an improved version of Wu's scheme. In this section, we briefly introduce the remote password authentication scheme proposed by Wu (Wu, 1995) firstly. Then, the attack and the improved scheme proposed by Chien, Jan and Tseng will also be reviewed.

In Wu's scheme, it is divided into three phases: (1) the registration phase, (2) the login phase, and (3) the authentication phase. In the registration phase, a new user has to register with central authority (CA) to become a legal user. In the login phase, when a user wants to login to the computer system remotely, he/she delivers the login request to the system. The system will authenticate the legitimacy of the login user in the authentication phase. In the following, we describe the processes of each phase. Initially, the central authority (CA) chooses a large prime p, a one-way hash function f, and a secret point $(x_0,\ y_0)$ on the Euclidean plane.

The registration phase

A new user U_i freely chooses his password PW_i, and then presents $f(PW_i)$ to CA. Then the CA performs the registration steps as follows.

1. The CA chooses the identity ID_i for the user U_i.
2. The CA chooses two points r_{iw} and r_{io}, where

$$r_{iw} = \big(0, f(PW_i)\big), \tag{1}$$

and

$$r_{io} = \big(f(ID_i) \cdot x_0, f(ID_i) \cdot y_0\big). \tag{2}$$

Then CA computes the middle point A_i between r_{iw} and r_{io} on the Euclidean plane. Thus, A_i can be expressed as

$$A_i = \Big(\frac{f(ID_i \cdot x_0)}{2},\ \frac{f(PW_i) + f(ID_i \cdot y_0)}{2}\Big) = (a_{i1}, a_{i2}). \tag{3}$$

3. The CA stores four parameters $\{ID_i,\ f,\ p,\ \text{and}\ A_i\}$ in a smart card and delivers the smart card to the user U_i.

The login phase

When U_i wants to login the system, U_i inserts his/her own smart card to a remote terminal and keys in the password PW_i. Then the smart card performs the following steps.

1. The smart card gets a timing sequence T from the system.
2. With the password PW_i, the smart card can compute $r_{iw} = (0,\ f(PW_i))$.
3. Since the point A_i is stored in the smart card, so the line L_i can be constructed by passing through the two points r_{iw} and A_i.
4. Let B_i be the middle point of r_{iw} and A_i, thus

$$B_i = \Big(\frac{a_{i1}}{2},\ \frac{a_{i2} + f(PW_i)}{2}\Big). \tag{4}$$

5. The smart card computes a point $r_{iT} = (0,\ f(PW_i) + f(T))$ on the y-axis. Therefore, a new line L_{WT} can be constructed by passing through r_{iT} and B_i.
6. Choose a random point C_i from the line L_{WT}. Then the smart card sends the login request $[ID_i,\ A_i,\ C_i,\ T]$ to the system.

Fig. 1 illustrates the concept of the login phase.

The authentication phase

After receiving the login request $[ID_i,\ A_i,\ C_i,\ T]$, the system performs the following tasks to authenticate the legitimacy of the login user.

1. The system checks the correctness of the identification number ID_i and the timing sequence T.
2. Next, the system computes the point $r_{io} = (f(ID_i \cdot\ x_0),\ f(ID_i \cdot\ y_0))$. Therefore, the line L_i can be reconstructed by passing through the two points r_{io} and A_i.

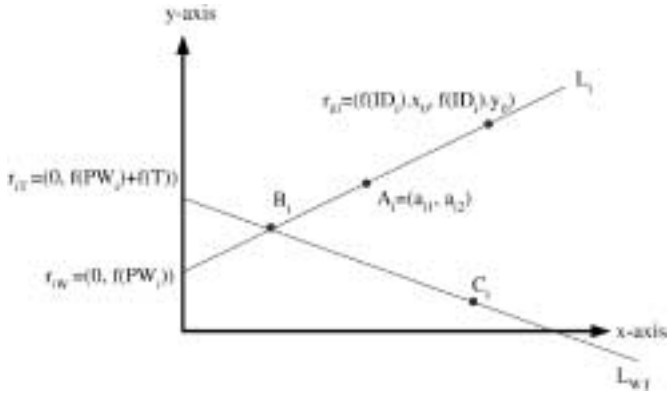

Fig. 1. Graphical result of the login phase.

