0-9825/2000/11(11)1460-07 ©2000 Journal of Software 软件学报 Vol. 11, No. 11

网络安全入侵检测:研究综述*

蒋建春, 马恒太, 任党恩, 卿斯汉

(中国科学院 信息安全技术工程研究中心,北京 100080)

E-mail: jianchun@ercist.iscas.ac.cn

http://www.ercist.ac.cn

摘要: 入侵检测是近年来网络安全研究的热点. 首先说明入侵检测的必要性,并给出入侵检测的概念和模型,概述了多种入侵检测方法及体系结构. 最后,讨论了该领域当前存在的问题及今后的研究方向.

关键词: 网络安全;入侵检测

中图法分类号: TP393 **文献标识码**: A

计算机联网技术的发展改变了以单机为主的计算模式. 但是,网络入侵的风险性和机会也相应地急剧增多. 设计安全措施来防范未经授权访问系统的资源和数据,是当前网络安全领域的一个十分重要而迫切的问题. 目前,要想完全避免安全事件的发生并不太现实. 网络安全人员所能做到的只能是尽力发现和察觉入侵及入侵企图,以便采取有效的措施来堵塞漏洞和修复系统. 这样的研究称为入侵检测,为此目的所研制的系统就称为入侵检测系统(intrusion detection system,简称 IDS). 本文将论述网络安全存在的漏洞和潜在的威胁,给出入侵检测的概念和模型,详尽地概括并分析传统的和最新的各种检测方法及体系结构,并提出 IDS 当前存在的问题及今后的研究方向.

1 入侵检测的必要性

一个安全系统至少应该满足用户系统的保密性、完整性及可用性要求. 但是,随着网络连接的迅速扩展,特别是 Internet 大范围的开放以及金融领域网络的接入,越来越多的系统遭到入侵攻击的威胁. 这些威胁大多是通过挖掘操作系统和应用服务程序的弱点或者缺陷(bug)来实现的. 1988 年的"蠕虫事件"就是一个很好的实例[1]. 目前,对付破坏系统企图的理想方法是建立一个完全安全系统. 但这样的话,就要求所有的用户能识别和认证自己,还要采用各种各样的加密技术和强访问控制策略来保护数据. 而从实际上看,这根本是不可能的. 首先,在实践当中,建立完全安全系统根本是不可能的. Miller[2]给出一份有关现今流行的操作系统和应用程序研究报告,指出软件中不可能没有缺陷,此外,设计和实现一个整体安全系统相当困难. 其次,要将所有已安装的带安全缺陷的系统转换成安全系统需要相当长的时间. 第 3,加密技术方法本身存在的一定问题. 第 4,安全系统易受内部用户滥用特权的攻击. 第 5,安全访问控制等级和用户的使用效率成反比. 第 6,访问控制和保护模型本身存在一定的问题[2]. 第 7,在软件工程中存在软件测试不充足、软件生命周期缩短、大型软件复杂性等难解问题.

基于上述几类问题的解决难度,一个实用的方法是,建立比较容易实现的安全系统,同时按照一定的安全策略建立相应的安全辅助系统,IDS 就是这样一类系统. 现在安全软件的开发方式基本上就是按照这个思路进行的. 就目前系统安全状况而言,系统存在被攻击的可能性. 如果系统遭到攻击,只要尽可能地检测到,甚至是实时地检测到,然后采取适当的处理措施. IDS 一般不是采取预防的措施以防止入侵事件的发生,入侵检测作为安全

* 收稿日期: 2000-03-14; 修改日期: 2000-07-14

基金项目: 中国科学院软件研究所青年创新基金资助项目(CXZK5606)

作者简介: 蒋建春(1971-),男,广西壮族自治区全州人,博士生,主要研究领域为计算机网络,信息安全对抗;马恒太(1970-),男,山东临朐人,博士生,主要研究领域为网络信息安全,分布式计算;任党恩(1975-),男,安徽人,硕士生,主要研究领域为网络信息安全;卿斯汉(1939-),男,湖南人,研究员,博士生导师,主要研究领域为信息安全理论与技术.

