基于 SAML 的真单点登录框架①

陆志刚[1,2,3], 王 杰[2,3], 魏 峻[2]

[1](苏州工业园区国有资产控股发展有限公司, 苏州 215028)
[2](中国科学院软件研究所 软件工程技术研究开发中心, 北京 100190)
[3](中国科学院大学, 北京 100190)

摘 要: 随着企业信息化进程的推进, 企业业务系统不断地增加. 陆续加入的业务系统往往采用不同实现技术和安全策略, 并且各自维护独立的认证授权体系, 这样很容易形成“信息孤岛”. 为消除这种系统访问控制孤立, 基于统一认证的单点登录 (SingleSignOn)系统应运而生. 然而, 现有的单点登录模型在安全性、扩展性、可维护性等方面都存在诸多不足. 本文基于安全断言标记语言 SAML, 设计了一个安全性高、互操作性好、松耦合的的统一认证单点登录框架, 主要包括身份提供者过滤器和服务提供者过滤器模块、单点登录交互协议和安全保障机制.

关键词: 安全断言标记语言 SAML; 单点登录; 统一认证; 断言

SAML-Based Single Sign on Framework

LU Zhi-Gang[1,2,3], WANG Jie[2,3], WEI Jun[2]

[1](SIP State Property Holding Co. Ltd., Suzhou 215028, China)
[2](Technology Center of Software Engineering, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)
[3](University of Chinese Academy of Sciences, Beijing 100190, China)

Abstract: With the development of enterprise informationization, the enterprise business system continually increases. The added business systems often use different technologies and security policies, and maintain separate authentication and authorization system, thus it is easy to form “islands of information”. Unified authentication based single sign on technique emerges at the right moment for eliminating such isolating access control. However, there are some disadvantages on the security, scalability and maintainability of existing single sign-on models. In this paper, based on the Security Assertion Markup Language(SAML), a unified authentication single sign-on framework with high security, interoperability, and loosely coupling is designed and implemented, which includes the identity providers filter (SSO-IDP) and service providers filter (SSO-SP) modules, single sign-on interaction protocol and security mechanisms.

Key words: security assertion markup language; single sign on; unified authentication; assertion

1 引言

随着企业信息化进程的推进和电子商务的蓬勃发展, 企业业务系统的数量在不断地增加, 企业内各业务系统之间的相关性甚至企业间业务系统的关联性越来越大. 然而企业信息化是一个循序渐进的过程, 陆续加入的业务系统往往是采用不同的技术、不同的安全策略, 各自维护着独立的认证授权体系, 形成“信息孤岛”. 对用户而言, 如果每天需要登录到许多不同的应用服务, 每个系统采用不同的安全策略, 如用户名、口令, 这样在使用上有着很大的不变, 而且通行词被非法截获和破坏的可能性也增加, 安全性不高. 如果用户忘记了某个网站的用户名或密码, 无法登录, 就需要通过某种方式找回密码, 造成了系统管理和安全管理的开销, 降低了效率.

① 基金项目:国家自然科学基金(61173005);国家科技支撑计划(2013BAH05F03)
收稿时间:2015-05-06;收到修改稿时间:2015-07-06

为解决这些问题, 基于统一身份认证的单点登录(SingleSignOn)系统应运而生. 单点登录是指访问同一服务器不同应用中的受保护资源的同一用户, 只需要登录一次, 即通过一个应用中的安全验证后, 再访问其他应用中的受保护资源时, 不再需要重新登录验证.

现有很多的单点登录模型在安全性、扩展性、可维护性等方面都有很多不足, 制约着企业信息化的发展. 当前单点登录的主流发展方向是基于安全断言标记语言(Seeurity Assertion Markup Language, SAML)的单点登录模型, 本文给出了一种结构松耦合可扩展、组件易插拔和互操作好、系统安全的统一认证单点登录框架的设计与实现.

2 相关技术

2.1 统一认证模式的单点登录

为与“伪”单点登录(为解决遗留系统问题, 而采用自动模拟表单登录的方式达到单点登录)区分开, 我们采用统一认证的单点登录方式. 在统一认证单点登录系统中, 应用系统与认证中心建立信息关系, 若认证中心认为用户具有合法身份, 那么应用系统就相信认证中心的“判断”, 承认该用户具有合法身份. 在这种机制中, 一旦用户在单点登录组件上登录成功, 以后再访问该单点登录框架中集成的任何应用时, 就不需要进行显示或隐式的登录操作. 也就是说, 对应用系统而言, 以前发生在其上的认证过程不再发生了, 在会话有效期结束前, 只需登录一次.

