Ticket-based service access scheme for mobile users

Hua Wang [1] **Jinli Cao** [1] **Yanchuan Zhang** [2]

[1] Department of Maths & Computing
University of Southern Queensland
Toowoomba QLD 4350 Australia
Email: (wang, cao)@usq.edu.au
[2] School of Computing
University of Tasmania
Hobart Tasmania 7001 Australia
Email: yan@utas.edu.au

Abstract

Security is one of the important issues in mobile computing, especially in mobile database systems since mobile environments are dynamic and traditional protection mechanisms do not work very well in such environments. For mobile database access across multiple service domains, the traditional access mechanisms rely on the concept of starting home location and cross domain authentication using roaming agreements. However, the cross domain authentications will involve many complicated authentication activities when the roam path is long. This limits the future mobile applications.

This paper presents a global solution for all kinds of mobile services, by a ticket-based service access model that allows anonymous service usage in mobile application and access. The service provider can avoid roaming to multiple service domains, only contacting the Credential Centre to check the user's certification. The user can preserve anonymity and read a clear record of charges in the Credential Centre at anytime. Furthermore, the identity of misbehaving users can be revealed by a Trusted Centre.

Keywords: Mobile computing, Signature, RSA, Security, Credential Centre.

1 Introduction

Mobile computing and communication is becoming an important factor in business. With wireless computing and communication, security and privacy issues are more critical. The dynamic mobile environment is incompatible with static security services. From the consumer's point of view, there is often a preference for a total solution for all kinds of service, some degree of anonymity such as no more cross authentification, and a clear statement of account when shopping over the Internet. There are a number of proposals for mobile systems [Mehrotra, 1997, Mehrotra and Golding, 1998, Frankel et al., 1995]. All of them lack some flexibility in security management. The Global system for mobile communications [Mehrotra, 1997], for example, provides mechanisms for user authentication as well as integrity and confidentiality, including protection of information exchanged between the mobile terminal and the fixed network. It provides only limited privacy protection for users by hiding their real identities from eavesdroppers on the radio interface [Mehrotra and Golding, 1998]. Another contemporary mobile communication system CDPD [Frankel et al., 1995] provides similar security services. However, there are some other issues and problems which need to be addressed:

Global solution. Current solutions can only solve particular service problems for mobile users. Users have to change mobile service systems in order to do other business on the Internet. This is not convenient for users.

Clear charging. Mobile users wish to see a clear and continuously up-dated statement account. Users do not like receiving a charging bill only monthly or bi-monthly, but like to be able to check it at anytime.

Trustiness. In most cases, it is assumed that mobile users trust service providers to bill their service usage correctly and not to misuse either users or service usage related information. This kind of trust model is not adequate for future mobile communication systems. With the rapidly growing number of service providers, most of which are new on the market, and unknown to the users, this assumption is no longer justified. This requires mechanisms that guarantee correct and indisputable billing and ensure anonymous service usage.

Scalability. Future mobile communication systems aim at offering access to any service, anywhere, at any time. The mechanisms of current mobile communication systems are not sufficiently scalable to be able to fulfil this requirement. Traditional solutions for implementing user mobility rely on cross domain authentication and roaming agreements. A user, when visiting a foreign domain and accessing a service there, has to authenticate himself to the foreign service provider with the help of his home domain agent. This may involve a potentially time consuming authentication protocol over long distances. Furthermore, cross domain authentication requires the foreign service provider to trust the home domain agent of the user. Today, this trust is based on roaming agreements between various service providers. With the rapidly growing number of service providers, however, roaming agreements are becoming inefficient and no longer feasible. New mechanisms are needed that do not require contact with the home domain of the user when accessing services in a foreign domain, nor business agreements between domains.

In the future, mobile communication systems should provide total solutions for all kinds of mobile services and guarantee higher levels of security than current systems. This means that, as well as requiring confidentiality and the protection of the integrity of the message exchanged between the user and the service provider, and authentication of the user to the service provider, future systems should also require authentication of the service provider to the user and guarantee higher levels of privacy. Furthermore, clear billing has to be ensured.

In this paper, a new approach to address the above-mentioned problems is proposed. This approach is based on the Credential Centre, and a ticket-based mechanism for service access. The main idea is illustrated in Figure 1.

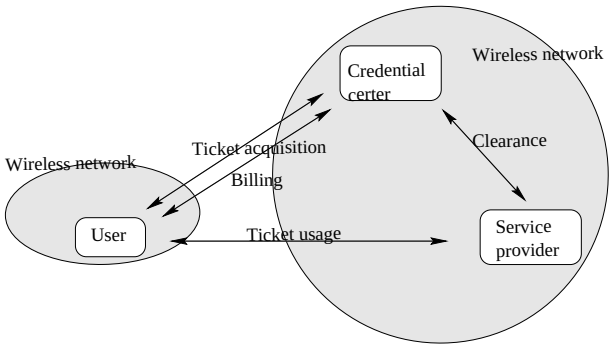

Figure 1: **Ticket Model**

In this model, each user is registered with a Credential Centre. This Credential Centre issues tickets to its users. The users can use the tickets to access services anonymously. When requesting a service, the user is required to hand over an appropriate ticket. After checking the ticket, the service provider provides the requested service to the user. Later, the user can see a clear charging bill in the Credential Centre and the Credential Centre pays for the services used by the user.

