网格环境下虚拟企业信息系统中单点登录问题研究*

林培旺,刘东苏,薛杰
(西安电子科技大学 经济管理学院,西安 710071)

摘 要 本文对网格环境下虚拟企业单点登录安全问题进行了分析,提出了一种基于安全断言标记语言(SAML)的单点登录模型。该模型具有与底层安全实现无关,可与现有安全系统无缝集成等特点,包括请求端、中心安全服务端和目标服务端三个主要功能模块,在设计模型工作流程时充分考虑了其安全性,并注意到网格环境下任务时长可能超出令牌生命周期的情况,给出了相应的解决办法。

关键词 网格,安全,虚拟企业,单点登录
中图分类号 TP393.08

1 引言

随着全球市场竞争的日益加剧,商业机遇稍纵即逝,在这样的环境下,企业利用信息技术,充分发挥自身核心竞争力,通过优势互补,形成了虚拟企业这一以市场为导向的企业组织形式。网格技术因其在跨平台分布式的共享与集成方面的优势,成为了商用信息技术中的新宠儿,其与虚拟企业的结合也已经成为必然的趋势。网格技术使得虚拟企业中信息与资源的共享与集成达到从未有过的程度,各成员对服务和资源的跨域访问引发了对身份验证的新需求。网格环境下的虚拟企业需要一种安全有效的跨越安全域的身份验证机制。单点登录(Single Sign-on)技术为这一问题提供了很好的解决思路,使得虚拟企业成员在访问服务与资源时不必频繁地进行身份验证操作,提高信息传递效率与安全性,做到一次登录,多次多域访问。本文主要提出了一种网格环境下虚拟企业的单点登录模型,并考虑了网格环境下令牌生命周期小于任务时间的情况。

2 问题分析

2.1 网格环境引起的特殊性

网格最根本的特点是共享性,现有的网络只能达到信息或数据层次的共享。网格环境下,资源共享的广度和深度都有了明显的提高。具体到网格环境下的虚拟企业信息系统,联盟成员之间共享的不再仅仅是一些数据信息、电子文档等,更多的是彼此的计算资源、存储能力、应用软件、制造设备等等;同时,网格环境下虚拟企业的最小元素不再是一个个的企业,而是企业中的一个部门[1]。如此大范围的资源共享和更加细化的组织结构对虚拟企业信息系统安全,特别是联盟成员的身份验证提出了严峻的挑战。采用单点登录技术可以对登录主体进行跨不同安全域的身份认证,使之可以跨越多个组织边界进行资源和服务的访问,还可以满足网格环境下登录主体复杂多变的情况。在网格环境

* 通信作者:林培旺,男,西安电子科技大学经济管理学院硕士研究生,E-mail:linpw007@yahoo.com.cn。

下，触发单点登录流程的不再仅仅是用户，还有可能是用户授权的委托程序。网格环境下虚拟企业的一个具体业务流程的处理还可能具有较长任务处理时间，可能会超过单点登录令牌的有效期限。

下表给出了传统网络环境下和网格环境下单点登录的区别：

表 1 传统网络环境和网格环境单点登录的比较

	传统网络环境	网格环境
登录主体	用户	用户或者委托程序
任务周期	一般不超出证书有效期	具有很大的不确定性
认证范围	一般是两个安全域	经常是跨越多个安全域的认证
触发条件	用户驱动，一次性触发	用户或程序驱动，可能多次触发
认证信息途经节点	点到点，或端到端	多中继，多中间节点

从表中可以看出，网格环境下的单点登录在登录主体、任务周期、认证范围、触发条件等方面都与传统网络环境下的情况有着明显的不同。

2.2 需求分析

由于虚拟企业各成员已有的安全体系和采取的具体安全技术各有不同，单点登录方案应采用一种与底层安全实现无关的方法，做到与现有系统的无缝集成，并可以与网格安全策略进行交流互通，满足企业成员动态加入和退出的情况[2]，并且要考虑到认证信息多节点传输的情况。从当前的情况来看，采用基于安全断言标记语言(SAML)的单点登录方案是比较好的选择。

