Secure Enterprise Computing with the Solaris™ 8 Operating Environment

A Technical White Paper

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
1 (800) 786.7638
1.512.434.1511

CHAPTER 1

Introduction

Organizations everywhere are leveraging Internet technologies to reach new markets, create additional revenue streams, and improve relationships with employees, vendors, and suppliers. As companies become more dependent on the Internet for both their internal and external business relationships, the importance of security increases as well. As the Internet's reach continues to expand, so do the sources of security threats.

Jeffrey Hunker, senior director of the National Security Council, has said countries that are militarily weaker will target America's Internet infrastructure (ZDNN, July 7, 1999). Organized groups are releasing software to attack vulnerabilities in Microsoft's Windows operating systems (CNN, July 7, 1999). And *Information Week* (July 12, 1999) reports that exploits like the Melissa virus affected 69 percent of U.S. companies in the last year, while the use of Trojan horse attacks more than doubled in the same time period — making it unclear whether attacks are coming from inside or outside of a company's firewall. Indeed, *Information Week's* global security survey reports that a shocking 76 percent of businesses encountered a security breach in the past year.

DataPro estimates that 80 percent of all computer crimes are committed by current employees. With the increase of viruses and Trojan horses that can be propagated by unknowing users, IT organizations are recognizing the need to protect enterprise networks from both internal and external attack. Information in an enterprise network can be compromised by interrupting its flow through denial-of-service attacks; interception through eavesdropping techniques; modification through man-in-the-middle attacks; and fabrication of authority through spoofing (FIGURE 1).

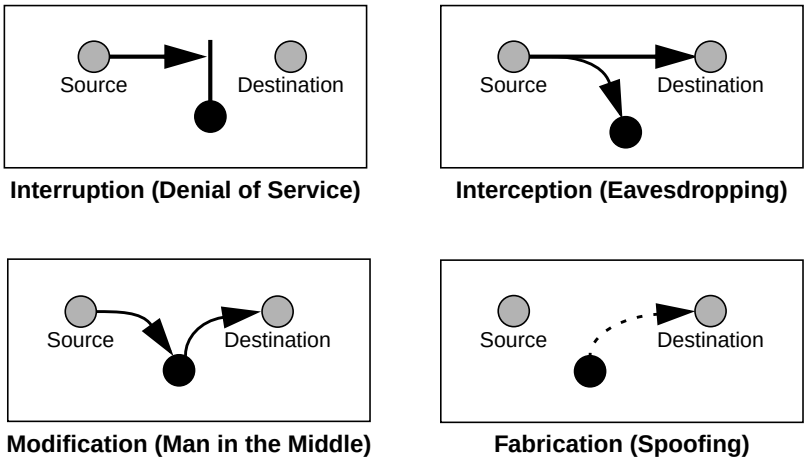

FIGURE 1 Information in enterprise networks can be compromised through interruption, interception, modification, and fabrication.

To protect systems and networks from these four types of attack, organizations require end-to-end security solutions that:

- Can securely identify and authenticate users
- Enable users to access only the application features they are authorized to use
- Maintain privacy and prevent unauthorized modification of sensitive data
- Host applications on servers that are secure from intrusion, yet accessible by large numbers of users in a broadly networked environment
- Facilitate secure communication between authenticated parties
- Can identify the source of security changes to the system, including file access, security-related system calls, and authentication failures

Securing systems and communications in enterprise networks that are simultaneously connected to millions of potential users on the Internet requires technologies that:

- Cover all aspects of security
- Are flexible, integrated, easily configured
- Interoperate with other open standards-based products

The technologies the meet these needs are found in the Solaris™ 8 Operating Environment.

The Solaris 8 Operating Environment delivers end-to-end security for enterprise computing, electronic commerce (e-commerce), and workgroup computing. Chosen by Internet service providers (ISPs) worldwide for its maturity, the Solaris Operating Environment provides easily configured, flexible, and independently certified security for today's .com businesses.

Security alone, however, is not enough. As companies grow, so must their IT infrastructure, Only Solaris Operating Environment scales from one to 128 processors in the same symmetric multiprocessing (SMP) server. Binary compatibility protects investments in server hardware with compatibility across Sun's entire server product line. Because security in the Solaris Operating Environment is based on open standards, it interoperates with key facilities of other products, including UNIX® systems and Microsoft Windows NT software.

