

文章编号:1001-9081(2005)11-2512-03

支持移动环境下信任迁移的设计

周 帆,余 堃,吴 跃

(电子科技大学 计算机科学与工程学院,四川 成都 610054)

(cdjianlibao@tom.com)

摘 要:在 SAML2.0 规范的基础上提出一种支持移动设备信任迁移的设计,规划出总体体系结构。在此基础上描述了整个系统运作流程,详细分析了潜在的安全性和部署等相关方面的问题,并提出了相应解决办法。

关键词:信任迁移;单点登录;安全断言标记语言;辅件

中图分类号: TN915.08 **文献标识码:** A

Scheme of supporting trust transfer in mobile environment

ZHOU Fan, SHE Kun, WU Yue

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan 610054, China)

Abstract: Based on SAML2.0 standard, a scheme of supporting trust transfer of mobile equipment was presented. The architecture and the flow of this system were described. Several problems and relative countermeasures about security and deployment were analyzed and proposed.

Key words: trust transfer; single sign-on; SAML(Security Assertion Markup Language); artifact

0 引言

长期以来,人们认识到需要提供一种机制在不同的协作域之间传递关于实体的信息,同时域又不失去对这些信息的所有权,交换的信息可以是关于主体或者验证信息的断言,这种方式也被称为单点登录。另外,如今从手机、PDA 或其他平台来存取网际网络的情况也越来越普及,因此以平台独立的方式来提供数字身份认证日益重要。比较著名的两种信任迁移方案是 Microsoft 的 Passport^[1] 和 SUN 倡导的“自由联盟”。Passport 内建于微软的产品与服务中(如微软网络、Hotmail、WebTV 等),是不开放的,且 Passport 采用中央统筹式的单一登录服务,不支持联邦式的网络服务架构。“自由联盟”的联盟身份管理^[2] 则致力于推动联合身份识别,提供可检视、管理和设定属于认证域和提供者的解释数据方式。安全断言标记语言(SAML)是完全基于 XML 的描述语言,因此具有 XML 良好的跨平台数据表示特性。设计 SAML 的目的是一是建立一种独立于协议和平台的验证和授权交换机制,另外就是使得使用者能够独立地部署环境,用于集中式、分布式以及联合式地部署场景。基于 Web 的方案如 Liberty Alliance, Shibboleth 等在一定程度上实现了基于 SAML 的认证和授权系统。如今,移动网络下的 Web Service 发展迅速, SAML 也被 OMA(Open Mobile Alliance)作为移动设备认证和授权的推荐方案,但是 OMA 和 SAML 都没有提供具体实现移动环境下认证迁移的方案细节。本文就此问题进行探讨,在基于 SAML2.0 规范的基础上提出了一种支持移动设备信任迁移的设计方案。对整个信任迁移流程进行分析,对涉及的

安全性问题进行说明,并解释部署等相关问题。

1 信任迁移与 SAML

网络环境下经常遇到需要提供个人信息的 Web 站点,以及验证或者通过个人首选项定制站点。最终,我们会发现在许多不同的地方有多个账户。如果每个站点都为此设立自己的用户资料库,结果就会造成对所有这些单独的站点都要考虑信息的安全,且多个站点不能协同为我们提供所感兴趣的更精细的服务。

SAML 被设计来解决这一问题,它允许只有少数经过选择的团体保留用户信息,并且如果需要,在得到允许之后这些团体可以与其他有关的团体共享这些信息。这意味着,我们的身份信息的安全地掌握在我们所信任的团体手中,并且可以访问一些供应商通过组织多种低层次服务所提供的高级服务。

此处介绍本文用到的关于 SAML 的部分重要概念:

断言(Assertion) 提供主体所执行的验证、主体属性、是否允许主体访问特定资源的授权决策等信息。SAML 定义了三种断言类型:认证断言,处理主体在特定时刻、特定机制下的身份验证;属性断言,提供联系特定属性与给定主体的一种机制;授权决策断言,管理主体访问资源的权限。

请求/响应协议(Request/Response Protocol) SAML 定义了用于获得断言的请求/响应协议。一个 SAML 请求用于获得一个断言;SAML 响应则根据请求回送相应的断言。

绑定(Binding) 详细说明了 SAML 协议与传输通信协议之间映射以及 SAML 消息与协议之间的绑定细节,目前 SAML 协议只支持 SOAP 绑定。

收稿日期:2005-07-05 基金项目:现代通信国家重点实验室基金项目(51436050203DZ0210)

