Secure Your Data Transparently

Vipin Samar
Vice President, Database Security
Agenda

• The Security Problem in the Real World
• The Security Problem in a Wizard World
• Key Data Security Challenges
• Oracle Approach to Providing Security
• Oracle Security Components
Protecting PII Data is a Top Concern

A contractor lost the tapes containing sensitive information while driving through New York State to a storage facility back in February.

By Sharon Gaudin
InformationWeek
May 16, 2007 12:30 PM

said on Wednesday that a contractor lost more than one tape containing identifying information on current and former employees.
The Insider Threat is Real

Massive Insider Breach

A researcher who worked for [redacted] 10 years before accepting a job with a competitor downloaded 22,000 sensitive documents and viewed 16,706 more in the company's electronic library.

By Larry Greeneemeier
InformationWeek
Feb 15, 2007 03:00 PM

The [redacted] U.S. attorney on Thursday revealed a massive insider data breach [redacted] company. A former scientist last year pleaded guilty to trying to steal $400 million worth of company trade secrets. He now faces up to a decade in prison, a fine of $250,000, and restitution when sentenced in March.
What Happened?

- *Internet* revolution brought a rush of new applications.
- *Need-to-know* enforcement policies became a back burner issue replaced by economies of scale/speed.
- *Least privilege* became more difficult to apply in the N*tier* architecture.
- *Scalability* and *Speed of Implementation* became more important than security.
- *Targeted attacks* motivated by gain (and not fame).
Now to the Wizard World…

Harry Potter / Hogwarts Security

- Password: 24 hour pwd, long Latin pwds, Challenge-response
- Full encryption/masking
- Auditing (memory threads)
  - Audit data can be viewed by unauthorized wizards
  - Audit data can be tampered – selective deletion
- Packet inspection around Hogwarts: Firewall
- Some tricks of the trade
  - Imperius Curse: Control the user
  - Expelliarmus: Repel the attack
  - Avada Kedavra: Attack with no trace left
  - PolyJuice Potion: Impersonation
- Insider threat: Snape
- “Ministry of Magic” driven security policies: Compliance
Key Drivers for Data Security

Regulatory Compliance

- Sarbanes-Oxley (SOX), J-SOX, HIPAA
- GLBA
- Payment Card Industry (PCI)
- EU Privacy Directives, CA SB 1386….
- Adequate IT controls, COSO, COBIT
- Separation of duty, Proof of compliance, Risk Assessment and Monitoring

Insider Threats

- Large percentage of threats go undetected
- Outsourcing and off-shoring trend
- Customers want to monitor insider/DBA
Enterprise Data Security Challenges

Secure Data NOW

- Many applications
  - Legacy and new
  - Custom & Off-the-shelf
- Many security models
  - One big user (n-tier)
  - Client server
- Many privileged users
  - DBAs
  - Application Users
- Custom security policies
  - Compliance-driven
  - Business-driven
- Distributed security information
  - Audit Logs
  - Security information unused
Why Transparent Security?

- No changes required to your applications
  - Can do it today and meet auditor’s reqmts
  - No expert security engineers needed
  - Can meet changing auditor requirements
- Provided
  - It is secure and fast
  - It is manageable, flexible, and easy-to-use
  - It is baked-in
Data Security Components

- User Management
- Access Control
- Monitoring
- Data Protection
- Core Platform Security
Data Security Components

User Management
- Directory Integration
- Strong Authentication

Access Control
- Controlling privileged users
- Custom security policies
- Row-level security

Core Platform Security

Monitoring
- Enterprise Audit
- Configuration

Data Protection
- Network Encryption
- Data Encryption
- Backup Encryption
Data Security: Oracle Products

User Management
- Oracle Identity Management
- Enterprise User Security

Access Control
- Oracle Database Vault
- Oracle Label Security

Core Platform Security

Monitoring
- Oracle Audit Vault
- EM Configuration Pack

Data Protection
- Oracle Advanced Security
- Oracle Secure Backup
Data Security: Oracle Products

