第16卷 第5期
2006年5月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol.16 No.5
May 2006

# 基于XML安全技术的电子公文交换系统

颜 勇,胡华平
(国防科技大学 计算机学院,湖南 长沙 410073)

**摘 要**:在跨越企业边界的电子公文交换系统中,如何提高信息的安全性、开放性和互操作性是一个重要的研究课题。文中针对目前Internet/Intranet环境中跨系统边界交换数据存在的关键数据的传送与储存不安全、各系统身份验证不统一、安全技术标准不统一等问题,提出了一个基于XML安全技术的电子公文交换系统模型。该系统采用基于SAML的单点登录和认证授权,基于XACML的集成访问控制,以及基于XML加密和签名的关键数据加密保护。并在此基础上分析系统面临的威胁,提出可以应对的措施。

**关键词**:安全声明标记语言;可扩展访问控制标记语言;XML加密;XML签名;访问控制;单点登录
**中图分类号**:TP309 **文献标识码**:A **文章编号**:1673-629X(2006)05-0103-03

# Electronic Documents Exchange System Based on XML Security Technology

YAN Yong, HU Hua-ping
(School of Computer Science, National University of Defense Technology, Changsha 410073, China)

**Abstract**: It has become an important subject for how to improve the security, opening and inter-operation of the information in the enterprise-spanning electronic document exchanging system. This paper presents a model of the electronic document exchanging system based on XML security technology aimed at the problems about the unsafety of the transmission and the storage of the key information, the disunity identity validation, the unconformance security specifications in the Internet/Intranet among different applications. This system based on the SAML-based single sign-on and authorization, XACML-based integrated access control, and the protection of key information using the XML encryption and signatures, and provided a solution against the menace to system.

**Key words**: SAML; XACML; XML encryption; XML signature; access control; single sign-on

## 0 引 言

随着计算机与互联网应用的高速发展,越来越多的传统企业开始将手工的文件交换形式转变为更加高效、更加节省成本、更加方便快捷的网络交换方式,出现了诸如B2B,B2C等形式的电子商务和电子政务热潮。随着越来越多的企业、机构以及其合作伙伴、职员、客户的参与,电子数据交换的安全性、开放性与参与者系统间的互操作性就显得尤为重要。

传统的应用中各系统采用专有的认证系统,如口令验证、证书验证等,而需要跨多个应用系统的情况,就必须在访问相关的每个系统时进行多次身份认证,从而导致孤立的业务关系和用户体验。消除这种访问孤立的关键是建立联合身份,而安全声明标记语言(SAML)就为建立基于联合身份的无缝事务操作的实现提供了技术框架[1]。在通过统一身份认证后,用户可能需要对相关的多个系统中的资源进行访问,目前多数系统都是采用专有访问控制机制,相关信息保存在ACL(访问控制列表)中。不同的专有系统有不同的实现ACL的机制,难以交换和共享访问控制的信息。而扩展访问控制标记语言(XACML)作为一种适合于描述分布式系统访问控制规则的语言,可以提供一种可移植的、标准的方式来屏蔽各系统访问控制实现的差异,对上层提供统一的访问控制规则接口[2]。

SAML与XACML是紧密相关的。它们有很多相同的概念,要处理的问题域也在很大程度上重叠:验证、授权和访问控制。但是在同一问题域中,SAML要解决的是验证,并提供一种机制,在协同实体间传递验证和授权决策;而XACML则专注于传递这些授权决策的机制[3]。同时,后端XML格式的企业数据使用XML加密、XML签名技术保护,提供了在应用层多颗粒度的安全访问服务。

## 1 相关XML安全技术介绍

### 1.1 SAML

SAML(Security Assertions Markup Language,安全声

**收稿日期**:2005-08-26
**作者简介**:颜 勇(1978-),男,湖南人,硕士研究生,研究方向为网络与信息安全;胡华平,博士后,教授,博士生导师,研究方向为网络与信息安全、密码学。

明标记语言)是在 2002 年 11 月由结构化信息标准推进组织(Organization for the Advancement of Structured Information Standards,OASIS)提出的安全服务语言[4]。这是一种基于 XML 的安全性标准,继承了 XML 跨平台数据表述特性,用于在不同的安全性域中交换身份验证和授权凭证。它是一种描述语言,而不是一种认证或授权的技术,它定义了一个基于 XML 的用于安全信息交换的框架。SAML 的主要设计目的是为认证和授权服务提供标准的安全信息描述和共享机制,使得不同企业的安全系统间可以通过共享有关用户、交易等安全信息实现互操作。

### 1.2 XACML

XACML(eXtensible Access Control Markup Language 可扩展访问控制标记语言)是在 2003 年 2 月 OASIS 批准通过的标准描述语言[5]。XACML 定义了一种标准的用于保护资源的策略语言和一种访问决策语言,用于表示控制信息访问的规则和策略,这些规则和策略与整体访问控制和保密策略的上下文的目标资源有关。XACML 的目标是使策略管理和访问决策标准化。

