Yet Another Simple Internet Electronic Payment System

J. Zhao, C. Dong and E. Koch

Fraunhofer Institute for Computer Graphics

64283 Darmstadt, Germany

Phone: +49 (06151) 155-412 (or 147)

Fax: +49 (06151) 155-444

Email: {zhao, dong, ekoch}@igd.fhg.de

Abstract

The potential service providers, customers, as well as financial institutions are constructing geographically the largest global business net in the business history over the Internet. The payment mechanism needed for this new business medium is a very important issue. This paper presents a simple debit-based electronic payment protocol QIPP (Quadro-way Internet Payment Protocol) and its implementation in an electronic commerce system on the World Wide Web. The aim of the QIPP is to provide sufficient security means and least changes to conventional business transaction and payment model for all participants involved in the global electronic commerce.

Keywords

Electronic Payment, Electronic Commerce, Security, Internet, World Wide Web (WWW)

1 INTRODUCTION

The Internet, especially the World Wide Web, is moving from a free, academic domain to a profitable commercial world. There is no need to emphasize the importance of electronic payment for the merging electronic market on the Internet and the unavoidability of such an Internet market. The decentralization of the Internet leads to less personal contact, less trust of participants in this gigantic market. Easiness of eavesdropping and forgery on the Internet incurs a variety of attacks from many sides. Security concerns of the potential customers, merchants and acquirers should be solved not only in technical aspects, but also in social aspects.

An electronic payment system should meet the following requirements: (1) sufficient security means for all the participants in the electronic commerce; (2) similar running scenario as the traditional business when ever possible to ease the doubts of the public and encourage them to participate; (3) less changes on the current financial system to avoid tremendous costs when electronic commerce is introduced.

In this paper we will present a simple, secure Internet electronic payment protocol QIPP (Quadro-way Internet Payment Protocol), which is based on an online debit model. In the

following, first the state-of-the-art electronic payment systems and proposals are presented. Second the QIPP protocol is described. Finally we will discuss briefly the implementation of the QIPP on the WWW through a flexible Web-development-independent security architecture.

2 RELATED WORK

Nowadays, commercial companies start up their Web shops on the Internet. In many cases, service order requires pre-registration of user. Where online payment is supported, credit card data or account PINs will be sent over Internet with more or less security protection in many cases. There are many approaches which target the electronic payment system to solve the problems.

IBM has proposed the iKP (Bellare et al., 1995), which is an online payment system applying CA-based security (i.e. the one-sided security scheme). The iKP can be implemented in different level, just as its name indicated: the 1KP, 2KP and 3KP. Different level of iKP offers different security level: The 1KP does not provide non-repudiation; The 2KP provides only non-repudiation of messages produced by merchant; The 3KP achieves non-repudiation for all messages and parties involved. In the iKP, the authorization of payment is based on the credit card number and associated PIN. The PIN will be encrypted with the public key of the acquirer, so that the merchant will have no chance to abuse the credit card of the customer. The iKP assumes that the PIN is not of necessity in these circumstances, since the signature of the customer already offers protection for the account of the customer.

The NetBill (Sirbu & Tygar, 1995) proposed by Carnegie Mellon University also relies on the public key security system (Kerberos). Micropayments are the major target of this online payment system. Both debit model and credit model are supported in NetBill. NetBill does not describe how to prevent malicious users from re-spending preloaded electronic fund in debit model. In the credit model, the risk of non-payment exists. Moreover, the PIN of a customer is clear to the bank site, so a malicious bank employee is a potential threat to the customer's account. On the other hand, the decryption key is known to the NetBill server (bank) and logged there, anyone who has access to the NetBill server database can intercept the electronic products sent to customer and then use the decryption key to decrypt them.

HP proposal (Mao, 1995) of Hewlett Parkard is another system for online payment. According to the disclaimer by the system designer W. Mao, the system does not utilize public key certification infrastructure, although some observers do not agree with him. The HP proposal applies the one-way hashed values of passwords which are centrally stored in financial institutions. The central point of this proposal is that no decryption algorithm is used for secret retrieval. This aims at the avoidance of the export and import restrictions set by USA and other governments, according to HP. The payment requirement in this system is sent by the merchant to the bank without the signature of the merchant. This could be vulnerable, since anyone can reuse the message in this step and send it to the bank without the real identity being found.

