Agenda

1. OBIEE
2. OBIEE Top Ten
3. 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**
  Oracle EBS, OBIEE, Databases, Sensitive Data, Penetration Testing

- **Compliance Assistance**
  SOX, PCI, HIPAA

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

**Integrigy**

- ERP Applications
  Oracle E-Business Suite

- Databases
  Oracle, SQL Server, MySQL

**You**

- Validates Security
- Verifies Security
- Ensures Compliance
- Protects Oracle EBS
- Builds Security
Agenda

1. OBIEE
   - Top Ten

2. Q&A
OBIEE Security Examined

Size of box proportionate to component's impact on security
Agenda

1. OBIEE
2. OBIEE Top Ten
3. Q&A
Top 10 OBIEE Security Vulnerabilities

1. Patching Policies and Procedures
2. Metadata database security
3. Key accounts not secured
4. RPD security
5. Weak overall security
6. Sensitive data not protected
7. Direct SQL access allowed
8. Write-Back enabled
9. Go URL and SQL access
10. No Usage Tracking
Patch Levels

- OBIEE 11.1.1.6.x end-of-life 2-April-2014
  - Sustaining support

- Recommend
  - Upgrade to OBIEE 11.1.1.7.x
Metadata Database Security

- Metadata repository database required for each Fusion Middleware product
  - OBIEE schemas: BIPLATFORM, MDS

- Recommendations
  - All standard database security best practices apply
  - Apply CPU patches
  - Do not manually edit or allow access
  - Do not use for Usage Tracking
<table>
<thead>
<tr>
<th>Key Accounts Not Secured</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OS owner of WebLogic</strong></td>
</tr>
<tr>
<td><strong>OS user that runs WebLogic</strong></td>
</tr>
<tr>
<td><strong>WebLogic administration user(s)</strong></td>
</tr>
<tr>
<td><strong>BI Admin User</strong></td>
</tr>
<tr>
<td><strong>BI System User</strong></td>
</tr>
<tr>
<td><strong>OracleSystemUser</strong></td>
</tr>
</tbody>
</table>
## Act-As and Impersonation

<table>
<thead>
<tr>
<th></th>
<th>Impersonate</th>
<th>Act-As</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level of access</strong></td>
<td>Full access</td>
<td>Full or read-only access, on a single user</td>
</tr>
<tr>
<td><strong>Users whose identity can be</strong></td>
<td>Any and all users, anytime</td>
<td>Defined list of users</td>
</tr>
<tr>
<td><strong>assumed by the proxy user</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access method</strong></td>
<td>Construct URL manually</td>
<td>Standard functionality of UI</td>
</tr>
<tr>
<td><strong>How to know if being used</strong></td>
<td>No indication given</td>
<td>Both proxy and Target are shown in the UI</td>
</tr>
<tr>
<td><strong>Security risk</strong></td>
<td>Credentials exposed in plain text when URL submitted</td>
<td>Little to none</td>
</tr>
</tbody>
</table>
Key Account Recommendations

- **Key accounts**
  - Reconcile as part of full audit of OBIEE
  - Regularly rotate all passwords per Oracle Support
    - Note 1365210.1
    - Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g (E10543-08) – Appendix C Troubleshooting Security in Oracle Business Intelligence

- **Act-As and Impersonation**
  - OBIEE security assessment
  - Set and/or review policy for using
  - Use Act-As if at all possible
  - Implement Usage Tracking
  - Log and Monitor
RPD Security

- **Password to encrypt and open RPD**
  - Protect all meta data and security rules

- **Export to XML option**
  - Connection pool passwords ARE encrypted

- **Recommendation**
  - Use complex passwords and regularly rotate password
  - Use different password for production
  - Secure access to XML export and put RPD under source code control
Weak Overall OBIEE Security

- No easy way to reconcile security and authorization.
  Three security solutions:
  - Catalog (ACLs)
  - Presentation Layer permission grants
  - Data level filters

- Commonly find
  - Rogue groups and users
  - Errors and gaps

- Recommendation
  - OBIEE security assessment
Sensitive Data Not Protected

- **Need to protect if defined in RPD**
  - May not need or realize exists
  - Can be result of prior engagement or accidental metadata import

- **Examples:**
  - Social security, credit cards, bank accounts
  - Salaries, sales and customer records
  - E-Business User table and passwords
Sensitive Data Not Protected

- **Need to project against**
  - Weak or no security within RPD and catalog
  - Direct SQL access
  - Write Back
  - GO URL SQL access

- **Recommendation**
  - OBIEE security assessment, inclusive of sensitive data discovery
Direct SQL Access And Write-Back

- Use only for debug
- Only objects in RPD can be queried
- Can combine with Write-back
- Security ACL grants rights to use
Example of exposing Oracle E-Business Suite Passwords from APPLSYS.FND_USER

Recommend

- OBIEE logging, monitoring and auditing
- Full audit of Security ACL
Write-Back

• Connection pools can be defined to allow users to create or update data
  - Has write back been enabled?
  - What tables allow write-back?
  - Who has security to access?
  - Can they also issue Direct SQL?

• Recommend
  - OBIEE security assessment
  - Logging and monitoring
Go URL And SQL Access

- Go URL used to integrate Presentation Services with external portals and applications
  - Set variables, session attributes

- Security concerns
  - Must authenticate first
    - Do you have a PUBLIC user?
  - Bypasses certain parts of security
  - Creates OHS (Apache) log entries
  - Can Issue SQL
Go URL & SQL Access

 Authenticate
http://<host>:<port>/analytics/saw.dll?GO&NQUser=weblogic&NQPassword=Password1

 Issue SQL
http://<host>:<port>/analytics/saw.dll?Go&SQL=select+thecolumn+from+subject_area

http://<host>:<port>/analytics/saw.dll?Go&SQL=select+person+salary+from+hr_salary_info

http://<host>:<port>/analytics/saw.dll?Go&SQL=select+encrypted_user_password+from+people_and_users
Go URL SQL Access

http://<host>:<port>/analytics/saw.dll?GO&NQUser=integrigy_test_1&NQPassword=test1234&SQL=select+encrypted_user_password+from+people_and_users

This test user CANNOT issue Direct SQL but still can query with Go URL

Being able to see passwords from APPLSYS.FND_USER is a BAD IDEA

Recommend to DISABLE GO URL
No Usage Tracking

- **Oracle provides sample RPD**
  - Manually copy or configure required components into your RPD

- **Reports on changes to**
  - Enterprise manager configuration changes
  - RPD changes
  - Who ran what report when

- **Recommendation**
  - Create new schema. Do not write to metadata schemas: BIPLATFORM or MDS
  - Make part of holistic log and audit solution
    - Integrigy Framework for Logging and Auditing
    - Pass to centralized logging (e.g. Splunk, ArcSight, etc...)
OBIEE Evaluate Function(s)

- Evaluate function(s) bypass all OBIEE security
  - Any DML statement may be issued directly against database: select, update and delete

- Any user can use. Not limited by Security ACL or by WebLogic
  - Limited only by database privileges of account used in connection pool

- Recommend to Disable
  - 11g only
Contact Information

Mike Miller
Chief Security Officer
Integrigy Corporation

web: www.integrigy.com
e-mail: info@integrigy.com
blog: integrigy.com/oracle-security-blog