文章编号: 1674-7070(2012) 02-0170-06

SAML 和 XACML 在单点登录中的应用研究与实现

王强[1]　傅德胜[1]

摘要

现代企业中出现的越来越多的应用系统往往各自提供一套身份认证方式，这不仅增加了用户的负担，而且降低了系统安全性. 企业内部另一重要的问题是管理员如何控制已验证身份的用户的访问请求. 基于 SAML 的单点登录技术和基于 XACML 的访问控制技术可以很好地解决这两个问题. 在对 SAML 和 XACML 规范进行了分析的基础上，提出了一个基于 SAML 和 XACML 的单点登录模型，分析了该应用模型的安全性，最后在微软. NET 平台上予以实现.

关键词

单点登录; 身份认证; SAML; XACML

中图分类号 TP309. 2

文献标志码 A

收稿日期 2010-10-19

作者简介

王强，男，硕士生，研究方向为信息安全. wongqiang@ yeah. net

傅德胜(通信作者) ，男，教授，博士生导师，主要从事信息安全及图像处理与模式识别方面的研究. dsfu@ nuist. edu. cn

1　南京信息工程大学　计算机与软件学院，南京，210044

0　引言

传统的身份认证解决方案是为每一个 Web 应用建立起一个为其自身服务的身份认证系统，然而，随着应用系统的增多，会带来一些问题. 比如，随着企业信息化的深入，某大型煤矿集团就建立起好几个为其自身服务的应用系统，其中包括财务系统、物资管理系统、设备管理系统、OA 等. 这些系统互相独立. 对某些用户(比如公司财务科的人员) 而言，他可能同时是其中几个系统的用户，该用户在使用每个系统之前都必须使用相应的系统身份进行登录，为此，用户必须记住多套用户名和密码，这显然增加了用户的负担. 更重要的是，随着系统的增多，出错的可能性就会增加，系统安全性就会相应降低. 出于效率和安全方面的考虑，人们迫切需要改变传统的认证方式，设计出一种更为高效、安全的网络认证机制. 重复认证的问题可以通过单点登录[1] (Single Sign-On，SSO) 技术解决. 所谓单点登录是指用户只需在网络中要进行一次必要的身份认证，然后就能够访问信任域中其他成员的受保护的资源，而无需再次认证. 企业内部另一重要问题是管理人员如何对已验证身份的用户的访问请求进行管理，它可以通过访问控制来解决，访问控制通过检查用户对特定资源是否有访问权限允许或者拒绝用户的访问请求.

1　相关技术

1. 1　单点登录

依据应用程序的登录方式，传统的单点登录主要分为 2 类[1]：一种是基于脚本(Script) 的 SSO 解决方案; 另一种是基于访问票据(Access Ticket) 的 SSO 解决方案. 基于脚本的 SSO 解决方案主要是通过脚本使登录过程自动化. 基于访问票据的单点登录解决方案主要是通过对目标系统进行改造，接受访问票据实现单点登录，典型的案例有微软的. NET Passport.

上述 2 种解决方案都在一定程度上解决了单点登录问题，减少了用户登录次数，提高了安全性，然而都存在一些不足. 例如，基于脚本的单点登录方案依赖于客户端软件，并且目标系统间用户数据难以安全交换; 基于访问票据的. NET Passport 则存在所谓的单点失效问题，还有一个不足之处就是对服务器端受保护的资源的访问控制做得不细[1].

针对传统单点登录技术存在的缺陷,本文提出了基于 SAML 和 XACML 的单点登录技术,通过 SAML 协议实现用户的单点登录,使用 XACML 技术实现对服务器端受保护资源的细粒度的访问控制.

1.2 SAML

SAML(安全声明标记语言,Security Assertion Markup Language)是结构化信息标准促进组织(OASIS)建立的安全标准,是一种基于 XML(可扩展标记语言)语言的面向 Web 服务的用于传输认证及授权信息的技术框架[2]. SAML 协议主要是为不同服务系统之间交换安全信息提供了一种机制,从而实现了不同安全系统之间的互操作性.

