基于角色访问控制的入侵检测系统研究

喻 伟，庄玉册，毛凤翔，周顺生

（信阳学院数学与信息学院，河南 信阳 46400）

摘 要： 入侵检测系统是新型网络安全策略，它结合防火墙等静态防护技术，实现网络系统安全的动态检测和监控。本文结合入侵检测和基于角色控制技术，提出一种基于角色访问控制的入侵检测系统的安全架构，给出基本模型和组成，对产品架构进行有效分析，从而保证服务系统的安全性和可用性。

关键词： 入侵检测；访问控制；角色；网络安全

中图分类号：TP309 文献标志码：A 文章编号：1003-7241(2019)06-0104-05

Research On Intrusion Detection System Based On Role Access Control

YU Wei, ZHUANG Yu-ce, MAO Feng-xiang, ZHOU Shun-Sheng

(School of mathematics and information, Xinyang college, Xinyang 46400 China)

Abstract: Intrusion detection system is a new type of network security strategy. It combines the static protection technology such as firewall to realize the dynamic detection and monitoring of network system security. Based on intrusion detection and role based access control technology, this paper pus forward a kind of intrusion detection system based on role access control security architecture are given, basic model and composition, effective analysis of product architecture are given, so as to ensure the safety and availability of the service system.

Key words: intrusion detection; access control; role; network security

1 引言

计算机结构趋于简便，易于携带，技术革新推动网络的快速发展，网络安全逐渐成为新兴学科，网络安全已深入生活各个层面，是集计算机科学，网络技术，通信技术，信息安全技术为一体，向网络大规模化，复杂程度高的发展转变，通过对网络的监测，查处，应用，降低网络入侵发生的机率，减少财产信息泄露的危险[1]。传统的网络防护是以防火墙技术为主体，其余网络技术加以运用，已不能满足日常生活的需求，入侵检测系统得以快速发展，用于网络安全的防护工作。

入侵检测系统（IDS）是运用入侵检测技术对计算机系统中的若干关键点，收集计算机系统内的信息，并对收集的信息分析处理，从而发现网络或者系统内是否有违反安全策略的行为和遭受袭击的迹象。入侵检测技术可提高系统的反应速度，加强防卫实现对信息的有效管理。目前入侵检测技术手段居于综合化，复杂化，主要有智能化入侵检测，分布式入侵检测，数据库入侵检测，无线网络入侵检测[5]。

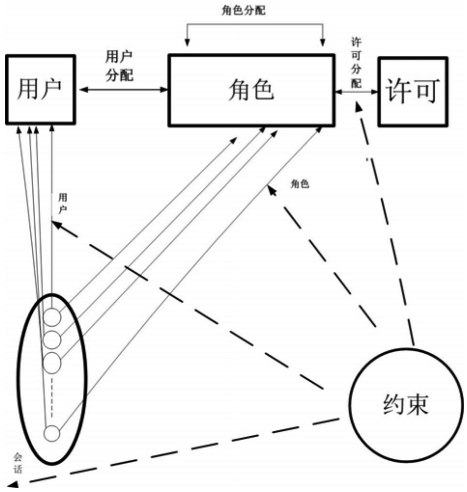

图1 角色访问控制流程

收稿日期：2018-03-28

如图1所示，基于角色的访问控制是当前较流行的访问控制方式，利用访问控制矩阵也可实现访问控制的目的。利用矩阵将单个用户与角色相互联系，从而给用户分配访问权，可对用户角色层次划分，达到对访问权限控制的目的。

用户与角色之间以及角色与许可之间的多对多关系比传统的自主访问控制(Discretionary Access Control. DAC)分配更加灵活及多粒度性，允许在文件中的一条记录中的一个字段的级别来控制访问[2]。

入侵检测系统不仅要防止外部有效的网络攻击进入到系统内部，渗透出机密性文件，而且要能够有预见性的对系统内部程序，器件有自我修复的能力，从防止入侵阶段至陌生网络信号进入阶段[3]，实时查询系统内部资源，寻找异常情况，一旦网络攻击成熟或频率升高，便自动启用系统的自我修复，以免自身检测系统因陌生不明攻击而停止正常工作，导致软件的进程提前结束。减少恶意程序代码对系统资源的破坏程度及内部程序资源的占用比。

