第 36 卷 第 4 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.4 Computer Engineering February 2010
·安全技术· 文章编号：1000—3428(2010)04—0110—02 文献标识码：A 中图分类号：TP393

基于 Ajax 的 J2EE 安全应用框架

许川佩，张 民，张 婧
(桂林电子科技大学电子工程学院，桂林 541004)

摘 要：针对基于 Ajax 的 J2EE 框架存在认证混乱、多重分散终端的安全问题，使用 Acegi 安全框架对其进行改进，实现权限访问控制，并成功应用到微波网管系统中。应用结果表明，改进框架具有很强通用性，能够满足企业级应用的各种安全需要，且提高了系统组件的可移植性。

关键词：Ajax 技术；J2EE 框架；安全

Ajax-based J2EE Security Application Framework

XU Chuan-pei, ZHANG Min, ZHANG Jing
(School of Electronic Engineering, Guilin University of Electronic Technology, Guilin 541004)

【Abstract】Aiming at the security problem of authentication chaos and multiple dispersion terminal of J2EE framework Ajax-based, this paper uses Acegi security framework to improve. Improved framework realizes accessing control right, and applies to microwave network management system. Application result shows that improved framework has well universal property, meets the variety of security needs in enterprise application, and increases portability of the system components.

【Key words】Ajax; J2EE framework; security

1 概述

Ajax 将请求与页面视图分离，解决了传统 Web 应用存在的众多缺点，使得 Web 应用的开发更加完善[1]。J2EE 架构是当前主流的架构之一，目前已有很多基于 Ajax 的 J2EE 框架，此类框架的出现使得 Ajax 开发变得越发简单，但此类框架存在安全验证、授权、存取控制和输入检查等安全问题。近年来，基于 Spring 应用的安全框架 Acegi，在入口级安全、数据域安全和系统级安全方面体现出显著的优越性[2]。

鉴于此，本文对基于 Ajax 的 J2EE 框架在安全性方面进行研究，利用 Acegi 框架对其改进，解决了安全问题，降低了对编程人员的要求和系统开发成本。

2 基于 Ajax 的 J2EE 框架

Ajax 是当前非常流行的 Web 开发技术，作为富互联网应用系统(Rich Internet Application, RIA)的一种实现技术，Ajax 可以改善用户体验，还可以简化 Web 开发，通过将页面高度模块化，数据与表现分离，使服务器端和客户端都可以很好地解耦，降低开发复杂度。J2EE 是当前主流 Web 框架之一，Ajax 技术与 J2EE 框架的结合可以使 Web 应用更加完善。基于 Ajax 的 J2EE 框架如图 1 所示。

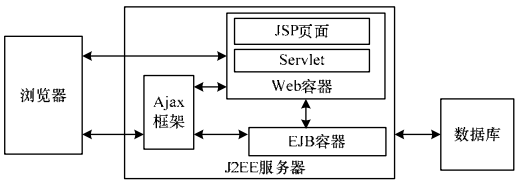

图 1 基于 Ajax 的 J2EE Web 框架

在 Web 应用领域，Ajax 本身并没有引入新的安全弱点。这些应用程序面临和经典 Web 应用程序同样的问题。但 Ajax 共同的最佳实现还没有发展起来，这就留下了安全漏洞。目前，Ajax 主要存在以下 3 个方面的安全问题[3]：

(1)多重分散的终端点以及调用隐藏。潜在的 Ajax 调用分散于整个浏览器页面，并且能够被各个事件分别调用，这样就导致了代码不规范。

(2)认证混乱。在很多情况下，Ajax 应用假定“另一方”(读取服务器端或者客户端代码)已经实现了认证，这种混乱导致了双方都没有实现适当的认证控制。

(3)动态脚本构成和执行。Ajax 通过调用定制的功能或者 eval 功能，随时更新 DOM 或者浏览器页面缓存的状态。未经认证的内容或者使用不安全的调用，轻则导致会话内容泄露，重则迫使浏览器执行恶意内容等严重后果。

