· 1999信息安全国际会议论文 · 文章编号：1000－3428(1999)特刊－0056－03 中图分类号：TP309；TP393.4

一个基于神经网络的入侵检测系统

汪立东，李亚平，方滨兴，贺龙涛，薛 园
(哈尔滨工业大学计算机科学系，哈尔滨 150001)

摘 要：当前的入侵检测技术主要有基于规则的误用检测和基于统计的异常检测。提出了一个多Agent入侵检测系统原型。在进行用户异常检测的同时，基于多数入侵者都是以已经确定的模式实施攻击这一事实，加入了网络入侵检测和特权程序执行追踪功能。可以利用多Agent的自治和合作来提高检测结果的准确性。各Agent用神经网络构造，可以利用其学习、快速识别和对噪音数据的处理能力，同时使系统具有更好的适应性。为了解决神经网络处理时间系列输入引起的拓扑和训练的复杂性，引入了事件滑窗来为神经网络提供输入，从而使用简单的前馈网络和BP算法即可获得较好的检测效果。

关键词：安全；入侵检测；入侵检测系统；神经网络

A Neural Network-based Intrusion Detection System

Wang Lidong, Li Yaping, Fang Binxing, He Longtao, Xue Yuan
(Dept.of Computer Science, Institute of Technology, Harbin 150001)

【Abstract】The current intrusion detection techniques mainly include rule-based misuse detection and statistics-based anomal detection. This paper proposed an IDS with multiple agents. Based on the fact that most intruders act in a determined pattern, our system prototype combines the functions of network detection and privileged program execution trace besides user anomal detection. The autonomy and co-operation of the agents help improve the accuracy of detection results. All agents are constructed with neural networks. Not only can its capabilities of learning, quick classification and processing of noisy data be used in intrusion detection, the system is also highly adaptive. In order to overcome the deficiency of series processing of neural networks, the event sliding-window is introduced for data input of neural networks. Better performance can be gained by only adopting simple feed-forward networks and BP algorithm.

【Key words】Security; Intrusion detection; Intrusion detection system; Neural network

当前的安全技术主要分为防范技术和检测技术。安全防范技术期望通过严格的认证和访问控制机制来建立一个完全安全的系统。然而完全安全的系统在实际上是不可能存在的，如软件或操作系统中不可避免存在bug、加密方法及构筑在其上的口令系统可能被攻破、内部用户可能滥用特权、系统易用性或性能因此受到显著影响、网络协议可能存在缺陷等。

虽然当前已开发出许多安全技术，而入侵事件仍是层出不穷。入侵检测作为安全的最后屏障，可以在一定程度上预防和检测来自系统内外部的入侵。虽然人们早就认识到ID技术的重要性，但直到80年代后期，它主要还是靠人工完成，如1988年Internet蠕虫事件就主要是靠手工检测的。攻击者的创造力及操作系统和网络通信的复杂性使得对入侵进行有效的识别很困难。在基于主机进行ID已显得很复杂的同时，Internet及电子商务的盛行和机密信息日益频繁地传输，也增加了对高效入侵检测系统的需求。对自动IDS的研究和开发已近10年，但高效ID技术的研究和IDS的开发仍具有相当大的难度[1,2]。

1 入侵检测方法

对不同的安全策略，入侵和入侵检测有不同的定义：

定义1 入侵是任何试图破坏计算机和网络系统的安全性(包括完整性、机密性和可用性)的行为。入侵检测即识别出----最好是实时----对计算机及网络系统的非法的和未授权的使用、误用和滥用。

IDS基于用户和系统的习惯及已知的入侵场景等来识别入侵活动，如不正常高的失败登录请求率可能意味外部渗透；与正常用户行为显著偏离可能意味冒充。对ID最有用的是审计数据，它记录了系统中一系列事件及其属性。由于入侵模式多、事件种类繁杂、审计数据量大等原因，单靠手工来分析入侵事件不仅要求对审计追踪技术具有足够的知识和经验，且往往在浪费了大量精力后也很难获得有价值的信息。故设计和开发可自动高效处理审计数据并发现入侵的IDS成为保障系统和网络安全运行的关键之一。

总体上说，ID可分为异常检测(Anomaly Detection)和误用检测(Misuse Detection)。

异常检测基于统计方法，使用系统或用户的活动轮廓(Activity Profile)来检测入侵活动。活动轮廓由一组统计参数组成，通常包括CPU和I/O利用率、文件访问、出错率、网络连接等。这类IDS先产生主体的活动轮廓，系统运行时，异常检测程序产生当前活动轮廓并同原始轮廓比较，同时更新原始轮廓，当发生显著偏离时即认为是入侵。此类IDS的优点是可动态学习用户的使用习惯，可检测冒充及未知攻击。其缺点有：需为每个主体建立轮廓；难以选择一组合适的统计参数；由于基于统计而忽略了事件间的顺序关系等。误用检测基于一组规则和专家系统，将当前已知的入侵行为和检测步骤编码为一组规则，在检测中采用专家系统来将这些规则匹配到审计数据，从而发现入侵活动序列。其优

