数据库入侵检测研究综述*)

钟 勇 秦小麟

(南京航空航天大学信息科学与技术学院 南京210016)

摘 要 网络的发展使数据库面临的安全形势更加复杂,而传统的以预防为中心的数据库安全机制存在不足,在此基础上总结了数据库入侵检测技术的发展现状,指出了在此方面进行研究的难点和需要解决的关键问题,最后对今后的发展趋势进行了展望。

关键词 数据库入侵检测,数据库安全,入侵容忍

A Survey on the Database Intrusion Detection

ZHONG Yong QIN Xiao-Lin

(Information Science and Technology Institute, Nanjing University of Aeronautics and Astronautics, Nanjing 210016)

Abstract With the development of network, database faces more serious security situation. Traditional prevention-centric security is not enough. Based on the problem the paper summaries the status of database intrusion detection techniques and points out the difficulties of research and the existing problems that need to be solved. Finally, the future direction in this field is discussed.

Keywords Database intrusion detection, Database security, Intrusion tolerant

传统的数据库安全机制以身份认证和存取控制为重点,身份认证和存取控制主要着眼于对外部用户的身份和权限约束的检查以确定用户或其操作的合法性,身份认证和存取控制是一种以预防为中心的被动安全机制,无法满足日益增长的对数据库安全的需要,特别是计算机网络化的发展,使数据库面临着前所未有的安全困境,数据库应该具有更加主动、积极的安全机制才能更加有效地防止网络互联给数据库带来的层出不穷的攻击。因此,近年来对主动型数据库安全机制的研究受到广泛的重视。

1 数据库的安全状况以及传统安全机制的不足

当前,信息已成为社会发展的重要战略资源,国际上围绕信息的获取、使用和控制的斗争愈演愈烈,信息安全成为保障经济健康发展、维护国家安全和社会稳定的一个焦点。随着Internet及计算机应用的日益普及,计算机信息系统成为社会生活和工农业发展中不可缺少的成分。一些关键的信息系统比如交通运输、金融、电力、国防等行业的信息系统是如此重要以至于这些系统的失效将给社会带来极大的损失,信息安全已经提高到一个前所未有的高度。信息安全保障能力是21世纪综合国力、经济竞争实力和生存能力的象征,是未来国际竞争的基础。

网络系统、操作系统和数据库管理系统(DBMS)是信息系统的支撑平台,网络主要解决信息的传输、操作系统主要解决信息的存储与资料的管理,而数据库管理系统主要解决信息的有效存取,这三者的安全性直接影响到整个信息系统的安全。目前人们把信息安全的重点放在网络安全上,对操作系统和数据库安全的研究远不如对网络安全的研究。而实际上在信息系统的整体安全中,数据库往往成为最吸引攻击者的目标。这是因为作为信息系统关键部件的数据库如今有着越来越重要的作用,例如,今天的数据库产品已经成为具有数十亿美元产值的工业,据统计,在1995年硬件服务器销售量的32%是由数据库产品的销售所带动的,而到达2000年这一比例达到39%[1]。数据库中往往保存着对公司或组织极为重要的数据,其重要性和价值对攻击者有很大的吸引力,受到蓄意攻击的可能性增加。同时,数据库系统本身的弱点也使其成为易受攻击的目标,由于数据库的数据经常需要更新以及其它众多的操作活动,再加上为了适应更新的需要许多数据库提供的优化接口,都可能受到攻击者的利用。而另一方面,网络化也使数据库面临着日趋严重的安全形势。网络化使数据库的使用不受时空的限制,延伸了受到攻击的时间和空间。在数据库受到攻击的可能性、空间和时间都大大增加的情况下,传统的以身份认证和存取控制为重点的数据库安全机制越来越无法满足安全需要,这主要体现在以下两个方面。

一方面,传统的数据库安全机制重点在于预防,着眼于对外部用户的身份和权限约束的检查,来保证用户操作的合法性,防止用户执行未授权的操作。然而,以身份认证和存取控制为主的数据库安全机制存在一定的限制。首先,经验显示我们不可能百分之百地预防所有的安全问题,黑客们常常使人吃惊,因为他们总能发现新的方法闯入或干涉我们的系统[2]。其次,对于合法用户特别是系统管理员的权限滥用,以预防为主的安全机制常常显得无能为力。而据统计计算机安全的主要威胁来自内部滥用而不是入侵,这些内部滥用者往往具有合法的身份认证和授权[3]。而对于一些来自网络的攻击,攻击者往往能窃取到合法的身份或权限,如利用密码嗅探(password sniffing)攻击者可能获得合法的用户账号和密码,利用会话骑劫(session hijacking)的攻击者可能伪装成合法的用

