Oracle9i
Application Server
v2 Security
What’s an Application Server?

- Development and deployment environment
  - Web (HTML, XML, SOAP)
  - J2EE
  - Provides standard environment in which to execute customer’s business logic

- Integration Tools
  - Centralized management functions
  - Portal
  - Reduce deployment cost

- Specific services
  - Presentation and UI
  - Business functions
  - Improves productivity, reduces deployment time
Oracle9i Application Server Security

- Framework for secure internet application deployment
  - Flexible, standards-based
  - Security for Java2 Enterprise Edition (J2EE)
- Integration Framework
  - Single Sign-On (SSO)
  - Oracle Internet Directory (OID)
- Specific tools
  - SSL
  - Java Authentication and Authorization Services (JAAS)
Security Features of Oracle9iAS

- Oracle9i AS Single Sign-On
- Directory-based Security in Oracle9iAS
- Oracle9i AS Java Security
- Oracle 9i HTTP Security
- Oracle9i AS Portal Security
SSO - The Internet Changes Everything...

- Unlimited connectivity = unlimited accounts and passwords!
- Insecure
  - Post-It™ password store
  - Admins can’t keep up with personnel changes
- Costly
  - Login for 10K person enterprise is o($10M)
  - 50% of helpdesk calls are password-related
Partner vs. External Applications

- **Partner applications**
  - Accept authentication by SSO Server
  - Modified to work in SSO framework
  - Mod_OSSO allows Oracle web listener to be partner application
  - SSO SDKs also available

- **External applications**
  - Not modified to work in SSO framework
  - Supplied with native username/password by Server
SSO Components

- **Applications**
  - Partner
  - External

- **Centralized SSO Server**
  - Verifies SSO password
  - Sets SSO cookie at client
  - External app username/password store

- **Username/Password managed in LDAP directory**
  - Oracle Internet Directory (OID)
  - Other LDAPv3 directory requires OID gateway
  - Users provisioned through OID Delegated Administrative Services (DAS)
SSO vs ASO

- **Oracle9iAS SSO for thin clients**
  - Part of Oracle9iAS infrastructure
  - Supports eBusiness suite (Applications 11i)
- **Oracle Advanced Security**
  - SSO for Net8 (fat) client-server
  - Kerberos, smartcards, PKI/SSL
- **PKI in all layers, clients, long-term**
New Features

- **Mod_OSSO**
- **OID/DAS Integration**
- **Enhanced Authentication**
  - PKI authentication via client certificate
  - Pluggable authentication via API - e.g., Netegrity Siteminder®
- **Paranoid Application Support**
  - Application can force reauthentication
  - For highly sensitive applications
- **Single Sign-Off**
- **Global Inactivity Detection**
Oracle/Netegrity Partnership

- **Oracle Supports Netegrity Single Sign-On (SSO)**
  - Oracle9i Application Server (Oracle9iAS)
  - Oracle eBusiness Suite
    - Applications 11i - ERP, CRM
    - Oracle Internet Developer Suite

- **Netegrity Supports Oracle Internet Directory (OiD)**
  - SiteMinder users in OiD
  - SiteMinder policies in OiD

- **Other SSO/authentication products supported through API**
Oracle & SiteMinder Integration

- Client Browser
- Oracle9i AS
  - mod_SM
- Partner Application
- SiteMinder Web Agent installed in Oracle9iAS web listener (mod_SM)
- Oracle SSO Server obtains user identity from mod_SM
- SiteMinder Policy Server users, policies managed in Oracle Internet Directory
Directory-based Security

• OID provides common framework for
  – User management
  – Password management
  – Authorization

• OID DAS provides
  – Common provisioning mechanism
  – Self Service Console (SSC)
  – API
Oracle Internet Directory

- **Scalability**
  - 500+ million user entries on a single server
  - 1000’s of simultaneous clients
- **High availability**
  - Multimaster replication using Oracle Advanced Symmetric Replication
  - Oracle8i hot backup/recovery
- **Security**
  - Sophisticated security model based on access control lists
- **Standards-based**
  - Native LDAPv3 implementation
  - Tightly integrated with the Oracle system management environment
OID - Common Authorization Framework

Oracle Internet Directory LDAP Service

LDAP Standard Interface
Oracle9iAS Java Security - JAAS

• What is JAAS?
  – Java package that enables services to authenticate users and enforce access controls (authorization)
  – Implements a Java version of the standard Pluggable Authentication Module (PAM) framework

• What is in Oracle9iAS?
  – Oracle’s JAAS (Java Authentication and Authorization Services) implementation, plus extensions
What does JAAS do?

