OASSF: 一个灵活的 Web 应用服务器安全框架*

陈华荣[1,2]，陈宁江[1,2]，樊会锋[1]

(1. 中国科学院 软件研究所 软件工程技术中心，北京 100080；2. 中国科学院 研究生院，北京 100039)

摘　要: 安全框架 OASSF 是在安全参考模型 OASSRM 的基础上提出来的一个分层结构的框架，它通过各种可配置的安全策略提供 WAS(Web 应用服务器) 的安全服务，为在 WAS 中集成和管理不同的安全机制提供了高度的灵活性和扩展性。该框架在中科院软件所自主研制的 OnceAS 应用服务器中得到了实现。

关键词: Web 应用服务器；J2EE；安全框架；安全模型

中图法分类号: TP393.08　　**文献标识码**: A　　**文章编号**: 1001-3695(2006)02-0089-03

Design and Implementation of Security Framework for Web Application Server

CHEN Hua-rong[1,2], CHEN Ning-jiang[1,2], FAN Hui-feng[1]

(1. Technology Center of Software Engineering, Institute of Software, Chinese Academy of Sciences, Beijing 100080, China; 2. Graduate School, Chinese Academy of Sciences, Beijing 100039, China)

Abstract: The Open Application Security Service Framework(OASSF) is layered based on the Open Application Server Security Reference Model(OASSRM). It provides security service through a variety of customized security policies, and it is fairly flexible and expandable for integrating different security mechanisms into OASSF. This framework is implemented in the application server OnceAS.

Key words: Web Application Server; J2EE; Security Framework; Security Model

在网络计算环境下的分布式应用会暴露给恶意者许多安全攻击点，因此，应用系统对作为底层支撑的 Web 应用服务器[1,2]所提供的安全能力有着非常重要的需求。目前主流的 Web 应用服务器建立在 J2EE 规范[3]的基础之上，J2EE 的安全需求主要包括服务器能够对接入的用户进行认证和授权、保障分布式环境下的敏感数据的完整性和保密性、组件间安全上下文的传递等。在 J2EE 的体系结构中，应用开发者负责开发组件来解决业务问题，Web 应用服务器负责为组件提供运行时的安全服务支持。

随着网络分布式应用需求的增长，Web 应用服务器正朝着可定制和可扩展的方向发展[2]，这要求应用服务器能够提供集成和管理多样化的安全技术，能够满足不同应用和运行环境的安全需求。目前主要的应用服务器产品在安全服务的可定制和配置能力上仍然不够充分，开放性不够。因此，本文主要研究了如何为 Web 应用服务器提供一个具有高度灵活性和扩展性的安全框架，在框架中方便地集成和配置所需的安全策略和机制，实现企业应用的安全需求。该工作基于中科院软件研究所研制的 OnceAS 应用服务器，并为后者的安全服务实现提供了良好的指导。

1　OASSRM 安全参考模型

J2EE 规范只规定了对应用服务器相关的安全需求和目标，但并未对安全实现提出具体的要求，这一方面给应用服务器提供商提供了很大的灵活性，可以提供自己的最有效的实现；另一方面也给应用服务器留下了一个问题，即如何提供一致的方式来集成和管理应用服务器中的各种安全技术。为了更好地设计和实现 Web 应用服务器的安全功能，借鉴安全参考模型的思想[5]定义了面向应用服务器的安全参考模型(Open Application Server Security Reference Model, OASSRM)。该模型规定了服务器安全服务的整体体系结构，通过定义不同的安全策略而获得安全功能的灵活性，为具体的实现提供指导作用。

OASSRM 是描述安全系统实施安全策略的地点和方式的一个模型，其中包含了各种具体的安全策略，通过对安全策略的组合与配置提供安全功能。其中，安全策略是指对某种类型的安全行为的操作描述，根据功能可分为认证策略、授权策略、审计策略等。