The Solaris Operating Environment can easily establish secure network communications from host to host and site to site using encrypted Internet Protocol Security Architecture (IPSec) connections. The Solaris Operating Environment provides strong public and secret key-based authentication and single network sign-on techniques using public key-based smart cards and Kerberos. It provides the tools for building secure applications and authentication using the Solaris Operating Environment's Public Key Infrastructure (PKI), and enables role-based access control (RBAC) to ensure that privileged users can modify system configurations based on pre-defined user profiles.

CHAPTER 2

Securing Systems and Communications with IPSec

IPSec provides an extremely powerful set of mechanisms for securing both servers and communication channels so that only authorized parties can communicate with them. Inbound and outbound communication can be restricted by IPSec security policies, controlling public access on a port-by-port basis. Similarly, authenticated hosts can be offered different levels of access depending on the security policy. Because IPSec operates at the Internet Protocol (IP) level, it can be used to restrict access to applications that are not completely secure.

The IPSec Authentication Header (AH) can be required to ensure the authenticity of a remote server or workstation, and network communication itself can be encrypted using the Encapsulated Security Payload (ESP). These two mechanisms facilitate a wide range of security options. Because IPSec is implemented at the IP level, it can be deployed so that it is transparent to applications, forming the basis for true, end-to-end security solutions. In fact, since IPSec is implemented in the lowest levels of the protocol stacks, only trusted, authenticated parties are able to reach the applications servicing IPSec-restricted ports.

Following are a few of the many security approaches enabled with IPSec.

- ISPs can secure their Internet servers so that only specific services are accessible to users. For example, a Web server can define policies allowing inbound HTTP connections to be established by external users, and outbound, encrypted NFS™ or JDBC™ technology connections to secure back-end content servers. With all other ports closed, the Web server is impervious to attacks other than those aimed directly at the carefully configured Web server process itself.
- Multitier enterprise applications can have secure communication between tiers so that even those with physical network access cannot view data they are not authorized to see, ranging from human resources information to strategic planning documents. Interdepartment communication, once vulnerable to interception, can now be fully secured.

- Virtual private networks (VPNs) can be established to enable remote offices – and even remote users – to communicate securely over the Internet to the home office (FIGURE 1). IPSec can encapsulate all traffic between a remote site or workstation and an IPSec-enabled gateway system that allows only authenticated, encrypted traffic from the Internet. With IP-packet forwarding turned on for this server, secure network traffic is forwarded on to the internal enterprise network to its true destination – including mail and file servers, internal Web sites, and private enterprise applications.

IPSec with the Solaris 8 Operating Environment

The implementation of IPSec supports both shared-secret and public-key encryption. 128-bit MD5 and SHA-1 algorithms are available for the authentication header; 56-bit DES and 168-bit Triple DES algorithms are available for payload encryption. (168-bit Triple DES is available only in the U.S.) Manual-key exchange is supported in the first release of Solaris 8 software; automated public-key management through Internet Key Exchange (IKE) support is planned for a future update.

