基于角色访问控制的入侵容忍机制研究

彭文灵[1,2],王丽娜[1],张焕国[1],傅建明[1]
(1. 武汉大学计算机学院,软件工程国家重点实验室,湖北武汉 430079;
2. 赣南师范学院网络中心,江西赣州 341000)

摘 要: 系统在受到入侵的情况下,如何仍能为用户提供规定的服务成为了当前网络安全技术中的一个重要问题. 该文结合入侵容忍和基于角色的访问控制技术的特点,提出了一种基于角色访问控制的入侵容忍安全架构,给出了它的模型和基本组成. 在网络分布式计算环境中,采用基于角色的访问控制技术的策略,从角色管理服务器、角色冒充、数据和应用服务器四个方面阐述了该架构的容侵机制,从而保证服务系统的安全性和可用性,实现整个系统的入侵容忍.

关键词: 入侵容忍; 访问控制; 角色; 信息安全
中图分类号: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2005) 01-0091-05

Research on Intrusion Tolerant Architecture Based on Role-Based Access Control

PENG Wen-ling[1,2], WANG Li-na[1], ZHANG Huan-guo[1], FU Jian-ming[1]
(1. *School of Computer, State Key Laboratory of Software Engineering, Wuhan University, Wuhan, Hubei* 430079, *China*;
2. *Network Center, Gannan Teachers College, Ganzhou, Jiangxi* 341000, *China*)

Abstract: It is an important problem that how can continue to function correctly and to provide the intended services to legitimate user in a timely manner even in the face of an attack. An intrusion tolerant architecture, which is based on role-based access control scheme, is proposed in this paper. Our method is built upon the analysis of intrusion effects rather than intrusion causes. The characteristics, model and components of intrusion tolerant architecture are discussed in detail. In the distributed network computing environment, utilized the strategy of role-based access control, the intrusion tolerant mechanism is expounded from role-administer server, role pretending, data server and application server. The presented intrusion tolerant architecture guarantees the security and availability of the protected server, which enhances intrusion tolerant ability of server.

Key words: intrusion tolerant; access control; role; information security

1 引言

随着计算机技术的迅速发展和广泛应用,网络安全显得尤其重要,其根本目标就是要保障计算机中信息的保密性、完整性和可用性. 为此,人们通过防火墙、入侵检测等安全技术,把非法入侵阻挡在被保护的系统之外. 但目前为止,它们只能较有效地抵挡已知的和定义好的攻击,而对于新出现的攻击方法,它们抵御和检测的措施或策略往往是滞后的,且目前入侵检测系统的性能(误警率和检测率)没有得到很大的提高,系统仍然有很大被入侵的可能,因此在系统存在入侵的情况下,系统如何仍能为合法用户提供服务就成为了一个重要问题.

人体的健壮性可以容忍大多病菌和病毒的入侵,给人们以启示,网络系统也可像人体一样形成具有容忍入侵能力的入侵容忍系统 ITS(Intrusion Tolerant System,简称容侵系统)[1]. 它与入侵检测技术不同,它主要考虑的是在存在入侵的情况下系统的生存能力,所关注的是入侵造成的影响而不是入侵的原因. 它必须具有能及时自我诊断、恢复和重构的能力,并能为合法用户提供所需的全部或者降级的服务.

同时,基于角色的访问控制 RBAC(Role-Based Access Control)技术是近年来安全访问控制领域的研究热点,越来越受到人们的重视. 特别是在互联网中安全管理机制由于具有很大的复杂性,而且用户对服务器资源的需求是动态变化的,RBAC 就提供了系统资源访问权限的有效控制,它提供角色的概念和基于角色的灵活的管理策略,适应于保证系统的安全性.

由于入侵容忍(简称容侵)技术不仅要考虑对入侵或攻击的防御,而且还要解决在入侵存在的情况下系统的生存性和抗毁能力问题. 通观病毒与入侵,不难发现试图干扰或侵害系统正常运行的恶意代码或数据都有一个共同点,这个共同点

收稿日期:2003-11-14;修回日期:2004-12-02
基金项目:国家自然科学基金(No. 60473023; No. 60373087; No. 90104005),国家 863 项目(No. 2002AA141051),教育部博士点基金项目(No. 20020486046).

