基于SAML的跨域单点登录的设计与实现

焦亚楠,胡春枝
(天津大学 计算机学院,天津 300072)

摘 要:随着网络技术的飞速发展,基于网络平台的应用系统逐渐进入各行各业中,带来巨大收益的同时对安全性提出了更高的要求,需要保证访问其资源的用户具有合法的权限。为了适应多系统平台的发展要求,实现对登录平台的用户信息进行统一认证和管理,文中设计了一个跨域的单点登录系统(CD-SSO),它采用SAML断言作为安全信息定义的标准化格式,通过SOAP消息传递安全元素,利用WS-Security来保障消息的完整性和机密性。它在方便用户访问的同时提供了完善的安全服务机制,可以保证消息和服务的保密性、完整性和有效性。

关键词:消息传输;联合认证;跨域单点登录
中图分类号:TP399 **文献标识码**:A **文章编号**:1673-629X(2012)01-0157-04

Design and Implementation of CD-SSO Based on SAML

JIAO Ya-nan,HU Chun-zhi
(School of Computer Science and Technology,Tianjin University,Tianjin 300072,China)

Abstract:Because of the network's openness,systems in the Multisystem Platform (MP) call for a higher security. To solve this problem and provide the users of MP with unified and secure access to resources,it designs a cross-domain single sign-on system (CD-SSO), with which the users do not need to authenticate identity repeatedly during a multi-service process. It uses SAML assertions as standardized format for security information and sends security element through SOAP message and uses WS-Security to protect message integrity and confidentiality. It can guarantee the security while helping users visit.

Key words:message delivery;unite authentication;CD-SSO

0 引 言

随着网络信息技术的广泛应用,基于.NET架构的信息系统越来越多地融入到各行各业中。目前在警务系统的多系统平台的应用环境中,存在着很多的应用系统,如考核系统、督察系统、刑侦管理系统、治安管理系统、户政管理系统、警员身份认证系统等。随着警务工作的不断深入,新的应用系统会大量涌出,每个应用系统一般都要求实现身份认证、用户权限、访问控制等功能,所有新应用系统大量的涌出,在与已有系统的集成和融合上,会带来很多问题。传统的单一身份验证系统已经不能适应该平台的发展,无法实现各个应用系统之间的统一管理、统一认证。因此,为了顺应时代的发展,开发跨域单点登录系统已成为督考平台工作发展的重中之重。

跨域单点登录的主要实现目标是对登录多系统平台的用户信息的统一管理,使用户访问诸多系统只需要登录认证一次,并保证用户信息和用户系统的安全性。跨域单点登录的机制是实现"一次登录,全网漫游,单点注销,全网失效"。

收稿日期:2011-05-27;**修回日期**:2011-09-04
基金项目:天津市科技支撑计划重点项目(10ZCGYSF01300)
作者简介:焦亚楠(1986-),女,硕士研究生,研究方向为计算机应用技术;导师:许林英,副教授,主要从事计算机数据库方向和网络方向的教学与研究。

1 相关技术研究

1.1 SAML

SAML[1](Security Assertion Markup Language,安全断言标记语言)基于XML[2]框架,用来交换安全信息,这些安全信息通过主体断言形式描述。断言包含的信息可以是主体以前的身份验证行为、主体的属性信息或者关于主体可以访问某种资源的授权决策信息,在一个断言中可以包括多种类型的信息。提出SAML的一个重要目的是为了解决跨域单点登录问题,即用户在一个域登录后访问其他域时,不需要重新登录。

SAML语言与WS-Security规范都是为了解决XML安全性或Web Services安全性的问题,因此容易混淆它们的区别。SAML语言是为了在通信多方之间传递认证与授权等安全信息的基于XML的框架语言,其目的是用XML的格式表示安全断言。而WS-Secu-

rity 规范的目的则是解决如何将安全信息嵌入到 SOAP 消息中,保证 SOAP 消息的完整性与机密性。

1.2 CD-SSO

CD-SSO(Cross Domain-Single Sign On,跨域单点登录)是通过用户的一次性鉴别登录,可以获取需要访问系统和应用软件权限的技术,其实质就是安全上下文或者凭证在多个应用系统之间传递和共享信息。主要包括三个角色,用户,多个应用系统和认证中心。

CD-SSO 具有以下优点[3,4]:

