基于 Agent 的网络入侵检测技术的研究*)

王 珺[1,2] 王崇骏[1] 谢俊元[1] 陈世福[1]
(南京大学计算机软件新技术国家重点实验室 南京 210093)[1]
(南京邮电大学通信与信息工程学院 南京 210003)[2]

摘 要 入侵检测作为一种主动的信息安全保障措施,已成为计算机安全特别是网络安全领域的研究热点。基于 Agent 技术的入侵检测系统因为其分布式协同处理和智能化的特点,正引起研究者的重视并成为未来入侵检测的一个发展方向。本文首先介绍了入侵检测系统的发展、分类与演变过程,然后分别对基于静态 Agent 与移动 Agent 技术的入侵检测系统的研究现状进行了阐述,分析了它们的研究重点与发展方向,最后指出了基于 Agent 技术的入侵检测系统的研究展望和面临的挑战。

关键词 入侵检测系统,Agent,人工智能,网络安全

Research on Agent-based Intrusion Detection Technique

WANG Jun[1,2] WANG Chong-Jun[1] XIE Jun-Yuan[1] CHEN Shi-Fu[1]
(National Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)[1]
(Nanjing University of Posts and Telecommunications, Nanjing 210003)[2]

Abstract Intrusion detection is a proactive network security protection mechanism, which has become a research focus in the field of the network security. Since the Agent-based intrusion detection systems have the features of the distributed coordination processing and intelligence, many researchers attach great importance to it and it has become a research trend for the next generation intrusion detection systems. In this paper, we first introduce the history of the intrusion detection systems (IDS)and its classifications. And then some recent research development that related to the key aspects of static Agent-based intrusion detection systems and mobile Agent-based intrusion detections systems are deeply explored. And their development treads are also given. In the end, we present some possible research directions and challenges for Agent-based intrusion detection systems.

Keywords Intrusion detection system, Agent, Artificial intelligence, Network security

1 引言

传统的网络安全技术都基本上立足于防护,但是防护技术只能做到尽量阻止攻击企图的得逞和延缓这个过程,而不能阻止各种入侵行为的发生。入侵检测(Intrusion Detection)作为一种主动的信息安全保障措施,有效地弥补了传统安全防护技术的缺陷,已成为网络安全研究的热点问题。

入侵是指系统的未授权用户试图或已经窃取了系统的访问权限,以及系统的被授权用户超越或滥用了系统所授予的访问权限,威胁或危害了网络系统资源的完整性、机密性或有效性的行为集合。入侵检测系统(Intrusion Detection System, IDS)是一种计算机软件系统,用于自动检测上述入侵行为,并收集入侵证据,为数据恢复和事故处理提供依据。有些入侵检测系统在检测到入侵特征后还试图做出某些响应,以遏制或阻止对系统的威胁或破坏。

在 20 世纪 80 年代早期,入侵检测就引起了部分研究人员的关注。1980 年 4 月 James P. Anderson 为美国空军做了一份题为《Computer Security Threat Monitoring and Surveillance》[1]的技术报告,第一次详细阐述了入侵检测的概念,提出了利用审计跟踪数据监视入侵活动的思想。1987 年 D. Denning[2]提出了第一个入侵检测模型:入侵检测系统专家框架(IDES)。而这几年入侵检测系统的发展很快,入侵检测系统也正从集中式向着分布式和智能化方向发展。

在国外,网络安全的研究起步较早,入侵检测技术相对成熟,已经有很多入侵检测系统产品开发出来,如 Cisco 公司的 NetRanger, Network Associates 公司的 CyberCop 等。这些产品各有特色,也各有局限性。作为商业产品,这些产品的技术比较保守,在检测方法和体系结构上仍有很大的不足,使得检测效果不能令人满意。另外,由于对攻击行为的认识,证据来源、攻击知识的获取与转换等方面的不确定性,导致目前入侵检测系统误检与漏检,以致造成网络系统的很大损失。如何能够对未知攻击进行分析、检测和防御成为网络防御系统的研究热点。

目前在学术界,有许多入侵检测项目在进行,其中以加州大学戴维斯分校的 GrIDS[5]、普度大学的 IDIOT[6]以及 SRI 公司承担的 EMERALD[7]等项目影响较大。特别是基于 Agent 的网络入侵检测技术近年来已经成为国际学术界的研究热点。基于 Agent 的入侵检测系统与常规入侵检测系统相比

*)本文得到国家自然科学基金(项目编号:60503021、60503049)和江苏省自然科学基金(项目编号:BK2005075)的资助。王 珺 博士生,工程师,从事分布式人工智能与多 agent 系统的研究;王崇骏 博士,研究方向:人工智能;谢俊元 博士生导师,研究方向:人工智能与网络安全;陈世福 博士生导师,研究方向:人工智能。

