网络入侵检测系统研究综述及发展趋势

The Overview and Trend of Network Intrusion Detection System Research

朱敏 厉晓华（杭州浙江大学校园网络中心 310027）

摘 要：本文介绍了入侵检测技术的工作原理、功能结构、攻击检测方法，并总结了入侵检测技术的研究现状及面临的一些挑战，最后给出了入侵检测系统的发展趋势及主要研究方向。

关键词：入侵检测 入侵检测系统 入侵模式

1 入侵检测系统的原理

入侵检测（Intrusion Detection），顾名思义，便是对入侵行为的发觉。它通过对计算机网络或计算机系统中的若干个关键点进行信息收集并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的痕迹。进行入侵检测的软件与硬件的组合便是入侵检测系统（Intrusion Detection System，简称IDS）。与其他安全产品不同的是，入侵检测系统需要更多的智能化，它必须可以将得到的数据进行分析，并得出有用的结果。一个有效的入侵检测系统能大大的简化管理员的工作，保证网络安全的运行。

入侵检测可分为实时入侵和事后入侵检测两种。

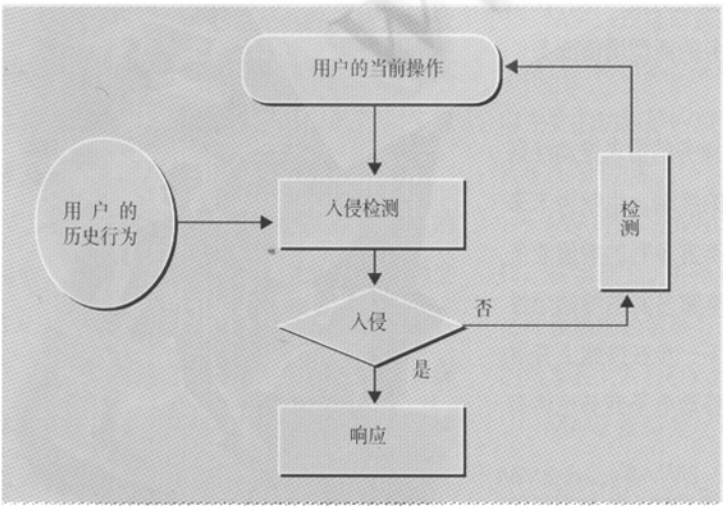

图 1 入侵检测系统的功能原理

实时入侵检测是在网络连接过程中进行的，系统根据用户的历史行为模型、存储在计算机中的专家知识以及神经网络模型对用户当前的操作来完成对入侵的检测，一旦发现入侵迹象立即断开入侵者与主机的连接，并收集证据和实施数据恢复。这个检测过程是不断循环进行的。而事后入侵检测有网络管理人员进行，他们具有网络安全的专业知识，根据计算机系统对用户操作所做的历史审计记录来判断是否有入侵行为，如果有就断开连接，并记录入侵证据和进行数据恢复。事后入侵检测是管理员定期或不定期进行的，不具有实时性，因此防御入侵的能力不如实时入侵检测系统。入侵检测系统的功能原理如图1所示。

2 入侵检测系统的功能和结构

入侵检测系统的功能有：

（1）监视并分析用户和系统活动，查找非法用户和合法用户的越权操作。

（2）检查系统配置的正确性和安全漏洞，并提示管理条例修补漏洞。

（3）对异常行为模式进行统计分析，发现入侵行为的规律。

（4）评估系统关键资源和数据文件的完整性。

（5）能够实时对检测到的入侵行为进行响应。

（6）操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

根据以上入侵检测系统的功能，可以把它的功能结构分为两大部

分：中心检测平台和代理服务器。代理服务器是负责从各个操作系统中采集审计数据，并把审计数据转换成平台无关的格式后传送到中心检测平台，或把中心平台的审计数据要求传送到各个操作系统中。而中心检测平台由专家系统、知识库和管理员组成，其功能是根据代理服务器采集来的审计数据进行专家系统分析，产生系统安全报告。管理员可以向各个主机提供安全管理功能，根据专家系统的分析向各个代理服务器发出审计数据的需求。另外，在中心检测平台和代理服务器之间是通过安全的RPC进行通信。

