

The State of the Art in Electronic Payment Systems

Electronic funds transfer over financial networks is reasonably secure, but securing payments over open networks like the Internet poses challenges of a new dimension. This article surveys the state of the art in payment technologies and sketches emerging developments.

N. Asokan
 Phillipe A. Janson
 Michael Steiner
 Michael Waidner
 IBM Zurich Research Laboratory

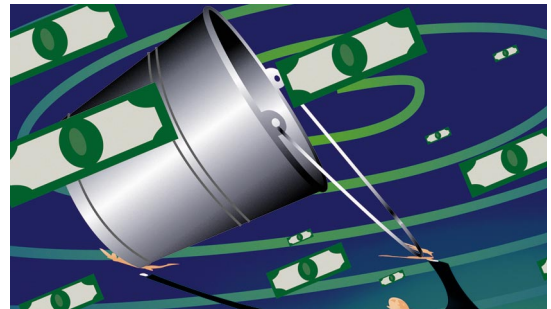
The exchange of goods conducted face-to-face between two parties dates back to before the beginning of recorded history. Eventually, as trade became more complicated and inconvenient, humans invented abstract representations of value. As time passed, representations of value became more and more abstract, progressing from barter through bank notes, payment orders, checks, credit cards, and now electronic payment systems.

Traditional means of payment suffer from various well-known security problems: Money can be counterfeited, signatures forged, and checks bounced. Electronic means of payment retain the same drawbacks and some additional risks: Unlike paper, digital “documents” can be copied perfectly and arbitrarily often; digital signatures can be produced by anybody who knows the secret cryptographic key; a buyer’s name can be associated with every payment, eliminating the anonymity of cash.

Thus without new security measures, widespread electronic commerce is not viable. On the other hand, properly designed electronic payment systems can actually provide better security than traditional means of payments, in addition to flexibility of use. This article provides an overview of electronic payment systems, focusing on issues related to security. Pointers to more information on several payment systems described can be found at <http://www.semper.org/sirene/outsideworld/ecommerce.html>.

ELECTRONIC PAYMENT MODELS

Commerce always involves a payer and a payee—who exchange money for goods or services—and at least one financial institution—which links “bits” to “money.” In most existing payment systems, the latter role is divided into two parts: an issuer (used by the



payer) and an acquirer (used by the payee). Electronic payment is implemented by a flow of money from the payer via the issuer and acquirer to the payee.

Figure 1 shows some typical flows of money in the case of prepaid, *cash-like* payment systems. In these systems, a certain amount of money is taken away from the payer (for example, by debiting the payer’s bank account) before purchases are made. This amount of money can be used for payments later. Smart card-based electronic purses, electronic cash, and bank checks (such as certified checks) fall into this category.

Figure 2 shows some typical flows of money in the case of bank-card-based systems, which include pay-now systems and pay-later systems. In pay-now payment systems, the payer’s account is debited at the time of payment. Automated-teller-machine (ATM) cards fall into this category. In pay-later (credit) payment systems, the payee’s bank account is credited the amount of sale before the payer’s account is debited. Credit card systems fall into this category. From a protocol point of view, pay-now and pay-later systems belong to the same class: Because a payment is always done by sending some sort of “form” from payer to payee (whether it be a check or credit card slip or some other form), we call these systems *check-like*.

Both types of payment systems are direct-payment systems: A payment requires an interaction between payer and payee. There are also indirect payment systems, in which either the payer or the payee initiates payment without the other party involved online. Electronic funds transfer is one example of an indirect payment system.

SECURITY REQUIREMENTS

The concrete security requirements of electronic payment systems vary, depending both on their features and the trust assumptions placed on their operation. In general, however, electronic payment systems must exhibit integrity, authorization, confidentiality, availability, and reliability.

Integrity and authorization

A payment system with integrity allows no money to be taken from a user without explicit authorization by that user. It may also disallow the receipt of payment without explicit consent, to prevent occurrences of things like unsolicited bribery. Authorization constitutes the most important relationship in a payment system. Payment can be authorized in three ways: via out-band authorization, passwords, and signature.

Out-band authorization. In this approach, the verifying party (typically a bank) notifies the authorizing party (the payer) of a transaction. The authorizing party is required to approve or deny the payment using a secure, out-band channel (such as via surface mail or the phone).

