Solaris™ 10 Operating System — Unparalleled Security to Enable and Protect Business

A Technical White Paper
September 2004

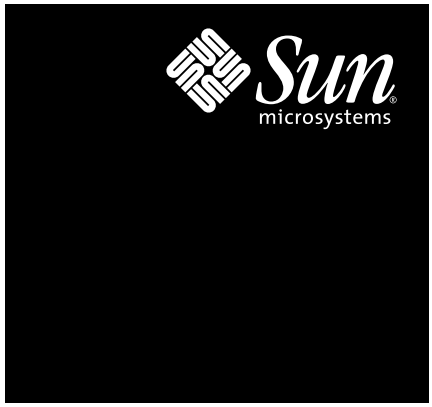

Table of Contents

Chapter 1
Introduction

The days of the enterprise as a castle — with deep moats and high, thick walls to protect assets from the attack of marauding invaders — are long gone. Business operations as a lone, well-protected structure with a single, guarded gateway in and out — both literally and figuratively — is no longer a viable model. Now it seems like everyone and everything is connected to the network. Businesses may have thousands — even millions — of employees, partners, suppliers, and customers accessing information and services from homes, hotels, and customer locations. Increasing connectivity is improving productivity.

Connectivity and access create conflicts and challenges that must be addressed by an environment capable of delivering comprehensive protection. To operate safely in a connected world, businesses need to secure their enterprise, with all of the systems, networks, applications, technologies, and users that make it work. How well an enterprise has deployed and integrated security into its network can be a significant contributor to its overall productivity. But security is not an object, nor is it simply a list of features. Security is an ongoing discipline that monitors what's happening — in an organization and out in the world — and applies this knowledge to the development and safe deployment of IT resources.

At Sun, this is a lifestyle that we have embraced for more than 20 years. Many Sun products are independently verified for their security capabilities, while Sun personnel help to drive the new standards-based capabilities in their work through the Internet Engineering Task Force (IETF). This work comes together in the Solaris™ 10 Operating System (OS). The Solaris 10 OS provides comprehensive, in-depth security capable of protecting the enterprise at multiple levels. It offers a new level of security, enabling today's enterprises to safely increase access to key computer systems by their business partners for around-the-clock commerce.

Overview

Security not only protects business assets, it also contributes to availability by reducing unplanned downtime caused by security compromises. Integrated, dynamic business operations demand flexible, accountable security models that span the globe while still preserving individual and business rights. Any solution needs to consider the speed at which new customers, suppliers, and partners are added or removed, as well as new government mandates such as the Health Information Portability and Accountability Act (HIPAA), Sarbanes-Oxley, and the European Union (EU) Directive on Data Protection Act.

Security-enabled business operations need protection at many levels — integrated into the IT fabric, not layered on top of everything. Access to IT resources needs to be very situation and role specific — users should get to use only the information and services they need to perform their jobs. Assets are protected from unauthorized use. Data, network traffic, and user information are protected as needed. There is protection at the edge, and additional protective mechanisms inside the intranet. Systems and processes are monitored. If a system should be compromised, it should not enable widespread access. Security systems should be safe, right out of the box, and easily and quickly updated.

Sun and the Solaris 10 OS provide all this and more. The Solaris 10 OS is the foundation for safe IT operations in a global marketplace.

Chapter 2
Solaris 10 OS Security Highlights

Identity Management

Scenario — Poor Password Management

Company X had no formal password management to speak of. Employees could choose their own passwords — often a first name, sometimes with a number after it — and were never required to change them. Inevitably, a security breach happened: A salary and bonus report was posted to an external Web site. Subsequent analysis showed the same name/password pair was used around the company, sometimes simultaneously from four different places. The user account belonged to a manager who had left the company three months earlier. Other name/password pairs also showed signs of multiple users per account, indicating that users had shared their login information with others.

Passwords are considered the first line of defense in security. The Solaris 10 Operating System improves password protection by enforcing limits on how long they can be used, how frequently they can be reused, and the number of login attempts allowed. Passwords can be checked against a database of forbidden text strings — employee names, for example. Policies on their length, mixing of letters and numbers, and so on can be enforced. Many password encryption mechanisms ship with the Solaris OS, including MD5, Blowfish, and DES. Solaris software also supports an extensible mechanism that extends the way passwords are checked and validated. Through the Pluggable Authentication Module (PAM) architecture, customers can customize password security to fit unique requirements by changing their password encryption mechanism. While representing a strong first line of defense, passwords are part of an overall identity management solution.

