ELSEVIER

Computer Standards & Interfaces 19 (1998) 1–8

COMPUTER STANDARDS & INTERFACES

Greater protection for credit card holders: a revised SET protocol

Jing-Jang Hwang *, Sue-Chen Hsueh

Institute of Information Management, National Chiao Tung University, Hsinchu, Taiwan

Abstract

MasterCard International and VISA International recently proposed the Secure Electronic Transaction (SET) protocol. Constrained by being an extension of the existing card payment networks to the Internet, SET does not satisfy the concern about privacy infringement, in particular, caused by data aggregation. This paper revises SET, guided by the principle of information segregation and hiding. The revision allows cardholders to take part in account reporting, and offers them a credit card surrogate to conceal their credit card identification in the electronic marketplace. The result is a successful counter to privacy infringement in both the small scope of a transaction and the much broader scope of data aggregation.

Keywords: Credit card; Data aggregation; Electronic commerce; Payment system; Privacy; Public-key certificate

1. Introduction

On-line payment by credit card is an option open to consumers. Current practice allows a consumer to conceal, by encryption, his credit card number while sending purchase orders through an Internet browser. Cryptographic routines for encoding and decoding credit card numbers are encapsulated in SHTTP (Secure HyperText Transfer Protocol) [1] within the application layer, or in the SSL (Secure Sockets Layer) protocol [2] within the session layer. While these protocols ensure integrity and confidentiality of transmitted card numbers, senders must still trust receivers. A receiver who is an unscrupulous merchant may steal senders' numbers. Such possibilities discourage security-sensitive consumers from shopping in electronic stores. Clearly, there is a need for secure credit card payment protocols.

Two competing proposals, STT (Secure Transaction Technology) and SEPP (Secure Electronic Payment Protocol), on standards for credit card payment schemes were published in 1995 by VISA International [3] and MasterCard International [4], respectively. In February next year, the two major credit card brands agreed to jointly develop the Secure Electronic Transaction (SET) protocol, and later publish SET as open specifications for the industry [5–7]. The protocol was designed, with technical assistance provided by IBM, GTE, MicroSoft, Netscape, SAIC, Terisa, and Verisign, and it borrows the basic ideas and principles from IBM's Internet Keyed Payment protocol, *i*KP [8]. While the family of protocols *i*KP ($i = 1, 2, 3$) has been submitted to IETF (Internet Engineering Task Force) as an Internet draft [9], the discussions around SET currently dominate the stage of credit card payment over the Internet. Whether SET can emerge as a de factor standard is yet unknown. It will certainly be a basis for future development.

* Corresponding author. E-mail: jjhwang@cc.nctu.edu.tw

0920-5489/98/$19.00
PII S0920-5489(97)00003-2

As a major player in the field, SET deserves a closer look. The protocol aims to be the Internet extension to the existing card payment infrastructure. It implements credit card based transactions between the customer and the merchant while using the existing financial network for clearing and authorization. As such, it serves the banking industry and the credit card brands in particular, but leaves intact the ability of a bank to aggregate consumers' transactional data. This poses a serious concern. One authority notes [10]: ''The principal risk of a fully electronic commercial environment is not that of any particular transaction being improperly handled. Rather, the risk is that of surveillance and data aggregation.'' While SET does protect information from surveillance, it does not address the concern of data aggregation.

In this paper, we present a revision of SET. Basic underlying concepts are these two: (1) We reexamine the information needs of each participating party and hide from a party that data not necessary for the party to perform its function. (2) We create a credit card certificate, which contains an anonymous pseudonym of the cardholder's account number. A business model is developed to describe the revision.

2. The business model

The existing, not-Internet-based infrastructure of the payment card business has defined four roles for participants: Issuer, Acquirer, Merchant, and Cardholder. An *issuer* is the financial institution that establishes an account for a *cardholder* and issues the payment card. An *acquirer* is the financial institution that establishes an account with a *merchant* and processes payment authorizations and payments. In the Internet environment, SET also defines a payment gateway as a device operated by an acquirer or a third party designated for the duty. Here, we do not distinguish between the two. Nor, in general, do we distinguish a party from the party's system.

