一种基于移动代理的入侵检测系统框架*

周海刚** 肖军模

(解放军理工大学通信工程学院 南京 210007)

【摘要】为了提高入侵检测系统的效率和灵活性，提出了一种基于移动代理的入侵检测系统框架。分析了已有的入侵检测系统，研究了移动代理的实现及如何保证移动代理和移动代理运行环境的安全。该框架对建立一个有效的入侵检测系统有一定的理论和现实意义。

关 键 词 移动代理; 网络入侵; 入侵检测; 网络安全

中图分类号 TP393.08 文献标识码 A

A Framework of Intrusion Detection System Based on Mobile Agents

Zhou Haigang Xiao Junmo

(Institute of Communications Engineering，PLA Univ. of Sci. & Tech. Nanjing 210007)

Abstract In this paper, the intrusion detection systems nowadays are analyzed, and a framework of intrusion detection system based on mobile agents is proposed. How to implement mobile agents are as well as how to ensure the security of the mobile agents and whose running environment is studied. This framework will be significant for building an effective intrusion detection system.

Key words mobile agent; network intrusion; intrusion detection; network security

为了保证网络的机密性、完整性和可用性，操作系统安全增强技术和防火墙技术应运而生。但作为静态的安全防御技术，对网络环境下日新月异的攻击手段缺乏主动的反应。因此作为动态的网络安全防御技术，入侵检测提供了对内部攻击、外部攻击和误操作的实时保护，使得网络系统在受到危害之前拦截和响应入侵，为网络安全人员提供了主动的防御手段。从网络安全立体纵深、多层次防御的角度出发，入侵检测系统受到了人们的高度重视。

1 已有入侵检测系统的分析

一般的入侵检测系统分为两类：1) 基于异常的入侵检测系统；2) 基于误用的入侵检测系统；异常的入侵检测系统是通过检测异常行为和计算机异常使用情况来检测入侵行为。一般有特征选择的异常检测、贝叶斯推理的异常检测、数据挖掘的异常检测、神经网络的异常检测、统计的异常检测等方法。基于误用的入侵检测是利用已知系统和应用软件的脆弱性攻击模式来检测入侵行为。一般有条件概率、模型误用推理和专家系统的误用入侵检测方法。入侵检测模型如图1所示[1]。

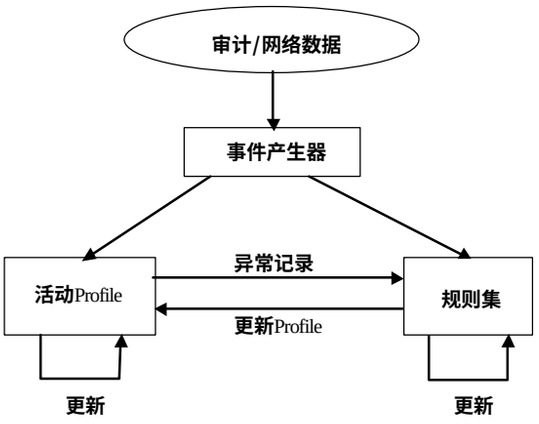

图1 入侵检测模型

2002年9月20日收稿

* 国家自然科学基金资助项目，编号：69931040

** 男 28岁 博士生 主要从事网络和信息安全、移动代理、网络管理等方面的研究

从体系的结构分析，入侵检测系统分为主机的入侵检测和网络的入侵检测。另外也出现了基于代理的分布式入侵检测系统[2]。主机的入侵检测系统检测的主要目标是主机系统和本地用户，根据主机的审计数据和系统的日志发现可疑事件。该系统已难以适应网络安全的需求。由于网络入侵行为已不再是单一的行为，越来越表现为相互协作的特点，所以网络的入侵检测系统也暴露出其弱点。代理的入侵检测系统通过相互独立运行的代理来检测入侵行为，并将检测结果传送到检测中心。但这种系统代理间的相互协作比较困难，消耗网络带宽较大，远程的交互较为固定，而且不能定制服务。

2 移动代理的入侵检测系统框架

2.1 系统框架

移动代理的入侵检测系统框架如图2所示，从图中可看出系统由控制与分析和被监控主机组成。控制与分析系统由控制子系统、分析子系统和告警子系统组成。控制子系统负责移动代理的创建和管理工作。

