Mastering Security on the Internet for Competitive Advantage

White paper

Sun microsystems

Mastering Security on the Internet for Competitive Advantage

August, 1997

Sun
microsystems

901 San Antonio Road, Palo Alto, California 94303 U.S.A.

This publication is provided “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

Changes are periodically added to the information herein; these changes will be incorporated in new editions of the publication. Sun Microsystems, Inc. may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time.

Table of Contents

1. **Introduction 1**

Network Security Architecture 2

Security Policy 3

Evaluating Risk 5

Implementing a Strategy. 6

2. **Network Security Technologies 9**

Encryption Techniques 9

Security Solutions 14

Access Control Solutions. 19

Java™ Platform Security 22

Solaris™ Security 22

International Issues 23

3. **Secure Payment Solutions. 25**

Merchant Servers 25

Java Electronic Commerce Framework — JECF. 29

4. Emerging Security Trends **31**

Elliptic Curve Cryptography 31

Smart Cards 32

Digital Rights Management 33

5. Summary **35**

A. Glossary **37**

B. References **39**

Introduction 1

Computer and network security are challenging topics among executives and managers of computer corporations. Even discussing security policies may seem to create a potential liability. As a result, enterprise management teams are often not fully aware of the many advances and innovations in Internet and intranet security technology. Without this knowledge, many corporations are not able to take full advantage of the benefits and capabilities of the network.

Together, network security and a well-implemented security policy can provide a highly secure solution. Employees can then confidently use secure data transmission channels and reduce or eliminate less secure methods, such as photo-copying proprietary information, sending purchase orders and other sensitive financial information by fax, and placing orders by phone.

The purpose of this white paper is to demystify intranet and Internet security. It will describe how easily and effectively a secure solution can be implemented by providing examples of how products from Sun Microsystems™ and its partners are being used for these applications.

Throughout this paper, we will use terms such as access control, encryption, firewalls, and SET. For those not familiar with some of these terms, a short glossary is provided at the end of this document. Another valuable resource is a list of security software providers, their phone numbers, and World Wide Web addresses, provided in Appendix B.

Network Security Architecture

At a basic level, threats to network security can be classified into three general areas:

- Unauthorized access to information
- Unauthorized modification of information
- Unauthorized denial of service

The term unauthorized implies that the release, modification, or denial take place contrary to some security policy. To combat these threats Sun Microsystems has defined a network security architecture. This architecture consists of the following components.

- *Access Control*

  Access control mechanisms ensure that information is controlled and access is granted by predetermined security policy. There are numerous approaches to achieving access control. These range from simple password protection to token-based mechanisms to more advanced biometric encryption technologies.

- *Privacy*

  The goal of privacy is to ensure that unauthorized people on the network cannot see the contents of the message being sent. Privacy is synonymous with confidentiality and secrecy.

- *Authentication*

  The purpose of authentication is to enable principals to communicate in confidence, knowing that the communication originates with one principal and is destined for the other. Principals can be people, machines, organizations, and network resources such as printers, databases, and file systems. All authentication schemes ultimately reduce to enabling each principal to obtain or possess some information that uniquely identifies the other.

- *Integrity*

  Data integrity addresses the unauthorized alteration or destruction of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

- *Management & Audit*

  Constant administration is essential to ensure the continued success of a network security system. This is achieved through maintaining detailed records and audit trail information. Audit also helps in subsequent reviews of security related events.

Advanced security solutions that meet all of the aforementioned requirements are available from Sun Microsystems and its partner independent software vendors (ISVs). Designed for the SPARC™/Solaris™ platform, these products enable enterprises to deploy applications that are both secure and scalable.

Security Policy

A underlying premise of Sun's network security architecture is the existence of a corporate security policy. Any implementation of a network security architecture must be consistent with an established security policy. The first step in defining a corporate security policy is to draft a high-level management policy statement to establish a framework and context for security within the organization. This policy needs to define the adequate and appropriate security measures necessary to safeguard a company's systems, networks, transactions, and data.

The next step is to start a systematic analysis of the assets of the organization, determining the value of information, or the possible damage should it be disclosed, along with possible risks. This step is no more difficult than the risk management that a corporation exercises every day. Most businesses already have established what information is valuable, as shown in the security hierarchy in figure 1-1. Most have also determined who should have access to it, and who has responsibility for protecting it.

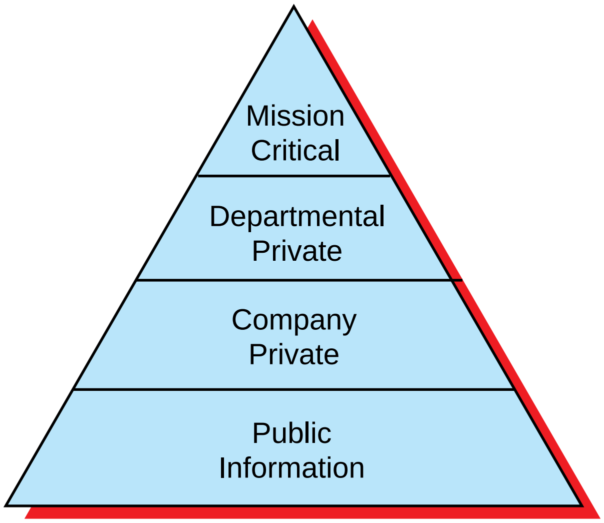


Figure 1-1 Security hierarchy

Information such as trade secrets, vault and authorization codes, and lock and key information are clearly *mission critical*. The disclosure of these security items could cause severe loss to a business or operation. Physical security is just as critical; restricting the use of modems and removable media, and controlling access to devices are all methods of securing the organization against theft and damage.

Departmental private information is typically data that is private to a particular department, such as payroll information in finance and medical records in personnel. There may be legal requirements for securing this information.

Company private information varies from company to company, but typically consists of information that should only be disclosed to employees and partners of a company, such as policy and procedure manuals. Of course, it's possible to get a bit carried away with what information is considered to be private (figure 1-2).

IT GIVES OUT YOUR NAME AND YOUR ADDRESS AND YOUR PHONE NUMBER!!! NOBODY'S SAFE!! WE'RE ALL NAKED!!
NEW WEB SERVICE?
NEW PHONE BOOK.

Figure 1-2 Cartoon courtesy John Klossner, © 1996, amy@airs.com

Public information is information such as product literature, brochures, and catalogs that needs to be freely available to anyone, but whose integrity needs to be assured to prevent unauthorized alteration. This information is often provided to customers and interested parties by means of Web servers and the Internet.

Evaluating Risk

Evaluating risk is a critical step in choosing a security solution. Perceptions often differ substantially from actual risks.

> *"The perception of risk is much higher than the actual risk. When someone calls up by phone, we are not afraid that they are impersonating a customer."*
>
> *Paul Moorhead, British Telecom*

Often the primary risk is found to be internal. For example, system administrators often have access to sensitive information otherwise limited to executives. A remote dial-in line set up for debugging could be used to gain general access to internal systems, bypassing other security safeguards. The organization should identify and evaluate all such risks, and assess the value of all assets.

Implementing a Strategy

Having evaluated the value of assets and determined potential risks, the organization can implement a strategy for protecting its assets. The objective is to make it more expensive to illegally obtain assets than they are worth, while spending the minimum amount required to protect them. This requires careful examination of all options, including a well-defined internal security policy. To quote Paul Moorhead once again:

> *"Operating processes are just as important as the software used to implement security."*

Implementing a security policy has its price. The more security desired, the greater the cost. And it is important to ensure that the added security does not unduly reduce network performance or employee productivity, increasing the likelihood that employees will bypass security measures to meet their productivity goals.

