

Oracle Security

Dan Norris

norris@celeritas.com

Celeritas Technologies, LLC

July 15, 2003

Version 1.0.1.332.523.1.0.0.0



Agenda

➤ **Introductions**

- Demonstration Environment Overview
- Security Overview
- OS Security
- Database Security
- 9iAS Security
- Q & A

Who are you?

- DBAs
- Developers (Java, Oracle Tools, MS VB, ASP, .NET)
- System Administrators
- Network Administrators
- Security Administrators

Agenda

- Introductions
- **Demonstration Environment Overview**
- Security Overview
- OS Security
- Database Security
- 9iAS Security
- Q & A

Demo Environment

100Mbit Ethernet

Windows XP
Oracle 9.2.0 client
Oracle 8.1.7 client

Sun SPARC v100
Solaris 8
Oracle 9.2.0 database

Agenda

- Introductions
- Demonstration Environment Overview
- **Security Overview**
- OS Security
- Database Security
- 9iAS Security
- Q & A

Security Overview

- Who needs security?
- Who is responsible for security?
- What is the cost of security?

Agenda

- Introductions
- Demonstration Environment Overview
- Security Overview
- **OS Security**
- Database Security
- 9iAS Security
- Q & A

Operating System Security

- High-level examination
- Think like an attacker and use their tools
- Nmap, Nessus, tripwire, ... (a very long list)
- Use ssh, scp, sftp for terminal access to *nix systems and consider using it for Windows systems too (www.cygwin.com)

OS Security Resources

- www.sans.org: Mailing lists, research, excellent conferences and training
- www.giac.org: Certification information
- www.securityfocus.com: Collection of security information
- www.cisecurity.org: Center for Internet Security
- www.cert.org: Advisories, alerts, etc.

Agenda

- Introductions
- Demonstration Environment Overview
- Security Overview
- OS Security
- **Database Security**
- 9iAS Security
- Q & A

DB Security: Security-related initialization parameters

- OS Authentication: remote_os_authent, remote_os_roles, os_roles
- Remote Management: remote_login_passwordfile
- Filesystem access: utl_file_dir
- Auditing: audit_trail

DB Security: Default User Accounts

- DBSNMP: select_catalog_role
- OUTLN: execute any procedure
- CTXSYS: dba, resource
- WKSYS: drop user, drop tablespace
- WMSYS: unlimited tablespace
- MDSYS: drop user, drop tablespace
- RMAN: alter session, unlimited tablespace

DB Security: Privilege Exploits

- ALTER SESSION SET EVENTS 'IMMEDIATE TRACE NAME SYSTEMSTATE LEVEL 10';
- SELECT * FROM sys.link\$;
- ALTER DATABASE DATAFILE '/a/file.dbf' OFFLINE DROP;

DB Security: Privilege Exploits

- ALTER SYSTEM
 - kill session 'sid,serial#'
 - enable restricted session
 - set transactions = 4
 - archive log stop
 - flush shared_pool

DB Security: Profiles

- Use profiles to:
 - limit failed login attempts
 - limit password life time
 - limit password reuse
 - set a password verification function

DB Security: Network Security

- Set (encrypted) password on TNS listeners
- TCP.VALIDNODE_CHECKING,
TCP.INVITED_NODES,
TCP.EXCLUDED_NODES (sqlnet.ora)
- SQLNET.TRACE_LEVEL_* (DoS)
- TRACE_LEVEL_LISTENER (DoS)
- Use encryption, strong authentication if possible (Advanced Security Option)

DB Security: Application Security

- Secure Application Role (identified by procedure)
- Non-default password-authenticated role
- Login Triggers to set roles (possibly check a table for privilege level)
- Shared schemas (Enterprise Users)
- Proxy users (n-tier environments)
- Use regular DB users and AUTHID CURRENT_USER in PL/SQL
- Exclusive use of PL/SQL for all table access

DB Security: Data Security

- DBMS_OBSFUCATION_TOOLKIT
- Application Encryption (client or midtier)
- PL/SQL-only interfaces to all data
- Fine-grained Access Control (FGAC)
- Virtual Private Database (VPD)
- Oracle Label Security (OLS): add-on option

DB Security: Data Security

- DBMS_OBSFUCATION_TOOLKIT
 - Offers PL/SQL procedures to encrypt and decrypt strings of data
 - PROs: Not even the DBA can read the data, Backups are safer from prying eyes, DES3 is considered relatively strong
 - CONs: “secure key storage” is difficult, only DES or DES3 algorithms supported, PL/SQL programming knowledge required

DB Security: Data Security

- Application Encryption (client or midtier)
 - Methods: Java offers JCE, Microsoft (VB, VBScript, ASP, C++) offers CryptoAPI
 - Pros: In 2-tier, can replace ASO functionality; network encryption not necessary, key storage can be easily kept outside the DB, many different algorithms available
 - Cons: requires powerful client/midtier, can lead to difficult-to-support application implementations

DB Security: FGAC

- Fine-grained Access Control (FGAC)
 - Applies a *WHERE* predicate to all statements against a particular object automatically
 - You must write the function to produce the *WHERE* clause
 - `DBMS_RLS` is the package implementing the APIs for policies
 - Pros: Powerful architecture, “Free”, no way to bypass it with adhoc tool
 - Cons: Requires some PL/SQL programming

