PeopleSoft
Database Security

May 12, 2016

Michael Miller
Chief Security Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation
PeopleSoft Database Security

Oracle Database Attacks

What You Should Be Doing

Database Security Program

Q&A
About Integrigy

**Products**

**AppSentry**
ERP Application and Database Security Auditing Tool

**AppDefend**
Enterprise Application Firewall for the Oracle E-Business Suite

**Services**

**Security Assessments**
ERP, Database, Sensitive Data, Pen Testing

**Compliance Assistance**
SOX, PCI, HIPAA

**Security Design Services**
Auditing, Encryption, DMZ

**Databases**
Oracle, Microsoft SQL Server, MySQL, Sybase, DB2

**ERP Applications**
Oracle E-Business Suite, PeopleSoft, SAP
PeopleSoft Database Security

Oracle Database Attacks

What You Should Be Doing

Database Security Program

Q&A
Does PeopleSoft protect and secure the database? **No**
Database security decays over time due to complexity, usage, application changes, upgrades, published security exploits, etc.
Database Security is a complex challenge

Every direct database connection is a security risk
Agenda

1. PeopleSoft Database Security
2. Oracle Database Attacks
3. What You Should Be Doing
4. Database Security Program
5. Q&A
Advanced Persistent Threat (APT)
Organized Crime
State Sponsored
Anonymous, LulzSec, Legion of Doom, ...
<table>
<thead>
<tr>
<th>Range</th>
<th>Information</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 – $5</td>
<td>First and last name, Social Security number</td>
<td>Tax information (e.g., 1099)</td>
</tr>
<tr>
<td>$20 – $40</td>
<td>First and last name, Social Security number, Current address, Date of birth</td>
<td>Health care Human Resources</td>
</tr>
<tr>
<td>$30 – $100</td>
<td>First and last name, Social Security number, Current address, Date of birth, Bank account number or credit card number, Salary</td>
<td>Payroll</td>
</tr>
</tbody>
</table>

*Assuming financial and not political and/or hacktivist motivation*
Oracle Database Attack Tools

- **Used for both white-hat (good) and black-hat (evil)**
  - Mature, powerful and freely downloadable tools
  - Do not require expert Oracle knowledge
  - Most exploits seek to gain full control over database
  - Come with user guides and examples
  - Tools: Metasploit and Oracle Attack Tool

- **Older and unpatched versions of Oracle are much more vulnerable**
  - All databases with default and weak passwords are at risk
# Asset and Data Discovery Techniques

<table>
<thead>
<tr>
<th>Passive</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Search internal knowledge repositories for architecture diagrams, design documents, code repositories, etc.</td>
<td>▪ Compromise DBA credentials through phishing or social engineering attacks</td>
</tr>
<tr>
<td>▪ Find TNSNAMES.ORA files</td>
<td>▪ Install malware on DBA machines and steal credentials, such as saved in SQL Developer</td>
</tr>
<tr>
<td></td>
<td>▪ Use Nmap to scan internal network for Oracle Databases on default port 1521 – very noisy</td>
</tr>
</tbody>
</table>
# Default Oracle Password Statistics

<table>
<thead>
<tr>
<th>Database Account</th>
<th>Default Password</th>
<th>Exists in Database %</th>
<th>Default Password %</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS</td>
<td>CHANGE_ON_INSTALL</td>
<td>100%</td>
<td>3%</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>MANAGER</td>
<td>100%</td>
<td>4%</td>
</tr>
<tr>
<td>DBSNMP</td>
<td>DBSNMP</td>
<td>99%</td>
<td>52%</td>
</tr>
<tr>
<td>OUTLN</td>
<td>OUTLN</td>
<td>98%</td>
<td>43%</td>
</tr>
<tr>
<td>MDSYS</td>
<td>MDSYS</td>
<td>77%</td>
<td>18%</td>
</tr>
<tr>
<td>ORDPLUGINS</td>
<td>ORDPLUGINS</td>
<td>77%</td>
<td>16%</td>
</tr>
<tr>
<td>ORDSYS</td>
<td>ORDSYS</td>
<td>77%</td>
<td>16%</td>
</tr>
<tr>
<td>XDB</td>
<td>CHANGE_ON_INSTALL</td>
<td>75%</td>
<td>15%</td>
</tr>
<tr>
<td>DIP</td>
<td>DIP</td>
<td>63%</td>
<td>19%</td>
</tr>
<tr>
<td>WMSYS</td>
<td>WMSYS</td>
<td>63%</td>
<td>12%</td>
</tr>
<tr>
<td>CTXSYS</td>
<td>CTXSYS</td>
<td>54%</td>
<td>32%</td>
</tr>
</tbody>
</table>

