一个基于分权机制的分布式网络安全系统模型研究*)

A Distributed Security Model Based on Divide and Rule

陈 越 戴英侠 李镇江

(中国科大研究生院 信息安全国家重点实验室 北京100039)

Abstract In this paper, the authors analyze the defects of classical security model and ACL, which is now the most popular used method in access control. Then a new resolution based on "divide and rule" is discussed and a correspondent security model is depicted. In this model, the security system is divided into three parts: the policy management, the policy execution and the inspection. At last, the new model is compared with the classical one and its strongpoint is presented.

Keywords Distributed security model, Divide and rule, Polity, Inspection, Access control, ACL

1. 前言

网络技术飞速发展的今天,网络安全成为普遍关注的重要问题。最为经典的安全模型是Bell Lapadula模型,该模型以访问控制作为安全防卫的基本防线,把安全系统抽象为安全主体、访问对象和访问控制三大要素。从本质上说,Bell Lapadula模型是一个集中控制模型,我们认为这种集中控制模型在如下三方面存在缺陷:

1)目前安全系统所依赖的操作系统平台并不完全可靠,一旦入侵者控制或破坏了模型中的访问控制部件,整个安全系统就将陷入瘫痪失效状态,如防火墙系统,入侵者如果成功地占领一个防火墙,那他便可以以此为跳板,向下一个目标发起攻击;

2)目前各种分布式网络应用的安全需求细致而复杂,同一个安全访问主体在不同场合下可能具有完全不同的权限级别,被保护的被访问对象可能是带宽、路由等复杂的概念,难以用简单的实体概念来归纳,对它们的操作也不再是简单的读、写和添加;

3)分布计算环境下各个安全部件需要协同以完成统一的防卫目标,而经典的安全模型中并未提供相应的反馈、协同机制。例如,一个网上银行系统的防火墙规划、配置和维护就是一项艰难的工作,如何保证各个防火墙之间规划的一致性,如何监控这些防火墙的有效性,当网络银行内部主机受到外部IP的攻击时如何及时切断相应的网络连接并修改防火墙的过滤规则,如何有效地在协同各个安全部件时建立统一一致的安全审计信息,都是令人棘手的问题,消耗了大量的资源。

2. 改进思路

2.1 权限的分立

安全系统中,权限始终是进行控制的主要手段。与社会政治相类似,安全系统中权限的过分集中,如超级用户的设置,会给系统安全带来巨大风险,比如,一个黑客一旦掌握了操作系统的超级用户的口令,那么他将能够控制整个操作系统。

为了避免此类情况的发生,我们的基本思路是进行分权。把安全系统的基本角色划分为安全策略的管理者(立法)、安全策略的执行者(执法)和安全系统行为的监察者(监督)三个部分。安全策略的管理者负责表述、维护用户意图,把用户意图明确表达为安全系统所能理解的形式即策略规则,并在分布环境中维护其一致性;安全策略的执行者负责根据安全策略管理者所提供的描述,执行既定的安全策略;而监察者负责监督检查安全系统行为的有效性,根据监察策略提交监察报告,反馈到策略管理机构。

分权机制尤其是监督机制的引入有效减小了入侵者控制一个系统部件,从而可以取得整个系统的控制权。例如当入侵者取得策略执行部件的控制权而执行非法操作时,其行为就可能被监察者发现,从而触发系统的响应恢复行为。为了减小监察机构被入侵者攻破的概率,我们引入了镜像监察员机制,使非法入侵者对监察机构的破坏难度大幅度增加,这一机制将在稍后详细讨论。

2.2 监察机制

一个好的网络安全系统应该具备的重要功能是能对自身的有效性进行自动检测,即以一个较好的概率

*)基金项目:国家重点基础研究发展规划项目,项目编号 G1999035801。陈 越 研究生,研究方向:网络系统安全,分布式环境下的网络安全技术。

检测自身的异常，同时应能对其安全辖域内的被保护对象进行监察。

在传统的安全系统中，一般由系统管理员（人）对安全系统的所有部件直接进行监察，随着安全系统的日益复杂，人工监察方法已经难以适应复杂的网络环境。为此，我们在安全模型中引入了监察员（程序），由监察员对各个安全部件的有效性进行监察，保证安全系统的有效性维持在一个较高的水平。