3 入侵检测方法的类型

3.1 特征检测(Signature-based detection)

特征检测，又称Misuse detection，这一检测假设入侵者的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。对已知的攻击或入侵的方式作出确定性的描述，形成相应的事件模式。当被审计的事件和已知的入侵事件模式相匹配时，即报警。

原理上与专家系统相仿。其检测方法上与计算机病毒的检测方式类似。目前基于对包特征描述的模式匹配应用较为广泛。该模型的结构如图2所示。

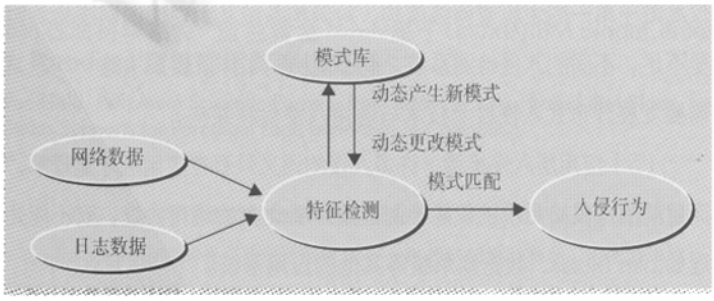

图 2　特征检测模型

特征检测型IDS的优点：能够十分有效准确地检测已知的入侵行为，而不会产生惊人的误警信息，但对于无经验知识的入侵与攻击行为无能为力。特征检测的难点在于如何设计模式既能够表达“入侵”现象又不会将正常的活动包含进来。

目前，基于特征检测系统主要采用了专家系统、模式识别等人工智能技术。

3.2 异常检测(Anomaly detection)

基于异常检测技术则是先定义一组系统“正常”情况的阈值及系统内部配置的知识库中储着网络系统、操作系统、应用系统的弱点和攻击模式，进行异常行为统计。例如，检查CPU利用率、内存利用率、磁盘空间是否一下子缩小、用户登录失败次数增加、文件校验和等等（这类数据可以人为定义，也可以通过观察系统、并用统计的办法得出），然后将系统运行时的数值与所定义的“正常”情况、知识库进行比较，得出是否有被攻击的迹象。该模型的结构如图3所示。

异常检测型IDS的优点：在没有详细特定的情况下，可以检测出攻击发生的症状，不必了解异常行为背后的黑幕就能判断出发生了入侵，所谓不见其人已闻其声。但容易造成漏报。异常检测的难点在于如何定义所谓的“正常” 情况及知识库维护和更新。

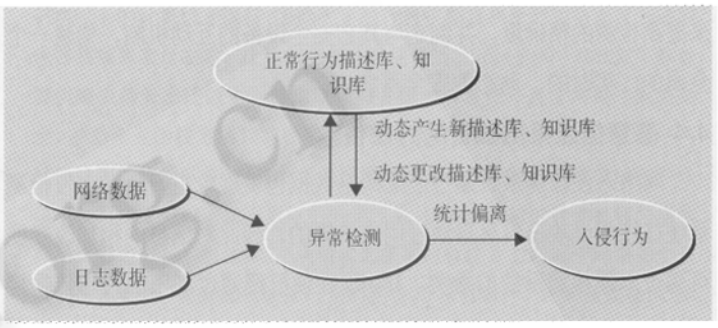

图 3　异常检测模型

目前，基于异常检测系统主要采用了统计、神经网络等技术。

4 入侵检测系统面临的主要挑战

与防火墙技术相比，入侵检测系统还存在着许多问题，主要应从下述几个方面改进。

4.1 提高入侵检测系统的检测速度，以适应网络通信的要求

网络安全设备的处理速度一直是影响网络性能的一大瓶颈。入侵检测系统通常以并联方式接入网络，如果其检测速度跟不上网络数据的传输速度，那么检测系统就会漏掉其中的部分数据包，从而导致漏报而影响系统的准确性和有效性。在入侵检测系统中，截获网络的每一个数据包，并分析、匹配其中是否具有某种攻击的特征需要花费大量的时间和系统资源，因此大部分现有的入侵检测系统只有几十兆的检测速度，随着百兆、甚至千兆网络的大量应用，入侵检测系统技术发展的速度已经远远落后于网络速度的发展。

