一种基于双令牌机制的单点登录模型研究

嵇智辉[1,2],倪 宏[2],刘 磊[1,2],匡振国[1,2]
JI Zhi-hui[1,2],NI Hong[2],LIU Lei[1,2],KUANG Zhen-guo[1,2]

1.中国科学院 研究生院,北京 100039
2.中国科学院 声学研究所 国家网络新媒体工程技术研究中心,北京 100080
1.Graduate University of Chinese Academy of Sciences,Beijing 100039,China
2.National Network New Media Engineering Research Center,Institute of Acoustics,Chinese Academy of Sciences,Beijing 100080,China
E-mail:jizh@dsp.ac.cn

JI Zhi-hui,NI Hong,LIU Lei,et al.Research of single sign-on model based on dual-token mechanism.Computer Engineering and Applications,2008,44(30):131-134.

Abstract: Single sign-on is techniques which can overcome disadvantages of traditional authentication mechanism in service integration process,and is also a key issue must be investigate in multi-service operation system.After comparing many single sign-on schemes,especially the scheme based on SAML model,provides a single sign-on model based on dual-token mechanism.Besides SAML token,the model introduces session key and session token,and uses local session dynamic active algorithm,meets the demands in security and efficiency.

Key words: single sign-on;security assertion markup language;SAML token;session key;session token;dynamic active algorithm

摘 要:单点登录技术克服了业务整合过程中传统认证机制不足,是多业务运营平台需要重点研究的问题之一。对多种单点登录解决方案进行比较,重点分析安全断言标记语言(SAML)模型,提出一种基于双令牌机制的改进单点登录模型。模型在应用SAML令牌作为用户身份载体基础上,引入会话密钥和会话令牌,并采用本地会话缓存周期动态激活算法,满足了运营平台对认证授权体系整体安全性和处理效率等方面的要求。

关键词:单点登录;安全断言标记语言;SAML令牌;会话密钥;会话令牌;动态激活算法
DOI:10.3778/j.issn.1002-8331.2008.30.040 **文章编号:**1002-8331(2008)30-0131-04 **文献标识码:**A **中图分类号:**TP309

1 引言

随着信息化进程的逐步深化和用户对网络信息服务需求的不断增长，多业务运营平台中包含的应用服务系统越来越多。这些应用系统通常由不同的组织开发,具有各自的用户管理体系,用户在各个应用系统中保持各自的身份,在使用各应用服务前都需要按照相应的系统身份登录,降低了访问操作的便利性;同时,应用系统具有独立认证授权体系和安全管理策略,带来较高的平台管理与维护成本。用户登录应用系统的繁琐性以及平台认证授权体系的复杂性,使得用户身份信息在网络传输过程中受到非法截获和破坏的可能性随之增大,并导致平台扩展能力下降,整体安全性降低,管理和维护成本非线性增加。为提升用户体验,提高多业务运营平台整体性能,需要对认证授权进行统一管理,实现用户认证信息在应用系统间的传递和共享。

单点登录正是实现业务整合、增强系统可用性的关键解决方案,它将用户认证功能独立为一种基础性服务,并利用信任关系的移植,使用户只需要采用统一的登录验证系统完成一次登录认证,即可访问所有相互信任的应用系统,只有超越信任关系范围才需要再次登录。单点登录机制对认证授权体系和安全策略进行统一管理,保证了用户信息在多业务运营平台中的一致性，实现了用户在平台各个应用系统间自由切换和穿梭,提升了用户操作的便利性和系统平台的整体安全性。

2 传统单点登录方案分析

当前存在多种单点登录解决方案,各种方案实现方式差异较大。有些方案采用Cookie记录并携带认证信息;有些方案通过Session共享认证信息;还有方案采用Kerberos或PKI作为认证机制,利用服务票据或数字证书实现信任关系的移植。这些方案在各自应用环境中有着自身的优越性，但是没有标准安全信息交互格式实现方案间的互通，因此在组合不同组织提供的产品时,存在可行性和实用性等方面的问题。对此,结构信息标准化促进组织(OASIS)提出了基于SAML[1]的单点登录解决方案。

