数据库管理系统的入侵容忍技术研究进展*)

陈伟鹤 殷新春 谢 立
(南京大学计算机软件新技术国家重点实验室 南京 210093)
(南京大学计算机科学与技术系 南京 210093)

摘 要 传统数据库安全的研究重点是如何防止非授权用户对数据库的恶意干扰和破坏,事实上根本无法阻止所有的攻击。因此,在信息战语义下,更为紧迫的是如何找到有效的措施来缓解或消除恶意用户的攻击,而入侵容忍(即抗恶意用户攻击和攻击后DBMS的恢复能力)是数据库安全最为重要的。本文概述了信息战中数据库入侵容忍技术研究的现状,指出了目前存在的问题和未来的研究方向。

关键词 信息战,数据库安全,入侵容忍,恶意用户,可信恢复

The State of the Art of Database Intrusion Tolerance Research

CHEN Wei-He YIN Xin-Chun XIE Li
(State Key Laboratory for Novel software, Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract Traditional database security focuses on how to prevent the unauthorized users from stealing data and making damage to data. It can not do anything to mitigate the damage caused by malicious authorized users. Especially in information warfare context, it is more urgent to find effective measures to alleviate or eliminate the damage caused by malicious authorized users. Information Warfare has been one new challenge of Database Security research. In information warfare context, Database Intrusion Tolerance, the ability of anti-malicious authorized users attacks and post-attacks recovery of DBMS, is an emergent principle of database security. It can enhance database survivability. In this paper, we survey the state of the art of database intrusion tolerance in information warfare and present some open problems and possible future research directions.

Keywords Information warfare, Database security, Intrusion tolerance, Malicious authorized users, Trusted recover

1 信息战语义下的数据库安全研究

信息战[1,2]语义下的数据库安全与传统意义上的数据库安全存在很大区别。传统数据库安全的研究重点是探讨如何通过访问控制、身份认证等安全预防机制防止非授权用户对数据库的恶意干扰和破坏,同时为授权用户提供安全、及时、可靠的数据服务。而信息战语义下的数据库安全不但要求采取传统意义上的数据库安全措施尽量阻止对系统的攻击,更重要的是,它认为这些传统的数据库安全措施无法阻止所有的攻击,最终总会有一些恶意攻击取得一定程度的成功,对系统造成一些破坏。因此,信息战语义下的数据库安全研究的重点是在数据库管理系统遭受到恶意攻击时,能够从被攻击的状态中恢复,同时能够保留尽可能多的未受恶意攻击影响的其它授权用户在系统受攻击期间的工作结果,并且能够不间断地提供可靠服务。20世纪90年代后期,以Graubart和Jajodia为代表的美国信息安全专家和数据库专家对信息战语义下的数据库安全进行了研究[3,4],重新定义了信息战语义下对敌人能力的假设,敌人的攻击手法以及对数据库安全的特殊要求。

在传统的信息安全研究[5,6]中,认为没有获得系统授权的用户的所有行为都是违背系统安全策略的,应该禁止;而系统授权用户的符合授权的行为都是不会造成系统破坏的行为。但是这个假定在信息战语义下是不成立的。这是因为,在信息战环境下必须考虑恶意授权用户问题。由于信息系统总是存在着授权用户的,因此存在恶意授权用户的可能性是无法否认的。例如,外部攻击者可以通过某些攻击手段获取合法用户的身份,得到相应的授权。系统内部的授权用户也可能出于经济、宗教信仰、政治等原因而成为恶意攻击者。这些都是恶意授权用户。仅仅从行为本身是否符合系统安全策略是不能区别恶意授权用户的行为和普通授权用户的行为的。在恶意授权用户被发现之前,他们的某些"符合授权"的行为极可能对系统数据造成破坏。对于系统授权用户的破坏行为(即内部安全威胁[6~8]),现有的基于预防策略的系统安全机制无能为力。这也就是为什么信息战语义下的数据库安全必须考虑某些恶意攻击能够取得一定程度成功的原因。

