网络安全管理技术研究

伏 晓 蔡圣闻 谢 立
(南京大学计算机科学与技术系 软件新技术国家重点实验室 南京 210093)

摘 要 针对新的安全形势,网络安全管理作为一类更全面、更智能化的综合技术业已得到越来越多的关注,不少相关产品也已经出现在市场上。网络安全管理的作用是通过对各种安全技术和安全产品的统一管理和协同来实现整体的安全。首先总结比较了现有的网络安全管理实现体系结构。然后,回顾了在网络安全管理中占重要地位的安全策略研究的进展,介绍了信息集成、智能分析引擎、协同及通信规范这3种网络安全管理的关键实现技术。最后,分析了网络安全管理当前的不足以及未来的发展趋势。

关键词 网络安全管理,安全管理体系结构,安全管理协议,协同,安全本体

Survey of Network Security Management

FU Xiao CAI Sheng-wen XIE Li
(State Key Laboratory for Novel Software Technology, Department of Computer Science and Technology, Nanjing University, Nanjing 210093, China)

Abstract Network security management (NSM) is a new promising technology. It can achieve the global security by comprehensive uniform and cooperative management of all security products and technologies. Currently, researchers in this field mainly focus on the architectures of security management and the security policies for control. Many ideas in other fields, including multi-agent system, network management and so on, have been used to design network security management system. As to the key techniques for implementing NSM, such as information integration and intelligent analyzing engine, there are still so many problems to be solved. Presently NSM has received much attention. In order to make much progress, common standards, just as SNMP in network management, have to be developed by all producers and researchers. In the future, NSM will integrate more techniques and the scope controlled by it will expand from one network to multiple networks. All of these will make it more complex and bring researchers more challenges. This paper gave an overview of NSM. Firstly, current popular architectures of security management were summarized and compared. Then the research progress on security policy, which is very important for security management, was reviewed. After these, three key techniques of security management were introduced. Finally the shortages and new directions in this field were analyzed.

Keywords Network security management, Architecture of security management, Security management protocol, Cooperation, Security ontology

1 引言

面对复杂的安全环境,现有的安全体系通常由众多异构且彼此独立的安全产品堆积而成,既难以管理,又难以获得准确的全局安全视图,不利于整体安全策略的制定和实施。而且,在遭遇复杂的综合型攻击时,由于缺乏产品之间的协同联动,安全防护常常十分脆弱。这些问题迫切需要更为灵活、智能的方案来解决。在这样的背景下,一种新的技术——网络安全管理应运而生,并成为近年来安全领域的研究热点。

网络安全管理是一种综合型技术,需要来自信息安全、网络管理、分布式计算、人工智能等多个领域研究成果的支持。其目标是充分利用以上领域的技术和方法,解决网络环境造成的、计算机应用体系中各种安全技术和产品的统一管理和协调问题,从整体上提高整个网络的防御入侵、抵抗攻击的能力,保持系统及服务的完整性、可靠性和可用性。网络安全管理包括对安全服务、机制和安全相关信息的管理以及管理自身的安全性两个方面,其过程通常由管理、操作和评估3个阶段组成[1]。管理阶段是由用户驱动的安全服务的初始配置和日常更新;操作阶段是由事件驱动的安全服务状态的实时检测和响应;评估阶段则用于衡量安全目标是否达到,以及系统当前的改变会产生何种影响。

对网络安全管理的研究具有重要的理论和实践意义。该

到稿日期:2008-03-03 本文受国家863计划(No. 2003AA142010)资助课题,江苏省自然科学基金(No. BK2002073)资助课题,2005年国家信息安全重大专项基金项目资助。

伏 晓 博士研究生,研究方向为网络安全、机器学习,E-mail:fuxiao1225@hotmail.com;蔡圣闻 博士研究生,研究方向为网络安全、分布式计算;谢 立 教授,博士生导师,CCF会员,主要研究领域包括信息安全、分布式计算和先进操作系统等。

技术一方面能够通过智能分析和自动响应，将管理者从海量的报警数据和繁重的安全管理任务之中解放出来，另一方面能够辅助制定和执行安全决策，通过产品联动提高整体安全防护能力。因此，在日趋复杂的网络环境和严峻的安全形势下，它是解决众多棘手问题的有效手段。近年来大量该类产品的涌现和广泛应用就是很好的佐证。目前这类产品主要包括关注海量安全信息管理的安全信息管理系统(SIMS)、安全事件管理系统(SEMS)，着眼于多种安全产品协同的统一威胁管理(UTM)，以及近年来涌现的两方面兼顾的综合开放平台(如 Check Point 的 OPSEC)等。

