Ensuring Privacy in Smartcard-based Payment Systems: A Case Study of Public Metro Transit Systems

Seng-Phil Hong[1], Sungmin Kang[2]

[1] School of Computer Science & Engineering Sung Shin Women's University, Seoul, Korea
philhong@sungshin.ac.kr
[2] College of Business Administration, Chung-Ang University, Seoul, Korea
smkang@cau.ac.kr

Abstract. The advances in technology have enabled us to share information, process data transactions, and enhance collaborations with relevant entities effectively. Its unparalleled adoption in both the public and private sectors is raising heightened concerns, particularly in the areas of the collection and management of personal information. The use of personal information can provide great benefits, including improved services for customers and increased revenues and decreased costs for businesses. However, it has also raised important issues such as the misuse of their personal information and loss of privacy. In this paper, we propose a framework to preserve privacy in new Public Metro Transit Systems that incorporates smartcard-based payment systems. The proposed framework leverages cryptographic protocols and an innovative privacy model to ensure the protection of privacy information of the cardholders. We also overview our system architecture for the proposed framework including case learned.

1. Introduction

The recent survey indicates that online and offline retailers lost $6.2 billion in sales because of privacy issues [1]. A separate survey found that more than 50% of consumers reported leaving e-commerce sites they have been using because of privacy reasons. These surveys signify that the use of personal information can provide great benefits, including improved services for customers and increased revenues and decreased costs for businesses. However, it has also raised important issues such as the misuse of their personal information and loss of privacy. We have recently witnessed similar issues in new transportation systems in South Korea. One of major cities in South Korea has introduced new metro transportation systems, adopting highly innovative technologies since 2004. They have implemented an overhaul of their public transportation systems, introducing new bus routes, numbers, colors, and adjustments in bus and subway fares. The new transportation systems are designed to achieve both faster and more convenient transit services to the citizens. The new transportation systems have brought many changes and one of important changes is the new type of e-payment smartcard called TP card.

TP card works as an e-cash card, which can be used to pay for transportation fares conveniently, and it can be recharged for the further usage. Since TP card has an integrated circuit chip, it can not only be used as an ID card and pay for transit fares, but also be used to make small purchases at the convenient stores, restaurants, and movie theaters. More specifically, it is a smartcard with the improved security technologies based on domestic security technology standards and international security algorithms. Application areas of TP can be extended to e-payment for other transportation fares and e-ticketing for product and service purchases in the near future.

With 12 months of its usage in effect, there are advantages in newly adopted Public Metro Transit System, called e-PTS, and some early problems are encountered with challenges of requirements to resolve the inconvenience of new e-payment systems and technical threats related to security and privacy issues. In this paper, we identify the problems that exist with the advent of e-PTS and suggest countermeasures to resolve such technical problems. A recent case of criminal mischief led us to consider the above-mentioned issues. The law enforcement agency caught the criminals by tracing TP card usage information in e-PTS. However, this is an important wake-up call to other users because it can be a critical problem to the protection of their privacy. Therefore, no trace at all or only limited trace of personal information should be allowed on payment methods, providing assurance level of anonymity. This prompts the need for more secure method of transportation fare payment. Limited tracing of personal information needs to be implemented with the cooperation of few designated agencies. The goal of this work is to suggest and analyze the practical privacy model to the existing e-PTS.

The rest of this paper is organized as follows. Section 2 discusses background technologies followed by the overview of e-PTS in Section 3. In Section 4, we propose a privacy model for e-PTS including system architecture. Section 5 describes features of the proposed model. Section 6 concludes this paper.

2. Background Technologies

2. 1 Public Key Infrastructure (PKI) and Digital Signature

PKI is an infrastructure for disseminating the public key in a secure and reliable channel. One of important components of PKI is a set of certificate authorities (CAs) that archives public keys of certified users or entities. The user or entity that wishes to participate in this infrastructure must successfully prove their identity to the CA [2, 3, 4]. Even though some argued the risks on security services of PKI [5], PKI has been considered as a viable solution for security and privacy services by healthcare industries. Hence, our work utilizes PKI to develop a scalable privacy model for e-payment system.

2.2 Smart Token Technologies

Smart tokens are devices with a memory and a processor which can generate and store keys. It also supports cryptographic functions such as encryption, digital signature, or key agreement. Some noticeable characteristics of smart tokens are portability, tamper-resistant storage, and isolation of computational activities (i.e. leveraging the features of cryptographic functions without revealing private keys to other system components) [6].

