计算机科学2002Vol. 29№. 3

分布式入侵检测系统综述*)

A Survey of Distributed Intrusion Detection System

董晓梅　王丽娜　于　戈　王国仁
(东北大学信息学院　沈阳110004)

Abstract The trend of the research on the intrusion detection systems is to design and set up distributed intrusion detection systems. In the paper, the concepts, methods and architectures of intrusion detection are presented, and the application of agent technology in intrusion detection system is introduced. Several representative architectures of distributed intrusion detection systems based on agent and the common Intrusion Detection Framework and its application and extension are summarized. The existing problems and the future researching direction in this field are proposed.

Keywords Distributed system, Agent, Intrusion detection, Collaboration

1　入侵检测

随着 Internet 在全世界范围内的迅速扩展,计算机网络的安全问题越来越成为人们关注的一个热点问题。入侵检测(Intrusion Detection, ID)就是保障计算机及网络安全的措施之一。近几年,对于入侵检测技术的研究发展很快,出现了很多入侵检测系统。但是,随着新的攻击方法的不断出现,尤其是一些互相协作的入侵行为的出现,给入侵检测领域的研究带来了新的课题。早期的集中式入侵检测系统已经不能有效地防止这一类的入侵。因此,研究分布式入侵检测系统是十分必要的。

1.1　入侵检测的概念

入侵检测是指发现非授权用户企图使用计算机系统或合法用户滥用其特权的行为,这些行为破坏了系统的完整性、机密性及资源的可用性。为完成入侵检测任务而设计的计算机系统称为入侵检测系统(Intrusion Detection System, IDS)。IDS 的作用是检测对系统的入侵事件,一般不采取措施防止入侵行为。一个入侵检测系统应具有准确性、可靠性、可用性、适应性、实时性和安全性等特点[1]。

1.2　入侵检测的方法

入侵检测技术主要分为误用入侵检测和异常入侵检测两类。

(1)*误用入侵检测*　使用事先收集到的有关某些特定攻击和系统弱点的知识来检测入侵行为,也称为基于知识的入侵检测。IDS 包含有关系统弱点的信息,并寻找试图利用这些弱点的行为。一旦发现这样的行为,就发出报警信息。因此,所有不是明确被认为是攻击的行为都是可以接受的。误用入侵检测方法的误警率较低,但这种方法与具体的操作系统、版本、平台和应用程序密切相关,而要检测来自内部的滥用特权的攻击就更困难。误用入侵检测方法包括专家系统、签名分析、Petri 网和状态转换分析等[2~6]。

(2)*异常入侵检测*　方法假设可以通过观察与系统或用户的正常或期望的行为的偏差来检测入侵。正常或有效行为的模型可以从收集到的参考信息中抽象出来。入侵检测系统比较该模型与当前的活动,如果观察到一个偏差,则发出一个警告。这样,任何与事先已知的行为不符的活动都被认为是入侵。因而,异常入侵检测的准确性较差。异常入侵检测方法可以检测到利用新的未知弱点的攻击,它不太依赖于具体的操作系统,且可以检测滥用特权的攻击。但是,由于在学习阶段可能没有覆盖系统的所有行为,因此异常入侵检测方法的误警率较高。而且,系统行为可能会随时间而变化。异常入侵检测方法包括统计方法、专家系统、神经网络、用户意图识别、数据挖掘和计算机免疫学方法等[1,2,7~12]。

1.3　入侵检测系统的结构

入侵检测系统可分为集中式入侵检测系统和分布式入侵检测系统。

(1)*集中式入侵检测系统*　在固定数量的场地进行数据分析,包括基于主机的和基于网络的 IDS。基于主机的 IDS 分析主机的审计数据,直接监视一台主机,常与操作系统相结合。基于网络的 IDS 被动地监视主机间的通信,根据网络上数据包的内容和格式来推断其行为,分析对敏感信息的公开请求和重复失败的违反系统安全策略的企图。早期的 IDS 都是集中式 IDS[13~15]。

(2)*分布式入侵检测系统*　运行数据分析部件的场地数量与被监视的主机数量成比例。随着网络结构的复杂性增加,网络资源一般都是分布的,而入侵活动也逐渐具有协作性,因此集中式的 IDS 就暴露出其局限性。目前对 IDS 的研究趋向于设计和建立分布式的 IDS,由多个检测实体监控不同的主机和网络部分,各实体间相互协作完成检测任务。

