基于信任计算的跨域访问控制研究

徐学东 张志俊 长春工程学院机电学院

DOI:10.16589/j.cnki.cn11-3571/tn.2016.20.045

基金项目：吉林省教育厅科研项目(吉教科合字[2014]第 337 号)；吉林省科技攻关计划项目(20140204060SF)；

【文章摘要】

大型分布式多域网络环境中不存在统一的认证控制中心,传统基于实体身份的认证方式无法满足要求。研究跨域陌生实体交互的身份认证及控制系统的架构,通过信任计算对陌生实体域外访问权限进行授权,给出具体的设计及处理流程。后续实践表明该架构体系具有良好的网络适应性以及较高的域间访问控制交互成功率。

【关键词】

分布式多域网络、陌生实体、信任计算

引言

传统访问控制机制需在确认实体身份的基础上才能正确实施，主要适用于适应于单域非合作环境。在云计算等大规模分布式多域网络环境中不存在统一的控制中心，存在跨域的大量陌生实体访问需求，参与交互的陌生实体在跨域访问时没有事先定义的信任关系，或者虽能认定其身份和域外权限，却没有定义其在本域内的资源访问权限，必须研究新的访问控制机制解决前述难题。以面向多域网络的分布式访问控制机制为研究目标，参考普适网络[1]、P2P 网络[2]信任模型，研究由信誉评估上升到信任管理的跨域访问控制系统的体系架构及流程。

1. 应用场景

在多信任域之间共享资源的情况下，网络资源的调度存在着域内调度和域间调度，因而产生了域内和域间两种信任关系[3]。应用场景如图 1 所示，在每个网络域中部署域管理代理服务端，各用户应用或资源通过异构系统规格化接口接入。

域管理代理是该域的访问控制管理核心，负责为域内全部用户节点进行信任建模、实施信任计算、发放并维护信任证明，并协同域内、域间的管理信息交流。各节点在访问资源时可以使用管理服务，通过管理代理获得相应授权并被分配到安全信任度较高的资源。管理代理则根据信任值和访问控制策略选择资源，并进行信任协商，确认是否可以使用资源。

2. 系统的总体架构

系统的总体架构参考基于信任的跨域安全认证模型 TB-WSCDSA[4] 进行设计，包括两个部分，实现域管理代理服务的服务端和实现本地认证的客户端。架构如图 2 所示。

（1）实体端

实体端主要指网络中访问发起端。用户可以在本地认证信息库保持一些根证书，还有已知实体 / 资源的信任信息，以选择访问已信任的资源，加快访问速度。

（2）服务端

服务端指域管理代理服务器，负责总体管理。如果访问者需要访问本地资源，要提交自己的证书，当然也可以要求域管理方也提供证书来证明管理者的身份。域管理器先进行身份鉴别，然后再通过自己的信任信息库，查看该实体的信誉历史，计算应赋予其何种权限。

如果访问者访问外部资源，本域管理器与目标域的管理器进行交互，确保可靠的实体 / 资源来为访问者服务。信任管理部分负责评估其它域管理器的信誉情况，并信任对方推荐的信誉好的服务者。

每次交易结束，域管理者可以根据用户满意度等因素，为双方评价信誉情况，使得信任信息动态更新。较差的服务提供者和用户均被降低信任值，直接影响访问权限。

3. 系统组成

系统总体框架如图 3 所示。本系统可以分为六个部分，分别是服务提供者（SP）、身份认证服务（IDP），信任管理服务、委托管理、安全审计模块（ATS）以及访问控制（AC）。其中：

（1） SP 负责对用户身份进行核查，该用户是否已经登录以及用户属性获取；

（2） IDP 是整个系统的核心，主要负责对用户身份进行认证，授权以及用户属性查询；

（3） AC 服务根据用户权限对用户的访问进行控制；

（4）信任管理服务包括信誉信息收集器和信任证明管理器。信誉信息收集器负责管理本域内实体的实体信誉信息以及跨交互过程中的域信誉信息。信任证明管理器计算实体信任值和域信任值，为实体提供相应的信任证明，并负责调整信任信息；

（5）委托管理建立子域管理系统，并进行委托授权；

（6）安全审计模块实现访问行为的日志记录，可实现行为追溯。

4. 系统功能流程

系统功能流程包括域内关系节点访问登录流程，域内节点访问登录流程，域间节点访问登录流程，节点访问单点登出流程，新实体端信任记录建立流程等。下面以域间节点访问登录流程为例介绍具体登录及验证过程。

功能描述：首先实体端向外域服务提供端发送资源访问请求，自动定向到本域管理服务端，提交自身的信任证书，域管理服务验证信任证书。与外域服务提供端所在域服务器（简称“外域管理服务端）连接，发送验证信息，外域服务端完成双方验证，完成域间验证过程。