Tickets are in two categories and different mechanisms relate to each ticket group. Users are anonymous in purchasing since no private message needs to be shown to service providers. Use of a ticket-based system can avoid roaming multiple service domains. A simple case is a single signature. This case can be used in tickets with only one bound entity (users, service providers or services). The bound entity uses a signature to authenticate a ticket. To cope with the cases of two or more bound entities, it is extended to v Signer_roles. This means that a user can get a service if all v entities agree. The v Signer_roles case can also associate with the other services provided by many providers. A Credential_role in the Credential Centre is set up to issue tickets and control the user's charging bill, and a Trusted_role is also set up to judge conflicts. Each user's statement of account can be seen clearly in the Credential Centre. Furthermore, it is dynamic, since new users and providers can join the ticket-based system at anytime.

The model has the following three important features:

1. It is anonymous for users.
2. It provides a global solution for all types of service.
3. It is scalable and dynamic.

This paper is organized as follows: in section 2, the basic model and ticket types are introduced. Some basic definitions and some simple examples are reviewed in section 3. The single signature scheme for ticket group_1, its security analysis and ticket usage are presented in section 4. In section 5, a multi-signature scheme for ticket group_2, its security and ticket usage are discussed, while related work is given in section 6. Finally the conclusions are presented in section 7.

2 Basic model and ticket types

2.1 Basic model

There are three roles (the user, the service provider, and the Credential Centre) and a protocol with several subprotocols (ticket acquisition, ticket usage, clearance, and billing) in this model. We assume that each user is registered with a Credential Centre. The user obtains tickets by running the ticket acquisition protocol with the Credential Centre. These tickets can be used to access services anonymously. In the ticket usage protocol, the user presents an appropriate ticket to the service provider, which can verify the validity of the ticket and the legitimacy of the user to use it. While the user's private identity is not revealed in this protocol, the service provider authenticates itself to the user. If the verification of the ticket is successful, then the service provider provides the service to the user according to the conditions on the ticket. Based on the received tickets, the Credential Centre prepares a clear bill for each user. The exact form of the clearance (payment to the service provider) and billing (payment to the customer care agency) protocols are not specified in our model. They can use some electronic payment protocols such as Wang and Zhang suggest [Wang and Zhang, 2001].

A global solution is proposed for all kinds of service in which users do not have to change the mobile service system when they do different kinds of business on the Internet, and in which the users can see a clear charging bill in the Credential Centre. The problems of lack of trust and scalability are also addressed as follows:

Trust. Tickets provide anonymous access to services for users, therefore, users do not need to fully trust service providers to handle user and service usage related information. On the other hand, service providers authenticate themselves to accessing users, thus, the user can be sure that the service is provided by the selected service provider. Service providers can verify the validity of the tickets and check if they were used by their legitimate users. If necessary, anonymity can be revoked and users who behave in a malicious way can be traced by the Trusted Centre.

Scalability. Instead of contacting the home domain agent of the accessing user, in this model, the service providers only need to verify the ticket. None of users require long distance protocols but connect to the Credential Centre. In most cases, the ticket will be acquired by the user from the Credential Centre before roaming into the foreign domain. Thus, ticket acquisition usually does not require long distance protocols.

2.2 Ticket types

There are several advantages in using tickets for accessing services [Buttyan and Hubaux, 1999]:

Flexibility. Users can easily construct personalised service profiles by buying the appropriate set of tickets. They do not have to enter into long term contractual relationships with service providers. Instead, they can choose services as they need them and in a way that matches their personal requirements.

Scalability. Tickets can contain all the necessary information for the service provider to decide if it should provide the service or not. Thus, there is no need to run long distance protocols with some trusted agent of the accessing user in order to perform authentication.

Privacy. Users only have to demonstrate that they are legitimate holders of tickets, and they do not necessarily have to reveal their real identities. Thus, no private information is available to service providers.

Transfer. In real life, not all tickets can be transferred. It is not convenient for users to limit the wide use of tickets. In this ticket-based service access mechanism, a ticket can be lent to other users even though it is bound with the user. This means the ticket buyer and the ticket user do not have to be the same.

Although, in the most specific case, a ticket binds a given user, a given service, and a given service provider together, this is not necessarily always the case. Consider, for instance, a bus ticket, which usually does not specify who can use it (i.e., the user) or a travel card, which may not restrict the means of transport (i.e., the service). Based on this observation, there are eight types of tickets. These are illustrated in Table 1, where 'Θ' means that the corresponding entity, user, service provider or service is bound by the ticket, while '$-$' means that it is not.

A ticket of type t_0, for instance, does not restrict the service for which it can be used, the service provider which accepts it, or the user who can use it. This is much like cash in real life. The other extreme is a ticket of type t_7, which can only be used by a given user, for a given service, provided by a given service provider. An example of this type is the flight ticket.