4.2 减少入侵检测系统的漏报和误报，提高其安全性和准确度

基于模式匹配分析方法的入侵检测系统，检测主要判别网络中搜集到的数据特征是否在入侵模式库中出现。因此，面对着每天都有新的攻击方法产生和新漏洞发布，攻击特征库不能及时更新是造成入侵检测系统漏报的一大原因。而基于异常发现的入侵检测系统，则通过流量统计分析建立系统正常行为的轨迹，当系统运行时的数值超过正常阈值，则认为可能受到攻击，这种技术本身就导致了其漏报和误报率较高。另外，大多数的入侵检测系统是基于单包检查的，协议分析得不够，因此，无法识别伪装或变形的网络攻击，也造成大量漏报和误报。

4.3 提高入侵检测系统的互动性能和安全性能

在大型网络中，网络的不同部分可能使用了多种入侵检测系统，甚至还有防火墙、漏洞扫描等其它类别的安全设备，这些入侵检测系统之间以及入侵检测系统和其它安全组件之间，如何交换信息，共同协作来发现攻击，作出响应并阻止攻击是关系整个系统安全性的重要因素。

因此，厂商应从多个方面来提高入侵检测系统的技术水平和性能。在建立入侵检测标准和接口的同时，可利用多点分析和关联技术来提高检测的精确度，并制定与其它安全设备的互动机制，构建一个全面的、实时的、动态的安全系统。

4.4 恶意信息采用加密的方法传输

网络入侵检测系统通过匹配网络数据包发现攻击行为，入侵检测系统往往假设攻击信息是通过明文传输的，因此对信息的稍加改变便可骗过入侵检测系统的检测。TFN现在便已经通过加密的方法传输控制信息。还有许多系统通过VPN（虚拟专用网）进行网络之间的互联，如果入侵检测系统不了解其所用的隧道机制，则会出现大量的漏报和误报。

4.5 必须协调、适应多样性的环境中的不同的安全策略

网络及其中的设备越来越多样化，即存在关键资源如邮件服务器、企业数据库，也存在众多相对不是很重要的PC机。不同企业之间的这种情况也往往不尽相同。入侵检测系统要能有所定制以更适应多样的环境要求。

4.6 不断增大的网络流量

用户往往要求入侵检测系统尽可能快的报警，因此，需要对获得的数据进行实时的分析，这导致对所在系统的要求越来越高，商业产品一般都建议采用当前最好的硬件环境（如NFR5.0要求主频最少700以上的机器）。尽管如此，但对百兆以上的流量，单一的入侵检测系统仍很难应付。可以想见，随着网络流量的进一步加大（许多大型ICP目前都有数百兆的带宽），对入侵检测系统将提出更大的挑战，在PC机上运行纯软件系统的方式需要突破。

5 入侵检测技术的发展趋势

目前国内外一些研究机构已经开发出了应用于不同操作系统的几种典型的入侵检测系统（IDS），它们通常采用静态异常模型和规则的误用模型来检测侵入。而这些入侵检测系统的检测基本上是基于主机或基于网络的。基于主机的入侵检测系统采用服务器操作系统的检测序列作为主要输入源来检测侵入行为，而大多数基于网络的入侵检测系统则以监控网络故障作为检测机制，但有些则用基于服务器的检测模式和典型的入侵检测系统静态异常算法。早期的入侵检测系统模型设计用来监控单一服务器，是基于主机的入侵检测系统；然而近期的更多模型则集中用于监控通过网络互连的多服务器，是基于网络的入侵检测系统。目前已有的入侵检测系统已经远远不能满足入侵检测的需要，今后的入侵检测技术主要朝以下几个方面发展：