本文就网络安全管理的一些重要研究领域和研究现状进行了综述。第 2 节总结和比较了网络安全管理的 4 种常见实现结构；第 3 节对网络安全管理领域中的策略研究以及基于策略的安全管理进行了介绍；第 4 节介绍了实现网络安全管理所需的关键技术。最后，对网络安全管理的当前障碍和未来发展进行了总结与展望。

2 网络安全管理体系结构

网络安全管理系统的体系结构是近年来的研究热点。一个有效的体系结构首先要满足安全管理的功能，然后要具备稳定性、可扩展性和可复用性。对于网络安全管理而言，其结构需要支持的功能包括：安全策略的制定、分发与实施，安全事件的监控与响应，安全机制/服务的管理，安全状态评估和决策支持等。因为被管理的安全机制通常来自不同厂商并且位于不同网络结点，所以异构性和分布性是安全管理体系结构需要考虑的重要问题。目前流行的体系结构主要有以下几种。

2.1 基于多 Agent 的结构

多 Agent 结构的思想来源于分布式人工智能领域基于 MAS(Multi-Agent system)的方法。它是一种分布式结构：系统中的 Agent 被分成不同类别，以某种方式组织起来，协同完成安全管理任务。因为 Agent 具有自治能力，所以不用将所有信息都传递到管理中心处理，这样就有效地减少了传输开销，减轻了管理中心的负荷。这类框架需要解决的关键问题是如何将任务分解给多个 Agent 以及单个 Agent 的设计。框架的典型包括 IA-NSM 和 SAMARA。

IA-NSM 是 Karima 等提出的基于智能 Agent 的安全管理模型[2-4]。在该模型中 Agent 被分为 2 组，分别是管理组和本地监督组。管理组负责网络的整体安全管理，由安全策略管理 Agent 、网络管理 Agent 和内网管理 Agent 组成，主要功能包括数据处理与控制、与管理员交互以便接收策略定义、向管理员告警等。本地监控组仅负责一个域(domain)内的安全管理。它由若干分布在本地网络内的本地监控 Agent 组成，其功能包括：根据安全策略过滤安全相关事件；彼此交互进行分析与决策；根据自身的内在属性、知识和经验进行推理。

SAMARA 则是 Torrellas 等人提出的一种自治安全评估及网络安全管理系统[5,6]。该系统包括离线的安全分解、在线的网络安全评估和网络安全执行 3 个阶段。其中 Agent 被划分为调度 Agent、安全评估 Agent、辅助 Agent、一般安全状态 Agent、容错 Agent、通信 Agent、监控 Agent、图形化模拟 Agent、安全评估计划 Agent 9 种类型，它们联合工作以满足本地或全局安全目标。值得一提的是，SAMARA 将非管理类任务，如通讯、图形化模拟等也分配给专门的 Agent 完成。

这两种框架的主要区别在于：在 IA-NSM 中 Agent 被组织成树型结构，底层 Agent 负责本地子网的管理并接受高层 Agent 的控制。这种方式结构清晰、便于安全策略的统一制定和分发，但缺陷在于分层结构中为数较少的高层 Agent 容易成为系统的瓶颈。另外，对于底层无法处理的事务，逐层上报会导致响应时间的延长。而 SAMARA 则完全从功能的角度划分 Agent。整个系统是扁平的网状结构：每个 Agent 专门负责一种任务，通过所有 Agent 的协作才能构成完整的安全管理系统。这种方式避免了树型结构的缺陷，适用于缺少中央控制中心的多域安全管理。其主要缺点是 Agent 之间的通讯开销增大，统一的安全策略制定需要复杂的协调计算。

2.2 基于网络管理的结构

另一种实现网络安全管理的方式是利用现有网络管理体系结构来构建安全管理系统。安全管理与网络管理关系密切，安全管理系统常需要网管系统的支持(如提供网络拓扑信息)，所以在网管体系结构上扩展安全管理功能非常方便。目前这类系统大多建立在基于 Web 的网络管理之上。基于 Web 的网络管理结构主要包括 WBEM(Web-Based Enterprise Management)，JMX(Java Management Extensions)等。限于篇幅，本文仅介绍 WBEM，如图 1 所示。