作者简介：汪立东（1970～），男，博士生，主要研究方向：网络安全

收稿日期：1999－08－01

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

点是可以检测到专家已知的攻击；缺点是仅能检测已知攻击，安全度相当于人工专家。

当前的IDS主要基于上述技术构造，如NIDES、Haystack、NADIR，有些具有较好的性能。其它研究有基于图(GrIDS)的和基于状态转换分析(如USTAT)的IDS。

2 基于神经网络的多Agent入侵检测系统

2.1 神经网络用于ID

为研制具有学习和适应能力的IDS，人们开始研究在ID中应用神经网络和遗传编程(Genetic Programming)技术，但目前这些工作仍是有限的，并无成型的系统。神经网络有能力来解决当前ID方法所遇到的许多问题，它可作为异常检测中统计方法的替代品。本文基于多数入侵者是利用已确定的模式实施入侵这一事实，提出了一个多Agent IDS，结合了网络检测、用户异常检测和特权程序系统调用追踪功能。每个Agent都采用神经网络构造，在完成训练后可以获得较好的检测性能。各Agent的协作提高了ID的准确率，降低了误报率和漏报率；同时各Agent又是自治的，可被动态地加入或移出IDS。基于神经网络的IDS的优点是：具有学习和识别未曾见过的入侵的能力；对噪音和不完全数据的处理很好；以非线性方式进行分析的能力，处理速度快，适应性好[3]。

由于神经网络在处理时间系列事件上的缺陷，使其在ID中的应用受到了限制。有人对前馈网络进行了一些改进以将其用于ID，但网络拓扑和训练算法却因此变得复杂。这里引入了事件滑窗来为神经网络提供输入，不仅使得采用简单的前馈网络即可解决问题，同时克服了神经网络对序列事件处理的弱点和复杂性。

定义2 一个事件是某个粒度级上的一个与安全相关的动作。如一个用户命令、一个网络数据包信息、一个系统调用等。

定义3 设事件系列为$E_1, E_2, \ldots, E_i, \ldots, E_n, E_{n+1}, \ldots, E_{n+i}, \ldots$，事件滑窗是一个定长的先进先出的队列，队列中的每个元素是一个结构，对应一个事件，滑窗随时间步对事件系列执行队列操作。滑窗每个时间步可滑过k个事件，其中k与特征事件采样频率有关。如设滑窗长度为n，k为1，若时间步n时滑窗对应的事件系列为$E_1, E_2, \ldots, E_n$，至时间步n+i时对应的事件滑窗为$E_i, \ldots, E_n, E_{n+1}, \ldots, E_{n+i}$。

2.2 系统模型

系统模型由3类Agent构成：NetworkDetector、UserDetector和ProgDetector。每类可包含若干个Agent。NetworkDetector是网络检测类，用于SYN和ICMP洪泛、扫描和网络跳跃等检测；UserDetector用于用户异常检测；ProgDetector用于特权程序执行踪迹检测。所有Agent向Manager告警，由Manager处理后再向管理员告警。各Agent均用神经网络构造，在拓扑上是同构的，但其连接权值由于训练数据的不同而不同。如图1所示。

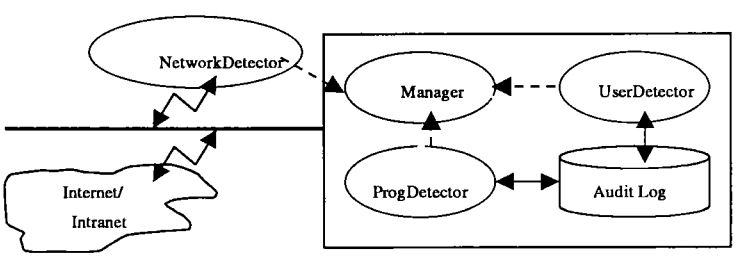

图1 基于神经网络的多Agent IDS

2.3 用户异常检测

传统的异常检测基于统计方法进行。活动轮廓由一组统计参数组成，Denning D E提出了一组参考轮廓[4]。可以采用的统计参数包括登录频度、口令失败次数、会话时间、CPU利用量、IO利用量、命令或程序执行频度、拒绝执行次数、使用敏感程序(如cc、gcc编译程序、口令破解程序、发掘系统已知弱点的程序等)比率、文件访问(读/写/执行)频率、文件访问失败次数、访问敏感文件(如/etc下的一些文件、审计信息文件等)数等。

