一种基于 SAML 带自验证的单点登录模型

A self – validating Single Sign – on model which based on SAML technology

龚家兵 曹彩凤 崔方龙 (合肥 中国科技大学信息管理与决策科学系 230026)

摘要:应用系统的安全问题一直备受重视,身份认证是一种常用的安全实现方式。本文分析了现有的身份认证方式的种种弊端,提出了一种基于 SAML 技术的带自验证单点登录模型,并对这种模型进行了安全性分析。

关键词:SAML(Security Assertion Markup Language) 自验证 单点登录

1 集成环境中身份认证模式现状

认证技术是信息安全理论与技术的一个重要方面。身份认证是安全系统中的第一道关卡,用户在访问应用系统之前,首先经过身份认证系统识别身份,然后访问监控器根据用户的身份和授权决定用户是否能够访问某个资源。大致上来讲,身份认证方式可分为分散式身份认证方式和集中式身份认证方式。现有的身份认证方式大多都存在种种弊端,详细分析如下。

1.1 分散式身份认证方式的弊端

随着信息化程度的提高,各组织机构中运行的应用系统越来越多,这些系统都有各自的身份认证模块,在集成环境下分散式身份认证方式主要存在以下的不足:

(1) 目前大多数应用系统都有自己独立的用户管理与身份认证模块,表面上这样的设计更加灵活,实际上这样会给组织部门管理和用户个人带来很多不便。例如:新生入学时需要办理各种入学手续,如户籍、一卡通、邮箱等。那么在这种模式下,就需要该生在每个部门都创建用户名和密码。这样的操作是重复劳动,费时费力。如果每个部门的用户名和密码的长度要求不一样的话,该生就必须要记住各个帐号的用户名和密码,这样会给新生带来很多的不便[2]。

(2) 在集成环境下,每个子系统都有自己独立的身份认证模块,都有各自不同的安全要求,一般都没有从整体上考虑安全性问题。这样各个系统之间就会产生安全隐患,比如:用户对身份认证信息记忆的混淆、如果两个不同的系统中身份认证信息相同,这样就会造成系统内部数据的泄漏。

(3) 每个应用系统之间都有类似的身份认证模块的设计,造成了软件的重复开发。同时也不利于集成系统的安全管理。

1.2 集中式身份认证方式分析

在集成环境下的集中式身份认证是通过单点登录模型(SSO,Single Sign – on)来实现。一般的单点登录模型都是采用无自验证用户信任凭证方式。下面我们详细的分析下:该模型使用的是 SAML 断言。所谓 SAML 断言就由两部分组成。第一部分是通用部分,包含有版本号、主体等;第二部分是一个或多个实际的、关于身份验证、属性或授权语句[5]。目前这种断言被很多安全实现方式和模型采用,应用系统都能够接受 SAML 断言。因此它可以被从一个网络应用程序传递到另一个网络应用程序,从而可以避免再次登录。这样就能够在集中环境中,安全和方便的鉴别和管理用户。

特别的,分布式系统由独立的安全域组合而成,这些域包含与操作系统和应用程序相关的独立平台,这意味着终端用户需分别向他要访问的每个域证实自己的身份。用户向最初登录的域(主域)提交一整套适用于该域的凭证(credentials),例如用户名和密码,然后才能和该域建立对话。调用另一个域(次域)内的服务时,用户需要再次进行登录,即进一步提交他的个人凭证。

单点登录是一种可以在企业内部的不同域之间集成用户登录功能和账户管理功能的技术。它考虑到系

统的整体的实用性和安全性，它将终端用户和管理看得同样重要。采用单点登录方式时，系统需要从用户那里收集所有必要的证明和用户凭证信息（登录主域时的部分信息），用以支持可能会与之发生作用的次域对用户的身份验证。

在无自验证用户信任凭证单点登录模型中，每个请求都需要向安全认证机构验证用户凭证。用户先向安全认证机构提交用户凭证，如：用户名和密码，通过认证后返回一个会话令牌（token），凭此令牌用户可以申请希望得到的网络服务，在得到服务之前网络服务需借助认证机构来验证令牌的有效性，只有包含有效会话令牌的网络服务请求才能被允许；当用户要访问位于其他安全域的网络服务时，将会话令牌出示给新的网络服务，而新的网络服务需再次让认证机构验证令牌的有效性后才能向用户提供服务。然后再由用户决定是否访问，如果采用 Kerberos 作为潜在的认证机制，则安全认证机构为 Kerberos 服务器，发出的会话令牌是有效期为八小时的许可服务票据（Ticket – Granting Service，TGS）；如果采用 PKI 作为认证机制，则安全认证机构为 CA，相应的会话令牌为数字证书。

