基于 SAML 与 XKMS 的安全单点登录认证模型的研究与实现 *

陈天玉[1], 谢冬青[1,2], 杨小红[1], 杨海涛[1]
(1. 湖南大学 软件学院, 长沙 410082; 2. 广州大学 计算机科学与教育软件学院, 广州 510006)

摘 要: 针对 Browser/Artifact 方式进行单点登录时存在的安全性问题,设计出一种基于 SAML 与 XKMS 的安全单点登录认证模型。它采用一种结合传统 PKI 与 XML 密钥管理规范(XKMS)的统一密钥管理子层来提供密钥管理,使用 XML 数字签名和加密技术来保证 SAML 声明传递的安全性。通过在 J2EE 平台上实现,证明了该模型可以很好地解决 Browser/Artifact 方式传递 SAML 声明存在的安全性问题。

关键词: 单点登录; 安全声明标记语言; XML 密钥管理规范; XML 数字签名; XML 加密; Web 服务
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2010)03-1019-03
doi:10.3969/j.issn.1001-3695.2010.03.058

Research and implementation of security SSO authentication model based on SAML and XKMS

CHEN Tian-yu[1], XIE Dong-qing[1,2], YANG Xiao-hong[1], YANG Hai-tao[1]
(1. *College of Software, Hunan University, Changsha* 410082, *China*; 2. *School of Computer Science & Educational Software, Guangzhou University, Guangzhou* 510006, *China*)

Abstract: For the security problem existing in the process of SSO which used Browser/Artifact mode, this paper designed a security SSO authentication model based on SAML and XKMS. It used a key management layer which combined traditional PKI with XKMS to provide the key management service, at the same time, this model applied XML digital signature technology and XML encryption technology to ensure the security of sending SAML statement message. Through the implementation on the platform of J2EE, the result proves that the security SSO model can be a very good solution to the security problem in the delivery of SAML statement by Browser/Artifact mode.

Key words: SSO; SAML; XKMS; XML digital signature; XML encryption; Web service

随着企业信息化进程的不断深化、电子商务的不断发展,人们在企业活动中需要接触的应用系统越来越多。这些系统各自维护着不同的安全策略,使用独立的认证授权体系,用户被迫保持多个身份,从而导致孤立的业务关系和用户体验。消除这种访问孤立的关键是建立一种联合身份。建立联合身份、实现联合商务需要实施一种标准化的、跨管理域的、基于 Web 架构的通用技术。单点登录就是一个 Web 服务用来向另一个 Web 服务传达有关用户认证信息的技术。安全声明标记语言 SAML 通过定义联合识别、验证和授权的基本形式为单点登录的实现提供了技术框架[1~3]。但是 SAML 对于自身的安全性问题却没有相关的解决方案,本文主要通过结合 XKMS 和 XML 数字签名和加密来解决 SAML 声明传递的安全性问题。

1 SAML 技术

1.1 SAML 介绍

SAML 是由 OASIS 组织高级结构化信息标准组织批准,基于 XML 语言的,用于在多个信任合作者之间传输认证和授权信息的安全访问控制框架体系和协议[1]。SAML 的核心是声明,目前共定义了三种声明:认证声明,定义了用户的认证信息;属性声明,定义了相关的属性信息;授权声明,定义了对特定资源的授权信息。SAML 还定义了一组 XML 格式的请求/应答消息。三种声明可以嵌入请求/应答消息中进行传递[1~3]。

SAML 提供了 Artifact 和 Post 两种基于浏览器的方式来传递声明消息[1,2]。Browser/Artifact 提供的是一种由目的站点从源站点 pull 的声明获取方式。Post 方式提供的是一种由源站点从目的站点 push 的声明获取方式。由于目前业界主要使用的是 Browser/Artifact 方式[1,2],本文主要介绍这种获取声明的方式。

1.2 Browser/Artifact 方式

Browser/Artifact 方式认证的具体过程如图 1 所示。

1)用户 U 向 IDP(认证服务提供商)发送认证请求,要求访问 IDP,U 和 IDP 之间的消息传递不包含认证信息的消息传递。

收稿日期: 2009-07-04; **修回日期**: 2009-08-17 **基金项目**: 国家自然科学基金资助项目(60673156);国家教育部科学技术研究重点基金资助项目(105129)

作者简介:陈天玉(1984-),男,硕士研究生,主要研究方向为信息安全(chentianyu8424@126.com); 谢冬青(1965-),男,教授,博导,主要研究方向为算法分析与设计、信息安全; 杨小红(1982-),女, 硕士研究生,主要研究方向为网络安全、分布式计算;杨海涛 (1983-),男, 硕士,主要研究方向为信息安全.