3. According to the line L_i and y-axis, the intercept point r_{iw} can be computed and let r_{iw}=$(0,\ E_i)$.
4. The system computes the point $r_{iT} = (0,\ E_i + f(T))$, and then reconstructs the line L_{WT} which is passing through r_{iT} and C_i.
5. Compute the intercept point D_i of the lines L_i and L_{WT}. The system checks whether D_i is the middle point of A_i and r_{iw} or not. If so, then the system accepts the login request; otherwise rejects the login request.

Unfortunately, Wu's scheme was broken by Chien, Jan and Tseng (Chien *et al.*, 2001). The attack is illustrated as follows.

An attacker eavesdrops two login requests $[ID_i,\ A_i,\ C_i,\ T]$ and $[ID_i,\ A_i, C_i',\ T']$ for U_i at time T and T', respectively. Since f, T, and T' are known, the values $f(T)$ and $f(T')$ can be computed by the attacker. Suppose that $r_{iw} = (0, k)$, where $k = f(PW_i)$, hence the points r_{iT} and $r_{iT'}$ become $(0,\ k+f(T))$ and $(0,\ k+f(T'))$. According to the points $(r_{iw},\ A_i)$, $(r_{iT},\ C_i)$, and $(r_{iT'},\ C_i')$, the attacker can reconstruct three equations from the lines L_i, L_{WT} and L'_{WT}, respectively. Since the three equations intercept at the same point B_i and only contains three variables k, x, and y, the attacker can easily derive the variable k. Therefore, the attacker can reconstruct the secret line L_i. Thus, the system is not secure. Fig. 2 illustrates the graphical result of Chien, Jan and Tseng's attack.

On the other hand, Chien, Jan and Tseng also presented an improved scheme. They modified $r_{iT} = (0,\ f(PW_i) + f(T))$ to become $r_{iT} = (0,\ f(PW_i) \oplus f(T))$ in Step 5 of the login phase and the system computes $r_{iT} = (0,\ E_i \oplus f(T))$ in Step 4 of the authentication phase, where $\oplus$ is the bit-wise exclusive OR operation. The other steps are kept the same as in Wu's scheme. The modified scheme is claimed that it is secure against Hwang's and Chien-Jan-Tseng's attack.

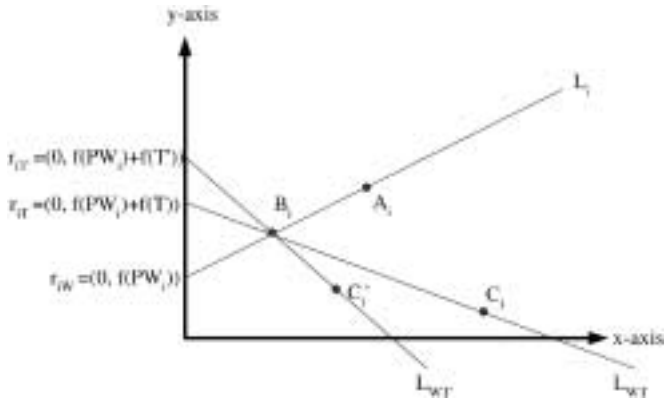

Fig. 2. Graphical result of Chien, Jan and Tseng's attack.

3. The Weakness of Chien, Jan and Tseng's Modified Remote Login Authentication Scheme

In Chien, Jan and Tseng's attack, an attacker can easily derive the secret point r_{iw} from the eavesdropped login requests. If we denote r_{iw} as $(0, k)$, then the points r_{iT} and $r_{iT'}$ can be expressed as $(0,\ k + f(T))$ and $(0,\ k + f(T'))$, respectively. Since the values of $f(T)$ and $f(T')$ can be computed, the attacker can reconstruct three equations from the lines L_i, L_{WT}, and $L_{WT'}$, which contain only three variables k, x, and y. So the attacker can compute the value of k. The idea of this attack is to find the directed distances $\overrightarrow{r_{iw}r_{iT}}$ and $\overrightarrow{r_{iw}r_{iT'}}$.