Types	t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7
user	-	-	-	-	Θ	Θ	Θ	Θ
provider	-	-	Θ	Θ	-	-	Θ	Θ
service	-	Θ	-	Θ	-	Θ	-	Θ

Table 1: Ticket types

As mentioned, tickets t_1, t_2 and t_4 have only one entity bound and tickets t_3, t_5, t_6 and t_7 have two or three entities bound. The tickets are divided into two groups, one is ticket group_1 including tickets t_1, t_2, t_4, and another one is ticket group_2 including t_3, t_5, t_6, t_7. That are ticket group_1 $= \{ t_1, t_2, t_4 \}$ and ticket group_2 $= \{ t_3, t_5, t_6, t_7 \}$.

In the remaining parts, the way the protocols work for these two groups will be explained. The ticket t_0 does not require discussion since it is a very simple case.

3 Some basic definitions

To facilitate discussions, some well known primitive cryptographic terminologies which will be used in the remaining sections of the paper are reviewed.

One-way function, is a function which is relatively easy to compute, but significantly hard to reverse. That is, given x it is easy to compute $f(x)$, but given $f(x)$ it is hard to compute x [Beimel et al., 1999].

Breaking a plate is a good example of a one-way function. It is easy to smash a plate into a thousand tiny pieces. However, it is not easy to put all of those tiny pieces back together into a plate.

Hash function, $h(x)$ is a hash function. For a given Y it is computationally hard to find a x such that $h(x) = Y$, where x might be a vector.

Hash functions have been used in computer science for a long time. They are a major building blocks for several cryptographic protocols, including pseudo-random generators [Bellare et al., 1996], digital signatures, and message authentication [Waleffe and Quisquater, 1990].

RSA, is a public key cryptosystem that offers both encryption and digital signatures (authentication) [Rivest et al., 1978]. RSA works as follows: taking two large primes p and q, and computing their product $n = pq$; n is called the modulus. Choosing a number e, less than n and relatively prime to $(p-1)(q-1)$. Finding another number d such that $(ed-1)$ is divisible by $(p-1)(q-1)$. The public key is the pair (n, e), the private key is d. The factors p and q may be kept with the private key or destroyed.

It is currently difficult to obtain the private key d from the public key (n, e). RSA is often used in modern environments [Chaum, 1981], especially on the Internet, since an individual needs not send any private secret key to others when they want to contact him.

Multi-signatures, are multiple signatures signed on the same document. There are two ways to implement multi-signature. One is that each person signs separately, the other is that the message is signed simultaneously [Stinson, 1995]. A multi-signature is the enhancement of a single signature.

4 Single signature scheme for ticket group_1

This section introduces a single signature scheme for tickets t_1, t_2, t_4. The single signature scheme is introduced then analysed to show how it works for a ticket. There are four roles in the single signature scheme, Signer_role, Verifier_role, Credential_role and Trusted_role. Depending on tickets, the Signer_role can be a user, service or service provider that signs a signature as a ticket. The Verifier_role might be a user or service provider that verifies the signature of the Signer_role. The Credential_role in the Credential Centre will issue tickets. It provides information for the Verifier_role to check the signature. Whether the signature is valid or not depends on the information. The Trusted_role is a judge to solve the conflict between users, service providers and services. This is because only the Trusted_role has the secret key of the system and can trace users and service providers. Each Signer_role has a different but fixed public key I, which is validated once the Signer_role is registered in the Trusted Centre. Ticket t_4, for instance, is bound to a user only. A user can follow this scheme to sign a signature as a ticket, the service provider verifies it and then sends some information to the Credential_role and asks for payment. Tickets t_1, t_2 are similar to ticket t_4, the signers are service provider and service separately but not users.

4.1 Initialization of the system

Usually, there are two components in a signature scheme, one is the Signer_role played by consumers, service provider, or service; the other is the Verifier_role played by service consumers or service providers. As a ticket, a signature is valid only if its verification is correct.

The following is an outline of the process of the scheme. In the system initialization, the Trusted_role sends the private messages (r, S) to the Signer_role when the Signer_role is set up. In the second step, the Credential_role verifies if the data (I, r, D) sent by the Signer_role are valid or not. Data (I, D) will be put on a public directory in the Credential centre if the data are valid. At this time, the Signer_role can do a signing message job.

If the Signer_role signs a message m, the Signer_role will send the signed (t, T, m) to the Verifier_role, and the latter checks if it is true or not. The data (I, D) in the Credential Centre are needed. The Verifier_role will not verify if the data (I, D) in the Credential centre are not correct. Then the Credential_role can revoke the anonymity of the Signer_role,

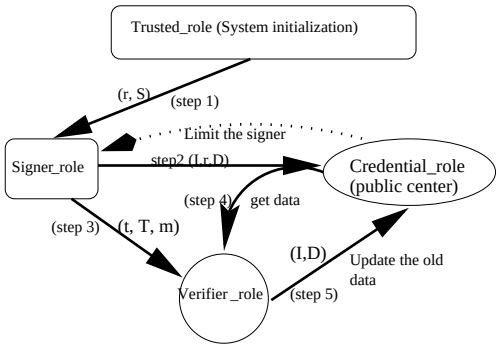

Figure 2: **Single signature scheme for ticket group_1**

and even find who is the user if it contacts the Trusted_role. In the final step, the Verifier_role sends the new data to update the old data in the Credential Centre if the signed message is true. This can be expressed as in Figure 2 detailed below.