技术其作用在于:(1) 识别入侵者;(2) 识别入侵行为;(3) 检测和监视已成功的安全突破;(4) 为对抗入侵及时提供重要信息,阻止事件的发生和事态的扩大. 因此,入侵检测非常必要.

2 入侵检测的定义及分类

Adenrson 在 80 年代早期使用了"威胁"这一概念术语,其定义与入侵含义相同. 将入侵企图或威胁定义为未经授权蓄意尝试访问信息、窜改信息,使系统不可靠或不能使用[3]. Heady 给出另外的入侵定义,入侵是指有关试图破坏资源的完整性、机密性及可用性的活动集合[4]. Smaha[5]从分类角度指出入侵包括尝试性闯入、伪装攻击、安全控制系统渗透、泄漏、拒绝服务、恶意使用 6 种类型.

入侵检测技术主要分成两大类型:异常入侵检测和误用入侵检测. 第 1 种是指能够根据异常行为和使用计算机资源情况检测出来的入侵. 异常入侵检测试图用定量方式描述可接受的行为特征,以区分非正常的、潜在的入侵性行为. Anderson[3]做了如何通过识别"异常"行为来检测入侵的早期工作. 他提出了一个威胁模型,将威胁分为外部闯入、内部渗透和不当行为 3 种类型,并使用这种分类方法开发了一个安全监视系统,可检测用户的异常行为. 外部闯入是指未经授权计算机系统用户的入侵;内部突破是指已授权的计算机系统用户访问未经授权的数据;不当行为是指用户虽经授权,但对授权数据和资源的使用不合法或滥用授权. 误用入侵检测是指利用已知系统和应用软件的弱点攻击模式来检测入侵. 例如,Internet 蠕虫攻击使用了 fingerd 和 sendmail 错误[4],故可以归结到误用入侵这种类型. 与异常入侵检测相反,误用入侵检测能直接检测不利的或不可接受的行为,而异常入侵检测是检查出与正常行为相违背的行为.

入侵检测技术模型最早由 Dorothy Denning 提出,如图 1 所示[6]. 目前,检测技术及其体系均是在此基础上的扩展和细化.

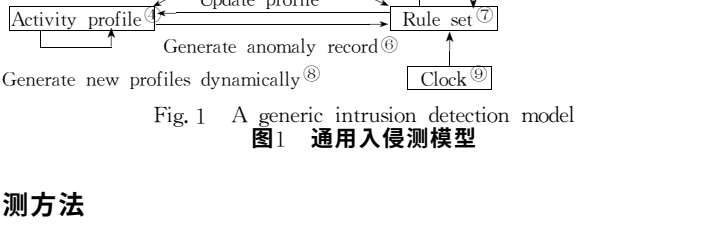

Fig. 1 A generic intrusion detection model

图1 通用入侵测模型

3 入侵检测方法

3.1 异常入侵检测

异常入侵检测的主要前提条件是将入侵性活动作为异常活动的子集. 理想状况是异常活动集与入侵性活动集等同. 这样,若能检测所有的异常活动,则可检测所有的入侵性活动. 但是,入侵性活动并不总是与异常活动相符合. 这种活动存在 4 种可能性:(1) 入侵性而非异常;(2) 非入侵性且异常;(3) 非入侵性且非异常;(4) 入侵且异常. 异常入侵要解决的问题就是构造异常活动集并从中发现入侵性活动子集. 异常入侵检测方法依赖于异常模型的建立,不同模型构成不同的检测方法. 异常检测是通过观测到的一组测量值偏离度来预测用户行为的变化,然后作出决策判断的检测技术.