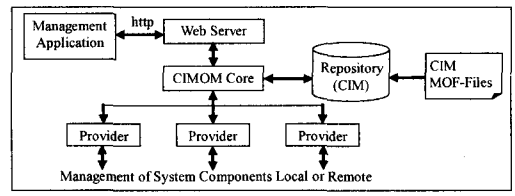

图 1 WBEM 结构

WBEM 是 DMTF(Distributed Management Task Force)定义的标准之一[7]。其核心是存储管理信息的数据库，其中管理信息根据 CIM(Common Information Model)[8]模型被存储为被管理对象文件(MOF)的形式。管理应用可通过 http 协议与数据库交互。该存取过程是标准化的，并在 CIM 与 XML 之间转换。Provider 负责将数据库中的管理信息翻译成适用于特定网络构件或平台的信息，而 CIM 对象管理者(CIMOM)负责控制 Web Server 和 Provider 对数据库的存取。

在基于 Web 的网管结构上构建安全管理体系的典型包括 Policy-Maker 和文献[9]中提出的大型计算机网络安全管理系统。

Policy-Maker[7]是 A. Pilz 提出的一种基于策略的安全管理框架。其中，CIM 形式的安全策略通过图形用户接口“Policy-Editor”由管理员统一定义，然后在 WBEM 结构中处理执行。安全策略被分成“直接策略”和“非直接策略”两类。“直接策略”能被安全组件直接处理，而“非直接策略”由 Provider 翻译成“直接策略”后再交由安全组件执行。策略的集成和关联由系统通过模板自动处理。另外，框架还包含了用于显示当前网络拓扑和配置的“网络可视化”模块以及用于测试配置的“网络模拟”模块。

文献[9]提出的安全管理体系目标是管理大规模网络中的多个异构防火墙，实现这些防火墙之间基于统一策略的配

置和协同。为统一管理策略，作者定义了通用的防火墙管理信息基(MIB)以及通用的事件记录格式。此外，IDS 通过 SNMP 协议也被集成到系统之中，以便进一步处理防火墙发现的可疑事件。为解决 Web 存取带来的安全问题，系统还具备了认证和基于角色的存取控制功能。

从对网络安全管理功能的支持来看，这两种框架均有效实现了安全策略的统一管理，区别在于文献[9]采用自定义的格式描述策略，而且局限于防火墙规则描述。而 Policy-Maker 的策略用 CIM 模型表示，更具通用性。另外，文献[9]通过与 IDS 的联合，实现了安全事件的监控与联合响应，并且关注管理系统自身的安全性问题。而 Policy-Maker 则没有这些功能，但它的"网络可视化"模块实现了简单的安全状态评估，这是文献[9]没有的。

2.3 基于模块的结构

用基于模块(Module)的体系结构实现安全管理是当前另一种流行的方法。这里的模块是对组件、插件、构件等技术(如 EJB，DCOM，CORBA)的统称。这种方法的基本思想是将各种安全服务，甚至统计、决策支持功能，设计成可由第三方开发的、"即插即用"的自治功能组件(component)。通过将这些安全组件集成到一个可扩展的基础平台，就可以创建出一个安全管理体系。

这类结构的典型是 Shervin Erfani 提出的模块化安全管理系统功能框架[10]，该框架具有层次化的功能结构。其基本结构元素包括：功能层、安全管理信息基(SMIB)、安全协议和基于标准的接口。系统包含 5 个层次，每一层由一个或多个良好定义的、可配置、可互操作的功能单元组成，这些功能单元即称为"模块"。这 5 个层次从上到下分别为：安全策略与商业需求层、安全管理层、安全服务层、安全机制层、安全原语层。

目前国内关于这种安全管理框架的研究较多，文献[11，12]都是这方面的例子。

2.4 基于层次化模型的结构

前几种体系结构的主要思想是将安全管理体系视为一个可扩展的平台，而各种安全机制被视为"设备"，可以在平台上"即插即用"，同时又由统一的策略控制。此外，还有一种从纵向考虑问题的实现方式，即从网络协议栈的角度管理安全机制、提供安全服务。当前网络异构性的一个重要体现就是网络结点的安全机制可能被应用在不同的协议层，例如网络层的 IPSec、传输层的 SSL、应用层的数字签名等。需要有一种方法来管理不同协议层的安全机制，创建一个完全分布的基础设施用以协商和设置安全信道，并在网络面临压力时重新配置这些安全机制，以维持某一层次的安全服务[13]。

