入侵检测系统中的智能化方法

陈云芳[1,2],王汝传[2]
(1.苏州大学 计算机学院,江苏 苏州 215006;
2.南京邮电大学 计算机学院,江苏 南京 210003)

摘 要:入侵检测系统很好地弥补了访问控制、身份认证等传统机制所不能解决的问题。目前的入侵检测技术正处在第一代技术向下一代技术的过渡时期,未来的入侵检测研究需要融合其他学科和技术领域的知识,充分利用许多成熟的信息智能处理技术。文中讨论和研究了三种典型的智能检测技术,其中对统计学方法、专家系统进行了总体概述,重点阐述数据挖掘技术中的关联规则分析、序列模式分析和数据分类分析的工作原理。

关键词:入侵检测;智能方法;数据挖掘;统计学;专家系统
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2006)06-0132-04

Intelligent Method in Intrusion Detection System

CHEN Yun-fang[1,2], WANG Ru-chuan[2]
(1.School of Computer Sci. and Techn., Soochow University, Suzhou 215006, China;
2.School of Computer Sci. and Techn., Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Intrusion detection system, as a supplement of traditional access control and identity authentication, provides critical protections from potential attempts to exploit computer resource vulnerabilities. Intrusion detection is going to the next generation and will combine methods from other fields, exploiting many mature information technology and artificial intelligence, such as statistics method, expert system, neural network, agent and data mining etc. in the future. In this paper, discuss three kinds of typical intellectual detection technologies. And statistics method, expert system are comparatively briefly introduced. The association rule analysis, sequence patterns analysis and data classification analysis of data mining technology are emphatically illustrated.

Key words: intrusion detection; intelligent method; data mining; statistics; expert system

0 引 言

入侵行为主要是指对系统资源的非授权使用,可以造成系统数据的丢失和破坏、系统拒绝服务等危害[1]。相对于入侵检测而言,网络攻击可以分为4类:

1)检查单个IP包(包括TCP、UDP)首部即可发觉的攻击,如winnuke,ping of death,land.c,部分OS detection,source routing等。

2)检查单个IP包,但同时要检查数据段信息才能发觉的攻击,如利用CGI漏洞、缓存溢出攻击等。

3)通过检测发生频率才能发觉的攻击,如端口扫描,SYN Flood,smurf攻击等。

4)利用分片进行的攻击,如teadrop,nestea,jolt等。

收稿日期:2005-09-19
基金项目:江苏省自然科学基金资助项目(BK2005146);江苏省高技术研究计划(BG2004004);江苏省计算机信息处理技术重点实验室基金(kjs050001)
作者简介:陈云芳(1976-),男,江苏镇江人,博士研究生,研究方向为计算机网络、信息安全、移动代理等;王汝传,教授,博士生导师,研究方向为计算机网络、信息安全、移动代理和虚拟现实技术等。

入侵检测系统的基本功能是信息收集、分析并判断是否为入侵行为。但由于网络中的信息纷繁复杂,因此一个检测过程同时也是一个复杂的信息处理、识别过程。目前的入侵检测技术还存在着漏报率、误报率高,系统的智能性差,预警功能缺乏等普遍问题,因此,入侵检测研究领域需要融合其他学科和技术领域的知识以提供新的入侵检测解决方法。

1 智能检测技术

1.1 基于统计的入侵检测

统计分析是应用最为广泛的一种异常检测技术,它使用统计学方法来学习和检测用户行为。其通常使用按一定时间间隔采样并计算出的一系列参数变量来描述系统或者用户的当前行为,如每个会话进程的登录和退出时间,占用资源的时间长短及其在每个进程中占用的CPU、内存、硬盘等资源的多少等。采样的时间间隔从几分钟到一个月长短不等。在基于统计的入侵检测系统中,通常假设正常的网络操作存在着一定的统计规律。如:在一定的时间内,发向一个特定服务器的SYN数据包应少于一定限度;一个用户的登录访问频率存在着一定的规律。如果