Smartcard. The smartcard, an intelligent token, is a plastic card embedded with an integrated circuit chip. It provides not only memory capacity, but computational capability as well. The security features of smartcard make it resistant to security threats. A smartcard is a card that is embedded with either a microprocessor and a memory chip or only a memory chip with non-programmable logic. The microprocessor card can add, delete, and manipulate information on the card, while a memory-chip card can only undertake a pre-defined operation. [7, 8].

2.3 Threshold Cryptography

The idea of threshold cryptography is to protect information (or computation) by fault-tolerantly distributing it among a cluster of cooperating computers [9, 10, 11]. First consider the fundamental problem of threshold cryptography, a problem of secure sharing of a secret. A secret sharing scheme allows one to distribute a piece of secret information among several servers in a way that meets the following requirements: (1) no group of corrupt servers (smaller than a given threshold) can figure out what the secret is, even if they cooperate; (2) when it becomes necessary that the secret information be reconstructed, a large en**oug**h number of servers (a number larger than the above threshold) can always do it.

3. e-PTS: Architecture and Privacy Issues

The e-PTS consists of three major components: Sub, Main, and Linkage systems. Sub, Main, and Linkage systems are interconnected through enterprise application integration (EAI) interface. Sub system components perform activities related to re/charging the transportation fare for bus and subway systems. Main center components store information gathered from sub system components and manage and administer the collected information efficiently. Further, Linkage system relays the processed information to the relevant sites, which require metro and e-payment information gathering. .Figure 1 illustrates the architecture of e-PTS.

With the introduction of new Public Metro Transit Systems, we have witnessed critical privacy concerns that need to be studied and analyzed to investigate relevant countermeasures. Our study indicated that some of privacy issues are still raising inevitable business problems as follows:

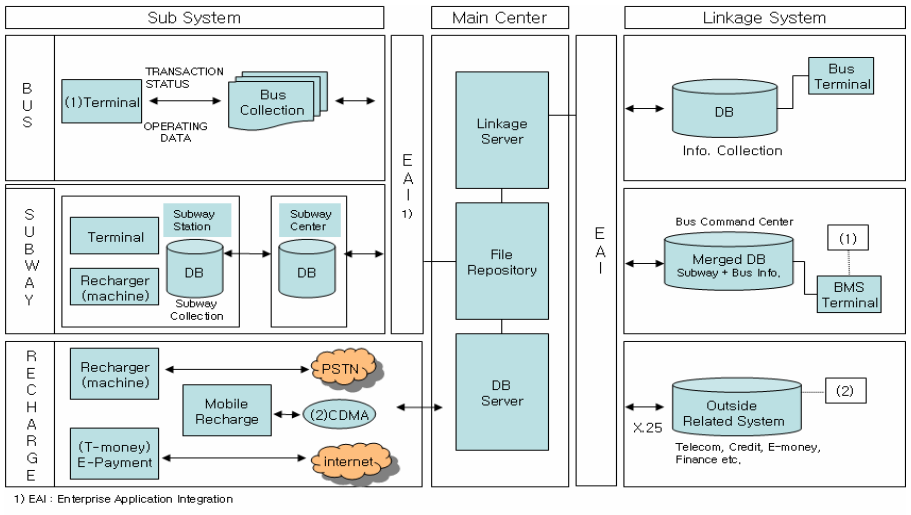

Fig. 1. e-PTS Architecture

Anonymity: It enables users to make use of e-PTS without being tracked and keep the state of being anonymous or virtually invisible. A user could spend all day using e-PTS but the sites or location information the user visits should be protected.

Pseudonymity: Like characteristics of anonymity, a user cannot be identifiable but the user can be tracked through an alias or persona that the user has adopted.

Unlinkability: It refers to the inability to link pieces of related information. This could mean isolating multiple transactions made using the same TP card. The ability to link transactions could reveal an idea of daily routes or how much expenses have been consumed over a month.

Unobservability: This refers to the inability to observe (or track) while a user is accessing a service. The multi-purpose TP card can be used to abuse payment information without cardholder's permission or legitimate access when the TP card is used for other services. However, it may be useful to observe activities of the user under certain circumstances such as disaster or medical emergency.

Authorization privacy: To recharge a TP card, users are often required to present their identifications. This can be used to track how often a user recharges the TP card, even though it is important only to know that the bearer deserves access to the facility.

Data management: Collected and managed data information can be often misused with malicious intent or by mistakes.

In the subsequent sections, we attempt to articulate possible solutions for key issues involved with the above privacy concerns.

