AN EFFICIENT REMOTE USE AUTHENTICATION SCHEME USING SMART CARDS
Hung-Min Sun
Department of Computer Science and Information Engineering
National Cheng Kung University
Tainan, Taiwan 701
Email: hmsun@mail.ncku.edu.tw

ABSTRACT
Based on the discrete logarithm problem, Hwang and Li [1] proposed a remote user authentication scheme using smart cards. Their scheme is very novel because no password table is required to keep in a system. In this paper, we further propose an efficient and practical remote user authentication scheme using smart cards. The proposed scheme not only provides the same advantages as that of Hwang and Li’s scheme, but also significantly reduces the communication and computation costs.

Keywords: Authentication, Network Security, Cryptography, Password, Data Security

1. INTRODUCTION
Remote password authentication scheme, proposed by Lamport [2] in 1981, is a method to authenticate remote users over an insecure channel. Since then, several schemes [3-6] have been proposed to address this problem. Recently Hwang and Li [1] proposed a remote user authentication scheme using smart cards. Their scheme is very novel because no password table is required to keep in a system. In this paper, we further propose an efficient and practical remote user authentication scheme using smart cards. The proposed scheme not only provides the same advantages as that of Hwang and Li’s scheme, but also significantly reduces the communication and computation costs.

The remainder of this paper is organized as follows. In section 2, we review Hwang and Li’s remote password authentication scheme. In section 3, we propose an efficient and practical remote user authentication scheme. In section 4, we analyze the security of our scheme. In section 5, we evaluate the efficiency of our scheme. Finally, we conclude this paper in section 6.

2. HWANG AND LI’S SCHEME
In this section, we briefly review Hwang and Li’s remote password authentication scheme. The security of Hwang and Li’s scheme is based on the difficulty of the discrete logarithm problem [7]. There are three phases in Hwang and Li’s scheme. These phases include a registration phase, a login phase and an authentication phase. We review these three phases in the following.

Registration Phase: Let \( P \) be a large prime number which makes the discrete logarithm problem infeasible. Without loss of generality, we assume that \( P \) is of 1024 bits. Let \( x \) be a secret key maintained by the system. Assume that a new user \( U_i \) submits his identity \( ID_i \) to the system for registration. The system computes a password \( PW_i \) for the user \( U_i \) as follows:

\[
PW_i = ID_i^x \mod P.
\]

The registration center issues a smart card which contains a pair of public parameters (\( h, P \)), where \( h \) is a one-way function. The registration center also delivers \( PW_i \) to the user \( U_i \) through a secure channel.

Login Phase: If the user \( U_i \) wants to login, he attaches his smart card to his input device. Then he keys in his identity \( ID_i \) and password \( PW_i \) to the device. The smart card will perform the following operations:

1. Generate a random number \( r \).
2. Compute $C_1 = ID_i^t \mod P$.

3. Compute $t = h(T \oplus PW_i) \mod (P-1)$, where $T$ is the current date and time of the input device and $\oplus$ denotes an exclusive operation.

4. Compute $M = ID_i^s \mod P$.

5. Compute $C_2 = M(PW_i)^{-1} \mod P$.

6. Send a message $C = (ID_i, C_1, C_2, T)$ to the remote system.

**Authentication Phase:** After receiving the authentication message $C$, the system authenticates the login user using the following steps. Assume that the system receives the message $C$ at $T'$, where $T'$ is the current day and time of the system.

1. Check the validity of $ID_i$. If the format of $ID_i$ is not correct, then the system rejects the login request.

2. Check the validity of the time interval between $T$ and $T'$ in order to resist replaying attacks. If $(T' - T) \geq \Delta T$, where $\Delta T$ denotes the expected valid time interval for transmission delay, then the system rejects the login request.

3. Compute $PW_i = ID_i^y \mod P$ and $t = h(T \oplus PW_i) \mod (P-1)$. If $C_2(C_1)^{-1} \mod P = ID_i^t \mod P$, then the system accepts the login request. Otherwise, it rejects the login request.

3. **OUR SCHEME**

In this section, we propose an efficient remote password authentication scheme using smart cards. Unlike Hwang and Li's scheme, the security of our scheme is based on one-way function. We demonstrate our scheme as follows:

**Registration Phase:** Let $x$ be a secret key maintained by the system. Let $h$ is a one-way function with output of 64 bits. Assume that a new user $U_i$ submits his identity $ID_i$ to the system for registration. The system computes a password $PW_i$ for the user $U_i$ as follows:

$$PW_i = h(ID_i, x).$$

The registration center issues a smart card which contains the public one-way function $h$. The registration center also delivers $PW_i$ to the user $U_i$ through a secure channel.