3.1.1 基于特征选择异常检测方法

基于特征选择异常检测方法是通过从一组度量中挑选能检测出入侵的度量构成子集来准确地预测或分类已检测到的入侵. 异常入侵检测的问题是在异常活动和入侵活动之间难于作出判断. 判断符合实际的度量是复杂的,因为能否合适地选择度量子集依赖于检测到的入侵类型,一个度量集对所有的各种各样的入侵类型不可能是足够的. 预先确定特定的度量来检测入侵可能会错过单独的特别环境下的入侵. 最理想的检测入侵度量集必须动态地决策判断以获得最好的效果. 假设与入侵潜在相关的度量有 n 个,则这 n 个度量所构成的子集数是 2^n 个. 由于搜索空间与度量数是级数关系,所以穷尽寻找最理想的度量子集的开销不是有效的. Maccabe[7]提出

用遗传方法来搜索整个度量子空间以寻找正确的度量子集.其方法是使用学习分类器方案生成遗传交叉算子和基因突变算子,除去降低预测入侵的度量子集,而采用遗传算子产生更强的度量子集取代.这种方法与较高的预测度量子集相结合,允许搜索的空间大小比其他启发式搜索技术更有效.其他的特征选取技术概况参见文献[8,9].

3.1.2 基于贝叶斯推理的异常检测方法

基于贝叶斯推理的异常检测方法是通过在任意给定的时刻,测量 $A_1,A_2,\ldots,A_n$ 变量值,推理判断系统是否有入侵事件发生.其中每个 A_i 变量表示系统不同方面的特征(如磁盘 I/O 的活动数量,或者系统中页面出错的数量).假定 A_i 变量有两个值,1 表示异常,0 表示正常.I 表示系统当前遭受入侵攻击.每个异常变量 A_i 的异常可靠性和敏感性表示为 $P(A_i=1/I)$和 $P(A_i=1|\neg I)$,则在给定每个 A_i 值的条件下,由贝叶斯定理得出 I 的可信度为

$$P(I|A_1,A_2,\ldots,A_n)=P(A_1,A_2,\ldots,A_n|I)\frac{P(I)}{P(A_1,A_2,\ldots,A_n)},$$

其中要求给出 I 和 $\neg I$ 的联合概率分布.又假定每个测量 A_i 仅与 I 相关,且与其他的测量条件 A_j 无关,$i\neq j$,则有

$$P(A_1,A_2,\ldots,A_n|I)=\prod_{i=1}^{n}P(A_i|I),$$

$$P(A_1,A_2,\ldots,A_n|\neg I)=\prod_{i=1}^{n}P(A_i|\neg I).$$

从而得到

$$\frac{P(I|A_1,A_2,\ldots,A_n)}{P(\neg I|A_1,A_2,\ldots,A_n)}=\frac{P(I)}{P(\neg I)}\frac{\prod_{i}^{n}P(A_i|I)}{\prod_{i}^{n}P(A_i|\neg I)}$$

因此,根据各种异常测量的值、入侵的先验概率及入侵发生时每种测量到的异常概率,能够检测判断入侵的概率.但是,为了检测的准确性,还必须考虑各个测量 A_i 之间的独立性.一种方法是通过相关性分析,确定各个异常变量与入侵的关系[10].

3.1.3 基于贝叶斯网络的异常检测方法

贝叶斯网络是实现贝叶斯定理揭示的学习功能,发现大量变量之间的关系,进行预测、分类等数据的有力工具.基于贝叶斯网络的异常检测方法通过建立起异常入侵检测贝叶斯网,然后将其用作分析异常测量结果.贝叶斯网络允许以图形方式表示随机变量间相关的原因,并通过指定的一个小的与邻接节点相关的概率集计算随机变量的联接概率分布.按给定全部节点组合,所有根节点的先验概率和非根节点概率构成这个概率集.贝叶斯网络是一个有向图 DAG,有向图中的弧表示父节点和孩子节点之间的依赖关系.这样,当随机变量的值变成可知时,就允许把它吸收成为证据,按给定的这个证据为其他的剩余随机变量条件值的判断提供计算框架.但是,通常情况下,判断根节点先验概率值和每个有向弧连接矩阵是重要的.至今,有关贝叶斯网络入侵检测系统的实际系统尚未出现,详细资料参看文献[11].