In summary, establishing a corporate security policy involves:

- Developing a high-level management policy statement
- Systematically analyzing the organization's assets
- Examining risks
- Developing an implementation strategy

Sun Microsystems, through its professional services organization, has many programs in-place to offer consulting services to guide an organization through the different phases of setting a security policy and deploying solutions consistent with that policy. Packaged solutions are also available for quick deployment of security services using proven methodologies and established training materials.

Sun Educational Services^{SM} provides complete training solutions to help ensure that customers have the necessary skills to implement and manage their network security strategy. Sun's educational consultants can work with customers to perform a security skills assessment to identify any skill gaps within the organization. This information provides the basis for developing a customized education plan that provides the training needed to help ensure that valuable data and networked systems are protected.

The rest of this paper outlines some of the technology and solutions available on SPARC/Solaris platforms. These solutions range from encryption and virtual private networks to secure payment systems for electronic commerce. This paper concludes with insights into some emerging trends in the security arena.

Network Security Technologies 2

Once a security policy has been established, the next step is to implement the policy using industry strength security products. Most network security products use some level of encryption to achieve the goals defined in the network security architecture.

This chapter gives an overview of encryption and introduces both Sun™ and third party solutions available to implement a security policy. Of particular interest is Solstice™ SunScreen™, which provides advanced enterprise level network security using virtual private networks.

We also introduce Java™ as a platform for building secure applications for deployment on interconnected networks. With many built-in features, the Java platform enables robust, secure, scalable, and easy deployment of enterprise class applications on intranets and the Internet.

Encryption Techniques

> *"Anyone can use encryption. Unfortunately, it's also true that anyone can use encryption badly.... But if you are using bad encryption or if you are using good encryption badly, you might be lulled into a false sense of security while your confidential information remains available to others."*
>
> *Simson Garfinkel,*
> *PGP: Pretty Good Privacy, January 1995*

Encryption is the transformation of data into a form unreadable by anyone without a decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data. For example, one may wish to encrypt files on a hard disk to prevent an intruder from reading them. In a multi-user setting, encryption allows secure communication over an insecure channel.

There are two principle methods of encryption, *private key* and *public key* encryption.

Private Key

With private key encryption, the sender uses a secret key to encrypt the message, and the receiver uses the same secret key to decrypt the message. This method is also known as *secret-key cryptography*. The main problem is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, or a phone system, or some other transmission system to not disclose the secret key. Anyone who overhears or intercepts the key in transit can later read all messages encrypted using that key. The generation, transmission, and storage of keys is called key management — an issue all cryptosystems must deal with. Secret-key cryptography often has difficulty providing secure key management.

Public Key

In this system, each person gets a pair of keys, called the public key and the private key. Each person's public key is published while the private key is kept secret. The need for sender and receiver to share secret information is eliminated — all communications involve only public keys, and no private key is ever transmitted or shared. No longer is it necessary to trust some communications channel to be secure against eavesdropping or betrayal. Anyone can send a confidential message just using public information, but it can only be decrypted with a private key that is in the sole possession of the intended recipient. Furthermore, public-key cryptography can be used for authentication (digital signatures) as well as for privacy (encryption).

The Diffie-Hellman Scheme

The *Diffie-Hellman* scheme, shown in figure 2-1, is a way to achieve secure, two-way communication across the Internet without exchanging keys. Each party obtains the public key for the other from a certificate authority, and performs a special calculation with their own private keys. The result of the algorithm will be the same for both parties, and may be used as the new secret shared key for secure communications between them.

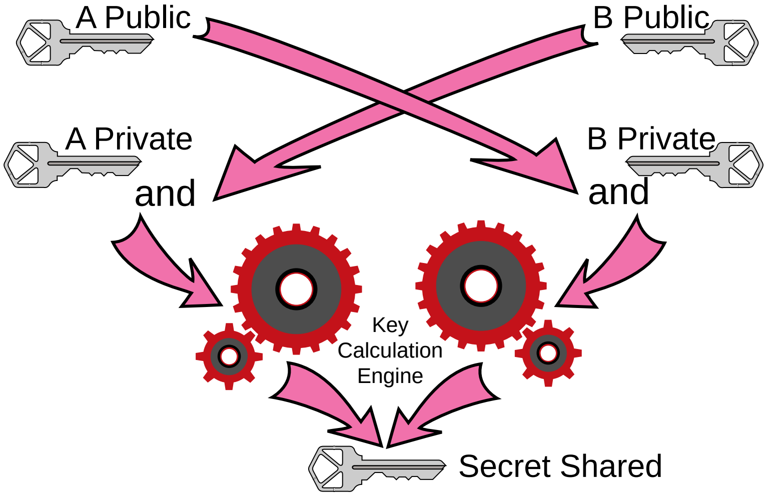


Figure 2-1 Diffie-Hellman calculation

Pretty Good Privacy — PGP

Pretty Good Privacy (PGP) is a program for protecting the privacy of email and computer files. It runs on virtually every UNIX® system, as well as on the Amiga and on PCs running DOS, Windows, OS/2, and MacOS. PGP provides the means for encrypting files and email, creating public and private keys, maintaining a database of public keys, adding digital signatures to documents, and certifying keys and obtaining keys from key servers.

In May 1994, a version of PGP was released that includes a license from RSA Data Security. This allows the legal, non-commercial distribution of PGP. Commercial versions of PGP are distributed by ViaCrypt.

SunScreen™ SKIP

SunScreen SKIP enables secure business over Internet and intranet by encryption of data and authentication of the IP traffic stream. SunScreen SKIP provides encryption and key management capabilities to the desktop and remote users, enabling secure authenticated communication in a heterogeneous networked environment. SunScreen SKIP is available as an easy-to-install software module and provides security without modification of existing applications.

SunScreen SKIP is based on SKIP (Secure Key-management for Internet Protocols), an emerging IETF standard and an ANSI standard for IP encryption key management. SunScreen is available in different versions for domestic and global use and uses Diffie-Hellman keys.

Certificate Authorities

To use public key encryption across the Internet, steps must be taken to ensure the integrity of the public key and the identity of its owner. A trusted third party, called a *certificate authority*, provides a unique *digital signature* for the public key, which cannot be forged. It identifies the owner of the key and certifies that the key has not been altered.