网格环境下虚拟企业信息系统单点登录过程中需要考虑的具体安全需求如下：

(1) 不影响企业成员底层安全实现，在应用层解决单点登录问题，可以与已有的安全系统集成和互操作，不要用新的机制代替之前的安全系统；

(2) 应当提前做好虚拟企业成员间安全策略的表达、交流和互通，这一过程应在虚拟企业生命周期中的准备阶段完成，这些策略和规则在单点登录过程中出现如令牌生命周期结束，或者由程序驱动引发新的单点登录请求时将起到重要作用；

(3) 机制灵活，能够满足企业成员动态加入和退出的情况而不对整个虚拟企业信息系统产生影响；

(4) 网格环境下任务执行时长具有不确定性，需要对请求资源的主体进行令牌时效验证，能够自动进行代理证书周期到期通知与更新。

3 当前研究现状

目前，国内外关于单点登录问题的研究正处于起步阶段，网格环境下单点登录的需求也已受到充分重视，在 OGSA 网格安全模型中，证书与身份转换模块主要需要实现的功能就是单点登录[3]。Jan De Clercq 对单点登录的模型做了系统的整理与综述[4]；Sinnott, R. O. 等人研究了单点登录技术在动态虚拟企业中的应用[5]；师少帅，王建民提出了一种轻量级的单点登录方案[6]；尹星等提出了一种改进的基于 SAML 的单点登录模型，并对其进行了模拟仿真[7]。当前网格环境下的单点登录实现方法主要是基于代理证书及其在不同安全机制(如 PKI 和 Kerberos)下的转换。

在网格环境下，虚拟企业的信息共享更加广泛，业务流程更加复杂，单点登录主体所提交的任务时长更加不确定，这增加了身份认证的复杂程度，虽然国内外的学者当前对单点登录技术的研究已做了大量工作，但当前的单点登录模型还存在着开放性与标准性不足、安全性不高、跨域实施困难以及实现流程复杂等局限，考虑到当前单点登录技术存在的上述局限性，并考虑到网格环境下虚拟企业本

身特有的安全需求特点，本文的单点登录模型在设计时主要从以下方面进行了改进：

（1）尽量做到与各联盟企业安全系统的底层实现无关，与现有系统进行无缝集成，在应用层解决单点登录问题，避免各联盟企业在信息系统安全方面的重复投入，节省成本，提高了经济性；

（2）简化模型运行流程，并充分考虑到各步骤的信息安全保护；

（3）SAML 令牌由请求端保管，减轻了中心安全服务器的存储压力，分散了安全风险。

此外，考虑到网格环境下任务时长的不确定性，本文的单点登录模型通过在 SAML 令牌生成时向其中加入令牌生命周期信息，使得被访问的安全域可以对令牌时效性做出判断，提高了安全性；同时还考虑到任务处理过程中程序自发驱动新的单点登录请求的情况。

4 一种单点登录方案

4.1 单点登录模型

在网格环境下，每个虚拟企业的成员都可被视为一个独立的安全域，成员之间遵循 Liberty Alliance 联邦信任，SSO 中心验证服务由虚拟企业联盟中的盟主企业提供。

模型中并未采用 SAML 配置文件中的 PULL 模式或 PUSH 模式，如此可以简化验证流程，提高验证效率和灵活性，符合网格环境下对信息传输的要求。SAML 令牌的传递仅仅在请求主体和中心服务器以及请求主体和身份验证服务器之间进行，令牌维护工作由请求主体自身承担，这样可以防止可能出现的服务器拥塞和针对中心验证服务器的攻击，也符合网格的分布性设计思想。

安全策略库是网格环境下虚拟企业安全策略与规则的集合，其中包含了联盟成员事先协商好的各种安全相关的信息数据，在此模型中，主要使用的是令牌过期时的相关安全规则。

授权模块放置在目标服务端，这样可以保证各成员企业的独立性，可以对自身的资源及服务的访问权限拥有自主决策权，使单点登录过程不与各成员企业原有的安全授权体系相冲突。授权模块不放置在中心安全服务端，增加了系统的灵活性和可扩展性，也减少了登录流程的复杂性。