安全参考模型 OASSRM 如图 1 所示，它的核心在于以安全策略为中心的安全域(Security Realm)。一个安全域包含一个对象集合，这些对象的安全行为被授予特定于安全域配置的安全策略。安全域的关键在于各种安全策略的配置和管理，每个安全域拥有一个域管理器，用于管理和实施安全策略。每个安全策略提供统一的安全提供者接口和安全决策接口，以实现可替换的安全行为。每个安全域均拥有一个策略信息数据库，称之为 Registry，它用于保存用户名、密码及角色等安全信息，安全域管理器以及各种安全策略提供者利用这些信息进行安全校验。Registry 提供了一致的接口，为安全域内的各种安全提供者提供安全信息的存储抽象表示，用户可以使用文件、数据库、LDAP 服务器等多种方法来实现 Registry。

2　应用服务器的安全框架 OASSF

以 OASSRM 为指导给出了一个安全框架 OASSF(Open

收稿日期: 2005-03-03；修返日期: 2005-04-18

基金项目: 国家自然科学基金重点资助项目(60173023)；国家“863”计划资助项目(2003AA413010)；国家“973”计划资助项目(2002CB312005)

Application Server Security Framework),如图 2 所示。安全框架采用分层的结构,对外以接口的形式提供安全服务,对内集成不同的安全提供者所提供的安全机制。

OASSF 安全框架的主要组件如图 3 所示。

2.1 安全服务接口层(Security Service Interfaces)

安全服务接口层是安全服务层对外的接口,外部模块(如 EJB 容器)等通过这些接口调用安全服务。主要的接口如下:

(1) PrincipalAuthenticator 提供用户认证功能。

(2) RealmAccessController 提供存取权限控制功能。

(3) RealmInfo 提供当前安全域内的实体信息。

(4) RealmMapping 提供安全域间的映射功能,即把此域的安全信息转换为另一个域的安全信息。

(4) SecurityCollaborator 继承自上面四个接口,是对安全参考模型中安全域管理器的抽象,它的具体实现将提供所有父接口的安全功能。

2.2 安全服务层(Security Service)

安全服务层位于安全服务接口层和安全服务提供者接口层之间,一方面它对安全服务接口进行具体实现,提供外界所需的安全功能;另一方面它通过安全服务提供者接口使用安全提供者来完成相关的安全功能。其主要组件包括:

(1) SecurityCollaboratorImpl 类 安全协作者 SecurityCollaborator 的实现类,负责安全处理和调度任务。

(2) SecurityContext 类 用于封装安全上下文信息,如用户名、口令和证件等,上下文在客户端和服务器端、组件间传递。

(3) 安全域信息模块(SecurityRealmInfo) 管理安全域的具体配置信息等。

(4) SSL 模块(SSL) 为 EJB 容器提供 SSL 工厂类,以实现 EJB/Web 请求的机密性和完整性。

(5) 加密模块(Crypto) 为有关安全服务模块提供加密支持。

2.3 安全服务提供者接口层(Security Service Provider Interfaces, SSPI)

SSPI 是安全服务层和安全提供者层之间的一个契约,安全提供者层通过实现 SSPI 的接口集成到安全框架中,而安全服务层通过 SSPI 来调用安全提供者的实现。通过实现 SSPI,用户能够根据自己的需要定制实现具体的安全功能。

(1) 认证模块(LoginModule) 封装认证逻辑,执行认证任务,识别访问者是否为系统的合法实体。

(2) 授权策略(AccessDecision) 用于实施存取控制,判断访问者是否有权限对系统资源进行某项操作。

(3) 授权协调(Adjudicator) 用于对多个存取控制结果进行仲裁,决定是否允许该操作。

(4) 审计(AuditEvent) 用于记录访问者的行为,以便对访问者进行跟踪和安全审查。

(5) 映射(CredentialMapper) 用于进行安全信息在不同的安全域间的映射。

2.4 安全提供者层(Security Providers)

安全提供者层通过实现安全服务提供者接口提供具体的安全机制。OnceAS 通过使用 JAAS[6], JSSE, JCA 和 JCE 等标准软件包提供了一组安全提供者的缺省实现,它们能满足基本的安全需求。如果用户需要定制实现自己的安全策略,则通过实现 SSPI 来将定制的安全实现集成到框架中。