作者简介:周帆(1981-),男,四川眉山人,硕士,主要研究方向:网络信息安全;余堃(1967-),男,四川成都人,教授,博士,主要研究方向:网络与信息安全、分布式计算、中间件技术、电子商务、电子政务;吴跃(1958-),男,上海人,教授,博士生导师,主要研究方向:数据挖掘、移动代理技术。

辅件(Artifact) 当权限请求对于 HTTP 重定向而言太长时,SAML 定义了一种辅件机制,用来实现对断言的引用。一个 SAML 辅件作为 URL 查询字符串的一部分带给服务提供站点,在返回给身份提供站点时用来明确地引用一个断言。

2 支持移动环境下信任迁移的设计

2.1 体系结构

无线环境下的单点登录与有线网络环境下有类似之处,但也有其特殊性,SAML 规范为移动网络环境应用定义了单独的标准。当用户的身份认证信息从无线的移动环境传送到有线的服务应用环境时,必须考虑以下几个问题:

1) 需要有能够在无线与有线环境之间传送信息的协议与设备;2) 用户身份认证信息在传送过程中的安全性与完整性;3) 系统必须能够正确处理用户在各个应用之间的身份信息。

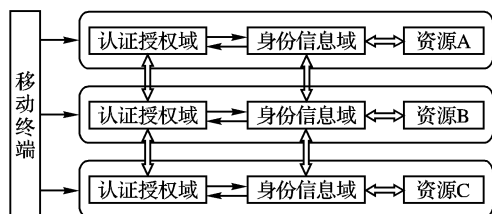


图1 支持移动设备信任的总体结构

认证授权域为对用户进行身份认证以及认证授权的系统;身份管理域为存储用户身份的数据库;资源包括用户需要访问的应用程序和设等各种资源。

站点 A、B、C 建立起彼此信任关系,能够共享用户信息;移动设备只要登录其中任意一个,则其他站点就与该设备自动建立起信任关系,以此种方式实现信任的迁移。

2.2 系统流程

考虑到移动设备运算能力不足等问题,在移动设备的认证过程中必须尽量减小其运算负荷。因此,我们采用让设备持有 artifact 的方式来引用断言。图2描述了依靠持有 artifact 来实现信任迁移的详细工作流程。

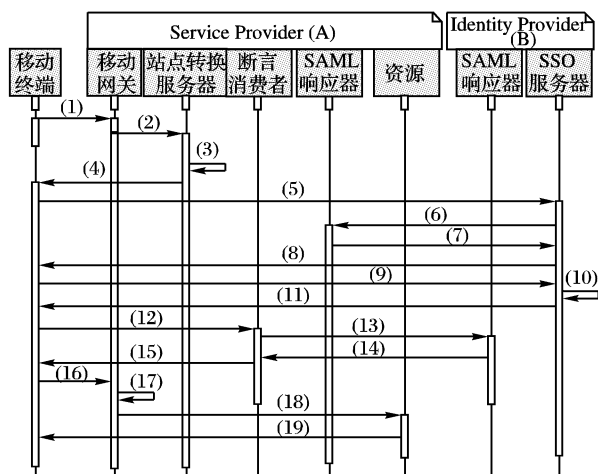


图2 信任迁移时序图

过程1 移动设备请求访问服务提供站点的资源

(1) 移动终端发送 HTTP 请求。(2) 网关将用户请求定向到站点交互转换服务器。请求中包含了 A 站点上的资源的 URL 地址,请求的形式如下:

<https://www.A.com:8080/InterSiteTransfer?TARGET=http://www.B.com/index.asp>

过程2 重定向移动设备到身份提供站点

(3) 产生 < AuthnRequest >^[5] 消息和一份 artifact。(4) 返回一份 HTML 表单,包含 artifact。(5) 发送包含 HTML 表单的 HTTP 消息。SSO 服务器(一般就是认证权威)从 SAML 辅件中解析出源 ID,此时,源 ID 和 A 站点上的 SAML 响应器之间的映射被建立起来。于是,断言消费者知道访问 URL 中所描述的服务提供站点上的 SAML 响应者。

