INPUT

STRATEGIC MARKET PERSPECTIVE

Electronic Storefront Security

Electronic Commerce Program

APRIL 1997

Electronic Storefront Security

INPUT®

Frankfurt • London • New York • Paris • San Francisco • Tokyo • Washington D.C.

INPUT®

About INPUT

Clients make informed decisions more quickly and economically by using INPUT's services. Since 1974, information technology (IT) users and vendors throughout the world have relied on INPUT for data, research, objective analysis and insightful opinions to prepare their plans, market assessments and business directions, particularly in computer software and services.

Contact us today to learn how your company can use INPUT's knowledge and experience to grow and profit in the revolutionary IT world of the approaching millennium.

Subscription Services

- Information Services Markets
  - Worldwide and country data
  - Vertical industry analysis
- Systems Integration / Professional Services
- Client / Server Software
- Outsourcing
- Information Services Vendor Profiles and Analysis
- Internet Opportunities
- Electronic Commerce
- U.S. Federal Government IT Markets
- IT Customer Services Directions (Europe)
- Software Support (Europe)

Service Features

- Research-based reports on trends, etc. (More than 100 in-depth reports per year.)
- Frequent bulletins on events, issues, etc.
- 5-year market forecasts
- Competitive analysis
- Access to experienced consultants
- Immediate answers to questions
- On-site presentations
- Electronic report delivery

Databases

- Software and Services Market Forecasts
- Software and Services Vendors
- U.S. Federal Government
  - Procurement plans (PAR, APR)
  - Market Forecasts
  - Awards (FAIT)

Custom Projects

For Vendors—Analyze:

- Market strategies and tactics
- Product / service opportunities
- Customer satisfaction levels
- Competitive positioning
- Acquisition targets

For Buyers—Evaluate:

- Specific vendor capabilities
- Outsourcing options
- Systems plans
- Peer position

Other Services

- Acquisition / partnering searches

Contact INPUT at: info@input.com, or http://www.input.com

Frankfurt • Perchstatten 16, D-35428, Langgöns, Germany, Tel. +49 (0) 6403 911 420, Fax +49 (0) 6403 911 413

London • Cornwall House, 55-77 High Street, Slough, Berkshire, SL1 1DZ, England, Tel. +44 (0)1753 530444,
Fax +44 (0)1753 577311

New York • 400 Frank W. Burr Blvd., Teaneck, NJ 07666, USA, Tel. (201) 801-0050, Fax (201) 801-0441

Paris • 24, avenue du Recteur Poincaré, 75016, Paris, France, Tel. +33 (1) 46 47 65 65, Fax +33 (1) 46 47 69 50

San Francisco • 1881 Landings Drive, Mountain View, CA 94043, USA, Tel. (415) 961-3300, Fax (415) 961-3966

Tokyo • 6F#B, Mitoshiro Bldg., 1-12-12, Uchikanda Chiyoda-ku, Tokyo 101, Japan, Tel. +81 3 3219-5441,
Fax +81 3 3219-5443

Washington, D.C. • 1921 Gallows Road, Suite 250, Vienna, VA 22182, USA, Tel. (703) 847-6870, Fax (703) 847-6872

Abstract

Many Internet storefront operators currently have relatively little awareness of the security issues involved in conducting on-line commerce.

This report from INPUT's Electronic Commerce Program examines the security technology and services that are enabling commerce via Internet storefronts.

The primary source of information is from user interviews conducted within INPUT's research framework. In this context, a user of security technology is an Internet merchant—either a storefront merchant or an Internet mall operator.

Published by
INPUT
1881 Landings Drive
Mountain View, CA 94043-0848
United States of America

Electronic Commerce Program

Electronic Storefront Security

The information provided in this report shall be used only by the employees of and within the current corporate structure of INPUT's clients, and will not be disclosed to any other organization or person including parent, subsidiary, or affiliated organization without prior written consent of INPUT.

INPUT exercises its best efforts in preparation of the information provided in this report and believes the information contained herein to be accurate. However, INPUT shall have no liability for any loss or expense that may result from incompleteness or inaccuracy of the information provided.

EEB6 • 683 • 1997

Table of Contents

I Introduction 1

A. Objective 2
B. Scope 2
C. Research Methodology 2
D. Related INPUT Reports 3

II Executive Overview 5

A. Storefront Operators Accept Packaged Security 5
B. Security Is a Part-Time Function 6
C. Best Practices for Internet Commerce Security 6
1. Policy 6
2. Technology 6
3. Protect Internal Systems 7
D. Markets and Forecast 8
E. Recommendations 9
1. Current Storefront Operators 9
2. Future Storefront Operators 10
3. Security Technology Vendors 10

III Enabling Trends 13

A. Security Services 13
1. Encryption 14
a. DES and Symmetric Key Encryption 14
b. Public Key Cryptography 15
2. Encryption Software 15
3. Certificates 16
4. Secure Web Servers 16
5. JEPI 17

IV Internet Storefront Operator Profiles 19

A. Introduction 19
B. Internet Commerce Platforms 19

C. Support for Transaction Types 21
1. Purchase Orders 21
2. Credit Card Authorization 21
3. Digital Cash 24

V Internet Commerce Security—Importance and Satisfaction 27
A. E-mail Security 27
B. Web Security 29
C. Confidence in E-mail and Web Commerce Security 30

VI Policies and Practices for Secure Internet Commerce 33
A. Best Practices for Conducting Internet Commerce 33
1. Implementing Security Policy 33
2. Technology 35
3. Protecting Internal Systems 35
4. Encryption 36
B. Problems Faced in Conducting Internet Commerce 36
1. Hacking/Fraud 36
2. Public Perception 37
3. Technology 37
4. Encryption Export Restrictions 37
C. Improving Security 37

VII The Role of the Chief Security Officer 41
A. The Need for a CSO 41
B. Current Commerce-Related Security Responsibility 42
C. Future Commerce-Related Security Responsibility 44
1. Current Operators 44
2. Future Operators 45
D. Responsibilities of the Current Security Officer 45
1. Technology 45
2. Policy 46

VIII Market Forecasts 49
A. Value of Goods and Services Sales Enabled by Security 49
B. Secure Commerce-Enabling Web Server Software 50

A Security Technology, Vendors, and Consortia 51

A. The Major Elements of Security 51

1. Confidentiality 51
2. Integrity 51
3. Authentication 51
4. Nonrepudiation of Receipt 52
5. Nonrepudiation of Origin 52

B. Public Key and Private Key Encryption 52

1. Private Key (Symmetric) 52
2. Public Key (Asymmetric) 52
3. Mixed Public/Private Key Encryption 53

C. Transport and Data Security 54

1. Transport Security 54
2. Data Security 55

D. DES Encryption 56

E. RSA Data Security Encryption 57

F. PEM (Privacy Enhanced Mail) 57

G. MOSS (MIME Object Security Services) 58

H. S/MIME (Secure MIME) 58

I. Terisa Systems 58

J. VeriFone/EIT 59

K. VeriSign 59

L. Netscape 60

M. Microsoft 61

N. IBM 61

O. Nortel Entrust 62

P. SET 62

(Blank)

Exhibits

II

-1 Value of Goods and Services Sold Worldwide via Internet Enabled by Security, 1996-2001 (Non-EDI sales) 8

-2 Worldwide Expenditure on Web Software Server Products for Commerce, 1996-2001 9

IV

-1 Hardware Platform Deployment 20

-2 Operating System Deployment 20

-3 Web Server Deployoment 20

-4 Credit Card Transactions, 1995 23

-5 Anticipated Credit Card Transactions, 1996 24

V

-1 Importance and Satisfaction of Security to E-mail 28

-2 Importance and Satisfaction Ratings of Security for Web Commerce 29

-3 Confidence in E-mail and the Web for Internet Commerce 31

VI

-1 Best Practices for Operating a Commerce-Enabled Web Site 34

-2 Problems Faced in Conducting Internet Commerce 36

-3 Areas for Security Improvement 38

VII

-1 Job Title with Current Security Responsibility 43

-2 Full-time/Part-time Security Responsibility 44

VIII

-1 Value of Goods and Services Sold Worldwide via Internet Enabled by Security, 1996-2001 49

-2 Worldwide Expenditure on Web Server Software Products for Commerce, 1996-2001 50

A

-1 Advantages and Disadvantages of Public and Private Key Encryption 53

-2 Digital Envelopes—Mixed Private/Public Encryption 54

-3 Transport Security—Network to Network 55

-4 Data Security—Application to Application 56

I

Introduction

A Objective

Commerce over the Internet has the potential to change the ways organizations and individuals conduct business. The Internet can open up vast new markets to companies by removing geographical restrictions, increasing the number of potential customers, and drastically cutting distribution overheads.

But for all the benefits it could deliver, Internet commerce is still in its infancy. The most apparent reason is the current lack of industry-standard security technology on which commerce transaction applications can be built. This lack of technology serves to make users wary of using the technology that is available. A critical mass of people performing Internet transactions must be reached before Internet commerce achieves widespread acceptance.

This report examines the security technology and services that are enabling Internet commerce. The primary objectives are to:

- Identify the best products and practices for good security
- Define the emerging role of the Chief Security Officer in user organizations
- Size and forecast the markets related to Internet security

B
Scope

This study focuses on the security used by Internet storefront operators to enable Internet commerce. INPUT categorizes that security into:

- Confidentiality
- Integrity
- Authentication
- Nonrepudiation of receipt
- Nonrepudiation of origin

Public and private key cryptography, and data and transport security are discussed.

The primary source of information is from user interviews conducted within INPUT's research framework. In this context, a user of security technology is an Internet merchant—either a storefront merchant or an Internet mall operator.

The study excludes governmental issues such as the export restriction of cryptography technology and the Clipper chip.

C
Research Methodology

This study is based on interviews with 30 user organizations in the U.S. Companies were included in the survey if they currently support commerce transactions from their Web site (i.e., they have an Internet storefront) or if they plan to do so. It is also based on interviews with vendors of security products. All interviews were conducted during May, 1996.

The study also draws on secondary research including the Internet, on-line discussion groups and vendor-supplied literature.

The remaining chapters of this report are as follows:

- Chapter II is an executive overview that provides a summary of the major findings of the study.
- Chapter III discusses trends in security, messaging infrastructure, and Internet shopping.
- Chapter IV is an overview of storefront operators and their current use of security.
- Chapter V presents storefront operators' views of the importance of e-mail and Web security.
- Chapter VI is a look at users' perceptions of the best practices for Internet commerce.
- Chapter VII is a review of the role of the Chief Security Officer.
- Chapter VIII provides a forecast of the Internet commerce security-related market.

D

Related INPUT Reports

Other INPUT reports that address topics related to the subjects discussed here include the following:

- *Electronic Commerce Over the Internet, 1995*
- *Electronic Catalogs, Web Storefronts, and Internet Malls — 1996*
- *Electronic Payment Methodologies*
- *The Next Generation Travel Smart Card*
- *Electronic Commerce Markets and Forecast, 1995-2000*
- *Revolutionary Migration of Applications to the Internet*

(Blank)

II

Executive Overview

A

Storefront Operators Accept Packaged Security

Many Internet storefront operators currently have relatively little awareness of the security issues involved in conducting on-line commerce.

Currently, storefront operators are willing to accept and trust the security built in to commerce-enabled Web servers such as the Netscape Commerce Server. Beyond this, little or no security technology is applied for the purposes of performing Internet transactions.

Netscape Commerce Server is used by approximately three-quarters of Internet storefronts. Its users rate it highly on all aspects of security, giving it an overall security-related satisfaction rating of 4.4 out of 5.

While the availability of “out of the box” commerce-enabled Web servers undoubtedly assists smaller merchants in getting on line, they run the risk of making that process almost too easy.

It is now possible to set up an Internet storefront with adequate security for most circumstances without having to plan security rigorously. This could create a false sense of security, leading to less than thorough protection.

For example, while evaluating security requirements, a new storefront operator could possibly be satisfied that purchasing a Web server that supported transaction encryption was good enough. However, simply using encryption is not necessarily adequate security. Steps must be taken to ensure that the server is protected from outside connections by using a firewall, and, where appropriate, the machine itself should be physically protected from unauthorized internal access.

B
Security Is a Part-Time Function

Only about 10% of storefront operators see the need to allocate a full-time position for Internet security.

Three-quarters of storefronts currently assign security responsibility to the IS manager, in-house software developer, or Webmaster, and that is unlikely to change.

While security technology users (storefront operators) are clearly not enthusiastic to create full-time security positions, vendors take the opposite view. Vendors are more certain overall of the need for a CSO within an organization handling Internet transactions.

This is a predictable reaction. The vendors' view is that the widespread creation of a new CSO job title would simplify their relationships with customers and would extend the security market. INPUT recognizes that a significant underlying benefit to vendors of a widespread CSO role would be the increased ease with which they can target individuals with specific security-related purchasing power within organizations, and that account management from the vendor side would be simplified.

C
Best Practices for Internet Commerce Security

1. Policy

The best practice for conducting secure commerce is the definition, implementation, and enforcement of sound security policies and education. These include password management, managing access to systems, directories, and files, and sensitive traffic routing.

Staff education is critical in making any security policy work.

2. Technology

Some storefronts do not yet use a secure Web server; but as important as installing secure servers and gateways is using them effectively. Easy-to-use security management software is required to make the installation, configuration, and maintenance of security technology easy enough to be done properly. This technology is being developed by vendors of Web servers, and, in some cases (Netscape Commerce Platform, for example), security management technology is being developed and packaged specifically for storefront operators.

3. Protect Internal Systems

Isolating—or at least protecting—sensitive internal systems is an important factor in a storefront's security policy.

All operating systems have security loopholes. Where confidential customer information is concerned, it is not good enough to rely on an operating system alone to protect against unauthorized access. Passwords and domain authentication are relatively weak forms of security. Storefront operators recommended installing a firewall between internal systems and the Internet, and even physically removing sensitive systems from any internal network connected to the Internet.