3 基于 OASSF 的 WAS 安全实现机制

3.1 OASSF 与应用服务器的集成

在 OnceAS 应用服务器中,所有的服务都可以通过 MService 的形式集成到服务器中[7]。MService 是 Web 应用服务器所有服务最基本的单位,它约定服务从创建、初始化、运行到停止整个过程所有的接口,描述一个服务自身的元信息。MService Server 是 Web 应用服务器所有基础服务的服务器,客户对基础服务的调用均由 MService Server 调度,并将处理结果返回给客户。如图 4 所示,OASSF 通过两个 MService 来实现与 OnceAS 应用服务器的集成,即 SecurityRealmMangagerMService 和 SecurityCollaboratorImpl。SecurityRealmMangagerMService 根据配置文件 Security-realm. xml 构造相应的安全域,并将它们绑定到名字服务器上;然后安全协作类 SecurityCollaboratorImpl 通过名字服务器找到相应的安全域,调用配置指定的安全提供者的实现来完成相关的安全功能。

3.2 EJB 容器的安全结构

应用 OASSF 在 OnceAS 应用服务器中为 EJB 容器、Web 容器、事务管理器、资源集成服务等模块提供了灵活的安全服务,下面以 EJB 容器的安全机制为例进行说明。EJB 容器[4]是 EJB 的运行环境,为 EJB 提供一组运行时服务,包括事务、持久性和安全等。根据 J2EE 规范,J2EE 容器提供两种类型的安全:声明性安全和程序性安全。程序性安全是指应用程序自身对安全行为作出决策,组件开发者通过调用 J2EE 规范所规定的 API 来完成程序性安全。声明性安全通过部署描述符进行安全需求描述,由容器读取部署描述文件中的各种元信息,并根据组装者提供的指令信息提供运行时刻的支持。在 OnceAS

中, 基于 OASSF 和 JAAS 所实现的 EJB 容器的安全结构如图 5 所示。

拦截器(Interceptor) 是广泛应用于分布式软件系统的一种设计模式[8], 它允许各种服务透明地加入到一个框架, 并且当特定的事件发生时能自动地被触发以完成特定的任务。SecurityHandler 是一个位于 EJB 容器中的 Interceptor, 被设置在 EJB 客户请求处理的路径上。在 EJB 的方法被调用前, SecurityHandler 将会被容器触发, 拦截 EJB 请求, 进行安全控制的操作。SecurityContext 是封装了安全上下文的对象, 用于在请求处理过程中传递安全信息。AccessDecision 负责具体的授权处理。LoginContext 是 JAAS 负责认证的类, 根据配置信息调用相应的 LoginModule 完成认证; LoginModule 负责通过访问 Registry(文件、LDAP 服务器或数据库) 来完成具体的认证工作, 其中包含具体的认证算法。XMLConfiguration 从 SecurityRealmManagerMService 获取 LoginContext 所需的配置信息。

EJB 容器的安全处理的典型流程如下:

(1) EJB 容器根据 EJB 部署描述文件(Deploy Descriptor) 中的安全信息(如对 EJB 的方法的访问控制) 来初始化 SecurityHandler 中的属性;

(2) 将客户调用传递进来的 SecurityContext 传给 SecurityHandler;

(3) SecurityHandler 从 SecurityContext 中取出安全信息, 如用户名、口令和证书等;

(4) SecurityHandler 调用 SecurityCollaboratorImpl 的认证函数, SecurityCollaboratorImpl 将会调用 LoginContext 进行认证, 若认证失败, 抛出 EJBException;

(5) 在 SecurityHandler 里, 如果调用者在部署描述文件里声明 run-as[4] 标志来进行安全代理, 转(6) , 否则转(7) ;

(6) SecurityHandler 从传递进来的 SecurityContext 中取出 run-as 的角色, 并判断该角色是否有权限进行相应的操作, 若没有, 抛出 EJBException, 否则转(8) ;

(7) SecurityHandler 调用 SecurityCollaboratorImpl 的授权函数, SecurityCollaboratorImpl 将会调用 AccessDecision 进行授权, 若失败, 抛出 EJBException, 否则转(8) ;