这类结构的典型是基于协议栈的安全管理系统 Celestial System[13]。它能够沿任意网络路径自动发现有效的安全策略和机制，实现跨协议层和网络的安全机制动态配置，其核心构件是安全管理 Agent(SMA)。SMA 是驻扎于有安全需求或提供安全服务的网络结点(如终端、路由器、交换机)上的软件模块，它与协议栈的每一层安全协议交互，管理它们的各种信息，并且有权动态配置这些协议的本地安全机制。它与应用程序也有接口，用于为应用提供不同的安全服务。通过沿数据路径的所有 SMA 之间的协作即可建立一个安全通道。

2.5 网络安全管理体系结构比较

上述几种安全管理体系结构各有优劣。从应用领域上看，由于 Agent 的灵活性和高自治能力，基于多 Agent 的框架比其它框架更能适应动态环境和复杂用户行为。尤其在涉及多个动态安全域的大规模安全管理体系中，这种结构能较好地解决动态域管理、移动用户以及控制中心的瓶颈问题。这种结构的缺点是系统比较复杂，而且 Agent 技术本身还不够成熟，诸如 Agent 安全性等对于安全管理系统至关重要的问题目前仍处于研究阶段。

基于网络管理平台的体系结构是直接在现有网管平台上扩展安全管理功能，所以对已有 IT 基础设施改变较小、性价比高，适用于安全环境相对简单的中小规模组织。这种结构在收集网络信息、控制网络设备以及响应安全事件方面较为方便，但是由于受到网管平台的限制，灵活性一般不高，常常难以实现安全管理的全部功能。

基于模块的体系结构采用当前流行的构件、插件等技术，适用范围广，基础技术成熟，对跨平台和扩展性的支持较好，并且可配置和重用。该方法与基于多 Agent 的结构有些类似，区别在于 Agent 的自治能力更强，所以需要较少的集中管理，而基于模块的结构通常需要一个强大的中央控制中心。另外，在多 Agent 框架中 Agent 可在网络结点间移动，Agent 之间可直接通讯，而在基于模块的结构中模块一般都是静止的，模块之间通常不能直接通讯。

基于层次化模型的结构主要针对的是不同协议层的安全机制管理，其目标是实现跨网合作或建立安全通信通道。它采用的是完全分布的结构并且从纵向解决问题，所以这种结构更适用于无控制中心的多组织或多网络合作的情况。

除应用领域不同之外，这几种框架在性能方面也不尽相同。表 1 给出了它们在性能方面的比较。在实际的安全管理产品中，根据不同的需求，常采用多种体系结构相结合的方式，以便扬长避短。

表 1 网络安全管理框架性能比较

Architectures	Stability	Scalability	Reusability	Distribution	Supportability of Heterogeneity
Architecture Based on MAS	Excellent	Excellent	Excellent	Partly/Fully	High
Architecture Based on Network Management Platform	Good	Normal	Good	Partly	High
Module-based Architecture	Good	Good	Excellent	Partly	High
Architecture based on Level Model	Excellent	Excellent	Excellent	Fully	High

3 网络安全管理的安全策略

网络安全管理的一个重要特征是综合性，即在整体安全策略指导下，实现不同厂商、不同类别安全产品的协同、联动。因此，无论采用何种实现结构，安全策略都将在其中扮演重要角色。在网络安全管理中，安全策略的内容主要涵盖以下几

个方面[14]：反映特定组织或安全域成员安全需求的规则集；被管理安全服务的策略集；指导组织管理、保护和分布敏感信息的法律、规则、策略集。安全策略一般采用层次式结构，包括用自然语言描述的高层策略、用统一策略语言表示以便分析推理的中层策略，以及可由安全部件直接执行的底层策略。近年来，随着策略研究的发展，一种特殊的安全管理类别——基于策略的安全管理更逐渐成为安全管理的主流。本节首先介绍策略研究的现状，然后介绍基于策略的安全管理。

3.1 网络安全管理中的策略研究

网络安全管理中对于策略的研究主要关注安全策略模型、策略表示语言、策略细化和分析几个方面。

3.1.1 策略模型

策略模型的功能是用通用语法抽象描述各安全组件的相关信息，为策略结构的标准化提供指导。用它表示的安全策略能方便地映射成多种数据格式（如 XML，LDAP），便于策略解析和传输，但它并未提供策略的具体描述[15]。CIM 和 PCIM(Policy Core Information Model)是应用较广的两种建模方式。