Careful selection and thorough configuration of a suitable, secure Web server and firewall provide adequate security for conducting commerce over the Internet between locations where strong encryption is allowed (for example, the U.S.). Despite reports of security loopholes in early Internet technology, transaction fraud is considerably more likely to take place outside the Internet by traditional means—card theft, telephone fraud, etc.

D

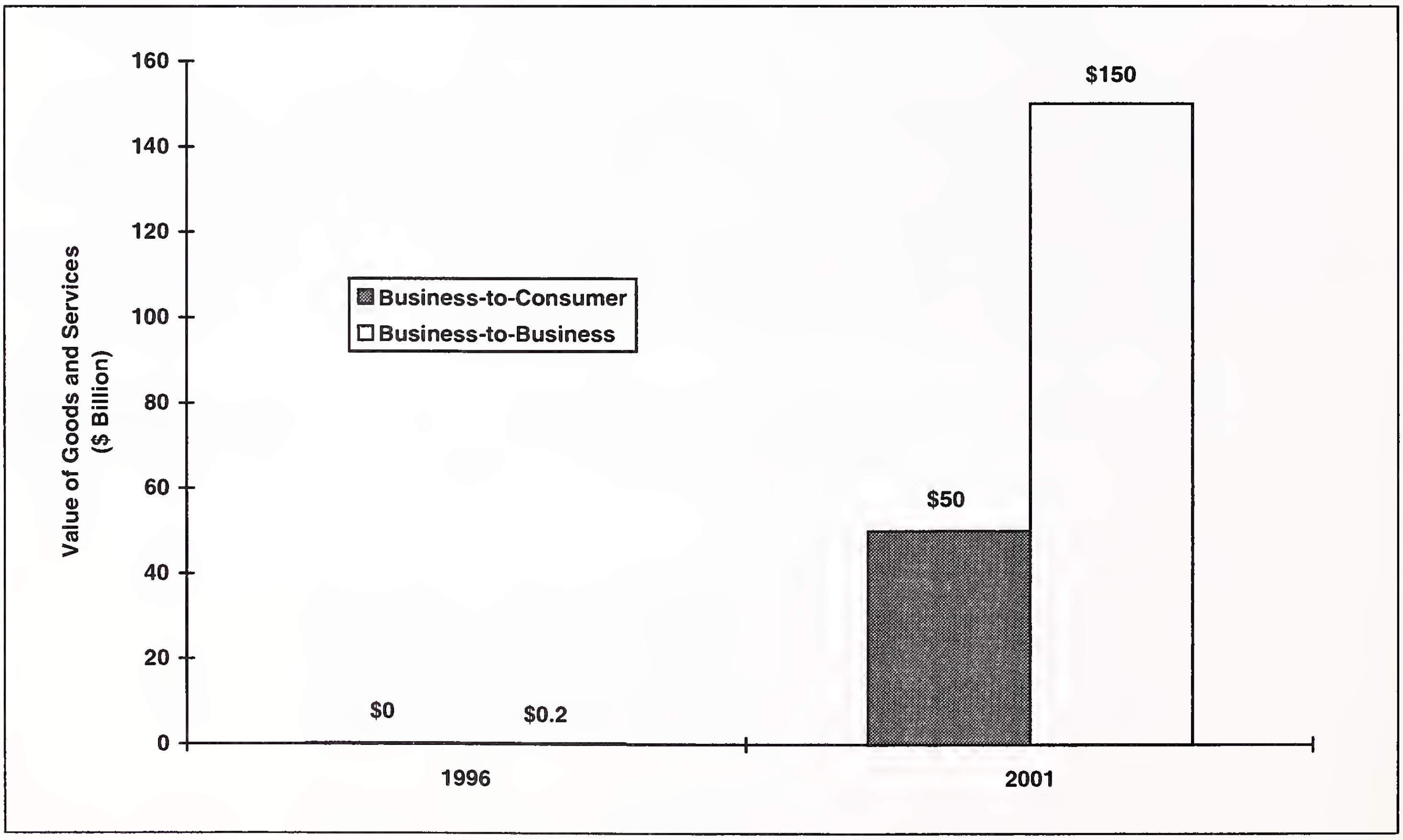
Markets and Forecast

The value of goods and services sold via the Internet will reach $370B by 2001. Of the this total, $140B is forecast to be spent on EDI-based sales.

A total of $220B is forecast to be spent on goods and services sold via the Internet without the use of EDI in 2001. Exhibit II-1 shows the value of these goods and services that will be purchased via software that is enabled for security.

Exhibit II-1

Value of Goods and Services Sold Worldwide via Internet Enabled by Security, 1996-2001 (Non-EDI sales)



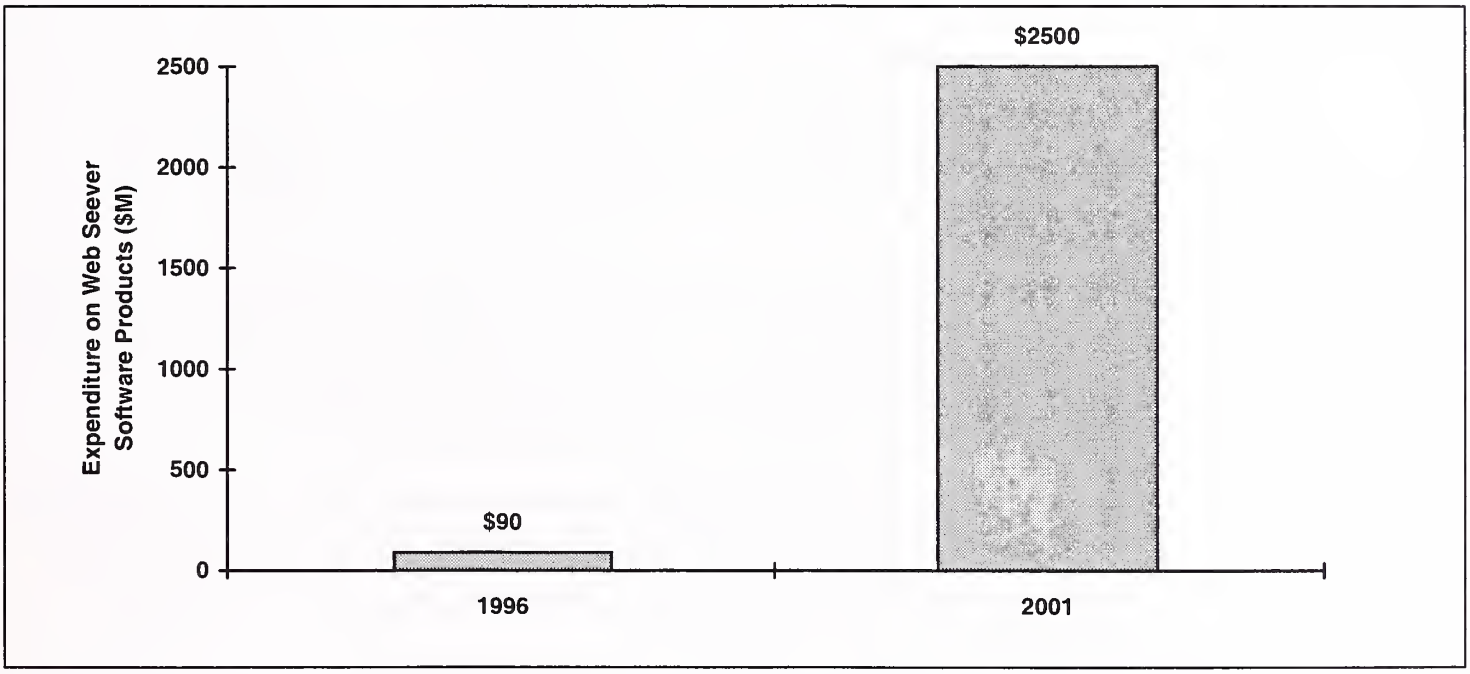
Source: INPUT

In some cases security functionality will be disabled and this will be the case in purchases valued at $20B in 2001. This underlines a major change in the use of security functionality — in 1996, the default is for security to be the exception but by 2001 the use of security will be the default.

The worldwide market for web-server software products designed to manage and facilitate Internet commerce will grow from an estimated $90 million in 1996 to approximately $2.5 billion in 2001. This equates to a compound annual growth rate (CAGR) of 94% over the 5 years. This high CAGR is due in some part to the rapid uptake of this type of software over the next 2-4 years. The growth between 2000 and 2001 will reduce to 25% but have an absolute value of nearly $500 million.

Exhibit II-2

Worldwide Expenditure on Web Software Server Products for Commerce, 1996-2001



Source: INPUT

E Recommendations

1. Current Storefront Operators

Current storefront operators need to appoint someone to oversee security related to the use of Internet technology within their organizations. Where warranted by size of company, complexity of operation, and/or turnover, they are encouraged to consider creating a Chief Security Officer (CSO) position.

The rapid pace of development in the Internet arena, in particular in the area of Internet commerce, means an Internet merchant runs the risk of losing customers through non-implementation of security technology, or worse, of security compromise through use of flawed security technology.

2. Future Storefront Operators

Organizations currently developing a storefront are encouraged not only to look at the technology, but to focus as much if not more attention on the planning and implementation of the policies behind the technology. In particular, companies must consider how security policy will be integrated into the business so that it does not become an isolated area seen only by IS staff.

3. Security Technology Vendors

Developers and suppliers of security technology related to Internet commerce should heed the messages contained in Chapter VI of this report (Policies and Practices for Secure Internet Commerce).

Current and prospective users of security technology make clear that the most important factors in creating and maintaining a secure environment for Internet commerce is the use of robust technology and the implementation of sound security policy and education.

Security is not a shrink-wrapped product, and security vendors should be looking toward providing extensive implementation, consultancy, and training services to support their products if these are not in place already.

The most important ways in which security might be improved, according to these users, were:

- Use “better technology”—by which stronger security and more robust technology is implied
- Implementation of automated security
- Integration of industry standards into security products

In 1996, security is a feature that, while often included within a product, must be “switched on” if its use is required—by 2001, security will be a default feature that must be turned off if it is not required.

Automation is the key to ubiquitous security (i.e., when all traffic, regardless of its nature, is encrypted). As this ubiquity will maximize the security vendors' market, it should be built into products at the earliest opportunity.

Likewise with industry standards, for example SET. The products that are first on the market with integrated support for these important standards will be the ones accepted by users.

(Blank)

III

Enabling Trends

This chapter discusses trends in security, messaging infrastructure, and Internet shopping.

A
Security Services

Any payment system is subject to fraud, theft, and corruption. Security is rapidly gaining prominence in electronic payment processes. It is a trade-off between risk and cost.

Banks are extremely risk averse and will pay highly for security. Tom Wills of CommerceNet emphasizes that security is an ongoing process "Fraud control (for credit cards and other means of payment) is a game where you build a wall high enough to stop hackers for a while, then they figure out a way in and you build a higher wall. ... It's an ongoing game."

Central to controlling fraud loss is:

- Encryption of sensitive data
- Keys to prevent unauthorized access
- Certificates to ensure authenticity

The basics of security are:

- Message or user authentication—to ensure that the source of a transaction is genuine
- Message integrity—to ensure that the message is not tampered with

- Message nonrepudiation—to ensure that the sender will not deny sending the message at a later date
- Message confidentiality—to ensure that only those for whom a message is intended are able to access it

1. Encryption

a. DES and Symmetric Key Encryption

The Data Encryption Standard (DES) was recommended by the National Bureau of Standards (NBS) in the 1960s as a way to encrypt government data. DES was adopted as a Federal Standard in 1977. It is widely used in the banking and financial industries, as well as for software products. Both sides must be equipped with the same key; this is a symmetric or secret key method. DES was expected to be phased out in 1977, as its original 56-bit key that encrypts data in 64-bit blocks can no longer be considered secure. However, the National Institute of Standards (NIST) reluctantly recertified it until 1997.

The Promotion of Commerce Online in the Digital Era Act of 1996 or "Pro-CODE" act is currently being heard and aims to enable DES encrypted code to be exported and to prevent third parties from holding keys that enable them to tap into secure communications.

Two issues—export controls and key escrow—are tied together politically. The thinking of U.S. government officials is that they will grant companies permission to export encrypted code with keys greater than 40 bits in return for companies enabling the government to "wiretap" supposedly secure communications.

Senators Burns, Leahy, and others side with the computer industry in the Pro-CODE act in trying to stop the government from regulating transactions with keys in escrow or "Clipper" chips that the FBI can use to unlock encrypted code.

Several other symmetric key encryption algorithms besides DES have appeared, including the International Data Encryption Algorithm (IDEA) that uses a 128-bit key. The PGP (Pretty Good Privacy) protocol for e-mail encryption uses this algorithm.

RSA Data Security's Ron Rivest invented the RC4 algorithm for secure key encryption. RSA widely licenses its code and international versions of Netscape Navigator, which incorporate the RC4 algorithm, limited to a 40-bit key as required by the U.S. government.

In July 1996, Netscape was the first company to get permission from the U.S. government to allow international customers to use code that had previously been declared illegal to export.

Users outside the U.S. can download Netscape Navigator and Netscape FastTrack (its low-end Web server) with 128-bit RC4 code, increasing its security. Permission was not granted to export higher quality security in Netscape's higher end servers.

Wells Fargo Bank checks that Netscape Navigator is used with 128-bit security and will not allow users with inferior 40-bit security to perform account management using the Web.

b. Public Key Cryptography

Public key algorithms are slower than secure key algorithms, so are used to encode short messages like keys and signatures.

To ensure that both sides of a transaction have the same key, it must first be sent from one side to the other using asymmetric public key cryptography at the start of a transaction. Well-known algorithms used in public key cryptography include MD4, MD5 and SHA (Secure Hashing Algorithm).

2. Encryption Software

RSA Data Security is the leader in providing general encryption algorithms that have been used by leading software, network equipment, and telecommunications providers. Its BSAFE software suite provides code for:

- RSA and Diffie-Hellman public key algorithms
- The DSA government signature algorithm
- DES, Triple-DES and DESX secret key ciphers
- Exportable RC2 and RC4 variable key size ciphers
- RC5 symmetric block cipher
- Bloom-Shamir secret sharing and key escrow
- The MD2, MD5 and SHA1 hashing algorithms and routines for pseudorandom number generation

3. Certificates

A hacker could intercept a message and invent a public/private key pair. If a user thought the message came from a merchant the user could be fooled into accepting the public key and sending the hacker private information. To avoid this situation, certificates are published rather than the public key itself.