Identity-Enabled Computing

It is challenging to give employees, partners, and suppliers safe and easy access to the information they need to be productive. In a dynamic business environment, how does an organization cost-effectively manage secure access to IT resources?

It starts with comprehensive password management at the point of first contact and continues with Kerberos-enabled single sign-on (SSO) and LDAP authentication to deliver secure single sign-on capabilities across multiple operating systems. End-to-end identity management solutions can be achieved by integrating the computing infrastructure with the Sun Java™ Enterprise System security products.

User identity attributes are often stored in many different places and formats within a company. There is no single authoritative source where user access privilege and profile information can be store and retrieved. In fact, there are many reasons why it is not practical to consolidate such information — lack of trust, incomplete technology, dubious cost-effectiveness, giving up organizational control, and so on. For these reasons and more, Sun provides single sign-on capabilities throughout corporate intranets, using the Kerberos standards as well as userID/password management, through a nonintrusive concept called federated identity management that integrates the management of distributed data stores while leaving identity information in its native locations. When combined with state-of-the-art techniques for the management of access privileges and entitlements, a federated identity management network enables a company to integrate its disparate business operations. By doing so, the benefits that can be leveraged include increased revenues, reduced costs, and gaining a massive competitive edge.

Sun's identity management suite provides current, consistent, and accurate identity information within and across enterprise boundaries. Sun identity management products — Java System Directory Server Enterprise Edition, Java System Access Manager, and Java System Identity Manager — provide a complete solution that replaces manual methods with automated, flexible, rules-driven processes. The Solaris 10 OS includes enhanced identity management with centralized management capabilities.

1. Secure LDAP authentication enables user names, passwords, network configuration, home directories, and other common identity attributes to be centrally stored in the included enterprise-class LDAP directory server. Sun includes a license for 200,000 user entries of the Java System Directory Server for exactly this purpose. UserIDs and passwords are protected while on the network using military-strength, SSL-encrypted communications; when stored in the LDAP directory, similar strong encryption is used.
2. The LDAP authentication methods have been enhanced to utilize the Generic Security Services API (GSS-API) and Simple Authentication and Security Layer (SASL), two standards for flexible authentication mechanisms. This provides interoperability with Kerberos and improved interoperability with Microsoft Active Directory. The Solaris 10 OS implements open, interoperable standards that enable secure enterprise-wide administration of computing infrastructures.
3. Sun Enterprise Authentication Mechanism™ (SEAM) software implements the Kerberos v5 standards. Interoperability with Microsoft Active Directory and other Kerberos single sign-on systems is easily achieved. The result is increased security and reduced costs by centralizing the management of user identities.
4. Remote access and file sharing commands, such as Telnet, `rcp`, `rsh`, `rlogin`, and NFS, are enhanced in the Solaris 10 OS to interoperate with Sun Enterprise Authentication Mechanism and Kerberos v5 systems. Users' enterprise identity is securely carried with them throughout their remote access and file sharing uses.

All together, identity-enabled computing provides visibility and control over access to corporate assets as they are shared across the entire value chain.

Authentication

Scenario —Too Many Passwords and Too Much Power

Organization Y has seven large systems, though most people need access to only four: Their department's main system, e-mail server, company portal server, and remote access system. The management team takes security seriously and enforces a policy that requires a different password for each system, which must be renewed every 60 days. Passwords have to be at least eight characters and cannot contain real words. Many people have been granted superuser access to the system in order to manage privileged operations such as print queue administration. Despite — or perhaps because of — all this, 300 MB of unlicensed music files were posted on the portal server, and analysis showed they were accessed more than 5000 times. It's hard to pin down exactly where the passwords were compromised — when a PDA fell out of a coat pocket at the airport or when any of the printouts used by many employees to record passwords fell into the trash, which the cleaning crew delivered to the dumpster.

Who You Are and What You Can Do

A single sign-on facility is a partial and well-known solution to the problem of multiple passwords. Unfortunately, people in general are not very good at remembering good passwords, such as those containing upper and lower case characters, mixes of letters and numbers, and so on — especially if they have to change them frequently. And if a single sign-on password is compromised (lost or stolen), then the new user has access to everything allowed for that user account.