SAML 协议规范主要包含以下几方面:SAML 断言(Assertion)、SAML 请求响应协议(Protocol)以及绑定(Bindings)[2]. 主框架如图 1 所示[3].

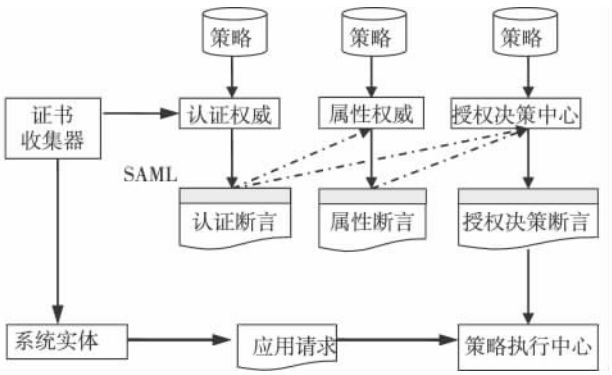

图 1 SAML 框架

Fig. 1 SAML architecture

1.2.1 SAML 断言

SAML 断言是 SAML 权威机构对访问主体所执行的身份验证操作相关信息、属性信息以及是否允许主体访问某一资源的授权决策的 XML 描述. SAML 标准共提供了 3 种类型的断言[2]:1)认证断言,主要描述了 SAML 权威机构对认证主体通过某种方式进行身份认证的相关情况;2)属性断言,主要描述认证主体相关的属性信息,比如主体的职位、角色等;3)授权决策断言,用于断言主体是否对某个资源有访问的权限.

1.2.2 请求/响应协议

SAML 协议描述了 SAML 元素(比如断言)如何在 SAML 请求/响应中组织,以及 SAML 实体在发布断言或者消费断言的时候必须遵循的规则. SAML 定义了一组请求/响应协议,对两点间共享 SAML 数据所需交换的报文种类和格式做出定义. 用户可以向 SAML 权威发送请求(如对认证断言、属性断言和授权决策断言等信息的查询),并从 SAML 权威获得响应.

1.2.3 SAML 绑定

SAML 绑定就描述了请求响应如何与现有的一些传输协议(如:HTTP、MIME、SMTP、FTP 以及 SOAP 等)进行绑定以实现安全传输. 这种绑定方法使 SAML 具有良好的开放性和扩展性,可以利用这些协议原有的安全机制实现 SAML 协议传输的简单的安全性.

1.3 XACML

XACML(可扩展访问控制标记语言,Extensible Access Control Markup Language)同样是由 OASIS 建立的基于 XML 的安全性标准,用于表示控制信息访问的规则和策略[4]. XACML 除了给出策略的描述语法之外,也给出了一个标准化的访问控制决策模型[5],模型如图 2 所示.

