行政院國家科學委員會補助專題研究計畫成果報告

行動通訊系統中的安全身份驗證協定

A Secure Authentication Protocol in Mobile Communication System

計畫類別：∨個別型計畫　　□整合型計畫
計畫編號：NSC　89-2213-E-009-004
執行期間：88 年 8 月 1 日至 89 年 7 月 31 日

計畫主持人：謝續平教授

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

執行單位：國立交通大學資訊工程學系

中　華　民　國　89 年　10 月　1 日

行政院國家科學委員會專題研究計畫成果報告

行動通訊系統中的安全身份驗證協定

A Secure Authentication Protocol in Mobile Communication System

計畫編號：NSC 89-2213-E-009-004
執行期限：88 年 8 月 1 日至 89 年 7 月 31 日

主持人：謝續平教授　國立交通大學資訊工程學系

中文摘要

由於新世代的行動通訊網路的全球性與可移動性，使得其應用層面愈趨廣泛，推及商業、娛樂、以及個人助理等服務，而安全性即成為影響行動服務品質的重要因素之一。在本計劃中，我們分別考慮三種重要的安全議題。首先，探討於不同的環境限制下，建構安全的通訊管道：在跨網域、線上及時漫遊的環境下，我們提出了”鏈式身分驗證”；而在離線漫遊的環境下，則針對信用電話的服務功能提出一個 IC 卡的付費機制；針對“弱連結”環境，我們提出一個安全的訊息交換協定，使每個被傳送的訊息都具有身份驗證、保證資料隱密與完整的功能。最後，針對具重複使用性服務內容（如以行動碼組成的軟體）的非法盜版問題，特別設計了一個軟體的授權與保護模式，來避免如行動碼之類的服務內容被使用者盜拷並散佈出去。

關鍵詞：行動計算，安全性，身分驗證，軟體授權，軟體盜用，行動碼，統計式資料庫。

Abstract

Due to the mobility of new generation mobile computing networks, more and more applications are introduced for commerce, entertainment, personal assistant services, and so on. Security is the one of critical factors affecting the quality of mobile services. In this project, we consider three critical security issues and propose the solutions. First, we discuss the security problems of establishing communication channels under different mobile environment restrictions. For the inter-domain on-line roaming environment, we propose a *chain authentication scheme*. For the off-line roaming environment, we propose an IC card-based billing scheme for credit card phone services. We also propose a secure message exchange protocol for the “weak connection” environment. In this protocol, every message itself provides authentication, confidentiality, and integrity of message data. Finally, the piracy problem of some reusable service contents, such as mobile codes is considered. We herein design a software authorization and protection model to protect valuable service contents (e.g. mobile codes) from being copied or distributed by unauthorized users.

Keywords: Mobile computing, security, authentication, software authorization, software piracy, mobile code, and statistical database.

1. Authenticating Mobile Users in Inter-domain On-line Roaming Networks

The inter-domain on-line roaming environment is the trend of network infrastructures of future mobile computing services. And authentication for communication entities is the base of security functions at the access phase of mobile services. However, the conventional schemes either do not authenticate all communication entities or suffer from heavy overhead on networks. Therefore, these schemes are impractical for global mobile networks. The scheme proposed herein authenticates all communication entities and guarantees the confidentiality of all data transmissions. In addition, our scheme is suitable for multiple service providers within a geographical area, and reduce the connection overhead and satisfy the security requirements in an enormous and heterogeneous network.

1.1 Chain Authentication

The *chain* implies that all domains, visited by MS, constitute a roaming path, which is a virtual trusted chain. And the chain originates HLR and ends at the VLR_n that he is currently visiting. *A* trusts *B* only if *A* can successfully authenticate *B* by a pre-defined protocol. Therefore, each entity in the trusted chain must authenticate the neighbors and trust them. Figure 1. depicts the authentication history for MS. When MS lies in the domain of HLR, the authentication of both MS and HLR is trivial because HLR knows its subscriber MS. If MS roams to VLR_1, some authentication procedure must be applied to establish mutual trust. Since VLR_1 is strange to MS before registration of MS, VLR_1 must query HLR to authenticate MS. Prior to authentication, however, HLR and VLR_1 should authenticate each other. Upon establishing authentication, HLR can authenticate MS for VLR_1, and relay MS's security related information to VLR_1. VLR_1 and MS must then authenticate each other. Afterwards, if they can trust each other, VLR_1 can be included in the MS's trusted chain. These steps are repeatedly executed as MS travels until MS roams to VLR_i, the trusted chain being from HLR to VLR_{i-1}; i.e., they all trust MS, and vice versa.

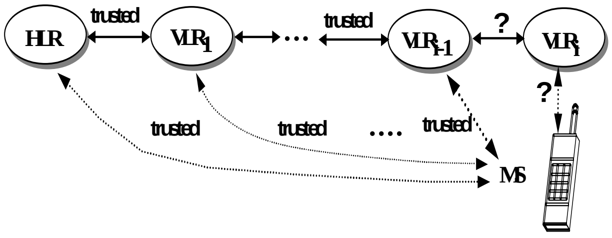


Figure 1. The chain authentication protocol

Since the proposed protocol uses only VLRi-1 to establish authentication between VLRi and MS, we use VLRo and VLRn to denote the old domain VLRi-1 and the new visited domain VLRi, respectively (Figure 1). If some authentication procedures can be applied to guarantee that (1) VLRo trusts the authentication request claimed by MS, (2) VLRn trusts the response of VLRo, and (3) MS trusts the authentication result issued from VLRo, who is trusted; then, VLRn and MS can trust each other. Therefore, we define a basic rule for the authentication in VLRn using VLRo when MS moves from the trusted VLRo to the new visited domain VLRn. The rule of the chain authentication protocol is as follows:

given
MS and VLRo trust each other,
if
1) VLRo and VLRn trust each other,
2) VLRn proves to VLRo that MS has arrived in the new domain, and
3) VLR_n proves to MS that VLR_o trusts and authorizes VLR_n,
then,
MS and VLR_n trust each other.

