IT Security Briefing:
Security Risks in the Oracle Database

Stephen Kost
Chief Technology Officer
Integry Corporation

Phil Reimann
Director of Business Development
Integry Corporation

November 18, 2010
Background

Speaker

Stephen Kost
- CTO and Founder
- 16 years working with Oracle
- 12 years focused on Oracle security
- DBA, Apps DBA, technical architect, IT security, ... 

Company

Integrigy Corporation
- Integrigy bridges the gap between databases and security
- Security Design and Assessment of Oracle Databases
- Security Design and Assessment of the Oracle E-Business suite
- AppSentry - Security Assessment Software Tool
Agenda

1. Security Challenges
   - Key Database Security Risks

2. DB Security Strategy

3. DB Security Solutions

4. Q&A

INTEGRIGY
Database connectivity is a complex problem.

- Ad-hoc Users
- Application
- Reporting Tools
- Batch Processing
- Interfaces and Feeds
- DBAs
- Application Admins
- Backup Tools
- Management Tools
Database security **decays** over time.
Organizational Misalignment

- **IT Security**
  - Excellent at network and operating system security
  - Limit or no understanding of database security
  - Securing Oracle EBS is different than networks and operating systems
    - SQL, application architectures, data warehousing, etc.

- **Risk Management**
  - Database risk not properly quantified
  - Data classification not extended to caretaker of data
  - Databases and applications poor at handling data classification

- **Database Administrators (DBAs)**
  - Not aware of security requirements nor security-focused
  - No time to properly secure the database and application
  - Always afraid of impacting the application or performance of the database
Security and Compliance Drivers

- **Sarbanes-Oxley (SOX)**
  - Database object, structure, and configuration changes
  - User and privilege creation, deletion, and modification
  - Reports for sampling of changes to change tickets

- **Payment Card Industry - Data Security Standard (PCI-DSS)**
  - 12 stringent security requirements

- **Privacy (National/State Regulations)**
  - Read access to sensitive data (National Identifier and Bank Account Number)
  - California and Massachusetts data privacy laws

- **Business Audit and Security Requirements**
  - Internal adoption of COBIT or COSO
  - Preventative and detective controls
PCI-DSS Compliance Example

- PCI 6.1 – “Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.”

- Few Oracle customers install patches within 30 days
- Most customers are 1 to 2 quarters behind
- Business must prioritize applying security patches – effort to functionally test and apply, down-time

- See Integrigy Whitepaper “Oracle Applications 11i: Credit Cards and PCI Compliance Issues”
Agenda

1. Security Challenges
2. Key Database Security Risks
3. DB Security Strategy
4. DB Security Solutions
5. Q&A
Key Security Risks

1. Exploitation of Oracle security vulnerabilities
2. Brute forcing of Oracle database passwords
3. Lack of and trustworthiness of DB auditing
# Database Vulnerabilities (October 2010)

<table>
<thead>
<tr>
<th>Supported Database Version</th>
<th>Exploitable Without Authentication</th>
<th>PUBLIC</th>
<th>Other Advanced Privileges (i.e., SELECT_CATALOG_ROLE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.0.5</td>
<td>CVE-2010-2407 - XDK</td>
<td>CVE-2010-2419 - JVM CVE-2010-2391 - Core</td>
<td>CVE-2010-2415 - CDC</td>
</tr>
<tr>
<td>10.2.0.4</td>
<td>CVE-2010-2407 - XDK</td>
<td>CVE-2010-2419 - JVM</td>
<td>CVE-2010-2415 - CDC</td>
</tr>
<tr>
<td>11.1.0.7</td>
<td>CVE-2010-2407 - XDK</td>
<td>CVE-2010-2419 - JVM CVE-2010-2412 - OLAP</td>
<td>CVE-2010-2415 - CDC</td>
</tr>
<tr>
<td>11.2.0.1</td>
<td></td>
<td>CVE-2010-2419 - JVM</td>
<td>CVE-2010-2415 - CDC</td>
</tr>
<tr>
<td>Unsupported Versions</td>
<td></td>
<td></td>
<td>CVE-2010-1321 - CDC CVE-2010-2411 - Job Queue</td>
</tr>
</tbody>
</table>
Who can exploit a PUBLIC bug?

