第 33 卷　第 23 期　　计　算　机　工　程　　2007 年 12 月
Vol.33　No.23　　Computer Engineering　　December 2007
·安全技术·　　文章编号：1000—3428(2007)23—0173—03　　文献标识码：A　　中图分类号：TP309

动态网络安全模型的应用

何　翔，薛建国，汪　静
（北京市烟草专卖局信息中心，北京　100027）

摘　要：在可适应网络安全理论模型 PDR 和 P2DR 的基础上加入管理因素，将模型扩展为 P2DRM 模型以实现动态网络安全管理的功能。将数据挖掘关联算法和 Agent 技术加入到 P2DRM 模型中，并通过各子系统的协作实现分布式网络入侵监控、响应过程。该模型在网络安全监控系统的应用能有效提高网络安全管理的效率，满足网络安全动态变化的要求。

关键词：动态网络安全；管理代理；分布式管理；关联算法

Application of Dynamic Network Security Model

HE Xiang, XUE Jiang-guo, WANG Jing
(Beijing Tobacco Monopoly Administration Information Center, Beijing 100027)

【Abstract】 By adding the management factor, the network security adapted key models of PDR and P2DR are extended to P2DRM model to implement dynamic network security management. Also, correlation algorithm and agent technology are integrated into P2DRM, and monitor on attach and response of distributed network are implemented through sub-systems. This model can be used in network security monitor system to make network security management efficient and to meet network security dynamic monitor requirement.

【Key words】 dynamic network security; agent; distributed management; correlation algorithm

1　可适应网络安全模型

可适应网络安全理论主要有 PDR 模型和 P2DR 模型[1]，它能够根据网络动态变化的情况及时做出相应的调整，以维持网络系统相对安全稳定的状态。PDR 模型通过防护(protection)、检测(detection)和响应(response)三位一体来保障网络系统动态和整体的安全性(图 1)。P2DR 模型在 PDR 模型的基础上增加了策略(policy)。但是，PDR 模型和 P2DR 模型都没有考虑网络安全的管理和控制要素，因此缺乏管理、人为处理因素，不便于网络系统信息安全整体的监视和控制。

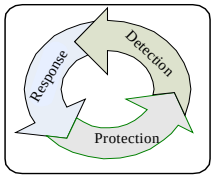

图 1　PDR 模型

2　可适应网络安全模型的改进

在 PDR 模型和 P2DR 模型中，将管理因素加入，将原来的模型扩展成为 P2DRM 网络信息安全模型(图 2)，用于北京烟草的网络安全综合管理系统。该系统架构具有动态响应机制，能使多种网络安全技术分工合作、有机结合，通过检测、决策、响应三位一体的联动，有效提高系统入侵检测、防御、保护的能力。

通过多种类型的网络防御、人工管理和协同工作机制，共同完成网络系统的安全目标，实现网络系统信息安全多层次的监视和控制。策略、防护、检测和响应 4 种要素及各种安全措施都需要在安全管理的指导下实施。在此体系框架下将来源于分布式人工智能领域的 Agent 技术融入网络安全系统体系中。同时，系统通过多 Agent 的之间的协作、交互等手段构成一个基于安全管理的动态网络安全模型。系统总体框架如图 3 所示。