就是所有这些破坏因素都离不开两个关键因素:资源与控制(Resource and Control).但 RBAC 对于系统资源访问权限的有效控制具有非常好的基础,为此,本文将 RBAC 策略与 ITS 技术相结合,建立容忍入侵的系统结构,即一旦攻击者的入侵使入侵检测系统出现漏检的情况,仍可以在规定程度上屏蔽入侵对系统功能的影响,并继续为合法用户提供全部或者降级的服务.

2 入侵容忍系统和基于角色的访问控制

2.1 入侵容忍系统

网络入侵容忍系统,也就是当一个网络系统遭受非法入侵后,其中的防护安全技术都失效或者不能完全排除入侵所造成的影响时,即使系统的某些组件遭受攻击者的破坏,但容侵系统仍能及时自我诊断、恢复和重构,并能为合法用户提供所需的全部或者降级的服务[2].

从定义和设计目标上可以看出,作为一个整体,容侵系统 ITS 成为了网络安全保护的最终防线,系统在遭到一定的入侵后,提供服务的应用服务器(或服务器组)不仅需要能够抵抗一些简单攻击和发现入侵行为,更关键的是,能够在受到攻击或已经被入侵的情况下,仍能提供其既定的服务,必要的时候提供降级服务,并保持一定的安全底限,保护服务器上数据的秘密性和完整性.

容侵系统与容错系统不同,后者所容忍的主要着眼于故障、大多是非人为的;而前者所容忍的是入侵、主要是人为的且是不可预知的.

由于 ITS 是建立在入侵检测、容错理论和密码理论基础上的系统,因此它所采取的方法也大多来源于这些方面,它涉及到:

(1) 检测:容侵系统中最前线的就是入侵检测系统.但容侵系统的检测模块与独立的入侵检测系统不同在于:前者的行为往往与容侵系统的其他部分是联动的、紧密耦合的.容侵系统对前者在实时性、准确性方面提出了更高的要求.因此,前者在结构、方法等方面有别于后者.而后者更注重于学习性、自适应性等方面.

(2) 相关算法:由于容侵系统是主要建立在容错理论和密码理论基础上的网络安全系统,因此容侵系统中将会使用到许多与容错和密码相关的算法.例如:冗余(redundancy)/屏蔽(mask)算法,检错/纠错算法,门限密码方法,分布式密钥生成算法及其使用方法等.同时,作为网络系统,容侵系统还涉及到相关协议.

(3) 重组与恢复:在容侵系统中,重组与恢复更多地考虑参与各方的诚实性和连续性.在重组和恢复过程中,系统将整体的安全性和继续提供服务(或部分服务)的能力放在了首要的位置上.

2.2 基于角色的访问控制 RBAC

基于角色的访问控制(RBAC)是美国 NIST(National Institute of Standards and Technology)在 90 年代初提出的一种新的访问控制技术[3].访问控制服务的主要目标就是阻止非授权用户对机密信息的访问,防止非法用户的侵入或合法用户的不慎操作所造成的破坏.

RBAC 模型主要由三部分组成,即用户、角色和权限,其中用户是指信息系统的合法使用者,包括普通用户和系统管理员;角色是指权限的集合,包括普通角色和管理角色;权限是指用户对客体(信息系统)的操作功能,包括普通用户权限和管理权限.

RBAC 的基本思想[4]是:如图 1,由用户在一个组织中担当的角色来确定用户在系统中的访问权限,也就是用角色来充当用户行使权限的中介,安全的管理就可以根据需要定义各种各样的角色,并设置合适的访问权限,而用户根据其责任和权利被指派为不同的角色.这样整个访问控制过程就被分成了两部分,即访问权限与角色相关联,角色再与用户相关联,从而实现了用户与访问权限的逻辑分离.RBAC 技术用角色实施对系统资源访问权限的统一管理,具有减少授权管理复杂性,降低系统开销的特点.

