Deploying Oracle Database 11g Securely on Oracle Solaris

Glenn Brunette
Senior Director, Enterprise Security Solutions
The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Agenda

• **Introduction**
  – Why Focus on Operating Systems?
  – How Can Oracle Solaris Help?

• **Deploying On A Strong Foundation**
  – Reduced Attack Surface
  – Separation of Duty and Least Privilege
  – Strong Isolation and Resource Control
  – Comprehensive Monitoring

• **Embracing a Defense in Depth Architecture**
  – Hardware, Operating System and Database Security
Why Focus on the Operating System?

• Burglars Don’t Always Use the Front Door
  – Similar goals can be achieved using different methods
Why Focus on the Operating System?

• Burglars Don’t Always Use the Front Door
  – Similar goals can be achieved using different methods
• Attacks Don’t Always Originate in the Database
  – Operating system access provides unique opportunities
Why Focus on the Operating System?

• Burglars Don’t Always Use the Front Door
  – Similar goals can be achieved using different methods
• Attacks Don’t Always Originate in the Database
  – Operating system access provides unique opportunities
• Security Must Be Systemically Applied
  – A chain is only as strong as its weakest link
How Can Oracle Solaris Help?

• Reduced Attack Surface
  – Package Minimization
  – (Network) Secure by Default

• Separation of Duty and Least Privilege
  – User Rights Management
  – Process Rights Management

• Strong Isolation and Resource Control
  – Logical Domains
  – Containers

• Comprehensive Monitoring
  – Auditing
Reduced Attack Surface
Oracle Solaris Package Minimization

• Selectively install only what is needed
  – Reduce the operating system file footprint
  – 3.6 GB vs. 550M (disk consumed by Entire+OEM vs. Reduced Networking)

• Uninstalled software…
  – cannot be executed or exploited
  – does not need updates or patching
  – does not need configuration or maintenance

• Foundation for specialized deployments and appliances
Reduced Attack Surface
Oracle Solaris Secure by Default

• **Expose only required services to the network**
  – Reduce the operating system network footprint
  – Most services are disabled; a few are set to “local only”
  – Secure Shell is the only exposed service by default

• **Integrated with Service Management Facility**
  – Common administrative model for all service operations
  – Fully customizable based upon unique site requirements

• **Foundation for Additional Network Protections**
  – Host-based packet filtering (Solaris IP Filter)
  – Secure authentication (Solaris Kerberos)
  – Secure network communications (Solaris IPsec / IKE)
Separation of Duty
Oracle Solaris User Rights Management

- Method for composing collections of administrative rights
- Rights can be assigned to individual users and roles
- Rights are specified using hierarchical profiles and authorizations
- Roles can only be assumed by authorized users
- Auditing always tracks the 'real' user – no anonymous admin!
Separation of Duty Example
Oracle Solaris User Rights Management

- System Maintenance, Troubleshooting
- System Security Review, Audit Trail Review
- Database Administration

Rights
User Rights Management
User Roles

System Admin.
Internal Auditor
Oracle DBA
Separation of Duty Example
Oracle Solaris User Rights Management

Users
  jdoe@ozone

Roles
  oracle

Rights Profiles
  Oracle Management

Authorizations
  solaris.smf.manage.oracle.database
  solaris.smf.manage.oracle.listener
Least Privilege
Oracle Solaris Process Rights Management

- Eliminates need for many services to start as ‘root’
- Reduces potential exposure to a variety of security attacks
- Decomposes administrative capabilities into discrete privileges
- Completely compatible with traditional super-user privilege model
- Always enabled and enforced by the Solaris kernel
Least Privilege Example
Oracle Solaris Process Rights Management

Privilege Collection #1
Privilege Collection #2
Privilege Collection #3

Privileges
Process Rights Management
Processes
Least Privilege Example
Oracle Solaris Process Rights Management

$ pfexec ppriv -S `pgrep rpcbind`
933: /usr/sbin/rpcbind
flags = PRIV_AWARE
  E: net_bindmlp,net_privaddr,proc_fork,sys_nfs
  I: none
  P: net_bindmlp,net_privaddr,proc_fork,sys_nfs
  L: none

$ pfexec ppriv -S `pgrep statd`
5139: /usr/lib/nfs.statd
flags = PRIV_AWARE
  E: net_bindmlp,proc_fork
  I: none
  P: net_bindmlp,proc_fork
  L: none

Every process has a unique set of privileges.
Strong Isolation and Resource Control

<table>
<thead>
<tr>
<th>Hard Partitions</th>
<th>Hypervisor Mediation</th>
<th>Kernel Separation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPARC M-Series</td>
<td>SPARC T-Series</td>
<td>SPARC T-Series</td>
</tr>
<tr>
<td>Oracle Dynamic Domains</td>
<td>x86/x64</td>
<td>SPARC M-Series</td>
</tr>
<tr>
<td></td>
<td>Oracle VM Server for SPARC</td>
<td>x86/x64</td>
</tr>
<tr>
<td></td>
<td>Oracle VM Server for x86</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oracle VM VirtualBox</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Oracle Solaris Containers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Zones + SRM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Oracle Solaris</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trusted Extensions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Oracle Solaris 8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and 9 Containers</td>
</tr>
</tbody>
</table>

Multiple OSes → Single OS
Strong Isolation and Resource Control
Oracle Solaris Containers