2.1 SAML方案

SAML,安全断言标记语言,是基于XML的安全标准,用于

基金项目:国家科技支撑计划项目(National Key Technology R&D Program under Grant No.2006BAH02A22)。
作者简介:嵇智辉(1979-),男,博士研究生,主要从事宽带网络通信、电信运营支撑管理等方面的研究;倪宏(1964-),男,研究员,博士生导师,主要研究方向包括多媒体技术、宽带网络通信、嵌入式系统等;刘磊,男,博士研究生;匡振国,男,博士研究生。
收稿日期:2007-11-28 **修回日期:**2008-01-04

在 Internet 不同安全域中交换身份验证和授权凭证，可令不同类型的安全服务系统间实现交互。基于 SAML 的单点登录解决方案在 SAML 框架下建立一个安全协同工作体系环境，环境中每个应用系统都可以为用户身份验证和授权建立各自的策略，只要满足 SAML 定义的接口、信息交互格式和流程规范，相互间就可以无缝结合，进而实现安全的授权、认证和信息交换。SAML 通过断言[1]实现登录和授权信息交互。SAML 断言是对主体身份和权限等信息的描述集合，可传递主体执行的认证信息、属性信息和主体访问资源的授权决定。SAML 包括认证、属性和授权三种安全断言，认证断言声称主体已经通过认证；属性断言描述主体和授权相关的属性；授权断言提供主体访问特定资源的许可查询和权限检查结果。SAML 体系环境中包含主体、断言方和信任方三种角色。主体是与身份信息相关的用户；断言方提供安全信息，即身份提供者；信任方利用断言信息，提供接入控制和用户服务，具有代表性的信任方是业务提供者。SAML 工作原理如图 1 所示。

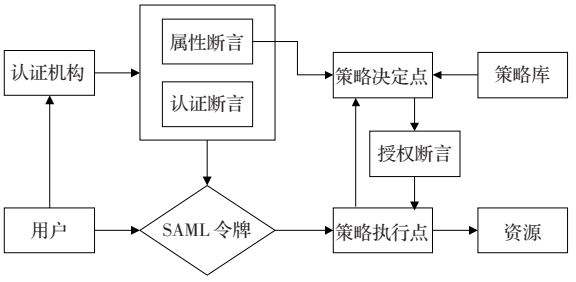

图 1 SAML 工作原理

终端用户作为主体向认证机构提交用户凭证；认证机构作为断言方对用户凭证进行检验，生成由认证断言和多个属性断言组成的 SAML 令牌作为用户身份信息载体，并对其进行数字签名；用户使用 SAML 令牌登录应用系统访问受保护的资源，策略执行点截取用户对受保护资源的访问请求，通过签名验证可以得到令牌发行者身份，并根据令牌中的认证断言认证申请服务的用户身份；同时将 SAML 令牌提交给策略决策点，策略决定点基于主体属性信息和策略信息产生授权决定，并将授权断言返回给策略执行点，由其实现用户对受保护资源的访问控制。

2.2 需求分析

随着用户规模的扩大和多种应用业务的出现，为提升服务质量，更好地满足客户需求，多业务运营平台对单点登录系统提出了更高的要求，主要表现为系统整体安全性和认证授权处理性能两方面。传统的单点登录解决方案重点研究信任关系移植载体和认证授权处理过程，没有过多关注于上述两方面内容。

2.2.1 整体安全性

单点登录系统对平台认证授权进行管理，是用户登录运营平台的统一入口。通过单点登录系统认证，用户可登录运营平台中所有应用系统，因此保障认证授权过程中数据传输安全性，对多业务运营平台至关重要。

安全保护的目的主要是防止机密信息被窃取并抵御非法攻击。机密信息窃取包括用户和认证机构间传送的认证信息被侦听，并被利用获得登录应用系统权限；用户与应用系统间传输机密信息被非法窃取，如窃取传输的用户信用卡信息；非法窃取站点间传送的用户身份令牌，利用此令牌获取用户身份，伪造用户登录应用系统。非法安全攻击主要包括拦截用户与认证机构或应用系统间传输信息，实现重放攻击[2]；拦截用户与应用系统间的通信，冒充用户作为中间人与应用系统交互，获得登录应用系统权限（通常称为中间人攻击[2]）；伪造业务系统[3]，与用户和认证机构通信，窃取用户机密信息。现有单点登录解决方案通常采用加密和签名机制保证传输数据的机密性和完整性，但是没有提出针对诸如重放攻击和中间人攻击等安全攻击的标准解决方案。