图 1 基于角色的访问控制技术的基本思想

定义 1 权限(Privileges)定义为一个二元组(ob,op),其中 ob(objects)是系统中的客体,客体是一种可识别的信息实体,它们蕴涵或接收信息,如文件、目录、服务等,一个客体可以包含另外一个客体,如 owner,group name 等.它也可以用 object ID 表示;op(operations)是客体 ob 上的访问方法集,它是一个集合,可能包含不止一种访问方法,如 read,write,execute,create 或 rw,rc 等.

定义 2 角色(Roles)是一个或一群用户在组织内可执行的操作的集合.它是一个可以完成一定权限的命名组,定义为一个二元组(rname,rpset),其中:rname 是角色的名称;rpset 是角色的权限集合.

定义 3 用户(Users)是系统的使用者,因为任务不同而拥有不同的权限.它定义为一个三元组(uname,urset,uarset),其中:uname 是用户名或用户的惟一标识 ID;urset 是用户的可以担当的角色集合;uarset 是用户已经激活(Activate)的角色集合.

由此,基于角色的授权原理是,先确定角色对服务的权限规范,用户被授予适当角色,然后再激活运行的角色,从而获得调用相应服务的权限.一个角色被激活,表示该用户正在履行此角色的职责.

利用集合的概念,我们就可给出基于角色的访问控制的一种简单的形式化描述[3~6].RBAC 的模型种类繁多,其中最著名的是 Sandhu[5]等人提出的 RBAC96 模型.但是目前 RBAC 还没有一个统一的国际标准,Ferraiolo[6]等人提出了 NIST 的 RBAC 建议标准,如果采用这个标准,RBAC 可以概括为以下主要操作[7]:

规则 1 把角色 R 授予用户 U,即把 R 放到用户 U 的 urset 中, $U.urset = U.urset + \{R\}$

规则 2 删除用户 U 的角色 R,即把 R 从用户 U 的 urset 中删去, $U.urset = U.urset - \{R\}$

规则 3 把权限 P 授予角色 R,即把权限 P 放到 R 的 rpset 中, $R.rpset = R.rpset + \{P\}$

规则 4　删除角色 R 的权限 P,即把权限 P 从 R 的 rpset 中删除掉,　R. rpset = R. rpset-{P}

规则 5　激活角色 R:

若 R ∈U. urset,则 U. uarset = U. uarset + {R},否则 U. uarset = U. uarset

规则 6　角色之间的限制:

角色之间的限制 SSD(static separation of duty):如果 R1 和 R2 满足 SSD,则两个角色不能同时分配给一个用户,即如果 R1 ∈U. urset,则 R2 ∉U. urset,反之亦然.

角色之间的限制 DSD(dynamic separation of duty):如果 R1 和 R2 满足 DSD,则两个角色虽然可以同时分配给一个用户,但不能被同时激活,即如果 R1 ∈U. uarset,则 R2 ∉U. uarset,反之亦然.

3　RBAC-ITS 的架构

3.1　RBAC-ITS 的架构

基于角色的访问控制技术的入侵容忍系统模型如图 2 所示,其中系统防御机制用防火墙等表示.

基于角色的访问控制技术的入侵容忍系统(RBAC-ITS)主要包括:角色管理组,服务器组,容侵审计组.

(1)角色管理组:它主要由一个或多个角色管理服务器(Role-assign,简记为 RA)组成,其中的一个称为主 RA,主 RA 的职责是:①过滤(filtering)和净化(sanitizing)用户的服务请求;②针对用户的服务请求,授权相应的角色,并起到负载平衡的作用;③并根据用户请求激活角色相对应的权限 AS;④AS 在处理角色激活的请求后返回到主 RA,主 RA 经过判断后,将结果提交给客户;⑤接收 ITA 传来的 AS 服务器信息,进行相应角色的权限调整,并及时通知各 RA 更替角色-权限信息. 其余 RA 是起辅助作用的,称为辅助 RA,辅助 RA 的负责是:①监督主 RA 的职责,当发现主 RA 滥用职责(角色不符)、主 RA 出现故障或被攻击时,同时通知其余 RA,在全体一致同意下,选取一个辅助 RA 取代主 RA 继续工作;②主 RA 忙时,接收主 RA 的指定临时协助任务完成,并及时返回主 RA 执行;③当主 RA 出现故障或被攻击时,及时恢复重构主 RA 的信息.

