An Oracle White Paper
June 2010

Total Information Protection: Using Oracle Solaris to Address Payment Card Industry Data Security Standard Compliance

Introduction

The Oracle Solaris operating system, an advanced operating system (OS) from Oracle, is an ideal choice for organizations addressing the Payment Card Industry Data Security Standard (PCI DSS). Fully supported on more than 800 SPARC-based and x64/x86–based systems, Oracle Solaris includes hundreds of features making it efficient, secure, and reliable. This white paper presents security features of Oracle Solaris 10 and related technologies and describes how organizations can use them in complying with the PCI DSS. Administrative, managerial, procedural, or physical controls specified by the PCI DSS that Oracle Solaris does not directly address are outside the scope of this white paper.

Note that a prescriptive solution for addressing the PCI DSS is not documented here, as compliance is site, application, infrastructure, and deployment specific. Rather, the intent is to identify Oracle Solaris features and options that can be leveraged to help address the PCI DSS.

A Definition of the Payment Card Industry Data Security Standard

According to the PCI Security Standards organization,[1] "The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data."

PCI DSS compliance is an exercise in risk management with the purpose of reducing risk in IT environments so that payment information can be processed without compromise. Given the nature of payment information and the variety of regulations that apply, IT systems must exhibit a sufficient level of security assurance to provide for the confidentiality, integrity, availability, and privacy of both data and processing resources. For example, these resources must be protected so that they cannot be adversely affected by being delayed, deleted, modified, or disclosed by an unauthorized entity.

The PCI DSS is a "living" standard that is reviewed and updated as necessary to address new and evolving technologies and threats. An adaptive security approach such as the total information protection feature in Oracle Solaris is recommended to accommodate change and keep up with the evolving nature of the standard.

The primary information security objectives or principles of the PCI DSS version 1.1 are summarized in Table 1.

TABLE 1: PCI DSS PRINCIPLES AND ASSOCIATED REQUIREMENTS

1. BUILD AND MAINTAIN A SECURE NETWORK.	
Requirement 1:	Install and maintain a firewall configuration to protect cardholder data.
Requirement 2:	Do not use vendor-supplied defaults for system passwords and other security parameters.
2. PROTECT CARDHOLDER DATA.	
Requirement 3:	Protect stored cardholder data.
Requirement 4:	Encrypt transmission of cardholder data across open, public networks.
3. MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM.	
Requirement 5:	Use and regularly update antivirus software.
Requirement 6:	Develop and maintain secure systems and applications.

[1] PCI Security Standards Council, pcisecuritystandards.org

4. IMPLEMENT STRONG ACCESS CONTROL MEASURES.	
Requirement 7:	Restrict access to cardholder data by business need-to-know.
Requirement 8:	Assign a unique ID to each person with computer access.
Requirement 9:	Restrict physical access to cardholder data.
5. REGULARLY MONITOR AND TEST NETWORKS.	
Requirement 10:	Track and monitor all access to network resources and cardholder data.
Requirement 11:	Regularly test security systems and processes.
6. MAINTAIN AN INFORMATION SECURITY POLICY.	
Requirement 12:	Maintain a policy that addresses information security.

A Systemic Approach to Security

It is important to understand that the PCI DSS is not a prescriptive list of mandated controls. Rather, the underlying intent of the standard is to ensure that organizations design, architect, implement, and manage a comprehensive risk management and security program. An integral component of this security effort is a security architecture based upon systemic security principles.

The total information protection feature in Oracle Solaris is a comprehensive architectural approach that allows organizations to implement and manage controls that are capable of responding to new and different threats over time. The primary principles of this approach to security (versus, for example, a prescriptive or checklist approach) are self-preservation, defense in depth, least privilege, compartmentalization, and proportionality. The security architecture is designed, implemented, and managed within the context of a continuous improvement schema, helping organizations mature over time to anticipate evolving threats. These features make a security architecture based upon total information protection an ideal solution for addressing the PCI DSS.