The DigiCash (Chaum, 1992) is an online electronic cash system. The DigiCash system aims to provide the privacy of customers, based on blind signature. When the customer consumes digital cash, the DigiCash multiplies the note number by a random factor and sends it to the bank for signing. Thus, the bank knows nothing about what it is signing except that it carries customer's digital signature. After receiving the blinded note signed by the bank, the customer divides out the blind factor and uses the note as before. The blinded note numbers are unconditionally untraceable. That is, even if the shop and the bank collude, they cannot determine who spent which notes. Because the bank has no idea of the blinding factor, it has no way of linking

the note numbers that merchant deposits with customer's withdraws. The anonymity of blinded notes is limited only by the unpredictability of customer's random numbers.

The AT&T has proposed an Anonymous Credit Card (ACC) system (Low et al., 1994). The ACC utilizes an intermediary to separate the information among the parties involved. To achieve the privacy of the customer, a double locked box (DLB) is used to let message initiator send the message without knowing the destination and vice versa. The major difficulty in implementing this proposal is that the conventional financial system suffers great changes. Social acceptability and legal concerns are other obstacles to this proposal: anonymous credit card requires anonymous account at bank, which may cause problems in some countries where opening anonymous account at bank is not allowed.

CAFE (Conditional Access for Europe) is a project in the European Community's program ESPRIT (Boly et al. 1994). In general, the CAFE system is a prepaid offline payment system and utilizes electronic cash (like the DigiCash). The basic devices of the CAFE system are tamper-resistant electronic wallet, and POS (Point-Of-Sale) terminals which accept the payment from the electronic wallet. The core technique to prevent the same digital cash from multiple uses is to place a guardian chip with a crypto processor inside a wallet. No transaction will be possible without guardian's cooperation: no payment is accepted unless the guardian says OK, and for each unit of electronic money, the guardian gives its OK only once. This is somewhat like a signature by the guardian, but it is a blind signature in the CAFE scenario to protect the privacy of the customer.

Recently, MasterCard and Visa have announced the SET (Secure Electronic Transaction) draft (MasterCard & Visa, 1996) for public comments. This draft also images electronic commerce built on the CA-based security. The SET includes a payment section, which is able to deal with different credit cards. The SET applies acquirer payment gateway which is able to authorize using the existing bankcard networks. In the authorization request sent by merchant to acquirer, the purchase instruction of customer enables the acquirer to verify that the merchant and customer agree as to what was purchased and how much the authorization is for.

Many other electronic payment systems have been developed and more and more are being proposed, for example, the payment system in the European R&D Semper (Secure Electronic Marketplace for Europe) project (Semper, 1995), Kerberos-based NetCash (Medvinsky & Neuman, 1993) and NetCheque systems developed at the Information Sciences Institute of University of Southern California.

3 QIPP – A SIMPLE, SECURE INTERNET ELECTRONIC PAYMENT

QIPP (Quadro-way Internet Payment Protocol) to be described in this section aims to provide a simple yet secure electronic payment for the electronic market on the World Wide Web. Unlike most other payment systems discussed above, the payment will be initiated by the customer, and the merchant is not directly involved in the payment process. Thus, the merchant is virtually excluded from the attacks towards account of customer at the bank, i.e., re-charge or multi-charge is impossible for the merchant. The QIPP simulates the conventional payment in the following three steps: Customer gets the bill from the shop serviceman, pays it by the cashier, and finally shows the receipt to the shop and to get the goods. The interests of the partners in this payment system are well protected, in particular the interests of the customer. In QIPP, customer's bank accounts are double-protected. QIPP introduces minimal changes to current financial systems and to the customer's shopping habits, and naturally does not intend to supplant any other payment systems.

QIPP Overview

An architecture of Internet electronic market is illustrated in Figure 1. As shown in this figure, there are four kinds of players: Customers, Service Providers (or called merchants), Financial Institution presented by acquirer gateway linking to the conventional financial clearing network, and Trusted Third Party (TTP) or Certificate Authority (CA) responsible for all kinds of certification and certificate archiving (Schneier, 1994). The main process of the QIPP protocol consists of four dataflows between the customer and the acquirer. They will be described in detail in the following.

