Ticket-based mobile commerce system and its implementation

Hua Wang
Department of Maths & Computing
University of Southern Queensland
Toowoomba QLD 4350 Australia
wang@usq.edu.au

Xiaodi Huang
School of Maths, Stati & Computer Sci
University of New England
Armidale NSW 2351 Australia
xhuang@mcs.une.edu.au

Goutham Reddy Dodda
Department of Maths & Computing
University of Southern Queensland
Toowoomba QLD 4350 Australia
dodda@usq.edu.au

ABSTRACT

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

This paper presents a solution for all kinds of mobile services through short message service (SMS) systems and a ticket-based service access model that allows anonymous service usage in mobile applications. A service provider can avoid roaming to multiple service domains, only contacting the Credential Centre in the model to check a user's certification. The user can preserve anonymity and read a clear record of charges in the Credential Centre at anytime, and the identity of misbehaving users can be revealed by a Trusted Centre. Furthermore, the solution has been demonstrated by the implementation with SMS and RS232.

Categories and Subject Descriptors: H.4.3 [Information Systems Applications]: Communications Applications; H.3.4 [Information Storage and Retrieval]: Systems and Software

General Terms: Algorithms, Design

Keywords: Mobile commerce, Signature, SMS.

1. INTRODUCTION

The number of mobile phone users are more than two billion in the world and it is still increasing. Mobile computing and communication is becoming an important factor in our daily life. With wireless computing and communication, security and privacy issues are more critical [9]. 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 [6, 4, 13]. All of them lack some flexibility in security management. The Global system for mobile communications [6], for example, provided mechanisms for user authentication as well as integrity and confidentiality, including protection of information exchanged between the mobile terminal and the fixed network. It provided only limited privacy protection for users by hiding their real identities from eavesdroppers on the radio interface [7]. Gandon and Sadeh described a semantic e-wallet [4] which aimed at supporting automated identification and access of personal resources, each represented as a semantic web service. A key objective was to provide a semantic web environment for open access to a user's contextual resources, thereby reducing the costs associated with the development and maintenance of context-aware applications. However, there are some other issues and problems which need to be addressed such as Global solutions, SMS implementation, Clear charging, Trustiness and Scalability.

In the future, mobile commerce systems should provide total solutions for all kinds of mobile services, guarantee higher levels of security than current systems, and implement with a convenient mobile application such as short message service (SMS). 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, mobile service systems should also require authentication of the service provider to the user and guarantee higher levels of privacy [10, 12]. Furthermore, clear billing has to be ensured.

In this paper, a new approach to address the above mentioned problems is proposed. This approach involves a Trusted Credential Centre (*TCC*), a Trusted Authentication and Registration Centre (*TARC*) (via *UDDI*) and a secure ticket based mechanism for service access. Users and service providers register with the *TARC* and are authenticated. Services are described in the *TCC* and Service Provider by WSDL [3].

Q2SWinet'06, October 2, 2006, Torremolinos, Malaga, Spain.

Based on authentication, tickets are issued by the TCC to the users and transferred using SOAP [1]. Tickets carry authorization information needed for the requested services. The main idea is illustrated in Figure 1.

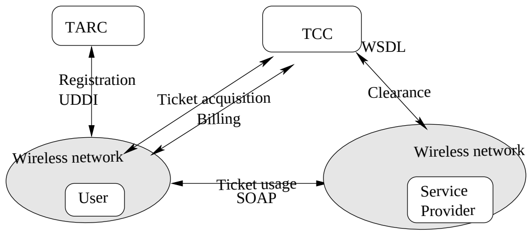

Figure 1: M-service Model

This paper is organized as follows: in section 2, ticket types for mobile commerce are introduced. The single signature scheme for ticket group_1 and the multi-signature scheme for ticket group_2 are discussed insection 3. The system implementation demonstration with SMS is described in section 4 while related work is given in section 5. Finally the conclusions are in section 6.

2. TICKET TYPES

There are several advantages in using tickets for accessing services such as flexibility, scalability, privacy and transfer [2].

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 $'\Theta'$ means that the corresponding entity, user, service provider or service is bound by the ticket, while $'-'$ means that it is not.

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 are explained. The ticket t_0 does not require discussion since it is a general case of e-payment methods.

3. ALGORITHMS FOR THE TWO GROUPS

3.1 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 TCC issues 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 in the $TARC$ 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 $TARC$. 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 a service provider and service separately but not a user.

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.