2.2.2 处理性能

单点登录系统中，所有用户认证都需要认证中心处理，用户规模扩大和访问量增长，对认证中心处理性能提出了更高的需求。除对认证中心采用集群技术外，各种单点登录解决方案都在应用系统端对通过认证的用户信息进行会话期缓存，对用户会话期间内登录采用本地处理方式，以降低认证中心负载，提升系统整体性能。在常规解决方案中，一般将用户信息的本地缓存周期设定成一个静态值，没有考虑应用系统实际情况和用户访问特性，如果缓存周期设定过短，将导致信息交互频繁，失去缓存价值；缓存周期设定过长，会造成应用系统资源浪费，同时令牌被窃取可能性也将增大。

3 双令牌机制单点登录模型

针对业务发展对单点登录系统提出的更高要求，提出一种基于双令牌机制的单点登录模型。模型充分利用 SAML 令牌信任可移植特性，采用 SAML 令牌作为用户身份载体，并对传送过程中的 SAML 令牌采用 XKMS 机制进行加密，保证令牌传输过程中的安全性；同时引入临时会话密钥[4]和会话令牌，利用会话令牌实现会话期内的安全管理，防止信息窃取和安全攻击。同时，为解决本地令牌缓存周期静态化问题，在对用户访问特性分析基础上提出了本地会话缓存周期动态激活算法，有效地实现了本地令牌缓存周期的动态扩展。通过与用户管理、信任管理和资源管理等子系统协同，保证了用户、认证机构和应用系统间消息传输的机密性、不可抵赖性和完整性，实现了对用户访问动态、细粒度的管理。

3.1 模型元素

模型中包含三类实体元素，用户（User）、令牌（Token）和资源（Resource）。

定义 1 $\forall u \in User, attr \in Attribute, t \in Token$；$u$ own $attr$, t own $attr$, if login u own t。

用户（User）是资源访问的主体，具有属性信息，属性包括用户 ID、年龄、住址等非敏感信息和信用卡、密码等敏感机密信息，能够决定对资源进行操作的权限。登录系统前，用户身份凭证是用户名/密码或证书，登录后，其身份凭证转换为平台颁发的令牌，用户属性包含在令牌中。

定义 2 $Token=\{SAML\ Token, Session\ Token | SAML\ Token \cap Session\ Token=\phi\}$, $SAML\ Token=\{Authentication\ assertion, Attribute\ assertion, Authorization\ Decision\}$, $Session\ Token=\{userID, Session\ Key, expire, attrs\}$。

令牌（Token）是系统生成并颁发给用户用于资源访问的凭证，模型中包括 SAML 令牌（SAML Token）和会话令牌（Session Token）两类令牌。SAML 令牌携带认证、授权和属性断言，是用户身份与属性的可移植载体，应用系统用其验证用户身份和权限属性，确定是否进行授权；会话令牌携带用户身份 ID、会话期临时密钥、密钥有效期和部分用户非敏感基本属性信息，用于提供会话期间管理所需信息。

定义 3 *Resource*={*Authentication Resource*,*Consume Resource* |*Authentication Resource* ∩*Consume Resource* =ϕ},*Authentication Resource create Token*,*Consume Resource provide service*}。

资源是服务的提供者,包含认证资源(Authentication Resource)和消费资源(Consume Resource)。认证资源提供认证功能,并负责为经过认证的合法用户颁发令牌。应用资源是用户获取应用服务的实体,具有访问控制策略,通过对用户令牌中包含的属性和自身策略进行校验,确定用户是否有权限对该资源进行相应的操作。

3.2　模型体系架构

模型采用双令牌机制实现单点登录,SAML 令牌作为用户身份凭证,会话令牌提供会话信息,实现会话期管理,同时采用 XKMS 机制保障用户身份 SAML 令牌的安全传输。