* Sample of 120 production databases
Database Link Case Study

**Overview**
- Organization with about 150 production Oracle Databases
- Integrigy assessed 15 key SOX and PCI compliance Oracle databases
- Reviewed database links for connectivity and appropriateness

**Conclusion**
Database links are widely used in most organizations
## TNS Poisoning Attack – Man-in-Middle

<table>
<thead>
<tr>
<th>Vuln #</th>
<th>Component</th>
<th>Protocol</th>
<th>Package and/or Privilege Required</th>
<th>Remote Exploit without Auth.?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2012-1675</td>
<td>Listener</td>
<td>Oracle Net</td>
<td>None</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### CVSS VERSION 2.0 RISK

<table>
<thead>
<tr>
<th>Base Score</th>
<th>Access Vector</th>
<th>Access Complexity</th>
<th>Authentication</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Last Affected Patch set (per Supported Release)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5</td>
<td>Network</td>
<td>Low</td>
<td>None</td>
<td>Partial+</td>
<td>Partial+</td>
<td>Partial</td>
<td>ALL VERSIONS</td>
</tr>
</tbody>
</table>

- **This vulnerability is not patched by a SPU or PSU.** The TNS Listener configuration must be secured.
- **ALL VERSIONS** of the Oracle Database are affected.
- 12c and 11.2.0.4 protected by default, but vulnerable when Valid Node Checking Registration (VNCR) is disabled.
# TNS Poisoning Mitigation

<table>
<thead>
<tr>
<th>Database Version</th>
<th>SSL Encrypt with Cert</th>
<th>COST class of secure transport</th>
<th>VNCR Valid node checking registration</th>
</tr>
</thead>
<tbody>
<tr>
<td>References</td>
<td>See ASO</td>
<td>1453883.1 1340831.1 (RAC)</td>
<td>1600630.1</td>
</tr>
<tr>
<td>8.1.7.x – 10.2.0.3</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.2.0.3 – 10.2.0.5</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>11.1.0.x</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>11.2.0.1 – 11.2.0.3</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>11.2.0.4*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>12.1.0.x*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

* 11.2.0.4 and 12c does not allow remote registration by default.
Agenda

1. PeopleSoft Database Security
2. Oracle Database Attacks
3. What You Should Be Doing
4. Database Security Program
5. Q&A
Traditional Database Security Approaches

Database security checklists are used to secure databases one at a time.

- **Excellent baseline and starting point**

- Often in conflict with application configuration

- Too many exceptions required to handle application limitations

- Security decay requires constant or periodic assessments
## Supported Database Versions and CPUs

<table>
<thead>
<tr>
<th>Database</th>
<th>PeopleTools</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>8.55</td>
</tr>
<tr>
<td>12.1.0.2</td>
<td>✔</td>
</tr>
<tr>
<td>12.1.0.1 (7/2016)</td>
<td>✔</td>
</tr>
<tr>
<td>11.2.0.4 (10/2020)</td>
<td>✔</td>
</tr>
<tr>
<td>11.2.0.3</td>
<td>✔</td>
</tr>
<tr>
<td>11.2.0.2</td>
<td>✔</td>
</tr>
<tr>
<td>11.1.0.7</td>
<td>✔</td>
</tr>
<tr>
<td>10.2.0.5</td>
<td>✔</td>
</tr>
</tbody>
</table>

Do you need to apply both application and database CPUs?  Yes

Is database security more than just applying CPUs? Yes
Integrigy #1 Security Recommendation

- Limit direct database access whenever possible
  - Much harder to hack database if attacker cannot connect