在无自验证用户信任凭证单点登录模型中，身份认证模式避免了分散式身份认证模式的一些弊端，实现了用户身份认证的集中管理，用户只进行了一次身份认证。但是在每次申请新的服务之前，认证机构都需要重新对会话令牌验证，所以整个实现过程比较复杂。更重要的是过多的请求对认证服务器的硬件要求很高，很可能会阻塞认证服务器，不仅令牌生效请求得不到响应，还有造成服务器崩溃的隐患。于是需要寻求一种新的单点登录方式来简化这一过程。

综合上面的各种弊端本文提出了基于 SAML 技术来实现在一个企业中各个应用系统间的单点登录模型，实现身份验证的一次性。这样能带来更大的方便和安全。

2　基于 SAML 自验证单点登录模型

2.1　SAML 的安全服务功能

SAML 作为 XML 的一种描述语言，其关注的重点不仅仅局限于信息的描述，而是如何用 SAML 实现信息的安全共享。使得在 Internet 环境下，可以用标准的方式描述和使用已经广泛采用的安全技术。SAML 支持一次登录（Single Sign On，SSO），使得用户在访问多个应用系统时，仅需登录一次。用户在一个应用系统进行身份认证，应用系统之间可以通过 SAML 传输、共享用户的安全信息，而不需要用户多次登录、认证。同时由于 SAML 定义了在多个信任合作者之间进行交互的技术规范（B2B 中不可或缺的信任关系），这样企业与企业之间的互访成为可能，这也使得 SAML 自定义很快得到了大型软硬件厂商的支持，包括 IBM，SUN，Microsoft，Novell，Oblix，RSA 等。

（1）SAML 体系结构。在典型的 SAML 体系结构中（如图 1 所示），中继方（Relaying Party）是向发行机构发送 SAML 请求的发送方。该发行机构随后生成一个 SAML 断言响应。这些基于 XML 的请求和响应的消息格式，可以与许多不同的潜在通信传输协议绑定，目前 SAML 定义的绑定是在 HTTP 上通过 SOAP（Simple Object Access Protocol，简单对象访问协议）封装传送，但应用程序可以用各种请求/响应协议定义和交换断言[4]。

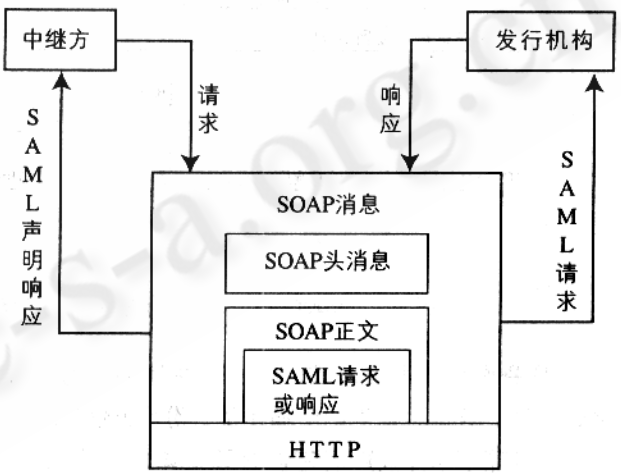

图 1　SAML 体系结构

（2）SAML 声明。SAML 规范描述包括声明、请求/响应协议、绑定和配置文件。声明包含有关主体所执行的身份验证操作的相关信息、主体属性信息以及是否允许该主体访问特定资源的授权决策。这些内容是通过 XML 结构表示的，并包括嵌套结构。单个声明包括多个有关身份验证、授权和属性的内部声明。声明是由 SAML 授权机构发行的，即身份验证授权机构、属

性授权机构和 Policy Decision Points（PDP，策略决策点）。通过 SAML 定义的一种协议，客户端程序可以从 SAML 授权机构请求声明，并获得一个响应。该协议包括基于 XML 的请求和响应消息格式，可以被绑定到多种基础通信和传输协议中。SAML 授权机构可以使用各种信息源，如在请求中作为传入信息接收的外部策略存储和声明，以便于创建对应的响应。因此，客户端程序始终只能使用声明，而 SAML 授权机构既可以使用声明，也可以生成声明。SAML 提供如下的 3 种类型的声明：