### 1.3 XML 加密

W3C 和 IETF 制定了一项标准来对一个 XML 文档中的数据和部分内容进行加密[6]。如果一个文档只是某些敏感部分需要进行保护,就可以对其单独进行加密。对同一个文档中的不同部分用不同的密钥进行加密,就可以把同一个 XML 文件发给不同的接受者,而接受者只能看见和他相关的部分。

### 1.4 XML 签名

XML 签名和 XML 加密紧密相关。和安全认证签名相似,XML 也是用于确保 XML 文件内容没有被篡改。通过确保对数据完整性、可靠性和不可否认性的支持,XML 签名提供了在 XML 文档可信交换所需的关键功能。XML 签名能对 XML 文档的整体或文档中特定部分进行签名。XML 签名和 XML 加密结合在一起,可以确保数据发送和接收的一致性。

## 2 集成 XML 安全技术的电子公文交换系统的设计和实现

通过分析当前电子公文交换安全与实际应用需求,笔者基于以上所述的 XML 安全技术标准以及现有的一些安全技术,设计和实现了集成 XML 安全技术的电子公文交换系统(XML Security based Electronic Data Exchange System,XEDES)。该系统面向企业间电子数据的交换的过程,它包括 3 个部分:基于 SAML 的统一身份认证服务、基于 XACML 的集中访问控制系统、基于 XML 签名/加密的安全数据交换服务,以解决企业关键资源保护和集成跨企业边界的安全信息共享的问题。该系统建立在 SUN 公司的 JDK1.4 及其扩展和 SAML、XACML 等标准描述语言之上,具有跨平台、易扩展等特性,可为各种跨越企业边界的数据交换、电子商务应用提供安全服务。

### 2.1 XEDES 的总体设计

文中提出的安全电子公文交换系统是由统一身份认证服务与集中访问控制安全服务与安全数据交换服务三部分组成。其中统一身份认证服务由部署于逻辑独立的 XEDES 服务器中的认证服务与具体企业的应用服务器上的安全服务接口组成,提供跨越企业边界的认证授权服务;集中访问控制安全服务由 XEDES 服务器端和分布在具体的企业应用服务器中的安全服务接口组成,提供跨企业边界的对不同企业关键资源的集中访问控制;安全数据交换服务部署在具体的企业应用服务器端,通过对企业关键资源的 XML 签名/加密封装,为企业关键资源的储存与传输提供保护。具体见图 1。

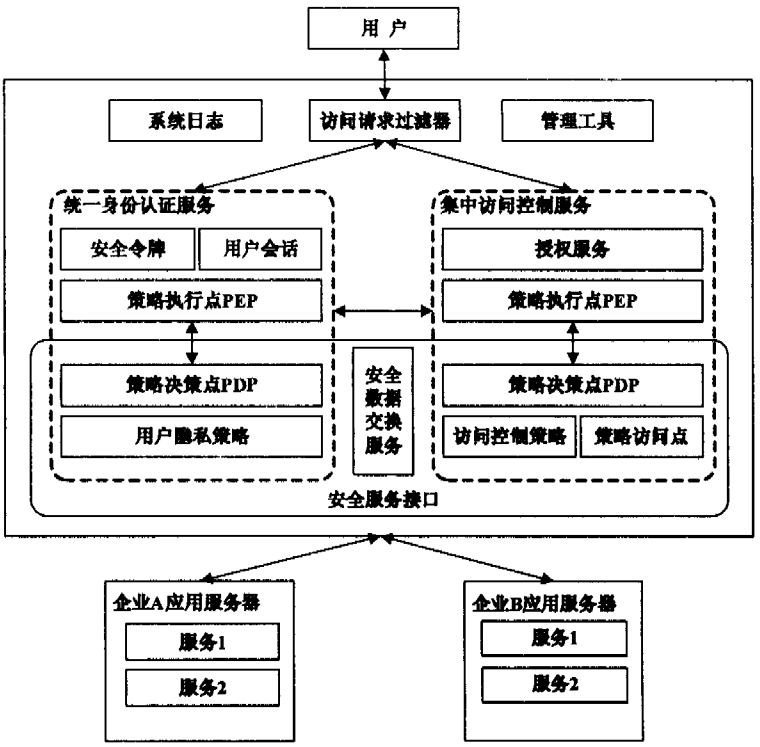


图 1 XEDES 的组成与体系结构

### 2.2 XEDES 的设计与实现

#### 2.2.1 访问请求过滤器

该模块用于截取用户的访问请求,从中析取相关的用户信息,如用户的身份、所请求的资源、所希望的操作等,并根据不同的请求类型将请求转发给相应的功能模块进行处理,如果是登录系统的请求,过滤器将激活身份认证模块,对用户身份进行验证;如果是对特定资源的访问请求,系统将激活集中访问控制模块,根据用户身份、所请求的资源和进行的动作进行分析,并判断是否有权限进行这次访问。

#### 2.2.2 统一身份认证服务

统一身份认证服务提供单点登录功能(SSO),对不同企业用户进行统一的身份认证服务,使用户在访问不同企

业资源时无需在每个企业进行登录。它包含以下部分:

1)安全令牌服务:该服务接受用户的验证请求,将用户提交的验证信息发送给具体企业应用系统中的安全服务接口进行验证,并为成功登录的用户生成安全令牌;该服务还对来自系统其它模块的对安全令牌的验证请求进行验证,并返回相关的安全声明。

2)用户会话服务:该服务在用户登录验证后开始保存该用户的身份信息(安全令牌),使用户在不同应用系统自由访问时,能够根据会话保存的安全信息对用户身份验证提供高效率的认证服务,直到用户退出或者访问超时的时候,用户会话服务将释放该用户的身份信息。

3)策略执行点PEP:策略执行点接收到用户验证请求,将请求封包成SAML请求并发送到策略决策点PDP,它对请求进行评估,返回一个SAML断言,PEP根据该SAML断言对用户的请求进行响应。

4)策略决策点PDP:将请求中的用户名/密码、证书等形式的登录验证信息传递到企业应用服务中相关服务进行处理,得到并根据返回结果构造相应的SAML断言返回到PEP。

5)用户隐私策略:对企业应用系统中的用户信息进行过滤,屏蔽或者加密用户敏感的信息,保证用户敏感信息的安全性。

2.2.3　集中访问控制服务

1)授权服务:该服务接受用户对特定资源进行访问和操作的请求,并根据附带的安全令牌,调用统一身份验证服务进行身份验证,如果得到合法的SAML断言,该服务将这次请求传递给策略执行点;如果得到的是非法的SAML断言,该服务将拒绝用户的访问请求。

2)策略执行点PEP:策略执行点接受到用户访问特定资源的请求,将该请求封包成SAML请求并发送到策略决策点PDP,它对请求进行评估,返回一个SAML授权决策断言,PEP根据该SAML断言对用户的请求进行相应的响应。

3)策略决策点PDP:PDP评估请求中的相关策略和规则后会作出决策。可以应用的策略有多种,PDP并没有评估所有的策略,而是根据策略目标选择相关的策略进行评估。策略目标包括关于主体、动作和其他环境属性的信息。

4)决策访问点PAP:决策访问点提供访问策略和维护策略的服务。为策略决策点提供访问策略库的服务,并为企业应用提供维护策略库的接口。

5)访问控制策略:访问控制策略包括目标、规则、规则组合算法和义务几种组件,为PDP做出授权决策提供依据。本系统中策略扩展到企业应用服务中,即具体的策略的定义由企业应用来执行,能灵活地适应各系统中对访问控制的需求。

2.2.4　安全数据交换服务

XEDES中,服务端与企业应用服务器中的安全服务接口之间的消息传递格式主要以SAML和XACML这种描述语言为主,而访问的资源也以XML格式进行传送,因此要对这些数据进行有效的保护,防止窃听、篡改等恶意攻击。安全数据交换服务能够提供对基于XML标准格式的文档进行数字签名和按多颗粒度进行加密的服务,加强了消息的有效性和准确性。

2.2.5　系统日志

记录系统中用户登录与访问资源的历史信息。

2.2.6　管理控制台

通过管理控制台,用户可以管理和配置系统相关的设置项。

## 3　结束语

文中在研究XML安全技术的基础上,针对跨企业应用边界的电子公文交换的安全性需求,提出了一种基于XML安全技术的电子公文交换系统,以期为Intranet/Internet中跨企业应用边界的关键数据的交换提供统一的身份认证与访问控制服务。与现有的其他系统相比,本系统具有如下特点:

a.采用了统一的基于SAML的安全数据描述、服务访问接口定义、安全上下文传递,为跨企业应用提供一个安全的上下文环境;

b.采用了基于XACML的访问控制策略定义、集中访问控制服务,为对具有不同操作语义的企业应用中的资源的访问提供了一种统一的语言基础;

c.对企业间传递的关键数据采用基于XML加密和数字签名的不同颗粒度的数据保护,为不同层面的需求提供不同的安全的数据视图。

在今后的工作中,一方面,笔者将对基于XML安全技术的电子公文交换系统中可能存在的安全问题及解决方法进行研究;另一方面,将继续对SAML/XACML/XML加密签名等规范进行研究,并结合实际的应用,对以上规范进行合理的扩展,以期更好地满足跨企业电子公文交换的安全性需求。

**参考文献:**

[1] Ramachandran J. 设计安全的体系结构[M]. 胡　骏,詹文军译. 北京:机械工业出版社,2003.

[2] Gilbraith B, Hankison W. Web服务安全性高级编程[M]. 吴旭超,王　黎译. 北京:清华大学出版社,2003.

[3] Verma M. XML Security: Control information access with XACML[Z]. IBM developer Works, 2004.

[4] Verma M. XML Security: Ensure portable trust with SAML[Z]. IBM developer Works, 2004.

[5] Dournaee B. XML安全基础[M]. 周永彬,贺也平,刘　娟译. 北京:清华大学出版社,2003.

[6] Atreya M. 数字签名[M]. 贺　军译. 北京:清华大学出版社,2003.