Sun and Security

This white paper was originally written in December 1996 for Sun Microsystems. While many of the companies mentioned in this paper have been acquired or gone out of business, it still provides an useful overview of many of the issues regarding Internet security.

Introduction

Computer and network security are topics that many executives and managers avoid talking about. Many feel that discussing their security implementations and policies will cause their companies to become vulnerable to attack. This lack of dialog has resulted in some executives not being fully aware of the many advances and innovations in security technology, that are enabling companies to confidently take full advantage of the benefits and capabilities of the Internet and intranets.

Ironically, computer networking security can provide a more secure solution, as well as one that is faster and less expensive than traditional solutions compared to security problems of employees photo-copying proprietary information, faxing or mailing purchase orders, or placing orders by phone.

The purpose of this white paper is to demystify and inform the executive how intranet and Internet security can easily and effectively be implemented, by providing examples of how products from Sun Microsystems and its partners are being used for these applications.

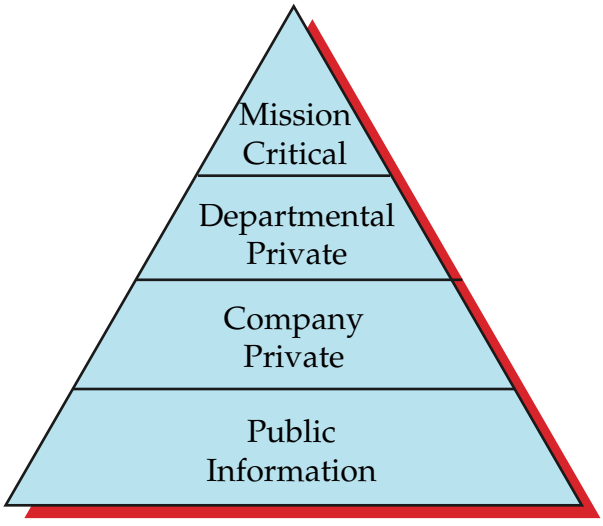
Throughout this paper, we've used terms such as access control, encryption, firewalls and SET. For those not familiar with some of these terms, a short glossary is provided in the appendix.

General Security Principles and Architecture

Fundamentally, security means risk management. It's something that we personally deal with each day. We have keys for our car, for our house, and file cabinets. We have card keys that we use at offices, athletic facilities, and hotels. We place different values on the contents secured by the locks. We may choose to have multiple locks on our front door, but are content with a combination lock on an locker. Yet a safety deposit box requires two keys, possessed by two people, to access it. So without realizing it, most of us have already established an individual security policy.

The first step in defining a corporate security policy is to draft a high-level management policy statement establishing a framework and context for security within an organization. This policy needs to define what are 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 an organization, determining the value of information, or the possible damage to reputation should it be disclosed, along with possible risks. Yet this step in fact is no more difficult than the risk management that a corporation already exercises every day. Most businesses already have clearly established what information is valuable, who should have access to it, and who has responsibility for protecting it, as the following security hierarchy illustrates:



Security Hierarchy

Information such as trade secrets, vault and authorization codes, lock and key information,

are clearly of a mission critical nature, whose unintended disclosure could cause severe loss to a business or operation. In addition to computer security, attention should be given to physical security, e.g. restricting the use of modems, removable media, and controlling access to devices.

Departmental 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 . . .

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 by means of Web servers to customers and interested parties by means of the Internet.

A careful and systematic examination of risks is needed, since perceptions often differ substantially from actual risks. Often the primary risk is found to be internal. For example, system administrators often are among the lowest paid individuals in an organization, yet have access to sensitive information otherwise limited to executives. In other cases, a remote dial-in line used for debugging, could be used to gain general access to internal systems, bypassing other security safeguards. Care needs to be taken to rationally evaluate risk. It is often helpful to examine how existing situations are handled.

> "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

Having evaluated the value of assets and determined potential risks, an implementation strategy for protecting assets can be developed. The objective is to make obtaining the data more expensive than its value, while spending the minimum amount required to protect it. This requires careful examination of alternatives. For example, disconnecting a system from the network can be the simplest and most cost effective way to solve a network security problem. And no amount of hardware and software will substitute for establishing and implementing effective security policies and procedures. Paul Moorhead also feels that:

> "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 required to provide it. Similarly, care needs to be taken to ensure that the added security does not unduly reduce network performance or employee productivity, or there will be considerable temptation to bypass or defeat corporate security measures.

