Winter 12-4-2009

Secure and Transferable Mobile Ticketing Using Digital Rights Managements

Sue-Chen Hsueh

Shih-Chi Chuang

SECURE AND TRANSFERABLE MOBILE TICKETING USING DIGITAL RIGHTS MANAGEMENTS

Sue-Chen Hsueh[1], Shih-Chi Chuang[2]
Department of Information Management Chaoyang University of Technology, Taiwan
[1]schsueh@cyut.edu.tw; [2]s9714619@cyut.edu tw

Abstract

The increasingly matured mobile commerce enriches our daily lives. Mobile ticketing, a process that allows consumers to order, make payment, acquire, and authenticate tickets using their mobile phones, will become popular since it can be conducted from anywhere and at anytime. In addition to the convenience of use, the fabrication and distribution costs of traditional paper-tickets can be greatly reduced with mobile tickets. Many applications, such as traffic tickets, concert tickets, movie tickets, and so on, may take the advantages of mobile ticketing. Such tickets, in their paper-forms, can be transferred to anyone before use since no specific identity is recorded in these tickets. Nevertheless, current schemes restrict mobile tickets to be non-transferable because the transferring will result in the tickets being invalidated. To overcome the non-transferability problem, we use the idea of digital rights managements to separate the content and the usage-rules of mobile tickets, and propose a transferrable mobile ticketing scheme. The usage-rule, i.e. the rights object of the ticket, registers the ticket identification and a hashed number comprising an issuer's random number and the International Mobile Equipment Identity (IMEI) of the ticket owner. The rights object is independently issued by a trusted third party. When a ticket is transferred, the issuer will be notified and he will modify the rights object with a new hash value, computed from a new random number and the IMEI of the new owner who receives the transferred ticket. Therefore, mobile tickets are secured and transferrable in our proposed mobile ticketing scheme.

Keywords: Mobile Commerce, Mobile Ticket, Information Security, Digital Rights Management

Introduction

Ticket ordering today is evolving from direct sales from physical stores to online ordering via Internet [1]. Consumers may easily inquire the related information of tickets and order tickets using the Internet. Ticket issuers, viewing this trend, have made possible online ordering of their products through Internet. Example applications such as traffic tickets, concert tickets, movie tickets, and so on [2] [3], all take the advantages of ticketing online.

E-tickets transactions have to provide many application services that allow consumers to order tickets. The E-ticket enables consumers to efficiently collect ticket information and to reduce the time cost of lining up. Nevertheless, E-tickets are restricted to be acquired in fixed locations, thereby inducing the poor portability and low usage rate. Benefiting from the mature development of the mobile environment, mobile users may connect to Internet with the handheld devices wirelessly and obtain information real time [4]. Moreover, mobile ticket services provide not only convenient but also flexible transactions to the mobile users. In addition to order and acquire tickets, mobile users are flexible to transfer tickets in case of traffic accidents [5] [6], potential lateness or absence. The loss of the consumer can be minimized since the ownerships of tickets can now be transferred anytime before the expiration of the tickets.

A mobile ticket is a valuable digital product so that it should be protected against tampering, forging, and other security issues in the mobile phone. Therefore, this paper aims to design a mobile ticket transaction protocol of necessary security, emphasizing the transferability of mobile tickets. A mobile user obtains a ticket, accompanied with a hash value computed with the IMEI and a random number from the ticket issuer. Thus, the security of the ticket can be protected while the user may effectively own the rights of the ticket. To protect the legitimacy of ownership and un-forge-ability of the mobile ticket, the Right Object (RO) that used in the digital rights management is independently issued by the trusted right issuer. Hence, trading can be performed so that the owner's right is protected. Therefore, mobile users may have the confidence of using mobile ticketing in the secure mobile environment.

Related Work

From some of the information security issues that deliver mobile tickets to the mobile user through the handheld device, such as information has been intercepted, tampered and forged. Hence, we use the

encryption technology or the RO of way to protect the rights of mobile users. There have two technologies were used to protect mobile tickets.

First, Moni Naor et al. used the Visual Secret Sharing (VSS) method [7]. The third party will generate a pair of ticket, X-part and Y-part, and the user own X-part, the issuer own Y-part. When the users want to acquire the ticket, the issuer generates a password that combine X-part and Y-part. In this paper, we use the X, Y-part of concept. The mobile user delivers a portion of ticket information and the IMEI to the exchange server, and the exchange server can be verifies the part of own of ticket issuer. If the all part were correct, the mobile user will be obtain a mobile ticket.