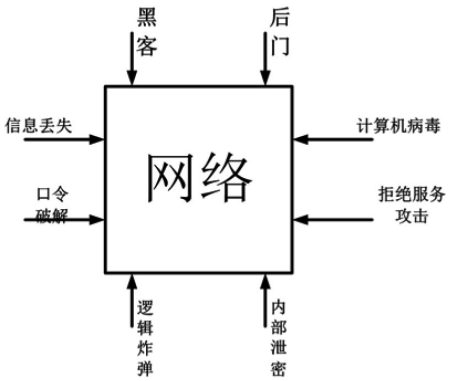

图2 网络入侵方式

如图2为网络入侵的主要方式，常规式病毒入侵人体，以第一道屏障作为保护，防止外部病毒的进入，但病毒一旦入侵人体，便产生宿主细胞，对人体感染，破坏，因此，入侵检测系统必须要有能够自动修复破坏程序的能力，阻止恶意程序的复制，有效的保障信息安全。

2 入侵检测系统和基于用户角色的访问控制

2.1 入侵检测系统

入侵检测系统能协助系统管理员的工作，为管理员的系统信息管理提供更加便捷性的服务，基本模型为通用入侵检测模型(Denning模型)，层次化入侵检测模型，管理式入侵检测模型(SNMP-IDSM)，入侵检测的原理是从信息源中收集信息[4]，包括计算机运行状态，内存存储，并对所接收的信息进行处理分析，能实现更好的应用效果，并对入侵用户产生进程攻击，破坏其非法入侵。如图3为典型网络入侵流程。

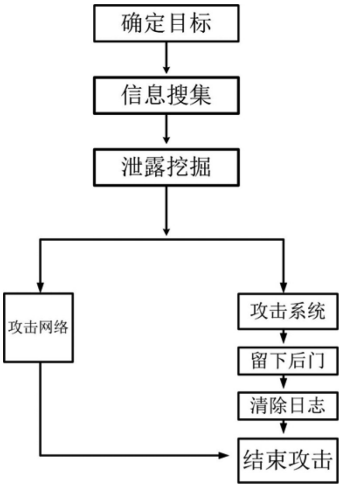

图3 典型网络入侵流程

基于传统网络布局的设计，入侵检测系统是网络安全保护的关键环节，系统内部资源信息在遭受陌生不明用户的入侵很大部分会造成内部系统资源的丢失[9]。入侵检测系统的工作流程同时会造成影响破坏，无法起到对内部人员的监视，或者不能够实时监测系统的正常工作及定时扫描侵入系统的错误代码，从而造成检测系统的瘫痪。

2.2 入侵检测系统的工作模式

(1) 管理器(Manager)：用于对用户提供收集到的各种数据及相应的分析结果。用户通过对管理器进行不同的参数设置完成用户目的期望，实现产品的检测功能的完善，使结果数据更加突出，更好的协助用户对计算机内部资源信息的管理。

传统的入侵检测系统的管理器工作模式过于单一，无法实现大规模的网络化管理，由于大规模集成电路出现，更加便捷性的管理器得以推广，应用更为普及。

感应器(Sensor)：负责收集信息，所收集的信息来源于系统主机的日志记录，网络数据包，或者来自于其他入侵检测系统的数据信息，利用感应器对所收到的信息，进行综合性的处理，以便于快速的到检测结果。

分析器(Analyzer)：用于判断所收集到的信息是否发生入侵行为，若检测到发生入侵行为，及时对入侵行为进行处理，拒绝为其继续提供服务，并将信息及时反馈给管理员。

(2) 常用算法：入侵检测系统应保持快速处理机制，使用改进的并行化K-Means算法CPK-Means和并行

化FT-Growth算法LBPEP.

