Application of Electronic Currency on the Online Payment System like PayPal

Rafael Martínez Peláez, Francisco J. Rico Novella
Technical University of Catalonia (UPC), Department of Telematics Engineering
C/Jordi Girona 1 i 3, 08034 Barcelona, Spain
{rafaelm, f.rico}@mat.upc.es,
http://www-entel.upc.es/

Abstract. Credit card payment system is the most popular way to make a purchase on electronic commerce. The main problem about using it is that the customer gives his personal information and credit card number to merchant or payment service provider when he makes a purchase in Internet. The result of this action is the lost of customer's anonymity and privacy in both the real world and Internet. We propose a new electronic currency scheme which guarantees customer anonymity and privacy. Also, we integrate our scheme with PayPal system.

1 Introduction

The success of electronic commerce has created the need to develop an electronic payment system to pay for goods and services. Many different electronic payment systems have been proposed [1-8]. Different researches and analysis have been realized about its evolution [9, 10, 11] obtaining a common result, the acceptance of an electronic payment system extended on great scale. Among other reasons, that avoid the acceptance of an electronic payment system are the following: security problems in a public network [12], vulnerabilities in customer's terminal and merchant's server [9], and deficiencies in web applications [13].

Credit card is the mean most popular to develop electronic payment systems [14, 15] accepted by customers and merchants in Internet. Unfortunately, it is not the best method from the anonymity and privacy point of view. Financial institutions (MasterCard and Visa) and payment service provider are still developing systems [16, 17] to motivate the use of credit card in the electronic commerce.

Electronic currency is an alternative to develop electronic payment systems. The concept was introduced by Chaum [18]. Researchers and financial institutions have proposed many systems based on its use [1, 3, 4, 6, 19]. However, its adoption by the

customers is low. The causes that affect its market penetration are: integration between different e-payment systems, security and technological aspects. Some challenges are the global implementation, and the absence of incentives to use electronic currency [19].

In this paper, we propose to integrate the use of Electronic Currency in an Online Payment System (OPS) accepted by customers and merchants of electronic commerce. The paper begins with an electronic currency overview in section 2. In section 3, we examine an Online Payment System: PayPal system, and present a comparison study of efficiency with other OPS based on credit card. We present our proposal and compare it with the current PayPal system in section 4. In section 5, we present our conclusions.

2 Electronic Currency Overview

Money represents the price of products and services on the present society. It is the way most used by customers to make purchase in the real world. The money has different utility in the current economy: store of value, medium of exchange and standard of value [20]. The users of electronic commerce require an electronic currency with similar characteristics to the real money. The electronic currency must be for exclusive use in Internet. Additional, the electronic currency must to permit low value payments and reduce the cost per financial transaction.

2.1 Characteristics and Properties

Electronic payment systems based on electronic currency involve the following participants: customer, merchant and TTP (Trusted Third Party). In the payment protocol where only participate the customer and merchant is named offline payment. In this case, the use of a secure device is necessary. Smart card is a tamper proof device that can to control spending limits of money for customer [6, 9]. For other hand, the protocol that involves all the participants is named online payment. The TTP (bank or payment service provider) must verify the authenticity of electronic currency in each transaction [6, 9].

The success of use of electronic currency in e-payment system depends on the following characteristics [3]:

- Anonymity: The real identity of the customer must be protected. An adversary should not have the option to monitor the customer's activities or knowing the payment's source.
- Acceptability: The electronic currency must be accepted for different financial institutions and payment service provider.
- Scalability: E-payment system based on the electronic currency must be efficient at any time. The increase of users or fails in the communications must not represent a problem in the performance of the system.
- Security: Double spending detection and forgery prevention are basic requirements.

According on the e-payment system, the electronic currency may to satisfy one or all the following properties [20]:

- Atomicity: Permits to link multiple operations logically, so that either all of them are executed or none of them. In Tygar [21], are explained three different levels of atomicity (money, goods and certified delivery) for protecting the protocols and e-commerce.
- Consistency: The participants of an economic transaction must agree about the price of the good and settlements.
- Isolation: The transactions should not interfere with others at the same time. Each transaction must be considered independent of the other ones.
- Durability: The system must be able to recover the information after a disaster. The transaction must be recovered in the last state before the communication was interrupted. If the information stored is modified, the system must recover it.