最大的特征是可以自动感知外界环境并能够对外界进行自动的响应。为此引入各种思维模型来解决这些问题，如著名的BDI模型[3]。目前应用BDI模型进行入侵检测系统的研究主要有MANSMA[9]以及FASA[17]等。另外还有由Purdue大学提出的一种层次结构的基于自治Agent的入侵检测框架AAFID[10]，并用perl实现了它的原型。在国内，近两年计算机安全特别是网络安全已成为研究热点，但在入侵检测技术方面的研究还只是刚刚起步，处于跟踪国外技术阶段。投入实际使用的入侵检测系统较少，系统功能还比较简单。

本文主要介绍基于静态Agent的入侵检测系统和基于移动Agent的入侵检测系统的关键技术，并给出一些系统的实例。

2 入侵检测(IDS)系统

一个典型的入侵检测系统一般由数据采集、数据分析和事件响应3个部分组成。数据采集是入侵检测的第一步，包括收集系统、网络数据、用户活动状态和行为数据。而且需要在计算机网络系统中的若干不同关键点(不同网段和不同主机)收集信息；数据分析是入侵检测系统的核心部分，主要是对数据进行深入分析，根据攻击特征集发现攻击，并根据分析的结果产生响应事件，触发事件响应。事件响应在发现入侵后会及时做出响应，包括切断网络连接、记录事件和报警等。下面主要介绍入侵检测系统分类和体系结构的演变。

2.1 入侵检测系统的分类

入侵检测系统目前还没有严格的分类标准，大致可以按照使用的方法和信息来源收集方式来分类。

2.1.1 按照使用的分析方法分类

(1)异常检测(Anomaly detection)：假设入侵者活动异常于正常主体的活动，系统将对出现异常的行为做出反应，根据这一理念建立主体正常活动的“特征档案”，将当前主体的活动状况与“特征档案”相比较，当违反其统计规律时，认为该活动可能是“入侵”行为。

(2)误用检测(Misuse detection)(又称Signature detection)：这一检测假设入侵者活动可以用一种模式来表示，系统的目标是检测主体活动是否符合这些模式。其检测方法上与计算机病毒的检测方式类似。

误用检测依据特征库进行判断，所以准确度高，但系统依赖性太强，移植性不好，特征库需要经常更新，维护工作量较大，且不能发现未知的攻击。异常检测与系统无关，通用性好，可以检测以前未出现过的攻击，缺陷在于误检率高。目前的入侵检测系统往往结合这两种检测技术。

2.1.2 依照信息来源收集方式进行分类

(1)主机型入侵检测系统(Host-based Intrusion Detection System，HIDS)：早期的入侵检测系统结构，其检测的目标主要是主机系统和系统本地用户，检测原理是根据主机的审计数据和系统日志发现可疑事件。这种方法的优点：准确率高，实时性好。缺点是在网络环境下会出现漏检的情况，比如有些活动对于单机来说构不成威胁，对于整个网络来说可能是入侵活动。

(2)基于网络的入侵检测系统(NIDS)：这种系统使用原始网络包作为数据源。NIDS在一个或多个网络关键点部署入侵检测点。数据源来自“网络流”，通过对包头和内容的分析来识别可疑的网络入侵。NIDS通常利用一个运行在混杂模式下的网络适配器来实时监视并分析通过网络的所有通信业务。其优点是：成本低；能够检测到主机型检测系统检测不到的攻击行为；入侵者消除入侵证据困难；不影响操作系统的性能。其缺点是：如果网络流速高时可能会丢失许多数据包，容易让入侵者有机可乘；无法检测加密的数据包；对于直接对主机的入侵无法检测出。

2.2 入侵检测系统体系结构的演变

2.2.1 集中式双组件体系结构

第一代入侵检测系统使用双组件的体系结构：收集组件和分析组件，收集组件从主机审计日志和内部接口或监视网络上的包来搜集信息，然后把这些信息传给中央分析组件，中央分析组件可使用一种或多种不同的检测技术。这两个逻辑组件或者配置在一个主机上或者物理上分布。这种结构又可以分为两类：(1)集中采集、集中分析方式：即数据采集和检测分析在同一台主机上，此时数据采集和分析都是集中的；(2)分布采集、集中分析方式。

上述集中式的模型存在几个明显的缺陷：(1)面对大规模、异质网络基础上发起的入侵行为，中央分析组件的业务可能会达到不可承受的地步，以至会造成许多重大信息事件的遗漏，大大增加了漏报的概率；(2)由于网络的延时，到达控制台的数据包中的事件消息已经不能反映当前状态；(3)可扩展性差；(4)异质网络环境所带来的差异会给系统带来诸多困难。

2.2.2 分布式体系结构

随着网络技术的发展，网络攻击呈现出以下趋势：(1)攻击的综合化与复杂化；(2)攻击主体对象的间接化；(3)攻击的规模扩大；(4)攻击技术的分布化；(5)攻击对象的转移。