A certificate is a message containing user identification, the user's public key and other information such as date of issue and date of validity of the certificate. The certificate is signed by a trusted third party.

The U.S. Post Office sees itself as a potential trusted third party. Banks, credit card companies, and governments are other potential Certificate Authorities.

VeriSign, founded in 1995 as a spin-off of RSA, with investors that include Ameritech, Security Dynamics (owner of RSA), and Visa, sells certificate software, tools for administering certificates, and Digital IDs. Its development partners include Netscape, Open Market, and IBM. It sees itself as becoming a leading certificate authority that can vouch for the authenticity of its certificates.

In nine European countries Compagnie Bancaire, an affiliate of the Paribas banking group, is the trusted third party of the Globe ID system. Globe ID is marketed by GC Tech (New York, NY and France) which develops certificate and Web security software.

Certification Authorities (CAs) will set up cross-certificates that enable them to trust each other's public keys and customer base.

Setting up the boundaries of trust is a major issue when integrating on-line services. If trust is extended too far, then the risk of fraud is increased. If it is not extended far enough, interoperability will be hindered.

Setting up networks of trusted domains means that a transaction may have three or four digital signatures attached to it, lengthening its processing time. Typically, a service provider will offload authentication and certificate validation onto separate processors.

4. Secure Web Servers

The basic interaction is between the client's wallet, the payment system, and the merchant's transaction server.

Wallets are for storing the value of money. They are just starting to appear. Merchant servers from Open Market, Microsoft, and Netscape are also emerging. In between, many options for securing the payment, as discussed later in this report, are possible.

It is because Web servers have been made secure that payment systems are possible.

5. JEPI

The Joint Electronic Payment Initiative (JEPI) is a standard proposed by the World Wide Web Consortium (W3C) and CommerceNet for Internet purchasing. It basically provides standard interfaces for the client wallet and merchant server to process credit cards and other payment instruments, such as digital cash.

Whereas SET is just for credit card payments, JEPI standardizes the entire credit card, digital cash, and E-Check payment transaction. It can handle multiple sites, not just client and server.

Participants include:

- CUC International
- CyberCash
- GC Tech
- IBM
- Microsoft
- Open Market
- VENDAMALL
- Xerox Corporation

Digital Equipment and VeriFone are supporting the design effort. A wider set of companies that includes NACHA, banks, leading Internet vendors, technology suppliers, and telecommunications companies is involved in the review process.

A specification with demonstrations in Europe and the U.S. is expected in early 1997.

(Blank)

IV

Internet Storefront Operator Profiles

A

Introduction

In order to put the use of Internet commerce security into context, this chapter presents the characteristics of the Internet storefronts whose operators INPUT interviewed for this study.

The data presented in this chapter is taken from these interviews. It is not representative of organizations overall, therefore.

Organizations were included in the survey if they either run or intend to run an Internet storefront or mall. Of the eight respondents who intend to operate a storefront or mall but do not do so now, seven stated that they would be in operation by the end of 1996. The eighth stated its intention to begin operating early in 1997.

B

Internet Commerce Platforms

Different Web server, hardware, and operating system platforms support different levels of security technology, and so INPUT believes it is necessary to identify which platforms are currently in use for Internet commerce.

The deployment of hardware, operating system, and Web server platforms among the survey sample echoes overall commercial Internet platform deployment.

Exhibit IV-1

Hardware Platform Deployment

Platform	Percent of Sample
PC	42%
Sun	33%
IBM	17%
Silicon Graphics	8%

Source: INPUT

Exhibit IV-2

Operating System Deployment

Operating System	Percent of Sample
UNIX	70%
Windows NT	30%

Source: INPUT

Exhibit IV-3

Web Server Deployment

Web Server	Percent of Sample
Netscape	71%
Microsoft IIS	14%
NCSA	7%
Netsite	7%

Source: INPUT

The most striking difference between commercial Internet platforms and Internet server platforms overall is in Web server usage.

For all classes of application (commercial, nonprofit, academic, scientific, etc.), the most common server platforms are those from NCSA (including the NCSA variant, Apache) and CERN, according to the many Web server surveys published on the Internet. These freely available servers account for over half of all Web servers. Within the commercial sector, however, Netscape is dominant (the company currently using the NCSA Web server indicated it is considering moving to Netscape).

Businesses are prepared to pay the up-front cost of a commercial Web server so as to receive the support that goes with it, and to invest in a brand that is established among commercial organizations.

Web server prices are falling—just as Internet vendors seek to capture the Web browser market by "low or no" pricing, so they have recognized that the server market is an extremely lucrative one.

INPUT forecasts the worldwide Web server market to reach $3.6 billion by 2001 and expects Web server vendors to compete on price to capture a share of this market.

For commerce, Wintel platforms are also more common than they are within the Internet as a whole—for example, 30% of respondents are running their storefronts on Windows NT.

In the noncommercial sector—educational, research, and scientific organizations—UNIX is the dominant operating system.

Within the commercial sector, UNIX is still very popular, but Windows NT is catching up.

INPUT forecasts that by 2001, the worldwide UNIX Web server market will be worth $1 billion and the NT Web server market will be worth $1.6 billion. As commercial organizations will lead the way in adopting NT, the current 30% market share of commercial Web servers held by NT is not surprising.

C
Support for Transaction Types

1. Purchase Orders

A third of companies interviewed that have an active storefront or mall currently support purchase orders—prearranged accounts between businesses that are credited and debited as orders are received and authenticated. But within the survey, no current storefront or mall operator will provide support in the future for purchase orders who does not already provide such support, and only one of the future storefront operators said it would support them. The number of companies that said they would never support purchase orders was the same as the number that currently support purchase orders.

This indicates that these storefront operators believe that purchase orders have reached their peak for Internet commerce. The ease with which credit card and digital cash transactions will be made in the future, as relevant standards and technology are defined and adopted, leaves little to recommend purchase orders. While credit card transactions will still be largely confined to consumers and small-scale business expenditure, digital cash will provide an extremely low-cost method of conducting both consumer-to-business and business-to-business commerce.

2. Credit Card Authorization

Of the current storefront and mall operators interviewed, nearly three-quarters currently support credit card transactions. The remainder will provide support in the near future.

Of the companies planning to open a storefront in the future, all intend to support credit card transactions from the outset.

Credit card authorization is the current standard for Internet storefront commerce, and will achieve near-ubiquity among Internet merchants by early in 1997. Most credit card business is accounted for by consumers, with digital cash expected to be adopted for business-to-business commerce. The increase in support for credit card authorization to this level will be driven by several interdependent factors, including:

- Maturing of supporting technology—Secure Web servers are no longer first-generation products, and have increased in stability, security, and performance through extensive development and use in the field

- Consolidation of standards—Where there were several competing standards for credit card authorization, now there is effectively one, SET, which is being developed by all of the previously competing players

- Increased user confidence—Internet credit card commerce is still in the early adopter stage, but will attain early majority status during 1997

Exhibits IV-4 and IV-5 show the number of credit card transactions conducted by individual organizations and the average value of those transactions. The two charts show the changing picture between 1995 and 1996.

Although the sample is small, it is apparent that the average transaction value and the number of transactions per organization will increase.

Most credit card transactions will remain consumer-to-business, regardless of their move onto the Internet. For business-to-business commerce, digital cash is more likely to be adopted.

Exhibit IV-4

Credit Card Transactions, 1995

	Average Transaction Value ($)					
Number of Transactions	$6-10	$11-20	$21-50	$51-100	$101-250	$251-500
1-50						✖
51-100					✖	
101-250						
251-500						
501-1,000					✖	
1,001-2,000						
2,001-5,000				✖		✖
5,001-10,000			✖✖			
10,001-50,000	✖		✖			
50,001+			✖		✖	

Source: INPUT

Exhibit IV-5

Anticipated Credit Card Transactions, 1996

	Average Transaction Value ($)					
Number of Transactions	**$6-10**	**$11-20**	**$21-50**	**$51-100**	**$101-250**	**$251-500**
1-50						
51-100						
101-250				✖	✖	
251-500			✖			✖
501-1,000						
1,001-2,000						
2,001-5,000						
5,001-10,000					✖✖	✖
10,001-50,000	✖		✖			
50,001+		✖	✖✖		✖	✖

Source: INPUT

3. Digital Cash

Considering the immaturity of digital cash, it is understandable that Internet storefront operators were less sure of their plans in this area than for credit card authorization.

No Internet storefront supported digital cash at the time this survey was conducted. Two-thirds of companies interviewed indicated a timeframe for introducing a digital cash facility (most by the end of 1996), and the remainder were adopting a "wait-and-see" approach.

Of the organizations planning to open a storefront in the future, around half intend to support digital cash.

A surprising reaction came from two respondents, a current storefront operator and a current mall owner, who said they would never support digital cash. As it is highly unlikely that a company conducting Internet commerce would forego the benefits of supporting a widespread, low-cost payment mechanism, were digital cash to attain that status, INPUT regards this reaction as an indicator of the fear, uncertainty, and doubt that currently surrounds digital cash, and expects such reactions to diminish sharply over the next two years.

Primary reasons for the increased use of digital cash include:

- The definition and widespread adoption of relevant standards and technology
- Business and public acceptance of conducting digital cash transactions
- The low costs involved in maming and processing digital cash transactions
- The ease of procuring digital cash

(Blank)

V

Internet Commerce Security—Importance and Satisfaction

A E-mail Security

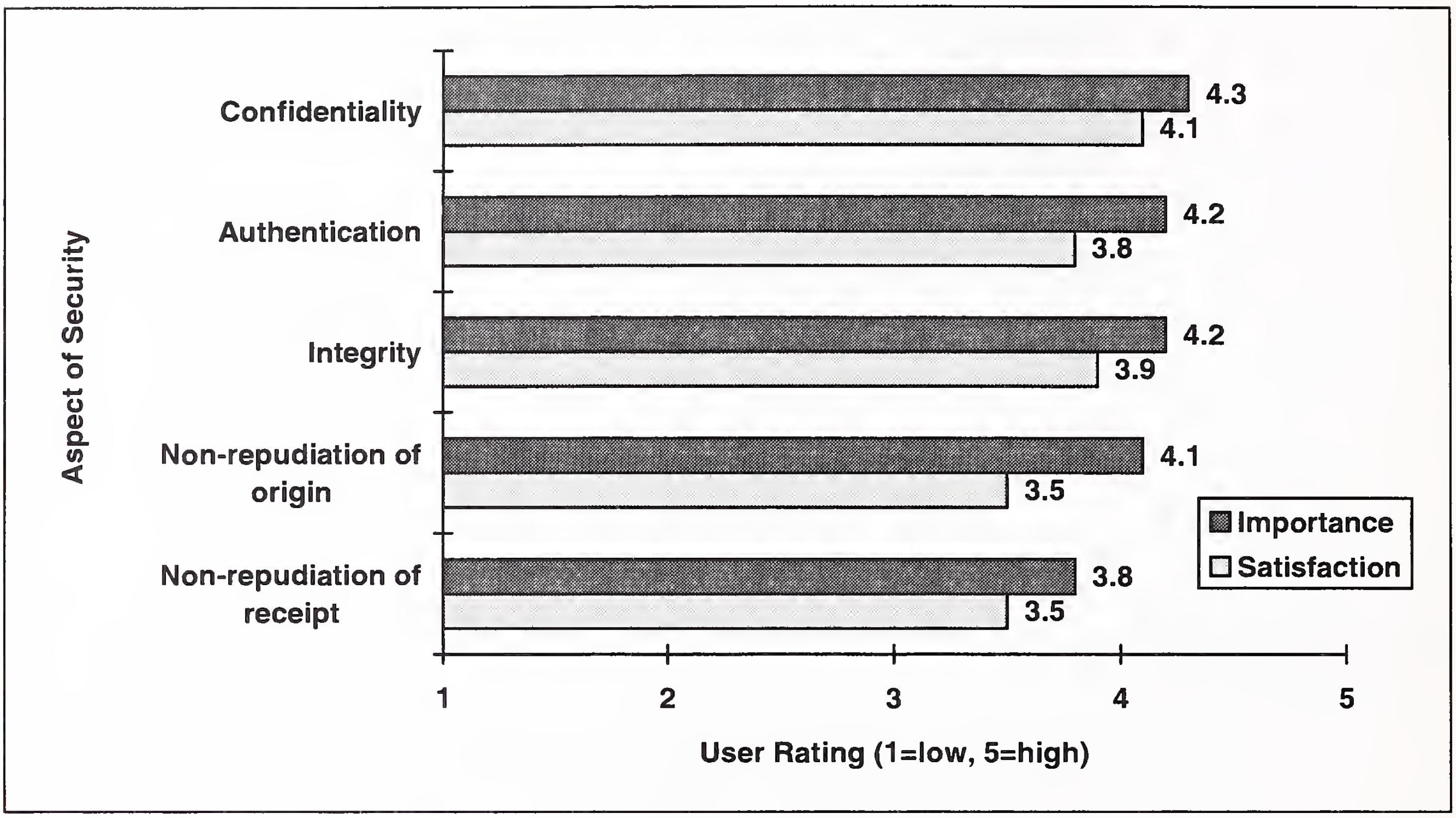
Survey participants were asked to indicate how important the individual aspects of security were to them for both e-mail and Web commerce. All aspects were rated as highly important, although for both e-mail and Web commerce, nonrepudiation of receipt and nonrepudiation of origin were rated as least important.

Respondents were also asked to rate how satisfied they were with their current e-mail and Web security. Again, nonrepudiation of receipt and of origin were rated lowest in both cases.

Exhibit V-1 shows users' ratings of importance and associated satisfaction with various aspects of e-mail security.

Exhibit V-1

Importance and Satisfaction of Security for E-mail



Source: INPUT

Satisfaction with confidentiality and integrity (and nonrepudiation of receipt, although this was least important) came closest to matching their importance.

