

Electronic commerce technology

Richard T. Watson (University of Georgia, USA)

Introduction

In the first chapter, we argued that organizations need to make a metamorphosis. They have to abandon existing business practices to create new ways of interacting with stakeholders. This chapter will provide you with the wherewithal to understand the technology that enables an organization to make this transformation.

Internet technology

Computers can communicate with each other when they speak a common language or use a common communication protocol. Transmission Control Protocol/Internet Protocol (TCP/IP) is the communication network protocol used on the Internet. TCP/IP has two parts. TCP handles the transport of data, and IP performs routing and addressing.

Data transport

The two main methods for transporting data across a network are circuit and packet switching. Circuit switching is commonly used for voice and package switching for data. Parts of the telephone system still operate as a circuit-switched network. Each link of a predetermined bandwidth is dedicated to a predetermined number of users for a period of time.

The Internet is a packet switching network. The TCP part of TCP/IP is responsible for splitting a message from the sending computer into packets, uniquely numbering each packet, transmitting the packets, and putting them together in the correct sequence at the receiving computer. The major advantage of packet switching is that it permits sharing of resources (e.g., a communication link) and makes better use of available bandwidth.

Routing

Routing is the process of determining the path a message will take from the sending to the receiving computer. It is the responsibility of the IP part of TCP/IP for dynamically determining the best route through the network. Because routing is dynamic, packets of the same message may take different paths and not necessarily arrive in the sequence in which they were sent.

Addressability

Messages can be sent from one computer to another only when every server on the Internet is uniquely addressable. The Internet Network Information Center (InterNIC) manages the assignment of unique IP addresses so that

TCP/IP networks anywhere in the world can communicate with each other. An IP address is a unique 32-bit number consisting of four groups of decimal numbers in the range 0 to 255 (e.g., 128.192.73.60). IP numbers are difficult to recall. Humans can more easily remember addresses like aussie.mgmt.uga.edu. A Domain Name Server (DNS) converts aussie.mgmt.uga.edu to the IP address 128.192.73.60. The exponential growth of the Internet will eventually result in a shortage of IP addresses, and the development of next-generation IP (IPng) is underway.

Infrastructure

Electronic commerce is built on top of a number of different technologies. These various technologies created a layered, integrated infrastructure that permits the development and deployment of electronic commerce applications (see Exhibit 9). Each layer is founded on the layer below it and cannot function without it.



Exhibit 5.: Electronic commerce infrastructure

National information infrastructure

This layer is the bedrock of electronic commerce because all traffic must be transmitted by one or more of the communication networks comprising the national information infrastructure (NII). The components of an NII include the TV and radio broadcast industries, cable TV, telephone networks, cellular communication systems, computer networks, and the Internet. The trend in many countries is to increase competition among the various elements of the NII to increase its overall efficiency because it is believed that an NII is critical to the creation of national wealth.

Message distribution infrastructure

This layer consists of software for sending and receiving messages. Its purpose is to deliver a message from a server to a client. For example, it could move an HTML file from a Web server to a client running Netscape. Messages can be unformatted (e.g., e-mail) or formatted (e.g., a purchase order). Electronic data interchange (EDI), e-mail, and hypertext text transfer protocol (HTTP) are examples of messaging software.

Electronic publishing infrastructure

Concerned with content, the Web is a very good example of this layer. It permits organizations to publish a full range of text and multimedia. There are three key elements of the Web:

- A uniform resource locator (URL), which is used to uniquely identify any server;
- A network protocol;
- A structured markup language, HTML.

Notice that the electronic publishing layer is still concerned with some of the issues solved by TCP/IP for the Internet part of the NII layer. There is still a need to consider addressability (i.e., a URL) and have a common language across the network (i.e., HTTP and HTML). However, these are built upon the previous layer, in the case of a URL, or at a higher level, in the case of HTML.

Business services infrastructure

The principal purpose of this layer is to support common business processes. Nearly every business is concerned with collecting payment for the goods and services it sells. Thus, the business services layer supports secure transmission of credit card numbers by providing encryption and electronic funds transfer. Furthermore, the business services layer should include facilities for encryption and authentication (see See Security).

Electronic commerce applications

Finally, on top of all the other layers sits an application. Consider the case of a book seller with an on-line catalog (see Exhibit 6). The application is a book catalog; encryption is used to protect a customer's credit card number; the application is written in HTML; HTTP is the messaging protocol; and the Internet physically transports messages between the book seller and customer.