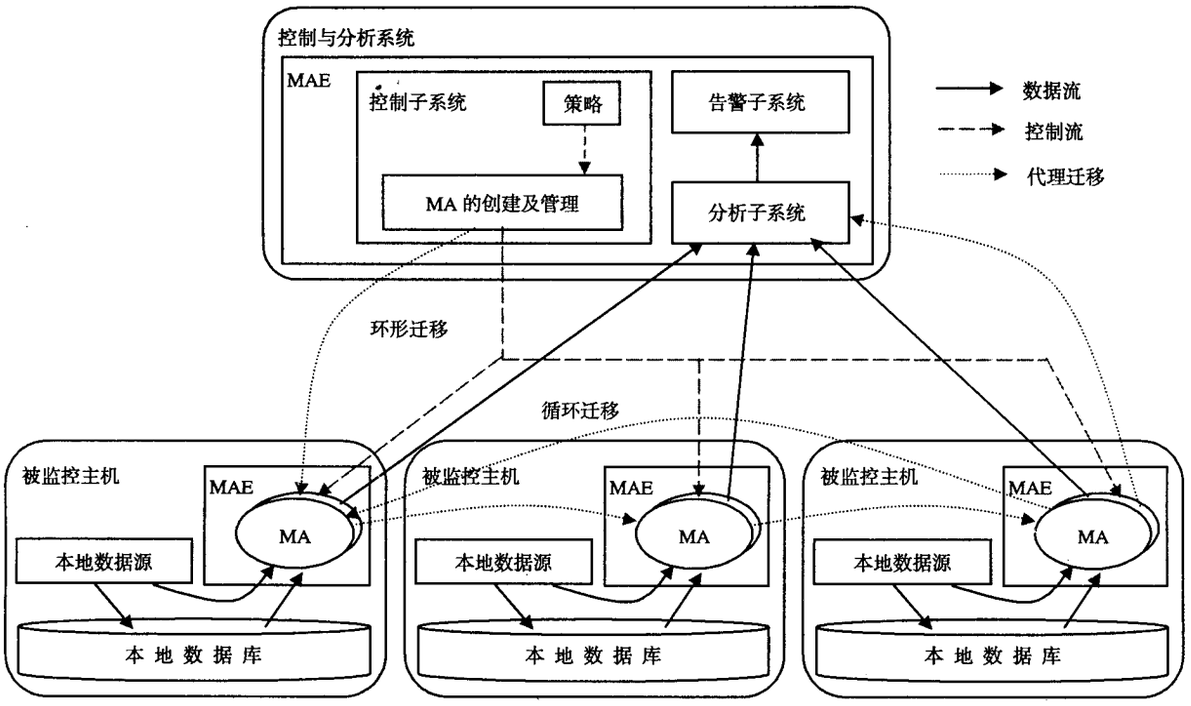

图2 移动代理的入侵检测系统框架

分析子系统综合分析MA提交的数据，并向告警子系统提交告警信息。告警子系统对检测到的入侵行为提出告警。被监控主机系统由本地数据源、数据库、MAE和MA组成。本地数据源即各种网络数据和审计记录等。本地数据库将本地数据源存储下来。MAE即为移动代理环境，是一个分布在网络各种计算设备上的软件系统，是移动代理能够运行的所必须的支撑环境。MA即移动代理，是能够存活在MAE中的软件实体。MA可以移动，MA的移动就是从一个MAE移动到另一个MAE。其工作过程如下：1) 控制子系统根据入侵检测系统的策略需求创建相应的移动代理，并附于一定的路由信息和智能，然后发送给相应的被监控主机来完成相应的入侵检测任务。2) 当一个主机上的任务完成后，该移动代理将根据路由信息或当前主机的信息来决定下一个到达的被监控主机，然后就可以到达新的被监控主机上继续执行其入侵检测任务。3) 根据移动代理本身携带的信息，它可返回到第一台主机来循环迁移，也可返回到分析子系统。也就是说移动代理可以有两条迁移路径：一条是在被监控主机间的循环迁移，另一条是在控制与分析系统和被监控主机间的环形迁移。迁移路径可根据系统的策略动态而改变。4) 由于移动代理的自治性具备一定的智能，所以当它到达被监控主机后，就以代理实例的形式在MAE中执行来完成其入侵检测任务。5) 移动代理一方面直接从本地数据源来获取实时的网络数据，另一方面从本地数据库中获取历史和分类数据。然后对数据进行过滤和分析，最后根据一定的规则进行入侵行为的检测。6) 检测后的结果或移动代理不能肯定的可疑数据将有两种

方式送给分析子系统在循环迁移的情况下直接发送给分析子系统，在环形迁移的情况下将数据暂存起来最后一起交给分析子系统。7) 分析子系统将移动代理送过来的检测结果和可疑数据进行综合分析，最终形成告警信息发送给告警子系统。告警子系统则对检测到的网络入侵行为向管理员提出告警。

2.2 移动代理的实现

系统的核心部件就是移动代理。本文中MAE采用JVM(Java虚拟机)，那么移动代理就是一个Java程序段。使用Java的主要原因有以下三点[3]：1) JVM便于程序移植和高效执行；2) Java的安全性允许不可信任的代码段在本地执行；3) Java使得产业界容易接受。一个移动代理包含代码、属性和状态信息。其中代码定义了移动代理的操作；属性包括发起者、移动历史、认证域、资源需求和管理知识等；状态信息定义了一些变量，这些变量反应了移动代理的当前状态，包括创建、就绪、传输、阻塞、执行和结束等。