This is the current approach for credit cards involving mail orders and telephone orders: Anyone who knows a user's credit card data can initiate transactions, and the legitimate user must check the statement and actively complain about unauthorized transactions. If the user does not complain within a certain time (usually 90 days), the transaction is considered "approved" by default.

Password authorization. A transaction protected by a password requires that every message from the authorizing party include a cryptographic check value. The check value is computed using a secret known only to the authorizing and verifying parties. This secret can be a personal identification number, a password, or any form of shared secret (defined in the sidebar "Basic Concepts in Cryptography and Security").

In addition, shared secrets that are short—like a six-digit PIN—are inherently susceptible to various kinds of attacks. They cannot by themselves provide a high degree of security. They should only be used to control access to a physical token like a smart card (or a wallet) that performs the actual authorization using secure cryptographic mechanisms, such as digital signatures.

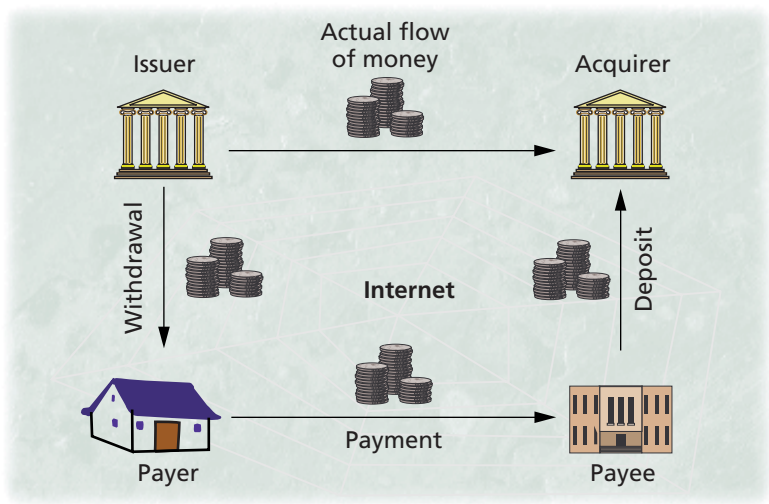


Figure 1. Money flow in a cash-like payment system.

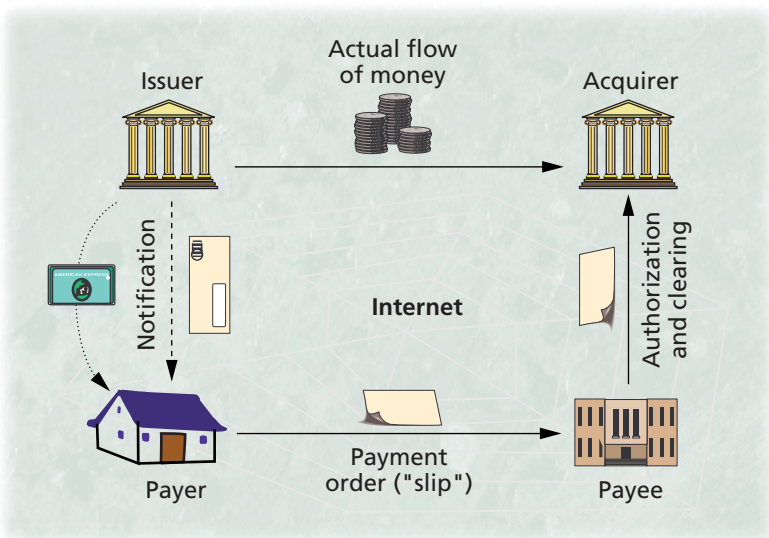


Figure 2. Money flow in a check-like payment system.

Signature authorization. In this type of transaction, the verifying party requires a digital signature of the authorizing party. Digital signatures provide nonrepudiation of origin: Only the owner of the secret signing key can "sign" messages (whereas everybody who knows the corresponding public verification key can verify the authenticity of signatures.)

Confidentiality

Some parties involved may wish confidentiality of transactions. Confidentiality in this context means the restriction of the knowledge about various pieces of information related to a transaction: the identity of payer/payee, purchase content, amount, and so on. Typically, the confidentiality requirement dictates that this information be restricted only to the participants involved. Where anonymity or untraceability are desired, the requirement may be to limit this knowledge to certain subsets of the participants only, as described later.

