End-to-End Security Protocol for Mobile Communications with End-User Identification/Authentication*

Chin-Chen Chang† Kuo-Lun Chen† Min-Shiang Hwang‡

Department of Computer Science and Information Engineering†
National Chung Cheng University
Chiayi, Taiwan 62107, R.O.C.

Department of Management Information System‡
National Chung Hsing University
250 Kuo Kuang Road,
402 Taichung, Taiwan, R.O.C.
Email: mshwang@nchu.edu.tw

January 16, 2004

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-005.

‡Responsible for correspondence: Prof. Min-Shiang Hwang

End-to-End Security Protocol for Mobile Communications with End-User Identification/Authentication

Abstract

As great progress has been made in mobile communications, many related researches on this topic have been proposed. In most of the proposed protocols so far, it has been assumed that the person using the mobile station is the registrar of the SIM card; as a matter of, the previous protocols for authentication and session key distribution are built upon this assumption. This way, the mobile user can only verify the identity of the owner of the SIM card. This means that the mobile user can only know that who registers the SIM card with which he communicates. Note that the human voice can be forged. To make sure that the speaker at the other end is the right owner of the SIM card, concept of the password is involved to construct the end-to-end security authentication protocol. In the proposed protocol, each mobile user can choose a password. When two mobile users want to communicate with each other, either user can request to perform a end-user identification process. Only when both of the end users input the correct passwords can the correct common session key be established.

Keywords: Authentication, Cryptography, Mobile communication, Session key.

1 Introduction

With wireless communications travel farther and wider and faster, the researches on the topics concerned also get hotter. To assure that every user is charged reasonably and that any conspirator cannot misuse the resources, the authentication of the identity of the users must be ensured [7, 6]. Due to the special property of wireless communications that any piece of message is transmitted through the open air it is an important issue to prevent transmitted messages from being intercepted. Encryption is the best option before the message is transmitted. There are two major cryptosystems ready for use: the symmetric cryptosystem and the public key cryptosystem. The symmetric cryptosystem is easily implemented with quite a low computation complexity, but the public key system provides more versatile security services.

In one of the most popular mobile communication systems, GSM, to simplify the computation, both the authentication and the data encryption employed symmetric cryptosystems. However, the improvement of hardware techniques has by now also made it possible to use the public key system in the authentication process. In other words, both user authentication and session-key establishment can be based on the public key cryptosystems. The communication is based on the symmetric cryptosystem with the session key established.

In the previous researches, the focus has been on the secure communication between the mobile user and the base station. Because the communication is done through the open air, it is very easy for an eavesdropper to capture a message [11, 15, 16]. However, even though the security between the mobile user and the base station is assured, the communication between two base stations is insecure. For example, if mobile station A (MS_A) is visiting base station A (BS_A) and mobile station B (MS_B) is visiting base station B (BS_B). The message sent from MS_A to MS_B will be encrypted by MS_A and transmitted it to BS_A. After decrypting the message, BS_A sends the unmodified message to BS_B. Finally, the message will be encrypted again by BS_B and decrypted by MS_B. The message is not under protection between the two base stations. Since that, any malicious user can intercept the unmodified messages between the two base stations. To guarantee the end-to-end security, the two base stations should not know the unmodified messages and the messages should be encrypted by a session key.

To achieve end-to-end secure communications, some protocols have been proposed [13]. The concept for achieving secure end-to-end communications is to establish a session key between two mobile users for communication encryption. Just as all the other protocols, mutual authentication is also needed here.

In the protocols proposed so far, all information for communication and authentication is stored in a Subscriber Identity Module (SIM) card or a smart card. Like the secret and public keys for a mobile user, the public key of the Certification Authority (CA), the certificate signed by CA for the mobile user and the identity (ID) of the mobile user, etc., everything is stored in the card. Therefore, it is assumed that the person using a certain SIM card is the same person who registers the SIM card or someone authorized by the registrar.

Now, here comes the problem. If the SIM card is stolen, the conspirator may impersonate the registrar to communicate with anyone. Note that the voice can be forged. It can get really serious when the registrar is someone who owns great power like the President of a country, the President of a company or a commander of a military base. By stealing the SIM card, the conspirator can impersonate the registrar to communicate with someone and make the decisions at will. Therefore, it does not seem to be sufficient to authenticate the identity of the user at the other end using the information stored in the SIM card or a smart card.

To make sure that other persons cannot use the SIM card, the easiest way is to set a password stored in the smart card. Before using the mobile phone, the user is required to input a password. When the entered password is correctly provided, the user can use the phone. In GSM system, PIN (Personal Identity Number) can achieve this objective and is required at default. Furthermore, the user can optionally decide the use of a password request. The user at this end cannot force the user at the other end to prove his/her identity by employing the password function.

