跨域访问控制与边界防御方法研究 *

邹 翔, 金 波, 倪力舜
(公安部第三研究所 信息网络安全公安部重点实验室 国家反计算机入侵与防病毒研究中心, 上海 200031)

摘 要: 为保障跨域访问过程中的信息网络安全,在深入分析其所面临安全风险的基础上,提出了一种跨域访问控制与边界防御模型,该模型将跨域访问过程划分为域内和跨域两个阶段,同时结合相关安全技术进行策略决策和策略实施,保障了信息传输的保密性、完整性和可用性,从而有效地解决了跨域访问过程中的访问控制和边界防御问题。

关键词: 访问控制; 安全域; 边界防御; 身份认证; 安全策略
中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2010)04-1481-03
doi:10.3969/j.issn.1001-3695.2010.04.077

Research on cross-domain access control and border protection technique

ZOU Xiang, JIN Bo, NI Li-shun
(*National Research Center for Anti-Computer Invasion & Virus Prevention, Key Laboratory for Information & Network Security of Ministry of Public Security, Third Research Institute of Ministry of Public Security, Shanghai* 200031, *China*)

Abstract: In order to protect the information and network security during cross-domain access, this paper proposed a model for cross-domain access control and border protection based on in-depth analysis of the security risk faced by it. The model divided policy enforcement and policy decision into two phases: intra-domain and cross-domain, and applied various security techniques in addition. Also protected the confidentiality, integrity and availability during information transmission process effectively. As a result, solved the access control and border protection problems of cross-domain access process effectively.
Key words: access control; security domain; border protection; identity authentication; security policy

根据 ISO/IEC 18028-3 [1]标准定义的安全域(domain)概念为:具有相同安全需求的一组资产和资源的集合,即同一安全域内部具有相同的安全保护需求,服从相同的整体安全策略。不同安全域内运行不同的业务功能,而彼此之间需要信息交换。

定义安全域内部包括以下基本元素:公钥基础设施 PKI、授权管理基础设施 PMI、用户(user)、资源(resource)、策略实施点(policy enforcement point,PEP)、策略决策点(policy decision point,PDP)、策略库(policy repository,PR)等。

PKI 为内部用户颁发用户数字证书(userCreds)用于身份识别,PMI 的属性权威(AA)服务器通过签发属性证书(attrCreds)为用户分配角色完成对用户的授权。

安全域内部的资源包括 Web 服务、文件服务等各类应用系统。

策略实施点(PEP)是介于用户与目标资源之间的一种应用或服务,被用来根据策略决策实施访问操作。当用户申请访问时,PEP 向 PDP 申请授权,并根据授权决策的结果实施决策,即对目标资源执行访问或者拒绝访问。在具体的应用中,策略实施点可能是应用程序内部中进行访问控制的一段代码,也可能是安全的应用服务器(如在 Web 服务器上增加一个访问控制插件),或者是进行访问控制的安全网关。

策略决策点(PDP)也叫授权策略服务器,它接收和评价授权请求,根据请求上下文(context)及预定义的安全策略作出策略决策。当接收到一个授权请求时,PDP 会从 PR 中获得策略数据,根据策略逻辑、访问者的安全属性以及当前条件进行决策,并将决策结果返回给应用。在应用中,决策点是一个判断逻辑,它或者与实施点结合在一起,或者单独运行于一个独立的服务器上。最简单的情况是决策点根据访问控制列表(access control list,ACL)进行查表操作,判断用户的权限。

策略库存储授权策略(policy),即用于确定一个主体是否能对客体拥有访问能力的一套规则。

假定需进行跨域访问的任意两个域间存在不经过第三方域的直接网络通道。

跨域访问所面临的安全风险主要集中在三个方面:a)信任关系问题,即如何建立跨域访问过程中的相互信任关系和确定资源访问的权限;b)边界防御问题,即如何防范跨域访问过程中对安全域的攻击、入侵及病毒传播;c)信息交换问题,即如何保证跨域访问过程中信息传输的保密性、完整性和可用性。

1 相关研究

访问控制模型定义了主体、客体、访问是如何表示和操作的,它决定了授权策略的表达能力和灵活性。传统的访问控制模型包括自主访问控制(DAC)和强制访问控制(MAC)模型。除自主访问控制和强制访问控制外,目前主要的访问控制模型包括基于角色的访问控制(RBAC) [2]、基于属性的访问控制

收稿日期: 2009-06-29; **修回日期**: 2009-08-31 **基金项目**: 国家"863"计划资助项目(2006AA01Z450,2008AA01Z412)
作者简介:邹翔(1977-),男,安徽马鞍山人,副研究员,博士,主要研究方向为信息安全、网络安全(xiangz@mail.trimps.ac.cn);金波(1972-),男,研究员,博士,主要研究方向为信息安全、网络安全;倪力舜(1979-),男,助理研究员,硕士,主要研究方向为网络安全、数据库.