(2)COTS 应用服务器(Application Servers,简记为 AS):应用服务器组由在功能上具有一定冗余的多个服务器构成,其主要功能是为客户提供应用服务. 这些应用服务器分别运行于不同的操作系统平台,所有应用服务器都具有相同的功能. 考虑由多个主机 1,2,…,n 组成的一个服务器组和某一种可能具有安全隐患的系统属性 Attribute,属性可以有多种属性值,如数据库服务器组可以建立在不同的数据库管理系统 SQL Server、ORACLE 等. 即:Attribute = {S1,S2,…,Sn}. 其中:

Attribute(1) = …= Attribute(K1) = S1

Attribute(K1 + 1) = …= Attribute(K2) = S2

……

Attribute(Kn-1 + 1) = …= Attribute(Kn) = Sn

当某种类型的属性值可被攻击者成功利用时,认为该属性值的所有主机都可能同时为入侵者所成功入侵.

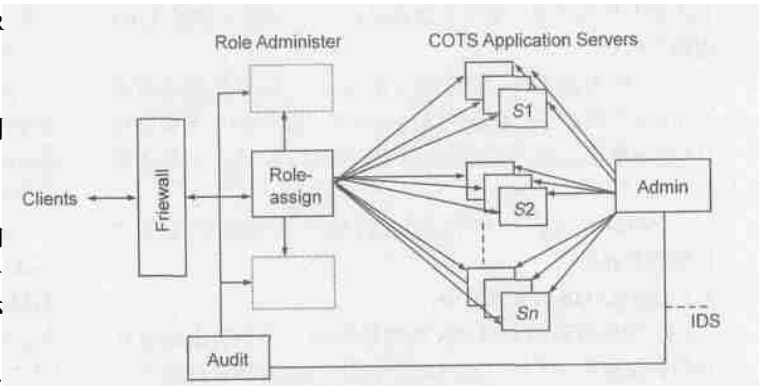

图 2　基于角色的访问控制技术的入侵容忍系统总体框图

应用服务器的个数取决于系统性能高低的要求. 机密的服务数据通过秘密共享[8]的方式加以保存,其中门限机密性保证了服务数据的机密性,门限可用性保证了服务数据的可用性;对于非机密的服务数据,其机密性无关紧要,重点是保持数据的可用性,因此仅需通过将服务数据复制在每台主机中即可.

(3)容侵审计组(Intrusion Tolerance Audit,ITA):它主要由包括一个或多个管理服务器(Administrator)的入侵检测系统和容侵审计服务器(Audit)组成.

管理服务器主要是及时发现出现问题或可疑的应用服务器,并暂时中断该类服务器的应用,进行故障处理. 同时,反馈给审计服务器调整 RA 中的 AS 使用策略和权限. 它定期向各 AS 发出请求,通过返回结果来确定系统的正确性,并正确调整各 AS 和 RA 对 AS 的状态记录. 每一应用服务器 AS 有一状态记录模块,由容侵审计组负责调整,同时 RA 也有各 AS 状态记录. 系统可划分为一系列的状态等级:正常状态(good state),脆弱状态(vulnerable state),被攻击状态(active attack state),安全关闭状态(fail secure state),降级状态(graceful degradation state),失控状态(failed state)等[9],ITA 可根据不同状态采取相应的策略进行 AS 的恢复.

审计服务器起着仲裁 RA 的运行和故障处理. 它对系统中有关安全的活动进行记录、检查及审核,主要目的就是检测和阻止非法用户篡夺角色或滥用权限对计算机系统的攻击.