CIM[8]是 DMTF 定义的一种面向对象信息模型，它由内核模型与通用模型组成。内核模型提供了所有管理领域通用的类、关系和属性；通用模型则用继承的方法定义了系统、设备、网络、应用和物理这 5 个与实现无关的管理模型，构成了许多管理应用的基础。通用模型还能进一步拓展细化为具体的扩展模型。

PCIM[16]是 DMTF 与 IETF(Internet Engineering Task Force)的策略框架工作组合作开发的一种专用于策略表示的 CIM 模型，它定义了两种对象类：结构类描述策略信息和控制信息；关联类描述各结构类实例间的关系。PCIM 还能够统一表示策略优先级和策略组合。

3.1.2 策略表示语言

与策略模型相比，策略语言给出了策略的具体描述，表达能力更强。但是往往局限于特定领域，目前尚无能统一描述各种安全服务/机制的语言。

现有的策略语言很多，较有代表性的有基于逻辑、基于事件和面向对象等几种[15]。基于逻辑的语言分析推理能力较强，但难以理解和使用，而且未必都能转化为可实现的底层策略，这类语言的典型是 RDL[17](Role Definition Language)。基于事件的语言由事件驱动，常采用 event-condition-action 格式来描述策略，其代表为 SPL[18](Security Policy Language)。面向对象式策略语言将面向对象的继承等概念引入到策略表示中，描述的策略种类更多，表达能力也更强。Ponder[19]是一种著名的陈述式面向对象策略语言，它能够说明安全和管理类策略，基本策略类型包括 authorization，information filtering，delegation，refrain，obligation 5 种，还能通过策略继承、分组实现组合策略。

3.1.3 策略细化

策略细化的主要工作是完成安全策略在各抽象层次的映射，还可用于确定为满足策略需配置何种资源，以及辅助分析底层策略是否与高层策略匹配。策略细化的过程应保证完备性，即正确性、一致性和结果集的最小化[15]。

目前中层策略到底层策略的自动转换机制已经有很多，例如已有不少根据 Ponder 语言生成防火墙规则、Windows 存取控制模版和 Java 安全策略的工具[20]。高层策略到中层策略的映射多数仍由手工实现，但也有了自动化的尝试，例如文献[11]即实现了自然语言表达的安全策略到一种基于逻辑的策略语言的自动映射。此外，从各类需求文档中抽取安全策略，可以借鉴机器学习在文本知识抽取方面的研究工作。而需求工程领域的目标细化(goal refinement)技术也可被策略细化研究借鉴。

3.1.4 策略分析

策略分析的主要工作是策略的一致性校验和冲突消解。策略冲突的分类方式很多，例如可以分成[15]形式冲突和应用相关冲突，或分成静态冲突和动态冲突。

现有的策略分析方法主要包括：①基于手工的冲突消解，当冲突发生时直接报错，人工干预。②静态校验和冲突消解，在策略运行前通过语法分析等一致性分析，检查出策略冲突，再通过局部调整避免冲突。③基于优先级的冲突消解，根据某种原则为策略分配优先级，当冲突发生时，选择优先级高的策略执行。④基于元策略的冲突消解，元策略是关于策略描述的顶层策略，可用于描述多个策略间的关系。这种协调机制比较复杂，但更为灵活。⑤对于 event-condition-action 格式的策略，还能通过忽略某些 event 或取消某些 action 来避免冲突。

3.2 基于策略的网络安全管理

基于策略的网络安全管理是当前流行的一种安全管理技术。它是基于策略的管理在网络安全管理领域的应用，其特征及优势在于将策略管理与策略实施相分离，灵活性高。它的结构一般与 IETF 定义的通用策略体系结构相符，即由策略管理工具、策略存储库、策略决策点和策略执行点组成。其基本工作流程是：首先由安全目标生成安全策略，然后将安全策略分发到指定位置并进行策略校验，最后由安全实体执行安全策略。安全策略在这类安全管理中占主导地位。根据中层策略表示和处理方式的不同，基于策略的网络安全管理又可以分为以规则为中心和以安全本体为中心。

3.2.1 以规则为中心

这种方式下安全策略被表示成形式化规则的集合。其中大部分规则采用了 if〈condition〉 then〈action〉模式，即每条规则包含一个条件集和相应的行为集。条件定义了策略规则何时激活。当规则被激活时，会执行一个或多个行为来改变系统状态。上述的 PCIM 及大部分策略语言都属于这种类型。现有的基于策略的安全管理系统也大多采用这种模式（见文献[9,21]）。