Another, Kazuo Matsuyama et al. proposed the architecture of ownership [8]. Users have to transfer the owner to others from the website of third party. The third party transfer the ownership to the others account. But the third party do not guaranteed or recognized the validity of tickets.

In this paper, we proposed the RO concept in the DRM, it protect the security of tickets. The RO records the ownership of ticket and issuers, and open-card that writes the valid period by RO issuer. Therefore, the RO can be prevents a malicious user to do anything, such as tamper and forgery of tickets. We use the main technologies to protect ticket, namely asymmetric encryption and hash function.

Mobile Ticket

The method use mobile devices as a communication platform for mobile users. The mobile ticket allows consumer to order, acquire, or transmission of the tickets using their mobile phones, will enhance the portability and convenience. Combination of the International Mobile Equipment Identity (IMEI) as the mobile user's identification, can be to prevent the malicious forgery and tampering with the ticket. Not only use of one-time password to ensure the mobile user's identification, but also protect the ticket content using the security technology, can be to achieve the data integrity. We protect the owner using the Right Object (RO) in the mobile ticket. When you want to transfer the mobile ticket to others, the RO will be verified that re-create a new RO, it prevent amount of the mobile ticket be transferred. In this session, we introduce the system architecture, the process that allows consumers to order, acquire, and transfer tickets. Separately illustrate order, acquire, (Figure 1) and transfer phases (Figure 2) of the process of functional and security.

System Architecture

The architecture consists of Mobile User, Ticket Issuer, Right Object (RO) Issuer and Exchange Server, and the main of a process that allows the order, acquire, and transfer tickets. First phase, the way that mobile users use through the wireless by the mobile device, and order tickets toward the ticket issuer. The ticket issuer generates a proof of purchase that the demands of the mobile user and deliver for the mobile user. Second phase, the proof of purchase

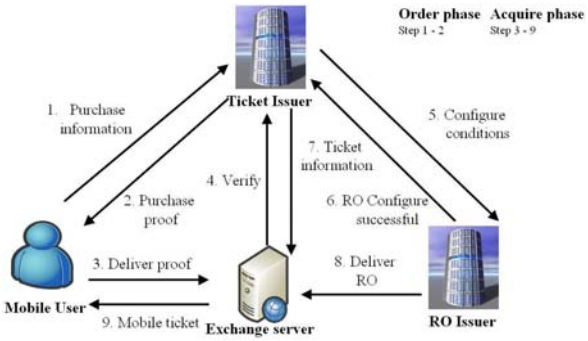

Figure 1: Mobile ticket system architecture

is sent to the exchange server when the mobile user wants to use the mobile ticket. From the exchange server, verify that the legitimate mobile users, and deliver relevant information to the ticket issuer. The ticket issuer delivered the demand list to the RO issuer, the RO issuer configures conditions of the RO, i.e. the effective date and transferable constraints of the RO and deliver to the exchange server. When the ticket issuer receives the return message, the ticket issuer delivers the ticket information to the exchange server. And the exchange server generates a mobile ticket that combines the ticket information and RO.

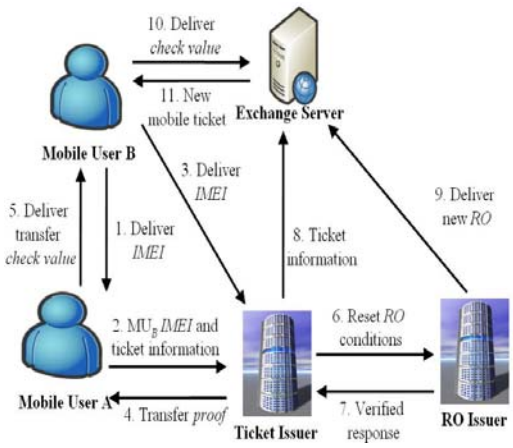

Figure 2: Mobile ticket transfer architecture

When the mobile user A want to send to the mobile user B, and the mobile user B must be change the own IMEI into the authentication code. Separately deliver the IMEI and the authentication code to the mobile ticket and the mobile user A. when the user A receives the authentication code, it combines the mobile ticket and deliver to the ticket issuer. The ticket issuer confirms the identity of the mobile user B. When the identity is correct, the RO issuer generates a new RO that updated the owner and date and delivered to the exchange server. The exchange server generates a new mobile ticket that

combines the ticket and the new RO, and delivers to the mobile user B.