- Multiple, independent services
- File, network, user, process, and resource isolation
- Security protections
- Single operating system instance
- Centralized management and monitoring
$ pfexec zonecfg -z ozone info
zonename: ozone
zonepath: /export/zones/ozone
[…]
[max-lwps: 300]
[cpu-shares: 100]
fs:
    dir: /etc/security/audit_control
type: lofs
    options: [ro, nosuid, nodevices]
[…]
inherit-pkg-dir:
    dir: /lib
inherit-pkg-dir:
    dir: /platform
inherit-pkg-dir:
    dir: /sbin
inherit-pkg-dir:
    dir: /usr
[…]

Each Container can have its own defined set of resources, file systems, network interfaces, etc.
Comprehensive Monitoring
Oracle Solaris Auditing

- Integration with the Solaris kernel enables fine-grained introspection
- Captured events include administrative actions, commands, syscalls
- Configurable audit policy at both the system and user level
- Containers can be audited from within the global zone
- Audit logs can be exported as binary, text, or XML files
Comprehensive Monitoring
Oracle Solaris Auditing Example

Event: **profile command**
time: 2010-09-08 11:56:11.511 -04:00 vers: 2 mod: host: quasar
SUBJECT **audit-uid**: gbrunett uid: root gid: joe ruid: joe pid: 5015
sid: 685 tid: 0 0 quasar
PATH: /usr/sbin/reboot
CMD
RETURN errval: success retval: 0
ZONE name: ozone

[...]

Event: **reboot(1m)**
time: 2010-09-08 11:56:11.522 -04:00 vers: 2 mod: host: quasar
RETURN errval: success retval: 0
ZONE name: ozone

Activity is captured retaining the ID of the original actor
Assembling the Pieces

Oracle VM for SPARC

CONTROL DOMAIN

GUEST DOMAIN / GLOBAL ZONE

HYPervisor

Copyright © 2010 Oracle Corporation
Assembling the Pieces

Oracle VM for SPARC

CONTROL DOMAIN

GUEST DOMAIN / GLOBAL ZONE

Package Minimization

HYPERVISOR

Oracle VM for SPARC

SOLARIS

SOLARIS

ULTRASPARC
Assembling the Pieces

Oracle VM for SPARC

CONTROL DOMAIN

Oracle SOLARIS

Secure by Default / Network Hardening

Package Minimization

GUEST DOMAIN / GLOBAL ZONE

HYPERVERSOR

Sun ULTRASPARC
Assembling the Pieces

Oracle VM for SPARC

CONTROL DOMAIN

Oracle VM for SPARC

HYPERVERSOR

Resource Control

Secure by Default / Network Hardening

Package Minimization

GUEST DOMAIN / GLOBAL ZONE
Assembling the Pieces

Oracle VM for SPARC

CONTROL DOMAIN

Oracle VM for SPARC

HYPERVERSOR

Auditing

Resource Control

Secure by Default / Network Hardening

Package Minimization

GUEST DOMAIN / GLOBAL ZONE
Assembling the Pieces

Oracle VM for SPARC

CONTROL DOMAIN

CONTAINER

Auditing

Resource Control

Secure by Default / Network Hardening

Package Minimization

GUEST DOMAIN / GLOBAL ZONE

HYPervisor
Assembling the Pieces

Oracle VM for SPARC

CONTROL DOMAIN

CONTAINER

Auditing

Resource Control

Secure by Default / Network Hardening

Package Minimization

GUEST DOMAIN / GLOBAL ZONE

HYPervisor

Copyright © 2010 Oracle Corporation
Assembling the Pieces

Oracle VM for SPARC

CONTROL DOMAIN

CONTAINER

Process Rights Management
Auditing
Resource Control
Secure by Default / Network Hardening
Package Minimization

GUEST DOMAIN / GLOBAL ZONE

HYPervisor

Copyright © 2010 Oracle Corporation
Assembling the Pieces

Oracle VM for SPARC

CONTROL DOMAIN

Oracle VM for SPARC

HYPERVERSOR

CONTAINER

Process Rights Management

User Rights Management

Auditing

Resource Control

Secure by Default / Network Hardening

Package Minimization

GUEST DOMAIN / GLOBAL ZONE

Copyright © 2010 Oracle Corporation
Just the Tip of the Iceberg

• **ZFS Data Security and Integrity**
  – Ensures end-to-end data integrity by design
  – Delivers delegated administration, fine-grained access control, and hierarchical enforcement

• **Unified Cryptographic Framework**
  – Enables hardware acceleration of algorithms
  – Integrates with PKCS#11, JCE, OpenSSL, etc.

• **Service Management Facility**
  – Provides unified way to describe, manage and execute services

• **Trusted Extensions**
  – Enforces multi-level security access control policies
Oracle Database Security
Defense-in-Depth

Encryption and Masking
- Oracle Advanced Security
- Oracle Secure Backup
- Oracle Data Masking

Access Control
- Oracle Database Vault
- Oracle Label Security

Auditing and Tracking
- Oracle Audit Vault
- Oracle Configuration Management
- Oracle Total Recall

Blocking and Monitoring
- Oracle Database Firewall
Complete Set of Secure and Proven Solutions

- Transparency, Governance, and Compliance
- Secure Service Oriented Architectures
- End-to-End Identity and Access Management
- Comprehensive Information Protection and Monitoring
- Security-Enhanced Service Delivery Platforms
- Flexible and Strong Workload Isolation
- Integrated High-Performance Cryptography
- Tamper Resistant Key Storage
For More Information…

An Oracle White Paper
August 2010

Hardening Oracle Database with Oracle Solaris Security Technologies
Oracle Database Security Hands-on-Labs

- Thursday
  - Advanced Security 12:00PM | Marriott Marquis, Salon 10 / 11
  - Audit Vault 1:30PM | Marriott Marquis, Salon 10 / 11
  - Check Availability
  - Check Availability
The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
SOFTWARE. HARDWARE. COMPLETE.