3.2　RBAC-ITS 的工作机制

当用户请求服务时,运行过程如下:

(1)经过系统防御机制后,主 RA 过滤和净化用户的服务请求;

(2)针对有效用户的服务请求,主 RA 授权相应的角色 urset,按照算法(见 3.3 节)激活相应角色 uarset,并起到负载平衡的作用;

(3)根据用户激活的角色对应的权限访问 AS;其中角色—权限的建立取决于用户的操作对象,若是对一般数据进行操作,选择完成一个或多个 AS 的角色来处理用户请求. 若对机密数据进行操作,则必须选择能完成 t 个 AS 访问的角色来完成;

(4)辅助 RA 监视主 RA 的工作,发现主 RA 滥用职责(角

色不符)、出现故障或被攻击出现异常时,立即建立新的主 RA 继续工作;

(5) AS 根据角色—权限建立的用户请求,将处理结果返回 RA,ITA 根据安全策略判断,主 RA 在一定时间内未接收到 ITA 的异常报告后,结果返回用户,同时回收用户的角色授权.

(6) ITA 负责监视 AS 和各 RA 的运行,发现异常,立即进行隔离和处理.

3.3 RBAC-ITS 的容侵机制

3.3.1 角色管理服务器 RA 的容侵机制 用户请求经过系统防御机制后,RA 也可成为攻击者的目标.而该系统运行过程中,外界只与主 RA 联系,主 RA 的运行状态一直被辅助 RA 和 ITA 监视着,一旦发现异常或故障,立即发出信号,大家认可后,ITA 立即进行隔离和处理主 RA,并重新选取一个辅助 RA 代替主 RA 工作[10].

RA 的监视协议如下:

(1) 当主 RA 出现下列情况之一,认为异常或有故障:

A、滥用职责,即授权给用户的角色不符合、超出用户请求的;

B、不能在有限时间内授权、激活或回收角色给用户的;

C、辅助 RA 接受主 RA 的定期内部通信应答出现错误或故障;

当辅助 RA 出现下列情况之一,认为异常或有故障:

A、发出主 RA 异常的报警信息,经过其余辅助 RA 投票认为是错误的;

B、与其余 RA 的定期内部通信应答出现错误或故障的;

C、协助主 RA 工作时,滥用职责.

(2) 辅助 RA 或 ITA 发现主 RA 异常或有故障,进行广播,各辅助 RA 判断后,若多数认同,就选取一个辅助 RA 成为新的主 RA.若多数认为有误,对于发出信息的辅助 RA 由 ITA 进行隔离检查,等修复重构后投入工作.

3.3.2 "角色冒充"的容侵机制 基于角色的访问控制技术中,攻击者的目标就集中在"角色"的验证上,假设用户 A 向客体 ob(即各 AS)直接证明自己的角色,而攻击者 I 为了破坏 A 与 ob 相互"身份验证",只需要在他们之间将 A 发给 ob 的"角色"身份截取并转发给 ob,而将 ob 发给 A 的消息发给 A,在两者之间充当一个"桥梁",这样 I 就成功地对 AS 直接冒充了 A 的身份.如果首先进行主客体双方的角色安全激活,然后再进行握手,并将用户的激活角色提交给 AS,AS 从而判断用户的权限予以通信和提供服务,且在角色激活过程中不交换任何数据,便可有效在防止角色的直接冒充.

该用户的角色激活算法表示如下(在整个协议的设计中也可采用公钥算法与对称算法相结合):

Step1:U →RA:{uname,request}

Step2:RA →U:{uname,urset}

有效用户 U 向 RA 提出服务请求,主 RA 授权相应的角色 urset;

Step3:RA →AS:{uname,(ob,op)}

RA 根据 urset 集合中的应用服务器 AS 对应的客体 ob(一个或一组),与应用服务器 AS 发送服务请求.

Step4:AS →RA:{uname,ob,ST,B(Task)}

若 ob 是一组,每一个 AS 在接收到服务请求后都发送状态报告.状态报告包括本机的状态 ST 和忙闲因子 B(Task);忙闲因子由本机的性能指标和正在执行的任务数决定.

Step5:RA →U:{uname,uarset}

主 RA 或辅助 RA 根据各 AS 的状态 ST 和忙闲因子 B(Task),与本 RA 各 AS 状态 ST 记录相比较,以防 AS 欺诈,同时选择能完成请求的状态且忙闲因子最小或最小 t 台的 AS 决定激活用户角色 uarset.