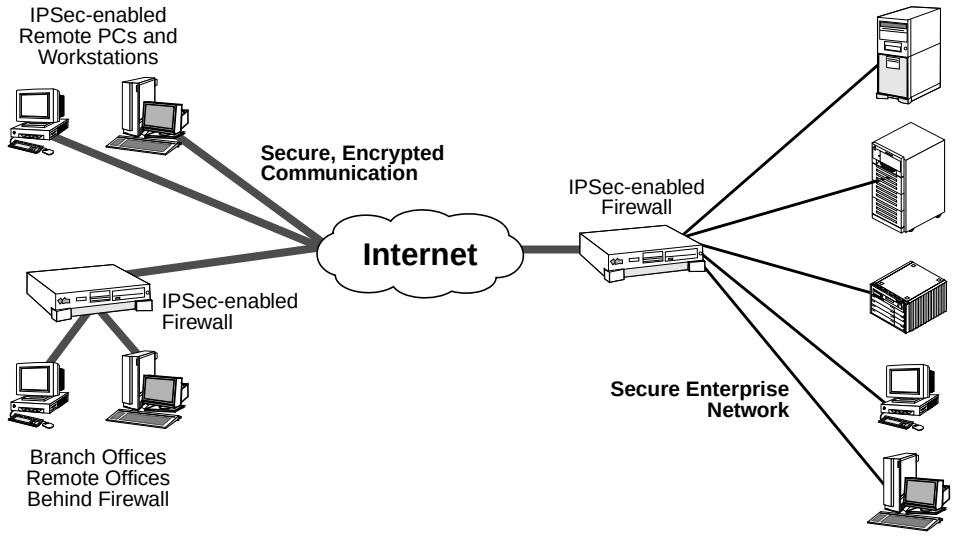

FIGURE 1 Virtual private networks can be established using IPSec with no additional VPN software required — enabling secure communication between remote users, field offices, and the main enterprise network.

Sun believes that interoperability is best achieved through the use of open standards. IPSec is implemented following Internet Engineering Task Force (IETF) specifications. As a result, servers running the Solaris Operating Environment will operate seamlessly with vendors that adhere to IETF standards, including UNIX-based systems from Hewlett-Packard and IBM. A significant advantage of the Solaris Operating Environment is that it runs on Sun SPARC™ processors as well as Intel Architecture-based platforms, giving customers freedom to choose the server platform that best suits their needs.

An additional benefit of Sun's implementation of IPSec is that Solaris software includes application programming interfaces (APIs) that enable application-level specification of IPSec policies. Thus, application developers can set security policies that are designed to meet their specifications and provide high levels of application security, independent of the choices made by system administrators.

CHAPTER 3

Providing Strong User Authentication

Sun's implementation of IPSec enables organizations to secure network-based systems and help ensure the privacy of communication between them. The next component of Sun's end-to-end security strategy is the establishment of strong user authentication facilities that allow only authorized users to access specific systems and services. These features are key for building the highly-secure applications needed for e-commerce, banking, and enterprise applications.

Sun understands that enterprise security requirements are complex and may vary from application to application and company to company. This is why the Solaris 8 Operating Environment provides a flexible set of facilities for strong user authentication that can be used out of the box or integrated into applications as service-specific security features. The facilities include:

- The *Pluggable Authentication Module (PAM) interface* provides a uniform means for applications – and the Solaris Operating Environment itself – to access user authentication facilities
- *Smart card support* provides uniform mechanisms for the operating environment and third-party applications to interface with smart card-based encryption, personal data, and Java™ software applet management facilities
- *Kerberos support* enables users to sign on to their workstation once to obtain a security credential that can subsequently be used to transparently authenticate access to other requested network-based services

Pluggable Authentication Module Interface

Solaris 8 software's Pluggable Authentication Module (PAM) interface provides a set of APIs that can be used by third-party applications as well as the Solaris Operating Environment itself. Easily-configured PAM modules can be constructed to support site-specific authentication requirements. For example, a PAM module can be developed to interface with biometric scanning devices like palm geometry scanners. With a simple configuration file modification, all facilities that utilize PAM for authentication will require a palm scan at user login time. For even higher security, PAM configurations can require combinations of authentication mechanisms, such as smart card insertion and palm scan.

Smart Card Support Framework

When used in conjunction with public-key encryption facilities, smart cards can boost security to an unprecedented level. This is because smart cards are able to provide cryptographic functions and store private keys with no way to extract them from the card. The smart card support framework provides packaged solutions for authentication and tools that enable custom applications to access smart card features. The functions supported include:

- Authentication

  The Solaris 8 Operating Environment provides out-of-the-box support for smart card authentication at login time. With secret keys stored on smart cards, and a smart card PAM module configured to require authentication via smart card insertion, both operating environment login functions and application user authentication can be protected with the highest level of security possible. Using other mechanisms, smart cards can also be used for complex application functions such as digitally-signed electronic mail.

- Storing Personal Information

  Smart cards provide a way for applications to store personal information, such as name, password, office location, machine state, etc. For example, the Sun Ray™ 1 enterprise appliance stores all user state on the current user's smart card, restoring even the state of the caps lock key on any other appliance into which the smart card is subsequently inserted.