Figure 1 QIPP in an Internet market architecture

There are two assumptions in this protocol. First, the acquirer has widely distributed its public key to the public, so that both customer and merchant has this public key at hand. Second, the public key of both the customer and the merchant shall be exchanged when the business transaction begins. In addition, the widely applied Certificate Authority plays an important role in issuing the certificates to all participants of the electronic business.

Before proceeding, we explain the following notations which will be used to describe the protocol in detail:

- ACQ: The acquirer, which is a gateway to the conventional financial network. We also call the acquirer the bank in this paper.
- MER: The merchant (or called the service provider).
- CUS: The customer (or the user).
- PAYMENT: The information segment indicating payment requirement.
- RESPONSE: The information segment indicating challenge response.
- ACCEPT: Positive response to the prior request.
- REJECT: Negative response to the prior request.
- PK_X: Public key of party X, e.g. PK_CUS is the public key of customer.
- TID: Transaction ID, which must be a unique number produced for each transaction.
- SIG_X: Digital signature of party X using X's private key, e.g. SIG_MER is the signature of the merchant.
- ENC_X: Encryption operation using the public key of party X.
- H(data): One way hash operation on data, e.g. md5 (Schneier, 1994).

- RAN_X: Random number created by party X.
- DATE_X: System date and time obtained by party X during the transaction.
- DESC: Description of the articles provided by the service provider, including article name, article price, amount of article the customer wants to purchase, clearing type (debit or clearing while purchasing), payment type (pay before or after delivery), credit card type, delivery type (on- or off-line), purchase date, delivery date, delivery address (physical or electronic). Besides the essential information described below, the merchant can also extend this structure.
- ID_X: The bank account ID of party X.
- MON_X: The amount of payment requested by party X, e.g. MON_MER is the payment amount that merchant wants customer to pay for the GOODS.
- OT: One-time-key for online delivered goods used by merchant for encryption and by customer for decryption.
- INVOICE: It contains H(DESC), ACCEPT, RAN_MER, DATE_MER, TID, ID_MER, MON_MER. It may optionally include ENC_ACQ(ENC_CUS(OT)).
- GOODS: The article in the transaction, including digital articles (pictures, videos, etc.) as well as non-digital physical articles, which must be delivered offline.

Double protection

Security based on the public key certification authority utilizes a pair of complimentary encryption keys. The public/private key pair serves for secure communication between partners. The key pair is usually physically stored in the system on which the secure application of user runs. Therefore, it relies on the security ability of the system to protect the key pair against potential abuse. If the private key is stolen under certain circumstances, then the security based on this key pair will be a dangerous false friend for the user if the security of all the secret of the user relies on this security key pair, especially when user pays against his account over Internet. This leads us to the idea of double protection, i.e., another protection layer in addition to normal complimentary key pair. The credit card number and its associated PIN, which may be known to the merchant or to the bank, are not suitable for this purpose since a malicious merchant or bank employee can virtually do every thing with this credit account what the user can do with.

To prevent the bank from knowing customer's PINs, the QIPP stores a hashed value of the customer account's PIN in the bank. The following hash function given in (Schneier, 1994) is used in the QIPP:

$$g^x \bmod p \quad (1)$$

if g is a generator modular p and g is less than the prime number p , there will be some x where $g^x \equiv n \pmod{p}$ for each n from 0 to $p-1$. When p is a large prime (Mao, 1995), say, $p=2q+1$, where q is a prime. Then, the user can choose his/her PIN, u , in the interval $[3, q-1]$ and $[q+1, p-2]$ with the conditions that $u \neq 1$, $u \neq 2$, $u \neq q$, and $u \neq 2q-1$. The user gives the result of $g^u \bmod p$ (denoted by $\mathcal{G}^u$) to the bank, stored as a hashed PIN in the bank database.

