External Authorization vs. Authentication

Christian Patrascu, Oracle Corporation

Keywords: Authorization, Authentication, Single Sign On, SSO, Identity Management, IdM, I&AM, Identity and Access Management.

Please write down your Keywords. Authorization, Authentication, Single Sign On, SSO, Identity Management, IdM, I&AM, Identity and Access Management

Introduction

Unlike authentication, which happens only once per session, authorization is active throughout the session, controlling every action and every piece of information displayed to the user. Authorization is the "Glue" which ties Compliance and Security requirements with application code and human workflow. Enterprise-wide authorization solutions focus on technology, business process and compliance requirements. This session covers all aspects involved in deploying end-to-end enterprise wide authorization solutions, lessons learned from field and best practices. The talk will include an overview of the new release of OES 11g, and a discussion with customers about their deployment of OES.

Oracle Entitlements Server

Oracle Entitlements Server (OES) is a fine grained authorization service which can be used to secure applications and services end-to-end across the enterprise. It provides authorization for a broad set of ecosystems including Java EE, Java SE, .NET, SOA, content management systems and databases. OES comes with several out-of-the-box (OOTB) integrations which can be dropped into a given deployment with minimal impact. It allows for separation of development and deployment cycles, so application developers can be agnostic of deployment issues. As OES is Oracle's strategic authorization solution for all our applications and technology it has been designed to meet the performance and scalability requirements of Oracle's largest and most complex customer deployments. Unlike authentication, authorization requests have latency constraints in order of micro seconds and a single web page access can generate over 50 individual authorization requests. OES provides a rich hierarchical policy model based on the Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC) standards. It supports multi-level delegated administration which allows for precise control over authoring and management of security policies. OES is the most mature fine grained authorization product in the market and it has been in continuous use for well over a decade.

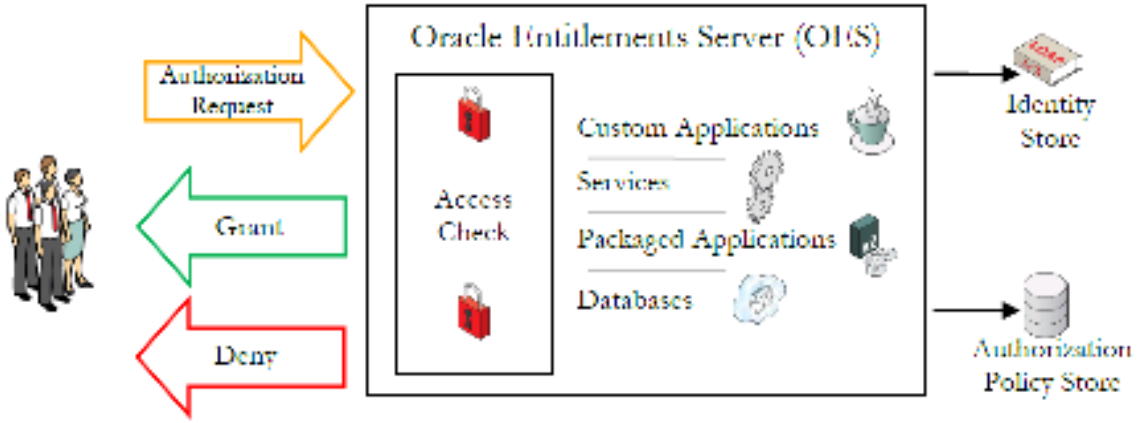

Illustration. 1: Overview of Oracle Entitlements Server

The figure above provides a high level overview of OES. Users as part of their normal activities, such as accessing web pages, generate access requests. OES maps these requests into a normalized form and performs checks against authorization policies. During policy evaluation OES can utilize information from external data sources such as LDAP systems, databases and Web Services. At the end, OES sends an authorization response back to the caller in the form of an Authorization Decision and Obligations (Obligations are described in the section Policy Design).

Component Architecture

Oracle Entitlements Server (OES) consists of the following components:

a) Administration Console: The Administration Console provides a rich Web based UI for policy authoring and management. It also serves as a provisioning service and can distribute policy updates to applications. It has import, export and migration tools for policy lifecycle management.

b) Policy Store: The Policy Store serves as a central persistent store authorization policies. This helps in centralized management of security. Applications can optionally bypass the Policy Distribution Service and get policies directly from the central policy store.

c) Security Module (SM): This is the runtime component which includes the core authorization engine (also known as Policy Decision Point or PDP). When the SM gets an authorization request from a user or application, it evaluates this request against all relevant policies and gives a final authorization result. As part of policy evaluation, the SM can look up information from external data sources such as LDAP systems, databases, Web Services and other data sources. An SM also includes PEPs (Policy Enforcement Points), which can be used to automatically enforce OES authorization decisions in environments such as WebLogic and SharePoint among others. An SM can also be optionally configured to directly administer policy. This allows a single application to perform Policy Administration, Policy Decision and Policy Enforcement.

d) Policy Distribution Service: This acts a bridge between the OES administration server and various Security Modules. Policy distribution process is initiated when an administrator decides that a set of policy changes are ready to be distributed. The Policy Distribution Service then automatically handles the provisioning lifecycle and computes the delta between what the SM already has and the latest set

of policies to minimize distribution payload. Apart from ensuring transport level security the Policy Distribution Service also makes sure that only the required set of authorization policies are sent to each SM /Application. When an SM starts up it gets all pending policy updates from Policy Distribution Service. Optionally customers can replace the OES Policy Distribution Service with their own provisioning solution.

e) Policy lifecycle management tools: OES provides automated tools for moving policies from development-to-test and test-to-production. Customers can also store the policy files along with their source code in a revision control systems. Migration tools can be used for policy backup, restore and disaster recovery.

As part of computing authorization decisions, Security Modules (SM) can use information from external identity stores, databases and web services (Policy Information Points or PIPs).

Conclusion

Embedding authorization decisions in application code leads to brittle and static policies which cannot keep pace with changing security requirements. Not having a centralized policy management and uniform enforcement infrastructure leads to security silos where each application uses a different security mechanism and the resulting authorization policies cannot be reused across organizations. Over time these types of deployments become complex, unmanageable and expensive to maintain. Lack of insight combined with poor auditing facilities leads to compliance and security nightmares. Using standards based COTS authorization solutions, enterprises can regain control over how security is managed across different organizations. Security requirements can be easily mapped to authorization policies. Centralized policy management combined with automated provisioning ensures that security policies are uniformly enforced in all applications and services across the enterprise. Oracle Entitlements Server as an authorization service has been designed to meet stringent regulatory, business, and security requirements with minimal runtime overhead while allowing developers and administrators the ability to administer policies in a business-user friendly manner. As Oracle's strategic authorization engine, it is embedded within several Oracle products. It uses standards as a foundation to deliver highly available, scalable, externalized authorization management solution with a rich policy model for applications, middleware and databases. Oracle Entitlements Server helps organizations centrally manage entitlements, provides a central view of access rights across applications in the enterprise and generates audit records which can be used by reporting and analytics tools. It provides developers with shared services for fine-grained authorization to ensure quicker compliance and better business agility as policies can be quickly adapted based on market, security, regulatory and business requirement changes. Oracle Entitlements Server not only supports cutting edge industry standards and features, but it also brings over a decade of experience in building a robust authorization solution which can be relied on for securing critical applications and services.

Contact address:

Christian Patrascu
Oracle Corporation
Senior Manager – EMEA Oracle Fusion Middleware Product Management

Phone: +491775941037
Email CHRISTIAN.PATRASCU@ORACLE.COM