A complete program should include the following features:

- A security governance structure to ensure that executive management is accountable for and actively promotes security throughout the enterprise
- A security policy that dictates which security elements should be implemented to enable appropriate risk management, privacy, and security controls
- A comprehensive security architecture built upon and leveraging the systemic security principles

Oracle Solaris Features

Oracle Solaris should be considered not in isolation but as an integral component of an overall security effort. It is within this context of an overall security approach that the various Oracle Solaris security features are described. As an OS, Oracle Solaris is not oriented toward direct support of administrative or managerial requirements such as a security policy or security procedures development. However, Oracle Solaris is a critical component in the infrastructure used to enable compliance with these and other requirements of the standard.

The following Oracle Solaris features can be used to address the pertinent PCI DSS requirements:

- File integrity and secure execution
- User and process rights management
- Network service protection
- Cryptographic services and encrypted communication
- Flexible enterprise authentication
- Repeatable security hardening and monitoring
- Containment and mandatory access control

Each of these features is covered in more detail in the following sections. Each feature is briefly described, followed by a discussion of how that item can be applied to help address PCI DSS compliance.

File Integrity and Secure Execution

System administrators can detect possible attacks on their systems by monitoring for changes to file information. In Oracle Solaris 10, binaries are digitally signed, enabling administrators to track changes easily. In addition, all patches or enhancements are embedded with digital signatures, eliminating the false positives associated with upgrading or patching file-integrity-checking software. Any binary can be signed—third-party commercial offerings, open source, or code developed onsite—without needing access to the source code.

Oracle Solaris 10 also introduces the Basic Audit and Reporting Tool (BART), a file-integrity-checking application for datafiles and customer applications. The BART utility allows customers to create snapshots of their own data, applications, and critical system files and periodically scan for changes to these files.

Additionally, the Oracle Solaris fingerprint database project provides digital fingerprints for all files shipped in Oracle Solaris, spanning many previous generations of the OS. The Oracle Solaris fingerprint database offers free online verification utilities that allow administrators to check the integrity of Oracle Solaris files on any existing system, to help confirm that no hacker has modified critical system files. Used individually or together, these file integrity tools provide powerful, flexible ways to monitor for changes to the OS platform.

Addressing the PCI DSS

The embedded digital signatures and file-integrity-checking tools in Oracle Solaris 10 can be used as part of a vulnerability management program and can assist in maintaining and monitoring network security. These features help identify changes to data or applications and can be scripted into a reactive response mechanism. Maintaining a vulnerability management program includes consideration of antivirus scanning applications. It is important to note that Oracle Solaris does not itself suffer from Microsoft Windows–specific viruses, a common cause of computer vulnerability.

The built-in Oracle Solaris 10 file integrity features help to mitigate and react to inappropriate changes to files, and these features should be integrated within a comprehensive detection practice. For example, a system administrator can utilize the `bart` command with a given set of special privileges in a nightly process to scan critical system files and data for possible changes. If the nightly scan detects a change in a file, it can notify an administrator or take other corrective action. When used with privileges as noted, the file scanning process itself would not need to run with unlimited superuser power and could not be used as an attack vector to modify data.

User and Process Rights Management

In traditional UNIX platform–based OSs, applications and users often need administrative access to perform their jobs. However, most implementations offer just one level of higher privilege: root or superuser. In this situation, any user or application given root access has the ability to make major changes to the OS—and root access like this is typically the target of hacking attempts.

Oracle Solaris 10 offers unique user rights management (also known as *Role-Based Access Control*, or RBAC) and process rights management (also known as *privileges*). Together, user and process rights management technologies reduce risks by granting users and applications only the minimum capabilities needed to perform their duties. Unlike other solutions on the market, no application changes are required to take advantage of these security enhancements.

Oracle Solaris applications also are protected from a possible form of intrusion known as *stack smashing* by a nonexecutable stack feature. Oracle Solaris applications running on 64-bit SPARC, AMD, and Intel processors work together to prevent virus and Trojan applications from executing code, without requiring application recompilation or suffering the performance penalties of other OSs.