4. Privacy Model for e-PTS

In this section, we propose a policy model for e-PTS, called Privacy Model for Public Metro Transit System (PMPTM). In our model, we focus on the following privacy issues that need to be solved in large-scale distributed environment: when a cardholder conducts multiple smartcard transactions at different places, the cardholder's personal information, transaction data, and critical payment information could be revealed without cardholder's recognition at each location of card transaction.

In our model, we seek mechanisms to help reveal personal information only to the authorized users/entities and enforce privacy policies which are specified by and assigned to the cardholders.

PMPTM architecture is illustrated in Figure 2. It consists of two important components: Privacy Check Box and Policy Bank. The functionalities of each component are as follows:

Privacy Check Box (PCB). PCB is a module for maintaining the confidentiality of a cardholder's information and checking his/her privacy conditions concerned with PMPTM. After a session is established through PMPTM, authentication unit not only checks the cardholder's identification but also determines the cardholder's critical information that is not available for anyone by using a threshold cryptographic protocol. PCB then verifies and validates the cardholder's privacy condition within privacy condition box.

Policy Bank (PB). PB is a set of access control policies for passing a system's request to another system between cardholders and card managers. The PMPTM defines the policy framework consisting of policy gathering component, policy repositories for the assigned policy, and policy enforcement for handling policy decisions. Policies are rules governing the choices in behavior of a system.

Privacy Model for Public Metro Transit System (PMPTM) works as shown in the following process. Once a smartcard holder attempts to access PMPTM mechanism (1), SSL connection is established and Session Management provided to the cardholder's credentials are passed to Authentication Unit (2). Authentication Unit accesses PCB to authenticate the cardholder and PCB (Privacy Condition Box) verifies the cardholder's privacy condition related to privacy information which maintains usernames, privacy policy type, level and principle of privacy policy actions (3). PR (Privacy Repository) gathers privacy information if the cardholder's privacy condition checking is successfully completed. PR retrieves or gathers privacy policy information from private policy database and generates privacy information if it needs to update (4, 5). After PR stores the information and PE (Policy Enforcement) takes an action that provide the well-define access control according to privacy policy (6), PMPTM then triggers the requested service and sends the signed crypto API to the cardholder's smartcard for further transactions and file repository (7, 8). Finally the requested service is provided to the user from PMPTM Service.

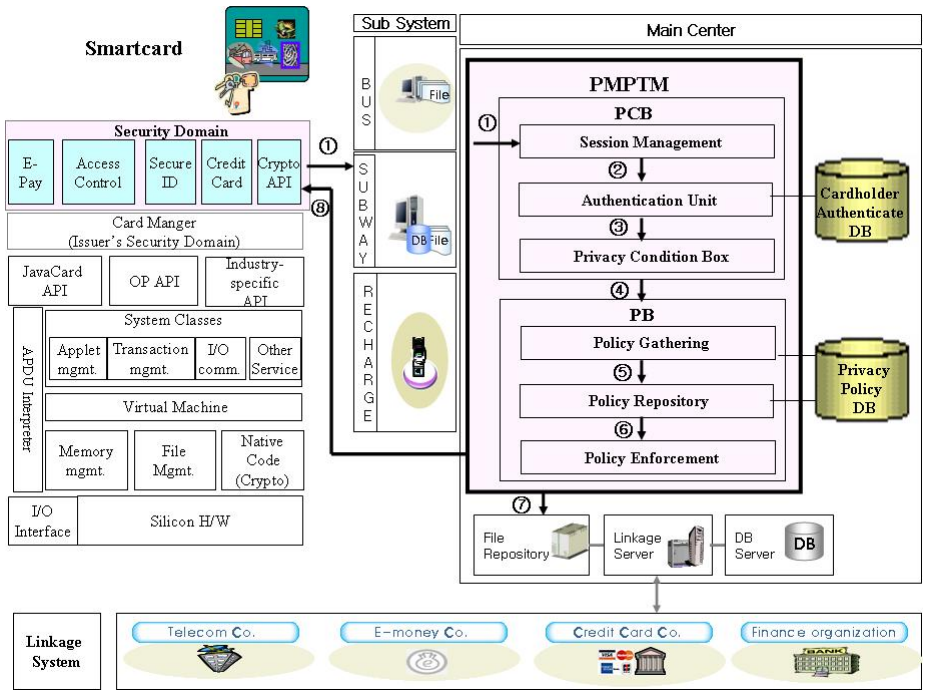

Fig.2. PMPTM Architecture

In our model, policy types are categorized as one of the following access control policies, which depend on what activities a subject can perform on a set of target objects:

- Policy_Type_A/A′ : A set of subjects must do / not perform a set of target objects.
- Policy_Type_B : A set of subjects must validate the conflict of access control policies to a set of target objects.
- Policy_Type_C/C′ : Actions are permitted to / prohibited from a set of subjects or a set of target objects
- Policy_Type_D : Actions are delegated to a set of subjects or a set of target objects.

