The importance of ensuring privacy and security is acute because of the rapid progress and prevalence of multi-user computing environments. Various types of security mechanisms have been employed to preclude information leakage in the computer systems being disclosed, destroyed, altered or copied by unauthorised users. The password mechanisms have been employed to preclude information leakage. However, these mechanisms can be easily broken down if the test patterns or verification tables are modified by malicious users in these approaches. Chang and Wu [2] proposed a password authentication scheme without verification tables. In their scheme, the system is burdened with requests for additional information other than the ID and PW in the login stage.

Consider only the remote password authentication schemes in remote access systems. The privacy and security problems are threatened by potential attacks from the remote terminals, along the communication links, as well as the system itself [13]. Lamport [11] proposed a scheme which protects against attacks of replaying previously intercepted requests. This scheme is insecure if the encrypted password stored in the centre is modified by an intruder. Denning [5] proposed another method by using the signature scheme of a public-key cryptosystem. That system also maintains verification tables. A remote password authentication system has the following characteristics:

(i) The system does not need to store or maintain verification tables.
(ii) The login request should be verified easily and quickly.
(iii) The scheme is secure against attacks of replaying previously intercepted requests.

Inspired by Shamir's identity-based signature scheme [18], a remote password authentication scheme based on the Chinese remainder theorem is proposed. A brief review of Shamir's identity-based signature scheme is stated before presenting the scheme.

2 Review of Shamir's identity-based signature scheme

The identity-based cryptosystems and the signature scheme proposed by Shamir [18] enable any pair of users to communicate securely and to verify each other's signature without exchanging private or public keys and without keeping key directories. It also eliminates use by a third party. Shamir's identity-based signature scheme is described first.

Let n, p, q, e and d be parameters in the RSA scheme [16], where p and q are large primes and n = pq, e and d be parameters in the RSA scheme [16], where p and q are large primes and n = pq, ed = 1 mod (p - 1)(q - 1). The system publishes e and n. p, q and d are kept secret. That is, d is known only to the key generation centre. The ith user's secret key $K_i$ is computed by the centre as

$$K_i = (ID)^{d_i} \mod n$$

where $ID_i$ is the ith user's identity. The ith user may sign a message $m$ and the signature of $m$ can be verified by anyone who knows $ID_i$ as

$$t = r^e \mod n$$

$$s = K_i^{e_i} m \mod n$$
where \( r \) is a random number selected by the user and \( f \) is
a one-way function. The pair \((t, t)\) is the signature of \( m \).
To anyone who knows \( ID_i \), the signature of \( m \) can be
easily verified using the test
\[
s^* = ID_i f^{10^m} \mod n
\]
(4)

For physical implementation, the secret key generated by
the centre is issued to the user in the form of smart card
when the user first registers to the system. A smart card is
an IC processor which can efficiently perform computational operations [14]. The smart card possessed by
the user contains a microprocessor, and I/O port, a RAM, a
ROM with the user’s secret key and programs for generating
and verifying the signature [18]. Any pair of users
can verify each other’s signature easily and quickly.

When the user first registers to the system. A smart card is
issued to the user in the form of smart card

The merits of Shamir’s identity-based signature scheme is that it is simple and secure. It is also suitable
for remote access systems. It is weak against the potential attack of replaying previously intercepted authentication keys if an intruder knows the identity \( ID_i \) and eavesdrops
on the signature message \( s \) and \( t \).

A new remote password authentication scheme is presented. The concept of timestamps [6] is employed to avoid attacks by using the strategy of replaying previously intercepted passwords.

3 Proposed scheme

Since the scheme uses the Chinese remainder theorem (CRT), the theorem is described. Given \( 2n \) positive integers \( m_1, m_2, \ldots, m_n \), and \( r_1, r_2, \ldots, r_n \), a constant \( C \) can be found such that
\[
C = r_i \mod m_i, \quad C = r_j \mod m_j, \quad C = r_k \mod m_k
\]
if \( m_i, m_j, \) and \( m_k \) are relatively prime for all \( i \neq j \) [17].

