计算机数据库入侵检测技术应用分析

朱 波

（阳泉师范高等专科学校，山西阳泉 045000）

【摘要】数据库是目前各行业运营的重要信息保障，数据库安全关系着企业内部信息的安全，数据库安全需要通过制定数据安全管理机制来实现。当下各行业的信息逐渐繁杂，并且数据容量庞大，为了保障在当下信息化时代数据库的安全问题，就必须要不断提高数据库入侵检测技术。本文将简单探讨传统数据库的安全机制，并且根据当下的检测技术存在的问题进行总结，提出相应的解决方案，希望能够为我国各行业内部信息提供安全保障。

【关键词】数据库；入侵检测；计算机

Application Analysis of Computer Database Intrusion Detection Technology

【Abstract】 Database is an important information guarantee for the operation of various industries at present. Database security is related to the security of enterprise internal information. Database security needs to be implemented through the development of data security management mechanisms. At present, the information of various industries is gradually complicated and the data capacity is huge. In order to ensure the security of the database in the current information age, it is necessary to continuously improve the database intrusion detection technology. This article will briefly discuss the security mechanism of traditional databases, and summarize the problems existing in current detection technologies, and propose corresponding solutions, hoping to provide security guarantees for internal information in various industries in our country.

【Keywords】database; intrusion detection; computer

【中图分类号】TP309;TP311.13

引言：伴随着国家经济以及科研技术的发展，人们的日常生活愈发离不开网络信息技术，尤其是在各个行业的生产与运营过程中，更是需要网络信息技术的加持。但是网络信息技术带来的不仅仅是便捷，还有一定的风险，在网络信息技术下，人们最为关注的就是个人信息泄露问题，尤其是对于计算机数据库而言，数据库一旦受到攻击，那么其中的信息就会直接泄露出去，甚至影响个人以及企业的日常生活和生产，对经济造成严重的损失。为了加强数据库内部信息的安全，就必须要在当下的安全机制情况下，不断加强数据库入侵检测技术，以此为数据库信息的安全提供保障。

一、传统数据库安全机制

（一）用户标识与识别

在传统的数据库安全保护中，用户标识与识别是较为常见的[1]。所谓的用户标识，就是在数据库系统中，让用户自行设计一个标识，并以此标识代表自己的身份，并且根据实际要求为这个身份赋予相应的读取、写入权限。过去，大部分用户标识都由数字和字母组成，也就是所谓的用户名，而登入需要相应的密码，用户名以及密码都可以由用户自己设定。但是这样的标识方法极易被窃取，因此，需要定期更换密

码，以此保障数据库的安全。但是伴随着科研技术的发展，用户标识系统逐渐发展出虹膜标识以及指纹标识，不但有效提高了安全性，还提供了更为便捷的登入方式，但是该种标识方式并没有在各行业中得到大力推广。

为了让数据库的安全性提高，用户也可以借助计算机自带的计算功能，在用户输入用户名或者标识后，由系统向用户发送一个函数，用户对这个函数进行计算后，输入到系统之中，再由系统验证函数的计算是否正确。这样的识别方法可以有效抵御可能的外来入侵。

（二）存取控制

基于用户标识与识别技术，数据库可以根据不同的用户名，赋予不同的读取或者写入权限[2]。这样的模式不仅需要将各种信息进行分层管理，也要确保每个用户都切实拥有相应的写入能力，保障整个系统不会过于紊乱。另外，这样的安全机制，可以让“绝密文件”处于系统的最深层，即便系统被攻击也能最大化增加“绝密文件”泄露出去的时间，给相关的操作人员更多的处理时间。另外，这样的安全机制也可以基本保障数据库内信息有条理的储存，避免信息内容过于紊乱，让用户更为直接地找到自己需要的内容。

（三）数据加密处理

在部分“绝密文件”的保存中，一般采用数据加密处理，这类文件直接关系着企业财务或者国家军事机密[3]。加密处理是依循计算机技术，将部分可视化数据转换成不可识别的格式，同时，数据转换也有特殊的算法，以保障黑客入侵时不能第一时间还原数据。还有一种转换方式就是采用置换的方法，即是将数据的顺序打乱，并且进行重新排列。上述两种加密方式的安全性都不够高，但是两者相结合就拥有更高的安全性。虽然如此，这两种方法的加密过程耗时较长，在恢复文件时也较为困难，占用的系统空间也更大。