Table 1: Notations

Notation	Statement	Notation	Statement
T_i	Ticket，i=0,1,…,n	*proof*	Purchase proof
OI	Order information	*PID*	Proof number
date	Purchase data	R_i	Random number，i=0,1,…,n
K_{TS}	Between the TI and ES symmetric encryption key	K_{TR}	Between the TI and RI symmetric encryption key
K_{RS}	Between the RI and ES symmetric encryption key	*valid period*	Proof of purchase of the valid period
UID	User number	pw_i	One time password, i=0,1,…,n
check	Confirm the mobile ticket	*TC*	Transferable certificate
MAC	Message Authentication Code	*CID*	Certificate number
success	Success message	*content*	Purchase items
now	Now of time	*Req*	Request message
Record	Record in the database	*Response*	Response message

Order Phase

Following order of the steps (Figure 3):

Step1: The mobile user selected conditions of the ticket before order a mobile ticket. The conditions contain ticket type, date, and transferable, will be formed by order information (*OI*).

Step2: After the ticket issuer receives the OI, the ticket issuer generates a ticket number (*TID*) and contains within the confirm message (*Req*).

Step3: When the content is confirmed, the ticket issuer will be generated a responsive message (*Response*) that combined the *IMEI* and *TID*.

Step4: When the responsive message is received, the ticket issuer will be modified the *IMEI* with a hash value as the user ID (*UID*) and recorded in the database. The ticket issuer generates a purchase proof that combines the *OI* and UID_A. To overcome the security problem, we use the idea of symmetric encryption to protect the purchase proof and the one time password.

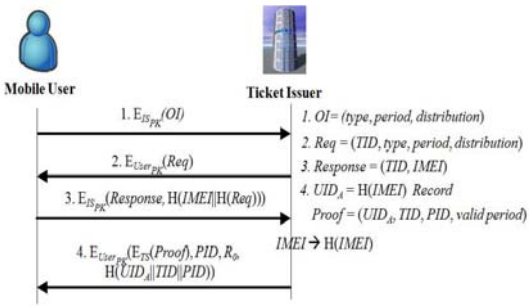

Figure 3: Order phase

Acquire Phase

Following transfer of the steps (Figure 4, 5):

Step1: Mobile users want to acquire the mobile ticket that deliver the purchase proof to the exchange server.

Step2: When the purchase proof is confirmed, the exchange server delivers the proof information to the ticket issuer.

Step3: The ticket issuer takes out the conditions from the database using the *TID*, and delivered to configure conditions by RO issuer.

Step4: When the message is confirmed, the RO issuer submits the success message that notified the ticket issuer will be delivered the ticket information to the exchange server.

Step5: The ticket issuer delivers the ticket information and this one time password that protects message at each time, and next password using the public key of the mobile user ($E_{User_{PK}}$).

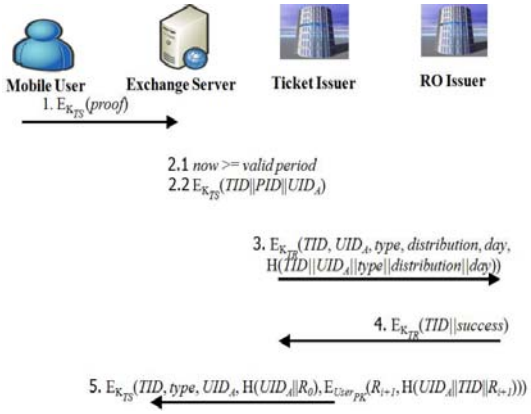

Figure 4: Acquire phase (a)

Step6: The RO issuer generates a RO that configured conditions and valid period, and delivered to the exchange server.

Step7: The exchange server request to the mobile user.

Step8: The mobile user sends the password (pw_0) to the exchange server, and verified the password.

Step9: The exchange server generates a mobile ticket (T_0) that combined the ticket information and the RO and delivers the next one time password to the mobile user. The mobile user will be verify the mobile ticket, computed the *IMEI* and next one time (pw_{i+1}) with a hash value.

