Seamlessness & Privacy Enhanced Ubiquitous Payment

Kyoung Jun Lee[1], Mu Jeong Jeong[2], Jeong-In Ju[3]

[1, 3] School of Business, Kyung Hee University
Hoegi-dong, Dongdaemun-gu, Seoul, 130-701, Korea
{klee, jji99} @khu.ac.kr
[2] Design House, Taigwang Bldg., 162-1,
Jangchung-dong 2-ga ,Jung-gu, Seoul, 100-855, Korea
coolcoom@design.co.kr

Abstract. Payment is in nature an act of money transfer from one entity to another, and it is obvious that a payment method will be valued as long as the transaction can be completed with safety no matter what technology was used. The key to U-payment is convenience and security in the transfer of financial information. The purpose of this paper is to find a desirable U-payment scheme promoting seamlessness and privacy with a strong personal device and peer-based information transactions. We propose U-SDT(Secure Direct Transfer) Protocol as a way to make transactions seamless, secure and privacy-protected.

1. Introduction

As ubiquitous computing environments evolve, business transactions are taking place more seamlessly. As a RFID tag is embedded in products, the process of entering information was replaced with just passing the RFID tag through an electromagnetic reader. Local telecommunications technologies like Blutooth and irDA incessantly send dynamic digital information to the device of others (without saving information in a USB storage device and inserting it into the counterpart's payment device to retrieve the information). Based on this technology, U-Commerce makes the real-world seamless communication of each entity's digital information possible and a seamless U-payment procedure becomes reality.

Another issue is privacy concern as mentioned heavily in many other papers on Ubiquitous computing. In some of the papers, Floerkemeier et al. (2004) proposed a RFID Protocol using "Watchdog Tag" as a way to prevent infringement of privacy. Roussos & Moussouri (2004) suggested that users in the ubiquitous computing environments should have control over their personal information through user focus group interview about MyGrocer and expressed a grave concern about exposing private information to outsiders, especially to a profit-oriented company. In addition, Acquisti(2002) explained the economic efficacy of privacy protection technologies and Langheinrich (2001) proposed to set principles of privacy protection and impose responsibility for invisible services as a way to protect privacy in the ubiquitous computing environments. Zugenmaier & Hohl (2003) emphasized the importance of

keeping anonymity in the ubiquitous computing environments in order to protect user ID from being exposed to personal information collection. However, payment, more than any other areas, is susceptible to privacy concerns and thus merits special attention.

Cash payment is the best payment scheme to avoid privacy concerns. Many payment mechanisms were invented afterwards to enhance payment convenience, but they came at the expense of privacy. In this respect, e-cash or digital cash can be an answer to the privacy issue at a time when we have digital payment methods like e-Payment. But when we look at the evolution of e-cash, the chance is slim that e-cash becomes commonly used payment method as though the ubiquitous environment is setting foot. A future payment system will allow only publicly authorized institutions to possess minimum amount of information such as account numbers when a money transfer is made, and make it hard for merchants to collect any personal information by taking a buyer's credit card or card number to make a payment, and let buyers have control over their personal information while making a payment. This could be an alternative answer to privacy protection while condoning some involvement of a payment server for the sake of payment convenience.

In this paper, we propose a seamless U-Payment method with least privacy concern. To that end, we explain important characteristics and desirable features of ubiquitous computing environments and present a scenario in which such characteristics and features can be found and ultimately, a detailed System Architecture.

2. Characteristics of U-Payment Environment

Important characteristics of user payment environment under the ubiquitous computing environments are that creation, conversion, and transfer of payment information are made seamlessly, and functions of users' payment device, computing power and storage capacity are all very much strengthened. Such characteristics in the U-Payment environments propose a brand-new payment method to users.

2.1 Seamlessness

Seamless payment information processing simplifies payment process. For example, when you take the subway, you have had to buy a ticket and insert your ticket into the ticket slot to pass through the gate. But now, one touch of a smart card embedded with an IC chip will deliver your payment information seamlessly to the payment system of the subway. In this process, the information about cash payment is seamlessly translated into a digital form and sent to the central subway system. Even though we are using smart cards, there are some occasions that we experience some disruptions in seamless payment since the application is payee-oriented. For instance, when an elderly person or a physically challenged person tries to get a free-ride, they need ID authentication by a train officer to get a free ticket. If more seamless payment system is in place, what they have to do is just contacting the smart card embedded with the bearers' payment ID to prove they are eligible for a free-ride.