3.3.3 机密数据的容侵机制 对于非机密的服务数据,其机密性无关紧要,重点是保持数据的可用性,因此仅需通过将服务数据复制在每台主机中即可.

对系统中的机密数据通过秘密共享的方式加以保存,采用(n,t)门限密码体制实现容忍入侵,其中门限机密性保证了服务数据的机密性,门限可用性保证了服务数据的可用性.将系统中的机密数据分成 n 份,分别存储在这 n 个应用服务器中,其中任何 t 个以上的应用服务器才能够重构机密数据,但任何小于 t 个应用服务器都不能重构机密数据,且不在任一台服务器上重构数据.这样只有当入侵者同时控制 n 个应用服务器中的 t 个以上,才能实现对机密数据操作.这样即使某个应用服务器被攻击,只要被攻破的服务器没有达到 t 个,就能够保证对机密数据的安全读取.且使得 K1,K2-K1,…,Kn-Kn-1 均小于 n-t 台,当某种类型的属性值可被攻击者成功利用时,认为该属性值的所有主机都可能同时为入侵者所成功入侵,在权限中二元组(ob,op)中 ob 将删除这些客体,也能保证其余属性的服务器 t 个以上的应用服务器重构机密数据.

3.3.4 应用服务器器容侵机制 (1) 攻击者盗用角色或滥用角色正对 COTS 应用服务器成功进行入侵时,当某 AS 或 ITA 系统及时发现后,

①对正提供攻击者处于服务状态的 AS,ITA 中管理服务器(Administrator)通知这些 AS 中止对该用户 uname 的权限服务;

②立即通过 ITA 通知 RA 停止分配和激活含有这些入侵客体 AS 的角色.

(2) 攻击者已对 COTS 应用服务器成功进行了入侵,当系统激活另一角色后,需要这一(组)AS 处于服务状态时,

①对于非机密的服务数据由于复制在每台主机中,若某用户要求服务而又无法提供时,或者某台服务器已经处在非正常状态时,ITA 通知 RA,在该用户包含该客体权限的角色删除,RA 重新激活新角色,进行服务.

②系统中的机密数据通过秘密共享的方式在 n 个应用服务器中,RA 选定 t 个完好的应用服务器,并激活相应角色,当在服务过程中,若 ITA 发现某台或几台服务器已经受到攻击时,ITA 通知 RA,在该用户的角色中将该角色回收(或删除),RA 重新激活另 t 个客体的角色,提供服务.

3.4 实例分析

假设当某用户(攻击者)A 已经取得角色激活(A,〈S1,rwc〉,〈S1,r〉)后,〈S1,r〉表示 A 具有对 S1 的读权限,但当 A 对

S1 服务器进行攻击,它可通过向被攻击的服务器发送大量的 ping 包,迫使其由正常状态变为被攻击状态,从而服务器服务关闭.

在这个实例中,当 S1 服务器服务关闭后,下一个角色中的 S1 服务激活就无法成功,RA 改用其他服务器提供相似服务.同时,ITA 发现 S1 已经进入服务关闭,通知 RA 对角色 S1 改为〈S1,0〉,攻击者 A 的激活角色也变为〈S1,0〉,这样 A 的访问停止.S1 由服务关闭状态恢复为正常状态,同时 RA 对角色 S1 又恢复为〈S1,rwc〉.

4　RBAC-ITS 的容侵的性能分析

(1)保证系统的安全性.安全管理包含了整个活动:授权、验证、监控和审计.用户在访问服务之前与客体无直接联系,他只有通过角色才享有该角色所对应的权限,从而访问相应的客体.当任务完成或有异常情况时,即失去角色,也就失去了对客体的访问权限.

如果一个应用服务器 S1 被攻击者掌握或泄露,由于 ITA 定期核查,当发现 S1 异常时,及时通知 RA,对应用 S1 的所有角色回收或删除.至于泄露秘密共享份额 di,服务器组 AS 具有多种系统属性 Attribute,可以预防同一种攻击造成对所有服务器的破坏,而且监控角色的活动,及时回收和删除也能控制攻击者的攻击范围扩大.