Oracle Solaris also offers an extensive system event audit trail collection facility. Essentially all system events can be audited, with selective controls on which classes of events are audited governed on a per-user basis. Access to files, devices, roles, system services, and applications is recorded. This audit trail is part of the Common Criteria independent security certification of Oracle Solaris 10 and offers the ability to be exported into an open XML format or automatically transported to another system.

Addressing the PCI DSS

User and process rights management technology can be used to build and maintain secure networks and implement strong access control measures. For example, all UNIX platform–based Web server software traditionally requires root access to serve applications on port 80, a commonly used Web TCP/IP port. However, with user and process rights management, a Web server application on Oracle Solaris 10 can be granted just the privileges required to enable it to bind to low-numbered ports (port 80) without providing additional administrative access. If the Web server software is attacked, the hacker cannot escalate privileges, launch additional attacks, or gain further access to the system, nor compromise files and material related to cardholder data. The Web server itself could be managed by only a select group of users who have a specific role defined just to manage this particular service and no other. This example is fully detailed in the document "Eliminating Web Page Hijacking Using Solaris Security," as seen in Appendix B.

As another example, a person or group of people performing the task of system log analysis on a given set of machines need not have the ability to create or delete system log information. The user and process rights management features can be used to create a role for those individuals. This role can grant them read-only access to certain commands and certain files that they do not own themselves, without granting them full administrative rights on the system. Because Oracle Solaris records the real identity of the person doing the activity in addition to the name of the role, all actions are accounted for on an Oracle Solaris system.

Network Service Protection

Oracle Solaris 10 ships with IP filter firewall software preinstalled. This integrated firewall can reduce the number of network services that are exposed to attack and provides protection against maliciously crafted networking packets. Starting with the Oracle Solaris 10 8/07 release, the IP filter firewall can also filter traffic flowing between Oracle Solaris Containers when it is configured in the global zone. In addition, TCP wrappers are integrated into Oracle Solaris 10, limiting access to service-based allowed domains. For example, access to an FTP server could be limited only to the internal.foo.com domain.

Oracle Solaris also provides protection against inappropriate use of network resources through its secure by default networking configuration. At installation time, a system administrator is offered a choice of running a system with many networking services disabled, and other more commonly used services are configured for use only by the system itself. An administrator can also choose to enable or disable how an individual network service listens for network connections and can reset the entire system to a secured state with one simple command. When configured in this manner, an Oracle Solaris 10 system retains a usable GUI interface and can browse the Web, send e-mail, and do other outbound communications. Only the secure shell encrypted remote access method in Oracle Solaris is allowed for inbound communication.

Addressing the PCI DSS

The networking and filtering features of Oracle Solaris 10 can be used to help build and maintain a secure network. The IP filter firewall and TCP wrappers are integrated into Oracle Solaris, enabling administrators to configure access to specific resources for specific customer segments and also to help protect against certain types of denial-of-service attacks. By utilizing the secure by default networking configuration, system administrators start from a known good configuration in which no networking services are exposed for unencrypted communication. From this starting point, an administrator can enable only the services needed for their specific site, thereby reducing exposure to attack by leaving other services disabled.

Cryptographic Services and Encrypted Communication

For high-performance, systemwide cryptographic routines, the cryptographic framework in Oracle Solaris adds a standards-based, common API that provides a single point of administration and uniform access to both software- and hardware-accelerated cryptographic functions. The pluggable cryptographic framework can balance loads across accelerators, increasing encrypted network traffic throughput. This framework is available to applications written to use Public Key Cryptography Standards (PKCS) #11, OpenSSL, and Java Cryptography Extension (JCE) software.

Starting with the Oracle Solaris 10 8/07 release, the key management framework in Oracle Solaris is available to assist in managing digital certificates. The key management framework provides a single set of administrative commands for digital certificate creation requests, manipulation, and loading across the most common formats used by OpenSSL, PKCS #11, and the NSS cryptographic libraries. A system administrator can now easily manage the full lifecycle of a digital certificate, regardless of whether they deploy the certificate for use by a Web server, a virtual private network (VPN) connection, a cryptographic accelerator card, a database, or any other application.