2.2 User's Requirements

Internet is an opportunity for organizations and institutions to know the customer's purchase habits, make a market research, and trace the customers, making possible the Big Brother problem. The customers of electronic commerce need the following features in e-payment system [22].

- Anonymity: The electronic currency should not disclosed information about the customer's real identity to any participant in the transaction (merchant and TTP).
- Applicability: The electronic currency should be accepted for different merchants and financial institutions.
- Trust: The electronic currency should be durable all the moment. In case of attack, the electronic currency must not give any information to the adversary.
- Convertibility: The electronic payment system must accept different foreign currency.
- Efficiency: If the customer requires generating his/her EC the process should not implicate a high computational cost, and the use of an external device.
- Reliability: The electronic currency should be verifiable by any TTP.

2.3 Micropayments

Micropayment systems were developed to reduce the transactions cost and permit low value payments. Several schemes have been proposed. Each of them can be divided by the representation of the electronic currency: hash value chain, random token and script.

Hash chain

A hash function is a computationally efficient function mapping bits strings of different length, to bits strings of specific length. Hash function H() is computationally unfeasible to find two distinct inputs which hash to a common value. Given a specific hash value y is computationally unfeasible to find an input x, such that h(x) = y. Hash chain was introduced by Lamport [23]. The application of hash chain in electronic payment system was proposed in [24]. Hash chain is a

collection of values, such that each value Z_i is a one-way function of the next value Z_{i-1}. The system is initialized by a seed. The customer randomly chooses a seed X and compute:

$$Z_i = X, Z_{i-1} = H(Z_i), Z_{i-2} = H(Z_{i-1}) \ldots Z_0 = H(Z_1)$$

When a customer wants to make a payment sends the value Z_{i-n} and Z_0 such that is possible to verify the exact payment. In order to verify its validity and authenticity a TTP signs the root value (Z_0) using a public key algorithm. The hash chain technique is used in [5].

Random token

Random token was introduced in Chaum [25]. The random token is based on public-key cryptography and blind signature scheme. The customer executes the blind signature protocol to obtain his/her electronic currency signed by the bank. Blind signature provides the double spending detection, forgery prevention and avoids tracing a customer, keeping his anonymity. The user's anonymity is based in the option to verify the authenticity and validity of electronic currency for any entity using the bank's public key. Moreover, the signer does not know anything about the correspondence between the payer and payee. With this initiative, many protocols have been proposed [6] and basic security requirements have been defined for electronic payment systems [9, 11].

Script

Medvinsky and Neuman [3] proposed the use of new electronic currency based on a script. The script is a set of specific information as IP address, monetary value or time stamping. A characteristic is the use of public key cryptography to encrypt message between participants. Unfortunately, the information stored in the script contains more information that can be used to reveal the users' identity, payment source and gives the ability to know the user's behaviour. Other electronic payment systems based in the script appear in Sirbu and Tygar [7].

3 Online Payment System: PayPal

PayPal is an Online Payment System. It is built on the existing financial infrastructure of bank accounts and credit cards. The main advantage of PayPal is the acceptation by customers and merchants to make payments in Internet. Customer requires creating a system account. When the customer gets an account he/she can have access to resources and services offered by PayPal. PayPal stores user's personal information and credit card information, that can be divided in three subset: (1) create an account (first name, last name, address, city, state, ZIP code, country, and home telephone), (2) PayPal account login (Email address), and (3) payment information (credit card type, name on card, card number, and expiration date).

3.1 PayPal Payment Model

The participants involved in the payment systems are: customer, merchant and PayPal. This system has multiple agreements with different financial institutions like MasterCard and Visa. PayPal works as authorization system in the payment process between the customer and the merchant. The merchant must have a business relationship with PayPal in order to use the payment tools offered by PayPal. With the same account the merchant has the option to maintain the funds in his account of PayPal or transfer it to his bank account [26].

