ORACLE
SOLARIS

An Oracle White Paper
August 2010

Using Oracle® Solaris 10 to Overcome Security Challenges

ORACLE

Introduction

In today's hyper-connected economy, organizations of every kind and size depend on networked computing systems to conduct business. This reliance on computing systems can leave organizations vulnerable to a wide variety of potential cyber attacks. Over time, hackers have honed sophisticated methods for gaining access to systems, applications, and data. These methods can include network attacks, code attacks, and social engineering, and can originate from within the organization itself, or from anywhere around the globe. Indeed, IT staff may not even be aware that their systems have been compromised. As a result, security is foremost in the minds of IT managers, with most assuming the IT infrastructure is a target for attacks and other security threats.

In addition to concerns over intrusions, IT managers must be able to meet requirements for security, privacy, and internal auditing that are being imposed worldwide. Some examples include legislation such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Sarbanes-Oxley Act of 2002 in the U.S, and the European Union Data Protection Directive of 1995 in Europe. Regulatory oversight requires that data, applications, and systems be properly secured. Proper audit controls and other procedures must be instituted to safeguard identities and data. HIPAA privacy rules require appropriate measures to protect the privacy of personal health information and set limits and conditions on the uses and disclosures that may be made of such information.

The security enhancements in Oracle® Solaris 10 make it attractive to organizations that require comprehensive system security features. IT departments seeking an effective and efficient solution to computer security can take advantage of these unique and powerful features to protect the enterprise from potential threats, comply with corporate and regulatory requirements, and stay ahead of daunting security challenges.

Security Features in Oracle Solaris 10

Oracle Solaris 10 is a robust, premier enterprise operating system that offers proven security features. With a sophisticated network-wide security system that controls the way users access files, protect system databases, and use system resources, Oracle Solaris 10 addresses security needs at every layer. While traditional operating systems can contain inherent security weaknesses, Oracle Solaris 10 facilitates new approaches to protect the entire compute environment from the datacenter, through the network, and to the desktop. Following is a discussion of key security approaches and how administrators can utilize Oracle Solaris 10 to implement greater enterprise-wide safety measures.

Reduce and Securely Delegate Privileges

Most operating systems require applications that need to perform privileged operations to run as the root user, making the application all-powerful. In this case, any vulnerability in the application can be exploited by hackers to escalate their privileges, take over the system, damage data, or even conduct a zombie attack.

Another approach used by some Linux distributions is to constrain applications using the Security-Enhanced Linux policy. Implementing this policy can be quite complex and typically requires vast quantities of policy code in order to get commercial applications to run. In addition, modifications to policy files can require full system reboots, making it more difficult to implement and administer Linux systems[1].

Process Rights Management

Oracle Solaris 10 adopts a different approach, utilizing the principle of least privilege. Over 65 discrete, fine-grained privileges are built into the kernel and user access space. The concept of privileges as implemented in Oracle Solaris 10 is extended throughout the operating system — even the built-in tools take these rights and privileges into account. Using this approach, administrators can grant new or existing applications only the appropriate privileges necessary to perform tasks. Many system components such as NFS, the Oracle Solaris Cryptographic Framework, IP Filter, file system mount commands, and more, are already configured to run with reduced privileges by default, with no configuration required by the administrator.

Implementing privileges is a simple task and requires an amendment to a policy file for most typical applications[2]. Oracle Solaris 10 also invokes the proper privileges for an application service when started by the service management facility (SMF) in Oracle Solaris. As a result, the application does not

[1] See the Security-Enhanced Linux Users Guide at http://docs.fedoraproject.org/en-US/Fedora/13/html/Security-Enhanced_Linux/

[2] See http://docs.sun.com/app/docs/doc/835-8005/6ruu381qp? for more information.

need to be modified, and is not granted unlimited system access. The system or security administrator can determine which privileges to grant or deny to the application, tightening security and eliminating the need for extensive coding changes. This approach helps to prevent the hacking of applications that are running with super user privileges, yet maintains full compatibility with existing applications.

For example, Web server applications typically run as `root` in order to bind to port 80 on the system, which is a privileged port. Oracle Solaris 10 contains a special privilege, `net_privaddr` that can be granted to the Web server application in order to be able to bind to the privileged port 80, as illustrated in Figure 1. When the Web server application starts, the Oracle Solaris 10 kernel checks for Process Rights Management attributes, finds the `net_privaddr` privilege, and starts the server without `root` or superuser access.

