安全管理研究综述

姚 键 叶保留 蔡圣闻 袁卫忠 茅 兵 黄 皓 谢 立
(软件新技术国家重点实验室 南京大学计算机科学与技术系 南京 210093)

摘 要 本文提出了安全管理的三大目标：集成管理、综合管理和智能管理，综述了安全管理的模型、体系结构、产品和关键技术，强调了安全管理在安全领域的重要地位，指出了需要进一步研究的问题。

关键词 安全管理，信息模型，安全策略，智能管理

A Survey of Security Management Research

YAO Jian YE Bao-Liu CAI Sheng-Wen YUAN Wei-Zhong MAO Bing HUANG Hao XIE Li
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)
(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract This paper proposes three objects of security management—Integrity, cooperation and intelligence. It introduces model, architecture, product and key technique in security management. It emphasizes the important role of security management in security field and points out the problem to be farther researched.

Keywords Security management, Information model, Security policy, Intelligent management

1 引言

安全管理的概念最早作为网络管理的五大功能之一被提出(配置管理、性能管理、故障管理、计费管理和安全管理)，对分布式系统的机密性、完整性、可用性和抗抵赖性进行监视和控制。长期以来，安全管理注重对某种安全特性的满足，并且取得了明显效果。例如，安装防病毒软件查杀病毒，安装防火墙抵御外部的普通攻击，采用入侵监测系统发现入侵等。但是，这些管理是单点、分散的，需要安全管理人员逐一配置，人工汇总、分析各安全设备的反映的数据，而且许多机构在部署了这些安全产品后仍然无法保证网络安全。细究原因，可以发现当前安全管理三个方面的困难：1、安全产品种类繁多，标准不一，互操作困难；2、安全管理工具功能单一，各自为政，难以满足安全管理的综合性、全局性和连续性要求；3、安全管理缺乏灵活与智能，管理人员管理任务繁重。

针对这三个困难，形成了当前安全管理的三大目标：集成管理、综合管理和智能管理。集成管理指对不同厂商、不同类别的安全产品提供集中、一致的管理。综合管理指在整体的安全策略下，使安全产品和非安全产品相互配合、协同工作。智能管理指对安全数据分析并提供决策支持，自动处理部分安全事件，分担管理人员管理任务。

本文分析了当前安全管理研究的状况和技术难点，并介绍了相关工作进展。第2节介绍安全管理模型和体系结构研究状况；第3节介绍代表性的安全管理产品；第4节讨论了其中的一些关键问题。最后对全文进行了总结。

2 安全管理研究现状

2.1 安全管理模型研究

2.1.1 ISO 模型[1] 1989年ISO 7498-2从对安全服务角度建立模型，定义安全管理活动有三大类，以及安全管理自身的安全。OSI 安全环境维护一个安全管理信息库(SMIB)，SMIB 存储开放系统所需的与安全有关的全部信息。ISO 安全管理的分类如下：

(1)系统安全管理。包含：总体安全策略、与别的OSI管理功能的相互作用、与安全服务管理和安全机制管理的交互作用、事件处理管理、安全审计管理、安全恢复管理。

(2)安全服务管理。包含：为某种安全服务决定与指派安全保护的目标、指定与选择规则、安全机制协商、与其他安全管理功能和安全机制管理功能的交互作用。

(3)安全机制管理。包含：密钥管理、加密管理、数字签名管理、访问控制的管理、数据完整性管理、鉴别管理、通信业务填充管理、路由选择管理、公正管理。

ISO 对安全管理从功能上作了明确的界定和分类，对其后各类安全产品的发展起到了积极的指导作用。

2.1.2 PPDR 模型(可适应网络安全模型)[2] 随着计算机和网络技术的发展，传统的计算机安全管理理论侧重于静态防御，不再适应动态变化的、多维互联的网络环境，ISS公司提出了 PPDR 模型，也称可适应网络安全模型。如图1。该模型包含4个主要部分：Policy(安全策略)、Protection(防护)、Detection(检测)和 Response(响应)。在安全策略的指导下，防护、检测和响应组成了一个完整的、动态的安全循环，以及一个螺旋上升的过程。安全策略在安全管理中占核心地位，安全技术措施产品不是盲目引进，而是围绕整体安全策略的需求有序地组织在一起，架构一个动态的安全防范体系。防护指安全规章的制定、安全配置的落实和安全措施设备的采用。检测针对网络的动态变化，弥补漏洞发现或攻击手段发明与