为了克服集中式体系结构的缺点以及适应新的攻击，分布式结构的入侵检测系统应运而生。它在收集和分析组件间引入中间组件构成分层，这些中间组件将从收集进程获得的信息预处理且合并起来输入到分析进程。分布式结构又可分为分级组织模型、网状组织模型或者二者的混和模型。

分布式入侵检测(distributed intrusion detection)是目前入侵检测乃至整个网络安全领域的热点之一，国内外众多的大学、研究机构、安全团体、商业组织都致力于这方面的研究工作。到目前为止，还没有真正实用的分布式入侵检测的商业化产品，但研究人员已经提出并完成了多个原型系统，如UC Davis的DIDS系统(distributed intrusion detection system)[4]，GrIDS系统(graph-based intrusion detection system)[5]。

2.2.3 基于Agent的入侵检测系统

尽管分布式入侵检测系统改善了网络抗攻击的能力，但这种系统也存在很多的局限性，比如局部故障会影响整体，难以动态配置和跨异构平台工作等等。一些学者提出，因为Agent技术具备分布式协同处理和智能化的特点，将之引入入侵检测领域，正好可以弥补传统入侵检测系统的不足，基于Agent的网络入侵检测系统具有以下的特点：

(1)Agent的自治性使得各个Agent之间的依赖很小，单个Agent失效并不会影响系统的整体工作。如果Agent之间存在着协作，它会影响到与之协作的Agent，但是并不会把故障扩散到整个系统。

(2)Agent的应用使得系统可以动态配置和升级，而不需要重新启动整个系统。如果需要检测一种新的入侵，只需要添加并启动能检测到它的特定Agent就可以了，而不会对其它Agent造成影响。同样，如果想要删除对一种过时的入侵

形式的检测，只需要停止相应的 Agent 即可。

(3)Agent 可以较好地应用在异构环境下。目前很多大型企业网都存在多种计算平台和设备，应用 Agent 技术，可以对它们实现应用层互操作。

(4)基于 Agent 的入侵检测可以实现传统入侵检测技术不具备的能力，如实现多点检测，跨越基于主机和基于网络的入侵检测的传统边界。

(5)Agent 的移动特性也为入侵检测提供了很多新的思路，譬如可以减轻网络的负担，缩短网络延时等。

基于 Agent 的入侵检测技术(Agent-Based Intrusion Detection)逐渐引起研究者的重视，成为未来入侵检测的一个重要发展方向。基于 Agent 的入侵检测系统一般可以分为静态 Agent 的 IDS 和移动 Agent 的 IDS。

3 基于静态 Agent 的入侵检测技术

Agent 可以看作是在某一环境中持续自主发挥作用，有生命周期的计算实体[8]。持续和自主反映了 Agent 可以响应环境的变化而不依赖人工干预做出灵活和智能的反应能力。在理想状态下，连续运行一段时间的 Agent 应具有从过去的经历中学习的能力。在同一环境中共存的 Agent 集体具有能相互合作的能力。本文中的 Agent 是指：在主机上进行某项安全检测功能的软件 Agent。静态 Agent(Stationary Agent)是最先提出的应用于入侵检测系统的 Agent 技术，目前已经有很多这方面的研究。静态 Agent 是指 Agent 驻留于某一固定的位置或某个固定的平台。

3.1 基于静态 Agent 的入侵检测系统的关键技术

基于 Agent 的入侵检测系统的研究近几年一直是入侵检测领域研究的重要领域，对它的研究涉及很多内容，主要有：数据缩减技术，数据协同分析，Agent 之间的协作与通信以及如何将思维模型应用到基于 Agent 的入侵检测中。

3.1.1 数据缩减技术[11]

数据缩减：从大量数据中识别出重要数据，以提高数据处理的效率。一方面可以减少数据的存储量，缓解模块之间数据通信及分析的压力，还可以减少系统的训练时间，提高学习的准确性。同时由于减少冗余数据，便于发现数据的特征。数据缩减主要通过以下方法实现。

(1)数据过滤(Data Filtering)：在数据处理之前过滤那些和入侵无关的数据。DIDS[4]、MIDAS[12]等系统采用的是专家系统的方式建立规则来进行数据过滤，也有系统采用了神经网络来实现。

(2)特征选择(feature selection)：研究如何利用人工智能的方法从大量数据中选取和入侵有关的特征来进行分析。这一方面的研究比较少，文[13,14]中做了这方面的研究，主要提出两种方法进行特征选择：支撑矢量机(SVM)和人工神经网络(ANN)技术。

(3)数据聚类(Data Clustering)：通过存储聚类的特征而不是实际的数据可以达到进一步数据缩减的目的，常用的方法有：K 均值算法、基于密度算法以及自组织图算法等，最近的相关研究有文[15]。