过程3 身份提供站点的 SAML 请求

(6) 发送 SAML < ArtifactResolve >^[5] 消息,包含由站点交互转换服务器提供的 artifact。

过程4 服务提供站点的 SAML 响应

(7) 返回 SAML < ArtifactResponse >^[5] 消息,包含 < AuthnRequest > 消息。

过程5 身份验证

(8) 返回要求提供有效身份凭证的消息。(9) 提供有效的身份凭证。此时身份提供站点与用户的信任关系被建立起来。(10) 产生一份断言及一份 artifact。(与(3)类似,但不是同一份 artifact)。(11) 发送一份 HTML 表单,包含 SAML artifact。(12) 从 artifact 中解析出源 ID。此时,源 ID 和 B 站点上的 SAML 响应器之间的映射被建立起来。于是,断言消费者知道访问 URL 中描述的身份提供站点上的 SAML 响应者。

过程6 服务提供站点的 SAML 请求

(13) 断言消费者向身份提供站点上的 SAML 响应器发送一份 < ArtifactResolve > 消息,包含由 B 站点开始提供的 artifact(在第(10)步产生)。

过程7 身份提供站点的 SAML 响应

(14) 返回一份 < ArtifactResponse > 消息,包含了此前由 SSO 服务器产生的断言(第(10)步产生)。如果在此步中收到了一份有效的断言,则用户和服务提供站点之间的安全会话就被正式建立起来。

过程8 返回用户所请求资源

(15)~(19)断言消费者向浏览器发送一份请求目标资源的 HTTP 重定向消息,网关收到该消息后检查该 artifact 的完整性,如果断言正确,将资源返回给用户。

图2中服务提供站点是用户需要访问的资源所在地,也称为目的站点;身份提供站点是集中管理用户身份信息的用户信任站点,也称为源站点。服务提供者主要包括了移动网关、站点转换服务器(Intersite Transfer Service, ITS)、断言消费者、SAML 响应器和资源5个部分。其中,移动网关是服务站点的门户代理,主要负责检查到来的 HTTP 请求,并将请求定向到 ITS;ITS 是身份提供站点上所有组件的集中管理者,并能依据地址信息对消息进行转发;断言消费者负责处理断言,并能够从 artifact 中解析出对断言的引用;SAML 响应器(包括身份提供站点上的)是 SAML 消息的处理者,负责各种 SAML 消息的处理和转发;资源包括从设备到程序等各种用户需要访问和使用的数据信息。身份提供站点上的 SSO 服务器就是认证权威,负责管理用户身份信息并对用户产生断言。

当用户的身份信息在多个域之间切换时,并不需要用户干预,这为用户和管理者都带来了方便。所使用的认证方式可以是任何既有的认证方式,如:Password, Kerberos, X.509 证书,SSL/TSL 认证,以及基于 XML 的数字签名/加密等。

从上述过程中可以看到,涉及到签名、认证等复杂计算都是在有线网络下进行的,而移动设备只需要持有对断言的引用 artifact 和进行身份认证,就可以有效地克服移动设备运算能力不足带来的问题。

2.3 安全性

此处分析几种可能的安全性问题,并给出解决方案。

2.3.1 中间人攻击 (Man-in-the-Middle, MITM)

如果 MITM 依靠 DNS 欺骗控制了服务提供站点的站点交互转换服务器和移动终端,则 MITM 可以拦截所有服务提供站点与移动终端之间通信的消息。图 3 为 MITM 示意图。

MITM 转播请求,直到取得断言或者 artifact,并返回给终端一个伪造的,这样 MITM 可以窃取资源。图 3 中第(1*)步转发请求资源的 HTTP 请求;第(2*)步转发认证请求;第(5*)步转发身份信息,可能是断言或者 artifact;第(6*)步转发资源响应。

解决方案:最重要的是使用双向的强认证增大 MITM 插入会话的难度。但是,MITM 进行双向地转发并窃取返回的断言或断言句柄的可能性仍然存在。因此,应该使用保证机密性的方法来防止消息窃听,以及使用保证数据完整性的方法来阻止消息转发时任何改变数据的企图。如在 TLS/SSL 层使用适当的加密措施以及使用 X509v3 证书进行认证等。