按照逻辑位置,模型分平台统一管理中心和应用服务监控管理中心两部分。平台统一管理中心负责用户登录平台认证、颁发令牌等全局管理工作;应用服务监控管理中心通过与平台统一管理中心交互,实现对用户资源访问的认证授权管理。平台统一管理中心由认证中心、LDAP 会话管理库、UDDI 注册中心、XKMS 管理中心和用户信息库等功能实体组成;应用服务监控管理中心包括策略执行点(PEP)、上下文处理点(CH)、策略信息点(PIP)、策略决定点(PDP)、策略管理点(PAP)、属性库和策略库等功能实体。依据基础功能与应用功能,将模型抽象成为认证层、实施层、数据层和基础服务层 4 个层次。系统模型层次如图 2 所示。

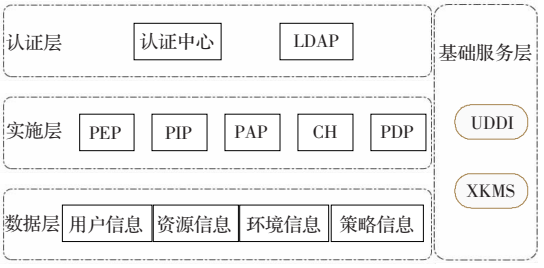

图 2　模型层次图

认证层对用户身份进行认证,通过认证的用户才能使用平台服务。认证层包括认证中心和 LDAP 会话管理库。认证中心是模型核心功能实体,通过与用户信息库交互,对资源访问主体身份进行验证,并为合法用户生成临时密钥、颁发 SAML 令牌和会话令牌。为提升并发效率和整体性能,认证中心可以包含多个认证服务器,认证服务器之间通过标准的通信协议,互相交换认证信息。LDAP 会话管理库[5],负责存储和管理已登录用户临时密钥和 SAML 令牌等用户会话期信息,接受认证中心指导实现用户信息存储与查询。

实施层实现用户资源访问控制管理,由策略执行点、策略信息点、策略管理点、上下文处理点和策略决定点组成。策略执行点拦截用户资源访问请求,提取会话令牌,并根据用户身份到认证中心获取用户 SAML 令牌与会话信息,验证用户身份;同时对合法用户建立一个基于主体、资源、动作和环境等属性的授权请求,通过上下文处理点转发给策略决定点,根据策略决定点返回的授权断言,判别用户访问资源的权限并执行策略。策略信息点负责提供授权决策所需要的用户属性、环境属性和资源属性。策略管理点提供策略和策略集。上下文处理点对上述实体间交互进行管理,负责转发授权请求并为策略决定点采集属性信息,同时将策略决定点生成的授权断言反馈到策略执行点。策略决定点根据策略评估处理认证和属性断言,并依据评估的结果发布批准或拒绝用户访问的授权断言。

数据层提供认证层和实施层需要的用户、资源、环境和策略信息,包括用户信息库、资源信息库、环境信息库和策略信息库。

基础服务层为上述三层提供基础服务,包括 UDDI 注册中心和 XKMS 管理中心。UDDI 注册中心,对平台合法应用服务提供注册管理,认证中心通过其判别用户请求服务是否在平台管理范围内。XKMS 管理中心,对站点间传输的 SAML 令牌提供安全保护。XKMS[6]是基于 XML 的 PKI,遵循 XML 数字签名和加密标准,能够简化了客户端 PKI 实现,降低了客户配置的复杂度。

3.3　模型数据流程

系统初始化阶段,应用服务到 UDDI 中心注册,成为平台认可的合法服务,同时 XKMS 管理中心为应用系统和认证中心发布证书,用于登录认证过程中提供安全保护。用户登录认证具体数据流程如图 3 所示。

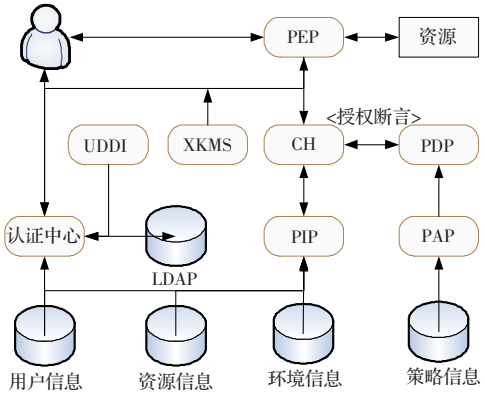

图 3　数据流程图

(1)用户登录系统,将 *ID* ‖ *Ep*(*ID* ‖ *Passwd* ‖ *TS*)发送到认证中心。

(2)认证中心接受用户请求,到用户信息库提取用户信息,利用用户密码解密,校验用户身份,为合法用户生成 *SKey*、SAML 令牌和会话令牌,并将 *SKey* 和 SAML 令牌保存到 LDAP 会话管理库中。