3.2.2 以安全本体为中心

这种方法用本体代替形式化规则建模安全知识。本体(Ontology)的概念来自自然语言处理领域。它是现实的结构化模型，由词汇、语义关联和简单的逻辑规则组成。而安全本体(Security Ontology)则是“基于一个信息系统的安全方面创建的本体，可以作为从信息源中抽取的信息系统安全需求的容器”[22]。与传统的形式化语言相比，本体更接近人们描述世界的方式，其语义和推理机制更适用于决策支持，还能方便地查询和扩展。因此，用它代替形式化规则表示安全策略，将能有效地提高分析、决策的准确性及效率。

目前在这方面的研究仍处在起步阶段。现有的代表性工作是文献[22,23]。它们用本体来表示安全需求，提出了一种

基于知识的、以本体为中心、可用于任意信息系统安全管理的框架，用基于本体的方法实现了高层策略与底层安全控制规则的自动转换。其本体表示采用 CIM 加 OWL 的方式，即在 CIM 模型中扩展本体语义，使其既能建模安全管理信息，又兼具本体特征。但该框架仍需借助基于策略的管理系统 Ponder 来实现安全行为的实施和监控。

4 网络安全管理的实现技术

为了实现安全管理，除了需要完善的体系结构、准确可行的安全策略之外，还需要信息集成、智能分析和有效的协同通信规范等技术的支持。本节将分别对这些技术加以介绍。

4.1 信息集成

网络安全管理系统需要管理不同种类和厂商的安全产品，所以如何从这些异构产品中采集所需信息并加以处理，以便进行关联分析，是安全管理需要解决的首要问题。它不仅关系到管理平台能够支持的安全产品的种类和数量，还关系到分析结果的准确性。信息集成技术研究的就是这一问题。其任务主要包括两个方面：数据采集和数据预处理。数据采集的目标是从各种安全产品的数据库、配置文件等相关数据源中收集关联分析所需信息。该过程既要考虑信息收集的充分度，又要尽量减少数据总量。而数据预处理的工作是净化去除数据中的冗余或错误信息，并将其统一成某种方便分析的格式。

对于信息集成的研究在数据仓库、数据挖掘等领域已有很多。目前网络安全管理主要是借鉴这些已有工作，专门针对安全管理中信息集成的研究文献很少。在安全管理中，信息集成的难点在于许多安全产品没有提供信息采集的接口，导致许多重要信息难以获取。这一问题并非仅技术所能解决，而是需要各安全厂商达成共识并制定通用的开放接口标准。

4.2 智能分析引擎

智能分析引擎是网络安全管理系统的核心部件，其作用是关联分析安全数据以识别威胁、自动响应部分安全事件以及产生告警。其中关联分析是重点和难点，它的特点在于综合分析多种安全组件的安全数据，例如漏洞和攻击情况可以综合分析，同一时间不同地点的事件也可以综合分析。这种综合能产生单独分析没有的信息，提高分析的准确性。安全管理平台的优势在很大程度上正是由这种分析方式体现的。

目前这一领域的研究仍处于起步阶段。许多现有系统依靠手工写成的关联规则实现安全事件综合分析及自动响应。例如，文献[9]中提出了一种由管理员设置的陷阱事件，防火墙检测到符合告警规则的数据会自动触发陷阱，向 IDS 转发包含可疑信息的 trap 包，供其进一步分析。这种手工方式不可能覆盖所有威胁，而且常滞后于攻击，缺陷很多。因此，如何实现自动关联分析，是当前智能分析引擎面临的最大难题。另外，由于网络安全管理综合了各种安全服务，因此获得的数据也是普通安全产品的几倍。如何有效分析和及时处理这些海量数据，也是智能分析引擎需要解决的重要问题。因为数据挖掘能有效地分析海量数据、自动挖掘关联规则，所以已有研究者提出将其应用于网络安全管理。例如，文献[24]将数据挖掘技术应用到基于策略的网络安全管理系统中，提出了一种采用数据挖掘机制的报警分析器（由关联规则挖掘器、频繁项集挖掘器和聚类挖掘器组成），最终实现的告警分析和高层分析的挖掘系统能有效地支持安全策略管理。但该系统侧重入侵检测类应用，尚未实现对多种安全产品的告警事件的综合分析。