(ABAC)[3]和 usage control(UC)模型[4]。

RBAC 的基本思想是在用户与访问权限(permission)之间引入角色(role)的概念,用户与特定的一个或多个角色相联系,角色与一个或多个访问许可权相联系,角色可以根据实际的工作需要生成或取消。RBAC 在 2004 年 2 月被美国国家标准委员会(ANSI)和 IT 国际标准委员会(INCITS)接纳为 ANSI INCITS 359—2004 标准。

基于属性的访问控制模型是近年来较受关注的访问控制模型,ABAC 不是以用户的标志来进行访问控制,而是使用用户、对象以及环境的属性来进行访问控制,特别适合于如 Web services、P2P 系统等用户群数量庞大的网络应用。

Usage control 模型主要关注分布式信息的访问控制,包含四个基本元素,即主体、客体、权限和授权规则,另外也定义了义务(obligation)、条件(condition)、持续性(continuity)和易变性(mutability)。授权规则、条件、义务与授权过程相关,它们是决定一个主体是否有某种权限能对客体进行访问的决策因素。

在跨域访问控制方面,基于角色转换的域间互操作模型 IRBAC2000[5]提出一个安全域间动态角色转换模型,通过在安全域间两两相互定义角色转换关系,完成域间角色的动态转换。IRBAC2000 支持角色层次概念,所有上层角色在跨域映射中同样获得所有目标域的映射角色的所有下层角色的权限。文献[6]基于 PKI 实现跨域访问控制,系统使用两种证书验证用户角色权限,用户角色证书标志用户身份和角色,角色层次证书标志角色层次关系。服务域对客户域中某角色授权后,客户域用户如果拥有该角色或其上级角色,则可通过提供为此用户分配的角色证书以及此角色到相应角色的角色层次证书(可能是一个证书链)获得对服务域的访问。文献[7,8]提出扩展经典的 RBAC 模型以解决分布式协同环境中分布式层次资源的管理和访问控制问题,使用 XACML(extensible access control markup language)描述安全域间访问控制策略。

以上跨域访问控制研究考虑了域间角色映射与转换及角色、资源层次等问题,但在跨域访问过程中,各安全域边界所面临的安全风险进一步增加。如何解决整个跨域访问过程中各安全域的边界防御问题缺乏较好的解决方法。

网络边界安全防御一直是防范外部攻击和内部信息泄露的重要手段。ISO/IEC 18028-3[8]将安全域的划分与网络区域相结合,将保证安全策略的安全措施实现集中地落在了安全域的边界上。DODD8500.1[9]提出对安全域的保护是通过安全域边界保护和飞地边界保护共同实现的,既防止内部用户的越权访问,同时防止来自飞地外部的攻击和防止内部信息泄露到飞地外部。

2　跨域访问控制与边界防御模型

针对跨域访问控制所面临的安全风险,笔者设计了跨域访问控制与边界防御模型,如图 1 所示。

在策略实施方面,每个 domain 将 PEP 分为内部策略实施点(internal policy enforcement point,IPEP)和边界策略实施点(border policy enforcement point,BPEP)两部分。其中 IPEP 位于 domain 内部,根据策略决策实施对 domain 内部所有资源的访问操作;BPEP 位于 domain 边界,根据策略决策实施所有跨域访问操作。以图 1 中 domain A 为例,即 IPEP-A 与 BPEP-A。

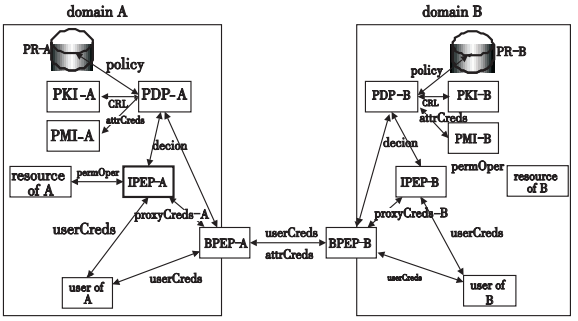

图1　跨域访问控制与边界防御模型图

BPEP-A 不仅负责根据策略决策实施来自其他安全域(如 domain B)访问请求的所有跨域访问操作,同时作为 domain A 中所有对外访问请求的策略实施点,可以实施链路、网络、应用等多层次边界防御措施。同时,BPEP-A 还可作为审计控制点,实施对所有进出 domain A 边界行为的安全审计。在实施对 domain A 内部资源的访问过程中,为保护 domain 内部资源和网络安全,BPEP-A 并不允许其他安全域用户直接访问内部资源,而是根据角色映射关系,将其他安全域用户映射为 BPEP-A 中预设的代理用户(以代理证书 proxyCreds 方式表示),然后以 proxyCreds 身份将访问请求以应用代理方式发送给 IPEP-A,IPEP-A 所看到的只是代理证书,可采用与其他 domain A 内部用户一致的方式实施由 PDP-A 作出的策略决策。