*)基金项目:航空科学基金(编号:02F52033)资助项目。钟 勇 博士研究生,讲师,主要研究方向数据库安全、网络安全。秦小麟 教授,博士生导师,主要研究方向安全数据库、空间数据库、时空数据库、GIS等。

户。

另一方面，数据的保密性，完整性和可用性是数据库安全研究领域主要关心的问题[4]，而身份认证和存取控制主要着眼于数据库的保密性以及某些商业完整性（如 RBAC 中对责权分离和组织体系结构的模拟[5]），对数据本身的完整性和可利用较少涉及，而对于数据库安全来说，数据的完整性和可利用性具有和保密性同等地位的重要性，如在信息战（Information Warfare IW）的条件下，信息战的防卫要求采取任何手段防止攻击。但是在现有的条件下我们必须承认防止信息攻击的手段是不充分的，在某种程度上不可避免，总有攻击能够取得成功，因此对攻击的识别和受到攻击以后恢复手段是必要的[2]。

2 数据库入侵检测的必要性

入侵检测通过对运行系统的状态和活动进行检测，分析出非授权的访问和恶意行为，发现入侵行为和企图，为入侵防范提供有效的手段。入侵检测已成为信息安全中的一个重要研究课题，在多年的研究中，入侵检测技术取得了长足的进步。例如在美国国防高级研究计划局（DARPA）98 年的入侵检测评估报告[6]中指出最先进的误用检测技术能达到 70% 的检测率，在文[7]中对欺骗性信用卡事务检测的结果也显示可以达到 80% 的检测率和少于 17% 的误警率。虽然入侵检测的研究取得了不少的成果，但这些研究大多集中在对网络和操作系统的入侵检测上[8,9]，对数据库的入侵检测则较少涉及。

对数据库来说，仅仅依靠工作在文件和系统命令级的底层操作系统和网络入侵检测系统无法保证检测的效率和精度，比如 SQL 注入（SQL injection）技术是一种入侵者使用精心伪造恶意 SQL 语句来获取用户特权的方法，SQL 注入常常利用数据库应用程序的漏洞，这种入侵是操作系统和网络入侵检测系统所难以检测的。现有的操作系统和网络入侵检测系统主要有两种模式，一是通过检测用户行为是否偏离正常模式的异常检测（Anomaly Detection）方法，一种是通过检测用户行为是否符合某个已知攻击模式的误用检测方法（Misuse Detection）方法。而据统计，入侵者往往来自于系统内部，内部入侵者至少构成了入侵者的 50%[10]。由于内部入侵者往往具有合法的用户身份，他们往往不会严重地偏离预期的行为，也不会执行特定的入侵行为[10]，因此，对他们的非法行为往往很难检测。而在数据库中的数据具有自己的结构和语义，数据库用户有自己的独特行为，通过数据库入侵检测可以弥补操作系统和网络入侵检测的不足，提高检测的准确度和有效性。

3 现存的数据库入侵检测技术

基于主机和网络的入侵检测系统的一些研究思想和成果可以应用到数据库入侵检测中来，但数据库具有自己的结构和语义，数据库入侵检测应能够在更细的粒度上检测用户的行为，但也由于数据库结构的复杂性，使数据库入侵检测具有比主机和网络入侵检测更为复杂的内容和难点。