(2)保证服务的可用性.当入侵者对系统部分服务器的攻击已经成功以后,角色管理服务器利用自身的容错性、自治性,在系统中建立安全机制.如果一个应用服务器 S1 被攻击者掌握或泄露,而且通过角色的激活时调整访问客体,重新选取同属性或其他相同备份的服务器进行角色激活,而且应用服务器 AS 采用门限密码体制,将服务、数据等分散存储多个节点,通过节点集的安全保证系统的服务或降级服务,并可通过 ITA 的审计和监控,由于只须关注入侵造成的影响,所以只要判断不同状态采取相应的策略进行 AS 的重组和恢复,使整体系统回到正常状态、降级状态等提供服务.

(3)保证服务器上机密数据的秘密性.入侵者很难通过非法的途径同时获取了对全部或大部分服务器数据的访问角色,且门限机密性保证了服务数据的机密性.

5　结论

基于角色的访问控制技术随着网络的迅速发展,已经成为一种主流的访问控制技术,且在很多系统中被实现.入侵容忍技术是网络安全的又一个新方向,该文采用基于角色的访问控制技术的策略,将 RBAC 技术应用于容侵机制的研究,利用 RBAC 对系统资源访问权限的有效控制特性,以及网络系统自身的容错性、自治性,采用门限密码体制,提供的结构可以有效的抵御来自内、外的攻击,保护数据库等服务系统在受到攻击或已经被入侵的情况下,仍继续提供正确的服务,系统具有一定的灵活性,在电子商务等领域中有广阔的应用前景.

参考文献:

[1] 王丽娜,张焕国,傅建明.网络入侵容忍研究综述[A].第三届中国信息和通信安全学术论文集[C].北京:科学出版社,2003.39-45.

[2] Y Deswarte,L Blain,J C Fabre. Intrusion tolerance in distributed computing systems[J]. In Proc. of the International Symposium on Security and Privacy,Oakland (Ca.),IEEE press,May 20-22,1991. 110-121.

[3] R Sandhu,P Samarati. Access control:principles and practice[J]. IEEE Communications,1994,32(9):40-48.

[4] M Lebkicher. Role Based Access Control[EB/OL]. http://www.giac.org/practical/GSEC/Michael_Lebkicher_GSEC.pdf,2000.

[5] R Sandhu,E Coyne,H Feinstein,et al. Role-based access control models[J]. IEEE Computer,Feb 1996,29(2):38-47.

[6] D Ferraiolo,R Sandhu,S Gavrila,et al. Proposed NIST Standard for Role-Based Access Control[J]. ACM Transactions on Information and System Security (TISSEC),Aug 2001,4(3):224-274.

[7] 李斓,冯登国.多级关系数据库中的 RBAC[A].第三届中国信息和通信安全学术论文集[C].北京:科学出版社,2003,329-333.

[8] A Shamir. How to share a secret[J]. Communications of the ACM,1979,22(11):612-613.

[9] Gong F M,Katerina G,Wang F Y,et al. Characterizing Intrusion Tolerant Systems Using A State Transition Model[EB/OL]. http://www.anr.mcnc.org/projects/SITAR/papers/darpa00.pdf,2001.

[10] A Valdes,M Almgren,S Cheung,et al. An Adaptive Intrusion-Tolerant Server Architecture [EB/OL]. http://www.sdl.sri.com/users/valdes/DIT_arch.pdf,2002.

作者简介:

彭文灵　男,1969 年 11 月出生于江西宁都,副教授,现为武汉大学计算机学院博士研究生,研究方向为网络安全,网络管理. E-mail:whwlpeng@163.com.

王丽娜　女,1964 年 10 月出生于辽宁营口,现为武汉大学计算机学院教授,博士生导师,主要研究方向为网络安全,信息隐藏等.

张焕国　男,1945 年 6 月出生于河北元氏,中国密码学会理事,中国计算机学会容错专业委员会委员,现为武汉大学计算机学院教授,博士生导师,主要研究方向为演化密码,纠错编码,可信计算,智能卡,网络安全等.

傅建明　男,1969 年 9 月出生于湖南宁乡,博士,现为武汉大学计算机学院副教授,主要研究方向为网络行为,网络安全.