(1)对应每个用户的权限与特权,仅有一个授权列表。

(2) 用户不至于再陷入多次登录的麻烦,也不用再为访问网络资源要记住多个密码。

(3) 所有可用的 SSO 方法均提供了安全身份验证,并提供了对用户与网络资源的会话进行加密的基础。

2 CD-SSO 模型设计

文中采用一种改进的基于 SAML 的 CD-SSO 模型[5~7]图与处理流程如图 1 所示。

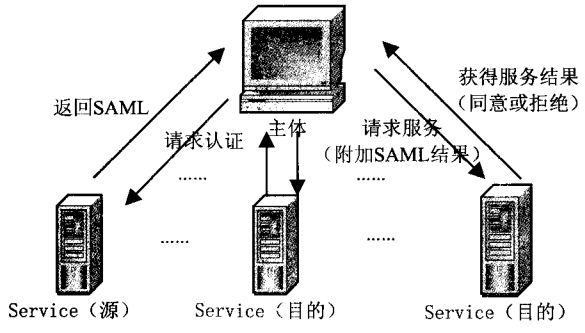

图 1 CD-SSO 模型图

3 详细设计

文中将跨域单点登录划分为消息传输、信任服务、联合认证三个模块,下面对各模块进行详细设计。

3.1 消息传输的实现方式

消息传输模块的主要功能是将 SAML 令牌生成的 SOAP 消息传送给其它模块,采用"二次验证"[8]实现,保证消息在传输过程中的安全性及其对应用系统的安全访问。服务端通过确认收到的口令认证信息的有效性,来决定是否接受客户端的请求,如果确认是有效的,则服务端允许用户对服务端的资源进行访问,否则拒绝,并将结果回送给客户端。

3.2 信任服务的解决方案

文中使用的是基于证书的信任服务检验策略,并且对传输消息在加密前进行数字签名,指定相应的证书。需要在<extensions>指定使用策略断言的策略集,在<policy>中设置相应的策略,并在<serviceToken>指定总部服务器的含有密钥的证书。片段代码示例如下:

```
<policy name="ManagerPolicy">
< usernameForCertificateSecurity establishSecurity-
Context="true" renewExpiredSecurityContext="true"
requireSignatureConfirmation="false" messageProtection-
Order="SignBeforeEncrypt" requireDerivedKeys="true"
ttlInSeconds="300">
<serviceToken>
<x509 storeLocation="CurrentUser" storeName="
My" findValue="CN=MyServiceCert" findType="Find-
BySubjectDistinguishedName" />
</serviceToken>
<protection>
<request signatureOptions="IncludeAddressing, In-
cludeTimestamp, IncludeSoapBody" encryptBody="true"
/>
< response signatureOptions="IncludeAddressing,
IncludeTimestamp, IncludeSoapBody" encryptBody="
true" />
</protection>
</usernameForCertificateSecurity>
</policy>
```

3.3 认证中心的实现方法

联合认证模块是跨域单点登录的核心,主要行使认证域管理、协同认证域完成用户认证功能。本模块实现为 ASP.NET 应用程序,主要由查询验证和访问验证两大部分组成。

3.3.1 查询验证

该模块接收所有用户的请求,然后检查请求和会话,判断用户请求的类型,主要分为以下几种情况:

(1) 用户提交用户名称和密码,请求登录系统;直接转入登录验证模块处理;

(2) 用户已经登录,请求退出系统;保存用户登录的相关信息,转入登录验证模块进行退出,用户可以通过直接关闭浏览器进行退出;

(3)用户已经登录,请求访问某个 Web 应用系统;直接转入访问验证模块进行处理;

(4) 用户首次访问系统,请求中没有任何访问信息;不作任何处理,直接转入登录验证模块;

(5)用户首次访问系统,但是请求中带有跨域访问的记录信息;先保存跨域访问的记录信息,然后转入验证模块进行重新验证。

3.3.2 访问验证

该模块提供已登录用户访问 Web 应用系统的入

口。对于从登录验证模块转发来的请求,首先从数据库中取出用户可以访问的 Web 应用系统的信息,并将其与用户请求一起传递给相应的 Web 窗体,由 Web 窗体生成 Web 应用系统列表并返回给用户。对于访问 Web 应用系统的用户请求(由程序查询模块转发),访问验证模块调用 SAML 断言管理模块的方法为本次访问生成断言,并把该断言加入到请求中,然后按照保存的 IP 地址或域名地址将请求转发给相应的 Web 应用系统。

3.3.3　所用到的接口及说明

(1) Identity 类:封装了各个应用系统最基本的登陆信息,包括用户名(username)、密码(password)等认证信息,认证域中的属性(domain)将这个认证信息映射到应用系统相应的认证模块。同时,在 Identity 中还包含了一个统一认证的标识号(unifiedld),用来将各个应用系统的身份认证信息关联在一起。