- Use firewalls in front of data center, network ACLs, TNS invited nodes, Oracle Connection Manager, Oracle Database Firewall, etc.
  - DBAs should use bastion hosts to manage databases
Database Security Preventative Controls

- **Apply Oracle Critical Patch Updates on a regular basis on all databases**
  - Reduce risk of compromise and escalation of privileges

- **October 2014 PeopleTools CPU must be applied**
  - Connect ID used to authenticate users has access to the table PSACCESSPRFL
  - Script to decrypt to Access ID password freely available on Internet
  - CPU changes encryption: 8.52.24, 8.53.17, 8.54.04
PeopleSoft Database Security Specific Controls

- **Secure PeopleSoft database passwords**
  - Secure key accounts: Connect Id, Access Id, IB and PS
  - Change regularly and no defaults e.g. PEOPLE/PEOP1e
  - Password should never equal username or be shared

- **Default tablespace should never be ‘SYSTEM’**
  - Never for Connect ID
  - Only SYS and SYSTEM should use the SYSTEM tablespace

- **Encrypt SYSADM password**
  - Use psadmin utility to encrypt passwords in config files

- **Ensure EnableDBMonitoring is ALWAYS enabled**
  - Enabled by Default (psappssrv.cfg)
  - Populates client_info with user, IP address and program name
PeopleSoft Database Security Specific Controls

- **One PeopleSoft database per Oracle RDBMS instance**
  - Production must be exclusive
  - No demo databases for production

- **User tablespaces should never use PSDEFAULT**
  - Reserve for application use only

- **Do not use SYSADM for day-to-day support**
  - Use named accounts

- **Check for Public grants**
  - Any connection to the database has ‘PUBLIC’
PeopleSoft – Application

- **Application Accounts**
  - Standard accounts and default passwords
  - Password policies

- **Application authorization**
  - Guest account menus and roles
  - Administrator and webprofile roles
  - Sensitive roles and menus
  - PeopleTools

- **Application auditing**
PeopleSoft - Additional

- **WebLogic**
  - Passwords
  - Security baseline
  - Console security and whitelisting

- **Security settings**
  - Web portal
  - Jolt
  - Tuxedo
  - Integration Broker

- **PSKEY password and template file encryption**
Create Fewer Insiders With Password Controls

1. Don’t share passwords between production and non-production
2. Rotate passwords regularly
3. Use a password safe
4. Don’t forget about Oracle database default accounts
Constantly Check for Weak and Default Passwords

- Use Oracle’s DBA_USERS_WITH_DEFPWD
  - Limited set of accounts
  - Single password for each account

- Command line tools (orabf, etc.)
  - Difficult to run – command line only

- AppSentry
  - Checks all database accounts
  - Uses passwords lists - > 1 million passwords
  - Allows custom passwords
# Use Database Profiles to Manage Passwords by Risk

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT</td>
<td>None</td>
</tr>
<tr>
<td>&lt;your org&gt;_PROFILE</td>
<td>All named accounts</td>
</tr>
<tr>
<td>DB_PROFILE</td>
<td>All standard Oracle Database accounts and all non-interactive application accounts (e.g. SYS, SYSTEM, DBSNMP, CTXSYS, etc.)</td>
</tr>
<tr>
<td>APP_PROFILE</td>
<td>All interactive application databases including web application and interface accounts (e.g. PS owner, access and PS IDs)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Resource Name</th>
<th>Current Default</th>
<th>Suggested Default</th>
<th>&lt;your org&gt;_PROFILE</th>
<th>DBPROFILE</th>
<th>APP_PROFILE</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAILED_LOGIN_ATTEMPTS</td>
<td>UNLIMITED</td>
<td>10</td>
<td>5</td>
<td>10</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>PASSWORD_GRACE_TIME (Days)</td>
<td>UNLIMITED</td>
<td>7</td>
<td>10</td>
<td>10</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>PASSWORD_LIFE_TIME (Days)</td>
<td>UNLIMITED</td>
<td>180</td>
<td>90</td>
<td>365</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>PASSWORD_LOCK_TIME (Days)</td>
<td>UNLIMITED</td>
<td>1</td>
<td>DEFAULT</td>
<td>DEFAULT</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>PASSWORD_REUSE_MAX (Passwords)</td>
<td>UNLIMITED</td>
<td>UNLIMITED</td>
<td>DEFAULT</td>
<td>DEFAULT</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>PASSWORD_REUSE_TIME (Days)</td>
<td>UNLIMITED</td>
<td>UNLIMITED</td>
<td>DEFAULT</td>
<td>DEFAULT</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>PASSWORD_VERIFY_FUNCTION</td>
<td>NULL</td>
<td>XOR_VERIFY_FUNC</td>
<td>XOR_VERIFY_FUNC</td>
<td>XOR_VERIFY_FUNC</td>
<td>XOR_VERIFY_FUNC</td>
</tr>
<tr>
<td>Database Accounts</td>
<td>None</td>
<td>None</td>
<td>All individual accounts</td>
<td>All standard Oracle DB accounts</td>
<td>All interactive application accounts</td>
</tr>
</tbody>
</table>
Operational Controls Around Oracle Password Profiles