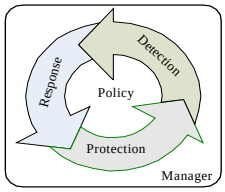

图 2　P2DRM 模型

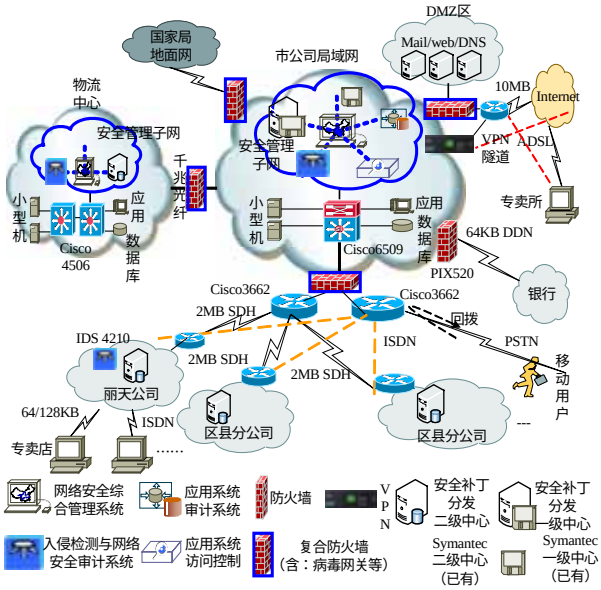

图 3　系统结构

作者简介：何　翔(1963－)，女，硕士、高级工程师，主研方向：计算机网络安全和管理；薛建国，工程师；汪　静，助理工程师

收稿日期：2006-12-28　**E-mail：**hexiangbox@sina.com

3 动态网络安全模型设计与实现

动态网络安全模型主要由防护(protection)、检测(detection)、策略(policy)和管理(manager) 4 部分组成。

3.1 防护(protection)

P2DRM 模型的 f 防护功能由防火墙、防病毒和补丁分发来实现。防火墙[2~3]定义网络边界的防护，作为网络边界最基本的信息安全防护措施，对流过的数据，定义基本的访问控制。北京烟草网络包括多个边界，例如因特网、区县局、国家局等。防火墙部署结构如图 4 所示。

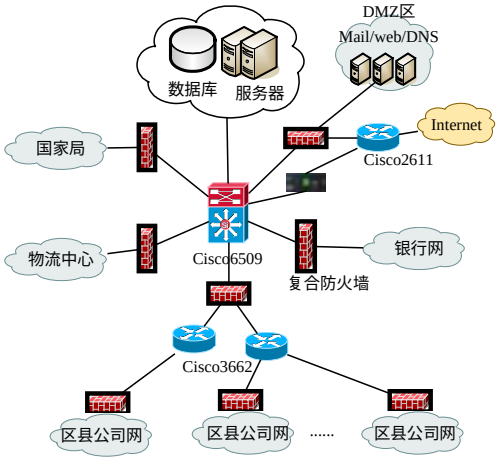

图 4 防火墙部署结构

考虑到现在来自网络攻击的复杂性和多样性，系统设计了统一的因特网出口，以确保对因特网访问的控制和保护内部企业网。对于出口处的防火墙，在上面建立 DMZ 网段。同时做到在实现基本的逻辑隔离和访问控制的基础上，进一步对流经防火墙的信息流进行内容扫描，防止病毒入侵和非法入侵的行为，并做到内容过滤。

随着病毒品种的日益增加，病毒的防范显得愈加重要。系统采用网络防病毒的解决方案，建立一个控制中心和一级防病毒服务器、每个下属单位建立一个二级防病毒服务器及各个客户终端构成。病毒定义码和扫描病毒引擎的更新由一级防病毒服务器及时分发，控制中心快速方便实现集中管理，以降低对网络性能的影响。

操作系统程序上的漏洞，造成许多病毒专门针对程序漏洞进行攻击，因而需要及时安装补丁程序。由于各单位计算机的数量较多，操作系统又不一致，因此经常出现部分计算机没有及时安装补丁程序，感染了计算机病毒或被入侵攻击。为了做到及时、有效地为系统内所有客户端分发系统安全补丁，增强内部桌面系统自身的抗攻击性等目标，系统部署了安全补丁分发子系统。系统采用类似网络防病毒的架构，建立一级 SMS 服务器、每个下属单位建立一个二级 SMS 服务器，实现对客户终端的补丁管理。

3.2 检测(detection)

在网络安全循环过程中，入侵检测是非常重要的一个环节，它帮助系统有效对付网络攻击，增强系统管理员的安全管理能力，提高信息安全基础结构的完整性。系统采用复合型防火墙，防火墙自身具备入侵检测的功能，服务于整个网络系统。同时根据需要配置入侵检测的特征库，设置检测到入侵行为之后的动作，进行安全事务处理。

漏洞扫描系统主要用来评估网络系统的安全性能。通过漏洞扫描，及时知道网络中存在哪些安全漏洞以及这些漏洞的危害并根据检测结果提供有关安全风险和评估报告。本文采取了外包服务的方式进行漏洞扫描及安全加固，便于用第三方身份来进行系统漏洞发现，也可以根据需要随时满足扫描系统的升级、可扩充性等要求。

3.3 响应(response)

响应在安全系统中占有最重要的地位，是解决安全潜在威胁最有效的办法，因为安全问题就是要解决响应和异常处理问题。要解决好响应问题，就要制订好响应的方案，在发现了攻击企图或者攻击之后，安全系统需要及时地进行反应：

