SETIT 2005
3rd International Conference: **S**ciences Of **E**lectronic, **T**echnologies Of **I**nformation And **T**elecommunications
March 27-31, 2005 – TUNISIA

New probabilistic scheme with Variable Sized Micropayments

Mohamed Hashem 1*, Ahmed M. Hamad 2**,
Mohamed M. kouta 3*** and Yasmine Afify 4*

* Faculty of Computer & Information Sciences, Ain Shams University, Cairo, Egypt.
Email: mhashem100@yahoo.com
Email: yasmine_fcis@yahoo.com
** Vice dean for environment & community affairs, FCIS, Ain Shams University.
Email: amhamad13@yahoo.com
*** Chairman of MIS Department, Arab Academy for Science and Technology.
Email: mmkouta@hotmail.com

Abstract. Micropayments are low-value payments; therefore, the cost of the corresponding electronic transactions should also be kept low. MR2 is an efficient, non-interactive, highly secure probabilistic micropayment scheme designed to facilitate very small scale monetary transactions over the World Wide Web. It uses cryptographic selection to aggregate small payments from different customers into fewer, larger payments, whose processing costs (by the bank) are relatively small. This paper presents a new scheme based on the MR2 scheme proposed earlier by Rivest and Micali. The new scheme handles variable sized micropayments which made it even more feasible and significantly reduced the processing workload for the customer as well as the merchant.

Keywords: cryptographic selection, electronic commerce, micropayments, offline, probabilistic payments.

1 Introduction

In carrying out electronic commerce over the Internet, it is necessary to consider the case where there is a high volume of small value transactions; typically, each transaction's value ranging from a few cents to a few dollars. These payments are called to playing a major role in the expansion of electronic commerce: example applications are access to non-free web pages, pay-per-view TV, music downloads, etc.

To support micropayments, a high degree of efficiency is required; otherwise the cost of the mechanisms will exceed the value of the payments. The micropayment schemes must be able to withstand security attacks such as double spending and coin forgery. However, dealing with very small values makes small losses acceptable. But any large scale cheating must be detected and countered.

The goal of this paper is to present a new probabilistic scheme based on MR2 scheme with the additional feature of handling variable sized micropayment making it more applicable in real commerce applications. By investigating all the aspects of the system, we can explore how each party interacts and determine how to design a micropayment system that is both secure and transparent.

The paper is organized as follows. Section 2 presents an overview of electronic payment systems. Section 3 introduces the micropayment environment. Section 4 reviews the MR2 scheme. Section 5 presents the proposed scheme. Finally, section 6 concludes the paper.

2 Overview of Electronic Payment Systems

Existing protocols such as Cybercash (Cybercash Inc.), NetBill (Cox & al., 1995) and SET (Visa and Master Card 1996) are not suitable for supporting micropayments, as these systems suffer from high transaction costs as compared to the amount of

payments. The cost of transactions is kept high due to the complexity cryptographic protocols used for achieving a certain security level. However, micropayments do not need as much security as speed and simplicity in terms of computing.

Software-only electronic payment systems can be secure if they are fully on-line, so that the issuer participates in each transaction (as in iKp (Bellare & al., 1995) or NetCheque (Neuman & al., 1995)). However, this is not acceptable in micropayments since the communication requirements are excessive regarding that a purchase may cost a fraction of a dollar; therefore, many micropayments schemes have been proposed: PayWord (Rivest & al., 1996), Millicent (Glassman & al., 1995) and NetCard (Anderson & al., 1996) which are off-line. These protocols are based on decentralized validation of electronic payments at the merchant's server, thereby removing any unwanted communications. They don't provide all the desirable features of the conventional payment schemes, but are more efficient and should be adequate for the small sums involved in the micropayments.

Another category of schemes is the probabilistic schemes. Probabilistic schemes can be divided into two categories: probabilistic checking and probabilistic payment. The first two probabilistic checking protocols are: "An efficient micropayment system based on probabilistic polling scheme" (Jareski & al., 1997) and "Agora: A minimal Distributed Protocol for Electronic Commerce" (Gabber & al., 1996). The final category is the probabilistic payment, where the time the vendor cashes to the bank is done probabilistically in order to limit the amount of over-spending (by tuning the rate with which vendor talks to the bank to be a probabilistic function depending on the transaction size). Schemes in this category are: "The electronic lottery tickets as micropayments" (Rivest 1997), "Transactions using bets" (Wheeler 1996) and "Micro-Payments via efficient coin-flipping" (Lipton & al., 1998). MR2 belongs to this category as well.