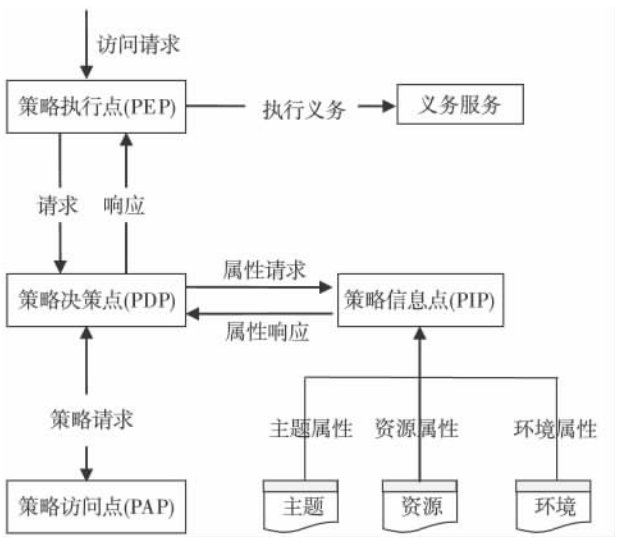

图 2 XACML 访问控制决策模型

Fig. 2 XACML access control model

典型的访问控制和授权场景包括 3 个主要实体:主体、资源和动作以及它们的属性[5]. 主体请求得到对资源执行动作的权限. 在专有访问控制系统中,这些实体及其属性的信息保存在资料库中. 这种资料库称为访问控制链表(ACL). 不同的专有系统有不同的实现 ACL 的机制,因此难以交换和共享信息. XACML 的提出解决了这 2 个问题:1)创建一种可移植的、标准的方式来描述访问控制实体及其属性;2)提供一种机制,以实现细粒度的控制访问[5],而不是简单的拒绝或授权.

XACML 的一些组件可以与 SAML 共享. 基本流程为访问主体请求策略执行点(PEP) 授权访问某一资源时,PEP 会创建一个 XACML 请求并发送到策略决策点(PDP) ,后者评估并返回一个响应. 该响应可以是允许访问,也可以是拒绝访问,并具有适当的义务.

PDP 评估请求并做出决策的过程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. 为了获得策略,PDP 要用到策略访问点(PAP) ,PAP 编写策略和策略集,供 PDP 使用. PDP 也可以调用策略信息点(PIP) 服务检索与主体、资源或者环境有关的属性值. PDP 做出的授权决策被发送到 PEP,PEP 履行义务,并根据 PDP 发送的授权决策允许或拒绝访问.

2 基于 SAML 和 XACML 实现安全的 SSO

基于 SAML 和 XACML 的 SSO 包括 3 个实体[6]. 分别是: 1) 用户代理(User Agent) ,用户访问资源的实体,通常为用户的浏览器; 2) 服务提供者(Service Provider,SP) ,是为用户提供某种服务的应用系统; 3) 身份提供者(Identity Provider,IDP) ,它为其他实体提供身份认证服务.

2.1 2 种典型的认证场景

2.1.1 Browser/Post 方式

Browser/Post 方式实现过程如图 3 所示: 1) 客户端请求服务提供方(SP) 的受保护的资源; 2) 由于用户未经认证,所以 SP 将用户重定向至 IDP 单点登录(SSO) 服务,并附带上 SP 对 IDP 的断言请求; 3) 用户向身份认证服务器(IDP) 请求单点登录服务,IDP 收到 SP 的断言请求,要求用户向认证服务器提交自己的身份凭证,这个凭证可以是用户名/密码或者证书等常见的身份认证方式; 4) IDP 返回认证结果,将对用户的断言包含在一个 HTML Form 中,返回给用户; 5) 用户请求 SP 的断言验证服务,确认自己的身份; 6) 如果验证通过,则 SP 为用户建立相应的会话,同时将用户再次重定向到请求的资源; 7) 用户再次请求 SP 受保护的资源; 8) 由于用户在 SP 已经经过认证,SP 直接返回给用户相应的资源.

2.1.2 Browser/Artifact 方式

Browser/Artifact 方式实现过程如图 4 所示: 1) 请求 SP 的受保护的资源; 2) SP 将向 IDP 发出 AuthnRequest 断言请求,要求 IDP 对用户身份进行断言,但是,SP 并不将实际的 AuthnRequest 内容发给 IDP,而是发布一个代表该请求的 Artifact,发送给 IDP 的单点登录服务(SSO) ; 3) 客户端请求 IDP 的单点登录(SSO) 服务,同时 IDP 会收到 SP 发出的代表断言请求的 Artifact; 4) IDP 的 SSO 服务请求 SP 的 Artifact 解析服务; 5) SP 的 Artifact 解析服务返回 AuthnRequest 全文; 6) SSO 服务验证客户身份,同时对该客户断言,同样,这里并不返回对客户的断言的实际内容,而是发布一个代表该 AuthnStatement 断言的 Artifact; 7) 客户端凭借该 Artifact 去访问 SP 的断言验证服务(ACS) ; 8) SP 请求 IDP 的 Artifact 解析服务,请求 Artifact 的全文; 9) IDP 的 Artifact 解析服务返回给 SP 断言 AuthnStatement 的全文,并且 SP 的断言验证服务对该断言进行验证,以证实用户的身份; 10) 如果验证通过,ACS 为客户建立相应的会话,并将用户重定向至当初请求的受保护的资源; 11) 用户