The following equation is used for challenge verification:

$$(g^x \bmod p)^n \bmod p = (g^n \bmod p)^x \bmod p. \quad (2)$$

During the payment, the bank sends a challenge $g^n \bmod p$, denoted as $\mathcal{G}^n$. Only the holder of the PIN can answer this challenge correctly: The holder of the PIN replies the challenge with

$(\mathcal{G}^n)^u \bmod p$ to the bank. The bank computes $(\mathcal{G}^u)^n \bmod p$ and then compares it with $(\mathcal{G}^n)^u \bmod p$ – if they are equivalent the challenge is answered correctly.

QIPP protocol descriptions

(1) Send bill:

```
ENC_CUS(DESC,
    SIG_MER(H(DESC), ACCEPT, RAN_MER, DATE_MER,
        TID, ID_MER, MON_MER,
        [ ENC_ACQ(ENC_CUS(OT)) ] # this item is an option
    )
) or
```

```
ENC_CUS(DESC, SIG_MER(INVOICE))
```

The item RAN_MER and DATE_MER prevent replay and provide transaction record. The bank account ID_MER is given to the user for money transfer. The ENC_ACQ(ENC_CUS(OT)) is only for the case of online delivery.

(2) Initiate payment:

```
ENC_ACQ(PK_CUS,
    SIG_CUS(H(DESC), PAYMENT, RAN_CUS, DATE_CUS,
        TID, ID_CUS, MON_CUS
    ),
    H(SIG_MER(INVOICE))
)
```

The MON_CUS is given by the customer to the bank, which should be the same as MON_MER, otherwise, the merchant will not deliver the goods afterwards. The H(SIG_MER(INVOICE)) is kept by the bank for the legal evidence in case of discrepancy.

(3) Authorization of challenge:

```
SIG_ACQ(RAN_ACQ, DATE_ACQ,  $\mathcal{G}^n$ ,
    TID, H(INVOICE), ID_CUS
)
```

The nonce to generate $\mathcal{G}^n$ is a large random number, so that each payment challenge will have different $\mathcal{G}^n$. The random number RAN_ACQ is used to prevent replay.

(4) Challenge response:

```
SIG_CUS(RESPONSE, ID_CUS, RAN_CUS, DATE_CUS,
    TID, H(INVOICE),  $(\mathcal{G}^n)^u$ 
)
```

The $(\mathcal{G}^n)^u$ is only correct when the customer gives right PIN, i.e., the u.

(5) Authorization reply:

```
SIG_ACQ(ACCEPT/REJECT, MON_ACQ,
    TID, H(INVOICE), ID_MER, ID_CUS, DATE_ACQ, RAN_ACQ
)
```

The MON_ACQ indicates that the bank has the payment requirement in amount of MON_ACQ.

The invoice sent by the merchant to the customer is signed by the merchant to provide non-repudiation. In case of shopping electronic information goods, an one-time key (OT-key)

encrypted with customer's public key and then re-encrypted using the acquirer's public key is also included in the invoice. The OT-key will be used in the online delivery for encryption of information goods in order to protect the interests of both the customer and merchant, which is realized in the subsequent delivery protocol.

During the payment process, the bank sends a challenge to the customer, only the customer who owns the clear PIN can reply with the correct answer. The payment request sent by the customer is encrypted with acquirer's public key, so that eavesdropper cannot get any information about the payment. The payment amount and other contractual information included in the payment request are signed by the customer to provide authenticity and non-repudiation. Finally, the payment response from the bank is also signed by the acquirer so that both the customer and the merchant can keep acquirer's signature as legal evidence.

4 IMPLEMENTATION

The QIPP has been implemented as one of the three components in an electronic commerce system ELITE (Secure Electronic Commerce on the Internet) developed at the Fraunhofer Institute for Computer Graphics in Darmstadt. The other two protocols in ELITE are for electronic negotiation and for online and offline goods delivery. ELITE has been implemented on the World Web without any specific prerequisites (on security or technology). Figure 2 shows the implementation architecture of the ELITE.