The evaluation of electronic payment systems is quite difficult, because we experience short of clear and well-defined criteria of the appreciation of the functionality and the quality of such systems. Some of the parameters used for the evaluation are: Confidentiality, Authentication, Client anonymity, Message Integrity, Non-repudiation, Untraceability, Transaction cost, Unforgeability, Double spending prevention, Divisibility, Change return, Software only and Scalability.

3 Micropayment Environment

We consider a system consisting of three major components, the customers (Cs), the merchants (Ms) and a bank (B) (we do not address the issue of multiple banks in this paper). These modules interact with each other to enable a customer to purchase web pages from a merchant.

We assume that the parties have the following parameters:

C: has a secret key SK_C with its corresponding public key PK_C.
has a public key certificate $Cert_C$ issued by the bank.
has a bank account number P issued by the bank.
has the public key of the bank.

V: has a secret key SK_m with its corresponding public key PK_m.
has a public key certificate $Cert_m$ issued by bank.
has the public key of the bank.

B: has a secret key SK_B with its corresponding pubic key PK_B.
has public key of customers and merchants.

A public key certificate contains at least the following: (B, C, PK_U, T, VP) $_{SKBK}$, where U denotes the identity of customer C, T the time at which the certificate was generated, PKc the public key of customer C and VP the period for which the public key is valid . The certificate is digitally signed by the bank.

4 The MR2 scheme

MR2 micropayment scheme retains some of the ideas of two micropayment systems: "PayWord" (Rivest & al., 1996), and "Electronic lottery tickets as micropayments" (Rivest 1997). It also fixes some of their drawbacks. Rivest's lottery tickets suffers from two problems: Interaction in the payment process and that it may charge the customer more than the total value of the checks he has written. PayWord suffers from a main problem: A merchant cannot aggregate micropayments of different customers.

MR2 scheme solved both schemes problems by using a selective-deposit phase, making payment non-interactive while allowing the merchant to learn immediately whether or not check is selected for payment. It also guarantees that an honest customer is never charged more than he actually spent by modifying the charging protocol to depend on the serial numbers of the user's checks. The small risk of excessive payment is shifted from the customer to the bank. For more details, please refer to the original paper (Rivest & al., 2002).

MR2 scheme uses universal aggregation (cryptographic selection), in which, each participating merchant processes micropayments of different customers directly, using special cryptographic software. Universal aggregation turns what was probably a money-losing proposition into a profitable operation for the merchant (Rivest 2004).

4.1 Basic Scheme

Set up: Between each customer and merchant for a secure digital signature scheme.

Payment: Customer pays merchant by sending him a check C = SIGc (T). T includes the transactions details (U, M, bank, web page no, check value, time) and customer's SN. Merchant checks the validity of the transaction by verifying customer's digital signature on the check. If valid, delivers the merchandise to the customer. Check C qualifies for an upgrade if F (SIGm (C)) < s (selection rate). If check is payable, then the merchant sends it along with (SIGm (C)) to the bank. If not, the merchant logs the non-qualifying micropayments.

Selective Deposit: Bank verifies customer and merchant signatures, and that it is a new payable check. It then credits the merchant with 1/s cents. If the serial number SN of the check is greater than maxSN -the maximum serial number of a check of customer processed by bank so far- the bank debits the customer's account by SN – maxSN cents and sets the new SN.

Selective Discharge: The bank keeps statistics and throws out of the system (by revoking their certificates) customers with malicious behavior.

4.2 Features of MR2 scheme

-Offline.
-Authentication: The persons in a transaction are who they claim to be.
-Message Integrity: The information has not been altered since the data was signed.
-Payment Confidentiality: Payment details must not become known to electronic observers able to spy on network traffic.
-Nonrepudiation: Preventing a signatory of a document from denying the submission, delivery or integrity of its contents.
-Software Only.
-Low Transaction Costs (for bank and merchants).
-For customers, there is some anonymity, as bank knows only a fraction of the transactions that the customer made, (but does know which merchants he deals with).

5 Proposed Scheme

In this section, we propose a new scheme based on the above MR2 scheme. It handles micropayments of variable sizes in a smooth and efficient manner; which makes it more feasible and applicable for real commerce applications. A check worth v cents should be treated as a bundle of v one-cent checks with consecutive serial numbers. Instead of the exhaustive operation of sending v one-cent checks to the merchant; in the new scheme, the user will write a single check that, rather having one serial number has a serial number interval, [SN, SN+v] where v is the price of the web page. This will greatly reduce the work carried out by the customer as well as the merchant.

The only relevant factor is the ratio between the macropayment and the micropayment size. For example, for ten-cent micropayments and a 10$ macropayment size, approximately one in every 100 micropayments will qualify for such an upgrade to a 10$ macropayment. The resulting macropayment size will be a fixed system parameter, such as 10$.