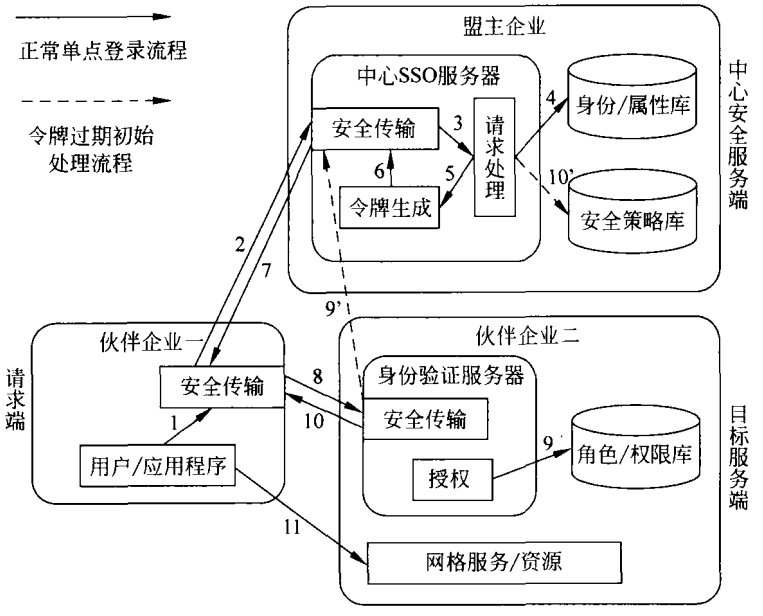

图 1 网格环境下虚拟企业信息系统单点登录模型

4.2 功能模块

网格环境下虚拟企业信息系统单点登录模型如上图所示。模型包含请求端(图中为伙伴企业一)、中心安全服务端(图中为盟主企业)和目标服务端(图中为伙伴企业二)这三个端点。请求端为用户提供单点登录的接口,是SAML令牌的请求者和使用者;中心安全服务端是请求端身份的验证者和SAML令牌服务的提供者;目标服务端则是SAML令牌的验证者与网格服务和资源的提供者。

请求端的主要功能是接收用户的输入信息或者代理程序的请求信息,生成SAML请求,对该请求进行安全处理。在发出经过安全处理的请求消息之后等待SAML响应。然后使用中心安全服务端颁发的SAML令牌访问目标服务以及接收服务调用结果。

中心安全服务端主要功能是根据请求端发来的请求消息对用户提供基于数字签名的身份验证,同时根据SAML请求信息生成SAML响应信息,通过对其进行签名、加入令牌生命周期信息然后加密生成安全的SAML令牌,并返回至请求端。

目标服务端主要功能是验证SAML令牌的可用性、安全性、时效性以及来源。然后解析SAML令牌,根据令牌中的用户信息,实现基于角色的访问控制,即根据用户的角色对用户进行授权。最后对经过授权的用户或程序进行网格服务调用与资源访问。

安全传输模块对每个端点的输入/输出信息进行安全处理并且负责XML信息的包装和SOAP消息的收发。它符合WS-Security规范,主要提供以下功能:XML加密和解密、XML签名和验证、附加标识符和令牌生命周期信息。XML签名可以保证消息的完整性和对消息源的验证,XML加密则用来确保消息的机密性,添加标识符信息可以防止重放攻击,上述三个功能结合起来共同保证SOAP消息所需的安全性需求。加入令牌生命周期信息可以应对任务周期的不确定性。然后此模块将XML信息包装成SOAP消息发送出去,在模型的另一端此模块接收SOAP消息并从消息体中提取XML信息。

4.3 工作流程

上文主要描述了模型的组成模块及各模块的功能,下面将根据图1详细描述模型的工作流程。单点登录模型的正常工作流程如下:

(1) 单点登录开始时用户或应用程序提供登录所需身份信息,请求端程序根据身份信息生成相应的SAML请求。

(2) 请求端的安全处理模块使用请求端与中心SSO服务器事先协商好的密钥A将上一步生成的SAML请求进行正向处理(签名、加密、加入标识符),然后将其打包成SOAP消息发送至中心安全服务端,并等待应答。

(3) 中心SSO服务器的安全传输模块负责监听和接收请求端发来的请求消息,并对该消息进行反向处理(解密与验证数字签名和标识符)。通过对请求消息中数字签名的验证,可以确认该请求来自合法用户,完成了身份认证的过程,然后将原始SAML请求发送给请求处理模块。