3.1.2 数据协同分析

数据分析是对收集到的有关系统、网络、数据及用户活动的状态和行为等信息，一般通过 3 种技术手段进行分析：模式匹配、统计分析和完整性分析。入侵监测不仅需要利用模式匹配和异常监测技术来分析某个监测引擎所采集的数据，以发现一些简单的入侵行为，还需要在此基础上利用数据挖掘技术，进行数据协同分析。

当监测引擎面对并非单一的数据时，综合使用各种监测技术就显得十分重要。数据分析协同需要在两个层面上进行，一是对一个监测引擎采集的数据进行协同分析，综合使用监测技术，以发现较为常见的、典型的攻击行为；二是对来自多个监测引擎的审计数据，利用数据挖掘技术进行分析，它通过审计数据的相关性发现入侵，以发现较为复杂的攻击行为。

3.1.3 思维模型在入侵检测系统中的应用

基于 Agent 的入侵检测系统与过去入侵检测系统相比最大的特征就是可以自动感知外部环境并能够对外界进行自动响应，为了达到这个目的，需要引入各种思维模型来解决这些问题，如 BDI 模型[3]。目前应用 BDI 模型进行入侵检测的主要有 MANSMA[9]，以及 FASA[16]，它们使用 BDI 模型来建立数据分析和响应 Agent。因为 BDI 模型能够针对当前的环境和已有的知识进行推理并可以根据目标采取合理的行为，因此通过使用 BDI 模型可以模拟网络管理员的分析推理能力。

3.1.4 Agent 间的协作与通信

基于 Agent 的入侵检测系统的体系结构中，各个 Agent 之间相互独立，但同时又相互协作，以完成共同的检测任务。这种协作有多种模式。相同的 Agent 之间互相协作，可以防止系统和 Agent 失效；一旦有 Agent 失效，其它 Agent 可以采取措施，通过承担起失效 Agent 的任务或者启动新的 Agent 的办法来进行失效弥补。另外异种和不同功能的 Agent 之间也可以进行互补性协作完成共同的目标。美国国防高级研究计划署(DARPA)提出的公共入侵检测框架 CIDF(Common Intrusion Detection Framework)[17]中定义了入侵检测系统中的 6 种协同方式，分别是：分析(Analyzing)、互补(Complementing)、互纠(Reinforcing)、核实(Verifying)、调整(Adjusting Monitoring)和响应(Responding)。入侵检测系统要完成检测任务，就离不开协作，而协作就是通过分布式入侵检测系统中 Agent 之间的通信来实现的。Agent 间通信可以使用 KQML(Knowledge Query and Manipulation Language)，也可以自行设计一套通信协议。

3.2 典型方案的系统结构

3.2.1 MANSAM 入侵检测系统

文[9]提出的 MANSMA (Multi-agents System-based Network Security Management Architecture)是基于 Agent 技术并是最早使用 BDI 模型来处理入侵检测的系统。在 MANSMA 中，Agent 具有认知能力，可以对复杂的入侵进行分析，并且具有反应能力，迅速适应环境的变化的能力。其逻辑结构为图 1 所示。

MANSMA 模型是两层 Agent 结构：管理层和本地层。管理层：管理大型网络中全局网络的安全性；本地层：只管理自己域内的安全性。管理层分为三层：安全策略管理 Agent (Security Policy Manager Agent：SPMA)、外网管理 Agent (Extranet Manager Agent：EMA)和内网管理 Agent(Intranet Manager Agents：IMA)。本地层(local layer)是由一组(local agent：LA)组成的。每个 LA 可以用于不同的特性。Agent 具有三个功能：过滤功能(filtering function)、交互功能(interaction functions)和思考功能(deliberation function)。其中思考模块代表 Agent 的信念，目标，意图和知识，它为达到 Agent的目标对收到的信息进行处理和响应。

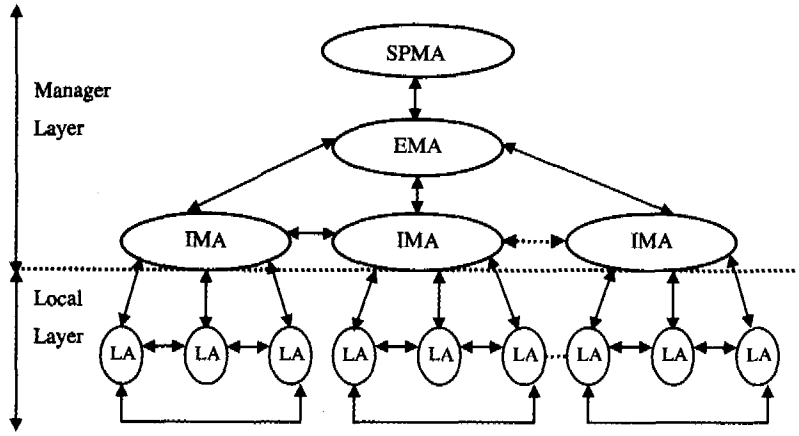

图 1　MANSMA 逻辑结构图

3.2.2　AAFID 入侵检测系统

文[10]提出的 AAFID(Autonomous Agent for Intrusion Detection)是由 Purdue 大学提出的一种层次结构的基于自治 Agent 的入侵检测框架,并用 perl 实现了它的原型。它的逻辑结构如图 2 所示。AAFID 包含 4 个部件:监视器(Monitor)、收发器(Transceiver)、代理(Agent)和过滤器(Filter)。这些部件中的每一个都称为 AAFID 实体,它们分布在系统中各处,具有自治性,独立完成各自的任务。