In summary, establishing a corporate security policy involves the following:

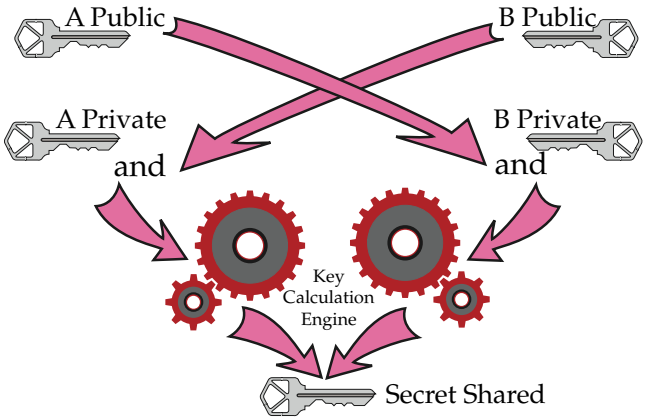
- High-level management policy statement
- Systematic analysis of organizations assets
- Examination of risks
- Develop implementation strategy

Public / Private Key Encryption

For many business and electronic commerce applications, it is necessary to transmit information over communications lines and networks where there is the potential for data to be altered, forged or illicitly introduced. A powerful technique for securely sending information is public key encryption. Two keys exists, one public, the other private. The public key is freely distributed, and is used to encrypt the information to be sent. The private key is retained by the recipient, and is used to decrypt the received information. Messages encrypted using long bit-length keys are currently regarded as essentially impossible to crack.

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

To achieve secure, two-way communication across the Internet, without having previously exchanged keys, the Diffie-Hellman scheme may be used. 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 the two parties.



Diffie-Hellman Calculation

In 1996, Sun Microsystems introduced SKIP (Simple Key Management for Internet Protocol) and proposed it as a IETF standard. SKIP provides efficient transparent encryption of any TCP/IP protocol suite, using encryption keys that are changed by default, every 30 seconds or 500 KB. It facilitates the management of encryption keys, and the certification of public keys. SKIP supports a variety of authentication and encryption schemes, including Diffie-Hellman, RC2, RC4 and DES (data encryption standard) to provide secure communications with remote or mobile employees and customers, via their laptops, servers or workstations.

International Issues

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

Sun's Leadership in Security

Sun Microsystems has several groups that are focused on bringing innovative security products to market. Many highly talented individuals are involved in the design and inspiration of these products, several of whom have international reputations: Widely recognized for his work in the mid-1970s in developing the family of techniques now known as public-key cryptography, Whitfield Diffie has written numerous articles and papers on issues pertaining to computer security. He is the recipient of an Honorary Doctorate from the Swiss Federal Institute of Technology and is regarded by many as the father of modern cryptography.

A widely known Internet computer security expert, Tsutomo Shimomura and New York Times reporter John Markoff wrote the book "Takedown," detailing their experiences in detecting and identifying Kevin Mitnick, resulting in his successful prosecution for illegally accessing various government and private sites. (Mr. Shimomura is a consultant to Sun.)

Sun Security Products

Sun Microsystems has four primary groups with responsibilities for developing security products. The Internet Commerce Group, a division of SunLabs, was formed in 1994 to bring to market, products facilitating electronic commerce. Currently the group offers three award-winning products: SunScreen SPF-100, SunScreen EFS (encryption firewall server), and SunScreen SKIP. SPF-100 combines transparent encryption with a firewall, facilitating using the Internet to deploy secure corporate Intranets. EFS provides encryption of the data stored on a server, minimizing the possibility of internal break-ins. SKIP enables telecommuters and mobile employees to encrypt all data sent from a PC or laytop to various hosts.

SunSoft's security group is also developing a variety of security products. While it has already released SKI (secure key-management infrastructure), facilitating the creation of public key certificates and their storage in repositories, a wide variety of other security products are under development, including support for new protocols and authentication systems.

Sun's JavaSoft division has created the Java language as a means of writing highly portable applications. The capabilities of Java have presented unique security challenges which have been systematically addressed in the design and implementation of the language. JavaSoft has also created a set of extensions to the language called JECF (Java Electronic Commerce Framework) which facilitate the development of highly secure electronic commerce applications.