3.1 对数据推理的检测

对数据推理的检测可以看作是一种早期的数据库滥用检测。数据推理指的是用户在不存取某些数据的情况下也能推断出这些数据，如在多级安全数据库中用户利用低密级数据或外部知识推理出某些高密级数据，使用推理进攻的往往是具有某些合法权限的内部滥用者。对推理的检测可以在数据库的设计阶段或运行阶段。在设计阶段，主要通过对数据库模式的分析以找到推理渠道，比如利用属性的函数依赖图查找第二条路径的方法，如果两个属性之间存在两条路径且这两条路径是不同的分类密级就有可能发生推理进攻[11]，对查找到的推理渠道，可以通过提升路径密级[12]的方法或重新设计数据库模式和分级属性[13]来避免推理。使用数据库模式分析推理在数据库设计阶段较为有效，但也存在两个缺点：一是数据库模式不能捕获数据库实例中的所有依赖关系，二是数据库模式中存在的推理路径不一定就会导致推理行为的发生。Hinke 等使用基数联系，Hale 等使用不精确和模糊关系，以及存在其它一些数据库设计阶段的检测方法等。在数据库运行阶段，通过检测数据库事务以确定这些事务是否会导致非法推理，如果导致非法推理则对该事务做相应的调整或取消。LDV（Lock Data Views）项目使用分级约束来限制数据推理，当用户查询提交后，其查询结果首先按照分级约束升级然后再返回给用户。文[14]使用查询修改的方法，查询提交前首先检查该查询是否会导致非法推理，如果是则修改查询使其不能导致非法推理。Yip[15]提出了一个数据级的推理检测方法，他认为利用数据库中的数据本身可以检测出更多的推理，提出了能用于推理进攻的五种关系并提出了一个基于规则的方法以方便与检测系统的集成，在进一步研究中，Yip 扩展了这些关系并对其应用作了讨论。数据库运行阶段的推理检测需要保存用户的查询和返回的元组，因而代价较高，而且对某些推理的检测需要保持用户查询的历史信息，这可能易招致某些否认服务（denial of service）的进攻。

3.2 对存储篡改的检测

对数据库的存储篡改（storage jamming）是一种恶意修改数据库中的存储数据以降低数据质量的行为，存储篡改的目的是以错误或低质量数据误导和妨碍对手的行为，存储篡改是一种内部滥用行为。

McDermott 和 Goldschlag[16,17]在研究检测存储篡改的方法中提出使用检测物（detection object）的方法，检测物是一种检测篡改数据的恶意行为的抽象机制，在数据库中，检测物一般是不被正常用户和应用所使用但篡改者又无法将其与正常数据区分开的伪造数据，如果发现检测物不在正常或可预期的状态则表示可能发生了数据篡改行为。

对防止和检测企图绕过数据库管理系统在磁盘级破坏数据的入侵者，加密和签名是主要的安全机制，Maheshwari[18]通过将数据库加密和在小块可信存储中保存的散列验证数据库正确性的方法来检测不可信程序对数据库的非法读取和修改。对于一般的签名机制，入侵者可能使用旧的磁盘块映像来替换现有的数据而不被检测到，Barbara 等[19]提出了一个通过两级校验码来检测绕过数据库管理系统在磁盘级破坏数据的入侵者，通过将两级签名连接到数据库的数据项从而形成内部的追踪机制，入侵者的非法更新如果想不被检测到，必须执行大量实际上无法完成的额外块复制工作，Barbara 的方法可以有效地检测到块映像替换等入侵手段。

3.3 基于数据挖掘的检测方法

数据挖掘指从存储数据中识别出隐藏的固定模式或异常现象的高级处理过程，由于数据挖掘技术能够发现隐藏在数据背后的用户模式和特征，因此，在基于主机和网络的入侵检测中，基于数据挖掘的检测方法是重要的研究课题，也存在着来自统计、模式识别、机器学习等多个领域的数据挖掘算法。

Christina 在其原型系统 DEMIDS 中提出使用用户轮廓(user profiling)检测数据库用户的误用行为[20]，用户轮廓是在关系数据库中用户和角色的典型行为，DEMIDS 重点在于检测合法用户的滥用行为，DEMIDS 使用频繁项(frequent itemsets)来表示用户的正常行为，频繁项是用户参考的属性及其值，频繁项是按照数据结构、模式语义(主键、外键依赖)和用户日志使用一定的挖掘算法挖掘出来的。在挖掘用户的频繁项算法中，DEMIDS 使用了距离的概念来测量属性间的紧密度(出现在同一操作语句中的可能性)，距离的度量使用了用户查询语句中的主键和外键的函数依赖关系。Christina 进一步改进了 DEMIDS 的算法[21]，并将可以体现特定领域知识的概念体系应用到用户轮廓的挖掘中，从而可以形成不同抽象级和粒度的用户轮廓，并使用兴趣度(Interestingness Measure)来发现用户的行为模式，一个数据项 I 的兴趣度 $M(I)$ 由其在日志会话中的支持度 $Sup(I)$，在概念体系中的深度 $Depth(I)$，距离 $Dist(I)$，数据项的大小 $Size(I)$ 四个变量组成，一个简单的计算兴趣度的公式可表示为

$$M(I) := \frac{Sup(I)+Depth(I)+1-Dist(I)+Size(I)}{4} \in R[0,1]$$

更复杂的计算可以在这四个变量前加入不同的权值。在 Christina 的数据库误用检测算法中，使用了数据库数据的数据结构、模式语义和领域知识，但也存在一定的问题，Christina 的方法假设合法的用户使用数据库的方式有一定程度的一致性，如果这个假设不成立或者检测阈值配置不合适将会导致较高的误警率(false positive rate)