被监控主机的框架结构如图3所示。图中S_MA实例为完成某类入侵检测任务的移动代理实例，D_MA实例为功能委派的移动代理实例。S_MA实例可以有多个，分别完成各自不同类的入侵检测任务。一般S_MA实例的代码段较长，但是相对静止，使得网络的负荷得到较大的减小。每台主机一般只有一个D_MA实例，它通过MACP(移动代理通信协议)与S_MA实例进行交互。将移动代理分为S_MA和D_MA的出发点是这种方法相对简单并易于实现。相对静止的S_MA完成任务较重的数据收集、过滤和分析工作。相对动态的D_MA在不同的主机间不停地迁移来与S_MA交互获得数据，最终将结果数据交给分析子系统。

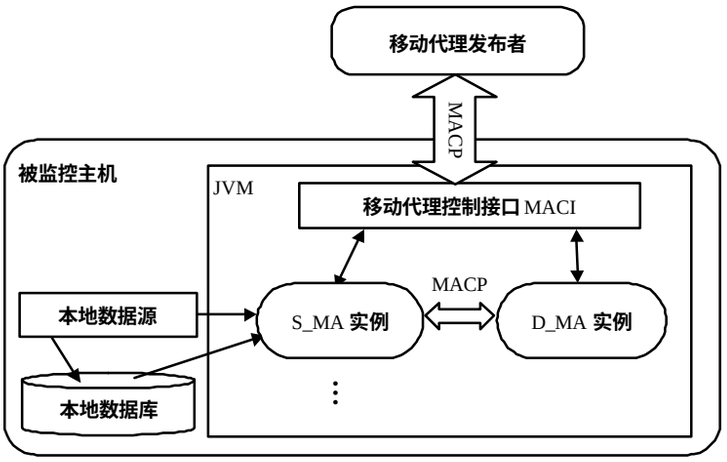

图 3　被监控主机的框架结构

移动代理发布者通过MACP经MACI(移动代理控制接口)与被监控主机联系，发送移动代理，并根据网络状态信息控制其行为。MACI提供被监控主机和移动代理发布者按照MACP通信的接口，是移动代理发布者与JVM交互的界面。MACI检查发布者的身份，并将相应的控制指令发送给S_MA和D_MA。MACI还对移动代理进行控制，它根据状态信息和知识来申请、接收移动代理、创建移动代理实例、阻塞和转发移动代理。

3 移动代理的安全性保证

移动代理是一种比较新的技术，在大规模、分布式、跨平台的应用中，移动代理拥有独特的优势[4]。应将移动代理技术应用到网络入侵检测系统中，并能实现全局范围内的入侵检测功能，具有清晰的系统结构和良好的可扩展性，及优良的可移植性能，对网络系统和主机资源的占用较低，减少了出现瓶颈的可能，而且易于分发服务。但移动代理的安全问题却需要得到更多的重视[5]。在系统中，提出一种算法来保证移动代理和位于被监控主机上的移动代理环境(MAE)的安全。具体算法为：假设控制与分析系统是在严格的安全保护下，安全的可被移动代理和MAE信任；设共有N台被监控主机，这些被监控主机上的MAE分别拥有自己的证书C_1，C_2，…，C_N，其公钥/私钥对分别为K_1/k_1，K_2/k_2，…，K_N/k_N。设控制与分析系统也有本身的证书C，其公钥/私钥对为K/k。所有的MAE和控制与分析系统都知道彼此的公钥。选择一个单向散列函数$h(\cdots)$。其步骤如下：

1) 控制与分析系统根据系统的策略创建相应的移动代理MA，用本身的私钥k加密本身的证书C和时标T：$E_k(C,T)$，然后计算散列值$h(\mathrm{MA}, E_k(C,T))$形成签名Sig。在将这个携带有签名的数据发送给某个MAE前，控制与分析系统首先用Diffie-Hellman密钥交换协议和这个MAE协商一个通信时用到的会话密钥S[6]。最后，假设要发送给MAE_i，那么发送的信息为：$E_S(\mathrm{MA}, E_k(C,T), Sig)$；

2) MA到达MAE_i后，MAE_i首先要完成以下四项任务：(1) 用会话密钥S解密，然后计算散列值

$h(\mathrm{MA}, E_k(C,T))$并与Sig比较是否相等来判断签名是否有效；(2) 用控制与分析系统的公钥K对$E_k(C,T)$解密得到C和T；(3) 根据证书C判断信息来源是否有效；(4) 根据时标T判断该信息是否处于有效时间段内。如果签名有效、来源可靠且该信息位于有效时间内，那么MAE_i赋予MA一定的权限并启动它。MA启动后，就执行相应的入侵检测任务。任务完成后，MA通知MAE_i将要去往的下一个MAE，假设为MAE_{i+1}；