The Trusted_role computes a public composite modulus $n = pq$ where factors are strong primes. The Trusted_role chooses also prime exponents e and d such that:

$$e * d = 1 \ (mod\, \phi(n)).$$

Where $\phi(n) = (p-1)(q-1)$. The pair (n, e) are made public, and d is kept secret by the Trusted Centre as the system key. The Trusted_role computes:

$$r = k^e \ (mod\, n), \quad S = k * I \ (mod\, n)$$

where $k \in_R Z_n$ ($a \in_R A$ means that the element a is selected randomly from the set A with uniform distribution). Then

$$S^e = r * I^e \ (mod\, n).$$

let $D = S^e \ (mod\, n)$. The Trusted_role secretly sends (r, S) to the Signer_role whose public identity is I. S will be used as the first signature key. Obviously, it is hard to compute S from D without system key d under the RSA assumption.

The Signer_role with the public key I sends (I, r, D) to the Credential_role, and the latter verifies the following equation:

$$D = r * I^e \ (mod\ n).$$

The data (I, r, D) is valid if the equation is successful, in which r and D are computed by the Trusted_role; otherwise the (I, r, D) is invalid. The Credential_role publishes in a public directory the pair (I, D) for the Signer_role with the public key I when the Signer_role is set up. The public data D will be changed each time by a Verifier_role when it verifies that the signature is valid.

4.2 The single signature scheme

The Verifier_role can access the public values n, e and the public pair (I, D) registered in the Credential Centre. The data D in the Credential Centre must be right, otherwise the Verifier_role can not verify if the signed message is true or not.

To express the general process of the single signature scheme, it is assumed that messages $m_1, m_2, ..., m_{l-1}$ $(l \geq 1)$ sent by $l-1$ users have already been signed by the Signer_role with public key I. The messages $m_1, m_2, ..., m_{l-1}$ $(l \geq 1)$ can indicate different service requirements. A user can get a valid ticket if the signature is right. The corresponding public key (I, D_{l-1}) $(D_0 = D)$ of the Signer_role is now registered in the public directory of the Credential Centre. The message m_l will be signed by the Signer_role using the secret key $S_{l-1}(S_0 = S)$. The Signer_role and the Verifier_role perform the following:

Input: (I, D_{l-1}, e, n),
Signer_role:
1. Picks $r_{l-1} \in_R Z_n$ and computes: $T_{l-1} = r^e_{l-1}(mod\, n)$.
2. Computes: $S_l = S_{l-1} * m_l \ (mod\ n)$, S_l will be used as the secret key by the Signer_role with public key I in the next signing operation.
3. Computes the Hashing value
$d_{l-1} = h(T_{l-1}, m_l) \ (mod\ n)$.
4. Computes the final witness
$t_{l-1} = r_{l-1} * (S_{l-1} * m_l)^{-d_{l-1}} \ (mod\ n)$.

Note: A ticket is the signature (t_{l-1}, T_{l-1}, m_l). The ticket will be sent to a service provider when the user wants to go shopping.

Verifier_role:
5. The Verifier_role gets (t_{l-1}, T_{l-1}, m_l) and knows (I, D_{l-1}), then checks that:

$$d_{l-1} = h(t^e_{l-1} * D^{d_{l-1}}_{l-1} * m_l^{e d_{l-1}} \ (mod\ n), m_l) \ (mod\ n).$$

It is easy to see that if the Signer_role follows the protocol, the equation will be valid. Indeed:

$$\begin{aligned} d_{l-1} &= h(T_{l-1}, m_l) \ (mod\ n). \\ T_{l-1} &= r^e_{l-1} \ (mod\ n) \\ &= (t_{l-1} * (S_{l-1} * m_l)^{d_{l-1}})^e \ (mod\ n) \\ &= (t^e_{l-1} * D^{d_{l-1}}_{l-1} * m_l^{e d_{l-1}}) \ (mod\ n). \end{aligned}$$

Using this protocol the Verifier_role is convinced with overwhelming probability that the Signer_role knows the secret key S_{l-1}. This S_{l-1} is used but not revealed at the end of the protocol.
6. The Verifier_role sends the new public pair (I, D_l) to the Credential_role in order to update the public directory (I, D_{l-1}), where

$$D_l = D_{l-1} * m_l^e \ (mod\ n) = S_l^e \ (mod\ n).$$

Remark: The Verifier_role must use the public data D in the Credential Centre when it checks whether the signed message is true or not. The signed message will be unavailable if the data D is changed, then the Credential_role can revoke the anonymity of the Signer_role.

4.3 Security analysis

This section analyses threats to the system from all parts, including the outside part which is the people who do not join the system. There are four roles in the scheme. They are the Signer_role, the Verifier_role, the Credential_role and the Trusted_role.

Outside: knows the public data (I, D_l). It is hard to compute the secret key S_l from D without system key d under the RSA assumption.