在下面的证明中可以看到，引入监察员后的系统入侵发现概率要优于未引入时的情况。如图1所示，我们希望对B的异常进行监察。假设没有引入监察员A之前，当B异常时，系统管理员能以概率Pb监察B的异常，引入A后，在A没有被攻破的条件下，监察员A（程序）能以概率Pab监察B的异常，设A被入侵者攻破的概率为Pca，若当A被攻破后则不能对B进行有效监察，那么在A的监察下B的异常的检测概率Pb′为：

$$Pb' = [1-(1-Pb)(1-Pab)](1-Pca)+Pb\ Pca \quad (1)$$

可以看到，当Pb和Pca一定时，B的异常检测概率Pb′与A对B的检测概率Pab成线形递增关系，极端情况下，即使系统管理员对B的异常发现概率Pb为零，系统也能以概率Pab(1-Pca)检测出B的异常，当A失灵即Pca=1时，系统的异常检测概率下降为Pb。

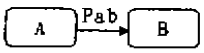

图1

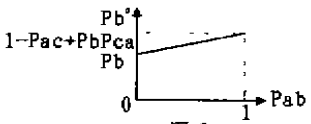

图2

图1　　图2

上述的监察模型依赖于A是否能正常工作，在A正常工作的情况下才能对B的有效性作出评价，A的可靠性越高，即Pca越小，则系统的监察可靠性越高。因此，如图3所示，我们引入镜像监察员机制，由两个相互独立的而又相互监督的实体组成。如果我们能创建特定的环境，使入侵者同时破坏这两个相互监督的监察实体（面对面的哨兵）足够困难，那么我们就可以信任这个镜像监察对进行系统的监察，从而分担系统管理员的负担。

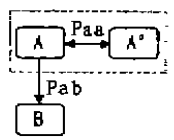

图3

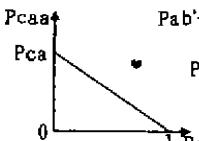

图4

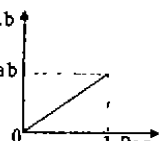

图5

下面证明镜像监察员优于单个的监察员。为了简化分析，不妨假设系统管理员不参加监察，即系统管理员的异常发现概率Pb=0。

假设A和A′是一对镜像监察员，当A(A′)没有被攻破时，它们之间的相互异常检测概率为Paa，A对B的异常检测概率为Pab，在A、A′不会被同时攻破的条件下，假设A单独被攻破的概率为Pca，A′单独被攻破的概率与A相同，当A和A′其中之一被攻破时，则说A对B进行的监察无效，假设A或A′被攻破但被及时发现，那么系统管理员可以立即对此进行有效恢复，但如果A、A′之一被攻破而且没有被发觉，那么我们说这对镜像监察员被攻破了。在镜像监察对中，A被攻破的概率Pca′=Pca(1−Paa)，同理，A′被攻破的概率也是Pca(1−Paa)，如果攻击者在镜像监察对的攻击中，首先攻击A的概率为P，首先攻击A′的概率为1−P，则整个镜像监察对被攻破的概率Pcaa=P Pca′+(1−P) Pca′=Pca(1−Paa)。可以看到，Pcaa与Paa成线形递减关系，且有Pcaa<pca，如图4所示，当镜像监察对之间的检测概率Paa趋近于1时，镜像监察对被攻破的概率Pcaa趋近于0，可见，镜像监察对的引入提高了监察员的可靠度。

根据上述推理，在系统管理员不参与的情况下(Pb=0)，A单独对B的异常监测概率Pab′=Pab(1−Pca)，其中Pab为A正常工作条件下对B异常的检测概率。引入镜像监察员A′后，镜像监察员对B的异常检测概率Pab″=Pab[1-Pca(1-Paa)]，其检测水平的提高幅度为Pab″−Pab′=PabPcaPaa，它与镜像监察对之间的异常检测概率Paa成线性递增关系，如图5所示。