Exhibit 6. An electronic commerce application

Electronic commerce applications	Book catalog
Business services infrastructure	Encryption
Electronic publishing infrastructure	HTML
Message distribution infrastructure	HTTP
National information infrastructure	Internet

Electronic publishing

Two common approaches to electronic publishing are Adobe's portable document format (PDF) and HTML. The differences between HTML and PDF are summarized in Exhibit 7.

Exhibit 7. HTML versus PDF

HTML	PDF
A markup language	A page description language
HTML files can be created by a wide variety of software. Most word processors can generate HTML	PDF files are created using special software sold by Adobe that is more expensive than many HTML creator alternatives
Browser is free	Viewer is free
Captures structure	Captures structure and layout
Can have links to PDF	Can have links to HTML
Reader can change presentation	Creator determines presentation

PDF

PDF is a page description language that captures electronically the layout of the original document. Adobe's Acrobat Exchange software permits any document created by a DOS, Macintosh, Windows, or Unix application to be converted to PDF. Producing a PDF document is very similar to printing, except the image is sent to a file instead

of a printer. The fidelity of the original document is maintained—text, graphics, and tables are faithfully reproduced when the PDF file is printed or viewed. PDF is an operating system independent and printer independent way of presenting the same text and images on many different systems.

PDF has been adopted by a number of organizations, including the Internal Revenue Service for tax forms. PDF documents can be sent as e-mail attachments or accessed from a Web application. To decipher a PDF file, the recipient must use a special reader, supplied at no cost by Adobe for all major operating systems. In the case of the Web, you have to configure your browser to invoke the Adobe Acrobat reader whenever a file with the extension pdf is retrieved.

HTML

HTML is a markup language, which means it marks a portion of text as referring to a particular type of information.⁶ HTML does not specify how this is to be interpreted; this is the function of the browser. Often the person using the browser can specify how the information will be presented. For instance, using the preference features of your browser, you can indicate the font and size for presenting information. As a result, you can significantly alter the look of the page, which could have been carefully crafted by a graphic artist to convey a particular look and feel. Thus, the you may see an image somewhat different from what the designer intended.

HTML or PDF?

The choice between HTML and PDF depends on the main purpose of the document. If the intention is to inform the reader, then there is generally less concern with how the information is rendered. As long as the information is readable and presented clearly, the reader can be given control of how it is presented. Alternatively, if the goal is to influence the reader (e.g., an advertisement) or maintain the original look of the source document (e.g., a taxation form or newspaper), then PDF is the better alternative. The two formats coexist. A PDF document can include links to a HTML document, and vice versa. Also, a number of leading software companies are working on extensions to HTML that will give the creator greater control of the rendering of HTML (e.g., specifying the font to be used).

Electronic commerce topologies

There are three types of communication networks used for electronic commerce (see Exhibit 8), depending on whether the intent is to support cooperation with a range of stakeholders, cooperation among employees, or cooperation with a business partner. Each of these topologies is briefly described, and we discuss how they can be used to support electronic commerce.

Exhibit 8. Electronic commerce topologies

Topology	Internet	Intranet	Extranet
Extent	Global	Organizational	Business partnership
Focus	Stakeholder relationships	Employee information and communication	Distribution channel communication

The Internet is a global network of networks. Any computer connected to the Internet can communicate with any server in the system (see Exhibit 5). Thus, the Internet is well-suited to communicating with a wide variety of stakeholders. Adobe, for example, uses its Web site to distribute software changes to customers and provide financial and other reports to investors.

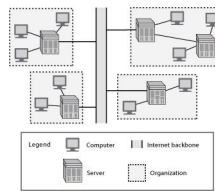


Exhibit 9.: The Internet

Many organizations have realized that Internet technology can also be used to establish an intra-organizational network that enables people within the organization to communicate and cooperate with each other. This so-called intranet (see Exhibit 10) is essentially a fenced-off mini-Internet within an organization. A firewall (see See Firewall) is used to restrict access so that people outside the organization cannot access the intranet. While an intranet may not directly facilitate cooperation with external stakeholders, its ultimate goal is to improve an organization's ability to serve these stakeholders.