**Database Security Standard**

Standard set of profiles and settings are defined for all database.

ACME_USER, ACME_SERVICE, ACME_DBA, ACME_DEFAULT

**Database Configuration Validation**

1. Check for standard set of profiles
2. Check settings for profiles
3. Check all accounts assigned standard set of profiles (rogue accounts, procedure violations)

**Database Auditing**

1. Alert on out of compliance changes to profiles
2. Audit all changes to profiles and capture change ticket number

**Database Security Compliance**

1. Use database profiles to categorize accounts for reporting and quarterly access reviews
Database auditing in most organizations done simply for a compliance checkbox.

- Auditing poorly defined
- No review of audit data
- No mapping of business requirements to auditing, alerts, or reports
- Zero value to the organization
Native Oracle Database Auditing

1. Listener
   - LOGGING_name = ON
   - TNS_ADMIN/log dir

2. DB Alert Log
   - DB Alert Log
   - BG_DUMP_DEST dir

3. SYS Auditing
   - AUDIT_SYS_OPERATIONS
   - AUDIT_SYSLOG_LEVEL
   - Syslog
   - BG_DUMP_DEST dir

4. Native Auditing
   - Standard Auditing
   - AUDIT_TRAIL
   - DB
   - AUD$ table
   - AUDIT_FILEDEST dir

5. Fine Auditing
   - Fine Grained Auditing
   - DBMS_FGA.add_policy
   - AUDIT_FILE_DEST dir
   - FGA_LOG$ table

Type of auditing and logging
Audit and logging parameters
Location of audit data
Intelligent and business-focused auditing and monitoring

- Transform audit data into actionable information
- Use auditing as mitigating control when necessary
- Auditing is in harmony with database security program to proactively identify non-compliance
- Solve compliance and security challenges – change ticket tracking and workflow
Integrigy Framework for Database Auditing

- Payment Card (PCI DSS)
- SOX (COBIT)
- HIPAA (NIST 800-66)
- FISMA (NIST 800-53)
- IT Security (ISO 27001)

Foundation security events and actions
(logins, logoffs, account creation, privileges, etc.)

Database
- Native Auditing
- Syslog
- DB log files

Application
- Signon
- Audit Tables
- Navigation

Centralized Logging Solution (e.g. Splunk)
- Protected Audit Data
- Alerting & Monitoring
- Reporting
- Correlation

Integrigy Framework for Auditing and Logging
The foundation of the framework is a set of key security events and actions derived from and mapped to compliance and security requirements that are critical for all organizations.