当系统管理员的检测概率Pb不等于0时，根据(1)式，A单独实施监察时B的异常检测概率Pb′=[1-(1-Pb)(1-Pab)](1-Pca)+PbPca，在引入镜像监察对AA′后，对B的异常检测概率Pb″=[1-(1-Pb)(1-Pab)][1-Pca(1-Paa)]+PbPca(1-Paa)。引入镜像监察员后检测水平的提高幅度为Pb″−Pb′=PabPcaPaa(1-Pb)。可见，镜像监察员的引入提高了系统的异常发现水平。

2.3　策略控制

如前所述，经典的安全模型把安全系统划分为安全主体、被保护对象和访问控制规则集合等三个基本要素。目前访问控制最常用的描述方法是ACL方法，其推理逻辑可以概括为：因为该用户证明了其合法身份，所以根据访问控制表定义的规则，该用户可以对某个被保护资源进行某种访问操作。在复杂的分布式环境下，ACL方法已难以对各种复杂的访问控制需求作出贴切的刻画，其不足体现在几个方面：

首先，对于被保护资源的理解不能只限于简单的实体的概念，而应该扩展到一个更广泛的范畴。例如，一个文件控制系统把文件视为受保护的资源，但防火墙则可能把应用、路由和网络带宽视为受保护的资源，

CPU 的周期，包转发的优先级等都可以是资源，可以看到，对于资源的理解显然不是能用一个简单的实体的概念所能概括的。

其次，对于 资源访问控制所需满足的先决条件不能简单局限为安全主体的身份认证。一个主体要取得某个资源的访问权限，除了证明他自己的身份之外，完全有可能还要满足其他一系列条件。例如，一个公司的销售人员要远程获取该公司的机密技术资料时，他不仅要出示他的公司员工数字证书，还应该出示公司相关技术部门的授权证书，甚至有可能他所出示的授权证书对于该技术资料的访问时间只限于某个时间范围之内，或该技术资料需要至少有两个该公司的不同人员在场（出示数字证书）才能打开，这样的复杂情况是很难用经典的安全模型作出精确描述的。

再者，对于资源所能采取的操作不能简单理解为读、写、添加等简单的访问操作。例如路由的转发；再如受保护的资源完全可能是一个对象，而某个主体只有在满足安全策略所规定的一系列先决条件之后，才能以某一参数触发该对象的某个动作。

最后，经典的安全模型是一个集中式模型，难以清晰地描述分布条件下各地安全系统之间的协同关系。例如，在一个网站防卫系统中，WWW 服务器的入侵检测系统发现某个 IP 有非法企图，这时该入侵检测系统应该通知前端防火墙切断该 IP 的连接请求，这种协同关系用经典的安全模型同样难以描述。

策略方法是上述问题的较好解决方法。所谓安全策略就是描述一组安全策略规则集合的被命名的对象，是安全需求的高层规范与提供服务的底层配置之间的一种连接。策略方法的基本推理逻辑是：因为安全主体能够证明他满足安全策略所定义的先决条件集合 C，所以根据安全策略规则集合 R，该安全主体的行为可以限制在某一行为集合 T 之内，此外还可以定义协同策略以维护各个安全子系统策略的一致性。策略方法不仅可以使用规则集合描述复杂的情况，而且允许在规则间建立复杂的逻辑关系。和 ACL 方法相比，基于安全策略的解决办法能够更好地描述复杂的安全应用需求，能够更有效地在分布环境中进行协同，具有更优越的可伸缩性和灵活性。就目前的研究进展来看，策略控制同样是解决协同问题的有效方法，是目前研究的热点问题。

3. 一个基于分权机制的分布式网络安全模型

基于以上的分析与比较，下面提出一个分布式网络安全综合防卫模型，它基于古老的分权思想，在分布环境下把现代网络安全系统划分为安全策略的制定（立法）、安全策略的实施（执法）和监督三个环节，以策略控制作为系统协同的主要途径。与 Bell Lapadula 模型相同，本模型也以访问控制作为安全防卫的基本防线，与 Bell Lapadula 模型不同，本模型引入了监督机制，并以策略执行部件替代了经典的基于 ACL 的访问控制部件，模型示意图如下：