*)基金项目：国家863计划(No. 2001AA142010)资助课题，江苏省自然科学基金项目(No. BK2002073)资助课题。**姚 键** 博士研究生，主要研究领域为网络安全。**叶保留** 博士研究生，研究方向为分布式计算与并行处理。**蔡圣闻** 博士研究生，主要研究领域为网络安全。**袁卫忠** 主要研究领域为网络安全。**茅 兵** 博士，教授，研究方向为分布式计算与并行处理。**黄 皓** 教授，博士生导师，网络安全。**谢 立** 教授，博士生导师，研究方向为分布式计算与并行处理。

相应的防护措施的建立之间的时间差，包括异常监视和攻击发现。响应在发现攻击企图或攻击之后，进行报告、记录、反应、恢复等活动，负责事件处理并将系统调到"最安全"或"风险最底"的状态。PPDR 模型强调整体的安全目标和连续的管理周期。

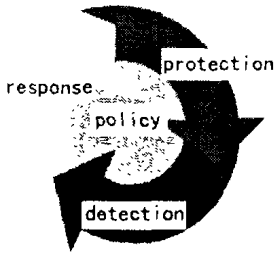

图 1　PPDR 模型示意图

1998 年，George Mason 大学的 Sandhu 等提出 CCSA (Concentric Supervision of Security Applications)[3]安全管理模型。与 PPDR 安全管理类似，该模型也将安全管理看作是连续的循环活动过程；不过，该模型更注重可操作性，它按管理的职责划分将安全管理过程分为三各阶段。(1)管理(administrative)：本阶段的任务是按既定的目标配置安全系统，一般采用批的方式。(2)操作(operation)：本阶段的任务是对不可预料的安全事件，采取措施，一般采用实时的方式。(3)评估(assessment)：本阶段的任务是检测安全目标是否满足，潜在的变化是否影响系统安全。有两种方式：其一，短期方式—支持对操作阶段检测到的安全威胁作出反应。其二，长期方式—支持安全威胁趋势分析、保护质量评价和安全策略修订等等。

2.2　安全管理体系结构研究

2.2.1　*基于策略的安全管理体系结构*[4]　该体系结构包含三种支撑服务：策略服务、域服务和事件服务。1、策略服务存放编译后的策略类，创建和分发新的策略对象。2、域服务管理分布的、层次结构的域对象并支持主体和客体集运行时赋值，每个域对象既关联对应的受管对象也关联对应的策略对象。域服务类似 LDAP 目录服务且可以通过事件改变一个目录的所属关系，域服务也可以用数据库实现。域对象代表的内容有：各受管对象(设备、文件、应用程序、网络通信流等等)、各安全实体(设备监控模块、文件系统、应用程序安全模块、网络安全模块等等)，域对象按其实际相互关系组织成层次关系。3、事件服务负责从被管对象和系统中收集和组织系统事件，并将它们发送给策略管理组件。图中能产生事件的对象称为事件发布者。

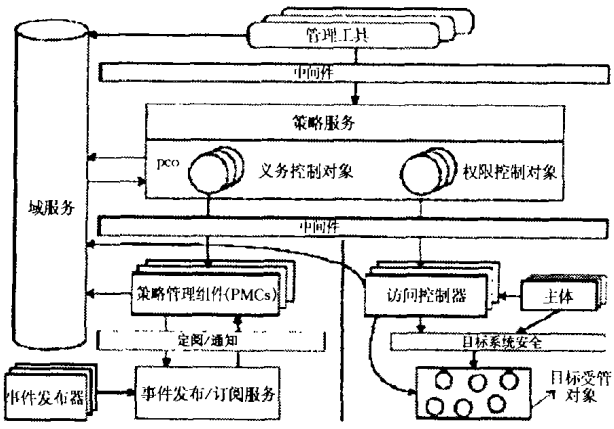

图 2　基于策略的安全管理体系结构[4]