The ***Secure Software Engineering Group*** of Sun Federal provides Trusted Solaris and is working upon other trusted implementations of Sun products.

Network Security

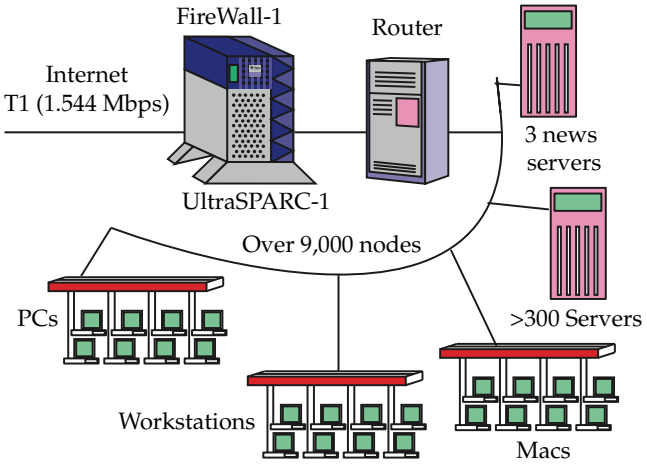
Firewalls are a basic means for providing network security. They act like the moat around a medieval castle, by restricting information to enter and leave at carefully controlled points, and preventing unacceptable attempts at accessing resources within the firewall.

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 SunSoft from CheckPoint Software Technologies. Widely used on Solaris systems, FireWall1 examines each connection attempting to pass through its firewall, using multiple rules defining the myriad applications, services and users allowed access to each specific internal server. It is ideal for securing and compartmentalizing intranets.

San Diego State University

San Diego State University uses a Sun UltraSparc-1 with 256 MB memory running CheckPoint FireWall-1 software to provide campus access to the Internet via a T1 communications line. Currently the University has over 9,000 nodes on campus, hundreds of web servers and three news servers.



San Diego State University Configuration

The University's security policy is that anything not specifically allowed is denied. Access to each server on campus was determined by sending an email to all responsible faculty, administrators and staff, requesting them to fill out a Web form to obtain a firewall exception. The form lists 200 services that can be allowed for each server. After each request is incorporated into a "rule," notifying email is sent informing the requester of the implementation of their request. To date, over 150 security rules have been implemented.

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 transport protocol) access to a particular departmental server for connections originating over the Internet.

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

Secure Payment Solutions

Electronic Commerce Merchant Server

The World Wide Web (WWW) represents a new distribution channel that rapidly growing numbers of companies are taking advantage of. Indeed, some firms are selling a sizable portion of their products by means of their 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 provide three functions:

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

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

Authentication Verify that a client is communicating with an intended server.

Encryption Helps prevent data from being understood by an unintended party, and insures that data was not altered in transit.

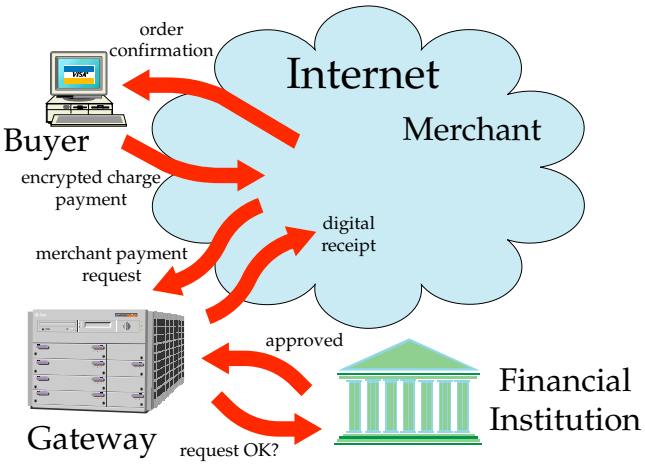
Netscape browsers offer integrated support for SSL. All of its browsers support at least a 40-bit RC4 stream encryption algorithm designed by RSA Data Security . Netscape servers support SSL-based certificates, allowing any SSL-compatible client to verify their identify.

Mastercard/Visa SET

Another protocol that CyberCash, Microsoft, Netscape and other vendors have announced support for is Mastercard/Visa's SET protocol. The advantage of SET is that only the card holder and acquiring bank are able to see the actual credit card number, i.e. the merchant never sees the number. This provides a higher degree of security for credit card transactions.

