

ORACLE®

A Novel Approach to creating secure Java-based Enterprise Applications

Yekeša Kosuru
Principal Software Engineer
Oracle Corporation

Agenda

- **Case study of security issues addressed in Business Intelligence Beans**
- **Java 2 Enterprise Edition (J2EE) Security**
- **Java Authentication and Authorization Service (JAAS)**
- **Securing J2EE applications using Oracle Infrastructure**
- **Questions & Answers**

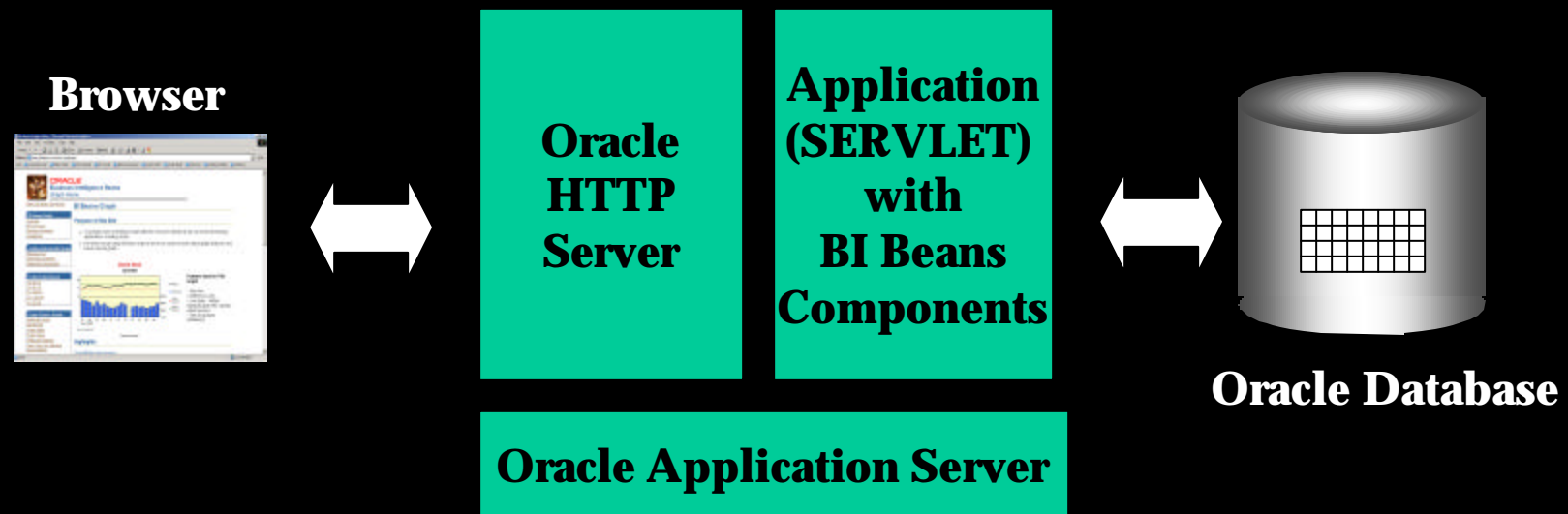
Oracle Business Intelligence Beans

- J2EE application component(s)
- Provide technology for rapid development of business intelligence applications
 - Perform Advanced Analytics
 - Data analysis (sales, budget ...)
 - Forecasting
- Java API for analytical functions
- Utilizes other Oracle technologies such as Oracle OLAP, JDBC
- Deployed as Java or Web Application

What is a Web Application ?

- Client interacts with server using HTTP
- Usable over a WAN, and through a firewall
- Users interact with browser
- Retrieves data from a variety of data sources
- Typically has three tiers:
 - Presentation Tier (Client Tier)
 - Business Logic Tier (Middle Tier)
 - Data Tier (Server Tier)

BI Beans Application Architecture



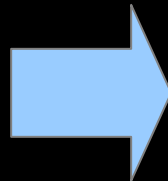
- Application (thin) can be JSP, Servlet, UIX
- Application uses BI Beans API
- BI Beans connects to an application schema in the database

Security Challenges

- To name a few...

Issues

- User Identity
- Unauthorized data access
- Data tampering & theft



Resolutions

- Authentication
- Authorization
- Network Encryption

Authentication

- Ensures that the user is who he claims he is
- Known forms of web-tier authentication:
 - Basic Authentication
 - Digest Authentication
 - Forms Authentication
- Oracle Single Sign-On Authentication
 - Username/password authentication
 - Strong authentication with 3rd party industry leaders (Kerberos, Smart Cards, RADIUS etc)
- Oracle BI Beans relies on Oracle Single Sign-On for authentication



Oracle Single Sign-On

- Allows users to login once and be authenticated to multiple applications
- Uses an encrypted login cookie to identify the authenticated users (web apps)
- Enables single user identity across all tiers and applications
- Supports JAAS
- BI Beans Applications partner with Oracle SSO via Oracle HTTP Server module (mod_osso)
- Oracle SSO technology utilizes Oracle Internet Directory (user repository)