Because the cryptographic and key management frameworks provide transparent application to high-speed cryptographic routines and accelerator cards, customers can process encrypted data more easily and for less computational cost than in previous Oracle Solaris releases. This capability can help customers utilize encrypted communications in new situations and potentially perform more transactions per second than was previously possible.

Oracle Solaris also provides protection against theft of sensitive material by encrypting communications using IPSec/IKE and secure shell protocols. IPSec/IKE in Oracle Solaris complies with industry standards to provide encryption of data between two or more systems over the network without requiring any application modification. Because IPSec/IKE are standards-based protocols, Oracle Solaris can communicate with other OSs, routers, and firewalls to provide data privacy and over-the-wire encryption. The secure shell protocol is a specific set of utilities in Oracle Solaris that have been modified to allow for encrypted remote access and file transfer between two systems. The secure shell protocol implements the SSHv2 protocol and thus can interoperate with other OSs or devices that utilize these protocols.

Addressing the PCI DSS

The encrypted communication capabilities in Oracle Solaris 10 directly address protecting cardholder data. Sensitive data can be encrypted as it is moved between one or more systems using the IPSec/IKE and cryptographic framework. Because the cryptographic and key management frameworks provide a single point of administration, customers can easily disable encryption algorithms that they have not authorized for use, and all applications will be disallowed access to those algorithms. This capability helps with compliance and auditing requirements to use strong encryption of sensitive material.

Flexible Enterprise Authentication

Oracle Solaris 10 delivers a number of flexible authentication features. The pluggable authentication modules (PAMs), a key foundation of Oracle Solaris, make it possible to add authentication services to

Oracle Solaris dynamically. Oracle and third-party vendors provide numerous PAMs, and customers can create their own modules to meet specific security needs. Technologies such as the Kerberos service and Lightweight Directory Access Protocol (LDAP) utilize the PAM framework in Oracle Solaris to deliver strong authentication of users and applications.

The Kerberos service delivers Kerberos-enabled remote applications such as rsh, rcp, telnet, Oracle Solaris secure shell protocol, and NFS file sharing. Kerberos-based protocols allow for enterprise single sign-on, authorization, and encrypted communication. In addition, Kerberos-based applications never transmit a password over the network unencrypted, and they are interoperable with many different OSs.

LDAP client-side authentication and interoperability enhancements enable enterprisewide, secure, standards-based access to servers and applications. To enable easier integration with existing environments, existing native LDAP authentication software offers NIS and NIS+ to LDAP gateways. Oracle Solaris supports encrypted LDAP authentication requests and can utilize strong password encryption, account lockout, password history, and other features provided by Oracle Directory Server Enterprise Edition. All Oracle Solaris user and process rights management information can also be stored centrally through the LDAP-based directory server, allowing for centralized management of users and security role definitions.

Local passwords on the Oracle Solaris platform have strong password encryption options, including MD5 and Blowfish, as well as account lockout, password history and complexity checking, and a banned-passwords list. With strong password encryption, systems are less subject to successful password cracking should a password file ever be lost or stolen.

Addressing the PCI DSS

The strong authentication capabilities in Oracle Solaris can be used to implement strong access control and help maintain a secure network. Specifically, each site can choose to change the default password encryption algorithm and can utilize technologies such as Kerberos and LDAP to encrypt their passwords. Systems that use encryption technologies such as these are more secure and less subject to being compromised by passwords or sensitive data transmitted unencrypted over the network. Requirements for strong passwords can also be enforced through the password complexity controls as well as flexible password encryption algorithms.

The PCI DSS also requires unique IDs per user. Centralization of those identities through industry-standard LDAP-based directory servers or Kerberos Key Distribution Centers allows for standardization and unification of logins.

Repeatable Security Hardening and Monitoring

New features in Oracle Solaris 10 make it easier than ever to minimize and harden a system. *Minimization* is the process of reducing the number of running processes on a system to just those needed for the system to perform its task. *Hardening* a system is the process of changing the system configuration to choose more-secure methods of communication and authentication. The reduced networking metacluster installation option creates a minimized Oracle Solaris image, ready for administrators to add functionality and services in direct support of their system's purpose. This minimized Oracle Solaris installation acts as a building block and offers no exposed network services and a very minimal number of running processes.

