Cryptanalysis of a remote login authentication scheme *†

Li-Hua Li [†] Iuon-Chang Lin [‡] Min-Shiang Hwang [†]

Department of Information Management [†]
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@mail.cyut.edu.tw
Fax: 886-4-3742337

Department of Computer Science and [‡]
Information Engineering,
National Chung Cheng University,
Chaiyi, Taiwan, R. O. C.

August 25, 2001

A Remote Password Authentication Scheme for Multi-Server Architecture Using Neural Networks

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC89-2213-E-324-001.

†Responsible for correspondence: Prof. Min-Shiang Hwang

Cryptanalysis of a remote login authentication scheme

Abstract

In this paper, we present a cryptanalysis of Wu's proposed an efficient remote login authentication scheme which is based on simple geometric properties on the Euclidean plane. We show that the scheme contains pitfalls in the authentication phase.

Keywords: cryptography, password authentication, remote login

1 Introduction

In 1995, Wu proposed an efficient remote login authentication scheme [2] which is based on simple geometric properties on the Euclidean plane. Wu's scheme is much simpler to implement than other remote login authentication schemes. The main advantage of this scheme is that users can choose and change freely their passwords, and the proposed system does not need verification tables for authenticating login requests.

Wu claimed that the security of his scheme is based on the shared line L_i constructed in the registration phase. However, if an illegal user has the ability to reconstruct L_i, then he can impersonate a legal user by forging a valid authentic message and replaying it to pass the check in the authentication phase. In this paper, we show that an illegal user may intercept a valid login request and replay it later to impersonate a legal user.

2 The Weakness of Wu's Scheme

The proposed remote login authentication scheme is based on simple geometric properties on the Euclidean plane [2]. It is divided into three phases: registration, login, and authentication. The registration phase is completed by the central authority (CA), whose main role is to deliver a smart card to each registered user. The smart card contains four public parameters, denoted as ID_i, f, P, and A_i, which are used in the login and authentication phases. The paraments are defined as follows:

- ID_i is a random integer given to each registered user.
- f is a one-way function [1].
- P is a large prime.
- A_i is the middle point of r_{iw} and r_{io} on the Euclidean plane. Here,

$$
\begin{aligned}
r_{iw} &= (0, f(PW_i)), && (1)\\
r_{io} &= (f(ID_i \cdot x_0), f(ID_i \cdot y_0)), && (2)\\
A_i &= (\frac{f(ID_i \cdot x_0)}{2}, \frac{f(PW_i) + f(ID_i \cdot y_0)}{2}), && (3)\\
&= (a_{i1}, a_{i2}),
\end{aligned}
$$

  where the pair (x_0, y_0) is a random integer and kept confidential by the system; PW_i is the password of the registered user U_i.

In the login phase, the user U_i first inserts his own smart card into a terminal and keys in his password PW_i. Next, the smart card constructs four public parameters, denoted as ID_i, A_i, C_i, and T, which are transmitted to the system and used in the authentication phases. The paraments are defined as follows:

- T is a timing sequence from the system.

- C_i is a random point on the line L_{WT} which passes through r_{iT} and B_i. Here,

$$\begin{aligned} r_{iT} &= (0, f(PW_i) + f(T)), & (4) \\ B_i &= (\frac{a_{i1}}{2}, \frac{f(PW_i) + a_{i2}}{2}). & (5) \end{aligned}$$

Figure 1 illustrates the graphical result of the login phase for user U_i.