<table>
<thead>
<tr>
<th>Event/Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1 - Login</td>
<td></td>
</tr>
<tr>
<td>E2 - Logoff</td>
<td></td>
</tr>
<tr>
<td>E3 - Unsuccessful login</td>
<td></td>
</tr>
<tr>
<td>E4 - Modify auth mechanisms</td>
<td></td>
</tr>
<tr>
<td>E5 - Create user account</td>
<td></td>
</tr>
<tr>
<td>E6 - Modify user account</td>
<td></td>
</tr>
<tr>
<td>E7 - Create role</td>
<td></td>
</tr>
<tr>
<td>E8 - Modify role</td>
<td></td>
</tr>
<tr>
<td>E9 - Grant/revoke user privileges</td>
<td></td>
</tr>
<tr>
<td>E10 - Grant/revoke role privileges</td>
<td></td>
</tr>
<tr>
<td>E11 - Privileged commands</td>
<td></td>
</tr>
<tr>
<td>E12 - Modify audit and logging</td>
<td></td>
</tr>
<tr>
<td>E13 - Create, Modify or Delete object</td>
<td></td>
</tr>
<tr>
<td>E14 - Modify configuration settings</td>
<td></td>
</tr>
<tr>
<td>Security Events and Actions</td>
<td>PCI DSS 10.2</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>E1 - Login</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E2 - Logoff</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E3 - Unsuccessful login</td>
<td>10.2.4</td>
</tr>
<tr>
<td>E4 - Modify authentication mechanisms</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E5 - Create user account</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E6 - Modify user account</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E7 - Create role</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E8 - Modify role</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E9 - Grant/revoke user privileges</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E10 - Grant/revoke role privileges</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E11 - Privileged commands</td>
<td>10.2.2</td>
</tr>
<tr>
<td>E12 - Modify audit and logging</td>
<td>10.2.6</td>
</tr>
<tr>
<td>E13 - Objects Create/Modify/Delete</td>
<td>10.2.7</td>
</tr>
<tr>
<td>E14 - Modify configuration settings</td>
<td>10.2.2</td>
</tr>
</tbody>
</table>
EnableDBMonitoring allows database auditing to capture web application end-users and correlate the application end-user to SQL statements.

Use CLIENT_INFO for DAM solutions (e.g. Splunk)

<table>
<thead>
<tr>
<th>DB User</th>
<th>OS User</th>
<th>Client IP</th>
<th>Program</th>
<th>SQL</th>
<th>Application User</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSADM</td>
<td>PS</td>
<td>192.168.1.11</td>
<td>PSAPPSRV.exe</td>
<td>select * from ps_person</td>
<td>jack</td>
</tr>
</tbody>
</table>

```
select sid, serial#, username, program, module, client_info from v$session
```
Database Auditing Effort by Task

- Monitoring, Alerting, Reporting, Reviewing: 80%
- Archiving & Purging: 10%
- Designing: 5%
- Enabling: 5%
Encryption Options

- **Storage (Data at rest)**
  - Disk, storage, media level encryption
  - Encryption of data at rest such as when stored in files or on media

- **Access (Data in use)**
  - Application or database level encryption
  - Encryption of data with access permitted only to a subset of users in order to enforce segregation of duties

- **Network (Data in motion)**
  - Encryption of data when transferred between two systems
  - SQL*Net encryption (database)
Misconceptions about Database Storage Encryption

- **Not an access control tool**
  - Encryption does not solve access control problems
  - Data is encrypted the same *regardless* of user
  - Coarse-grained file access control only

- **No malicious employee protection**
  - Encryption does not protect against malicious privileged employees and contractors
  - DBAs have full access

- **Key management determines success**
  - Access to Oracle wallets (TDE) controls everything
  - You and only you can should control the keys

- **More is not better**
  - Performance cost of encryption
  - Cannot encrypt everything
### Storage/Access Oracle Encryption Solutions

| Application (access ~ role) | PeopleCode Encryption  
|                           | Database Encryption API (DBMS_CRYPTO/Voltage) |
| Database (access ~ db account) | View/Trigger Encryption |
| Disk/Storage (access = database) | Transparent Data Encryption (TDE)  
|                                 | Third-party Solutions (e.g., Vormetric)  
|                                 | Disk/SAN Vendor Encryption Solutions  
|                                 | Backup Encryption (e.g., RMAN) |
PeopleTools Application Encryption

- **Encrypt, decrypt, sign, and verify fields in a database or external files**
  - Obtain library (e.g. PGP). Open source OpenSSL provided.
  - Develop API glue code to library (if not OpenSSL or PGP)
  - Write PeopleCode to invoke

- **Note full table encryption (PTENCRYPTPET/PTDECRYPTPET) “is not intended for widespread usage”**
  - Used to encrypt encryption keys (DOC ID 1382024.1)

- **PeopleTools Application Designer option for field “column” level encryption with Oracle TDE**
  - Will cover later

What is Oracle TDE?