安全管理员使用图形化的管理工具与域服务和策略服务交互，进行设计域结构、定义新策略编译后存入域服务。策略控制对象由策略服务在运行时生成和维护，并被自动分发到策略执行组件，同时域服务动态建立域对象及其策略的关联关系。

执行策略的实体称为策略执行组件，策略执行组件对来自策略控制对象的策略对象具有加载/卸载、使能/使不能的接口。

PBSMA 将安全决策与安全执行分离，以策略驱动安全管理过程，具有灵活性，当安全策略改变时，不需要改变安全执行部件。

2.2.2　*基于多代理的安全管理体系结构*　与集中式安全管理体系结构相对，基于多代理的安全管理体系结构是一种分布式体系结构。Agent 技术源于人工智能，20 世纪 90 年代中后期研究达到高潮[5]，目前在多领域得到应用。Agent 是具有某些特性的自主的计算实体，特定的 Agent 的特性是以下特性的子集或超集：(自主性、智能性、协作性、移动性、安全性)。图 3 是基于多代理的安全管理体系结构示意图。

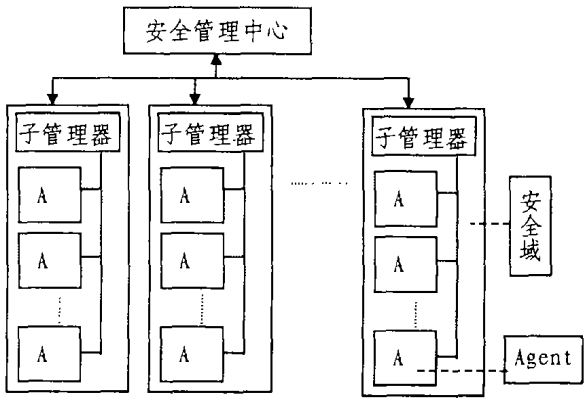

图 3　基于多代理的安全管理体系结构示意图

基于多代理的安全管理体系分为 3 个层次：(1)安全管理中心负责全系统的安全管理，包括协调控制各子管理器，处理各子管理器上交的任务。(2)子管理器负责本安全域的安全管理，创建、删除、启动、停止下属各 Agent，接受、处理下属 Agent 的报告，向安全管理中心报告。(3)Agent 完成子管理器指派的管理任务，并收集、提供子管理器需要的安全数据。

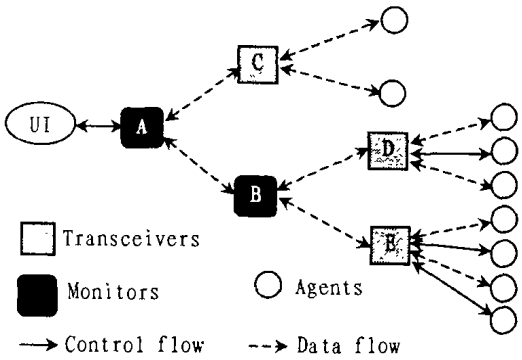

图 4　AAFID 的逻辑结构图[6]

1. 这个模型与现有的标准管理模型的主要区别是大部分管理任务依靠 Agent 和本地管理器在本地自治地完成，而不必将管理信息传递到管理者处进行集中处理。只是在需要多 domain 协同工作和远程监控时，才通过通信网络汇总管理信息，以有效减轻安全管理中心的繁重负荷。

2. 这是一个分布式的、自治的、协同工作的安全管理模型。实现这样的模型，会有效地节约网络中传递管理信息的带宽，提高安全管理的实时性。

Purdue 大学的 AAFID 系统(autonomous Agent for intru-sion)[6]是基于 Agent 的入侵检测系统,该系统具有:(1)系统结构易扩展;(2)每个 Agent 独立测试独立部署;(3)Agent 既可各自执行简单功能,也可结成组完成复杂功能。

3 安全管理产品现状和趋势

3.1 Cisco Secure Policy Manager[7]

Cisco 公司的 Cisco Secure Policy Manager(安全策略管理器)提供下列功能:1、CSPM 让用户可以从一个中央地点制定、分发、实施和审计整个网络的安全策略;2、自动地将网络策略转换成相应的 PIX 防火墙和 VPN 路由器的命令行配置;3、验证它所管理的网络拓扑、所制定的安全策略和所生成的配置的完整性和配置的正确性。CSPM 仅限于 Cisco PIX 防火墙和 IP 安全(IPSec)虚拟专用网(VPN)路由器。