策略访问点 PDP-A 接收和评价 IPEP-A 和 BPEP-A 授权请求,根据用户、角色、资源、请求类型等信息,依据安全策略作出不同的策略决策。PDP-A 可从策略库 PR-A 查询已制定的安全策略,从 PKI-A 查询用户证书 userCreds 状态,从 PMI-A 查询用户证书对应的属性证书 attrCreds。PKI-A 和 PMI-A 提供 LDAP 服务单元或 OCSP 服务单元,支持对证书状态信息(包括证书撤销列表 CRL)和属性证书信息的非实时和实时查询。

策略决策分为对内和对外两类:对内策略决策决定是否允许对内部资源的访问请求,请求可以来自于本安全域内部或其他安全域;对外策略决策决定是否允许用户(user)对外发起访问请求。

3　访问控制过程

定义跨域访问用户 user 所在安全域为发起域(originate domain),记为 domain-O;目标资源 resource 所在域为目标域(target domain),记为 domain-T。

跨域访问控制过程可划分为两个阶段,即域内阶段和跨域阶段。域内阶段指在访问用户在 domain-O 内部的访问控制过程,跨域阶段指用户从 domain-O 边界到完成对 domain-T 内的目标资源访问或访问中止的访问控制过程。

3.1　域内阶段

域内阶段访问控制过程如图 2 所示。

a)步骤(1)~(3),domain O 中 user 向 BPEP-O 发出跨域访问请求,BPEP-O 要求 user 提供身份证书及其他认证信息,user 提交自己的用户身份证书 userCreds 给 BPEP-O。

b)步骤(4),BPEP-O 根据预置的 PKI-O 证书链,验证 userCreds 是否为 PKI-O 颁发,即是否为本安全域内可信主体。

c)步骤(5),BPEP-O 为通过认证的 user 生成决策请求,并将其发往 PDP-O。

d)步骤(6)~(8),PDP-O 进行策略决策。

PDP-O 首先向 PKI-O 检查用户身份证书状态,检查可基于定时下载的证书撤销列表 CRL 或基于 OCSP 协议进行实时查询。如果证书状态不正常(撤销、停用、过期等),则返回出错信息给 BPEP-O,访问中止(6.1)。接着,PDP-O 向 PMI-O 查询用户对应的属性证书,属性证书一般以 LDAP 形式发布。如果无法获取属性证书,说明该用户尚未进行授权,则返回出错信息给 BPEP-O,访问中止(7.1)。最后,PDP-O 向策略库 PR-O 查询安全策略,通过匹配规则判断是否允许本次跨域访问。如果没有匹配到允许访问的规则,则返回出错信息给 BPEP-O,访问中止(8.1)。

e)步骤(9),PDP-O 向 BPEP-O 发送决策结果。

f)步骤(10),如果决策结果为允许,BPEP-O 执行跨域访问,进入跨域阶段。

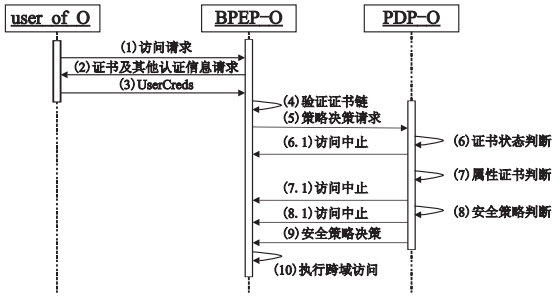

图2 域内阶段访问控制过程图

3.2 跨域阶段

跨域阶段访问控制过程如图 3 所示。

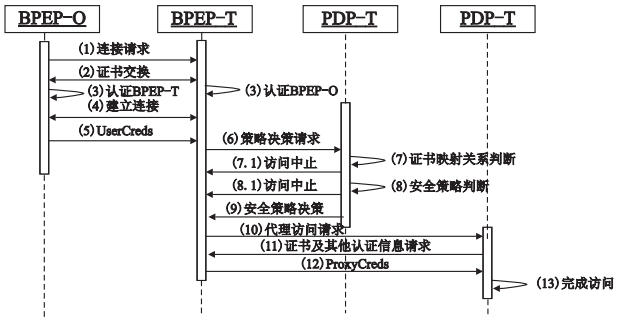

图3 跨域阶段访问控制过程图

a)步骤(1)~(4),BPEP-O 与 BPEP-T 进行基于数字证书的双向身份认证,建立安全连接。此过程可以预先进行,如 BPEP-O 和 BPEP-T 启动时进行。并且,假定 domain O 和 domain T 已预先交换证书链或相互签发交叉证书[10]。BPEP-O 与 BPEP-T 交互认证成功后,可建立 IPSec 或 SSL 方式的安全隧道,可有效保障信息传输过程中的保密性和完整性。