VeriSign

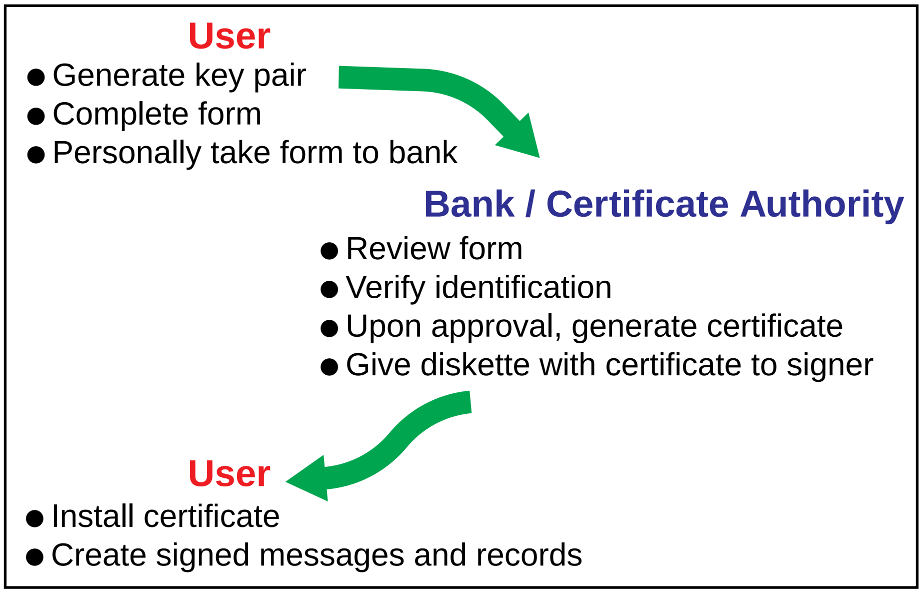
VeriSign is a commercial certification authority that issues digital certificates verifying the identity of an individual. A VeriSign digital certificate contains the following information:

- The owner's public key
- The owner's name
- The expiration date of the public key
- The name of the issuer (Verisign)
- The serial number of the certificate
- Verisign's digital signature

Additional information may also be present, depending on the type of certificate. VeriSign has facilities in California and Japan that issue digital certificates. These facilities provide the digital identification for specific individuals and maintain lists of revoked digital certificates.

VeriSign provides two types of digital certificates: personal certificates to verify the identity of an individual, and secure server certificates to protect communications with a given server and to allow verification of the server identity. Its Class 1 personal certificates provide a unique name and email address within its repository. A Class 2 personal certificate requires confirmation of name, mailing address, and other personal information by an Equifax consumer database. It also includes a physical mail-back process to insure that the request was not generated by someone with access to an applicant's personal information.

In the future, it is expected that there will be many certificate authorities available, ranging from banks to firms such as Pitney-Bowes. The process of obtaining a certificate will be similar to that shown in Figure 2-3.



User

- Generate key pair
- Complete form
- Personally take form to bank

Bank / Certificate Authority

- Review form
- Verify identification
- Upon approval, generate certificate
- Give diskette with certificate to signer

User

- Install certificate
- Create signed messages and records

Figure 2-2 The certification process recommended by RSA

Security Solutions

There are a number of network security solutions available today. In this paper we will discuss two types: *firewalls* and *secure virtual private networks*.

Firewalls

Firewalls are a basic means for providing network security, behaving like a moat around a medieval castle. Firewalls restrict information entering and leaving at carefully controlled points, and prevent unacceptable attempts at accessing resources within the firewall. While an important use of firewalls is to enable secure Internet access to corporate networks, they are also used to restrict access to departmental private and mission critical information.

A popular firewall product is Solstice™ FireWall-1™, licensed by Sun from CheckPoint Software Technologies. Widely used on Solaris systems, FireWall-1 examines each connection as it attempts to pass through its firewall. It uses multiple rules to define the many applications, services, and users allowed access to each specific internal server. This service is ideal for securing and compartmentalizing intranets.

Case Study — San Diego State University

San Diego State University provides campus access to the Internet via a T1 communications line. The configuration includes a Sun Ultra™ 1 workstation with 256 MB memory running FireWall-1. Currently the University has over 9,000 nodes on campus, hundreds of web servers and three news servers (Figure 2-3).

Security rules specify that connections from a particular source are allowed to connect to specific destinations for obtaining specific services, whether or not subsequent activity should be logged, and whether this rule applies to outbound traffic as well. For example, the Chemistry Department could allow only Web and FTP (file transfer protocol) access to a particular departmental server for connections originating over the Internet.

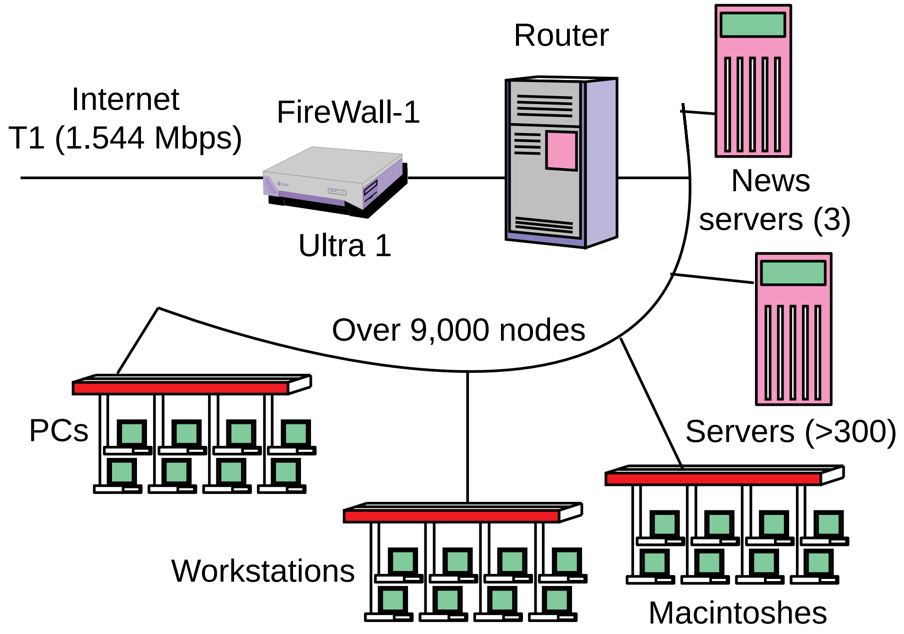


Figure 2-3 San Diego State University configuration

A 30-day log is kept of all denied and accepted requests. This enables the network systems manager to monitor which services are having high rates of denials, to detect security problems, or to advise people that a server is being changed.

SunScreen EFS

SunScreen EFS from Sun Microsystems provides advanced firewall technology and addresses the requirements of commercial organizations looking to secure their communication over public networks or corporate networks and intranets. SunScreen EFS enables authentication and private connections between mobile, remote, or dial-in users and the corporate network. SunScreen EFS allows administrators and managers to extend security to every single server on the network.

Customers can use SunScreen EFS to setup secure communication between tens of thousands of remote users or sites using SKIP. SunScreen EFS has also been optimized for maximum performance as a SKIP encryption server. In addition, it supports easy-to-set-up security policy definitions for groups.

SunScreen EFS uses dynamic packet screening technology and provides security at any point where there is access to a network. Also, it can be used to protect all the servers on the intranet, and the large number of branch offices that need secure communication with those sites.

Secure Virtual Private Networks

Many corporate networks used for Electronic Data Interchange (EDI) and funds transfer have been implemented using either private networks or costly services from specialized telecommunications network providers. Corporations can significantly reduce internal corporate networking costs[1] by using secure, encrypted, IP-level network communications over less expensive public networks called secure virtual private networks (SVPNs). Implementing SVPNs demands authentication of the sources of all data, privacy from competitors and intruders, and assurance of the integrity of all data to minimize the possibility of fraud.

SunScreen SPF-200

One product that can be used to implement SVPNs is SunScreen SPF-200. SunScreen SPF-200 is a platform for creating a perimeter defense to provide secure business operations over the Internet. To assure a high level of security, SunScreen SPF uses stealth design to guard against attack and SKIP encryption to protect data on the network.

SunScreen SPF-200 is a dedicated hardware and software solution with a stealth design making it more secure because intruders cannot address the machine. The platform running SunScreen SPF-200 does not allow other applications to run on the system thus reducing exposure to security breaches.

[1] A comprehensive analysis of these costs are contained in the report by U.S. Computer, P.O. Box 3150, Saratoga, CA 95070-1150, sales@usc.com, “Internet-Based Secure Virtual Private Networks: The Cost of Ownership,” 1996.