Verifier_role: knows (I, D_l) and (t_{l-1}, T_{l-1}, m_l). But no useful message can be obtained from (t_{l-1}, T_{l-1}, m_l) to identify the secret key, the Verifier_role knows no more information about the key than the outside.

Credential_role: can control the ability of the signer_role to sign messages. It knows only (I, D_l), so it too can not get the secret key.

Signer_role: knows the secret key and the ticket, but can not use the secret key S_l and the ticket twice. Use, for a second time, of the same secret key S_l to produce another ticket implies a second verification. If the previous verifier was honest, the public data in the Credential Centre would be updated and the second ticket would be rejected.

Trusted_role: knows the system key d, and can get the signer's key S_l. So the Trusted Centre must be trusted. Here the Trusted_role can be a judge.

The secret key S_l is not revealed at the end of the process and no secret information is revealed during the running of the system. The secret S_l is only dependent on the Trusted_role, and does not depend on the Credential_role. The security is also improved since the secret key S_l is changed once a message is signed.

4.4 The usage of tickets in ticket group_1

Tickets in group_1 are records which can be signatures, and the Credential_role can remember the records. Ticket t_4, for instance, is a signature of a user and can be bought by the user. The following analysis is only of ticket t_4 since the signature for tickets t_1, t_2 are similar to that of t_4.

When the user requests a ticket from the Credential Centre, the Credential_role will send a message including the current time, the requirement and the public key of the user etc to the user. As a Signer_role, the user signs the message and makes a ticket (t_{l-1}, T_{l-1}, m_l). The ticket (t_{l-1}, T_{l-1}, m_l) can be used to obtain a service from a service provider. As a Verifier_role, the service provider verifies if the ticket is valid or not, using the data (I, D_{l-1}) in the Credential Centre. Neither the service provider nor the Credential_role knows the user's identity. Only the Trusted_role can trace the user's identity from the public key I. After the service provider updates the data in the Credential Centre, everyone, including the user, can see the public data, then the charging bill will be clear. This is what consumers expect when they do business on the Internet. Finally, the Credential_role can send a bill to the user.

In this mechanism presented here, the user can also lend the ticket to others. He/She gives only the ticket (t_{l-1}, T_{l-1}, m_l) to others. This is very convenient for the mobile users. Furthermore, most computing in this scheme is done by the terminal side (the user or the provider); this can reduce the resource of the mobile system.

The new single signature scheme has the following properties:

1. It is anonymous for the signer.
2. The ticket can be transferred and its security is improved by the once-a-time key S_l.

However, this scheme only suits the ticket in ticket group_1. The problems of tickets t_3, t_5, t_6, t_7 can not be solved in the scheme of this section. A multi - signature scheme to solve these problems is explained in the next section.

5 Multi-signature scheme for ticket group_2

A multi-signature scheme will be described in this section for tickets t_3, t_5, t_6, t_7. The number of signers is not limited to two or three, but v signers. Then the scheme can also be used when some services are provided by many providers.

This is, in brief, the process of the multi-signature scheme. In the system initialization, the Trusted_role sends the private messages (r_i, S_i) to the

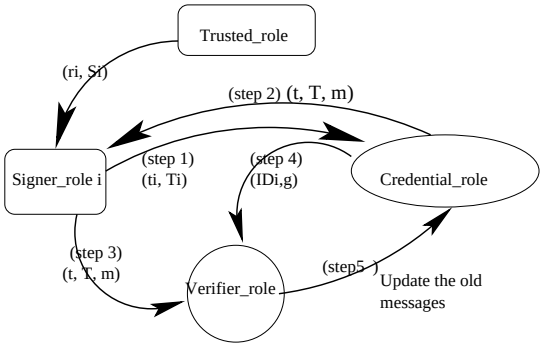

Figure 3: **Multi-signature scheme for ticket group_2**

Signer_roles with public key ID_i in the group (suppose v Signer_roles) when the Signer_roles are set up. The public key ID_i is similar to the public key I from the last section, and only the Trusted_role can trace whose public key is ID_i. In the second step, the Credential_role verifies if the data (ID_i, r_i, D_i) sent by the Signer_roles is valid or not. A vector $(ID_1, ID_2, ..., ID_v, g_1)$, as the group public key, will be put in the Credential_role, then the group can sign.

In the signature process, the Credential_role gets v pairs of data (t_i, T_i) from the Signer_roles with identity $ID_i (1 <= i <= v)$. In the next step, the Credential_role sends the signed message (t, T, m) to the Signer_role as a ticket. The ticket will be sent to the Verifier and the Verifier_role checks if it is true or not. The Verifier_role may not verify if the data g_1 in the Credential Centre is not right, and then the signed message is invalid and then the Credential Centre can revoke the anonymity of the Signer_roles. In the final step, the Verifier_role sends the new data to update the old data in the Credential Centre and then the Credential Centre can record it. This process is shown in Figure 3.

Suppose there are v Signer_roles $U_1, U_2, ..., U_v$ in the signature system to sign a message simultaneously, for tickets t_3, t_5, t_6, t_7, two or three signers are enough. The scheme can also cope with some other cases for example some services provided by many providers. Ticket t_6, for instance, is bound to the user and the service provider. Then the ticket will include the agreement between these two components. Only a basic multi - signature scheme is shown. Signers will be changed in order to suit different kinds of tickets.