**User Management**
- Oracle Identity Management
- Enterprise User Security

**Access Control**
- Oracle Database Vault
- Oracle Label Security

**Monitoring**
- Oracle Audit Vault
- EM Configuration Pack

**Data Protection**
- Oracle Advanced Security
- Oracle Secure Backup
Enterprise User Security (EUS)

- User Management
  - Centralized User Management
  - Consolidate database accounts with shared database schemas
  - Integrated with Oracle Virtual Directory
- Enterprise Strong Authentication
  - Kerberos (MSFT, MIT)
  - PKI (x.509v3)
  - Password
- Database Enterprise Edition Feature
  - Available since Oracle 8.1.6
Data Security: Oracle Products

**User Management**
- Oracle Identity Management
- Enterprise User Security

**Access Control**
- Oracle Database Vault
- Oracle Label Security

**Monitoring**
- Oracle Audit Vault
- EM Configuration Pack

**Data Protection**
- Oracle Advanced Security
- Oracle Secure Backup

**Core Platform Security**
Need for Stronger and Transparent Access Control

- **Key Drivers**
  - Restrict full access to data for Privileged users
    - Administrators
    - Developers/QA
    - Application Users
  - Easily implement environment based access control
    - User parameters
    - Network parameters
    - Database parameters

- **Key Requirements**
  - Applying on existing legacy applications
  - Support for custom policies
  - Difficult to circumvent
  - Minimal Performance impact
Oracle Database Vault
Compliance and Insider Threats

- **Controls on privileged users**
  - Restrict DBA access to application data
  - Provide Separation of Duty
  - Security for database and information consolidation

- **Enforce data access security policies**
  - Control who, when, where and how is data accessed
  - Make decision based on IP address, time, auth…

- **Available on Oracle 10gR2 and 9iR2**
- **Validated with PeopleSoft**
- **E-Biz & other Apps validation underway, including 3rd party**
Oracle Database Vault

Protection Realms

- Database DBA views HR data
  Compliance and protection from insiders

- HR DBA views Fin. data
 Eliminates security risks from server consolidation

Realms can be easily applied to existing applications with transparency and minimal performance impact
Oracle Database Vault
Transparent Multi-factor Authorization

SELECT ....
Unexpected IP address
HR account

CREATE ...
Business hours
FIN DBA
Oracle Database Vault
Transparent Protection

1. Define Realms (Block Highly Privileged Users)
2. Add SQL Command Rules (Optional)
3. Add other security policies (Optional)
4. PL/SQL scripts to deploy security policies
5. Test your application
6. Consider application maintenance
Validation Use Case: Peoplesoft

- Created a PeopleSoft Realm
  - Protected all objects owned PeopleSoft Access Id (SYSADM)
  - Protected PeopleSoft database roles
- Created PSFTDBA account for Application maintenance
  - Can do patching and maintenance but can’t do SELECT
- Associated a security policy
  - Restricted access to middle tier process – no ad-hoc tools access
  - Can be restricted by hostnames and IP addresses
- Authorized PEOPLE user SELECT on specific user login tables
- Delivered as a script that customers can further customize
Need for Label based Access Control

• Key Drivers
  • Sharing of data across authorization levels
  • Data Classification
  • Consolidating different copies of the application

• Key Requirements
  • Applying on existing application
  • Customizing for customer use
  • Difficult to circumvent
  • Minimal Performance impact
Oracle Label Security
Label Based Access Control

- Industry leading data classification solution
- Enables Multi-level Security for government
- Need-to-know for commercial organizations
- Flexible and Adaptable
  - Comprehensive GUI + Comprehensive API
  - Overcomes traditional LBAC limitations
  - Hidden column provides application transparency
Don’t Understand Labels?
Labels are really just Factors

Allow Action
IF
User Label Factor

Equals or Exceeds
Object Classification

- Exec Only
- Secret
- Confidential
Oracle Label Security
Manageability

- Policy based model
  - Multiple policies supported
    - ACME, HR, Legal
  - Policies are umbrellas applying to one or more tables, schemas, users
- Web based management
  - New EM for Oracle Database 11g R1
- Integrated with Oracle Identity Management
## Oracle Label Security

**Complete Flexibility**

### Enforcement Controls
- Read Control
- Insert Control
- Update Control
- Delete Control
- Label Default
- Label Update
- Label Check
- No Control

### Extended Privileges
- READ
- FULL
- WRI TEDOWN
- WRITEUP
- WRITEACROSS
- PROFILEACCESS (Proxy)
- Trusted Stored Procedures
SQL Predicate Extension

- Extends OLS beyond just labels
- Transparently adds *where* clause to SQL
- Enforced by OLS policy without need to write PL/SQL procedures
“Instead of maintaining security policies in our applications and database, Oracle Label Security allowed us to apply these access controls where it matters most: the centralized database on a scalable Oracle RAC system.”

