A NOVEL PEER-TO-PEER PAYMENT SYSTEM

Despoina Palaka
Information Processing Laboratory, Electrical and Computer Engineering Department
Aristotle University of Thessaloniki, 540 06 Thessaloniki, Greece

Petros Daras, Kosmas Petridis and Michael G. Strintzis
Informatics and Telematics Institute
1st km Thermi-Panorama Road, GR-57001 Thermi, Thessaloniki, Greece

Keywords: peer-to-peer, e-payment, anonymous payment.

Abstract: In this paper a novel payment system for Peer-to-Peer (P2P) commerce transactions is presented. It implements electronic cash-based transactions, between buyers and merchants. In this system, financial institutions become partners in the e-commerce transaction, conducted by their customers over the Internet. The innovation of the proposed system is the reduction of the involvement of the financial institutions to ancillary support services. Moreover, the proposed system can be characterized as distributed allocation of provinces to merchants, who are responsible for locally authorizing payments. Finally, it is optimized for repeated payments to the same merchants.

1 INTRODUCTION

With the turn of the century over 70 million computers are connected to the Internet. Successful electronic business sites like Amazon.com (http://www.amazon.com/) or ebay (http://www.ebay.com/) had foreseen the business potential of the huge number of users and offer world-wide services to consumers for buying and selling goods using their web browsers. These business sites provide a centralized trading platform, which offers a certain degree of security to its customers. The advantage of such a centralized architecture is that rules can be enforced easily. However, this turns into a severe problem if we switch the point of view: In any centralized architecture the central entity is a single point of failure and a bottleneck in terms of bandwidth and computing recourses which limits scalability and in turn causes high infrastructure requirements.

Nowadays these kinds of drawbacks have lit a fire under the peer-to-peer (P2P) movement. P2P computing, a term coined after the strong and delivering contents using peer users' computers, scheme, is increasingly receiving attention as a new distributed computing paradigm for its potential to harness "edge" computers, such as PCs and handheld devices, and make their underutilized resources available to each other. In P2P architecture inexpensive computation power, bandwidth and storage are being exploit. Further, computers that traditionally have been used solely as clients communicate directly among themselves and can act both as clients and servers, assuming whatever role is needed at each moment. The new P2P networking paradigm offers new possibilities for electronic commerce. Customer peers interchange roles with merchant peers in this new network economy.

In this paper a new electronic-payment system is presented. The proposed electronic payment system is based on the novel "peer-to-peer" protocol (P. Daras, 2003). This system is considered able to exploit the capabilities offered by P2P networks. The new system provides a complete anonymous, secure and practical framework in which each peer can act both as a merchant and a customer. Further, the proposed system provides a full and secure payment mechanism where personal information (order information) cannot be exposed to unauthorized third parties.

The proposed peer-to-peer payment system uses the basic feature of the Secure Electronic Transaction (SET) protocol (Mastercard, 1997), the digital envelope technique. In SET, message data is encrypted using a randomly generated key that is further encrypted using the recipient's public key. This is referred to as the "digital envelope" of the message and is sent to the recipient with the encrypted message. it can be used for macro-payments as well as for micro-payments. It

Palaka D., Daras P., Petridis K. and G. Strintzis M. (2004).
A NOVEL PEER-TO-PEER PAYMENT SYSTEM.
In *Proceedings of the First International Conference on E-Business and Telecommunication Networks*, pages 245-250
DOI: 10.5220/0001388802450250

enables merchants to locally authorize payments and it uses Millicent's (S. Glassman, 1995) main concept, scrip, which is electronic cash issued by the bank or the merchant.

The rest of the paper is organized as follows. In the following Section a short discussion about traditional (client/server) payment systems and P2P ones, along with some basic definitions and notation, is given. Security considerations regarding the SSL protocol are presented in Section 3. In Section 4 the main transaction steps of the novel peer-to-peer payment protocol are drawn. A short description of the proposed payment system, is given in Section 5. Some security threats and adversaries as well as the security requirements of each party, are described in Section 6. Finally, conclusions are drawn in Section 7.