For effective speaker identity authentication, a new protocol is proposed. By adopting a password into the protocol, any end user can request both of the end users to process a double mutual authentication. When the communication is not so important, the protocol lets go like others do. Each end user can verify the identity at the other end with the certificate signed by CA. However, when any end-user feels that the identity of the other speaker needs to be verified furthermore, she/he can request a end-user identification. During the end-user identification process, both of the users are requested to input their passwords. When the passwords of both end users are correct, a new session key can be established for communication. When one of the passwords of the end users is wrong, a true session key will not be established. The password-based authentication protocol provides the protection against fraudulent use of the mobile set. Here, we do not focus on non-repudiation. Non-repudiation can guarantee that mobile users cannot deny using resources provided by server. Many researchers have been studied this feature. One-way hash function can be applied to achieve the non-repudiation [8, 9]. We also can apply it to achieve the non-repudiation in our study.

By involving the password in the protocol, this further identity authentication can be achieved. The certificate stored in the SIM card can be used for the first authentication of the users' identities. The password request can be regarded as the double authentication process.

2 Review Of The Previous Protocols

In this section, a previously proposed end-to-end communication protocol will be reviewed. Park proposed the protocol in 1997, and more details can be found in [13]. The protocol is a certificate-based authentication and session key exchange protocol. The session key exchange protocol is based on the Diffie-Hellman key exchange protocol [3]. By involving two random numbers, the session key for each communication between two users is unique. The protocol is described as follows.

Let N and g be known to all. The secret key of the mobile user is X_{MS} and the public key is $Y_{MS} = g^{-X_{MS}} \bmod N$. In this same way, both secret and public keys of the base station are X_{BS} and $Y_{BS} = g^{-X_{BS}} \bmod N$, respectively. Both secret and public keys of the certification authority are S_{CA} and P_{CA} , respectively. Let R_{MS} be the random number chosen by the mobile user and R_{BS} the one chosen by the base station. The certificates of the mobile station and the base station are as follows.

$$\begin{aligned} Cert_{MS} &= (ID_{MS}, Y_{MS}, date_{MS}, [h(ID_{MS}, Y_{MS}, date_{MS})]_{S_{CA}}), \\ Cert_{BS} &= (ID_{BS}, Y_{BS}, date_{BS}, [h(ID_{BS}, Y_{BS}, date_{BS})]_{S_{CA}}). \end{aligned}$$

The certificate can be verified using the public key of the CA.

In the protocols described in this paper, the statement in each step means the transmission direction and transmitted message between the MS and the BS. The arrow means the direction of message transmission and the data after the colon is the transmitted message. For example, the statement, ($MS \longleftarrow BS$: $g^{R_{BS}+X_{BS}}, Cert_{BS}$), means that the messages $g^{R_{BS}+X_{BS}}$ and $Cert_{BS}$ are transmitted from the BS to the MS.

Protocol 1:

1. $MS \longleftarrow BS$: $g^{R_{BS}+X_{BS}}, Cert_{BS}$

   After receiving the message, the MS computes $k_s = (Y_{BS} \cdot g^{R_{BS}+X_{BS}})^{R_{MS}} \bmod N = g^{R_{BS}R_{MS}} \bmod N$, where the public key of the BS can be obtained from $Cert_{BS}$. The MS can also verify the $Cert_{BS}$ using the public key of CA, Y_{CA}.

2. $MS \longrightarrow BS$: $R_{MS} + X_{MS}, Cert_{MS}, f(k_s, [ID_{MS}, ID_{BS}])$

   The BS then computes $k_s = (Y_{MS} \cdot g^{R_{MS}+X_{MS}})^{R_{BS}} \bmod N = g^{R_{MS}R_{BS}} \bmod N$ and $f(k_s, [ID_{BS}, ID_{MS}])$. The BS can also verify the certificate of the MS.

3. $MS \longleftarrow BS$: $f(k_s, [ID_{BS}, ID_{MS})$

In the protocol above, the MS and BS exchange their certificates and the parameters to establish the session key $k_s = g^{R_{MS}R_{BS}} \bmod N$. The function $f(k_s, [ID_{MS}, ID_{BS}])$ means to encrypt the message $[ID_{MS}, ID_{BS}]$ with the key k_s. The identities are also encrypted and exchanged for authentication and verification that a common session key is shared with one another. With the common session key, k_s, the MS and the BS can encrypt the messages exchanged with each other over the insecure channel.