尤其值得注意的是,在信息战语义下,要求数据库系统在消除恶意攻击对数据库的影响时,必须能够保留尽可能多的非恶意操作的结果,提高系统的可用性,并且可以在对数据库系统进行即时(on-the-fly)恢复时响应用户新的数据处理要求,保持连续服务能力。这些是传统数据库安全研究中没有涉及到的。强调保持连续服务能力,是因为在战争情况下,如果数据库恢复必须离线进行,那么就很可能意味着己方的战斗运作暂停,进入被动挨打状态,这在实际情况下是不允许的,因此必须在遭受攻击的情况下进行即时恢复,而且在恢复的

*)本文得到国家"863"高技术(NO:2001AA144010)经费资助。**陈伟鹤** 博士研究生,主要研究方向为信息安全和分布式系统。**殷新春** 博士研究生,主要研究方向为信息安全和分布式系统。**谢 立** 教授,博士生导师,主要研究领域为信息安全和分布与并行计算机系统。

同时能够继续提供数据服务。

美国国防部DARPA[6]和MITRE[3]公司从20世纪90年代后期开始对信息战语义下的数据库安全研究这一新兴领域的资助。数据库管理系统的入侵容忍技术[3,4]正是在这一背景下提出来的。它研究的主要内容是如何使数据库管理系统在遭受到成功的恶意攻击时，能够在对受到破坏的数据进行恢复的同时保留尽可能多的未受恶意攻击影响的其它授权用户在系统受攻击期间的工作结果，能够保持一定的及时提供可靠数据服务的能力。具有入侵容忍服务能力的数据库管理系统的理想情况是：数据库管理系统在遭受到恶意攻击破坏的情况下，能够发现系统被入侵，并及时对受到入侵影响的数据进行隔离和恢复，在系统恢复的同时能够保留尽可能多的未受恶意攻击影响的用户在系统受恶意攻击期间的工作结果；不间断地提供尽可能多的可靠、及时的数据服务；对系统自动进行重新配置，消除攻击者在此次攻击中所利用的入侵途径，避免同样问题再次发生。

国际上对数据库管理系统入侵容忍技术的研究起源于美国，主要是GMU的Sushil Jajodia，Paul Ammann和UMBC的Peng Liu以及North Dakota University的Branjendra Panda等几个研究组。据公开资料，国内浙江大学计算机系蔡亮、杨小虎、董金祥等对信息战语义下数据库管理系统的恶意行为作了研究。我们将在后面对这些工作分别作评述。

2 已有的数据库管理系统入侵容忍研究工作

国外的信息战环境下数据库管理系统入侵容忍技术研究可以分成以下两类：一类是对可疑入侵行为进行入侵隔离[14,15]的事前预防；另一类是对受到攻击破坏后的系统自动进行破坏范围评估和恢复[16~21]的事后补救。对可疑入侵行为进行入侵隔离的基本想法是在一个可疑入侵行为被确认之前，采取预防措施，限制该行为可能对系统造成的破坏，同时又必须能够在判定该行为不是恶意攻击时能尽可能多地保留它的操作结果，节省资源，提高系统性能。而对受到攻击破坏后的系统自动进行破坏范围评估和恢复的研究则着眼于解决恶意授权用户攻击，以及由于许多入侵没有能够检测出来或是因较长的检测时间延迟从而导致的受恶意攻击影响数据库系统的破坏范围评估和恢复问题，是事后补救。