3.1.4 基于模式预测的异常检测方法

基于模式预测的异常检测方法的假设条件是事件序列不是随机的而是遵循可辨别的模式.这种检测方法的特点是考虑了事件的序列及相互联系.Teng 和 Chen 给出基于时间的推理方法,利用时间规则来识别用户行为正常模式的特征[11].通过归纳学习产生这些规则集,并能动态地修改系统中这些规则,使之具有较高的预测性、准确性和可信度.如果规则大部分时间是正确的,并能够成功地运用预测所观察到的数据,那么规则就具有高可信度.TIM 给出了一条产生规则[12]:

$$(E1!\ E2!\ E3)(E4=95\%,E5=5\%),$$

其中 $E1\sim E5$ 表示安全事件.

这条规则是根据前面观测到的事件 $E1$ 模式后面是 $E2,E3,E4,E5$.观测到 $E4$ 事件的概率是 95%,观测到

事件 $E5$ 的概率是 95%.通过事件当中的临时关系,TIM 能够产生更多通用的规则.根据观察到的用户行为,归纳产生出一套规则集来构成用户的轮廓框架.如果观测到的事件序列匹配规则的左边,而后续的事件显著地背离根据规则预测到的事件,那么系统就可以检测出这种偏离,这就表明用户操作是异常的.由于不可识别行为模式能匹配任何规则的左边,从而导致不可识别行为模式作为异常判断,这是该方法的主要弱点.相反,如果能预测出不正常的后继事件的片段,则在一定程度上可以断定用户行为的异常性.这种方法的主要优点有:(1) 能较好地处理变化多样的用户行为,并具有很强的时序模式.(2) 能够集中考察少数几个相关的安全事件,而不是关注可疑的整个登录会话过程.(3) 对发现检测系统遭受攻击,具有良好的灵敏度.因为根据规则的蕴涵语义,在系统学习阶段,能够更容易地辨别出欺骗者训练系统的企图.

3.1.5 基于贝叶斯聚类的异常检测方法

基于贝叶斯聚类的异常检测方法通过在数据中发现不同类别的数据集合,这些类反映了基本的因果机制(同类的成员比其他的更相似),以此来区分异常用户类,进而推断入侵事件发生来检测异常入侵行为.Cheeseman 和 Stutz 在 1995 年开发的自动分类程序(AutoClass Program)是一种无监督数据分类技术[11].AutoClass 实现了使用贝叶斯统计技术对给定的数据进行搜索分类.这种方法尽可能地判断处理产生的数据,没有划分给定数据类别,但是定义了每个数据成员.其优点是:(1) 根据给定的数据,AutoClass 自动地判断决定尽可能的类型数目;(2) 不要求特别相似测量、停顿规则和聚类准则;(3) 可以自由地混合连续的和离散的属性.

统计入侵异常检测对所观测到的行为分类处理,到目前为止,所使用到的技术主要集中于监督式的分类,这种分类是根据观测到的用户行为来建立起用户轮廓.而贝叶斯分类方法允许最理想化的分类数、具有相似的轮廓的用户群组以及遵从符合用户特征集的自然分类.但是,该方法是新的,在入侵检测系统中还没有实现测试.自动分类程序在怎样处理好固有的次序性数据(如审计跟踪)以及将统计分布特性植入分类中等方面,效果并不十分明显.当自动分类程序支持处理在线数据时,对新数据在使用时能否递增式地分类或者是否立即需要全部输入数据等问题的处理尚未定论.由于统计所固有的特性,自动分类程序还存在选定合适的异常阈值和用户逐步地影响类型分布能力的困难.

