A User Friendly Implementation of Smart Card Access with Threshold Scheme

Shyi-Tsong Wu and Bin-Chang Chieu
Department of Electronic Engineering
National Taiwan University of Science and Technology
stwu@ilantech.edu.tw

Abstract

An implementation of security scheme with smart cards to access coffers is proposed in this paper. For some safety consideration, that access to coffers by a person is inadmissible but a group of authorized people. This involves the problem of secret sharing, and the adopted secret-shared scheme is threshold scheme. Every participant possesses a secret shadow, which will be encrypted and saved in the smart card. After correct reconstruction the shared secret, it is permissible to access the coffer’s door. For resisting dishonest participants, cheating detection and cheater identification will be included. That the user can change his password of smart card freely and need not to memorize his assigned lengthy password and shadow as traditional ID-based scheme makes our implementation much more user friendly.

1 Introduction

The security strength of access facilities with mechanical lock is poor for leaving no traces of identify of person who enter or exit the facility. Mechanical lock controlled by electronic key-card system is recommended. A user just only attaches his smart card to the card reader and keys in his password then can access the facility after authentication procedure. Based on the smart card and shared-secret scheme, Leong and Tan [1] described an elaborate implementation to access a laboratory door.

In this paper, a system that includes smart cards, shared-secret scheme, ID-based scheme, authentication, cheating detection and cheater identification is proposed. The user need not to memorize the lengthy shared-secret code and can change his password randomly at his will. The access data, including people's ID, access time, etc. are centralized saved at the control center host rather than distributed smart card memory for the accommodation of further analysis.

2 Some related cryptographic scheme

In this section, we will describe some cryptographic schemes that will be applied in our implementation. These are ID-based scheme, shared-secret scheme and cheater identification.

ID-based scheme

In conventional password authentication scheme, when a user requests to login a system, he must enter his ID and password for authentication. A directory table is used to store users' IDs and PWs. The storing password schemes often hash the password with a one-way function rather than plain password in the directory table.

Some enhanced authentication schemes with smart card [2], [3], [4], [5] are proposed to eliminate the drawbacks of using directory table. These schemes adopted the ID-based signature scheme and have the following advantages: (1) neither secret nor public keys need to be exchanged, (2) the public key directory table is not needed, and (3) the assistance of a third party is not required.

The first ID-based signature scheme was proposed by Shamir [6]. However, in Shamir’s ID-based scheme, the secret key corresponding to an ID was assigned and the concept of timestamp was absent. Chang and Wu’s scheme [4] had the same problem that a user’s password was assigned by password generation center and it is against the users’ habit.

Yang and Shieh proposed password authentication schemes with smart card [7] that applied the timestamp concept and allowed the user choose and change his password as will. In our implementation, timestamp concept and the characteristic of user friendly will be adopted.

Shared-secret scheme

The solution of access to coffer of bank by a group of authorized people is threshold scheme. It divides secret data S into n pieces S₁, S₂, …., Sₙ in such a way that: (1) any k-1 or less shadows reveal no knowledge about S; (2) any k or more shadows can be used to reconstruct S. This is known as (k, n) threshold scheme.

Shamir [8] published the threshold scheme based on a polynomial interpolation. Each member was assigned a shadow associated to the interpolating polynomial.
A polynomial, so that any k or more members together can reconstruct the secret. Shamir’s threshold scheme is an ideal threshold scheme for the reason that the domain of shadow is the same as the domain of secret [9].

Prior to using \( a_0 = S \) as the secret, the shadow distributor randomly choose \((k - 1)\) number of \( a_i \)s, for \( 1 \leq i \leq k - 1 \), to establish a polynomial \( f(x) \) of degree \((k - 1)\):

\[
f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}
\]