- **Transparent database encryption**
  - Requires no application code or database structure changes to implement
  - Only major change to database function is the Oracle Wallet must be opened during database startup
  - Add-on feature licensed with Advanced Security Option

- **Column or Full Tablespace**

- **Column encryption restrictions (not Tablespace)**
  - Cannot be a foreign key or used in database constraint
  - Only simple data types like number, varchar, date, ...
  - Less than 3,932 bytes in length
What does TDE do and not do?

- TDE only encrypts “data at rest”

- TDE protects data if following is stolen or lost -
  - disk drive
  - database file
  - backup tape of the database files

- An authenticated database user sees no change

- Does TDE meet legal requirements for encryption?
  - California SB1386, Payment Card Industry Data Security
  - Ask your legal department
PeopleSoft Oracle TDE Support

- **Supports both Column and Tablespace Encryption**
  - Column ‘field’ encryption supported from Application Designer (e.g. Social Security Number field is tagged for encryption)
  - No changes required for Tablespace encryption

- **Certifications**
  - PeopleTools release 8.46 and higher on Oracle 10gR2 and higher can use TDE column encryption
  - PeopleTools release 8.48 and higher on Oracle 11g and higher can use TDE tablespace encryption

- **More information:**
Consider Using Oracle Database Vault

- **Enhanced data protection**
  - Prevent ad-hoc access to sensitive data by privileged users
  - Define and enforce trusted paths & operational controls
  - Segregation of duties between DBA and security administrator

- **Layer on top of existing database**
  - No effect on direct object privileges or PUBLIC object privileges

- **Rule driven**
  - Control individual SQL commands, privileges
  - Control by IP address, time, etc.

- **Includes audit reporting**
  - Privilege analysis and success/failure

- **Add-on option, licensed separately**
  - PeopleTools 8.46 and higher
  - Out-of-box realms for PeopleSoft
Oracle Database Vault

- Database DBA attempts remote "alter system"
  Rule based on **IP Address** blocks action

- PeopleSoft DBA performs unauthorized actions during production
  Rule based on **Date and Time** blocks action

Factors and Command Rules provide flexible and adaptable security controls
Database Vault Support for PeopleSoft

- **Database realm for PeopleSoft**
  - Default realm protects all PeopleSoft data against unauthorized access by privileged users and DBAs

- **New PSFTDBA account created for DBAs**
  - Blinds DBAs to PS data while allowing day-to-day support
  - Access Id used only by application
  - Recommend auditing usage of Access Id, SYSTEM, SYSDBA

- **Filters for direct database access using Connect command rules**
  - Pre-defined list of processes: middle tier, PeopleTools, Cobol
  - Recommend extending to specify IP address or hostname

*Value proportionately diluted by who has what password*
### Database Vault Protection Matrix (Default)

<table>
<thead>
<tr>
<th>Database Vault</th>
<th>Access Id (SYSADM)</th>
<th>DBA (PSFTDBA)</th>
<th>SYSTEM</th>
<th>SYSDBA</th>
<th>O/S Root</th>
</tr>
</thead>
<tbody>
<tr>
<td>PeopleSoft Realm</td>
<td>Owner</td>
<td>When/How?</td>
<td>When/How?</td>
<td>No protection</td>
<td></td>
</tr>
<tr>
<td>Drop Tablespace Command Rule</td>
<td>Disabled Rule Set</td>
<td>When/How?</td>
<td>When/How?</td>
<td>No protection</td>
<td></td>
</tr>
</tbody>
</table>

* Can still issue all other DML e.g. UPDATE
Use Command Rules to limit Direct Database Access