In the Internet, the processing of card payment transactions resembles that of the mail order or telephone order environment. This corresponds to a transaction where the order and payment information is sent to the merchant by the cardholder, in contrast to a card-present transaction at a store. As shown in Fig. 1, a model for card payment in the Internet will

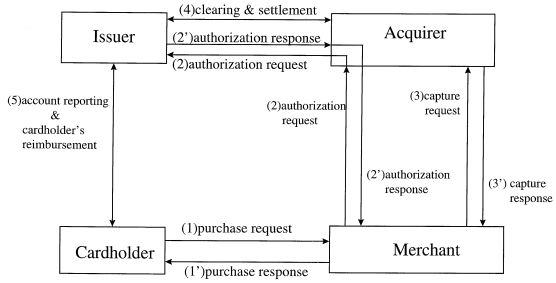


Fig. 1. The business model.

typically proceed through the following stages: (1) Purchase Request, (1′) Purchase Response, (2) Authorization Request, (2′) Authorization Response, (3) Capture Request, (3′) Capture Response, (4) Clearing and Settlement, and (5) Account Reporting and Cardholder's Reimbursement. The SET protocol focuses primarily on stages 1 and 1′, 2 and 2′, 3 and 3′. To further discern the information needs for the issuer and the acquirer, we include in our model the clearing and settlement stage (4). Clearing and settlement is a periodic process by which financial institutions settle charges against each other. We also include in our model the stage of account reporting and cardholder's reimbursement (5). Sending monthly statements to cardholders, the issuer reports on balances in their accounts and asks them for reimbursements. This final stage completes the information cycle.

There are many variations possible with this processing model. If a merchant agrees to ship a purchase prior to the authorization approval, it is at his own risk. A merchant may process captures either in a batch or in a transaction-by-transaction basis. Both authorization and capture messages may be reversed. As one more scenario, a merchant should use a credit message if a cancelled order has been processed. While such variations add to model complexity, the core procedures will determine basic information requirements for all participating parties.

3. Information necessary and information not really necessary

Cardholders can visit Web pages of virtual storefronts or search through CD-ROM catalogues. They

may negotiate with merchants via on-line talks, present a membership to share in a discount, and so forth. Once a cardholder decides on a purchase and opts to use a payment card on-line, he initiates payment processing by sending the purchase order. The cardholder receives a copy of his purchase order called the customer copy, after paying by a credit card in a physical store. Similarly, cardholders would expect to have on-line purchasing records.

Merchants need to obtain information regarding every sale: Who is the customer? What he has decided to buy? Where to deliver the goods? How much he agrees to pay? Purchase orders sent by cardholders fulfill this requirement. Merchants also need to obtain payment instructions from cardholders. The cardholder has an obligation to include in the payment instruction the amount to be debited against his credit card account. If the merchant agrees to the amount, he must forward the instruction to his acquirer.

Fig. 2 shows a mail order form. In SET, as well as our revision, this form is divided into two digital documents, the 'purchase order' and the 'payment instruction'. This division is for the sake of information segregation. The cardholder sends the former to the merchant, and sends the latter to the acquirer via the merchant.

In SET, the essential item bound with the payment instruction is the cardholder's credit card number. SET hides, by encryption, the number from the merchant, but lets the acquirer see the number. What then is the underlying assumption? Is the acquirer trustworthy but not the merchant? The reason that SET trusts financial institutions rest more on SET being an Internet extension to the existing card brand's financial networks than on who is trustworthy. The SET protocol defines the main function of the acquirer's payment gateway as serving interfaces to these networks, such as VisaNet and BankNet. It would seem that the acquirer's access to the card number arises from the existing business practice.

However, is the card number indispensable to the acquirer in performing his duties? A card number links payments with a cardholder's account established by an issuer. The issuer, who must debit payments against a cardholder's account, of course needs to know the account card number. At an acquirer site, a card number, when bound with the payment data, bears an evidence. The acquirer cannot independently take action on the account; rather,

