The following paper was originally published in the
Proceedings of the First USENIX Workshop on Electronic Commerce
New York, New York, July 1995.

Payment Switches for Open Networks

David K. Gifford, Lawrence C. Stewart
Andrew C. Payne, G. Winfield Treese
Open Market, Inc.

For more information about USENIX Association contact:

1. Phone: 510 528-8649
2. FAX: 510 548-5738
3. Email: office@usenix.org
4. WWW URL: http://www.usenix.org

Payment Switches for Open Networks

David K. Gifford*†
Lawrence C. Stewart
Andrew C. Payne
G. Winfield Treese
Open Market, Inc. ‡

Abstract

We describe the first operational Internet payment switch that provides real-time authorization suitable for direct use by merchant servers. A payment switch is a server that creates digital representations of conventional financial instruments, and forwards authentic payment orders on these instruments to their corresponding conventional financial networks and institutions. Our payment switch provides support for time-based and item-based pricing, implements switch based authorization and settlement aggregation for micro-payments, and includes an extensive customer support system in order to provide a high level of customer confidence in electronic commerce. Fraud control is based on a transaction-specific multi-level security model that accommodates existing Internet browsers. Multiple authentication technologies are applied to every transaction.

1 Introduction

The recent rapid growth of information applications on the Internet suggests that public computer networks have the potential to establish a new kind of open marketplace for goods and services. A central requirement for a marketplace is a payment mechanism. However there is no merchant independent payment mechanism available for computer networks, that permits users to utilize conventional financial instruments such as credit cards, debit cards, and demand deposit account balances for real-time purchases. We expect that both retail payment and wholesale payment mechanisms will be required for networks; consumers will use the retail mechanism for modest size purchases, and institutions will use the wholesale mechanism for performing settlement between trading partners. In order to achieve wide acceptance the retail mechanism will need to be a logical evolution of existing credit-card [10], debit card [9], and Automated Clearing House facilities. Similarly the wholesale mechanism will need to be an evolved version of corporate electronic funds transfer [4].

An unavoidable property of public computer networks is that they are comprised of switching, transmission, and host computer components controlled by many individuals and organizations. Thus it is impossible for a network payment system to depend upon a specified minimum required degree of software, hardware, and physical security for all of the components in a public network. For example, secret keys stored in a given user's personal computer can be compromised, switches can be tampered with to redirect traffic, and transmission facilities can be intercepted and manipulated. We have developed threat models for open networks. These threat models have shown us that cryptographic protocols, while important, do not in and of themselves solve the security requirements of payment services. Our findings are consistent with Anderson's work on security failures in electronic banking systems [2].

The risk of performing retail payment in a public network is compounded by statutes that make a payment system operator in part liable for the security lapses of its users. Existing Federal statutes in the United States, including the Electronic Funds Transfer Act and the Consumer Credit Protection Act, re-

*Also with the Electrical Engineering and Computer Science Department, Massachusetts Institute of Technology, Cambridge, MA.

†The authors can be reached via electronic mail at {gifford,stewart,payne,treese}@openmarket.com.

‡© 1995 IEEE. Reprinted, with permission, from *Proceedings of Compcon '95*, March, 1995, San Francisco, CA, pp. 26–31. Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the IEEE copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Institute of Electrical and Electronics Engineers. To copy otherwise, or to republish, requires a fee and specific permission.

quire the operator of a payment mechanism to limit consumer liability in many cases. Payment system operators may have other fiduciary responsibilities for wholesale transactions. Similar responsibilities exist in other countries for retail and wholesale transactions [3].

Conventional commerce systems are designed to allow merchants to conduct business without exposing the merchants to undue risk. For example, in existing credit card payment systems, a credit card's issuing bank takes on the fraud risk associated with misuse of the card when a merchant follows established card acceptance protocols. Standard acceptance protocols can include verifying a cardholder's signature as like the one on the back of the card, and obtaining on-line authorization. However, in network based commerce a merchant cannot physically examine a purchaser's credit card, and thus the fraud risk may revert to the merchant in so called "card not present" transactions. Many merchants cannot take this risk because of their limited financial resources.