Anyone with a database account

Remember those application accounts with generic passwords such as APPLSYS/PUB in Oracle E-Business Suite
### Oct 2010 DB Bugs – Highest Risk

<table>
<thead>
<tr>
<th>CVE</th>
<th>Component</th>
<th>CVSS 2.0</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2010-2419</td>
<td>Java Virtual Machine</td>
<td>6.5</td>
<td>Requires only CREATE SESSION system privilege</td>
</tr>
</tbody>
</table>
|             |               |          | Conf = Partial+  
|             |               |          | Integrity = Partial+  
|             |               |          | Avail = Partial+  
|             |               |          | Requires Auth = Yes  |
| CVE-2010-2412 | OLAP          | 5.5      | Requires only CREATE SESSION system privilege                        |
|             | 11.1.0.7 only |          | Conf = Partial+  
|             |               |          | Integrity = Partial+  
|             |               |          | Avail = None  
|             |               |          | Requires Auth = Yes  |
| CVE-2010-2319 | Core RDBMS    | 3.6      | Requires only CREATE SESSION system privilege                        |
|             | 10.1.0.5 and 10.2.0.3 only |          | Conf = Partial  
|             |               |          | Integrity = Partial  
|             |               |          | Avail = None  
|             |               |          | Requires Auth = Yes  |

*Similar to April 2010 Java Bugs (CVE-2010-0866 and CVE-2010-0867)*
Vulnerability Demonstration

Oracle Database Java 0-day release at Black Hat DC 2010 – February 2, 2010
Oracle CPU Patching Metric

Security Patches - Months Behind

Months

Production Databases
Oracle CPU Patching Metric

Security Patches - Months Behind

- “n-1” patching standard
- No patches since last upgrade
- No patches and unsupported

Months

0 3 6 9 12 15 18 21 24 27 30 33 36 39 42 45 48+
## Database Upgrades and CPU Patches

<table>
<thead>
<tr>
<th>Database Version Upgrade Patch</th>
<th>Latest CPU Patch Included In Upgrade Patch</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2.0.8</td>
<td>July 2006</td>
</tr>
<tr>
<td>10.1.0.5</td>
<td>October 2005</td>
</tr>
<tr>
<td>10.2.0.3</td>
<td>October 2006</td>
</tr>
<tr>
<td>10.2.0.4</td>
<td>April 2008</td>
</tr>
<tr>
<td>11.1.0.6</td>
<td>October 2007</td>
</tr>
<tr>
<td>11.1.0.7</td>
<td>January 2009</td>
</tr>
<tr>
<td>11.2.0.1</td>
<td>January 2010</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>ORDPLUGINNS</td>
<td>ORDPLUGINNS</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
Oracle Database Passwords

Oracle Password algorithm is published on the Internet
- Algorithm uses two cycles of DES encryption with the username to produce a one-way hash of the password
- Oracle 11g – hash changed to SHA-1 – old DES hash also stored

Hash is unique to the username, but common across all versions and platforms of the Oracle database
- SYSTEM/MANAGER is always D4DF7931AB130E37 in every database in the world
- Oracle databases often cloned to test and development

Database installed with 8 to 20 default database accounts
- All have default passwords
- Many default password lists published on the Internet
Brute Forcing Database Passwords

A number of efficient password brute forcing programs exist for Oracle
- Speed is at least 1 million passwords per second for desktop/laptop
- Speed is around 100 million passwords per second for specialized hardware (FGPA/GPU)
- Only the username and hash are required
- Estimated time to brute force a password of x length –

<table>
<thead>
<tr>
<th>Length</th>
<th>Permutations</th>
<th>Time (desktop)</th>
<th>Time (GPU)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>26 (26)</td>
<td>0 seconds</td>
<td>0 seconds</td>
</tr>
<tr>
<td>2</td>
<td>1,040 (26 x 39)</td>
<td>0 seconds</td>
<td>0 seconds</td>
</tr>
<tr>
<td>3</td>
<td>40,586 (26 x 39 x 39)</td>
<td>0 seconds</td>
<td>0 seconds</td>
</tr>
<tr>
<td>4</td>
<td>1,582,880</td>
<td>1.5 seconds</td>
<td>0 seconds</td>
</tr>
<tr>
<td>5</td>
<td>61,732,346</td>
<td>2 minute</td>
<td>6 seconds</td>
</tr>
<tr>
<td>6</td>
<td>2,407,561,520</td>
<td>40 minutes</td>
<td>24 seconds</td>
</tr>
<tr>
<td>7</td>
<td>93,894,899,306</td>
<td>1 day</td>
<td>15 minutes</td>
</tr>
<tr>
<td>8</td>
<td>3,661,901,072,960</td>
<td>42 days</td>
<td>10 hours</td>
</tr>
<tr>
<td>9</td>
<td>142,814,141,845,466</td>
<td>1,600 days</td>
<td>16 days</td>
</tr>
</tbody>
</table>
Enabling auditing is the easy part