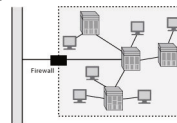


Exhibit 10.: An Intranet

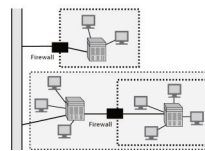


Exhibit 11.: An extranet

The Internet and intranet, as the names imply, are networks. That is, an array of computers can connect to each other. In some situations, however, an organization may want to restrict connection capabilities. An extranet (see Exhibit 7) is designed to link a buyer and supplier to facilitate greater coordination of common activities. The idea of an extranet derives from the notion that each business has a value chain and the end-point of one firm's chain links to the beginning of another's. Internet technology can be used to support communication and data transfer between two value chains. Communication is confined to the computers linking the two organizations. An organization can have multiple extranets to link it with many other organizations, but each extranet is specialized to support partnership coordination.

The economies gained from low-cost Internet software and infrastructure mean many more buyers and supplier pairs can now cooperate electronically. The cost of linking using Internet technology is an order of magnitude lower than using commercial communication networks for electronic data interchange (EDI), the traditional approach for electronic cooperation between business partners.

EDI

EDI, which has been used for some 20 years, describes the electronic exchange of standard business documents between firms. A structured, standardized data format is used to exchange common business documents (e.g., invoices and shipping orders) between trading partners. In contrast to the free form of e-mail messages, EDI supports the exchange of repetitive, routine business transactions. Standards mean that routine electronic transactions can be concise and precise. The main standard used in the U.S. and Canada is known as ANSI X.12,

and the major international standard is EDIFACT. Firms following the same standard can electronically share data. Before EDI, many standard messages between partners were generated by computer, printed, and mailed to the other party, that then manually entered the data into its computer. The main advantages of EDI are:

- paper handling is reduced, saving time and money;
- data are exchanged in real time;
- there are fewer errors since data are keyed only once;
- enhanced data sharing enables greater coordination of activities between business partners;
- money flows are accelerated and payments received sooner.

Despite these advantages, for most companies EDI is still the exception, not the rule. A recent survey in the United States showed that almost 80 percent of the information flow between firms is on paper. Paper should be the exception, not the rule. Most EDI traffic has been handled by value-added networks (VANs) or private networks. VANs add communication services to those provided by common carriers (e.g., AT&T in the U.S. and Telstra in Australia). However, these networks are too expensive for all but the largest 100,000 of the 6 million businesses in existence today in the United States. As a result, many businesses have not been able to participate in the benefits associated with EDI. However, the Internet will enable these smaller companies to take advantage of EDI.

Internet communication costs are typically less than with traditional EDI. In addition, the Internet is a global network potentially accessible by nearly every firm. Consequently, the Internet is displacing VANs as the electronic transport path between trading partners.

The simplest approach is to use the Internet as a means of replacing a VAN by using a commercially available Internet EDI package. EDI, with its roots in the 1960s, is a system for exchanging text, and the opportunity to use the multimedia capabilities of the Web is missed if a pure replacement strategy is applied. The multimedia capability of the Internet creates an opportunity for new applications that spawn a qualitatively different type of information exchange within a partnership. Once multimedia capability is added to the information exchange equation, then a new class of applications can be developed (e.g., educating the other partner about a firm's purchasing procedures).

Security

Security is an eternal concern for organizations as they face the dual problem of protecting stored data and transported messages. Organizations have always had sensitive data to which they want to limit access to a few authorized people. Historically, such data have been stored in restricted areas (e.g., a vault) or encoded. These methods of restricting access and encoding are still appropriate.

Electronic commerce poses additional security problems. First, the intent of the Internet is to give people remote access to information. The system is inherently open, and traditional approaches of restricting access by the use of physical barriers are less viable, though organizations still need to restrict physical access to their servers. Second, because electronic commerce is based on computers and networks, these same technologies can be used to attack security systems. Hackers can use computers to intercept network traffic and scan it for confidential information. They can use computers to run repeated attacks on a system to breach its security (e.g., trying all words in the dictionary for an account's password).

Access control

Data access control, the major method of controlling access to stored data, often begins with some form of visitor authentication, though this is not always the case with the Web because many organizations are more interested in attracting rather than restricting visitors to their Web site. A variety of authentication mechanisms may be used (see Exhibit 12). The common techniques for the Internet are account number, password, and IP address.

Exhibit 12. Authentication mechanisms

Class	Examples
Personal memory	Name, account number, password
Possessed object	Badge, plastic card, key, IP address
Personal characteristic	Fingerprint, voiceprint, signature, hand size

Firewall

A system may often use multiple authentication methods to control data access, particularly because hackers are often persistent and ingenious in their efforts to gain unauthorized access. A second layer of defense can be a firewall, a device (e.g., a computer) placed between an organization's network and the Internet. This barrier monitors and controls all traffic between the Internet and the intranet. Its purpose is to restrict the access of outsiders to the intranet. A firewall is usually located at the point where an intranet connects to the Internet, but it is also feasible to have firewalls within an intranet to further restrict the access of those within the barrier.