Policy gathering and policy repository components should guarantee to determine correct access constraints and appropriate policy management including modification and revocation of policies. The policy enforcement should trigger an action to retrieve policies from policy repository and evaluate the policy condition when policy is executed from policy repository.

Table 1. Notation in PMPTM

A (subject)	A principal or system that requests an action
B (object)	A principal or system that can perform an action requested by A
Action	A list of operations: request/response/check/order/cancel/pay/debt
t_1	Time that an input call starts
t_2	Time that an output call starts
r_1, r_2	Random numbers
$cert_A$	A's public key certificate
$cert_{PM}$	PMPTM's public key certificate
pc_A	A's privacy condition attributes. It would be representing to general information and other information such as payment information and payment profiles.
P	Priority information. It has three attributes: low/medium/high
σ_A	Signature of Cardholder A
σ_{PM}	Signature of PMPTM

Next, we describe how each component in PMPTM works to support the proposed architecture. We use notations in Table 1 to explain the details. The PMPTM architecture works as follows:

1. Input Call
   - A cardholder "A" sends a message to the PMPTM making an input call using contactless smartcard based on ISO14443 Type A/B format. The cardholder requests the privacy information to all registered manufacturers in PMPTM.
     - $Input\_call =< A, B, t_1, r_1, request, \sigma_A, cert_A, pc_A >$

2. Policy Check Box
   - Session Management: A user inputs information for establishing a session in PMPTM.
   - Authentication Unit: User Interface sends a session establishment input to PCB. Secure connection (such as X.25) is established and the cardholder's credentials (such as X.509 Certificates) are passed to PCB. And it forwards the cardholder's information to authentication unit then verifies the cardholder's signature using the associated public key.
   - Privacy Condition Box: Authentication unit transmits the cardholder's authentication information to PCB if the authentication check is successfully completed. Then it checks the validation of the cardholder's privacy condition within PCB. Reference monitor transmits the cardholder's information to the PB if the validation check is successfully completed.

- After all, PMPTM checks the information which request from the cardholder A
  - Check the validation of $cert_A$ using PKI.
  - Verify the signature σ_A in an input call using $cert_A$.
  - Check pc_A.

3. Policy Bank
   - Policy Gathering: It collects the cardholder's information from PCB, then retrieves privileges granted to the corresponding user's action
   - Policy Repository: It assigns reasonable policies that provide a set of cardholder's information from policy repository. It includes action, priority, and policy.
   - Policy Enforcement: It validates and enforces a selected policy.
     - If pc_A is valid, retrieve a privacy information from pc_A.
     - PB executes the policy gathering from the policy repository (as shown in Table 2) and the policy enforcement procedures.

Table 2. Cardholder Domain Table in Policy Repository

SUBJECT	ACTION	Policy TYPE	PRIORITY	OBJECT
Cardholder A	REQUEST	Policy_Type_B	Middle	Card Manager B (PMPTM)
Cardholder A	PAY	Policy_Type_C	High	Card Manager B (PMPTM)

4. Output Call
   - Finally, a reformatted message is sent to a set of target objects or returns to cardholders. PMPTM generates output call for each registered card manager B in PMPTM
     - $Output\_call =< A, B, t_2, r_2, pc_A, P, \sigma_{PM}, cert_{PM}, >$

       Where pc_A *is general information and P is middle.*

   - PMPTM resends output call to cardholder A. The procedure of response is the same as the request procedure. The cardholder A can gather the authentication information, privacy condition and price from each response. The requests such as "order" and "pay" can be executed through PMPTM mechanism.

5. Features of PMPTM

This section describes the strength of PMPTM in comparison with previously discussed problem statement in section 3.

Strong Privacy Control: Among the various functions of smartcard service, information leakage should be prevented, as a cardholder needs to protect his or her privacy. Using the threshold cryptography protocol, the card holder's personal and transaction information, which can be exposed to others by service provider without cardholder's consent, should be informed to the cardholder first before sharing the information. Moreover, we tried to resolve the "privacy issues" in the large-scale distributed environment by suggesting the efficient access control measures in the PMPTM architecture. Through these access control measures, we emphasize the importance of data confidentiality and data integrity that have been overlooked previously due to data traceability and data availability. We believe data confidentiality and data integrity should be considered as more important security requirements from the privacy perspective.