When you buy something at a local store, you will experience a similar situation. For example, when you buy an electronic gadget at a local store, if you want a money transfer via mobile, you need to enter price, account number of the merchant into the payment device and when the transfer is completed, the merchant checks the transfer was made properly and then you will get the product in your hand. On the other hand, if an RFID Tag is attached to every single product, the mobile payment device of the payer reads the information like price and account number of the payee and transfers money to the account with one touch, both the payer and the payee can complete the payment seamlessly with lower transaction costs.

Seamlessness under the U-Payment environment is a major feature that brings about changes to the user payment mechanism with regard to processing and networking of payment information. In the past U-Payment environment, conversion of the information - turning information into a digital format and vice versa - should be carried out at a high price. At local stores, information on the price and payment means are stored on a price tag or a paper manual, but in this case other substantial information remains un-encoded. However, as the information is digitalized in a seamless manner, the payment environment becomes much simpler and users are spared the hassle they had in the past and seamless payment comes into action at last.

However, the seamlessness does not mean Calm Payment. Boddupalli et al.(2003) explained that among the requirements of the U-Payment, calmness and user involvement should be balanced. Moreover, calmness should be mostly realized in low value transactions. Likewise, seamlessness of the U-Payment is not consistent with calm payment because this is just a technology-oriented payment method that fails to reflect psychological aspect of users when making a payment. When a calm payment - a payment made without a user's knowledge – is made, the user basically will not condone the fact that the payment was made without his (or her) authorization or confirmation because a payment is subtracting money from the balance of one's account and every user wants to be highly involved in the payment procedure. What we refer to as "seamlessness" here does not describe a payment made without user's consciousness but a payment made without information conversion costs.

2.2 Strong User Device

It is highly likely that individuals in the U-Commerce environments will have a personal mobile device equipped with information processing and networking functions like UDA (Ubiquitous Digital Assistant). This is the rite of path given that every transaction in the ubiquitous environments is all about information processing and networking. In particular, every individual becomes an independent commercial entity when (s)he conducts business transactions. It is a generally accepted view that people would not like the idea of incorporating such a device into a human body in the form of a microchip. Thus, chances are that a personal ubiquitous device will be a must-have item for each user.

Such a user device like UDA will perform a function as a payment device for individuals. A stronger role of a user device as a payment entity requires a more

sophisticated, independent device with better information processing and networking capabilities. A user device performs the following three functions in the payment process.

Information Gathering
A payer's payment device performs a role as a seamless payment-related information reader. In the abovementioned example, when you buy an electronic gadget at a local store, a payer device reads the price and payee's bank account codified on the RFID tag. In the same way, the payer device, just like Bluetooth, will deliver seamless value to users by gathering payment-related information that is statically stored on a RFID tag and information on dynamically adjusted service charges.

Information Processing
A payer device does A to Z with regard to payment information processing. In specific, it runs a banking application, sends financial information of a buyer to the merchant's bank account after user authentication, and verifies the result of the transfer. The whole process of payment is working in a payer device.

Information Storing
Every payment-related information – during and after a transaction – will be initially stored in the Payer Device. Under the previous payment systems, payment-related information was mostly stored at a credit card company or bank that serves as a main server for the transaction. But when you use the payer device, such information is stored in the PIB (Personal Information Base) installed inside the payer device. Thus, the U-payment can be carried out while privacy of the payer is better protected.

The significance of the change in the payment scheme with the advent of strong user device can be found in the fact that payee-oriented system has given way to payer-oriented system as the main payment scheme of the ubiquitous environment. It is anticipated, as such a trend prevails, that the payer device carries out functions of both payer device and payee device, and ultimately facilitates the coming of the U-Commerce environment where each individual evolves into a business entity.

3. Suggestions of U-SDT Protocol

As described above, seamlessness and strong user device are the two important features of the U-Payment environment. Privacy protection, a thorny issue of the ubiquitous computing environments, is a critical element in the architecture of U-Payment method from the initial stage. Reflecting these factors, we propose U-SDT(Secure Direct Transaction) Protocol as a U-Payment Method which provides new value to payment entities by consolidating functions of the RFID, Payer Device, and financial institutions.

