Security In the Solaris™ Operating Environment

The Solaris™ 8 Operating Environment delivers end-to-end security for business-critical enterprise applications and robust workgroup computing. Easily configured, flexible, and independently certified, security in the Solaris Operating Environment protects your systems and network from unauthorized access and other threats, helping keep your organization open for business.

THE SOLARIS OPERATING ENVIRONMENT

The Solaris 8 Operating Environment is the established OS leader for availability, scalability, and security in the Internet age. In Solaris 8 software, Sun delivers a trustworthy, universal platform to meet the needs of dot-com businesses – from small startups to large Fortune 1000 enterprises.

It's no surprise that the Solaris Operating Environment is the leading UNIX® environment today. Solaris software was originally designed with the Internet in mind. TCP/IP, the central Internet protocol, has been at the core of Solaris networking for more than 15 years. Through its time-tested design – a small, stable kernel, modular and extensible components, and well-defined interfaces – Solaris software delivers rock-solid stability and predictability for business-critical applications. And the Solaris 8 Operating Environment provides complete compatibility with prior versions, so you can be confident that your current applications will continue to run.

Firewalls

Firewalls control the data flow between two networks, according to security policy rules. The Solaris 8 Operating Environment offers built-in firewall functionality, with both the lite- and full-product versions.

- SunScreen™ Secure Net 3.1 is a full-featured firewall product that can be deployed throughout an organization to implement a secure business network including extranets, secure intranets, and remote access. It offers affordability, strong cryptography, centralized management, and high availability for screening and encryption.
- SunScreen™ 3.1 Lite is a firewall product designed to protect individual servers or very small workgroups. It is built from the same code as the full SunScreen Secure Net 3.1 product, provides high-speed, dynamic stateful packet-filtering, and includes a subset of the features offered with the full version.

Virtual Private Networks (VPNs)

VPNs represent a cost-effective means of using the Internet to communicate securely between two or more points. By encrypting and decrypting all traffic between VPN nodes, businesses can send private information securely over the Internet – unwanted users are unable to read or modify data. The Solaris Operating Environment supports both the Internet protocol security (IPSec), and Simple Key-Management for Internet Protocols (SKIP) technology for implementing and deploying VPNs.

IPSec

A key feature of the Solaris 8 Operating Environment security is the IPSec architecture. IPSec is an initiative to add security services to the IP protocol. It secures communication channels and ensures that only authorized parties can communicate on them.

Sun's implementation of IPSec in the Solaris 8 Operating Environment supports shared-secret encryption. 128-bit MD5 and SHA-1 algorithms are available for datagram authentication and integrity; 56-bit DES and 168-bit Triple DES algorithms are available for payload encryption. In addition, the Solaris platform also supports 'manual keying' today, and there are plans to support IKE functionality, which features automatic certificate exchanges and compatibility

- IPSec suite of communication channel security protocols
- Shared-secret and public-key encryption; 56-bit, 128-bit algorithms
- APIs that enable application-level specification of IPSec policies
- Pluggable authentication modules
- Smart card support
- Kerberos support for single sign-on
- Role-based access control
- Access control lists
- Interoperable with a broad range of server and processor offerings
- Advanced services offer enhanced integrity and security

with Public Key Infrastructure (PKI) products, in a future release.

IPSec is implemented following Internet Engineering Task Force (IETF) specifications, ensuring that servers running the Solaris Operating Environment will operate seamlessly with systems from other vendors adhering to IETF standards. And because the Solaris Operating Environment runs on both Sun SPARC™ processors and Intel Architecture-based platforms, you have the freedom to choose the platform that best suits your needs.

Solaris software includes APIs that enable application-level specification of IPSec policies, enabling your application developers to dictate security policies independently of system administrators. In addition, because IPSec operates at the Internet protocol (IP) level, you can use it to restrict access to applications that are not completely secure.

With these powerful capabilities, you can implement many security approaches in the Solaris 8 Operating Environment, such as:

- Restricting ISP Internet services so that only specific services are accessible to users.
- Securing communications between the tiers of multitier enterprise applications, so that even those with physical network access cannot view data they are not authorized to see.
- Establishing VPNs to enable remote offices and users to communicate securely over the Internet to the home office. An advantage of IPSec is that security arrangements can be handled without requiring changes to individual computers.

IPSEC AND SECURE SOCKETS LAYER (SSL)

To some extent IPSec and SSL are two approaches to the same problem of end-to-end authentication and encryption. However, the basic approaches are different.