Smart cards, including the Java Card™ platform, when coupled with passwords ensure that the people using the system are who they say they are. Using multifactor authentication (something known, such as a PIN, and something you possess, such as a one-time password generator or digital certificate) provides an extremely high degree of certainty that a user is authentic. This enables enterprises to create an IT environment that enables employees to work anywhere — floating offices, in the field, or at home.

The Solaris OS supports many smart card APIs, including the Java Card platform, Solaris Smart Card Framework, MUSCLECard open source IFD drivers, PKCS #11, and PC/SC Lite smart cards. Strong authentication can be enabled through built-in smart card interfaces or virtually all of the USB-enabled smart card readers.

Once a user is authenticated, granting access privileges is the next step. Users should have access only to the applications (and in some cases, only some features within an application) they need according to the role they serve within the organization. The Solaris 10 OS supports Solaris User Rights Management, which covers individuals and groups, and restricts access to selected applications and other Solaris 10 OS functions. This increases security by reducing the chances of administrative errors or accidental/malicious use of IT resources. Using the Solaris Role-Based Access Control capabilities of Solaris User Rights Management, privileged users can be granted just the capabilities needed to run a select number of commands consistent with their needs rather than being granted full superuser access to the system. Solaris Role-Based Access Control information is centrally managed for reduced administration cost and increased flexibility for rapidly changing business requirements. Effective security reduces downtime, raises quality of service, and keeps costs low.

Containment

Scenario — Hacker Attack

Company Z thought it was doing everything right. Management used a firewall to protect their network infrastructure, and passwords were secured using MD5 encryption. Still, a determined hacker sent a request for information to the Webmaster and took note of the IP addresses contained in the return message header. A few days' worth of traffic was collected, analyzed by the hacker, and a simple exploit to the company's Web server was found. After a few minutes, the hacker was in. Once past the firewall and into the main network, there was very little additional security. It only took a little more time and effort to get what he wanted: The credit card database.

Sometimes, even when nearly everything conceivable is done, hackers get through. The Solaris 10 OS offers strong perimeter protection, making it very difficult to break through the firewall. If hackers do penetrate it, in-depth protection and containment help limit any potential damage. The Solaris 10 OS offers many ways to protect systems from break-ins, and to contain them if such events do occur.

1. The built-in stateful Solaris IP Filter firewall controls interaction of services on the network. Solaris IP Filter firewall can control access to IP services not only at the gateway, but also to systems inside the firewall. Solaris IP Filter firewall is fully supported by Sun.
2. Solaris Containers (formerly N1™ Grid Containers) technology offers a way to virtualize system resources and use multiple software partitions within one instance of the operating system. By providing a virtual, security-isolated instance of the Solaris OS — including separate IP addresses and root passwords — where applications can be run, it isolates the application and other associated resources and hides system details. This powerful capability enables businesses to consolidate resources without compromising security. It is now possible to host multiple, competing customer or supplier applications on the same system while isolating each set of processes from the others.
3. Solaris Process Rights Management, enabled through Solaris Privileges, provides fine-grained control of the security of services and applications, increasing security and helping prevent them from being used to compromise a system or the data within it. Privileges assigned to processes are restricted only to those necessary to perform its function, reducing exposure to security exploits. This limits what processes can do, regardless of the user — unprivileged processes cannot do damage to the overall system. System administrators can deploy Solaris Process Rights Management to existing applications without modifying any code, and user retraining is not required.

Chapter 3
Solaris 10 OS Security Technology

The Solaris 10 Operating System offers superior security that helps to protect an IT infrastructure from the moment the software is installed. This release contains many new features and capabilities, extending Sun's proven history of delivering the protection enterprises need.

System-Level Security

Enhanced Security at Installation

The Solaris 10 OS offers unparalleled built-in security. For administrators who want to customize their installation, the Solaris 10 OS offers the Reduced Networking metacluster — the smallest, most secure install of Solaris software to date. In the near future, the Solaris 10 OS is scheduled to feature a new Services Management Infrastructure and add enhanced security settings as an install-time choice. When customers choose the enhanced security settings, Solaris 10 software protects the system from attack and misuse by disabling many commonly unused services. The system helps ensure usability by enabling local-only access to many other useful services, such as the GNOME or CDE desktop. For administrators who want protection during remote installations, the Solaris 10 OS features the SSL-encrypted WAN boot capability. Administration costs can be reduced and security enhanced by enabling centralized installation of remote systems.