Other features of SunScreen SPF 200 include advanced dynamic packet filtering, network address translation (NAT), and secure remote administration.

Case Study — Federal Home Bank of Dallas

The Federal Home Bank of Dallas provides financial services to support the mortgage lending activities of commercial banks, savings and loans, credit unions, and insurance companies. Most of the bank's applications are implemented as client-server applications, mostly running on UNIX-based servers and a few Tandem non-stop systems. Currently the bank is deploying a virtual private network, allowing its clients to securely access its services over the Internet using web browsers. The bank plans to have 200 customers using the system by the end of 1997, and 600 to 700 customers when the system is fully deployed. The proposed configuration is shown in Figure 2-4.

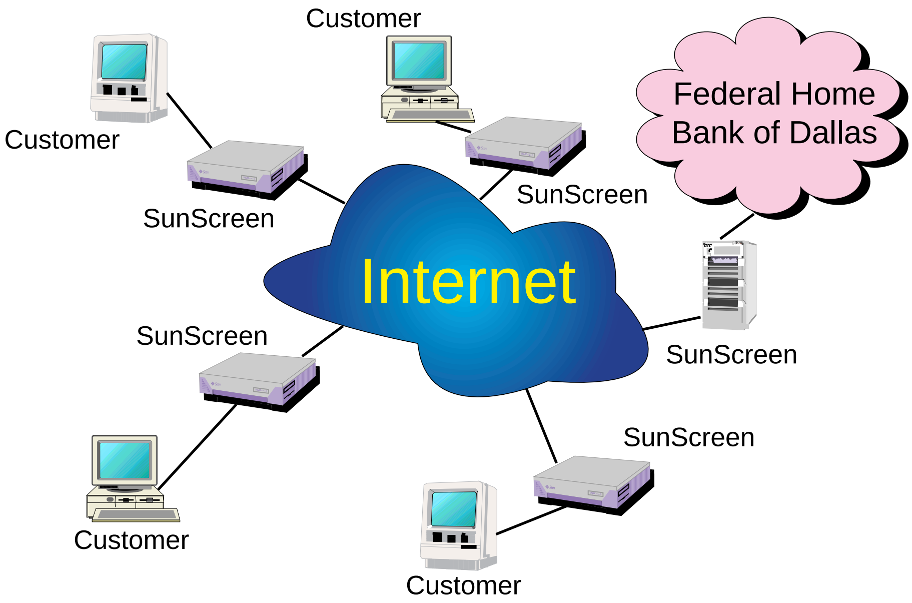


Figure 2-4 Federal Home Bank of Dallas

In defining its security policy, the bank identified distinct internal and external requirements. Responsibility for overall security mechanisms was centralized within its information technology group, but responsibility for granting permissions to individuals for specific datasets was given to the departments which generated and maintained the data.

A particular concern for the bank has been to protect its own private data. This includes transaction information on loans outstanding, wire transfers, and secure safe keeping of bonds and capital stocks. The bank has established a number of rules regarding authentication and encryption to minimize the possibility of anyone eavesdropping or subverting a user session.

> *"SunScreen was the answer to our prayers, in its providing both encryption and firewall capabilities. It lets us control who has access to our systems, what traffic is allowed, and what are permissible IP addresses."*
>
> *Laurie Elvie, Federal Home Bank of Dallas*

Another measure taken by the bank was the use of firewalls from other vendors in addition to SunScreen (figure 2-5). The bank is being very cautious in interconnecting its internal systems to the Internet, and avoids mentioning the vendors it uses to avoid inadvertently compromising the Bank's security. Despite the use of multiple firewalls, the bank is obtaining excellent network response times.

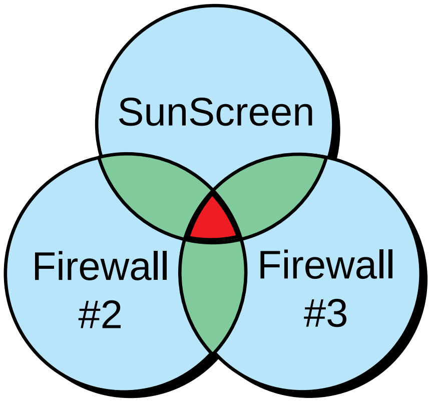


Figure 2-5 Increased protection via multiple firewalls

Access Control Solutions

One aspect of implementing a security policy is being able to control which users have access to particular systems, and the data that they can access. There are a variety of security products available today for regulating access and securing information through encryption.

Sun Security Manager™

This new access control product is part of the overall Sun's security strategy. Sun Security Manager™ augments the SunScreen product line by protecting domains behind the firewall. This enhanced security-strategy is especially important to corporations with sensitive data issues and who are concerned with both Internet and internal security breeches.

Sun Security Manager provides advanced access control for clients, servers, and applications by augmenting standard Solaris access controls. It also has features for extensive logging to monitor accesses, changes made to secure databases, super user accesses, etc.

Token Based Systems

Within a company, card keys and security personnel can insure that only employees are accessing its systems. But for remote users, there is a much higher perceived security risk. Passwords can be stolen and security can be breached by "hackers." Many companies provide each of their remote users with a digital token card, or "hard token," to verify the identity of these users.

Engima Logic's SafeWord DES cards (figure 2-6) are hard tokens that generate single-use passwords without requiring synchronization with a host. SafeWord DES cards are able to generate over a million unique six- to eight-digit passwords. To log on, the user presses the ON button and a new password is displayed. The user then types the password shown on the display in response to the system prompt. The system decrypts the password using a DES key and verifies it. Each password can only be used once, which prevents replay attacks.

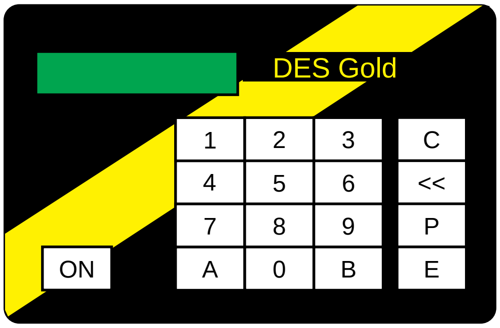


Figure 2-6 SafeWord DES Gold Card

Case Study — American Express

American Express has been using Enigma Logic hard token security technology products for over ten years. Originally the tokens provided secure remote access to the corporate mainframes. Today the tokens are used for secure remote access to the company's global network of client-server systems through dial-up lines. American Express has over 10,000 nodes connected to a wide variety of workstations, servers, minicomputers and mainframes (figure 2-7). Currently, hard tokens are only used by remote users, but they are expected to be available to desktop and Web-based users in the future.

> *"Being in the financial business, we are controlled by banking regulations. We won't and can't compromise on security. We are always wanting to improve and obtain better security. All it takes is one loss to offset the price of putting in the necessary security to prevent that loss."*
>
> *George Bateman,*
> *Director of Technology, American Express*

American Express's security policy has been to centralize its security database, since it believes that a dispersed security architecture is difficult to administer. The primary exception to this policy is that access must be provided for local maintenance personnel. A consistent security policy for all divisions and subsidiaries is established by a central information security group.

"It is just as important to provide information on who penetrated our security, and what they did, as it is to provide measures to prevent penetration. While we want to know who attempted to penetrate our security, we need to be able to backtrack as well."