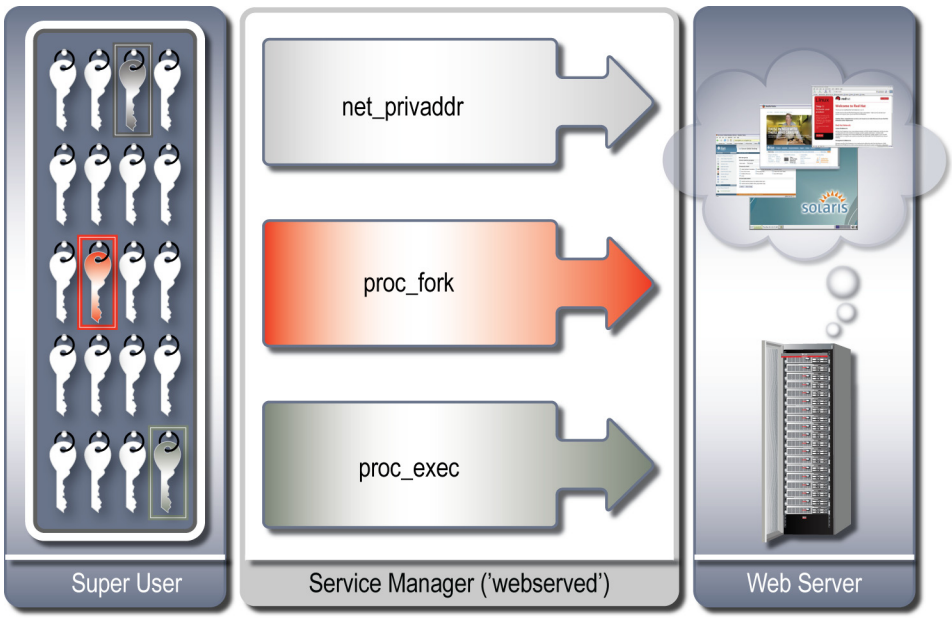

Figure 1. Process Rights Management can be used to set privileges that restrict the access rights of applications.

User Rights Management

System administrators frequently are faced with the need to limit access to administrative functions while being able to delegate certain specific privileged operations at the same time. Much like Process Rights Management, User Rights Management gives administrators the ability to grant or deny privileges to individual users in order to let them perform some privileged operations without needing to give them full superuser powers. Also known as Role-Based Access Control, User Rights Management lets administrators create roles for users. Each role has a set of profiles that determine what tasks and commands the role can perform, and the privileges, or process rights, with which the commands run. Oracle Solaris 10 includes a number of standard pre-defined profiles that can be combined into roles. Administrators also can create customized per-site role definitions as needed, and are not limited by the Oracle Solaris concept of system administration. By utilizing roles, administrators

can delegate specific operations to different users on the system and grant only the privileges required to accomplish those operations.

There is an additional layer of security built into the user roles functionality. Roles are assigned to specific users and each user must log in to his or her own user ID and then assume the role they have been granted. As a result, users are never logging into a given role anonymously, and system administrators can always see who did what where, when, and how on the system. For example, administrators can define a Web server administrator role and apply it to those users that need to be able to perform Web server administrative tasks without being the superuser. Role definitions can be stored in a naming service such as NIS, NIS+ or LDAP to allow administration of Web servers on any system within the network. Any other administrative access to the server is not allowed. Figure 2 illustrates the use of roles to grant specific administrative privileges needed for users to complete certain tasks. With support for a centralized repository, roles and profiles can be changed centrally and then automatically propagated throughout the enterprise.

