TRANSFERRING SECRET ELECTRONIC PAYMENT

Rajendra Prasad Pandey[1], Pradeep Kumar Shah[2]

[1]*College of Computing Sciences and Information Technology, TMU, Moradabad*
[2]*College of Computing Sciences and Information Technology, TMU, Moradabad*

Abstract

Transferring an E-payment scheme on NETWORK is described. It can work on personal computers or smart phones. This particular property is useful to suppress double spending. Nevertheless it has benefits that are expected from electronic money such as anonymity. This money scheme can be used in both, online and offline mode. In online mode, double spending is strictly avoided. In offline mode, double spending is easily detected, if attempted. In particular we have given implementation of this scheme for personal computer and may be mobile phone devices. These devices have a lot of memory and processing power constraints. A payment scheme should work reasonably efficient on these devices. These devices provide a number of choices for wireless connectivity also.

Keywords—*Double Spending, E-payment*

----------***----------

1. INTRODUCTION

With huge growth in electronic commerce the need for electronic money is gradually increasing. A number of notational and token based payment systems have been proposed so far to fulfil this requirement.

Key feature of electronic cash is anonymity as provided by conventional cash. Notational payment systems provide banks with transactional history of payer and payee. With huge growth in electronic commerce, mobile commerce and availability of electronic devices, number of payment transactions per day has increased to a large extent. Notational payment systems are creating serious concerns regarding privacy of users through providing spending profiles and transactional history.

2. REQUIREMENT OF PAYMENT SYSTEM

Following are the typical requirements of a payment system to be widely accepted by the users and merchants, studied in [17][18].

2.1 Ease of Use

Currently there are two payment systems widely accepted by users and merchants. They are cash and credit card payments because they are fairly easy to use. So any new payment system to be accepted by users must be as easy as these systems. Usage of a system can be divided into three categories initial setup, transactions and monitoring or administering.
a. Initial setup may involve application download and installing or upgrading, filling out forms for respective banks.
b. Transactions involve capturing payments, refunding.
c. Administering involves accounting and verification.

A payment system should be very easy in its usage. Initial setup overhead must be least. Quantity of clicks or user typing must be minimal.

2.2 Expenses

Expenses to use the system should be least. Expenses involve following factors.

For Merchants
a. Initial set-up fee may be needed to buy the software and devices.
b. Monthly fee may be charged by the financial institutions.
c. Each transaction may be charged by bank due to involved processing overhead.
d. Certification fee may be charged by the Certification Authorities.

For End-users
a. In payment systems, generally users are not charged directly for making payments.
b. But depending on the technology used user may be charged.
c. If SMS or GPRS is used for communication then the service provider may charge the user accordingly.

For system providers
a. There may be deployment cost involved. E.g. deploying application over the air.
b. There is also system maintenance cost involved.
Expenses involved in above mentioned factors should be least for a payment system to be widely accepted.

2.3 Security

Security is a fundamental requirement of any payment system. If security is not acceptable then other cost and overhead factors make no difference. Sensitive data from all the parties must be secured during transmissions and receptions throughout the system. Some of the security related issues like confidentiality, integrity, authentication etc must be addressed.

2.4 Technical Convenience

It includes the following.
a. System should work with all kinds of devices and heterogeneous platforms.
b. It should be network independent.
c. Performance should be acceptable always

2.5 Other Factors

This includes the following.
a. Reliability
b. Regulatory framework
c. Regulation
d. End-user protection.

3. CURRENT ELECTRONIC PAYMENT SYSTEMS

A number of electronic payment systems have been proposed. In this section we will study few popular electronic payment systems.

3.1 Point of Sale Payments

Credit card payments are most popular payment system used in POS payments. Merchants check signature of the payer on the credit card for verifying payer's identity. Magnetic stripe based credit card's physical properties are checked to verify the validity of the card.