To remedy this weakness, Chien, Jan and Tseng replaced the addition operation with the bit-wise exclusive OR operation to compute the secret points r_{iT} and $r_{iT'}$. They claimed that the attacker can not know the directed distances of $\overrightarrow{r_{iw}r_{iT}}$ and $\overrightarrow{r_{iw}r_{iT'}}$ from the values of $f(T)$ and $f(T')$ in their improved scheme. Therefore, the attacker has no ability to impersonate a legal user and this improved scheme can withstand all possible attacks. However, the modification is not secure. We still can derive the directed distances from the values of $f(T)$ and $f(T')$. In the following, we present an approach to break Chien, Jan and Tseng's scheme.

Different from Chien, Jan and Tseng's attack, an attacker has to eavesdrop at least three login requests such as $[ID_i,\ A_i, C_i,\ T]$, $[ID_i,\ A_i, C_i',\ T']$, and $[ID_i,\ A_i, C_i'',\ T'']$ for U_i at time T, T' and T'', respectively. Then, the attacker performs the follows steps.

1. Since $f()$ is public and T, T', and T'' are known, the attacker computes the values of $f(T)$, $f(T')$, and $f(T'')$.
2. Let the bit positions of a binary expression from right to left be $0, 1, 2, \cdots, l$. The attacker computes the different bit positions between $f(T)$ and $f(T')$. Meanwhile, the attacker computes the different bit positions between $f(T)$ and $f(T'')$. Then, the attacker obtains a set $S_{TT'}$, which is $\{a_1, a_2, \cdots, a_n\}$, where $a_1, a_2, \cdots, a_n$ are the different bit positions between $f(T)$ and $f(T')$. And the attacker obtains another set $S_{TT''}$, which is $\{b_1, b_2, \cdots, b_m\}$, where $b_1, b_2, \cdots, b_m$ are the different bit positions between $f(T)$ and $f(T'')$.
3. Let $r_{iT} = (0,\ z)$ be a point on y-axis, where $z = f(PW_i) \oplus f(T)$. And $r_{iT'}$ and $r_{iT''}$ denoted as $(0,\ z + u)$ and $(0,\ z + v)$ be two points on y-axis, where $u = (f(PW_i) \oplus f(T')) - (f(PW_i) \oplus f(T))$ and $v = (f(PW_i) \oplus f(T'')) - (f(PW_i) \oplus f(T))$.
4. The attacker does not know the value $f(PW_i)$, so he/she can not compute the difference between u and v. But, the attacker has the ability to obtain some possible values of u from computing the different bits between $f(T)$ and $f(T')$. Let PV_u be the set of possible values of u, which can be expressed as $PV_u = \{x \mid x = \pm 2^{a_1} \pm 2^{a_2} \pm \cdots \pm 2^{a_n}\}$. Furthermore, the attacker can obtain some possible values of v from computing the different bits between $f(T)$ and $f(T'')$. Let PV_v be the set of possible values of v, which can be expressed as $PV_v = \{x \mid x = \pm 2^{b_1} \pm 2^{b_2} \pm \cdots \pm 2^{b_m}\}$. Therefore, the numbers of possible values of u and v are 2^n and 2^m, respectively. The set of possible pairs of (u, v)'s are $PP = \{(u, v) \mid\ u \in PV_u$ and $v \in PV_v\ \}$.