As mentioned previously, Oracle Solaris 10 now includes a secure by default networking configuration that disables many unused network services, while configuring all other services for local system-only communications. Administrators can customize which services are running by utilizing the service manager feature in Oracle Solaris 10. This functionality can be further protected using user and process rights management in Oracle Solaris 10 to control exactly who can manage which services and with what privileges those services run.

The freely available security toolkit for Oracle Solaris assists in the process of installing and maintaining a minimized and hardened OS security configuration. The toolkit integrates with the Oracle Solaris JumpStart installation process or can be used on an existing system to harden a system according to a site-defined security profile. A collection of sample profiles, based upon the knowledge gained through years of installation experience, is provided. The toolkit also includes an audit mechanism to compare a running system configuration against a site-specified hardening profile. In this way, the toolkit can be used to both verify and enforce compliance with an organization's OS security standards.

Addressing the PCI DSS

The security hardening and minimization tools available for Oracle Solaris help to build and monitor secure systems and networks. Specifically, the ability to customize an Oracle Solaris installation to include only the functionality that is absolutely necessary for proper functioning can help to reduce risk of exposure to attack. By utilizing Oracle Solaris installation tools and the security toolkit, customers can also document the security hardening and minimization techniques they used to install Oracle Solaris and can dynamically check their system to ensure that they are still in compliance with their desired security state.

To assist customers during their regular security checks, the security toolkit can be run in an audit mode that compares current file permissions, password settings, enabled services, software loaded onto a system, and more against the known list of security profiles used to install the system. If the current system state is different than the original installation state, the toolkit can automatically reapply the needed security changes.

Containment and Mandatory Access Control

Oracle Solaris 10 includes isolation technology known as *Oracle Solaris Containers*. Each Oracle Solaris Container acts as an isolated Oracle Solaris instance with its own users, administrators, application software, file system, and networking. However, each instance also allows the global administrator to lock down certain settings such as network interface configuration and read-only shared directories. Applications running inside an Oracle Solaris Container do not have the ability to see or directly communicate with files or processes running inside another Oracle Solaris Container on the same system. All applications on an Oracle Solaris Container also run with fewer maximum privileges than they would have running outside of an Oracle Solaris Container. In essence, an Oracle Solaris Container is a security boundary for an application and data.

Oracle Solaris with trusted extensions enhance Oracle Solaris Containers and implement mandatory access control (MAC) based on sensitivity labels applied to an Oracle Solaris Container. The security policy in Oracle Solaris is extended to support labels on elements of the OS so that data marked as "confidential" can't be accessed by public services such as Web browsers and e-mail applications, regardless of who attempts the access. In addition, data can't be written to a device, such as a CD or USB flash drive, that is labeled with a lower classification than the data itself, which helps protect most sensitive data. Labeling extends to network packets, the Common Desktop Environment (CDE) and Java Desktop System interfaces, file systems, devices, printers, and all processes.

Addressing the PCI DSS

Containment and MAC help address the PCI DSS principles of maintaining secure networks, protecting cardholder data, and implementing strong access control measures. One requirement of the PCI DSS is to isolate services onto separate servers. Oracle Solaris Containers provide this separation, with all Oracle Solaris Containers isolated from each other. Even administrative or subversive action attempts within an Oracle Solaris Container do not directly affect data or applications running in another Oracle Solaris Container, because Oracle Solaris resource management allocations for virtual memory, CPU share, and networking bandwidth override any errant process that exists within an Oracle Solaris Container.

Starting with the Oracle Solaris 10 8/07 release, a separate network stack and interface card can be assigned to each Oracle Solaris Container to further separation. Additionally, the use of Oracle Solaris with trusted extensions helps to address the need to control the access to cardholder data. Data can be classified for internal use only once it's obtained, thus moving it to a different Oracle Solaris Container where it cannot be maliciously or accidentally written to a Website, CD, or inappropriate storage location to be compromised or stolen. Beyond OS containment, network containment models such as Oracle's service delivery network architecture can provide greater levels of security and agility.

