Requirements for Network Payment: The NetCheque™ Perspective

B. Clifford Neuman Gennady Medvinsky

Information Sciences Institute
University of Southern California

Abstract

Secure methods of payment are needed before we will see widespread commercial use of the Internet. Recently proposed and implemented payment methods follow one of three models: electronic currency, credit-debit, and secure credit card transactions. Such payment services have different strengths and weaknesses with respect to the requirements of of security, reliability, scalability, anonymity, acceptability, customer base, flexibility, convertibility, efficiency, ease of integration with applications, and ease of use. NetCheque is a payment system based on the credit-debit model. NetCheque is described and its strengths with respect to these requirements are discussed.

1 Introduction

In the past year, the number of users and organizations reachable through the Internet has increased dramatically. The Internet is now seen by many organizations as an efficient means to reach potential customers. To date, most commerce on the Internet consists of the interactive dissemination of "advertising material" through World Wide Web home pages and product databases. In most cases, the actual purchase of the product occurs outside the network. Nevertheless, we have started to see commercial transactions on the Internet. Several pilots, and even a few production systems, have appeared on the Internet to support electronic purchases. The absence of a secure payment service that can be used over an open network has limited such use of the network so far.

This paper discusses some of the requirements of payment mechanisms for open networks, and describes the NetCheque™ system under development at the Information Sciences Institute of the University of Southern California. The paper discusses the benefits and drawbacks of alternative approaches, and describes how the different methods can be used together to provide financial infrastructure for the Internet.

2 Requirements

Important characteristics for an Internet payment system include security, reliability, scalability, anonymity, acceptability, customer base, flexibility, convertibility, efficiency, ease of integration with applications, and ease of use. Some of these characteristics, like anonymity, are more important in some communities, or for certain kinds of transactions, than they are in other communities. These characteristics are presented for discussion and comparison. The NetCheque system meets many of these characteristics better than other systems.

Security - since payments involve actual money, payment systems will be a prime target for criminals. Since Internet services are provided today on networks that are relatively open, the infrastructure supporting electronic commerce must be usable and resistant to attack in an environment where eavesdropping and modification of messages is easy.

Reliability - as more commerce is conducted over the Internet, the smooth running of the economy will come to depend on the availability of the payment infrastructure, making it a target of attack for vandals. Whether the result of an attack by vandals, or simply poor design, an interruption in the availability of the infrastructure would be catastrophic. For this reason, the infrastructure must be highly available and should avoid presenting a single point of failure.

Scalability - as commercial use of the Internet grows, the demands placed on payment servers will grow too. The payment infrastructure as a whole must be able to handle the the addition of users and merchants without suffering a noticeable loss of performance. The existence of central servers through which all transactions must be processed will limit the scale of the system. The payment infrastructure must support multiple servers, distributed across the network.

Anonymity - for some transactions, the identity of the parties to the transaction should be protected; it should not be possible to monitor an individual's spending patterns, nor determine one's source of in-

come. An individual is traceable in traditional payment systems such as checks and credit cards. Where anonymity is important, the cost of tracking a transaction should outweigh the value of the information that can be obtained by doing so.

Acceptability - the usefulness of a payment mechanisms is dependent upon what one can buy with it. Thus, a payment instrument must be accepted widely. Where payment mechanisms are supported by multiple servers, users of one server must be able to transact business with users of other servers.

Customer base - the acceptability of a payment mechanism is affected by the size of the customer base, that is the number of users able to make payments using the mechanism. Merchants want to sell products, and without a large enough base of customers using a payment mechanism, it is often not worth the extra effort for a merchant to accept the mechanism.

Flexibility - alternative forms of payment are needed, depending on the guarantees needed by the parties to a transaction, the timing of the payment itself, requirements for auditability, performance requirements, and the amount of the payment. The payment infrastructure should support several payment methods including instruments analogous to credit cards, personal checks, cashier's checks, and even anonymous electronic cash. These instruments should be integrated into a common framework.

Convertibility - users of the Internet will select financial instruments that best suit their needs for a given transaction. It is likely that several forms of payment will emerge, providing different tradeoffs with respect to the characteristics just described. In such an environment it is important that funds represented by one mechanism be easily convertible into funds represented by others.