DB Security: Data Security

- Virtual Private Database (VPD)
 - Designed as a “dynamic view” by appending WHERE clauses to every statement against a particular table. WHERE clause is produced by a function you write
 - Can be used to allow multiple companies to use the same application database (and same tables), but separate data (think hosting)
 - Pros: Once implemented, very safe, “Free”
 - Cons: Design phase can be difficult, some PL/SQL programming is necessary

DB Security: Data Security

- VPD (cont.)
 - VPD is a group of features: FGAC, application context, and global application context

DB Security: Data Security

- Oracle Label Security (OLS)
 - Built on top of VPD, but requires no coding
 - Add-on \$\$\$ option
 - Used heavily by military and government
 - Performance trade-off
 - Tested security compliance

DB Security: FGA

- Fine-grained Auditing (FGA)
 - Records audit events based on specific data accessed (DBA_FGA_AUDIT_TRAIL)
 - Audit events recorded without any code
 - Can also invoke a custom procedure to do almost anything (for example, send a pager alert)

DB Security: FGA Example

```
CREATE PROCEDURE sec.log_id (schema
    varchar2, table varchar2, policy varchar2)
    AS BEGIN
UTIL_ALERT_PAGER(schema, table, policy);
END;
/***** add the policy *****/
DBMS_FGA.ADD_POLICY( object_schema => 'hr',
    object_name => 'emp',
    policy_name => 'chk_hr_emp',
    audit_condition => 'dept = ''SALES'' ',
    audit_column => 'salary',
    handler_schema => 'sec',
    handler_module => 'log_id',
    enable => TRUE);
```

DB Security: Backups

- Secure backup location (disk or tape)
- Offsite security (if you have offsite storage)
- Transportation security (to/from offsite), think Finance and Healthcare
- File permissions on DB host
- Safety of standby site is just as important as running production site

DB Security: Archived Redo Logs

- Archived redo logs contain all the data in your database
- Even without catalog, useful information can be gleaned from Logminer
- Back them up just as carefully as datafiles
- Ensure they are created with proper OS privileges and permissions

DB Security: Advanced Security Option (ASO)

- Provides:
 - Authentication options: SSL, Kerberos, Biometrics (some versions), Entrust PKI, RADIUS, Smart Cards, Token Cards (SecurID)
 - Network Encryption: DES, 3DES, RC4, AES
 - Checksumming: SHA, MD5
 - Enterprise Users: Global roles, global users

If you were asleep...

- Lock/drop unused database accounts
- Verify password strength
- Check for TNS listener password
- Check OS group privileges
- Keep up-to-date patch levels
- Investigate security of backups
- Investigate application security options
- Use lowest privilege levels necessary

DB Security: Resources

- Server Documentation (yes, really): Developer's Guide, ASO Guide, much better in recent versions than previous ones
- www.sans.org: CVE, Summary Reports include Oracle bugs/vulnerabilities
- metalink.oracle.com: of course 😊
- otn.oracle.com/deploy/security/alerts.htm: postings of current Oracle security alerts

Agenda

- Introductions
- Demonstration Environment Overview
- Security Overview
- OS Security
- Database Security
- **9iAS Security**
- Q & A

9iAS Security

- Turn off all non-necessary services (find them all first)
- Do not run the server as root
- Exclude UTL_% and DBMS_% from mod_plsql DADs
- Change all default passwords (OEM, OID, DAS, webcache, portal, mod_plsql users)
- Use most restrictive file permissions possible on all config files (until server breaks)

9iAS Security

- Ensure status URLs (internal and external) are protected by IP address (allow, deny)
- Watch for security alert announcements and patch server ASAP
- Ensure that all network firewalls are as restrictive as possible
- Use only encrypted methods for username/password transmission (HTTPS for web, SSH for terminal)

Q & A

Dan Norris

norris@celeritas.com

Celeritas Technologies, LLC



Copyright © 2003 Celeritas Technologies, L.L.C.

This work was created by Celeritas Technologies, L.L.C. (“Creator”). This work and all rights therein and thereto, including copyright rights and/or patent rights, are owned by Creator and/or another entity (collectively, “Owner”). This shall serve as notice of such ownership as of the date of this and associated files or subject matter, if any, as depicted above and/or as depicted with an electronic file date stamp and/or any versions thereof and their associated dates, if any.

This work may not be reproduced for any purpose, distributed, modified, reverse-engineered, stored in a retrieval system, transmitted, used, made, offered for sale, or sold, in whole or part, in any form or by any means, electronic, mechanical, audio, photocopying, recording, or otherwise, without the prior written permission of Owner.

This work may not be exported unless in compliance with the applicable technology export laws. While this information is presented in good faith and believed to be accurate, Creator does not guarantee satisfactory or any results from reliance upon such information.

Creator reserves the right, without notice, to alter or improve the designs, specifications, creations, or works of the subject matter herein. Nothing herein is to be construed as a warranty or guarantee, express or implied, against infringement, or regarding performance, merchantability, fitness, or any other matter with respect to products, processes, or any other subject matter herein, and such warranties and guaranties are expressly disclaimed. Nothing herein is to be construed as a recommendation to use any product or process in conflict with any third party rights in any intellectual property.

All products, languages, or trademarked names that are mentioned in this work are acknowledged to be the proprietary property of the respective owner.