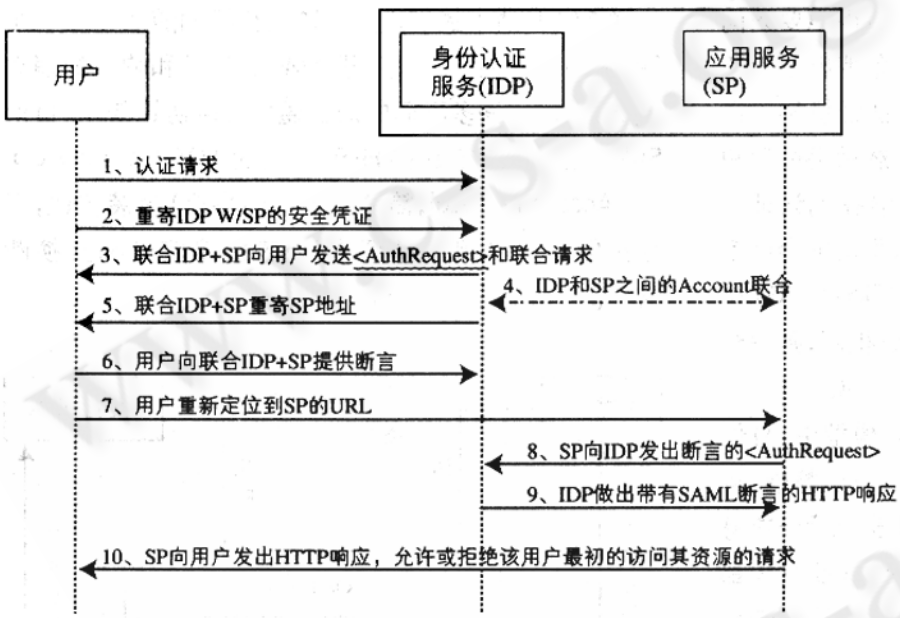

图 2　federated sso 的消息交换和处理过程

① 身份验证声明，在该声明中，主体的身份已经通过验证。身份验证声明中描述了身份验证信息。

② 属性声明，该声明包含有关主体的特定信息，如主体的信用限制、访问级别、信用等级或其他合法声明。

③ 授权决策声明，该声明指明主体可以执行或被授权执行的操作。例如，该声明可以声明主体是否已经通过授权、可执行特定的事务。

（3）SAML 的优势

① 可令不同类型的安全服务系统之间实现交互。

② 提供单次登录身份验证功能。该功能可以大幅度地减少站点之间的复制安全性和身份验证信息的需求。

③ SAML 不依赖于它所交互的任何系统。每个系统都可以为用户的身份验证和授权建立自己的策略。

④ 提供基于属性的身份验证。这种方式显然优于当前基于 XML 数字签名的身份验证。

2.2　基于 SAML 自验证单点登录模型

在基于 SAML 自验证单点登录模型中，其内部消息交换和处理过程是通过联合 IDP + SP 的方式来实现的，可用下面的图表[3]描述（如图 2）：

（1）用户向联合 IDP + SP 发出 < AuthRequest > ；

（2）用户重寄 IDP W/SP 的安全凭证；

（3）联合 IDP + SP 向用户发送 < AuthRequest > 和联合请求；

（4）IDP 和 SP 之间的 Account 联合；

（5）联合 IDP + SP 重寄 SP 地址；

（6）用户向联合 SSO 提供断言；

（7）用户重新定位到 SP 的 URL；

（8）SP 向 IDP 发出断言的 < AuthRequest > ；

（9）IDP 做出带有 SAML 断言的 HTTP 响应；

（10）SP 向用户发出 HTTP 响应，允许或拒绝该用户最初的访问其资源的请求。

通过这样的消息交换和处理过程，通过 SAML 技术就可以减少对安全凭证验证的次数，从而简化了单点登录模型的实现，如下（图 3）：

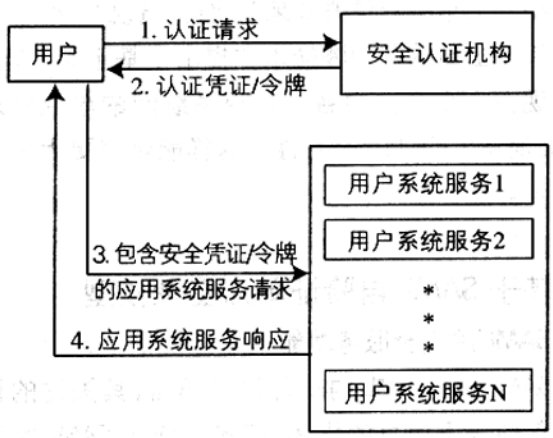

图 3　带自验证用户信任凭证的单点登录模型

基于 SAML 带自验证用户信任凭证的单点登录模型是一种不需要频繁向安全认证机构验证认证令牌，因为在该模型中，安全认证机构采用 SAML 断言作为会话令牌，令牌中包含的用户凭证通常由安全机构进行数字签名，安全凭证的接受方能自验证这些安全凭证，不需要再去请求安全认证机构验证该安全凭证的有效性。自验证安全凭证通常是被安全认证机构认证通过的，安全认证机构发放一个有数字签名的安全令牌，该数字签名是用自己的私有密钥。安全凭证的接受方用安全认证机构发放的授权公共密钥来证实。这个授权公共密钥是已经被确认的。这样收到此令牌的应用系统服务可间接认证了申请服务的用户身份；在这种情况下如果用户再次申请别的网络服务，只需将 SAML 机构颁布给他的认证令牌出示给新的网络服务即可。不需要去安全认证机构验证认证令牌。

换言之，用户在一个应用系统服务上取得认证授权，当需要访问另一个相关应用系统服务的资源时，目的站点（保护资源的持有者）能够使用 SAML 从源站点调取用户的证书信息。此时 SAML 对信息交换的处理发生在后台，因此用户的资源实际上被不同的安全系统进行了定位。