Set up: the same as in the original scheme.

Payment: Customer pays merchant by sending him a check C = SIGc (T). T includes the transactions details and a serial number interval [SN, SN+v]. Merchant checks the validity of the transaction by verifying customer's digital signature on the check. If valid, he checks if the interval value [SN+v – SN] matches the price of the specified web page. If valid, he delivers it. Check C qualifies for an upgrade as in the original scheme.

Selective Deposit: Bank makes the same validations, if valid check, it credits the merchant with 10$. If the upper bound of the serial number interval SN+v of the check is greater than maxSN -the maximum serial number of a check of customer processed by bank so far- the bank debits the customer's account by SN+v – maxSN cents and sets the new maxSN by SN+v.

Selective Discharge: the same as in the original scheme.

6 Conclusions

We proposed a new probabilistic scheme based on MR2 scheme that handles micropayments of variable sizes in a smooth and efficient manner. It provides an effective solution to the micropayment problem. It's simple, highly secure, significantly reduces the transaction costs for the bank, minimizes the transaction processing fees for the merchants, and minimizes the number of rounds of interaction between customers and merchants in the payment phase. The customers are only billed for the amount they actually spent. The new scheme seems to be significant for use in practical off-line micropayment systems.

References

(Anderson & al., 1996). R. Anderson, C. Manifavas C. Sutherland, "Netcard - a practical electronic cash system". *Fourth Cambridge Workshop on Security Protocols*. Springer Verlag, *Lecture Notes in Computer Science*, April 1996. Available online URL http://www.cl.cam.ac.uk/users/rja14

(Bellare & al. 1995). M. Bellare, J. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik and M. Waidner, "iKP – A family of secure electronic payments protocols". *First USENIX Workshop on electronic Commerce,* New York, July, 1995.

(Cox & al. 1995). B. Cox, J.D. Tygar, M. Sibru, "NetBill Security and Transaction Protocol". *Proceedings of First USENIX Workshop on Electronic Commerce,* New York, July 11-12, 1995.

(Cybercash Inc.). "The cybercash [tm] system – how it works". http://www.cybercash.com/ cybercash

(Gabber & al., 1996). E. Gabber, A. Silberschatz, "Agora: A Minimal Distributed Protocol for Electronic Commerce". *USENIX Workshop on electronic Commerce*, Oakland CA November, 1996.

(Glassman & al., 1995). S. Glassman, M. Manasse, M. Abadi, P. Gauthier, P. Sobalvaro, "The Millicent Protocol for Inexpensive Electronic Commerce". *Fourth International World Wide Web Conference*, Boston, December, 1995.

(Jareski & al., 1997). S. Jareski, A. Adlyzko, "An efficient micropayment system based on probabilistic polling". *Proceedings of Financial Cryptography Conference* 97, February 1997, Anguilla, BWI.

(Lipton & al., 1998). Richard J.Lipton and Rafail Ostrovsky, "Micro-Payments via efficient coin-flipping". *Proceedings of Second Financial Cryptography Conference*, '98, volume 1465 of *Lecture Notes in Computer Science LNCS*, February 1998.

(Neuman & al. 1995). Clifford Neuman and Gennady Medvinsky, "Requirements for Network Payment: The Netcheque perspective". *Proceedings of IEEE COMPCON*, March 1995.

(Rivest 1997). Ronald L. Rivest, "Electronic Lottery tickets as Micropayments". *Proceedings of Financial Cryptography Conference* 97, LNCS series 1318, pp. 306-314.

(Rivest 2004). Ronald L. Rivest, "Peppercoin Micropayments" ©IFCA 2004. *Proceedings of Financial Cryptography Conference* 2004. Springer.

(Rivest & al., 2002). R. L. Rivest and S. Micali," Micropayments Revisited". In B. Preneel, editor, *Proceedings of Cryptography Track at RSA Conference* 2002, pages 149-263. Springer, 2002.

(Rivest & al., 1996). R. Rivest and A. Shamir, "Payword and Micromint: Two simple micropayment schemes". *Fourth Cambridge Workshop on Security Protocols*. Springer Verlag, *lecture Notes in Computer Science*, April 1996. Available online URL http://theory.lcs.mit.edu/ rivest/publications.html

(Visa and Master Card 1996). "Secure Electronic Transactions (SET) specification". Available online URL http://www.mastercard.com/SET

(Wheeler1996). "Transactions using bets". In *security protocols Int. Workshop*, cambridge, UK April 1996. In LNCS 1189 pp. 89-92. Available online URL http://www.cl.cam.ac.uk/users/cm213/ Project/project publ.html