There are several approaches to operating a firewall. The simplest method is to restrict traffic to packets with designated IP addresses (e.g., only permit those messages that come from the University of Georgia—i.e., the address ends with uga.edu). Another screening rule is to restrict access to certain applications (e.g., Web pages). More elaborate screening rules can be implemented to decrease the ability of unauthorized people to access an intranet.

Implementing and managing a firewall involves a tradeoff between the cost of maintaining the firewall and the loss caused by unauthorized access. An organization that simply wants to publicize its products and services may operate a simple firewall with limited screening rules. Alternatively, a firm that wants to share sensitive data with selected customers may install a more complex firewall to offer a high degree of protection.

Coding

Coding or encryption techniques, as old as writing, have been used for thousands of years to maintain confidentiality. Although encryption is primarily used for protecting the integrity of messages, it can also be used to complement data access controls. There is always some chance that people will circumvent authentication controls and gain unauthorized access. To counteract this possibility, encryption can be used to obscure the meaning of data. The intruder cannot read the data without knowing the method of encryption and the key.

Societies have always needed secure methods of transmitting highly sensitive information and confirming the identity of the sender. In an earlier time, messages were sealed with the sender's personal signet ring—a simple, but easily forged, method of authentication. We still rely on personal signatures for checks and legal contracts, but how do you sign an e-mail message? In the information age, we need electronic encryption and signing for the orderly conduct of business, government, and personal correspondence.

Internet messages can pass through many computers on their way from sender to receiver, and there is always the danger that a sniffer program on an intermediate computer briefly intercepts and reads a message. In most cases, this will not cause you great concern, but what happens if your message contains your name, credit card number, and expiration date? The sniffer program, looking for a typical credit card number format of four blocks of four digits (e.g., 1234 5678 9012 3456), copies your message before letting it continue its normal progress. Now, the owner of the rogue program can use your credit card details to purchase products in your name and charge them to your account.

Without a secure means of transmitting payment information, customers and merchants will be very reluctant to place and receive orders, respectively. When the customer places an order, the Web browser should automatically encrypt the order prior to transmission—this is not the customer's task.

Credit card numbers are not the only sensitive information transmitted on the Internet. Because it is a general transport system for electronic information, the Internet can carry a wide range of confidential information (financial

reports, sales figures, marketing strategies, technology reports, and so on). If senders and receivers cannot be sure that their communication is strictly private, they will not use the Internet. Secure transmission of information is necessary for electronic commerce to thrive.

Encryption

Encryption is the process of transforming messages or data to protect their meaning. Encryption scrambles a message so that it is meaningful only to the person knowing the method of encryption and the key for deciphering it. To everybody else, it is gobbledygook. The reverse process, decryption, converts a seemingly senseless character string into the original message. A popular form of encryption, readily available to Internet users, goes by the name of Pretty Good Privacy (PGP) and is distributed on the Web. PGP is a public domain implementation of public-key encryption.

Traditional encryption, which uses the same key to encode and decode a message, has a very significant problem. How do you securely distribute the key? It can't be sent with the message because if the message is intercepted, the key can be used to decipher it. You must find another secure medium for transmitting the key. So, do you fax the key or phone it? Either method is not completely secure and is time-consuming whenever the key is changed. Also, how do you know that the key's receiver will protect its secrecy?

A public-key encryption system has two keys: one private and the other public. A public key can be freely distributed because it is quite separate from its corresponding private key. To send and receive messages, communicators first need to create separate pairs of private and public keys and then exchange their public keys. The sender encrypts a message with the intended receiver's public key, and upon receiving the message, the receiver applies her private key (see Exhibit 13). The receiver's private key, the only one that can decrypt the message, must be kept secret to permit secure message exchange.

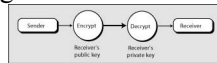


Exhibit 13.: Encryption with a public-key system

The elegance of the public-key system is that it totally avoids the problem of secure transmission of keys. Public keys can be freely exchanged. Indeed, there can be a public database containing each person's or organization's public key. For instance, if you want to e-mail a confidential message, you can simply obtain the sender's public key and encrypt your entire message prior to transmission.