(2) 接口 IdentityManager,负责管理各种认证信息和统一标识号之间的关联。

(3) 接口 AuthHandler,负责执行认证的动作。

根据以上提供的接口[9],在进行不同的认证服务需求时,提供相应的实现类即可。

3.3.4　安全模型的实现

文中设计消息安全处理模块[10]主要由加密、解密、签名、签名验证、添加标识符和消息有效性验证这几个子模块组成。

对于安全处理的顺序,由于标识符信息也是需要保护的安全信息,因此必须在进行安全处理之前将标识符信息附加到原始 XML 信息上。文中设定对将要发送的消息处理顺序为先添加标识符信息,然后进行数字签名,最后再加密。

此消息安全处理模块可同时部署在 Web 服务的客户端和服务端,提供独立于平台和底层传输机制的端到端的安全。

中心安全服务端主要由如下几个部分组成:请求解析器、属性查询和 SAML 响应生成器,如图 2 所示:

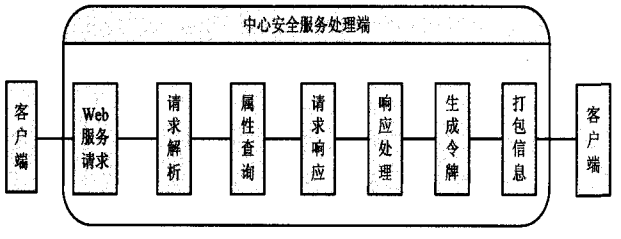

图 2　中心安全服务端结构图

运行流程为:

(1) Web 服务器接收到客户端传来的 SAML 请求,将其传送至中心服务端;

(2)中心服务端将该请求转换成包含 SAML 请求的 XML 对象,调用消息安全处理模块,通过使用中心与用户协商的密钥库进行解密和签名验证处理,验证用户的身份,以及请求消息的保密性和完整性。经过安全处理后,得到还原后的 SAML 请求的 XML,并将该 XML 转换成 SAML Request 对象;

(3)调用 SAML 请求解析器,从 SAML Request 对象中提取用户名和属性;

(4)调用属性查询模块,根据用户名和属性名到用户信息库中查找并提取该用户的相关属性值;

(5)调用 SAML 响应生成器,以用户的主体对象和属性信息为参数生成 SAML Response 对象;

(6)中心服务端将 SAML Response 对象转换成 SAML 响应的 XML,接着调用消息安全处理模块,形成安全的 SAML 令牌;

(7)调用传输模块将安全处理的 XML 信息打包成 SOAP 消息发送至客户端。

3.3.5　CD-SSO 的应用

将上述设计的 CD-SSO 应用于多系统平台中,用户只需要登录一次就可以使用平台中的多个系统。系统运行流程为:

(1)用户第一次使用该平台时调用 CD-SSO 客户端程序,输入用户名称和口令,根据用户输入的信息生成 SAML 请求;然后客户端调用安全传输模块将此请求信息打包成 SOAP[11]消息发送至中心安全服务端,并等待中心安全服务端的应答。

(2)中心安全服务端监听和接收客户端发来的 SAML 请求消息,并将该消息传递给安全处理模块,对消息进行处理,采用数字签名的验证,确认该 SAML 请求是否来自合法用户。

(3) 安全处理模块验证用户合法后,将 SAML 请求响应通过传输模块返回客户端,客户端等待接收该信息。同时客户端通过授权模块,对用户进行权限查询,用以判断用户是否有权访问他所请求的 Web 服务。

(4) 根据授权结果,为用户进行 Web 服务调用,并将调用结果返回客户端。即完成了一次单点登录调用 Web 服务的全过程。此时,如果用户还需要调用其它域中的 Web 服务,该用户只需要持有安全的 SAML 请求响应访问该站点,之后的步骤与上面所描述的完全一致,无需用户再次执行登录并进行判断操作。

根据上面描述的运行流程,CD-SSO 划分为 4 个主要模块。各接口功能如下:

(1) SAML RM(SAML Request Manager)对客户端传入的用户名称和密码解密,这里采用的解密方法是非对称加密解密法,同时随用户名称和密码一起传入客户端产生的非对称密钥,用得到的非对称密钥进行

解密,确保传入信息的完整性。如果用户通过验证,则 SAML RM 创建并生成 SAML 请求,同时将 SAML 请求发送给 SAML MM。

(2) SAML MM (SAML Message Manager) 捕获 SAML Request Manager 创建并生成的 SAML 请求,查找对应有效的 SAML 令牌[12],通过系列处理,生成 SOAP 消息,传送给 SAML Check Manager 等待验证。

(3) SAML CM (SAML Check Manager) 接收 SAML MM 发送的 SOAP 消息,通过验证处理,生成相应的 SAML 验证结果;将 SAML 验证结果发送给 SAML 消息传输模块,等待返回客户端。