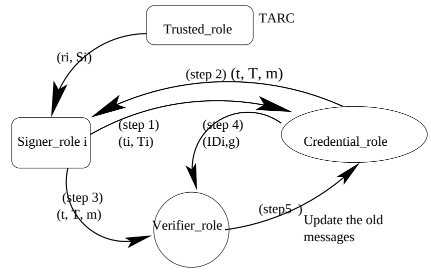

Figure 2: Multi-signature scheme for ticket group_2

3.2 Multi-signature scheme for ticket group_2

A multi-signature scheme is 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 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, is 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 user as a ticket. The ticket is 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 TCC is not right, and then the signed message is invalid.

the TCC can revoke the anonymity of the Signer_roles if it contacts to the $TARC$. In the final step, the Verifier_role sends the new data to update the old data in the TCC and then the TCC can record it. This process is shown in Figure 2.

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 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 includes the agreement between these two components. Only a basic multi - signature scheme is shown. Signers are changed in order to suit different kinds of tickets.

4. IMPLEMENTATION WITH SMS

This section presents the implementation of the mobile service system with SMS and RS232. SMS is a service available on most digital mobile phones that permits the sending of short messages between mobile phones, other handheld devices and even landline telephones. RS232 is a standard for serial binary data interconnection between a data terminal equipment and a data communication equipment, and it is commonly used in computer serial ports. Figure 3 shows the implementation framework.

To get the system working, we need:

1. Windows XP operating system,
2. .Net Framework 1.1 (Minimum),
3. GSM phones with AT+C modem command support,
4. Supporting data cable.

A mobile user (User1, User2, etc) has to register with the system by sending a message to a mobile phone in My System in Figure 3 before applying a ticket. The mobile phone connect to the server through RS232. This is an automated system, no human interaction is needed. When the system is set to auto mode the system is ready to send, receive and process messages accordingly. The user's public information (I, D) are in a public directory. For simplicity, we suppose the system initialization is: $p = 11, q = 23$ and $n = 253$, $e = 7, d = 63$ such that $e * d = 1\,(mod\,220)$. Here $220 = (p-1)(q-1)$. For simplicity, we suppose the hash function is $H(x, y) = 3^x * 5^y$.

Let us assume that a user I is $I = 25$. Randomly selecting $k = 4$ then $(r, S) = (192, 100)\,(mod\,253)$, computes $D = 163\,(mod\,253)$. The Trusted_role sends $(r, S) = (192, 100)$ to the user with $I = 25$.

Suppose the first time the user needs to sign the message $m_1 = 9$ which includes the service information, etc. The user sends $(I, r, D) = (25, 192, 163)$ to the Credential_role, the Credential_role verifies whether $D = r * I^e$ or not. $(I, D) = (25, 163)$ is published by the TCC.

When the user requires a movies ticket, the system creates a ticket following the signature procedures described in the previous sections. The Verifier_role must get the public pair $(I, D_0) = (25, 163)$ in the TCC when s/he verifies whether the ticket is available or not. The ticket is unavailable if the public pair $(25, 163)$ is changed. After the Verifier_role checked the availability of the ticket, he/she sends new data to the TCC to update $(25, 163)$. The implementation of the system is shown in Figure 4.

5. RELATED WORK

There is some related work on this topic of mobile communication security such as [5, 11, 15]. For example, a ticket-based service access are described by Pratel and Crowcroft in 1997, and Buttyan and Hubaux in 1999 [8, 2]. In [8], 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 [2], 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 TCC. It is a global solution for all kinds of mobile services and the tickets can be lent to others, which is very convenient and useful for mobile environment users. The users can see a clear record of charges in the TCC 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.

6. CONCLUSION

In this paper, a ticket-based mobile service system for mobile users is proposed and also implemented with SMS system. First, the TCC 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 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.

7. REFERENCES

[1] D. Box. *Simple Object Access Protocol (SOAP) 1.1*. World Wide Web Consortium (W3C), Cambridge, MA, USA, 2000.

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

[3] R. Chinnici, M. Gudgin, J. Moreau, and S. Weerawarana. *Web Services Description Language (WSDL) 1.2*. World Wide Web Consortium (W3C), Cambridge, MA, USA, 2002.

[4] F. Gandon and N. Sadeh. semantic web technologies to reconcile privacy and context awareness. *Web Semantics Journal*, 1(3), 2004.

[5] A. Lubinski and A. Heuer. Configured replication for mobile applications. *Rostocker informatik berichte*, 24:101–112, 2000.