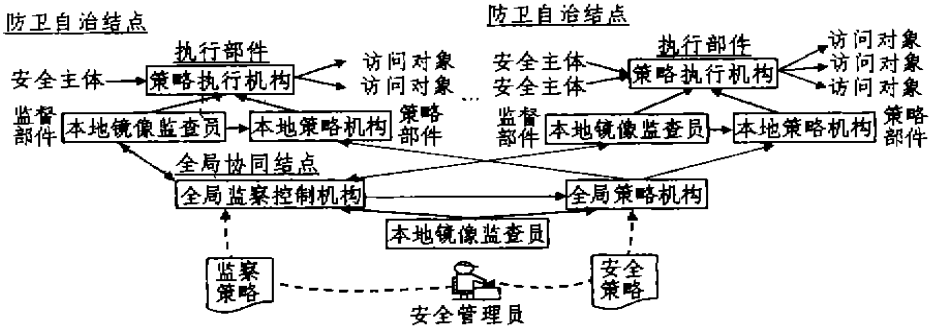

图6 模型示意图

模型由三个部件组成：1）基于安全策略部件，包括全局策略机构和各地策略机构；2）监督部件，包括全局监察控制机构和各地监察机构；3）执行部件，包括各地的策略执行部件。模型采用星型拓扑结构，由策略树和监察树复合组成，其中包括两类结点：防卫自治结点和全局协同结点。防卫自治结点负责对其安全辖域内的注册资源进行保护，全局协同结点则在全局范围内负责各自治结点间的协同。

全局策略机构 是安全管理上层意图的系统表述者，它负责制定、管理和维护辖域内的全局安全策略，协同、管理各地策略部件，分析、处理由全局监察控制部件提交的安全监测报告并及时修正安全策略，生成审计报告提交安全管理员，同时接受本地镜像监察员的监察。其中，策略的管理和维护包括策略的一致性检查与冲突检测、策略本身的安全性维护和策略的生存周期管理等内容。

本地策略机构 在全局策略机构的管理和协同下根据全局策略制定、管理和维护本地安全策略，分析、处理由本地监察部件提交的安全监测报告并修正本地安全策略，同时接受本地监察机构的监察。本地策略机

构的策略更新方式有两种，一种是全局策略机构主动对目标本地策略进行强制性更新，一种是本地策略机构主动向全局策略机构查询最新策略并进行更新。

本地执行机构 是安全访问主体与被访问对象之间的隔离者和基本防线，它监督、评价和控制安全访问主体对被访问对象的访问行为、贯彻执行由策略部件提供的安全策略，其行为的基本内容包括访问控制、协同和响应等，同时它还必须接受本地监察机构的监察。

全局监察控制机构 制定、管理和维护全局监察策略、管理、协同各地监察机构的监察行为，收集处理各地监察机构提交的监测报告并作进一步分析，生成全局监测报告递交全局策略机构，生成审计报告，同时接受本地镜像监察员的监督。

本地监察机构 在全局监察机构的管理下对本地安全策略机构和本地策略执行机构实施监督，采集监察范围内的各种安全事件信息并进行分析和评定，根据评定的结论生成监测报告，根据不同的评测结论监测报告分为两种，一种直接递交到本地策略机构作为本地安全策略响应或修正的依据，另一种上报到全局监察控制机构在全局范围内做进一步评判，同时本地监察机构还必须对监测信息作出审记备份并提交系统管理员。

