关于计算机数据库入侵检测技术的几点思考

殷仲磊，赵广鹏

（河南理工大学现代教育中心，河南 焦作 454000）

摘 要：当前社会中计算机数据库面临很多的风险，计算机数据库的防护对于计算机安全是非常重要的。本文在分析了计算机入侵检测技术存在问题的基础上，提出了解决办法，进一步确保计算机的安全运行。

关键词：数据库；入侵；挖掘技术

中图分类号：TP309.2 **文献标识码**：A DOI: 10.3969/j.issn.1003-6970.2012.05.025

Computer Database Intrusion Detection Technology Reflections

YIN Zhong-lei,ZHAO Guang-peng

(*Henan Polytechnic University center of modern education*, *Jiaozuo* 454000, *China*)

【Abstract】In the current society, database faces many risks, a computer database protection for computer security is very important. Based on the analysis of the computer intrusion detection technology on the basis of existing problems, puts forward the solutions, to further ensure the safe operation of computer.

【Key words】Database; Invasion; Mining technology

0 引 言

随着社会信息化的发展，计算机已经在人们平常的生活中发挥着越来越重要的作用，网上购物、网上聊天、网络汇款等网络活动越来越频繁，很多人将各种资料都放在网络上，但是一旦计算机数据库被非法分子侵入，就会对个人和企业隐私产生威胁，甚至于对整个社会产生巨大的破坏作用。所以计算机的数据库系统的安全保障工作是非常重要的，为了最大限度的保护计算机的数据安全，防止病毒侵入数据库，就需要加强计算机入侵检测技术，计算机数据库入侵检测技术对保护计算机安全来说是非常重要的。

1 保护计算机数据库的重要性

计算机数据库面临很多的风险，概括起来有两方面：一方面是对计算机网络中设备的安全产生威胁，另一方面是对于计算机数据库中的信息产生威胁。计算机的信息安全可以有效保护计算机网络信息的保密性和可用性。在整个计算机面临的威胁中由于数据库是信息系统的关键，对整个计算机的运行发挥着重要的作用，所以数据库面临的威胁是最强大的。目前看来，威胁数据库的主要是计算机病毒的侵入和黑客攻击，每年由于计算机数据库遭到非法侵入造成的经济损失高达数亿美元，平均每天有 2 万多个网页会受到病毒或者是黑客的攻击，这种情况给人们的正常生活带来巨大的损失，所以计算机数据库的防护是对于计算机安全是非常重要的。

2 计算机数据库入侵监测技术的涵义

计算机数据库入侵检测技术就是在计算机的数据库和网络上设置很多程式和资料认证，比如，当进入计算机时需要对进入者身份和信息进行验证，当外部异常行为出现或者是非法强行侵入计算机行为发生时，入侵检测技术就会对这些行为做出相应的反应 [1]。计算机入侵检测技术主要对计算机数据库重要的地方进行关卡设置，也就是我们平常认为的网络陷阱，在网络遭遇非法侵入时，利用网络运行环境来采集相关数据进行检测，对所采集到的数据进行有效的分析，判断是否是非法行为，根据判断采取防御措施有效阻止攻击行为。

3 常用计算机数据库入侵检测技术

3.1 误用检测技术

误用检测技术就是计算机对已知的病毒、入侵活动或者是攻击模式进行有效检测。它主要通过系统进行假定，所有的网络入侵活动和异常行为都可以用一种特征或者模式进行表达，它首先是分析已知的入侵行为并建立相应的特征模式，当网络异常发生时，它就会自动根据自己建立的已有模型来寻找入侵行为中与之相匹配的特征 [2]，如果两者之间是匹配的，系统就会检测出这个行为是一种攻击行为，反之，两者之间没有匹配的特征它就会认为不是异常侵入或者是非法入侵。这种技术的优点在于，对已知的入侵特征的检测准确度很高，缺点是只能对已知侵入特征进行比较检测，无法对未知的类型进行检测，

作者简介：殷仲磊（1976–）男，硕士，助教，研究方向为高性能计算、并行计算、数据库等；赵广鹏（1986–）男，硕士，助教，研究方向为高性能计算。

并且有极高的可能性检测不到网络上新的病毒和攻击体[3],需要定期跟新检测系统中的数据模型。

3.2 异常检测技术

相对于误用检测技术来说,异常检测技术拥有更高的准确度和更广泛得的检测范围。异常检测技术就是指将用户平时习惯用的行为特征作为模型储存在数据库中,当计算机中用户进行操作的时候,计算机就会与用户平时储存的行为特征进行对照,对用户的活动进行详细的分析,统计所有不同于正常用户活动状态的数量,如果两者相差较大的时候,就表明计算机有了异常行为或者是非法入侵。这种计算机入侵检测技术的优点在于无需依赖经验,将收集的大量信息形成规律,运用到数据库入侵检测系统中,面对大量的数据,能够掌握检测的知识和规则[4]。异常入侵检测技术能够检测还未被识别的对象,监控对计算机系统企图侵入的行为,而且对于已识别对象的非法操作也进行监控。这种检测方法的优点在于无需依赖经验,比无用检测技术拥有更加简单的检测规律,检测的结果也更加准确。