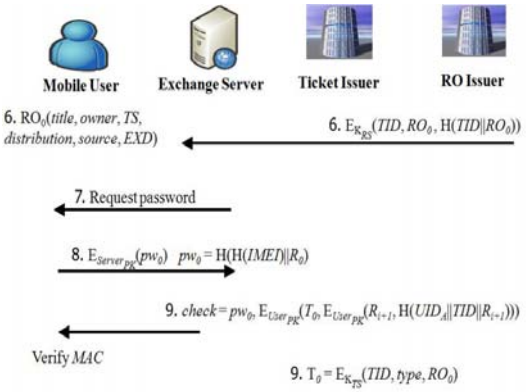

Figure 5: Acquire phase (b)

Transfer Phase

When the mobile user A does not want to useable and effective of the mobile ticket, will be transferred the mobile ticket and changed owner to the mobile user B. Following transfer of the steps (Figure 6, 7):

Step1: The mobile user B computes the *IMEI* with a hash value, it can as a proof of the validation.

Step2: The mobile user A delivers the mobile ticket (T_0), $H(IMEI)_B$, and one time password (pw_{i+1}) to the ticket issuer and changes the owner. And the ticket issuer can be verified one time password.

Step3: The mobile user B delivers the IMEI to the ticket issuer and the ticket issuer can be checked the IMEI.

Step4: The ticket issuer generates a transferable certificate (*TC*) that will be redeemed a new ticket.

Step5: The mobile user A delivers the check value in the transferable certificate to the mobile user B.

Step6: The ticket issuer takes out the RO and delivered to the RO issuer, and verified the RO and created a new RO.

Step7: To Verify confirmed and return message to the ticket issuer.

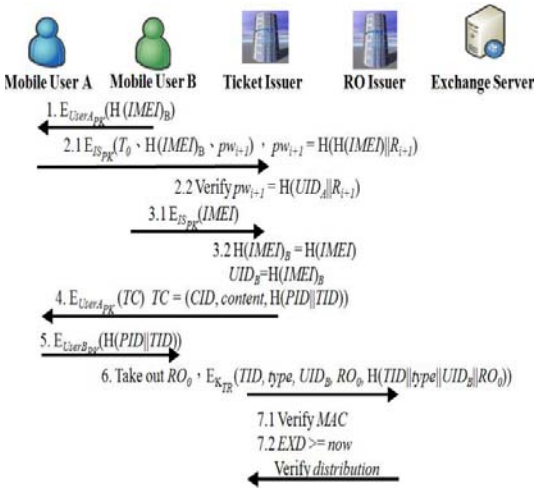

Figure 6: Transfer phase (a)

Step8: The ticket issuer delivers the new ticket information and one time password (R_{i+2}) to the exchange server.

Step9: The RO issuer delivers the RO after he updates it.

Step10: The exchange server receives and verified the check value.

Step11: When the check value is confirmed, the exchange server generates a new mobile ticket that combines the ticket information and the new RO. The mobile user B will be verify the mobile ticket, computed the *IMEI* and next one time (pw_{i+2}) with a hash value.

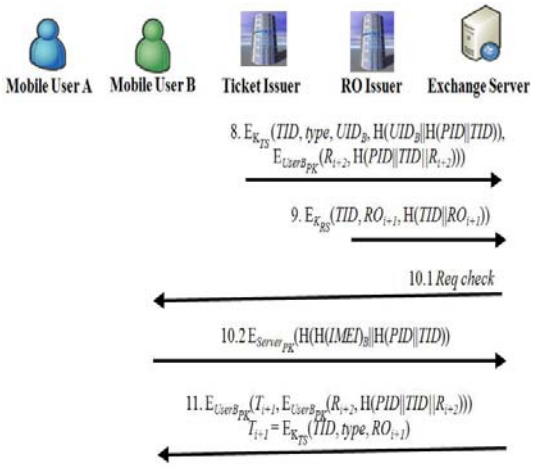

Figure 7: Transfer phase (b)

Analysis and Discussion

In the purchase and acquire phase, we can achieve the integrity of the contents of the mobile ticket. Because the ticket issuer sends the random number to the mobile user and used the password for next transmission. When the mobile user receives the mobile ticket, he will be computed random number as a MAC value, to confirm that this mobile ticket is unmistakable.