George Bateman
Directory of Technology, American Express

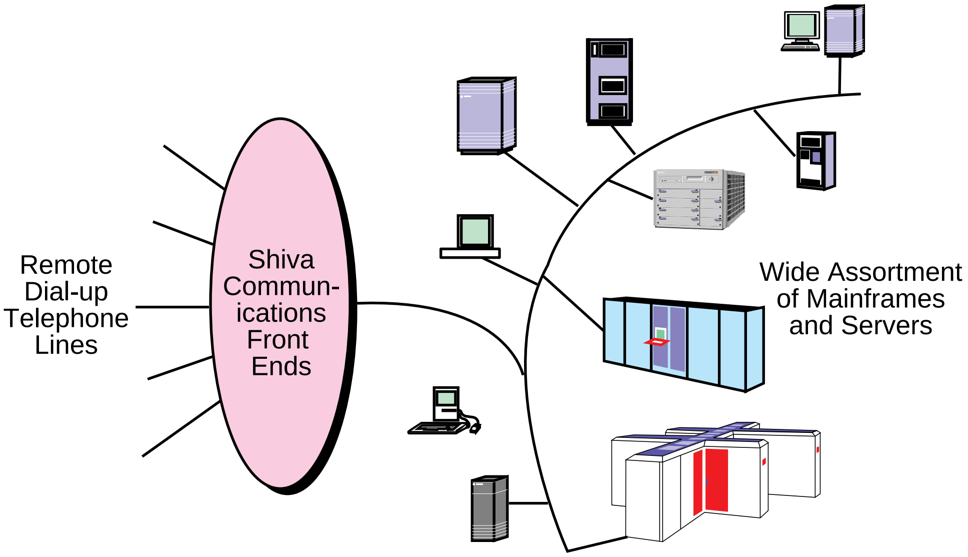


Figure 2-7 American Express remote user configuration

At American Express, work is being performed to develop profiles of each user to enable the company to flag any activity that is out of the ordinary. Additionally, by collecting all possible information, including user and caller IDs, a much greater assurance of correct identity can be obtained.

American Express customers are allowed direct access to their accounts via ExpressNet on AOL (American On Line) using a user ID and password. Customers can pay bills online using a bank account of choice. Customers can also use a Web browser for online investing and for purchasing airline tickets.

Java Platform Security

The Java language enables small applications, called applets, to be downloaded to user systems. The user can execute downloaded applets either directly or through a browser such as Microsoft Explorer or Netscape™ Navigator™. Since the Java language has been implemented on a large and growing number of platforms, tremendous portability is achieved by writing applications in Java. While the ability to download Java applets offers tremendous capabilities, these characteristics at first sight might appear to make client systems vulnerable to viruses and tampering.

It was for these and other concerns that Sun designed Java with security and robustness as major design goals. The first step taken was to simplify the Java language, eliminating dangerous aspects such as pointer arithmetic that are common to other languages. The design team also added mechanisms to minimize outside manipulation of internal objects. Another area of concern was the potential vulnerability incurred in patching applets. To eliminate this weakness, the software that loads applets first checks each applet to verify that it conforms to the runtime rules of the Java language specification.

Another mechanism Java offers is its security manager. The security manager distinguishes between applets known to be safe or trusted, and those which were downloaded and are not known to be safe. Untrusted applets are not allowed to read or write files or start-up new applets. Also, users can add a digital signature to applets. This makes it possible to download trusted applets with the assurance that the applet was created by a specific author, and that it has not been modified by anyone else.

Solaris Security

Solaris security features enhance the robustness and security of Solaris systems used in demanding technical and commercial applications. Solaris has a number of built in security products such as SVID compliant access control enhancement, ASET automated audit tool, ARM account protection, and ONC+ federated security authentication technologies. In addition, Solaris incorporates the Basic Security Model (BSM), bringing into compliance with C2-level specifications. These features provide the following benefits:

- Security mechanisms that extend over the network
- Automated system security checking
- Tailorable client and server authentication schemes

Trusted Solaris™

The operating system of choice for high-level security requirements provides enhanced security to meet and exceed B1-level specifications. Configurable to fit in a wide variety of customer security policies, Trusted Solaris™ implements strong, role-based control of both user and system administrator actions. Data and system resources are fully protected by a multilevel file system, preventing unauthorized access by either internal or external threats.

International Issues

In the past, the United States has regarded products incorporating encryption as munitions, and has required permits from the Department of State for their export. In October 1996, the Department of Commerce was given jurisdiction for encryption products. Products with up to 56-bit key-length encryption may be exported for two-years, beginning in 1997, after which key recovery technologies must be provided.

Secure Payment Solutions 3

A rapidly growing number of companies are taking advantage of the World Wide Web (WWW) as a distribution channel. As technologies emerge for secure payment over the Web, the demand for such services will increase. This chapter describes merchant servers and other secure payment solutions.

Merchant Servers

Some firms are selling a sizable portion of their products through Internet merchant servers. Merchant servers typically provide a variety of electronic commerce services such as search engines, generation of product pages from catalog databases, sales analysis, automated shipping, and sales tax calculation. With respect to security, merchant servers have three functions:

- Enabling customers to securely order merchandise and services and specify payment method
- Offering secure payment processing methods, typically via EDI, to banks and financial institutions
- Restricting, controlling and monitoring access to the merchant server

Secure Sockets Layer — SSL

There are many companies offering merchant servers for electronic commerce applications. One of the most widely installed products is the Netscape Merchant System™. The Netscape Merchant System uses a protocol called SSL

(Secure Sockets Layer). SSL allows private information, such as credit cards and purchase orders, to remain private when traveling across intranets and the public Internet. SSL supports:

- *Authentication* to verify that a client is communicating with an intended server
- *Encryption* to help prevent data from being understood by an unintended party, and to insure that data was not altered in transit

Netscape browsers offer integrated support for SSL. All of its browsers support at least a 40-bit RC4 stream encryption algorithm designed by RSA Data Security[1]. Netscape servers support SSL-based certificates, allowing any SSL-compatible client to verify identity.

Case Study — CDworld

CDworld is a family-owned, online discount-music retailer, which began its electronic commerce operations in March 1995. As of October 1996, the retailer offered 172,000 products, including 100,000 compact disks and 45,000 cassettes, as well as a variety of laser disks and video games. It is in the process of adding another 35,000 products to its online catalog.

CDworld uses a merchant server consisting of a Sun SPARCserver™ 1000 with four CPUs, 256 MB of RAM, and an eight gigabyte disk array. It runs both Netscape Commerce Server and Secure Server, in conjunction with a Sybase DBMS. Connected to a T1 communications line, this system (illustrated in figure 3-1) supports over 200,000 hits each day.

CDworld addressed two fundamental security concerns: customer security and internal security. The company employed Netscape SSL for customer security, using a 40-bit RC4 encryption algorithm, to make the service available internationally.

[1] RSA is now a subsidiary of Security Dynamics.