(8) EJB 容器继续 EJB 其他调用。

4　结论

对应用服务器中的安全支撑机制进行了研究。引入安全参考模型 OASSRM, 该模型的基础是以安全策略为中心的安全域, 并定义了一系列安全策略的职责和类型, 这些都为安全服务的设计和实现提供了指导和约束。根据安全服务参考模型和实际需求, 给出了一个安全服务框架 OASSF, 它通过层次型结构和一致的接口, 为各种安全技术集成进应用服务器提供一种具有高度灵活性和扩展性的解决方案。该框架已经在 OnceAS 应用服务器中得到了实现, 它通过各种可配置的安全策略很好地满足了企业应用的安全需求。

参考文献:

[1] 陈宁江, 金蓓弘, 范国闯. 多层企业应用的关键: J2EE 应用服务器[J] . 计算机科学, 2003, 30(1) : 149-153.

[2] 范国闯, 陈宁江, 钟华. Web 应用服务器: 新一代中间件[J] . 计算机科学, 2004, 31(1) : 1-4.

[3] Sun Microsystems Inc. Java 2 Platform Enterprise Edition Specification, version 1. 4[EB/OL] . http: //java. sun. com/j2ee/1. 4/download. html, 2001-07-27.

[4] Sun Microsystems Inc. Enterprise JavaBeans™ Specification, version 2. 1[EB/OL] . http: //java. sun. com/products/ejb/docs. html, 2001-08-14.

[5] OMG. CORBA Security Service Specification, version 1. 8[EB/OL] . http: //www. omg. org/technology/documents/formal/omg_security. htm#Security_Service, 2002-03.

[6] Sun Microsystems Inc. JAAS[EB/OL] . http: //java. sun. com/products/jaas, 2004-10.

[7] 林世彪. Webframe 应用服务器 EJB 容器关键技术研究与实现[D] . 北京: 中国科学院软件研究所, 2003. 17-22.

[8] D Schmidt, M Stal, H Rohnert, *et al*. Pattern-Oriented Software Architecture: Patterns for Concurrent and Networked Objects [M] . Wiley, 2000. 101-125.

作者简介:

陈华荣(1979-) , 男, 广东遂溪人, 硕士研究生, 主要研究方向为软件工程、网络分布式计算和系统安全; 陈宁江(1975-) , 男, 博士研究生, 主要研究方向为软件工程和网络分布计算; 樊会锋(1980-) , 男, 硕士研究生, 主要研究方向为软件工程和网络分布计算。

(上接第 80 页) 及跨企业的合作提供了良好的基础, 并将成为新一代 OA 的主要特征。

本系统具有开放、一致和方便使用的特点, 使企业中处于孤岛的信息能相互集成。它不仅适应分布式办公, 更以系统开放的环境为实现跨部门、跨企业的供应链的不同工作流程互操作打下了基础, 使客户、供应商或合作者都可以方便地参与企业的工作流程, 从而提高了工作效率。

参考文献:

[1] 微软公司. 微软开发平台研究[R] . 2001.

[2] Workflow Handbook[EB/OL] . http: //www. wfmc. org/.

[3] 张文增, 赵东斌, 孙振国, 等. ASP. NET——动态网页开发趋势[J] . 计算机工程, 2002, 28(3) : 7-9.

[4] 胡杰, 党延忠. 基于 Web 的工作流技术在办公信息系统中的应用[J] . 计算机应用研究, 2002, 19(9) : 117-119.

[5] 张涛, 战洪飞, 孙静, 等. 基于 Web 的企业工作流管理系统的研究[J] . 计算机应用研究, 2002, 19(5) : 130-133.

[6] 曾月, 范玉顺. 基于 COM 和 ASP 技术的工作流管理系统的设计与实现[J] . 计算机工程与应用, 2002, 38(1) : 241-244.

作者简介:

金正淑(1954-) , 女, 吉林人, 副教授, 主要研究方向为信息管理系统、软件工程; 闫文耀(1979-) , 女, 吉林人, 硕士研究生, 主要研究方向为信息管理系统、软件工程; 陈薇(1977-) , 女, 吉林人, 硕士研究生, 主要研究方向为嵌入式系统应用; 王学通(1977-) , 男, 河北人, 助教, 硕士, 主要研究方向为 Internet 及应用。