A fundamental goal of our work is to create a network payment service that will reduce the risk of network fraud, and thus permit more merchants to participate in network commerce. A payment switch is a network service that authorizes and executes digital payment orders which are backed by external accounts. A payment switch authenticates a payment order, checks for sufficient funds or credit, and then originates funds transfer transactions to carry out the payment order. A payment switch acknowledges acceptance or rejection of a payment order. More than one payment switch may exist on a given network, and a given payment switch may operate on more than one host to increase the payment switch's reliability, availability, and performance.

In the remainder of this paper we will discuss related work (Section 2), our payment switch technology (Section 3), and close with observations on our operational experience and plans (Section 4).

2 Related Work

Our work builds on related work in network based order entry, on-line payment servers, and off-line digital cash:

Network based order entry. Many Internet merchants allow buyers to complete network based order forms for hard goods. Network based order entry systems perform merchandise ship time authentication of the credit card account used for payment. In most cases, order form transactions are unencrypted and thus are vulnerable to eavesdropping. Certain merchants permit users to set up accounts with associated credit card numbers. In these systems merchandise is charged to a user's account. This eliminates the need for credit card information to pass in the clear over the network each time an order is placed. In the near future it is likely that cryptographic protocols will provide communication security for order entry. In most cases, even with cryptographic protocols, common network threats such as workstation compromise, Trojan horse client software, and the use of stolen credit card instruments are not addressed.

On-line payment servers. Recent work on payment servers is closely related to our work, but existing payment servers do not connect to the financial system for authorization or do not provide unforgeable real-time authorizations suitable for direct use by merchant servers. Existing network payment system proposals include the Simple Network Payment Protocol [7], CMU's Internet Billing Server [13], and ISI's NetCash [12]. Though these payment servers do not require trust between the parties in a transaction, the parties must trust the payment server, and the payment server must be on-line during the transaction. Kristol, Low, and Maxemchuk [11] propose a system for anonymous payment that protects all parties from being cheated. The key feature in their system is the careful separation of information, so that only "need to know" information is exposed to any participant in the transaction.

Another on-line payment server is the First Virtual system. The First Virtual [8] payment server provides each user with an account with a unique identifier backed by a credit card. A customer gives the identifier to a vendor when purchasing an item. The vendor reports the transaction to First Virtual, which sends electronic mail to the customer asking for confirmation of the transaction. The customer may approve the transaction, refuse payment, or claim that fraud has occurred. The vendor is at some risk because the customer may refuse to pay. Because the marginal cost of information products is low, vendors of such products may often find this risk acceptable.

Off-line digital cash. It is possible that network payment systems will include support for digital cash. Digital cash is a negotiable financial instrument that is an analog of conventional cash. An advantage of digital cash is that users can exchange value between themselves without using an on-line server. In order to permit off-line operation, digital cash systems require protected devices, such as smart cards, that are tamperproof [1]. If desired, digital cash transactions can be anonymous [6].

Our system has several benefits not found in many of these previous approaches. These include:

Digital analogs of conventional financial instruments. When an authentic payment order is presented to a payment switch, a corresponding conventional financial transaction is executed in real-time. Confirmation of the transaction is immediately available to relevant principals. Payment switch interfaces to external financial systems are implemented as modules that permit a payment switch to be easily expanded to handle new financial institutions or payment instruments.

The First Virtual payment system is the closest to our approach, but it does not provide real-time confirmation suitable for direct use by merchant servers because of the delay inherent in their electronic mail confirmation system. Thus, while the First Virtual system can be used for real-time vending of soft goods such as documents and software, the vendor takes on the risk of a valid account being unable to pay when the transaction is settled later.

Multiple authentication technologies. A payment switch applies more than one authentication technique to every request, and the techniques used depend upon the transaction type and value. Both system and user determined policies are applied in determining which authentication technologies are employed. This multi-level approach permits the balance between security and customer convenience to be adjusted depending on the risk profile of a transaction and a merchant. In addition, using multiple techniques guards against the complete failure of a single technique.