1.2 Advantages of the Chain Authentication Protocol

The chain authentication protocol has the following merits:

- No assistance from HLR
- Low overhead
- Subscriber identity confidentiality
- Communication confidentiality
- Authenticating overall participant communication entities
- Consideration of multiple service providers in a local area
- Domain separation
- Session key confidentiality
- Low cost for preventing replay attacks

2. A Credit Card-based Billing Scheme for Inter-domain Off-line Roaming Environment

Another important mobile network is the inter-domain off-line roaming environment. A well-known and existing example is the credit card-based commercial networks. The credit card is the MS, the issuer (bank) of the card is the home service provider, and each store is a visited service provider. Whenever the user uses the credit card, a new service session is created again and initiated from the access phase. During the service session, the mobile user does/can not roam to another domain, that is, the handover process is unnecessary in this environment.

Although Visa and MasterCard have jointly developed the Secure Electronic Transaction (SET) protocol as a secure payment method for card transactions over open networks, it still has drawbacks and cannot fit in some applications, such as telephone systems. In the project, we propose a credit card-based payment scheme, which can securely authenticate cardholders without exposing their secret information on networks. And the payment scheme supports the capability of non-repudiation. Thus the mobile user can not deny the bills generated by service providers. The scheme also supports anonymity of cardholders, that is, the service provider (VLR) does not know who requires the service and the credit card company does not know what service is demanded by the user.

2.1 The proposed credit card-based billing scheme

The credit card-based billing scheme is shown as Figure 2.

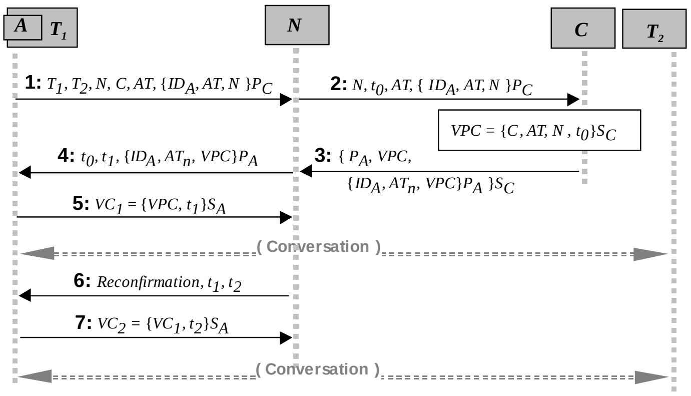

A
T_1
N
C
T_2
1: $T_1, T_2, N, C, AT, \{ID_A, AT, N\}P_C$
2: $N, t_0, AT, \{ID_A, AT, N\}P_C$
$VPC = \{C, AT, N, t_0\}S_C$
4: $t_0, t_1, \{ID_A, AT_n, VPC\}P_A$
3: $\{P_A, VPC, \{ID_A, AT_n, VPC\}P_A\}S_C$
5: $VC_1 = \{VPC, t_1\}S_A$
(Conversation)
6: $Reconfirmation, t_1, t_2$
7: $VC_2 = \{VC_1, t_2\}S_A$
(Conversation)

Figure 2. The proposed credit card-based billing scheme

Step 1: Alice inserts her credit card ***A*** to the card reader of $\boldsymbol{T_1}$. First, Alice dials her personal identification number (PIN) to enable the card. If PIN is correct, ***A*** will get the identity of the telephone company ***N*** from $\boldsymbol{T_1}$ and generate the message $\boldsymbol{X_{11}} = \{\boldsymbol{ID_A}, \boldsymbol{AT}, \boldsymbol{N}\}\boldsymbol{P_C}$. Then ***A*** will give $\boldsymbol{T_1}$ the following data: the identity of CCAC ***C***, its authentication token ***AT***, and the message $\boldsymbol{X_{11}}$. Finally, Alice dials the callee's telephone number $\boldsymbol{T_2}$, and $\boldsymbol{T_1}$ sends the message ($\boldsymbol{T_1}$, $\boldsymbol{T_2}$, ***N***, ***C***, ***AT***, $\boldsymbol{X_{11}}$) to ***N***.

Step 2: When the telephone network system *N* receives the message, it will verify if *C* is a legal and contracted credit card company that supports the service of credit card phone. If yes, it will keep the data T_1, T_2, *C*, and *AT* in the database itself. Then *N* generates a timestamp t_0 that denotes the startup time for billing. And the message $X_{21} = (N, t_0, AT, X_{11})$, where X_{11} was received from T_1, is sent to *C*.

Step 3: The credit card authentication center ***C*** uses its secret key $\boldsymbol{S_C}$ to decrypt the message $\boldsymbol{X_{11}}$. Then ***C*** knows the caller's credit card number $\boldsymbol{ID}_A$, the authentication token ***AT***, and the telephone company ***N***. Since only ***C*** and ***A*** know the credit card number $\boldsymbol{ID_A}$ and the current token ***AT***, ***C*** can distinguish whether the message is new and generated for a phone call by ***A***. If the verification is successful, the message $\boldsymbol{X_{11}}$ is not masqueraded. ***N*** hence is the telephone company which is chosen by the caller to deliver the call. After the authentication, ***C*** makes sure whether $\boldsymbol{t_0}$ is within the valid interval or not. If $\boldsymbol{t_0}$ is much larger or smaller than the local clock in ***C***, the message may be modified by a hostile or masqueraded by ***N*** itself. ***C*** thus discards the message and denies the request for the phone call. Otherwise, ***C*** generates a virtual phone card $\boldsymbol{VPC} = \{\boldsymbol{C}, \boldsymbol{AT}, \boldsymbol{N}, \boldsymbol{t_0}\}\boldsymbol{S_C}$ for this phone call, and randomly selects a new authentication token $\boldsymbol{AT_n}$ for ***A***. To secretly transmit $\boldsymbol{AT_n}$ to ***A***, ***C*** uses ***A***'s public key to generate the message $\boldsymbol{X_{31}} = \{\boldsymbol{ID_A}, \boldsymbol{AT_n}, \boldsymbol{VPC}\}\boldsymbol{P_A}$. Then ***C*** sends ***N*** the message $\boldsymbol{X_{32}} = \{\boldsymbol{P_A}, \boldsymbol{VPC}, \boldsymbol{X_{31}}\}\boldsymbol{S_C}$. Note that ***A***'s public key $\boldsymbol{P_A}$ is encapsulated in $\boldsymbol{X_{32}}$. That is because ***N*** does not know ***A***'s credit card number and its public key.