2　基于代理的分布式入侵检测系统

基于代理(Agent)的分布式入侵检测系统一般使用多个代理,每个代理完成一项特定功能,各代理间通过通信互相协作。

2.1　代理技术及其在分布式入侵检测系统中的应用

一个代理可以定义为:在包含其他进程和代理的环境中连续自治地运行的一个软件实体。每个代理有自己的执行线程。代理的一个突出特点就是自治性,其执行是由操作系统来

*)本文得到教育部跨世纪优秀人才基金和高等学校优秀青年教师教学和科研奖励基金资助。董晓梅　讲师,博士生,主要从事信息安全与保密方面的科研与教学工作。于　戈　教授,博士生导师,主要从事数据库、虚拟企业信息集成的科研与教学工作。

调度的。移动代理可以从网络上的一台主机迁移到另一台主机上，它的突出特点是自治性和移动性。移动性是指允许代理移动到物理存储数据的主机上，因而可以避免在网络中传输大量的数据。代理在本地访问数据，只将结果返回给用户。这种方法有两个优点：低网络通信量和更好地使用网络资源[16]。

在 IDS 中，一个代理可以在一个主机上完成一项专门的安全监视功能。由于代理是独立运行的实体，因此可以在不改变其他部件且不需要重新启动 IDS 时加入、删除和重新配置代理。也可以用一组代理来分别完成简单的功能，彼此交换信息以得出更复杂的结果。因此，可以使用代理技术构造分布式 IDS。

2.2 AAFID 系统

美国普渡大学设计了一个基于自治代理的分布式入侵检测结构 AAFID[17]，为第一个使用代理进行入侵检测的结构。该结构使用代理作为数据收集和分析的最低层的元素，系统中共包含4种部件：代理（Agent）、过滤器（Filter）、收发器（Transceiver）和监视器（Monitor）。这些部件都称为 AAFID 实体，由这些实体组成的系统就称为 AAFID 系统。

一个 AAFID 系统可以分布于网络中的任意多台主机上，每台主机包含任意多个监视主机上发生的敏感事件的代理。代理可以使用过滤器以独立于系统的方式得到数据，主机上的所有代理将其发现报告给一个收发器。在每个主机上有一个收发器，负责该主机上所有运行的代理的操作，可以开始、停止和向代理发送配置命令，还可以缩减从代理处收到的数据。收发器将结果报告给一个或多个监视器，每个监视器负责管理几个收发器的操作。监视器有权访问整个网络中的数据，因此可以完成高级的关联和检测包含多个主机的入侵。监视器可以按层次组织，一个监视器可以依次向更高级的监视器报告。收发器也可以向一个以上的监视器报告。最后，一个监视器负责与用户接口交互。AAFID 系统的结构如图1所示。

AAFID 的第一个原型系统在1995到1996年间实现，综合使用了 C，Bourne shell，AWK 和 Perl 语言。当前版本的 AAFID 是第二个原型系统，称为 $AAFID_2$，使用 Perl 5语言，在 Solaris 和 Linux 上通过了测试。

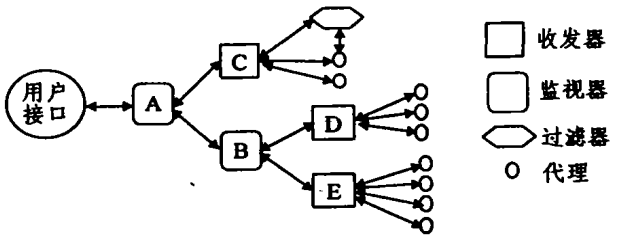

图1 AAFIDT 系统逻辑结构

2.3 基于攻击策略分析的分布式入侵检测系统

Huang M 等提出了一个基于攻击策略分析的大型分布式入侵检测框架[18]，将完成局部事件分析的分布式 IDS 代理与协作的全局代理相结合，注重于通过分析入侵者的攻击策略和将局部事件处理从全局分析中分离来使协作 IDS 代理一起工作。