Extensive customer service support. A payment switch maintains an automated customer support system that provides information on committed payment transactions. A payment switch maintains complete logs of all transactions, and provides every buyer and merchant with Smart Statements[1] that describe their activity. Smart statements provide a fixed point of access for goods purchased, allowing a buyer to view transaction detail information and to fill out automated customer service forms on the products purchased. Smart statement entries that correspond to information products allow a buyer to view the product again directly from the smart statement. In the event of communication failure during the commit of a purchase transaction a buyer can refer to his or her smart statement to discover the transaction's disposition. The customer service support provided by a payment switch provides a high level of buyer comfort because buyers are assured of a complete accounting of their purchases as well as an effective means to resolve questions.

Compatibility with existing protocols. Our approach is based on existing network protocols, such as HTTP [5]. Thus existing browsers can be used without modification in many forms of electronic commerce using our payment switch and merchant server systems.

3 The Payment System

The overall architecture of our payment system is a distributed collection of clients, content servers, and payment switches that are not under common administrative control. Client capacity, performance, and availability can be increased by adding network capacity, content servers, and payment switches.

We will introduce our payment system by following a typical payment transaction, and then return to discuss how the payment switch functions as part of this transaction and elaborations of the basic protocol. In our discussion we will use the following terms:

Buyer The principal purchasing an item.

Merchant The principal selling an item.

Client The software being used by a buyer.

Content Server The software being used by a merchant.

Authenticated The payment switch has decided that a transaction was originated by the buyer specified by the transaction within a degree of certainty appropriate for the transaction, the buyer, and the merchant.

Authorized The payment switch has decided a buyer has sufficient funds or credit for a given transaction.

Committed The payment switch has decided to settle a transaction, and funds will flow from the buyer to the merchant.

The ten messages involved in a typical purchase transaction (Figure 1) are:

1. The client requests a product description page from the content server using HTTP using a GET request. The page includes one or more payment URLs that describe products.

   A payment URL (Uniform Resource Locator) is a string that includes:

[1] Smart Statement is a trademark of Open Market, Inc.

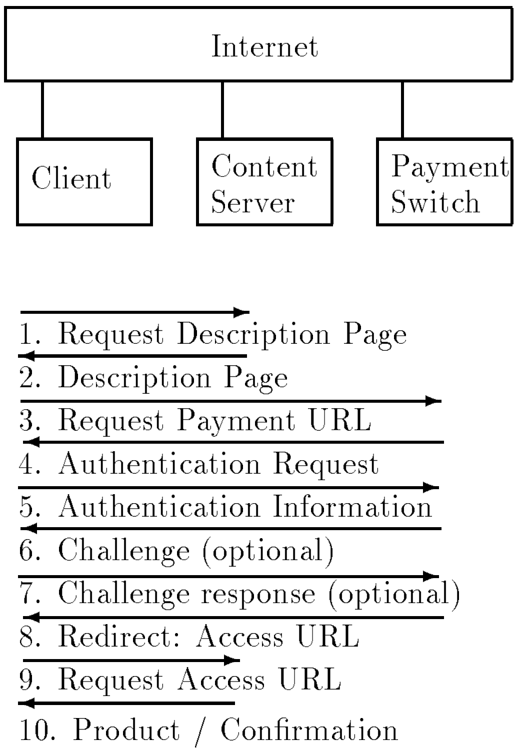

Figure 1: Purchase transaction steps

Payment switch host name The host the client will contact when this URL is activated.

Merchant identifier The principal identifier of the merchant selling the product. This is principal which will be paid when a sale is committed using the payment URL.

Product price The product price and currency. Multiple currencies are supported, including vendor currencies such as frequent flyer miles.

Target URL for product fulfillment This describes a URL that will provide product fulfillment. In the case of information products, this is a description of the information being sold. In the case of hard goods, this is a description of the product that will be fulfilled by the merchant server.

Expiration time of the payment URL A time and date at which the offer represented by the payment URL will expire.

Authenticator A digital signature of the payment URL using the private key of the merchant.

2. The product description page is returned to the client and displayed. The client then activates one of the payment URLs to purchase the product the URL describes.

3. The payment URL is forwarded to the payment switch by the client.

4. The payment switch requests the principal identifier of the buyer and the principal's password.

5. The principal identifier and password are sent to the payment switch. The payment switch now knows the sending principal (the buyer), the beneficiary principal (the merchant), the amount of the transaction, the product being purchased, and the URL to be used for product fulfillment. The payment switch also knows the sender's apparent IP address, the client type and its capabilities, and the type of channel (insecure, secure) that the client is using. Based on all of this information, the payment switch chooses a set of authentication techniques appropriate to the buyer, the merchant, and the transaction.