Acegi 框架能够很好地解决上述问题。Acegi 为 J2EE 应用提供了完善的认证和授权服务，并提供一站式安全性解决方案。应用中的各种资源都在 Acegi 的保护范围之内，Acegi 具有以下特点[4]：(1)支持 J2EE 规范规定的各种认证策略，以及 Remenber-Me 认证服务、Web 容器层的匿名认证服务，并支持各种认证源。(2)可以有效地保护 Http 请求，即 Web 资源、业务层的业务方法和领域对象。(3)采用非侵入式架构，提供丰富的 JSP 标签库。其代码成熟稳定。

基于 Acegi 的特点，本文将该框架应用于基于 Ajax 的 J2EE 框架中，以达到提高应用安全性的目的。

3 基于 Ajax 的 J2EE 框架的改进

对 Ajax 应用程序而言，唯一的安全方式就是使用服务器

基金项目：广西科学研究技术开发计划基金资助项目(桂科攻 0537015-2)
作者简介：许川佩(1968－)，女，教授、博士，主研方向：自动测试与控制系统；张 民、张 婧，硕士研究生
收稿日期：2009-06-17 **E-mail：**zhangmin0215@gmail.com

端的 authC/authZ 验证和审核。当同时存在 Ajax 路径和普通 Web 应用路径时，若采用服务器端验证审核的方式，则不能对任何一种路径进行优先处理，仅能够在服务器端进行安全维护。但在 J2EE Web 应用中，有许多敏感资源是需要保护的，并不是任何访问者都能够操控被保护资源，尤其不能让恶意的访问者操控此类敏感资源，如 Web 资源、业务服务以及领域数据等。因此，本文提出基于 Ajax 的 J2EE 安全应用框架，框架中集成 Acegi 框架来解决原框架中存在的安全问题，集成后的框架如图 2 所示。

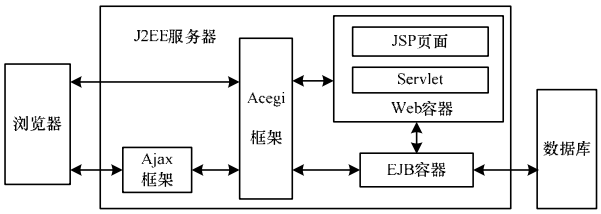

图 2　集成 Acegi 后的 J2EE 框架

在集成 Acegi 框架后，可以实现业务对象方法的安全访问控制粒度。它提供以下 3 个方面的应用程序的安全保护：

(1)URL 资源的访问控制。所有用户可以访问登录页面，而只有授权的用户可以访问其他页面。通过正则表达式或 Ant 风格的路径表达式定义 URL 模式，让授权用户访问某一 URL 匹配模式下的对应 URL 资源。

(2)业务类方法的访问控制。Spring 容器中所有 Bean 的方法都可以被 Acegi 管理，只有授权用户可以调用特定方法。

(3)领域对象的访问控制。业务类方法代表一个具体的业务操作，如更改、删除、审批等，业务类方法的访问控制解决了用户是否有调用某种操作的权限，但并未对操作的客体(领域对象)进行控制。

Acegi 通过多个不同用途的 Servlet 过滤器对资源进行保护，在请求受保护资源前，Acegi 的 Servlet 过滤器先判断用户是否有权访问目标资源，如果是授权者则开放访问，若未被授权者则将被禁止访问，在此基础上可以实施服务器端的服务器端访问控制安全策略。结合 Acegi 的特点，开发者可以在服务器端进行身份验证、授权、审计等工作。因此，本文改进的框架在解决应用系统安全方面具有以下特点：

