Web 2.0 in the Enterprise: Balancing Participation and Security

Manish Devgan
Product Manager – Oracle WebCenter & Portal Products
The preceding 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 remains at the sole discretion of Oracle.
Introduction

• Product Manager – Oracle WebCenter & Portal Products
• Prior Experience
  • Lead/Architect for WebCenter Security Framework
  • Architect for BEA WebLogic Portal (WLP) Services
• Patents in Collaboration, Security, Entitlement Management
• Books
  • BEA WebLogic Platform – SAMS Publishing 2003
  • Contributing author: Reshaping Your Business with Web 2.0 – McGraw Hill 2008
• Featured speaker at various conferences
Chapter 8

Security and Compliance: Maintaining Control While Providing Flexibility

By Vince Casarez

Manish Devgan
Program Agenda

Web 2.0
- Advent of Web 2.0 in the Enterprise
- Security Considerations for RIA
- Securing Enterprise Applications
- Oracle WebCenter Security Framework
- Balancing Participation and Security
Web 2.0

Wikis are indispensable tools for knowledge

Blogs provide information, analysis and opinion

Social networks connect and illuminate

Widgets and mashups extend functionality

Link analysis surfaces most relevant content

Tags and bookmarks personalize content
What is Web 2.0?

• Not a new technology

• Web 2.0 is the combination of three distinct avenues of Web design:
  • RIA (Rich Internet Application)
  • Collaboration / relationship based Web experience
  • Mashups
Rich Internet Applications (RIA)

- RIAs are Web applications that have the features & functions of client/server-style applications.

- RIAs implement:
  - Client-side processing to allow richer, more responsive UI than traditional Web applications
  - Asynchronous communication with the server (generally AJAX) allowing partial page refresh
Collaborative Web

Primary characteristics of the Web 2.0 Platform:

- Ability for users to contribute to, and collaborate on, the nature of information and how it relates to their needs
- Social networking that allows users to define relationships with others to optimize the access to, and use of, the available information
Mashups

“A Web-based application that combines data from more than one disparate source into a single integrated service”
Program Agenda

• Web 2.0
• Advent of Web 2.0 in the Enterprise
• Security Considerations for RIA
• Securing Enterprise Applications
• Oracle WebCenter Security Framework
• Balancing Participation and Security
Advent of Web 2.0 in the Enterprise

Internal Resources
- Oracle E-Business Suite
- PeopleSoft
- Siebel Call Center
- Oracle Transportation Management
- JD Edwards EnterpriseOne
- Siebel CRM On Demand
- Other CRM

External Resources
- Email
- Phone
- Browser
- IM
- RSS
- Desktop

Manish Devgan
Structured Processes & Unstructured Interactions
Creating a “Web 2.0-Enabled” Enterprise

- **Capture** information, people, processes, systems, connections
- **Deliver** it all in context via highly interactive applications
- **Engage** the user in an interactive, collaborative experience
Translating Web 2.0 to the Enterprise

<table>
<thead>
<tr>
<th>Technology</th>
<th>Consumer (Web 2.0)</th>
<th>Enterprise 2.0*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blogs</td>
<td>Sharing opinions, reviewing products</td>
<td>Thought Leadership, Product Evangelism</td>
</tr>
<tr>
<td>Social Networks</td>
<td>Meeting friends &amp; acquaintances</td>
<td>Connecting with Subject Matter Experts, content, and processes</td>
</tr>
<tr>
<td>Mashups</td>
<td>Maps</td>
<td>Integration of data from multiple applications</td>
</tr>
<tr>
<td>Search/Tagging</td>
<td>Page ranking – relevant content</td>
<td>Activity Ranking – relevant business information</td>
</tr>
<tr>
<td>Wiki</td>
<td>Sharing knowledge</td>
<td>Project information sharing &amp; managing deliverables</td>
</tr>
<tr>
<td>Discussions</td>
<td>Open discussions on common topics of interest</td>
<td>Forums for customer support and engagement for product feedback</td>
</tr>
</tbody>
</table>

* Word coined by Professor MacAfee of the Harvard Business School in 2006
Web 2.0 and Enterprise 2.0

Security Paradigms

• Consumer Space
  • Need ultimate User engagement and interaction at the cost of lower security enforcement for viral adoption

• Enterprise Space
  • Need a balance between Participation and Security
Program Agenda

- Web 2.0
- Advent of Web 2.0 in the Enterprise
- Security Considerations for RIA
- Securing Enterprise Applications
- Oracle WebCenter Security Framework
- Balancing Participation and Security
RIA – AJAX Model