3 入侵检测系统的工作模式

传统的自主访问控制(Discretionary Access Control.DAC)系统定义了单独的用户和访问权限,实体可以被授予这样的访问权限,按其意图使另一个实体访问系统的资源,但基于角色的访问控制是因主体的访问角色而自定的访问权限控制,便于管理,减少系统的内存资源的分配[2]。

基于角色的访问控制使角色,访问权,用户,系统资源,四者关系紧密联合,用户若[7]访问系统资源,得到内部存储信息记录必须由系统赋予用户一个角色,以便于认证处理,角色不同,访问权限不同,一个用户可以被分配多个角色,多个角色同时可以被分配一个角色,角色的复杂性越高,所访问系统资源越多,便于减少系统授权管理的复杂性。

定义1 用户(user)

用户是访问系统资源的直接访问者通过对用户分配不同的角色,用户访问系统的权限不同,可为用户定义为一个五元组<user,role,ID,time,where>,user为用户所访问时的用户名,便于统一管理存在于访问控制矩阵,便于下一次用户方便的进入,减少系统资源的开销[1],实现用户基本信息的对比,记录,为系统用户身份检测做准备。若同一个用户都以相同的角色访问系统资源,假使其中一次与多次与累积用户角色信息不符,可启动快速反应机制,对异样数据处理。ID为每一个用户都有的必须身份证明,系统授权每个用户的ID各不相同,保障系统认证安全,防止陌生用户盗取ID,欺骗系统实现获取系统资源的目的[10]。time是为方便记忆用户每次登录访问系统的时间,便于查询用户正常的工作机制。where为标注用户所访问的地点,可以自动获取用户访问的网络端口号及ip地址。

定义2 角色(role)

机构中控制计算机系统的命名工作职责,为每一个访问系统的用户定一个角色,角色可定义为三元组<role,access right,duty>表示所定义角色的访问权限及访问系统的资源的程度,但涉及核心系统资源的问题,系统可拒绝服务,减少信息泄露的风险。duty为角色访问的职责,有利于对系统的维护管理。

定义3 会话(session)

会话为用户与为其分配的角色集的激活子集之间的映射,定义会话为三元组<user,session,relation>,relation为用户与角色之间的对应关系。

定义4 约束(restrict)

约束提供另一种RBAC适应机构中的管理与安全策略的手段,便于对角色进行有效的管理。可定义约束为四元组<restruction,ruser,role,max>restrict为访问用户所分配的角色,通过互斥角色,指定前提条件,可使系统管理用户的能力提高,对角色的层次划分,上层角色可使用下层角色的权利,下层角色所访问的区域,上层角色都可以进行有效访问,max为定义最多的角色个数,最大范围内所行使的角色能力[7],为最大上限个数,所分配的角色不能越权进行系统资源的访问,各种访问角色之间有相同抑制的结果。

为便于对上述思想描述的更为具体清晰,故转化为集合表示,利用集合形式进行有效展示:

规则1:把角色role授予用户user,即是把角色添加用户user指定目录index中:

表示为:User.index=User.index+{role}

规则2:删除用户(user)的角色(role),即是把角色从用户(user)的指定目录index删去:

表示为:User.index=User.index-{role}

规则3:把权限Power许可给角色Role,即把权限Power放到role的index中:

表示为:Role.index=Role.index+{Power}

规则4:把权限收回,即不再许可角色给Role,即把权限从角色role的index中撤出power:

Role.index-{Power}

规则5:用户申请访问时,对用户所赋予的角色进行激活,使用户能够完成正常的访问活动。

若Role是User的子集,则表示为User.index=User.index+{role}

否则User.index=User.index

角色之间可进行相互限制,用户所访问的权限范围,在对角色激活的结果中,不能超过角色的最大使用个数,以免造成系统管理的混乱,对系统安全性构成威胁。

4 RBAC-IDS的架构

基于角色的访问控制的入侵检测系统的结构如图4。

主要包括:检测网络环境器(Check the network environment),角色管理组(role-assign),系统资源分配器(System resource distributor),监视系统(Monitor-