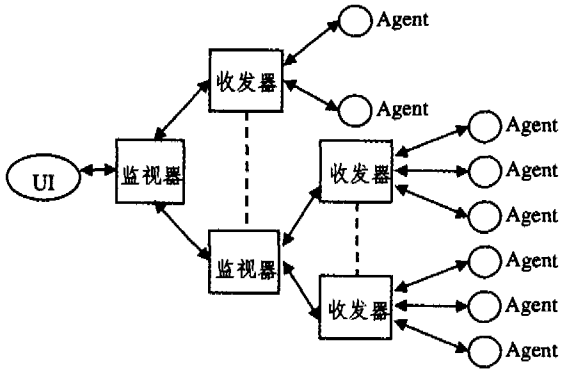

图 2　AAFID 的逻辑结构图

AAFID 系统可以分布在网络中任意数目的主机上,在一台主机上可以运行任意数目的 Agent。Agent 可以通过过滤器来获取数据,也可以直接获取,每一台主机上的各个 Agent 执行特定的检测任务,并向收发器汇报检测结果。每台主机上只有一个收发器,它监管本机上的所有 Agent 的运行情况,收发器将自身汇总的数据报告给一个或多个监视器。监视器监控收发器的运行,对收发器汇报的数据进行综合并使用用户界面来提供信息给最终用户。在 AAFID 体系结构中,Agent 之间不进行通信,只是把各自生成的信息发给转发器,由收发器根据 Agent 的配置信息和参数来决定如何处理这些信息。此外,Agent 也没有直接的报警权利,一般由收发器或监视器对用户生产警报。此方案的缺点:监视器是一个单一失效点。

4　基于移动 Agent 的入侵检测系统(MAIDS)

基于静态 Agent 的 IDS 很好地解决了传统 IDS 的一些固有缺陷,但同时又带来了一些新问题,如网络数据流量大,系统配置困难等等。为此,研究者又提出将移动 Agent 技术运用到入侵检测中来,构建基于移动 Agent (MA: Mobile Agent)的 IDS(MAIDS)。移动 Agent 是一类特殊的软件 Agent,它除了具有软件 Agent 的基本特性外,还具有移动性,即它可以在网络上从一台主机自主地移动到另一台主机,代表用户完成指定的任务。

移动性和自主性应用于入侵检测机制可实现一种理想的"哪里有入侵哪里就有检测"的系统模型。不仅能实现全网络范围内的入侵检测功能,具有良好的可移植性,而且对网络系统和主机的资源占用较低,减少网络时延,减少出现网络瓶颈的可能,使得分布式入侵检测更为灵活。其缺点是移动 Agent 的安全性比较难保障,引入移动 Agent 会对原有系统的性能有所影响。因此过多地采用移动 Agent 会对检测性能带来副作用,解决方法是:将静态 Agent 和移动 Agent 结合使用。

4.1　基于移动 Agent 的入侵检测系统的关键技术

对基于移动 Agent 的入侵检测系统的研究主要有:Agent 的迁移问题、移动代理间的通信以及 Agent 的安全问题等。

4.1.1　Agent 的迁移问题

移动 Agent 的迁移分为强迁移和弱迁移两种。

强迁移是指在迁移目的地,从 Agent 的断点处执行,如果移动 Agent 包含多个线程,则多个线程同时从断点处执行。强迁移要求 Agent 代理系统提供捕捉执行状态、恢复执行状态的功能。弱迁移只携带代码状态和数据状态,根据需要只把移动 Agent 的部分执行状态存入数据状态中随 Agent 一起移动。由于传输的数据量有限,弱迁移操作的开销小,执行效率高,但它改变了移动后的执行语义。

移动机制主要研究移动的实现方式,不同的系统采用的移动机制不同。目前移动 Agent 采用的移动机制分为两大类:一类是将移动 Agent 的移动路线、移动条件隐含在移动 Agent 的任务代码中,其代表系统是 IBM 的 Aglets;另一种是将移动 Agent 的移动路线、移动条件从移动 Agent 的任务代码中分离,用所谓的"旅行计划"表示,其代表系统是 Mitsubishi 公司的 Concordia。