b)步骤(5),BPEP-O 将用户身份证书 userCreds 和属性证书 attrCreds 提交给 BPEP-T。

c)步骤(6),BPEP-T 根据 userCreds 和 attrCreds 生成决策请求,并将其发往 PDP-T。

d)步骤(6)~(8),PDP-T 进行策略决策。

PDP-T 首先根据 userCreds 和 attrCreds 查询证书映射表,获取证书映射关系。如果无法获取证书映射关系,说明该用户或角色在 domain T 中尚未进行授权,则返回出错信息给 BPEP-O(BPEP-O 可进一步传递出错信息),访问中止(6.1)。

接着,PDP-T 向策略库 PR-T 查询安全策略,通过匹配规则判断是否允许本次跨域访问。如果没有匹配到允许访问的规则,说明该用户或角色在 domain T 中不允许进行本次操作,则返回出错信息给 BPEP-T(BPEP-T 可进一步传递出错信息),访问中止(7.1)。

e)步骤(9),PDP-T 向 BPEP-T 发送决策结果和证书映射关系。

f)步骤(10)~(12),BPEP-T 生成代理访问请求发送给 IPEP-T,并根据证书映射关系取出本地存储的代理证书提交给 IPEP-T。

g)步骤(13),IPEP-T 收到代理访问请求,根据代理证书判断出本次访问为代理访问,则执行访问请求,完成对目标资源的操作。

4 结束语

本文首先就跨域访问问题和所涉及的面临的安全风险进行了定义,在分析相关研究的基础上,设计了跨域访问控制与边界防御模型,该模型将策略实施点 PEP 分为内部策略实施点和边界策略实施点,相应地将策略决策也划分为域内和跨域两类。最后,详细分析了基于上述模型的跨域访问控制过程。在此过程中,该模型基于发起域与目标域的安全策略实现了发起域边界和目标域边界的网络访问控制,以及目标资源的应用访问控制,从而有效解决了安全域的边界防御以及信息资源的访问控制问题。下一步工作将着眼于该模型的实现优化和应用等方面。

参考文献:

[1] ISO/IEC 18028-3,信息技术.安全技术.IT 网络安全.第 3 部分:使用安全网关的网络间的安全通信[S]. Switzerland: ISO/IEC, 2005.

[2] FERRAIOLO D, SANDHU R, GAVRILA S. *et al*. Proposed NIST standard for role-based access control[J]. ACM Trans on Information and System Security, 2001, 4(3):224-274.

[3] YUAN E, TONG J. Attribute based access control(ABAC) for Web services[C]//Proc of IEEE International Conference on Information Technology: Coding and Computing. Orlando, Florida: IEEE Computer Society, 2005:561-569.

[4] PARK J, SANDHU R. The UCONABC usage control model[J]. ACM Trans on Information and System Security, 2004, 7(1): 128-174.

[5] KAPADIA A, MUHTADI J A, CAMPBELL R H, *et al*. IRBAC secure interoperability using dynamic role translation, UIUCDCS-R-2000-2162[R]. [S.l.]: University of Illinois, 2000.

[6] DENKER G, MILLEN J, MIYAKE Y. Cross-domain access control via PKI[C]//Proc of the 3rd International Workshop on Policies of Distributed Systems and Networks. [S.l.]: IEEE Press, 2002:202-205.

[7] DEMCHENKO Y, De LAAT C, GOMMANS L, *et al*. Domain based access control model for distributed collaborative applications[C]// Proc of the 2nd IEEE International Conference on E-Science and Grid Computing. [S.l.]: IEEE Computer Society, 2006:24.

[8] DEMCHENKO Y, GOMMANS L, De LAAT C. Extending role based access control model for distributed multidomain applications[C]// Proc of International Federation for Information Processing. Boston: Springer, 2007:301-312.

[9] Department of Defense. Department of Defense Directive 8500.1 [EB/OL].(2002)[2007-04-23]. http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf.

[10] LINN J. Trust models and management in public-key infrastructures [R]. [S.l.]: RSA Data Security Inc, 2000.