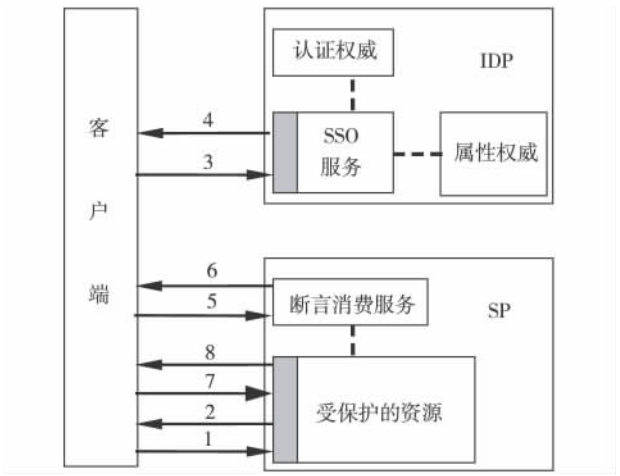

图 3 Browser/Post 方式
Fig. 3 Browser/Post style

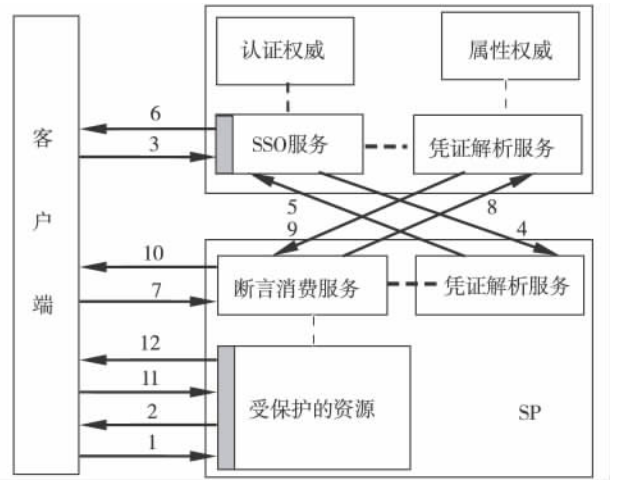

图 4 Browser/Artifact 方式
Fig. 4 Browser/Artifact style

再次请求受保护的资源;12) SP 直接返回给用户请求的资源.

2.2 基于 SAML 和 XACML 的单点登录模型

通过以上对 SAML 实现单点登录的典型模式的分析,以及 XACML 实现访问控制的策略的讨论,本文提出一个基于这 2 种技术的单点登录模型,SP 联合 IDP 实现基于 SAML 的单点登录,避免了具有相同角色的用户每次登录服务站点都需做身份认证,用 XACML 简化授权管理的复杂度并有效地进行访问控制. 为了有效地处理上下文信息,在 SP 端引入了"上下文控制器"模块,用于处理或发送请求以及协调系统的各个组件. 模型框架如图 5 所示.