（1）分布式入侵检测：第一层含义，针对分布式网络攻击的检测方法；第二层含义，使用分布式的方法来实现分布式的攻击，其中的关键技术为检测信息的协同处理与入侵攻击的全局信息的提取。

（2）智能化入侵检测：使用智能化的方法与手段来进行入侵检测。所谓的智能化方法，现阶段常用的有神经网络、遗传算法、模糊技术、免疫原理等方法，这些方法常用于入侵特征的辨识与泛化。利用专家系统的思想来构建入侵检测系统也是常用的方法之一。特别是具有自学习与自适应能力的专家系统，实现知识库的不断升级与扩展，使设计的入侵检测系统防范能力不断增强，具有更广泛的应用前景。应用智能体的概念来进行入侵检测的尝试也有报道。较为一致的解决方案应为高效常规意义下的入侵检测系统与具有智能检测功能的检测软件或模块相结合的使用。

（3）全面的安全防御方案：使用安全工程风险管理的思想与方法来处理网络的安全问题，将网络安全做为一个整体工程来处理。从管理，网络结构，加密通道，防火墙，病毒防护，入侵检测多方位全面对所关注的网络作全面的评估，然后提出可行的全面解决方案。

（4）分布式入侵检测与通用入侵检测架构：传统的入侵检测系统仅局限于单一的主机或网络架构，对异构系统及大规模的网络检测明显不足，不同的入侵检测系统之间不能协同工作。要解决这一问题，需要发展分布式入侵检测技术与通用入侵检测架构。

（5）应用层入侵检测：许多入侵的语义只有在应用层才能理解，而目前的入侵检测系统仅能检测诸如Web之类的通用协议，而不能处理如Lotus Notes、数据库系统等其他的应用系统。

（6）入侵检测的评测方法：用户需对众多的入侵检测系统进行评价，评价指标包括入侵检测系统检测范围、系统资源占用和入侵检测系统自身的可靠性。从而设计通用的入侵检测测试与评估方法的平台，实现对多种入侵检测系统的检测已成为当前入侵检测系统的另一重要研究与发展领域。

（7）入侵主体对象的间接化，即实施入侵与攻击主体的隐蔽化：通过一定的技术，可掩盖攻击主题的源地址及主机位置。即使用了隐蔽技术后，对于被攻击对象攻击的主题是无法直接确定的。

（8）入侵或攻击技术的分布化：以往常用的入侵和攻击行为往往是由单击执行。由于防范技术的发展使得此类行为不能奏效。所谓分布式拒绝服务（DDOS）在很短的时间内可以造成被攻击主机的瘫痪。而且此类分布式攻击的单机信息模式与正常的通信无差异，所以，往往在攻击发动的初期不易被确认，分布式攻击是近期最常用的攻击手段。

下转第70页 >>

上接第78页

（9）攻击对象的转移：入侵和攻击常以网络为侵犯的主体，但近来的攻击行为却发生了策略性的改变，由攻击网络改为攻击网络的防护系统，且有愈演愈烈的形势。现在已经有了专门针对入侵检测系统作攻击的报道。攻击者详细的分析了入侵检测系统的审计方式、特征描述、通信模式及找出入侵检测系统的弱点，然后加以攻击。

（10）基于大规模的信息采集和网络攻击预警技术的研究问题等。

（11）与其他网络安全技术相结合：如结合防火墙、PKIX、具有人工智能特性的自适应访问控制技术、多重身份认证技术、安全电子交易SET等新的网络安全与电子商务技术，提供完整的网络安全保障。

6 结束语

未来的入侵检测系统将会结合其他的网络管理软件，形成入侵检测、网络管理、网络监控三位一体的工具。强大的入侵检测软件的出现极大的方便了网络的管理，其实时报警又为网络安全增加了一道保障。尽管在技术上仍有许多有待研究的问题，但正如攻击技术不断发展一样，入侵检测系统也会不断地更新、成熟和发展。