Confidentiality is most important for e-mail-based commerce. As e-mail uses a store-and-forward mechanism, it is possible that potential eavesdroppers may have more time to discover an e-mail transaction being held on a mail gateway or server, and consequently to make a copy, than they would with a Web transaction, which is direct and immediate rather than stored for later retrieval.

Authentication is a particular concern for all e-mail transactions, be they confidential or not. It is a trivial matter to forge an e-mail message, including all the relevant headers that make up an e-mail message's credentials. Where purchase orders are used, an e-mail forger would in most cases have little to gain—the receiver would already hold a record of the customer's account and contact details, and would use these to process any order, not only what was contained in an e-mail itself.

This implies that e-mail security is, or can be, sufficient for requesting delivery against previously negotiated goods and service contracts. However, timing of delivery is critical for many EDI-related orders. This may be a key deterrent to the use of e-mail for electronic commerce because of the potential delay in arrival of messages and subsequent delay in shipment/delivery of goods.

Integrity, like confidentiality, is a potential problem for e-mail messages in that, as well as being intercepted en route, they may be discovered on a mail server pending transmission.

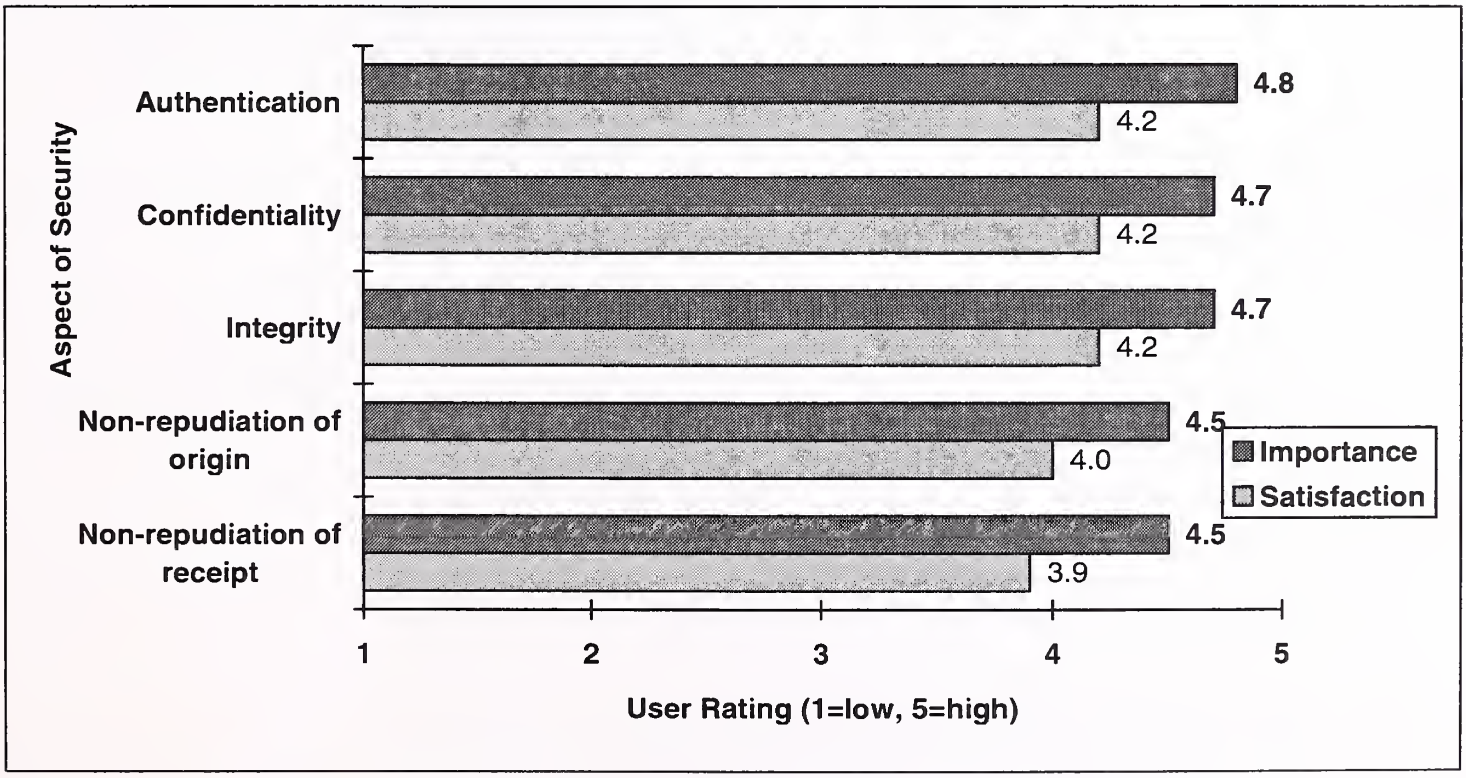
PGP (Pretty Good Privacy) is often used to satisfy all the above security requirements—to encrypt a message en route, to digitally sign an e-mail, and to ensure that a message arrives as it was sent—but PGP is relatively cumbersome to use and not legal in many countries.

B
Web Security

Users were also asked to rate the importance of and satisfaction with the security of the Web when used as a medium for electronic commerce. Exhibit V-2 shows the ratings for importance and satisfaction.

Exhibit V-2

Importance and Satisfaction Ratings of Security for Web Commerce



Source: INPUT

As with e-mail, the three most important characteristics of Web security are confidentiality, authentication, and integrity.

Satisfaction with current Web security is rated worse than e-mail security, comparative to the importance given to each category.

Authentication is the most important category, and in certain respects is less easy to regulate than with email. For example, many individuals within companies, and many consumers, do not retain the same IP address from one connection to another. These "dynamic" addresses are more anonymous than an e-mail address and, as their name suggests, a lot less static. For this reason, a customer's Web browser presents itself using a different identification each time it connects to a Web server.

Aside from the uncertainty of rapidly changing valid addresses, addresses can easily be forged, like e-mail headers. "IP spoofing" is a common method used to gain access to servers without authorization, or to masquerade as another user.

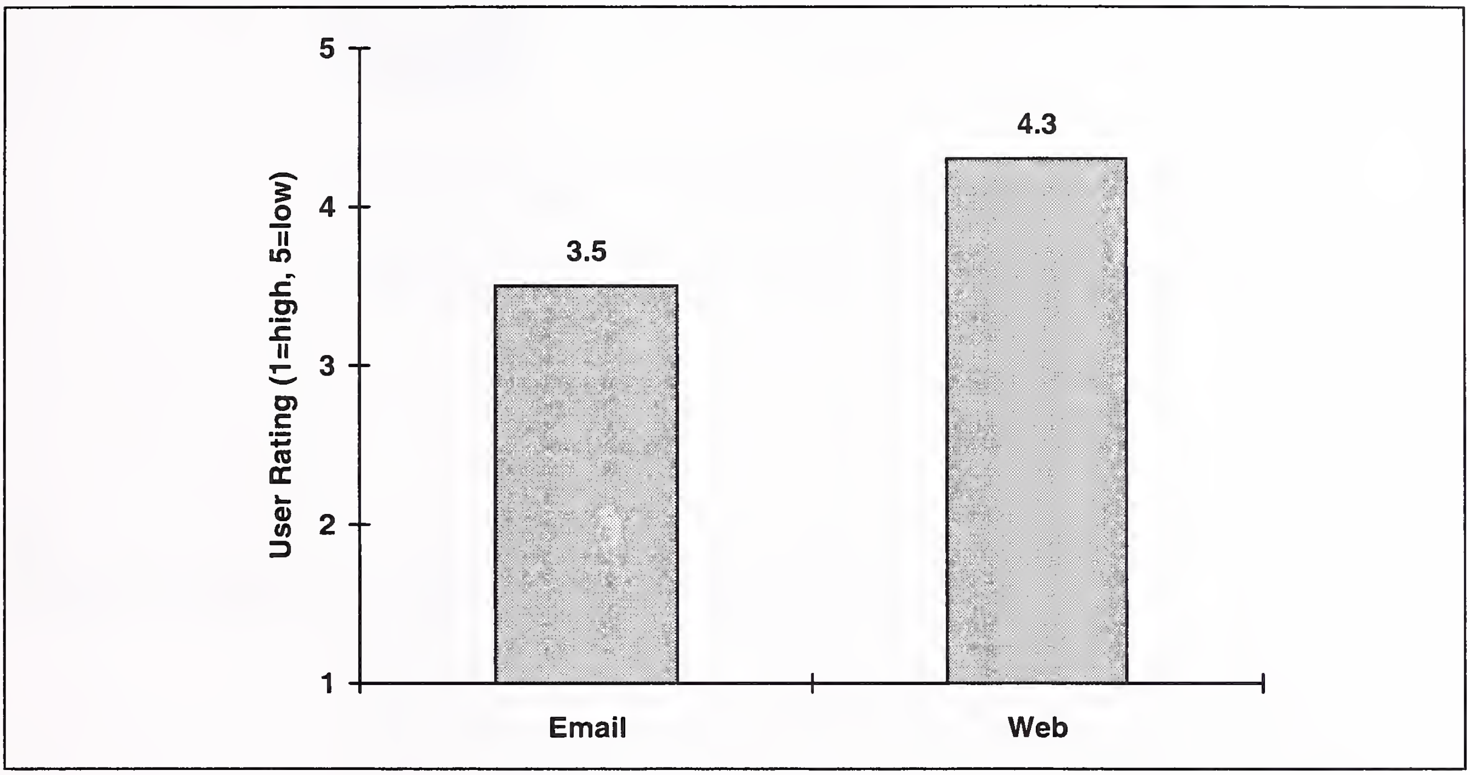
There is little a Web server can do against IP spoofing, beyond simple measures such as converting a numerical IP address into a meaningful name that can be checked against a range of valid addresses (the process is called reverse DNS lookup), and is the reason for the high importance placed on security technology that can manage this authentication uncertainty.

C
Confidence in E-mail and Web Commerce Security

INPUT asked storefront operators to indicate how confident they were that commerce could be conducted securely by e-mail via the Web. Significantly less confidence is put into e-mail as a medium for Internet commerce, as Exhibit V-3 shows.

Exhibit V-3

Confidence in E-mail and the Web for Internet Commerce



Source: INPUT

Reasons for placing greater confidence in the Web than e-mail for commerce might include:

- Real-time connection, not store and forward—a Web transaction is not queued in a server pending collection as e-mail is, sometimes for hours or days. Instead, it is immediate and happens in real time. This gives less opportunity for a transaction to be discovered and copied.

- Acceptance of the Web as a standard computing environment—the Web is a platform for applications, whereas e-mail is a simple message-passing medium. As more software applications migrate to the Web (for example, groupware), the greater the uptake of Web technology within companies in the form of intranets. INPUT's report *Revolutionary Migration of Applications to the Intranet* studies this in detail. The Web will become an environment used for all computing applications, and will be treated as a known, familiar environment.

- Security for the Web is becoming standardized—for example, the SET consortium's specification for credit card security over the Web. The same is not true to the same degree with e-mail, where a mix of different security technologies is employed.

(Blank)

VI

Policies and Practices for Secure Internet Commerce

A
Best Practices for Conducting Internet Commerce

INPUT asked storefront and mall operators to identify which security policies and practices they thought most important for conducting Internet commerce. Exhibit VI-1 shows how often the categories were mentioned as a proportion of all respondents who expressed a view.

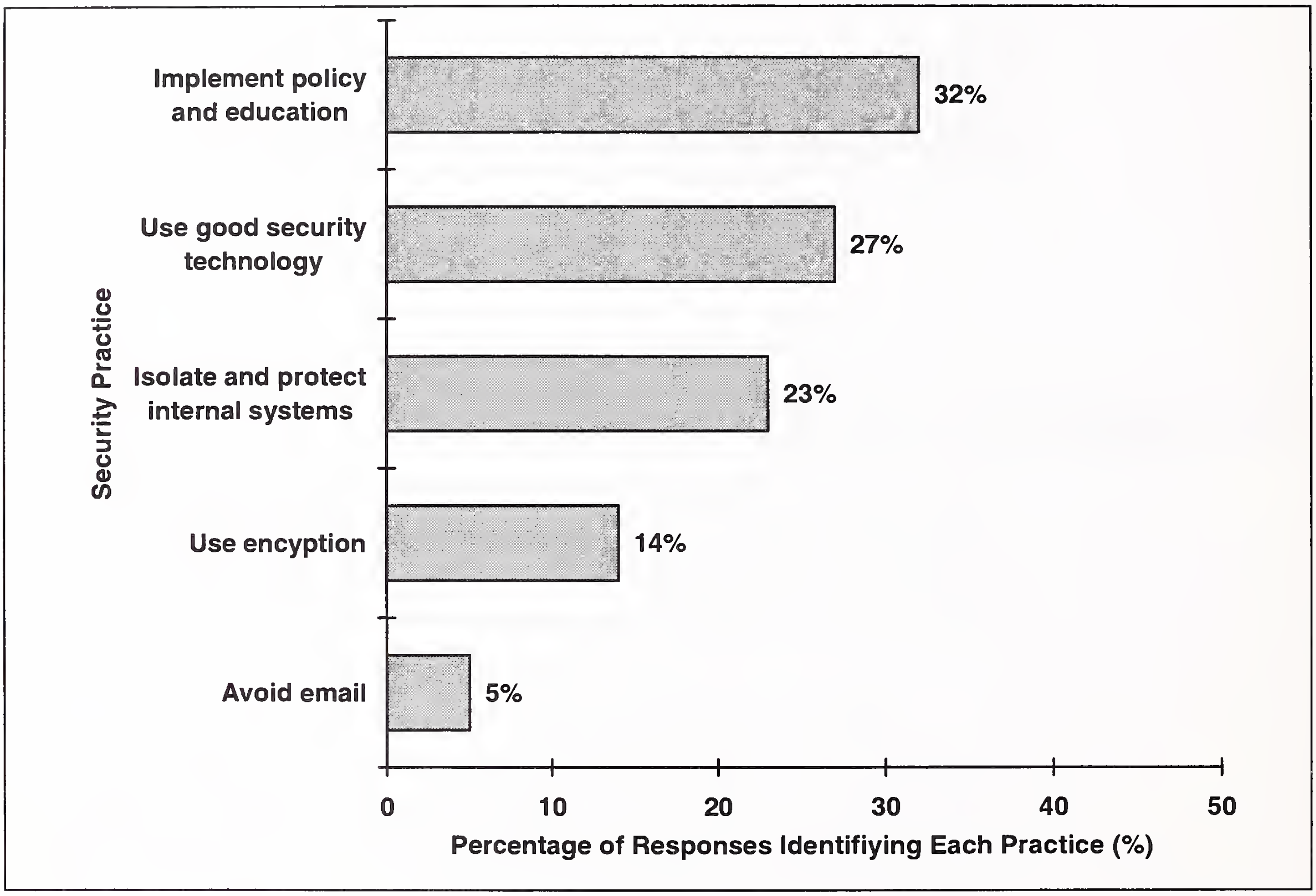
1. Implementing Security Policy

According to the sample, the best practice for conducting secure commerce is the definition, implementation, and enforcement of sound security policies and education. These include password management, managing access to systems, directories, and files, and sensitive traffic routing.