Efficiency - royalties for access to information may generate frequent payments for small amounts. Applications must be able to make these "micropayments" without noticeable performance degradation. The cost per transaction of using the infrastructure must be small enough that it is insignificant even for transaction amounts on the order of pennies.

Ease of integration - applications must be modified to use the payment infrastructure in order to make a payment service available to users. Ideally, a common API should be used so that the integration is not specific to one kind of payment instrument. Support for payment should be integrated into request-response protocols on which applications are built so that a basic level of service is available to higher level applications without significant modification.

Ease of use - users should not be constantly interrupted to provide payment information and most payments should occur automatically. However, users should be able to limit their losses. Payments beyond a certain threshold should require approval. Users should be able to monitor their spending without going out of their way to do so.

3 Payment models

Recently proposed, announced, and implemented Internet payment mechanisms can be grouped into three broad classes: electronic currency systems, credit-debit systems, and systems supporting secure presentation of credit card numbers.

3.1 Electronic currency

With electronic currency systems like Chaum's DigiCash system [1], currently being tested on the Internet, and USC-ISI's NetCash™ system [5], customers purchase electronic currency certificates from a currency server. They pay for the certificates through an account established with the currency server in advance, or by using credit cards, electronic checks, or paper currency accepted through a reverse automatic teller machine. Once issued, the electronic currency represents the value, and may be spent with merchants who deposit the certificates in their own accounts or spend the currency elsewhere.

The principal advantage of electronic currency is its potential for anonymity. In Chaum's approach, one can't identify the client to which a certificate was issued even if all parties collude. However, a client attempting to spend the same certificate twice gives up enough information to determine his identity.

ISI's NetCash provides a weaker form of anonymity. If all parties collude, including the currency servers involved in the transaction, it is possible to determine who spent a certificate. However, the client gets to choose the currency server it uses and can choose one it trusts not to keep information needed to track such transactions.

The principal disadvantage of electronic currency mechanisms is the need to maintain a large database of past transactions to prevent double spending. In Chaum's approach, it is necessary to track all certificates that have been deposited. With ISI's approach, it is necessary to keep track of all certificates that have been issued, but not yet deposited.

3.2 Credit-debit instruments

In payment mechanisms that use the credit-debit model, including CMU's NetBill [8], First Virtual's InfoCommerce system, and USC-ISI's NetCheque system, customers are registered with accounts on pay-

ment servers and authorize charges against those account. With the debit or check approach, the customer maintains a positive balance that is debited when a debit transaction or check is processed. With the credit approach, charges are posted to the customer's account and the customer is billed for or subsequently pays the balance of the account to the payment service. The implementation of the electronic payment instrument is the same for both approaches.

An important advantage of the credit-debit model is its auditability. Once a payment instrument has been deposited, the owner of the debited account can determine who authorized the payment, and that the instrument was endorsed by the payee and deposited. This is extremely important for payments by businesses and, we assert, desired by individuals for a significant percentage of their transactions. This model does not typically provide anonymity, though it may be extended to do so [4, 5].

For credit-debit or electronic currency systems to move beyond trials with play money, a separate tie to the existing banking system is needed to convert account balances and electronic currency to and from real money in a customer or merchant's bank account. Though funds can circulate electronically, such an outside connection is required to settle imbalances between the funds spent and received electronically by an individual. The form and timing of such transfers is a contractual issue between the payment service provider and the customer or merchant, and is beyond the scope of this paper. How these transfers are made is an important distinguishing characteristic between different payment services.

3.3 Secure credit card presentation

Secure credit card transactions constitute the third class of network payment services. Though the details remain proprietary for most of the recently announced network payment collaborations, we believe that many will initially follow this model. For secure network credit card transactions, a customer's credit card number is encrypted using public key cryptography so that it can only be read by the merchant, or in some approaches by a third party payment processing service.

The biggest advantage of this approach is that the customer does not need to be registered with a network payment service; all that is needed is a credit card number. This provides a much larger customer base for merchants accepting this method of payment. Encryption using this approach prevents an eavesdropper from intercepting the customers credit card number. In approaches where the credit card number and amount are encrypted using the public key of a third party payment processing service, the merchant doesn't see the card number either, providing some protection against fraud by the merchant.