2 P2P PAYMENT SYSTEMS

Combining the P2P characteristics with the electronic commerce, many companies are promoting payment services via the P2P infrastructure (Trymedia Systems, Lightshare, PinPost, Center-Span, First peer). All these companies claim to support P2P commerce, by using e-mails or SSL (Secure Socket Layer) (A.O. Freier, 1996) for the purchase transaction. But, these systems enable payments through the legacy infrastructure (e.g., clearing and settlement systems) of the financial institutions. In these payments systems there is not a direct communication (P2P communication) between payer (customer) and payee (merchant) (Figure 1). Additionally, the luck of the acquirer gateway is essential, because the "single point failure" problem is eliminated. On the other hand, in existing non-P2P systems, like SET, which is considered to be the most successful and secure payment system, the problem introduced by the payment gateway is essential, but it would be naive to neglect that the acquirer gateway's role is essential for security and financial reasons and it cannot be omitted. In the proposed system three parties are involved (Figures 2,3): the customer (who makes the actual payment), the merchant (who receives the payment) and the acquirer gateway (who acts as an intermediary between the electronic payment world and the existing payment infrastructure and authorizes transactions by using the latter). Hereafter, the acquirer gateway will be addressed as simply the broker. The broker, who is used to "bless" the transactions and to enable a trust relationship between the parties, introduces the problem of "single point failure". However, in this payment system the broker's participation in the transactions has been minimized in order to minimize the effect of the problem that the broker introduces.

In the propsed payment system the broker's role is essential only in the first two transaction steps (P. Daras, 2003) till a trustworthy relationship between the customer and the merchant is established. In the third step, which is the payment transaction, its role is the one of a trusted observer that records the details of the transaction, so that disputes can be handled.

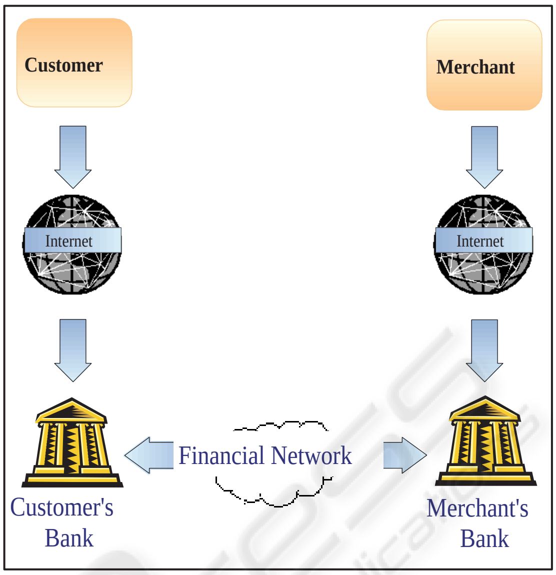


Figure 1: Electronic Commerce models

In the proposed payment system the merchant can authorize payments. This is accomplished by the use of the scrip. As described in (P. Daras, 2003) there are two kind of scrips: BrokerScrip and VendorScrip. The first one can be produced and verified only by the broker and it is used by customers in order to obtain VendorScrip. VendorScrip can be produced and verified by merchants and can be redeemed only to its producer. The main reason for using this type of electronic cash (scrip) is to relieve the banks front-end (broker) from overload and to distribute it in the other parties involved in a product's purchase. Thus, though the proposed system is based on a central entity (broker), its major differentiating factor from traditional electronic commerce models is the reduction of the competence of the financial institutions.