2)IDP 通过对 U 认证后,生成一个认证声明,同时建立对应的 SAML Artifact,然后将此 Artifact 返回给用户。

3)用户被重定向到 SP(服务提供商),与 SP 建立连接,并将 Artifact 传递给 SP。

4)SP 根据 Artifact 查询 IDP。

5)IDP 根据对应关系将声明返回 SP,并删除声明与 Artifact 之间的对应关系。

6)SP 通过声明判断用户身份,如是合法用户则将页面返回给用户;如是非法用户则返回错误信息。

1.3 Browser/Artifact 安全性分析

1)截取 SAML Artifact 和声明 攻击者作为代理人,在用户 U 与 IDP 或 IDP 与 SP 之间的通信中冒充其中一方,实现欺骗。在此过程中,攻击者可以轻松获取用户、IDP 和 SP 之间的所有数据,包括 SAML Artifact 和 SAML 声明[2,4]。

2)拒绝服务攻击 SAML 协议比较容易遭受拒绝服务 DoS 攻击。这是因为服务器端处理一个 SAML 请求时,首先需要从请求信息的 XML DOM 树中提取相关信息,然后从数据库或文件中查询相应请求数据的结果来构造应答消息,这需要花费很多时间。而客户端构造请求消息却简单得多。这使得攻击者可重复发送请求消息,从而造成服务器拥塞、崩溃,使正常的请求服务无法进行[2,4]。

3)窜改消息 中间人截取 SAML Artifact 或者 SAML 声明后,可以窜改其中的内容。

4)重放攻击 攻击者冒充用户不断发送重复的应答消息达到重放攻击目的。

随着单点登录技术的发展快速,传统的安全保护技术方法已经不能胜任,如何传递安全可信 SAML 声明成为单点登录中必须解决的关键问题。由于 SAML 声明是基于 XML 的,自然而然会想到使用基于 XML 数字的签名[5,6]和加密[6]来解决 SAML 声明安全性问题。XML 数字签名以保证发送方身份的确认性和不可抵赖性,以保护数据的完整性。XML 的加密方法是为了保证数据的私密性。关于 XML 签名和加密将在接下来部分详细介绍。

2 XML 数字签名和加密

2.1 XML 数字签名

XML 数字签名是一种安全协议,其目的是为了保护数据的完整性,采用公共密钥机制(PKI),通过私钥加密消息摘要实现数字签名,通过公钥解密验证数字签名[5~7]。

2.2 XML 加密

XML 加密采用了对称算法和非对称算法,前者用于 XML 数据元素的批量加密,后者用于交换对称密钥[6]。但是数字签名和加密时用的密钥要依赖于 PKI,而 PKI 的实现比较复杂。为了解决这个问题,这里提出了一种新的替代方案,即 XKMS。XKMS 为访问和集成公钥 PKI 拟出了一种容易的机制。

3 XKMS

3.1 XKMS 两种规范

XKMS 规范由两个规范组成,其中一个规范与公钥的注册有关,即 XML 密钥注册服务规范(XML key registration service specification,XKRSS)。这一部分为将密钥对注册到服务提供程序提供机制。另一个规范关心的是基于密钥信息的信息检索,即 XML 密钥信息服务规范(XML key information service specification,XKISS)[8]。这一部分为允许客户机应用程序认证经过加密/签名的数据提供机制。