(1)可以在服务器端提供身份验证，身份验证的强度是与初始身份和凭证类型(口令、令牌等)这些因素直接相关的，因此，强验证是服务器端基础架构的需要。

(2)在服务器上执行安全执行，解决了客户端对程序依赖性引出的安全问题，避免了开发者通过客户端执行非安全控制。

(3)有效地保护了系统中的各种资源，如 Web 页面、业务类方法以及领域对象。

(4)填补了客户端和服务器之间的间隙，引入 Acegi 能够缩短最终用户和面向服务构架接口之间的距离。

(5)使应用系统在实施安全策略时更容易进行测试工作，使用 Acegi 提供的辅助测试类，将更加容易开展应用系统的安全策略工作。

4　访问控制在 Acegi 框架上的实现

对于任何一个完整的应用系统，完善的认证和授权机制是必不可少的。Acegi 利用 Spring 提供的反转控制(Inversion of Control, IOC)和面向方面编程(Aspect Oriented Programming, AOP)机制实现安全控制，其认证策略由类似于 AOP 切面对象的过滤器驱动。在授权策略中，利用内置的 AOP 拦截器进行公平投票。系统通过配置和扩展 Acegi 框架实现安全需求功能。

采用角色访问控制(Role Based Access Control, RBAC)模型在 Acegi 框架上实现复杂的权限访问控制系统。为了建立一个良好的权限管理系统，必须首先规划好系统的数据库。RBAC 引入了角色的概念，使用户和权限分离，一个用户拥有多个角色，一个角色拥有多个相应的权限，从而减少了权限管理的复杂度，可以更加灵活地支持安全策略。同时引入资源的概念，一个资源对应多个权限[5]。

系统资源可分为 3 类：URL 资源，业务方法资源和网元对象资源。用户分为系统管理员、系统操作员和系统监视员。系统管理员对所有的资源具有增删改的权限；系统操作员只能在特定业务范围内拥有资源权限，对于超越自己业务权限范围的操作，系统予以拒绝；系统监视员只能查看系统状态，不能对任何资源进行操作。

Acegi 针对不同的安全处理，提供不同的过滤器。其提供的主要的过滤器有 httpSessionContextIntegrationFilter，根据 Session 中的存放信息，httpSessionContextIntegrationFilter 组装 ContextHolder(主要用于存放 SecureContext，包括用户的权限信息)，之后再由 authenticationProcessingFilter 处理认证请求，由 anonymousProcessingFilter 匿名用户处理，如果用户尚未登录，则将生成一个匿名用户的 Authentication 存放到 ContextHolder 中；securityEnforcementFilter 强制安全验证过滤器。验证所请求的 URL 以及执行的业务方法和领域对象是否在用户的权限范围内。因此，通过结合 RBAC 模型的数据库信息，对 Acegi 的过滤器进行相应的配置，实现系统的权限访问控制。由于该方法利用了 Acegi 非侵入式框架的特点，因此能够将业务无关的代码从业务代码中剥离，使业务代码更干净，从而提高了系统的通用性和可移植性。

5　结束语

本文研究了 J2EE 框架的安全性，针对 Ajax 技术在前端表现层具有突出优势，但在安全性方面存在缺陷的问题，提出基于 Ajax 技术的 J2EE 安全应用框架。该框架使用目前非常成熟的 J2EE 技术构建后台服务端，实现 Web 应用架构，在该框架的基础上，集成 Acegi 安全框架解决 Ajax 给应用系统带来的安全问题，提高了系统的安全性。该框架已经在 SDH/PDH 综合微波网络管理系统中得到验证，并在该框架上实现了 RBAC 权限访问控制系统。

实验结果证明，该框架在安全性方面得到了很大的改进，能够很好地保护基于 Ajax 的 J2EE 应用系统。

参考文献

[1] Garrett J J. Ajax: A New Approach to Web Applications[EB/OL]. (2005-02-18). http://www.adaptivepath.com/ideas/essays/archives/000385.php.

[2] 陈　雄. Acegi 安全框架[EB/OL]. (2007-02-05). http://tech.it168.com/j/2007-05-22/200705221448921.shtml.

[3] Shah S. Top 10 Ajax Security Holes and Driving Factors[EB/OL]. (2006-11-10). http://www.net-security.org/article.php?id=956&p=1.

[4] 罗时飞. 敏捷 Acegi, CAS——构建安全的 Java 系统[M]. 北京: 电子工业出版社, 2007.

[5] 高正宪, 李中学. Web环境下基于角色的访问控制策略及实现[J]. 计算机工程, 2004, 30(8): 133-135.

编辑　陆燕菲