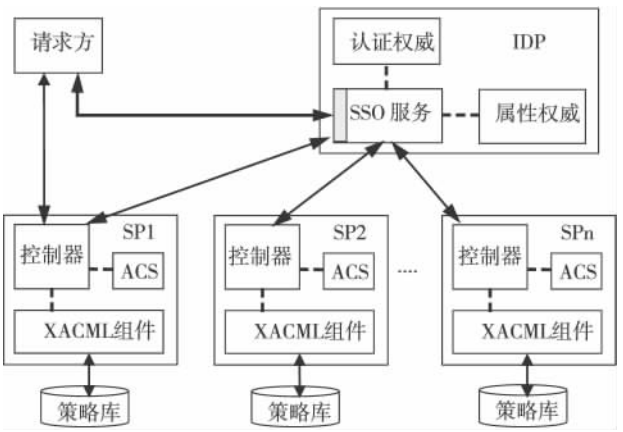

图 5 基于 SAML 和 XACML 的单点登录模型

Fig. 5 SSO model based on SAML & XACML

首先,用户对服务站点 SP1 提出访问请求,该请求被 SP1 的上下文控制器截获,由于是用户第 1 次访问,需要验证用户身份,于是将用户重定向至 IDP 进行身份验证,这其实就是一个单点登录的过程,这里可以使用上文中讨论过的 Pull 或者 Push 模式. IDP 通过认证权威验证用户的身份信息,并且通过属性权威获取用户的属性信息,同时对这 2 种信息进行断言,然后将对用户的认证以 SAML 断言的形式发送给 SP1. 上下文控制器收到该断言后交由断言验证服务(ACS)进行验证,上下文处理器再负责处理验证结果. 如果用户通过身份认证,并不能立即返回请求的资源,还需要对用户进行访问控制. 在这里上下文控制器还充当了策略执行点(PEP)的角色,它负责整理用户的身份信息、属性信息以及请求的资源信息,生成 XACML 请求,发送给 XACML 组件,请求授权决策. XACML 组件进行访问控制,负责动态地获取资源、环境以及策略信息,并进行策略评估,最后对访问请求做出判决,决定该用户是否可以调用此服务及访问受保护资源,然后上下文控制器(策略执行点)将提供用户请求的受保护的资源.

如果用户还需要访问其他的服务站点,同样首先要对用户身份进行认证,只不过不会再要求用户再次提供身份凭证,对用户的身份验证都在后台进行,对用户透明. 限于篇幅,这里就不再赘述详细的验证过程.

2.3 安全性分析

由于 SAML 在 2 个拥有共享用户的站点间建立了信任关系,所以安全性是需考虑的一个非常重要的因素. 基于 SAML 和 XACML 的单点登录系统在信息传递的过程中主要有以下风险[7].

1) 窃听. 断言和用户口令等信息在传输的过程中可能被窃听,解决的办法是用户与各 SP,IDP 之间以及 SP 与 IDP 之间均采用 SSL/TLS 加密.

2) 篡改断言. 这个风险可通过数字证书和数字签名解决. IDP 对于断言均用自己的私钥签名后才发出,接收方(SP)利用公钥验证签名. 数字签名可以确保断言的真实性和不可抵赖性.

3) 重放攻击. SAML 使用时间窗机制防止了这种形式的攻击. SAML 断言中包含的 NotBefore 和 NotOnOrAfter 属性指定了一个一定长度的时间窗,在时间窗之内断言有效,在时间窗之外,即使断言来源真实,该断言也是无效的,因为断言已经过期. 时间窗机制有效地防止了重放攻击.

另外,文献[8]提出了一种针对基于 SAML 的 SSO 的称为"最弱点攻击"的攻击方式. 这种攻击方式通过在客户端同时向不同的服务提供方(SP)的发出登录请求,这些服务提供方要求客户端不同程度的身份验证,例如一方只要求客户以用户名/密码方式验证,另一方则要求证书验证. 该攻击者没有证书,在 IDP 的验证显然会失败,但是基于用户名/密码的验证会成功,于是该攻击者可利用基于用户名/密码验证的成功响应去替代失败的响应,然后再发起重放攻击,从而达到一种类似于特权提升的效果. 不过这种攻击方式只要通过在 SAML 响应中指明身份认证主体验证方式,并且对该响应进行数字签名就可以避免.

3 模型的实现

基于以上提出的基于 SAML 和 XACML 的单点登录模型,本文在. NET 平台上实现了一个基于 B/S 结构的单点登录应用. 出于实验目的,整个系统由一

个认证服务器和一个应用服务器构成(实际应用中应包括所有参与单点登录过程的应用服务器).