Step 4: After receiving $\boldsymbol{X_{32}}$, ***N*** uses ***C'***s public key to verify the message: $\boldsymbol{P_C}$ is used to decrypt $\boldsymbol{X_{32}}$ to get $\boldsymbol{P_A}$, ***VPC***, and $\boldsymbol{X_{31}}$. $\boldsymbol{P_C}$ is used again to decrypt ***VPC*** to get four numbers: ***C'***, ***AT'***, ***N'***, and ***t'***. If 1) ***C'*** and ***N'*** is respectively equal to ***C*** and ***N***, 2) ***AT'*** is equal to ***AT*** received from ***A*** in Step 2, and 3) ***t'*** is equal to the timestamp $\boldsymbol{t_0}$ that ***N*** itself sent to ***C*** in Step 2, ***VPC*** is a legal virtual phone card. That is, ***C*** has authenticated the caller as a legal credit card user and permitted her to make the credit card phone. Since ***VPC*** is trusted, $\boldsymbol{P_A}$ is also trustworthy. Then ***N*** generates a new timestamp $\boldsymbol{t_1}$ that indicates the expiration time of the first conversation interval. And ***N*** sends $\boldsymbol{T_1}$ the message $\boldsymbol{X_{41}}$ that contains the startup time $\boldsymbol{t_0}$, the expiration time $\boldsymbol{t_1}$, and the message $\boldsymbol{X_{31}}$.

Step 5: When $\boldsymbol{T_1}$ receives $\boldsymbol{X_{41}}$, it forwards the message to the IC card ***A***. ***A*** uses its secret key to decrypt the ciphertext $\boldsymbol{X_{31}}$ and adopts the same process mentioned in Step 4 to verify whether ***VPC*** is legal. If ***VPC*** is legal, ***A*** generates a virtual coin $\boldsymbol{VC_1}$ as the first evidence of the following conversation interval, where $\boldsymbol{VC_1} = \{\boldsymbol{VPC}, \boldsymbol{t_1}\}\boldsymbol{S_A}$. While ***N*** receives $\boldsymbol{VC_1}$, it should use ***A***'s public key $\boldsymbol{P_A}$, ***VPC***, and $\boldsymbol{t_1}$ to verify whether the evidence is legal. If yes, it establishes the communication channel between $\boldsymbol{T_1}$ and $\boldsymbol{T_2}$. The virtual coin should be collected to charge the credit card company the cost of calls in the future.

Step 6: In advance, the telephone network system ***N*** needs to negotiate a reconfirmation interval with the credit card authentication center ***C*** by a contract. If the conversation between $\boldsymbol{T_1}$ and $\boldsymbol{T_2}$ is longer than the interval time, ***N*** should issues a reconfirmation signal to $\boldsymbol{T_1}$ periodically. The reconfirmation message should contain the expiration time of the next interval ($\boldsymbol{t}_2$ in Figure 2).

Step 7: When $\boldsymbol{T}_1$ receives the reconfirmation message, it forwards the message to ***A***. Then ***A*** will generate a new virtual coin $\boldsymbol{VC}_2 = \{\boldsymbol{VC}_1, \boldsymbol{t}_2\}\boldsymbol{S}_A$ and send it to ***N*** as the next conversation evidence. ***N*** also needs to verify whether the evidence is legal with ***A***'s public key $\boldsymbol{P}_A$, $\boldsymbol{t}_2$, and the old evidence $\boldsymbol{VC}_1$. If yes, the channel between $\boldsymbol{T}_1$ and $\boldsymbol{T}_2$ is kept for another time interval. And the evidence $\boldsymbol{VC}_2$ is saved.

Suppose $\boldsymbol{VC}_j = \{\boldsymbol{VC}_{j-1}, \boldsymbol{t}_j\}\boldsymbol{S}_A$ is the last evidence. The telephone company ***N*** sends ***C*** the message (***N***, ***C***, ***AT***, $\boldsymbol{t}_0$, $\boldsymbol{t}_j$, ***VPC***, $\boldsymbol{VC}_j$) as a bill for the charge of this call. When ***C*** gets this bill, the token ***AT*** and the startup time $\boldsymbol{t}_0$ are used as indices to search the corresponding credit card number $\boldsymbol{ID}_A$ and its public key $\boldsymbol{P}_A$. Then ***C*** verifies the virtual coin:

1) Decrypt ***VPC***. Check if the content is equal to (***C***, ***AT***, ***N***, $\boldsymbol{t}_0$) or not.
2) Repeatedly decrypt the virtual coin $\boldsymbol{VC}_j$ for j times to get the result (***VPC'***, $\boldsymbol{t}_1$). Check if ***VPC'*** is equal to ***VPC*** or not.
3) Check if the time list ($\boldsymbol{t}_0$, $\boldsymbol{t}_1$, …, $\boldsymbol{t}_j$) computed from the above step is valid (the sequence should be monotonically increased and the interval should be equal to the predefined value).

If it is correct, ***C*** has to pay this call. The charge of this call will appear on the caller Alice's monthly credit card statements.