The CRT can be applied to encrypt the plaintext and
decrypt the ciphertext. Let \( d_1, d_2, \ldots, d_n \) be \( m \) large relatively prime numbers and \( a_1, a_2, \ldots, a_n \) be \( m \) plain messages. The encrypted data is
\[
C = a_i \mod d_i, \quad i = 1, 2, \ldots, m
\]
The value \( a_i \) can be recovered computing
\[
a_i = C \mod d_i
\]
Let \( D = d_1 d_2 \ldots d_n \) and \( b_i \) satisfy
\[
\left( \begin{array}{c}
D
\end{array} \right) b_i \equiv 1 \mod d_i, \quad i = 1, 2, \ldots, m
\]
The encryption keys can be computed as
\[
e_i = \left( \begin{array}{c}
D
\end{array} \right)^{-1} a_i, \quad i = 1, 2, \ldots, m
\]
By the CRT
\[
C \equiv \left( \sum_{i=1}^{n} e_i a_i \right) \mod D
\]
The proposed remote password authentication scheme can be divided into three phases. In the initial phase,
when a user registers to the system, the password generation centre generates a password (PW) for the user
according to the presented identity (ID). The password is
returned to the user through a very secure channel or by
hand. A smart card, storing the information used by the
login and authentication phases, is constructed and
delivered to the user. In the login phase, the user attaches
the smart card to a terminal and submits the ID and PW.

In the authentication phase, the system verifies the remotely submitted password to check if the login
request is accepted or rejected.

Let \( d_1, d_2, \ldots, d_n \) be large relatively prime numbers
and \( D = d_1 d_2 \ldots d_n \), where \( d_1, d_2, \ldots, d_n \) are known
only to the password generation centre. Let \( g \) be a pseudo-random number generating function and \( f \) be a
one-way function. The algorithm of \( g \) should be kept
secret in the system, i.e., anyone who knows \( x \) cannot
predict the value of \( g(x) \), and the value of \( g(x) \) is less than
\( D \). \( D \) and \( f \) can be made public.

Initial phase: When a new user \( U_i \) registers to the system,
the identity \( ID_i \) should be presented to the system. The
password generation centre does the following:
(i) Generate a password \( PW_i = (w_{11}, w_{12}, \ldots, w_{1m}) \),
\[
w_j = g(ID_i) \mod d_j \quad j = 1, 2, \ldots, m
\]
(10)
and \( m \) is predetermined integer, say \( m = 5 \).
(ii) Deliver a smart card, which contains the information
\( \{ f, e_1, e_2, \ldots, e_n \}, d_i \), to the user \( U_i \).
The smart cards possessed by all users are the same. The
smart card contains a microprocessor which can perform
arithmetic operations quickly, an I/O port, a RAM, a
ROM in which is stored the algorithmic description of
the one-way function \( f \) and parameters \( e_1, e_2, \ldots, e_n \)
and \( D \), and programs for generating signature and
authenticating message.

Login phase: For login the system, \( U_i \) first attaches the
smart card to a terminal. The \( ID_i \) and \( PW_i \) are then keyed in.
The smart card performs the following tasks:
(i) Generate a random vector \( (r_1, r_2, \ldots, r_n) \).
(ii) Let \( PW_i = (w_{i1}, w_{i2}, \ldots, w_{im}) \). Compute
\[
t = \left( \sum_{i=1}^{n} e_i r_i \right) \mod D
\]
(11)
\[
s = (w_{11}, w_{12}, \ldots, w_{im}) + (r_1, r_2, \ldots, r_m) f(t, T)
\]
(12)
where \( T \) is the login current date and time used as time-
stamp.
(iii) Construct the authenticating message \( C = [ID_i, t, \ s, T] \) and transmit \( C \) to the system by communication
link.
The pair \((t, s)\) computed by the smart card is used as the
signature. The timestamp \( T \) is employed to withstand
potential attacks of replaying previously intercepted
passwords. When the login procedure is finished, the authen-
tication phase follows.