- Applet Management

  The Write Once, Run Anywhere™ characteristics of the Java platform extend to smart cards that have the capability to install, remove, and manage Java applets. Using a security model designed so that each applet runs in its own sandbox, applets can be loaded on smart cards to manage funds for purchases in the company cafeteria, authenticate access to secure networks, and even deliver responses to digital challenges before opening a door.

Sun believes so strongly in the security of smart cards that future desktop systems from Sun will be delivered with smart card readers. In fact, Sun is already making plans to equip every one of its employees with a smart card that can be used for personnel change management, e-mail signatures, travel expense accounting, and purchase authorizations.

For off-the-shelf use, Sun supports the Open Card Framework (OCF) implemented for the Schlumberger Cyberflex Access Card as well as the Dallas Semiconductor iButton and Java Ring — all of which support the Java virtual machine. The Schlumberger Micro Payflex Card also supports non-Java language-based secure storage. Java language-enabled cards support cryptographic operations using RSA algorithms; X.509 certificates can be stored, and Kerberos authentication will be supported in the future.

Single Sign-On with Kerberos

A recent Gartner Group survey suggests that user productivity could be increased by more than 40 hours per year by reducing the number of times each user must go through a login sequence. Kerberos solves this problem by providing a strong, distributed, enterprise-wide authentication mechanism. Kerberos requires users to authenticate once, and enables subsequent secure access to distributed systems and applications. Kerberos provides network application-level security on a per-access granularity and is ideal for intranet use where a central server can be installed for key management.

Under Kerberos, users authenticate themselves to their desktop system and provide an additional Kerberos password, which is also known by a central security server called the Key Distribution Center (KDC) (FIGURE 1). Following proper authentication, the user is issued a Ticket Granting Ticket (TGT) that is stored locally and used in future application authentication requests. When the user wishes to access a Kerberos-aware application on a remote system, the local system uses the TGT to obtain a service ticket that is passed to the remote application. The remote, Kerberos-aware application validates the service ticket (using a shared secret known only to itself and the KDC) and then uses the ticket's user identity for the session.

The Solaris 8 Operating Environment includes client software — conforming to the IETF specification for Kerberos Version 5 — that consists of protocol and encryption support, PAM modules, and tools to manage TGTs, Kerberos passwords, and system configuration. Server-side components are provided with the Sun Enterprise Authentication Mechanism™ product. These components include a KDC server, an administration system, tools for creating keys, and Kerberized applications such as *rlogin*, *rcp*, *telnet*, and *ftp*.

Sun's implementation of Kerberos interoperates with Microsoft's Windows 2000 Active Directory architecture. A KDC operates on either a Solaris Operating Environment or a Microsoft Windows 2000 server (Windows 95 and 98 do not support Kerberos). In addition, Sun's Kerberos implementation integrates with publicly-available Kerberos software available from MIT. Sun is actively involved in extending Kerberos into the smart card realm, and enabling it to utilize X.509 certificates.

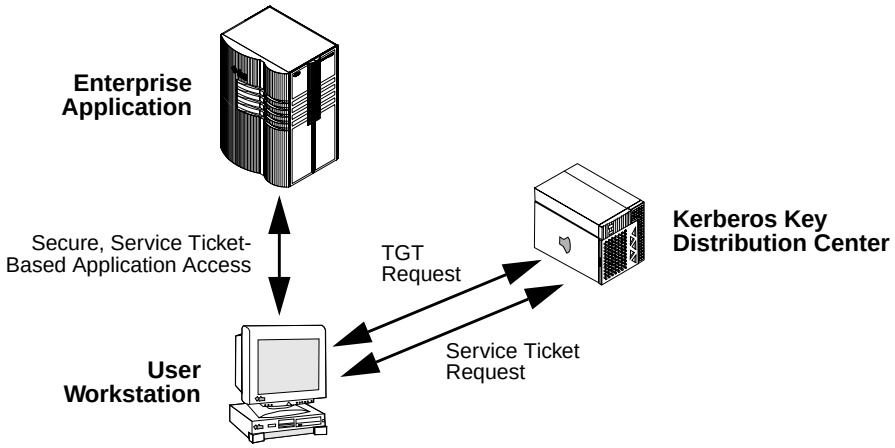

FIGURE 1 Kerberos provides single sign-on to remote applications with a per-user and per-access granularity that is ideal for secure, enterprise-wide networks.