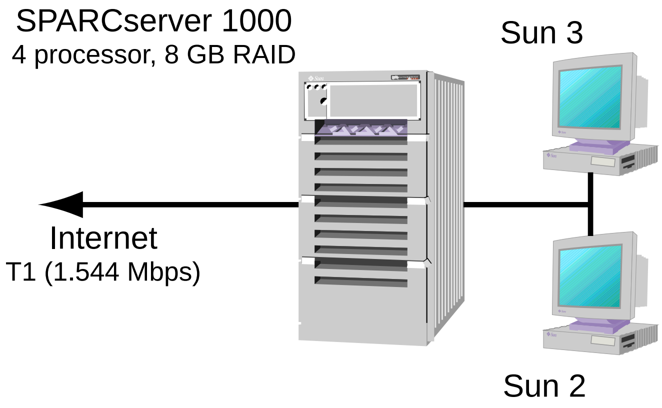


Figure 3-1 CDworld configuration

> *"We've seen a shift in fear levels. Initially, users were very timid, and we had to provide them with the means to fax us the actual order with their credit card information. With the introduction of Cybercash, the fear level has decreased dramatically. Today, 95 percent of all of our orders are done electronically, the remaining 5 percent are a combination of fax and phone orders.*
>
> *"Our basic internal security philosophy is to restrict the people who can access our systems to as small a number as possible."*
>
> *Bruce Pettyjohn, President,*
> *CDworld, October 1996*

The first step in providing internal security at CDworld was to purchase firewall software from Livingston. This software uses one IP address outside the firewall, and a second IP address inside the firewall. The usernames and passwords required by Netscape, Sun, and Sybase software provide additional security.

Mastercard/Visa SET

Mastercard/Visa's SET protocol is another data security protocol available today. The advantage of SET is that only the card holder and acquiring bank are able to see the actual credit card number. The merchant never sees the number, ensuring a high degree of security for credit card transactions.

The Java Electronic Commerce Framework, explained later in this chapter, has mechanisms to support SET as part of the framework. The Java Wallet™ product from Sun Microsystems supports SET at the client level.

CyberCash Wallet

There are a number of other companies providing mechanisms that enable secure payment to occur over the Internet. One such company is CyberCash. The CyberCash Wallet allows merchants to accept a range of payment options. It also verifies the customer's identity, and verifies that they possess a valid credit card or Cybercash digital coin belonging to them.

The CyberCash payment authorization process is illustrated in figure 3-2.

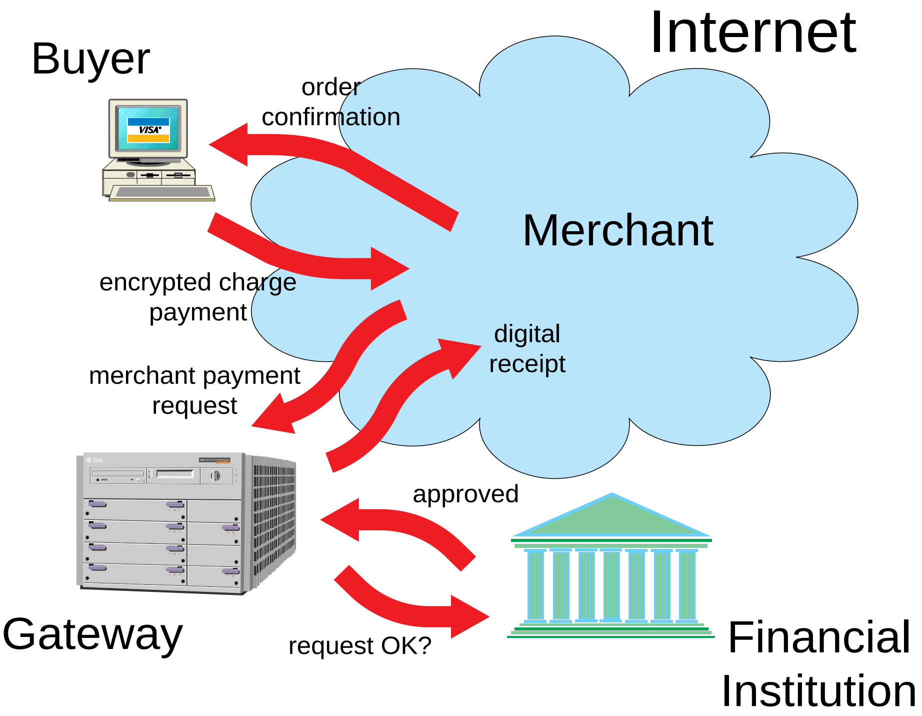


Figure 3-2 CyberCash payment authorization process

When a customer selects a CyberCash Pay button on a Web page, their Wallet automatically opens, allowing a payment instrument to be selected. An encrypted charge payment message is sent to the merchant server for merchant identification. The message is then forwarded to a CyberCash gateway server which decrypts the message, authenticating the transaction and the validity of the merchant. If valid, the gateway server sends a message to the appropriate financial institution over a secure, private network, requesting charge approval. Once the charge is approved, the merchant receives a digital receipt and the customer receives confirmation of their order.

First Virtual VirtualPIN

Another example of a secure payment service is offered by First Virtual Holdings. Formed in early 1994, First Virtual has been offering an Internet payment service since October of that year. With First Virtual's system, non-sensitive information travels over the Internet, and secure information such as credit card information is obtained either by telephone call or mail. When making a purchase, the buyer provides a VirtualPIN (personal identification number) and an email is sent to the buyer asking for a confirmation of the purchase. This process eliminates the need for encryption and allows any Internet user to immediately make use of this payment service.

Java Electronic Commerce Framework — JECF

The Java Electronic Commerce Framework (JECF) is part of the overall *Java Commerce Project*. The goal of the Java Commerce Project is to create an integrated solution that:

- Makes purchasing a seamless part of browsing the Internet
- Allows applets to charge for execution and content delivery
- Creates an open platform for purchasing, banking, and finance

This client and server platform are common services (application programmer interfaces) on top of Java for creating payment and financial applications. The first phase of the project is JECF, which provides:

- A common graphical user interface
- A secure encrypted database
- A mechanism to provide fine-grained access control
- Access to strong cryptography
- Applets and infrastructure for purchasing

JECF Terminology

To better understand the JECF, it is useful to define some of the terms used in the JECF model of Electronic Commerce Architecture, JavaSoft's architecture to support electronic business transactions. The consumer uses a Java-enabled browser to navigate an online merchant's site and select goods or services for purchase. In doing so, they will encounter some common concepts:

- A *wallet* is a graphical user interface that the consumer uses for business transactions.
- The *merchant* offers goods or services for sale on the World Wide Web using Java applets. These applets reference reusable code modules.
- A *shopping cart* is a program that keeps track of the items a consumer intends to purchase. A shopping cart may run as a Java applet on the consumer's machine or as a process on the merchant's server.
- A *cassette* is a Java package that can be separately distributed and installed on a consumer's machine. Cassettes are distributed in cassette distribution files, which are digitally signed by cassette providers, such as banks, merchants, etc. A cassette's digital signature provides it with rights called *capabilities*.
- An *instrument* facilitates an electronic commerce transaction. One example of an instrument is a credit card. Instruments embody such constructs as communication protocols, authentication mechanisms, administrative facilities, with JECF facilitating the development of payment methods and other financial services applications in Java-enabled environments. JECF includes security features that encrypt and store information locally in a client, and control and restrict how information can be used by different applets. JECF also provides mechanisms for local user identification and authentication. Access control lists specify what database objects can be made available to which applets, and which applets can invoke other applets and resources.

These JECF security features enhance data privacy. For example, an applet created by one credit card company could be prevented from obtaining information on user accounts owned by another credit card company. However, applets that require greater access, such as a tax program, can be granted access to a wider range of information. JavaSoft is actively working to promote JECF as a standard for electronic commerce.

Emerging Security Trends 4

In the future, users will see the introduction of a variety of new security tools and technologies. In this chapter three important emerging technologies will be discussed: elliptic curve cryptography, smart cards, and digital rights management.

