基于安全声明标记语言(SAML)实现单点登录

Implementation of Cross Domain Single Sign-On Based On SAML

纪 方 (中国科学院研究生院 100039)
鲁士文 (中国科学院计算技术研究所 100080)

摘 要: 本文介绍SAML的体系结构以及基于SAML实现跨越企业边界的单点登录方法，并且分析了在SAML环境中面临的威胁，提出了可以采取的应对措施。

关键词: 安全声明标记语言 单点登录

如何提高跨越企业边界的安全信息互操作性，使得交易企业可从其他企业获取有关用户和交易等授权参考数据，是目前国际工业界和学术界所致力解决的关键问题之一。

为了促进上述问题的解决，国际标准化组织OASIS的安全服务技术协会（Security Service Technology Committee）分别于2002年11月和2003年9月制定了安全标准——安全声明标记语言（Security Assertion Markup Language）1.0版和1.1版。设计SAML的一个主要目的是单点登录，所谓单点登录（Single Sign On），指的是只要在一个网站上通过身份认证登录后，就可以使用多家相关网站的信息。SAML促进了不同安全系统之间的互操作性。

1 安全声明标记语言(SAML)的体系结构

安全声明标记语言(SAML)是用于交换安全信息的基于XML的框架。SAML并不是一项新技术。确切地说，它是一种语言，进行单一的XML描述，允许不同安全系统产生的信息进行交换。

1.1 SAML声明

安全信息以声明（assertion）的形式表述主体，主体是指在某个安全域中有身份的实体（用户或计算机）。声明描述主体的认证行为，主体的属性，以及是否允许主体访问某一资源的授权决定。

声明是SAML的基本数据对象，是对主体的身份、权限等信息进行的XML描述，它包括SAML权威生成的三种声明：认证声明（Authentication Assertion）、属性声明（Attribute Assertion）和授权决定声明（Authorization Decision Assertion）。声明是由SAML权威发布的，SAML权威包括：认证权威，属性权威和策略决定点。SAML权威可以是安全应用程序或者是权限管理基础设施（Permission Management Infrastructures），在实践中，一个SAML权威可以生成和发布上述三种声明。

SAML声明包括以下一些常规信息：发行者和发行时间戳，声明标识，主体（名称和安全域，可选的主体信息，如：公钥），条件（在什么条件下声明有效），通知（声明是如何生成的）。其中，认证声明描述SAML权威对主体在某一时刻以某种方式进行认证的声明，认证方式包括：口令、Kerberos、安全远程口令（Secure Remote Password）、SSL/TLS客户端身份认证、基于X.509公钥的认证等方式。属性声明描述SAML权威对主体的相关属性的声明，例如：主体为“Bob”，属性为“Department”，属性值为“Engineering”。授权决定声明描述SAML权威对主体访问某资源的请求的授权决定的声明。对SAML声明进行数字签名，可以保证数据的完整性和不可否认性。图1所示是SAML模型。其中：

实体（Entity）：请求访问某种资源的实体（个人、组织或过程）。

认证权威（Authentication Authority）：负责验证用户提供的凭证，确定用户身份，并生成认证声明。

属性权威（Attribute Authority）：负责保存有关用户的属性信息，并根据请求生成属性声明。

策略决定点（Policy Decision Point，简称PDP）：根据相应的安全策略，对用户身份、请求的操作及所要访问的资源进行评估，做出授权决定。

策略执行点（Policy Enforcement Point，简称PEP）：负责执行策略决定点做出的授权决定。

1.2 SAML协议

SAML定义的请求/响应协议规定了两点间共享SAML数据所需交换的报文种类和格式。通过协议，用户可以向SAML权威发送请求（包括对认证声明，属性声明，授权声明等相关信息的查询），并从SAML权威获得响应。SAML请求由SAML客户端发起，安全服务返回SAML响应。