Graciela Mucci, CIO, ARTEAR

Sept. ‘06
Oracle Label Security
Deployment Guide

1. Identify and define labels based on company programs and/or data
   New ones can be defined later

2. Provision user label authorizations
   Database or Oracle Identity Management

3. Apply OLS functions in applications or database (optional)
   Extend Database Vault Factors, Command rules, Separation of Duty

4. Use GUI or API to protect application tables (optional)
   Required only if you want transparent access mediation

5. Label data (optional)
   Required only if you want transparent access mediation
Data Security: Oracle Products

User Management
• Oracle Identity Management
• Enterprise User Security

Access Control
• Oracle Database Vault
• Oracle Label Security

Core Platform Security

Monitoring
• Oracle Audit Vault
• EM Configuration Pack

Data Protection
• Oracle Advanced Security
• Oracle Secure Backup
The Need for Encryption

• Key Drivers
  • Millions of records lost and many more vulnerable
  • Worldwide privacy, security and compliance regulations
    • Personal privacy data: Credit Cards, Social ID, …
    • PCI, California SB 1386, Country-specific laws

• Key Requirements
  • Encrypting data in existing applications with minimal perf impact
  • Automated Key Management

Customer Credit Card Numbers

Disks replaced for maintenance

Laptops stolen

Backups lost
Oracle Advanced Security
Encryption and Strong Authentication Services

Strong Authentication

Network Encryption

Data Automatically Encrypted

Data Automatically Decrypted

Transparent Data Encryption

Transparent Data Encryption with RMAN can Encrypt entire Backups sent to Disk
Transparent Data Encryption

Easy Uptake

- No changes to existing applications
  - No triggers, no views
  - Minimal performance impact
  - Build-in key management
- No crash-course needed in encryption or key management; just focus on business logic
- Include changes in a script

TDE Supported by Oracle E-Business Suite and SAP
Transparent Data Encryption

Deployment Steps

1. Identify columns holding sensitive data
   Credit Cards, SSN...

2. Verify TDE supports the datatype?
   TDE supports most all commonly used datatypes

3. Verify column is not part of a Foreign Key?
   Simple Data Dictionary Query

4. Encrypt existing and new data
   SQL*Developer GUI or Command line DDL, Alter Table.....

Visit OTN for a complete list of data types and more
Oracle Secure Backup

Protect Backup Data

- Oracle Secure Backup
  - Media mgmt software
  - Up to 256 bit AES
  - Encryption Modes
    - PKI
    - Password
  - Encrypt at the database or tablespace level
- Integrated Solution
Data Security: Oracle Products

**User Management**
- Oracle Identity Management
- Enterprise User Security

**Access Control**
- Oracle Database Vault
- Oracle Label Security

**Core Platform Security**

**Monitoring**
- Oracle Audit Vault
- EM Configuration Pack

**Data Protection**
- Oracle Advanced Security
- Oracle Secure Backup
Need for Auditing Database Activity

• Key Drivers
  • Regulatory Compliance (SOX, PCI, Privacy, …)
    • Risk assessment and compensating controls
    • Demonstrate controls for compliance
  • Security
    • Detect misuse of privileges

• Key Requirements
  • Collect Audit trail data from many audit silos
  • Automate review of the audit trail logs, and raise alerts
  • Centralize audit policy management
  • Secure the audit trail
  • Minimize performance impact on production systems
Auditing in the Oracle Database
Robust, Flexible, and High Fidelity Audit

- Types of Audit events
  - Statement based (DML, DDL)
  - Privilege, Objects, Users
  - System event
  - Failure or Success
  - SYS Auditing
- What is Collected?
  - Who: DB user, OS user, clientid, guid..
  - Where: Host, terminal#, process#
  - When: Timestamp, SCN, logofftime...
  - What: DML/DDL, SQL-Text, SQL-Bind...
- Policy/condition based auditing
- Minimal performance impact
Oracle Audit Vault
Trust-but-Verify

• Collect and Consolidate Audit Data
  • Oracle 9i Release 2 and higher
  • Audit Data and Transaction logs