（1）基于攻击策略分析的分布式入侵检测系统结构　代理分为局部代理和全局代理。局部代理进行数据收集和局部分析，以独立于机器和上下文的格式通知全局代理。全局代理进行策略分析和命令及控制。系统结构如图2所示。该结构的一个重要特性是揭示入侵者攻击策略的分析过程，该分析过程基于过去的事件序列来预言潜在的入侵行为。由于这个分析过程是决策层完成的，所以结果是独立于平台的。在这一层，用一系列逻辑相关但不必是完全的攻击步骤－攻击子目标来刻画攻击，每一步代表入侵者执行一个入侵（最终目标）时的一个完成状态。

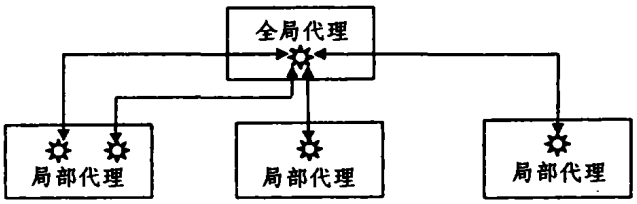

图2 基于攻击策略分析的分布式入侵检测系统结构

（2）攻击策略表示和分析　以目标树来表示策略，树根代表入侵目标，低层结点代表要完成上层目标的选项或子目标。目标树表示法有三种基本结构：OR 结构代表任何能实现上层目标的子目标集合；AND 结构代表要完成上层目标，所有子目标都必须完成；ORDERED-AND 结构中，上层目标的所有子目标都遵从一个特定顺序。OR 结构的分支可以加权来标示使用的子目标的可能程度，权越重，攻击者就越可能使用该子目标去完成高层目标。

当一个特定的攻击子目标被证实时，相应结点被填充。分布式 IDS 代理检查局部数据时，将证实的结点填充。在一个给定的时间，被填充的结点连结起来构成一个或多个水平线路。这些线路一般不完整，有一些洞（未填充结点）。一条线路代表攻击进展的一个逻辑序列，其中的洞表示需要证实的攻击子目标。IDS 代理可以根据一棵部分填充的树来进行分析，以决定最有可能的攻击路线。分析包括：长度分析、权重分析和时间分析。

2.4 基于 Agent 的分布式入侵检测系统模型

马恒太等[19]提出了一个基于 Agent 的分布式入侵检测模型，采用无控制中心的多 Agent 结构，每个检测部件都是独立的自治 Agent。系统中共有3类 Agent：入侵检测 Agent（IDA），通信服务 Agent（TSA）和状态检查 Agent（SDA）。系统模型框架如图3所示。

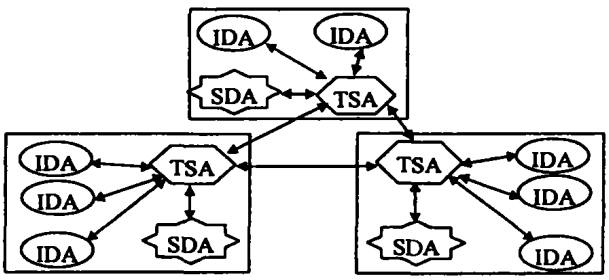

图3 基于 Agent 的分布式入侵检测系统模型框架

TSA 专门用于通信服务，在每台主机上是唯一的，负责主机内和协作主机间的通信；SDA 在每台主机上也唯一，定时检查协作主机 TSA 和本机 IDA 的状态，并向系统管理员报告；IDA 是最基本的检测单元，分布在主机和网络各处，每个 IDA 独立承担一定的检测任务，各 IDA 间通过通信相互协作。不同的 IDA 可能采用不同的检测方法和技术。此外，该模型还采用了一定的状态检查和验证策略，以保证各 Agent 自身的安全和通信安全。

2.5 使用移动代理的分布式入侵检测系统结构

Mell P 等提出了一种能抵抗拒绝服务攻击的入侵检测结构，使 IDS 部件对于攻击者不可见。同时使用移动代理技术，在遭到攻击后，IDS 部件可以重新定位到其他主机上[20]。

对于在 Internet 上可见的主机，无法防止其受 flooding 拒绝服务攻击。但是，象 IDS 等应用程序没有必要在 Internet 上可见，因此可以采取措施来抵御这种攻击。Mell 等提出的结构中，将一个组织的网络元素（如路由器、交换机、防火墙或主机）分成集合，如图4所示。该模型可以定义为：

$Enterprise = \{Domain_1, Domain_2, \cdots, Domain_m\}$；

$Domain = \{Backbone, Region_1, Region_2, \cdots, Region_n\}$，其中 $n \geqslant 0$；

$Backbone = \{CriticalSet, ProxySet\}$；

$Region = \{ChildSet\}$.