3.2 TOPSEC Manager[8]

天融信公司 TOPSEC Manager 是一个综合的安全管理系统。具有下列功能:1、能获取 TOPSEC 公司的防火墙、入侵检测、防病毒等设备提供的安全事件。2、能根据策略库中预定义的策略对安全事件处理。3、能将原本孤立的安全设备有机地集合在一起。

其它公司的产品情况大致相同,安全管理产品已从分散管理发展到集中管理同厂商的同类产品或几类产品阶段。由于安全产品标准不同,很难实现多厂商产品的集中管理。部分安全厂商组建安全联盟,例如,Checkpoint 倡导的 Opsec 联盟、Topsec 倡导的 Topsec 联盟,联盟内厂商的安全产品可以被集成管理,以此扩大管理对象的范围。安全产品管理标准化是大势所趋。

4 几个关键问题

4.1 协同纽带

协同是安全管理的目标之一,管理者与被管对象(代理)、管理者之间、被管对象(代理)之间需要一种联系纽带,即安全管理信息库(SMIB)。安全管理信息库中的信息格式可以有:标量、策略和程序代码。

4.1.1 *标量* 借鉴 SNMP[9]网络管理中的成功经验,安全管理者与被管对象之间的信息交换定义成标量集,并遵循 SMI 组织成树结构,注册到 MIB 中。通过 SNMP set 操作,实现安全管理者对被管对象的控制;通过 get、get next 操作实现安全管理者对被管对象的监控;安全被管对象也可以通过 SNMP TRAP 功能主动向安全管理者发信息。SNMP 第三版本身提供了鉴别加密服务,可保障安全信息通信自身的安全。

由于 SNMP 的广泛应用,通过扩充用于安全管理的 MIB,进行安全管理的信息交换,能够方便地在现有网络管理框架内嵌入安全管理功能。目前大多数厂商的安全产品具有 SNMP 代理。

问题在于:(1)MIB 是静态的,不能适应安全设备、安全机制、安全服务和安全协议的发展需求;(2)是标量集,表示安全管理者与被管对象之间的复杂交互有困难或效率低下。

4.1.2 *策略* 近来,策略应用在管理领域较为盛行,包括网络 QoS 和安全管理。简单地讲,策略就是规则,一般具有(if 条件 then 动作)这样的形式。IETF 策略工作组(Policy workgroup)在 DMTF 的 CIM 的基础上提出了策略的信息模型,即 Policy Core Information Model (PCIM)[10],PCIM 定义了两种类型的类:一种称为"策略类",包括策略和对策略的控制,具体为 policy rule,policy group,policy condition,policy action,policy time period condition,policy repository 类;另一类称为"联系类",用来反映"策略类"间的联系。PCIM 是一种通用的能反映任何策略的模型,具体应用的策略可直接使用 policy rule,policy group 和 policy time period condition。具体应用相关的条件和动作可从 policy condition 和 policy action 派生子类。VendorPolicyCondition 和 VendorPolicyAction 是为厂商相关的策略提供一种标准的扩展机制。PCIM 具有统一表达策略优先级、策略组合等特性的能力。PCIM 为策略结构的标准化提供了指导,且以信息模型表示的安全策略,能方便地映射成多种数据模式,例如 XML 格式,LPAP 格式等,便于传输和解析。

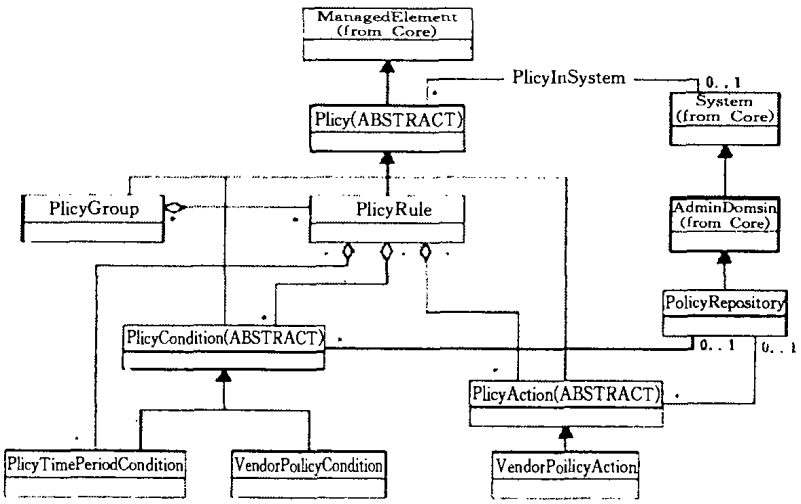

图 5 PCIM 类图[10]