以上测量值超过给定的阈值,即视为可能的入侵行为。

基于统计学方法的一个典型的系统是SRI International的NIDES(Next－generation Intrusion Detection Expert System)[2]。SRI的第一代入侵检测系统模型为IDES,是一个具有双重分析的实时入侵检测系统。NIDES是在该系统基础上发展起来的第二代模型,它不仅包含了异常检测的模块,也包含了基于专家系统的误用检测模块。基于专家系统的入侵检测系统将在下一节中介绍。

NIDES使用Agent完成数据提取和格式化功能,并提交给分析模块。统计分析组件通过学习用户的行为,完成基于异常的入侵检测功能。检测到的信息被Resolver过滤后,由Archiver组件存储或使用用户界面查看。NIDES的总体检测流程如图1所示。

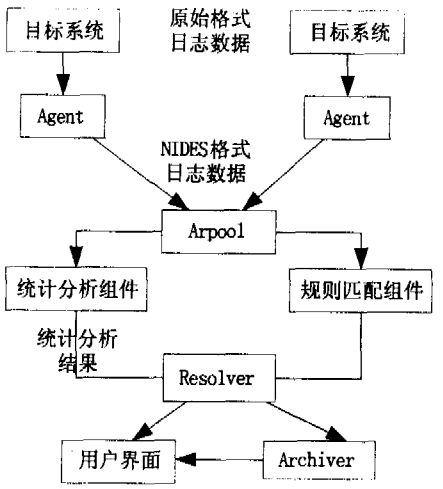

图1　NIDES检测流程图

NIDES引入了下列概念来更好地完成学习和比较的过程:

1)度量(Measure):主体行为的特性使用度量(如文件访问、CPU利用率、使用时间等)来表示。在NIDES系统中为每一种度量构造了一个长期行为和短期行为的概率分布。

2)半周期(Half－life):在NIDES系统中,构成短期行为和长期行为的审计记录的数量或进行审计记录的天数可以通过指定半周期的方法来进行设置。对于长期概率分布而言,通常NIDES将半周期设为30天,这意味着在长期概率分布中,半周期也就是最近30天的审计记录所占的权重为最新记录的一半,而下一个半周期(60天)的审计记录的权重则是四分之一,以此类推。采用这种方法,越新的活动所占的权重越大,因此在长期概貌中很早期的活动就会被忽略。这体现了近期行为对整个长期行为有着更大的影响,使其具有简单学习能力。

3)统计方法:度量的长期概貌和短期概貌的差异程度是通过Q统计来计算的。Q统计是类似于Chi－Square统计的方法,长期行为的概貌充当真实的概率分步,而短期行为的概貌作为被考察的对象。得出的Q值越大,说明该度量的长期概貌和短期概貌的差异越大,也就是在短期行为中的疑点越多。

1.2　基于专家系统的入侵检测

采用人工智能方法,将规则描述引入了入侵检测系统。所谓基于专家系统的入侵检测是指在检测系统中,将每一种攻击手段抽象为一条或多条规则,将事件采集器采集到的网络行为与专家系统的规则库进行匹配,以判断目标系统是否受到攻击[3]。

专家系统的建立依赖于知识库的完备性,知识库的完备性进一步取决于审计记录的完备性。特征入侵的特征抽取与表达,是入侵检测专家系统的关键。一个基于规则的专家系统应该在专家的指导下随着经验的积累利用自学习能力进行规则的扩充和修改。

基于专家系统的入侵检测系统包含以下几个要点:

(1)规则的描述。

规则是构建基于专家系统的入侵检测系统的前提。在入侵检测系统中,规则有多种表达方式,可以是基于决策树的描述和基于图形的描述等。

(2)推理方法。

现有的入侵检测系统中,大多数采用的是一种基于事实驱动的正向推理方法,将网络的状态和专家知识库中的规则进行匹配,从而判断是否存在入侵行为。该方法实现简单,实时性好,但缺乏对未知入侵行为的预报能力。