When the base station is not in the home system range of the mobile station, the mobile station is thus served by another roaming network. We assume that there is a CA in each network system and single trusted certificate authority issues each network's certificate. Each home system server maintains a database of the public keys of CAs in other systems with which a roaming agreement has been set up. The identity of the home register network of the mobile station can be stored within the identity of a mobile station in the certificate. In this way, according to the ID_{MS} stored in the certificate, the identity of the home network of the mobile station can also be known. With this network identity, by searching the database in the system, one can find the public key of the corresponding network system.

Based on Protocol 1, the end-to-end security protocol can be set up. The protocol proposed by Park [13] is shown as follows. Let the two mobile stations be MS_A and MS_B. MS_A is served in a base station BS_A, and MS_B in BS_B.

Protocol 2:

1. $AuthKey_A$: In this step, the certificate of MS_A will be verified by BS_A. A mutual authentication is performed successfully using Protocol 1 between MS_A and BS_A. At the same time, BS_A can also compute the key distribution information $DH_A = g^{R_{MS_A}+X_{MS_A}} \bmod N$ based on $R_{MS_A} + X_{MS_A}$ sent by MS_A.

2. $CallReq$: In this step, MS_A sends a call request to request a communication with MS_B. The certificate $Cert_{MS_A}$ and DH_A are transmitted from BS_A to BS_B.

3. Paging and $AuthKey_B$: In this step, the MS_B will be paged and the certificate of MS_B is also verified by BS_B. Moreover, the necessary information for the key distribution is also transmitted. After paging MS_B, a mutual authentication process is also performed between MS_B and BS_B using the Protocol 1. At the same time, the key distribution information $DH_B = g^{R_{MS_B}+X_{MS_B}} \bmod N$ can also be obtained by BS_B.

4. DH_1: In this step, the necessary information for key distribution will be transmitted from BS_B to MS_B. BS_B sends the certificate of MS_A, $Cert_{MS}$, and the information DH_A to MS_B. With the information, MS_B can compute the session key $k_s = (Y_{MS_A} \cdot g^{R_{MS_A}+X_{MS_A}})^{R_{MS_B}} \bmod N = g^{R_{MS_A}R_{MS_B}} \bmod N$ and $RES_B = f(k_s, [ID_{MS_B}, ID_{MS_A}])$.

5. DH_2: In this step, the necessary information for key distribution is transmitted from MS_B to BS_A. MS_B passes RES_B to BS_B. BS_B then sends RES_B, the certificate $Cert_{MS_B}$, and DH_B to BS_A. BS_A then sends them all to MS_A.

6. DH_3: In this step, MS_A can compute the common session key with the received information for key distribution. After computing the session key $k_s = (Y_{MS_B} \cdot g^{R_{MS_B}+X_{MS_B}})^{R_{MS_A}} \bmod N = g^{R_{MS_B}R_{MS_A}} \bmod N$, MS_A

verifies RES_B and then computes $RES_A = f(k_s, [ID_{MS_A}, ID_{MS_B}])$. RES_A is sent to MS_B through the network. MS_B can also verify RES_A.

According to Protocol 2, two mobile users can establish a common session key to encrypt and decrypt the messages exchanged with a symmetric cryptosystem. However, in the protocols described above, there exist some drawbacks. In Protocol 1, according to the second move between MS and BS, MS transmits $R_{MS} + X_{MS}$ to BS rather than $g^{R_{MS}+X_{MS}} \bmod N$. Although there is a random number in the message, it can still be viewed as to encrypt the secret key of MS by adding a random number into the secret. Actually, the channel between MS and BS is through the open air. This manner reduces the security level. An illegal user may obtain the secret key of MS by solving a linear equation rather than a discrete logarithm problem. Therefore, to transmit $g^{R_{MS}+X_{MS}} \bmod N$ rather than $R_{MS} + X_{MS}$ is a more secure way. If the power of computation of the mobile station is considered, the concept of Server-Aided Computation can be employed to solve the problem [10].

The other concept is that in this protocol, as in other protocols, the authentication process can only check the identity of the owner of the SIM card or the smart card. It means that a mobile user can only know for sure that the certificate of the other user with whom she/he communicates is valid. Hence, the mobile user can only check the identity stored in the certificate and know who the owner of the SIM card is. The mobile user can not make sure that the person she/he is talking is truly the owner of the SIM card. Because the voice can be forged, a conspirator may steal the SIM card or the whole handset with the SIM card and impersonate the owner of the SIM card to communicate with others. For example, a conspirator may steal the SIM card of the President of a country and call the commander of a military base. The voice can be forged of the President to ask the commander to launch missiles towards an enemy. In the previous protocols, the commander can only make sure that the SIM card on the other end is actually owned by the President. The commander can not check the actual identity of the speaker further.

