May 2012
Oracle Spatial User Conference
Hayri Tarhan
Senior Manager
Oracle Public Sector
Security and Oracle Database 11g
Is Your Data Secure?
Program Agenda

• The State of Security
• Oracle Maximum Database Security Architecture
• Protecting Enterprise Databases
  – What is the threat?
  – How is it exploited?
  – How can you protect against it?
• Q&A
Why Maximum Security?

Two thirds of sensitive and regulated information now resides in databases … and doubling every two years

Classified Govt. Info.
Trade Secrets
Competitive Bids
Corporate Plans
Source Code
Bug Database

Source: "Effective Data Leak Prevention Programs: Start by Protecting Data at the Source — Your Databases", IDC, August 2011
The 2000-2010 Decade

Landscape

• IT Landscape
  – Highly available and scalable
  – Outsourcing, off-shoring, Third Party Service Providers

• Threat Landscape
  – SQL Injection introduced (Oct 2000), Insider Threats
  – Advanced Persistent Threats (APT), Organized Crime, State Sponsored,….

• Regulatory Landscape
  – Payment Card Industry (2.0 in Oct 2010), Breach disclosure laws
Landscape Looking Ahead

• IT Landscape
  – Vanishing perimeter dissolves insider/outsider differences
  – Data consolidation, massive warehouses
  – Public/private cloud, partner, globalization

• Threat Landscape
  – Sophisticated hacking tools, bot networks, supply chain
  – Cyber terrorism and warfare sponsored by nation states
  – Databases to become a prime target

• Regulatory Landscape
  – Moving from pure detective controls to preventive controls
  – All countries and states joining in protecting PII data
“Forrester estimates that although 70% of enterprises have an information security plan, only 20% of enterprises have a database security plan.”
Database Security – Big Picture

- Applications
- Network SQL Monitoring and Blocking
- Activity Audit
- Compliance Scan
- Vulnerability Scan
- Patch Automation
- Encrypted Database
- Data Masking
- Unauthorized DBA Activity
- Multi-factor authorization
- Auditing
- Authorization
- Authentication
Sources of Vulnerability

Attacks can come from anywhere

<table>
<thead>
<tr>
<th>Category</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>• SQL Injection attack</td>
</tr>
<tr>
<td></td>
<td>• Application Bypass</td>
</tr>
<tr>
<td>Test and Dev</td>
<td>• Access to production data in non-secure environment</td>
</tr>
<tr>
<td></td>
<td>• Access to production systems for trouble shooting</td>
</tr>
<tr>
<td>Administrative Account Misuse</td>
<td>• System admin, DBA, Application admins</td>
</tr>
<tr>
<td></td>
<td>• Stolen credential, Inadequate training, Malicious Insiders</td>
</tr>
<tr>
<td>Operations</td>
<td>• Lost / Stolen Backups</td>
</tr>
<tr>
<td></td>
<td>• Direct OS Access</td>
</tr>
</tbody>
</table>
# Sources of Vulnerability

Attacks can come from anywhere

<table>
<thead>
<tr>
<th>Category</th>
<th>Sources</th>
</tr>
</thead>
</table>
| Application Users      | • SQL Injection attack  
                        |   • Application Bypass                                                 |
| Test and Dev           | • Access to production data in non-secure environment  
                        |   • Access to production systems for trouble shooting                 |
| Administrative Account | • System admin, DBA, Application admins  
                        |   • Stolen credential, Inadequate training, Malicious Insiders         |
| Misuse                 |                                                                         |
| Operations             | • Lost / Stolen Backups  
                        |   • Direct OS Access                                                  |
Operations

**What**
- Data files can be accessed directly at the operating system (OS) level, bypassing all database controls

**How**
- Gain access to OS root account, Oracle software account, Oracle DBA account
- Copy or search raw database files

**Protection Strategy**
- Encrypt database files
- OS level auditing
- Limit accounts on production servers
Transparent Data Encryption
Oracle Advanced Security