Figure 2 Implementation architecture

Each customer in this architecture is equipped with a WWW browser (NCSA Mosaic 2.7) and a CCI (Common Client Interface) application. The CCI-application, which interacts with the browser according to the CCI protocol (Malgieri & Sanderson, 1995) and communicates with the WWW-server via the browser, is responsible for fulfilling the security functions on the client's side. Each merchant or each acquirer is provided with three components: a WWW-server, a merchant or acquirer application, and a CGI (Common Gateway Interface) program connecting them. The merchant/acquirer application runs as a background daemon to securely perform customer's requests. A set of specific MIME (Multipurpose Internet Mail Extension) types are defined between the CCI applications and the CGI program for re-routing messages from the customer's browser to the CCI applications.

The security packages used in the CCI application and in the merchant/acquirer application are based on an implementation of the GSS API (Generic Security Service) (Lim, 1994), which in turn is based on a secure development security toolkit SeCUDE (Schneider, 1995).

5 CONCLUSION

The QIPP is a simple, flexible protocol for Internet electronic payment system. In sum, it provides the following features: (1) Proof of the payment acceptance for both customer and merchant, (2) Exclusion of unauthorized payment by double protection on customer's account, (3) Protection against eavesdropper, (4) Customer's privacy (but no full anonymity), (5) Minimized changes to current financial system, (6) Minimized attack possibility towards customer's bank account, (7) Unchanged shopping habit for the customer.

The QIPP has been implemented on the World Wide Web and is completely compatible to the Web application in the sense that neither the Web browser nor the Web server need to be changed in order to apply the QIPP. Moreover, the approach to the implementation of the QIPP allows the participants in an electronic commerce to use security mechanisms that are independent of the Web development.

6 REFERENCES

- Bellare, M. et al. (1995) iKP – A family of Secure Electronic Payment protocols, in *Proc. of the First UNENIX Workshop on Electronic Commerce (New York, July 1995)*, also available in <http://www.zurich.ibm.com/Technology/Security/extern/ecommerce>.
- Boly, J. P. et al. (1994) The ESPRIT Project CAFE – High Security Digital Payment Systems, in *EXOR-IC94 (Third European Symposium on Research in Computer Security)*, LNCS 875, Springer-Verlag, Berlin, 1994, pp.217-230.
- Chaum, D.; Fiat, A.; Naor, M. (1988) Untraceable Electronic Cash, in *Advances in Cryptology CRYPTO'88*, S. Goldwasser (Ed.), Springer-Verlag, pp. 319-327.
- Lim, J. (1994) Generic Security Service Application Program Interface, IETF RFC 1508, available as <ftp://ftp.internic.net/rfc/rfc1508.txt>.
- Low, S. H.; Maxemchuk, N. F.; Paul, S. (1994) Anonymous Credit Cards, in *Proc. of 2nd ACM Conference on Computer and Communication Security (Nov. 2-4, 1994)*.
- Mao, W. (1995) A Secure, Cheap, Scalable and Exportable/Importable Method for Internet Electronic Payment, available as <http://www.hp.co.uk/projects/vishnu/main.html>, May 19, 1995.
- Medvinsky, G. and Neuman, B. C. (1993) NetCash: A design for practical electronic currency on the Internet, in *Proc. of the 1st ACM Conference on Computer and Communication Security (Nov. 1993)*.
- Malgiery, T. and Sanderson, B. (1995) Writing Web Software through Client APIs (Mosaic CCI, Netscape), *Tutorial of the Forth International World Wide Web Conference (Boston, Dec. 11-14, 1995)*, also available as http://www.w3.org/pub/Conferences/WWW4/Tutorial_Abstracts.html#D.
- MasterCard & Visa (1996) Secure Electronic Transaction (SET) Specification, available as <http://www.visa.com/cgi-bin/vee/sf/set/settech.html>, Feb. 23, 1996.
- Schneider et al. (1995) SeCUDE 4.4 Overview, available as <http://www.darmstadt.gmd.de/TKT/security/secude/overview.html>, GMD-TKT, Darmstadt, Germany, 1995.
- Schneier, B. (1994) *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Son, Inc., New York et al., 1994.
- Semper (1995) SEMPER – Project AC026 – ACTS Programme, in <http://semper.zurich.ibm.com>. March 1995.
- Sirbu, M. and Tygar, J. D. (1995) NetBill: An Electronic Commerce System Optimized for Network Delivered Services, in *IEEE Personal Commun.*, August 1995, pp. 34-39.