Effort

Task

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

Native

Fine-grained

Triggers

Outside

Network-based

Agent-based

Log-based

Native Protective
## Native Audit Trail Destination Options

<table>
<thead>
<tr>
<th>Oracle Version</th>
<th>AUDIT_TRAIL</th>
<th>SYSDBA</th>
<th>FGA</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.0.x</td>
<td>OS/DB</td>
<td>-</td>
<td>DB</td>
</tr>
<tr>
<td>9.2.x</td>
<td>OS/DB</td>
<td>OS</td>
<td>DB</td>
</tr>
<tr>
<td>10.1.x</td>
<td>OS/DB</td>
<td>OS</td>
<td>DB</td>
</tr>
<tr>
<td>10.2.x</td>
<td>OS/DB/XML/SYSLOG</td>
<td>OS/XML</td>
<td>DB/XML</td>
</tr>
<tr>
<td>11.1.x</td>
<td>OS/DB/XML/SYSLOG</td>
<td>OS/XML</td>
<td>DB/XML</td>
</tr>
<tr>
<td>11.2.x</td>
<td>OS/DB/XML/SYSLOG</td>
<td>OS/XML</td>
<td>DB/XML</td>
</tr>
</tbody>
</table>
# Audit Trails Destinations and Values

<table>
<thead>
<tr>
<th>Session Value</th>
<th>V$SESSION View</th>
<th>SYS_CONTEXT Function</th>
<th>SYS.AUD$ DBA_AUDIT_*</th>
<th>FGA_LOG$ AUDIT_TRAIL</th>
<th>Audit Vault</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB User Name</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Schema Name</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS User Name</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Machine</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Terminal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Program</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Client Process ID</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Info</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Client ID</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
# Auditing Session Data

<table>
<thead>
<tr>
<th>Database User Name</th>
<th>OS User Name</th>
<th>Schema Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Machine/User host</td>
<td>Terminal</td>
</tr>
<tr>
<td>Program</td>
<td>Client Process ID</td>
<td>Module</td>
</tr>
<tr>
<td>Action</td>
<td>Client Info</td>
<td>Client ID</td>
</tr>
</tbody>
</table>
# Auditing Session Data – Spoofable

<table>
<thead>
<tr>
<th>Database User Name</th>
<th>OS User Name</th>
<th>Schema Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Machine/ User host</td>
<td>Terminal</td>
</tr>
<tr>
<td>Program</td>
<td>Client Process ID</td>
<td>Module</td>
</tr>
<tr>
<td>Action</td>
<td>Client Info</td>
<td>Client ID</td>
</tr>
</tbody>
</table>

INTEGRIGY
Key Security Risks

1. Exploitation of Oracle security vulnerabilities
   - Apply security patches
   - Limit direct connectivity to the database
   - Prohibit use of generic accounts by individuals

2. Brute forcing of Oracle database passwords
   - Limit access to password hashes
   - Change all database passwords in test and development

3. Lack of and trustworthiness of DB auditing
   - Must enable database auditing
   - Need to understand issues with audit data
Agenda

1. Security Challenges
   2. Key Database Security Risks
   3. DB Security Strategy
   4. DB Security Solutions
   5. Q&A
Traditional Database Security Approaches

- **Database security checklists**
  - 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

- **Database security assessments**
  - Expensive and time consuming
  - Must be performed periodically to be effective
  - Database-centric or arbitrary standards often used

- **Database monitoring and auditing tools**
  - Expensive and time consuming
  - Difficult to implement with complex applications
Database Security Checklists

- **Center for Internet Security (CIS) Oracle Benchmark**
  - Oracle 8i, 9i, 10g, 11g checklists

- **Department of Defense DISA Oracle STIG**
  - Database Security Checklist and Guidance
  - Oracle 9i, 10g, 11g checklists

- **Oracle Security Whitepaper and Checklists**
  - Included with Oracle Security Guide manual