• Protects from unauthorized OS level or network access
• Efficient encryption of all application data
• Built-in key lifecycle management
• No application changes required
### Account Misuse

<table>
<thead>
<tr>
<th>Category</th>
<th>Issues</th>
</tr>
</thead>
</table>
| Applications           | • SQL Injection  
                         • Application Bypass                                                  |
| Test and Dev           | • Access to production data in non-secure environment  
                         • Access to production systems for trouble shooting                 |
| Administrative Account | • System admin, DBA, Application admins  
                         • Stolen credential, Inadequate training, Malicious Insiders         |
| Misuse                 | • Lost / Stolen Backups  
                         • Direct OS Access                                                   |

---

**Oracle Spatial User Conference 2012**
Account Misuse

What
• Privileged accounts are a targets of attack

How
• Privileged accounts have unfettered access

Protection Strategy
• Limit administrative account access to the database
• Audit privileged user activity
• Preventive controls around application data
Database Operational Controls
Oracle Database Vault

- Limit powers of privileged users, and enforce SoD
- Protect application data and prevent application by-pass
- Enforce who, where, when, and how using rules and factors
- Securely consolidate application data
- No application changes required
Audit Consolidation & Reporting
Oracle Audit Vault

- Consolidate audit data into secure repository
- Detect and alert on suspicious activities
- Out-of-the-box compliance reporting
## Test and Dev

<table>
<thead>
<tr>
<th>Applications</th>
<th>Test and Dev</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SQL Injection attack</td>
<td>• Access to production data in non-secure environment</td>
</tr>
<tr>
<td>• Application Bypass</td>
<td>• Access to production systems for trouble shooting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Administrative Account Misuse</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• System admin, DBA, Application admins</td>
<td>• Lost / Stolen Backups</td>
</tr>
<tr>
<td>• Stolen credential, Inadequate training, Malicious Insiders</td>
<td>• Direct OS Access</td>
</tr>
</tbody>
</table>
# Test and Dev

## What
- Product data frequently copied to development and test
- PII data unnecessarily exposed

## How
- Test and dev systems may not be as well monitored or protected as production systems

## Protection Strategy
- Mask sensitive production data before transferring
- Restrict connectivity between test/dev and production
Irreversible De-Identification
Oracle Data Masking

- Reduce scope of audit with irreversible de-identification on non-production databases
- Referential integrity preserved so applications continue to work
- Extensible template library and policies for automation
### Applications

<table>
<thead>
<tr>
<th>Category</th>
<th>Issues</th>
</tr>
</thead>
</table>
| Applications           | • SQL Injection attack  
                       |   • Application Bypass                                                 |
| Test and Dev           | • Access to production data in non-secure environment  
                       |   • Access to production systems for trouble shooting                |
| Administrative Account | • System admin, DBA, Application admins                               |
| Misuse                 |   • Stolen credential, Inadequate training, Malicious Insiders         |
| Operations             | • Lost / Stolen Backups  
                       |   • Direct OS Access                                                  |
Applications

| What | Applications may be vulnerable to SQL Injection attacks  
|      | Legacy applications particularly vulnerable |
| How | Application input fields can be misused |
| Protection Strategy | Monitor in-bound application SQL  
|                 | Block unauthorized SQL before it reaches the database |
• Monitors database activity, and prevents attacks and SQL injections
• White-list, black-list, and exception-list based security policies based upon highly accurate SQL grammar based analysis
• In-line blocking and monitoring, or out-of-band monitoring modes
Database Security – Big Picture

- Applications
- Network SQL Monitoring and Blocking
- Activity Audit
- Data Discovery
- Compliance Scan
- Vulnerability Scan
- Patch Automation
- Auditing
- Authorization
- Authentication
- Encrypted Database
- Data Masking
- Unauthorized DBA Activity
- Multi-factor authorization
- Multi-factor authorization
Issues to Ponder?

1. Is our IP secured?
2. Can we defend against APTs and other attacks?
3. Would we know if we were breached?
4. Do privileged users know what they should not?
5. Are we in compliance with all regulations?
Q&A