3.1.6 基于机器学习的异常检测方法

这种异常检测方法通过机器学习实现入侵检测,其主要的方法有死记硬背式、监督学习、归纳学习(示例学习)、类比学习等[13].Terran 和 Carla E. Brodley 将异常检测问题归结为根据离散数据临时序列学习获得个体、系统和网络的行为特征,并提出一个基于相似度的实例学习方法(instance based learning,简称 IBL),该方法通过新的序列相似度计算将原始数据(如离散事件流,无序的记录)转化成可度量的空间.然后,应用 IBL 学习技术和一种新的基于序列的分类方法,从而发现异常类型事件,以此检测入侵,其中阈值的选取由成员分类的概率决定[14,15].新的序列相似度定义如下:

设 l 表示长度,序列 $X=(x_0,x_1,\ldots,x_{l-1})$ 和 $Y=(y_0,y_1,\ldots,y_{l-1})$,

$$w(X,Y,i)=\begin{cases}0, & \text{if } i<0 \text{ or } x_i\neq y_i\\ l+w(X,Y,i-1), & \text{if } x_i\neq y_i\end{cases},$$

$$Sim(X,Y)=\sum_{i=0}^{l-1}w(X,Y,i),$$

$$Dist(X,Y)=Sim_{\max}-Sim(X,Y).$$

令 D 表示用户的模式库,由一系列的序列构成,X 表示最新观测到的用户序列,则

$$Sim_D(X)=\max_{Y\in D}\{Sim(Y,X)\}.$$

上式用来分类识别,检测异常序列.实验结果表明,这种方法检测迅速,而且误检率低.然而,此方法在用户动态行为变化以及单独异常检测方面还有待改善.复杂的相似度量和先验知识加入到检测中可能会提高系统的准确性,但需要做进一步的工作.总的来说,机器学习中许多模式识别技术对安全领域都有参考价值.

3.1.7 基于数据采掘的异常检测方法

计算机联网导致大量审计记录,而且审计记录大多是以文件形式存放(如 UNIX 系统 Sulog),若单独依靠手工方法去发现记录中的异常现象是不够的,往往是操作不便,不容易找出审计记录间的相互关系.Wenke Lee 和

Salvatore J. Stolfo 将数据采掘技术应用到入侵检测研究领域中,从审计数据或数据流中提取感兴趣的知识,这些知识是隐含的、事先未知的、潜在的有用信息,提取的知识表示为概念、规则、规律、模式等形式[16~18],并可用这些知识去检测异常入侵和已知的入侵.基于数据采掘的异常检测方法目前已有现成的 KDD 算法可以借用,这种方法的优点是可适应处理大量数据的情况.但是,对于实时入侵检测则还存在问题,需要开发出有效的数据采掘算法和相适应的体系[19,20].

3.1.8 其 他

由于篇幅所限,基于神经网络、统计异常检测方法参见文献[10,21].

3.2 误用入侵检测技术

误用入侵检测的主要假设是具有能够被精确地按某种方式编码的攻击,并可以通过捕获攻击及重新整理,确认入侵活动是基于同一弱点进行攻击的入侵方法的变种.误用入侵检测指的是通过按预先定义好的入侵模式以及观察到入侵发生的情况进行模式匹配来检测.入侵模式说明了那些导致安全突破或其他误用的事件中的特征、条件、排列和关系.一个不完整的模式可能表明存在入侵的企图,模式构造有多种方式.下面来分析各种各样的误用检测方法.