- JAAS provides key security services for
  - Authentication (identifying users)
  - Authorization (limiting what they can do)
  - Delegation (enabling code to run securely, with privileges of other users)
JAAS Authentication Features

• LoginModules
  – Enables customers to add strong authentication for Java-based applications
    – SSO
    – SSL
    – Custom
  – For example, a Java-based banking app could require challenge-response authentication

• Benefits
  – Ability to integrate Java apps with SSO
  – Extensible authentication
JAAS Authorization Features

- **JAAS Authorization**
  - Support for hierarchical, role-based access control
  - Support for principal (that is, user) and code-based policies
  - Full support for Java2 permission model

- **JAAS-LDAP**
  - Centrally manage users, access control policies in Oracle Internet Directory
  - Scales to very large user communities

- **JAAS-XML**
  - Manage users, access control policies in XML files
  - Lighter weight than LDAP
  - Unlike principals.xml, obfuscates passwords
JAAS Delegation Features

- **Impersonation**
  - support for impersonation of a specified user
  - includes RunAsClient and RunAsID

- **Benefits**
  - Enforcement of security principle of ‘least privilege’
    - users have *fewest* privileges required to do their jobs
    - users only exercise privilege in context of a well-formed business rule (e.g. an enterprise bean)
HTTP Server Security

- Configuration and management
- Network Encryption (confidentiality)
- Authentication
- Access control / Authorization
Configuration and Management

- Access specified using Apache directive configuration files
- E.g., to restrict files in the directory “internalonly” to hosts with IP address 192.168.1.*:

```html
<Directory /internalonly/>
  order deny, allow
  deny from all
  allow from 192.168.1.*
</Directory>
```
Network Encryption

• Secure Sockets Layer (SSL)
  – Internet standard encryption protocol for http
  – a.k.a. HTTPS
  – Provided by mod_OSSL

• Provides
  – Data confidentiality on the network
  – Data integrity on the network
  – Optional user authentication via PKI (X.509v3 certificate)

• Strong crypto for world-wide use
  – RC4/128
  – 3DES
Authentication

• Basic authentication
  – Username/Password
  – Widely used

• SSL
  – Based on “entire” client X.509v3 Cert

• SSO
  – Integrates HTTP Server with Oracle SSO
  – Uses mod_OSSO
Access Control

• Access control enforced on
  – URL patterns
  – Files
  – Directories

• Access protection based on combination of:
  – X.509 Certificate pattern
  – User identity
  – Group membership
  – Host name
  – IP address
  – Other characteristics (e.g., browser type)
Portal Security

- Users/Groups
- Authentication
- Authorization
- Session management
- Application integration
Users

- SSO Server authenticates users
- Users created and managed in OID
  - Provisioning via OID DAS
- Users are assigned privileges and may belong to groups
Groups

• Groups are collections of users and may also contain other groups
  – Can be hierarchical - like mailing lists
  – Can be private
Authorization Features

• Oracle Portal defines application-specific privileges
• Extensible privilege model
• Privileges can be granted to users or groups
Application Integration

- Portal Application
  - Obtains user identity from Portal
  - Only works for applications on Portal
- Partner Application
  - Obtains user identity from SSO Server
- External Application
  - Applications maintains its own username/password
  - SSO Server provides these to external application when it is accessed through Portal
Security to Oracle9i Database

- **Proxy User Authentication**
  - AS authenticates as itself, sets “real user” context
  - Can be limited to specific users, roles per AS
  - Both identities (AS and user) are audited, can be used for access control

- **Oracle Advanced Security for additional protection**
  - Net8 encryption
  - Advanced Authentication
Three Tier Security

Employee
- SSL

Partner
- SSL

Supplier
- SSL

Customer
- SSL
- HTTP

App Server 1
acting on behalf of Scott

Advanced Security

Net*8
IIOP
JDBC
Oracle9iAS Security - Summary

- Basic web security through HTTP Server
  - Extended with mod_OSSL and mod_OSSO
- Single Sign-On for Oracle and third party applications
- Directory-based authentication, authorization, provisioning
- Java Security through JAAS
- Secure Portal Framework with Oracle9iAS Portal