3 SECURITY CONSIDERATIONS OF SSL

While scalability and fault-tolerance come implicitly with P2P infrastructures, as has been proven by successful P2P systems like Kazaa (http://www.kazaa.com/) or Gnutella

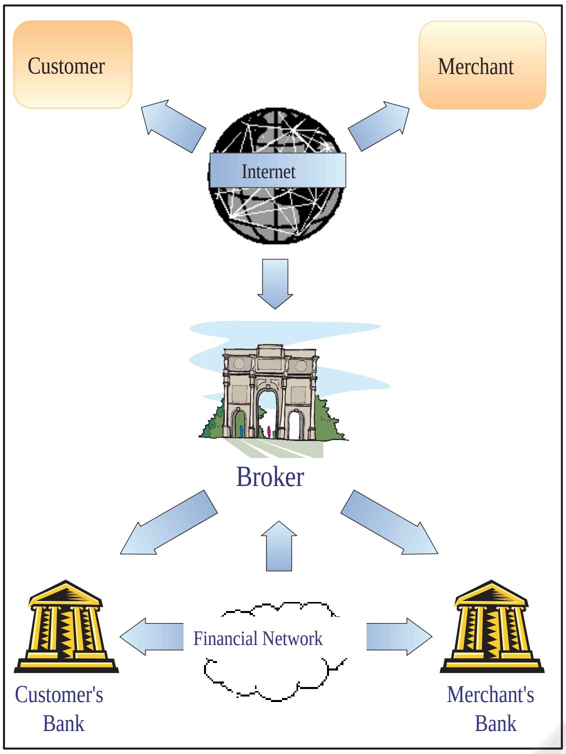


Figure 2: P2P payment system

C	Customer
M	Merchant
B	Broker

Figure 3: Parties

(http://gnutella.wego.com/), security guarantees similar to centralized architectures are more difficult to be achieved in a distributed environment. Moreover, there is a widespread agreement that electronic commerce means for secure electronic payments are needed. Indeed, the appeal of electronic commerce without electronic payment is limited. Further, insecure electronic payments are more likely to impede, than to promote, electronic commerce. Thus the premise of security for electronic payments is of the most importance. SSL is the de facto standard for secure (i.e., encrypted and integrity-protected) communication on the web and it is integrated in almost all web browsers and servers. SSL uses asymmetric encryption but typically only the merchants have public-keys and the customers are anonymous. Encrypting bank account data with SSL is certainly better than sending them in the clear, but the gain in payment security is very limited.

- Regarding the broker, the use of SSL is completely transparent since no messages are signed, thus the merchant does not gain any security.
- SSL does not hide bank account numbers or any other information from the merchant. Thus, it cannot be used in ID-based authorization.
- Unlike SET or peer-to-peer protocol (P. Daras, 2003), SSL does not mandate any specific public-key infrastructure. Thus, there is no guarantee that a customer can verify the merchant's public-key.
- In SSL, merchants and brokers need additional mechanisms (beyond SSL) to transmit bank account data and authorization information.

K_A	is a 192-bits long, symmetric key.
K_{Pr}	is a 1024-bits long, private (asymmetric) key.
K_{Pu}	is a 1024-bits long, public (asymmetric) key.
$Enc_{KA}(.)$	Symmetric encryption using the AES (Rijndael) algorithm.
$Sign_{KPr}(.)$	Digital signature that uses the SHA1 algorithm for hashing and the RSA algorithm for encrypting.
$SignOnly_{KPr}(.)$	Asymmetric encryption (using the RSA algorithm) of a message digest produced by the SHA1 algorithm.
$Enc_{KA}(SignOnly_{KPr}(.))$	Symmetric encryption (using the Rijndael algorithm) of the cipher-text produced by the SignOnly $_{KPr}(.)$ function.
$PKEnc_{KPu}(.)$	Asymmetric encryption using the RSA algorithm.
X,Y	X is concatenated with Y.

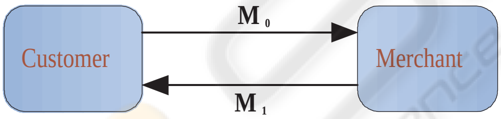
Figure 4: Cryptographic Primitives

4 THE NOVEL PEER-TO-PEER PROTOCOL

In Figure 4 the notation of cryptographic primitives used in the protocol is presented, while in Figure 5 the notation of the basic message elements used in the payment protocol is shown.

