



Java 2 Enterprise Edition Security

Kevin Osborn
Sun Microsystems
July 15, 1999
DocSec '99



Slide 1



Agenda

- History
- Summary of J2EE scope/features
- Futures
- Discussion



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 2

Java, EJB, Servlets, etc.

- Java Platform is very popular for writing middleware
- Programming productivity
- Easy distributed Programming (RMI)
- Many Enterprise technologies
- JDBC
- Java IDL
- RMI/IIOP
- JTA
- JTS
- Servlets
- EJB



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 3

What's the problem

- Divergence in application servers
- Difficulty in deployment
 - Are all the required services available?
 - Complex installation instructions
- Security embedded in applications



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 4

Enter the Enterprise Platform

- Standard set of services/api's
- XML deployment descriptor
 - Relates components
 - communicates intentions of the programmer or assembler
 - Transactional needs
 - Environment needs
 - Security Needs
- Security handled by the platform (mostly)



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 5

EJB Foundation

- Java Component Model
- Container takes care of
 - transactions
 - security
 - environment
- Session Beans
- Entity beans (container managed persistence)
- Distributed transaction support
- Deployment descriptors
- Small Role API for fine grained access control/behavior modification.



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 6

J2EE 1.2

- **Extends EJB 1.1 deployment model to web, application components.**
- **Login to web server managed by the platform**
- **Communicating the Security Model**
 - Platform spec
 - Application Programming model
 - Security whitepaper.



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 7

Security

- **Declarative security**
- **Container requirements**
 - Deployment Descriptor interpretation
 - authorization
 - identity propagation
- **Proxy authentication for browsers**
 - Login session management



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 8

Roles

- **Functional decomposition based on logical roles**
- **Roles assigned to method permissions**
- **May also be referenced in code**
 - `isCallerInRole(String role)`
- **Roles are mapped at deployment time**
- **Authorization based on role determination done by container**



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 9

Login sessions

- **Maintained by server**
- **New Servlet api (2.2) for interaction**
 - `logout`
 - `getCallerPrincipal()`
 - `isCallerInRole()`
- **Span multiple applications**



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 10

Form based login

- GUI control for logging in
- Login still handled by server, not application
- Associated with content in deployment descriptor



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 11

Futures

- Additional service contracts
 - User
 - Administrator
 - developer/assembler
- JAAS integration
 - authentication
 - code authorization
- Interoperability
 - Mandated trust boundaries?



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 12

Declarative security

- Extension of EJB declarative model
- First appearance in Web DD
- Constraints (inbound/outbound)
 - Authentication
 - Auditing
 - Confidentiality
 - Integrity
 - Delegation



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 13

The CORBA Connection

- Sun is OMG participant
- Many EJB implementations rely on RMI/IIOP
- RMI/IIOP required for platform vendors to support CORBA connectivity
- JTA and distributed transactions mostly supported with OTS (JTS)
- IIOP required EJB protocol for interoperability in next version.



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 14

Work with me people

- What is the sweet spot for portable interoperable distributed components?
- How important is security service replace-ability
- Email:
 - kevin.osborn@east.sun.com
- Web: <http://java.sun.com/products/j2ee>



7/15/99

Sun Microsystems Proprietary and Confidential: V. 6

Slide 15