



JBoss Security for Java EE Developers

Anil Saldhana and Scott Stark

JBoss Division
Red Hat Inc.
February 15, 2008



Speakers

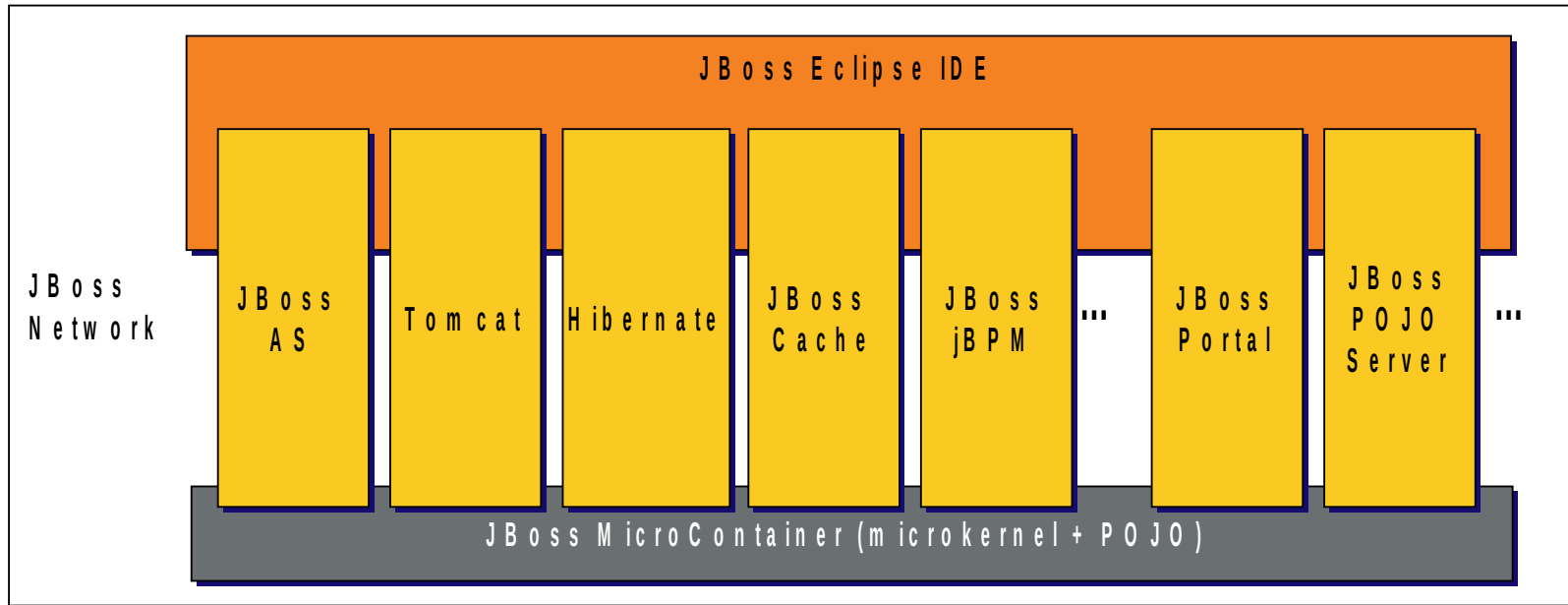
- Anil Saldhana is the project lead of JBoss Security and Identity Management.
 - Represents JBoss/Red Hat at the JCP, Oasis and W3C.
- Scott Stark is the Vice President of Technology and Architecture in the JBoss Division of Red Hat.
 - Former CTO of JBoss.

Agenda

- Introduction
- Security Domain
- Security For the Web Layer
- Security For the EJB Layer
- What's new in JBoss5?
- Future Direction
- Q&A

Introduction

JBoss Security is a cross cutting concern



Introduction

- JBoss Security provides access control feature for the following components of Java EE specification:
 - EJB
 - JCA
 - JMS
 - Web
 - Web Services ...
- And other components that run on JBoss AS such as JBoss Portal.

Security Domain

- Security Domain represents
 - A collection of pluggable modules for various aspects of Security.
 - A set of JAAS login modules (JBoss 4.x)
 - A set of authorization, audit, mapping ... modules (5.x)
 - JNDI Name of the JBoss Security Managers (4.x)

Security Domain

- Configured in an XML file (conf/login-config.xml)

```
<application-policy name = "jmx-console">
  <authentication>
    <login-module
code="org.jboss.security.auth.spi.UsersRolesLoginModule"
    flag = "required">
      <module-option name="usersProperties">props/jmx-console-
users.properties</module-option>
      <module-option name="rolesProperties">props/jmx-console-
roles.properties</module-option>
    </login-module>
  </authentication>
</application-policy>
```