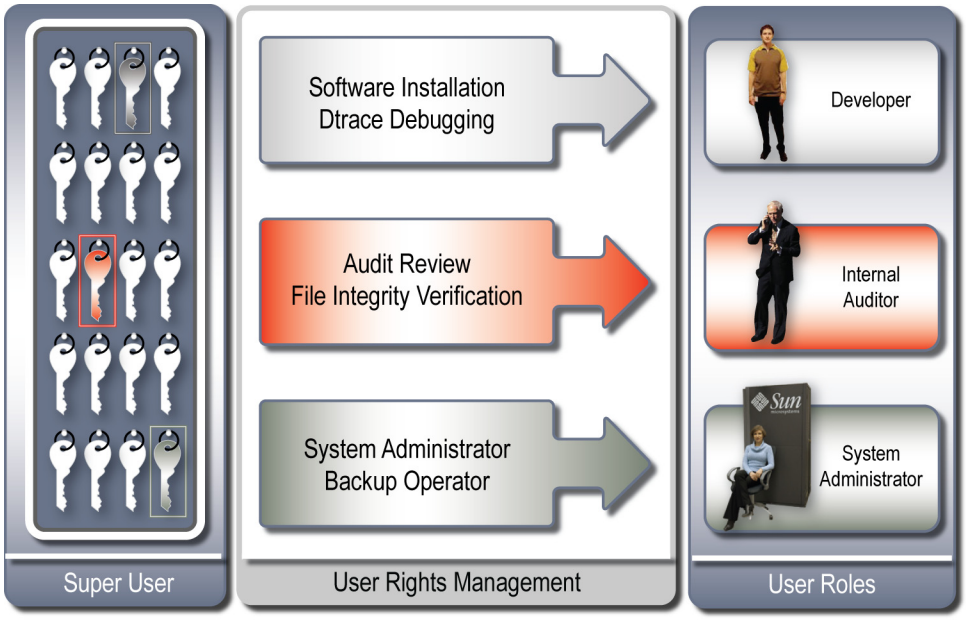

Figure 2. Using roles grants certain administrative privileges for specific tasks without `root` or superuser access.

Network Security and Encryption

Remote access to systems is vital. Administrators frequently need to be able to administer systems remotely, and users often require the ability to log onto servers from other locations. Typically, any system that provides remote capabilities offers a means for intruders to gain access. Network services, such as Telnet, FTP, file sharing, or even interactive user accounts, pose potential security risks for enterprises if they are not administered carefully. In addition, regulations typically require that communications, even when self-contained within the datacenter, be encrypted in the event that data is confidential or sensitive. Oracle Solaris 10 offers a number of features that can help administrators secure systems from intruders and comply with regulatory or corporate requirements.

Securing the Default Networking Configuration at Install Time

There are a number of services in UNIX® operating systems that are configured to listen for external network connections when the system is first booted after installation. These services can present security holes, particularly if an administrator is unaware of a specific service functionality. Oracle Solaris 10 offers a choice of Secure by Default Networking during the installation, which changes the state of these services so that they can only communicate with other processes on the same system by default. When configured this way, the only service that can be accessed from outside the system is the secure shell service in Oracle Solaris. However, Oracle Solaris 10 can still be used to connect to external services such as mail, print, and file sharing services, and runs with a fully functional administrative and interactive desktop interface. Any of these services can be turned on for internet listening or be disabled completely. This approach is far more secure and resource efficient than merely placing a firewall on the system.

IP Packet Filtering Firewall

Every company uses firewalls to protect internal IT infrastructure from network-based attacks. Oracle Solaris 10 integrates an IP packet filtering firewall within the TCP/IP stack. Providing stateful packet filtering and network address translation (NAT), the IP Filter firewall also includes the ability to create and manage address pools. A popular choice for Oracle Solaris administrators, the IP Filter can filter by IP address, port, protocol, network interface, and traffic direction, as well as by an individual source IP address, a destination IP address, a range of IP addresses, and more. Security administrators gain a high degree of control and can block specific internet addresses that may be part of an organized attempt to gain access to the system. Support for both IP4 and IP6 addressing makes it possible for administrators to deploy the firewall with existing or emerging new generation networks.

TCP Wrappers

Controlling access to network services is one of the most important security tasks facing a server administrator. TCP wrappers add an additional layer of protection by defining which hosts are allowed to connect to *wrapped* network services. Oracle Solaris 10 contains integrated TCP wrappers, making it possible to restrict access to TCP services based on domain name, host name, IP address, network address, and more. For example, administrators can set up an FTP service for addresses of a newly-acquired company (*.foo.com). Any system attempting to access the FTP service from within the *.foo.com domain can be granted access. In addition, TCP wrappers provide access control to a host and service depending on the origin of the request, and log both successful and unsuccessful connections to that host.