Computing \( S_i = f(X_i) \), \( i = 1, 2, \ldots, n \), the \( S_i \)s called the shadow of \( S \) for \( X_i \). Any \( k \) or more \( X_i \)s with \( S_i \), \(( X_i, S_i )\), can easily reconstruct \( f(x) \) and obtain the secret \( S = f(0) \). Given a set of two-tuples that includes at least \( k \) distinct \((X_1, S_1), (X_2, S_2), \cdots, (X_n, S_n)\), we can compute the \( f(x) \) of degree \((k - 1)\) by using Lagrange interpolation [10]:

\[
f(x) = \sum_{i=1}^{k} S_i \prod_{j=1, j \neq i}^{k} \left( \frac{x - X_i}{X_i - X_j} \right) \mod p \tag{2}
\]

To prevent obtaining \( S \) by exhaustive search, \( p \) must be relatively large and \( S \) must be relatively long in terms of bit length. Length of 128 bits will be sufficient for our application.

**Cheater detection and cheater identification**

Tompa and Woll’s suggested a \((k, n)\) threshold protecting policy to safeguard the secret [11]. However, their method cannot deterministically detect cheating and identify the cheater. Wu and Wu [12] applied one-way hash function for cheating and cheater identification. Their scheme is as following:

- **Initialization**
  Shadow distributor performs the following steps:
  1. Use Shamir’s \((k, n)\) threshold scheme to distribute shadows \( S_i \) to \( U_i \), for \( i = 1, 2, \ldots, n \)
  2. Choose a one way function \( h(\cdot) \) and a prime number \( p \) such that \( h() < p \).
  3. Compute

\[
t = \sum_{i=1}^{n} h(S_i) \cdot p^{2(i-1)} + \sum_{i=1}^{n-1} C \cdot p^{2i-1} \tag{3}
\]

Where \( C \) is a positive constant randomly chosen over \( GF(p) \).

4. Publish \( t \) and \( p \).

- **Cheater identification**
  Suppose any \( k \) participants want to pool their shadows to reconstruct the secret and let \( G \) be the set of these participants. The cheating detection and cheater identification is achieved by applying the following procedure.

1. All \( U_j \in G \) present their possessed shadows \( S_j \)s and compute

\[
t^* = \sum_{U_j \in G} h(S_j^*) \cdot p^{2(j-1)}
\]

2. For \( U_j \in G \), check the equation

\[
\left| \frac{t - t^*}{p^{2(j-1)}} \right| \mod p = 0 \ ?
\]

If the equation holds, \( U_j \) is honest; otherwise, \( U_j \) is a cheater. It is because that

\[
= h(S_j) - h(S_j^*) \mod p
= 0 \quad \text{if and only if} \quad h(S_j) = h(S_j^*)
\]

In our secret sharing implementation, the cheater detection and cheater identification scheme will be used as a precaution for resisting the deleted user’s and dishonest participant’s login.

**3 The proposed system overview**

The proposed system employs DES encryption, shared-secret and smart card technology to control the unlocking of remote coffer doors. The overall system diagram is shown as Fig. 1. The Control Center controls the Remote Terminal Units (RTU) via the internet. That is cheaper and has simpler communicating connection configuration for the Control Center, compared with the leased lines.
Components of RTU are layout in Fig.2. The main component of RTU is Personal Computer (PC_{RTU}) which communicates the microchip (ATmel AVR AT90S2313) with RS-232 and the Control Center with internet. Internal Card Reader and External Card Reader provide the interfaces for smart cards to communicate with the PC_{RTU}. Signal level is different between microchip and RS-232, a signal level converter will be included. As shown in Fig.3, the IC MAX232 with +5V single power supply is used to implement the signal conversion.

![Figure 2. Remote Terminal Unit](image)

![Figure 3. Signal conversion between RS-232 and TTL](image)
Every authenticated member has his own smart card. During entry request, the members insert their smart cards to the External Card Reader and key in their passwords via keypad. The PC_{RTU} authenticates the smart cards and computes the secret S. If the secret is correct, microchip unlocks the Door Access Unit under the instructions of PC_{RTU}. After unlocking the door a few predefined minutes, the door will close automatically.