3.2.1 基于条件概率的误用入侵检测方法

基于条件概率的误用入侵检测方法将入侵方式对应于一个事件序列,然后通过观测到事件发生的情况来推测入侵出现[11].这种方法的依据是外部事件序列,根据贝叶斯定理进行推理检测入侵.令 ES 表示事件序列,先验概率为 $P(\text{Intrusion})$,后验概率为 $P(ES|\text{Intrusion})$,事件出现的概率为 $P(ES)$,则

$$P(\text{Intrusion}|ES)=P(ES|\text{Intrusion})\frac{P(\text{Intrusion})}{P(ES)}.$$

由于通常情况下网络安全专家可以给出先验概率 $P(\text{Intrusion})$,对入侵报告数据统计处理得出 $P(ES|\text{Intrusion})$和 $P(ES|\neg\text{Intrusion})$,于是可以计算出

$$P(ES)=((P(ES|\text{Intrusion})-P(ES|\neg\text{Intrusion}))\cdot P(\text{Intrusion})+P(ES|\neg\text{Intrusion}),$$

故可以通过事件序列的观测,推算出 $P(\text{Intrusion}|ES)$.基于条件概率的误用入侵检测方法是在概率理论基础上的一个普遍方法.它是对贝叶斯方法的改进,其缺点是先验概率难以给出,而且事件的独立性难以满足.

3.2.2 基于状态迁移分析的误用入侵检测方法

状态迁移分析方法将攻击表示成一系列被监控的系统状态迁移.攻击模式的状态对应于系统状态,并具有迁移到另外状态的条件断言.通过弧将连续的状态连接起来以表示状态改变所需要的事件,允许事件类型被植入到模型并且无须同审计记录一一对应.采用这种方法的系统包括 STAT(state transition analysis techinque)[12]和 USTAT(state transition analysis tool for UNIX)[22].攻击模式只能说明事件序列,因此不适合描述更复杂的事件.而且,除了通过植入模型的原始断言,没有通用的方法来剪除部分攻击匹配.

3.2.3 基于键盘监控的误用入侵检测方法

基于键盘监控的误用入侵检测方法假设入侵对应特定的击键序列模式,然后监测用户击键模式,并将这一模式与入侵模式匹配以此就能检测入侵[11].这种方法的不利之处是,在没有操作系统支持的情况下,缺少捕获用户击键的可靠方法,存在无数击键方式表示同一种攻击.而且,没有击键语义分析,用户使用别名命令很容易欺骗这种技术.例如,用户注册的 SHELL 提供了简写命令序列工具,可以产生所谓的别名,类似宏定义.因为这种技术仅仅分析击键,所以不能够检测到恶意程序执行结果的自动攻击.

3.2.4 其 他

由于篇幅所限,基于专家系统、模型误用推理及 Petri 网状态转换的误用入侵检测方法参见文献[21].

4 入侵检测系统的体系结构

入侵检测系统的体系结构大致可以分为基于主机型(Host-Based)、网络型(Network-Based)和主体型(Agent-Based)3 种[23].

基于主机入侵检测系统为早期的入侵检测系统结构,其检测的目标主要是主机系统和系统本地用户.检测

原理是根据主机的审计数据和系统的日志发现可疑事件,检测系统可以运行在被检测的主机或单独的主机上[5,23,24].这种类型系统依赖于审计数据或系统日志的准确性和完整性以及安全事件的定义.若入侵者设法逃避审计或进行合作入侵,则基于主机的检测系统就暴露出其弱点,特别是在现在的网络环境下.单独地依靠主机审计信息进行入侵检测难以适应网络安全的需求.这主要表现在:① 主机的审计信息弱点,如易受攻击、入侵者可通过使用某些系统特权或调用比审计本身更低级的操作来逃避审计.② 不能通过分析主机的审计记录来检测网络攻击(域名欺骗、断口扫描等).因此,基于网络的入侵检测系统对网络安全是必要的,这种检测系统根据网络流量、协议分析、简单网络管理协议信息等数据检测入侵,如 NetSTAT 检测系统就是基于网络型的[12].