Where security is concerned, no amount of technology can substitute for well-planned and -implemented policies, and staff education is critical to ensure that any policy works. It is currently the case—and will remain so for the foreseeable future—that policy will remain at least as important as technology. It is possible in some cases to provide satisfactory security with good policies and no technology, but it is not possible to provide satisfactory security with good technology and no policies.

Exhibit VI-1

Best Practices for Operating a Commerce-Enabled Web Site



Source: INPUT

2. Technology

Use of good security technology was specified by many respondents. An obvious statement, perhaps, but some respondents stated their dissatisfaction with the security provided by the Netscape server and said it should improve. This may be a reaction to the security flaws uncovered in Netscape's products during 1995, which have been corrected, but nevertheless remain a concern.

Although it is possible to provide security with good policies and little technology, as stated above, that is an extreme. Good technology configured and used properly is clearly important in maintaining a secure environment.

3. Protecting Internal Systems

Isolating—or at least protecting—sensitive internal systems is an important factor in a storefront's security policy. All operating systems have security loopholes—that in UNIX's send mail, for example—and where confidential customer information is concerned, it is not good enough to rely on an operating system alone to protect against unauthorized access.

Passwords and domain authentication are relatively weak forms of security. Respondents recommended installing a firewall between internal systems and the Internet, and even physically removing sensitive systems from any internal network connected to the Internet.

INPUT believes that careful selection and thorough configuration of a suitable secure Web server and firewall is adequate security for conducting commerce over the Internet between locations where strong encryption is allowed (for example, in the U.S.). Despite reports of security loopholes in early Internet technology, transaction fraud is considerably more likely to take place outside the Internet by traditional means—card theft, telephone fraud, etc.

4. Encryption

The use of encryption also may seem obvious, but some transactions are carried out today without any encryption. Users may be unaware of the risk involved, or, at the other extreme, may be fully aware of the risks and, knowing that performing an unencrypted transaction over the Internet may be less vulnerable to compromise than everyday transaction practices (giving a credit card number over the phone in an open office, for example), are willing to take that risk. All storefront operators interviewed for this report use a secure Web server, or a server than can be extended to support encryption.

INPUT believes that soon after encryption standards have been accepted and are in use by most Internet users, all Internet data packets will be encrypted. This will include all e-mail and Web traffic, whether confidential or not. When it requires no extra effort on the user's part to encrypt data, and when all Internet software supports the accepted standards, there will be little point in not using encryption at all times.

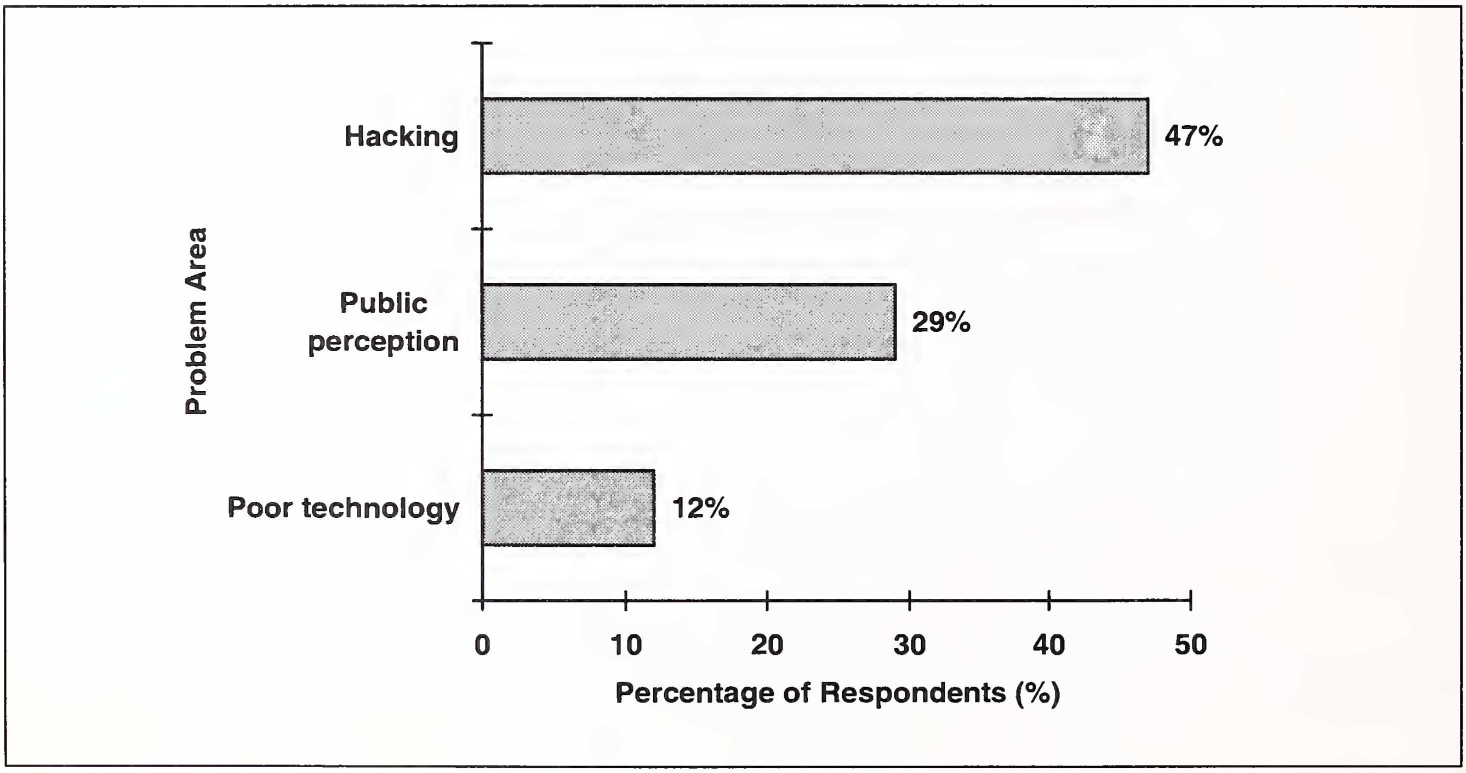
Prospective storefront operators expressed similar opinions on the best practices for conducting Internet commerce, with particular emphasis on the use of sound technology. Mention was made of password management, user education, automated security breach monitoring, isolation of sensitive internal systems, and adherence to industry standards (such as SET) as they emerge and are accepted.

B
Problems Faced in Conducting Internet Commerce

Users were asked to identify the major security-related problem they face in operating a site that supports commerce transactions. Exhibit VI-2 shows the mix of responses.

Exhibit VI-2

Problems Faced in Conducting Internet Commerce



Source: INPUT

1. Hacking/Fraud

Smentioned major problems perceived by storefront operators, and were categorized as follows:

- Intercepting transactions, or "line sniffing"—Monitoring a line until an unencrypted transaction is made and capturing the details, or capturing a weakly encrypted transaction and attempting to crack it

- Fraud—Passing fraudulent credit card information

- Cracking—Breaking into internal systems storing customers' credit card details

2. Public Perception

Public confidence in transmitting credit card details over the Internet remains a serious problem for Internet merchants.

User education is effective, but some merchants believe only the passing of time will allay users' concerns about giving their details on line.

3. Technology

Lack of sufficiently secure technology was another problem mentioned. One respondent company develops some of the software it needs in-house, as it does not consider commercially available Web browsers secure enough.

4. Encryption Export Restrictions

Although not counted as a major problem category (this survey was conducted among U.S. merchants), a Canadian storefront said that obtaining high-quality security technology was difficult outside the U.S.

This applies to any non-U.S. storefront operator and will remain a problem until the U.S. government relaxes its restriction on the export of encryption technology. For example, the version of PGP that is cleared for export only allows the use of 40-bit keys, legally, although this is regarded as breakable encryption.

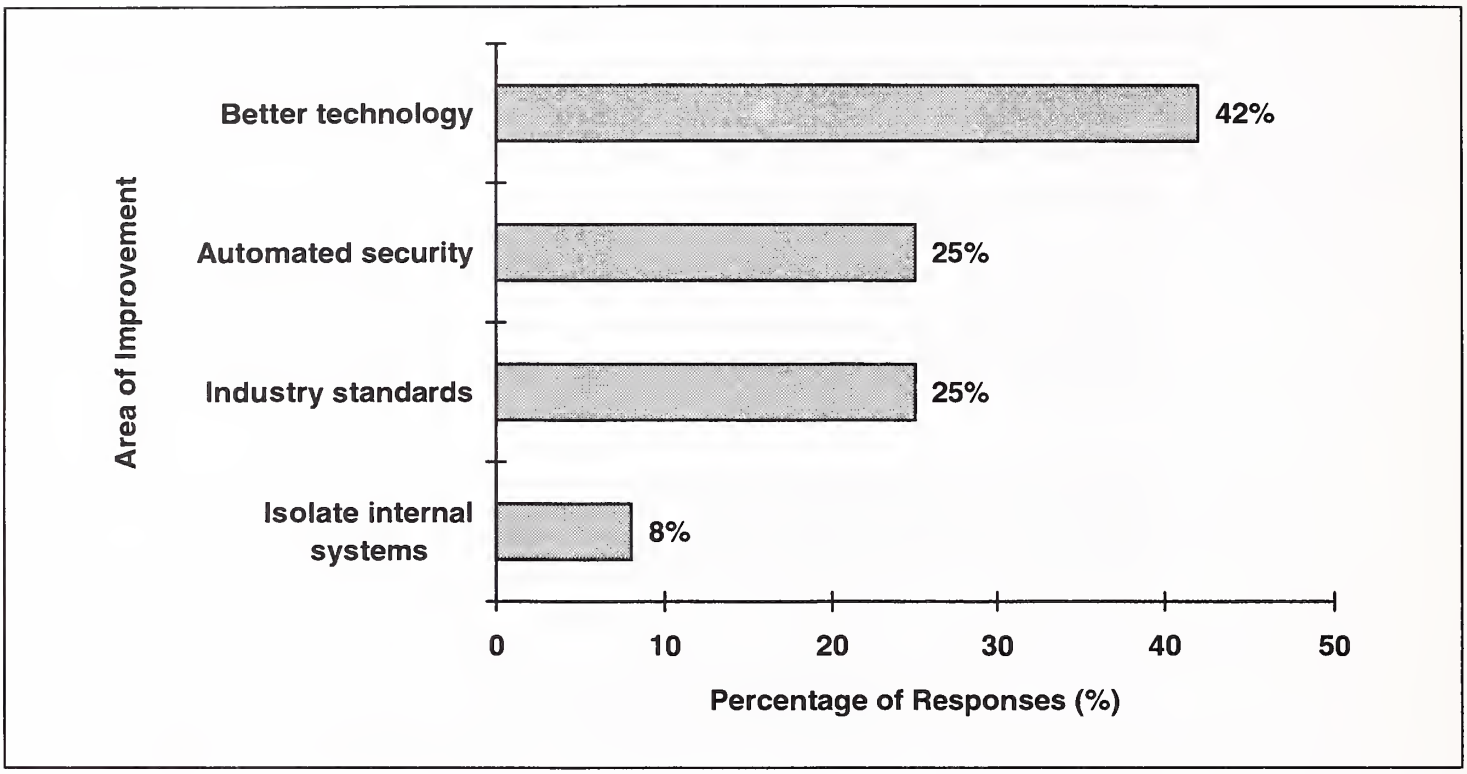
It will also remain an issue for U.S. companies wishing to conduct business over the Internet with customers and suppliers outside the U.S. The current inability of U.S. organizations to perform secure and legal transactions internationally will both restrict commerce and encourage security vendors to negotiate internationally acceptable encryption technology.

C
Improving Security

INPUT asked respondents how they felt the security technology and products they used could be improved (see Exhibit VI-3).

Exhibit VI-3

Areas for Security Improvement



Source: INPUT

The need for improved security technology was mentioned by nearly half of current storefront operators expressing an opinion, although the lack of high-quality security technology was perceived as an actual problem by fewer companies.

The high-profile reports over the last two years of security flaws in popular Web browsers, notably Netscape's, damaged the Internet's credibility as a secure environment for commerce, even though most of the flaws discovered were minor and presented little threat to most users.

The automation of security mechanisms was also a popular choice, as was the development and acceptance of industry standards for security protocols. SET was mentioned as an example of how this is developing. Internet merchants are concerned to capture the largest possible potential customer base, and this is easiest for them to accomplish if they are confident that any Web browser can communicate securely with their Web server, using accepted underlying standards.

Security automation and industry standards are both required to make security invisible to users and ubiquitous. When this happens, most or all Internet traffic will be encrypted regardless of its confidentiality.

When encryption is a standard feature of all Internet software, the potential market for Internet security technology suppliers, at the extreme, includes all applications purchased by all users. INPUT expects all Internet applications to be accessed eventually through a Web client. This includes applications currently accessed and executed using traditional platforms—groupware, database, ERP, and personal productivity applications, for example.