- **SANS S.C.O.R.E**
  - Last updated 2006

- **ISACA - Information Systems Audit and Control Association**
  - Security, Audit and Control Features Oracle Database, 3rd Edition

- **SANS Oracle Security Step by Step Book**
  - Last updated 2004
Defensive Security Strategies Themes

- **Reduce security vulnerability exposure**
  - Almost all database security vulnerabilities require a valid database session
  - Jump off or slow down the security patch hamster wheel

- **Classify databases and act appropriately**
  - The data determines the acceptable level of risk per database

- **Capturing audit data is the easy part**
  - Storing, protecting, and reporting is the hard part
  - Must transform audit data into actionable information
  - Auditing should enable information and action, not act as a black-hole
Defensive Security Strategies

- **“Virtual perimeters” for databases**
  - Limitation and segregation of access
  - Understand, channel, and manage ad-hoc access
  - Perimeters may be implemented at network, OS, database, and application layers

- **Configuration and vulnerability management**
  - Standardize configuration and operations where possible while minding application dependencies
  - Implement configurations that reduce security risk
  - Create consistency whenever possible
  - Mitigating controls when exceptions due to application limitations
  - Use existing management tools to validate and enforce configurations – continuously

- **Intelligent and business-focused auditing and monitoring**
  - Use auditing to enhance understanding of database operations
  - Intelligently capture, store, and disseminate information
  - Avoid auditing performance pitfalls
Agenda

1. Security Challenges
   - Key Database Security Risks

2. DB Security Strategy

3. DB Security Solutions

4. Q&A
Database Security Solutions

- A database security program is the solution
  - Starts with a database security strategy
  - Effective and monitored policies and procedures are critical
  - Standardized configurations through a documented database configuration and security standard
  - Implement products to solve specific problems
Database Security Program

- Access and Authorization
- Auditing, Logging, and Monitoring
- Security Patching
- Configuration Standards
- Change Management
- Encryption
Database Security Solution Products

- Auditing and Monitoring
  - Guardium
  - Imperva
  - Lumigent
  - Oracle
  - Sentrigo
  - AppSec

- Security and Vulnerability Assessment
  - Oracle
  - Sentrigo
  - AppSec

- Encryption
  - Oracle
  - Vormetric
  - Protegrity
  - Voltage

- Database Access Control
  - Oracle DB Vault
  - Oracle Advanced Security

** Not all vendors listed
Third Party Auditing Solutions

- Define your **STRATEGY** first
  - Database security and auditing strategy is critical to successful implementation
  - Define responsibilities for DB security and auditing
    - difficult in most organizations
  - The strategy will drive the requirements

- **Goal is a complete auditing strategy**
  - No one tool or auditing technology is sufficient
## Third Party Auditing Solutions

- **There are fundamental differences among the vendors**
  - Database activity capture vs. intrusion detection
  - Data Capture Techniques = network, agent, log, native
  - Architecture = appliance vs. software
  - Bells and whistles = connection pooling, blocking, assessment, etc.

<table>
<thead>
<tr>
<th>Application Security</th>
<th>Embarcadero</th>
<th>Guardium</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AppRadar</strong></td>
<td><strong>DSAuditor</strong></td>
<td><strong>SQLGuard</strong></td>
</tr>
<tr>
<td>Imperva</td>
<td>Fortinet*</td>
<td>Lumignet</td>
</tr>
<tr>
<td>DB Monitoring</td>
<td>IPLocks</td>
<td>Audit DB</td>
</tr>
<tr>
<td>Nitro Security</td>
<td>Oracle</td>
<td>Sentrigo</td>
</tr>
<tr>
<td>NitroGuard DBM</td>
<td>Oracle Database Firewall</td>
<td>Hedgehog</td>
</tr>
<tr>
<td>Symantec</td>
<td>Tizor*</td>
<td>Oracle</td>
</tr>
<tr>
<td>Database Security</td>
<td>Mantra</td>
<td>Audit Vault</td>
</tr>
</tbody>
</table>
Integrify Contact Information

Stephen Kost  
Chief Technology Officer  
Integrify Corporation  
e-mail: info@integrify.com  
blog: integrify.com/oracle-security-blog

For information on -

- Oracle Database Security
- Oracle E-Business Suite Security
- Oracle Critical Patch Updates
- Oracle Security Blog

www.integrify.com