4 计算机数据库入侵检测技术面临的问题

由于计算机大面积进入我国的时间不是很长,计算机入侵检测系统和计算机入侵检测技术在我国的运用时间还很短,我国的计算机入侵检测技术还没有深入的发展,处在一个萌芽的阶段,入侵检测的系统建立不是很完善,入侵检测手段相对比较落后,很多新的技术还没有真正运用到实践中去,所以我国的计算机入侵检测系统还存在很多的问题

4.1 计算机入侵检测的结果准确率比较低,误报和漏报概率比较高

由于计算机入侵检测技术的运用是为了维护计算机数据库的安全,数据库中的信息包括私人信息和企业信息,对于信息所有者来说,信息的安全是非常重要的,所以在研发计算机入侵检测技术时,研发团队就会抱着“宁可错杀一千,不能放过一个”的态度,想着能防患于未然,对于检测技术开发过程中关键点的设置要求就很严格,几乎到苛刻的地步,尽可能的检测出任何可疑的行为。这种情况会导致很多外部的病毒侵入,在检测中就会出现错误的检测结果,为了对这些问题进行弥补,在技术上就会采取一些防护措施,而这些防护措施对数据库又会产生一定的影响,所以整体来看,现阶段的检测技术很大程度上存在错误检测,不仅降低了检测的准确性,而且,降低了系统的服务质量。

4.2 计算机入侵检测的效率相对较低

在计算机或者是网络中,任何一个数据入侵和反侵入都需要二进制编码经过庞大的数据运算,运算之后才能够使其有效运行,因此整个的计算量非常的庞大,相应地,异常检测技术的计算代价也加大了,不仅要维护正常用户活动记录,而且随着时间的变化需要更新,这时误用检测技术需要再次地更新匹配特征,这样会增加运营成本,使得检测费用也随之升高。在检测过程中大量的二进制计算不仅是时间上的浪费,而且对于检测成本也会相应地提高。这样的检测效率在信息化高速发展的形势下,已经不能满足网络蓬勃发展的现状。

4.3 计算机入侵检测技术本省的自我防御能力有限

由于当前计算机入侵检测系统本身的缺点和设计人自身专业素质的限制,使得入侵检测技术本身就有一定的缺陷,总体来说计算机入侵检测技术本身缺乏较强的自我防御的能力,在受到对于异常检测技术本身的攻击时,异常检测技术不能发挥应该有的作用,不能对入侵行为进行有效的记录,长此以往就会对数据库的安全造成极大的威胁,导致数据库被盗、系统被病毒破坏等现象的发生。

4.4 计算机入侵检测技术的可扩展性较差

计算机入侵检测技术的可扩展性差者是计算机检测技术中最需要解决的问题,由于检测技术无法进行自动更新造成的病毒入侵是病毒蔓延最主要的原因。在目前的技术手段下,一台计算机需要安装入侵检测技术,在安装之后,这个入侵检测技术就会一成不变,在以后的使用过程中就不能再次对其进行更新,检测技术本身也不会根据网络环境的变动和数据的需要进行自动更新,当网络上一旦有新的病毒入侵或者是有新的异常行为发生时,入侵检测技术由于无法识别,造成病毒的侵入。

5 计算机入侵检测技术优化的方法

5.1 以优化 Apriori 算法来降低计算机入侵检测时庞大的计算量

当今社会,计算机的数据库越来越复杂,综合性也越来越高,面对这样的情况就需要用 Apriori 算法中剪枝候选集的功能。Apriori 算法是一种最有影响的挖掘布尔关联规则频繁项集的算法。其核心是基于两阶段频集思想的递推算法,其广泛应用于各种领域。由于 Apriori 算法相对复杂,在操作过程中还有很多不便的地方,而且操作过程需要更加小心和谨慎。所以要进一步改进 Apriori 算法,从而减少计算机进行入侵检测时的计算量。

Apriori 算法改进步骤就是:

1) 减少候选项目集的数量,当计算中的项目集小于支持度时,就需要进行相应的删减,目的是为了达到最佳候选集的数量;

2) 对数据库进行有计划地控制,对计算机数据库的扫描过程进行正确的操作,让数据库对编码的操作可以一次性完成,在以后的运算中可以利用本次操作来提高计算机计算的效率。

5.2 建立相关的数据库知识标准

计算机数据库的入侵检测技术的一个关键点在于对入侵行为特征的分析和了解,把握住入侵的特征的准确性和入侵行为所覆盖的范围。在进行数据挖掘技术时,比较常用的技术手段就是相关研究,主要就是给定一个记录,在数据库的系统中

进行详细分析和研究,对潜在的入侵行为做出整理,能够较快的发现隐形的入侵威胁。数据挖掘主要包括以下两个方面:

1) 对数据库复杂项集进行检测需要采用迭代技术,要时不时地对数据库进行全方位的扫描,保证数据库的准确度;