The door status will be detected with an infrared detector, which includes an infrared emitter and an infrared receiver. The infrared emitter employs an oscillator of some kilo-Hz of frequency to excite the driver circuit and infrared LED, as shown in Fig.4. The infrared receiver is composed of photo-diode, amplifiers, waveform shaping circuit, shown as Fig.5. The received signal is amplified by OPA1 and shaped by OPA2 as an input to the microchip. If the signal detected by microchip AVR AT90S2313 via PB1 has square waveform with fixed period indicates the door open status, otherwise indicates the closed status when the signal without square waveform or with square waveform but its period beyond some fixed range. That the door status, the door open time, and the participants who access the door will be transmitted to Control Center via the internet and be recorded in the Control Center data base.

4 Implementation

4.1. Set-up

The set-up procedures are performed for each RTU as followings.

1. Control center chooses random secret number S for each RTU and \( a_1, a_2, \ldots, a_{k-1} \in \mathbb{Z}_p \), which corresponding to the coefficients of the polynomial of equation (1).

2. Control Center generates random \( X_1, X_2, \ldots, X_n \in \mathbb{Z}_p \) and computes the set share \( \{(X_i, S_i) \mid 1 \leq i \leq n \} \).
for each RTU.
3. Control Center selects a prime number \( p \) and 64 bits DES keys \( K_{RTU} \), which is hold by each RTU, and computes the \( t \) as equation (3).
4. Each \( PC_{RTU} \) possesses its own parameters \{ DES(S, \( K_{RTU} \), t, \( p \) \}. Where \( DES(m, k) \) is the DES encryption of \( m \) with the key \( k \). Control Center also possesses the key of each RTU ( \( K_{RTU} \) ) and its secret \( S \).
5. Control Center personalizes the smart cards with the followings:
\[
\{ \text{CID}_i, \text{ID}_i, \text{DES}(X_i \| S_i, K_{RTU}) \}
\]
\[
b_i = (\text{CID}_i)^{K_{RTU}} \pmod{p},
\]
\[
B_i = b_i^{PW_i} \pmod{p}
\]
Where the symbol, \( \| \), indicates concatenation, \( \text{CID}_i \) is the identifier of smart card and \( \text{ID}_i \) is the identifier of user \( U_i \).

### 4.2. Local Login

When a user wants to login the local RTU to access the door of coffer, he must pass the authentication procedure. The procedures are described as followings.

**Local Login Phase**

1. The user inserts his smart card to the exterior card reader and keys in his password \( PW_i \).
2. The smart card generates a random number \( r_i \) and calculates the following two integers.
\[
Y_i = (ID_i \cdot (b_i^{PW_i})^{\ell_i})^T \pmod{p} \quad (6)
\]
\[
Z_i = (B_i^\ell)^T \pmod{p} \quad (7)
\]
Where \( T \) is the current date and time of the exterior card reader and is used as a timestamp.
3. Send a message \( M = \{ \text{ID}_i, \text{CID}_i, b_i, T, S_i, Y_i, Z_i \} \) to RTU, where \( S_i \) is the piece of secret of \( U_i \).

**Verification Phase**

After receiving the message \( M \), the \( PC_{RTU} \) will perform the following steps:
1. Check the formats of \( \text{ID}_i \) and \( \text{CID}_i \). If they are illegitimate, the RTU will ignore the local login of \( U_i \).
2. Compare \( Y_i^T \) and \( (\text{ID}_iZ_i) \). If they are equal, then the RTU accepts the request of local login, otherwise rejects the request. This is because that
\[
Y_i^T = (ID_i \cdot (b_i^{PW_i})^{\ell_i})^T \pmod{p} = ID_i \cdot b_i^{PW_i} \pmod{p} \quad (8)
\]
and
\[
ID_i \cdot Z_i = ID_i \cdot (B_i^\ell)^T \pmod{p} = ID_i \cdot b_i^{PW_i} \pmod{p} \quad (9)
\]
If the equation \( Y_i^T = ID_iZ_i \) holds, it indicates that the password \( PW_i \) is equal to \( PW_o \). Then the RTU believes that the message \( M \) is really sent by \( U_o \), and allows \( U_i \) to login.
3. After \( k \) or more member pass the local login phase, the \( PC_{RTU} \) use the Lagrange Polynomial Interpolation to reconstruct the \( S^r \). If \( S^r \) is correct, the \( PC_{RTU} \) will transmit an open signal and a number to the microchip. The open signal will unlock the door of coffer and the number will inform the microchip how many members will login. If the \( S^r \) is incorrect, \( PC_{RTU} \) will compute the parameter \( t \) of equation (4), detect the cheater and record the \( ID_i \)s of the participant.
4. The microchip uses sensors to count the login member. When the counting number is equal to the data just before the \( PC_{RTU} \) transmitted, the door of the coffer will lock, and the number of login member will be sent to the \( PC_{RTU} \).