Basic Concepts in Cryptography and Security

Cryptographic techniques are essential tools in securing payment protocols over open, insecure networks. Here we outline some relevant basic concepts.

Message authentication

To authenticate a message is to prove the identity of its originator to its recipient. Authentication can be achieved by using shared-key or public-key cryptography.

Shared-key cryptography

The prover and the verifier share a common secret. Hence this is also called *symmetric authentication*. A message is authenticated by means of a cryptographic check value, which is a function of both the message itself and the shared secret. This check value is known as the *message authentication code* (MAC).

Public-key cryptography

Each entity has a matching pair of keys. One, known as the signature key, is used for computing signatures and is kept secret. The other, known as the verification key, is used to verify signatures made with the corresponding signature key; the verification key is made public along with a certificate binding an entity's identity to its verification key. Certificates are signed by a well-known authority whose verification key is known a priori to all verifiers. A message is authenticated by computing a digital signature over the message using the prover's signature key. Given a digital signature and a certificate for its verification key, a verifier can authenticate the message. Authentication of messages using MACs does not provide nonrepudiation of origin for the message, whereas authentication using digital signatures does.

Attacks

Electronic payment protocols can be attacked at two levels: the protocol itself or the underlying cryptosystem.

Protocol-level attacks

Protocol attacks exploit weaknesses in the design and/or implementation of the high-level payment system. Even if the underlying cryptographic techniques are secure, their inappropriate use may open up vulnerabilities that an attacker can exploit.

Freshness and replay. A protocol may be attacked by replaying some messages from a previous legitimate run. The standard countermeasure is to guarantee the freshness of messages in a protocol. Freshness means that the message provably belongs to the current context only (that is, the current payment transaction) and is not a replay of a previous message. A nonce is a random value chosen by the verifying party and sent to the authenticating party to be included in its reply. Because nonces are unpredictable and used in only one context, they ensure that a message cannot be reused in later transactions. Nonces do not require synchronization of clocks between the two parties. Consequently, they are very robust and popular in cryptographic protocol design. In general, nonces are an example of the challenge-response technique.

Fake-terminal. Protocols that perform authentication in only one direction are susceptible to the fake-terminal attack. For example, when a customer uses an ATM, the bank and the machine check the authenticity of the customer using a PIN. The customer, however, cannot be sure whether the ATM is a genuine bank terminal or a fake one installed by an attacker for gathering PINs. Using a trusted personal device, such as a smart

card or electronic wallet, helps avoid this attack.

Cryptosystem attacks

Cryptosystem attacks exploit weaknesses in the underlying cryptographic building blocks used in the payment system.

Brute force attack. The straight-forward cryptosystem attack is the brute force attack of trying every possible key. The space from which cryptographic keys are chosen is necessarily finite. If this space is not large enough, a brute force attack becomes practical. Four-digit PIN codes have a total of 10,000 permutations in the key space. If a value X is known to be the result of applying a deterministic transformation to the PIN, one can use this X to search the set of all possible PINs for the correct one. In some applications one can increase the protection against brute force attacks by randomization. Even if the key space is large, the probability distribution of keys is not necessarily uniform (especially for user-chosen PINs, which are likely to be related to the user's birthday, phone number, and so on). It might then be possible to mount dictionary attacks. Instead of trying every possible key as in the brute force attack, the attacker will only try the keys in "dictionary" of likely words, phrases, or other strings of characters.

Cryptanalysis. More sophisticated attacks, called cryptanalysis, attempt to explore weaknesses in the cryptosystem itself. Most cryptosystems are not proven secure but rely on heuristics, experience, and careful review and are prone to errors. Even provably secure cryptosystems are based on the intractability of a given mathematical problem (such as the difficulty of finding graph isomorphism), which might be solvable one day.

Availability and reliability

All parties require the ability to make or receive payments whenever necessary. Payment transactions must be atomic: They occur entirely or not at all, but they never hang in an unknown or inconsistent state. No payer would accept a loss of money (not a significant amount, in any case) due to a network or system crash.

Availability and reliability presume that the underlying networking services and all software and hardware components are sufficiently dependable.

Recovery from crash failures requires some sort of stable storage at all parties and specific resynchronization protocols. These fault tolerance issues are not discussed here, because most payment systems do not address them explicitly.