3.1 基础框架

SAML2 规范的核心是其定义的断言的语义信息以及推荐的建立在具体协议之上的绑定方式. 为保证完全满足 SAML2 的 Schema 的完整性,利用 XML 架构定义工具(Xsd. exe)将所用的 Schema 自动生成了所有的公共语言运行库类,保证了所产生的 SAML 消息都是基于标准的 Schema 产生. 为方便应用的开发,本文定义了几个命名空间: Saml. Saml2、Saml. SamlHelper、XacmlComponent,提供诸如创建 SAML 断言、提取 SAML 断言、处理 SAML 断言、断言签名等常用功能. 在应用时,为了使用相应的逻辑功能需要引用对应的命名空间.

3.2 系统配置

为了模拟基于 SAML 和 XACML 的单点登录过程,本文开发了 2 个 WEB 应用: WebIdp 和 WebSp. 其中 WebIdp 为源站点,其身份为 Identity Provider; WebSp 为目标站点,其身份为 Service Provoder.

基于以上讨论的单点登录模型,为了保证断言传输的安全,需要在 WebIdp 和 WebSp 间启用 SSL 安全传输. 由于是在 WebSp 上的 acs 处认证断言,因此将 WebSp 上 acs 目录配置成要求安全通道(SSL),具体配置过程不再赘述.

为了保证断言的真实性和不可抵赖性,WebIdp 需要对其发布的断言签名,WebSp 验证签名. 为完成这个签名和验证的过程,需要生成不对称的密钥对,并加载进 WebIdp 和 WebSp 所在服务器的密钥库.

3.2 应用场景

在本应用场景中,用户 user@ nuist. edu. cn 请求 http: // localhost/samlsp/default. aspx,由于用户未经认证,WebSp 请求 WebIdp 的 SSOService 对该用户断言. WebIdp 响应断言的片段如下所示(限于篇幅,省略了部分标签和属性).

```
< Assertion Version = "2. 0" >
< Issuer > Idp < /Issuer >
< Subject >
< NameID NameQualifier = "www. idp. org" >
user@ nuist. edu. cn
< /NameID >
< SubjectConfirmation
Method = "urn: oasis: names: tc: SAML: 2. 0: cm: bearer" >
< /SubjectConfirmation >
< /Subject >
< Conditions
NotBefore = "2010-05-13T12: 43: 04. 484375Z"
NotOnOrAfter = " 2010-05-13T12: 48: 04. 484375Z" >
< /Conditions >
< AuthnStatement
AuthnInstance = "2010-05013T12: 43: 04. 484375Z" >
< AuthnContext >
< AuthnContextClassRef > … < /AuthnContextClassRef >
< /AuthnContext >
< /AuthnStatement >
< /Assertion >
```

从该断言中可以看到断言的发行者(Idp)、断言的主体(user@ nuist. edu. cn)、断言验证成功的条件(Conditions 标签)以及主体通过何种方式(Subject-Confirmation 标签)通过了验证等信息.

WebSp 收到该断言后则由 ACS(断言消费服务)验证断言,并将验证结果交给上下文控制器. 上下文处理器重新组装成请求信息并转发给 Xacml 组件(策略决策点),策略决策点从策略信息点中取得策略信息文件进行授权评估,判定用户有权访问所请求的文件,并向上下文处理器发回响应,该应用中的策略文件如下所示. 根据该策略文件,如果用户身份信息验证无误,将被授权访问请求的页面.

```
< Policy >
< Target >
< Subject >
< AttributeValue > user @ nuist. edu. cn < /AttributeValue >
< /Subject >
< Resource >
< AttributeValue >
http: // localhost/samlsp/default. aspx
< /AttributeValue >
< /Resource >
< /Target >
< Rule RuleId = "ReadRule" Effect = "Permit" >
< Target >
< Action > < AttributeValue > read < /AttributeValue > < /Action >
< /Target >
< /Rule >
< /Policy >
```

4 结束语

SAML 和 XACML 是基于 XML 的工业标准,结

合使用基于 SAML 的单点登录和基于 XACML 的访问控制将用户的认证和授权信息在多个应用程序之间安全交换,促进了不同安全系统之间的互操作性,并且提供了细粒度的访问控制. 在未来的研究中,将进一步完善其功能,同时消除该模型中可能存在的其他一些安全隐患.

