SOA SECURITY: ORACLE WEB SERVICES MANAGER

SOA SECURITY SOLUTION

Standards Supported:

- Encryption algorithms: AES-128, AES-256, 3-DES
- Message digests: MD5, SHA-1
- Message structure: XML / SOAP / WS-Security 1.0
- Security token profiles: Username, X.509, SAML
- Message integrity: XML Signature
- Message confidentiality: XML Encryption
- Policy format: WS-Policy
- PKI
  - Key encryption: RSA OAEP-MGF1P, RSA V1.5
  - Signature algorithms: RSA (PKCS #1) (1024-, 2048-bit keys), DSA
  - Credentials store, wallets: JKS, PKCS#12

Platforms Supported:

- Operating Systems: Windows, Linux, Solaris, AIX
- Applications Servers: Oracle Application Server, IBM WebSphere, BEA WebLogic Server, JBoss
- Database Systems: Oracle Database, Microsoft SQL Server.

Companies worldwide are actively implementing service-oriented architectures (SOA), both in intranet and extranet environments. While SOA offers many advantages over current alternatives, deploying networks of web services still presents key challenges, especially in terms of security and management. Oracle addresses SOA security and management with a standards-based solution, Oracle Web Services Manager (WSM), delivered both as a standalone product and as part of the Oracle SOA Suite.

Introduction

Oracle WSM is a J2EE application designed to define and implement web services security in heterogeneous environments, provide tools to manage web services based on service-level agreements, and allow the user to monitor runtime activity in graphical charts.

Oracle WSM can be used by developers to test security on individual web services at development time or systems administrators to implement company-compliant security leveraging identity management infrastructures in production environments.

Declarative Security

Oracle WSM supports a declarative security approach, i.e., no programming is required. Oracle WSM includes the following components:

- Policy Manager
- Policy Enforcement Points
- Operational Management and Monitoring

Policy Manager

Oracle WSM's Policy Manager is a graphical tool for attaching predefined security and management policies to web services. Policies are persisted in a database and propagated to the enforcement points by the Policy Manager.

Policy Enforcement Points

Policy enforcement points (PEPs) intercept requests made to a web service and apply policies defined for that web service.

PEPs can be Agents deployed into the application to be protected (end-to-end security) or Gateways providing the flexibility of a proxy server.

ORACLE IDENTITY MANAGEMENT PRODUCTS

Oracle Access Manager delivers critical functionality for access control, single sign-on, and user profile management in the heterogeneous application environment.

Oracle Identity Manager is a powerful and flexible enterprise identity provisioning and compliance monitoring solution that automates the creation, updating, and removal of users from enterprise systems such as directories, email, databases, and ERP.

Oracle Identity Federation is a self-contained solution that enables cross-domain single sign-on and business partner management.

Oracle Internet Directory is a robust and scalable LDAP v3-compliant directory service that leverages the high availability capabilities of the Oracle 10g Database platform.

Oracle Virtual Directory provides Internet and industry standard LDAP and XML views of existing enterprise identity information without synchronizing or moving data form its native location.

Oracle Enterprise Single Sign-on provides users with unified sign-on and authentication across all their enterprise resources including desktops, client-server, custom, and mainframe applications.

Pipeline Metaphor

The user defines sequential policy steps in an incoming pipeline for a web service request (example of steps are Authenticate, Authorize). Policy steps are executed at runtime and if successful, the request is granted access to the protected web service.

The user defines sequential policy steps in the outgoing pipeline for a web service response, for example: Encrypt, Sign message. Policy steps are executed at runtime.

Operational Management and Monitoring

Oracle WSM's Monitor collects data from the enforcement points at runtime and aggregates the information to be rendered in dashboard views.

The user can define service-level agreements (SLAs), for example, assured latency, scheduled downtime, maximum failure rate. SLAs are enforced at runtime and execution details are displayed in graphical charts.

Oracle WSM provides a visual representation of security statistics, for example the number of failed authentications or authorizations, as well as traffic analysis, for example the number of messages and bytes per service or operation.

Governance

Oracle WSM integrates with UDDI –compliant registries and allows for implementation of corporate rules or government regulations through policies executed and monitored at runtime.

Deployment

Oracle WSM leverages the underlying application server's infrastructure for scalability, high availability, and backup and restore. Oracle WSM's Gateway allows the user to redirect web services requests to available web services when the web service invoked is down, and allows the user to redirect requests to specific web services based on the content of the request (content-based routing).

Integration

Oracle WSM is the Oracle SOA Suite's security lynchpin. Oracle WSM protects BPEL and ESB processes using both types of policy enforcement points (Agents and Gateways).

In addition to LDAP directories, Oracle WSM can leverage identity management infrastructures such as Oracle Access Manager or CA eTrust SiteMinder for authentication and authorization.

ORACLE