(Blank)

VII

The Role of the Chief Security Officer

A
The Need for a CSO

The issue uppermost in many people's minds whenever the Internet is discussed is security. The image of the Internet as an insecure environment in which to conduct commerce is a strong one, particularly among those with less Internet experience or knowledge.

The reality is that commercial transactions can be made securely over the Internet, provided the right technology is used. As with any security system, adequate policies and training must be established for that technology to effective.

Using traditional transaction methods—telephone, fax, postal mail, private networks, managed networks, and direct dial-up connection—security is typically either provided or otherwise guaranteed by a third party (private or managed networks), or little specific security is available (telephone or fax).

The Internet falls somewhere between a managed network and the public telephone system. Unlike a managed network, no single party owns or controls the means of communication between companies conducting business, and so a security breach cannot be blamed on the network provider. Yet unlike the telephone network, which is as open to eavesdropping as the Internet, individual parties can use technology to ensure private communication. Although they normally cannot hold another organization responsible for the security of their transactions, they can take steps themselves to satisfy their own security needs.

These steps are currently not seamless, transparent, or standardized, and so take skill and care in implementing and managing. This is one of the biggest differences between the Internet as it stands today and other, longer-established methods of communication.

The rate at which security technology is being developed and integrated into standard Internet software is matched by the rate at which Internet commerce is increasing (INPUT expects 45% of all electronic commerce by value worldwide to be conducted using the Internet by 2001).

Combining the rapid growth in use of the Internet for commerce and the still incompletely available security indicates that there is a need for security to be taken extremely seriously by users. Though it may be considered adequate for security responsibility to be assigned to a general IS role for organizations that use the Internet only for external browsing and email, this may not be sufficient for companies performing sensitive business transactions.

INPUT examined the perceived need for a full-time security role within storefront organizations, which by definition are using the Internet for commerce, and also gained the views of Internet security-related vendors.

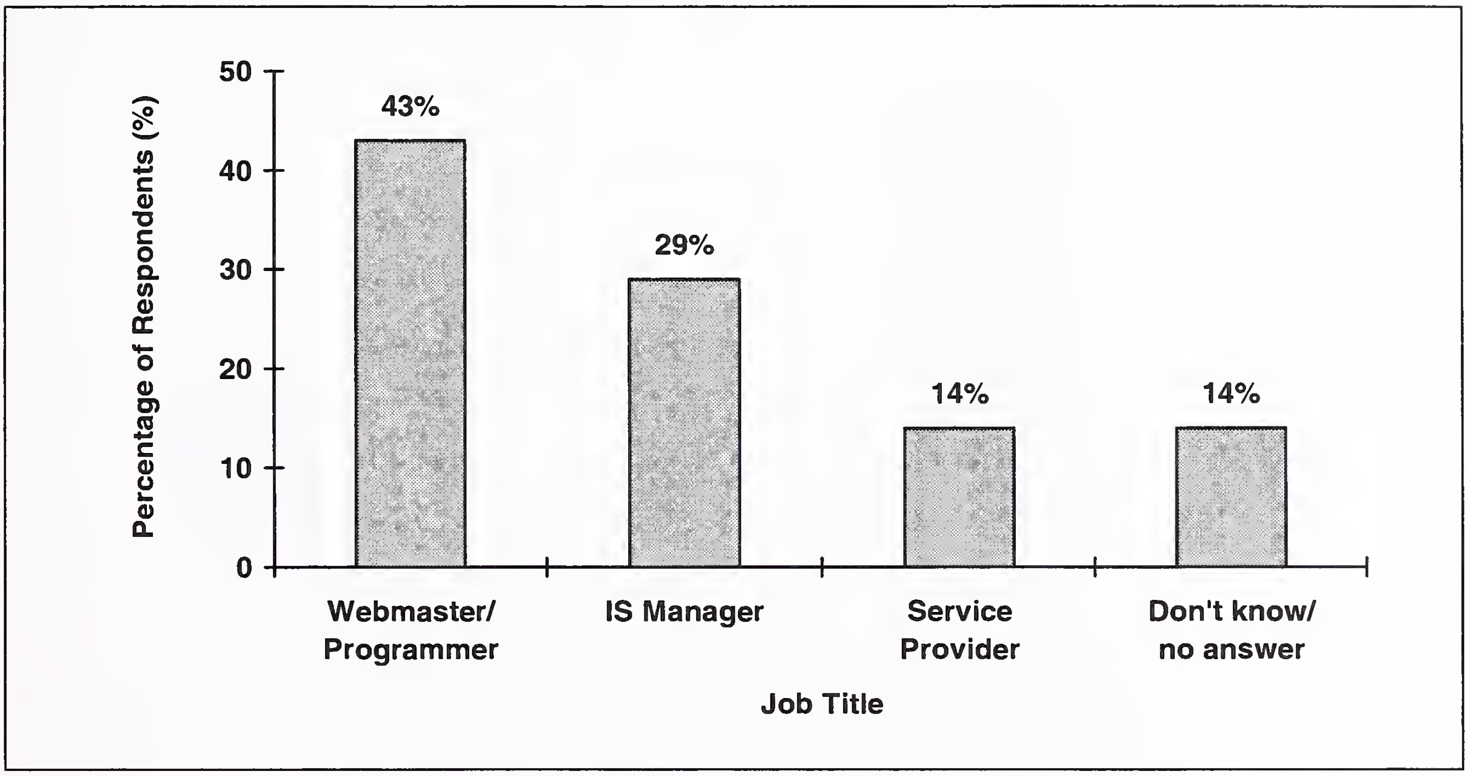
B

Current Commerce-Related Security Responsibility

Exhibit VII-1 shows the job titles of staff currently assigned commerce-related security responsibility among storefront and mall operators. Within storefronts that run their own Web sites, nearly all assign security to an existing member of the IS department. This shows that Internet security seems to be treated no differently from general computer and network security—it is one of the many responsibilities held by existing IS staff.

Exhibit VII-1

Job Title with Current Security Responsibility



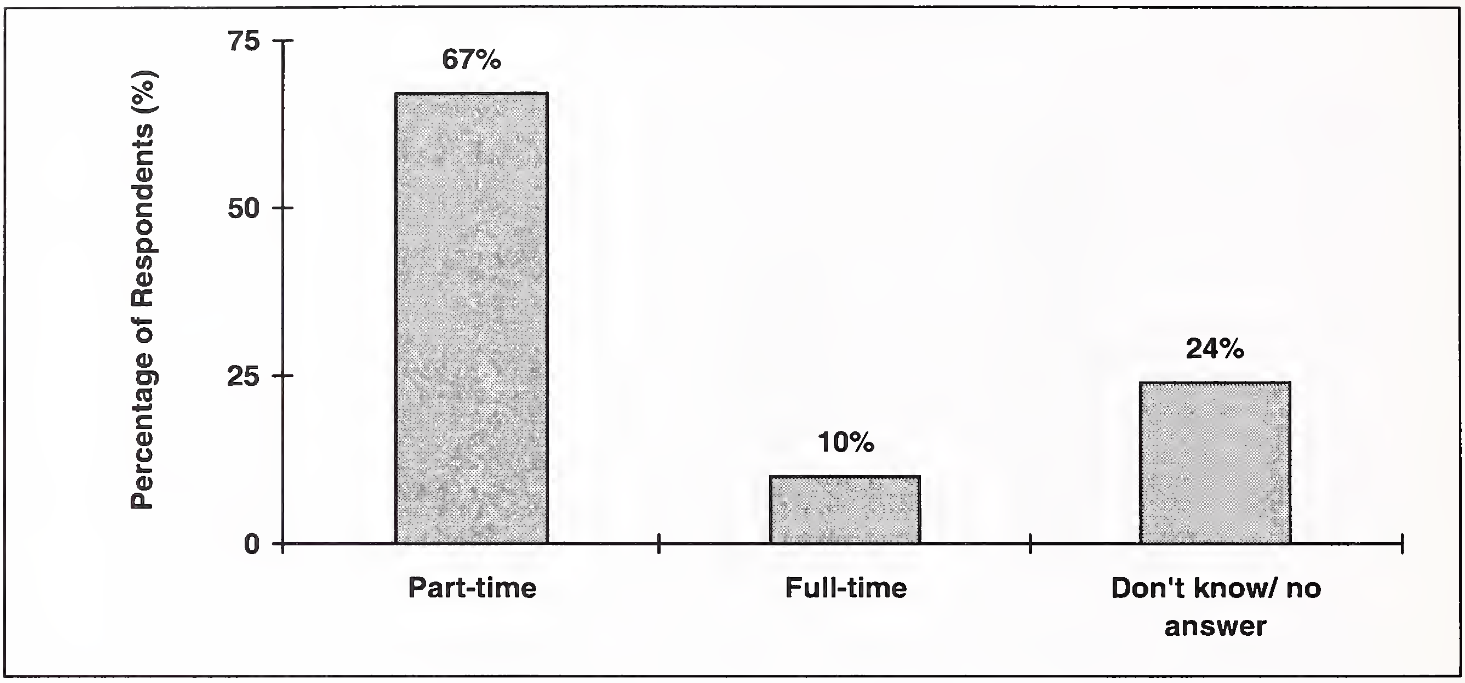
Source: INPUT

As shown in Exhibit VII-1, security is not currently a full-time occupation. The function is usually combined with existing responsibilities in an existing function.

As Exhibit VII-2 shows, only a tenth of current storefront and mall operators interviewed said they have created a full-time security position for Internet commerce.

Exhibit VII-2

Full-time/Part-time Security Responsibility



Source: INPUT

Although storefront operators clearly are not eager to create full-time security positions, vendors take the opposite view. Vendors interviewed were more certain overall of the need for a CSO within an organization handling Internet transactions. The vendors' view is that the widespread creation of a new CSO job title would simplify their relationships with customers and would extend the security market.

C
Future Commerce-Related Security Responsibility

INPUT questioned current and prospective storefront owners about their future plans for a full-time security position. Although respondents who were still developing their storefront site were more enthusiastic about the idea of a CSO role than were those who had already begun operating, the overall picture is one of "business as usual." The interviews indicated that Internet merchants do not see a great need for a CSO.

1. Current Operators

Of the current storefront operators interviewed, only one planned to initiate a full-time security position. That organization planned to create this position during 1997, intending to designate it "Online Security Manager."

Over half of current storefront companies said they would never create a full-time position for commerce security.

2. Future Operators

Companies intending to set up a storefront or mall in the future were split equally between those intending to create a full-time security position and those who are not; only two companies said they would never create a full-time position.

This is the opposite of the practices and plans reported by current storefront operators. While future storefront organizations have good intentions, the views of current operators are based on experience.

Therefore it appears, based on these responses, that there is little requirement for a full-time Chief Security Officer.

Future storefront operators also varied in their choice of staff members to perform commerce-related security. Most believed that security would come into the realm of the IS department (being assigned to such staff as Webmaster or IS manager), but one intended to assign a full-time Chief Security Officer (CSO).

D

Responsibilities of the Current Security Officer

INPUT asked respondents what were the major responsibilities held by the person currently in charge of security. Two main areas emerged: technology and policy.

1. Technology

Around half of respondents stated that procuring and installing security technology was a major area of responsibility for the person involved. This includes Web browsers and servers, and authentication and encryption technology. As around three-quarters of respondents allocate security responsibility to the IS department, this responsibility often involves overseeing the maintenance of security technology alongside other internal systems for which the IS department is responsible.

Integration with existing back-end systems is included in the procurement and installation of security technology.

The second most frequently mentioned technology-related responsibility is ensuring that systems are in place to block access to internal systems from the outside world. This includes primarily the procurement, installation, and maintenance of firewalls, but also the implementation of password control policies.

Ensuring that communications links to customers and banks (and in the case of malls, communications links to merchants) are reliable and secure and that adequate capacity planning is performed are additional duties of the security personnel.

As Webmasters are currently involved in implementing security, there is an element of storefront design involved. Webmasters with security responsibilities design front ends for transaction-oriented pages in a way that ensures that security is overseen from client transaction to back-end processing.

INPUT expects that, in addition to the above responsibilities, a CSO would be charged with tracking (and implementing, where appropriate) emerging security technology and, particularly, standards as they are adopted by existing and potential customers. An example is SET, the standard in development for credit card transactions. A CSO would monitor the status of SET specification and supporting technology and enhance the storefront's transaction infrastructure at the relevant time.

2. Policy

Security technology without corresponding security policy is of little use. Security policy and planning was mentioned by nearly as many respondents as pure technology issues among the major responsibilities of current security assignees. Security policies mentioned include the following:

- Password management—Defining and enforcing password creation and allocation, expiry times, password file access restrictions, and password confidentiality

- Staff availability—Ensuring that security staff are on call at all times in case of server failure, intruder alerts, or other security breaches

- General procedures—Defining usage policies based on security requirements, including restricting access to systems, directories, and files based on clearance levels, and defining to which systems and people confidential information is routed within an organization and the routes taken

- Security balancing—ensuring that security is implemented and enforced transparently enough so that neither the effectiveness of the systems being protected, nor staff productivity is affected

INPUT views policy as the critical element of any Internet commerce environment. As well as taking into account the above points, a coherent commerce security policy should be integrated into the company's overall business model where relevant to ensure consistency of goals and ways to achieve them. A holistic approach to integrating security into the business is not as convenient as an additive set of isolated, technology-related policies, but is the surer method of achieving a robust and secure environment.