<table>
<thead>
<tr>
<th>User</th>
<th>IP Address</th>
<th>Program</th>
<th>OS User</th>
</tr>
</thead>
<tbody>
<tr>
<td>o1 - SYS</td>
<td>database server</td>
<td>unlimited</td>
<td>oracle</td>
</tr>
<tr>
<td>o2 - SYSTEM</td>
<td>PS server</td>
<td>unlimited</td>
<td>oracle/ps</td>
</tr>
<tr>
<td>o3 - Management</td>
<td>OEM server</td>
<td>unlimited</td>
<td>oracle</td>
</tr>
<tr>
<td>o4 - Backup</td>
<td>backup server</td>
<td>unlimited</td>
<td>oracle</td>
</tr>
<tr>
<td>a1 - Interactive</td>
<td>PS server</td>
<td>unlimited</td>
<td>oracle/ps</td>
</tr>
<tr>
<td>a2 - Data Owner</td>
<td>PS server</td>
<td>unlimited</td>
<td>oracle/ps</td>
</tr>
<tr>
<td>a3 - Interface</td>
<td>per interface</td>
<td>per interface</td>
<td>per interface</td>
</tr>
<tr>
<td>u1 - DBA</td>
<td>PS server &amp; jump</td>
<td>unlimited</td>
<td>unlimited</td>
</tr>
<tr>
<td>u2 - Client/Server</td>
<td>none</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>u3 - Ad-hoc</td>
<td>unlimited</td>
<td>approved list</td>
<td>unlimited</td>
</tr>
</tbody>
</table>

1 Could you attempt the same with VPD and logon triggers?
2 Program and OS user may be spoofed by the client and are not fully reliable.
<table>
<thead>
<tr>
<th>Data Access Method and Threats</th>
<th>Oracle Options</th>
<th>1 App Encrypt</th>
<th>2 Trigger View</th>
<th>3 Oracle TDE</th>
<th>4a FGAC</th>
<th>4b Internal Audit</th>
<th>4c External Audit</th>
<th>3 + 4 TDE + Auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Application access by end-users (role/RBAC)</td>
<td></td>
<td>E</td>
<td>E</td>
<td></td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>2. Application access by application administrators</td>
<td></td>
<td>E+</td>
<td>E-</td>
<td></td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>3. Database access by DBA</td>
<td></td>
<td>E</td>
<td>E</td>
<td></td>
<td>C</td>
<td>A+</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>4. Database access by application DBA (SYSTEM, SYSADM)</td>
<td></td>
<td>E+</td>
<td>E+</td>
<td></td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
</tr>
<tr>
<td>5. Database access by other database accounts</td>
<td></td>
<td>E</td>
<td>E</td>
<td></td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>6. Operating system access to database data files</td>
<td></td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td></td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>7. On-line or off-line access to database backups</td>
<td></td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td></td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>8. Exploitation of applications security vulnerabilities</td>
<td></td>
<td>E-</td>
<td>E-</td>
<td></td>
<td>C+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
</tr>
<tr>
<td>9. Exploitation of Oracle Database security vulnerabilities</td>
<td></td>
<td>E+</td>
<td>E+</td>
<td></td>
<td>C+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
</tr>
<tr>
<td>10. Exploitation of operating system security vulnerabilities</td>
<td></td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td></td>
<td>E</td>
<td></td>
</tr>
</tbody>
</table>

E = Encrypted,  C = Access Controlled,  A = Access Audited,  + = Mostly  - = Partially
Agenda

1. PeopleSoft Database Security
2. Oracle Database Attacks
3. What You Should Be Doing
4. Database Security Program
5. Q&A

What You Should Be Doing
# Database Security Program Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inventory</strong></td>
<td>- An inventory of all databases and sensitive data locations &lt;br&gt;- Methods and processes to maintain the inventories</td>
</tr>
</tbody>
</table>
Processes should be unified, but standards and procedures need to be vendor specific.

Unified Database Security Processes

- Oracle Standards & Procedures
- SQL Server Standards & Procedures
- DB2 Standards & Procedures
- Big Data/NoSQL Standards & Procedures
DB Security Standards - Structure

Security Baseline – All Databases

- Security
- IT General Controls
- Basic Change Management

Oracle Standard
SQL Server Standard
DB2 Standard
Big Data/NoSQL Standard

SOX
Financial Data
External Audits

PCI
Credit Cards
QSA Audits

HIPAA
Health Data

Additional compliance and security requirements
Contact Information

web: www.integrigy.com

e-mail: info@integrigy.com

blog: integrigy.com/oracle-security-blog