(1)报告：无论系统的自动化程度多高，都需要管理员知道是否有入侵事件发生。

(2)记录：必须将所有的情况记录下来，包括入侵的各个细节以及系统的反映。

(3)反应：进行相应的处理以阻止进一步的入侵。

(4)恢复：清除入侵造成的影响，使系统正常运行。

实际上，响应就是进一步防护。经过一段时间的运行，系统可以把入侵、病毒等事件报告、记录到管理平台上，根据上报的数据发现问题，在统一策略的指导下，动态调整防火墙，及时阻止入侵行为，更好地保护系统安全。

3.4 策略(policy)

安全策略是安全管理的核心，要实施动态网络安全循环过程，必须首先制定企业的安全策略，所有的防护、检测、响应都要依据安全策略实施，企业安全策略为安全管理提供管理方向和支持手段。

在安全策略实现上，主要按照最小授权的原则，一般只开放业务应用需要的端口，同时为了保障业务系统的最高优先级，在做好相应的 QoS 的同时，对内部人员到外网的访问进行必要的限制等。同时在允许的规则中起用防火墙具有的内容检测、过滤等功能。其次按照纵深防御原则，网络安全防护系统应该是一个多层次的安全系统，避免网络中的“单点失效”，网络系统设计的过程中关键的部分都采用了备份网络设备。

3.5 管理(managent)

管理是实现 P2DRM 模型的关键。北京烟草的网络系统采用了安全综合管理平台，以实现将多个异构的、来自不同厂商的安全产品进行有效的集中管理，及时了解网络中存在的安全事件，进行事件关联分析和挖掘，为整个网络安全风险提供趋势分析等功能。它对进一步发挥现有安全系统的作用，提升网络安全管理水平提供很大的帮助。

在网络系统部署了安全综合管理平台，通过该平台有效地对现有的安全系统进行全面的管理，实现了综合防范、集中管理的功能，构筑了安全防御技术体系，将网络层、主机与系统层、应用层等各个层面的安全系统融入到安全综合管理平台中。通过分析、挖掘、关联等手段，将以前的单独防范、互不干预的情况，演变成为具备信息关联分析、快速定位安全事件源头、及时安全预警等目标的综合性的统一安全管理平台。

4 关键技术

在动态网络安全模型中需要解决数据挖掘关联算法、子系统之间通信技术、Agent 技术等关键技术。

4.1 数据挖掘关联算法

数据挖掘在集中安全管理应用中主要使用了 Apriori 算法来进行安全事件的关联挖掘。关联挖掘就是从大量的数据

中挖掘出有价值的描述数据项之间相互联系的有关知识。Apriori 算法是挖掘产生布尔关联规则所需频繁项集的基本算法，该算法利用了一个层次顺序搜索的循环方法来完成频繁项集的挖掘工作。这一循环方法就是利用 k-项集来产生(k+1)-项集。Apriori 算法利用了一个重要性质，又称为 Apriori 性质来帮助有效缩小频繁项集的搜索空间。

若将系统内各种安全产品所能产生的所有安全事件主题设为一个集合，每个安全事件主题均为一个布尔值(真/假)的变量以描述该安全事件是否在(1 个)网络设备上产生。因此，所有安全产品针对每个网络设备产生的安全事件都能用一个布尔向量来表示。分析相应的布尔向量就可以获得哪些安全事件是伴随(关联)发生的。如木马病毒安全事件(来自防病毒)产生同时也会产生尝试读取非常规端口安全事件(来自入侵检测)的事件关联就可以用以下的关联规则来描述：

troj_virus=>read_illegal_port_ids[support=20%, Confidence==80%] (1)

关联规则的支持度(support)和信任度(confidence)是两个度量有关规则的方法。它们分别描述了一个被挖掘出的关联规则的有用性和确定性。规则(1)的支持度为 20%，就表示所分析的系统中有 2%网络设备同时发生了木马病毒事件和尝试读取非常规端口事件。信任度为 80%则表示所有发生木马病毒事件的网络设备中的 80%同时还会发生尝试读取非常规端口事件。通常如果一个关联规则满足最小支持度阈值和最小信任度阈值，那么就认为该关联规则是有意义的；而用户或专家可以设置最小支持度阈值和最小信任度阈值。满足最小支持度阈值和最小信任度阈值的关联规则就称为强规则。一个数据项的集合就称为项集。一个包含 k 个数据项的项集就称为 k-项集。因此，集合{ troj_virus, read_illegal_port_ids}就是一个 2-项集。