3.1 Scenario

James who works in the IT industry goes shopping in a department store to buy a present to celebrate the one year anniversary with his girl friend. James discovers a dress in the show window of a women's clothing store and goes into the store to check out the blue dress. Satisfied with the fabric and condition of the dress, James decides to purchase it. The store clerk takes the dress to the store register which reads the information included in the product tag. The product and price shows up on the monitor of the register and James has his UDA to read the payment information on the register. A payment application runs on James' UDA and James who confirms the product name, size, and price etc. on the UDA screen authenticates an official authentication. A few seconds later, the money transfer confirmation window appears on James' UDA screen from James' bank account and after the shop clerk confirms the payment through the shop's monitor on which the account confirmation window is run, he/she clicks the menu to generate a receipt. James, who thinks he might exchange it or get a refund in case his girlfriend does not like the dress, presses the reading button on the payment device and receives an electronic receipt.

The scenario above describes a form of payment focused on the buyer device in a ubiquitous environment. On the surface this is similar to the payment scenario that has been described in various papers (the payment scenario of BluePay and MyGrocer, an automatic payment process in which a mobile device of the buyer is used to recognize the product's RFID Tag) but a marked distinction exists in the flow of the payment information and its storage location and the main information processing device. In the above scenario, the biggest difference is that the processing and storage etc. of the payment information is not performed in the payee's device or server of a financial institution but is mainly performed on the payer device, which is the reason why the protection of privacy of the users is enhanced in the U-SDT.

Another important aspect that has not been revealed in the scenario is the appearance of a payment system based on the Transaction ID used in the payment transaction. This element enables payment using a financial institution without exposing the ID of the payer or payee, which was inevitable in all kinds of payments except cash payment. The generation of transaction ID is also designed not to be dependent on the existing payee device but to be a part of a system where the payer and payee mutually generate and authenticate with equal authority and unique Transaction ID is generated from the two Transaction IDs made by the payer and payee devices. A Transaction ID, which has uniqueness and representing nature, also plays an important role in the refund process. In the existing refund process, steps should be taken to confirm the breakdown of the account through the financial institution in the refund process, while when using the transaction ID all that has to be done is the refund authentication for the Transaction ID of the relevant transaction in the payee account to confirm the payment information which the Transaction ID represents in the Payment account. Such a Transaction ID plays the role of protecting privacy and enhancing efficiency of the payment.

3.2 System Architectures of U-SDT Protocol

Fig.1 shows the system architecture of the U-SDT protocol and the flows as follows:
(1) The product tag is read in or the service ID is inputted in the payee device
(2) The payee device reads in the Product ID which the payee device generates, the price amount, the encrypted payee ID (ID & account number), payee_TID
(3) After confirming the product list and price, the official authentication is confirmed (payment approval of the payer)
(4) Transport the payer_TID+payee_TID to the Payee Device and simultaneously order payment and TID to the payer account
(5) Transfer money
(6) Transport TID and payment results
(7) Confirm receipt of money
(8) Generate final TID which has the authentication of the payee's payment completion (receipt) and which the payer device reads in

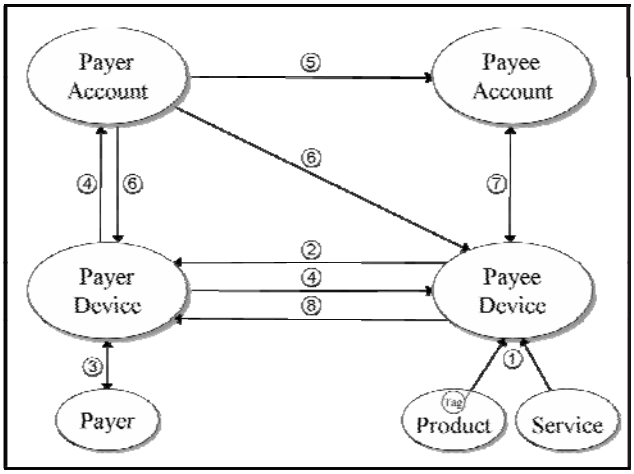

Fig. 1. U-SDT System Architecture

Payment-Related Entities
The elements involving the U-SDT payment can be divided into four categories.

First, the payer device plays the role of gathering, processing, and storing the payment-related Information. Payment-related information is read in from the payee device and the payer's Transaction ID is added to the Transaction ID which the payee device generates, creating an equal, mutual and unique Transaction ID. Through the confirmation of the official authentication with the payer, a user authentication process is created and payment process in which the actual amount of money is transferred also is processed by an application which runs on the payer device. Therefore, the payer device is the main element among the U-SDTs and possesses the largest amount of payment-related Information.