TECHNOLOGY OVERVIEW

Electronic payment systems must enable an honest payer to convince the payee to accept a legitimate payment and at the same time prevent a dishonest payer

from making unauthorized payments, all the while ensuring the privacy of honest participants. The sidebar “Information Sources for Representative Payment Systems” lists some examples of payment systems, categorized according to the technique used for authorizing a money transfer from the payer to the payee.

Online versus offline

Offline payments involve no contact with a third party during payment—the transaction involves only the payer and payee. The obvious problem with offline payments is that it is difficult to prevent payers from spending more money than they actually possess. In a purely digital world, a dishonest payer can easily reset the local state of his system to a prior state after each payment.

Online payments involve an authorization server (usually as part of the issuer or acquirer) in each payment. Online systems obviously require more communication. In general, they are considered more secure than offline systems. Most proposed Internet payment systems are online.

All proposed payment systems based on electronic hardware, including Mondex and CAFE (Conditional Access for Europe), are offline systems. Mondex is the only system that enables offline transferability: The payee can use the amount received to make a new payment himself, without having to go to the bank in between. However, this seems to be a politically unpopular feature. CAFE is the only system that provides strong payer anonymity and untraceability. Both systems offer payers an electronic wallet, preventing fake-terminal attacks on the payer’s PIN. CAFE also provides loss tolerance, which allows the payer to recover from coin losses (but at the expense of some anonymity in case of loss). Mondex and CAFE are multicurrency purses capable of handling different currencies simultaneously.

All these systems can be used for Internet payments, and there are several plans for so doing, but none is actually being used at the time of this writing. The main technical obstacle is that they require a smart card reader attached to the payer’s computer. Inexpensive PCMCIA smart card readers and standardized infrared interfaces on notebook computers will solve this connectivity problem. Another system being developed along these lines is the FSTC (Financial Services Technology Consortium) Electronic Check Project, which uses a tamper-resistant PCMCIA card and implements a check-like payment model.

Instead of tamper-resistant hardware, offline authorization could be given via preauthorization: The payee is known to the payer in advance, and the payment is already authorized during withdrawal, in a way similar to a certified bank check.

Trusted hardware

Offline payment systems that seek to prevent (not merely detect) double spending require tamper-resistant hardware at the payer end. The smart card is an example. Tamper-resistant hardware may also be used at the payee end. An example is the security modules of point-of-sale (POS) terminals. This is mandatory in the case of shared-key systems and in cases where the payee does not forward individual transactions but the total volume of transactions. In a certain sense, tamper-resistant hardware is a “pocket branch” of a bank and must be trusted by the issuer.

Independent of the issuer’s security considerations, it is in the payer’s interest to have a secure device that can be trusted to protect his secret keys and to perform the necessary operations. Initially, this could be simply a smart card. But in the long run, it should become a smart device of a different form factor with secure access to a minimal keyboard and display. This is often called an electronic wallet.

Without such a secure device, the payers’ secrets and hence their money are vulnerable to anybody who can access his computer. This is obviously a problem in multiuser environments. It is also a problem even on single-user computers that may be accessed directly or indirectly by others. A virus, for example, installed on a computer could steal PINs and passwords as they are entered. Even when a smart card is available to store keys, a virus program may directly ask the smart card to make a payment to an attacker’s account. Thus for true security, trusted input/output channels between the user and the smart card must exist.¹

Cryptography

A wide variety of cryptographic techniques have been developed for user authentication, secret communication, and nonrepudiation. They are essential tools in building secure payment systems over open networks that have little or no physical security. There are also excellent reference works on cryptography.²⁻³

“Cryptofree” systems. Using no cryptography at all means relying on out-band security: Goods ordered electronically are not delivered until a fax arrives from the payer confirming the order. First Virtual is a cryptofree system. A user has an account and receives a password in exchange for a credit card number, but the password is not protected as it traverses the Internet. Such a system is vulnerable to eavesdropping. First Virtual achieves some protection by asking the payer for an acknowledgment of each payment via e-mail, but the actual security of the system is based on the payer’s ability to revoke each payment within a certain period. In other words, there is no definite authorization during payment. Until the end of this period, the payee assumes the entire risk.

Generic payment switch. A payment switch is an

Cryptography is an essential tool in building secure payment systems over open networks that have little or no physical security.