3.2 基于 XKMS 的密钥管理子层描述

传统 PKI 有着完善的功能和结构,但是其部署十分繁琐,文中给出了一个基于 XKMS 的密钥管理层,将 XML 与传统 PKI 进行了结合,很好地屏蔽了传统 PKI 部署的复杂性,使用户不必理解复杂的 PKI 体系结构,方便地使用 PKI 提供的密钥服务。基于 XKMS 的密钥管理层结构如图 2 所示。

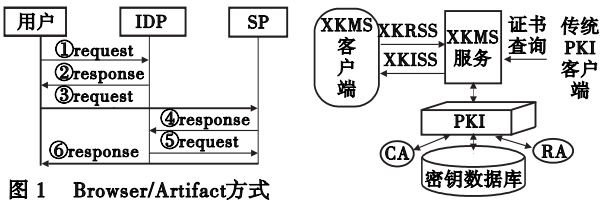

图 1 Browser/Artifact方式单点登录过程

图2 基于XKMS的密钥管理层

对于 XKMS 的客户端来说,若客户端是一个密钥的所有者,那么它可以通过 XKRSS 向 XKMS 服务提供商注册它的密钥,而 XKMS 服务器则利用一个底层的 PKI 来保存和绑定密钥。在整个安全 Web 服务调用过程中,基于 XKMS 的管理层都将提供密钥管理服务,Web 服务调用端在对 Web 服务的安全调用之前必须将生成的密钥对注册到 XKMS 服务,Web 服务提供者在验证调用者签名之前必须先到 XKMS 服务对调用者提供的公钥信息进行有效性验证。服务调用者和提供者可能在同一个 XKMS 服务安全域内,也可能在不同的 XKMS 服务安全域内[8]。

4 安全单点登录认证模型的提出与实现

根据前文的分析,本章提出了一种结合 XML 数字签名、加密技术以及 XKMS 系统来保证 SAML 声明和 Artifact 的安全传递的安全单点登录模型。该模型中使用 XML 数字签名技术让发送方提供 SAML 消息签名,保证数据的完整性[5~7],同时使用 XML 加密技术来加密 SAML Artifact 和 SAML 声明,保证消息私密性[6],为了保证 XML 签名加密过程中密钥的安全性,使用 XKMS 来管理密钥[8]。SAML Artifact 传递的安全性和声明传递的安全性都可以通过这种模型来解决。下面以解决 SAML 声明传递的安全性为例来详细分析这种单点登录认证模型的签名和加密过程。接下来会详细分析整个单点登录过程。以下的发送方为 IDP,接收方为 SP,具体说明请参考图 1。

4.1 发送方生成 SAML 数字签名过程

1)发送方生成 RSA 密钥对,公钥和私钥 其中公钥在 XMKS 服务注册处进行注册,私钥用来生成 SAML 数字签名;

2)发送方的原始消息经过 SHA-1 生成散列消息;

3)利用 RSA 私钥和生成的散列消息生成 SAML 数字签名;

4)公钥、原始消息和 SAML 数字签名组成签名消息。

4.2 发送方加密 SAML 声明过程

1)接收方首先产生非对称密钥,公钥和私钥,把公钥在 XKMS 服务处注册,然后发送给发送方;

2)发送方收到公钥后到 XKMS 服务处进行验证;

3)验证成功后生成一对对称密钥;

4)利用对称密钥加密需要加密的 SAML 消息;

5)用接收方的公钥加密对称密钥;

6)把加密后的 SAML 声明和加密后的公钥组成加密消息。

签名消息和加密消息嵌入 SOAP 头部发送给接收方。

发送方生成 SAML 签名和加密 SAML 声明的详细过程如图 3 所示。

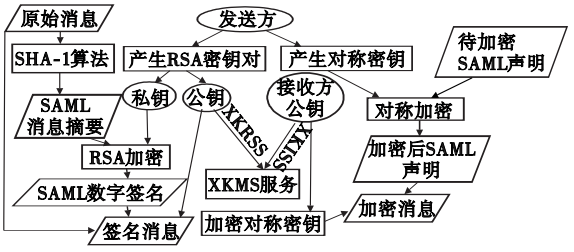

图3　发送方生成SAML数字签名和加密SAML声明过程

4.3　接收方验证 SAML 数字签名过程

1)接收方收到 SAML 签名消息和加密的 SAML 声明消息,首先验证数字签名,验证通过才继续解密加密的声明消息;