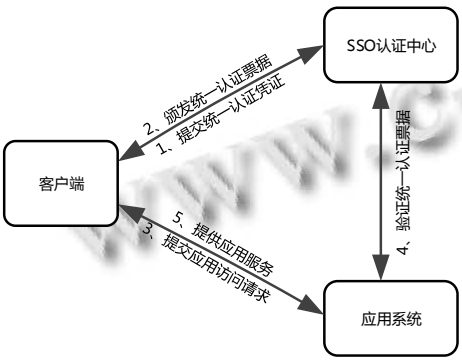

图 1 基于统一认证的单点登录

统一认证单点登录如图 1 所示, 其执行过程如下:

1)在用户使用单点登录组件之前, 管理员需要向单点登录组件注册所有应用系统的相关信息; 用户向认证中心提供认证凭证, 证明其合法身份;

2)若用户通过主认证, 单点登录组件将根据相关规则为其生成一个用于联系该用户和被请求应用的票据, 并将该票据发送给用户;

3)当用户申请登录某个应用程序时, 票据将随着用户的请求一起转发至应用程序;

4)应用系统收到带有票据的用户请求之后, 为了验证票据是否有效, 将利用票据与单点登录组件进行一次交互, 单点登录组件进行验证之后再向应用返回肯定或否定的答案.

5)应用根据票据验证结果决定是否向用户返回资源.

统一认证单点登录过程, 类似第三方认证过程. 这种解决方案的优点是: 用户信息维护成本较低; 用户认证信息的安全性较高; 可以实现如单点登出, 用户集中管理等其他功能.

2.2 安全断言标记语言 SAML

安全断言标记语言(SAML)[1]是一个基于 XML 的协议, 用于交换关于主体的安全断言信息. 主体[1]是指拥有某安全领域的身份信息的实体. 在 SAML 体系中还包括服务提供者和身份提供者. 身份提供者(IDP)[1]是为一个主体产生断言的系统或管理域, 通常也被称为 SAML 权威或断言方[1]. 服务提供者(SP)[1]是依赖身份提供者发出的断言的系统或管理域, 通常也被称为信任方.

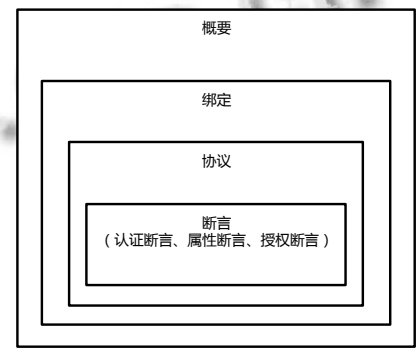

图 2 SAML 的组成

SAML 组件如图 2. 各部分组件描述如下:

断言[2]: SAML 允许一方为实体的特征或属性发出断言. 例如一个断言可以描述, 对于用户“John”的邮件地址是“john@example.com”, 改用户所在的组是“engineering”. SAML 断言被编码为一段 XML, 可以携带 3 种声明: 1)认证声明: 声明主体被成功认证. 包

括断言声明者, 被认证主体, 有效期, 及其他认证相关的信息. 2)属性声明: 声明主体具有的属性. 包括与该主体所关联的属性. 3)授权声明: 声明主体的授权权限. 包括包括被断言的主体, 被授予权限的资源(URL), 及与授权决策相关的信息.

协议[2]: 定义了一系列的请求、响应对, 用于在不同的实体间传递断言.

绑定[3]: 将 SAML 协议对应到标准消息或通讯协议, 如 http, soap 协议.

概要[4]: 规定了如何采用 SAML 断言、协议和绑定来支持特定用例, 如单点登录概要.

SAML 的域模型围绕着 SAML 断言的生产和消费来运作. SAML 工作原理如图 3.

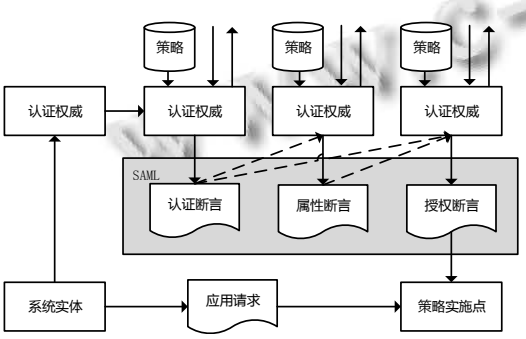

图 3

SAML 的域模型是认证授权解耦的设计. 认证实体, 属性实体以及策略实施点可以分散在系统中不同的物理机上. 当一个系统实体(客户端)试图发送应用请求访问受保护资源, 凭证收集器对相关联的认证断言、属性断言、和授权断言进行认证, 然后才决定授予客户端访问权限. 策略实施点根据该授予的权限来处理应用请求. SAML 断言被封装在 SAML 协议中在不同实体间传递.