3) MAE_i计算散列值$h(\mathrm{MA}, E_{k_i}(C_i,T_i))$形成签名$Sig_i$，此时的MA为携带有数据的移动代理，$k_i$、$C_i$和$T_i$分别为$\mathrm{MAE}_i$的私钥、证书和时标。然后用Diffie-Hellman密钥交换协议与MAE_{i+1}协商一个会话密钥S_i，最后发送给MAE_{i+1}加密的带有签名数据的信息：$E_{S_i}(\mathrm{MA}, E_{k_i}(C_i,T_i), Sig_i)$；

4) MA到达MAE_{i+1}后，MAE_{i+1}同样要先完成以下四项任务：(1) 用会话密钥S_i解密，然后计算散列值$h(\mathrm{MA}, E_{k_i}(C_i,T_i))$并与$Sig_i$比较是否相等来判断签名是否有效；(2) 用$\mathrm{MAE}_i$的公钥$K_i$对$E_{k_i}(C_i,T_i)$解密得到$C_i$和$T_i$；(3) 根据证书$C_i$判断信息来源是否有效；(4) 根据时标$T_i$判断该信息是否处于有效时间段内。如果签名有效、来源可靠且该信息位于有效时间内，那么MAE_{i+1}赋予MA一定的权限并启动它。MA启动后，就执行其相应的入侵检测任务。任务完成后，MA通知MAE_{i+1}将要去往的下一个MAE；

5) 改变i的值，循环执行Step3和Step4，直到MA遍历了所有的MAE，然后转Step6；

6) 根据系统的策略，如果MA的迁移路径是循环迁移，那么返回Step3。如果MA的迁移路径是环形迁移，或者由循环迁移变为了环形迁移，那么MA就要返回控制与分析系统。假设此时MA所处的MAE为MAE_j；

7) MAE_j计算散列值$h(\mathrm{MA}, E_{k_j}(C_j,T_j))$形成签名$Sig_j$，然后用Diffie-Hellman密钥交换协议和控制与分析系统协商一个会话密钥S_j，最后发送给控制与分析系统带有签名数据的信息：$E_{S_j}(\mathrm{MA}, E_{k_j}(C_j,T_j), Sig_j)$。控制与分析系统完成Step4中类似的四项任务，如果签名有效、来源可靠且该信息位于有效时间内，那么控制与分析系统将对MA携带回来的数据进行分析。

在算法中，先用Diffie-Hellman密钥交换协议协商一个会话密钥，然后再用一种对称加密算法(如AES)加密数据，这与使用公开密钥加密算法加密传输的数据相比将大大提高算法的效率。发送数据的一方在发送前都是先用本身的私钥加密证书和时标，这样数据发送到对方后就能判断数据来源的可靠性，因为只有用相对应的公钥才能解密。时标表示了一个时间段，用来防止网络中的重放攻击。利用本算法，一方面可以保护运行移动代理的被监控主机，保证移动代理是来自合法的主机，同时移动代理被赋予了一定的权限，不会滥用资源；另一方面可以保护移动代理本身，保证只有合法的主机才能获得移动代理的实例。

4 结 束 语

入侵检测发展至今，仍然存在着许多有待解决的问题，比如告警的准确性、入侵检测系统本身的安全性和决策支持问题等。入侵检测的研究同样涉及许多方面问题：如体系结构、操作系统、模式识别、数据挖掘和人工智能等，这些问题的进展都将促进入侵检测研究的逐步深入。随着新技术的发展，越来越多的新方法可用在入侵检测上。从目前的发展来看，将移动代理应用到入侵检测系统中去，仍有许多研究的新课题。新技术的产生既解决了许多旧问题，同时也带来了许多新问题。但只要有入侵行为的存在，入侵检测系统的研究将会进一步持续。

参 考 文 献

[1] Denning D. An intrusion-detection model[J]. IEEE Transactions on Software Engineering, 1987, 13(2): 222-232

[2] 马恒太, 蒋建春, 陈伟锋, 等. 基于Agent的分布式入侵检测系统模型[J]. 软件学报, 2000, 11(10): 1 312-1 319

[3] 朱淼良, 邱 瑜. 移动代理系统综述[J]. 计算机研究与发展, 2000, 11(11):16-25

[4] Fuggetta A, Picco G P, Vigna G. Understanding code mobility[J]. IEEE Transactions on Software Engineering, 1998, 24(5): 342-361

[5] Karjoth G, Lange D B, Oshima M. A security model for Aglets[J]. IEEE Internet Computing, 1997, 1(4): 68-77

[6] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

编 辑 刘文珍