CyberCash Wallet

There are a number of other companies providing mechanisms allowing secure payment to occur over the Internet. One such company is CyberCash. The CyberCash Wallet provides the means for merchants to accept a range of payment options, while obtaining assurance of the customer's identify, and that they possess a valid credit card or Cybercash digital coin belonging to them.



CyberCash Payment Authorization Process

When a customer selects a CyberCash Pay button in 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, where merchant identification is added, and forwarded to a CyberCash gateway server who 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 financial network, requesting charge approval. If positive, the merchant receives a digital receipt and the customer receives confirmation of their order.

Netscape LivePayment

Netscape also provides a secure payment processing product called LivePayment. Using the SSL protocol, it allows EDI connections to banks, permitting real-time credit card processing over the Internet. CyberCash and other payment vendors have stated that they will also support LivePayment.

Access to the Netscape merchant server is also controlled by features ensuring server authentication by certificates, data encryption, data integrity and user authorization. More conventional access control and monitoring is provided by means of passwords and audit logs.

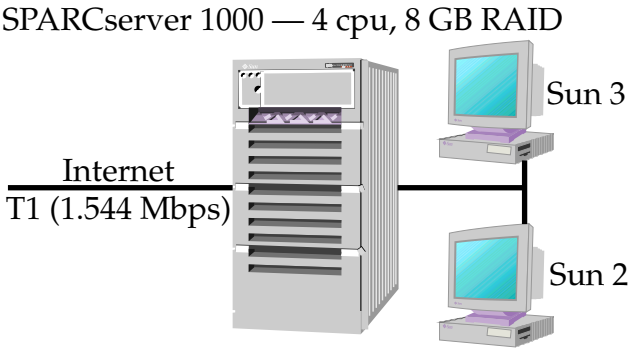
First Virtual VirtualPIN

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 1994. Rather than rely upon technology, First Virtual has implemented a process to ensure secure transactions. 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 their VirtualPIN (personal identification number) and an email is sent to the buyer asking them to confirm their purchase. This process eliminates the need for encryption and allows any Internet user to immediately make use of this payment service.

CDWorld

CDworld is a family-owned, on-line discount-music retailer, who first started doing electronic commerce 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 on-line catalog.

The retailer uses a merchant server consisting of a Sun SPARCserver 1000 with 4 cpus, 256 MB RAM, and a RAID with 8 GB. It runs both Netscape Commerce Server and Secure Server, in conjunction with a Sybase DBMS. Connected to a T1 communications line, this system supports over 200,000 hits each day.



CDWorld Configuration

With respect to security, CDworld addressed two basic concerns, customer security and internal security. Customer security was addressed by means of Netscape SSL, using 40-bit RC4 encryption algorithm, allowing its use internationally.

"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." Bruce Pettyjohn, President, CDWorld, October 1996

The first step in providing internal security at CDworld was the use of firewall software from Livingston, which uses one IP address outside the firewall, and a second IP address inside the firewall. Additional security is provided by the usernames and passwords required by Netscape, Sun and Sybase software.

"Our basic internal security philosophy is to restrict the people who can access our systems to as small a number as possible."

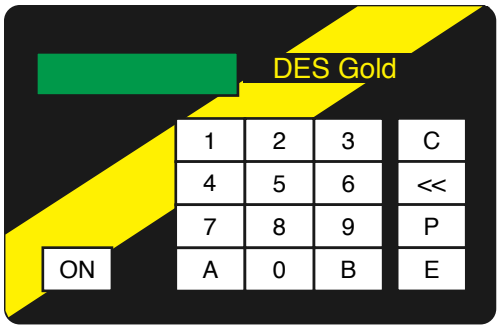
Controlling Access

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 for regulating the users allowed access to a system, or providing the means to secure information by encryption.

Authenticated Access

When an user logs into a system, what measures can be taken to insure that they are a valid user, as opposed to someone who has stolen their password? 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. Many companies provide each of their remote users with a digital token card (also called hard tokens), to increase their assurance of the identify of each remote user.