- SSL implements its functionality above the kernel, and does not require any changes to the operating system. SSL operates on top of the TCP layer. Applications that want to use SSL must be rewritten to use this functionality. Virtually all leading Web browsers available today offer built-in SSL functionality.
- IPSec was designed to operate without requiring changes to an application or its APIs. IPSec operates below the TCP layer, and is transparent to the applications and their APIs.

IPSec is a very strong, network-level protocol. It can protect against a variety of threats, such as sniffing, spoofing, flooding, and hijacking. However, it blocks hosts that don't support it or otherwise have a security association with the initiating host. For Web traffic, where the majority of traffic does not require security of any kind, IPSec may need too much overhead. IPSec is well suited for VPNs and extranets.

SSL is well accepted and widely used on the Web. SSL offers better control over which security measures are used, and can automatically apply encryption and integrity protection to the data it carries.

SKIP

SKIP secures the network at the IP packet level – any networked application gains the benefits of encryption, without requiring modification. SKIP is unique in that it offers "on-the-fly" encryption. An Internet host can send an encrypted packet to another host without requiring a prior message exchange to set up a secure channel. Some of the advantages of SKIP include:

- No connection setup overhead.
- High-availability; encryption gateways that fail can reboot and resume decrypting packets instantly, without having to renegotiate existing connections.
- Allows unidirectional IP (for example, IP broadcast via satellite or cable).
- Scalable multicast key distribution.
- Gateways can be configured in parallel to perform instant failover.

STRONG USER AUTHENTICATION

In a business-critical environment, you need to ensure that only authorized users can access specific systems and services. Solaris 8 software provides a flexible set of facilities for strong user authentication that can be used out of the box or can be integrated into applications as service-specific security features.

SUN ENTERPRISE AUTHENTICATION MECHANISM™ 1.0 SOFTWARE

Sun Enterprise Authentication Mechanism software provides a distributed, enterprise-wide authentication mechanism for single sign-on

that reduces the number of times each user must go through a login sequence.

Sun Enterprise Authentication Mechanism software allows one computer to prove its identity to another across an insecure network through an exchange of encrypted messages. Once identity is verified, Sun Enterprise Authentication Mechanism software provides the two computers with encryption keys for a secure communication session.

Note that Kerberos clients are bundled with the Solaris 8 Operating Environment, and the Kerberos server is freely downloadable as part of the Solaris Admin Pack. Sun Enterprise Authentication Mechanism software may be purchased separately, for users of previous versions of the Solaris Operating Environment.

Pluggable Authentication Modules (PAMs)

PAMs provide a uniform means for third-party applications, as well as the Solaris Operating Environment itself, to access user authentication facilities. You can easily construct PAMs to support your site-specific authentication requirements (for example, an interface with a biometric scanning device such as a palm scanner for user identification).

As current authentication mechanisms evolve, and as new authentication mechanisms are introduced, system entry services such as login, rlogin, and telnet must continually be customized to incorporate these changes. However, with PAM framework, multiple authentication technologies can be added without changing any of the login services, thereby preserving existing system environments. PAM can be used to integrate login services with systems based on different authentication technologies, such as RSA, DCE, Kerberos, S/Key, or smart cards. Thus, PAM enables networked machines to seamlessly interact in an environment where multiple security mechanisms are in place.

Public Key Infrastructure (PKI)

PKI is an authentication mechanism that is used for verifying the identities of parties in Internet transactions. It can also be used for nonrepudiation purposes so that users can protect themselves in online transactions.

With a PKI, businesses can use an insecure public network, such as the Internet, to securely and privately exchange data. This is enabled through the use of a public and a private cryptographic pair that is obtained and shared through a trusted authority, commonly called certificate authority. The public key infrastructure provides for both a digital certificate that can identify individuals or organizations, and directory services that can store or revoke certificates.

Smart Card Support

Smart cards can offer a tremendous enhancement to your security architecture. Smart card functionality, including authentication, personal information storage, and Java™ applet management enable you to implement smart card solutions to your applications and business environment. The Solaris Operating Environment smart card feature implements the OCF 1.1 standard, and supports out-of-the-box support for smart card authentication at login. Smart cards provide basic public key infrastructure to manage user access; users are authenticated at login (using CDE), and when challenged by applications. The Solaris 8 Operating Environment supports three smart card features: Schlumberger Cyberflex Access Card, Dallas Semiconductor iButton (Java technology-based), and Schlumberger Micro Payflex.