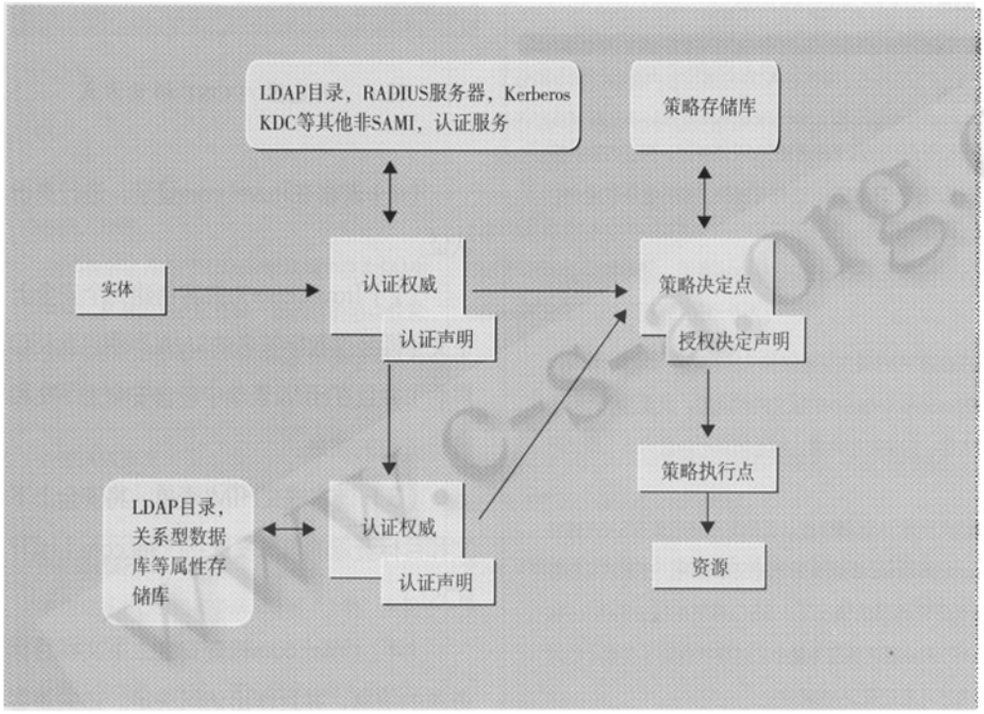

图 1　SAML 模型

1.3 SAML 绑定

请求/响应协议规定了两点间共享SAML数据所需交换的报文种类和格式，而两点间的消息传输通过与具体传输协议的绑定实现。SAML绑定是指将SAML请求/响应协议信息映射到标准的通信协议中。SAML定义了一个绑定，即SOAP /HTTP：用SOAP查询SAML权威并获得响应。

图 2　SAML 绑定

1.4 SAML 档案（Profile）

SAML档案是指用于描述SAML声明如何在协议中嵌入和取出的一组规则集。SAML定义了两个支持单点登录（SSO）的基于Web浏览器的档案：浏览器/辅件（Artifact）档案和浏览器/POST档案。在基于Web浏览器的档案中采用了两个基于HTTP的技术，用于使用通用浏览器从源站点到目的站点的信息传输。即：

SAML辅件：它是一种限定大小的数据，可以识别声明和源站点。它作为 URL 查询字符串的一部分传递，并按重定向路径传送到目的站点。

表单POST：SAML声明装载到HTML表单中，当用户提交表单时，作为HTTP POST载荷的一部分，SAML声明被传输到目的站点。

在这两个档案中都没有用到Cookies,因为Cookies限制源站点和目的站点需同属一个Cookie域。

2 实现跨越企业边界的单点登录

要实现跨越企业边界的单点登录，各企业应事先达成合作协议，且各企业的安全系统都可以识别SAML 数据，可根据SAML声明判断用户的身份，或决定用户在本企业内的访问许可权。例如：旅行站点(Travel.com)和宾馆服务站点(Hotel.com)签订合作契约，凡是在Travel.com 处参加旅行团的游客，可以在Hotel.com处预定宾馆房间。用户只需在站点Travel.com 登录一次，就可以访问Hotel.com站点。

在具有SAML功能的Web单点登录环境中，用户可以通过ID/口令等认证技术登录到源域中。源域利用包含SAML认证声明和属性声明的信息，向一个或多个目的域发送认证决定以及为这一决定提供安全上下文的其他信息。