Information Sources for Representative Payment Systems

Online Systems, Traceable

Credit-card payment system without cryptography

First Virtual
<http://www.fv.com>

Credit-card payment systems with cryptography

CyberCash
<http://www.cybercash.com>
iKP
<http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/iKP.html>

Proposed standard

SET
<http://www.mastercard.com/set/set.htm>

Micropayments

NetBill
B. Cox, J. D. Tygar, and M. Sirbu, "NetBill Security and Transaction Protocol," Proc. First Usenix Electronic Commerce Workshop, Usenix, Berkeley, Calif., July 1995, pp. 77-88.
Phone-Ticks (CAFE)
T. Pedersen, "Electronic Payments of Small Amounts," *Lecture Notes in Computer Science*, No. 1189, 1996, pp. 59-68.

Millicent
<http://www.millicent.digital.com/>
μ-iKP
<http://www.zurich.ibm.com/Technology/Security/publications/1996/HSW96.ps.gz>
MiniPay
http://www.ibm.net.il/ibm_il/int-lab/mpay/

Payment switches

OpenMarket
<http://www.openmarket.com/>

Offline, Traceable

Electronic purses that use smart cards with shared key

Danmønt/Visa
<http://www.visa.com/cgi-bin/vee/sf/cashmain.html?2+0>

Electronic purses that use smart cards with public key

CLIP
<http://www.europay.com/brand/clip.htm>

Electronic purses; encryption unknown

Mondex
<http://www.mondex.com/>

Standards

CEN Intersector Electronic Purse
CEN/TC224/WG10, Intersector Electronic Purse, draft European standard, Comite

European de Normalization, Brussels, 1992-1994

EMV Electronic Purse
<http://www.visa.com/cgi-bin/vee/sf/chip/circuit.html>

Electronic check

FSTC Electronic Check Project
<http://fstc.org/projects/echeck/echeck2.html>

Online Systems, Untraceable

Anonymous remailers for change

NetCash
<http://gost.isi.edu/info/netcash/>
Anonymous Credit Cards
S.H. Low, N.F. Maxemchuk, and S. Paul, "Anonymous Credit Cards," *Proc. 2nd ACM Conf. Computer and Communication Security*, ACM Press, New York, 1994, pp. 108-117.

Offline Systems, Untraceable

Anonymous ("blind") signatures

e-cash
<http://www.digicash.com>

Anonymous ("blind") signatures

CAFE

http://www.semper.org/sirene/publ/BBCM1_94CafeEsorics.ps.gz

online payment system that implements both the pre-paid and pay-later models, as exemplified by the OpenMarket payment switch. OpenMarket's architecture supports several authentication methods, depending on the payment method chosen. The methods range from simple, unprotected PIN-based authentication to challenge-response-based systems, in which the response is computed, typically by a smart card.

Actually, OpenMarket uses passwords and optionally two types of devices for response generation: Secure Net Key and SecureID. User authentication therefore is based on shared-key cryptography. However, authorization is based on public-key cryptography: the OpenMarket payment switch digitally signs an authorization message, which is forwarded to the payee. The payment switch is completely trusted by users who use shared-key cryptography.

Shared-key cryptography. Authentication based on shared-key cryptography requires that the prover (the payer) and a verifier (the issuer) both have a shared secret. A DES key is one example of a shared secret; a password and PIN are other examples.

Because both sides have exactly the same secret information, shared-key cryptography does not provide nonrepudiation. If payer and issuer disagree

about a payment, there is no way to decide if the payment was initiated by the payer or by an employee of the issuer. Authenticating a transfer order on the basis of shared keys is therefore not appropriate if the payer bears the risk of forged payments.⁴

If authentication is to be done offline, each payer-payee pair needs a shared secret. In practice this means that some sort of master key is present at each payee end, to enable the payee to derive the payer's key. Tamper-resistant security modules in point-of-sale terminals protect the master key. Most offline systems (Danmønt/Visa and the trial version of Mondex) and online systems (NetBill, and the 2KP variant of iKP) use a shared secret between payer and issuer for authentication.

Public-key digital signatures. Authentication based on public-key cryptography requires that the prover have a secret signing key and a certificate for its corresponding public signature verification key. The certificate is issued by a well-known authority. Most systems now use RSA encryption, but there are several alternatives.