主机和网络型的入侵检测系统是一个统一集中系统,但是,随着网络系统结构的复杂化和大型化,系统的弱点或漏洞将趋向于分布式.另外,入侵行为不再是单一的行为,而是表现出相互协作入侵的特点[25].入侵检测系统要求可适应性、可训练性、高效性、容错性、可扩展性等要求.不同的 IDS 之间也需要共享信息,协同检测.于是,美国普度大学安全研究小组提出了基于主体入侵检测系统[26].其主要的方法是采用相互独立运行的进程组(称为自治主体)分别负责检测,通过训练这些主体,并观察系统行为,然后将这些主体认为是异常的行为标记出来,并将检测结果传送到检测中心.另外,S. Staniford 等人提出了 CIDF (common intrusion detection framework).目前,CIDF 正在开发和讨论之中,有可能成为入侵检测系统的标准[27].

对于入侵检测系统的评估,主要的性能指标有:(1) 可靠性,系统具有容错能力和可连续运行;(2) 可用性,系统开销要最小,不会严重降低网络系统性能;(3) 可测试,通过攻击可以检测系统运行;(4) 适应性,对系统来说必须是易于开发的,可添加新的功能,能随时适应系统环境的改变;(5) 实时性,系统能尽快地察觉入侵企图以便制止和限制破坏;(6) 准确性,检测系统具有低的误警率和漏警率;(7) 安全性,检测系统必须难于被欺骗和能够保护自身安全[23,28~30].

5 结束语

本文就入侵检测的必要性、异常和误用检测的主要方法、入侵检测系统的结构等作了分析和概括.随着网络入侵技术的不断发展,入侵的行为表现出不确定性、复杂性、多样性等特点.入侵检测面临许多有待解决的关键问题,如高效率的检测算法、入侵模式确认、入侵实时监测、入侵描述语言、检测数据标准化、高速网络中的入侵检测、IDS 评估、IDS 与其他系统的协同工作等一系列问题都有待进一步研究和实现.

References:

[1] Spafford, E. H. The internet worm program: an analysis. ACM Computer Communication Review, 1989,19(1):17~57.

[2] Miller, B. P., Koski, D., Lee, Cjin Pheow, *et al*. A re-examination of the reliability of UNIX utilities and services. Technical Report, Department of Computer Sciences, University of Wisconsin, 1995.

[3] Anderson, J. P. Computer security threat monitoring and surveillance. Technical Report, James P Anderson Co., Fort Washington, Pennsylvania, 1980.

[4] Spafford, E. Crisis and aftermath. Communications of the ACM, 1989,32(6):678~687.

[5] Smaha, S. E. Haystack: an intrusion detection system. In: Orlando ed. Proceedings of the 4th Aerospace Computer Security Applications Conference. Washington. DC: IEEE Computer Society Press, 1988. 37~44.

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

[7] Heady, R., Luger, G., Maccabe, A., *et al*. The architecture of a network level intrusion detection system. Technical Report, Department of Computer Science, University of New Mexico, 1990.

[8] Doak, Justin. Intrusion detection: the application of feature selection——a comparison of algorithms, and the application of a wide area network analyzer [MS Thesis]. Department of Computer Science, University of California, Davis, 1992.

[9] Bian, Zhao-qi, Yan, Ping-fan, Yang, Cun-rong. Pattern Recognition. Beijing: Tsinghua University Press, 1988 (in Chinese).

[10] Lunt, T. F., Tamaru, A., Gilham, F., *et al*. A real-time intrusion detection expert system (IDES). Technical Report, Computer Science Laboratory, SRI International, Menlo Park, California, 1992.

[11] Kumar, G. Classification and detection of computer intrusions [Ph. D. Thesis]. Purdue University, 1995.

[12] http://www.cs.ucsb.edu/~kemm/NetSTAT/documents.html.