(3)自适应更新。

由于基于专家系统的入侵检测系统对未知入侵行为缺乏报警能力,因此需要增强其自适应能力。引入自适应更新机制,不但可以扩充专家知识库,增强检测能力,还可以对规则进行不断的修正。对于基于专家系统的入侵检测系统自适应更新机制,可以在专家知识的指导下,采用神经网络等技术来实现。

由于专家系统的不可移植性与规则的不完备性,基于专家系统的入侵检测系统不宜单独用于入侵检测。较适用的方法是将专家系统与采用软计算方法技术的入侵检测系统结合在一起,构成一个以已知的入侵规则为基础,可扩展的动态入侵事件检测的智能IDS,自适应地进行特征与异常检测,实现高效的入侵检测及其防御。

NIDES同时也是一个典型的基于专家系统的入侵检测系统。在图1检测流程中的规则匹配组件就是包含了基于专家系统的误用检测模块。该组件使用了一个由PBEST(Product－Based Expert System Tool,基于产品的专家系统工具)生成的规则库。它接受一个规则库规范,并将每一个规则转换成一系列函数,这些函数实现了改进的Rete算法。同时它还产生用于将所有不同类型的事实加入到知识库的函数。除了由PBEST工具所产生的代码外,还有一个包括规则库引擎代码的支持库和其他对所有规则库通用的支持代码。

1.3　基于数据挖掘的入侵检测

入侵检测系统的关键是如何从大量的审计数据中提

取出具有代表性的系统特征模式,识别用户的正常行为和异常行为。数据挖掘技术提供了处理安全事件数据的智能化方法,通过利用关联规则分析、序列模式分析等算法提取与安全相关的系统特征属性,根据系统特征属性生成安全事件的分类模型,从而自动识别网络或主机中的入侵行为[4]。

数据挖掘也称为数据库中的知识发现技术,是指从大量、不完全、有噪声、模糊、随机的数据中发现隐含数据中的关系,建立模型,提取具有潜在价值、可信、新颖、有效并能被人所理解的信息和知识的过程。数据挖掘是一种决策支持过程,其主要基于人工智能、机器学习、统计学等技术,高度自动化地分析大量的数据,做出归纳性的推理,从中挖掘出潜在的模式。数据挖掘的技术基础是人工智能,它利用了人工智能的一些已经成熟的算法和技术,比如人工神经网络、遗传算法、决策树、规则推理等。数据挖掘的一般过程是:①选择数据源;②采集数据;③计算统计变量,对数据进行描述,发现数据间的关系;④选定相应的数据挖掘算法,建立预言模型;⑤验证模型的合理性、准确性,并完善模型;⑥通过模型指导决策。

目前已提出了很多数据挖掘的方法或算法,按照挖掘任务的不同可以分为以下几个主要类型:

1)关联规则分析(Association),相应的算法有 Apriori, AprioriTid 等;

2)序列模式分析(Sequential Patterns),相应的算法有 AprioriAll, AprioriSome, DynamicSome 等;

3)数据分类分析(Data Classification),相应的算法有 RIPPER, C4.5 等;

4)聚类分析(Clustering),相应的算法有 CLARANS, BIRCH 等。

当前数据挖掘的研究重点已逐渐从发现方法转移到系统应用,并且注重多种发现策略和技术的集成,以及多学科之间的相互渗透。将数据挖掘技术应用到入侵检测系统,提高入侵检测系统的智能检测能力,已经成为当前 IDS 发展的一个重要研究方向。

2 入侵检测系统中的数据挖掘技术分析

利用数据挖掘算法对审计数据进行处理,要求所选取的安全审计数据具备以下两个前提特性:

1)网络流量中入侵数据只占极少数;

2)攻击总是使安全审计数据的某些特征变量明显地偏离正常值。

当然,这两个前提在实际应用中都是成立的。首先,攻击事件相对于正常的网络或系统访问是很少见的,通常入侵行为只占不到 5%;其次,安全审计数据在正常情况下非常稳定,入侵行为与正常行为的区别很大,攻击行为的一些特征变量和正常值之间偏离也很大[5,6]。目前在入侵检测系统中的数据挖掘技术主要集中在关联规则分析、序列模式分析和数据分类分析上。