(4) 请求处理模块对通过验证的用户的SAML请求进行解析,获取用户需查询的指定的属性信息名称,并根据属性名称到用户身份/属性库中查找用户指定的属性信息。

（5）请求处理模块将查询的结果生成用户的属性声明，该声明构成用户登录目标服务站点时使用的SAML令牌的核心。

（6）SAML声明被发送至安全处理模块进行安全处理，使用中心服务端与目标服务端事先协商的密钥B进行加密和签名，形成安全的SAML令牌。因此只有合法的目标服务端才能获得SAML令牌中的声明信息。

（7）中心SSO服务器的安全处理模块使用与请求端协商好的密钥A再次对安全的SAML令牌进行处理，加密、签名，并加入令牌生命周期信息，然后打包成SOAP消息返回至请求端。

（8）请求端的安全传输模块等待和接收中心安全服务端返回的响应消息，并对消息进行反向处理，解密、验证数字签名并得到令牌生命周期信息。此时用户已经获取了可以访问目标站点的安全的SAML令牌，用户可以使用该安全的SAML令牌，但却无法知道令牌中的信息。此时用户或应用程序提供要访问的目标服务端的URL、指定的网格服务的名称和参数。安全的SAML令牌经过安全处理模块的处理，将之与标识符一起用中心SSO服务器提供的密钥K加密，然后发送至目标服务端。

（9）目标服务端的身份验证服务器对接收到的消息进行两次验证，第一次使用密钥K解密，可以确信请求端已得到中心安全服务端的验证，并同时得到令牌的生命周期信息，并对令牌是否过期进行判断，如果没有过期，则进行第二次验证，使用与中心安全服务端协商好的密钥B进行解密与验证，可以确信SAML令牌是由中心SSO服务器颁发的。经过解密和验证，得到原始的SAML断言，目标服务端使用SAML规范解析令牌中的声明，获取SAML权威为该用户生成的声明信息。授权模块根据声明信息中包含的用户属性信息，结合本地的安全策略，访问本地的角色/权限库，对用户或应用程序进行基于角色的授权，判断用户是否有权访问他所请求的网格服务与资源。

（10）目标服务端的安全传输模块将判断结果返回给请求端。

（11）请求端的用户或应用程序对目标服务端的网格服务与资源进行访问。

上述过程为模型的正常工作流程。需要说明的是，在第8步，身份验证服务器对接收到的令牌信息进行解密，读取令牌生命周期信息后，如果发现此时令牌已过期，工作流程则转向图1中第9'步，向中心SSO服务器发出更新令牌的请求信息，中心SSO服务器的请求处理模块访问安全策略库（图1中第10'步），参考虚拟企业联盟的事先协商的相关安全策略做出相应的处理，根据请求端提交的任务性质，处理结果可能为自动更新令牌回传给身份验证服务器以完成单点登录流程，或者中止此次单点登录的过程，并向请求端回复相应出错信息，直到请求端的用户再一次驱动单点登录流程。

5 模型可行性论证

上文主要描述了模型的工作流程，下面主要针对文中模型的特点，从三个方面来简要说明此模型的可行性。

（1）组织可行性

虚拟企业的生存周期一般分为概念、建立、竞标、配置、执行和终止六个阶段，而对于安全问题的考虑应该在这六个阶段一以贯之，特别是在网格环境下建立虚拟企业，由于网格技术可使信息与资源

的共享达到很高的层次，这也同时带来了更多的安全隐患，所以网格环境下的虚拟企业信息系统在提供业务与实现功能时都要特别注重各步骤的安全保护，如在虚拟企业的建立阶段联盟企业各方就应进行细致沟通，确定模型中安全策略库中的各种安全规则与约束；在配置阶段便可按照已约定的安全规则与约束对已经有的安全系统进行相应调整与改造。

(2) 经济可行性

虚拟企业的各联盟企业一般都已拥有自己的企业信息安全系统，并在其上进行了大量先期的投入，文中的模型在解决单点登录问题时没有限定参与各方的底层具体安全实现，各方只需在应用层进行相应的改造即可。