3.2 PayPal Transaction Protocol

The payment protocol begins after the customer decided to pay for an item in a web shop. The price negotiation is outside the PayPal payment protocol. To make the payment in Internet using PayPal, the customer needs to choose “pay with PayPal” (Fig. 1 step 1). The merchant’s web site redirected the customers to PayPal Web site (Fig. 1 step 2). After the step 2, the communication between the customer and PayPal is a secure connection by SSL (Secure Socket Layer). PayPal requests to customer’s identification through his account (Fig. 1 step 3). The customer log in or sign up to PayPal (Fig. 1 step 4). PayPal ask for confirmation or “You made a payment” in PayPal web page (Fig. 1 step 5). The customer accepts or rejects the charge (Fig. 1 step 6). If the customer accepts receive a notification, in the other case, the protocol transaction finishes. PayPal shows to customer the reviews payment information (Fig. 1 step 7). Finally, PayPal redirects the customer to merchant's web shop.

3.3 Protecting Electronic Payment

PayPal creates a secure connection to its server through SSL [14]. SSL is a protocol used to manage the security of the message in a transmission of data across a public network. SSL integrate security services in the session layer for applications as encrypted and integrity over Hyper Text Transfer Protocol (HTTP).

The fraud problem is resolved by the authentication service. This process involves the knowledge of a password that only knows the owner of the account. The repudiation problem is resolved by the authorization of the payment. As additional security parameter the customer receives a notification with the payment details by email

The privacy problem is not resolved, because the user discloses his/her personal and financial information to PayPal. In addition, the financial institutions can obtain knowledge about the customer’s purchase habits. In comparison with other electronic payment system, PayPal requests information to the customer only in the process of creation an account. The information is stored in a central server. In the other case, the user must deliver his/her information to many companies.

Another advantage is the use of pseudonym inside the system. With this pseudonym the merchant does not know the real identity of the customer and does not receive any information directly to him/her [26].

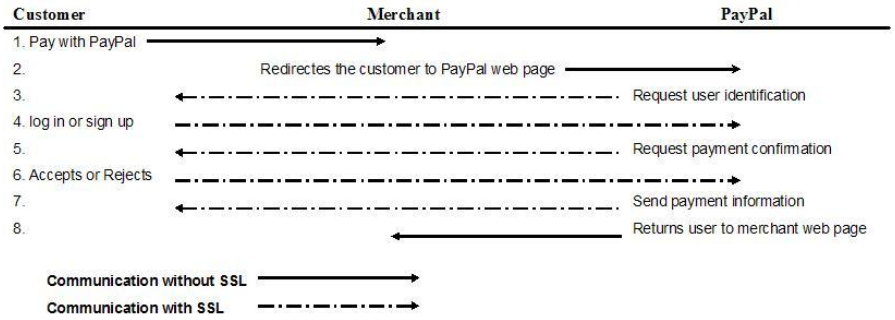

Fig. 1. Transaction Protocol

3.4 Comparison of the current Online Payment System based on Credit Card

Nowadays, there are four online payments systems based on the use of credit card with good acceptance by customers and merchants. The characteristics of SSL, SecureCode (MasterCard), 3-D Secure (Visa) and PayPal are compared in Table 1.

Table 1. Comparison of the actual Online Credit Card Payment System

	SSL	SecureCode	3-D Secure	PayPal
Acceptability	Very popular	Good	Good	Very popular
Anonymity	External entities are able to know information	Only the issuer bank knows information	Only the issuer bank knows information	External entities are not able to know information
Authenticity	Use weak authentication	Use of a secure code	Use of a PIN	Use weak authentication
Compatibility	Good	Good	Good	Good
Convenience	Good: Consumer only need to have a credit card	Good: Customer need to create his private code in his issuer's Web bank	Good: Customer need to create an account in 3D-Secure	Good: Customer need to create an account in PayPal
Financial risk	All the participants can be victims of a fraud	Good	Good	Good
Mobility	Yes	Yes	Yes	Yes
No-repudiation	No	Yes	Yes	Yes
Payment confirmation	No	Yes	Yes	Yes
Privacy	Faulty	Good	Good	Acceptable

4 Proposed New Electronic Currency Scheme

Our proposal provides an alternative scheme to make payments with different merchants using OPS accepted by customers and merchants. With this scheme the issuer of electronic currency and merchant does not have the ability to determine the identity of the payer in the withdrawal and payment transaction. For illustration purpose of the electronic payment scheme, we applied it in PayPal system.