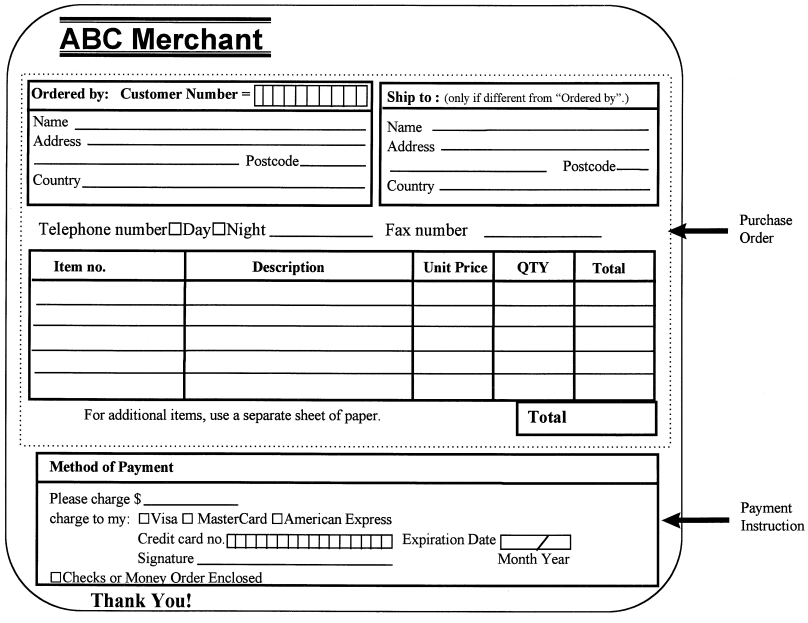


Fig. 2. A mail order form.

he shows the evidential information to the issuer to secure payments. A line can be drawn. An acquirer's job is to secure payment from the issuer, not to charge the account. Therefore, the card number is not really necessary for the acquirer as long as he gets something bearing the same evidential meaning to present to the issuer. What is needed is an anonymous surrogate for the credit card. The criterion is this: Neither the merchant nor the acquirer can deduce the card number from the surrogate, but neither can the cardholder and the issuer repudiate its equivalence to presenting the card number. This demands a cryptographic solution, which is put off until the next section.

What are the cardholder's information needs? Cardholders would like to keep copies of purchase orders for their own reference. They would also like to review purchasing records in days or months. Containing payment amounts and other purchasing information such as where and when purchases took place, a conventional monthly statement satisfies this need. Nevertheless, the monthly statement is a data aggregation. If cardholders want to keep some purchasing data confidential, they cannot leave preparation of the statement to the issuer alone.

We suggest a method that cardholders can use in the reporting stage. Monthly, the issuer sends to the cardholder a statement on which a transaction ID and the payment amount are listed for every purchase. The cardholder fills in other details—what, where, and when he purchased—from his retained copies of purchasing orders; this completes the statement. Given computational power at his desk, the cardholder can get the job done in minutes. The transaction ID is the information linkage.

In the programmer's guide of SET [[6]: p. 248], the transaction ID is defined as a combination of a few consecutive identifications: (1) LID_C: local ID, convenience label generated by and for the cardholder (system); (2) LID_M: local ID, convenience label generated by and for the merchant (system); (3) XID: globally unique ID; (4) PReqDate: purchase request date; (5) PaySysID: used by some associations to label transaction from time of authorization onward; (6) Language: language tag for the entire transaction; (7) SWIdent: identification of the software (vendor and version) initiating the request.

To produce a complete monthly statement, either LID_C or XID is the data item to link the information provided by the issuer with the information stored at the cardholder's site. Fig. 3 illustrates the concept.

The variety of identifiers in the transaction ID provides a powerful tool for information segregation

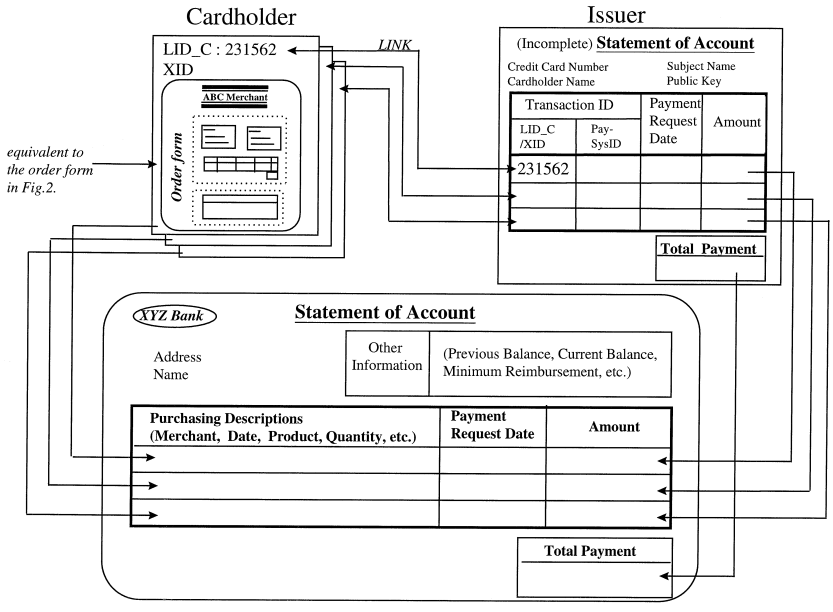


Fig. 3. Monthly reporting.

and linkage. The usage of LID_C or XID in the reporting stage is one example. Another example is the usage of PaySysID, which enables the existing card brand's network to relate each message to the transaction. Except payments related information, much purchasing information is irrelevant to the acquirer's job. Using PaySysID to collate messages, the acquirer is able to perform his duties, i.e., requesting the issuer to authorize payment, confirming the merchant, responding to the merchant with payment captures, requesting clearing, and so forth.