Engima Logic's SafeWord DES cards are hard tokens that generate single-use passwords without requiring synchronization with a host. They are able to generate over a million unique 6 to 8 digit passwords. Each time the ON button is pressed, a new password is displayed. The user types the password shown on the display in response to the system prompt. The system upon receiving the password, decrypts it using a DES key and verifies it. Once a password has been used, it is not allowed to be reused, preventing replay attacks.

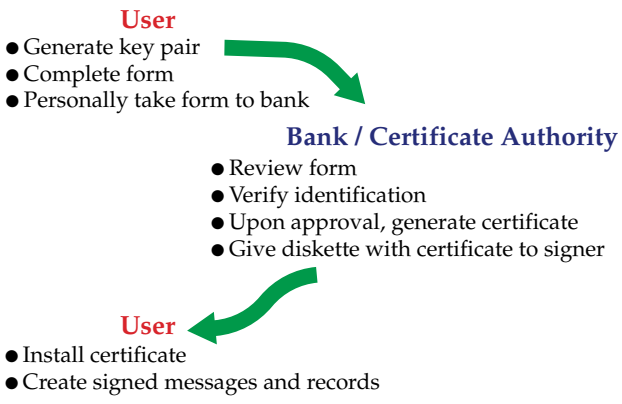


SafeWord DES Gold Card

Earlier in this white paper, mention was made of trusted third parties, called "certificate authorities." Verisign is a commercial certification authority that issues digital certificates providing assurance of the identify of an individual. Typically a Verisign digital certificate contains the owner's public key, name, expiration date of public key, name of issuer (Verisign), serial number of the certificate and 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, provide the digital identification for specific individuals, and maintain lists of revoked digital certificates.

Verisign provides two types of digital certificates, personal certificates to provide assurance of the identity of an individual and secure server certificates to protect communications with a given server and allow verification of the identity of a server. Its Class 1 personal certificates provide an unique name and email address within its repository. A Class 2 personal certificate requires confirmation of name, mailing address and other personal information by a Equifax consumer database, along with 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 below:



RSA Recommended Certification Issuing Process

Privacy and Encryption

Another means of controlling access to information is to encrypt it. With a sufficiently long encryption key, the cost and time required to break the key will greatly exceed the value of the data. Encryption should only be used in a carefully thought out manner, as part of how a security policy is implemented, not as a substitute.

> "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

PGP (Pretty Good Privacy) is a program for protecting the privacy of email and computer files. It runs on virtually every Unix system, as well as PCs running DOS, Windows, OS/2, MacOS, and the Amiga. 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 to certify keys and obtain keys from key servers. In May 1994, a version of PGP was released that includes a license from RSA Data Security, allowing the legal, widespread non-commercial distribution of PGP. Commercial versions of PGP are distributed by ViaCrypt.

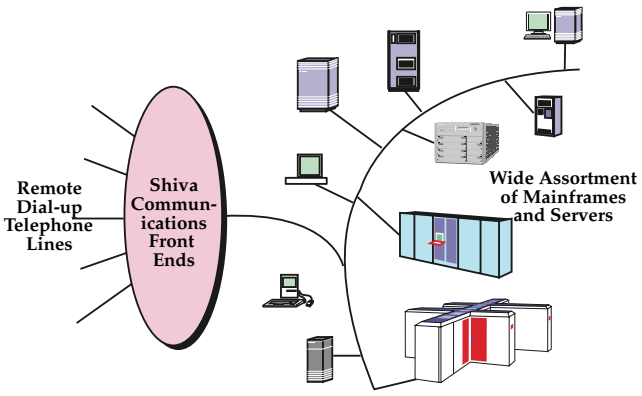
SKIP for Solaris is an encryption product that ensures that all data interchanged over a public network between two or more SKIP-nodes remains secure. All encryption and deencryption between nodes is performed in a manner completely transparent to both users and applications running on the systems. In addition to being part of the Solaris SunScreen SPF-100 product, SKIP is also planned to be released as a standalone product for Windows, NT and Macintosh platforms.

PGP Offers the advantage of running on a wide variety of systems, and providing individuals with the ability to keep certain data confidential.

SKIP An ideal product for enterprises needing to provide automatic and consistent protection of all data sent over unsecured networks.

Controlled Access - American Express

American Express has been using Enigma Logic hard token security technology products for over ten years, originally to provide secure remote access to its mainframes, and currently to provide secure remote access to its global network of client-server systems through dial-up lines connected to Shiva front-ends. It has over 10,000 nodes connected to a wide variety of workstations, servers, minicomputers and mainframes. While currently hard tokens are only used by remote users, it is anticipated that these tokens will be used by desktop/Webtop users in the future.