在支持Web单点登录的SAML互操作性环境中，有两种实现方式：即浏览器/辅件（Artifact）档案和浏览器/POST档案。

2.1 浏览器/辅件（Artifact）档案方式

2.1.1 实现过程

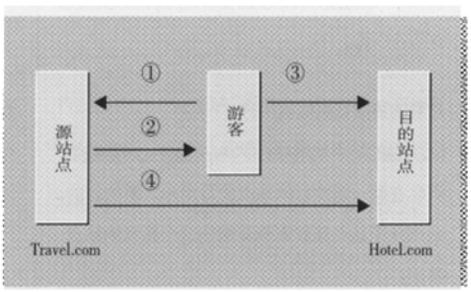

图 3　浏览器/辅件（Artifact）档案方式

（1）游客在Travel.com登录，进行身份认证；

（2）Travel.com为游客创建一个安全上下文（即SAML声明）并保存，然后为SAML声明生成一个固定长度（8字节）的SAML辅件并返回给游客；

（3）游客访问Hotel.com。URL包括目的站点，SAML辅件和目标资源（通常通过HTTP/SSL访问）。

例如：https://hotel.com?SAMLartifact=8BhexNumber&target=reservation/myfile.html

（4）Hotel.com用SAML辅件的信息从Travel.com获取有关游客的SAML声明，并做出访问决定。如果游客有访问权限则可以直接访问无需再次进行身份认证。

2.1.2 面临的威胁和采取的措施

下面就浏览器/辅件档案方式中面临的威胁以及采取的措施作一些讨论，见表1。

表1

面临的威胁	采取的措施
窃取SAML辅件 (如果偷听者可以复制用户的SAML辅件,那么偷听者就可以用用户的SAML辅件构造URL,并且到目的站点冒充用户。)	1. 在站点和用户浏览器之间传输SAML辅件时，保证传输的机密性，即使用HTTP/SSL。这样可以防止偷听者获取用户的SAML辅件。 2. 源站点和目的站点可以利用时间同步服务，将双方时间同步。 3. 源站点追踪SAML辅件创建时和从目的站点接收载有SAML辅件的<samlp:Request>的报文的时间差，设置这个时间差的最大值，如果超出此值，则源站点不向目的站点提供声明。 4. 当源站点创建SAML辅件或从目的站点接收载有SAML辅件的<samlp:Request>的报文时创建SSO声明。在源站点和目的站点正常通信的情况下，SSO声明的NotBefore和NotOnOrAfter属性值应尽量小。这样就保证了在很小的时间窗内才可能窃取SAML辅件。 5. 目的站点检查从源站点获得的声明有效期，拒绝接受过期的声明。
攻击SAML协议的报文交换 (报文交换会遭受各种攻击，包括：窃取SAML辅件和声明，篡改报文，重放攻击，中间人(MITM)攻击。)	使用HTTP/SSL，即：使用SSL双向身份认证，保证报文的完整性和机密性。
恶意的目的站点假冒用户 (因为目的站点从用户获取SAML辅件，恶意的站点会在某一新的目的站点假冒用户。新的目的站点从源站点获取声明并相信这个恶意的站点是用户。)	当新的目的站点获取与SAML辅件相应的声明时，需要向源站点验证身份。
伪造SAML辅件	恶意的用户会重复猜测有效的SAML辅件值，因此，源站点对于反复查询SAML辅件应加以限制。
浏览器状态暴露 (在浏览器/辅件档案中从源站点“下载”SAML辅件到浏览器，作为浏览器状态的一部分，可以获得这个信息。通常这个信息保存在用户的系统中。因此，这个SAML辅件在以后面临被重用的危险。)	SAML辅件的“一次性使用”特性保证它不会被其他浏览器重用。