(4) MT (Message Transport) 等待接收从 SAML CM 传来的 SAML 结果,并将其转发给客户端,即完成一次单点登录的过程。

4 结束语

文中结合网络平台的发展需求,提出了一种基于 SAML 的跨域单点登录系统,主要针对浏览器访问 Web 服务的方式,采用 SAML 断言作为安全信息定义的标准化格式,通过 SOAP 消息传递安全元素,利用 WS-Security 来保障消息的完整性和机密性。

通过 CD-SSO,多系统的用户在进行一个涉及多个服务的业务流程时不需要反复认证身份,而是只要验证一次身份就可以完成业务流程;该单点登录系统能够抵御常见的网络攻击,在方便用户使用的同时没有降低原有系统的安全性;对于平台的系统管理员,该机制易于配置和管理。

参考文献:

[1] Lutz D J, Stiller B. Combining identity federation with payment: the SAML-based payment protocol[C]//2010 IEEE/IFIP Network Operations and Management Symposium-NOMS 2010. [s. l.]: [s. n.], 2010: 495-502.

[2] Hughes J, Maler E. Technical Overview of the OASIS Security Assertion Markup Language (SAML) Committee Draft[M]. [s. l.]. National Security Institute, IEEE, 2003.

[3] Ha M, Kim Joong-Ho, Oh D, et al. A study of reduced-terminal models for system-level SSO noise analysis[C]//2010 IEEE 19th Conference on Electrical Performance of Electronic Packaging and Systems. [s. l.]: [s. n.], 2011: 49-52.

[4] 沈 杰,朱程荣. 基于 Yale—CAS 的单点登录的设计与实现[J]. 计算机技术与发展,2007,17(12):144-146.

[5] Wu Kaixing, Yu Xiaolin. A model of unite-authentication single sign-on based on SAML underlying web source[C]// 2009 2nd International Conference on Information and Computing Science. [s. l.]: [s. n.], 2009: 211-213.

[6] Chen Tianyu, Xie Dongqing, Yang Xiaohong, et al. Research and implementation of security SSO authentication model based on SAML and XKMS[J]. Application Research of Computers, 2010, 27(3): 1019-1021.

[7] 黄 滨,周德俭,卫传征. 基于 SAML 的新型单点登陆模型研究[J]. 计算机技术与发展,2008,18(9):219-221.

[8] 马一杰. 电子阅览室管理系统的设计与实现[D]. 天津:天津大学,2009.

[9] 李幼红,梁京章. 基于 J2EE 平台的单点登录模块的设计[J]. 计算机技术与发展,2006,16(5):232-233.

[10] Kormann D P, Rubin A D. Risks of the Passport Single Sign on Protocol[J]. Computer Networks, 2009, 33(6): 51-58.

[11] 耿丽丽,余雪丽. 基于 SOAP 的通信协议本体建模[J]. 计算机技术与发展,2010,20(8):64-65.

[12] Liu Weiyi, Tan Yue, Zhang Enwei. Service token for identity access management[C]//Services Computing Conference, 2009. [s. l.]: IEEE Asia-Pacific, 2009.

(上接第 142 页)

参考文献:

[1] 印 鉴,陈忆群. 搜索引擎研究与发展[J]. 计算机工程,2005,31(14):54-56.

[2] 李振龙. Web 信息检索的技术分析与发展策略研究[J]. 计算机科学,2006,33(4):181-184.

[3] Hatcher E, Gospodnetic O. Lucene in Action[M]. [s. l.]: Manning Publications Co., 2005.

[4] 郑榕增,林世平. 基于 Lucene 的中文倒排索引技术的研究[J]. 计算机技术与发展,2010,20(3):80-83.

[5] Salton G, Wong A. On the specification of term value in automatic indexing[J]. Journal of Documentation, 1973, 29(4): 35-40.

[6] 李永春,丁华福. Lucene 的全文检索的研究与应用[J]. 计算机技术与发展,2010,20(2):12-15.

[7] 林碧英,赵 锐,陈良臣. 基于 Lucene 的全文检索引擎研究与应用[J]. 计算机技术与发展,2007,17(5):184-186.

[8] 张讯涞. 搜索引擎的设计剖析[J]. 计算机工程与科学,2002,24(4):18-20.

[9] 赵恒永,沈 坚,山 岚. 基于专业信息深度挖掘的搜索引擎 Spider 的设计与实现[J]. 计算机工程与科学,2009,31(6):18-20.

[10] 郎小伟,王申康. 基于 Lucene 的全文检索系统研究与开发[J]. 计算机科学,2008,35(6):152-154.

[11] Brin S, Page L. The Anatomy of a Large-Scale Hypertextual Web Search Engine[D]. Stanford: Computer Science Department, Stanford University, 2000.

[12] Hammer J, Fiedler J. Using Mobile Crawlers to Search the Web Efficiently[J]. International Journal of Computer and Information Science, 2000, 1(1): 36-58.