2.1 关联规则分析

关联规则描述在一个事务中事物之间同时出现的规律的知识模式。更确切地说,关联规则通过量化的数字描述一个事物的出现对另一个事物的出现有多大的影响。

设 $I = \{i_1, i_2, \cdots, i_m\}$ 是一组数据项集合,其中的元素称为项(item)。D 是一组事务集合,D 中的每个事务(Transaction)T 是一组数据项,并满足 $T \subseteq I$。假设有一个数据项集(Itemset)X,一个事务 T,如果 $X \subseteq T$,则称事务 T 支持数据项集 X。

一个关联规则是指符合以下形式的一种数据隐含规则:$X \Rightarrow Y$,其中 X, Y 是两组数据项,满足 $X \subset I$, $Y \subset I$, 并且 $X \cap Y = \varnothing$。

一般用支持度(support)和置信度(confidence)来描述一个关联规则的属性。

规则 $X \Rightarrow Y$ 在事务集中的支持度是指事务集中包含 X 和 Y 的事务数与所有事务数之比,记为 support($X \Rightarrow Y$),即 support($X \Rightarrow Y$) = $|\{T: X \cup Y \subseteq T, T \in D\}| / |D|$。

规则 $X \Rightarrow Y$ 在事务集中的置信度是指包含 X 和 Y 的事务数与包含 X 的事务数之比,记为 confidence($X \Rightarrow Y$),即 confidence($X \Rightarrow Y$) = $|\{T: X \cup Y \subseteq T, T \in D\}| / |\{T: X \subseteq T, T \in D\}|$。

关联分析的目的是从已知的事务集 D 中,产生数据项集之间的关联规则,保证其支持度和置信度大于用户预先指定的最小支持度(minimum support)和最小置信度(minimum confidence)。

挖掘关联规则通常分为两个步骤来进行:

(1)从事务集 D 中找出所有支持度大于最小支持度的数据集项,称之为大数据项集(large itemsets),其他不满足支持度要求的数据项集则称之为小数据项集(small itemsets)。

(2)使用大数据项集(large itemsets)产生期望的关联规则。产生关联规则的基本原则是其置信度必须大于预先指定的限定值。

在入侵检测系统中,可以用关联规则分析来找出入侵行为之间的相关性。

2.2 序列模式分析

序列模式分析和关联规则分析相似,其目的也是为了挖掘数据的联系,但不同的是关联分析用于挖掘数据记录中不同数据项之间的关联性,而序列分析则是发现不同数据记录之间的相关性。序列分析的目标是在事务数据库中挖掘出序列模式,即满足用户指定的最小支持度要求的大序列,并且该序列模式必须是最高序列。

挖掘序列模式通常按以下 5 个步骤进行:

(1)排序阶段(sort phase):以事务的主体为主键,事务时间为次主键,对原始数据库进行排序,将其转换为主体序列(customer sequences)的数据库;

(2)大数据项阶段(large itemset phase):找出所有的大

数据项集 L,把大数据项集映射为一组相邻的整数,每个大数据项对应一个整数;

(3)转换阶段(transformation phase):将数据库中主体序列的每一次事务用该事务包含的大数据项集(映射的整数)代替;

(4)序列阶段(sequence phase):利用大数据项集挖掘序列模式(large sequences);

(5)序列最高化阶段(maximal phase):找出所有序列模式(large sequences)的最高序列集。

在入侵检测领域中,由于攻击者的许多入侵行为都是有先后关系,具有一定的时序性,例如黑客在实施攻击时,一般要先对系统的端口进行扫描,找出具体的漏洞后再实施进一步的入侵,因此,利用序列模式分析可以挖掘入侵行为之间的联系。

2.3 数据分类分析

数据分类的目的是提取数据库中数据项的特征属性,生成分类模型,该模型可以把数据库中的每个数据项都映射到给定类别中的一个。

数据分类的步骤通常为:

(1)获得训练数据集(training set),该数据集中的数据记录具有和目标数据库中数据记录相同的数据项;