To prevent this problem, a new protocol with end-user identification is proposed below. Based on Protocol 2, this new protocol can provide the mobile user with the ability to check the actual identity of the speaker. In other words, the protocol can help the mobile user make sure that the speaker is really the owner of the SIM card before the communication takes place. The end-user identification means that the mobile user not only can check if the certificate of the other user is valid but also check the identity of the speaker by requesting some information only known to the owner of the SIM card. With the information, a new session key can be established. Besides, when no mobile user feels like asking for the double authentication process, the protocol performs just like Protocol 2. This means that no redundant computation is needed for normal communication. The new protocol will be described in the next section.

3 Proposed Protocol

Similar to Park's protocol [13], there is a CA in each network. Let X_{MS} be the secret key of the mobile user and $Y_{MS} = g^{-X_{MS}} \bmod N$ is the public key. In the same way, Let X_{BS} and $Y_{BS} = g^{-X_{BS}} \bmod N$ be secret and public keys of the base station, respectively. Let S_{CA} and P_{CA} be the secret and public keys of the CA, respectively. When the mobile user wants to register her/his own SIM card for communication, the system will ask the user to choose a password (SPWD) for end-user identification. The password is long-term and does not change from session to session. The password will be requested when the end-user identification process is performed. The session password is not necessarily long; the length of the session password is decided as to make it easy the user to remember. Therefore, the certificates of the mobile station and the base station are shown as follows.

$$\begin{aligned} Cert_{MS} &= (ID_{MS}, Y_{MS}, Y'_{MS}, date_{MS}, [h(ID_{MS}, Y_{MS}, Y'_{MS}, date_{MS})]_{S_{CA}}), \\ Cert_{BS} &= (ID_{BS}, Y_{BS}, date_{BS}, [h(ID_{BS}, Y_{BS}, date_{BS})]_{S_{CA}}). \end{aligned}$$

There are some parameters to be further explained. Let $SPWD$ be the password chosen by the mobile user when she/he wants to get her/his own SIM card of the system. Let L be the $E(SPWD)$, where $E(\cdot)$ denotes an expansion function of $SPWD$ such that the length of L is equal to that of the secret key X_{MS}. Let X'_{MS} be the result of the bit-wise exclusive-OR of L and X_{MS}; that is, $X'_{MS} = L \oplus X_{MS}$. The result X'_{MS} can be viewed as a end-user identification secret key, and the corresponding public key will be the parameter in the certificate $Y'_{MS} = g^{-X'_{MS}} \bmod N$. Note that this X'_{MS} will not be stored in the SIM card or smart card. The value of X'_{MS} is obtained in real time. There is only one secret key needed to be stored in the SIM card. There are two public keys, Y_{MS} and Y'_{MS}, in the certificate. Y_{MS} is used for normal authentication process. Y'_{MS} is used for double authentication process.

The certificate can be verified with the public key of the CA. If the certificate is valid, the user can be convinced that the information stored in the certificate is true.

Based on the certificates above, another new protocol can be portrayed as follows:

Protocol 3:

1. $MS \longleftarrow BS$: $g^{R_{BS}+X_{BS}} \bmod N$, $Cert_{BS}$

   Here MS computes $k_s = (Y_{BS} \cdot g^{R_{BS}+X_{BS}})^{R_{MS}} \bmod N = g^{R_{BS}R_{MS}} \bmod N$, where the public key of BS can be obtained from $Cert_{BS}$. On the other hand, MS can also verify the $Cert_{BS}$ using the public key of CA, P_{CA}.

2. $MS \rightarrow BS$: $g^{R_{MS}+X_{MS}} \bmod N, Cert_{MS}, f(k_s, [ID_{MS}, ID_{BS}])$

BS computes $k_s = (Y_{MS} \cdot g^{R_{MS}+X_{MS}})^{R_{BS}} \bmod N = g^{R_{MS}R_{BS}} \bmod N$ and $f(k_s, [ID_{BS}, ID_{MS}])$. BS can also verify the certificate of the MS with the public key of the CA.

3. $MS \longleftarrow BS$: $f(k_s, [ID_{BS}, ID_{MS}])$

With Protocol 3, BS and MS can be mutually authenticated, and the session key k_s can also be established. In the second step, the message transmitted is $g^{R_{MS}+X_{MS}}$ rather than $R_{MS} + X_{MS}$ so as to ensure the security of the protocol. When one tries to obtain the secret key of the mobile station, to solve logarithm problem is needed.