Easier Implementation of Best Practices

The Solaris Security Toolkit is based on best practices in the real world and was created as part of the Sun BluePrints™ program. Informally known as the JumpStart™ Architecture and Security Scripts (JASS) Toolkit, it provides a flexible and extensible mechanism to minimize, harden, and secure Solaris OS systems according to the server's function. It is based on the best practices of thousands of customer installations by Sun Services, and the resulting systems are also supported by Sun Services.

The Trusted Solaris™ OS: For Government and Commercial Use

Once designed only for government use, the Trusted Solaris™ OS is being embraced by commercial organizations as well. It separates users, data, and resources, specifically granting access from users and processes. Elimination of the superuser and dividing these functions into multiple roles makes system penetration far more difficult. A combination of labeling all objects, clearance levels for each user, and strong audit capabilities makes all users accountable and all actions traceable, greatly diminishing the risk of security violations. Trojan horses, such as programs to intercept passwords or other sensitive data, are prevented by a graphical user interface and protocol. Mandatory Access Controls enforce a hierarchical compartmentalization of information, protecting sensitive information from general use.

Common Criteria certification represents Sun's commitment to the highest levels of security. Sun's longstanding practice of independently validating the security of the Solaris OS continues forward into Solaris 10 and Trusted Solaris software. The Solaris 10 OS is targeted at Controlled Access Protection Profile (CAPP) and Role-Based Access Control Protection Profile (RBACPP) at Evaluation Assurance Level 4+ (EAL 4+). The Trusted Solaris OS is the only enterprise-class OS that has been independently certified under Common Criteria Evaluation Assurance Level 4+ (EAL 4+) with three critical protection profiles: Labeled Security Protection Profile (LSPP), Controlled Access Protection Profile (CAPP), and Role-Based Access Control Protection Profile (RBACPP). All in all, it delivers proven protection.

Prevention of Stack Buffer Overflow Exploits

Stack buffer overflows enable many types of attacks. The Solaris 10 OS provides protection against exploits arising from stack buffer overflows with all 64-bit applications, and optionally for all 32-bit applications, through a simple configuration setting. Core system administration utilities also provide this protection by default. ISVs and corporate developers can link into designated libraries, protecting their application. This functionality is available for SPARC® and AMD64 processors, and unavailable on any operating system running on the Intel IA-32 platform due to limitations in the architecture of these CPUs.

Automated Patch Management

As new threats appear, Sun is committed to providing the tools and updates customers need to protect their systems. Solaris Patch Manager automatically gets the right patch for each system in the form of digitally-signed (verified) .jar files. Patches can be pushed to multiple servers and installed as required. Automated patch management enables administrators to be more productive and helps maintain systems at the highest levels of protection.

Accountability

Auditing

The ability to track what's happened on a system is a cornerstone of strong security as well as a regulatory and liability requirement. Auditing monitors system configuration changes and user activity, and watches for malicious behavior.

1. **File Integrity.** New in the Solaris 10 OS is the Solaris Basic Audit and Reporting Tool (BART). BART enables customers to generate digital signatures of files and attributes to those files, and compare them over time to check for changes.

2. **System-Level Files and Executables.** The Solaris Fingerprint Database (sfpDB) is used to verify that a file or executable has not been changed from an official binary distribution; an altered version may compromise system security and cause other types of problems. It compares an MD5 digital fingerprint with the trusted entry stored in the sfpDB and instantly identifies mismatches. This tool is accessed through a free Web interface located on the SunSolvesm Web site at sunsolve.sun.com.

   Sun also delivers digitally signed executables, binaries, and drivers for almost all of the Solaris 10 OS. Initially, system administrators can manually verify that an executable has not been modified or hacked. Administrators may also sign and verify their own in-house code or third-party executables as well. In a future update of the Solaris 10 OS, the system kernel itself will be able to dynamically verify the integrity of these files at run time, thus ensuring a high-integrity computing environment.

3. **Auditing Tools.** Solaris auditing tools track kernel, application, and user activity with fine-grained control. Solaris audit trails can be stored on a centralized system for later analysis. Administrators can continuously monitor and verify virtually any file or executable to check for changes.

Together, any file can be watched and alerts generated if there are changes. File and executable integrity can be maintained.

Secure Communication

Ensuring private data connections is the foundation of network-based business. The Solaris OS provides many different mechanisms to secure network traffic. Secure communication products now use the Solaris Cryptographic Framework, which delivers an across-the-board performance improvement of 15–130 percent.