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

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

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

[9] N. M. Sadeh. *m-Commerce: Technologies, Services and Business Models*. Wiley, 2002.

[10] H. Wang, J. Cao, and K. Yahico. Building a consumer anonymity scalable payment protocol for the internet purchases. In *The 12th International Workshop on Research Issues on Data Engineering: Engineering E-Commerce/E-Business Systems*, pages 159–168, San Jose, USA, 2002.

[11] H. Wang, J. Cao, and Y. Zhang. An electronic payment scheme and its rbac management. *Concurrent Engineering:*

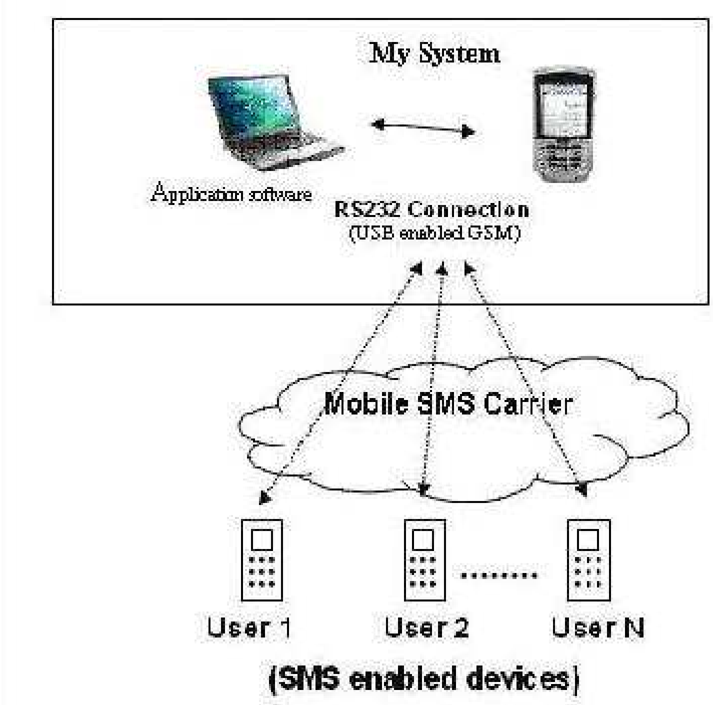

Figure 3: Implementation framework

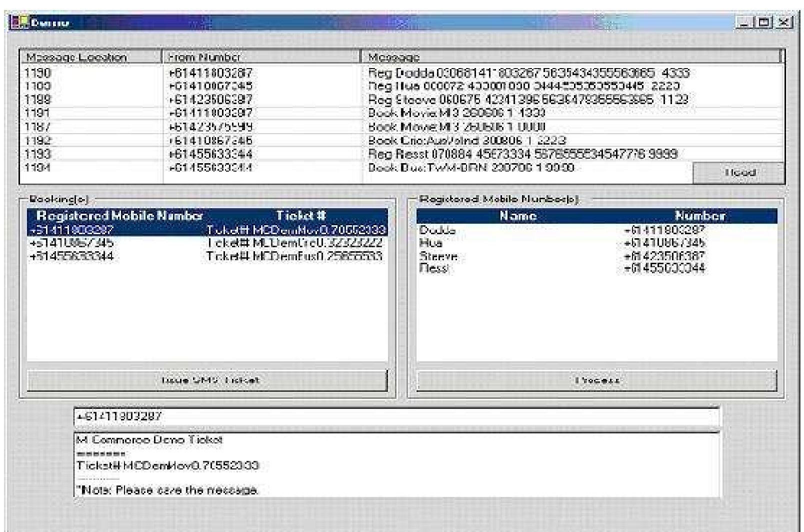

Figure 4: Mobile service system implementation

Research and Application Journal, 12(3):247–257, 2004.

[12] H. Wang, J. Cao, and Y. Zhang. A flexible payment scheme and its role based access control. *IEEE Transactions on Knowledge and Data Engineering*, 17(3):425–436, 2005.

[13] H. Wang and Y. Zhang. Untraceable off-line electronic cash flow in e-commerce. In *The 24th Australian computer science conference*, pages 191–198, GoldCoast, Australia, 2001.

[14] H. Wang, Y. Zhang, J. Cao, and V. Varadharajan. Achieving secure and flexible m-services through tickets. *IEEE Transactions on Systems, Man, and Cybernetics, Part A, Special issue on M-Services*, 33:697–708, 2003.

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