5.1 Initialization of the system

Similar to the previous section, the pair (n, e) are made public, and d is kept secret by the Trusted Centre as the system key. The Signer_role U_i of the system has a public key ID_i which is produced by the Trusted Centre when the signer joins the system. The Trusted_role computes:

$$r_i = k_i^e \ (mod n), \quad S_i = k_i * ID_i \ (mod n)$$

$k_i \in_R Z_n$. Then $S_i^e = r_i * ID_i^e \ (mod n)$. Let $D_i = S_i^e \ (mod n)$. The Trusted_role secretly sends (r_i, S_i) to the Signer_role with the public key ID_i. S_i will be used by U_i as the first signature key. It is hard to compute S_i from ID_i without the system key d under the RSA assumption.

The Signer_role U_i sends (ID_i, r_i, D_i) to the Credential_role, and the latter verifies the following equation:

$$D_i = r_i * ID_i^e \ (mod \ n) \qquad (1)$$

The data (ID_i, r_i, D_i) is valid if the equation (1) is successful, in which r_i and D_i are computed by the Trusted Centre. Otherwise the (ID_i, r_i, D_i) are invalid. If the equation is successful for $i = 1, 2, ..., v$, the Credential_role computes a system public key:

$$g_1 = \prod_{i=1}^{v} D_i \ (mod\ n) = \prod_{i=1}^{v} S_i^e \ (mod\ n).$$

The Credential_role registers in a public directory a vector $(ID_1, ID_2, ..., ID_v, g_1)$ for Signer_roles $U_1, U_2, ..., U_v$. The data g_1 in it will be used and changed each time by a Verifier_role when a valid signature is done.

5.2 The Multi-signature scheme

When the Verifier_role accesses the system public key n, e and the public vector $(ID_1, ID_2, ..., ID_v, g_1)$ in the Credential Centre, the data g_1 must be correct, otherwise the signature is unavailable since the Verifier_role can not verify the signed message.

Assuming that the message $m_l (l > 0)$ will be signed by the Signer_roles $U_1, U_2, ..., U_v$, z is a public prime number which is known to v Signer_roles and it will be used in the new multi-signature scheme.

Step 1. The Signer_role $U_i (i = 1, 2, ..., v)$ uses the secret key $S_{i\,l-1}$ $(S_i = S_{i0})$ to sign the message m_l .

Input:(ID_i, D_i, e, n),
Signer_role:
1.1 Picks $r_{il} \in_R Z_n$ and computes: $T_{il} = r_{il}^e (mod n)$.
1.2 Computes: $S_{il} = S_{i\,l-1} * m_l \ (mod n)$.
S_{il} will be used as the secret key by U_i in the next signing operation.
1.3 Computes: $t_{il} = r_{il} * (S_{i\,l-1} * m_l)^z \ (mod\ n)$.
1.4 Sends the pair (t_{il}, T_{il}) to the Credential_role.

The Credential_role can now to produce a ticket.

Credential_role:
Step 2. The Credential_role computes:

$$t_l = \prod_{il=1}^{v} t_{il} \ (mod\ n), \quad T_l = \prod_{il=1}^{v} T_{il} \ (mod\ n)$$

and sends (t_l, T_l, m_l) to the User. This is the ticket for the user.

The user will send the ticket to a service provider to ask for a purchase. The service provider, as a verifier, will verify the ticket. The verifier will follow the next steps when the ticket is received.

Verifier_role:
Step 3. The Verifier_role knows the public data $(ID_1, ID_2, ..., ID_v, g_l)$ in the Credential Centre and data (t_l, T_l, m_l), checks that:

$$T_l = t_l^e * g_l^{-z} * m_l^{-zve} \ (mod\ n) \qquad (2)$$

It is easy to see that if the Signer_role and the Credential_role follow the steps, the equation (2) will be valid. Indeed,

$$\begin{aligned} T_l &= \prod_{il=1}^{v} T_{il} \ (mod\ n) \\ &= \prod_{il=1}^{v} t_{il}^e * (S_{i\,l-1} * m_l)^{-ze} \ (mod\ n) \\ &= t_1^e * g_1^{-z} * m_l^{-zve} \ (mod\ n). \end{aligned}$$

Step 4. The Verifier_role sends the new public vector $(ID_1, ID_2, ..., ID_v, g_{l+1})$ to the Credential Centre in order to update the public directory $(ID_1, ID_2, ..., ID_v, g_l)$, where

$$g_{l+1} = \prod_{i=1}^{v} (S_{i\,l-1} * m_l)^e = g_l * m_l^{ve} \ (mod\ n).$$

Remark: The signed message in the multi-signature scheme will be invalid if the data g_l is changed. Then the Credential_role can revoke the ability to sign messages of the Signer_roles.

5.3 Security analysis

The security analysis is similar to the last section. This is the analysis of the attacks from the five parts.

Outside: knows the public data $(ID_1, ..., ID_v, g_l)$. They are not able to get any information about the secret key S_{il} from g_l since there is no relation between these two data.