2.2 浏览器/POST档案方式

2.2.1 实现过程

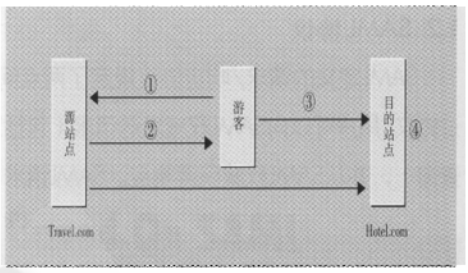

图4 浏览器/POST档案方式

（1）游客在Travel.com登录，进行身份认证；

（2）Travel.com为游客创建一个安全上下文（即经过数字签名的SAML声明包含SSO声明）并且在HTML表单中包含安全上下文和目标资源的信息；

（3）游客提交HTML表单。将安全上下文和目标资源的信息发送到Hotel.com（HTTP POST）。

（4）Hotel.com检查安全上下文和目标资源的信息，并且作出访问决定。如果游客有访问权限则可以直接访问无需再次进行身份认证。

2.2.2 面临的威胁和采取的措施

下面就浏览器/POST档案方式中面临的威胁以及采取的措施作一些讨论。见表2。

3 SAML的优越性

如图5所示，在模型A中，供应商必须与厂商保持用户目录同步，因为用户信息需要在参与交易的站点进行维护。这就需要重复的目录复制过程。在模型B即SAML模型中，不需要进行目录同步与复制。安全信息随同Alice和Bob一起移动。厂商并不知道Alice和Bob，厂商利用Alice和Bob各自所在的站点产生的SAML声明来判断用户，用户信息不需要在参与交易的站点进行维护，所以不需要进行目录复制。

表2

面临的威胁	采取的措施
窃取SAML声明 (如果偷听者可以复制用户的SAML声明,那么偷听者就可以构造POST体,并且到目的站点冒充用户。)	1. 站点和用户浏览器之间传输SAML声明时，保证传输的机密性，即使用HTTP/SSL。这样可以防止偷听者获取用户的SAML声明。 2. 源站点和目的站点可以利用时间同步服务，将双方时间同步。 3. 当声明从源站点传输到目的站点的过程中，SSO声明的NotBefore和NotOnOrAfter属性值，应尽量小。这样就保证了在很小的时间窗内才可能窃取SAML声明。 4. 目的站点检查从源站点获得的声明的有效期，拒绝接受过期的声明。
中间人攻击 (因为目的站点通过HTML表单从用户获取SAML声明，恶意的站点会在某一新的目的站点假冒用户。新的目的站点会相信这个恶意的站点是声明的主体。)	目的站点检查SAML响应的Recipient属性值是否与声明接收者的主机名和路径相匹配。因为SAML响应经过数字签名，Recipient属性值不能被恶意的站点修改。
伪造SAML声明	载有SAML声明的SAML响应需要经过数字签名，并且目的站点验证数字签名，保证报文的完整性。
浏览器状态暴露 (在浏览器/POST档案中从浏览器“上载”声明到目的站点，作为浏览器状态的一部分，可以获得这个信息。通常，这个信息保存在用户的系统中。因此，这个SAML声明在以后面临被重用的危险。)	使SSO声明的生存期尽可能短并且确保SSO声明只被提交一次。

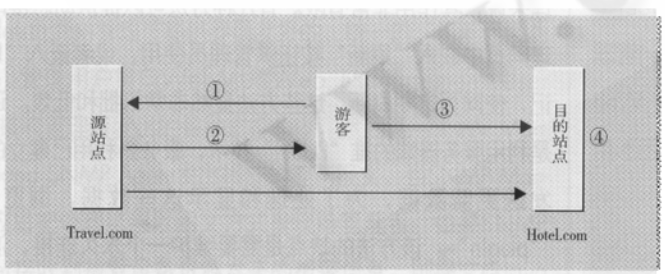

图5 模型比较

4 结束语

SAML规定了使用数字证书、将用户的认证和授权信息在多个网站之间安全交换的使用过程等，促进了不同安全系统之间的互操作性，实现跨越企业边界的单点登录，在电子商务和电子政务领域有很广阔的应用前景。

参考文献

1 Eve Maler, Prateek Mishra. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1. OASIS Standard, 2 September 2003. http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

2 Eve Maler, Prateek Mishra. Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1. OASIS Standard, 2 September 2003. http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

3 James Kobielus. SAML promises Web services security. http://www.nwfusion.com/news/tech/2002/0701tech.html

4 Internet X.509 Public Key Infrastructure Certificate and CRL Profile http://www.ietf.org/rfc/rfc2459.txt