ing System),自我修复系统(Self repair system)。

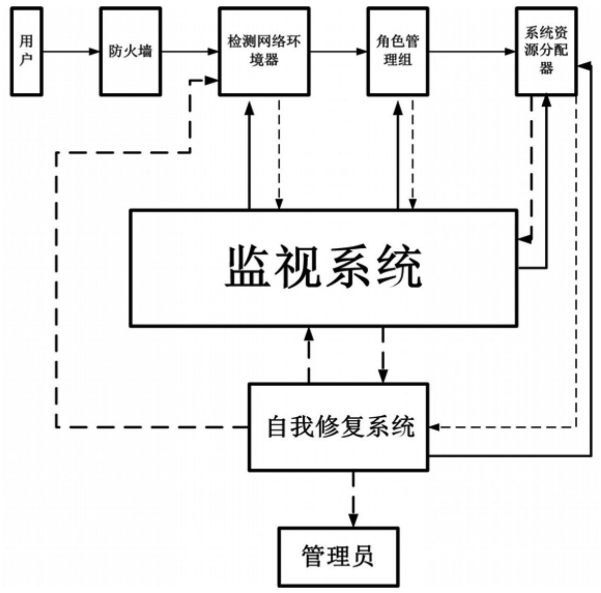

图4 RBAC-IDS系统框图

1.检测网络环境器[8](Check the network envirobment):当用户通过防火墙进入内网时,必需要使用检测网络环境器,保障正常的网络登陆环境,并可提前对用户进行入侵安全检测,充分确保可信赖的角色分配给用户实体,减少信息泄露的风险。

2.可对申请的信息进行过滤和净化,保持内部网络的通畅,针对不同的可疑用户请求的行为,采取不同的应对策略[6]。当某一时间节点突然出现大量用户访问时,并立即把反馈信息递交给监视系统,做好防护工作。

3.角色管理组(role-assign)

对用户所分配的角色进行管理,由二台服务器构成,其中一个为主服务器,当其中主服务器进行工作时,另一台辅助服务器负责对主服务器的行为进行监视,防止主服务器为傀儡主机,一旦发现数据库异常,用户访问权超过所角色赋予的权利之外,即判定主服务器发生异常,辅助服务器自动取代主服务器独立工作,同时在信道上发布广播数据包,告知所有连接点,对主服务器的申请信息进行屏蔽。

4.系统资源分配器(System resource distributor)

用户经合法检测认证后,可根据角色获取不同的访问权限,系统资源分配器对用户的角色进行分配,可允许多个角色同时访问,系统资源分配器可由多个系统服务器构成,满足大量用户进入的需求,方便统一管理,但当其中某台服务器出现异常,根据路由协议,其中最近的一台服务器负责识别,查询,并在路由列表中删除出现异常的服务器路由列表,立即在信道上广播处理。当自我修复系统收到信息,开始对异常服务器进行修复行为满足用户的访问需求。

5.监视系统(Monitoring System)(1)监视系统由一个或者多个入侵检测服务器组成,对于所在网络中的各个服务器,主机,一一进行监视活动,若发现异常活动,及时在网络中通知各个服务器,查询的一般方式是对各个服务器的日志,内存,流量进行监控和查看,便于及时发现网络中的可疑点,在处理信息方面,可和其他监视系统进行时时信息交换,即可以对自身原始数据审计,同时又可对本地检测系统报警结果统计。(2)监视服务器可对检测网络环境器,角色管理组,系统资源分配器发送简单报文,用于检测系统内的工作是否正常,提高安全性。同时对系统中有关的安全活动进行时时记录,跟踪,审核,其主要目的是检测和阻击非法用户篡夺角色或者滥用权限,导致危害系统资源信息的行为。

6.自我修复系统(Self repair system),应用于检测环境器,角色管理组,系统资源分配器等任何一方受到不同程度的攻击,用于以上服务器的修复工作。由监视系统发送反馈信息,自我修复系统负责对其修复工作,反馈的信息中涉及网络位置,产品信息等。已达到对其准确修复的目的[1]。

RBAC-IDS的工作机制

(1) 用户通过网络进入,申请系统资源访问,防火墙对用户访问机制进行控制,防止黑客的攻击。检测网络环境器对用户所处网络环境进行安全检测,并把信息反馈给监视系统。

(2) 针对有效的用户访问,角色管理组对用户角色赋值,激活用户角色权限,便于对系统资源的访问。

(3) 用户角色的信息传递给系统资源分配器,并对用户角色身份再次识别,确保用户身份安全并未出现数据异常的情况,开始授权用户的正常访问行为[8]。

(4) 用户进入内网,一直处于监视系统的监视范围之内,监视系统对于内网的服务器,主机,全面处理内存占用比率,网络中可以特征的行为,可对其隔离处理,或者拒绝为用户提供服务,把用户信息反馈给管理员。