4.1 Generation of electronic currency

In this section, we defined the protocol to generate the electronic currency. Each authenticate customer can to create an electronic currency. The structure of the electronic currency in our scheme includes among other field the last hash value chain signed with the PayPal private key. This signature identifies the value of the coin. The customer randomly chooses a seed X and compute the hash chain $Z_i = H(X)$, $Z_{i-1} = H(Z_i)$, $Z_{i-2} = H(Z_{i-1}) \ldots Z_0 = H(Z_1)$. An i_{max} field is part of the electronic currency allowing a PayPal to determine the denominations. Its value defines the maximum number of hash chain operations that represents the value of the electronic currency. The value_added field specifies the value of the electronic currency. The customer requests the cash that wants to spend using the value_added field. Foreign_currency field indicates the foreign currency that must be used on each payment. PayPal applies the signature on the electronic currency corresponding to the value indicated in the value_added field. The structure of the electronic currency is the next:

$$EC = s^1(Z_0 \parallel i_{max}, \text{value\_added}, \text{foreign\_currency})$$

4.2 Withdrawal phase

The scheme is based on the infrastructure of accounts. The customer must to have an account in PayPal system. In order to open an account the customer must to give personal information to PayPal system. PayPal stores specific information about the user, such as first name, last name, age, street address, city, state, ZIP code and country. Only authenticated customer can withdraw EC. First, the customer decides the value that wants to buy a PayPal and indicates it in the value_added field. Then, the customer chooses the distribution of the electronic currency denomination by the i_{max} field. The denomination permits low value payments and guarantees certain number of payments until the money is spent. The customer chooses which kind of foreign currency wants to use in the foreign_currency field during the payment phase. When a customer defines the foreign_currency value is not possible to modify it. For each electronic currency to be withdrawn from a user's PayPal account, the user executes the blind signature protocol. The customer chooses a blind value r^1 such that $r^1(EC)$. Then sends the value c(EC) to PayPal. PayPal ask to customer for confirmation transaction. If the user decided to reject the transaction the protocol is finalized. In the other case, PayPal applies its digital signature $s^1(r(EC))$ according to value_added field, and forward it to the customer. The customer must to apply the

inverse value r^{-1} to remove the blinding factor to obtain the electronic currency with the PayPal signature $r^{-1}(s^1(r(EC)) = s^1(EC)$. The withdrawal phase is shown in fig. 2.

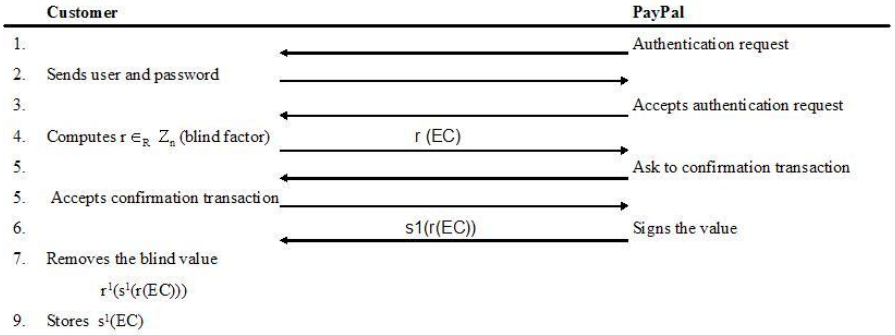

Fig. 2. Withdrawal of electronic currency

4.3 Payment phase

We assume the use of SSL to create a secure communication between the merchant to customer and merchant to PayPal. After the customer and merchant have an agreement about the item to purchases and the amount, the result is recorded in the AEPO (Agreement of Electronic Payment Order). The AEPO is an effort to represent a common payment process made everyday for a person. It contains specific information to make the payment. The payment for field specifies the item to purchase. This field represents an identifier of the product. The quantity field explains clearly how many items are purchased. The gross amount is specifies in the amount field. The cost of transportation is recorded in the shipping field. Fig. 3 shows a payment protocol.