2) 要对复杂项集进行转化,一般来说是将复杂的项集转化成相关的规定,规定的成型会产生另一种规则,系统在运行的过程中就需要依照形成的这种规定。

4.3 创建新型的系统模型

创建新型的数据库模型能够使得整个入侵检测系统发挥作用,它主要由以下几个部分组成:

1) 进行数据的收集:主要是对数据库的历史数据进行收集,因为在系统进行入侵检测时候需要对数据进行分析和掌握,所以历史数据的收集是越完整越好,这样才能为以后的检测工作打好基础;

2) 数据处理:主要是处理和集成收集到的各种数据,为下面过程中挖掘数据提取到准备的数据;

3) 挖掘数据:数据处理中提取的数据,提取相关的行为特征,旨在建立相对安全的数据库模型;

4) 知识的规则库:入侵检测系统将用户的行为与规则库中的模式行为进行比较,如果两者相符就表示不是入侵行为;

5) 采取与挖掘技术相同的技术,从目前的用户的行为中提取行为特;

6) 根据入侵检测技术,提取相关的规则数据,对目前计算机上面操作用户的行为进行检测,如果认定为入侵行为则需要采取一定的防御措施。

5 结　语

计算机数据库的入侵检测技术对保护计算机正常运行发挥着重要的作用,在当前计算机入侵行为日益猖狂的环境下,要不断提高计算机入侵检测技术,需要我们了解数据库入侵行为的特征,从而对计算机检测技术进行相应的改变和完善,让人们在使用计算机的时候能够抵御入侵行为,营造一个良好的使用环境。

参考文献

[1] 雷利香 . 计算机数据库的入侵检测技术探析 [J]. 科技传播,2011,(14).
[2] 夏炎,殷慧文 . 网络入侵检测技术研究 [J]. 沈阳工程学院学报 (自然科学版),2008,(04).
[3] 成龙,李科,肖军 . 计算机网络安全问题分析 [J]. 电脑知识与技术,2008,(17).
[4] 秦亮 . 浅析计算机数据库的入侵检测技术 [J]. 电脑知识与技术,2011,(03).

上接第 69 页

[2] 刘文涛 . 网络安全 [M]. 北京 : 机械工业出版社,2008,67-69.
[3] 谢昌荣,李菊英 . 一种适用于宽带网络的入侵检测系统的设计与实现 [J]. 自贡 : 四川理工学院学报,2007,20(3):82-85.
[4] W.Richard Stevens 著 . TCP/IP 详解 (第 I 卷,第五版)[M]. 范建华等译,北京 : 机械工业出版社 2000:66-73.
[5] Douglas E.Comer.TCP/IP 网络互联技术 : 设计与实现 [M]. 北京 : 机械工业出版社,2002:210-232.
[6] 张仕斌 . 网络安全技术 [M]. 北京 : 清华大学出版社,2004:101-116.
[7] Anonymous[美]. 网络最高安全技术指南 [M]. 北京 : 机械工业出版社,1998:35-47.
[8] 刘文涛 . 网络安全 [M]. 北京 : 机械工业出版社,2008:99-121.
[9] 窦喆 . 基于信息安全风险评估的天津移动数据网安全系统研究与建设 [D]. 北京邮电大学硕士论文,2009.09.17.
[10] 梁剑非 . 多线程端口扫描软件设计与实现 [D]. 电子科技大学硕士论文,2011.05.01.
[11] 高博 . 基于蜜罐的主动网络防御系统实现方法研究 [D]. 山东科技大学硕士论文,2009.05.01.
[12] 汤云革 . 一种信息系统安全漏洞综合分析与评估模型的研究 [D]. 四川大学硕士论文,2005.05.10.
[13] 康小军,何方白 . 基于 WinPcap 的网络吞吐量测试的设计与实现 [J]. 电子科技,2007,(11) .
[14] 逄淑文 . 试论计算机端口的侦听与扫描 [J]. 华章,2011.05.30.
[15] 彭哲 . 计算机端口简介及其应用 [J]. 高等函授学报 (自然科学版),2006,(S1) .
[16] 黄鹤 . 计算机端口与黑客防御 [J]. 科技经济市场,2006,(08) .
[17] 满萍 . 受控僵尸网络攻击实验平台的研究与实现 [D]. 北京邮电大学硕士论文,2009.02.15.
[18] 尤文坚 . 利用 Winpcap 捕获网络底层数据包的方法 [J]. 科技资讯 .2006,(25) .
[19] 李慧慧 . 一种基于多线程机制的端口扫描器的设计与实现 [D]. 太原理工大学硕士论文,2010.05.01.
[20] 刘咏 . 网络安全性能测试平台之端口扫描研究及实现 [D]. 四川大学硕士论文,2004.05.20.
[21] 权东晓 . 基于 Linux 的便携式网络测试仪的研究与实现 [D]. 西安电子科技大学硕士论文,2006.01.01.
[22] 唐宏 .BACnet 网络的安全问题及对策研究 [D]. 重庆大学硕士论文,2006.05.01.
[23] 宋诗波 .LonWorks 网络安全防范技术及解决方案研究 [D]. 重庆大学硕士论文,2007.04.01.