AJAX-enabled Web page

Application Container

Page Request

Page Submission

User Interaction

Application Services
- Method1()
- Method2()
- Method3()

Title: begins with

XMLHttpRequest

CallbackFunction() {
    • process response
    • Update DOM
}

<script type="text/javascript">
</script>
AJAX / RIA Security Considerations

• All the problems of traditional Web applications and more
• Increase in attack “surface”
  • State resides on the client
  • Client injections – DOM, JSON, RSS, ..
• Exposing business processes
• Dynamic content entry
  • Cross-site scripting (XSS)
  • Cross-site request forgery (CSRF/XSRF)
Security cannot be achieved by obscurity!
Program Agenda

• Web 2.0
• Advent of Web 2.0 in the Enterprise
• Security Considerations for RIA
• Securing Enterprise Applications
• Oracle WebCenter Security Framework
• Balancing Participation and Security
Enterprise Applications Security

Considerations & measures when adopting Web 2.0

- UI framework with a mature security model
- Service layer security and compliance
- Message-level data security
- Identities and Access Control
- Proliferation of Identities
- Fine-grained Authorization
- Compliance Policies for your business domain
A Typical Enterprise Application Today

The stakes for securing content are high

- Composite application brings disparate applications together
- Users can see the transaction context across applications, allowing them to focus on the business process
Program Agenda

• Web 2.0
• Advent of Web 2.0 in the Enterprise
• Security Considerations for RIA
• Securing Enterprise Applications
  Oracle WebCenter Security Framework
• Balancing Participation and Security
“Enterprise-Ready” Web 2.0 Services

Social Networking
- Announcements
- Blog
- Discussions
- Instant Messaging and Presence
- People Connections
- Wiki

Personal Productivity
- Documents
  - Events
  - Links
  - Lists
  - Page
  - Tags
  - Tasks
- Mail
  - Notes
  - Recent Activities
  - RSS
  - Search
  - To-Dos
  - Worklist

Manish Devgan
Building Enterprise Mashups Using WebCenter
WebCenter Security and Privilege Model

…enables the building of a rich application that is interactive and engaging, and enables team collaboration and productivity without giving away the keys to the castle!
RIA Without the Pain

- Java Server Faces (JSF) frameworks, such as ADF, allow for:
  - Definition of self-contained “rich” components
  - Validation code to be held on the server
  - Targeted JavaScript with limited points of exposure
  - Page designers to be shielded from the complexity of JavaScript

<af:trainButtonBar/>
<af:dialog>
<af:progressIndicator id="progId" value…}" />
Mature Security Framework

• ADF comes with a security framework built upon a pluggable architecture using JAAS
• The framework includes a security-aware model layer with predefined component-specific permissions
Security Enforcement at Service Layer

Application

Discussions  Tags/Links  Documents  Tasks  ...

Web 2.0 Services

Framework Extensions

Security
Search
Lifecycle

WebCenter Framework

Manish Devgan
Secure Identity Propagation

- WS-Security for Secure Identity Propagation
- Complete message protection (confidentiality and integrity)
- Various token profiles supported:
  - SAML
  - UsernameToken without password
  - UsernameToken with password
Authorization Models

Customized based on the service*

- Permission-based
  - Services sharing persistence store and permission model with the application
- Role-mapping based
  - Services that need to access remote back-end resources with independent permission models

* Web 2.0 Service
Program Agenda

- Web 2.0
- Advent of Web 2.0 in the Enterprise
- Security Considerations for RIA
- Securing Enterprise Applications
- Oracle WebCenter Security Framework
- Balancing Participation and Security
Secure Out-of-the-box...

- Secure by default
- Admin needs to "open it up"
- Explicit UI actions to provision and grant access
...with flexibility to open it up!
Maintaining Control..
..while maximizing participation

- Enabling public group spaces feature
- Easily opening site for maximum participation
Maximizing Participation

- Ability to join public group spaces by searching
- Ability to discover and subscribe to a group space
Enabling Balance Between Participation and Security

Manish Devgan
**Key Takeaways**

1. Web 2.0 is a combination of RIA, collaborative Web experience, and mashups

2. Enterprise Applications are rapidly leveraging Web 2.0 technologies

3. WebCenter security and privilege model provides a balance between participation and security

4. You can build a “Web 2.0-enabled” Enterprise Application without away giving the keys to the castle!
Oracle is the Information Company