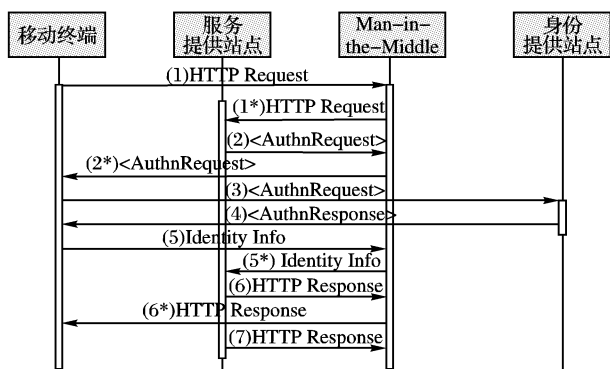


图 3 Man-in-the-Middle 示意图

2.3.2 重放攻击

攻击者截取数据并恶意地重复转发,一般作为伪装攻击的一个部分。因为攻击者在消息重放时并不需要了解消息内容,所以 XML 加密等方法并不能有效阻止重放攻击。

解决方案:最好的防治重放攻击的方法就是防治消息被截获。一些传输层的协议可以用来确保传输时的安全性,这可以有效防止重放攻击。例如,在 SAML 请求-响应会话时使用 HTTP/TLS 机制保证安全。另外,请求的时间标识和 ID 号可以帮助判断该请求是否是重放请求。

2.3.3 其他安全问题

其他可能的安全性问题,如:在主体到源站点认证的过程中是使用重复的认证信息,那么窃取认证信息将使攻击人可能模仿主体进行攻击;当认证断言包含了断言传输者的认证协议标识符时,窃取 artifact 将使攻击人可以冒充主体进行攻击;在信任迁移过程中还有诸如消息的删除、插入和篡改等可能。以下是应该采取的安全措施:

1) 目的站点在与主体浏览其连接时实行安全保护;对源站点和目的站点的传输进行安全保护;主体或目的站点应确保源站点在与主体进行连接时实行了安全保护;

2) 目的站点验证主体浏览器是被源站点直接定向的,且

源站点应是直接认证主体的;

3) 源站点拒绝多于一个的请求访问同一个断言,以断言 ID 来保证断言 ID 的唯一性;

4) 如果断言包含了识别特殊域的元素时,目的站点需要确定其是否为该域的成员;

5) 目的站点在与源站点进行通信时,始终检查源站点身份,确定是期望的源站点。

3 部署相关问题

为了保证用户认证信息的保密性与完整性,在信息传递过程中必须对该信息进行数字签名与加密。然而对于一般的无线移动设备,如手机,由于其处理器速度和存储容量相对于 PC 机来说都很有限,签名与加密操作是非常复杂的操作,出于降低减轻无线设备运算负荷的考虑应将这些操作交由有线网络中的计算机来完成。

SAML 标准规定了用户身份认证是通过 SAML 认证权威产生的认证断言信息来指明用户身份的。但若将断言进行加密签名后直接发送至移动设备,由于断言的复杂性,同样会给处理和存储能力都很有限的移动终端带来很大的负担。应该采用辅件来引用断言和指示源 ID。任何应用在得到辅件后,根据源 ID 找到断言所在地,然后根据断言引用找到相应断言,从而完成用户身份认证。而且既有的移动网络为基于 SAML 的信任迁移服务提供了较好的支持:

部署 artifact 模式兼容 WAP1. X 和 2.0,这意味着不需要为此安装新的支持软件和硬件。

安全性 在传输层上,在移动设备和服务提供者之间的加密连接并未获得 WAP1. X 协议的支持,而 WAP2.0 引入 TLS 来支持此连接安全。

SIM 卡支持 基于 GSM 的网络使用 SIM 卡,而 SIM 卡可以为基于身份的事务处理提供较强的安全保证。

漫游支持 移动设备漫游业务已经建立起了较好的在既有网络之间进行的用户信息迁移,这为基于 SAML 的信任迁移提供了最重要的基础设施支持。

参考文献:

- [1] Microsoft. net passport review guide [EB/OL]. http://www.microsoft.com/net/services/passport/review_guide.asp, 2004-01.
- [2] Liberty ID-WSF - a Web Services Framework [EB/OL]. <http://www.projectliberty.org/about/whitepapers.php>, 2004-05.
- [3] DIERKS T, ALLEN C. RFC 2246, The TLS protocol [S], 1999.
- [4] Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0 [S/OL]. <http://docs.oasis-open.org/security/saml/v2.0/>, 2005-03.
- [5] BHANSALI BB. Man-in-the-middle attack - a brief [Z]. SANS Institute, 2001.
- [6] ROUAULT J, WASON T. Liberty bindings and profiles specification [S/OL]. <http://projectliberty.org/specs/liberty-architecture-bindings-profiles-v.1.pdf>, 2003.
- [7] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 [S/OL]. <http://docs.oasis-open.org/security/saml/v2.0/>, 2005-03.
- [8] OMA Web Services Enabler (OWSER): Core Specifications Draft Version 1.0 [S/OL]. http://member.openmobilealliance.org/ftp/public_documents/mws, 2003.