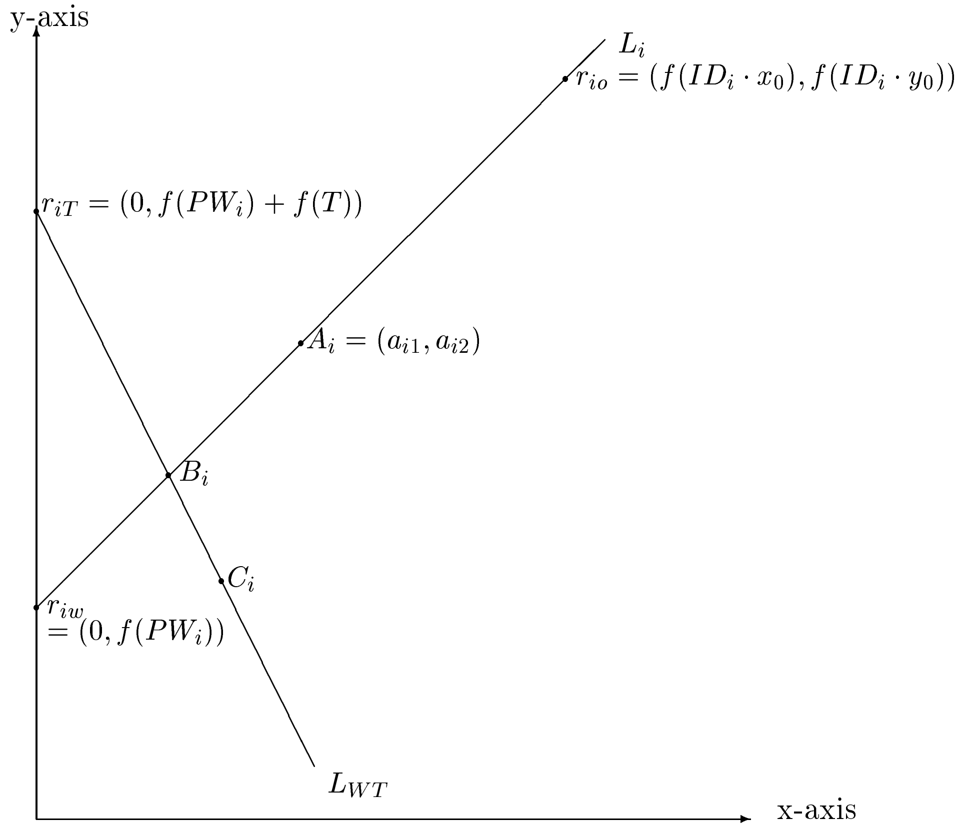

Figure 1: Graphical result of the login phase for user U_i

In the authentication phase, the system performs the following tasks to authenticate the user's login request.

- Validate the identity ID_i and the timing sequence T.
- Reconstruct the line L_i passing through points r_{io} and A_i, where $r_{io} = (f(ID_i \cdot x_0), f(ID_i \cdot y_0))$.
- Find the points r_{iw} and r_{iT} as follows.

$$r_{iw} = (0, E_i), \qquad (6)$$

$$r_{iT} = (0, E_i + f(T)), \tag{7}$$

where E_i is a intercept of the y-axis and line L_i.

- Find the intersection D_i of line L_i and L_{WT}. Here, L_{WT} is a line passing through points r_{iT} and C_i.
- If D_i is identical to the middle point of A_i and r_{iw}, then accept the login request; otherwise, reject the login request.

We give a simple example below to illustrate how Wu's scheme works.

Example 1:

Let $P = 23$, $(x_0, y_0) = (2, 3)$, $f = x^2 + 1 \bmod P$. Assume that the identity and password of the new user U_i are $ID_i = 8$ and $PW_i = 6$. In the registration phase, CA computes points $r_{iw} = (0, 14)$, $r_{io} = (4, 2)$, and $A_i = (2, 8)$; and stores four public parameters: $ID_i = 8$, $f = x^2 + 1$, $P = 23$, and $A_i = (2, 8)$ in a smart card which is delivered to U_i by hand.

In the login phase, U_i inserts his own smart card into a terminal and keys in his password $PW_i = 6$. Assume that the timing sequence T from the system is 7. The smart card computes points $r_{iT} = (0, 18)$ and $B_i = (1, 11)$ and constructs a line L_{WT}, $7x + y = 18(\mathrm{mod} 23)$, which passes through points r_{iT} and B_i. The smart card randomly chooses a point $C_i = (3, -3) = (3, 20)$ over GF(23) on the line L_{WT}. Next, the smart card transmits the public parameters ($ID_i = 8$, $A_i = (2, 8)$, $T = 7$, $C_i = (2, 4)$) to the system.

In the authentication phase, the system computes the point $r_{io} = (4, 2)$ and constructs the line $L_i = 3x + y = 14(\mathrm{mod} 23)$ passing through points r_{io} and A_i. The system computes the points $r_{iw} = (0, E_i) = (0, 14)$, $r_{iT} = (0, 18)$, and $D_i = (1, 11)$. Since $D_i = B_i$, the system accepts the login request.

The security of Wu's scheme is based on the shared line L_i constructed in the registration phase. If an illegal user has the ability to reconstruct L_i, then he can impersonate the legal user by forging a valid authentic message and replaying it to pass the check in the authentication phase [2]. Here, we show that an illegal user can obtain $f(PW_i)$ and the line L_i as follows.

1. Let point $R = (a_{i1}, y)$ and construct a line L_{RA}, $x = a_{i1}$, passing through points $R = (a_{i1}, y)$ and $A_i = (a_{i1}, a_{i2})$.

