

## Oracle Solaris Security Frequently Asked Questions

### Frequently Asked Questions

#### 1. What is Oracle Solaris Process Rights Management?

Solaris Process Rights Management, introduced in the Oracle Solaris 10 Operating System, gives system administrators the ability to limit and selectively enable applications to gain access to just enough system resources to perform their functions. This capability dramatically reduces the possibility of attack from a poorly written application, by eliminating inappropriate access to the system. Even if hackers gain access to an application's server, they are unable to increase operating privileges, thus limiting the opportunity to inject malicious code or otherwise damage data.

#### 2. What sort of attacks or hacking can Process Rights Management address?

Because Process Rights Management puts limits on the rights of any process, regardless of the user associated with the running process, a hacker who gains control over an application is similarly restricted.

A good example of this is a Web server. Normally on a UNIX system, Web servers must run as the “root” user (the system superuser) because of their usual requirement to connect to TCP port 80 (the privileged Web port). This means that the Web server is a great target for attacks; hackers can often gain full access to a server as the “root” user through a buffer stack overflow or other attack. With Process Rights Management, the Web server can be granted just one privilege other than that of a normal user—the ability to open a privileged port; a hacker will find they do not have additional privileges and thus cannot modify the security on the system or bypass it to access critical or private system resources.

Another good example is the Oracle Solaris Containers model. The groundbreaking Oracle Solaris Containers technology enables users to create dozens or even hundreds of secure, fault-isolated containers within a single Oracle Solaris

instance. Oracle Solaris Containers are isolated from each other so that users or applications in one container cannot see or access contents in another container or in the global system environment. Process Rights Management helps ensure that applications—even those run with privileges—are constrained to access resources only in their own Solaris Containers.

#### 3. How is Oracle Solaris Process Rights Management different from the Oracle Solaris User Rights Management feature?

Enhancements to the Oracle Solaris Role Based Access Control (RBAC) software, referred to in the Oracle Solaris 10 OS as the Solaris User Rights Management software, enable administrators to assign specific access rights to programs and commands for each user. This reduces the chance of administrative errors or accidental or malicious use of IT resources. User Rights Management is centrally managed to reduce costs and increase flexibility.

Thus, the Solaris RBAC software constrains a user's actions, and Process Rights Management constrains a process' capabilities.

#### 4. Will customer applications need to be changed to use Process Rights Management?

Existing Oracle Solaris applications will continue to work unmodified, since they are typically unaware of the constraints placed on them by Process Rights Management. Developers may write applications to explicitly use privileges granted by Process Rights Management but this is not required.

Administrators can add Process Rights Management's functionality to existing applications by using the `ppriv` utility included in the Oracle Solaris 10 OS. With the `ppriv` utility, administrators can determine the privileges required by a process and can set those privileges without modifying the applications.

For maximum compatibility with customer applications, the system is designed to let applications behave as they have in

## Oracle Solaris Security Frequently Asked Questions

the past although they are now additionally subject to privilege policies.

5. Do I have to purchase the Process Rights Management technology separately? If not, how do I access it?

Process Rights Management is a feature of the Oracle Solaris 10 OS, included at no extra cost and enabled by default, always on and always working.

6. How does Process Rights Management compare to privilege models provided by Linux, SGI Irix, or other UNIX operating systems?

The Oracle Solaris OS development team looked closely at the experimental Linux privilege patches and other UNIX models. These existing solutions failed to offer the flexibility to work with existing customer file systems, required application recompiling, or were fixed in size, limiting, for example, the number of allowed privileges. Solaris Process Rights Management's privilege model also has the advantage of growing out of the proven, extensive capabilities of the Trusted Solaris Operating System.

7. What is Oracle Solaris Secure Execution?

Solaris Secure Execution prevents modified or unsigned code from running by verifying the integrity of the executable portion of almost all applications, drivers, and modules on a Oracle Solaris system.

Oracle provides customers with the tools to sign their own or third-party applications with no additional changes needed. Manual signature verification is available today in the Oracle Solaris 10 OS, with automatic runtime verification planned for a future release.

8. What is the Oracle Solaris Basic Audit and Reporting Tool?

The Solaris Basic Audit and Reporting Tool (BART) helps system administrators validate the integrity of data files and associated meta information such as file ownership and size. BART complements the Oracle Solaris Secure Execution technology by providing tools to monitor the integrity of all files on the system at any point in time. System administrators, using simple scripts, can automate integrity checks using BART.

9. What is the Oracle Solaris IP Filter firewall?

The Solaris IP Filter firewall is firewall software that allows for stateful packet filtering. It can also be used to deliver network address translation (NAT) capabilities. IP Filter provides protection to a single server or a network of servers and clients. The IP Filter technology included in the Oracle Solaris 10 OS is based on the next-generation Version 4.x open source IP Filter. Enhancements made during the Solaris software development process have been placed back into the open source version of IP Filter.