(3)认证中心将 *Ep*(*SessToken* ‖ *TS*+1)返回给用户,用户解密获得会话令牌,同时比较时间戳,验证认证中心合法性。

(4)用户访问被保护资源,发送请求 *ID* ‖ *ESKey*(*SessToken* ‖ *TS*)。

(5)策略执行点截获用户资源访问请求,发送 *Ekuc*(*ID* ‖ *SID* ‖ *EKrs*(*ID* ‖ *TS*′))到认证中心获取用户信息。

(6)认证中心采用 *Krc* 解密请求,利用 UDDI 验证服务 *SID* 合法性,并通过比较 ID 验证应用系统签名;之后根据用户 ID 从 LDAP 中提取用户 SAML 令牌和 *SKey*,将 *Ekus*(*SKey* ‖ *SamlToken* ‖ *TS*′+1 ‖ *Ekrc*(*TS*′+1))返回策略执行点。

(7)策略执行点采用 *Krs* 解密处理认证中心响应,获取 *SKey* 和 SAML 令牌,验证时间戳和认证中心签名;根据 *SKey* 解密获取用户请求中 *SessToken* 和时间戳,判断 *SessToken* 合法性和有效性,并通过比较 *SessToken* 与用户请求中 ID,确认

消息没有被篡改,同时获取 *SessToken* 中用户基本属性。

(8)策略执行点发送资源访问请求到上下文处理点,上下文处理点根据 *SessToken*、SAML 令牌和通过策略信息点获取的资源和环境信息建立一个基于主体、资源、动作和环境等属性的授权请求,转发给策略决定点。

(9)策略决定点利用策略管理点获取策略集,对用户进行授权,将授权结果返回给策略执行点。

(10)策略执行点将 *ESKey*(*TS*+1)返回给用户,同时缓存用户 *SKey* 和令牌等会话信息;用户通过对 *TS* 进行校验,验证应用服务器身份。

至此完成用户登录应用系统,获得访问资源权限。对于终端用户,此处理过程完全透明,当用户在会话缓存周期内访问应用系统时均不需再次登录;同时对于用户与应用系统间传输的机密信息,可以采用 *SKey* 进行加密处理,以保证机密信息传输过程中的安全可靠。

ID=*USER ID*,*Passwd*=*USER Password*,*TS*=*timestamp*

Ep=利用 *Passwd* 加密,*SKey*=会话密钥,*SessToken*=会话令牌

SID=服务 *ID*,*Krs*=服务私钥 *Kus*=服务公钥 *SamlToken*=*SAML* 令牌,*Krc*=认证中心私钥 *Kuc*=认证中心公钥

3.4 安全性分析

用户认证授权过程主要涉及用户、认证中心和应用系统三个节点,在节点间数据传输过程中综合采用了签名、加密和时间戳等多种安全保障技术。用户与认证中心通信采用用户密码加密,只有用户与认证中心才能获取用户密码,保证了用户登录信息的机密性。应用系统和认证中心通信时,采用 PKI 机制,利用发送方私钥进行数字签名,并利用接收方公钥加密数据,保证了二者间传送数据的机密性、完整性和不可抵赖性。用户访问应用系统时,访问请求中携带临时会话密钥并利用会话密钥对请求进行加密,只有合法的应用系统才能访问认证中心获得会话密钥,响应用户请求,进而实现了用户和应用系统的双向验证,防止了攻击者伪造应用系统获取用户机密信息,也抵御了中间人攻击等安全威胁。同时上述各个通信过程中都加入了时间戳,有效地抵御了重放攻击。