Digital signatures can provide nonrepudiation—disputes between sender and receiver can be resolved. Digital signatures should be mandatory if the payer bears the risk of forged payments.

A rather general security scheme that uses public-key signatures is Secure Socket Layer. SSL is a socket-layer communication interface that allows two parties to communicate securely over the Internet. It is not a payment technology per se, but has been proposed as a means to secure payment messages. SSL does not support nonrepudiation.

Complete payment systems using public-key cryptography include e-cash, NetCash, CyberCash, the 3KP variant of iKP, and Secure Electronic Transactions (SET). The protocol ideas themselves are much older. The use of digital signatures for both online and offline payments, anonymous accounts with digitally signed transfer orders, and anonymous electronic cash were all introduced during the 1980s.⁵

Payer anonymity

Payers prefer to keep their everyday payment activities private. Certainly they do not want unrelated third parties to observe and track their payments. Often, they prefer the payees (shops, publishers, and the like) and in some cases even banks to be incapable of observing and tracking their payments. Some payment systems provide payer anonymity and untraceability. Both are considered useful for cash-like payments since cash is also anonymous and untraceable.

Whereas anonymity simply means that the payer's identity is not used in payments, untraceability means that, in addition, two different payments by the same payer cannot be linked. By encrypting all flows between payer and payee, all payment systems could be made untraceable by outsiders. Payer anonymity with respect to the payee can be achieved by using pseudonyms instead of real identities. Some electronic payment systems are designed to provide anonymity or even untraceability with respect to the payee (iKP, for example, offers this as an option).

Currently, the only payment systems mentioned here that provide anonymity and untraceability against payee and issuer are e-cash (online) and CAFE (offline). Both are based on public-key cryptography, a special form of signatures called *blind signatures*.⁶⁻⁷ A blind signature on some message is made in such a way that the signer does not know the exact content of the message. DigiCash's e-cash, which is also based on the concept of blind signatures, is a cash-like payment system providing high levels of anonymity and untraceability.

In an e-cash system, users can withdraw e-cash coins from a bank and use them to pay other users. Each e-cash coin has a serial number. To withdraw e-cash coins, a user prepares a "blank coin" that has a randomly generated serial number, blinds it, and sends it to the bank. If the user is authorized to withdraw the specified amount of e-cash, the bank signs the blind coin and returns it to the user. The user then unblinds it to extract the signed coin. The signed coin

can now be used to pay any other e-cash user. When a payee deposits an e-cash coin, the bank records its serial number to prevent double-spending. However, because the bank cannot see the serial number when it signs the coin, it cannot relate the deposited coin to the earlier withdrawal by the payer.

NetCash and anonymous credit cards also provide anonymity and untraceability. But they are based on the use of trusted "mixes" that change electronic money of one representation into another representation, without revealing the relation. Neither e-cash nor CAFE assume the existence of such trusted third parties.

MICROPAYMENTS

Micropayments are low-value payments (probably less than \$1) that are made very quickly, like paying for each tick of a phone call. Given these constraints, micropayment techniques must be both inexpensive and fast. Achieving both requires certain compromises.

A number of proposals assume repeated payments (such as pay-per-view), beginning with CAFE Phone Ticks and μ -iKP, the micropayment proposal for iKP. Both of these proposals use one-way hash functions to implement micropayments.

Content servers in the global information infrastructure will probably have to process such a large number of these low-value transactions that it will be impractical to use computationally complex and expensive cryptographic protocols to secure them. μ -iKP, designed with these goals in mind, is based on computationally secure one-way functions. Informally, a function $f()$ is one-way if it is difficult to find the value x given the value $y = f(x)$. The value x is the preimage of y . Given such a one-way function, the payer will randomly choose a seed value X and recursively compute:

$$\begin{aligned} A^0(X) &= X \\ A^{i+1}(X) &= f(A^i(X)) \end{aligned}$$

The values A^0, \dots, A^{n-1} —known as coupons—will enable the payer to make n micropayments of a fixed value v to one payee: First, the payer forwards A^n and v to the payee in an authenticated manner. Authentication can be achieved by sending these values to the payee as the payload of a normal iKP payment. The payee ensures, possibly via its bank, that A^n does in fact correspond to a good hash preimage chain that can be used for subsequent micropayments. The micropayments are then carried out by revealing components of the chain $A^{n-1}, A^{n-2}, \dots, A^0$ successively to the payee. To clear the payments, the payee presents the partial chain

$$A^i, \dots, A^j \quad (0 \leq i < j \leq n)$$

to its bank in return for a credit of value $v(j-i)$.