和标量比较,策略有较强的表示能力,通过在安全管理者与被管对象之间交换安全策略,能更直观、高效地实现安全管理过程。

4.1.3 *程序代码* 近些年,随着移动代理技术(mobile Agent)的发展[5],在基于移动代理的安全管理体系结构中,安全管理者可以向被管对象委派程序代码或者被管对象向安全管理者请求特定功能的程序代码,在被管对象本地完成指定的管理任务。被管对象或代理提供执行环境。安全管理者与被管对象交换程序代码可以减轻安全管理者负荷,提高管理效率,能够完成复杂的管理任务。这种方式的根本问题是安全管理本身的安全性难以保证。加拿大 Carleton 大学在 JDK1.1.6 上研制的 Mobile Code Toolkit 工具包提供了一种 Agent 开发平台[11],可使得安全管理功能模块以自主、移动和安全的 java 代码序列化。

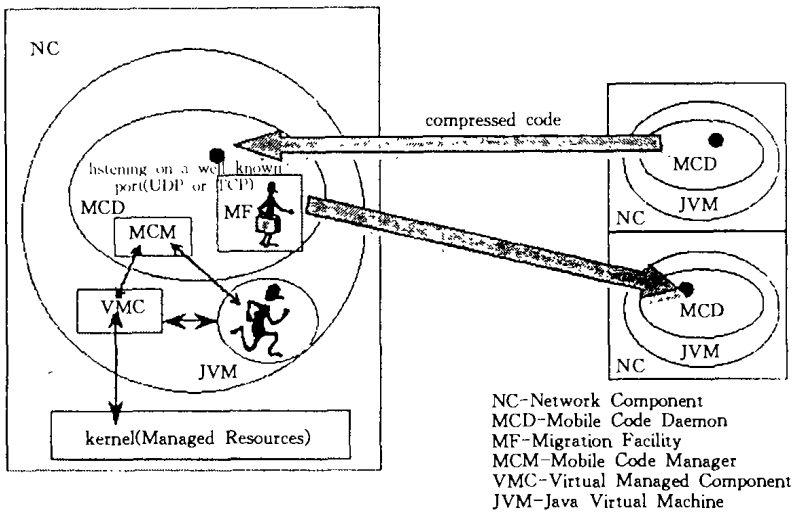

图 6 MCT 的结构图[11]

4.2 智能管理

正如人工智能技术广泛应用于网络管理一样，早期部分单一功能的安全产品，例如，基于网络的入侵检测系统，已经自觉或不自觉地引入了专家系统、神经网络等智能技术[18]，但由于功能单一性、安全管理框架的异构性和智能水平的多样性，智能技术在早期安全管理领域的应用都不成气候。伴随安全管理由分散到综合的进程，安全管理对智能技术提出了新的需求，智能技术也获得了广阔的表现空间。大体表现在下列几方面。

1. 安全服务的透明提供 用户正常使用各种应用(www、ftp、email 等等)，无需改变原来的操作习惯，完全感觉不到安全服务提供者的存在。安全管理系统根据用户身份和用户任务，自动生成安全策略，并根据整个安全系统的资源状况，具体实施安全策略。实施过程中，安全管理系统监视全系统的安全事件，根据变化动态修正有关安全策略。

其中的关键问题是安全目标到安全策略的自动映射，尚未找到一般方法，该过程现在是由安全专业人员手工完成或提供选项半自动完成。另外一个相关的问题是安全策略的完备性和一致性检验，即安全策略是否能充分保证安全目标、是否与其它策略一致，尚无形式化的证明方法。Lupu[12]提出一种语法分析方法，部分解决安全策略间冲突检验问题。