Elliptic Curve Cryptography

Recent improvements in integer factorization and parallel processing has resulted in a requirement for longer key sizes for most current public-key systems. Unfortunately, longer key sizes make these public-key systems even slower and more cumbersome. Use of Elliptic Curve Cryptography (ECC) allows increases in strength at the same time as decreasing overhead and latency.

ECC is a new cryptographic system that uses the algebraic system defined on the points of an elliptic curve to provide public-key algorithms. These algorithms can be used to:

- Create digital signatures
- Provide secure distribution of secret keys
- Provide a secure means for the transmission of confidential information

Applications such as financial transfers or wireless data transmissions requiring intensive use of signing, authentication, high speed, and limited bandwidth will benefit from the advantages offered by elliptic curve implementations.

Indeed, ECC will be valuable in a variety of circumstances:

- Where computational power is limited (smart cards, wireless devices, and PC cards)
- Where space is limited (smart cards, wireless devices, PC Cards)
- Where high speed is required
- Where intensive use of signing, verifying, or authenticating is required
- Where signed messages are required to be stored or transmitted
- Where bandwidth is limited (wireless communications)

Smart Cards

A smart card is like an electronic safe deposit box. The size of a credit card, a smart card contains a semiconductor chip with logic and non-volatile memory. The software within the card detects attempts at intrusion and tampering and monitors abnormal usage. Billions of smart cards have been made since their introduction in 1977. Smart cards have long been popular in Asia and Europe, and are gaining popularity in the United States. Some of the many applications of smart cards include:

- *Stored value card.* This type of smart card minimizes the need to carry cash. It can be used in stores, vending machines and pay phones.
- *Health care.* Health care smart cards provide a portable, customized health care file with medical emergency data, HMO and insurance information.
- *Access control in offices and hotels.* These smart cards can store information such as the time entered and exited, access conditions and identity.
- *Contactless tickets for ski resorts and airlines.* These smart cards increase the speed, convenience, and security of ticketing, and facilitate baggage checking.

Smart cards can be read using conventional contact readers or interrogated remotely by microwave or infrared signals. They offer superior security and lower life cycle costs than alternatives such as coins, paper money, or magnetic stripe cards. MasterCard Cash, Mondex, Visa Cash, and Wells Fargo P-ATM are examples of smart cards currently being introduced in the United States.

Security in smart cards is typically ensured by a combination of digital signature and public-key technology. There are many different algorithms in use for smart cards, but all act to verify the authenticity of cards and to prevent misuse or fraud. Smart cards incorporate write-once memory that cannot be modified once it has been programmed. This allows each card to contain a unique identification number. Limits are typically placed on the number of erroneous attempts, preventing brute-force access.

Sun Microsystems is actively working with numerous smart card vendors and companies developing applications for these cards to help insure a total, end-to-end smart card solution. As an example, on October 29, 1996, Sun Microsystems announced the Java Card API. This programming tool enables developers to write Java applications that will run on all ISO 7816-4 compliant smart cards.

Digital Rights Management

An emerging area in secure online commerce is the issue of digital rights management. Content distribution and information service companies need to build profitable electronic commerce businesses on the World Wide Web to stay competitive in an increasingly dynamic world. These information brokers want to protect digital content of all kinds, control the conditions under which it is purchased and used, measure the usage, and guarantee payment as this content is passed from hand to hand. Builders of corporate intranets face similar challenges as they seek to protect and track information and software worldwide.

A solution provider in this area is InterTrust Inc. The InterTrust System Developer's Kit addresses many of these issues and provides the foundation for the creation of practical digital content distribution systems and other electronic commerce interactions.

Summary 5

In summary, network security involves setting a corporate security policy. Then with the internet security architecture as a framework reference, customers can deploy Internet security solutions developed by Sun Microsystems and its ISVs. These solutions enable customers to create highly secure risk management environments to match their intranet and Internet needs. In particular, numerous solutions are available for:

- Authenticated Access
- Network Security and Firewall Systems
- Privacy and Encryption
- Secure Messaging and EDI
- Secure Payment Protocols
- Secure Virtual Private Networking (SVPN)
- Trusted Networks

This white paper has touched on a variety of security topics involved with managing risk. There are hundreds of vendors providing security solutions based on Sun Microsystems' products today. We have presented only a handful of these products as an introduction to Internet security solutions.

Glossary A

Access control

Regulating access to your network in a controlled and hierarchical manner.

Authentication

Also known as digital signatures, authentication is the use of cryptographic technology to verify the origin and integrity of a digital message.

Certificate

Certificates are often sent with a message. If the message has been tampered with, it is apparent when the signature contained within the certificate is verified. Certificates typically also contain public key owner information.

DES

Digital Encryption Standard. DES is a private-key cryptosystem, and the official standard of the United States Government.

EDI

Electronic Data Interchange. EDI is a form of electronic messaging used by business and government for purchases, payments, and other transactions.

Encryption

The transformation of data into an unreadable form by anyone without a decryption key.

Firewall

A computer or router, physically located between an external and internal network, which protects the internal network from unwanted intrusion from the outside network.

PGP

Pretty Good Privacy. PGP is a public-key encryption method created by Phil Zimmerman. It is a de-facto industry standard.

Private-key

Encryption and decryption using the same key.

Protocols

Communication specifications defining the make up and/or sequence of data packets to implement a particular function.

Public-key

Encryption and decryption using two different keys.

RSA

Rivet-Shamir-Adleman. RSA is the most widely used public-key cryptosystem.

SET

Secure Electronic Transaction. SET is an industry standard protocol for electronic commerce established by Visa and MasterCard.

SKIP

Simple Key Management for Internet Protocol. SKIP is a system for managing encryption keys by certifying the authenticity of public keys for companies and individuals. It enables efficient transparent encryption of any protocol within the TCP/IP protocol suite.

SSL

Secure Socket Layer. SSL provides an encrypted TCP/IP path between two hosts, and is commonly used by Netscape for Internet transactions. 40-bit keys should not be considered secure; 64-bit keys, however, are considered secure.

Signature

A unique piece of data attached to a document asserting that the named person wrote or otherwise agreed to the document. Also referred to as a digital signature, and included as part of a certificate.

WWW

World Wide Web, or “the Web.” The Web is a consistent means of accessing a variety of media in a simplified fashion across wide area networks (Internet).

References B

Books

The following computer security books are recommended:

Building Internet Firewalls; D. Brent Chapman, Elizabeth D. Zwicky; O'Reilly & Associates, November 1995

> This book provides a complete overview of firewalls, while remaining accessible and practical. The authors are authorities on firewalls.

Firewalls and Internet Security: Repelling the Wily Hacker; Addison-Wesley, June 1994

> This book has an extensive discussion of different types of firewalls, and their strengths and weaknesses. It describes potential attacks and tools used to launch the attacks.

Mecklermedia's Official Internet World Internet Security Handbook; William Stallings

> Stalling is one of the acknowledged experts in the field of Internet security.

Practical Unix & Internet Security; 2nd edition; Simson Garfinkel and Gene Spafford; O'Reilly & Associates, April 1996

> This comprehensive book discusses topics ranging from password vulnerabilities and policies to Unix permissions, dangerous accounts, log files, modems, network security, NFS, security incidents and firewalls. It does not provide extensive coverage on security tools.