3.2 Internet Payments with Credit/Debit Cards

A many payment systems exist which can be used over Internet. However credit card payments over Internet are the most popular payment system due to ease of use. Payer hands over the payment detail such as credit card number, payer's name and address etc to the merchant. Merchant uses this information to take an online authorization of the issuer's bank. All payment details are communicated over SSL/TLS [33]. Main problems presented by these systems are lack of anonymity and lack of support for small amounts of payments.

3.3 Secure Electronic Transactions

SET [21] is used to make secure credit card payments over Internet. It provides confidentiality and integrity of the transaction data. It also provides authentication of all the parties involved in a payment transaction. Symmetric key cryptography is used for providing confidentiality and digital signatures are used for providing integrity and authentication. SET specific certification authority issues certificates to all the participants.

3.4 Electronic Cheques and Account Transfers

Paper based checks are costly to process. Processing involves transport of the checks all the way to the bank on which the check is drawn. Before this it cannot be deduced whether payment can be made or not. Also there is a lot of expense involved in processing the returned checks or bounced checks. Analogous to paper counterpart electronic cheque [21] contains an instruction to the payer's bank to make a payment of a particular amount to the payee. A payer orders for goods and the payee sends an electronic bill to payer. For payment, the payer sends digitally signed cheque to the payee. Using pre-existing financial infrastructure the banks of payer and payee can clear the payment to deduct correct amount from payer's account and to credit same amount to payee's account at their respective banks. Electronic cheques can be cleared online so bounced cheques can be avoided by checking availability of funds instantly. If the payer and the payee have accounts in two different banks then account to account money transfer process is quite lengthy. If the two parties have accounts in same online centralized bank then payment transfer is very simple. The payer connects to the online bank securely and conveys that he wants to transfer some amount to payee's account. The bank then simply has to debit the payee's account and credit payer's account. No extra financial clearing services are needed. If anyone is allowed to open accounts then user to user payments can be easily made. There are a number of online payment systems using this principal. There are different methods to deposit money in centralized accounts. User can connect to these accounts using Secure Socket Layer. The information requested in many of these systems is very casual. Depending on the method of funding the account details of bank account number etc. are requested. The most popular method is using payment card. Any credit card can be used to make payments to this account. This bank acts as merchant accepting credit card payments and clears the payments through acquirer bank.

3.5 Once-off Credit Card Number

In traditional credit cards the credit card number is kept secret. If this number is compromised then attacker can use this information with name, address etc to carry out further transactions. So the obvious way to overcome this problem is to use new credit card number for each transaction. Orbison [21] first brought this system to the market in their product called O-card. Before the O-card system can be used the user must download the O-card application. Whenever a purchase is to be made the O-card application is run. The user can put upper limit on value of this transaction. After this Ocard securely establishes link with card issuer system and generates new card number for this transaction. These numbers are different from the real world credit cards. These numbers have a validity period of one month .Once a transaction is made the card issuer will mark this number as invalid and refuse to process any further transaction based on this number.

4. BLINDING THE PAYMENT

Assume that
R = payer,
E = payee,
R* = R's bank,
E* = E's bank,
xE = E's secret key shared with his bank.
aE = account number of E.

If R wants to pay a sum of money v to E then following steps are followed as shown in Figure 1.
a. R initiates the transaction by sending challenge to E.
b. E replies to the challenge by sending invoice and serial number.
c. R takes the signature of the bank on the serial number makes the payment to E.

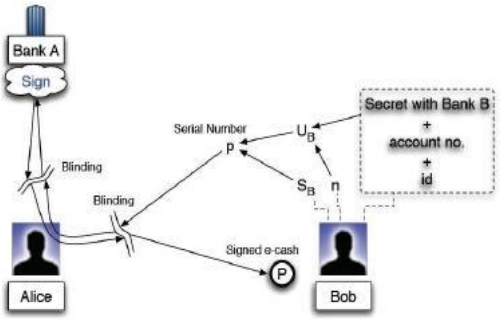

Fig 1: Alice pays Bob with e-cash P

Anonymity is one of the important features of e-cash. When *R* gets signature on the serial number received from E, R's bank *R** can note down the serial number. Later when E's bank *E** sends this serial number to *R** it can trace out that payment to the account of R. If *R** and E* collaborates then it can be traced that *R* has made a payment to *E*. To ensure anonymity, *E* can use blinding [2] of serial number. Blinding technique is proposed by Chaum. Blinding is a kind of transform. For any appropriate random number *r* and a private key *KRd* there is a function blindr and unblindr such that