2)利用 SAML 签名消息中的原始消息进行 SHA-1 散列得到散列消息;

3)到 XKMS 服务处通过 XKISS 验证发送方发过来的公钥;

4)验证通过后用该公钥解密 SAML 数字签名得到散列消息;

5)匹配生成的散列消息和解密后的散列消息;

6)若匹配则说明数据是完整的,没有窜改,否则就直接结束,解密过程不再进行。

4.4　接收方解密 SAML 声明过程

1)签名验证通过后用自己的私钥解密发过来的对称密钥;

2)用对称密钥解密 SAML 加密声明得到 SAML 原始声明。

接收方验证 SAML 签名和解密 SAML 声明消息如图 4 所示。

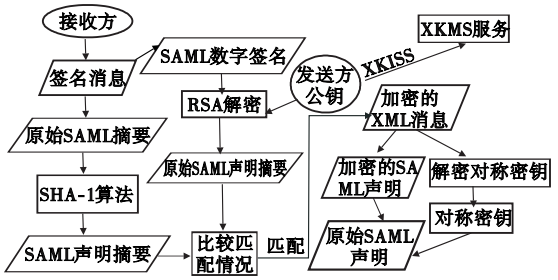

图4　接收方验证SAML签名和解密SAML声明过程

4.5　认证模型的实现

整个单点登录模型主要由五个部分组成,即身份认证服务、SAML 响应服务、XKMS 服务、XML 数字签名和加密、单点登录管理模块。其中前三个都是 Web service。整个系统以 J2EE 为开发平台,以 TOMCAT 作为 Web 容器,AXIS 作为 SOAP 引擎[9]。改进后的 Browser/Artifact 方式单点登录认证流程如图 5 所示。

1)用户 U 向 IDP(认证服务提供商)发送认证请求,要求访问 IDP,U 和 IDP 之间的消息传递不包含认证信息;

2)IDP 通过对 U 认证后,生成一个认证声明,同时建立对应的 SAML Artifact,然后将此 Artifact 加密同时生成一个签名返回给用户;

3)用户重定向 XKMS 服务处验证密钥;

4)XKMS 服务返回验证消息;

5)用户确认 Artifact 后重定向到 SP,与 SP 建立连接,并将重新加密的 Artifact 和签名后传递给 SP;

6)SP 到 XKMS 服务处验证密钥;

7)XKMS 服务返回验证消息;

8)SP 确认 Artifact 后建立了一条到 IDP 的安全通道,重新加密 Artifact 并生成签名发给 IDP 查询声明;

9)IDP 到 XKMS 服务处验证密钥;

10)XKMS 服务返回验证消息;

11)IDP 确认 Artifact 后根据对应关系将声明加密,同时生成签名返回 SP,并删除声明与 Artifact 之间的对应关系;