6. (Optional) If further authentication is required, a challenge is presented to the client. This challenge is based upon parameters previously set by the switch and the buying principal. Challenges can include client specific challenges, buyer specific challenges such as secondary passwords, and challenges to a buyer's smart card.

7. (Optional) The challenge response is returned to the payment switch. The payment switch can now authenticate the buyer based on the information the switch has received. If the payment switch decides that the request is not authentic, a rejection page is returned. If the payment switch decides the request is authentic, then the switch proceeds to authorization.

   Authorization is performed with respect to the financial instrument that backs a buying principal's account, and includes a switch specific component and an external financial system component. Switch based authorization includes negative and positive file checks, principal set spending limits and allowable product codes, address checks, velocity checks, and account type specific checks. Assuming that a transaction passes all switch based authorization checks, it is forwarded to the external financial institution that is responsible for the payment instrument connected with the buyer's account.

The payment switch is designed to handle "micropayments" even at the sub-cent level. Certain classes of authorizations for the same financial instrument are aggregated at the payment switch to reduce the load on external financial networks and to improve system performance. When authorizations are aggregated the payment switch may authorize a transaction without consulting an external financial system.

If a transaction is not authorized, a rejection page is returned to the buyer.

If a transaction is authorized, then it is recorded in a settlement log. Once a transaction has been stably recorded in the settlement log it is said to be committed, and settlement will occur.

8. Once a transaction is committed, an access URL is returned to the client as an HTTP redirect response. An access URL is a capability that permits a client to access the product which has just been purchased. An access URL includes:

   Content Server Name and Product Identifier The name of the server and product that were derived from the target URL in the payment URL.

   Buyer Authenticator A value that allows the content server to authenticate the buyer. At present, the buyer's IP address is included to restrict the access URL to delivering information only to the specified IP address. Other possibilities for buyer authenticators include the public key of the buyer, and legal ship to addresses.

   Expiration A time and date at which the access URL will expire. Fixed time access URLs are used to implement subscriptions.

   Access URL Authenticator A digital signature of the entire access URL that allows a content server to verify that the access URL was created by a payment switch.

9. The client forwards the access URL to the content server it describes. The content server validates the access URL, and either returns the product (soft goods), or queues a fulfillment order (hard goods).

10. Either the product or a description of the delivery instructions are delivered back to the client.

This basic processing flow is extended in our payment switch by other features designed to provide additional customer convenience.

For example, a buyer might like to shop for items and simultaneously a running total without committing to a purchase. A payment switch supports this functionality by using payment URLs called shopping cart URLs which do not cause a purchase to happen immediately. Instead, a product represented by a shopping cart URL is added to a buyer specific "shopping cart" at the payment switch when the shopping cart URL is activated by a buyer. By using a distinguished URL at the payment switch, a buyer can view his or her shopping cart, modify the contents of the cart, and atomically purchase all of the items in the cart.

The payment switch also provides buyers and merchants with direct access to a list of their respective committed transactions. In the case of buyer "smart statements," the statements include access URLs that will return the buyer to the purchased product. In addition, smart statements include extensive customer feedback capabilities.

The payment switch also implements duplicate purchase detection and principal specific account control. For example, a principal can set additional authorization criteria that limit an account to certain transaction types or dollar volumes. In addition, facilities for subscription and discount purchasing are included.

A payment switch includes modular authentication and settlement components which allow the switch to be readily adapted to new authentication protocols and additional financial networks and institutions (Figure 2). The form of payment orders can also be easily extended to accommodate new applications. As shown in Figure 2, the stable state of a payment switch is stored in a relational database. Roll-forward recovery is used to ensure that all transactions are properly processed in the face of payment switch and external financial system failures. Multiple transactions are used to process one payment order with intermediate state kept in the relational database. We have created a modular library of authentication techniques, and have written settlement modules for multiple financial networks in response to merchant requirements.