It is important to note, however, that without registration of customers using this approach, the encrypted credit card transaction does not constitute a signature; anyone with knowledge of the customer's credit card number can create an order for payment, just as they can fraudulently place an order over the telephone. Also, because payments processed using this approach are processed as standard credit card charges, costs are high enough that this method is not suited for payments whose amounts are on the order of pennies.

4 The NetCheque system

NetCheque is a distributed accounting service supporting the credit-debit model of payment. Users of NetCheque maintain accounts on accounting servers of their choice. A NetCheque account works in much the same way as a conventional checking account: account holders write electronic documents that include the name of the payer, the name of the financial institution, the payer's account identifier, the name of the payee, and the amount of the check. Like a paper check, a NetCheque bears an electronic signature, and must be endorsed by the payee, using another electronic signature, before the cheque will be paid.

As a distributed accounting service, properly signed and endorsed cheques are exchanged between accounting servers to settle accounts through a hierarchy, as shown in Figure 1. In addition to improving scalability and acceptability, clearing between servers allows organizations to set up accounts in their own in-house accounting servers with accounts corresponding to budget lines. Authorized signers write cheques against these accounts, while the organization maintains a single account with an outside bank, integrating its own internal accounting system with the external financial system.

The NetCheque accounting system was designed originally [6] to maintain quotas for distributed system resources, resulting in frequent transactions for small amounts. Thus, itis well suited to support small payments needed for some kinds of electronic commerce. This requirement for handling micropayments requires high performance which is obtained through the use of conventional, instead of public-key, cryptography. This gives up some support for independent verification of payment documents at each stage in the payment pipeline.

Figure 1: An accounting hierarchy

4.1 Implementation overview

The system is based on the Kerberos system [7], and the electronic signature used when writing or endorsing a cheque is a special kind of Kerberos ticket called a proxy [6]. The cheque itself contains information about 1) the amount of the cheque, 2) the currency unit, 3) an expiration date, 4) the account against which the cheque was drawn, and 5) the payee or payees, all readable by the bearer of the cheque, together with 6) the signatures and endorsements accumulated during processing, verifiable by the accounting server against which the cheque was drawn. For performance, the Kerberos proxy used as a signature is based on conventional cryptography, but it may be replaced by a signature using public key cryptography with a corresponding loss of performance.

To write a cheque, the user calls the write_cheque function, specifying an account against which the cheque is to be drawn, the payee, the amount, and the currency unit. Defaults for the account and currency unit are read from the user's .chequebook file. The write_cheque function generates the cleartext portion of the cheque, obtains a Kerberos ticket that will be used to authenticate the user to the accounting server, generates an authenticator with an embedded checksum over the information from the cheque, and places the ticket and authenticator in the signature field of the cheque. The cheque is then base 64 encoded and may be sent to the payee through electronic mail, or transfered in real time as payment for services provided through an on-line service.

The deposit_cheque function reads the cleartext part of the cheque, obtains a Kerberos ticket to be used with the payer's accounting server, generates an authenticator endorsing the cheque in the name of the payee for deposit only into the payee's account, and appends the endorsement to the cheque. An encrypted connection is opened to the payee's accounting server and the endorsed cheque is deposited. If the payee and the payer both use the same accounting server, the response will indicate whether the cheque cleared.

If different accounting servers are used, the payee's accounting server places a hold on the funds in the payee's account and indicates to the payee that the cheque was accepted for collection. The payee has the option of requesting that the cheque be cleared in real time, though we expect there may be a charge for this service. If a cheque accepted for collection is rejected, the cheque is returned to the depositor, who can take action at that time. As a cheque is cleared through multiple accounting servers, each server attaches its own endorsement, similar to the endorsement attached by the payee.

In some cases the payee's and payer's accounting servers can settle the check directly, bypassing higher levels of the hierarchy. This is possible when the cheque is drawn on an accounting server that is trusted to properly settle accounts. Such trust might be based on certificates of insurance [3] representing endorsement of the accounting server in much the same way that the FDIC insures banks in the United States. In such cases, the hierarchy would still be used to settle any imbalance between credits and debits for each accounting server at the end of the day, but the cost of these transfers would be amortized over the days transactions.