SAML 是面向基于 XML 的 Web 服务的架构，此标准用于在业务伙伴之间交换认证和授权信息。能够在多个企业运营的站点之间实现单点登录等基于网络的安全相互连接功能。利用 SAML，网络服务不需要频繁的向安全认证机构验证令牌的有效性，不但减少了安全认证服务器的信息负载、简化了单点登录步骤提高了工作效率，还带来了许多无自带验证单点登录方式所不具备的优点：

① SAML 是面向基于 XML 的 Web 服务的架构，允许企业及其供应商、客户与合作伙伴进行安全的认证、授权和基本信息交换。由于 SAML 是通过 XML 对现有的安全模式进行描述，因此它是一个中立的平台并且不需要依赖于供应商的基础结构。

② SAML 在为认证声明和认证属性建立了一个数据格式，其参数取决于安全服务产生的基于政策的认证结果。使用 SAML 标准作为安全认证和共享资料的中间语言，能够在多个站点之间实现单点登录。

③ 在这个模型中 SAML 的消息格式能够从一个源站点将声明发送给一个接受者。这个声明中包含安全凭证令牌这样就可以减少安全认证机构的访问次数，能使电子商务合作中的事务处理速度得到加快，并且使认证环境的复杂性得到全面的简化。

3 小结

在自验证单点登录模型中，用户身份认证声明采用 SAML 描述，而 SAML 继承了 XML 跨越平台的优点使该模型克服了以往单点登录模型受平台限制的缺陷，这个模型适用于 B2B 和 B2C 等电子商务系统和其他的组织的内部网络。一些著名计算机软件公司都在致力于开发单点登录系统的开发，例如 IBM 公司的 Websphere Portal Server、Microsoft 公司的 Windows 2000、.NET Passport。也有一些着力于互联网个人认证管理技术的标准化的组织。比如 Liberty Alliance Project（自由联盟计划），它是一个互联网个人认证管理技术的标准化组织，以 SAML 为基础进行开发。总之，自验证单点登录模型优化了网络系统的安全管理控制，减少企业间因为验证用户声明的通信，提高了用户工作效率，增强了系统安全性并且实现了异构网络的协同工作，在电子商务、电子政务中将会有很好的应用前景。

参考文献

1 Jorgen Thelin《Identity, Security and XML Web Services》Cape Clear Software Inc. 2003，P14－15.

2 孙超等，《基于 agent 技术的统一身份认证系统》，2005 年 vol3P138－140.

3 John C. Fowler《Portals, Identity Management in Education》Infrastructure Market Development Manager Global Education & Research .

4 Ben Galbraith 等著，吴旭超译，《Professional web services security》，清华大学出版社，2003 年 P264～267。

5 Bert Hartman 等著，杨硕译，《Mastering web Services Security》，清华大学出版社，2004 年 P87。