模型的运作过程是，首先，安全需求目标被明确描述为安全策略规则，其基本内容至少应包括访问控制策略、协同策略、响应策略和监察策略，其中监察策略由监察部件独立控制，其他策略由策略部件独立控制。安全系统管理员根据制定的策略分别对策略部件和监察部件进行初始化，然后各个结点的策略执行机构对受保护资源的访问进行控制，监察部件根据监察策略对系统行为进行监察和评测，如对审计、日志信息的分析、对被检测系统状态进行轮询等，当发现异常时及时生成监测异常报告，根据预定的监察策略提交相应的策略机构，针对异常情况及时作出反馈性策略调整和补漏，调整后的新策略由策略执行部件执行，其中响应行为可能包括防卫行为和反击行为，在这个反馈性的响应过程中系统安全策略不断得到修正和完善，使系统防卫水平得以不断提高。在分布环境下以上各个过程可能需要不同结点间的协同，其协同的方式由协同策略定义，由全局策略机构和全局监察处理机构共同协调完成。

上述监察行为所面临的一个关键问题是系统异常的判决和分类，其判决过程和入侵检测系统的原理相类似，主要技术手段包括概率统计方法、神经网络方法、专家系统、模型推理和状态转换分析等，如果采用智能化方法的话，可以选择在各地的监察模块间交流学习经验，缩短训练时间，并在运行中提高检测水平。

可以看到，上述模型中包含两个反馈环：本地反馈环和全局反馈环，即策略的制定→策略的执行→执行监察→响应/修改策略→执行新的策略这一周期性过程。当系统异常事件发生时，监督系统可能采取的反馈行为有两种，一是根据设定的逻辑生成本地检测报告并递交本地策略机构，触发诸如切断路由、事件审计等行为，这种行为属于本地反馈；二是上报全局监察管理机构，由全局监察管理机构在全局范围内作出行为分析，再反馈到全局策略机构触发全局范围内的安全防卫响应，第二种响应行为属于全局反馈。

4. 性能比较

1）和经典模型相比，上述模型的最大特点是引入了分权和监督机制。当入侵者试图控制执行部件或策略部件时，其行为都可能被监察部件发现；而当入侵者试图首先控制监察部件时，又由于监察部件中镜像监察员机制的引入，大大增加了入侵者进行跳板式攻击的难度（即首先占领目标系统的一个部分，再以此为根据地向其他部分发起攻击）。同时，监察机制的引入改变了以往所有系统监察任务都由系统管理员承担的状况，不仅提高了系统的异常检测水平，也减轻了系统管理员的负担。

2）上述模型采用基于策略控制的方法取代了经典的基于访问控制表 ACL 的方法，对经典访问控制的潜在逻辑作出了扩展，使得本模型能够更好地适应各种复杂的安全需求。

3）在分布计算环境中，基于策略的安全控制方法使得模型具有更好的可协同性、适应性和可伸缩性。

4）由于反馈机制的引入使模型具备了一定程度的自愈和学习功能，通过对系统安全状态的监测和评估，不断调整、完善安全策略，使得系统防卫水平得以提高。

结束语 安全模型的研究涉及领域广，发展时间短、理论体系不成熟。上述模型中，策略控制和异常监测是决定模型性能的重要因素，当前还有许多问题亟待解决。目前 IETF 对安全策略的研究正受到越来越多的重视，IBM 公司推出了基于策略管理的应用软件 AppDrvN，Cisco 公司也推出了支持策略路由的路由器。目前安全策略描述语言（Security Policy Specification Language，SPSL）应用较为广泛，它既可以用于描述基于结点的安全模型，也可以用于描述基于域的安全模型。入侵检测是异常检测的重要部分，异常检测包括入侵检测但不限于入侵检测，二者在技术上有很大的相通之处。目前，策略控制和异常检测都是当前研究的热点问题。

参 考 文 献

1 Lampson B，Rivest R. Cryptography and Information Security Group Research Project：A Simple Distributed Security Infrastructure：[Technical Report] MIT，1997

2 Blaze M，Feigenbaum J. The Role of Trust Management in Distributed Systems Security. AT&T Labs — Research，Distributed System Lab CIS Department，University of Pennsylvania，2000

3 Resnick P，Miller J. PICS：Internet Access Controls Without Censorship. Communications of the ACM，Oct. 1996

4 Kumar K，Spafford E. A Pattern Matching Model for Misuse Intrusion Detection. In：Proc. of the 17th National Computer Security Conf. 1994. 11～12