C_i	Label of the message .
UID_i	Unique identifier of the peer user.
W_t	Value of the BrokerScrip , VendorScrip or product.
N	Random generated nonce.
ID_i	Unique identifier of the customer's or merchant's bank account.
Br_j	BrokerScrip .
V_j	VendorScrip .
CS_t	BrokerScrip's or VendorScrip's corresponding CustomerSecret.
R	Authorization message. R="OK" or " NOK "
OI	Order information consisting of the product's name, price, quantity and a unique identifier.

Figure 5: Notation of some basic message elements

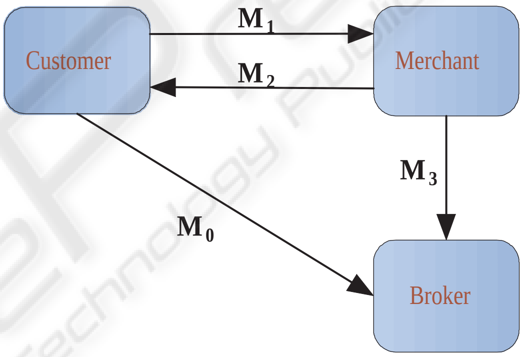


C_0	*BrokerScrip request*
X_0	W_{Br} , N
$\mathbf{M_0}$	$\mathbf{C_0}$ **,** $\mathbf{UID_C}$ **,** $\mathbf{Enc_{K0}(SignOnly_{KC}(ID_C))}$ **,** $\mathbf{Enc_{K0}(Sign_{KC}(X_0))}$ **,** $\mathbf{PKEnc_{KB}(K_0)}$
C_1	*BrokerScrip response*
X_1	Br_0 , CS_0 , N
$\mathbf{M_1}$	$\mathbf{C_1}$ **,** $\mathbf{UID_B}$ **,** $\mathbf{Enc_{K1}(Sign_{KB}(X_1))}$ **,** $\mathbf{PKEnc_{KC}(K_1)}$

Figure 6: Obtain electronic cash from the bank

4.1 Obtain electronic cash from the bank (BrokerScrip)

Initially the customer has neither BrokerScrip nor electronic cash from the merchant (VendorScrip). Through this transaction step (Figure 6), s/he establishes a connection to the broker and buys, using real-money, the desirable BrokerScrip. Having received the payment, the broker delivers the BrokerScrip to the customer. The customer possesses only one BrokerScrip and s/he can obtain a new one only if s/he has spent it all. The BrokerScrip is used so as to obtain electronic cash from a merchant.



C_0	*Initiate Purchase request*
X_0	UID_M , W_P
$\mathbf{M_0}$	$\mathbf{C_0}$ **,** $\mathbf{UID_C}$ **,** $\mathbf{Sign_{KC}(X_0)}$
C_1	*Purchase request*
X_1	V_0 , CS_{V0} , OI
$\mathbf{M_1}$	$\mathbf{C_1}$ **,** $\mathbf{UID_C}$ **,** $\mathbf{Enc_{K0}(Sign_{KC}(X_1))}$ **,** $\mathbf{PKEnc_{KM}(K_0)}$
C_2	*Purchase response*
X_2	V_1 , CS_{V1} , OI
$\mathbf{M_2}$	$\mathbf{C_2}$ **,** $\mathbf{UID_M}$ **,** $\mathbf{Enc_{K1}(Sign_{KC}(X_2))}$**,** $\mathbf{PKEnc_{KC}(K_1)}$
C_3	*Purchase request initiated*
X_3	UID_C , W_P
$\mathbf{M_3}$	$\mathbf{C_3}$ **,** $\mathbf{UID_M}$ **,** $\mathbf{Sign_{KM}(X_3)}$

Figure 7: Buy Item

4.2 Obtain electronic cash from the merchant

When a customer has electronic cash from the bank and s/he wishes to purchase an item from a merchant, s/he needs to obtain electronic cash from the specific merchant (VendorScrip). If the value of the owned BrokerScrip is bigger or equal to the one of the desirable VendorScrip, this transaction step is initiated (Figure 8).