[13] He Hua-can. Introduction to Artificial Intelligence. Xi'an: Northwestern University of Technology Press, 1988 (in

Chinese).
[14] Carla, T. L., Brodley, E. Temporal sequence learning and data reduction for anomaly detection. In: Reiter, M ed. Proceedings of the 5th Conference on Computer and Communications Security. New York: ACM Press, 1998. 150～158.
[15] Carla, T. L., Broaley, E. Detecting the abnormal: machine learning in computer security. Technical Report, TR-ECE 97-1, Purdue University, West Lafayette, 1997.
[16] http://www.usenix.org/publications/library/proceedings/sec98/full_papers/lee/lee_html/lee.html.
[17] Hu, Kan, Xia, Shao-wei. Large data warehouse-based data mining: a survey. Journal of Software, 1998,9(1):53～63 (in Chinese).
[18] http://www.cs.columbia.edu/～sal/hpapers/kdd99-id.ps.gz.
[19] http://www.cs.columbia.edu/～sal/hpapers/framework.ps.gz.
[20] http://www.cs.columbin.edu/～sal/hpapers/alg_chapter.ps.gz.
[21] Ruan, Yao-ping, Yi, Jiang-bo, Zhao, Zhan-sheng. The model and methodology of intrusion detection in computer system. Computer Engineering, 1999,25(9):63～65 (in Chinese).
[22] Ilgun, K. USTAT: a real-time intrusion detection system for UNIX [MS Thesis]. Department of Computer Science, University of California, Santa Barbara, 1992.
[23] Debar, H., Dacier, M. Andreas wespi towards a taxonomy of intrusion-detection systems. Computer Networks, 1999, 31(8):805～822.
[24] Lunt, T. F., Jagannathan, R., Edwards, D. L., *et al*. IDES——the enhanced prototype a real time intrusion-detection expert system. Technical Report, SRI-CSL-88-12, 1988.
[25] http://all.net/books/dca/top.html.
[26] http://www.cs.purdue.edu/coast/projects/aafid.html.
[27] Chen, S., Tung, B., Schnackenberg, D. The common intrusion detection framework-data formats. Internet draft draft-ietf-cidf-data-formats-00.txt, 1998.
[28] Sekar, R., Guang, Y., Verma, S., *et al*. A high-performance network intrusion detection system. In: Tsudik, G ed. Proceedings of the 6th Conference on Computer and Communication Security. New York: ACM Press, 1999. 8～17.
[29] Axelsson, S. The base-rate fallacy and its implications for the difficulty of intrusion detection. In: Tsudik, G ed. Proceedings of the 6th Conference on Computer and Communication Security. New York: ACM Press, 1999. 1～7.
[30] Liu, Mei-lan, Yao, Jing-song. Intrusion detection early warning systemand performance requirements. In: Qing, Si-han, Feng, Deng-guo eds. Information and Communication Security CCICS'99: First Chinese Conference Information and Communication Security Proceedings. Beijing: Science Press, 2000. 105～111 (in Chinese).

附中文参考文献:

[9] **边肇祺,阎平凡,杨存荣. 模式识别. 北京:清华大学出版社,1988.**
[13] **何华灿. 人工智能导论. 西安:西北工业大学出版社,1988.**
[17] **胡侃,夏绍玮. 基于大型数据仓库的数据采掘:研究综述. 软件学报,1998,9(1):53～63.**
[21] **阮耀平,易江波,赵战生. 计算机系统入侵检测模型与方法. 计算机工程,1999,25(9):63～65.**
[30] **刘美兰,姚京松. 入侵检测预警系统及其性能设计. 见:卿斯汉,冯登国编. 信息和通信安全 CCICS'99:第 1 届中国信息和通信安全学术会议论文集. 北京:科学出版社,2000. 105～111.**

A Survey of Intrusion Detection Research on Network Security

JIANG Jian-chun, MA Heng-tai, REN Dang-en, QING Si-han

(*Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijng* 100080, *China*)
E-mail: jianchun@ercist.iscas.ac.cn
http://www.ercist.ac.cn

Received March 14, 2000; accepted July 14, 2000

Abstract: Intrusion detection is a highlighted topic of network security research in recent years. In this paper, first the necessity of intrusion detection is presented, and its concepts and models are described. Then, many intrusion detection techniques and architectures are summarized. Finally, the existing problems and the future direction in this field are discussed.

Key words: network security; intrusion detection