PaySysID is essential to SET for it plays a key role in connecting this protocol with the existing card payment system, but the credit card number is not. This number only provides evidential information, its function at the merchant's and acquirer's sites can be fulfilled by the cryptographic means introduced in Section 4.

4. Credit card certificate: an anonymous surrogate for the credit card

Like all *i*KP protocols and other on-line payment means such as digital cash, SET is based on public–key cryptography. It uses public–key certificates for entity and message authentication; all are X.509 version 3 certificates [11] with standard and private extensions. Considering a credit card account as the subject in the X.509 terminology, we define a credit card certificate the same way. The certificate consists of two parts: one of them is the account's credentials in clear text—unique name of the subject (account), public key and expiry date; the other one is a certificate authority's (CA's) signature of the credentials. The legality of the CA's signature must be recognized by the card issuer, for the card issuer is obligated to pay charges to the certificate, which substitutes for a credit card. The card issuer or the card brand is the ideal agent of the CA. Fig. 4 illustrates the credit card certificate.

A copy of the credit card certificate must be included in the payment instruction. Following the principle of information segregation and hiding, the instruction is encrypted for the acquirer. The merchant cannot see the certificate, but the acquirer can.

What the acquirer identifies from the certificate is the subject name, which is an anonymous substitute for the card number. To maintain anonymity, correspondence between the card number and the subject name is only known to the cardholder and the issuer. Without purchasing information and the card number, the information that an acquirer can accumulate is limited and, above all, without identifications.

Also contained in the credit card certificate is a public key. The corresponding private key is given to the certificate owner, i.e., the cardholder. When the cardholder decides to pay on-line with his credit card, he includes the payment amount and his credit card certificate into the payment instruction, signs

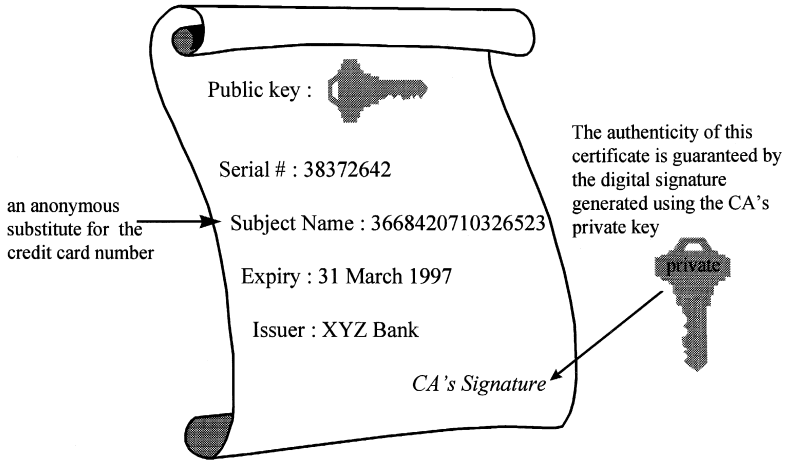


Fig. 4. A credit card certificate.