所有集合的超集称为企业（Enterprise），由一些域（Domain）组成。域是网络中最大的分区，其中主干（Backbone）中的每个元素与其中任何其他元素间都有一个高带宽的连接，该连接不通过任何公共网络。每个域同企业总线（Enterprise Bus）有一个物理的网络连接，企业总线可能包含 Internet 的某些部分或其他公共网络，所有域都可以通过企业总线来通信。假设所有域通过企业总线的通信都是加密的，而且已通过地址翻译防火墙和链路加密，或通过使用虚拟专网将源和目的 IP 地址隐藏起来。每个域包含一个主干和0或多个区（Region）。主干是一些防止网络渗透攻击的网络元素的集合：防火墙、路由器和交换机等。假设主干中的元素可以抵抗渗透攻击，但不能抵抗拒绝服务攻击。主干中的元素与企业总线间有一个直接的物理连接。假设区易受渗透和拒绝服务攻击，它只与其所在域中的主干有物理的网络连接，区之间、区与其他域以及与企业总线间都无直接物理的网络连接。每个域包含3种类型的专用主机：关键（Critical）主机、代理（Proxy）主机和子（Child）主机。相应地有3种移动代理：关键（Critical）代理、代理（Proxy）代理和子（Child）代理，分布在相应的主机上。移动代理可以在其各自的集合中的主机间自由移动，但是除了从代理集向区移动外，不能在集合间移动。

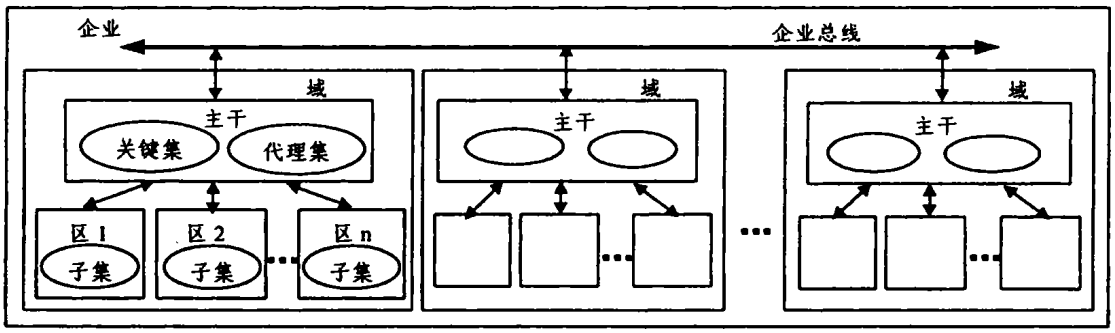

图4 Mell 模型结构（↔：物理网络连接 ▭：网络分区）

每个关键代理都有一个或多个备份代理，分别驻留在同一个域的不同的关键主机上，维护原代理的全部或部分状态信息。当一个关键主机被攻击者冻结或关闭时，该主机上代理的备份代理互相联系，选出一个作为被冻结或关闭的代理的后继，恢复其功能。未使用的备份代理终止或作为后继的备份。后继可能要产生备份并送往不同的关键主机。原来的代理如果被冻结，则检查系统时间，若超时则终止自身。如果中断时间很短，则与其备份联系，看是否已有后继，如有后继则原代理终止；否则恢复前面的工作。为保证系统安全，该模型中还使用了公钥认证体制。