2.2 Protocol Analysis

Since in telephone systems, we cannot guarantee the caller is in a secure environment. Thus, it is very important to protect callers' privacy and guarantee that the telephone company can charge the money for the phone calls it served. The proposed scheme can not only support the authentication of callers to guarantee they will pay for these calls via their credit card accounts, but also has four important features:

1) **Confidentiality**. In the protocol, all sensitive data is encrypted with the receiver's public key, and only the desired receiver can decrypt and share the information. Consequently, we can make sure that the credit card number $\boldsymbol{ID}_A$ is never disclosed and shared only by the credit card ***A*** and CCAC ***C***. With this shared secret, nobody can forge $\boldsymbol{X}_{11}$, and ***C*** can verify if the request is issued by ***A***. Note that the new token $\boldsymbol{AT}_n$ is also kept secret in Step 3 and 4. If the token is transmitted in the plaintext form, it is possible to be hostilely modified. Both values of $\boldsymbol{AT}_n$ in ***C*** and ***A*** will be different, so the authentication for the next phone call will fail.

2) **Anonymity**. Since ***A*** and ***C*** do not expose the credit card number $\boldsymbol{ID}_A$ in messages, the telephone company does not know who make the phone call. In addition, $\boldsymbol{T}_1$ and $\boldsymbol{T}_2$ are known only by ***N***, the credit card company cannot use the information to trace where its customer made the call and know who is the callee. The personal privacy is protected. Of course, if there exists an argument about the bill, ***C*** and ***N*** can cooperate to disclose the details of the phone calls, such as $\boldsymbol{ID}_A$, $\boldsymbol{T}_1$, $\boldsymbol{T}_2$, and $\boldsymbol{t}_0$.

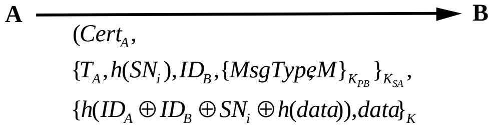
3) **Efficient reconfirmation**. The proposed protocol adopts a periodic payment scheme to resolve the problem that the caller may repudiate he/she made a call. A phone call consists of many conversation intervals. At the ending of an interval, ***N*** must reconfirm whether the caller will continue the conversation. If yes, the caller must give ***N*** a 'coin' to buy the next conversation interval. As the reconfirmation phase needs only two messages shown in Section 4.3, the time spending for the reconfirmation is very short.

4) **Non-repudiation.** Since the virtual phone card ***VPC*** and the corresponding virtual coins ***VC***s are encrypted with the secret keys of ***C*** and ***A***, respectively, the caller (and CCAC) can not repudiate that the call service has been supported by the telephone company.

3. A Secure Single-Message Exchange Protocol for Weak Connection Environments

The third type of mobile computing networks is the weak connection environment. In the general strong connection environment, the MS and the service provider can negotiate a session key at the access phase and then adopt the key to encrypt service contents at the service phase. But, in the weak connection environment, the session key scheme is infeasible because that the authentication and the session key generation/exchange must be executed again whenever the connection is re-established. The overhead spent by the access phase of re-connection will be proportional to the unreliability of radio paths. Herein, we propose a secure message exchange protocol, which is originally designed for supporting the security function of non-session-oriented applications. The proposed scheme needs only one message to authenticate the validity of messages. And, the confidentiality and integrity of service contents carried within the same messages is guaranteed by a message-oriented encryption key. Therefore, the service provider and MS do not need extra messages to establish a secure channel for transmitting the following service contents. The proposed message exchange protocol is especially suitable for the weak connection environment, e.g. wireless communication systems. In addition, it is also suitable for other non-session-oriented application, such as the security management of telecommunication management network (TMN), and Internet management systems.

The message structure of SSMEP looks similar to X.509. SSMEP includes a new verification scheme to verify the freshness of messages, namely, the synchronized-nonce (SN) scheme. The SN scheme is used to replace the timestamp of X.509 (see the next section for the details). The basic message of SSMEP is presented in Figure 3. The message consists of three segments: certificate, authentication, and data segments.



$$(Cert_A,$$

$$\{T_A, h(SN_i), ID_B, \{MsgType, M\}_{K_{PB}}\}_{K_{SA}},$$

$$\{h(ID_A \oplus ID_B \oplus SN_i \oplus h(data)), data\}_K$$

Figure 3. The secure single-message exchange protocol (SSMEP)

4. A Software Authorization and Protection Model for Mobile Codes

Encrypting service contents only can prevent from eavesdropping or modifying of hostile outsiders. If the content is software, other security threats may occur. For example, after a legal mobile user downloads demanded programs, he can arbitrarily copy and distribute these codes. That is the piracy problem. In the chapter, we propose a new software authorization and protection model. In this model, a software consists of multiple mobile codes, which can be dynamically downloaded from service providers. Some critical codes are executed on trusted proxies and the others are executed on the MS. The execution of a software is conducted by cooperation of the MS and the proxies containing codes. There are two important features in the proposed model.

- ♦ Preventing from software piracy: The unauthorized user holding part of mobile codes of the software will not be able to use the software without the help of these proxies.
- ♦ Reducing computation load of MSs: The powerful proxies can afford most of computation to enhance the performance of mobile computing services.

4.1 The Proposed Authorization and Protection Model

In mobile code systems, a program (software) is composed of a number of mobile codes. A code can be downloaded dynamically from the remote machine and executed on the local machine, and a job can be processed by the cooperation of these mobile codes. In the section, an authorization and protection model is proposed to enhance the security and protection of mobile codes by delegating some critical execution services to one or more trusted and protected proxies.

The execution of a program can be considered to include three parts: incoming messages, transformation processes, and outgoing messages. A mobile code participates in the transformation process for a message if the code sends or receives the message. If some critical codes are removed from a program, execution of the program cannot proceed.

With the RMI (Remote Method Invocation) technology for Java language that enables cooperating of computers on the network, we proposed a model that protects software with the help of trusted, protected computational proxy servers, instead of tamper-resistant hardware devices installed in the user's environment. In this model, mobile codes of the software are partitioned into two types, general and privileged codes. The users can acquire only general codes. And the privileged codes are forced to be executed in a protected environment, that is, the trusted computation proxy.