Stolfo[22]在研究信用卡欺骗检测中使用元学习(meta-learning)的方法来进行分布式事务模式挖掘，元学习是一种用于处理从大型分布式数据库中计算全局分类器(classifier)的技术，元学习首先在分布式数据库中使用学习程序并行的计算独立的分类器，然后再使用另一个学习程序在这些分类器上集成元分类器。在使用元学习得出异常或偏差事务模型后，使用模式指导的推理系统来检测欺骗事务，该算法来源于美国哥伦比亚大学完成的基于 Java 代理的元学习项目 JAM (java Agents for Meta-Learning)。

3.4 基于数据库事务级的入侵检测方法

数据库具有自己独特的事务处理机制和 SQL 语言查询，对用户使用 SQL 语句的模式进行检测是数据库入侵检测的一项重要内容。指印(fingerprints)技术[23,24]是一种基于 SQL 语句的入侵检测方法，指印是从合法事务中的 SQL 语句中推出的正则表达式，它代表用户正常的行为，用户的事务语句如果偏离指印集则表示可能的异常行为。指印技术特别适应类似于对互联网上的数据库入侵检测，比如 SQL 语句注入，因为在这些应用中往往使用数据库应用来查询数据库，而这些应用只通过一定接口使用固定的几种查询格式，不允许用户自构查询，在这种情况下即使事务较大用户较多误警率也较低。

3.5 基于数据库应用语义的检测方法

在许多场合中，独立于应用语义对数据库事务或用户进行检测并不足以识别用户的异常行为，如某个会计突然将自己每月工资增加一万元，在正常情况下这是不可能的，但对建立在独立于应用语义上的检测方法如对表存取统计、数据文件存取统计、会话统计或上述的各种检测方法并不能发现异常，这种异常检测只能建立在数据库的应用语义上。

Robert S. Sielken[10]提出在入侵检测中使用应用语义的应用入侵检测概念并列举了基于应用语义约束和统计的例子。对应用语义，例如医生病人之间的约束，医生只能查看他所治疗病人的病历，医生开出的处方只能是他专业范围内的，某种病人不能吃某种食品，儿童病人的年龄须小于某岁等，应用语义约束可以构成基于规则的异常检测系统；对应用语义统计方法，例如病人服某种药的次数和剂量应与其它相同的处方之间有一定的相似处，病人购药的订单应大多数发生在白天上班时间等，这些统计可构成基于统计的异常检测系统。数据库中应用语义的独特性和精确性可以有效提高入侵检测的准确性和粒度。

4 数据库入侵检测系统的实现方法

数据库本身是一个复杂的结构，从数据存储来说，有从数据文件、表、字段到元组等的不同粒度的存储单位；从数据库活动来说，有从系统调用层、进程、事务层、会话层到应用层等不同层面的活动级，因此，要设计一个完善的数据库入侵检测系统，必须面对几个问题：首先，要达到检测的精确度必须使用多层的入侵检测方法，不同活动级的检测要能合成在一起，由于数据库活动的多层次性，单一性的检测往往难以达到良好的效果。其次，数据库入侵检测系统不可能在数据库活动的所有层次上进行检测，必须能与底层操作系统和网络检测系统集成或数据交换。例如数据库入侵检测系统可能在事务级检测到入侵但可能无法识别用户的真正身份，而操作系统入侵检测系统可能识别出用户的身份，网络入侵检测系统可能判断入侵者的地址、主机。反之，操作系统入侵检测系统可能发现 DBMS 活动异常，例如突然产生大量日志或文件，但无法判断是正常还是异常而必须依赖数据库检测系统对数据库自身结构和语义的检测。最后，数据库入侵检测系统应能够捕获和使用应用语义，如 3.5 节所示，一些更细微的滥用或入侵行为的检测只能建立在数据库的应用语义上。