Bernardes 等也提出了一种基于移动代理的 IDS 的实现[21]，通过使移动代理经常地在内部信息通道中移动来防止来自内部和外部的攻击。

2.6 分析与评价

AAFID 和基于攻击策略分析的分布式入侵检测系统都是采用了分层结构，由一个控制中心来控制整个系统的工作。很多分层的分布式 IDS 结构都存在一个共同的弱点，即单点失效的问题。攻击者如果能破坏一个关键结点，则网络 IDS 的很大一部分都无法操作，攻击者就可以毫无顾忌地进行入侵。由于目前对于象 flooding 这样的拒绝服务攻击尚无有效的防御措施，因此攻击者可以通过拒绝服务攻击来使重要的 IDS 部件失效。此外，大量的检测数据传输到上层的分析部件，会增加系统开销，影响系统性能。针对这些问题，存在两种较好的解决方法：一种是采用非集中式的无层次的分布式系统结构，如文[19]；另一种是使用移动的可恢复部件，即使用移动代理技术，使重要的 IDS 部件在系统中迁移，以避开入侵者的攻击，如文[20]和文[21]。然而，实践证明设计和建立一个非集中式的 IDS 非常困难，目前该领域的研究十分活跃。使用移动代理的分布式 IDS 也并非尽善尽美，系统中仍存在着一些弱点，如文[20]中提出的系统，攻击者可以通过隔离域、切断关键主机与子主机之间的连接和对子主机的渗透等方法来破坏该系统。

3 通用入侵检测框架 CIDF

通用入侵检测框架（Common Intrusion Detection Framework，CIDF）是在 DARPA（Defense Advanced Research Projects Agency）领导下开发的一种通用的语言、协议和 API，允许异构 ID 部件互操作和共享信息[22]。CIDF 结构将一个 IDS 分成许多个有固定标识的部件，这些部件主要由软件代码及一些配置信息组成（数据库部件除外，它存储大量的数据），部件间通过通用入侵检测对象（Generalized intrusion detection object，GIDO）交换数据。这些部件通过一个分层结构进行通信。共有三层：GIDO 层、消息层和协商传输层。CIDF 结构定义了四种部件：事件产生器（“E 盒”）、事件分析器（“A 盒”）、事件数据库（“D 盒”）和响应部件（“R 盒”）。事件产生器从 IDS 外部的环境中获得事件信息，并以 GIDO 的格式发送给系统中的其他部分。事件分析器从其他部件接收 GIDO，进行分析，再返回新的 GIDO。事件数据库存储 GIDO 并接受查询。响应部件根据从其他部件收到的 GIDO 的指示，执行某种动作。GIDO 以一种标准的通用格式来表示，该格式由通用入

侵描述语言 CISL 定义。一个 GIDO 包括两部分：一个固定格式的头部和一个可变长的体。头部包括正使用的 CIDF 的版本信息、时间戳和体的长度等信息，如图5所示。GIDO 的逻辑格式为类似于 Lisp 表达式的 S-表达式结构。表达式的解析树用圆括号来分组。GIDO 体中包含实际数据（用单引号括起来）和语义标识符 SID。ASCII 格式的表达式效率不高，为节省空间，CISL 定义了一种编码，以字节序列来表示 GIDO 的逻辑结构中的信息。CIDF 部件交换 GIDO 时，实际是以这种编码格式进行的。

版本 ID (2字节)	类 ID (2字节)	长度 (4字节)	时间戳 (4字节)	线程 ID (4字节)	源 ID (16字节)	标志 (1字节)

图5 GIDO 头部格式

由 DARPA 支持的项目 IDIAN 采用 CIDF 结构，开发了一个谈判协议来允许分布式异构 ID 部件互操作并就彼此的 ID 信息处理能力和需要达成协议[23]。Ning P 等提出了一个协作 IDS 间的请求模型框架[24]，使用 CIDF 中的形式化方法，扩展 CIDF 部件以包含一个查询功能。目前，CIDF 小组仍在不断对其语言和协议等进行改进，CIDF 有可能成为一种标准。

结束语 本文分析和概括了几种有代表性的基于代理的分布式入侵检测系统、通用入侵检测框架结构及其应用和扩展。然而，目前的分布式入侵检测技术还不够成熟，还存在一些问题。例如，各 ID 部件可能会争用系统资源，如何有效地分配系统资源，提高系统效率是分布式入侵检测系统中要解决的一个实际问题。此外，随着新入侵方法的不断出现，IDS 将是入侵活动的一个重要目标，因而其自身的安全问题是当前研究的一个重要课题。CIDF 对异构 IDS 的通信进行了有益的探索，但 IDS 之间的信息交换与共享机制尚未形成一个统一的标准。许多技术还停留在理论研究和实验阶段，未达到实用化的程度，等等。这些问题都需要进一步的研究解决。