Integrated Cryptographic Framework and Key Management Framework

The increasingly distributed nature of computing resources necessitates the use of encryption and decryption operations, even where they were once considered impractical. Often under-utilized due to the system overhead it can generate, encryption is vital along with security standards and new regulations requiring greater use of encryption key factors. The cryptographic framework in Oracle Solaris provides a set of kernel-level and user-level cryptographic services, and includes several

software encryption modules for applications to offload cryptographic operations. The cryptographic framework provides access to the best available hardware or software encryption modules on the system without any configuration or customizing of the application. A standard feature of the operating system, the cryptographic framework is not a set of add-ons that must be installed later, nor does it incur any additional fees in order to be able to use it. Figure 3 shows the cryptographic framework.

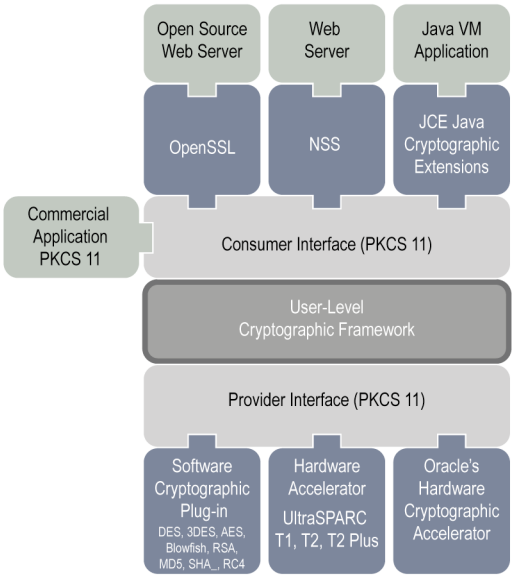

Figure 3. The standards-based cryptographic framework in Oracle Solaris.

Based on the PKCS#11 cryptography standard created by RSA Security, Inc, the cryptographic framework provides a consistent framework for application-level and kernel-level cryptographic operations. This framework gives applications access to the same hardware accelerators used by the operating system kernel and provides a mechanism and API by which both kernel- and user-based cryptographic functions can be executed by the same optimized encryption software or transparently use hardware accelerators configured on the system. The cryptographic framework helps to increase security and performance and brings the power of advanced, streamlined encryption algorithms and hardware acceleration to user-level C and Java programming language-based applications.

Oracle offers servers with built-in cryptographic acceleration hardware technology that speeds the process of encrypting and decrypting data. Indeed, many system services in Oracle Solaris, such as IPSec/IKE and Kerberos authentication, take advantage of the cryptographic framework and automatically utilize the hardware acceleration that is provided by the server hardware. Running Oracle Solaris on these servers can help to reduce system overhead, improve performance, and increase overall computing and network efficiency by improving responsiveness across the entire solution.

- **Oracle servers with CoolThreads Technology.** Running applications such as the JD Edwards Web server on Oracle servers with CoolThreads technology lets companies leverage on-chip

cryptographic acceleration and eliminates the need for additional co-processor cards, special licensing, network appliances, or power hungry add-on components.

- **Oracle x86 and x64 servers.** Enhancements for chip-based acceleration are incorporated on the latest Oracle x86 and x64 servers[3]. These servers contain Intel® Xeon® processors incorporating new hardware instructions that directly implement the Advanced Encryption Standard (AES) cryptographic algorithm within the hardware. This implementation provides significant performance improvements over the previous hand-coded machine language implementation.

For more information, see *http://wikis.sun.com/display/BluePrints/Taking+Advantage+of+Wire-Speed+Cryptography*.

IPSec/IKE

Many organizations utilize virtual private networks (VPNs) to provide remote users and locations with secure access to an organization's internal network. Deployed over public telecommunication infrastructure, VPNs offer a cost-effective alternative to leased lines, but present security challenges because of the use of public networks. In order to be secure, corporate data traveling over VPNs requires a protected communications channel. Internet Protocol Security and Internet Key Exchange (IPSec/IKE) is the technology used to implement secure communications over VPNs. Providing application-independent encryption, IPSec/IKE encrypts data as it leaves the system.