二、计算机数据库存在的安全问题和入侵检测技术功能概述

（一）数据库存在的安全问题

随着当下网络信息技术以及计算机技术的发展，目前人们的生活以及各行业的生产已经离不开计算机网络技术，并且在计算机网络技术的加持下，人们的生活水平得到了提高，各个行业的生产能力以及经济效益都得到了提高。但是，网络信息技术带来的也并非只有正面的影响，信息安全问题一直存在于网络信息技术中心，尤其是在计算机数据库中，大部分企业的数据库包含着大量的企业内部信息，一旦遭受攻击，极易导致企业的核心技术或者信息失窃，导致企业的经济效益以及运营受到影响。另外，一些网络病毒的传播也会破坏数据库的安全，导致个人信息以及企业信息泄露。

（二）入侵检测技术功能

计算机数据库入侵检测技术主要是计算机利用相应的算法，对登入的用户以及病毒进行识别、处理，主要服务于数据库内部信息的安全，抵御外来入侵以及内部非授权的行为，采用计算机数据库入侵检测技术可以为数据库中的信息安全提供保障，并且及时发现网络系统中可能存在的病毒。一般的计算机入侵检测系统主要包括如图 1 所示。

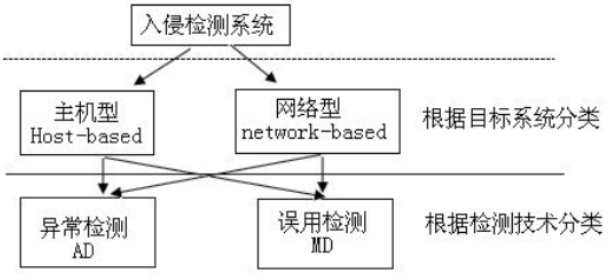

图 1 入侵检测系统

1. 误用检测技术

误用检测技术是在数据库运行过程中，对已知的病毒攻击方式以及入侵活动进行检测[4]。当病毒或者入侵活动发生时，计算机网络将自动把病毒以及入侵活动编译成可视化活动模型，一旦病毒或者入侵活动

对系统展开攻击，那么误用检测系统就会自动对病毒系统或者攻击者的入侵方式进行删除。

但是这种方法是基于已知病毒和入侵活动的，对于部分新型病毒以及未知的入侵活动并不能起到良好的防护。其主要原因在于误用检测技术的运行模式，其检测方法以及算法主要是将入侵的病毒以及活动与已知的病毒和活动进行对比，并且搜索出相应的应对方法，对于新型病毒，该种检测方法则不能直接认知其攻击性以及破坏性。

2. 异常检测技术

目前，异常检测技术的应用较为广泛，该种技术主要针对计算机网络中运行的病毒以及入侵活动都是不同于系统用户的正常活动，属于异常行为，在进行识别后直接进行攻击。该种检测系统会总结计算机的日常运行以及用户活动，并且以此建立一套计算机运行活动规律，在新活动出现且不符合该规律时，就会直接向该活动进行攻击。该种检测方式能够大大提高对病毒的攻击效率以及防护质量，能够为计算机提供更高的安全防护。

图 2 计算机数据库入侵检测技术存在的问题

三、计算机数据库入侵检测技术存在的问题

计算机网络相关技术的不断完善，对数据库的攻击手段也越来越多，在当下的数据库入侵检测技术中，仍然存在一定的不足，其中的问题如图 2 所示。

（一）无法保障准确率

目前，入侵检测技术在实际应用的情况下，经常会出现误报、不报的情况，误报多产生于异常检测技术中心[5]。在用户进行安全且不符合计算机日常运行规律的活动时，就会产生误报，导致用户信息丢失；或者是部分新型病毒，依循计算机日常运行规律对数据库进行攻击，导致该种检测技术难以识别。而不报的情况则多发生于误用检测技术中，在检测过程中，往往会因为缺少相应的病毒信息，无法直接识别病毒的攻击性，导致数据库受到攻击。

（二）防御能力较差

对于大部分计算机数据库的入侵检测技术而言，最为重要的就是其防护能力[6]。但是，目前的大部分检测技术的防御能力都较差，虽然可以直接识别病毒以及入侵者的攻击活动，但是却无法直接进行攻击或者删除。出现这种情况的主要原因是各检测技术过于重视检测工作，而忽略了系统的防御能力，在病毒以及外来入侵展开攻击活动时，往往能够第一时间向用户以及计算机系统进行报警，但是系统本身不具备较强的防御能力，导致系统在遭到攻击后的一段时间内都无法得到良好的处理，导致数据库中的信息丢失或者被窃取。