参考文献

References

[1] 林满山,郭荷清. 单点登录技术的现状及发展[J]. 计算机应用,2004,24(增刊1):248-250
LIN Manshan, GUO Heqing. Status and development of SSO technology [J]. Computer Applications, 2004, 24(sup1): 248-250

[2] OASIS SSTC. Assertions and protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 [EB/OL]. (2005-03-15) [2010-08-18]. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[3] 陈丽娜,韩进,谢俊元. 基于信任管理的 SAML 授权模型[J]. 计算机工程与设计,2008,29(24):6275-6277
CHEN Lina, HAN Jin, XIE Junyuan. SAML authorization model based on trust management [J]. Computer Engineering and Design, 2008, 29(24): 6275-6277

[4] OASIS SSTC. eXtensible Access Control Markup Language (XACML) Version 2.0 [EB/OL]. (2005-02-01) [2010-08-18]. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[5] Manish Verma. Control information access with XACML [EB/OL]. (2004-10-18) [2010-08-18]. http://www.ibm.com/developerworks/xml/library/x-xacml

[6] 陈波,徐鲁强,张晓丹. 基于 SAML 的单点登录模型[J]. 兵工自动化,2007,26(2):56-57
CHEN Bo, XU Luqiang, ZHANG Xiaodan. Single sign-on model based on SAML [J]. Ordnance Industry Automation, 2007, 26(2): 56-57

[7] OASIS SSTC. Security and privacy considerations for the OASIS Security Assertion Markup Language (SAML) V2.0 [EB/OL]. (2005-03-15) [2010-08-18]. http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf

[8] Chan Y Y. Weakest link attack on Single Sign-On and its case in SAML V2.0 Web SSO [C] // LNCS 3982. Computational Science and its Applications-ICCSA 2006. Glasgow, UK, 2006-01-01. Berlin Heidelberg: Spring-Verlag, 2006, 3982: 507-516

[9] Jeong J, Shin D, Shin D. An XML-based security architecture for integrating single sign-on and rule-based access control in mobile and ubiquitous web environments [C] // LNCS 4278. On the Move to Meaningful Internet Systems 2006. Berlin Heidelberg: Spring-Verlag, 2006, 4278: 1357-1366

[10] 韩涛,郭荷清. 基于 XACML 的访问控制策略[J]. 计算机工程与设计,2006,27(12):2127-2129
HAN Tao, GUO Heqing. Access control policy based on XACML [J]. Computer Engineering and Design, 2006, 27(12): 2127-2129

[11] Verma M. Ensure portable trust with SAML [EB/OL]. (2004-03-23) [2010-08-18]. http://www.ibm.com/developerworks/library/x-seclay4/

[12] Hommel W. Using XACML for privacy control in SAML-Based identity federations [C] // LNCS 3677. 9th IFIP-TC6 TC11 International Conference on Communications and Multimedia Security (CMS 2005), Salzburg, Austria, 2005-01-01. Berlin Heidelberg: Spring-Verlag, 2005, 3677: 160-169

Application of SAML and XACML in Single Sign-On technology

WANG Qiang[1] FU Desheng[1]

1 School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044

Abstract Most applications in modern enterprises will provide a set of authentication method of their own, which increase the user's burden and reduce the system security as well. Another serious problem is how to administer access requests of authenticated users. The Single Sign-On (SSO) based on SAML and access control based on XACML can provide a solution for these two problems. Based on the analysis of SAML and XACML specifications, an SSO model based on SAML and XACML is proposed in this paper, and applied on the platform of Microsoft. NET. The model shares user information including ID authentication and access level, which promote interoperability between different security systems and guarantees access control as well. The security of the model is also analyzed.

Key words SSO; ID authentication; SAML; XACML