移动 Agent 的移动策略是指根据移动 Agent 的任务、当前网络负载和服务器负载等外界环境,动态地为其规划出移动路径,使移动 Agent 在开销最小的情况下,最快最好地完成任务。移动策略的优劣直接影响移动 Agent 的性能直至任务的完成。移动策略一般可以分为静态路由策略和动态路由策略。在静态路由中,主机和访问次序在移动 Agent 执行任务之前就已经确定;在动态路由中,访问哪些主机及次序在移动 Agent 执行任务之前是无法预料的,由移动 Agent 根据任务

的执行情况自主的决定，一般由用户指定一个初始的路由表，移动 Agent 在按照这个表移动的过程中可以根据周围环境的变化自主的修改路由表。动态路由方式体现出移动 Agent 的反应性、适应性和自主性。

目前移动 Agent 的移动机制的研究比较广泛和深入，相比之下，有关移动策略的研究还比较少，未见有系统对移动 Agent 的移动策略给出一个较为精确和系统的说明。

4.1.2 *移动 Agent 的通信*

移动 Agent 采用的通信手段很多，包括消息传递、RPC、RMI 和 Agent 通信语言等。Agent 通信语言(Agent Communication Language，简称 ACL)是实现移动 Agent 与移动 Agent 执行环境，以及移动 Agent 之间通信的高级方式。开放式移动 Agent 系统的 ACL 系统应当具有环境无关、简洁、语法语义一致等特点。KQML 和 XML 是两种具有发展潜力的通信语言(或协议)，前者主要用于知识处理领域，后者在 Internet 环境(尤其是 WWW)中具有很好的支持能力。

4.1.3 *移动 Agent 的数据安全问题*[20]

移动 Agent 系统是由移动 Agent 和多个为移动 Agent 提供服务的主机组成的。但是我们并不能保证整个系统中每个主机都是完全可靠的，其中有可能存在一些恶意主机。这些恶意主机试图攻击移动 Agent，窃取移动 Agent 的重要信息，更为严重的是对 Agent 的信息进行篡改，使之产生不正确的结果。因此，当在潜在的恶意环境下执行，移动 Agent 的保护问题尤为重要的。对移动 Agent 的保护，具体到移动 Agent 所包含的数据来说，主要是保护移动 Agent 数据的机密性和完整性。

移动 Agent 数据的保护并不是一个简单的问题，目前在这方面进行了很多的研究，但是还没有完整的解决方案。当前在该领域的研究可以分为两类：

(1)基于检测的保护措施

根据对运行环境进行检测来判断其是否安全，以及对移动 Agent 的执行结果进行检测来判断其是否受到了攻击并遭受破坏，如使用可信任第三方实体(TTP)方法[21]、路径哈希链方法[22]和 Co-Signing 方法[23]等。

(2)主动的保护措施

基于检测的方法是被动的，它只能检测到主机对 Agent 的攻击，并不能真正保护移动 Agent 在不信任的运行环境上安全运行。要让移动 Agent 在不信任主机上完全地安全运行，目前大都是基于硬件的方案。如信任运行环境(TPE)就是一种基于硬件的保护方法[24]。

4.2 几种典型的基于移动 Agent 的入侵检测系统

20 世纪 90 年代初，General Magic 公司首先在推出其商业系统 Telescript，第一次提出了移动 Agent 的概念。目前比较有影响的系统有 IDA[18]，JAM[19]，MADIS[26]。

日本安全机构 IPA 提出的 IDA 系统(Intrusion Detection Agent System)的最大特点是利用 MA 实现了入侵追踪[18]。IDA 是一种层次结构的多主机 IDS，其由一个管理器、多个传感器、布告板和信息板(用于 Agent 之间的通信)、追踪 Agent 和信息收集 Agent 等组成。IDA 自定义一种可疑入侵者踪迹(Marks Left by Suspected Intruder，MLSI)来检测入侵。一旦发现 MLSI，IDA 会收集与 MLSI 有关的信息，进行分析，判断是否是入侵发生。

美国 Columbia 大学提出的 JAM(Java Agents for Meta-learning)[19]系统利用 MA 技术，将后向学习(Meta-learning)和分布式数据挖掘用于入侵检测。在 JAM 的分布式 Agent 中每个 Agent 运用数据挖掘，如分类、关联和序列分析等对知识和行为进行建模和推理。系统的设计包括两个核心组件：(1)本地的检测 Agent，主要用来在一个单一的团体信息系统中学习怎样去检测入侵。(2)一个后向学习系统，用来结合本地单个 Agent 学习的知识，以进一步发掘有用信息。

目前国外基于 MA 的 IDS 研究已有一定的成果，国内在基于 MA 技术的 IDS 方面的研究起步较晚，虽然近几年来国内各大高校也开始这方面的研究，但大多限于理论方面。