To determine account balances and find out about cleared cheques, authorized users can call the statement function which opens an encrypted connection to the accounting server and retrieves the account balance for each currency unit, together with a list of cheques that have been recently deposited to, or drawn on and cleared through the account. The entire cheque is returned, allowing the user's application to extract whatever information is needed for display to the user, or for integration with other applications.

5 Status

As of December 1994, a binary release of NetCheque is available for Sun4 systems. Releases for other architectures and a source release will be available in early 1995. The release contains programs for writing, displaying, and depositing cheques, and for retrieving account statements. Though, presently, cheques can only be cleared through a single server, clearing across multiple servers will be working by publication time.

USC intends to make the NetCheque client and server software available free of charge for personal, non-commercial, and limited commercial use. For more extensive commercial use, and for integration with commercial products, USC is prepared to license the technology on a non-exclusive basis.

Further information about NetCheque is available by electronic mail from NETCHEQUE@ISI.EDU and may be read through the URL:

http://nii-server.isi.edu/info/NetCheque/

6 Summary and Discussion

The NetCheque system is a distributed payment system based on the credit-debit model. The strengths of the NetCheque system are its security, reliability, scalability, and efficiency. Signatures on cheques are authenticated using Kerberos. Reliability and scalability are provided by using multiple accounting servers. NetCheque is well suited for clearing micropayments; its use of conventional cryptography makes it more efficient than systems based on public key cryptography. Though NetCheque does not itself provide anonymity, it may be used to facilitate the flow of funds between other services that do provide anonymity.

The principal weakness of NetCheque at this time is its small initial customer base. Users of NetCheque must be registered as NetCheque users before they can make payments. However, once registered with one server, cheques written by the user may be cleared through any NetCheque server.

Ease of integration and ease of use should be addressed in a mechanism-independent manner, so that the effort spent integrating payments with an application and developing user interfaces isn't duplicated for each payment service. There is a need for a common API and user interface for all of the evolving payment services. There is also a need for conversion of payment instruments between payment services. The NetCheque system has been designed to clear payments between NetCheque accounting servers, and is well suited for clearing payments between servers of different types.

Acknowledgements

Celeste Anderson, Charlie Lai, Paul Mockapetris, Brenda Timmerman, and Brian Tung commented on drafts of this paper.

References

[1] David Chaum. Achieving electronic privacy. *Scientific American*, pages 96–101, August 1992.

[2] D. Gifford, A. Payne, L. Stewart, and W. Treese. Payment switches for open networks. In *Proceedings of IEEE Compcon '95*, March 1995.

[3] Charlie Lai, Gennady Medvinsky, and B. Clifford Neuman. Endorsements, licensing, and insurance for distributed system services. In *Proceedings of the Second ACM Conference on Computer and Communications Security*, November 1994.

[4] Steven H. Low, Nicholas F. Maxemchuk, and Sanjoy Paul. Anonymous credit cards. In *Proceedings of the Second ACM Conference on Computer and Communications Security*, pages 108–117, November 1994.

[5] Gennady Medvinsky and B. Clifford Neuman. NetCash: A design for practical electronic currency on the internet. In *Proceedings of the First ACM Conference on Computer and Communications Security*, November 1993.

[6] B. Clifford Neuman. Proxy-based authorization and accounting for distributed systems. In *Proceedings of the 13th International Conference on Distributed Computing Systems*, pages 283–291, May 1993.

[7] B. Clifford Neuman and Theodore Ts'o. Kerberos: An authentication service for computer networks. *IEEE Communications*, 32(9), September 1994.

[8] Marvin Sirbu and J. Douglas Tygar. Netbill: An electronic commerce system optimized for network delivered information and services. In *Proceedings of IEEE Compcon '95*, March 1995.

This research was supported in part by the Advanced Research Projects Agency under NASA Cooperative Agreement NCC-2-539 and through Ft. Huachuca under Contract No. DABT63-94-C-0034. The views and conclusions contained in this paper are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the funding agencies. NETCHEQUE and NETCASH are trademarks of the University of Southern California. Figures and descriptions in this paper were provided by the authors and are used with permission. The authors may be reached at USC-ISI, 4676 Admiralty Way, Marina del Rey, CA 90292-6695, USA. Telephone +1 (310) 822-1511, e-mail bcn@isi.edu, ari@isi.edu.