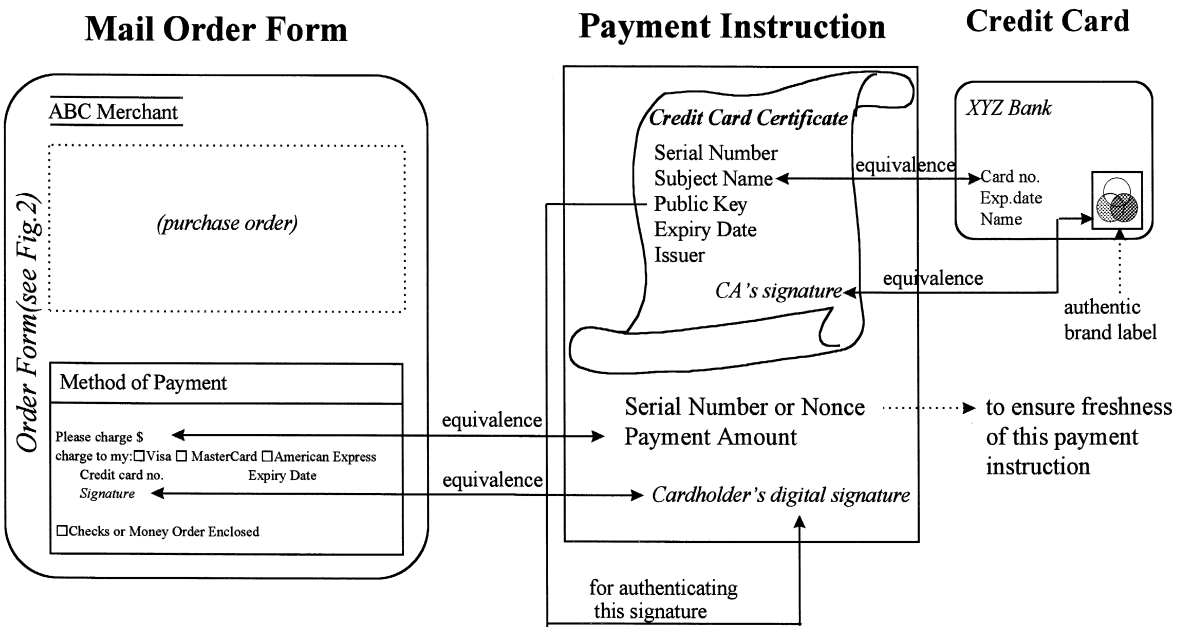


Fig. 5. Functions of the credit card certificate.

the digital document using this private key, and appends the digital signature at end of the payment instruction. These actions are equivalent to that, when filling a mail order, the cardholder fills the amount and his credit card number in the form of payment and gives his handwritten signature on the form. We illustrate this equivalence in Fig. 5.

To defend against replay attacks, a unique number is included in each payment instruction before the document being signed, as shown in Fig. 5. This figure also indicates that a challenge nonce is included to ensure the freshness of a new payment instruction. An on-line CRL (Certificates Revoked List) for the credit card certificate is also needed. Other techniques for security management can be found in the SET specifications [6,7] or in the X.509 document [11].

5. Credit card certificate vs. cardholder certificate

The usage of certificates in SET is already heavy. Table 1 is a complete list of all types of certificates needed in SET. Usage is mandatory for all certificates in this table except the cardholder certificate, whose usage is optional. This certificate offers a

Table 1
All types of certificates in SET [[4]: p. 28]

Entity	Message signature	Key-exchange	Certificate signing	Certificate revocation list (CRL) signing
Cardholder	X (optional)			
Merchant	X	X		
Acquirer Payment Gateway	X	X		
Cardholder CA	X	X	X	
Merchant CA	X	X	X	
Acquirer Payment Gateway CA	X	X	X	X
Geo-political CA			X	X
Brand CA			X	X

strong tool not only for authenticating messages but for authenticating the sender, the cardholder.

MasterCard and VISA have foreseen the necessity of the cardholder certificate. The usage of this certificate will become mandatory in later versions of SET [12]. Yet the credit card certificate, which we propose in this revision, and SET's cardholder certificate differ on one essential aspect. The former contains a substitute for the credit card number; this substitute replaces the real credit card number in all messages that require the number. The latter contains a hash value of the credit card account information, which is composed of the cardholder's credit card number, its expiration date, and the shared secret computed using independent nonces generated by the cardholder and the CCA (Cardholder Certificate Authority) [[6]: p. 69]; this hash is useful for validating the credit card number but *cannot* replace it. The difference is significant.

It is worth accentuating the difference further. The credit card certificate of this revision is a digital surrogate of the plastic credit card. The identification of the surrogate replaces the card number throughout the whole cycle of the payment transaction, which includes authorization and clearing stages conducted over the existing proprietary network. The (real) credit card number never enters the Internet. In contrast, the cardholder certificate is not a surrogate. This certificate is a tool for entity and message authentication but cannot fulfill, by itself, the demand for the credit card number. The SET protocol has to reveal the number to the acquirer.

6. Benefit and cost

Our revision adds greatly to the cardholder's privacy. Due to the principle of information segregation and hiding, no party can gather information beyond their business needs. In particular, using the credit card certificate, one can segregate credit card information from transactional payment information, and can hide the credit card number from the acquirer but allow the acquirer to ask the issuer for payments by presenting a copy of the certificate. The issuer must recognize it as being equivalence to a presence of the credit card since it bears the CA's signature. On the other hand, the cardholder must admit his liability for payment since the payment instruction bears his digital signature.