Exhibit 14: Message before encryption

To: George Zinkhan <gzinkhan@cbacc.cba.uga.edu> From: Rick Watson <rwatson@uga.edu> Subject: Money
 G'day George I hope you are enjoying your stay in Switzerland. Could you do me a favor? I need USD 50,000 from my secret Swiss bank account. The name of the bank is Aussie-Suisse International in Geneva. The account code is 451-3329 and the password is 'meekatharra' I'll see you (and the money) at the airport this Friday. Cheers
 Rick

Consider the message shown in Exhibit 10; the sender would hardly want this message to fall into the wrong hands. After encryption, the message is totally secure (see Exhibit 15). Only the receiver, using his private key, can decode the message.

Exhibit 15: Message after encryption

To: George Zinkhan <gzinkhan@cbacc.cba.uga.edu> From: Rick Watson <rwatson@uga.edu> Subject: Money-----BEGIN PGP MESSAGE----- Version: 2.6.2
hEwDfOTG8eEvuiEBAf9rxBdHpgdq1g0gaIP7zm1OcHvWHtx 9 ip27q6vI
tjYbIUKDnGjV0sm2INWpcohrarI9S2xU6UcSPyFfumGs9pgAAAQ0euRGjZY RgIPE5DUHG
ultXYsnIq7zFHVevjO2dAEJ8ouaIX9YJD8kwp4T3suQnw7/d 1j4edl46qisrQHRRwqHXons7w4k04x8tH4JGfWEXc5LB
hcOSyPHEir4EP qDcEPibIM9bH6 w2ku2fUmdMaoptnVSinLMtzSqIKQIHMfaJ0HM9Df4kWh
ZbY0yFXxSuHKrgbaoDcu9wUze35dtwiCTdf1sf3ndQNaLOFiJh5pis bUg
9rOZjxpEFbdGgYpcfBB4rvRNwOwizvSodxJ9H VdtAL3DIIsSJdNSAEuxjQ0 hvOSA8oCBDJfHSUFqX3ROtB3 yuT1vf/
C8Vod4gW4tvqj8C1QNte ehxg== =fD44-----END PGP MESSAGE-----

Signing

In addition, a public-key encryption system can be used to authenticate messages. In cases where the content of the message is not confidential, the receiver may still wish to verify the sender's identity. For example, one of your friends may find it amusing to have some fun at your expense (see Exhibit 16).

Exhibit 16: Message before signing

To: Rick Watson <rwatson@uga.edu> From: President@whitehouse.gov Subject: Invitation to visit the White House-----Dear Dr. Watson It is my pleasure to invite you to a special meeting of Internet users at the White House on April 1st at 2pm. Please call 212-123-7890 and ask for Mr. A. Phool for complete details of your visit. The President

If the President indeed were in the habit of communicating electronically, it is likely that he would sign his messages so that the receiver could verify it. A sender's private key is used to create a signed message. The receiver then applies the sender's public key to verify the signature (see Exhibit 17).



Exhibit 17.: Signing with a public-key system

A signed message has additional encrypted text containing the sender's signature (see Exhibit 18). When the purported sender's public key is applied to this message, the identity of the sender can be verified (it was not the President).

Exhibit 18: Message after signing

To: Rick Watson <rwatson@uga.cc.uga.edu> From: President@whitehouse.gov Subject: Invitation to visit the White House-----Dear Dr. Watson It is my pleasure to invite you to a special meeting of Internet users at the White House on April 1st at 2pm. Please call 212-123-7890 and ask for Mr. A. Phool for complete details of your visit. The President-----BEGIN PGP SIGNATURE----- Version: 2.6.2
iQCVAwUBMeRVVUblZxMqZR69AQFJNQQAwHMSrZhWyiGTieGukbhPGUNF3aB
qm7E8g5ySsY6QqUcg2zwUr40w8Q0Lfcc4nmr0NUujiXkqzTNb 3RL41w5x
fTCfMp1Fi5Hawo829UQAImN8L5hzl7XfeON5WxfYcxLGXZcbUWkGio6/d4r 9Ez6s79DDf9EuDIZ4qfQcyl iA==G6jB
-----END PGP SIGNATURE-----

Imagine you pay USD 1,000 per year for an investment information service. The provider might want to verify that any e-mail requests it receives are from subscribers. Thus, as part of the subscription sign-up, subscribers have to supply their public key, and when using the service, sign all electronic messages with their private key. The provider

is then assured that it is servicing paying customers. Naturally, any messages between the service and the client should be encrypted to ensure that others do not gain from the information.