Note, that the requested VendorScrip can be used for payments only to this specific merchant. The broker beyond the verification of the scrip, serves as an observer of the transaction who records the details of it.

4.3 Buy Item

If the customer wishes to purchase an item from a specific merchant and has the appropriate VendorScrip, this scrip can be sent to the merchant (Figure 7). The merchant checks and validates the VendorScrip, s/he reduces its value and sends a new VendorScrip (the change) to the customer. This interaction means that the customer has paid the merchant. In this transaction step both the customer and the merchant inform the broker that a transaction is about to take place or has taken place, respectively.

5 DESCRIPTION OF THE PROPOSED PAYMENT SYSTEM

The proposed payment system is as an on-line system; the central authority (broker) must be contacted during the “Obtain BrokerScrip” and “Obtain VendorScrip” transaction steps, in order to “bless” value transfers and in the “Buy item” transaction step in order to record the transaction details. Even though the online systems are more demanding in terms of communication complexity, than the offline systems, they are considered more secure than the last ones. Additionally, the proposed system can be characterized as direct-payment system, because it requires an interaction between payer and payee.

This system is proper for micro-payments as well as for macro-payments. The desirable usage scenario which fully exploits the benefits of the proposed system is the one where the customer obtains, using macro-payment, BrokerScrip and VendorScrip and then pays for the items using micro-payments. In this scenario the interaction with the broker is minimized and even more his/her role is reduced to the one of an external observer (less computation power is needed, because s/he has just to verify the digital signatures of the messages sent by the customer and the merchant, and then record to a file the details of the transaction).

Implemented on the JXTA (the term “JXTA” is short for juxtapose, as in side by side. It is recognition that P2P is juxtaposed to client-server or Web-based computing, which is today’s traditional distributed computing model) platform, the proposed system does not require any special hardware and it can be implemented in any platform.

Further, it offers some kind of divisibility by allowing users to pay small valued products using high valued scrip and returning the change as new scrip.

Regarding the role inversion the proposed system has interchangeable roles; it allows users to assume different roles (a user can act both as a merchant and a customer), when convenient. However, it does not allow users to become the bank.

In terms of security, the proposed system ensures user’s privacy by allowing anonymous purchases, securing transfers and protecting critical information. Furthermore, it provides the means to detect unauthorized data modification using an auditing mechanism so that errors or misuse can be detected.

6 SECURITY REQUIREMENTS AND SECURITY ANALYSIS OF THE SYSTEM

Internet is a heterogeneous network, without single ownership of the network resources and functions. In particular, one cannot exclude the possibility that messages between the legitimate parties would pass through a maliciously controlled computer. Further, the routing mechanisms in Internet are not designed to protect against malicious attacks. Therefore neither confidentiality nor authentication for messages sent over the Internet can be assumed, unless proper cryptographic mechanisms are employed.

Additionally, one must be concerned about the trustworthiness of the merchants providing Internet service. The kind of business that is expected in the Internet includes the so-called cottage industry-small merchants. It is very easy for an adversary to set up a shop and put up a fake electronic storefront in order to get customers’ secrets (e.g. (Wallich, 1999)). This implies that the customers’ bank account numbers or PINs should travel from customer to broker without being revealed to the merchant.

Finally, in a payment system based on electronic cash, customers should be considered trustworthy. Customers’ attacks on the proposed system are limited to scrip attacks. These attacks are: double-spending, faulty scrip attack and scrip forgery. Double spending involves spending scrip more than once, faulty scrip attack involves creation of scrip without the correct structure and scrip forgery attack involves forging the scrip's data.

1. *Double spending*: scrip is concatenated with two secrets the MasterScripSecret and the MasterCustomerSecret (P. Daras, 2003). These secrets are known only to the producer of the scrip. Each time a scrip is used, its secrets are deleted from the producer's look up tables, ensuring that the scrip cannot be re-spent.
2. *Faulty scrip*: each user of the payment protocol can act both as merchant and customer and s/he is able to produce scrip, but this scrip can only be used to authorize payments with its producer (the scrip carries the Producer's ID).
3. *Scrip forgery*: scrip consists of the scrip body, which contains the information of the scrip and a certificate, which is the signature of the scrip. Any alteration of the information contained in the scrip body can be detected by verifying the scrip's certificate.