12)SP 验证通过后通过声明判断用户身份,如是合法用户则将页面返回给用户;如是非法用户则返回错误信息。

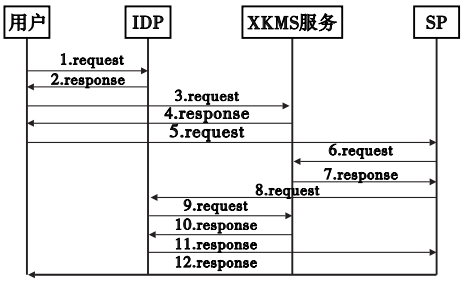

图5　基于SAML和XKMS的安全单点登录认证流程图

表 1　单点登录认证模块

模块	核心程序名称	实现功能及说明
身份认证服务	login( )	验证用户名和密码 类:UserService. java
SAML 响应	makeSaml( )	产生 SAML 声明,并返回 Artifact
服务	appendArtifact( )	在目标 Web 服务资源 URL 上附加 Artifact
	samlReceive( )	接收目标站点的 SAML 请求,提取 Artifact 信息
	assertRetrival( )	通过 Aritifact 检索对应 SAML 声明
	samlResponse( )	发送 SAML 声明 类:SamlService. java
XKMS 服务	xkrss( )	注册密钥
	xkiss( )	验证密钥 类:XkmsService. java
XML 数字签名和加密	smlSignature( )	产生 XML 数字签名
	xmlValidate( )	验证 XML 数字签名
	xmlEncrypt( )	加密 XML 文档
	xmlDecrypt( )	解密 XML 文档 说明:java se6 xml api
单点登录管理模块	artifactReceive( )	获取用户的 Artifact
	samlRequest( )	向源发送身份验证请示
	assertReceive( )	验证 SAML 声明并授权

4.6　新型单点登录认证模型与传统模型的比较

新型单点登录认证模型在原有模型的基础上,引入了 XML 数字签名和加密技术来保证声明的安全传递,同时引入 XKMS 密钥管理子系统来提供密钥管理服务。对于第 1 章提到的使用 Browser/Artifact 方式来传递 SAML 声明时存在的安全性问题都可以使用这种新型模型来解决。对于安全问题 1)截取 SAML Artifact 和声明,在新型模型中可以采用 XML 加密保证端到端安全,防止中间人攻击,同时可以使用时间戳来保证不接受过期的声明。对于安全问题 2)拒绝服务攻击,在新型模型中可以使用 XML 数字签名来解决。要求发送方进行数字签名,这样发送请求消息的难度增加,从而减少发送与接收消息时发送端与接收端工作量的不对称性,减少受到拒绝服务攻击的可能。对于安全问题 3)窜改消息,在新型模型中也可以使用 XML 签名来保证数据的完整性。对于安全问题 4)重放攻击,则可以使用时间戳保证数据的

(下转第 1025 页)

问及 CT 的解密询问。

Guess:最后,A 输出对 b 的猜测 b'。如果 $b=b'$,则B 输出 1,表示 $T=e(g,h)^{\alpha^{l+1}}$;否则,B 输出 0,表示 T 是 G_T 中一随机元素。因此,如果存在一个敌手以不可忽略的概率进行 CCA 攻击,那么就存在一个算法可以不可忽略的概率解决 DBDHE 问题,而这与 DBDHE 是一个困难问题相矛盾,故方案是 IND-sID-CCA 安全的。

3.4　方案效率

由于双线性对计算所花费的计算成本远高于元素的点乘运算和指数运算,只考虑双线性对的计算成本。文献[12,14]的签密和解密阶段所需的双线性对计算分别为 $n+2$ 和 3 及 1 和 2,密文长度分别为 $2n+3$ 及 $n+4$。在本方案中,签密和解密阶段分别需要计算 1 和 2 次,而密文长度为 5,因此方案具有较高的效率。

4　结束语

本文提出了一个密文长度固定的基于身份环签密方案。方案中无须借助随机预言机,在标准模型下可证明它是安全的。与现有的环签密方案相比,本方案中密文的长度固定,不随环的线性增长而增长,具有较高的效率。利用 DBDHE 问题和 DHI 问题的困难性,分别对方案的不可区分性和不可伪造性进行了安全性证明,并进行了相应的概率分析和时间复杂度分析。

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Proc of CRYPTO 1984. New York: Springer-Verlag, 1985: 47-53.

[2] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairin[C]//Proc of CRYPTO. Berlin: Springer, 2001: 213-229.

[3] BONEH D, BOYEN X. Efficient selective-id secure identity based encryption without random oracles[C]//Proc of EUROCRYPT. Berlin: Springer-Verlag, 2004: 223-238.

[4] BONEH D, BOYEN X. Secure identity based encryption without random oracles[C]//Proc of CRYPTO. Berlin: Springer-Verlag, 2004: 443-459.

[5] GENTRY C. Practical identity-based encryption without random oracles[C]//Proc of EUROCRYPT. Berlin: Springer-Verlag, 2006: 445-464.

[6] PATERSON K G, SCHULDT J C N. Efficient identity-based signatures secure in the standard model[C]//Proc of ACISP. Berlin: Springer-Verlag, 2006: 207-222.