Payers prefer to keep their everyday payment activities private. Certainly they do not want unrelated third parties to observe and track their payments.

It is now possible to achieve security for all parties, including the perfect untraceability of the payer. No one system will prevail; several payment systems will coexist.

The overhead of the setup phase is justified only when it is followed by several repeated micropayments. However, nonrepeated (or rarely repeated) micropayments are also a likely scenario in the electronic marketplace: A user surfing the Web may chance upon a single page that costs \$0.01. Neither the micropayment setup overhead nor the cost of a normal payment is justified in this case.

μ -iKP solves this problem with a broker: An isolated micropayment from payer P to payee Q is carried out by P, which makes one or more micropayments to broker B. Broker B then makes an equivalent micropayment to Q. In other words, a nonrepeating financial relationship between P and Q is achieved by leveraging on existing relationships between B and P and between B and Q.

On the other hand, if the amount of the transaction is small, developers can assume a lower risk and so opt to reduce security (for example, by foregoing nonrepudiation). A notable example is NetBill, which is founded on the shared-key technology Kerberos. It implements a check-like debit-payment model. The use of shared-key technology is justified by the performance required to process many micropayments in a short time. NetBill developers of both technologies have announced that they will migrate to public-key technology. MiniPay, from IBM Haifa Laboratory, is an example of a micropayment system based on public-key technology.

STANDARDS

The European Standardisation Organisation (CEN), as well as Europay, MasterCard, and Visa (known collectively as EMV), are working on standards for smart-card-based electronic payment systems. A CEN standard for an Intersector Electronic Purse already exists. There are currently no efforts to standardize an untraceable, offline payment system.

Two proposals, Visa's Secure Transaction Technology (STT) and MasterCard's Secure Electronic Payment Protocol (SEPP), began as competing standards for credit-card-based online payment schemes. Recently SET, a proposal designed by MasterCard, Visa, GTE, IBM, Microsoft, Netscape, SAIC, Terisa, and Verisign, has replaced these competing standards. SET is likely to be widely adopted for credit card payments over the Internet. The first prototypes of SET toolkits have been built.

SET is a pragmatic approach that paves the way for easy, fast, secure transactions over the Internet. It seeks to preserve the existing relationships between merchants and acquirers as well as between payers and their bank. SET concentrates on securely communicating credit card numbers between a payer and an acquirer gateway interfacing to the existing financial infrastructure.

In our classification, SET falls under the check-like

model. The transaction is initiated with a handshake, with the merchant authenticating itself to the payer and fixing all payment data. The payer then uses a sophisticated encryption scheme to generate a payment slip. The goal of the encryption scheme is to protect sensitive payment information (such as the credit card number); limit encryption to selected fields (to ease export approval); cryptographically bind the order information to the payment message; and maximize user privacy. Next the payment slip is signed by the payer and is sent to the merchant. The merchant sends the slip to its acquirer gateway, to authorize and capture the payment. The acquirer checks all signatures and the slip, verifies the creditability of the payer, and sends either a positive or negative signed acknowledgment back to merchant and payer.

Currently, discussions on SET dominate the stage of Internet payment systems, but there is a parallel demand for international standards of electronic cash-like payment schemes and schemes for micropayments.

TODAY'S SYSTEMS

In principle, the technology exists to secure electronic payment over the Internet. It is now possible to achieve security for all parties, including the perfect untraceability of the payer. No one system will prevail; several payment systems will coexist.

Micropayments (say, less than \$1), low-value payments (say, \$1 to \$100), and high-value payments have significantly different security and cost requirements. High values will be transferred using nonanonymous, online payment systems based on public-key cryptography implementing a check-like payment model. Within the next few years, smart-card readers will become widely available on PCs and workstations. This will enable payments of small amounts using prepaid, offline payment systems that provide a certain degree of untraceability.

Payment systems with and without tamper-resistant hardware at the payer's end will coexist for some time. Ultimately, payment systems based on smart cards and electronic wallets (having secure access to some display and keyboard, and communicating with the buyer's terminal via an infrared interface) will become prevalent for two reasons: They enable mobility of users and they clearly provide better security, allowing the payer to use untrusted terminals without endangering security.