1. IPSec provides a strong, standards-based framework for securing TCP data communication. Internet Key Exchange (IKE) manages the necessary encryption/decryption keys. IPSec/IKE can secure almost any protocol without changing the application in both IPv4 and IPv6 environments. Strong encryption is supplied by DES, 3DES, AES, and Blowfish, with support for X.509 certificates.

2. Solaris Secure Shell encrypts remote sessions, verifies both users and hosts, and hides passwords over the network. This latest version features enhanced encryption support and integrates with Kerberos authentication for enterprise single sign-on use.

3. OpenSSL, an open source set of libraries for secured Web transactions, is integrated with the Solaris Cryptographic Framework in the Solaris 10 OS. It delivers high-performance cryptographic algorithms and transparent hardware acceleration, improving throughput to secure Web servers. Out-of-the-box support for encrypted Web pages from an Apache Web server is also included in the Solaris 10 OS.

4. TCP Wrapper support enables administrators to grant access to specific services based on a domain name, for example, allowing FTP file transfer and SMTP e-mail access to everyone in engineering while denying access to sales and manufacturing. By selectively providing services to just those systems that need it, risk is reduced while availability is increased.

5. Solaris Enterprise Authentication Mechanism (SEAM) software provides strongly authenticated and encrypted file sharing through the NFS standard. This prevents rogue system administrators from inappropriately accessing individual data via the network file server. Solaris Enterprise Authentication Mechanism software in the Solaris 10 OS utilizes the Solaris Cryptographic Framework for strong, accelerated 3DES and AES Kerberos sessions.

Chapter 4

Strong Security in Your Enterprise

Your business and its employees, management, partners, and suppliers depend on well-implemented security. Beyond protecting intellectual property and preventing misuse of systems, security helps maintain availability and service levels.

How can you protect your enterprise? Work toward a goal of applying security pervasively and in depth — to every node, every device, every user, every IT asset, and every resource. Create and enforce an enterprise security policy that represents a coherent and comprehensive security architecture, and ensure that all devices and users conform to it.

Sun and the Solaris Operating System assist companies in achieving the secure enterprise, with products and technologies that have security designed and defined from the outset and provide protection by default. Strong, intrinsic security enables business commerce, reduces unplanned downtime, and increases services levels.

Sun has helped thousands of organizations with security assessment, planning, deployment, and support. Contact your Sun representative for more information on any of these services.

Security is a moving target, and Sun continues to invest. The Solaris 10 OS is the best example yet of our commitment.

More Information

Sun Security Information	
Sun Security Home Page	• sun.com/security
Solaris OS Security	• sun.com/solaris • sun.com/security/jass
Trusted Solaris OS	• sun.com/solaris/trustedsolaris
Java Platform Security	• java.sun.com/security
Network and Security Products	• sun.com/servers/entry/checkpoint • sun.com/networking
Solaris OS Patches and Fingerprint Database	• sunsolve.sun.com
Sun Security Coordination Team	• sunsolve.sun.com/security
Sun BluePrints for Security	• sun.com/blueprints • sun.com/software/security/blueprints

Sun Security Information

Sun Consulting Security Services	• sun.com/service/sunps/security
Sun Education Security Services	• suned.sun.com/US/catalog
Sun Support Services	• sun.com/service/support

Additional Security Resources on the Web

Network and Security Products	• humanfirewall.org
Generally Accepted System Security Principles (GASSP)	• web.mit.edu/security/www/gassp1.html
NSA INFOSEC Assessment Methodology	• certtest.com/nsa-iam.html
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)	• cert.org/octave

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** sun.com

The Network is the Computer™

Sun Worldwide Sales Offices: Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323 Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45 4556 5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0 Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India–Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-697-8111, Ireland +353-1-8055-666, Israel +972-9-9710500 Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +822-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100 The Netherlands +00-31-33-45-15-000, New Zealand–Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47 23 36 96 00, People's Republic of China–Beijing +86-10-6803-5588; Chengdu +86-28-619-9333 Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Saudi Arabia +9661 273 4567, Singapore +65-6438-1888 Slovak Republic +421-2-4342-94-85, South Africa +27 11 256-6300, Spain +34-91-767-6000, Sweden +46-8-631-10-00, Switzerland–German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888 Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44-1-276-20444, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800, or online at sun.com/store