2. Since an illegal user can easily intercept A_i, C_i, and T in the login phase and both f and P are made public, the illegal user can compute $f(T)$. Therefore, he can obtain y by computing:

$$y = a_{i2} - f(T). \tag{8}$$

3. Construct the line L_{WT} passing through points R and C_i.

4. Find the intercept point $r_{iT} = (0, f(PW_i) + f(T))$ of the y-axis and the line L_{WT}.

5. Obtain $f(PW_i)$ and the point $r_{iw} = (0, f(PW_i))$ by computing $r_{iT} - (0, f(T))$.

6. The line L_i can thus be constructed by passing through points A_i and r_{iw}.

It is easy to show that triangle $\triangle r_{iw} B_i r_{iT}$ is equal to triangle $\triangle A_i B_i R$ according to the Angle-Side-Angle (ASA) rule. Therefore, the point B_i is the middle point of points r_{iw} and A_i, and of points r_{iT} and R. Figure 2 illustrates the graphical result of our supposition.

We give the same example as Example 1 to illustrate the pitfalls of Wu's scheme. Assume that an illegal user have intercepted $A_i = (2, 8)$, $C_i = (3, 20)$, and $T = 7$ in the public network. Since both f and P are made public, the illegal user can easily obtain both $P = 23$ and $f = x^2 + 1 \bmod 23$.

Example 2:

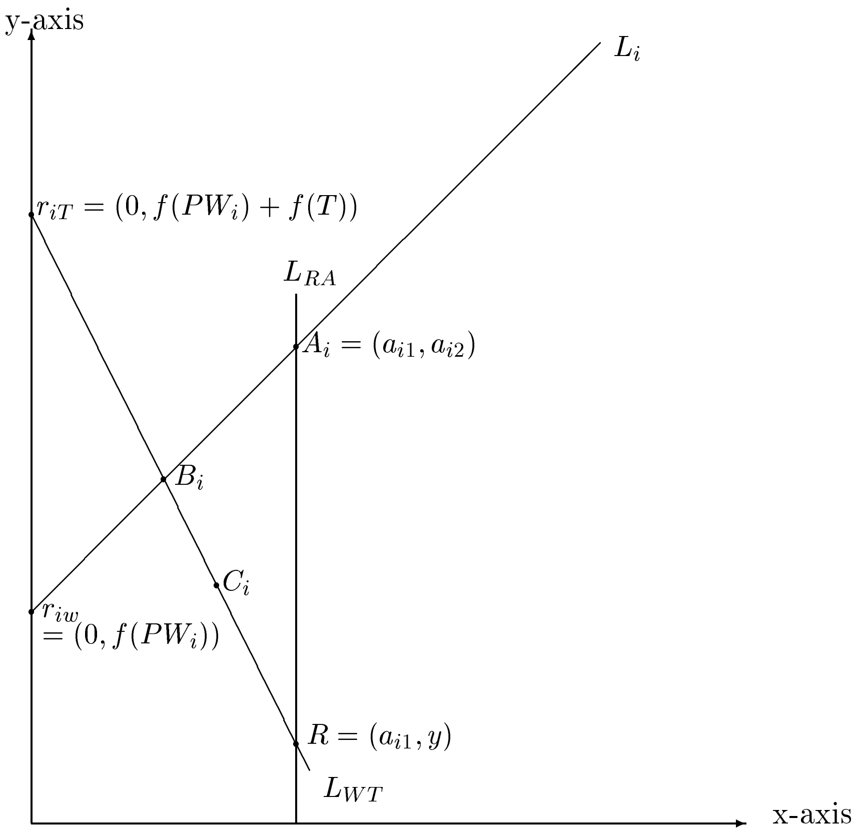

Figure 2: Graphical result of our supposition

1. Let point $R = (2, y)$ and construct a line L_{RA}, $x = 2$, passing through points $R = (2, y)$ and $A_i = (a_{i1}, a_{i2}) = (2, 8)$.

2. Compute $f(T) = 4$ and $y = a_{i2} - f(T) = 8 - 4 = 4$.

3. Construct the line L_{WT}, $8x + 11y = 14(\bmod 23)$, passing through points $R = (2, 4)$ and $C_i = (3, 20)$ over GF(23).

4. Find the intercept point $r_{iT} = (0, 18) = (0, f(PW_i) + f(T))$ of the y-axis and the line L_{WT}.

5. Obtain $f(PW_i) = 14$ and the point $r_{iw} = (0, 14)$.

6. Construct the line L_i, $3x + y = 14(\bmod 23)$, passing through points $A_i = (2, 8)$ and $r_{iw} = (0, 14)$.

3 Conclusions

In this paper, we present a cryptanalysis of Wu's remote login authentication scheme. We have shown that an illegal user can easily intercept a valid login request and replay it later to impersonate a legal user in the authentication phase.

References

[1] Lamport, L 'Password authentication with insecure communication', *Comm. ACM*, Vol 24 No 11 (1981) pp. 770–772

[2] Wu, T C 'Remote login authentication scheme based on a geometric approach', *Computer Communications*, Vol 18 No 12 (1995) pp. 959–963