CyberCash: Payments Systems for the Internet

Stephen Crocker <crocker@cybercash.com>
Brian Boesch <boesch@cybercash.com>
Brian Boesch <boesch@cybercash.com>
Alden Hart <ahart@cybercash.com>
James Lum <jimlum@cybercash.com>

(The full paper had not been received at the time of printing of the proceedings.)

Extended Abstract

This paper describes the CyberCash payment system which provides multiple means for users and merchants to move money on the Internet.

One of the critical technologies that must be in place to enable electronic commerce is the ability to move funds between parties. Until now, the only means that has been available have required separate arrangements for payments or very limited use of credit cards. Some have attempted to introduce an integrated eletronic mall with facilities for making credit payments within the context of the mall. Open Market, First Virtual and MCI are three examples. Others have attempted to define a more general scheme but have not yet been connected to the banking systems. The CyberCash system is a separate system which can be used by any user, any merchant, and any bank. Moreover, it is introducing a new form of payment, peer-to-peer, which permits individuals to pay each other without requiring the payee to be merchant authorized to accept credit cards.

Customer to Merchant Payments

CyberCash will provide two classes of payment services, customer to merchant and peer to peer. Customer to merchant payments include credit card and debit card. For customer to merchant payments, there are three parties connected to the Internet, the customer, the merchant and the CyberCash server. A customer will engage in a dialog with the merchant's web server, eventually arriving at a decision to buy some goods or services. All of the dialog related to the sale is under control of the merchant until it's time to make the payment. At that point, the merchant presents the user with the amount to be paid and a transaction identifier, and then turns control over to the CyberCash payment system.

The CyberCash payment system consists of "CC user software" on the user's machine, "CC merchant software" on the merchant's machine, and the CyberCash server (CC server). The user invokes the CC user software, provides his credit card information, and authorizes the sale for a specific amount. Using public key technology , the CC user software encrypts this information under the CC server's key and sends it to the merchant. The merchant thus has a message that it cannot read completely and cannot tamper with but which authorizes the purchase. The merchant adds his identification information and sends it to the CC server. The entire message is digitally signed by the merchant to prevent tampering in transit. The CC server unwraps the message and creates a standard credit card authorization request. The CC server then forwards the request to the appropriate bank or processing house for authorization and returns the result to the merchant.

This is the basic protocol, but there are a number of variations that can be accommodated. As noted, the credit card information is encrypted so the merchant cannot see it. This prevents handling errors such as unauthorized charges originating with the merchant, but some merchants may require the credit card information as part of their record keeping. If the merchant's bank authorizes the merchant to receive the credit card numbers, the CC server will forward the information back to the merchant with the authroization.

Not all transactions will take place via the web. Email and other forms of interaction are possible, and the same protocols are usable in those settings as well.

Peer to peer payments

CyberCash enables peer to peer payments between CyberCash account holders and from CyberCash account holders to others. CyberCash accounts are established by users on demand. A user who wishes to open a CyberCash account first obtains the CyberCash software for his machine and then contacts the CyberCash server. As part of this process, the user will generate a public/private key pair. The public key will be known to the CC server and will be identifier for

his account. The private key will be known only to the user and will permit the user to sign the instructions he gives to the SyberCash server.

Once the user has opened a CyberCash account, he can "load" his account by sending an instruction to move moeny out of his checking account. This instruction has to be digitally signed and accompanied by information which authenticates that the user legitimately has access to that checking account. The funds are then moved from the user's checking account to a CyberCash agency accunt in the same bank or another bank that is cooperating with the CyberCash service. At the same time, a notation is made on the CyberCash books that the user has those funds in his CyberCash account.

Whenever the user desires to make a payment to another CyberCash account, the user sends the CyberCash server an instruction to do so. The CyberCash server checks that the funds exist in the account and that the instruction is not a duplicate. It then updates both accounts and issues a signed receipt back to the user. The user may then present the receipt to payee to demonstrate that the payment has been made. The receipt is signed by the CC server and can be checked for validity without interacting with the CC server. The payee may also contact the CC server and check the status of his account.

Whenever the user desires to move the money out of his CyberCash account , he sends an instruction to the CC server and the funds are moved out of the yberCash account into the user's checking account. These funds are then available for any king transaction, including disbursement in cash.

Security

Security is obviously paramount in this operation. As noted above, public key technology is used, in combination with symmetric algorithms and hash algorithms, to protect the messages in transit and authenticate origins. The public key algoriithm is RSA, the symmetric algorithm is DES, and the hash is MD5.

Two other aspects of security are also important. The user must be certain he is using a true copy of the CyberCash code. To provide assurance to the user that he is not using modified code, a third party verification service will be available which provides certificates which convey the correct hash code for the software. Routines which check the hash code will be available from a variety of sources and will be well documented.

Protection of the user's private key is also paramount. User software will keep the user's private key encrypted and available only with a local password. Stron local protection of the password does not protect against loss of a private key, however., and a separate facility is needed in case the user loses access to his private key.

To solve this problem, users will be encouraged to make use of third party data recovery centers will can store encrypted information and make it available only upon successfully completing an interrogatory which had been provided by the user when the data was originally stored.