(5) 监测系统在用户访问的一段时间没若未收到异常报告,则把结果返回给用户,同时收回用户的角色授权。

5 基于角色访问控制的入侵检测系统性能分析

(1) 保证系统的安全性。当今大部分操作系统都存

在系统漏洞的问题，引起安全方面的担忧。外在用户便利用系统漏洞的存在，有针对性的对内部软件系统进行攻击，以获取内部机密信息，用户躲避过防火墙的阻拦，进入入侵检测系统，入侵检测系统开始对用户的身份认证，扫描，减少非法用户入侵的机率[7]。基于角色访问控制的入侵检测系统便是对入侵检测系统功能的更加完善，保持检测的准确性，减少发生错误的概率。

（2）保证系统内部资源的保密性。基于角色管理组对所访问的用户赋予不同的角色，控制用户访问系统资源的权限，用户只有通过角色管理组获去角色的分配。用户在访问服务之前与客体无直接联系，当一旦检测用户状态异常，便收回角色，即用户立即无法对系统资源进行有效的访问，无法获取系统资源，监视系统[10]对检测网络环境器，角色管理组，系统资源分配器全程实行网络监控，监视系统监视系统可对网络定期测试，保证系统的安全性。以便在最短的时间内，结合现代的入侵检测技术消除网络安全的隐患，在此过程中，可以使用适当的维护软件对部分内部重要的软件进行补丁更新，必要时管理员可对入侵检测系统的配置进行修改，以满足客户的需求，提高检测的效率[9]。

（3）保证系统的完整性。当非法用户对系统内部资源访问时，有可能对内部配置修改，插入后门，便于逃避入侵检测系统的检测，实现下次进入的便捷性。但基于角色访问控制的入侵检测系统，可对病毒攻击的程序代码进行有效恢复。由监视系统反馈的信息快速查找出错的位置，完成对机密文件的快速反应机制。

6 结束语

随着无线网络的快速发展，安全问题逐渐暴露出来，入侵检测系统是伴随网络攻防与安全技术的逐步完善而不断发展起来的安全检测的方式。角色控制的访问模式和入侵检测系统相互结合，为网络安全主动防御提供正确的宝贵思路，提供的系统安全架构在网络安全方面具有高度的灵活性，在未来生产中，有很大的应用前景。

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] 薛静锋，祝烈煌.入侵检测技术[M].北京：人民邮电出版社，2017，(4)：36-137.

[3] 戴新宇，陈波.一种采用数据挖掘技术的入侵检测系统[J].自动化应用与技术，2005，24(6)：34-36.

[4] 柳景超，周立兵.一个改进的入侵检测系统模型[J].计算机与数字技术，2007，35(1)：97-99.

[5] 刘明川，彭长生.混合型入侵检测系统的研究[J].计算机工程与设计，2009，30(3)：547-551.

[6] 陈艳芳，申铉京，谢冲.分布式入侵检测系统监视代理及数据融合算法[J].吉林大学学报(信息版)，2006，24(1)：62-66.

[7] 徐慧，刘凤玉.多特征融合的入侵检测[J].计算机工程，2004，30(8)：103-105.

[8] 王雪霞，张泽琦，李明，杜军，王景璟，姜春晓，任勇.一种基于入侵检测的空间网络安全路由技术[J].电子技术应用，2015，41(4)：101-104.

[9] 李昊，张敏，冯登国，惠榛.大数据访问控制研究[J].计算机学报，2017，40(1)：72-91.

[10] 季伟东，王克奇.入侵检测系统安全性研究[J].自动化技术与应用，2009，28(9)：40-42.

[11] 王琪.入侵检测的原理及其在网络信息系统中的应用[J].情报科学，2004，22(10)：1272-1276.

作者简介：喻伟(1996-)，男，本科在读，研究方向：计算机科学与技术。