American Express Remote User Configuration

> "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 administrate. 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."

At American Express, work is being performed to develop profiles of each user. Since users tend to behave in predicable manners, it is planned to log accesses and requests that are out of the ordinary for that user. Additionally, by collecting all possible information regarding an user such as user and caller ids, much greater assurance of an user's identify can be obtained.

Customers, however, are allowed direct access to their accounts via ExpressNet On AOL (American On Line) using an user ID and password. Bills can be paid on-line using the bank account of their choice. By means of a Internet Web interface, on-line investing and airline tickets may be purchased.

Secure Virtual Private Networks

Many corporate networks used for EDI and funds transfer have been implemented using either private networks or costly services from specialized telecommunications network providers. Significant reduction in internal corporate networking costs can be achieved by using secure, encrypted, IPlevel network communications over less expensive public networks, called secure virtual private networks (SVPN). Implementing such SVPNs requires 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.

One product that can be used to implement SVPNs is the Solaris SunScreen SPF-100 network security system. SunScreen acts both as a traditional rules-based packet screening firewall, and as a transparent encryption device using the previously mentioned privacy and authentication services provided by Simple Key Management for Internet Protocol (SKIP).

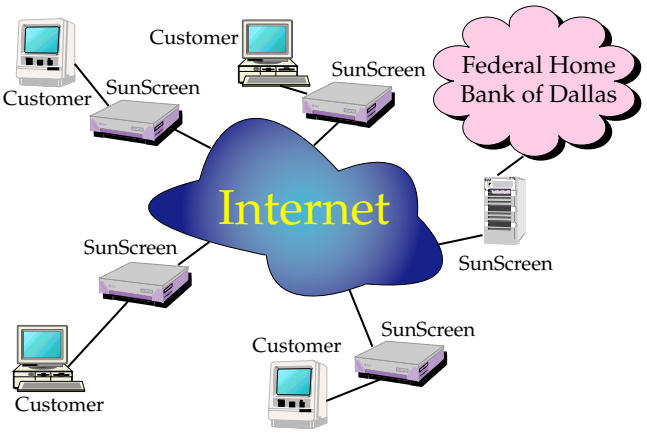
SunScreen uses a firewall technique called stateful packet security. This is an advanced form of dynamic packet filtering, designed to recognize the context as well as the content of each packet. The turn-key nature of SunScreen enables many users to regard it as a turn-key network appliance providing considerable security with a minimum amount of administration.

Federal Home Bank of Dallas

The Federal Home Bank of Dallas provides financial services to commercial banks, savings and loans, credit unions and insurance companies, to facilitate their mortgage lending activities. 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 in the process of deploying a virtual private network, allowing its clients to securely access its services over the Internet using browsers as the user interface. Current plans are to have 200 customers using the system by the end of 1997, and 600 to 700 customers when the system is fully deployed.

In defining its security policy, the bank identified distinct internal and external requirements. Responsibility for overall security mechanisms were 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.

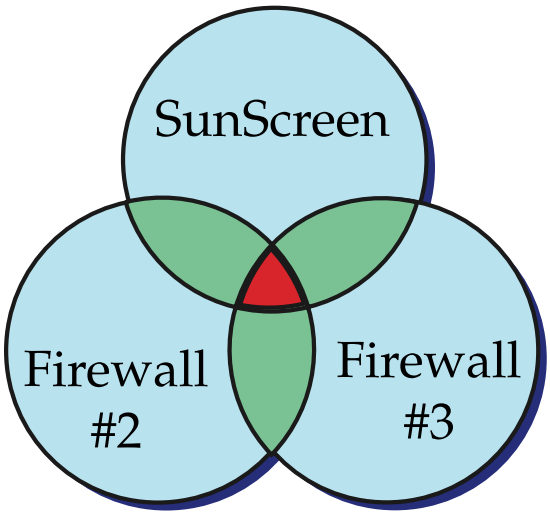
A particular concern for the bank has been to protect its private data that consists of transaction information on loans outstanding, wire transfers, and secure safe keeping of bonds and capital stocks. For these reasons, it has established a number of rules regarding authentication and encryption to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



Federal Home Bank of Dallas

> "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. For our smaller users, we are also currently considering using PC/SKIP."
>
> 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. 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.