(Blank)

VIII

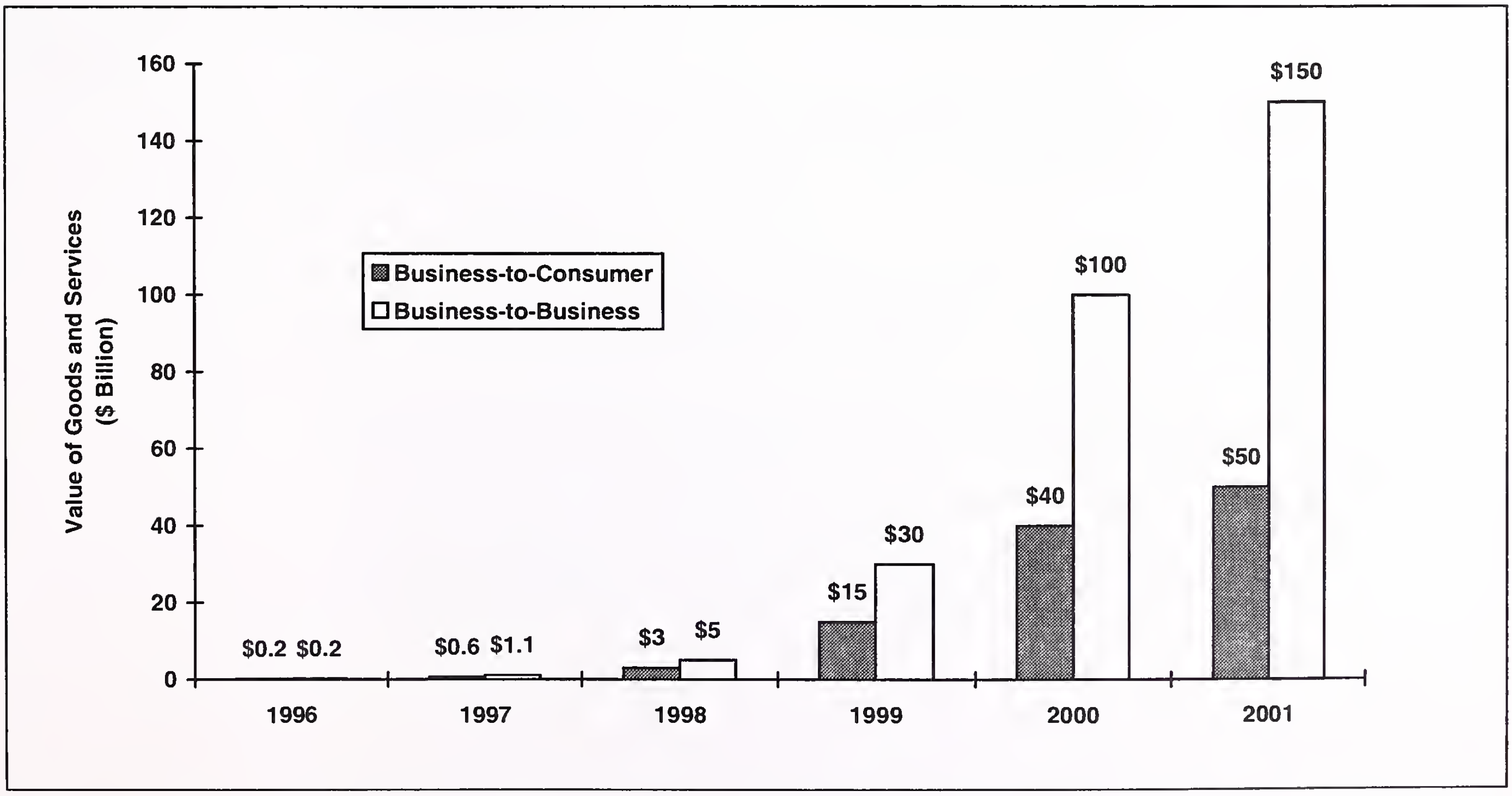
Market Forecasts

A

Value of Goods and Services Sales Enabled by Security

Exhibit VIII-1

Value of Goods and Services Sold Worldwide via Internet Enabled by Security, 1996-2001



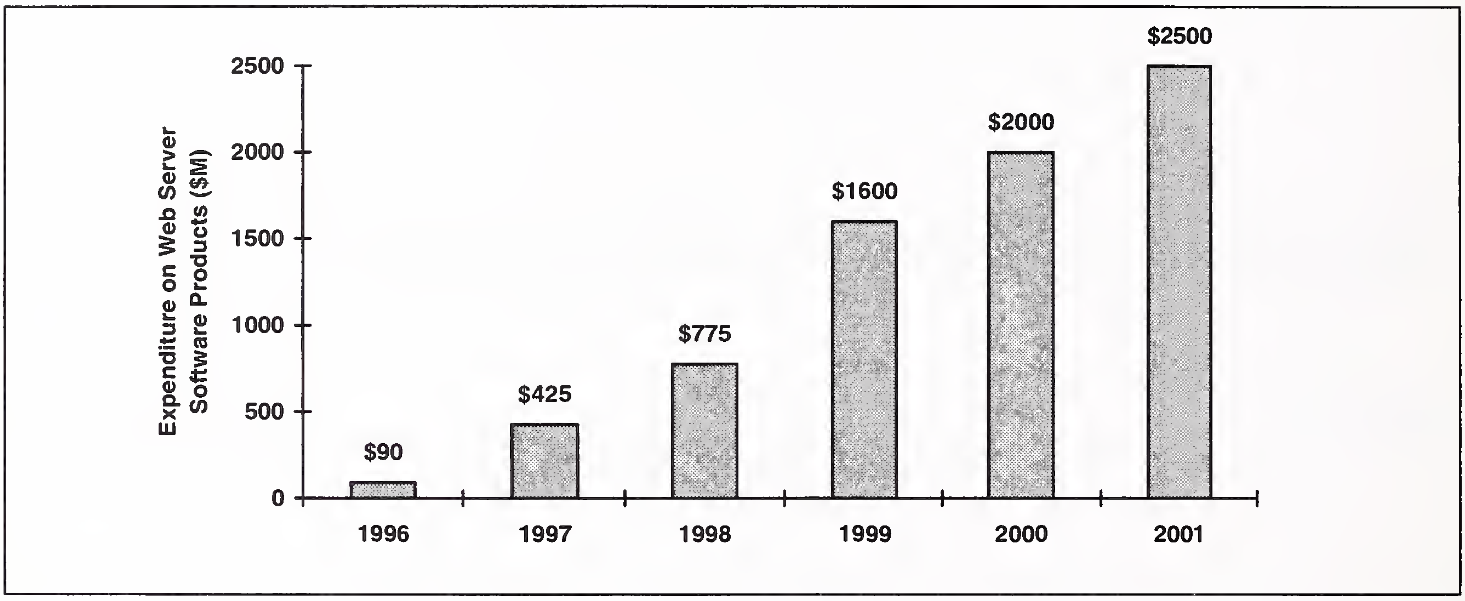
Source: INPUT

B

Secure Commerce-Enabling Web Server Software

Exhibit VIII-2

Worldwide Expenditure on Web Server Software Products for Commerce, 1996-2001



Source: INPUT

A

Security Technology, Vendors, and Consortia

A The Major Elements of Security

INPUT's definition of security (for Internet commerce) is comprised of five elements:

1. Confidentiality

The assurance that a message has not been intercepted and read en route to its destination.

Confidentiality is achieved through the use of encryption. See below for a description of public and private key encryption methodologies.

2. Integrity

The assurance that a message received is identical to and unchanged from the message that was transmitted.

Integrity checking can be performed if the original message is accompanied by a message digest (the result of performing a hashing algorithm on the original message). If the recipient also hashes the original message to get a new digest and this is not identical to the transmitted digest, then the message has been altered en route.

3. Authentication

The assurance that the person purported to have sent a message is the real sender. Authentication is provided by a digital signature.

4. Nonrepudiation of Receipt

The inability of a message recipient to deny that he or she received the message.

5. Nonrepudiation of Origin

The inability of a message sender to deny that he or she sent the message.

B Public Key and Private Key Encryption

1. Private Key (Symmetric)

A private key encryption system (also known as symmetric encryption) uses one key to both encrypt and decrypt a message. The sender and recipient of a message must therefore both know the key.

The advantage of private key encryption is that it is fast. It is well suited, therefore, to “bulk” encryption—encryption of large amounts of data.

The security of a private key system relies on that key being kept secret. This introduces a major problem for those contemplating using private key technology to encrypt Internet messages: how to transmit a secret key to a recipient without that key being intercepted, altered, or otherwise compromised en route. The practical answer is to use a combination of public key and private key encryption (see below).

The most common form of private key encryption is DES (Data Encryption Standard).

2. Public Key (Asymmetric)

A public key encryption system (also known as asymmetric encryption) uses two keys: a public key known to the world at large, and a private key stored securely on a user’s system and never divulged to anyone else.

The sender of a message uses the recipient’s public key to encrypt the message. The recipient then uses his or her private key to decrypt the message. The two keys are related so that only the private key corresponding to a certain public key can decrypt a message encoded with that public key. However, the private key cannot be ascertained from the public key.

The major advantage of public key encryption is that a user's private key is never transmitted over a network. This eliminates the chances of any sensitive key-related information being intercepted, although the usual security risks of storing any information on a computer, even a physically isolated one, are present.

The disadvantage of this method is that it is slow. Public key encryption is roughly 1,000 times slower than private key encryption. This makes it most suitable for encrypting keys and digital signatures, rather than entire long messages.

The most common form of public key encryption is RSA.

3. Mixed Public/Private Key Encryption

Public and private key encryption both have a major advantage and a major disadvantage (see Exhibit A-1).

Exhibit A-1

Advantages and Disadvantages of Public and Private Key Encryption

Encryption Method	Major Advantage	Major Disadvantage
Private key (e.g., DES)	Fast	Must transmit private key
Public key (e.g., RSA)	No need to transmit private key	Slow

Source: INPUT

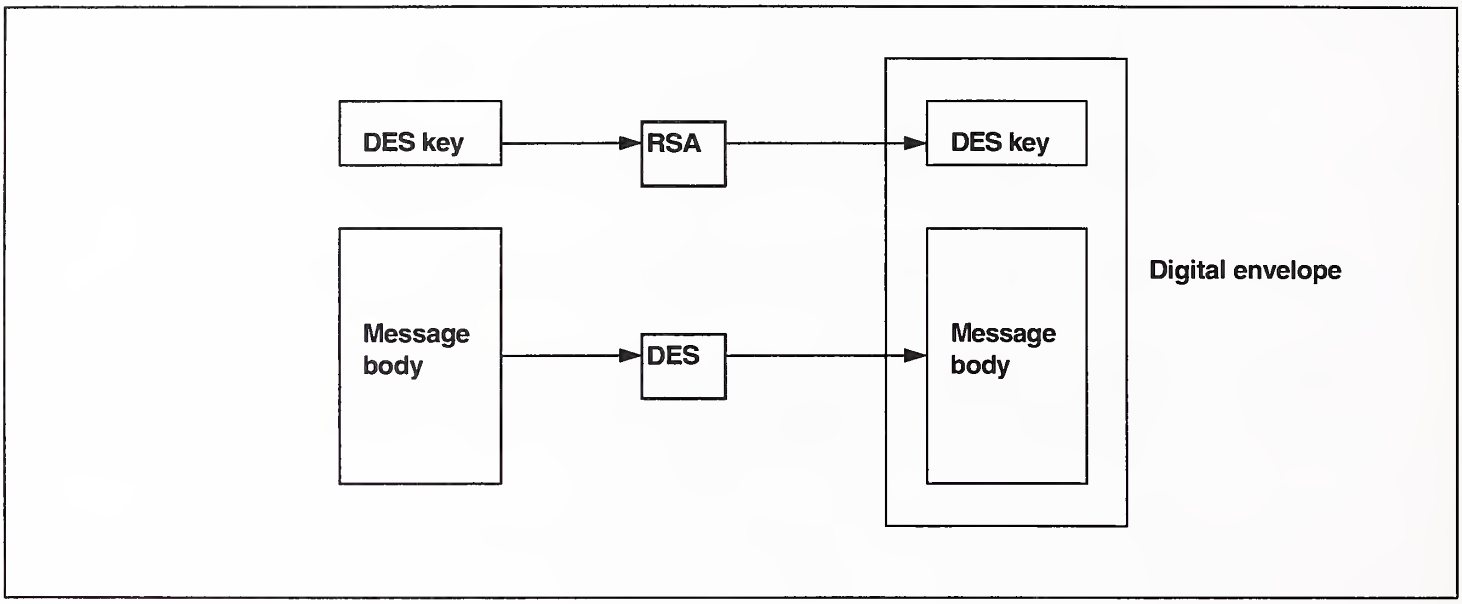
It is possible to combine private and public key encryption methodologies to keep both benefits and lose both disadvantages.

A mixed private/public key system encrypts the body of the message using private key encryption. It then encrypts the private key itself using public key encryption. The result is a "digital envelope" that can be transmitted over the Internet securely. The recipient uses the private key of his or her public key pair to decrypt the private key that will unlock the body of the message.

This method provides both the speed of private key encryption and the security of public key encryption without any of the disadvantages. Exhibit A-2 shows the construction of a digital envelope, using DES as the private key and RSA as the public key technologies.