• Simplify Compliance Reporting
  • Built-in reports
  • Custom reports

• Detect and Prevent Insider Threats
  • Alert suspicious activity

• Scale and Security
  • Robust Oracle Database technology
  • Database Vault, Advanced Security
  • Partitioning

• Lower IT Costs with Audit Policies
  • Centrally manage/provision audit settings
Audit Vault Reports

Out-of-the-box Audit Assessments & Custom Reports

- Out-of-the-box reports
  - Privileged user activity
  - Access to sensitive data
  - Role grants
  - DDL activity
  - Login/logout
- User-defined reports
  - What privileged users did on the financial database?
  - What user ‘A’ did across multiple databases?
  - Who accessed sensitive data?
- Custom reports
  - Oracle BI Publisher, Application Express, or 3rd party tools
Audit Vault Alerts

Early Detection With Alerting

• Alerts can be defined for
  • Directly viewing sensitive columns
  • Creating users on sensitive systems
  • Role grants on sensitive systems
  • "DBA" grants on all systems
  • Failed logins for application users
  • …

• Alerts evaluated on incoming audit data
Audit Vault Policies
Centralized Management of Audit Policies

- Audit Policies - collection of audit settings on the databases
- Compare against existing audit settings on source
- Provision audit settings centrally
- Demonstrate compliance
Audit Vault Data Warehouse
Scalable & Flexible Warehouse

• Audit Warehouse
  • Enable business intelligence and analysis
  • Enable reporting

• Audit Vault Warehouse Dimensions
  • Time, Host, Source, User, Event, …
  • Schema documented and published
  • Allows third party reporting tools

• Performance and Scalability
  • Built-in partitioning
  • Scales to Terabytes

• Oracle RAC certified
Audit Vault Dashboard
Enterprise-wide Security & Compliance view
Oracle Audit Vault

Transparency collecting audit data

1. Define Audit Policies
   Privileged Users, DDL, Fine Grained Audit (Sensitive Data)

2. Configure Collectors
   Aud$, OS, Redo

3. Setup Alerts
   New User Creations, Sensitive Data Access

4. Run Reports
   Out-of-the-box or build custom using open data warehouse schema
Integrating with Oracle Audit Vault

Different Levels of Integration

• Leverage native database auditing
  • Database auditing is turned ON by default in 11g
  • Low impact performance utilizing OS audit trail records
  • Create customized audit scripts or Fine-grained-audit (FGA) scripts specific to your situation

• Optionally add “Client identifier” to get “user” info. in audit trail

• Create Custom reports with the Audit Vault warehouse

• Use Audit Vault SDK (available for early adopters) for application specific auditing
Oracle Enterprise Manager
Configuration Management Pack

- Automate Database Security Assessment
  - Database Parameters
  - Database Profile
  - Database Access
  - Database File Permissions
  - Post-installation Checks

- Track Configuration Drift across monitored systems
- Supports 8i and higher database releases
- Maps to COBIT, CIS, and Oracle’s best practices
Security
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 remain at the sole discretion of Oracle.
Oracle Database 11g Security

In Brief

• Expanded encryption capabilities
  • Tablespace encryption for full application table encryption
  • Secure Files encryption (new LOBS)
  • HSM integration for high assurance key protection

• Secure by Default
  • Auditing by default
  • Password policies

• All new security manageability tools
  • Web based
  • Fully Integrated with Enterprise Manager
Simplified Manageability
Encrypt Sensitive Data from Enterprise Manager
Summary: Security Data Transparently

• Security transparency
  • No application changes required
  • Command lines for integration
  • Easy script based packaging
• Support existing applications
• Minimal performance impact
• Flexibility for customization
• Secure your data today!
Learn More

Technology Overview
• Visit: oracle.com/security
  View Whitepapers and webinars

Technical Information, Demos, Software
• Visit OTN: otn.oracle.com -> products ->
  database -> security and compliance
  • Step by step examples for Database Vault,
    Transparent Data Encryption and more
Oracle Database 11g
The Launch Event

• Where
  • The Equitable Auditorium, New York City

• When
  • Wednesday, July 11, 2007 (9:00am – 12:00noon EST)

• Who
  • Charles Phillips, Andy Mendelsohn and customer speakers

• How
  • Call 1.888.329.8636 or talk to your Oracle representative