unblindr ({blindr(p)} KRd) = {p}KRd

This illustrates that we can obtain an indirect signature on a data *p* by first blinding *p* to *p`* then taking signature as *{p`}d* and finally unblinding the signature to get References *{p}d.* This property can also be used in chaining i.e. unblindr ? unblinds is an inverse transform for blinds ? blinds. Actual implementation for RSA signatures is as follows. Suppose *m* is the modulus of the public key of the bank from which signature is to be obtained. Create a random blinding factor *r* such that *r* is relatively prime to *m*. Then create an unblinding factor *u*, which is multiplicative inverse of *r mod m*.
1. The serial number randomly created is blinded as follows.

*Serial#*r^e2(mod m).* Here assume that *e2* is the exponent of the public key of bank for rupees 2 denomination.

2. The bank signs the coin with rupees 2 secret key *d2*.

*(Serial#. r^e2)^d2 (mod m) = serial#^d2 * r^e2^d2 (mod m) = Serial#^d2* r (mod m)*

Here the bank cannot record *serial#* because it does not know *r*.

3. The user after receiving this value multiplies by unblinding factor *u* which is multiplicative inverse of *r mod m*.

*Serial#^d2 * r *u (mod m)*
*= Serial#^d2 * 1 (mod m)*
= Serial#^d2 (mod m)

In this way anonymity can be achieved.

5. TRANSFER THE PAYMENT

The receiver (E)can also transfer this payment to another(*C.*) To do so, *C* generates a serial number

q = H(uC||sC). Where *uC* and *sC* are defined similar to *uE* and *sE*.
Class RSASigner is used for signing the serial number. RSASigner signer = new RSASigner (privExp, modulus); BigInteger signature = signer.getSignature(srNo); Details of method getSignature() are as follows.

```
public BigIntegergetSignature(BigInteger message)
{
    signature = message.modPow(privExp, modulus);

                    return signature;
}
```

5. CONCLUSIONS

In this research work we have discussed various electronic payment systems. Secure Electronic cash schemes and implementation on smart phone platform was the main focus of this work. Some of popular electronic payment schemes have been studied. Different e-cash schemes have been compared.. Infrastructure required for electronic payment systems has been studied. Mobile phone devices provide necessary infrastructure needed for electronic payment systems. But there are very few efficient payment schemes on smart phone platforms. In this work e-cash scheme on smart phone platform has been implemented with secure manner.

For this blinding the e-cash payment must be required.

REFERENCES

[1]. B. Pfitzmann and M. Waidner: "Properties of Payment Systems: General Definition Sketch and Classification", Technical Report RZ 2823, IBM Zurich Research Laboratory, May 1996.
[2]. Chaum D.: "Blind Signatures for Untraceable Payments", CRYPTO82, Plenum Press, New York, USA, pages 199-203.
[3]. Chaum D. and Pedersen T. P.: "Wallet Databases with Observers", In CRYPTO '92 Proceedings of the 12th Annual International Cryptology Conference on Advances in