Verifier_role: knows $(ID_1, ..., ID_v, g_l)$ and (t_l, T_l, m_l). But no useful message can be gathered from (t_l, T_l, m_l) to obtain the secret key S_{il}. The Verifier_role, likes the Outside, can not get the secret key.

Credential_role: can revoke the anonymity of the users since it can control the ability to sign messages by the Signer_roles. It knows only as much as the Outside does, it can not get the secret key either.

Signer_roles: Whether the signed message is valid or not depends on the equation (2). If some Signer_roles use their keys twice, the equation (2) can not succeed because the data in the Credential Centre has been changed after the last signature. This means the ticket can not be used twice. Furthermore, if a signer misbehaves many times, the Credential Centre can contact the Trusted Centre to find who the signer is.

Trusted_role: knows the system secret key. It has to be trusted and can be a judge.

The secret key S_{il} is not revealed at the end of the scheme and no secret information is revealed during the running of the system. The security of the system is also enhanced by the secret key S_{il} being changed once a message is signed.

5.4 Usage of tickets in ticket group_2

The usage of tickets in ticket group_2, ticket t_6, for instance, binds a user and providers and it should be an agreement between the user and the providers. The usages of other tickets are similar to that of the ticket t_6. So only the ticket t_6 is analysed and the other tickets are omitted.

When the user requests a ticket t_6 from the Credential Centre, the Credential_role will send the user's requirement to the service providers. The Credential_role will issue a public key for the user and the service providers if the service providers agree to provide the service. The Credential_role sends a message including the current time, the requirement and the agreements of the service providers and so on to the user and the service providers. As Signer_roles, the user and the service providers use their secret key to sign this message, and then return the data (t_{il}, T_{il}) to the Credential Centre. The Credential_role makes a ticket (t_l, T_l, m_l). The ticket (t_l, T_l, m_l) can be used to the service provider. As a Verifier_role, the service provider verifies if the ticket is valid using the public data $(ID_1, ..., ID_v, g_l)$ in the Credential Centre.

Neither the service provider nor the Credential_role knows the user's real identity. Only the Trusted Centre can trace the user's identity from the public key ID_i. After the service provider updates the data in the Credential Centre, the user can see a clear charging bill in the Credential Centre, which is the expectation of the mobile consumers when they do business on the Internet. Finally, the Credential_role can send a bill to the user.

If a ticket is used twice, there are two signatures by the user. The providers will find that the last signature is invalid since the data in the Credential Centre has been changed. The new multi-signature scheme has the following features:

1. It is anonymous for the user.
2. The ticket can be lent to others.
3. The security of the system is improved very much since the secret key S_{il} is used only once.

Remark: This scheme can not only be used by mobile users but also by many other Internet users. The Credential Centre can be decentralized for increased numbers of users. Furthermore, the Trusted Centre can be a judge when users misbehave.

6 Related work

There is some related work on this topic of mobile communication security such as [Horn and Preneel, 1998, Martin et al., 1998, Lubinski and Heuer, 2000, Wilhelm et al., 1998]. Two approaches, similar to the one described in this paper, using ticket access for the third generation mobile system (UMTS) were presented by Horn and Preneel in 1998, and Martin etc in 1998 [Horn and Preneel, 1998, Martin et al., 1998]. In these solutions, the users obtain tokens from the UMTS service providers, who act as brokers. The tokens are then handed by the users to the value-added service providers as a proof of their credit worthiness. The settlements between the value-added service providers and the brokers are then accomplished off-line. The UMTS service providers will collect the billing information from all the value-added service providers accessed by given users and integrate them in a single bill addressed to the users. These mechanisms are a very significant improvement over the ones prevailing in the second generation mobile systems. However, they have the weakness of not providing anonymity to the users.

Other similar approaches for ticket-based service access are described by Pratel and Crowcroft in 1997, and Buttyan and Hubaux in 1999[Pratel and Crowcroft, 1997, Buttyan and Hubaux, 1999]. In [Pratel and Crowcroft, 1997], tickets are prepaid and can only be used with the service provider that issued them (according to the categorisation described here, tickets are type t_7 and require a special model). Anonymity can be provided for all services for which it is deemed appropriate. In [Buttyan and Hubaux, 1999], tickets are issued by customer care agents and can not be transferred to others. This approach only solves the case of ticket t_4. These two methods only solve the particular mobile access problems.

In the proposed ticket-based service access scheme, the users are anonymous since their private information is not revealed to service providers and the Credential Centre. It is a global solution for all kinds of mobile services and the tickets can be lent to others, which will be very convenient and useful for mobile environment users. The users can see a clear record of charges in the Credential Centre and identify any problems in the bill. Furthermore, the scheme can save mobile system resources, since most computing is done by users or service providers.

7 Conclusion

Mobile communication systems are becoming extremely popular, which makes the provision of services to mobile users an attractive business area. This can be regarded as a special form of ecommerce, where users buy services instead of products from service providers via the network. Some users prefer high security and clear bill charging.