The trusted computational proxy provides computation services for privileged codes, as shown in Figure 4. Only a trusted proxy has the capability to get privileged codes and execute them. The proxy executes the mobile codes on behalf of an authorized user and returns the result to the user (MS). In this way, an unauthorized user cannot acquire the results of privileged codes, and therefore benefit little from the software. A program may delegate all privileged codes to many proxies, and each proxy executes only a subset of the privileged codes. Thus, a compromised proxy will not leak all privileged codes. In the proposed model, mobile codes to be downloaded are encrypted by code keys, and the code keys for each mobile code are different. These keys are only available to trusted proxies or authorized users. The model consists of six major components:

- Software Vendor: The company who developed the software.
- Certification Authority: The party who signs and issues the certificate containing the user's public key.
- Software Authentication Center: An accredited organization that authenticates the software developed by software vendors, and signing legitimate parts of the software.
- Service Provider: The server who stores mobile codes provided by software vendors. When an MS wants to execute a mobile code, it first connects to the service provider and downloads the code from the server.
- Trusted Computational Proxy: The server that provides computational services of privileged codes for users (MS). These proxies need a service provider to support a communication channel to the MS.
- MS: The user's local host for executing the software. For simplification, we also use 'MS' to denote the user in the following discussion.

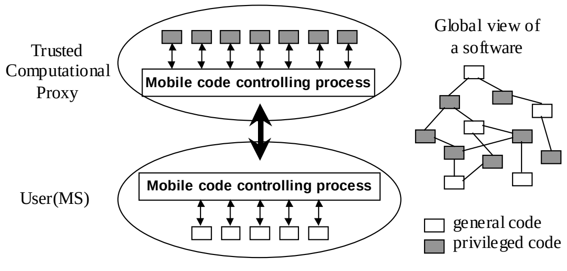

Trusted Computational Proxy
Mobile code controlling process
User(MS)
Mobile code controlling process
Global view of a software
general code
privileged code

Figure 4. The proposed protection model

5. *Conclusions*

In this report, we address the security problems of mobile computing services. First, the features of mobile computing networks are investigated. According to the environment, the possible security threats and the critical security issues are discussed. We also analysis GSM to illustrate the security problems occurring in modern mobile communication systems. Then, we propose our solutions to protect mobile computing services.

5.1 Comments on Protecting Mobile Communications

In the project, we consider three main types of mobile communication environment:
• the inter-domain on-line roaming networks,
• the inter-domain off-line roaming networks,
• the weak connection networks.
We propose three authentication protocols to protect communications between service providers and MSs under these environment restrictions.

The first environment is the trend of current mobile telecommunication systems. The proposed protocol, called chain authentication protocol, can efficiently authenticate all communication entities with the assistance of old visited service provider. In addition, our scheme can be adopted in networks that have multiple service providers within a geographical area. It is thus practical for an enormous and heterogeneous network.

The second environment is similar to the model of credit card-based mobile computing networks. Although the SET standard has been proposed to provide a secure environment for card transactions, the SET is not suitable for all credit card-based applications, such as the credit card-based phone services. In he project, we propose a credit card-based billing scheme for the inter-domain off-line roaming networks. The scheme does not only support the capability of authenticating entities, but also guarantee the anonymity of callers. Furthermore, we propose the concept of virtual phone cards to support a secure, non-repudiated, and efficient payment environment, which makes the communication load much lower than the SET standard.

The third environment is designed for wireless networks. In such environment, the connection has lower bandwidth and higher error rate, and is subject to frequent disconnection. We propose a secure single-message exchange protocol for efficiently and securely transmitting data. The data and a segment of security-related information are carried within a single message. The information provides the features of authenticating and enciphering the data. The proposed protocol adopts a synchronized nonce scheme, instead of a timestamp, to prevent from replay attacks. Thus, our scheme needs not synchronize the clocks of MSs and service providers.

5.2 Comments on Protecting Contents in Service Providers

In mobile computing networks, not all security threats occur on communications between MSs and service providers. Security mechanisms are also needed to protect contents in service providers. The contents may be mobile service contents (e.g. software programs) and management data (e.g. subscribers' accounting data). The project herein introduces a security mechanism to protect mobile code-based software.

We propose a software authorization and protection model for the new generation software, mobile code systems. In this model, a software consists of multiple mobile codes, and only independent mobile codes are executed on the MS. The other codes are executed on trusted proxies. Each mobile code produced by the software vendor has a publication license which is issued by a trusted third party. Before using software, the MS must request an execution license for demanded mobile codes. We do not only introduce the system components of the model for issuing the licenses, but also discuss how to partition software based on the considerations of computation/communication load and security. Thus, the proposed model can prevent from software piracy and reduce computation load of MSs. In addition, by verifying the mobile code with its publication license, the MS and proxy can detect whether the code has been unauthorizedly modified or not. This feature can reduce the risk of attacks from Trojan Horse or viruses.

6. Reference

[ANSI81] ANSI X3.92, "American National Standard for Data Encryption Algorithm," American National Standards Institute, 1981.

[Atk95a] R. Atkinson, "Security Architecture for the Internet Protocol," RFC-1825, Aug. 1995.

[Atk95b] R. Atkinson, "IP Authentication Header," RFC-1826, Aug. 1995.

[Atk95c] R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC-1827, Aug. 1995.

[Azi95] A. Aziz and M. Patterson, "Simple Key Management for Internet Protocols (SKIP)," Proceedings of the INET`95 Conference, Jun. 1995.

[Bal93] D. Balenson, "Privacy Enhancement for Internet Electronic Mail, Parts III: Algorithms, Modes, and Identifiers," RFC-1423, SRI Network Information Center, Feb. 1993.

[Bal96] E. Balas and J. Xue, "Weighted and Unweighted Maximum Clique Algorithms with Upper Bounds from Fractional Coloring," Algorithmica 15, pp. 397-412, 1996.