### 4.3. Management of access record

The access data including which user who login, when the access time is, what the status of RTU is and when the coffer open/close will all be saved in \( PC_{RTU} \) for future use. When the door of coffer was accessed to open, the \( PC_{RTU} \) will save the access records with the form:
\[
\text{DES( ID }_i \| T_{ent} \| \text{ENT, } K_{RTU})
\]
Where \( T_{ent} \) is the time of occurrence of \( U_i \) access to the \( PC_{RTU} \) for entry and \( \text{ENT} \) indicates the entry access. After \( k \) or more members pass the local login phase and the correct reconstruction of \( S \), the alternative status and the time will also be saved with the form:
\[
\text{DES( } T_{oa} \| \text{Status, } K_{RTU} \oplus S)
\]
Where \( T_{oa} \) is the time of coffer’s opening, Status indicates the status of the coffer on/off and the symbol, \( \oplus \), indicates Exclusive-OR operation.

Similarly, the exit records will save the \( U_i \)’s exit data with the following form:
DES (ID_i || T_{exit} || EXIT, K_{RTU} )
Where T_{exit} is the access time for exit and EXIT indicates the exit access.

The status of coffer on/off is periodically saved and transmitted to the Control Center with the form:
{ RTU_i, DES(ID_i || T || Status, K_{RTU} ) }.
The PC_{RTU} also feedbacks the entry record to the Control Center with the form: { RTU_i, DES(ID_i || T_{ent} || ENT, K_{RTU} ) } and the exit record with the form: { RTU_i, DES(ID_i || T_{exit} || EXIT, K_{RTU} ) }.

5 Discussions and conclusion

The strength of security of our scheme is based on DES and the discrete logarithm problem. Since B_i and PW_i are used to login the RTU, they must be tightly protected. The parameter of B_i is stored in the tamper-proof smart card and cannot be retrieved directly. Even B_i were compromised, PW_i remains secure because of the discrete logarithm problem. It is also difficult for an intruder to obtain the system generated random number r_i from the equations

\[ Y_i = ID_i \cdot (b_i^{PW_i^r})^\gamma \pmod{p} \]

and

\[ Z_i = (B_i^{\gamma^r})^\gamma \pmod{p}. \]

The scheme allows users to change their passwords freely. When a user wants to change his password, he submits his smart card and chooses a new password PW_i' to the PC_{RTU} via card reader. The PC_{RTU} will perform the new B_i' as B_i' = b_i^{PW_i'^r} \pmod{p} and write the new B_i' into U_i's smart card. After the replacement of B_i in the smart card of U_i, U_i can use the new PW_i' to login. The bit length of PW_i is chosen freely by user U_i, it need not be 128, 256 bits or other bit length, so the password is easy to memorize for the user.

In the case of losing smart card, user U_i can use his ID_i to re-register a new card CID_i'. After Control Center checks U_i's basic background data, the lost smart card CID_i will be invalid. The illegal holder of the lost smart card can not login because he have no password of U_i.

Addition of new user is easier. Its procedure just likes the set-up process. Deletion of user U_i is troublesome, if the smart card of the removed user is not recovered. It requires an update of all smart cards in the dedicated RTU. The update process, that includes the changes of secret S, t and some other operations, will be performed friendly. It needs only to insert his smart card and key in his corresponding password for the authorized users. Although the deleted user is able to login but that to open the door of the coffer in the threshold scheme will be in vain, because he will finally be detected by the cheating detection and cheater identification scheme.

References