参 考 文 献

1 蒋建春，马恒太，任党恩，等. 网络安全入侵检测：研究综述. 软件学报，2000，11(11)：1460～1466

2 Debar H, Dacier M, Wespi A. Towards a taxonomy of intrusion-detection systems. Computer Networks, 1999, 31(8): 805～822

3 Ilgun K, Kemmerer R A, Porras P A. State transition analysis: a rule-based intrusion detection approach. IEEE Transactions on Software Engineering, 1995, 21(3): 181～199

4 Ko C, Ruschitzka M, Levitt K. Execution monitoring of security-critical programs in distributed systems: A specification-based approach. In: IEEE. PROC IEEE COMPUT SOC SYMP RES SECUR PRIVACY. PISCATAWAY, NJ, (USA), 1997. 175～187

5 Hofmeyr S, Forrest S, Somayaji A. Intrusion detection using sequences of system calls. Journal of Computer Security, 1998, 6 (3): 151～180

6 Lindqvist U, Porras P A. Detecting computer and network misuse through the production-based expert system toolset (P-BEST). In: Proc. of the IEEE Computer Society Symposium on Research in Security and Privacy. 1999. 146～161

7 Debar H, Becker M, Siboni D. A neural network component for an intrusion detection system. In: IEEE. PROC SYMP SECUR PRIVACY. PISCATAWAY, NJ (USA): IEEE SERVICE CENTER, 1992. 240～250

8 Mukherjee B, Heberlein L, Levitt K N. Network intrusion detection. IEEE Network, 1994, 8(3): 26～41

9 Qu D, Vetter B, Wang F, et al. Statistical anomaly detection for link-state routing protocols. In: INT CONF NETWORK PROTOC. LOS ALAMITOS, CA, (USA): IEEE COMP SOC, 1998. 62～70

10 Lee W, Stolfo S, Mok K W. Data mining framework for building intrusion detection models. In: Proc. of the IEEE Computer Society Symposium on Research in Security and Privacy. 1999. 120～132

11 Paxson V. Bro: A system for detecting network intruders in real-time. Comput. Networks, 1999, 31(23): 2435～2463

12 Manganaris S, Christensen M, Zerkle D, et al. Data mining analysis of RTID alarms. Computer Networks, 2000, 34(4): 571～577

13 Yau S, Zhang X. Computer network intrusion detection, assessment and prevention based on security dependency relation. In: Proc IEEE Comput Soc Int Comput Software Appl Conf. 1999. 86～91

14 Cabrera J, Ravichandran B, Mehra R K. Statistical Traffic Modeling for network intrusion detection. In: IEEE. IEEE INT WORKSHOP MODEL ANAL SIMUL COMPUT TELECOMMUN SYST PR. PISCATAWAY, NJ, (USA), 2000. 466～473

15 Lippmann R, Haines J W, Fried D J, et al. 1999 DARPA off-line intrusion detection evaluation. Computer Networks, 2000, 34 (4): 579～595

16 Raibulet C, Demartini C. Mobile agent technology for the management of distributed systems — a case study. Computer Networks, 2000, 34(6): 823～830

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

18 Huang M, Jasper R, Wicks T. Large scale distributed intrusion detection framework based on attack strategy analysis. Computer Networks, 1999, 31(23): 2465～2475

19 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. 软件学报，2000，11(10)：1312～1319

20 Mell P, Marks D, McLarnon M. Denial-of-service resistant intrusion detection architecture. Computer Networks, 2000, 34 (4): 641～658

21 Bernardes M C, dos Santos Moreira E. Implementation of an intrusion detection system based on mobile agents. In: IEEE. INT WORKSHOP SOFTWARE ENG PARALL DISTRIB SYST PROC. PISCATAWAY, NJ, (USA), 2000. 158～164

22 http://www.isi.edu/gost/cidf/, 1999

23 Feiertag R, Rho S, Benzinger L, et al. Intrusion detection inter-component adaptive negotiation. Computer Networks, 2000, 34 (4): 605～621

24 Ning P, Wang X, Jajodia S. Modeling requests among cooperating intrusion detection systems. Computer Communications, 2000, 23(17): 1702～1715