Well-defined Privacy Policy: A cardholder wishing to access community resources contacts the PMPTM server. The card manager can easily keep track of cardholder's privacy condition and select fine-grained access control policies, because PCB mechanism can verify and validate cardholder's personal information. In PB, it also provides centralized monitoring condition, which handles how well card holders can present themselves to gain access on behalf of the business community condition. It could improve ease of use and accuracy of the administration process even if access control is implemented in a variety of heterogeneous components, and the cardholder or card manager needs to concentrate only on this very unit in which all security related configurations are maintained.

Trust Policy Management: The PMPTM mechanism should rely on a simple mode transaction that covers the different range of large-scale multi-organizational systems. Because PMPTM mechanism strictly enforces stored access policies that have been already defined in PB repository of PMPTM. This means that it is very hard to modify/delete our reserved rules or policies by unauthorized people. Additionally, our policies are supposed to reserve a couple of business action (Request/Response/Check/Verify/Pay/Debt) cases. There is no change in the policy type without permission or privilege.

Scalability and Performance: When cardholder sends the message to PMPTM, PMPTM checks user's status (subject, object, privacy condition, action, and security level). The priority information of message represents how important the business condition is. Practically, it is very helpful to control many users who have different security conditions simultaneously. If card manager finds the priority message (Security level-H: High), then they should more carefully execute the message such as dual verification and end-to-end monitoring, or the high level security message should be sent first if other messages/queues are waiting for next processing. This could enable congestion control. The cost of adding or removing participants, which corresponds to changing policy types, should not increase the number of resource providers participating in PMPTM. Therefore, resource administration overheads should also be controlled and minimized.

6. Conclusion and Future Work

The new transportation card system based on smartcard technology shifted a paradigm of public service from offline environment to online environment. We attempted to implement new IT infrastructure for automatic fare collection mechanisms and efficient management systems based on the use of smartcard in the distributed computing environment. In this paper, we proposed a new privacy model and architecture, which can be easily implemented in order to resolve the security and privacy issues that exist with respect to the protection of personal information and privacy. We have also described lessons learned through major features in e-PTS so that system engineers and software developers can adopt our approach to implement the relevant system. We believe our work will help facilitate the growth of e-payment service based on TP in e-PTS. As a future research direction, we plan to conduct a research by considering the extension of the suggested model and smartcard management using the notion of role-based access control effectively.

References

1. A list of privacy surveys,
   Available at http://www.privacyexchange.org/iss/surveys/surveys.html
2. Min Liu, Shudong Sun, and Miaotiao Xing, “Study on security based on PKI for e-commerce of statistics information system”, ACM International Conference Proceeding Series; Vol. 113, ACM Press, Xi'an, China, Aug. 2005, pp. 729 – 732.
3. L. Pearlman, V. Welch, I. Foster, C. Kesselman, S. Tuecke, “A Community Authorization Service for Group Collaboration Policies for Distributed Systems and Networks,” Proceedings of the Third International Workshop in 2002, pp. 50–59.
4. Pierangela Samarati, Michael K. Reiter, and Sushil Jajodia, “An Authorization Model for a Public Key Management Service,” ACM Transactions on Information and System Security, 4(4), Nov. 2001, pp. 453-482.
5. C. Ellison and B. Schneier. Ten Risks of PKI: What you are not being told about Public Key Infrastructure. *Computer Security Journal*, 16(1): 1-7, 2000.
6. Xinhua Zhang, Christoph Meinel, and Alexandre Dulaunoy, “A Security Improved OpenSST Prototype Combining with SmartCard,” Proceeding of the International Conference on Computer Networks and Mobile Computing, IEEE, 2003.
7. Blerim Rexha, “Increasing User Privacy in Online Transactions with X.509 v3 Certificate Private Extensions and Smartcards”, Proceedings of the IEEE International Conference on E-Commerce Technology, Washington, USA, July, 2005, pp. 293–300.
8. Yankiang Yang, Xiaoxi Han, Feng Bao, Deng R.H., “A Smart-card Enabled Privacy Preserving E-prescription System,” IEEE Transaction on Information Technology in Biomedicine, Vol. 8, No. 1, pp. 47-58.
9. A. Shamir, “How to share a secret,” Communication of the ACM, Vol. 22, No.11, pp. 612-613.
10. Anna Lysyanskaya, Chris Peikert, “Adaptive Security in the Threshold Setting: From Cryptosystems to Signature Schemes,” ASIACRYPT, 2001.
11. Ran Canetti, Shafi Goldwasser, “An Efficient Threshold Public-key Cryptosystem Secure Against Adaptive Chosen Ciphertext Attack,” EUROCRYPT, 1999, pp. 90-106.