When the mobile users wish to perform a end-user identification process, a modified protocol is needed to construct the whole end-to-end security protocol.

Protocol 4:

1. MS $\longleftarrow$ BS: $g^{R_{BS}+X_{BS}} \bmod N, Cert_{BS}$

   MS computes $k'_s = (Y_{BS} \cdot g^{R_{BS}+X_{BS}})^{R_{MS}} \bmod N = g^{R_{BS}R_{MS}} \bmod N$, where the public key of BS can be obtained from $Cert_{BS}$. MS can also verify $Cert_{BS}$ using the public key of CA, Y_{CS}. The mobile user is requested to input the password ($SPWD$) to perform the end-user identification process. With the $SPWD$, MS then computes $L = E(SPWD)$ and $X'_{MS} = L \oplus X_{MS}$, where the length in L is equal to that in X_{MS}.

2. $MS \longrightarrow BS$: $g^{R_{MS}+X'_{MS}} \bmod N, Cert_{MS}, f(k'_s, [ID_{MS}, ID_{BS}])$

   Once BS receives the signal that MS requests to perform the double authentication process, BS then computes $k'_s = (Y'_{MS} \cdot g^{R_{MS}+X'_{MS}})^{R_{BS}} \bmod N = g^{R_{MS}R_{BS}} \bmod N$ and $f(k'_s, [ID_{BS}, ID_{MS}])$. BS can also verify the certificate of MS with the public key of the certification authority.

3. $MS \longleftarrow BS$: $f(k'_s, [ID_{BS}, ID_{MS}])$

The difference between Protocols 3 and 4 is that, in Protocol 4, when BS receives the Double-Auth SIGNAL, it will choose the public key Y'_{MS} rather than Y_{MS}. When the password entered by the user is correct, the session key can be established correctly. The Double-Auth SIGNAL is a signal that can be sent by any end-user. If malicious user want to send this signal, the communication is blocked and the session key cannot be established correctly without knowing X'_{MS}. When an end-user wants to perform a double-authentication process, she/he can send a Double-Auth SIGNAL to announce the user in the other end and the base stations between she/he and the other end-user.

Based on Protocols 3 and 4, an end-to-end security protocol with end-user identification can be established. To illustrate the procedures of the protocol, let's have a look at the three performance conditions as follows. The first condition is that the communication between two mobile users is normal and double authentication is not necessary. In this condition, the protocol performs the same way as in Protocol 2. The second condition is that the messages are very important and the pager requests double authentication process. The third condition is that the receiver requests the end-user identification process. In the double authentication process, both of the end users are requested to input their passwords ($SPWD$) to establish the further session key. If one of the passwords is not correct, the session key will not be established. The protocol can be executed under these three conditions as described in the following.

3.1 Normal Communications

In this condition, the protocol performs just the same way as Protocol 2. The only difference is that Protocol 3 is used as a block to replace the function of Protocol 1. The step 1 of this protocol is different from the Protocol 2 shown as follows but others is the same.

1. $AuthKey_A$: A mutual authentication operation is performed successfully

using Protocol 1 between MS_A and BS_A. At the same time, BS_A can also receive the key distribution information $DH_A = g^{R_{MS_A}+X_{MS_A}} \bmod N$.

Then step 2 to step 6 of protocol 1 are followed and the session key k_s is generated to encrypt and decrypt messages exchanged between MS_A and MS_B.

3.2 End-User Identification Started By The Pager

In this condition, the pager asks the receiver to perform the end-user identification process.

1. $AuthKey_A$: After receiving their certificate, a mutual authentication is performed successfully using Protocol 4 between MS_A and BS_A. When a Double_Auth SIGNAL is received from MS_A to BS_A, BS_A can also receive the key distribution information $DH'_A = g^{R_{MS_A}+X'_{MS_A}} \bmod N$.

2. $CallReq$: MS_A requests a conversation with MS_B. The certificate, $Cert_{MS_A}$, DH'_A and a Double_Auth SIGNAL are transmitted from BS_A to BS_B.

3. Paging and $AuthKey_B$: After paging MS_B and receiving their certificate, a mutual authentication process is also performed between MS_B and BS_B using Protocol 4. At the same time, the key distribution information $DH'_B = g^{R_{MS_B}+X'_{MS_B}} \bmod N$ can also be obtained by BS_B.