（三）检测效率低下

计算机数据库入侵检测系统往往都是在系统遭到攻击后，再进行检测，这种检测不具备时效性。甚至于部分新型病毒以及外来入侵者都会提前做好相应的隐蔽工作，导致检测系统无法第一时间识别病毒以及外来入侵者的攻击性，第一时间做出反应，难以对相应的攻击行为做出有效的判断。不仅如此，由于计算机系统内部的计算量不断增加，也会直接导致计算机入侵检测效率降低。

四、计算机数据库入侵检测技术的应用分析

计算机数据库入侵检测技术属于一种新型技术，该技术主要服务于数据库的安全，对数据库系统进行自动防护。对于当下各行业的生产以及日常运营而言，数据库的安全就是企业运行的命脉，数据库内部信息将直接关系到各行各业的未来发展以及经济效益。而入侵检测技术，就是在外来入侵者对数据库进行攻击时，第一时间识别恶意系统，对恶意

系统进行攻击的技术。上文提到，目前主要应用的入侵检测技术主要有两种，分别为误用检测技术以及异常检测两种，然而这两种检测技术仍然存在一定的问题，为了解决这些问题，就必须要不断加强这两种技术的检测能力。

（一）数据挖掘方法

所谓的数据挖掘方法，就是数据库入侵检测系统通过对用户的行为特征进行分析，提高计算机数据库的安全管理。该方法在运行的过程中，会不断挖掘并总结数据库的运行模式，并且对用户的登入规律以及用户权限进行归纳，并且将数据库中的信息进行相应的排序，分析用户登入以及操作规律，构建一个独立的运行体系，在用户登入时，分辨登入活动是否符合日常运行规律。

（二）入侵容忍检测技术

入侵容忍技术能够有效地阻止病毒对数据库的入侵，也能分辨出外来入侵者的非法活动。在遭受攻击后，入侵容忍系统也能第一时间对数据库进行恢复，其主要工作流程如图 3 所示。

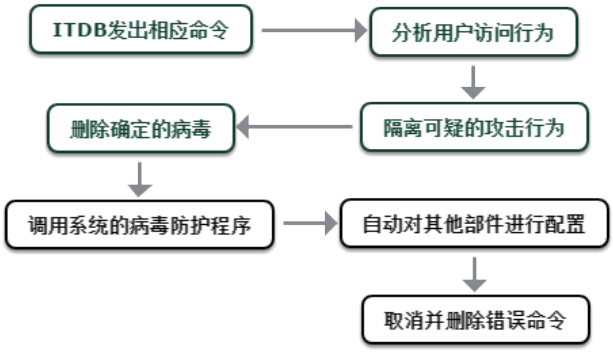

图 3 入侵容忍技术的工作流程

使用入侵容忍技术能够对数据库管理系统实现有效的自适应功能，在遭受攻击后，第一时间对病毒以及外来入侵者进行攻击，并且对受到破坏的信息进行恢复。入侵容忍技术能够对用户的访问以及读取行为进行控制和分析，根据用户访问表现总结其可能存在的异常行为，及时检测出可能存在的攻击行为，并采取相应的处理措施。

（三）应用入侵检测技术

对于数据库系统数据进行调用的过程中，需要对数据库中的信息进行相应的控制和保护。应用入侵检测技术就可以在数据信息进行调用过程中，对用户以及读取活动进行分析。该种技术主要面临多种形式的网络病毒，即便拥有相应的隐蔽手段的病毒，也能在较短时间内识别出来，不同于其他的入侵检测技术，该检测技术能够对数据库系统的相关命令进行调用，在活动产生时，利用数据库系统自身的动作完成对病毒的防护以及清除。

五、结束语

目前，针对计算机数据库安全管理和相关的入侵检测技术仍然存在一定的进步空间，想要提高计算机数据库入侵检测技术的准确度以及检测效率，就必须要不断加强检测系统的完善，以此保障各行业数据库中的信息安全。

参考文献：

[1] 秦程 . 计算机数据库入侵检测技术的应用 [J]. 电子技术与软件工程 , 2017, 03:222-223.

[2] 邹佳祥 . 计算机数据库入侵检测技术 [J]. 中国管理信息化 , 2017, 2003:124-125.

[3] 谷潇 . 关于计算机数据库入侵检测技术应用分析 [J]. 电子测试 , 2017, Z1:69-70.

[4] 李东利 . 探索入侵检测技术在计算机数据库的应用 [J]. 数字技术与应用 , 2019, 3703:193+195.

[5] 王建国 . 计算机数据库的入侵检测技术和安全管理 [J]. 电子元器件与信息技术 , 2019, 04:37-40.

[6] 梁铭 . 计算机数据库入侵检测技术应用探索 [J]. 信息与电脑（理论版）, 2019, 3123:111-112+115.