5 研究展望

基于 Agent 的入侵检测系统作为一个全新的研究领域，在理论研究和工程技术两个方面向我们提出了挑战。在未来的研究中，以下几个方向值得关注：

(1)如何追踪攻击者。为实现入侵追踪，IDS 需要嗅探每个以太网节点和分析每个主机。通常所需要的基本构件耗费很高，但对于安装了 Agent 平台的系统就变得容易多了。IDA 成功实现了局域网内部的入侵追踪，这对于大的局域网是相当有用的，因为可以追溯到入侵的起点，从而为入侵损失的评估和恢复提供更多的信息；文[25]也对这方面作了研究。对于因特网的入侵追踪，实现的难点更多，但随着网络技术的发展，是一个很有前景和挑战性的研究方向。

(2)如何建立灵活的响应机制。移动 Agent 用于 IDS 的最大潜力在于对入侵的反应而不是检测入侵。因为响应可以从网络中几乎任何地方启动，移动 Agent 能够用比传统的 IDS 更加理想的方式处理入侵。移动 Agent 可以提高 IDS 在目标主机处产生反应，对攻击源主机产生反应，从主机和网络组件收集攻击证据，隔离源主机和目标主机等。

(3)意图识别技术和建立对手思维模型来提高入侵检测系统的效率和准确率。入侵者出于自身意图对检测 Agent 有意回避甚至对关键节点 Agent 主动攻击，这两者之间就是典型的群体对抗问题。可以通过对意图识别的研究来提高入侵检测系统的检测准确性和效率。

(4)智能入侵检测技术。智能入侵检测技术现阶段常用的有神经网络、遗传算法、贝叶斯网络、模糊技术、免疫原理等方法用于入侵特征的辨识与泛化。但每种智能入侵检测技术都不可避免存在一定的缺点，因此下一步的发展趋势是将多种智能入侵检测技术进行融合，如引入数据挖掘技术进行数据获取和简化，引入模糊逻辑改善知识的表达，引入人工免疫、机器学习、模式匹配技术进行检测，充分发挥各种智能检测技术的优势，真正达到智能化入侵检测的目的。

结束语 传统的入侵检测系统因为其固有的局限性，面对日益翻新的网络攻击手段往往显得束手无策，基于 Agent 的入侵检测技术充分利用 Agent 的自治性与智能性，有效加强了安全防御体系的可靠性和稳定性。基于 Agent 的入侵检测技术是一个崭新的、非常有前途的研究领域，该领域已经成为国内外学者的研究热点，并已取得了许多的研究成果，但还有很多关键技术亟待解决。同时该领域的进一步发展存在着很多方向和不确定性，有赖于计算机智能科学上的研究和突破。

参 考 文 献

1 Anderson J P. Computer Security Threat Monitoring and Surveillance,[Technical report]. James PAnderson Co, Fort Washington, Pennsylvania, April 1980

(下转第 77 页)

检验合法性决定是否允许该客户对资源的访问。

4 性能分析

GCSAM授权模型，采用SPKI证书实现在网格环境中的授权管理。下面我们将对此授权模型进行评价。

不可伪造性：SPKI证书的签发和传递都是用证书的签发者的私钥进行签名，这样防止了证书的伪造。

不可抵赖性：SPKI证书是采用私钥签名的，公钥发布给接收者，使得资源所有者对所共享的资源负责，用户对资源进行访问受到了保护，不会有恶意病毒入侵的危险。

安全性：由于SPKI是采用密钥签发证书，增强了证书的私密性，也使系统的整体安全性进一步得以保证。

灵活性：采用SPKI证书委托授权，使得授权模型与CAS相比更加灵活。

SPKI电子证书采用"授权-公钥"机制，解决了CAS中的必须全球唯一的名字的限制，增强了系统的可操作性。并且资源通过SPKI证书链可以细粒度的控制客户访问权限。

参 考 文 献

1 Pearlman L, Welch V, Foster I, et al. The Community Authorization Service: Status and Future CHEP, 2003

2 Foster I, Kesselman C, Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International Journal of High Performance Computing Applications, 2001, 15(3): 200～222

3 Foster I, Kesselman C. Globus: A Metacomputing Infrastructure Toolkit. International Journal of Supercomputer Applications, 1998, 11 (2): 115～129

4 Boudriga N, Obaidat M S. SPKI-based Trust Manage ment in Communications Networks Computer and Telecommunication Systems[J], SPECTS, 2003. 719～726

5 Authorization processing for Globus Toolkit Java Web services. http://www-128. ibm. com/developerworks/grid/library/gr-gt4auth/ 2005. 12

6 Mjogeman M, Thomasson R. Performance Simulations ,of the UMTS Common Packet Channel. http://citeseer. nj. nec. com/443486. html

7 Koodli R, Puuskari M. Supporting packet-data Qos in next generation cellar networks. IEEE Communications Magazine, 2001, 39 (2)