Conclusion

Addressing the PCI DSS requires a comprehensive security program, and Oracle Solaris is one critical component of such a program. The various features of Oracle Solaris, as well as other products and services available from Oracle, provide a wide array of tools that can be used to address the vast majority of PCI DSS requirements.

These Oracle Solaris security features and other Oracle products noted in this white paper provide a solid foundation that can be used in conjunction with a comprehensive security architecture. Using a systemic security approach like this helps organizations mature over time, adapt to emerging threats, and continue to meet evolving security standards. It is only through such a holistic approach that an organization can fully address the requirements of the PCI DSS.

Appendixes

Appendix A: References

- PCI Security Standards Council
  - pcisecuritystandards.org
- Sun Security
  - sun.com/security
- Oracle Solaris Security
  - sun.com/solaris/security

Appendix B: Related Solaris Security Publications

- Thacker, Mark. "Eliminating Web Page Hijacking Using Solaris Security," Solaris 10 Security How-To Guides.
  - sun.com/software/solaris/howtoguides/s10securityhowto.pdf
- Sun, Ning and Bhattacharya, Pallab. "Using the Cryptographic Accelerator of the UltraSPARC T1 Processor," Sun BluePrints OnLine, March 2006.
  - sun.com/blueprints/0306/819-5782.pdf
- Brunette, Glenn. "Enforcing the Two-Person Rule via Role-based Access Control in the Solaris 10 OS," Sun BluePrints OnLine, August 2005.
  - sun.com/blueprints/0805/819-3164.pdf
- Brunette, Glenn. "Restricting Service Administration in the Solaris 10 Operating System," Sun BluePrints OnLine, June 2005.
  - sun.com/blueprints/0605/819-2887.pdf
- Brunette, Glenn. "Limiting Service Privileges in the Solaris 10 Operating System," Sun BluePrints OnLine, May 2005.
  - sun.com/blueprints/0505/819-2680.pdf
- Brunette, Glenn. "Integrating BART and the Solaris Fingerprint Database in the Solaris 10 Operating System," Sun BluePrints OnLine, April 2005.
  - sun.com/blueprints/0405/819-2260.pdf
- Brunette, Glenn. "Automating Centralized File Integrity Checks in the Solaris 10 Operating System," Sun BluePrints OnLine, March 2005.
  - sun.com/blueprints/0305/819-2259.pdf

Appendix C: Related Solaris Security Resources

- Solaris Security Learning Center
  - sun.com/solaris/secure
- Personalizing Security in the Solaris 10 Operating System (Instructor-led Training)
  - sun.com/training/catalog/courses/SC-301-S10.xml
- Solaris Security Toolkit
  - sun.com/security/jass
- OpenSolaris Security Community Library
  - opensolaris.org/os/community/security/library
- OpenSolaris Security Presentations
  - opensolaris.org/os/community/security/preso
- Solaris Fingerprint Database Tools
  - opensolaris.org/os/community/security/projects/sfpdb

Appendix D: Related Sun Security Publications

- Lofstrand, Mikael and Carolan, Jason. "The Service Delivery Network: A Case Study," Sun BluePrints OnLine, April 2006.
  - sun.com/blueprints/0406/819-6319.pdf
- Brunette, Glenn. "Toward Systemically Secure IT Architectures," Sun BluePrints OnLine, February 2006.
  - sun.com/blueprints/0206/819-5605.pdf
- Lofstrand, Mikael and Carolan, Jason. "Sun's Pattern-Based Design Framework: The Service Delivery Network," Sun BluePrints OnLine, September 2005.
  - sun.com/blueprints/0905/819-4148.pdf

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

Total Information Protection: Using Oracle Solaris to Address Payment Card Industry Data Security Standard Compliance
June 2010
Contributing Authors:
Glenn Brunette, Distinguished Engineer, GSS Security Office; Mark Thacker, Product Line Manager, Solaris; Joel Weise, Principal Engineer, GSS Security Office

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.