5. Pick out one possible pair (u, v) from PP, the line L_{WT} can be reconstructed by passing through the two points C_i and r_{iT}; similarly the line $L_{WT'}$ can be reconstructed by passing through the two points C_i' and $r_{iT'}$; the line $L_{WT''}$ can be reconstructed by passing through the two points C_i'' and $r_{iT''}$. Therefore, the attacker can build three equations from the reconstructed lines L_{WT}, $L_{WT'}$, and $L_{WT''}$, which only contain three variables z, x, and y. Obviously, the variable z and the point $B_i = (x, y)$ can be easily derived by solving the three equations.
6. After the values of z and $f(T)$ are computed, the attacker can easily compute $f(PW_i) = z \oplus f(T)$ and obtain the secret point $r_{iw} = (0,\ f(PW_i))$.
7. To validate the secret point r_{iw}, the attacker checks whether the derived point B_i is the middle point between r_{iW} and A_i. If so, the attacker confirms that the derived secret point r_{iW} is correct. Then the attacker can impersonate the legal user to forge a valid login request. Therefore, the system is not secure.

The concept of this attack is explained in Fig. 3.

In the following, we give a simple example to illustrate the weakness of Chien, Jan and Tseng's scheme.

Example

Assume that $p = 23$ and an attacker has eavesdropped three login requests $[ID_i, A_i, C_i, T]$, $[ID_i, A_i, C_i', T']$, and $[ID_i, A_i, C_i'', T'']$ from U_i, where $A_i = (8, 3)$, $C_i = (8, 7)$, $C_i' = (2, 12)$, and $C_i'' = (-4, 19)$. Then the attacker performs the following steps.

1. Since f, T, T', and T'' are known, the attacker can compute the values $f(T) = 11111011,\ f(T') = 11101011$, and $f(T'') = 11110010$.
2. After comparing $f(T)$ with $f(T')$ and $f(T'')$, the attacker obtains the set $S_{TT'} = \{4\}$ and $S_{TT''} = \{0, 3\}$, respectively.
3. Suppose that $r_{iT} = (0, z)$, then $r_{iT'} = (0, z + u)$ and $r_{iT''} = (0, z + v)$. The possible values of u are $PV_u = \{16,\ -16\}$, and the possible values of v are

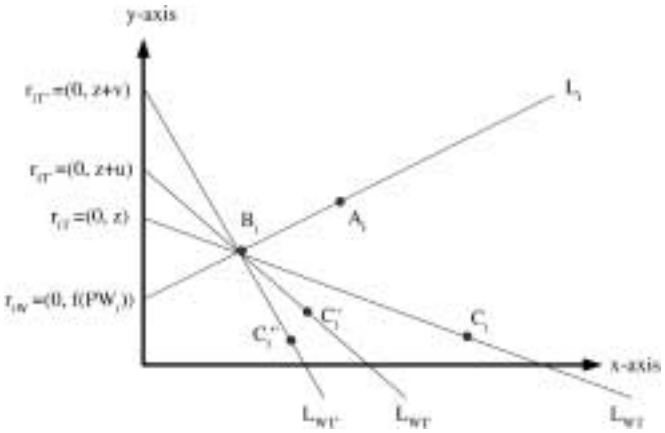

Fig. 3. Graphical result of our attack.

$PV_v = \{9,\ 7,\ -9,\ -7\}$. Therefore, there are 2^{1+2} possible pairs of $(u,\ v)'s$. They are $PP = \{(16,9),(16,7),(16,-9),(16,-7),(-16,9),(-16,7),(-16,-9),(-16,-7)\}$.

4. If we pick out $(u,v) = (16,9)$ from the set PP and we know the points $r_{iT} = (0,z)$, $r_{iT'} = (0,z+16)$, $r_{iT''} = (0,z+9)$, $C_i = (8,7)$, $C_i' = (2,12)$, and $C_i'' = (-4,19)$, we can reconstruct three lines.

$$L_{WT}: \quad y = z + \frac{7-z}{8}x \mod 23, \tag{5}$$

$$L_{WT'}: \quad y = z + 16 + \frac{-4-z}{2}x \mod 23, \tag{6}$$

$$L_{WT''}: \quad y = z + 9 + \frac{10-z}{-4}x \mod 23. \tag{7}$$

5. Since the three lines intercept at the same point B_i, and only contain three variables z, x, and y, so the attacker can solve these equations to obtain $z = f(PW_i) \oplus f(T) = 3$ and the point $B_i = (x,y) = (4,5)$. Moreover, the attacker derives $f(PW_i) = z \oplus f(T) = 7$ to get the feasible secret point $r_{iw} = (0, f(PW_i)) = (0,7)$.
6. Since the equation $B_i = (4,5) = (\frac{0+8}{2}, \frac{7+3}{2})$ holds, so B_i is the middle point between r_{iW} and A_i. Therefore, the attacker confirms that the point r_{iw} is correct. Then the attacker can impersonate U_i to forge a valid login request.