Increased Protection via Multiple Firewalls

Java Security

The Java language enables small applications called applets, to be downloaded to user systems and executed 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. The simple, interpreted object-oriented Java language makes it easy to debug and modify. While the ability to download Java applets provides 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 Java was designed with safety and robustness as major design goals. The first step taken was to simplify the Java language, eliminating dangerous aspects common to other languages such as pointer arithmetic, and by providing mechanisms to minimize outside manipulation of internal objects. A second area addressed by Java was the potential vulnerability provided by patching applets. To address this weaknesses, the class loader that loads applets checks each applet to verify it conforms to the runtime rules of the Java language specification.

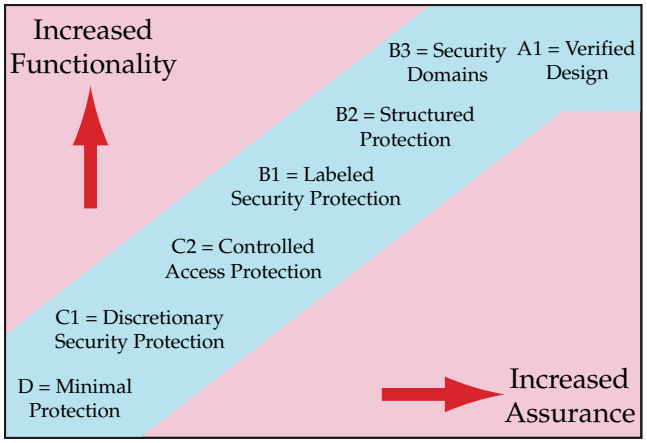
Another mechanism provided by Java is its security manager. The security manager distinguishes between applets known to be safe or trusted, and those which were downloaded and are not known to be safe, i.e. untrusted. Untrusted applets are not allowed to read or write files or start-up new applets. In the future, by adding a digital signature to applets, it will be possible for users to download trusted applets, since assurance can be provided that the applet was created by a specific author, and that it has not been modified by anyone else.

Sun Microsystems JavaSoft Electronic Commerce group has announced a set of API extensions to Java called JECF (Java Electronic Commerce Framework). JECF facilitates the development of payment methods and other financial services applications in Java-enabled environments. JECF includes security features that provide the ability to 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. It insures that the proper version of each class is used by inspecting their version numbers. Access control lists specify what database objects can be made available to which applets, and what applets can invoke other applets and resources.

These JECF security features enhance data privacy, e.g. preventing an applet created by Visa from obtaining information on the users' MasterCard or Amex transactions. Yet those applets that require greater access, such as a tax program, can be granted access to the required information. JavaSoft is actively working to promote JECF as an ubiquitous electronic commerce standard. For further information regarding Java Security and JECF, please access the web pages at http://java.sun.com/commerce.

Secure Operating System

In the United States, the Orange Book or Trusted Computer System Evaluation Criteria is used for the evaluation of secure operating systems. Similarly, France, Germany, the Netherlands and the United Kingdom have established ITSEC (Information Technology Security Evaluation Criteria), as the de-facto European security evaluation criteria.



Orange Book and ITSEC Ratings

While these certifications have traditionally been required in selling to national defense and intelligence agencies, banks and other commercial enterprises are beginning to consider the use of such operating systems, since they provide greater restrictions over the allowed and permitted use of a system.

The C2 rating provided by Solaris 2.4 allows restricting the type of access (read, update, delete) to files based on the identity of the user. Users are forced to identify and authenticate themselves before system access is allowed.

> "C2 security is adequate for most commercial systems products. Where you start to need better security is when you no longer know who is accessing your data."
>
> Paul Williams,
> Admiral Management Services

Based upon Solaris 2.5, Sun Microsystems Federal is introducing Trusted Solaris 2.5. The product has been submitted to an United Kingdom certification agency to validate its B1 level capabilities. Besides supporting all current Sun products and software, Trusted Solaris provides sensitivity labels, enabling explicit user and file access control, allowing access by a user only to files when their clearance equals or exceeds that of the data or resource.