3 系统设计与实现

真单点登录的解决方案实现简单, 但是对已经存在的应系统代码需要进行大量修改, 应用集成成本较高; 而且由于每个系统中真单点登录的实现不同, 当进行跨域的实体认证时, 需要对请求协议进行适配; 其安全问题容易成为薄弱环节. 为解决这些问题, 并考虑到遗留系统. 本文的目标是设计并实现松耦合、易插拔、互操作好、可扩展、安全的真单点登录框架.

3.1 总体架构

我们为认证中心 IDP 端和应用系统 SP 端分别设计了 SAML 单点登录组件. 他们作为过滤器过滤来自客户端的请求, 以提供支持 SAML 协议的单点登录, 其单点登录模型如图 4 所示. SSO-IDP 过滤器和 SSO-SP 过滤器为可配置、可插拔的组件.

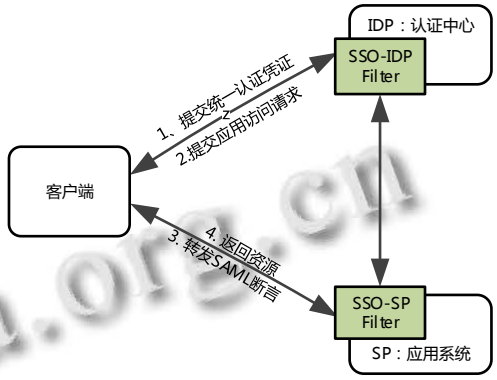

图 4 基于 SAML 的单点登录架构

3.2 系统模块结构

为实现支持 SAML 的单点登录, 我们在 Filter 中封装了单点登录服务、断言消费服务、访问控制、伪像解析服务等模块. 系统模块结构见图 5.

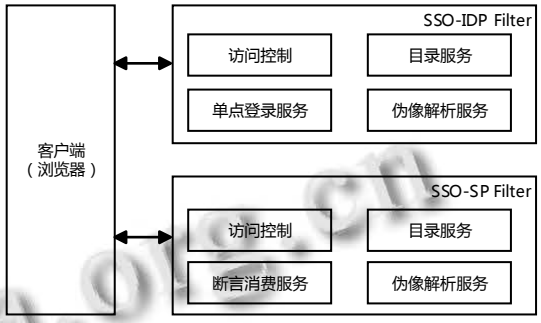

图 5 系统模块结构

该框架设计适用于支持 filter 的 J2EE 平台上的 WEB 应用, 采用的安全断言标准为 SAML2.0.

3.3 核心功能

身份提供者过滤器(SSO-IDP Filter): 部署在认证中心前端, 提供支持 SAML 的单点登录服务. IDP 过滤器能够理解遵守 SAML 规范的协议消息, 主要包括访问控制、单点登录服务、伪像解析服务、目录服务等模块. 访问控制模块主要用于维护用户安全上下文[5], 采用 SAML 认证请求中要求的认证策略对用用认证, 为用户授予权限; 单点登录服务提供对 SAML 的支持, 接受 SAML 认证请求, 根据认证结果生成断言并封装到 SAML 响应协议中; 伪像解析服务用于支持伪像绑

定, 若应用请求为一个 SAML 伪像请求, 则该服务检查该伪像合法性并主动向原始服务器拉取对应的 SAML 断言. 目录服务中保存了认证授权策略、及有效的断言.

服务提供者过滤器(SSO-SP Filter): 部署在业务系统端, 提供支持 SAML 的单点登录服务. SP 过滤器支持标准的 SAML2.0 协议. 主要包括访问控制、断言消费服务、伪像解析服务、目录服务等模块. 断言消费服务用于拦截用户请求, 若用户还没有建立安全上下文, 则为其生成 SAML 认证请求, 若用户携带一个包含认证或授权断言的 SAML 响应协议, 则验证该断言的合法性并决定授予用户权限. 其他模块同 IDP 端相同.

3.4 单点登录流程设计

图 6 描述了一个单点登录的流程. 概括来说, 在该流程中, 用户首先访问业务提供者, 然后被转移到身份提供者并提交用户凭证(透明的). 然后第二次访问另一个业务提供者时不再需要提交凭证.