4. DH_1: BS_B sends the certificate of MS_A, $Cert_{MS_A}$, a Double_Auth SIGNAL and the information DH'_A to MS_B. When MS_B receives the Double_Auth SIGNAL, with the information received, MS_B can compute the session key $k'_s = (Y'_{MS_A} \cdot g^{R_{MS_A}+X'_{MS_A}})^{R_{MS_B}} \bmod N = g^{R_{MS_A}R_{MS_B}} \bmod N$ and $RES_B = f(k'_s, [ID_{MS_B}, ID_{MS_A}])$.

5. DH_2: MS_B passes RES_B to BS_B. BS_B then sends RES_B, the certificate $Cert_{MS_B}$, and DH'_B to BS_A. BS_A then sends them all to MS_A.

6. DH_3: After computing the session key $k'_s = (Y'_{MS_B} \cdot g^{R_{MS_B}+X'_{MS_B}})^{R_{MS_A}} \bmod N = g^{R_{MS_B}R_{MS_A}} \bmod N$, MS_A verifies RES_B and then computes $RES_A = f(k'_s, [ID_{MS_A}, ID_{MS_B}])$. This RES_A is sent to MS_B through the network. MS_B can also verify RES_A.

In this way, the session key k'_s can be established and used to exchange messages.

3.3 End-User Identification Started By The Receiver

To make sure of the identity of the speaker, the person being paged should also have the right to decide whether or not to perform the end-user identification process when the caller does not choose to. For example, when MS_B is paged by MS_A, MS_B may want to make sure if the speaker's identity is indeed the same identity stored in $Cert_{MS_A}$. In such a case, the protocol is performed as follows.

1. $AuthKey_A$: A mutual authentication operation is performed successfully using Protocol 3 between MS_A and BS_A. At the same time, BS_A can also receive the key distribution information $DH_A = g^{R_{MS_A}+X_{MS_A}} \bmod N$.

2. $CallReq$: MS_A requests a conversation with MS_B. The certificate $Cert_{MS_A}$ and DH_A are transmitted from BS_A to BS_B.

3. Paging and $AuthKey_B$: After paging MS_B, a mutual authentication process is also performed between MS_B and BS_B using Protocol 4. Once BS_B receives the Double_Auth SIGNAL sent by MS_B, the key distribution information $DH'_B = g^{R_{MS_B}+X'_{MS_B}} \bmod N$ can also be obtained by BS_B.

4. $DoubleAuthRequest_1$: In this step, BS_B passes the request from MS_B to BS_A to perform a end-user identification process. BS_B sends the certifi-

cate $Cert_{MS_B}$, the key exchange information, DH'_B and a Double_Auth SIGNAL to BS_A.

5. *DoubleAuthRequest*$_2$: In this step, BS_A notifies MS_A that MS_B asks to perform a end-user identification process. Once BS_A receives the Double_Auth SIGNAL, BS_A sends the certificate $Cert_{MS_B}$, DH'_B and a Double_Auth SIGNAL to MS_A. After the receiving of the Double_Auth SIGNAL, Protocol 4 will be performed between MS_A and BS_A. The user of MS_A is requested to enter the password, and then the key exchange information will be obtained, $DH'_A = g^{R_{MS_A}+X'_{MS_A}}$.

6. DH_1: With the information received from BS_A, MS_A can compute the session key $k'_s = (Y'_{MS_B} \cdot g^{R_{MS_B}+X'_{MS_B}})^{R_{MS_A}} \bmod N = g^{R_{MS_A}R_{MS_B}} \bmod N$ and $RES_A = f(k'_s, [ID_{MS_A}, ID_{MS_B}])$.

7. DH_2: MS_A passes the RES_A and DH'_A to BS_B. BS_B then sends RES_A and DH'_A to MS_B.

8. DH_3: After computing the session key $k'_s = (Y'_{MS_A} \cdot g^{R_{MS_A}+X'_{MS_A}})^{R_{MS_B}}$ mod $N = g^{R_{MS_B}R_{MS_A}} \bmod N$, MS_B verifies RES_A, computes $RES_B = f(k'_s,$ $[ID_{MS_B}, ID_{MS_A}])$, and then sends RES_B to MS_A through the network. MS_A can also verify RES_B.

In the third step, Paging and $AuthKey_B$, if MS_B requests to perform a end-user identification process, then DH_A will be erased by BS_A. After Step 3, the process is similar to the execution in Section 3.2. The protocol can be performed as the execution in Section 3.2 by just viewing the MS_B as the caller and the MS_A as the receiver.

After introducing the protocol execution processes in the three conditions, an end-to-end security protocol has been described. Actually, the double authentication process can be invoked by one of the end users. When the process is invoked, Protocol 4 will be performed at both of the communication ends.

A new session key can be established after both of the end users enter their correct session passwords.