Fig. 3. Payment steps

In order to pay the money to the merchant, the customer sends a clear text message $M = s^1(EC), Z_j, J, V$, to the merchant. The hash value chain that indicates the payment is Zj. J is a pointer that represents the last value of the hash chain used in a purchase phase. V defines the number of hash chain operations that PayPal carries out from Z_j to Z_{i-n}. After verifying $s^1(EC) \equiv s^{-1}(EC) \bmod_n$, the merchant forwards the message, AEPO and it hash value H(AEPO) to PayPal. PayPal receives

the AEPO, H(AEPO) and s^1(EC) from the merchant, and applies the verification proof subprotocol to verify the H(AEPO) and s^1(EC). If the EC is valid, PayPal computes Z_j - Z_i to the last value of the hash chain indicated for J. The operations carried out by PayPal must be the same that the indicated it on V. In the first payment the value of J is equal to 0. PayPal stores all the payments transaction to avoid double spending. The description of the verification proof subprotocol is explained:

Customer SEND M = s^1(EC), Z_j, J, V TO Merchant
Merchant stores M
Verification proof
IF(s^1(EC) ≡ s^{-1}(EC) mod_n)
Merchant SEND M, AEPO & H(AEPO) TO PayPal
PayPal stores M, AEPO & H(AEPO)
Verification proof
IF(s^1(EC) ≡ s^{-1}(EC) mod_n) && (AEPO == H(AEPO))
PayPal stores Z_j, Z_i, J, and V
PayPal computes Z_j - Z_i
PayPal stores finished New Z_i, and J
PayPal SEND confirmation payment TO Merchant
ELSE
PayPal SEND rejects message TO Merchant
ELSE
Merchant finished transaction

PayPal knows the relationship between the merchant and his bank account; therefore, PayPal can maintain the funds in merchant's PayPal account for future use or transfer it to merchant's bank account. After the payment phase is completed, PayPal sends a confirmation payment to Merchant. Then, the merchant shows the confirmation payment through its web page. We present an example of the payment phase.

		Z_i	Z_j	J	V
Initial State		Null	0	0	0
PayPal Stores		Z_0	5	0	5
PayPal Computes		$Z_j - Z_i$ $H(Z_5) = Z_4, H(Z_4) = Z_3, H(Z_3) = Z_2, H(Z_2)=Z_1, H(Z_1) = Z_0$			
PayPal Stores finished		Z_5	0	5	0

4.4 Security Analysis

Properties

- Anonymity: When PayPal signs the electronic currency knows the customer's identity (he/she must be authenticated) but PayPal does not know the value EC

because it is blind under the value r. In the payment phase, PayPal and merchant can not know the customer's identity.

- Privacy: Anyone including PayPal and merchant can not determine to who purchase the item. PayPal and merchant know nothing about the payment source.
- Unforgeable: Only registered customers are able to obtain the PayPal signature. The security parameter in the electronic currency is the value Z_0. Nobody can compute the same hash value such as given a specific hash value y is computationally unfeasible to find an input x, such that h(x) = y.
- Unlinkable: In the payment phase, the merchant and PayPal do not have any information about the customer's identity.

Attacks

- Double spending detection: A customer sends the EC, Zj, J and V to make the payment. PayPal must to verify that EC is authentic. Then, compare the new value of J with the last value stored of J and PayPal verifies the number of operations from the new value Zj to Zi with the value of V too. If the result of both verifications is not the same, a double spending attack is detected.
- Forgery prevention: To have an authentic EC, the customer must to get a PayPal account. The authenticity of the EC is based on PayPal signature. If an attacker sends an EC without a legitimate signature, a forgery attack has been detected.

4.5 Comparison of the current PayPal system vs. Proposal

In Table 2 list the pros and cons of our proposal and PayPal system are measured against the user's requirements and characteristics described in Section 2.

Acknowledgments

This work has been partially supported by the Spanish Research Council (CICYT) under the project SECONNET (TSI2005-07293-C02-01), CREDO (TIC2002-00249), and graduate scholarship from CONACYT (Mexico).