Oracle Internet Directory

- Central repository for user and privilege management
- LDAP Version 3 Compliant
- Adds and deletes users in a central location
 - Supports GUI tools and interfaces for user management
- Supports
 - SSL
 - Directory Synchronization
 - Delegated Administration
 - User Provisioning
- Enables Single Sign-on
- BI Beans uses OID for SSO-enabled applications

Authorization

- Ensures that the user has access to the resource
- Declarative
 - No programming
 - Access control declared in deployment descriptor
 - J2EE Container performs access control
- Programmatic
 - Code performs access control
 - Can achieve granular access control
- BI Beans uses programmatic access control – object level security

J2EE Security

- Supports Basic, Digest, Form, and SSL client certificate-based authentication
- Declarative model security restricts access to URL patterns
- **Security Role** is a grouping of users with same permissions

<role>

<name>**SalesRep**</name>

<members>

All users in a role have the same level of access

<member>

<type>user</type>

<name>john</name>

</member>

</members>

</role>

- Provides API to retrieve the user, and role associated with the user

Java Authentication and Authorization Service (JAAS)

- Enables applications to authenticate and enforce access controls upon users
- JAAS supports Pluggable Authentication Module
- **Subject** represents the authenticated user
- Oracle JAAS implementation: Oracle JAAS Provider
- Oracle JAAS Provider
 - Supports Basic, Oracle Single Sign-On, and SSL Authentication
 - Comes with Oracle Application Server
 - Works in J2EE container and integrates with SSO & OID
 - Presents authenticated user identity to the application

Securing a J2EE Application (Single Sign-on Authentication)

orion-application.xml

```
<jazn-web-app auth-method="SSO" />
```

orion-web.xml

```
<login-config-props>
```

```
<auth-method>SSO</auth-method>
```

```
</login-config-props>
```

To use SSO, set the auth-method to SSO

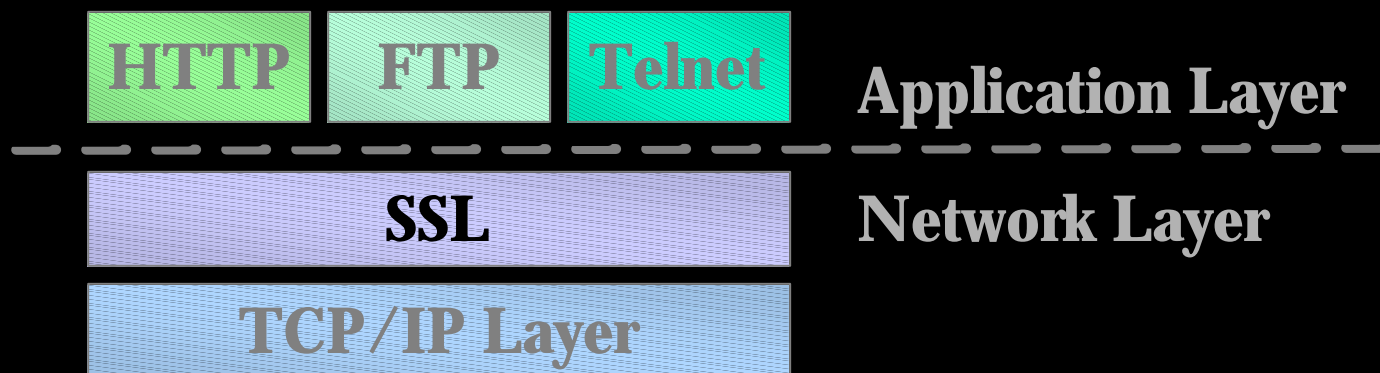
Securing a J2EE Application (Declarative Authorization)

Web.xml

```
<servlet>
<servlet-name>SalesApplication</servlet-name>
<servlet-class>com.xyz.sales.SalesApp</servlet-class>
<security-role><role-name>SalesRep</role-name></security-role>
<security-role><role-name>RegionalManager</role-name></security-role>
<security-constraint>
  <web-resource-collection>
    <web-resource-name>SalesApplication</web-resource-name>
    <url-pattern>/sales</url-pattern>
  </web-resource-collection>
  <!-- Declare Roles that have access to a web resource - ->
  <auth-constraint> <role-name>SalesRep</role-name> </auth-constraint>
  <auth-constraint> <role-name>RegionalManager</role-name> </auth-constraint>
</security-constraint>
```

Network Encryption

- Encrypt network traffic using Secure Sockets Layer
- Transport protocol that provides:
 - Confidentiality, using encryption
 - Integrity, using encryption
 - Authentication, using certificates



A large graphic featuring a grey 'Q' on the left and a grey 'A' on the right. A red ampersand (&) is positioned between them, overlapping the 'Q' and 'A'. The words 'QUESTIONS' and 'ANSWERS' are written in white, bold, sans-serif capital letters across the center of the graphic, with 'QUESTIONS' on the top line and 'ANSWERS' on the bottom line.

QUESTIONS
ANSWERS

ORACLE®

Oracle Technology Network Security Samples

http://otn.oracle.com/sample_code/deploy/security/9i_security.html

<http://otn.oracle.com/tech/java/oc4j/htdocs/how-to-security-JAAS.html>

BI Beans Application Architecture