CHAPTER 4

Role-Based Access Control

Even with state-of-the-art securing of systems and networks using IPSec and strong user authentication through mechanisms like smart cards and Kerberos, enterprise computing systems still have one remaining vulnerability: human error. The best system administrators and most trusted users are still fallible, and the most frequent source of system failures is operator error.

Role-based access control (RBAC), provided with the Solaris 8 Operating Environment, is an alternative to the all-or-nothing model of root access to UNIX systems. The traditional model gives the superuser ultimate power, while leaving ordinary users without the authority to solve their daily administration problems.

Role-based access control, once available only with Trusted Solaris™ software, enables the assignment of rights to perform specific operations. This allows individual trusted users to assume a higher privilege for performing limited administration functions, and can be used to partition root privileges among a group of administrators. Privileges that are managed with RBAC include serial port, file, log, and printer management, user login control, and system shutdown.

By separating powers and controlling the delegation of privileged operations to individual users, RBAC minimizes the chance that any user will go beyond their realm of expertise and inadvertently — or intentionally — make a change that results in a system failure.

Role-based access control is implemented using roles and attributes; once a user is logged in, they can assume roles that have been made available to them through the use of role-aware shells. By ensuring that users are authenticated first before any role is assumed, all privileged activities can be logged and associated with a person.

Access Control Lists

Hand in hand with the highly granular nature of RBAC is the ability to protect file access through access control lists (ACLs). With access control lists, file access rights can be controlled on a per-user basis rather than with broad user, group, and other access. ACLs are implemented for UNIX file system (UFS) and NFS software, and conform to the POSIX 1003.6 specification. Existing file permission mechanisms continue to be supported for cases where ACLs are not required.

CHAPTER 5

Integrated, End-to-End Security

The Solaris 8 Operating Environment provides integrated features that deliver the end-to-end security needed by electronic commerce, enterprise computing, and workgroup applications. IPSec enables servers and the network connections between them to be secured and encrypted, limiting access and ensuring privacy. Once secured with IPSec, smart cards and Kerberos provide strong user authentication so that network services are provided only to authorized users. For specific application security needs, Sun's smart card management facilities enable the construction of secure, customized applications. End-to-end security is complete only if authenticated users have just the right amount of power required to get their work done, and role-based access control and access control lists provide administrators with the fine-grained control they need.

Today's complex enterprise computing environments demand even more than comprehensive, integrated, end-to-end solutions, and the Solaris 8 Operating Environment provides just that — and more. Solaris 8 software delivers seamless interoperability with other systems that implement open standards-based interfaces such as IPSec, Kerberos, and public-key encryption. It provides flexibility for organizations to quickly deploy off-the-shelf solutions with technologies like smart cards, and employ the same building blocks used by Solaris software to construct their own applications. The Solaris Operating Environment can easily be configured to perform new functions — for example, using PAM to integrate fingerprint scanners with challenge-response password protection, or IPSec to build virtual private networks.

Having developed key technologies that drive the Internet, Solaris software is known for its maturity and scalability. For example, beginning with integrated TCP/IP networking in 1982, Solaris software's TCP/IP stack has been improved and refined over the years, eliminating many of the bugs that no doubt remain in less mature systems.

Sun's networking is multi-threaded, enabling more than one processor to prepare packets to be transmitted over local- and wide-area networks and increasing throughput for critical network-based systems. Indeed, the Solaris Operating Environment offers scalability that is unsurpassed in the industry. In addition to supporting Sun's own desktop and server products, the same versions of Solaris software also run on Intel Architecture systems. It is no surprise that organizations around the world are deploying their enterprise and Internet applications using the secure, scalable, end-to-end security solutions provided by the Solaris Operating Environment.

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303

1 (800) 786.7638
1.512.434.1511

http://www.sun.com/solaris/

January 2000