具体流程为：

（1）实体端访问外域服务提供端，请求服务；

（2）自动定向到本域管理服务端，本域服务端发送认证命令；

（3）实体端向本域管理服务端发送信任证书，本域管理服务端对其进行身份认证。如用户未进行过认证，则转到信任管理中查询该

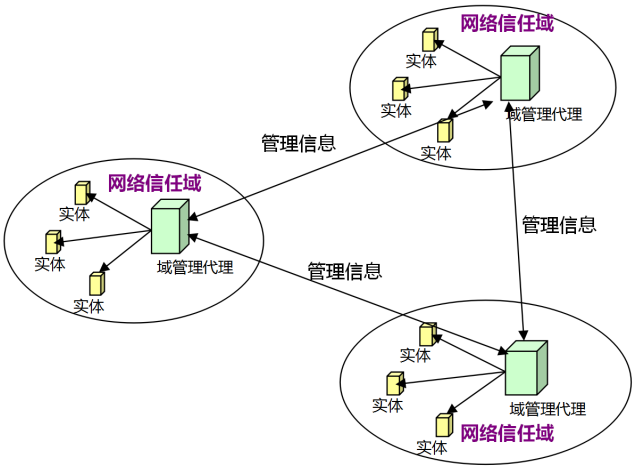

图 1 跨域分布式访问控制部署示意图

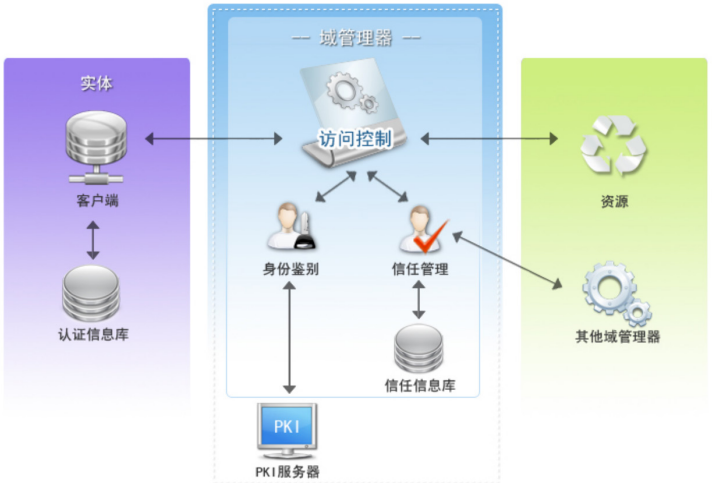

图 2 跨域分布式访问控制系统架构示意图

用户的信任记录；

（4）本域管理服务端对外域管理服务器发送认证命令；

（5）外域管理服务器接受认证信息，首先对本域管理服务器进行验证，如未进行过有效的认证，则转到信用管理中查询本域管理服务器的信任记录；

（7）如本域管理服务器的认证或信任得到确认通过，则外域管理服务端对外域服务提供端发送认证命令；

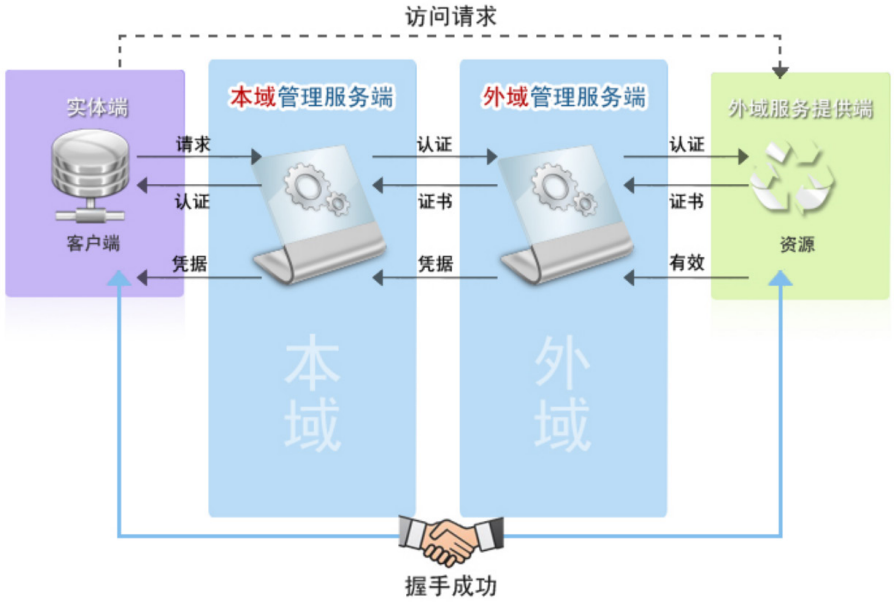

图 3 系统框架图

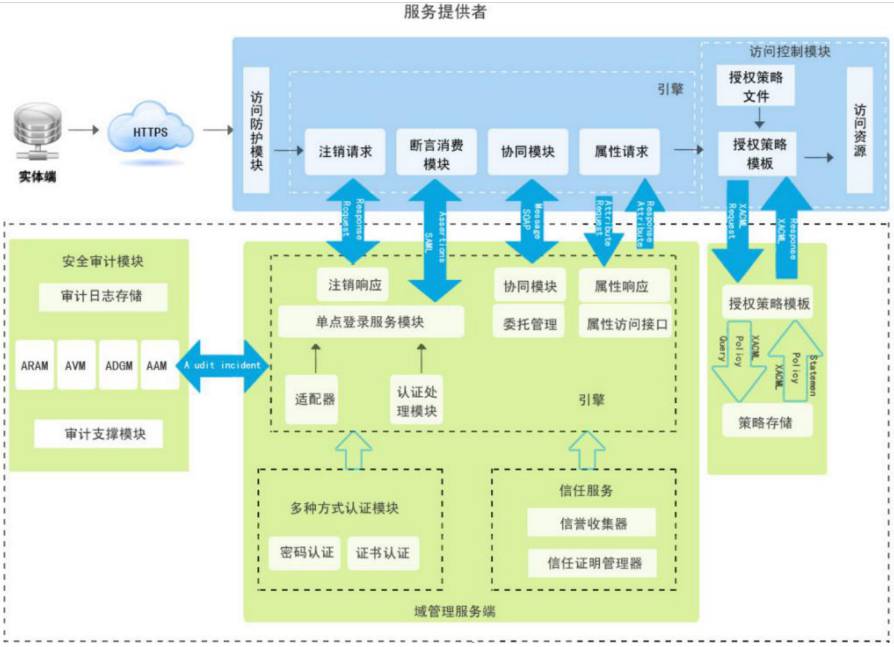

图 4 域间节点访问登录功能示意图

（8）外域服务提供端向外域管理服务端发送信任证书，本域管理服务对其进行身份认证。如未进行过有效的认证，则转到信任管理中查询该用户的信任记录；

（9）双方身份认证或信任信息确认，外域域管理服务端信任管理记录认证凭证并生成一个认证凭据，发送给服务提供者验证有效性；

（10）外域管理服务端将凭据返给本域管理服务端，本域管理服务端发送凭证、附上本域认证信息给实体端，记录本次认证凭证信息，以重定向方式返回给服务提供者；

（11）实体端将票据发送给服务提供者；

（12）服务提供者返回认证结果给用户，双方握手，建立服务连接。

5. 结语

多域网络环境中未明确权限实体跨域应用访问控制包括多方面研究，如基于信任计算的 RBAC 改进模型、基于本域权责和既往访问行为分析的信任计算算法、系统的架构及接口等。本文仅就系统的整体架构、组成和流程进行了分析和设计。经过实践表明该架构体系具有良好的网络适应性以及较高的域间访问控制交互成功率。后续将在另文介绍其它研究成果。