5 Conclusions

In this paper, we paid attention to introduce a new electronic currency scheme and its integration with PayPal. The application of this new electronic currency in an online payment system with good acceptability by customers and merchants has two benefits. First, the use of electronic currency with an Online Payment System extended to great scale can improve its adoption and finally its market penetration. Then the customer's anonymity and privacy in payment phase is maintained. We focus on explain the advantage and disadvantage of one of the most popular electronic payment systems at this moment. We make a comparison between the four current electronic payment systems based on the use of credit card. Finally, we comment the pros and cons of our proposal vs. the current PayPal system.

Table 2. PayPal based on credit card and electronic currency

	PayPal based on Credit Card	PayPal based on our proposal
Anonymity in payment phase	Partial: PayPal knows the customer's identity.	Good: No body knows the client's identity
Applicability	Good	Good
Convertibility	Yes	Yes
Confirmation	Yes: The client receives an email that confirms the payment and includes payment details for this purchase	Yes: The client receives a payment confirmation by the merchant
Ease of use	Yes	Yes
Efficiency	Good	Good
Information stored	Good: Only information about credit card and personal	Faulty: Its necessary to maintain a large database and records of electronic cash
Mobility	Good: Client requires have only a connection to Internet and a browser	Partial: Client requires to install an additional software
Privacy	Partial: PayPal knows the customer's activities and purchase habits	Very Good: Any entity know the customer's activities and purchase habits
Scalability	Good	Good
Traceability	Faulty: PayPal, the bank and other entities can trace the client in both the real world and Internet	Good: Any entity can't trace the client in both the real world and Internet
Transaction information	Merchant sends information about the purchase to PayPal and the client confidences credit card information to PayPal	Customer sends EC and merchant sends AEPO and H(AEPO) to PayPal
Transfer funds	Merchant receives the founds immediately while the bank receives the founds later	PayPal receives the founds before the electronic cash can be used it by the client, the merchant receives the founds immediately, and the bank receives the found later

References

1. B. Cox, J. D. Tygar, and M. Sirbu, NetBill Security and Transaction Protocol, in: *Proceedings of the First USENIX Workshop on Electronic Commerce (New York 1995)* (USENIX, Berkeley, CA, 1995), pp. 77-88, http://www.usenix.org/publications/library/proceedings/ec95/index.html.

2. M. S. Manasse, The Millicent protocols for electronic commerce, in: *Proceedings of the First USENIX Workshop on Electronic Commerce, (New York, 1995)* (USENIX, Berkeley,

CA, 1995), pp. 117-123, http://www.usenix.org/publications/library/proceedings/ec95/index.html.

3. G. Medvinsky, and B. C. Neuman, NetCash: A design for practical electronic currency on the Internet, in: *First Conference on Computer and Communication Security* (ACM, New York, 1993), pp. 102-106.

4. B. Mihir, and J. A. Garay, iKP – A Family of Secure Electronic Payment Protocols, in: *Proceedings of the First USENIX Workshop on Electronic Commerce, (New York, 1995)* (USENIX, Berkeley, CA, 1995), pp. 89-106, http://www.usenix.org/publications/library/proceedings/ec95/index.html.

5. R. Rivest, and A. Shamir, Payword and MicroMint: Two simple micropayment schemes, *Lecture Notes in Computer Science, Volume 1189-Security Protocols* (Springer-Verlag, Berlin, Heidelberg, 1996), pp. 69-87.

6. B. Schoenmakers, Basic Security of the ecash™ Payment System, *Lecture Notes in Computer Science, volume 1528-State of the Art in Applied Cryptography: Course on Computer Security and Industrial Cryptography* (Springer-Verlag, Berlin, Heidelberg, 1997), pp. 338-352.

7. M. Sirbu, and J. D. Tygar, NetBill: An Internet Commerce System Optimized for Network-Delivered Services, *IEEE Personal Communications* **2**(4), 34-39 (1995).

8. L. H. Stein, E. A. Stefferud, N. S. Borenstein, and M. T. Rose, *The Green Commerce Model*, (First Virtual Holding Incorporated, 1995), http://citeseer.ist.psu.edu/cache/papers/cs/3025/ftp:zSzzSzathos.rutgers.eduzSzinternet-draftszSzdraft-stein-green-commerce-model-00.pdf/stein95green.pdf.