Cryptology, volume 658, Santa Barbara, California, pages 89–105, USA.
[4]. Chaum D., Fiat A. and Naor M.: "Untraceable Electronic Cash", CRYPTO88 Proceedings on Advances in Cryptology, Springer, Santa Barbara, California, USA, pages 319-327, 2002
[5]. Cristian Zamfir, Andrei Damian, Ionut Constandache and Valentin Cristea: "An Efficient Ecash Platform for Smart Phones".
[6]. C. R. Mandal and Chris Reade: "A Scheme for Recipient Specific Yet Anonymous and Transferable Electronic Cash", Proc. Of WEBIST 2007, Barcelona, Spain, pages 204-209, March 3-6, 2009
[7]. Ebringer T and Thorne P: "Engineering an e-cash system", In Proceedings of 2nd International Information Security Workshop, ISW'99, Kuala Lumpur, pages 32-36, 6-7 November, 1999.
[8]. Heijden and Hans van der: "Factors Affecting the Successful Introduction of Mobile Payment Systems", Vrije Universiteit, Amsterdam, 2002.
[9]. H. Peterson and G. Poupard: "Efficient Scalable Fair Cash With Offline Extortion Prevention", Lecture Notes in Computer Science..
[10]. L. Ferreira and R. Dahab: "A Scheme for Analyzing Electronic Payment Systems", In Proceedings of 14th Annual Computer Security Applications Conference, IEEE Computer Society Press, pages 137-146, December 2000.
[11]. MacKie-Mason and J. K. White, "Evaluating and Selecting Digital Payment Mechanisms", Interconnection and the Internet: selected papers from the 2006 telecommunications policy research conference, Mahwah, NJ, pages 213-234, 2006.
[12]. Marten Trolin: "A Universally Composable Scheme for Electronic Cash" INDOCRYPT Lecture Notes in Computer Science 3797, pages 347-360, 2005.
[13]. N. Asokan, M. Steiner and M. Waidner: "The State of the Art in Electronic Payment Systems", IEEE Computer, pages 28–35, September 1999.
[14]. Odlyzko A. M.: "Discrete Logarithms in Finite Fields and Their Cryptographic Significance", In Theory and Application of Cryptographic Techniques, volume 209, Springer- Verlag, Berlin, pages 224-314, 1984.
[15]. Okamoto T.: "An Efficient Divisible Electronic Cash Scheme", Lecture Notes in Computer Science 963, 438–451, 1998.
[16]. "Multiple-Use Transferable E-Cash", International Journal of Computer Application, Volume 77 - No. 6, September 2013
[17]. Shon T.W. and Swatinan P.M.C.: ""Effectiveness Criteria for Internet Payment Systems", Internet Research: Electronic Networking Applications and Policy, Vol. 8, NO. 3, pages 202-218, 2008.
[18]. Anders Cervera: "Analysis of J2ME™ for Developing Mobile Payment Systems", Master's Thesis in Information Technology, IT University of Copenhagen, 2002.
[19]. Mansour Al-Meaither: "Secure Electronic Payments for Islamic Finance", PhD Thesis, University of London, 2004.
[20]. Bruce Hopkins and Ranjith Antony: "Bluetooth for Java",Apress, 2007.
[21]. Donal O'Mahony, Michael Peirce and Hitesh Tewari: "Electronic Payment Systems for E-Commerce", Second Edition, Artech House, 2001.
[22]. James Edward Keogh: "J2ME: The Complete Reference", McGraw-Hill, 2003.
[23]. Jonathan B. Knudsen: "Java Cryptography", First Edition,Oreilly, 2002.
[24]. William Stallings: "Cryptography and Network Security", Prentice Hall, 3rd edition, 2003.
[25]. Connected Limited Device Configuration (CLDC), JSR 30, JSR 139, http://java.sun.com/products/cldc.
[26]. JAVA Language http://java.sun.com/xml/ns/j2ee/
[27]. Java 2 Micro Edition http://developers.sun.com/techtopics/mobility/j2me/
[28]. Java Security: Tutorial by IBM. http://www-128.ibm.com/developerworks/library/j-midpds.html
[29]. JSR-000082 JavaTM APIs for Bluetooth. http://jcp.org/aboutJava/communityprocess/mrel/jsr082/index.html
[30]. JSR 120: " Wireless Messaging API", http://www.jcp.org/jsr/detail/120.jsp