[Bar89] W. C. Barker, "Use of Privacy-Enhanced Mail for Software Distribution," Fifth Annual Computer Security Applications Conference, pp. 344-347, 1989.

[Bel93] M. J. Beller, L. F. Chang, Y. Yacobi, "Privacy and Authentication on a portable Communications System," IEEE Journal on Selected Areas in Comm., Vol. 11, No. 6, Aug. 1993.

[Bha94] V. Bharghavan, "Secure Wireless LANs", ACM, pp.10-17, 1994.

[Bic96] L. F. Bic, M. Fukuda, and M. B. Dillencourt, "Distributed Computing Using Autonomous Objects," IEEE Computer, August 1996.

[Buc97] K. Buchanan, R. Fudge, D. McFarlane, T. Phillips, A. Sasaki, and H. Xia, "IMT-2000: Service Provider's Perspective," IEEE Personal Communications, Vol. 4, No. 4, Aug. 1997.

[Bur90] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication," ACM Transaction on Computer Systems, Vol. 8, No. 1, Feb. 1990.

[Cal97] M. H. Callendar, "International Mobile Telecommunications-2000: Standards Efforts of the ITU," IEEE Personal Communications, Vol. 4, No. 4, Aug. 1997.

[Car97] A. Carzaniga, G. P. Picco, and G. Vigna, "Designing Distributed Applications with a Mobile Code Paradigm," In Proceedings of the 19th International Conference on Software Engineering, Boston, Ma., May 1997.

[Cas90] J. Case, M. Fedor, M. Schoffstall, and J. Davin, "A Simple Network Management Protocol (SNMP)," RFC-1157, May 1990.

[CDP93] CDPD Consortium, "Cellular Digital Packet Data System Specification," Release 1.0, July 1993.

[Che88] G. H. Chen, M. T. Kuo, and J. P. Sheu, "An Optimal Time Algorithm for Finding a Maximum Weight Independent Set in a Tree," BIT 28, pp. 353-356, 1988.

[Chi79] F. Y. Chin and G. Ozsoyoglu, "Security in partitioned dynamic statistical databases," In Proceedings of the IEEE COMPSAC, pp. 594-601, 1979.

[Chi81] F. Y. Chin and G. Ozsoyoglu, "Statistical database design," ACM Trans. on Database Syst., Vol. 6(1) pp. 113-139, Mar. 1981.

[Chi82] F. Y. Chin and G. Ozsoyoglu, "Auditing and inference control in statistical databases," IEEE Trans. on Softw. Eng. pp. 574-582, Apr. 1982.

[Cho94] S. Chokhani, "Toward a National Public Key Infrastructure," IEEE Communications Magazine, Sep. 1994.

[Chr71] N. Christofides, “An Algorithm for the Chromatic Number of a Graph,” The Computer Journal, 14, p. 38, 1971.

[Chr75] N. Christofides, “Graph Theory,” Academic Press, London, 1975.

[Cia97] P. Ciancarini and D. Rossi, “Jada -- Coordination and Communication for Java Agents,” In Mobile Object Systems: Towards the Programmable Internet, pages 213-228. Springer-Verlag, April 1997. Lecture Notes in Computer Science No. 1222.

[Cit96] CitiBank, “Masterphone Service”, (http://www.citibank.com/argentina/e/gc/arcpdbaa.htm), 1996.

[Cla91] J. Clark and D. A. Holton,” A First Look at Graph Theory,” World Scientific, 1991.

[Cox80] L. H. Cox, "Suppression methodology and statistical disclosure control," J. Am. Stat. Assoc. Vol. 75, No. 370, pp. 377-385, Jun. 1980.

[Cur92] A. Curiger, and B. Stuber, “Specification for the IDEA Chip,” Technical Report No. 92/03, ETH Zurich: Institute for Integrate System, Feb. 1992.

[Cur94] D. Curtis, “Software Privacy and Copyright Protection,” WESCON/94, Idea/Microelectronics, Conference record, pp. 199-203, 1994.

[Dak95] K. J. Dakin, “Do You Know What Your License Allows?” IEEE Software, pp. 82-83, May 1995.

[Dea96] D. Dean, E. Felten, and D. Wallach, “Java Security: From HotJava to Netscape and Beyond,” Proc. IEEE Symp. Security and Privacy, pp. 190-200, May 1996.

[Del96] H. S. Delugach and T. H. Hinke, "Wizard: A database inference analysis and detection system," IEEE Tran. on Knowledge and Data Engineering, Vol.8(1), pp.56-66, Feb. 1996.

[Den] D. E. Denning, "Cryptography and Data Security," Addison-Wesley, Reading Mass.

[Den80] D. E. Denning, "Secure statistical databases under random sample queries," ACM Trans. on Database Syst., Vol. 5, No. 3, pp. 291-315, Sep. 1980.

[Den83a] D. E. Denning, "A security model for the statistical database problem," In Proceedings of the 2nd International Workshop on Management, pp. 1-16, 1983.

[Den83b] D. E. Denning and J. Schlorer, "Inference control for statistical databases," Computer, Vol. 16, No. 7, pp. 69-82, Jul. 1983.

[Dif76] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, Nov. 1976.

[Dob79] D. Dobkin, A. K. Jones and R. J. Lipton, "Secure databases: Protection Against User Inference," ACM Trans. on Database Syst., Vol. 4, No. 1, pp. 97-106, Mar. 1979.

[DoD85] "Trusted Computer System Evaluation Criteria," DoD STD-5200.28, Dec. 1985.

[Don94] S. Donovan, “Patent, Copyright and Trade Secret Protection for Software,” IEEE Potentials, pp. 20-24, August/September 1994.

[EIA95a] EIA/TIA, "Cellular Intersystem Operations (Rev. C)," Technical Report IS-41, EIA/TIA, 1995.