Second, the Payee device generates the initial Payment-Related Information through the product tag or the input of the service ID and generates a Transaction ID of the Payee. After payment, receipt information is generated to be transported to the Payer Device through the approval process of the Transaction ID and a signal which modifies the payment status from 'unpaid' to 'payment completed' is transported to the tag inside the product.

The third and fourth elements are the payer account and payee account which are the actual elements that transact financial information. The actual payment process is carried out between these two elements and provides value to the user with payment convenience by involving a financial server. On the other hand, since these elements perform the minimum function of exchanging financial information and do not monopolize payment-related information such as banks and credit card companies.

3.3 Structure of the information possession of each payment entity

Another feature of the U-SDT Protocol is that it has an information possession structure in which the relevant entities possess only the essential payment information thus maximizing the protection of privacy. A payer device and payee device does not posses the other party's ID information and the payer account and payee account should not possess product list information as in Fig. 2.

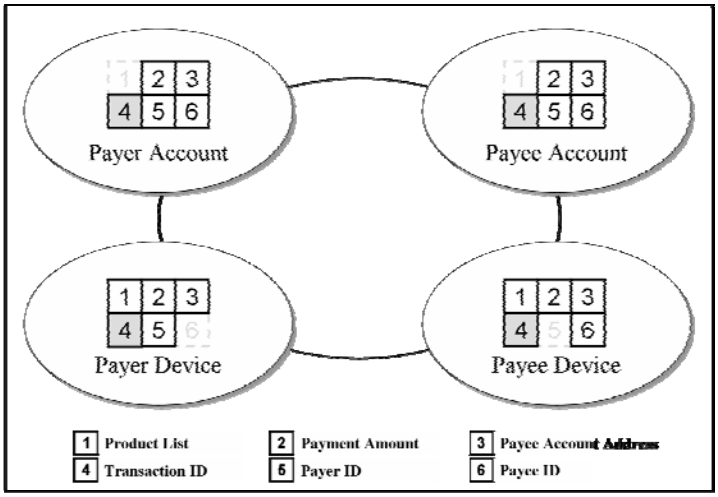

Fig. 2. The Structure of Payment-Related Information Possession in Each Entity

Classification of payment related information

The payment relevant information for the payment execution of U-SDT is as follows.

1. Product List: When possessed by a party who is not the payer the individual product name can be a serious threat to privacy. Therefore, this information should be directly possessed by those who are involved in the payment.

2. Payment Amount: Refers to the price information of a product or service. Refers to the total amount when there are a number of products and service.
3. (Encrypted) Payee Account number: The account number of the payee is the most important payment-related information required in the seamless payment process. This is encrypted and transported to protect the privacy of the payee.
4. Transaction ID: The unique Transaction ID of each transaction enables a payment and refund process to be executed using an ID for the relevant transaction without the Payer and Payee having to possess each other's ID. Such Transaction ID combines the information that is independently generated by the Payer and Payee.
5. Payer ID: Information required to confirm the payment of the payees in financial transactions between financial institutions.
6. Payee ID: Information required to confirm the payment of the payer in financial transactions between financial institutions.

The important feature of the above figure is that the payer account and payee account do not possess a product list and the payer and payee also do not possess each other's ID. A financial institution possesses the other party's ID for the transaction of financial information but since it is a third party in the payment process it does not possess information of the product list that might infringe on the privacy of the payer. In the case of buyer and seller, each financial institution that is involved in the payment and payment confirmation process may use a Transaction ID instead of exposing the IDs of the Payer and Payee to outside and prevent the leakage of privacy information such as the IDs of those participating in the transaction.

Eventually, for the value of 'seamlessness' and protection of privacy to be provided by each payment, each entity should exist in a form in which the minimum payment information essential for payment is categorized and the overall U-Payment architecture should be designed so that the payer account and payee account do not possess the product list and the payer and payee do not posses the other party's ID. Furthermore, for this to be possible, Transaction ID orientation is recommended rather than a Payer ID oriented payment.