用神经网络检测用户异常行为的一种简单神经网络模型如图2所示，它采用一个前馈的多层感知器(MLP)。输入层是活动轮廓的数量化的值，隐含层结点均采用S转换函数(1/(1 + exp (-x)))；两个输出结点，输出0.0, 1.0时表发生显著异常事件，1.0, 0.0表正常事件；采用BP算法。训练用的数据通过对各种审计数据(如/var/log下的文件、Sun和Solaris的BSM产生的审计信息等)加工后得到。当网络训练完成后，即可投入运行。

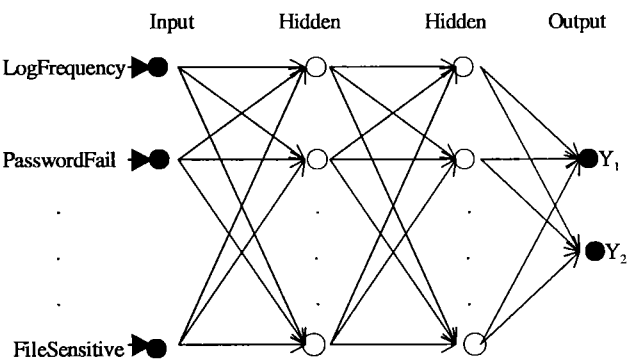

图2 用于用户异常检测的神经网络模型

上述模型仍用到了许多统计信息，而通过用户活动来跟踪学习用户习惯的IDS则具有更好的适应性。我们构造了一个基于事件序列来学习用户习惯的神经网络。若将事件定义在命令级则显得太粗，所以将事件定义在系统调用级，其相关属性包括时间戳、进程号、真实和有效用户号、真实和有效组号、当前目录、家目录、访问的文件名、命令参数、返回值等。为了克服神经网络对系列事件处理的弱点，引入了事件滑窗来为神经网络提供输入，每次输入n个事件对应的审计信息，这n个事件的信息相当于通过一个虚输入层后转换为一个向量作为网络的输入。通过使事件滑窗随时间步(每步可能滑过k个事件，k值同事件采样频率有关)移动，达到采用简单的前馈网络(如MLP)即可处理系列事件的效果。将事件(系统调用)各个特征域转化为数量值作为神经网络的输入；隐含层的层数和各层的结点数用神经网络模拟软件通过训练确定，其所有结点均采用S转换函数(1/(1 + exp (-x)))；输出层输出0.0, 1.0时表发生显著异常事件，1.0, 0.0表正常事件；在训练时误差控制采用后向传播BP(Back-propagation)算法。如图3所示。

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

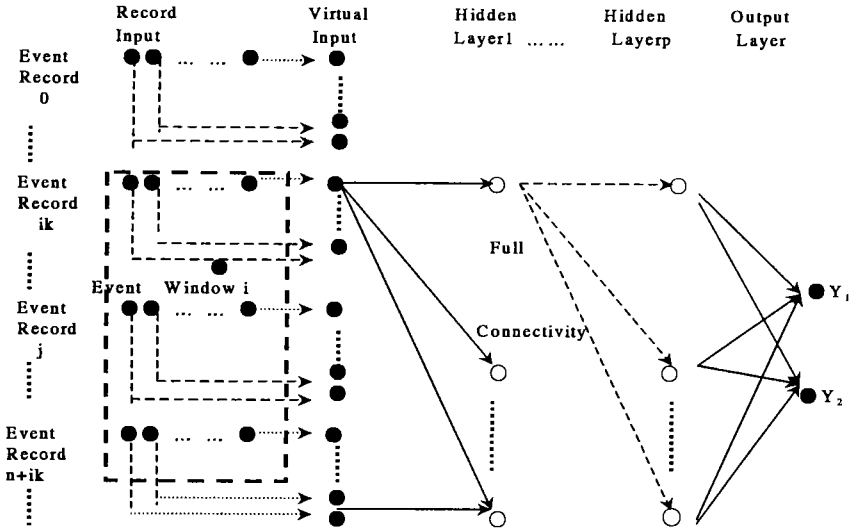

图3 基于神经网络的用户异常检测2

2.4 基于网络的检测

Internet和Intranet应用的扩展使人们更关心自己的系统和网络是否受到了未授权访问，基于网络进行ID不仅可以更早地发现一些入侵行为，同时它基于整个网络收集和分析数据，因而对具体系统和应用环境是独立的。通过对网络数据流的分析，可以得到一些统计数据，以此来进行ID。当前基于网络的较好的IDS有RealSecure等，主要是基于统计信息和一些规则来构造。Cannady等曾构造了一个由SOM(Self-Organized Map)和MLP(Multiple Layer Perceptron)组成的混合网络用于网络检测[3]。我们采用网络事件序列来进行ID，利用滑窗为神经网络提供输入。