10. Why was IP Filter integrated into Oracle Solaris 10?

The most popular packet filtering solution in use today is the open source IP Filter. Customers who deploy Linux or other UNIX operating systems don't want to deploy multiple solutions to obtain the same functionality. Oracle has included IP Filter in the Oracle Solaris OS to meet the needs of these customers.

11. What's so great about the Solaris IP Filter firewall?

The Solaris IP Filter firewall offers these key benefits:

- \* Strengthens security in Oracle Solaris by preventing unauthorized access to private computers or networks
- \* Enhances the integrity of networks that contain Oracle Solaris systems

## Oracle Solaris Security Frequently Asked Questions

\* Engineered to use stable interfaces to ensure high performance and easy manageability for Solaris software customers

It also provides the following capabilities:

\* Network address translation (NAT): I/O packets going through NAT can have their source or destination IP address changed to mask the real address, based on configurable rules.

\* Filtering: Packets can be allowed or not allowed into a network, based on configurable rules.

\* Accounting: Rules can be set up to record the number of bytes and packets entering and leaving the network, allowing for statistical analysis.

12. How are the offerings of the IP Filter technology different from other vendors' offerings?

IP Filter technology is different in a number of ways:

\* Oracle will fully support IP Filter deployed on Solaris servers, regardless of whether or not those servers are hosting Internet applications, protecting a network of internal servers, or protecting a single desktop client.

\* Oracle has incorporated performance enhancements and stability enhancements into IP Filter to ensure a high-quality customer experience.

\* Oracle is investigating continued improvements in both the IP Filter firewall and in the management of stateful packet filtering in general in the Oracle Solaris OS.

13. What is labeled security and how does Oracle Solaris Trusted Extensions relate to it?

Labeling data based on its sensitivity and controlling access to that data based on the label is known as labeled security and is a capability introduced with the Solaris Trusted Extensions feature of the Oracle Solaris 10 Operating System. Because access to data, users, process, files, network packets, windows

on the desktop and devices is enforced by the kernel and is based on the relationships of labels to each other, it is also known as a Mandatory Access Control (MAC) policy. Users and most privileged applications cannot override the Mandatory Access Control policy, ensuring a high degree of security to the system.

14. What features are provided by Solaris Trusted Extensions ?

Trusted Extensions provides labeled security as a configuration of Oracle Solaris 10. Separation of data, processes, memory, network traffic, windowing elements, device allocation and more is enforced by a Mandatory Access Control Policy that defines the relationship and flow of data based on a security classification (called a label). This technology includes two multi-level desktops (Trusted CDE and Trusted Java Desktop System), multi-level printing, multi-level device allocation, multi-level networking, LDAP client naming services, multi-level file system use and a full multi-level API.

15. Is there a separate fee for the use of Solaris Trusted Extensions?

No. There is no extra cost or fee for use of Trusted Extension for either end-users or OEMs. Solaris Trusted Extensions is a feature introduced in Solaris 10 11/06; it delivers labeled security to all users who wish to activate it. Trusted Extensions is installed as part of the Solaris OS and is enabled with the command "svcadm enable label".

16. How can Secure By Default Networking protect my system from network-based attacks?

During installation, customers can now set the default behavior for network services to run in a much more secure manner. Many non-essential network services are disabled and many more are set to listen for network connections only from the local system ("localhost"), thus reducing the exposure to attack. Users can still access their graphical interface, use Web browsers or Email clients and other services. Oracle Solaris

## Oracle Solaris Security Frequently Asked Questions

Secure Shell remains available for secure remote administrative access to the system.

### 17. Is Oracle Solaris 10 Common Criteria Certified?

Oracle Solaris 10 has many Common Criteria certifications and generally is tested against the Controlled Access Protection Profile (CAPP), Role Based Access Control Protection Profile (RBACPP) and Labeled Security Protection Profile (LSPP).

The latest update with Common Criteria certification is Solaris 10 5/09.

Solaris 10 5/09 has been certified using the Assurance Continuity process based on the certificate received for the evaluation of Solaris 10 11/06. The modifications made in Solaris 10 5/09 have been reviewed to ensure that their application does not introduce new security vulnerabilities and that the changes are consistent with the original certified Target of Evaluation (TOE).

Solaris 10 5/09 Trusted Extensions has been certified using the Assurance Continuity process based on the certificate received for the evaluation of Solaris 10 11/06 with Trusted Extensions. The modifications made in Solaris 10 5/09 Trusted Extensions have been reviewed to ensure that their application does not introduce new security vulnerabilities, and that the changes are consistent with the original certified Target of Evaluation (TOE).