(3) 技术可行性

在本文的模型中，各联盟企业遵循 Liberty Alliance 联邦信任，具有普适性与标准性，模型的工作流程中所采用的各种协议，如 SAML 令牌生成及传递协议，SOAP，XML 相关协议等都已发展成熟并被业界认可；同时模型在设计过程中也体现了模块化设计与可重用的思想，提高技术层面上模型实施的效率。模型中的安全传输模块就是这一思想的体现，它符合 WS-Security 规范，在各端点中该模块能根据输入信息的不同而自动进行对应的处理操作。

本模型作为网格环境下虚拟企业信息系统中一个具体安全问题(单点登录)的解决方案，其具体实施过程和工作条件应放在网格环境下虚拟企业信息系统安全的大环境中来考虑，网格环境下的安全问题纷繁复杂，单点登录问题只是冰山一角。这就需要各联盟企业对自身的安全系统进行不断的完善与改进，有了可靠的安全系统基础，应用层面的单点登录模型才能充分发挥出它的安全作用。

6 结论及进一步的工作

本文通过对网格环境下虚拟企业单点登录的具体安全需求分析，给出了单点登录模型，进行了功能模块划分和设计，并给出了具体的工作流程。考虑到在单点登录过程中可能出现的令牌生命周期小于任务时长的情况，在具体处理过程中给出了相应的方法。网格下的虚拟企业面对着复杂的网络环境，单点登录模型只能解决其中部分的安全问题，如何将单点登录与虚拟企业整体的安全策略与规则结合起来，形成统一高效的安全体系，是下一步值得研究的方向。

参考文献

[1] 张润彤，樊宁. 网格就是商务[M]. 北京：清华大学出版社，2006.

[2] Nagaratnam N, Janson P, Dayka J, Nadalin A, Siebenlist F, Welch V, Foster I, Tuecke S. The security architecture for open grid services[EB/OL]. http:// www . cs . virginia . edu / ~ humphrey / ogsa-sec-wg / OGSA-SecArch-v1-07192002. pdf，2002.

[3] Foster I, Kesselman C. 网格计算(第二版)[M]. 金海，袁平鹏，石柯，译. 北京：电子工业出版社，2004.

[4] Clercq J D. Single sign-on architectures [EB/OL]. http ://www. esat . kuleuven. ac. be/cosic/seminars/slides/SSO. pdf, 2002.

[5] Sinnott R O, Ajayi O, Stell A J, Watt J, Jiang J, Koetsier J. Single sign-on and authorization for dynamic virtual organizations [EB/OL]. http :// labserv. nesc. gla. ac. uk/projects/glass/doc/helsinkifinal. pdf, 2006.

[6] 师少帅，王建民. 一种轻量级单点登录模型的设计与实现[J]. 南京大学学报(自然科学)，2005，41：862-867.
[7] 尹星. 基于SAML的单点登录模型及其安全的研究与实现[D]. 镇江：江苏大学，2005.

Research on Single Sign-on of Virtual Enterprise Information System in Grid Environment

LIN Peiwang, LIU Dongsu, XUE Jie
(School of Economics and Management, Xidian University, Xi' an, 710071)

Abstract In this paper, an analysis is given to the single sign-on problem of virtual enterprise in grid environment. A model is purposed based on Security Assertion Markup Language with full consideration of safety, including three main function modules which are request node, central security server and target server, with the characteristic of independence from the bottom security implements and seamless integration with the existing security system, the fact that task time may exceed token life cycle has been taken into account and the corresponding solution is given as well.
Key words Grid, Security, Virtual Enterprise, Single Sign-on

作者简介：

林培旺，男，24岁，西安电子科技大学经济管理学院硕士研究生。主要研究方向：信息系统与信息安全，电子商务。

刘东苏，男，教授，现任西安电子科技大学经济管理学院副院长，长期从事信息系统分析与设计、电子商务、计算机网络与信息安全、数据库与数据仓库技术应用等方面的教学与研究工作。主要研究方向：信息管理，信息系统与信息安全，电子商务。

薛杰，女，25岁，西安电子科技大学经济管理学院硕士研究生。主要研究方向：信息系统与信息安全，电子商务。