【参考文献】

[1] Mieso K Denko,Tao Sun,Issac Woungang.Trustmanagement in ubiquitous computing:A Bayeian approach[J].Computer Communications，2011,34(3)：398-406.

[2] Florina Almenarez,Andres Marin. Trustmanagement for multi media P2P applications in autonomicnet working[J].Ad Hoc Networks，2011,9（4）:687-697

[3] 马满福，张龙．物联网中基于网关的跨域信任模型 [J]. 计算机工程与设计，2013,11(34)：3829～3834；

[4] 卢晓霞，韩坚华 .Web 服务中基于信任的跨域安全认证模型 [J]. 微型机与应用 .2012,3(31):50～55；

【作者简介】

徐学东 (1976－)，男(汉)，安徽阜南人，副教授，硕士，主要研究领域为过程控制，信息安全

（上接 029 页）

3. 总结

总之，变压器油纸绝缘老化是影响变压器运行稳定性和使用寿命的主要原因之一。为了确保变压器运行的稳定性，延长变压器使用寿命，必须要加强对变压器油纸绝缘老化影响因素的研究，提前判断变压器的运行情况，避免出现较为严重的事故。

【参考文献】

[1] 廖瑞金，杨丽君，郑含博，汪可，马志钦．电力变压器油纸绝缘热老化研究综述 [J]. 电工技术学报，2012,05:1-12.

[2] 陶凤源，张东，董新胜，王世荣．极化谱法在变压器油纸绝缘状态检测中的影响因素分析 [J]. 工矿自动化，2014,10:33-36.

[3] 柳岩，张吉刚．变压器油纸绝缘系统老化的影响因素 [J]. 民营科技，2015,07:21.