Security For The Web Layer

- You secure your web applications by defining `<security-constraint>` elements in your `web.xml`

```
<security-constraint>  
  <display-name>Restricted GET</display-name>  
  <web-resource-collection>  
    <web-resource-name>Restricted Access - Get Only</web-  
resource-name>  
    <url-pattern>/restricted/get-only/*</url-pattern>  
    <http-method>GET</http-method>  
  </web-resource-collection>  
  <auth-constraint>  
    <role-name>GetRole</role-name>  
  </auth-constraint>  
  <user-data-constraint>  
    <transport-guarantee>NONE</transport-guarantee>  
  </user-data-constraint>  
</security-constraint>
```

Security For The Web Layer

- web.xml define the mechanism used for transfer of security context from the browser (user agent) to the container
 - - FORM
 - BASIC (uses HTTP_BASIC)
 - DIGEST(uses HTTP_DIGEST)
 - CLIENT-CERT

```
<login-config>  
  <auth-method>CLIENT-CERT</auth-method>  
  <realm-name>JBoss JMX Console</realm-name>  
</login-config>
```

Security For The Web Layer

- Then you define a `<security-domain>` element in `jboss-web.xml`

```
<jboss-web>  
  <security-domain>java:/jaas/jmx-console</security-  
domain>  
</jboss-web>
```

- The login modules configured as part of your security domain define what is used for generating the Subject (an artifact used for access control)

Security For The EJB Layer

- Define EJB method permissions in ejb-jar.xml

```
<method-permission>  
  <description>The admin role may access any method of  
the  
  EmployeeServiceAdmin bean </description>  
<role-name>admin</role-name>  
<method>  
  <ejb-name>EmployeeServiceAdmin</ejb-name>  
  <method-name>*</method-name>  
</method>  
</method-permission>
```

Security For The EJB Layer

- Then you define a `<security-domain>` element in `jboss.xml`

```
<jboss>  
  <security-domain>java:/jaas/jmx-console</security-  
domain>  
</jboss>
```

- The login modules configured as part of your security domain define what is used for generating the Subject (an artifact used for access control)

What is new in JBoss5?

- Java Authentication SPI for Containers (JASPI)
- Authorization Framework
- Auditing Framework
- Identity Trust Framework
- Mapping Framework
- Instance Based Security (ACL Implementation)

What is new in JBoss5?

- Frameworks still defined at the security domain level

```
<application-policy name="someconfig">
  <authentication>
    <login-module
code="org.jboss.security.auth.spi.UsersRolesLoginModule"/>
  </authentication>
  <authorization>
    <policy-module
code="org.jboss.security.authorization.modules.DelegatingAuthorization
Module"/>
  </authorization>
  <rolemapping>
    <mapping-module
code="org.jboss.security.mapping.providers.DeploymentRolesMappingPr
ovider"/> </rolemapping>
</application-policy>
```

JBoss5 : JASPI/JSR-196

- JAAS is great for authentication but loses the message type during authentication.
 - Authentication for web layer does not have access to the web request/response
 - Authentication for ejb layer does not have access to EJB Invocation object.
- JASPI is a natural extension of JAAS which has ServerAuthModules that are provided the network message types
 - Servlet Request/Response for Web
 - SOAP Request/Response for WS.

JBoss5 : Authorization Framework

- Ability for Authorization Modules to be plugged in at the security domain level
- The modules can do regular, JACC, XACML, Custom Access Control for layers such as Web and EJB.

JBoss5 : Audit Framework

- Ability for Audit Providers to be plugged in at the security domain level
- The default provider is a logging provider that logs to log/audit.log (configurable)
- Log all access control access for Web and EJB methods.

JBoss5 : Identity Trust Framework

- Ability for Identity Trust Providers to be plugged in at the security domain level
- The providers can provide trust checks for the caller.
 - If the caller is trusted, go directly to authorization.
- Caller may come with SAML, WS-Trust, Kerberos tokens.

JBoss5 : Mapping Framework

- Ability for Mapping Providers to be plugged in at the security domain level
- The providers can map
 - Principal (Map one principal type to another)
 - Roles (Map one set of roles to another)

JBoss5 : Instance Based Security

- JBoss AS requires coarse-grained security.
 - Role Based Access Control (RBAC)
- Projects like Portal, jBPM, JBoss Rules need domain level or fine-grained authorization.
 - A portal page has multiple sub-components such as sub--pages, windows etc.
- The new Authorization Manager implementation in JBAS should provide both coarse-grained access control needed by the containers as well as fine-grained access control needed by JEMS projects.

Future Directions

- Ability to provide support for Federated Identity at the core.
 - SAML 2.0
 - WS-Federation/WS-Trust
 - OpenID
- Kerberos support for authentication.
 - SPNEGO/Windows Desktop SSO
 - FreeIPA (Fedora)
- Secure Configuration of JBoss AS.
 - Common Criteria Evaluation
 - SELinux Policies

Q&A & Resources

- <http://labs.jboss.com/jbosssecurity/>
- JBoss Security Beta Program
<https://www.redhat.com/mailman/listinfo/jboss-security-beta>