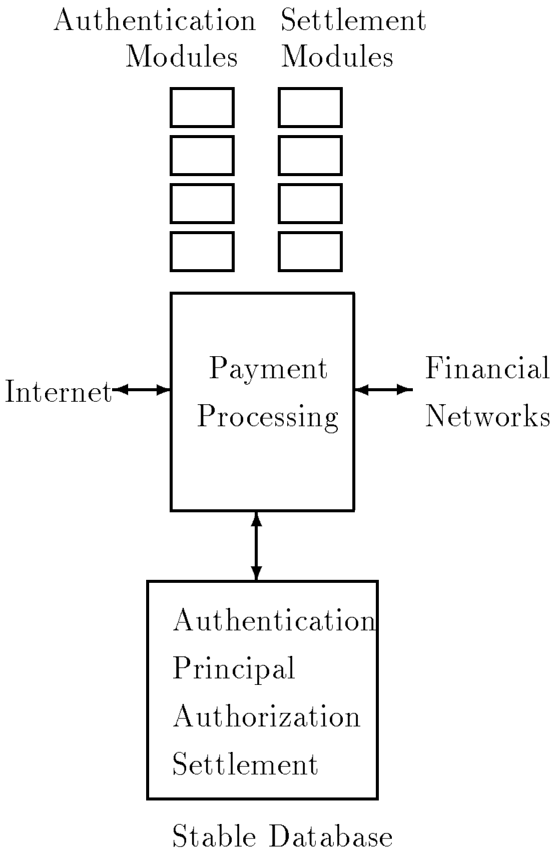

Figure 2: Payment switch internals

4 Conclusion

Payment switches that interconnect open networks with conventional financial instruments promise to permit new kinds of commerce. Our first payment switch went on-line in October 1994 and has been used continuously since then by Internet users. We have discovered that our provision for high quality automated customer service is an important component of our payment services. We are planning to make available new payment protocols in addition to our HTTP based payment service in the next year. We are also expanding our payment switch to run on multiple hosts to handle transaction volume growth and to permit merchants to operate their own payment switches.

It is our belief that electronic commerce offers a new frontier for both retail merchants and wholesale trading partners. The possibilities for doing business in an electronic medium seem limitless, and should allow new business models to flourish that will benefit the world.

References

[1] Anderson, R., UEPS–A Second Generation Electronic Wallet, Proc. of the Second European Symposium and Research in Computer Security (ESORICS), Touluse, France, November, 1992.

[2] Anderson, R., Why Cryptosystems Fail, Proc. 1st Conf. Computer and Comm. Security '93, November 1993, Virginia, Assoc. Computing Machinery, pp. 215-227.

[3] Bank Administration Institute, Payment Systems in Eleven Developed Countries, 1989.

[4] Bender, M., EFTS: Electronic Funds Transfer Systems, Kennikat Press, Port Washington, New York, 1975, pp. 43-46.

[5] Berners-Lee, T., Fielding R., Frystyk Neilsen, H., Hypertext Transfer Protocol–HTTP/1.0, IETF Internet Draft, December, 1994.

[6] Chaum, D., Achieving Electronic Privacy, Scientific American, August 1992, pp. 96-101.

[7] Dukach, S., SNPP: A Simple Network Payment Protocol, MIT Laboratory for Computer Science, Cambridge, MA, 1993.

[8] First Virtual, Inc., Introducing the First Virtual Internet Payment System for Information Commerce, 1994. Also see http://www.fv.com.

[9] Gifford, D., and Spector, S., Case Study: The CIRRUS Banking Network, Comm. ACM 8, 28 (August 1985), pp. 797-808.

[10] International Standards Orgnaization, ISO 8583: Bank card originated messages–interchange message specifications–content for financial transactions, August, 1987.

[11] Kristol, D., Low, S., and Maxemchuk, N., Anonymous Internet Mercantile Protocol, AT&T Bell Laboratories, March, 1994.

[12] Medvinsy, G., and Neuman, B. C., NetCash: A Design for Practical Electronic Currency on the Internet, Proc. 1st ACM Conf. on Comp. and Comm. Security, November, 1993.

[13] Sirbu, M. A., Internet Billing Service Design and Prototype Implementation, Information Networking Program, Carnegie Mellon University, 1993.