Peng Liu[25,26]在入侵容忍数据库的研究中建议使用一种灵活的子弹夹(cartridge)式的检测器，这种检测器提供接口让用户自己选择或提供新的子弹，这里的子弹包括检测算法、应用语义提取算法、基于应用语义的适应性政策。通过这种方式，检测器可以满足不同应用的入侵检测需要。检测器用基于规则的框架系统来插入检测算法和捕获应用语义，一个入侵检测规则分为 4 个部分：(1)事件。由于特定事务如插入、更新或删除数据库对象引起的数据库事件。(2)优先级。每条规则都安排一个优先级以方便在多个规则都满足时选取合适的规则。(3)警报。当条件满足时应该报告的怀疑级。(4)条件。条件是多个谓词的集合。为了能插入各种检测算法，捕获应用语义，条件表示为：$C = P_1 \wedge P_2 \wedge \cdots \wedge P_n$，$P_i(1 \leqslant i \leqslant n)$ 是返回正确与否的函数，$P_i = function(V_1, V_2, \cdots, V_n)$。$V_i$ 是任何 P_i 能接受的变量。通过这种方式，只要把任何现存的检测算法表示成符合函数规则的形式都可以插入到该系统中，如图 1 所示，通过将统计算法作为条件函数，实现了既支持基于规则的检测算法，也支持基于统计的检测算法。

基于规则示例 1：工资的增加额度不能超过 10000 元，否则异常度为 90
Event：Update(工资表)
Priority：80
condition：SharpIncrease(工资表，10000)
Alarm：90
基于统计示例 2：本周出纳的次数不能超过周平均次数为 10 倍，否则异常度为 70
Event：Insert(出纳表)
Priority：70

Condition:Over AveByweek(出纳表,10)
Alarm:70
函数示例:
SharpIncrease(工资表,threshold){
Return(工资表.工资.new-工资表.工资.old>threshold)
}

图1 入侵检测规则示例

结束语 现存的数据库安全机制无法做到防止所有的非法攻击,以预防为主的安全机制是不够的,一些关键部门如交通、银行等的信息系统在社会中占有非常重要的地位,它们可能需要提供一周七天、一天二十四小时的不间断服务,这些系统需要有较强的生存能力,比如在系统出错或受到攻击的情况下提供服务的能力。因此,对这些关键系统来说,以错误容忍为中心的主动保护机制对他们的安全来说有更为重要的意义。信息系统的可生存性代表系统在受到攻击、系统故障、意外事故的情况下能及时完成任务的能力[27]。可生存性要求系统在发生诸如硬件失效、软件错误、操作失误或恶意攻击时仍旧能提供一部分基本服务或替代服务。信息系统的可生存能力是一种以错误容忍为中心的保护机制,是系统对错误的可适应性。作为信息系统的重要组成部分,数据库的可生存能力也正在成为研究的热点之一。提高数据库的可生存性重点之一是提高数据库的入侵(主动错误)容忍能力,数据库的入侵容忍指的是数据库在受到攻击的情况下继续提供基本服务的能力[1],入侵容忍数据库扩展了传统数据库的安全能力,使之能够在受到攻击情况下有更强的生存和服务能力,将成为未来数据库安全研究的重点。而在入侵容忍数据库系统中,绝大多数入侵容忍操作是由入侵检测器所触发,很大程度上,入侵容忍数据库的效率依赖于入侵检测的能力,因此,对数据库入侵检测的研究在入侵容忍数据库的研究中有重要意义。

但由于数据库结构的复杂性,相对于网络和操作系统入侵检测,数据库入侵检测技术面临着更多的研究难点,迄今为止,数据库检测技术还处在研究阶段。完善的实用系统尚未见到。现今对数据库检测技术的研究远远不够,对数据库的入侵检测算法和应用结构还需要有深入的研究。

参考文献

1 Liu P. Architectures for Intrusion Tolerant Database Systems. In:Proc. of 18th Annual Computer Security Applications Conf. Las Vegas, Nevada,Dec. 2002

2 Ammann P,Jajodia S,McCollum C D, Blaustein B T. Surviving information warfare attacks on databases. In:Proc. of the IEEE Symposium on Security and Privacy,Oakland, CA, May 1997. 164～174

3 Carter,Katz. Computer crime: an emerging challenge for law enforcement. FBI Law Enforcement Bulletin,Dec. 1996

4 Castano S,Fugini M G,Martella G,Samarati P. Database Security. Addison-Wesley, 1995

5 Ferraiolo D,Sandhu R,Gavrila S,Kuhn D,Chandramouli R. Proposed NIST Standard for Role -Based Access Control. ACM TISSEC,2001,4(3)