5. Related Works

MyGrocer (Kourouthanasis et al. 2002) scenario describes the smart shopping cart automatically transporting payment information to the cashier. However, detailed information flow or system architecture is not provided. Boddupalli et al.(2003) describes a scenario of a payment system using a remote wallet and an e-tag stored in a laptop. However, it focuses on presenting requirements for a U-Payment design rather than presenting a detailed architecture. Seigneur & Jensen (2004) proposes a U-payment using anonymous digital cash stored in a mobile phone but the downside is that it is limited to incidents of small amount of payments. Gross et al. (2004) proposes a U-Payment test platform BluePay based on a PPA (Preferred Payment Architecture) and describes this using a detailed architecture and information flow. BluePay uses a device called a PTD (Personal Trusted Device) using RFID and Bluetooth technology. Payment information using short-range communication and the

POS has the feature of automatically recognizing the tag of a product. In addition, it is similar to the our study that it is working on eliminating or reducing explicit interaction of the customer and that payment relevant information of the payer is stored within the PTD in the Local Exchange. However, a PTD only stores the customer ID for user authentication and payment information such as a credit card or a bank account number is stored in the backend system of a bank or a third party and user authentication is achieved through a loading method and storage by such personal information presents a possibility that privacy is infringed. As a preventive measure, our approach replaces this with an internal authentication system between a payer and payer device. Another difference is that important payments are made within POS connected to external financial data base and clients' data base and this means that an initiative of payment is heavily owned by a seller. Such a way of payment has a weakness because a seller holds a heavy amount of payment devices while a buyer gives his own financial information to a buyer to make the payment possible. Our study as an alternative proposes that an important payment should be made through the reading of payee's payment information by the payment system embedded in a payer Device.

The differences between the existing payment system and the one this study proposes are that the device of user's payment system is always reinforced, that those participants in payment own and control all information and that privacy protection is to a great extent strengthened by the use of Transaction ID and prevention of the exposure of ID.

6. Conclusions

This paper explains U-SDT protocol designed to improve privacy protection through scenario and system architecture. It also proposes a kind of structure separated from control of information regarding payment of accounts as desirable features attached to it. The key issue in this approach is to considerably decrease the high transaction costs accompanied by the conversion of offline (physical) information and digital information through the characteristic called seamlessness of ubiquitous technology. The other purpose of this study is to find a way to better protect privacy in the ubiquitous environment where it is increasingly anticipated to be infringed. Therefore, if the design of U-Payment method is practical enough to meet the two purposes, it is not only highly valued by users, but also is likely to create an independent and smart payment business model and method.

Acknowledgments

This research is supported by the Ubiquitous Autonomic Computing and Network Project, the Ministry of Information and Communication (MIC) 21st Century Frontier R&D Program in Korea.

References

[1] Acquisti, A. (2002). “Protecting Privacy with Economics: Economic Incentives for Preventive Technologies in Ubiquitous Computing Environments,” *Workshop on Socially-informed Design of Privacy-enhancing Solutions, 4th International Conference on Ubiquitous Computing (UBICOMP 02).*

[2] Boddupalli, P., Al-Bin-Ali, F., Davies, N., Friday, A., Storz, O. and Wu, M. (2003) “Payment Support in Ubiquitous Computing Environments,” *IEEE Workshop on Mobile Computing Systems and Applications*, pp. 110-121.

[3] Floerkemeier, C., Schneider, R. and Langheinrich M. (2004) “Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols,” *Institute for Pervasive Computing.*

[4] Gross, S., Fleisch, E., Lampe, M. and Müller, R. (2004). "Requirements and Technologies for Ubiquitous Payment,” *Multikonferenz Wirtschaftsinformat, Techniques and Applications for Mobile Commerce.*

[5] Kourouthanasis, P., Spinellis, D., Roussos, G. and Giaglis, G. (2002). “Intelligent cokes and diapers: MyGrocer ubiquitous computing environment,” *In First International Mobile Business Conference*, pp. 150–172.

[6] Langheinrich, M. (2001). “Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems,” *Ubicomp*, pp. 273-291.

[7] Langheinrich, M. (2002). “A Privacy Awareness System for Ubiquitous Computing Environments,” *Ubicomp*, pp. 237-245.

[8] Roussos, G. and Moussouri, T. (2004) “Consumer perceptions of privacy, security and trust in ubiquitous commerce,” *Personal and Ubiquitous Computing*, Vol. 8, No. 6, pp.416-429.

[9] Seigneur, J. and Jensen, C.D. (2004). "Trust Enhanced Ubiquitous Payment without Too Much Privacy Loss," *In Proceedings of the 19th Annual ACM Symposium on Applied Computing*, Vol. 03, pp.1593-1599.

[10] Zugenmaier, A. and Hohl, A. (2003) “Anonymity for Users of Ubiquitous Computing,” *Security-Workshop at UbiComp.*