2. 安全数据的智能分析和安全事件的智能反应 综合安全管理系统可以获取全方位的安全信息，但海量的安全数据如何分析，而且要能保证应急响应的时效，显然超出人工能处理的极限。这就要求安全管理系统具有安全数据智能分析功能，能够识别入侵，并能对某些安全事件自动处理，对其它的安全事件报警，减轻安全管理人员的负担。该领域研究活跃，文[13,14]中报告数据挖掘方法在入侵检测中的应用和一种用 RIPPER 算法分析系统序列数据的方法，文[15]中报告一种用专家系统分析审计记录数据发现入侵的方法，文[16]提供一种状态转移方法分析渗透过程。

3. 安全管理系统的进化 安全管理系统作为一个完整的系统，其安全管理能力，在每个防御、检测和反应的周期运动中，应是螺旋上升的过程，安全管理系统具备评估能力以及评估结果的反应能力，根据评估结果修正安全策略，再评估安全策略的实际效果，如此循环，不断进化。

安全系统的评估研究较成熟，已形成很多标准，如 TCSEC、CC 和 BS7799 等等，文[3]提供了一种安全管理系统的进化宏观模型，安全管理系统的某方面的功能进化目前已有实例，如文[17]中介绍了一种基因算法用于入侵检测系统的优化。整个安全管理系统的进化还有很长的路。

结束语 安全管理是安全领域的重要组成部分，其重要地位越来越被重视，在最近一段时期内针对安全管理的体系结构、智能应用等研究日趋热烈。安全管理的研究与网络管理、人工智能等学科的发展紧密联系。最终实现安全管理的集成、协调和智能三大目标，还有许多问题期待解决。

参 考 文 献

1 信息处理系统开放系统互连基本参考模型-第二部分：安全体系结构. GB/T9387.2-1995
2 http://www.iss.net
3 Hyland P C. Concentric Supervision of Security Applications: A New Security Management Paradigm. In: Annual Computer Security Applications Conf. 1998
4 Damianou N C. A Policy Framework Management of Distributed Systems: [PHD dissertation]. Imperial college of Science, Technology and Medicine University of London, Feb. 2002
5 http://www.fipa.org
6 Balasubramaniyan J, Garcia-Fernandez J O, Spafford E H, Zamboni D. An Architecture for Intrusion Detection using Autonomous Agents: [Coast TR 98-05]. 1998
7 http://www.cisco.com
8 http://www.topsec.com.cn
9 Case J, et al. Message Processing and Dispatching for Simple Network Management Protocol(SNMP)RFC3412, Dec. 2002
10 Moore B, Ellesson E, Strassner J, Westerinen A. Policy CorPe Information Model-Version 1 Specification, RFC 3060. Available at: http://www.ietf.org, Feb. 2001
11 White T, Bieszczad A, Pagurek B. Distributed Fault Location in Networks Using Mobile Agents. In: Proc. of the Workshop on Intelligent Agents for Telecommunications Application (IATA'98), July, 1998
12 Lupu E, Sloman M. Conflict Analysis for Management Policies. In: Proc. of Vth Intl. Symposium on Integrated Network Management IM'97, San-Diego, May 1997
13 Lee W. A Data Mining Framework for Constructing Features and Models for Intrusion Detection System: [PHD thesis]. Columbia University, 1999
14 Lee W, Stolfo S J, Mok K W. A Data Mining Framework for Building Intrusion Detection models. In: Proc. of the 1999 IEEE Symp on Security and Privacy, May 1999
15 Lindqvist U, Porras P A. Detecting computer and network misuse through the production-based expect system toolset(P-BEST). In: Proc. of the 1999 IEEE Symp on Security and Privacy, Oakland, CA, May 1999
16 Porras P. STAT-A state transition analysis tool for intrusion detection: [Master's thesis]. Computer Science Dept., Uni. of California, Santa and Barbara, June 1992
17 Me L. Gassata, a genetic algorithm as alternative tool for security audit trails analysis. In: Proc. of the first international workshop on the recent advances in intrusion detection(RAID'98), 1998
18 戴英侠，连一峰，王航. 系统安全与入侵检测. 清华大学出版社，2002