8 CAS AlpahR2 Web site. http://www. globus. org/Security/cas/alpha-r2/, septmber 2002

9 Simple Object Access Protocal(SOAP)1. 1. W#C, 2000

10 The Globus Toolkit 4. 0 Release Manuals, 2005. http://www.globus. org/toolkit/docs/4. 0/

11 Foster I, Kesseman C. The Grid 2. 电子工业出版社, 2004

12 徐志伟，冯百明，李伟. 网格计算技术. 电子工业出版社, 2004

（上接第69页）

2 Denning D E. An Intrusion Detection Model. IEEE Transactions on Software Engineering, 1987(2): 222

3 Rao A, Georgeff M. Modeling rational agents within a BDI architecture. In: Proceedings of the Second International Conference on Principles of Knowledge Representation and Reasoning, 1991

4 Snapp S R, Smaha S E, Teal D M, et al. The DIDS (distributed intrusion detection system) prototype. In: Proc. of the Summer USENIX Conference. Berkeley, CA, USA, 1992. 227～2335

5 Chen S S, Cheung S, Crawford R, et al. GrIDS -A graph based intrusion detection system for large networks. In: The 19th National Information Systems Security Conference (NISSC), Baltimore, MD, USA, 1996. 361～370

6 Kumar S, Spafford E H. A pattern matching model for misuse intrusion detection. In: Proceeding of the 17th National Computer Security Conference, U. S. A, 1994. 11～21

7 Porras P A, Neumann P G. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In: Proceeding of the 20th National Information Systems Security Conference, Maryland, USA, Oct. 1997. 353～365

8 程显毅. Agent计算. 哈尔滨：黑龙江科学技术出版社, 2003

9 Boudaoud K, Guessoum Z. A Multi-agents System for Network Security Management. In: Proc. of Telecommunication Network Intelligence, IFIP TC6 WG6. 7. Sixth International Conference on Intelligence in Networks (SMARTNET 2000), Austria, September 2000. 172～189

10 Spafford E, Zamboni D. Intrusion detection using autonomous agents. Computer Networks, 2000, 34(4): 547～570

11 Frank J. Artificial Intelligence and Intrusion Detection: Current and Future Directions. In: Proceedings of the 17th National Computer Security Conference, 1994

12 Sebring M, Shellhouse E, Hanna M, et al. Expert Systems in Intrusion Detection: A Case Study. In: Proceedings of the 11th National Computer Security Conference, 1988

13 Siedlecki W, Sklansky J. On Automatic Feature Selection. International Journal of Artificial Intelligence , 1998, 2(2)

14 Sung A H, Mukkamala S. Identifying Important Features for Intrusion Detection Using Support Vector Machines and Neural Networks. In: Proceedings of the 2003 International Symposium on Applications and the Internet Technology, 2003. 209～216

15 Zhong S, Khoshgoftaar T M, Seliya N. Clustering-based Network Intrusion Detection. International Journal of Reliability, Quality and Safty Engineering, 2005

16 Shajari M, Ghorbani A A. Application of Belief-Desire-Intention agents in intrusion detection and response. In: Proceedings of Privacy, Security, Trust Conference, Fredericton, New Brunswick, October 2004. 181～191

17 Kahn C. Communication in the Common Intrusion Detection Framework. In: CIDF Working Group document, 1998. 100～105

18 Asaka M, Okazawa S, Taguchi A, et al. A Method of Tracing Intruders by Use of Mobile Agents. In: Proc. 9th Annual Internetworking Conference (INET'99), San Jose, CA, 1999. 1～12

19 Stolfo S, Prodromidisy A L. JAM: Java Agents for Meta Learning over Distributed Databases. In: Proceedings of the 3rd International Conference on Knowledge Discovery and Data Mining, CA, August 1997. 74～81

20 Karjoth G, Lange D B, Oshima M. A security model for Aglets. IEEE Internet Computing, 1997, 1(4): 68～77

21 Corradi A, Cremonini M. Mobile Agents integrity for electronic commerce applications. Information Systems, 1999, 24(6): 519～533

22 Karjoth G, Asokan N, Gle C. Protecting the computation results of free-roaming Agents. In: Rothermel K, Hohl F, eds. Mobile Agents: 2nd Int'l Workshop. London: Springer-Verlag, 1998. 195～207

23 Cheng JSL, Victor KW. Defenses against the truncation of computation results of free-roaming Agents. In: Deng RH, Qing SH, Bao F, et al. eds. Information and Communications Security. London: Springer-Verlag, 2002. 1～12

24 Wilhelm G, Staamann M. A pessimistic approach to trust in mobile Agent platforms. IEEE Internet Computing, 2000, 4(5): 40～48

25 Barrière L, Flocchini P, Fraigniaud P, et al. Capture of an Intruder by Mobile Agents. In: 14th ACM Symp. on Parallel Algorithms and Architectures (SPAA '02), Winnipeg, August , 2002

26 Slagell M. The Design and Implementation of MAIDS: [Technical Report TR01-07]. Iowa State University, Department of Computer Science, Ames, IA, USA, 2001