Access Control

Besides UNIX permission mechanisms, the Solaris Operating Environment enhances access control through access control lists (ACLs) and role-based access control (RBAC).

Access Control Lists (ACLs)

ACLs provide a listing of users and their associated access rights, providing fine-grain access control for every file. File access can be controlled not only on a group basis, but also on a per-user basis. ACLs are implemented for both the Solaris User File System (UFS) and the Network File System (NFS), and adhere to the POSIX 1003.6 specification.

Role-Based Access Control (RBAC)

RBAC helps protect against vulnerabilities caused by human error. RBAC is an alternative to the traditional superuser model of root access to UNIX systems, with its “all-or-nothing” approach. RBAC lets you assign rights to individual, trusted users and delegate what specific operations they can

perform. This may include access to such resources as serial port, file, log, printer management, user login control, system shutdown, and the right to execute certain programs. Users are authenticated before any role is assumed so that all privileged activities can be logged and associated with a person. With RBAC, superuser functions are divided into multiple roles — root password access does not provide unlimited access to the system.

Auditing

Auditing helps system administrators track security-related events, including many different types of access attempts. If a violation occurs, an audit log can help determine the cause and source of problems. The Solaris platform includes two methods for auditing: UNIX system logs, and Controlled Access Protection Profile (CAPP) at Evaluation Assurance Level 4 (EAL4) auditing.

- UNIX system logs (syslog) keep track of login events, resource usage, quotas, and more. Many system facilities use syslogs to record or alert the system administrator to important events. Shell scripts or wrappers can also be written to syslog databases to cover specific situations.
- CAPP EAL4 auditing – previously called C2 auditing– can produce detailed audit reports by user, event, and class. In addition, with CAPP EAL4 it is possible to log any event that a system administrator deems security relevant. In the Solaris platform, CAPP EAL4 auditing includes the Basic Security Mode (BSM) functionality, which enables event logging down to the system call level.

Should a security infraction occur, the Solaris Operating Environment auditing capabilities ensure system administrators a detailed account of relevant activity.

Solaris Fingerprint Database

This SunSolve℠ service enables you to verify the integrity of files distributed with the Solaris Operating Environment, such as the /bin/su executable file, Solaris software patches, and unbundled products such as SPARC compilers.

Solaris Fingerprint Database ensures that you are using a true file in an official binary distribution, and not an altered version that can compromise system security. If you suspect someone has changed your system without your authorization, you can use the Solaris Fingerprint Database to check files for alteration or damage.

Sun Enterprise™ Network Security Service

Sun Enterprise Network Security Service is a flexible Java technology-based security solution that permits organizations to audit and secure their systems and networks in a modern, heterogeneous, corporate intranet. The software provides you with a network service daemon that should be installed on each host in your network; these daemons can then be linked together in a hierarchy of trust. This hierarchy may be used for the distribution and execution of digitally-signed packets containing Java, script, or binary code, which may be used to proactively check and fix host security issues in a bulk, batch-oriented manner. Execution requests are also digitally signed, replay attacks are prevented, and network communications are secured by ACLs, PAMs, and security modules.

Sun BluePrints™ Program

Due to the general nature of the Solaris Operating Environment, changes may be required in some environments in order to provide additional security against unauthorized access and modification. Sun BluePrints books are available that discuss the Solaris Operating Environment subsystems and related security issues.

Systems running Solaris software are also shipped with a wide variety of network services, most of which are activated by default. For security reasons, it is in the best interest of each system (and its owner) to have all nonessential services deactivated. Properly deactivated network services eliminate any current or future threat of system penetration, control, or disabling via the network service. The Solaris platform has a simple procedure to identify and disable a service determined to be unnecessary. For details, refer to the following Sun BluePrints books:

- *Solaris Operating Environment Minimization for Security: A Simple, Reproducible, and Secure Application Installation Methodology*
- *Solaris Operating Environment Security*
- *Solaris Operating Environment Network Settings for Security*

INTEGRATED, END-TO-END SECURITY

In today's Internet age, "anytime, anywhere" access to information, electronic commerce, Web-based applications, and other mission-critical solutions creates new challenges for the data center when it comes to ensuring privacy and limiting the enterprise's exposure to business risks. The Solaris 8 Operating Environment provides integrated features that deliver the end-to-end security you need in order to safely deploy these powerful new solutions in your complex enterprise computing environment -- whether you need the agility of a dot-com startup, the predictability of a business-critical application, or both.

FOR MORE INFORMATION

To learn more about security and the Solaris Operating Environment, please visit our Web site at www.sun.com/security.