Security Software Companies

Many companies specialize in Internet security products. A few are mentioned in the following table:

Company	Type	Telephone	Web Address
Actra	EDI	408-542-3183	www.actracorp.com
Aventail	Firewall	206-777-5600	www.aventail.com
Certicom	Encryption	415-312-7970	www.certicom.com
Checkpoint Software Tech.	Firewall	415-562-0400	www.checkpoint.com
CyberCash	Payment	415-594-0800	www.cybercash.com
Digicash	Payment	415-321-0300	www.digicash.com
Enigma Logic	Access cntl	800-808-1111	www.safeword.com
Entrust	Encrypt., toolkit	613-247-3411	www.entrust.com
First Virtual	Payment	619-793-2700	www.fv.com
GlobeSet	Payments	512-427-5111	www.globeset.com
GTE CyberTrust	Certificates	800-487-8788	www.cybertrust.com
Gradient	Network manage.	508-624-9600	www.gradient.com
Haystack Labs	Virus preven.	512-918-3555	www.haystack.com
InterTrust	Rights mgt.	408-222-4173	www.intertrust.com
Internet Security Systems	Virus preven.	770-395-0150	www.iss.net
Mondex (London)	Payment	171-920-5505	www.mondex.com
Milkyway	Firewall	408-566-0800	www.milkyway.com
nCipher	Crypto. accel.	408-987-6559	www.ncipher.com
Netscape Communications	Payment	415-937-3777	www.netscape.com
OpenMarket	Payment	617-949-7000	www.openmarket.com
Premenos	EDI	800-578-4334	www.premenos.com
Raptor Systems, Inc.	Firewall	617-487-7700	www.raptor.com
Schlumberger	Smart cards	408-487-1890	www.schlumberger.com
Security Dynamics	Encryp., access	800-732-8743	www.securid.com

Company	Type	Telephone	Web Address
Sterling Commerce	EDI	972-868-5000	www.stercomm.com
Trusted Information Systems.	Firewall	301-527-9500	www.tis.com
Verisign	Certificates	415-961-7500	www.verisign.com
Xcert	Certificates	604-640-6210	www.xcert.com

Web Sites

Visit the following web sites to find information on Sun-based security solutions:

www.sun.com/security/

java.sun.com/security/

java.sun.com/commerce/

Sun Microsystems Computer Company
A Sun Microsystems, Inc. Business
901 San Antonio Road
Palo Alto, CA 94303 USA
415 960-1300
FAX 415 969-9131
http://www.sun.com

Sales Offices

Argentina: +54-1-311-0700
Australia: +61-2-9844-5000
Austria: +43-1-60563-0
Belgium: +32-2-716-7911
Brazil: +55-11-524-8988
Canada: +905-477-6745
Chile: +56-2-638-6364
Colombia: +571-622-1717
Commonwealth of Independent States:
+7-095-956-5470
Czech/Slovak Republics:
+42-2-205-102-33
Denmark: +45-44-89-49-89
Estonia: +372-6-308-900
Finland: +358-0-525-561
France: +33-01-30-67-50-00
Germany: +49-89-46008-0
Greece: +30-1-680-6676
Hong Kong: +852-2802-4188
Hungary: +36-1-202-4415
Iceland: +354-563-3010
India: +91-80-559-9595
Ireland: +353-1-8055-666
Israel: +972-9-956-9250
Italy: +39-39-60551
Japan: +81-3-5717-5000
Korea: +822-3469-0114
Latin America/Caribbean:
+1-415-688-9464
Latvia: +371-755-11-33
Lithuania: +370-729-8468
Luxembourg: +352-491-1331
Malaysia: +603-264-9988
Mexico: +52-5-258-6100
Netherlands: +31-33-450-1234
New Zealand: +64-4-499-2344
Norway: +47-2218-5800
People's Republic of China:
Beijing: +86-10-6849-2828
Chengdu: +86-28-678-0121
Guangzhou: +86-20-8777-9913
Shanghai: +86-21-6247-4068
Poland: +48-22-658-4535
Portugal: +351-1-412-7710
Singapore: +65-224-3388
South Africa: +2711-805-4305
Spain: +34-1-596-9900
Sweden: +46-8-623-90-00
Switzerland: +41-1-825-7111
Taiwan: +886-2-514-0567
Thailand: +662-636-1555
Turkey: +90-212-236-3300
United Arab Emirates:
+971-4-366-333
United Kingdom: +44-1-276-20444
United States: +1-800-821-4643
Venezuela: +58-2-286-1044
Worldwide Headquarters:
+1-415-960-1300

Printed in USA

For more information, contact your Sun Microsystems representative:

HEADQUARTERS

SUN MICROSYSTEMS COMPUTER COMPANY, 901 SAN ANTONIO ROAD, PALO ALTO, CA 94303-4900 USA
PHONE: 650 960-1300 FAX: 650 969-9131 INTERNET: www.sun.com

Sun microsystems

THE NETWORK IS THE COMPUTER™

SALES OFFICES

ARGENTINA: +54-1-311-0700 • **AUSTRALIA:** +61-2-9844-5000 • **AUSTRIA:** +43-1-60563-0 • **BELGIUM:** +32-2-716-7911 • **BRAZIL:** +55-11-524-8988 • **CANADA:** +905-477-6745 • **CHILE:** +56-2-638-6364 • **COLOMBIA:** +571-622-1717 • **COMMONWEALTH OF INDEPENDENT STATES:** +7-502-935-8411 • **CZECH/SLOVAK REPUBLICS:** +42-2-205-102-33 • **DENMARK:** +45-44-89-49-89 • **ESTONIA:** +372-6-308-900 • **FINLAND:** +358-9-525-561 • **FRANCE:** +33-01-30-67-50-00 • **GERMANY:** +49-89-46008-0 • **GREECE:** +30-1-680-6676 • **HONG KONG:** +852-2802-4188 • **HUNGARY:** +36-1-202-4415 • **ICELAND:** +354-563-3010 • **INDIA:** +91-80-559-9595 • **IRELAND:** +353-1-8055-666 • **ISRAEL:** +972-9-956-9250 • **ITALY:** +39-39-60551 • **JAPAN:** +81-3-5717-5000 • **KOREA:** +822-3469-0114 • **LATIN AMERICA/CARIBBEAN:** +1-415-688-9464 • **LATVIA:** +371-755-11-33 • **LITHUANIA:** +370-729-8468 • **LUXEMBOURG:** +352-491-1331 • **MALAYSIA:** +603-264-9988 • **MEXICO:** +52-5-258-6100 • **NETHERLANDS:** +31-33-450-1234 • **NEW ZEALAND:** +64-4-499-2344 • **NORWAY:** +47-2218-5800 • **PEOPLE'S REPUBLIC OF CHINA: BEIJING:** +86-10-6849-2828; **CHENGDU:** +86-28-678-0121; **GUANGZHOU:** +86-20-8777-9913; **SHANGHAI:** +86 21-6247-4068 • **POLAND:** +48-22-658-4535 • **PORTUGAL:** +351-1-412-7710 • **RUSSIA:** +7-502-935-8411 • **SINGAPORE:** +65-224-3388 • **SOUTH AFRICA:** +2711-805-4305 • **SPAIN:** +34-1-596-9900 • **SWEDEN:** +46-8-623-90-00 • **SWITZERLAND:** +41-1-825-7111 • **TAIWAN:** +886-2-514-0567 • **THAILAND:** +662-636-1555 • **TURKEY:** +90-212-236-3300 • **UNITED ARAB EMIRATES:** +971-4-366-333 • **UNITED KINGDOM:** +44-1-276-20444 • **UNITED STATES:** +1-800-821-4643 • **VENEZUELA:** +58-2-286-1044 • **WORLDWIDE HEADQUARTERS:** +1-415-960-1300

LFC3.1 Printed in USA 7/97 FE593-0/20K