未来这一领域的研究将主要关注自动关联分析，数据挖掘引擎将是一个重要的发展方向。由于安全管理系统需要实时响应安全事件，因此智能引擎的效率和性能非常重要。传统的数据挖掘算法一般用于处理非实时的离线分析，因此如何解决数据挖掘引擎的实时性和性能问题将是研究者需要关注的。

4.3 协同及通信规范

网络安全管理的另一个关键技术是实现安全部件间的无缝协同，它是安全事件综合分析与联合响应的前提。为了有效地协同，用户与安全部件之间、安全部件与宿主机之间、安全部件彼此之间需要有一个联系纽带。该联系可以是直接的，即通过消息、协议或接口的方式；也可以是间接的，即通过向公共安全管理信息基（SMIB）读写数据的方式。目前这一领域的研究工作也正集中在这两方面。

SMIB 是一个存储机构，由物理上的一个或多个数据库组成，存储了网络安全管理一般功能所需的所有控制信息和参数。它常被设计成知识库形式以便关联分析。其组织方式可以是集中式，也可以是诸如 Manager/Agent 的分布式结构。在某些简单安全管理体系中，甚至可以不设置专门的 SMIB，而是借助已有存储机制。例如文献[21]中即提出了一种用 LDA PServer 来存储策略及网络拓扑信息的方案。

接口、消息和安全管理协议是更为直接的协同方式。它们均可用于安全部件之间的通讯，区别在于安全管理协议的标准化程度更高。在接口和消息方面具有代表性的工作是 Check Point 的 OPSEC。它是一个得到多厂商认同的开放可扩展框架，包含一系列公开的 API，第三方可借助这些 API 开发各种安全管理应用并无缝集成到平台中。而在安全管理协议方面，业界目前尚无统一标准。简单网络管理协议（SNMP）是当前在网络管理领域广为接受的一种标准，因为网络管理与安全管理的天然联系，所以有不少研究者直接采用它作为安全管理协议（见文献[9,25]）。

未来协同及通讯规范领域的工作重点是确立统一的网络安全管理协议。正如 SNMP 之于网络管理，统一的协议标准必将极大地促进网络安全管理技术的发展。另外，随着安全管理系统规模的扩大、数据量的增加，如何提高 SMIB 的性能，使其适应网络规模的不断扩展也是急需解决的问题。在这方面，分布式 SMIB 将是值得关注的方向。

结束语 针对新的安全形势，网络安全管理作为一种更全面、更智能的综合技术业已得到越来越多的关注，不少相关产品已经出现在市场上。然而，现有的网络安全管理技术仍存在着不少不足，例如：业界对网络安全管理系统的功能缺乏统一的认识、缺少统一的安全管理协议、安全协作常局限于少数几项安全技术、网络安全管理系统的灵活性、扩展性、异构性较差等。值得庆幸的是，研究者和安全厂商已经注意到了这些情况，一些好的努力也已出现。未来安全管理系统的发展趋势是从小范围扩展到全网范围，从集中式安全管理发展为分布式安全管理，同时进一步扩展安全管理平台的集成能

（下转第 54 页）

nisms for Multi-Domain Grid Environments. Journal of Grid Computing, 2004, 2: 301-311

[50] Gagliardi F, Jones B, Reale M, et al. European DataGrid Project: Experiences of Deploying a Large Scale Testbed for E-Science Applications // Performance Evaluation of Complex Systems: Techniques and Tools, Performance 2002, Tutorial Lectures, Lecture Notes in Computer Science. Vol. 2459, Springer, 2002

[51] Freudenthal E, Keenan E, Pesin T, et al. DisCo: A Distribution Infrastructure for Securely Deploying Decomposable Services in Partially Trusted Environments (TR2001-820). Technical report. Department of Computer Science, New York University, 2001

[52] Winsborough W H, Li N. Safety in automated trust negotiation // Proceedings of the 2004 IEEE Symposium on Security and Privacy(S&P2004). Oakland, CA, USA, 2004: 147-160

[53] Winsborough W H, Li N H. Towards practical automated trust negotiation // Michael JB, ed. Proc. of the 3rd Int'l Workshop on Policies for Distributed Systems and Networks. Washington: IEEE Computer Society Press, 2002: 92-103

(上接第 19 页)

力(例如引入资源配置、资产配置等网络管理技术),逐步将不同的安全域和异构的网络也纳入管理范围。这些改变必将使协同变得更为复杂,对处理海量事件的能力要求更高。因此,还有许多问题亟待研究者解决。