6 Lippmann R,et al. Evaluating intrusion detection systems: The 1998 darpa off-line intrusion detection evaluation. In:Proc. of 2000 DARPA Information Survivability Conference and Exposition, Jan. 2000

7 Stolfo S,Fan D,Lee W. Credit card fraud detection using meta-learning: Issues and initial results. In:Proc. AAAI Workshop on AI Approaches to Fraud Detection and Risk Management, 1997

8 Axelsson S. Intrusion Detection Systems: A Survey and Taxonomy, Chalmers University of Technology, Dept. of Computer Engineering, Go¨teborg, Sweden:[Technical Report 99-15]. 2000

9 Allen J,et al. State of the Practice of Intrusion Detection Technologies:[Technical Report CMU/SEI-99-TR-028]. ESC-99-028, Carnegie Mellon University, Software Engineering Institute, Jan. 2000

10 Sielken R S. Application intrusion detection:[Technical Report CS-99-17]. Department of Computer Science, University of Virginia, June 1999

11 Qian X,et al. Detection and elimination of inference channels in multilevel relational database systems. In:Proc. of the 1993 IEEE Symposium on Research in Security and Privacy,1993. 196～205

12 Dawson S,et al. Maximizing Sharing of Protected Information. Journal of Computer and System Science, 2002, 64(3): 496～541

13 Hinke T H,Delugach H,Wolf R. A framework for inference-directed data mining. In: Proc. Tenth IFIP Working Conf. Database Security, Como, Italy, July 1996

14 Thuraisingham, Bhavani M. Security Checking in Relational Database Management Systems Augmented with Inference Engines. Computers and Security,1987,6:479～492

15 Yip R,Levitt K. Data Level Inference Detection in Database Systems. In:Proc. of the 11th IEEE Computer Security Foundations Workshop, Rockport, Massachusetts, June 1998. 179～189

16 McDermott J,Goldschlag D. Storage jamming. In:D. Spooner, S. Demurjian,J. Dobson, eds. Database Security IX: Status and Prospects,Chapman & Hall, London, 1996. 365～381

17 McDermott J,Goldschlag D. Towards a model of storage jamming. In: Proc. of the IEEE Computer Security Foundations Workshop,Kenmare, Ire-land, June 1996. 176～185

18 Maheshwari U,Vingralek R, Shapiro W. How to build a trusted database system on untrusted storage. In:Proc. of 4th Symposium on Operating System Design and Implementation, San Diego, CA, Oct. 2000

19 Barbara D,Goel R,Jajodia S. Using checksums to detect data corruption. In: Proc. of the 2000 Intl. Conf. on Extending Data Base Technology, Mar 2000

20 Chung C Y,Gertz M, Levitt K. DEMIDS: A Misuse Detection System for Database Systems. In:The Third Annual IFIP TC-11 WG 11.5 Working Conf. on Integrity and Internal Control in Information Systems, 1999

21 Chung C Y, Gertz M, Levitt K. Discovery of Multi-Level Security Policies. In:The Fourteenth Annual IFIP WG 11.3 Working Conf. on Database Security, 2000

22 Stolfo S,Fan D,Lee W. Credit card fraud detection using meta-learning: Issues and initial results. In:Proc. AAAI Workshop on AI Approaches to Fraud Detection and Risk Management, 1997

23 Low W L, Lee S Y,Teoh P. DIDAFIT: Detecting Intrusions in Databases Through Fingerprinting Transactions. In: Proc. of the 4th Intl. Conf. on Enterprise Information Systems(ICEIS). 2002. 264, 265, 267,269

24 Lee S Y,Low W L, Wong P R. Learning Fingerprints For A Database Intrusion Detection System. In: 7th European Symposium on Research in Computer Security(ESORICS 2002)

25 Liu P,et al. The Design and Implementation of an Intrusion Tolerant Database System:[Technical Report, PSU-S2-2002-003]. Penn State Cyber Security Group, 2002

26 Ingsriswang S,Liu P. AAID: An Application Aware Transaction-Level Database Intrusion Detection System:[Technical Report]. University of Baltimore -BC, Mar. 2001

27 ELLISON, Rl, ET AL. Survivability: Protecting your critical systems. IEEE Internet Computing,1999,3(6):55～63