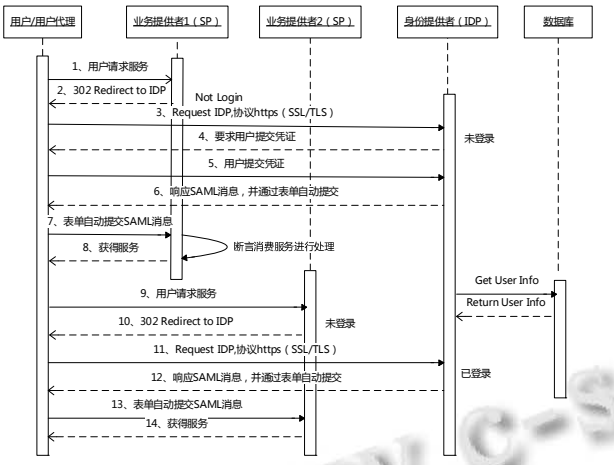

图 6 单点登录交互流程

(1) 用户访问 SP1

(2~3) SP1 发现用户未登录, 为其生成认 SAML 证请求并将其转移到 IDP 进行认证. 为保证协议信息的安全, 在此例中使用了 https 协议.

(4) IDP 解析认证请求, 若用户未登录, 则要求用户提交用户凭证

(5) 用户向 IDP 提交凭证, 如用户名, 密码.

(6~7) IDP 对用户进行认证, 并根据认证结果生成断言, 并通过绑定将用户转移回 SP1.

(8) SP1 从接收到的 SAML 协议消息中提取断言, 解析断言, 若断言有效, 则进行访问控制, 为用户提供服务.

(9) 用户访问 SP2

(10~11) SP2 发现用户未登录, 为其生成 SAML 认证请求并将其转移到 IDP 进行认证. 为保证协议信息的安全, 此例中使用了 https 协议.

(13) 由于用户访问 SP1 的时候, 在 IDP 已经进行过登录, 此时, IDP 可以根据符合 SAML 认证请求的一个认证上下文来为用户产生断言, 使得用户不需要再次提交凭证. IDP 通过绑定方式将用户转移到 SP2

(14) SP2 从接收到的协议消息中提取断言, 解析断言, 若断言有效, 则进行访问控制, 为用户提交凭证.

3.5 安全保障设计

为实现敏感信息的安全传递, 我们设计了可配置的安全模型. 图 7 展示了断言从生成到被接收方使用的过程.

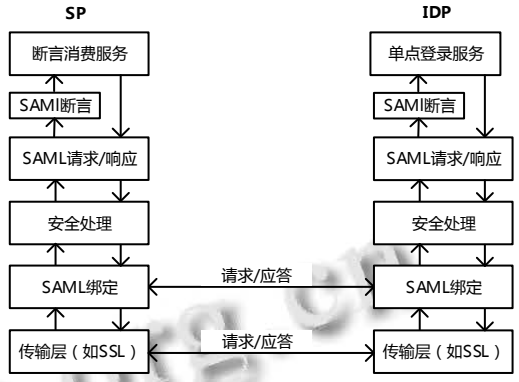

图 7 基于 SAML 的可配置安全保障

我们从以下角度来保证整个传输过程的安全:

(1) 机密性: 消息的内容只能通过制定的接收方进行解析, 其他实体不能阅读消息的内容. 为保证机密性, 我们采用 XML 加密技术[6,7]有选择的为 SAML 断言及协议提供加密; 另外可以依赖传输层安全协议来保证点到点的传输安全.

(2) 数据完整性, 不可否认性: 数据完整性是确认接收到的消息没有被篡改, 与发送方的消息版本一致; 不能否认指发送方不能否认发送信息的行为和信息的内容. 为保证数据完整性和不可否认性, 我们有选择的为 SAML 断言及协议的生产者生成的 XML 进行数字签名[6,8].

(3) 重放攻击[6]: 重放攻击指攻击者发送一个目

的主机已接收过的包, 来达到欺骗系统的目的. 为防止重放攻击, 我们在 SAML 断言及协议中明确限定有效期限或被认证的主体 IP 地址, 接受方应当验证该元素.

(4) 中间人攻击[6]: 指假冒断言请求、拦截并修改断言及伪造断言等行为. 预防此类攻击, 我们对 SAML 断言、协议及绑定阶段采取数字签名; 并通过传输层来降低中间人攻击.