Authentication phase: Let \( T' \) be the date and time when
the system receives the message \( C \) sent by the login user
\( U_i \). After receiving the message \( C \), the system verifies
the remote login with the following steps:
(i) Check if the format of \( ID_i \) is correct. If it is incorrect
then reject the login request.
(ii) Test if \( T' - T \leq \Delta T \), where \( \Delta T \) is the legal time
interval for transmission delay. If it is false, then reject
the login request.
(iii) Encrypt \( s \) by keys \( (e_1, e_2, \ldots, e_n) \). Then test if the
result is equal to \( g(ID_i) + f(t, T) \) \( \mod D \). If it is true,
then accept the login request; otherwise, reject the login
request.
Examining step (iii) of the authentication phase carefully, it is found that the result of encrypting $s$ is equal to

$$\left(\sum_{j=1}^{n} e_j x_j\right) \mod D$$

$$= \left(\sum_{j=1}^{n} e_j w_j + r_j f(t, T)\right) \mod D$$

$$= \left(\sum_{j=1}^{n} e_j w_j\right) \mod D + \left(\sum_{j=1}^{n} e_j r_j\right) f(t, T) \mod D$$

$$= g(ID_i) + r f(t, T) \mod D$$

4 Security analysis and discussions

The secrecy of the CRT is based on the factoring of the large number $D$. As pointed out in Reference 3, if one knows $(C, w_j)$ and $(C, w_j')$ pairs computed from

$$w_j = C \mod d_j$$

$$w_j' = C' \mod d_j$$

then

$$C - w_j = Q d_j$$

$$C - w_j = Q' d_j$$

for some $Q$ and $Q'$. It has a high probability of revealing $d_j$ by finding the greatest common divisor of $C - w_j$ and $C - w_j'$. In the initial phase of generating passwords, the password $PW_i$ has a one-to-one correspondence to the returned value of a secure pseudorandom number generating function $g$ with identity $ID_i$, as the seed of $g$. It can therefore prevent any two conspiratorial users with known $(ID_i, PW_i)$ and $(ID_j, PW_j)$ pairs from maliciously revealing $d_j$. It should be noted that the users with different identities may have the same passwords if the function $g$ is not a one-to-one mapping.

An intruder may try to masquerade as $U_i$ by replaying previously intercepted message $C = (ID_i, t, s, T)$. To pass step (iii) in the authenticating phase, the intruder must change the timestamp $T$ to $T^*$ such that $T - T^* \leq \Delta T$. Once the timestamp $T$ is changed, either $t$ or $s$ has to be changed. So the scheme can withstand potential attacks with the strategy of replaying a previously intercepted login request.

The encryption keys $e_j$'s can be predetermined in the scheme presented. The computational complexities of the scheme are examined in each phase. Let $T_f$ be the time required for the pseudorandom number generating function $g$, and let $T_f$ be the time required for the one-way function $f$. The time complexities in each stage are listed below.

**Initial phase:**

Time for password generation

$$= T_g + (m \text{ modular operations})$$

**Login phase:**

Time for computing $s = (m \text{ multiplications})$

$$+ \{m - 1\ \text{additions}\}$$

$$+ (1 \text{ modular operation})$$

Time for computing $t = T_f + (m \text{ multiplications})$

$$+ (m \text{ additions})$$

Authentication phase:

Time for encrypting $s = (m \text{ multiplications})$

$$+ \{m - 1\ \text{additions}\}$$

$$+ (1 \text{ modular operation})$$

Time for verification $= T_f + T_f' + (1 \text{ multiplication})$

$$+ (1 \text{ addition})$$

$$+ (1 \text{ modular operation})$$

$$+ (1 \text{ comparison})$$

The login and authentication phases can be performed easily and quickly by applying the smart card. However the user of the system cannot choose his password freely. If a user’s password has to be changed, for some security considerations, a new identity has to be reassigned to the user and the old identity should not be used by new users in the initial phase.

5 Conclusions

A remote password authentication scheme which does not use a directory of passwords or verification tables is presented. The scheme is very useful in remote access systems or computer networks with remote login under insecure communication links. By employing the concept of timestamps, the scheme can withstand attacks which use the strategy of replaying previously intercepted login request. A disadvantage of the scheme is that a very secure channel is required for the return of the password to the registering user. The users cannot freely choose their passwords. The problem of allowing users to freely choose their passwords in the authentication system without storing verification tables still remains open.

6 Acknowledgments

The authors would like to thank the referees for useful comments which have improved the presentation of this paper.

7 References


5 DENNING, D.E.: ‘Cryptography and data security’(Addison-Wesley, Massachusetts, 1982)


17 SCHROEDER, M.R.: 'Number theory in science and communication' (Springer-Verlag, Berlin, 1983)