参 考 文 献

[1] Hyland P C, Sandhu R. Concentric Supervision of Security Applications: A New Security Management Paradigm // Annual Computer Security Application Conference. Phoenix, USA, 1998

[2] Boudaoud K, McCatieNevile C. An Intelligent Agent - based Model for Security Management // The 7th IEEE International Symposium on Computers and Communications. Taormina, Italy, 2002

[3] Boudaoud K, Labiod H, et al. Network Security Management with Intelligent Agents // IEEE/IFIP Network Operations and Management Symposium. Honolulu, HI, USA, 2000

[4] Boudaoud K, Guessoum Z, et al. Policy-based Security Management Using a Multi-agent System // Workshop HPOWA. Berlin, 2001

[5] Torrellas G, Vargas L. Modeling a Flexible Network Security Systems Using Multi-agents Systems: Security Assessment Considerations // The 1st ACM International Symposium on Information and Communication Technologies. Trinity College, Dublin, Ireland, 2003

[6] Torrellas G, Cruz D. Security in a PKI-based Networking Environment: A Multi-agent Architecture for Distributed Security Management System & Control // The 2nd IEEE International Conference on Computational Cybernetics. Vienna, Austria, 2004

[7] Pilz A. Policy-Maker: a Toolkit for Policy-based Security Management // The 9th IEEE/IFIP Network Operations and Management Symposium. Seoul, Korea, 2004

[8] Distributed Management Task Force. CIM Specification 2.2 - 1999 Common Information Model

[9] Duan Haixin, Wu Jianping. Security Management for Large Computer Networks // APCC/OECC'99. Beijing, China, 1999

[10] Erfani S. Security Management System Functional Architecture for Enterprise Network // The 7th IEEE/IFIP Network Operations and Management Symposium. Honolulu, USA, 2000

[11] 黄承夏,杨林,马琳茹,等. 基于组件技术的网络安全管理架构研究. 信息安全与通信保密, 2006, 6: 61-63

[12] 陈汉章,张玉清. 一种基于插件与联动技术的复合安全网关. 计算机工程, 2006, 15(32): 143-145

[13] Xu C, Gong F, Baldine I, et al. Celestial Security Management System // DARPA Information Survivability Conference and Exposition. Hilton Head, USA, 2000

[14] Coyle J, Demerest J, McAllister R. A Proposed Security Management Framework for the Global Information Community // The 6th IEEE Workshop on Enabling Technologies Infrastructure for Collaborative Enterprises, Cambridge, MA, 1997

[15] Damianou N, Bandara A, Sloman M, et al. A Survey of Policy Specification Approaches. Tech Rep. London: Department of Computing at Imperial College of Science Technology and Medicine, 2002

[16] Internet Engineering Task Force. RFC3060-2001 Policy Core Information Model-Version 1 Specification

[17] Hayton R J, Bacon J M, Moody K. Access Control in an Open Distributed Environment // IEEE Symposium on Security and Privacy. Oakland, USA, 1998

[18] Ribeiro C, Zuquete A, Ferreira P, et al. SPL: An access control language for security policies with complex constraints // Network and Distributed System Security Symposium. San Diego, USA, 2001

[19] Damianou N, Dulay N, Lupu E, et al. The Ponder Policy Specification Language // Workshop on Policies for Distributed Systems and Networks. Bristol, UK, 2001

[20] Corradi A, Montanari R, Lupu E, et al. A Flexible Access Control Service for Java Mobile Code // IEEE Annual Computer Security Applications Conference. New Orleans, USA, 2000

[21] Jarnhour E. Distributed Security Management Using LDA PDirectories // The 21st International Conference of the Chilean Computer Science Society. Punta Arenas, Chile, 2001

[22] Tsoumas B, Gritzalis D. Towards an Ontology - based Security Management // The 20th IEEE International Conference on Advanced Information Networking and Applications. Vienna, Austria, 2006

[23] Tsoumas B, Dritsas S, Gritzalis D. An Ontology-Based Approach to Information Systems Security Management // Computer Network Security. Heidelberg: Springer Berlin, 2005: 151-164

[24] Shin M, Moon H, Ryu K H, et al. Applying Data Mining Techniques to Analyze Alert Data // The 5th Asia-Pacific Web Conference. Xian, China, 2003

[25] Bidou R. Security Operation Center Concept & Implementation. http://www.ossim.net/docs.php