(2)训练数据集中每一条数据记录都有已知的类型标识与之相关联;

(3)分析训练数据集,提取数据记录的特征属性,为每一种类型生成精确的描述模型;

(4)使用得到的类型描述模型对目标数据库中的数据记录进行分类或生成优化的分类模型(分类规则)。

通过综合运用关联规则分析、序列模式分析和数据分类算法,可以自动地从海量的安全审计数据和网络流量中提取出可用于入侵检测的知识和模式,识别用户访问的正常行为和入侵行为。

3 小　结

基于入侵检测研究领域未来的趋势是融合其他学科和技术领域的知识来提供新的入侵检测解决方法[7]。文中讨论和研究了基于统计、基于专家系统、基于数据挖掘等智能化入侵检测方法,详细阐述了基于数据挖掘这一目前和未来比较先进的检测方法。随着数据挖掘技术的不断发展,该检测方法将会有更广阔的应用前景。

参考文献:

[1] Lee Wenke, Stolfo S J, Mok K W. A Data Mining Framework for Building Intrusion Detection Models[Z]. US: Columbia University, 1999.

[2] Anderson D, Frivold T, Valdes A. Next-generation intrusion detection expert system (NIDES): A summary[R]. Technical Report SRI-CSL-95-07, Computer Science Laboratory, SRI International, 1995.

[3] Geib C W, Goldman R P. Plan Recognition in Intrusion Detection Systems[A]. In DARPA Information Survivability Conference and Exposition (DISCEX)[C]. [s. l.]: [s. n.], 2001.

[4] 徐　菁,刘宝旭,许榕生. 基于数据挖掘技术的入侵检测系统设计与实现[J]. 计算机工程,2002,28(6):9-10.

[5] 李　昀,李伟华. 分布式入侵检测系统的研究与实现[J]. 计算机工程与应用,2003,39(4):1-3.

[6] 张　颖,王　辉. 一种与入侵检测互动的 Internet 安全防范系统[J]. 计算机工程与应用,2003,39(7):168-169.

[7] 江　波,郭　巧. 基于网络的 IDS 的几点改进措施[J]. 计算机工程与设计,2003,24(3):43-45.

(上接第 131 页)

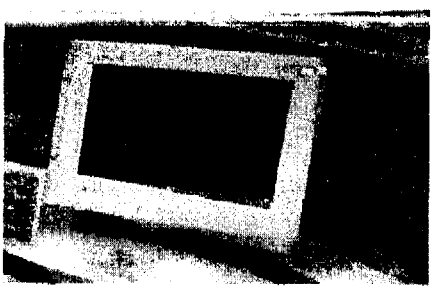

图 4　插补图像

参考文献:

[1] Greene N. Environment mapping and other applications of world projections[J]. IEEE Computer Graphics and Applications, 1986, 6(11): 21-29.

[2] Chen S E, Williams L. View interpolation for image synthesis [A]. in Proc. of ACM SIGGRAPH'93[C]. New York, NY, USA: ACM Press, 1993. 279-288.

[3] Rothwell C, Faugeras O, Csurka G. A comparison of projective reconstructionmethods for pairs of views[J]. Computer Vision and Image Understanding, 1997, 68(1): 37-58.

[4] Hartley R I, Zisserman A. Multiple View Geometry in Computer Vision[M]. Cambridge: Cambridge University Press, 2000.

[5] Gui Guofu, Zhang Quanbin. Human Face Warping Based On Images[A]. Second International Conference on Images and Graphics[C]. USA: SPIE, 2002.

[6] Wolberg G. Digital Image Warping[M]. Los Alamitos, California: IEEE Computer Society Press, 1990.

[7] Seitz S M, Dyer R. View Morphing[A]. In: Proc SIGGRAPH'96[C]. USA: [s. n.], 1996. 21-30.

[8] McMillan L, Bishop G. Plenoptic Modeling: An image-based rendering system[A]. in Proc. SIGGRAPH'95[C]. Los Angeles, California: [s. n.], 1995. 39-46.