In the transfer phase, we add a fair RO issuer that issues the RO and configures the conditions, i.e. valid period, times of usage, and will be finished of open-card, achieves the authentication of the mobile ticket. In addition, the RO cannot allow a malicious mobile user who sent mobile tickets to others, because the RO records the owner. Therefore, the mobile tickets can be prevent malicious destruction of others and secured of usage.

Security Analysis

This research method can reach the following security:

(1) Confidentiality: In the transmission process, mobile users and the ticket issuer use the public key to encrypt, $E_{User_{PK}}$ and $E_{IS_{PK}}$. If he wants to decrypt, must have the corresponding private key. Another, the symmetric keys were used between the issuers and servers. So we use encryption methods according to the different targets to ensure confidentiality of information.

(2) Verifiability: When the mobile users acquire mobile ticket at each time, we verify the password that computed the random number with a hash value, because the ticket issuer creates different password at each time. Another, he will be use the random number to verify, when mobile users get the mobile ticket.

(3) Authentication: In the purchase and transfer phase, the ticket issuer generates a user ID (UID) that used the IMEI of mobile user, and it can be used the

verification or RO. Specially, the RO issuer will be verify the identity of owner in the RO.

(4) Non-repudiation: The ticket issuer generates the mobile ticket and password using the IMEI, so the mobile users can be achieves the object of Non-repudiation. Another, the RO issuer needs to write the identity of himself, when he creates a RO.

(5) Integrity: In the transmission process, the mobile user and ticket issuer use the asymmetric key to encrypt. If the data has been tampered in the transfer process, mobile users and the ticket issuer will be unable to correctly decrypt, so it can be protects the integrity of data. In the acquire process, the ticket issuer generates the MAC value that used a hash function to create, and it can be judge this message were correct.

(6) Forgery: When the tickets were created, the RO protects the user's rights in the tickets. Because recorded the owner and transferable conditions of mobile user in the RO, so can not be used this mobile ticket by malicious mobile users. Therefore, the mobile tickets aren't forged.

Conclusion

In this paper, we propose a protocol that allows mobile users to order, acquire, and transfer e-tickets using the mobile phones without comprising the security. The RO is used to prevent illegal usage of the mobile ticket and the rights of the ticket owner. Thus, a fair third party (the RO issuer) is important. Whenever a mobile user acquires a mobile ticket, we verify the password generated from a computation of a random number with a hash value. In this way, we may not only authenticate the identity of the mobile user, but also verify the mobile ticket whether it is tampered. Therefore, mobile users may have the confidence of using mobile ticketing in the secure mobile environment.

References

[1] Sasu Tarkoma, Jani Heikkinen, and Mikko Pohja, "Secure Push for Mobile Airline Services," *Telecommunication Systems*, 35(3-4), 2007, pp. 177-187.

[2] Wei Lu, "An Analysis of Airline E-commerce Strategies in Ticket Distribution," *Proceedings of the IEEE International Conference on Service Systems and Service Management*, 2007, pp. 1-5.

[3] Tommy Bouchard, Mathieu Hémon, François Gagnon, Vivianne Gravel, and Olivier Munger, "Mobile Telephones Used as Boarding Passes: Enabling Technologies and Experimental Results," *Proceedings of the IEEE International Conference on Autonomic and Autonomous Systems*, 2008, pp. 255-259.

[4] Oliver Jorns, Oliver Jung, and Gerald Quirchmayr, "A Privacy Enhancing Service Architecture for Ticket-based Mobile Application," *Proceedings of the Second International Conference on Availability, Reliability and Security*, 2007, pp. 139-146.

[5] Yin-Ling Liong and Sudhir Dixit, "Digital Rights Management for the Mobile Internet," *Wireless Personal Communications of the ACM*, 29(1-2), 2004, pp. 109-119.

[6] Sai Ho Kwok, "Digital Rights Management for the Online Music Business," *SIGecom Exchanges of the ACM*, 3(3), 2002, pp. 17-24.

[7] Chun-Te Chen and Te-Chung Lu, "A Mobile Ticket Validation by VSS Tech with Time-Stamp," *Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service*, 2004, pp. 267-270.

[8] Kazuo Matsuyama and Ko Fujimura, "Distributed Digital-ticket Management for Rights Trading System," *Proceedings of the 1st Conference on Electronic Commerce*, 1999, pp. 110-118.