**Login Phase:** If the user $U_i$ wants to login, he attaches his smart card to his input device. Then he keys in his identity $ID_i$ and password $PW_i$ to the device. The smart card will perform the following operations:

1. Compute $C_1 = h(T \oplus PW_i)$ where $T$ is the current date and time of the input device.

2. Send a message $C = (ID_i, C_1, T)$ to the remote system.

**Authentication Phase:** After receiving the authentication message $C$, the system authenticates the login user using the following steps. Assume that the system receives the message $C$ at $T'$, where $T'$ is the current day and time of the system.

1. Check the validity of $ID_i$. If the format of $ID_i$ is not correct, then the system rejects the login request.

2. Check the validity of the time interval between $T$ and $T'$ in order to resist replaying attacks. If $(T' - T) \geq \Delta T$, where $\Delta T$ denotes the expected valid time interval for transmission delay, then the system rejects the login request.

3. Compute $PW_i = h(ID_i, x)$ and $C_1' = h(T \oplus PW_i)$. If $C_1'$ match with $C_1$, then the system accepts the login request. Otherwise, it rejects the login request.

4. **SECURITY ANALYSIS**

In this section, we analyze the security of our scheme
as follows:

1. Replaying attacks (Replaying an old \((ID_i, C_i, T)\) in Login Phase) cannot work because this will make Step 2 of Authentication Phase fail.

2. An attacker may try to modify an old \((ID_i, C_i, T)\) into \((ID_i, C_i, T'')\) where \(T''\) is the current date and time in order to make Step 2 of Authentication Phase succeed. However such modification will make Step 3 of Authentication Phase fail because \(h(T'' \oplus PW_i) \neq C_i\).

3. No one can forge a valid \(C = (ID_i, C_i, T)\) because \(C_i (= h(T \oplus PW_i))\) must be derived from \(PW_i\).

4. Given a valid \(C = (ID_i, C_i, T)\), no one can compute \(PW_i\) from \(C_i (= h(T \oplus PW_i))\) because \(h\) is a one-way function.

5. **EFFICIENCY**

In this section, we evaluate the efficiency of our scheme by comparing our with Hwang and Li’s scheme. Here we assume that in Hwang and Li’s scheme \(P\) is of 1024 bits in order to make the discrete logarithm problem infeasible. In table 1, we list the efficiency comparison of our scheme and Hwang and Li’s scheme. It is clear that our scheme is much more efficient than Hwang and Li’s scheme in terms of communication and computation cost.

6. **CONCLUSIONS**

In this paper, we propose a new remote user authentication scheme using smart cards. Compared with Hwang and Li’s scheme, our scheme is much more practical and efficient in terms of communication and computation cost. Moreover, the password used in our scheme is of 64 bits that is very easy for user to memory, while the password used in Hwang and Li’s scheme is of 1024 bits that is very hard for user to memory. Furthermore, the security of Hwang and Li’s scheme is based on the difficulty of the discrete logarithm problem. Once the discrete logarithm problem is solved, then their scheme will become insecure. On the contrary, the security of our scheme is only based on one-way function whose existence is commonly accepted.

### Table 1 Efficiency comparison of our scheme and Hwang and Li’s scheme.

<table>
<thead>
<tr>
<th></th>
<th>Hwang-Li scheme</th>
<th>Our scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password length</td>
<td>1024 bits</td>
<td>64 bits</td>
</tr>
<tr>
<td>Number of data bit</td>
<td>2048 bits</td>
<td>64 bits</td>
</tr>
<tr>
<td>transmitted for login</td>
<td></td>
<td></td>
</tr>
<tr>
<td>phase*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computations of</td>
<td>1 Exponential</td>
<td>1 hashing</td>
</tr>
<tr>
<td>registration phase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computations of login</td>
<td>3 Exponential +1 hashing</td>
<td>1 hashing</td>
</tr>
<tr>
<td>phase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computations of</td>
<td>3 Exponential +1 hashing</td>
<td>2 hashing</td>
</tr>
<tr>
<td>authentication phase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public information</td>
<td>((h, P))</td>
<td>(h)</td>
</tr>
<tr>
<td>stored in smart card</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* The non-cryptographic parameters \(ID_i\) and \(T\) are excluded from reckoning.

## ACKNOWLEDGEMENTS

This work was supported in part by the National Science Council, Taiwan, under contract NSC-89-2213-E-006-118.

## REFERENCES


BIOGRAPHY

Hung-Min Sun received his B.S. degree in applied mathematics from National Chung-Hsing University in 1988, his M.S. degree in applied mathematics from National Cheng-Kung University in 1990, and his Ph.D. degree in computer science and information engineering from National Chiao-Tung University in 1995, respectively. He was an associate professor with the Department of Information Management, Chaoyang University of Technology from 1995 to 1999. Currently he is teaching at the Department of Computer Science and Information Engineering, National Cheng Kung University. His research interests include cryptography, information theory, network security, reliability, and distributed systems.