A few almost equivalent payment systems with the same scope (in terms of the payment model and maximum amounts) will possibly coexist. The reasons are various cultural differences in the business and payment processes, national security considerations that might disqualify some solutions in some countries, and competition between payment system providers.

No electronic payment system is currently deployed on a large scale. But within a few years most of us will carry smart cards that can be used to buy things offline and in shops, as well as over the Internet. Several countries, most of them in Europe, are introducing such smart cards, but most cannot yet be used for cross-border payments. There is little chance that the world will ever agree on a single scheme for electronic purses in the near future.

Within the next two to three years, SET will become the predominant method for credit card purchases on the Internet. It will be implemented initially in software only, but will later be supported by smart cards. For some time, the currently preferred method of using SSL to encrypt payment details on their way from payer to payee will coexist with SET.

Beyond this, the future is much less clear. While it is likely that FSTC checks will be deployed within the US, the prospects for success are not clear. It is also not clear if the FSTC design will ever be used, or indeed can be used, internationally. Prepaid, online payment systems are becoming more and more attractive, with e-cash being the best-known system and the only one that supports strong privacy for payers. It is difficult to predict the future of payment systems that protect payer privacy because there are so many legal requirements and legal restrictions involved. Several micropayment systems will be used with microservice providers, but it is not clear yet whether there will be a single winner in the end. ❖

N. Asokan is a member of the network security research group at the IBM Zurich Research Laboratory and a doctoral candidate in computer science at the University of Waterloo. His interests include network security, electronic commerce, and mobile computing. He received a BTech in computer science and engineering from the Indian Institute of Technology in Kharagpur and an MS in computer science from Syracuse University. He is a member of the ACM.

Philippe A. Janson is the manager of the IT Solutions Department, which conducts research in IT applications relevant to IBM's industrial customers, and a member of the staff at the Zurich Research Laboratory, where he has worked on high-speed packet switches, the IBM Token Ring, LAN servers, and gateways. His research interests include operating systems, distributed systems, computer communication, and security. He has written several papers and holds several patents in these fields and is the author of a textbook on operating systems. He received a BS in electrical engineering from the University of Brussels and an MS, an EE, and a PhD in computer science from the Massachusetts Institute of Technology. He is a member of the IEEE Computer Society, ACM, SIGOPS and SIGCOMM, and Sigma Xi.

Michael Steiner is a research staff member of the network security group at the IBM Zurich Research Laboratory, where he works on security in network management and electronic commerce. His interests include secure and reliable systems as well as cryptography. He received a Diplom in computer science from the Swiss Federal Institute of Technology (ETH). He is member of ACM.

Michael Waidner is the manager of the network security research group at the IBM Zurich Research Laboratory. His research interests include cryptography, security, and all aspects of dependability in distributed systems. He has coauthored numerous publications in these fields. He received his diploma and doctorate in computer science from the University of Karlsruhe, Germany. He is a member of ACM, the GI, the IACR, and SIAM.

Contact the authors at IBM Research Div., Zurich Research Laboratory, CH-8803 Rüschlikon, Switzerland; {aso,pj,sti,wmi}@zurich.ibm.com.

References

1. A. Pfitzmann et al., "Trusting Mobile User Devices and Security Modules," *Computer*, Feb. 1997, pp. 61-68.
2. B. Schneier, *Applied Cryptography*, John Wiley & Sons, New York, 1996.
3. A. Menezes et al., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Fla., 1997.
4. R. Anderson, "Why Cryptosystems Fail," *Comm. ACM*, Nov. 1994, pp. 32-41; <ftp://ftp.cl.cam.ac.uk/users/rja14/wcf.ps.gz>.
5. H. Bürk and A. Pfitzmann, "Digital Payment Systems Enabling Security and Unobservability," *Computers & Security*, Aug. 1989, pp. 399-416; http://www.semper.org/sirene/publ/BuePf_89.ps.gz.
6. D. Chaum, "Privacy Protected Payments Unconditional Payer and/or Payee Untraceability," in *Smart Card 2000*, North-Holland, Amsterdam, 1989, pp. 69-93.
7. S. Brands, "Untraceable Off-line Cash in Wallet with Observers," *Lecture Notes in Computer Science 773*, 1994, pp. 302-318.