4 动态缓存周期解决方案

应用系统对用户 SAML 令牌和会话信息进行缓存,可以使会话期间内用户多次访问,只在第一次与认证中心交互,其余请求均在本地完成处理,能够有效降低应用系统与认证中心信息交互次数,提高系统并发认证能力和处理效率。用户令牌的本地缓存周期,是系统中需要重点研究的问题。常规解决方案一般设定一个静态值,没有考虑应用系统实际情况,也没有区分用户类型和用户访问特性,因此存在较多弊端。对此,提出了基于用户访问特性的本地缓存动态半周期自适应延长算法,解决了令牌缓存周期静态化问题。

4.1 用户访问特性分析

首先对用户日志进行预处理,利用用户年龄、学历、地址、登录时间、登出时间过滤冗余信息,同时假定登录与登出时间间隔半小时以内为同一次平台登录操作并合并记录。预处理后,将访问记录标记用户年龄段、地址范围,同时根据登录时间标定时间段(时间段分凌晨、上午、中午、下午、晚上和深夜)并计算访问时长(登出时间与登录时间差)。之后按照访问时间段、用户地址范围、用户年龄段、学历和访问时长顺序,依次对访问记录进行分组。最后对计算每组内记录访问时长均方根值,作为该类型用户初始缓存周期,并生成用户访问特征树,如图 4 所示。

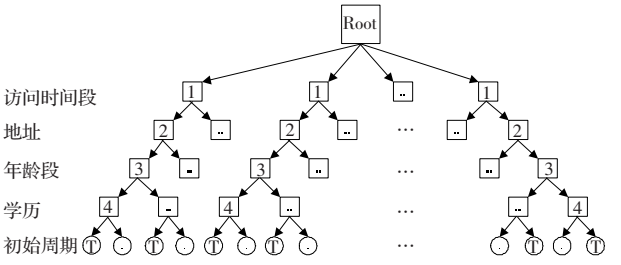

图 4 用户访问特征树

4.2 动态半周期自适应延长算法

在计算出用户初始缓存周期基础上,模型采用缓存周期动态半周期自适应延长算法,实现了对缓存周期动态化管理,算法描述如下。

用户登录应用系统,应用系统按照用户特征值,从树中根节点向下依次检索,选定对应叶节点,作为该用户初始缓存周期 T,设定 T_0=0,T_s=T=2L。0~L 时间段内,用户再次访问应用系统,应用系统本地实现对用户的认证授权管理。L~2L 时间段内,如果用户没有再次发送访问请求,则在 T_s=T=2L 时刻判定用户已经离开应用系统,清空用户缓存并释放资源;如果 L~2L 时间段内用户继续发送访问请求,应用系统除利用本地缓存实现认证授权外,还将本地会话缓存周期动态扩展 L 时长,即缓存到期时刻为 3L,并将缓存初始时刻设定为 L,使得 T_0'=L,T_s'=3L,以 T'作为新的缓存周期,进而实现了缓存周期的动态自适应扩展。

单点登录过程中,安全信息交互次数越多,信息暴露的机率就越大,同时认证中心负载越大,系统效率越低[7]。在应用系统段对用户令牌进行缓存,并采用本地缓存动态半周期自适应延长算法,用户令牌只在认证中心与策略执行点间进行了一次传输,降低了认证中心负载,提升了系统整体性能。

5 总结

单点登录已成为企业应用门户必备的基础功能。引入双令牌机制的单点登录模型,能够发挥 SAML 模型可移植性、标准性和通用性等方面优势,减少安全信息交互次数,简化登录流程,并能实现用户登录会话期间的安全访问和实时控制,防止诸如重放攻击、中间人攻击等一系列安全隐患。同时,模型体系架构灵活,便于扩展和新增应用动态加入,能够减少开发工作量特别是业务应用系统的开发量,易于应用和推广。

参考文献:

[1] Cantor S,Kemp J,Philpott R,et al.Assertions and protocols for the OASIS security assertion markup language(SAML) V2.0[S/OL].(2005). http://docs.oasis-open.org/security/saml/v2.0/.

[2] Hirsch F,Philpott R,Maler E.Security and privacy considerations for the OASIS security assertion markup language(SAML) V2.0[S/OL].(2005).http://docs.oasis-open.org/security/saml/v2.0/.

(下转 188 页)