Electronic money

When commerce goes electronic, the means of paying for goods and services must also go electronic. Paper-based payment systems cannot support the speed, security, privacy, and internationalization necessary for electronic commerce. In this section, we discuss four methods of electronic payment:

- electronic funds transfer
- digital cash
- ecash
- credit card

There are four fundamental concerns regarding electronic money: security, authentication, anonymity, and divisibility. Consumers and organizations need to be assured that their on-line orders are protected, and organizations must be able to transfer securely many millions of dollars. Buyers and sellers must be able to verify that the electronic money they receive is real; consumers must have faith in electronic currency. Transactions, when required, should remain confidential. Electronic currency must be spendable in small amounts (e.g., less than one-tenth of a cent) so that high-volume, small-value Internet transactions are feasible (e.g., paying 0.1 cent to read an article in an encyclopedia). The various approaches to electronic money vary in their capability to solve these concerns (see Exhibit 19).

Exhibit 19. Characteristics of electronic money

	Security	Authentication	Anonymity	Divisibility
EFT	High	High	Low	Yes
Digital cash	Medium	High	High	Yes
Ecash	High	High	High	Yes
Credit card	High	High	Low	Yes

Any money system, real or electronic, must have a reasonable level of security and a high level of authentication, otherwise people will not use it. All electronic money systems are potentially divisible. There is a need, however, to adapt some systems so that transactions can be automated. For example, you do not want to have to type your full credit card details each time you spend one-tenth of a cent. A modified credit card system, which automatically sends previously stored details from your personal computer, could be used for small transactions.

The technical problems of electronic money have not been completely solved, but many people are working on their solution because electronic money promises efficiencies that will reduce the costs of transactions between buyers and sellers. It will also enable access to the global marketplace. In the next few years, electronic currency will displace notes and coins for many transactions.

Electronic funds transfer

Electronic funds transfer (EFT), introduced in the late 1960s, uses the existing banking structure to support a wide variety of payments. For example, consumers can establish monthly checking account deductions for utility bills, and banks can transfer millions of dollars. EFT is essentially electronic checking. Instead of writing a check

and mailing it, the buyer initiates an electronic checking transaction (e.g., using a debit card at a point-of-sale terminal). The transaction is then electronically transmitted to an intermediary (usually the banking system), which transfers the funds from the buyer's account to the seller's account. A banking system has one or more common clearinghouses that facilitate the flow of funds between accounts in different banks.

Electronic checking is fast; transactions are instantaneous. Paper handling costs are substantially reduced. Bad checks are no longer a problem because the seller's account balance is verified at the moment of the transaction. EFT is flexible; it can handle high volumes of consumer and commercial transactions, both locally and internationally. The international payment clearing system, consisting of more than 100 financial institutions, handles more than one trillion dollars per day.

The major shortfall of EFT is that all transactions must pass through the banking system, which is legally required to record every transaction. This lack of privacy can have serious consequences.⁷ Cash gives anonymity.

Digital cash

Digital cash is an electronic parallel of notes and coins. Two variants of digital cash are presently available: prepaid cards and smart cards. The phonecard, the most common form of prepaid card, was first issued in 1976 by the forerunner of Telecom Italia. The problem with special-purpose cards, such as phone and photocopy cards, is that people end up with a purse or wallet full of cards. A smart card combines many functions into one card. A smart card can serve as personal identification, credit card, ATM card, telephone credit card, critical medical information record and as cash for small transactions. A smart card, containing memory and a microprocessor, can store as much as 100 times more data than a magnetic-stripe card. The microprocessor can be programmed.

The stored-value card, the most common application of smart card technology, can be used to purchase a wide variety of items (e.g., fast food, parking, public transport tickets). Consumers buy cards of standard denominations (e.g., USD 50 or USD 100) from a card dispenser or bank. When the card is used to pay for an item, it must be inserted in a reader. Then, the amount of the transaction is transferred to the reader, and the value of the card is reduced by the transaction amount.

The problem with digital cash, like real cash, is that you can lose it or it can be stolen. It is not as secure as the other alternatives, but most people are likely to carry only small amounts of digital cash and thus security is not so critical. As smart cards are likely to have a unique serial number, consumers can limit their loss by reporting a stolen or misplaced smart card to invalidate its use. Adding a PIN number to a smart card can raise its security level.