Oracle Solaris 10 incorporates standards-based IPSec/IKE encryption and can interoperate with other operating systems, including Windows, Linux, and HP-UX. Applications do not need to be modified, as data encryption occurs in the network stack, away from the knowledge of the application itself. Performance can be accelerated automatically if the systems connected through the VPNs are Oracle servers with CoolThreads technology, Oracle servers with Intel processors, or any system with a cryptographic accelerator card (either an Oracle's Sun Cryptographic Accelerator 6000 PCIe Adapter, or third-party accelerator with an Oracle Solaris plug-in).

The Secure Shell Service in Oracle Solaris

Administrators often need to maintain networked systems located in a variety of disparate locations. Using a shell, administrative staff can login to systems no matter where they are located—in another building, around the globe, outside the organizational intranet, in the cloud, or at a customer site. However, logging into and maintaining systems over an insecure network such as the internet leaves corporate data security and enterprise network integrity vulnerable.

The Secure Shell service in Oracle Solaris allows data to be exchanged over a secure channel between two networked systems. It replaces telnet and other insecure protocols that transmit sensitive data such

[3] http://blogs.sun.com/bigadmin/entry/how_to_optimize_oracle_solaris

as passwords in plain text, leaving communications vulnerable to packet analysis. Providing a way to protect against a number of network threats such as session eavesdropping, password theft or misuse, and session hijacking, the Secure Shell encrypts all network traffic, delivers stronger authentication, and monitors the integrity of network sessions. Because it is integrated into the Oracle Solaris 10 operating system, the Secure Shell environment can leverage the cryptographic framework in Oracle Solaris for even greater security.

Password Management

Password management can be a headache for system administrators. It can be difficult to ensure that passwords are not getting stale, being passed around, or accidentally given out. In addition, users are notorious for leaving written passwords in work areas and creating easily guessed passwords using the names of children or pets, or other non-secure methods. Oracle Solaris 10 contains enhanced password management functions that let administrators set policies for password length, complexity, reuse, dictionary checking, account locking, and defined password complexity levels. Password management functions work in conjunction with password setting policies from the NIS+ and LDAP naming services.

Kerberos

While password-based authentication schemes can work well for standalone systems, they fall short in networked environments. Passwords sent from one system to another can be intercepted as they travel across public and private networks, posing significant risk to users and the enterprise. To address this concern, Oracle Solaris 10 supports Kerberos, a standard for enabling single sign-on capabilities across the enterprise. Based on cryptography, Kerberos provides strong authentication methods that are based on industry-standard encryption algorithms. Capable of interoperating with other technologies, such as Microsoft's Active Directory or MIT Kerberos, passwords are never sent across the wire. Instead, Kerberos uses authentication tokens that are passed among the machines in a Kerberos realm. As a result, users are prevented from assuming root privileges on their local system and executing commands or accessing files that do not belong to them.

All basic remote access functions supported by Oracle Solaris 10 are Kerberos-aware, and services such as NFS v3 and NFS v4 can be secured. In fact, Oracle Solaris was the first operating system to secure NFS using Kerberos, and Oracle Solaris engineers defined the original IETF standard.

Oracle Solaris System Auditing

IT infrastructure forms the lifeblood of many organizations today, and corporate data can be irreplaceable. Whether a deliberate attempt to attack a system, or the result of user error, security-related system events must be tracked in order for system administrators to be able to safeguard valuable assets. Oracle Solaris auditing collects data that records how the system is being used and can report specific activity by users at a specific time and date. Administrators can configure audit tools to monitor and record specific system events and use included tools to assist with the analysis of collected data.

At login, after a user supplies a user name and password, a unique audit ID is associated with the user's process. This audit ID is inherited by every process that is started during the login session. Even if a user changes identity, all user actions are tracked with the same audit ID. Collecting and analyzing the data makes it possible to determine patterns of access and see the access histories of individuals and objects. While auditing cannot prevent hackers from unauthorized entry, it can help detect potential security breaches, misuse, or unauthorized activity, attempts to bypass the protection mechanisms, or the extended use of privilege that occurs when a user changes identity.

Auditing also provides an effective means to follow internal governance and maintain compliance with corporate, industry, or regulatory requirements. For example, the Sarbanes-Oxley legislation mandates checks to ensure that users are not performing unauthorized operations or masquerading as another process in order to gain additional privileges for which they are not authorized. Audit records can be exported either in real-time through `syslog` or XML for use with an external network intrusion detection service, and audit records can be viewed through `syslog` command output.