7 CONCLUSIONS

In this paper a new payment system is presented. This system is designed to be used in P2P networks. In this system the broker's participation is reduced in order to reduce the "single point of failure" problem. Further, the new system is compliant to all parties' requirements involved in a transaction and offers confidentiality and full anonymity to the customers. Moreover, it establishes a framework for enabling secure payment transactions.

REFERENCES

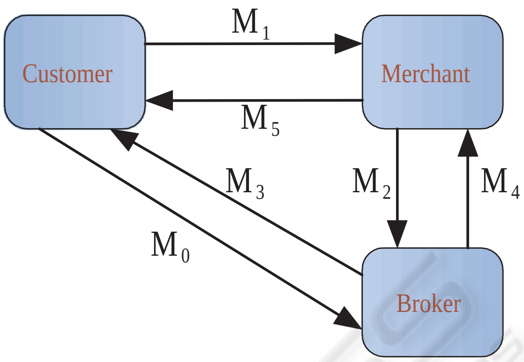
A.O. Freier, P. Kariton, P. K. (1996). The ssl protocol: Version 3.0.

Mastercard, V. (1997). Set 1.0 - secure electronic transaction specification. http://www.mastercard.com/set.html.

P. Daras, D. Palaka, V. G. D. B. K. P. M. S. (2003). A novel peer-to-peer payment protocol. In *Eurocon 2003, The International Conference on Computer as a tool*. Eurocon 2003.

S. Glassman, M. Manasse, M. A. P. G. P. S. (1995). The millicent protocol for inexpensive electronic commerce. In *Proceeding of the 4th International World Wide Conference*.

Wallich, P. (1999). Cyber view: How to steal millions in champ change. In *Sci. Amer., pp. 32-33*. Sci. Amer.



C_0	*Initiate VendorScrip request*
X_0	UID_M
$\mathbf{M_0}$	$\mathbf{C_0, UID_C, Enc_{K0}(SignOnly_{KC}(ID_C)), Enc_{K0}(Sign_{KC}(X_0)), PKEnc_{KB}(K_0)}$
C_1	*VendorScrip request*
X_1	Br_0, CS_{Br0}, W_V
X_2	W_V
$\mathbf{M_1}$	$\mathbf{C_1, UID_C, Enc_{K1}(SignOnly_{KC}(ID_C)), Enc_{K1}(Sign_{KC}(X_1)), PKEnc_{KB}(K_1), Enc_{K2}(Sign_{KC}(X_2)), PKEnc_{KM}(K_2)}$
C_2	*Authorization request*
X_3	W_V
$\mathbf{M_2}$	$\mathbf{C_2, UID_M, Enc_{K3}(SignOnly_{KM}(ID_M)), Enc_{K3}(Sign_{KM}(X_3)), PKEnc_{KB}(K_3), Enc_{K1}(SignOnly_{KC}(ID_C)), Enc_{K1}(Sign_{KC}(X_1)), PKEnc_{KB}(K_1)}$
C_3	*Change BrokerScrip*
X_4	Br_1, CS_{Br1}
$\mathbf{M_3}$	$\mathbf{C_3, UID_B, Enc_{K4}(Sign_{KB}(X_4)), PKEnc_{KC}(K_4)}$
C_4	*Authorization response*
X_5	R
$\mathbf{M_4}$	$\mathbf{C_4, UID_B, Sign_{KB}(X_5)}$
C_5	*VendorScrip response*
X_6	V_0, CS_{V0}
$\mathbf{M_5}$	$\mathbf{C_5, UID_M, Enc_{K5}(Sign_{KB}(X_6)), PKEnc_{KC}(K_5)}$

Figure 8: Obtain electronic cash from the merchant