4 Discussions and Security Analysis

Similar to the Park's protocol, once the certificate for a mobile station has been established as not valid; for example, the date in the certificate is not valid, then the new certificate can be transmitted to the mobile station through the network without affecting the security of the protocol. Because no secret value in the certificate is exposed unwantedly, the protocol is secure.

To make sure that the proposed scheme is secure and can satisfy the required properties, the security under some situations will be examined briefly.

1. The certificate of the mobile stations and the base stations can not be forged. The certificate of each participant in the system includes a signature signed by CA. Without the secret key of CA, the certificate can not be forged. If one tries to obtain the secret key of CA from the public key of CA, she/he needs to solve the discrete logarithm problem.

2. With the knowledge of the public key of the mobile station or the base station, that is Y_{MS} or Y_{BS}, the secret key X_{MS} or X_{BS} can only be obtained by solving the discrete logarithm problem. Even when an eavesdropper gets the information for a key exchange like DH_A, before the secret itself can be obtained there is still a discrete logarithm problem to be solved.

3. With the knowledge of the information for key exchange of both end users such as $DH_A = g^{R_{MS_A}+X_{MS_A}} \bmod N$ and $DH_B = g^{R_{MS_B}+X_{MS_B}} \bmod N$, the conspirator can compute the values of $g^{R_{MS_A}}$ and $g^{R_{MS_B}}$ using the public keys of MS_A and MS_B, respectively. The session key $g^{R_{MS_A}R_{MS_B}}$ still can not be obtained without knowing the values of R_{MS_A} or R_{MS_B}.

Unless the discrete logarithm problem is solved, the secret values are only known to their owners, MS_A and MS_B. It can defend against man in the middle attack. No one can forge DH_A and DH_B and he/she can only know the values of $g^{R_{MS_A}}$ and $g^{R_{MS_B}}$. Therefore, the middle man cannot attack our protocols.

4. According to the protocol described above, the session key can be obtained using the equation $k'_s = (Y'_{MS_A} \cdot g^{R_{MS_A}+X'_{MS_A}})^{R_{MS_B}} \bmod N = (Y'_{MS_B} \cdot g^{R_{MS_B}+X'_{MS_B}})^{R_{MS_A}} \bmod N$. If the session password of MS_A is not correct, the correct X'_{MS_A} will not be obtained. It means that when MS_B tries to compute the session key with the corresponding public key of MS_A, Y'_{MS_A}, the correct session key $k'_X = g^{R_{MS_A}R_{MS_B}} \bmod N$ will not be obtained. If the X'_{MS_A} provided is not correct, then $Y'_{MS_A} \cdot g^{X'_{MS_A}} \neq 1 \bmod N$. In the same situation, if MS_B does not enter the correct password, the correct X'_{MS_B} will not be obtained. When MS_A tries to compute the session key using the corresponding public key Y'_{MS_B}, the correct session key will not be obtained. Furthermore, the owner of the SIM card only knows the session password and the password is requested to be entered in real time. Though the SIM card is stolen, no one can compute the correct X'_{MS_B} without knowing the session password. Therefore, if the session key can be established successfully, then the user can be convinced that the one whom she/he is talking is the one with the identity stored in the certificate.

   The value of X'_{MS} is computed according to the password entered by the mobile user in real time as well as the secret key X_{MS} stored in the SIM card. When the conspirator wants to impersonate the mobile user, for example, MS_A, the conspirator must steal the SIM card of MS_A and force MS_A to expose the password and then forge the voice of MS_A. Because the password is supposed to be known only to the mobile user, it is impossible for a conspirator to impersonate the mobile user without being detected by the mobile user.

5. The protocols can against the replay attack. If an attacker wants to replay messages of MS, he/she first intercepts the messages $\{g^{R_{MS}+X_{MS}}$, $Cert_{MS}, f(k_s, [ID_{MS}, ID_{BS}])\}$. In next session, the attacker can replay these messages to BS. Although he/she can be authenticated by BS, the session key is not same. Once the BS cannot decrypt $f(k_s, [ID_{MS}, ID_{BS}])$, the BS can request MS to restart protocols. Furthermore, we can add time-stamp against the replay attack.

5 Conclusions

In the previously proposed protocols, the speaker is always assumed to be the one who owns the SIM card. Under such assumption, those protocols have provided only the means to verify the identity of the owner of the SIM card. The identity of the speaker can not be verified, especially when the voice can be forged. The conspirator may easily impersonate some mobile user by stealing the SIM card and forge the voice. In this paper, a new end-to-end security protocol with end-user identification is proposed. By involving the password into the protocol, any end user can request to perform a end-user identification process. According to our protocol, when one of the end users does not enter the correct password, the correct common session key will not be established successfully. In this way, the user can verify the identity of the one who is communicating with her/him. If the session key is established successfully, both of the end users can be convinced that the one at the other end is actually the right person with the identity stored in the certificate.