File Integrity and Validation

Some cyber attacks can involve unobserved system changes that leave administrators unaware of intrusions that result in compromised data, applications, or user accounts. Oracle Solaris 10 offers features that make it possible for administrators to determine whether a system has been compromised, verify systems against known good distributions, and check to ensure that data integrity is secure.

For example, almost every executable binary file in Oracle Solaris carries a signature in the system to validate its integrity. Any binary can be checked by using the `elfsign verify` command to validate the file against its embedded signature. All patches from Oracle are issued with signed binaries as well so that administrators can verify the integrity of each patch applied to a system. In addition, the cryptographic framework in Oracle Solaris self-validates its signatures at boot time or upon reload.

Oracle offers other tools to aid the validation process.

- **Basic Audit and Reporting Tool (BART).** With BART, administrators can generate cryptographic hashes to validate data, applications, and critical system files. Administrators can run BART from scripts or on command to detect changes.
- **Fingerprint Database.** The Oracle Solaris fingerprint database provides digital fingerprints for all files shipped in the Oracle Solaris operating system, including previous generations dating back to Oracle Solaris 2.1. With free online verification utilities, the fingerprint database allows administrators to check the integrity of Oracle Solaris files on any existing system to ensure that no hacker has modified critical system files. It provides a single point of comparison for known good files and MD5 hashes of those files. If the comparison yields matches, then administrators can feel certain that the system has not been compromised. A discrepancy indicates that changes have been made to the system.

Minimizing and Hardening the Operating System

Many operating systems can present security risks when installed on a system right out of the box. In an attempt to minimize risk, administrators with an urgent need to address security concerns often remove unneeded software from the system and tighten security settings. Such changes often are done in haste or without an understanding of the potentially far-reaching implications they can create. In fact, minimizing and hardening the system after it is in use can be a too little, too late approach.

To address these concerns, Oracle Solaris 10 gives administrators the ability to minimize and harden the system at the time it is installed. Administrators can reduce the features installed in order to provide fewer opportunities for hackers. Indeed, Oracle Solaris 10 offers significantly smaller packages than previous releases, separating functionality into smaller groups for finer installation granularity. For example, the telnet package is split into separate server and client software. A system can be installed with only the client portion, making it possible to allow users to initiate telnet sessions out to other systems yet prevent telnet connections into the system. In addition, security settings can be modified to harden the system against attack.

Reduced Networking MetaCluster

System administrators that need to install a minimal system can find it difficult to know which Oracle Solaris packages to install. Earlier versions of the Oracle Solaris operating system are packaged in five different software groups: Core, End User, Developer, Entire, and Entire+OEM. Oracle Solaris 10 offers an additional Reduced Networking MetaCluster, which provides the smallest Oracle Solaris installation that can or should be installed for a working and supported system. Table 1 lists the different MetaClusters and sizes.

Smaller than the smallest previously available software group, the Reduced Networking MetaCluster serves as a base configuration. Additional services and components are turned on or installed as needed to increase system capabilities. The Reduced Networking MetaCluster works with the Oracle Solaris JumpStart mechanism so that multiple systems can be installed and deployed rapidly and securely.

TABLE 1. METACLUSTER SIZES

METACLUSTER	SIZE (MB)	NUMBER OF PACKAGES
Reduced Networking	191	92
Core	219	139
End User	2,100	604
Developer	2,900	844
Entire	3,000	908
Entire + OEM	3,000	988

Oracle Solaris Security Toolkit

With many organizations requiring operations to be running 24x7 around the globe, it is critical to be able to rapidly and securely deploy new systems. The Oracle Solaris Security Toolkit, formerly known as the JumpStart Architecture and Security Scripts (JASS) Toolkit, provides a flexible and extensible mechanism to harden and audit Oracle Solaris operating systems. Designed to simplify and automate the process, the security toolkit is based on proven security best practices and practical customer site experience gathered over many years.