[7] REN Yan-li, GU Da-wu. Efficient hierarchical identity based signature scheme in the standard model[J]. Wuhan University Journal of Natural Sciences, 2008, 13(6): 665-669.

[8] ZHENG Yu-liang. Digital signcryption or how to achieve cost(signature & encryption) < < cost(signature) + cost(encryption)[C]// Proc of Advances in CRYPTOLOGY-CRYPTO. London: Springer-Verlag, 1997: 165-179.

[9] BAEK J, STEINFLD R, ZHENG Yu-liang. Formal proofs for the security of signcryption[C]//Proc of PKC. London: Springer-Verlag, 2002: 363-366.

[10] MALONE-LEE J. Identity-based signcryption [J/OL]. (2002). [2009-06-15]. http://eprint.iacr.org/.

[11] LIBERT B, QUISQUATER J J. New identity based signcryption schemes from pairings[EB/OL]. (2003). [2009-06-15]. http://eprint.iacr.org/.

[12] HUANG Xin-yi, SUSILO W, MU Yi, *et al*. Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world[C]//Proc of Advanced Information Networking and Application. 2005: 649-654.

[13] ZHANG Ming-wu, YANG Bo, ZHU Shen-lin, *et al*. Efficient secret authenticatable anonymous signcryption scheme with identity privacy [C]//Proc of PAISI. Berlin: Springer-Verlag, 2008: 126-137.

[14] ZHU Zhen-chao, ZHANG Yu-qing, WANG Feng-jiao. An efficient and provable secure identity-based ring signcryption scheme [EB/OL]. [2009-06-15]. http://dx.doi.org/10.1016/j.csi.

(上接第 1021 页)实时性。该新型模型增强了 Browser/Artifact 方式传递 SAML 声明的安全性,同时实现起来也并不复杂。

5　结束语

文中针对 Browser/Artifact 方式传递 SAML 声明过程中存在的安全性问题,介绍和研究了 XML 数字签名和加密以及 XKMS 技术,并且提出 XKMS 密钥管理子层模型。文中最后结合 SAML、XKMS 、XML 签名和加密设计出一种新型的安全的单点登录认证模型,该安全模型很好地解决了 Web 服务环境下 SAML 声明传递的安全性问题,为实施安全单点登录应用提供了一个有效的解决方案。

下一步,笔者将研究在该单点登录认证模型的基础上结合 LDAP(轻量级目录服务协议),实现用户的统一管理和认证,为大规模的系统集成应用中的安全身份认证提供支持。

参考文献:

[1] OASIS Final SAML v2.0 OASIS standard project[EB/OL]. [2005-03-15]. http://www.peoject.org/.

[2] THOMAS Gro (β). Security analysis of the SAML single sign-on browser/artifact profile[C]//Proc of the 19th Annual Computer Security Applications Conference. Washington DC: IEEE Computer Society, 2003.

[3] FUGKEAW S, MANPANPANICH P, JUNTAPREMJITT S. Adding SAML to two-factor authentication and single sign-on model for dynamic access control[J]. Communications & Signal Processing, 2007, 6(10): 1-5.

[4] 王秀毅,王凌燕,韩继红,等. 一种 SAML 单点登录实现方式的安全性研究[J]. 微计算机信息, 2007, 23 (8): 81-83.

[5] XML signature[EB/OL]. [2005-05]. http://www.w3.org/2005-05.

[6] 刘小览,许敏佳. 基于 XML 的网络安全技术[J]. 计算机工程, 2006, 32(2): 164-166.

[7] 车葵,邢书涛,牛晓太. 基于 XML 的数字签名技术研究与实现[J]. 计算机工程与设计, 2008, 29(23): 6171-6174.

[8] 陈莉,张浩军,祝跃飞. 基于 XKMS 的三层网络结构的 PKI 系统模型[J]. 计算机工程与应用, 2006, 42(14): 68-71.

[9] 张艳,周明天,佘垄. 基于 Web services 的 XML 引擎安全模型研究[J]. 计算机应用研究, 2008, 25(7): 2162-2164.