3.6 框架适用场景

本框架支持 SP 发起及 IDP 发起的场景, 并支持多种绑定方式.

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" … Version="2.0">
  --断言的签发方
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">Https://idp.once.org:8444/idp</saml:Issuer>
--响应的状态, 此处为成功
  <samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status>
--断言内容, 包括ID、签发时间等
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      ID="_6581efe78ce79a059f0fa63f975f16b5" IssueInstant="2013-04-14T09:32:55.130Z" Version="2.0">
      --断言签发着
            <saml:Issuer ...>Https://idp.once.org:8444/idp</saml:Issuer>
      证书和断言签名
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
      --断言描述的主体
      <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
          <saml:NameID>********@foxmail.com</saml:NameID></saml:Subject>
        --断言的使用条件, 包括时间限制、接收者的限制
      <saml:Conditions NotBefore="2013-04-14T09:32:40.183Z" NotOnOrAfter="2013-04-14T09:33:55.183Z" ...>
          <saml:AudienceRestriction><saml:Audience>https://saml.salesforce.com</saml:Audience> </saml:AudienceRestriction>
      </saml:Conditions>
      --认证声明, 包括声明的签发时间
      <saml:AuthnStatement AuthnInstant="2013-04-14T09:32:54.575Z" …>
          --认证声明的上下文类型, 此处是用户名密码方式
          <saml:AuthnContext><saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
          </saml:AuthnContext>
      </saml:AuthnStatement>
  </saml:Assertion>
</samlp:Response>
```

图 8 SAML 响应消息

SP 发起的场景指用户访问服务提供者上受保护的资源时, 服务提供者上的访问控制模块会索要认证属性和授权属性, 若发现用户处于未授权状态, 则将用户重定向到身份提供者, 身份提供者对用户进行认证、授权. 授权结果被封装在断言中返回, 此时服务提供者根据授权断言决定是否允许用户访问资源.

IDP 发起的场景指用户正在访问身份提供者上的资源并已经持有安全上下文, 此时用户访问服务提供者上的资源, 服务提供者将授权信息封装在断言中并提供给服务提供者使用, 服务提供者根据该授权断言决定是否允许用户访问资源. 门户应用就是典型的 IDP 发起的场景.

另外, 框架支持多种绑定方式, 包括 http 重定向及 post 形式的 push 模式, 及 artifact(伪像)形式的 pull 模式.

3.7 应用实例

本案例中, 我们将 SSO-IDP filter 部署在门户系统 OncePortal 上, SSO-SP filter 部署在被集成的应用上, 此例中为 Salesforce.

用户在 OncePortal 中已经登录, 此时访问被集成

的应用 Salesforce, SSO-IDP filter 将生成图 8 所示的 SAML 响应协议, 并将其发送给 salesforce. 当 salseforce 端的 SSO-SP filter 拦截到该 SAML 响应协议时, 将验证所包含的断言的合法性, 并决定是否授予用户权限.

4 总结

本文针对单点登录的不足, 设计了基于 SAML 的统一认证单点登录框架, 并充分考虑了各个环节的安全问题. 采用了 SP-client 分离的思想, 将支持 SAML 的单点登录部分分离出来, 提供一种通用的开发方法. 该框架是一种可插拔、可扩展、松耦合的实现方式. 使得开发人员通过提供的 IDP 和 SP 端组件, 很容易开发部署基于 SAML 的单点登录系统.

未来工作是提供对联合身份的单点登录支持和灵活的 SAML 元数据[10]配置支持.

参考文献

1 OASIS Security Services TC. Glossary for the OASIS SAMLv2.0. http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf.

2 OASIS Security Services TC. Assertions and Protocols for the OASIS SAMLv2.0. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

3 OASIS Security Services TC. Bindings for the OASIS SAMLv2.0. http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf.

4 OASIS Security Services TC. Profiles for the OASIS SAMLv2.0. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os. pdf.

5 OASIS Security Services TC. Authentication Context for the OASIS SAMLv2.0. http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf.

6 OASIS Security Services TC. Security and Privacy Considerations for the OASIS SAMLv2.0. http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf.

7 XML Encryption Syntax and Processing. http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html.

8 (Extensible Markup Language) XML-Signature Syntax and Processing. http://www.ietf.org/rfc/rfc3275.txt.

9 SAML Single Sign-On (SSO) Service for Google Apps. https:// developers.google.com/google-apps/sso/saml_referenc _imple- mentation.

10 OASIS Security Services TC. Metadata for the OASIS SAMLv2.0. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.