The toolkit contains a set of profiles and Oracle Solaris JumpStart scripts that can make it easy to quickly deploy a new purpose-built server with the appropriate software packages, system services, and more already installed according to the desired server type. The toolkit fully complies with Support Services requirements for system packaging and can be used to implement NSA Security Technical Implementation Guides. See *http://blogs.sun.com/gbrunett/entry/impacting_solaris_10_security_guidance* for more information.

Securing Virtualized Environments

Traditionally, IT organizations concerned about security deploy separate systems in order to isolate users and applications. However, utilizing dedicated servers can lead to rapidly growing numbers of systems, increased complexity, lowered resource utilization, and greater costs. Server virtualization is an important tool for administrators looking to consolidate systems and reduce operating costs. However, one application environment cannot be allowed to affect another — either through overconsumption of system resources, propagation of software faults, or security breaches. Oracle Solaris 10 offers technology that can help administrators isolate and protect applications and users.

Oracle Solaris Containers

Built into Oracle Solaris 10, Oracle Solaris Containers support the creation of a virtualized instance of the Oracle Solaris 10 operating system. Leveraging the Process Rights Management technology in Oracle Solaris, Oracle Solaris Containers provision many secure, isolated runtime environments for

individual applications using flexible, software-defined boundaries. All containers run under a single operating system kernel, enabling fine-grained control over rights and resources within a consolidated server without increasing the number of operating system instances to manage.

With Oracle Solaris Containers, applications can be managed independently of each other, placing one application in each virtual server to maintain isolation while simultaneously sharing hardware resources. Resource controls enable administrators to allocate CPU, memory, and network resources to each container, preventing any single container from monopolizing system assets. Applications that must communicate with one another to complete a job can be moved closer to one another to take advantage of intra-server scalability and eliminate latencies introduced by physical server-to-server network interaction. The result is significantly fewer systems that deliver strong performance improvements across a greatly reduced hardware footprint.

Deploying applications in Oracle Solaris Containers can help to improve security. For example, a Web server documentation directory can be mounted *read/write* in an Oracle Solaris Container used by content providers, while it is mounted *read only* where the Web server process itself is running. This procedure prevents intruders from modifying or hacking the Web server content even if they gain access to the `root` user ID within the Web server container. (For information, see *How to Eliminate Web Page Hijacking Using Oracle Solaris 10 Security* at *http://developers.sun.com/solaris/whitepapers/index.jsp*.)

The BART utility can monitor file changes (using a least privilege process) within a container from the global zone so that no intruder knows that its actions or modifications are being monitored and cannot see or change the audit system, its configuration, or its logs. Indeed, intruders that gain access to a container cannot delete audit data if the container is configured correctly. Processes within a container have no knowledge of overall system configuration, nor can they see other containers unless explicitly permitted.

Oracle Solaris Trusted Extensions

Many customers need to have explicit controls over how data is disseminated, and regulatory requirements for certain industries stipulate stringent data security policies. An integrated set of features within the operating system, Oracle Solaris Trusted Extensions provide an optional layer of secure label technology that makes it possible to implement Mandatory Access Control (MAC) security policies. Labeled security separates data security policies from data ownership, enables the operating system to support multilevel data access policies, and helps organizations to meet strict government regulatory compliance goals without modifying existing applications for underlying hardware platforms. The labeled security features within Oracle Solaris Trusted Extensions provide a platform for deploying high security desktops, database servers, firewalls, and communication gateways, as well as any application where access to sensitive information or networks must be strictly controlled.

Oracle Solaris Trusted Extensions is the only set of labeled security features that offer a complete enterprise security model that is ready for the real world. Capable of being implemented with both the Trusted CDE and GNOME interfaces, Oracle Solaris Trusted Extensions allow for both server-based and desktop use. Resources within the local system or on an LDAP server within a network are subject to policies for authentication and storage according to administrator-specified parameters. Printing, file

sharing, and complete device control on the network also follow labeled security policies, enabling administrators to control data on the network and how and where it can be accessed. Indeed, administrators implementing an Oracle Solaris Trusted Extensions security policy can supersede user decisions to share home directory files using world readable file permissions. Oracle Solaris Trusted Extensions limit sharing the directory files to those processes on the system that contain the same, or dominate, security label as the modified files, preventing a complete breach of security.