Our revision requires a minor cost at the cardholder's site. The cardholder must keep copies of purchase orders. The cardholder must pay this cost, if he wishes to have a *complete* monthly statement. Active engagement is an effective way to prevent the issuer from data aggregation.

A significant cost would arise from the accommodation of the existing card payment networks to the usage of cryptography. Here, we use a substitute, the subject name in the credit card certificate, to replace the traditional credit card number. The change is certainly not minor since it involves alterations to the existing systems, in particular, that at the issuer's site, where the link between each (real) credit card number and a substitute must be established. We believe, however, that the card brands and the financial institutions must pay the price given that consumers' privacy is more vulnerable to the threat of data aggregation in the environment of electronic commerce. It all comes down to providing an additional customer service in a highly competitive marketplace.

7. Conclusion

Security and privacy are two major concerns when consumers enter the world of electronic commerce. Addressing these issues, SET applies standard cryptographic techniques to entity authentication, data authentication, and confidentiality protection, on a transaction-by-transaction or message-by-message basis. Our revision goes two steps further. First, usage of the credit card certificate lets the cardholder present a credit card surrogate that conceals his credit card identification. Second, usage of the transaction ID lets the cardholder himself take part in monthly reporting. Consequently, data aggregation becomes impossible.

Some cryptographic applications are common sense. Some quite complex. The technology is something too important to leave to groups with special interests. Cryptographic applications must be guided by some principles that are compatible with personal preferences. Our basic guideline for the revision, information segregation and hiding, is a principle

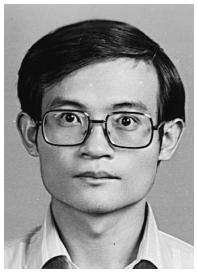
that respects the value of privacy. We believe this is one of fundamental principles in the field of electronic commerce.

Acknowledgements

The authors would like to thank Dr. Clinton H. Whitehurst for many useful comments. They also thank the support from the government of Taiwan, Republic of China, under the Contract No. NSC-86-2416-H-009-004.

References

[1] E. Rescorla, A. Schiffman, The Secure HyperText Transfer Protocol, Internet Draft, Enterprise Integration Technologies, December 1994.
[2] K.E.B. Hickman, Secure Socket Library, Netscape Communications, February 1995.
[3] VISA and MicroSoft, Secure Transaction Technology (STT) Specification, VISA International, September 1995.
[4] IBM, Netscape, GTE, CyberCash, MasterCard, Secure Electronic Payment Protocol (SEPP) Specification, MasterCard International, September 1995.
[5] MasterCard and VISA, Secure Electronic Transaction (SET) Specification, Book 1: Business Description (draft for testing), June 1996.
[6] MasterCard and VISA, Secure Electronic Transaction (SET) Specification. Book 2: Programmer's Guide (draft for testing), June 1996.
[7] MasterCard and VISA, Secure Electronic Transaction (SET) Specification. Book 3: Formal Protocol Definition (draft for testing), June 1996.
[8] M. Bellare, J.A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, M. Waidner, *i*KP-A family of secure electronic payment protocols, in: Proceedings of Usenix Electronic Commerce Workshop, July 1995.
[9] M. Linehan, G. Tsudik, Internet Keyed Payment Protocol (*i*KP), IBM, Internet Draft, July 1995.
[10] D.E. Geer, Electronic commerce, banking and you, Comp. Sec. J. 11 (2) (1995) 55–62.
[11] ITU Rec. X.509 (1993)\ISO/IEC 9594-8: 1995, Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, including Draft Amendment 1: Certificate Extensions (Version 3 certificate), ISO/IEC JTC1/SC21/WG4 and ITU-T Q15/7, April 1996.
[12] T. Lewis, Lecture Notes in the SET Technology, VISA International, November 1996.



Jing-Jang Hwang (jjhwang@cc.nctu.edu.tw) began his academic career in 1976 as an instructor at National Chiao Tung University in Taiwan, Republic of China. He is now the chairman and a professor of the Institute of Information Management at the same university. He received his PhD degree in 1987 from the University of Florida. In addition to teaching, he has been involved in research on subjects of management information systems, electronic commerce, information security, distributed systems, and cryptography. He has contributed research articles, in the English language as well as in the Chinese language, to various magazines and journals.

Sue-Chen Hsueh received her M.B.A. degree in 1994 with major in information management from National Chiao Tung University in Taiwan, Republic of China. She is currently doing research on the subject of on-line payment for her PhD degree.