A brief discussion detailed how to make sure that the protocol is secure enough and satisfies the required properties.

Acknowledgements

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC90-2213-E-324-005.

References

[1] G. B. Agnew, B. C. Mullin, and S.A. Vanstone, "Improved digital signature scheme based on discrete exponentiation," *Electronics Letters*, vol. 26, no. 14, pp. 1024–1025, 1990.

[2] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," *IEEE Journal on Selected Areas in Communications*, vol. 11, pp. 821–829, Aug. 1993.

[3] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[4] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469–472, July 1985.

[5] Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *to appear in IEEE Transactions on Knowledge and Data Engineering.*

[6] Min-Shiang Hwang and C. H. Lee, "Authenticated key-exchange in mobile radio network," *European Transactions on Telecommunications*, vol. 8, no. 3, pp. 265–269, 1997.

[7] Min-Shiang Hwang and W. P. Yang, “Conference key distribution protocols for digital mobile communication systems,” *IEEE Journal on Selected Areas in Communications*, vol. 13, pp. 416–420, Feb. 1995.

[8] Min-Shiang Hwang, Cheng-Chi Lee, and Yuan-Liang Tang, “An Authentication Scheme with Subscriber Anonymity in Personal Communication System,” *International Conference Advance Communication Technology 2001 (ICACT2001), Korea*, pp. 33–37, 2001.

[9] H. Y. Lin and L. Harn, “Authentication protocols with nonrepudiation services in personal communication systems,” *IEEE Communications Letters*, vol. 3, pp. 236–238, Aug. 1999.

[10] Tsutomu Matsumoto, Koki Kato, and Hideki Imai, “Speeding up secret computations with insecure auxiliary devices,” in *Advances in Cryptology, CRYPTO'88*, pp. 497–506, Lecture Notes in Computer Science, Vol. 403, Aug. 1988.

[11] A. Mehrotra and L. S. Golding, “Mobility and security management in the GSM system and some proposed future improvements,” *Proceedings of the IEEE*, vol. 86, no. 7, pp. 1480–1497, 1998.

[12] National Institute of Satndards and Technology (NIST). “Digital signature standard (DSS),”. Tech. Rep. FIPS PUB XX, NISS, US Department Commerce, 1993.

[13] C. S. Park, “On certificate-based security protocols for wireless mobile communication systems,” *IEEE Network*, vol. 11, no. 5, pp. 50–55, 1997.

[14] Makoto Tatebayashi, Natsume Matsuzaki, and Jr. David B. Newman, “Key distribution protocol for digital mobile communication systems,” in *Advances in Cryptology, Proceedings of Crypto'89*, pp. 324–334, 1989.

[15] X. Yi, E. Okamoto, and K.Y. Lam, "An optimized protocol for mobile network authentication and security," *ACM Mobile Computing and Communications Review*, vol. 2, no. 3, pp. 37–39, 1998.

[16] Y. Zheng, "An authentication and security protocol for mobile computing," *Mobile Communication - Technology, Tools, Applications, Authentication and Security (Proceedings of IFIP World Conference on Mobile Communications), Edited by J. L.Encarnacao and J. M.Rabaey,Chapman and Hall,Canberra, Australia.*, pp. 249–257, Sep. 1996.

BIOGRAPHY

Chin-Chen Chang was born in Taichung, Taiwan, the Republic of China, on November 12, 1954. He received his B.S. degree in Applied Mathematics in 1977 and his M.S. degree in Computer and Decision Sciences in 1979 from National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.d. in Computer Engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. From 1983 to 1989, he was among the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. Since August 1989, he has worked as a professor of the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Dr. Chang is a Fellow of IEEE and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China. His research interests include computer cryptography, data engineering, and image compression.

Kuo-Lun Chen was born in Changhua, Taiwan, Republic of China, on December 26, 1974. He received the M.S. degree in Computer Science and Information Engineering in 2001 from National Chung Cheng University, Chiayi, Taiwan. His research interests include Mobile Communications, Cryptography, Information Security, and Network Security.

Min-Shiang Hwang was born on August 27, 1960 in Tainan, Taiwan, Republic of China (ROC.). He received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, ROC, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic

Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He obtained the 1997, 1998, 1999, 2000, and 2001 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published 90 articles on the above research fields in international journals.