Labeled security delivers a powerful tool to prevent either deliberate or unwitting security breaches by users. Many sites can lose control of data to users who employ devices with removable media to copy sensitive data and carry it from the premises. Labeled security extends security policies to system devices including USB devices. This approach enables administrators to prevent users from copying confidential data onto a labeled device they are not authorized to use and removing it from the premises. Figure 4 illustrates how information is shared in a security hierarchy using Oracle Solaris Trusted Extensions.

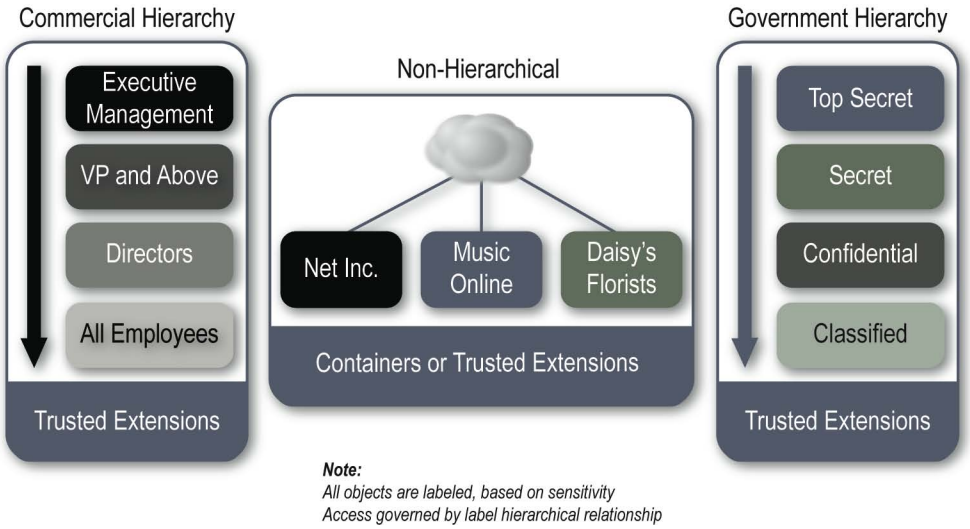

Figure 4. Oracle Solaris Trusted Extensions and labeled security help to implement stringent data security policies.

Independent Security Certifications

Certifications can be helpful indicators when evaluating the security of an operating system, but many operating systems have been tested using only bare minimum configurations. Oracle Solaris 10 is the only operating system to be fully certified using configurations found in many real-world deployments, including multiple systems, LDAP naming services, NFS file sharing, remote printing, and a labeled desktop interface. While it may seem like Red Hat Enterprise Linux holds the same Common Criteria Certifications, Oracle Solaris 10 testing includes multilevel file sharing, multilevel desktops, multilevel network printing, and naming services such as LDAP. In addition, Oracle Solaris 10 testing extends to workstation access for standard users. As a result, Oracle Solaris 10 supports secure, complex environments, ensures applications can run without modification, and eliminates the need for lengthy and complicated policy files.

For More Information

Organizations looking to implement strong corporate governance to meet stringent security regulations, or that want to protect corporate IT systems from a wide variety of cyber attacks, can adopt Oracle Solaris 10 security features for powerful solutions to security concerns. For more information on Oracle Solaris 10 security features, visit the sites listed in Table 2.

TABLE 2. REFERENCES

Oracle Solaris 10 Security Homepage	http://developers.sun.com/solaris/security/
Oracle Solaris 10 Security Best Practices	http:// blogs.sun.com/gbrunett/entry/new_solaris_10_security_best
Oracle Solaris Trusted Extensions Collection	http://docs.sun.com/app/docs/coll/175.9?l=en
Taking Advantage of Wire Speed Cryptography	http://wikis.sun.com/display/BluePrints/Taking+Advantage+of+Wire-Speed+Cryptography
How to Eliminate Web Page Hijacking Using Oracle Solaris 10 Security	http://developers.sun.com/solaris/whitepapers/index.jsp
Glenn Brunette's Security Weblog	http://blogs.sun.com/gbrunett/entry/impacting_solaris_10_security_guidance
Glenn Faden: Trusted Blogger	http://blogs.sun.com/gfaden/

Oracle is committed to developing practices and products that help protect the environment

Using Oracle Solaris 10 to
Overcome Security Challenges
August 2010

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

SOFTWARE. HARDWARE. COMPLETE.