9. N. Asokan, P. A. Janson, M. Steiner, and M. Waidner, The State of the Art in Electronic Payment Systems *IEEE Computer Society* **30**(9), 28-35 (1997).

10. Z. Y. Lee, H. C. Yu, and P. J. Kuo, An Analysis and Comparison of Different Types of Electronic Payment Systems, in: *Portland International Conference on Management of Engineering and Technology, PICMET'01* (PICMET, Portland, Oregon, 2001), pp. 38-45.

11. P. Putland, J. Hill, and D. Tsapakidis, Electronic Payment Systems, *BT Technology Journal* **15**(2), 32-37 (1997).

12. B. C. Neuman, Security, Payment, and Privacy for Network Commerce, *IEEE Journal on Selected Areas in Communications*, **13**(8), 1523-1531 (1995).

13. J. D. Tygar, and A. Whitten, WWW Electronic Commerce and Java Trojan Horses, in: *Proceedings of the Second USENIX Workshop on Electronic Commerce, (Oakland, CA, 1996)*, (USENIX, Berkeley, CA, 1996), pp. 243-250, http://www.usenix.org/publications/library/proceedings/ec96/index.html.

14.D. Wagner, and B. Schneider, *Analysis of the SSL 3.0 Protocol*, in: *Proceedings of the Second USENIX Workshop on Electronic Commerce, (Oakland, CA, 1996)*, (USENIX, Berkeley, CA, 1996), pp. 29-40, http://www.usenix.org/publications/library/proceedings/ec96/index.html.

15.Mastercard and Visa, *SET Secure Electronic Transaction Specification, Book 1: Business Description 1.0* (MasterCard and Visa Inc, 1997), http://www.serco.org/set_specifications.html.

16.Visa, *3-D Secure™ Introduction* (Visa International Service Association, San Francisco, CA, 2002), pp. 1-11.

17.GPayments Pty Ltd, *Visa 3-D Secure vs. MasterCard SPA* (Gpayments, French Florest, Australia, 2002).

18.D. Chaum, Blind Signatures for untraceable payments, *Advances in Cryptology Proceedings of CRYPTO 82* (Plenum Press, New York, 1983), pp.199-203.

19.E. Clemons, D. Croson, and B. Weber, Reengineering Money: The Mondex Stored Value Card and Beyond, In Proceedings of the 29th Annual Hawaii International Conference on System Sciences, 1996, (IEEE, Piscataway, NJ, 1996), pp. 254-261

20.L. J. Camp, M. Sirbu, and J. D. Tygar, Token and Notational Money in Electronic Commerce, in: *Proceedings of the first USENIX Workshop on Electronic Commerce, (New York, 1995)* (USENIX, Berkeley, CA, 1995), pp. 1-12, http://www.usenix.org/publications/library/proceedings/ec95/index.html.

21.J. D. Tygar, Atomicity in Electronic Commerce, in: *Proceedings of the fifteenth annual ACM symposium on Principles of distributed computing* (ACM, New York, 1996), pp. 32-43.

22.D. Abrazhevich, Classification and Characteristics of Electronic Payment Systems, in: *Lecture Notes in Computer Science volume 2115-Electronic Commerce and Web Technologies* (Springer Verlag, Berlin, Heidelberg, 2001), pp. 81-90.

23.L. Lamport, Password Authentication with Insecure Communication, *Communications of the ACM* **24,** 770-772 (1981).

24.T. P. Pedersen, Electronic Payments of Small Amounts, in: *Proceedings of the international Workshop on Security Protocols, 1996, Lectures Notes in Computer Science volume 1189* (Springer, Berlin, Heidelberg, 1997), pp. 59-68.

25.D. Chaum, A. Fiat, M. Naor, Untraceable electronic cash, in: Advances in Cryptology CRYPTO, 1988 (Springer Verlag, Berlin, 1990) pp. 319-327.

26.PayPal, *PayPal as a Payment Option: Standard Checkout Integration Guide* (PayPall, San Jose, CA, 2005).