Oracle Solaris 10 Security Frequently Asked Questions (FAQ)

Last updated 02/08/2013

1-How can I sandbox applications to prevent misbehavior or hacked applications from impacting the system?

Oracle Solaris Process Rights Management, introduced in Oracle Solaris 10, gives system administrators the ability to limit and selectively enable applications so they 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, which limits the opportunity to inject malicious code or otherwise damage data.

2-What sort of attacks or hacking can application sandboxing prevent?

Because Process Rights Management puts limits on the rights of a 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. Hackers will find they do not have additional privileges and, thus, they cannot modify the security on the system or bypass security to access critical or private system resources.

3-What is Role-Based Access Control?

The Oracle Solaris Role-Based Access Control (RBAC) framework enables administrators to assign specific access rights to programs and commands for each user, reducing the chance of administrative errors or malicious use of IT resources. User Rights Management is centrally managed to reduce costs and increase flexibility.

4-How does Role-Based Access Control differ from application sandboxing (Process Rights Management)?

Oracle Solaris RBAC software constrains a user's actions, and sandboxing (Process Rights Management) constrains a process' capabilities.

5-Will customer applications need to be changed to use sandboxing?

No. Application security policies can be applied either in the source code with knowledge of the process rights framework or at runtime without the application being aware of that framework.

6-What is Oracle Solaris Secure Execution?

Oracle 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 an Oracle Solaris system.

7-What is the Oracle Solaris Basic Audit and Reporting Tool?

The Oracle Solaris Basic Audit and Reporting Tool (BART) helps system administrators validate the integrity of data files and associated metainformation, such as file ownership and file size. System administrators, using simple scripts, can automate integrity checks using BART.

Oracle Solaris 10 Security Frequently Asked Questions (FAQ)

8-What is the Oracle Solaris IP Filter firewall?

The Solaris IP Filter firewall is firewall software that allows for stateful packet filtering and network address translation (NAT) capabilities.

9-What are the benefits of the Oracle Solaris IP Filter firewall?

The Oracle Solaris IP Filter firewall offers these key benefits:

- It strengthens security in Oracle Solaris by preventing unauthorized access to private computers or networks.
- It enhances the integrity of networks that contain Oracle Solaris systems.
- It is engineered to use stable interfaces to ensure high performance and easy manageability for Oracle 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—based on configurable rules—to mask the real address.
- Filtering: Based on configurable rules, packets can be allowed or not allowed into a network.
- Accounting: Rules can be set up to record the number of bytes and packets entering and leaving the network, allowing for statistical analysis.

10-What are labeled security and multilevel security?
Labeled security uses security classification metadata (such as classified, secret, and top secret) on files, networks, and other system resources to make access decisions. Multilevel security defines a relationship among security classifications so that data can be viewed and, if desired, moved to a defined hierarchy (for example, from secret to top secret).

11-What features are provided by Oracle Solaris Trusted Extensions?

Trusted Extensions technology enforces a labeled-security access-control policy for multilevel desktop, multilevel printing, multilevel device allocation, multilevel networking, LDAP client naming services, multilevel file system use, and a full multilevel API.

12-Is there a separate fee for the use of Solaris Trusted Extensions?

No. There is no extra cost or fee.

13-How can “secure by default” protect my system from attack?

Oracle Solaris 10 ships in a “secure by default” configuration with a reduced network footprint and some security features enabled by default. Many nonessential network services are disabled and other services are set to listen for network connections only from the local system (`localhost`), thus reducing exposure to attack. Oracle Solaris Secure Shell (`ssh`) is the only service exposed to the network by default, and it remains available for secure remote administrative access to the system.

14-Is Oracle Solaris 10 Common Criteria certified?

Oracle Solaris 10 has been evaluated and certified against the Common Criteria Controlled Access Protection Profile (CAPP), Role-Based Access Control Protection Profile (RBACPP), and Labeled Security Protection Profile (LSPP).

Oracle Solaris 10 Security Frequently Asked Questions (FAQ)

15-How can I get more news about Oracle Solaris?

Catch the latest news and information from our social media sites:

- Blog
- Facebook
- Twitter
- LinkedIn
- YouTube

For more information on Oracle Solaris 10, please visit the Oracle Technology Network Website.

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

Worldwide Inquiries:
Phone: +1.650.506.7000
+1.800.ORACLE1
Fax: +1.650.506.7200

oracle.com