Exhibit A-2

Digital Envelopes—Mixed Private/Public Encryption



Source: INPUT

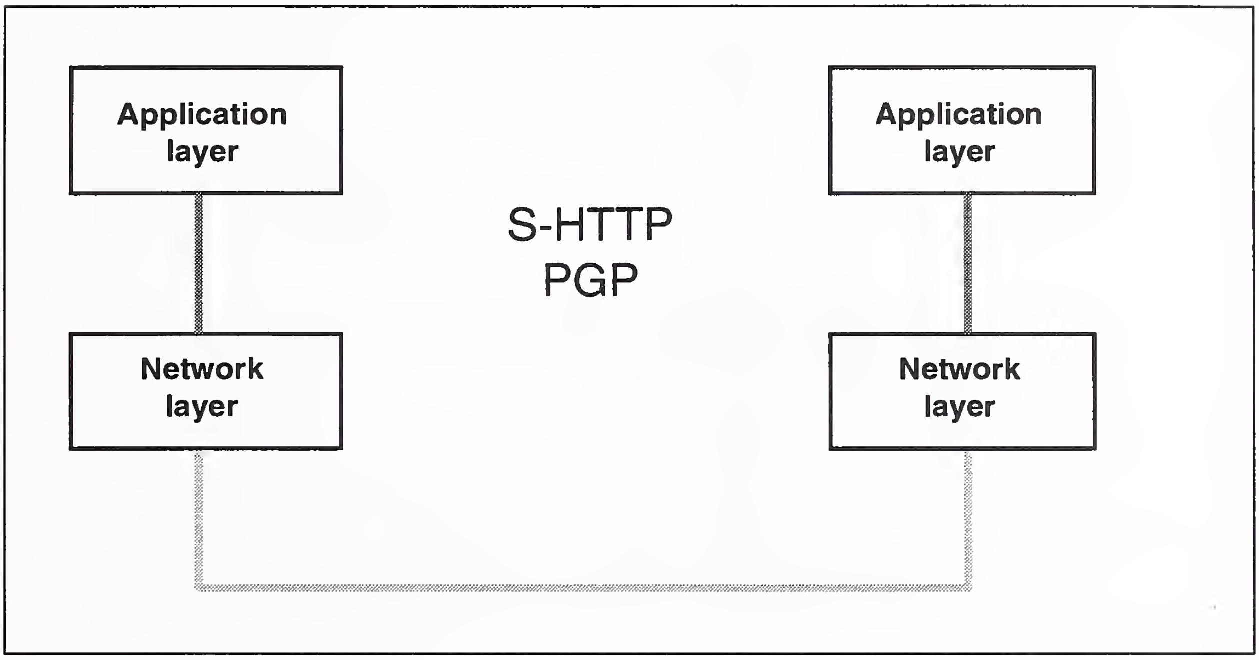
C
Transport and Data Security

1. Transport Security

Transport security is that which protects the channel between message sender and recipient. Specifically, it protects at the network layer—TCP/IP. Transport security does not take account of what type of data passes over the network; it is only aware of IP packets. An example is SSL (Secure Sockets Layer), which encrypts individual packets as they are routed through IP sockets (communications channels).

Exhibit A-3

Transport Security—Network to Network



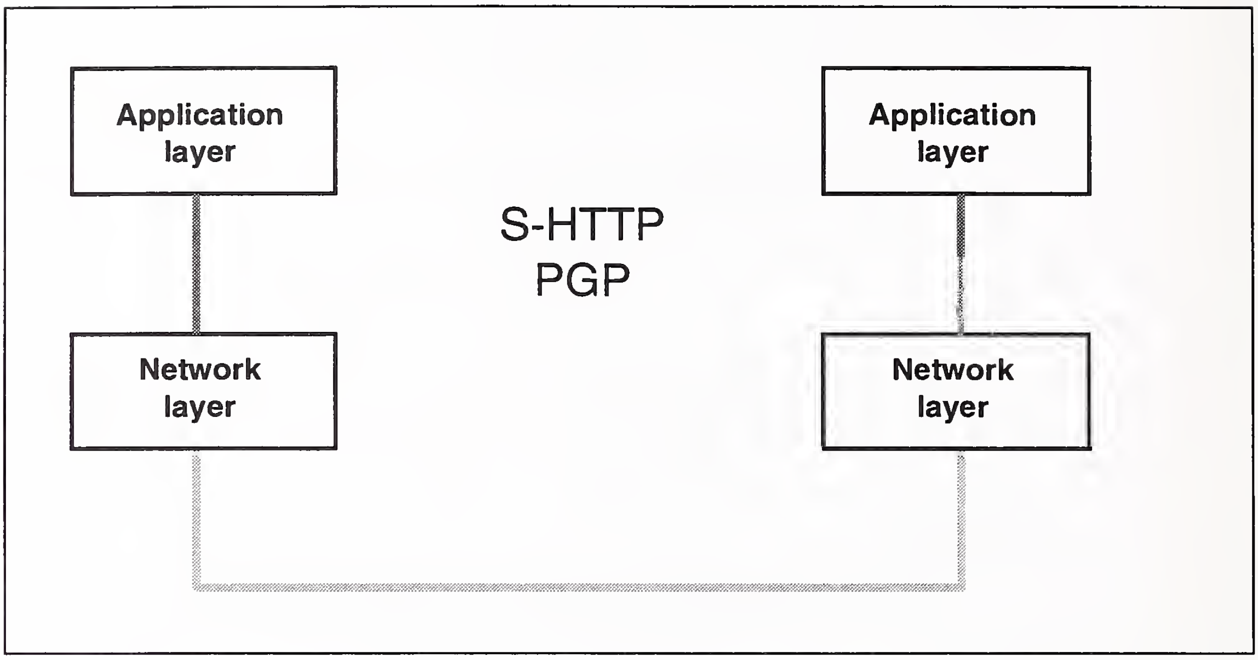
Source: INPUT

2. Data Security

Data security protects individual documents, messages, and transactions, based on the type of document or message being transmitted. A data security system must, therefore, be aware of the data format used. An example is S-HTTP (Secure-HTTP), which is a secure version of the Web's HTTP protocol for exchanging HTML documents.

Exhibit A-4

Data Security—Application to Application



Source: INPUT

D
DES Encryption

DES (Data Encryption Standard) is a relatively old symmetric key encryption technology originally developed by IBM in the 1970s. It is a symmetric mechanism, meaning that DES uses the same key both to encrypt and to decrypt messages.

DES encrypts data in blocks of 64 bits, and uses a 56-bit key. Despite the relatively short length of the key, DES has never been broken. DES is far more likely to be compromised by the acquisition of the secret key than by brute force cryptanalysis.

As it is a symmetric mechanism, DES encryption and decryption is fast. DES is well suited, therefore, to bulk encryption—encryption of large amounts of data.

If DES is to be used on its own, without public key encryption being used to transmit the DES secret key, it makes sense to minimize the chance of key acquisition and maximize the strength of DES's encryption. This means using the same secret key for multiple messages, or even not changing the secret key at all. The chances of individual messages being compromised are small, but the loss incurred if a key is discovered is considerable, as all messages are encrypted using the same key.

Using the mixed public/private key system of digital envelopes offers considerably greater security against both individual message compromise and key compromise (as the DES secret key can be changed for every message).

E
RSA Data Security Encryption

RSA Data Security is the developer of the RSA public key encryption technology. Like DES, RSA was originally developed in the 1970s.

RSA markets an encryption engine, BSAFE, which provides a library of encryption algorithms and modules for software developers to add encryption and authentication features to applications. BSAFE includes modules for other encryption mechanisms apart from RSA, including DES, Diffie-Hellman, RC2, RC4, and RC5.

RSA is providing the underlying encryption technology for the SET specifications. The company will also provide its own products based on SET. The first deliverable will be a SET upgrade for RSA's BSAFE 3.0 engine, followed by a SET development toolkit later in 1996. RSA will also work with partners, including Netscape, Microsoft, and Oracle, to build SET compliance into Web and e-mail clients.

In April 1996, RSA was acquired by Security Dynamics Technologies, a supplier of user identification and authentication products.

F
PEM (Privacy Enhanced Mail)

PEM (Privacy Enhanced Mail) adds the major security services—confidentiality, authentication, integrity, and nonrepudiation—to standard e-mail messages using a certificate-based key management mechanism. As it is designed to protect only basic e-mail, it works only with plain text messages.

Reflecting the trend of e-mail to encompass more than just plain text, PEM is not likely to become the dominant e-mail security standard unless it can support embedded multimedia, a development that has already taken place with MOSS.

G
MOSS (MIME Object Security Services)

MOSS (MIME Object Security Services) is based on PEM. The major difference is that PEM is confined to text-only messages, and MOSS includes support for multipart multimedia messages.

Also unlike PEM, which is based on a certificate architecture, MOSS uses only a public/private key pair.

H
S/MIME (Secure MIME)

S/MIME is a secure version of the e-mail MIME (Multipurpose Internet Mail Extensions) standard and is based on RSA.

Unlike PEM, which is limited to text, S/MIME inherently supports any data format, including multimedia—the MIME standard allows new content types to be supported as they appear.

S/MIME is expected to become the default standard for e-mail security, due to its widespread adoption by major vendors. These include Microsoft, Lotus, Netscape, and Nortel. Despite this, MOSS and S/MIME will vie for widespread adoption over the coming years.

I
Terisa Systems

Terisa Systems, developer of S-HTTP, was created in 1995 as a joint venture between RSA and EIT. The company's core security product for Internet commerce is the SecureWeb Toolkit.

Terisa is a privately held company that has received investment dollars from IBM, America Online, CompuServe, Netscape, Motorola, and Olivetti Telemedia in exchange for a seat on the Terisa board.

SecureWeb Toolkit is available in two versions: client (for integrating Web security protocols into client software) and server (for implementing certificate and encryption key management tasks on the server). An add-on is also available to support the SET specification.

By supporting all the major Web security protocols, SecureWeb Toolkit allows a developer to create an application that allows the user to open an SSL socket, generate an SET payment, and convert the HTTP request to S-HTTP.

J
VeriFone/EIT

VeriFone, by tradition a POS hardware and software supplier, acquired the Internet security company and developer of S-HTTP, EIT, in 1995. The result of the acquisition was Verifone's Internet Commerce Division (ICD).

ICD concentrates on payment systems more than core security technology. It uses off-the-shelf security such as SET, RSA, and SSL to build Internet commerce applications in a way that reflects VeriFone's POS history.

One such application is vGate, a security gateway between an Internet merchant and a bank. vGate handles decryption, translates messages to a format the bank's systems can read, receives authentications, encrypts messages back to the merchant, etc. vPOS is a similar gateway that sits between the merchant and a consumer, handling transactions and related administration.

vGate and vPOS both support the initial SET specifications, and VeriFone claims to be the first vendor to release SET-conformant products.

K
VeriSign

VeriSign is a spin-off company of RSA, set up in May 1995 to provide digital authentication products and services. The most important factor in a digital certificate provider's success is the confidence placed in it by users—consumers and merchants. VeriSign, with RSA behind it, has quickly become known as a trusted, safe organization.

A VeriSign digital signature is used to provide assurance that a message encoded with that signature is from the person it purports to be from. A transaction recipient is able to verify signed incoming messages against VeriSign's registry of stored signatures, rather than relying on authentication contained purely within the message itself.

VeriSign provides four levels of signature according to the level of security required. These range from password applications (where a document is protected only by user name and password), through transaction applications (on-line transaction and secure e-mail) and banking applications (where large sums of money change hands), to highest security applications. VeriSign's identification requirements (and costs) are scaled accordingly, from simple name and e-mail verification to personal interview and rigorous personal investigation.

VeriSign signatures are supported by, among others, IBM, CompuServe/Spry, Microsoft, Netscape, and Open Market.

L
Netscape

Netscape is the developer of SSL (Secure Sockets Layer) and is using SSL as the basis of its secure commerce server offerings.

SSL is a transport security protocol that runs beneath both secure and insecure application protocols (HTTP, S-HTTP, FTP, telnet, etc.). SSL includes server authentication (allowing any SSL client to verify the identity of the server using a certificate and a digital signature), client authentication, encryption (based on RSA), and integrity.

SSL supporters include Apple, Silicon Graphics, Microsoft and, probably most importantly, the SET consortium, led by MasterCard and Visa.

With Netscape's estimated 70% of the Web browser market, SSL is already an established standard, and will remain as popular a protocol as Netscape Navigator is a browser. Perhaps most critical in SSL's long-term success is its adoption in the SET specification. As SET will become the de facto credit card transaction mechanism, so SSL will become the default transport security protocol for commerce transactions.

M
Microsoft

Microsoft's Internet commerce-related security strategy is codified in its Internet Security Framework (ISF), unveiled in June 1996 and based on existing and new security technology. Unlike most of Microsoft's products, ISF is a cross-platform suite, running on Windows, UNIX, and Apple Macintosh.

ISF contains a number of technologies for implementing Internet commerce-related security, including authentication, encryption, and certificate services. At its heart is a set of APIs (called CryptoAPIs) that enable software developers to include encryption, hashing, and digital signatures in their applications.

N
IBM

IBM has developed a secure packaging mechanism for distributing goods over the Internet that contains the security required not only to protect the transaction, but also to manage the distribution and protection of property rights of products.

The system, Cryptolopes (cryptographic envelopes), is analogous to the shrink-wrapping on a product package. It allows the customer to view an abstract of the product and the licensing details, but not to get access to the product itself until it is paid for. Cyrptolopes are being developed alongside IBM's line of traditional security products such as firewalls, LAN security, and antivirus software, known as SecureWay.

A helper application must be installed on a user's machine, linked in to his or her Web client. This helper manages access rights for any downloaded Cryptolope file—it lets the user view the product abstract and licensing details. It also manages the payment transaction. After getting confirmation from the user that he or she wants to pay for the product, it issues a request to a clearing center for permission checking and to obtain the key required to unlock the product contained within the Cryptolope package. The Cryptolope security system incorporates encryption, authentication, and integrity.

O
Nortel Entrust

Nortel (Northern Telecom) develops and markets the Entrust line of public key encryption products. Entrust is a fairly standard mixed public/private key encryption mechanism (messages are encrypted in DES and keys in RSA), but its major feature is its large-scale key management architecture. Nortel has designed Entrust to provide an integrated encryption and management system for, it claims, environments of thousands of users.

As Entrust is an integrated environment, it is aimed at business-to-business (notably business-to-partner) commerce applications, due to the need to install Entrust software on both sender and recipient terminals. For consumer commerce, this is not a practical requirement. The key management system is based on an X.500 directory, and so is as scalable as an enterprise's current X.500 environment.

Companies using Entrust in their applications include Symantec, Hewlett-Packard, Tradewave, and Harbinger.

P
SET

The SET (Secure Electronic Transactions) consortium is the major force in developing an industry-wide standard for secure Internet credit card transactions. SET is a consolidation of two previously competing alliances: Netscape/MasterCard and Microsoft/Visa.

SET is led primarily by MasterCard and Visa; members include Netscape, Microsoft, IBM, GTE, Terisa, and American Express.

SET's stated aims are to provide:

- Confidentiality of order and payment information
- Integrity of all transaction data
- Authentication of the cardholder as a legitimate holder of a credit card account

- Authentication of the merchant as a legitimate partner of credit card institutions

- Openness of the protocol to ensure interoperability with all transport security mechanisms and all relevant software

(Blank)