[EIA95b] EIA/TIA, “Mobile Station-base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System, ” Technical Report TIA/EIA/IS-95-A, EIA/TIA, 1995.

[Gal93] J. Galvin and K. McCloghrie, “Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2),” RFC-1446, Apr. 1993.

[Gar79] M. R. Garey and D. S. Johnson, “Computers and Intractability: A guide to the Theory of NP-Completeness,” Freeman, San Francisco, CA., 1979.

[Ghe97] C. Ghezzi and G. Vigna, “Mobile Code Paradigms and Technologies: A Case Study,” In Proceedings of the First International Workshop on Mobile Agents, Berlin, Germany, April 1997.

[Gon92] L. Gong, “Security Risk of Depending on Synchronized Clocks,” ACM Operating System Review, Vol. 26, No. 1, 1992.

[Gon97] L. Gong, "New Security Architectural Directions for Java (Extended Abstract)" . In Proceedings of IEEE COMPCON, San Jose, California, pp. 97-102, Feb. 1997.

[Gos96] J. Gosling and H. McGilton, “The Java Language Environment,” Sun Microsystems, May 1996, http://java.sun.com/doc/language_environment/ .

[Gra95] R. S. Gray, “Agent Tcl: A Transportable Agent System,” In Proceedings of the CIKM Workshop on Intelligent Information Agents, Baltimore, Md., December 1995.

[GSM93a] "GSM 02.09: Security Aspects," European Telecommunications Standards Institute, Jun. 1993.

[GSM93b] "GSM 03.20: Security Related Network Functions," European Telecommunications Standards Institute, Jun. 1993.

[Gus98] E. Gustafsson, A. Herlitz, A. Jonsson, and M. Korling, “UMTS/IMT-2000 and Mobile IP/DIAMETER Harmonization,” Internet draft, draft-gustafsson-mobileip-imt-2000-00.txt, Nov. 1998. Work in progress.

[Har92] L. Harn, H.Y. Lin and S. Yang, “A Software Authentication System for Information Integrity,” Computers and Security, Vol.11, No.4, pp. 747-752, 1992.

[Hin96] R. M. Hinden, “IP Next Generation Overview,” Communications of the ACM, Col. 39, No. 6, Jun. 1996.

[Hon96] Hongkong Telecom, “International Calls”, (http://hkt.net// international.htm), 1996.

[Jai94] R. Jain, Y. B. Lin, C. Lo, and S. Mohan, "A Caching Strategy to Reduce Network Impacts of PCS," IEEE Journal on Selected Areas in Communications, Vol. 12, No. 8, Oct. 1994.

[Jai95] R. Jain, Y. B. Lin, and S. Mohan, "A Forwarding Strategy to Reduce Network Impacts of PCS," IEEE INFOCOM, 1995.

[Kar97] G. Karjoth, D. B. Lange, and M. Oshima, “A Security Model for Aglets,” IEEE Internet Computing, Jul. 1997.

[Ken93] S. Kent, "Privacy Enhancement for Internet Electronic Mail, Parts II: Certificate-Based Key Management," RFC-1422, SRI Network Information Center, Feb. 1993.

[Kob93] B. Z. Kobb, "Personal Wireless," IEEE SPECTRUM, Jun. 1993.

[Kop87] R. Kopf and G. Ruhe, “A Computational Study of the Weighted Independent Set Problem for General Graphs,” Foundations of Control Engineering, pp. 167-180, 1987.

[Lin93] J. Linn, "Privacy Enhancement for Internet Electronic Mail, Parts I: Message Encryption and Authentication Procedures," RFC-1421, SRI Network Information Center, Feb. 1993.

[Lin97] Y. B. Lin, Introduction to Mobile Network Management, Wei-Keg Publishing Co., 1997.

[M3010] “Principles for a Telecommunications Management Network,” CCITT Draft Recommendation M.3010.

[M3400] “TMN Management Functions,” CCITT Draft Recommendation M.3400.

[McL89] M. McLeish, "Further result on the security of partitioned dynamic statistical databases," ACM Trans. on Database Systems, Vol.14, No.1, pp.98-113, Mar. 1989.

[Mil92] D. L. Mills, “Network Time Protocol (Version 3) Specification, Implementation and Analysis,” RFC-1305, Mar. 1992.

[Mod90] A. R. Modaressi and R. A. Skoog, “Signalling System No. 7,” A tutorial, IEEE Communications Magazine, pp. 19-35, Jul. 1990.

[Mog88] M. Mogenstern, "Controlling logical inference in multilevel database systems," Proc. IEEE CS Symp. Security and Privacy, pp.245-255, Apr. 1988.

[Mol94] R. Molva, D. Samfat, G. Tsudik, "Authentication of Mobile Users," IEEE Network, Mar./Apr. 1994.

[Mou92] M. Mouly, M. B. Pautet, "The GSM System for Mobile Communications," ISBN: 2-9507190-0-7, 1992.

[Mu96] Yi Mu and Vijay Varadharajan, “On the Design of Security Protocols for Mobile Communications”, 1996.

[Nef94] R. E. Neff, “Software Piracy: International Copyright Overview,” WESCON/94, Idea/Microelectronics, Conference record, pp. 190-195, 1994.

[NBS77] NBS FIPS PUB 46-1, "Data Encryption Standard," National Bureau of Standards, U.S. Department of Commerce, Jan. 1977.

[Ozs90] G. Ozsoyoglu and T. A. Su, "On inference control in semantic data models for statistical databases," Journal of Computer and System Sciences, Vol.40, No. 3, pp.405-443, Jun. 1990.

[Pan97] R. Pandya, d. Grillo, E. Lycksell, P. Mieybegue, H. Okinaka, and M. Yabusaki, “IMT-2000 Standards: Network Aspects,” IEEE Personal Communications, Vol. 4, No. 4, Aug. 1997.

[Par91] P. M. Pardalos and N. Desai, “An Algorithm for Finding a Maximum Weighted Independent Set in an Arbitrary Graph,” Int. J. Comput. Math. 38, pp. 163-175, 1991.