网络检测其训练和输入数据可用tcpdump等得到，提取每个包的包头中的信息作为神经网络的输入。每个输入记录包括源地址、目的地址、端口号、标识位(SYN、FIN、RST等)、序列数、ACK序列数及其它相关选项。针对不同的检测目的可以从这些特征属性中选择若干个。所用的网络拓扑同图3，但隐含层数及各层结点数需要根据具体应用调整。

2.5 基于特权程序执行踪迹的检测

利用特权程序的漏洞是入侵者获取非法访问权限的重要手段之一，Kosoresow和Hofmeyr提出了通过分析特权程序执行过程的方法来监视特权程序的执行[5]。系统调用对检测异常行为是一个很合适的粒度层，所以分析特权程序执行时产生的系统调用序列即可以检测出它是否被合法执行。将这种跟踪方法与神经网络的识别能力结合起来，即可以利用神经网络来检测异常的系统调用序列。网络拓扑、学习算法等仍采用2.3节和图3所示基于事件滑窗输入的前馈网络，只不过其每个记录的属性的数目和意义有所不同。

2.6 一个简单的用户异常检测实验原型

我们设计了一个简单的神经网络原型来测试它对用户误用检测的效果。这个模型的隐含层结点数最终通过用神经网络模拟器训练决定。目前的原型为400-100-16-2(即400个输入结点，2个隐含层分别具有100和16个结点，两个输出结点)，全连接，转换函数L-S-S-S(L表线性，S表Sigmoid转换函数)。初始化权值范围为-1.000～+1.000，学习规则为Generalized Delta，学习率为0.2000，动力因子为0.2000。

训练和测试数据来自Solaris的BSM产生的审计信息，只对单个用户实验，事件个数48800；其中正常事件30000，冒充事件18800。对事件的预处理是取每个事件中的4个域：事件类型、有效与真实用户号之积、网络IP/终端号、返回值。滑窗长度100，故网络的输入结点数为400，这400个数据即形成一个输入向量。滑窗每个时间步滑过50个事件。从这些输入向量中抽取了600个作为输入，其中正常输入与误用输入个数为2：1。训练周期为5000。训练完成时最小均方误差(RMS)为0.2374。用抽取的500个输入向量测试，RMS为0.6602。而通过调整网络隐含层的结点数，训练和测试可以获得更好的效果。

2.7 优缺点

系统模型具有下面一些优点：

- 可扩展性：每个Agent是一个独立的程序，仅完成某个小任务，可被动态加入或移出；
- 鲁棒性：某个Agent发生问题不会影响到其它Agent，且可方便地将其从系统中卸去；
- 结合了网络检测、用户异常检测和特权程序执行踪迹检测，混合型IDS提高了ID结果的准确性，可以降低误报率(false positive)和漏报率(false negative)。
- 各Agent采用神经网络设计，具有较好的适应性，可通过加入新的训练数据并重新训练网络来识别新的入侵；
- 采用事件滑窗提供输入，使得采用简单的前馈网络和BP规则即可获得较好的检测效果。

其缺点是：

- 识别精度依赖于系统的训练数据、训练方法及训练精度；
- 难获得样本数据；
- 在学习阶段可能被入侵者训练。

3 结论

为进一步提高IDS的性能和效率，必须在IDS不断中引入智能、适应和学习能力。由于采用神经网络构造而使得系统具有较好的适应性，只要加入新的训练数据并重新训练网络即可用于识别新的入侵。神经网络技术为改善ID机制提供了一种有效的方法。

参考文献

1 Wilikens M. Workshop Report of RAID 98: First International Workshop on the Recent Advances in Intrusion Detection, 1998-09-28.

2 Newman D, Giorgis T, Issalou F Y. Intrusion Detection System: Suspicious Finds. Data Communications, 1998,27(11):72-82

3 Cannady J, Mahaffey J. The Application of Artificial Neural Networks to Misuse Detection: Initial Results. Proceedings of First International Workshop on the Recent Advances in Intrusion Detection, Louvain-la-Neuve, Belgium,1998-09-14

4 Denning D E. An Intrusion Detection Model. IEEE Transactions on Software Engineering,1987 ,SE13(2): 222-232

5 Kosoresow A P, Hofmeyr S A. Intrusion Detection via System Call Traces. IEEE Software, 1997,14(5):35-42

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net