Furthermore, in order to reduce the number of possible pairs in set PP, the attacker can eavesdrop more than three login requests, and then select three of these login requests such that $n+m$ is smallest.

4. Conclusions

In this article, we have shown how an attacker can know the directed distances of $\overrightarrow{r_{iw}r_{iT}}$ and $\overrightarrow{r_{iw}r_{iT'}}$ from the values of $f(T)$ and $f(T')$ in Chien-Jan-Tseng's modified remote login authentication scheme. Therefore, an attacker can derive the secret point for a legal user from some eavesdropped login requests, and then the attacker has the ability to forge the login request. Although the system modified by Chien, Jan and Tseng is not secure, it has opened a brand new research area for remote login authentication scheme on a geometric approach.

References

Chang, C.C., and T.C. Wu (1991). Remote password authentication with smart cards. In *IEE Proceedings-E*, 138. pp. 165–168.

Chang, C.C., S.M. Tsu and C.Y. Chen (1995). Remote scheme for password authentication based on theory of quadratic residues. *Computer Communications*, **18**(12), 936–942.

Chien, H.Y., J.K. Jan and Y.M. Tseng (2001). A modified remote login authentication scheme based on geometric approach. *The Journal of Systems and Software*, **55**, 287–290.

Hwang, M.S. (1999). Cryptanalysis of a remote login authentication scheme. *Computer Communications*, **22**(8), 742–744.

Liaw, H.T. (1995). Password authentication using triangles and straight lines. *Computers Math. Applic.*, **30**(9), 63–71.

Wu, T.C. (1995). Remote login authentication scheme based on a geometric approach. *Computer Communications*, **18**(12), 959–963.

Ch.-Ch. Chang received his BS degree in applied mathematics in 1977 and the MS degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his PhD in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980–1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University. From 1983–1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From August 1989 to July 1992, he was the head of, and a professor in, the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was a dean of the College of Engineering at the same university. From August 1995 to October 1997, he was the provost at the National Chung Cheng University. From September 1996 to October 1997, Dr. Chang was the acting president at the National Chung Cheng University. From July 1998 to June 2000, he was a director of the Ministry of Education of the R.O.C.. Since 2002, he has been a chair professor of National Chung Cheng University. Dr. Chang is a fellow of the IEEE, a fellow of IEE, a research fellow of National Science Council of R.O.C., and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, the International Association for Cryptologic Research, the Computer Society of the Republic of China, and the Phi Tau Phi Honorary Society of the Republic of China. His current research interests include database design, computer cryptography, image compression, and data structures.

I.-Ch. Lin received the BS in computer and information sciences from Tung Hai University, Taichung, Taiwan, Republic of China, in 1998; the MS in information management from Chaoyang University of Technology, Taiwan, in 2000. He received his PhD in computer science and information engineering in March 2004 from National Chung Cheng University, Chiayi, Taiwan. He is currently an assistant professor of the Department of Management Information System, National Chung Hsing University, Taiwan, ROC. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

Modifikuotos geometrinės nuotolinio prisijungimo autorizavimo schemos kriptoanalizė

Chin-Chen CHANG, Iuon-Chang LIN

1995 Wu pasiūlė geometrinę nuotolinio prisijungimo autorizavimo schemą. Tačiau Chien, Jan ir Tseng atlikta Wu schemos kriptoanalizė parodė, kad ši schema nėra saugi. Dėl to jie pasiūlė modifikuotą Wu schemos versiją. Šis straipsnis parodo, kad modifikuota nuotolinio prisijungimo autorizavimo schema turi rimtų trūkumų: nelegalus vartotojas gali lengvai suklastoti legalaus prisijungimo užklausą.