[Per96a] C. Perkins, Editor, “IP Mobility Support,” RFC 2002, Oct. 1996.

[Per96b] C. Perkins, "Mobile-IP Local Registration with Hierarchical Foreign Agents," IETF Internet-Draft, Feb. 1996.

[Rah93] M. Rahnema, "Overview of the GSM System and Protocol Architecture," IEEE Comm. Mag., Vol. 31, No. 4, Apr. 1993.

[Rei79] S. B. Reiss, "The practicality of data swapping," Technical Report No. CS-48, Dept. of Computer Science, Brown Univ., Providence, R.I., 1979.

[Rei80] S. B. Reiss, "Practical data-swapping: The first steps," In Proceedings 1980 Symp. on Security and Privacy, IEEE Computer Society, pp. 38-45, Apr. 1980.

[Rei84] S. B. Reiss, "Practical data-swapping: The first steps," ACM Trans. on Database Syst., pp. 20-37, Mar. 1984.

[Riv78] R. L. Rivest, A. Shamir, and L. Adelman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Commun. of the ACM, Vol. 21, No. 2, pp. 120-126, Feb. 1978.

[Rub95] A. D. Rubin, “Trusted Distribution of Software Over the Internet,” Proc. IEEE Symp. On Network and Distributed System Security , pp. 47-53, 1995.

[Rub98] A. D. Rubin and D. E. Geer, Jr., “Mobile Code Security,” IEEE Internet Computing, Nov. 1998.

[San96] R. S. Sandhu and E. J. Coyne, "Role-Based Access Control Models," IEEE Computer, Feb. 1996.

[Sch81] J. Schlorer, "Security of statistical databases: Multidimensional transformation," ACM Trans. on Database Syst., Vol. 6, No. 1, pp. 95-112, Mar. 1981.

[Sch96] B. Schneier, “Applied Cryptography: protocols, algorithms, and source code in C”, 2nd, pp.47-74, 1996.

[SET96] Visa and MasterCard, “Secure Electronic Transaction (SET) Specification, Book 1: Business Description”, June 17 1996.

[Shi95] S. P. Shieh, C. T. Lin, R. T. Hsueh, "Secure Communication in Global Systems for Mobile Telecommunications," Proceedings of Mobile Computing Workshop, April 1995.

[Shi96] S. P. Shieh and W. H. Yang, “An Authentication and Key Distribution System for Open Network Systems,” ACM Operating Systems Review, Vol. 30, No.2, 1996.

[Shi97] S.P. Shieh, W.H. Yang, and H.M. Sun, “An Authentication Protocol without Trusted Third Party,” IEEE Communication Letters, May 1997.

[Shi98] S. P. Shieh, C. T. Lin, M. J. Peng, W.C. Yang, and J.N. Yang, “A Secure Credit-Card Based Billing Schemes for Telephone Services,” International Conference on Mobile Computing, March 1998.

[Shi99] S.P. Shieh, C.T. Lin, S.Y. Wu, “Optimal Assignment of Mobile Agents for Software Authorization and Protection,” accepted for publication, Computer Communications, 1999.

[Ste88] J. G. Steiner, B. C. Neuman, J. I. Schiller, “Kerberos: An Authentication Service for Open Network Systems,” Proceedings of the Winter 1988 Usenix Conference, Feb. 1988.

[Sun96a] “Remote Method Invocation Specification”, Sun Microsystems Inc. http://www.javasoft.com/products/jdk/1.1/docs/guide/rmi/spec/rmiTOC.doc.html.

[Sun96b] “Signed Applets and Digital Signatures,” Sun Microsystems Inc. http://java.sun.com/products/JDK/1.1/docs/guide/signing.

[Suz97] S. Suzuki, K. Nakada, “An Authentication Technique Based on Distributed Security Management for the Global Mobility Network,” IEEE Journal on Selected Areas in communications, Vol. 15, No. 8, Oct. 1997.

[Tar77] R. E. Tarjan and A. E. Trojanowski, “Finding a Maximum Independent Set,” SIAM J. Comput., 6, no. 3, pp. 537-546, 1977.

[Tra84] J. F. Traub, Y. Yemini and H. Wozniakowski, "The Statistical Security of a Statistical Database," ACM Trans. on Database Syst., Vol. 9, No. 4, pp.672 – 679, Dec. 1984.

[Var96] V. Varadharajan and Y. Mu, “Design of Secure End-to-End Protocols for Mobile Systems”, Wireless’96.

[Ven97] B. Venners, “The Architecture of Aglets,” *Java World*, http://www.java-world.com/javaworld/jw-04-1997/jw-04-hood.html, April 1997.

[Voe86] J. Voelker and P. Wallich, “ How Disks are ‘Padlocked’,” IEEE Spectrum, p. 32, June 1986.

[Wel67] D. J. A. Welsh and M.B. Powell, “An Upper bound for the Chromatic Number of a Graph and its Application to Timetabling Problems,” Comput. J., 10:85-86, 1967.

[Wil97] A. Wilson, “Software Security and the DirectPlay API,” Dr. Dobb’s Journal, pp. 66, April 1997.

[Wor89] J. C. Wortmann and N. R. Adam, "Security-Control methods for statistics databases: A comparative study," ACM Computing Surveys, Vol. 21(4) pp. 515-554, Dec. 1989.

[X88] "Recommendation X.509 and ISO 9594-8, Information Processing Systems - Open Systems Interconnection - The Directory - Authentication Framework," CCITT Technical report, Mar. 1988.

[Xue94] J. Xue, “Edge-Maximal Triangulated Subgraphs and Heuristics for Maximum Clique Problem,” Networks, Vol. 24, pp. 109-120, 1994.

[Zha97] X. N. Zhang, “Secure Code Distribution,” IEEE Computer, Vol. 30, No. 6, pp. 76-79, June 1997.