Security Futures - Smart Cards

Logically, a smart card is equivalent to an electronic safe deposit box. Implemented as a credit-card-sized piece of plastic, a smart card contains a semiconductor chip with logic and non-volatile memory. The software within the card detects attempts at intrusion and tampering, as well as monitors abnormal usage. Billions of smart cards have been made since their introduction in 1977. While smart cards are popular in Asia and Europe, they are just beginning to be introduced in the United States. Some of the many applications of smart cards include:

- Stored value card - minimizes the need to carry cash, can be used to purchase items from merchants, vending machines and pay phones.
- Health care - portable, customized health care file with medical emergency data, HMO and insurance information.
- Access control in offices and hotels, allows storing time entered, exited, access conditions and identity.
- Contactless tickets for ski resorts and airlines - increases speed, convenience and security, and facilitates 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 and 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, allowing each card to contain a unique identification number. Limits are typically placed on the number of erroneous attempts, preventing brute-force attempts.

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 that facilitates writing Java applications that will run on all ISO 7816-4 compliant smart cards.

Summary

In summary, by using Sun Microsystems and its partners products, customers can be assured of the availability of all of the elements necessary for providing effective management of risk with respect to providing access to intranets and the Internet. 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 wide variety of security topics involved with managing risk. There are hundreds of vendors providing security solutions based on Sun Microsystems products, obviously only a handful of these products could be mentioned.

Glossary

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

Authentication Also known as digital signatures, the use of cryptographic technology to provide the receiver of a message with strong amount of evidence regarding the origin and integrity of a digital message.

Certificate Certificates are often sent with a message. If the message has been tampered with, it will become apparent upon verification of the signature contained within the certificate. Certificates typically also contain public key owner information.

DES Digital Encryption Standard. Private-key cryptosystem, official standard of United States Government.

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

Firewall A computer or router which is physically located between an external and internal network which performs the sole task of protecting the internal network from unwanted intrusion from the outside network.

PGP Pretty Good Privacy. Public-key encryption created by Phil Zimmerman, de-facto industry standard.

Private-key Encryption / 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 / decryption using two different keys

RSA Rivet-Shamir-Adleman. Most widely used public-key cryptosystem

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

SKIP Simple Key Management for Internet Protocol is a system for managing encryption keys, 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. Provides encrypted TCP/IP path between two hosts, commonly used by Netscape for Internet transactions. 40-bit keys should not be considered secure, 64-bit keys however are considered secure.

Signature An 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 Consistent means of accessing a variety of media in a simplified fashion across wide area networks (Internet)

References

The following computer security books are recommended:

1. *Building Internet Firewalls*; D. Brent Chapman, Elizabeth D. Zwicky; O'Reilly & Associates, November 1995. Provides a complete overview of firewalls, while remaining accessible and practical. Authors are authorities on firewalls and system administrators.
2. *Firewalls and Internet Security : Repelling the Wily Hacker*, Addison-Wesley; June 1994. Provides extensive discussion of different types of firewalls, and their strengths and weaknesses. Describes potential attacks and tools used to launch the attacks.
3. *Mecklermedia's Official Internet World Internet Security Handbook*; William Stallings. One of the acknowledged experts in the field.
4. *Practical Unix & Internet Security*; 2nd edition; Simson Garfinkel and Gene Spafford; O'Reilly & Associates, April 1996. Comprehensive book discusses topics ranging from password vulnerabilities and policies, through Unix permissions, dangerous accounts, log files, modems, network security, NFS, security incidents and firewalls. Does not provide extensive coverage on security tools.

Company	Type	Phone	Web
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
First Virtual	Payment		www.fv.com
Mondex (London)	Payment	171-920-5505	www.mondex.com
Netscape Communications	Payment		www.netscape.com
Premenos	EDI	800-578-4334	www.premenos.com
Raptor Systems, Inc.	Firewall	617-487-7700	www.raptor.com
Security Dynamics	Encryption	800-732-8743	www.securid.com
Solect Technology Group			www.solect.com
TAI Systems		314-530-1981	www.techapp.com
Trusted Information System.	Firewall	301-527-9500	www.tis.com
VeriFone Internet Commerce	Payment		www.verifone.com
Verisign	Certificat	415-961-7500	www.verisign.com

The following sites contain additional information on Sun-based security solutions:

www.sun.com/sunsoft/solstice/Networking-products/networksec.html

www.sun.com/sunsoft/solaris/security/security.html

java.sun.com/commerce