Twenty million smart cards are already in use in France, where they were introduced a decade earlier. In Austria, 2.5 million consumers carry a card that has an ATM magnetic stripe as well as a smart card chip. Stored-value cards are likely to be in widespread use in the United States within five years. Their wide-scale adoption could provide substantial benefits. Counting, moving, storing and safeguarding cash is estimated to be 4 percent of the value of all transactions. There are also significant benefits to be gained because banks don't have to hold as much cash on hand, and thus have more money available for investment.

Ecash

Digicash of Amsterdam has developed an electronic payment system called ecash that can be used to withdraw and deposit electronic cash over the Internet. The system is designed to provide secure payment between computers using e-mail or the Internet. Ecash can be used for everyday Internet transactions, such as buying software, receiving money from parents, or paying for a pizza to be delivered. At the same time, ecash provides the privacy of cash because the payer can remain anonymous.

To use ecash, you need a digital bank account and ecash client software. The client is used to withdraw ecash from your bank account, and store it on your personal computer. You can then spend the money at any location accepting ecash or send money to someone who has an ecash account.

The security system is based on public-key cryptography and passwords. You need a password to access your account and electronic transactions are encrypted.

Credit card

Credit cards are a safe, secure, and widely used remote payment system. Millions of people use them every day for ordering goods by phone. Furthermore, people think nothing of handing over their card to a restaurant server, who could easily find time to write down the card's details. In the case of fraud in the U.S., banks already protect consumers, who are typically liable for only the first USD 50. So, why worry about sending your credit card number over the Internet? The development of secure servers and clients has made transmitting credit card numbers extremely safe. The major shortcoming of credit cards is that they do not support person-to-person transfers and do not have the privacy of cash.

Secure electronic transactions

Electronic commerce requires participants to have a secure means of transmitting the confidential data necessary to perform a transaction. For instance, banks (which bear the brunt of the cost of credit card fraud) prefer credit card numbers to be hidden from prying electronic eyes. In addition, consumers want assurance that the Web site with which they are dealing is not a bogus operation. Two forms of protecting electronic transactions are SSL and SET.

SSL

Secure Sockets Layer (SSL) was created by Netscape for managing the security of message transmissions in a network. SSL uses public-key encryption to encode the transmission of secure messages (e.g., those containing a credit card number) between a browser and a Web server.

The client part of SSL is part of Netscape's browser. If a Web site is using a Netscape server, SSL can be enabled and specific Web pages can be identified as requiring SSL access. Other servers can be enabled by using Netscape's SSLRef program library, which can be downloaded for noncommercial use or licensed for commercial use.

SET

Secure Electronic Transaction (SET) is a financial industry innovation designed to increase consumer and merchant confidence in electronic commerce. Backed by major credit card companies, MasterCard and Visa, SET is designed to offer a high level of security for Web-based financial transactions. SET should reduce consumers' fears of purchasing over the Web and increase use of credit cards for electronic shopping. A proposed revision, due in 1999, will extend SET to support business-to-business transactions, such as inventory payments.

Visa and MasterCard founded SET as a joint venture on February 1, 1996. They realized that in order to promote electronic commerce, consumers and merchants would need a secure, reliable payment system. In addition, credit card issuers sought the protection of more advanced anti-fraud measures. American Express has subsequently joined the venture.

SET is based on cryptography and digital certificates. Public-key cryptography ensures message confidentiality between parties in a financial transaction. Digital certificates uniquely identify the parties to a transaction. They are issued by banks or clearinghouses and kept in registries so that authenticated users can look up other users' public keys.

Think of a digital certificate as an electronic credit card. It contains a person's name, a serial number, expiration date, a copy of the certificate holder's public key (used for encrypting and decrypting messages and verifying

digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. A digital signature is used to guarantee a message sender's identity.

The SET components

Cardholder wallet

The application on the cardholder's side is also called the digital wallet . This software plug-in contains a consumer's digital certificate, shipping and other account information. This critical information is protected by a password, which the owner must supply to access the stored data. In effect, an electronic wallet stores a digital representation of a person's credit card and enables electronic transactions.

Merchant server

On the merchant side, a merchant server accepts electronic credit card payments.

Payment gateway

The payment gateway is the bridge between SET and the existing payment network. A payment gateway application translates SET messages for the existing payment system to complete the electronic transaction.

Certificate authority

The certificate authority issues and manages digital certificates, which are proofs of the identities for all parties involved in a SET transaction.