In this paper, a ticket-based service access scheme for mobile users is proposed. First, the Credential Centre issues tickets for the users. Second, a ticket-based mechanism is implemented allowing the user to remunerate the service providers. Tickets provide a flexible and scalable mechanism for mobile access. The main contributions of this paper are that the scheme is a global ticket-based solution for mobile access service, an anonymous and dynamic system, and new users and new service providers can join at anytime. It is also scalable and users can check charges at anytime.

References

[Beimel et al., 1999] Beimel A., Ishai Y., Kushilevitz E., and Malkin T.(1999). One-way functions are essential for single server private information retrieval. In *Proc. of the 31st Annu. ACM Symp. on the Theory of Computing (STOC)*, pages 89–98.

[Bellare et al., 1996] Bellare M., Canetti R., and Krawczyk H. (1996). Pseudorandom functions revisited: The cascade construction and its concrete security. Extended abstract. In *37th Annual Symposium on the Foundations of Computer Science*, IEEE.

[Buttyan and Hubaux, 1999] Buttyan L. and Hubaux J.(1999). Accountable anonymous access to services in mobile communication systems. *Symposium on Reliable Distributed Systems*, pages 384–389.

[Chaum, 1981] Chaum D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM* , 24(2): 84–88,

[Frankel et al., 1995] Frankel Y., Herzberg A., Karger P., Krawczyk H., Kunzinger C. and Yung M.(1995). Security issues in a CDPD wireless network. *IEEE Personal Communications.*

[Horn and Preneel, 1998] Horn G. and Preneel B.(1998). Authentication and payment in future mobile systems. In Quisquater J., etc, editors, *Proceedings European Symposium on Research in Computer Security*, Lecture Notes in Computer Science, volume 1485, pages 277–293, Springer-Verlag.

[Lubinski, 1998] Lubinski A.(1998). Security issues in mobile database access. In *Proceedings of the IFIP WG 11.3 Twelfth Int. Conf. on Database Security.*

[Lubinski, 2000] Lubinski A.(2000). Database security meets mobile requirements. In *Proceedings International Symposium on Database Technology Software Engineering, WEB and Cooperative Systems*, Baden.

[Lubinski and Heuer, 2000] Lubinski A. and Heuer A.(2000). Configured replication for mobile applications. *Rostocker Informatik Berichte*, volume 24, pages 101–112.

[Martin et al., 1998] Martin K., Preneel B., Mitchell C., Hitz H., Poliakova A., and Howard P.(1998). Secure billing for mobile information services in UMTS. In *Proceedings 5th International Conference on Intelligence in Services and Networks'98* Lecture Notes in Computer Science, volume 1430, pages 535–548, Springer-Verlag.

[Mehrotra, 1997] Mehrotra A.(1997). *GSM System Engineering.* Norwood, Artech House.

[Mehrotra and Golding, 1998] Mehrotra A. and Golding L.(1998). Mobility and security management in the GSM system and some proposed future improvements. In *Proceedings of IEEE*, 86(7).

[Pratel and Crowcroft, 1997] Pratel B. and Crowcroft J.(1997). Ticket based service access for the mobile user. In *Proceedings of MobiCom: International Conference on Mobile Computing and Networking*, pages 223–232, Budapest, Hungary.

[Rivest et al., 1978] Rivest R. L., Shamir A., and Adleman L. M.(1978). A method for obtaining digital signatures and public-Key cryptosystems. *Communications of the ACM*, 21(2):120–126.

[Stinson, 1995] Stinson D. R.(1995). *Cryptography: Theory and Practice.* Boca Raton, CRC Press.

[Waleffe and Quisquater, 1990] Waleffe D. D. and Quisquater J. J.(1990). Better login protocols for computer networks. In Vandewalle J. edtor, *Proceedings European Symposium on Research in Computer Security*, Lecture Notes in Computer Science, Toulouse, France, Springer-Verlag.

[Wang and Zhang, 2000] Wang H. and Zhang Y.(2000). A protocol for untraceable electronic cash. In Lu H. and Zhou A., editors, *Proceedings of the First International Conference on Web-Age Information Management*, Lecture Notes in Computer Science, volume 1846, pages 189–197, Shanghai, China, Springer-Verlag.

[Wang and Zhang, 2001] Wang H. and Zhang Y.(2001). Untraceable off-line electronic cash flow in e-Commerce. In *Proceedings of the 24th Australian computer science conference ACSC2001*, pages 191–198, GoldCoast, Australia, IEEE Computer Society.

[Wang et al., 2001] Wang H., Cao J. and Zhang Y. (2001). A consumer anonymity scalable payment scheme with role based access control. In *2nd International Conference on Web Information Systems Engineering*, Kyoto, Japan, IEEE Computer Society.

[Wang et al., 2002] Wang H., Cao J. and Yahico K.(2002). Building a consumer anonymity scalable payment protocol for the Internet purchases. In *12th International Workshop on Research Issues on Data Engineering: Engineering E-Commerce/E-Business Systems*, San Jose, USA.

[Wilhelm et al., 1998] Wilhelm U. Staamann S. and Buttyan L.(1999). On the problem of trust in mobile agent systems. In *IEEE Network and Distributed Systems Security Symposium*, pages 11–13, San Diego, CA.