一个项集的出现频度就是整个安全事件记录数据集 D 中包含该项集的记录数。满足最小支持度阈值所对应的网络设备数就称为最小支持频度。满足最小支持阈值的项集就称为频繁项集。所有频繁 k-项集的集合记为 Lk。

安全事件的挖掘规则主要包含以下 2 个步骤：

(1)发现所有的频繁项集，根据定义，这些项集的频度至少应等于(预先设置的)最小支持频度；

(2)根据所获得的频繁项集，产生相应的强关联规则。根据定义，这些规则必须满足最小信任度阈值。

通过以上的算法和步骤，当安全事件的数量积累足够多的时候，可以有效挖掘出事件之间的关联特性。例如通过挖掘可以得到对网络的正常访问和非正常访问状况，为及时分析处理网络非正常访问提供有力帮助。

4.2 子系统之间通信技术

如何实现安全综合管理平台和防病毒、防火墙、入侵检测、漏洞扫描等多种安全产品之间的通信，是动态安全模型中的关键因素。

各子系统之间的互联及通信的协议，可采用多种不同技术。安全综合管理平台通过标准的或专用的协议实现对被监管系统内所有的数据源进行有效获取，它为各种设备或产品提供标准接口，协调和调度自身运行；通过轮询方式和监听接收方式对各种设备的安全、故障、性能数据进行采集，对采集到的数据进行整理和保存。采集方式与采集对象可以自由扩充，主要包括以下 3 种：

(1)日志文件的方式采集：采用基于模板的方法对日志中的重要信息进行分析、提取和转化，形成规范化日志记录再上报，实现对不同操作系统和应用平台的日志信息采集。

(2)远程轮询和主动探测方式采集：主要针对一些开设服务的安全设备、网络设备、应用服务等。根据安全策略进行判别，形成规范化的信息数据。采用了 SNMP, WMI, OPSEC, telnet, rlogin, ssh 等方式。

(3)被动信息接收采集方式：许多安全产品和应用平台本身具备多样化的报警响应机制，可以通过收集这些信息实现某些审计信息的收集。如接收 SNMP Trap, Syslog, Windows Message 等。

4.3 Agent 技术

Agent[4～5]具有以下特性：自治性(autonomy)，社交能力(social ability)，反应能力(reactivity)，预动性(pro-activeness)。Agent 不仅能简单地对环境变化作出反应，它们还能通过接受某些启示信息，做出面向目标的行为。除了以上特性外，还具有如知识、信念、意图、承诺等某些人类才具有的特性。

安全综合管理平台与各个安全系统和安全设备接口的 Agent，以及各个安全系统本身可能都是采用分布式的架构。构建一个基础的安全管理功能架构，在整个网络中构造各种安全 Agent，通过多个安全 Agent 的通信相互交互协作，可使信息得到及时的反馈和共享，提高网络安全监控系统的主动性和智能性，满足动态网络安全的要求。该架构和分布式体系架构、信息交互和通信模型共同构成了基于可适应网络模型的安全综合管理系统。

5 结束语

基于 P2DRM 模型统筹了技术、管理、人员等各方面的环节。以安全策略为指导，基于统一的安全管理技术平台，构建动态、完整、高效的信息安全整体构架，能有效提高网络系统的整体安全等级，为保证业务的健康发展和提升核心竞争力提供坚实的安全保障。当然以上并不代表网络的绝对安全，信息安全是一项复杂的工程，需要根据发展的情况不断进行调整、优化和完善。

参考文献

1 Buddhikot M M, Suri S, Waldvogel M. Space Decomposition Technique for Fast Layer-4 Switching[C]//Proceedings of Conference on Protocols for High Speed Networks. 1999: 25-41.

2 王世俊. 网络安全浅析[J]. 计算机时代, 2002, 4(1): 9-11.

3 胡道元. 网络设计师教程[M]. 北京:清华大学出版社, 2001: 275-286.

4 Wooldridge M, Jennings N R. Agents Theories, Architectures and Languages: a Survey[M]. Berlin: Springer-Verlag, 1995.

5 Wooldridge M. Intelligent Agents: Theory and Practice[J]. Knowledge Engineering Review, 1995, 10(2): 115-152.