The process

The following set of steps illustrates SET in action.

- The customer opens a MasterCard or Visa account with a bank.
- The customer receives a digital certificate (an electronic file), which functions as a credit card for on-line transactions. The certificate includes a public key with an expiration date and has been digitally signed by the bank to ensure its validity.
- Third-party merchants also receive digital certificates from the bank. These certificates include the merchant's public key and the bank's public key.
- The customer places an electronic order from a merchant's Web page.
- The customer's browser receives and confirms that the merchant's digital certificate is valid.
- The browser sends the order information. This message is encrypted with the merchant's public key, the payment information, which is encrypted with the bank's public key (which can't be read by the merchant), and information that ensures the payment can be used only with the current order.
- The merchant verifies the customer by checking the digital signature on the customer's certificate. This may be done by referring the certificate to the bank or to a third-party verifier.
- The merchant sends the order message along to the bank. This includes the bank's public key, the customer's payment information (which the merchant can't decode), and the merchant's certificate.
- The bank verifies the merchant and the message. The bank uses the digital signature on the certificate with the message and verifies the payment part of the message.
- The bank digitally signs and sends authorization to the merchant, who can then fill the order.
- The customer receives the goods and a receipt.
- The merchant gets paid according to its contract with its bank.
- The customer gets a monthly bill from the bank issuing the credit card.

The advantage of SET is that a consumer's credit card number cannot be deciphered by the merchant. Only the bank and card issuer can decode this number. This facility provides an additional level of security for consumers, banks, and credit card issuers, because it significantly reduces the ability of unscrupulous merchants to establish a successful Web presence.

In order to succeed, SET must displace the current standard for electronic transactions, SSL, which is simpler than SET but less secure. Because of SSL's simplicity, it is expected to provide tough competition, and may remain the method of choice for the interface between the on-line buyer and the merchant. The combination of SSL and fraud-detection software has so far provided low-cost, adequate protection for electronic commerce.

Cookies

The creator of a Web site often wants to remember facts about you and your visit. A cookie is the mechanism for remembering details of a single visit or store facts between visits. A cookie is a small file (not more than 4k) stored on your hard disk by a Web application. Cookies have several uses.

- Visit tracking: A cookie might be used to determine which pages a person views on a particular Web site visit. The data collected could be used to improve site design.
- Storing information: Cookies are used to record personal details so that you don't have to supply your name and address details each time you visit a particular site. Most subscription services (e.g., The Wall Street Journal) and on-line stores (e.g., Amazon.com) use this approach.
- Customization: Some sites use cookies to customize their service. A cookie might be used by CNN to remember that you are mainly interested in news about ice skating and cooking.
- Marketing: A cookie can be used to remember what sites you have visited so that relevant advertisements can be supplied. For example, if you frequently visit travel sites, you might get a banner ad from Delta popping up next time you do a search.

Cookies are a useful way of collecting data to provide visitors with better service. Without accurate information about people's interest, it is very difficult to provide good service.

Both Internet Explorer and Netscape Navigator allow surfers to set options for various levels of warnings about the use of cookies. Visitors who are concerned about the misuse of cookies can reject them totally, with the consequent loss of service.

Conclusion

The rapid growth of electronic commerce is clear evidence of the reliability and robustness of the underlying technology. Many of the pieces necessary to facilitate electronic commerce are mature, well-tested technologies, such as public-key encryption. The future is likely to see advances that make electronic commerce faster, less expensive, more reliable, and more secure.

Cases

Austin, R. D., and M. Cotteleer. 1997. Ford Motor Company: maximizing the business value of Web technologies . Harvard Business School, 9-198-006.

Parent, M. 1997. Cisco Systems Inc.: managing corporate growth using an Intranet. London, Canada: University of Western Ontario. 997E018.

References

Applegate, L. M., C. W. Holsapple, R. Kalakota, F. J. Rademacher, and A. B. Whinston. 1996. Electronic commerce: building blocks for new business opportunity. *Journal of Organizational Computing and Electronic Commerce* 6 (1):1-10.

Kalakota, R., and A. B. Whinston. 1996. *Frontiers of electronic commerce* . Reading, MA: Addison-Wesley.

Watson, R. T., P. G. McKeown, and M. Garfield. 1997. Topologies for electronic cooperation. In *Telekooperation in Unternehmen* , edited by F. Lehner and S. Dustdar. Weisbaden, Germany: Deutscher Universitäts Verlag, 1-11.