国内浙江大学的工作[22]则是在信息战语义下，研究如何防止从国外进口的数据库管理系统本身的恶意行为，它的重点不同于国外的研究。

2.1 对可疑入侵行为的入侵隔离

虽然入侵检测[23]能够弥补访问控制机制的不足，但是必须认识到它的作用也是有限的：它既可能把无辜的用户误认为是恶意攻击者，也可能让恶意攻击者逍遥法外，尤其是难以解决恶意授权用户构成的安全威胁。针对入侵检测技术的上述局限，Sushil Jajodia等提出了对可疑行为的入侵隔离思想。它的主要想法是在应用层采用隔离可疑用户提交的操作，而不是立即终止该用户提交的数据库事务操作的方法，这样如果数据库系统在后续操作中发现该数据库用户不是恶意攻击者时，数据库系统能够以较少的资源消耗，达到保留该用户尽可能多的事务操作的目的。该方法把数据库分成主版本和嫌疑数据库版本。当数据库系统发现某个用户具有恶意攻击嫌疑时，它就透明的把该用户和主数据库版本隔离开来，防止（可能造成的）系统破坏的进一步蔓延。同时生成一个对应的嫌疑数据库版本，并把该嫌疑用户的所有后续操作转换为对此嫌疑数据库版本的操作。当发现该嫌疑用户不是恶意攻击者时，数据库管理系统将对应于该用户的嫌疑数据库版本和主数据库版本合并，从而实现既减轻恶意攻击可能造成的危害，又尽可能多保留非恶意用户工作的目的。由于主数据库版本和嫌疑数据库版本之间可能存在着不一致，在进行版本合并时需要找到并消除冲突。它以优先图[14](precedence graph)作为工具，描述主数据库版本和嫌疑数据库版本之间是否存在合并时冲突的关系。采用的是基于完全隔离策略的数据库版本隔离协议[14]。

Sushil Jajodia等也同时给出了静态和动态识别与消除数据库版本冲突的算法[14]。

Amgad Fayad等对Sushil Jajodia等的工作[14]作了两个方面的扩展[15]：第一，不再采用完全隔离的策略；第二，提出了一个新的发现版本冲突的算法。具体的内容参考文[15]。

2.2 数据库系统受恶意攻击后破坏范围自动确定与恢复

对受到恶意攻击破坏的数据库系统进行破坏范围自动确定和恢复的方法可以分为两类：基于事务的[16~18]；基于数据依赖的[19~21]。

2.2.1 数据库系统受恶意攻击后基于事务的破坏范围自动确定与恢复方法 一个消除恶意攻击事务影响的简单方法就是撤消掉历史[10~12]中自恶意攻击事务开始的历史中的所有事务，然后重新执行这段事务历史中被撤消掉的无辜事务。它的缺点在于许多无辜事务可能被不必要的撤消掉并不得不重新执行，而这可能正是攻击者希望达到的攻击目的[3,4]。而基于事务的数据库系统恢复算法[16~18]能够克服这个缺点。

基于事务的数据库管理系统入侵容忍技术研究都基于以下两个前提：(1)系统能够发现恶意的攻击事务；(2)数据库管理系统的事务处理系统产生的是一个严格的可串行化历史。数据库日志不能被用户所修改，且当事务执行时，日志也相应地增长并且数据库系统不对日志进行清除。

前提(1)的意义在于，一旦系统发现了恶意事务，具有入侵容忍技术的数据库系统就能及时判定哪些无辜事务(benign transaction)受到了恶意事务的直接/间接影响，阻止正在执行的事务和新提交给事务调度系统的事务读取被破坏的数据，从而防止破坏的进一步蔓延，并进行相应的系统恢复工作。前提(2)的意义在于保证日志的可靠性(因为日志不能被用户修改，所以日志就不能被破坏)，使恢复过程能够及时得到日志信息。

基于事务的数据库恢复算法又可以分为基于事务语法的[16,18]和基于事务语义的[17,18]。

1)基于事务语法的破坏范围自动确定与恢复。美国GMU的Paul Ammann和UMBC的Peng Liu合作提出了一组基于事务语法的数据库抗恶意攻击的恢复算法[16,18]。一旦发现了恶意攻击事务，它们能够把恶意事务以及其它受到直接/间接影响的事务对数据库状态的改变撤消掉，使数据库就像没有发生过恶意攻击一样，还能使攻击发生后未受恶意事务影响的无辜事务的工作结果保留下来。它们可以分成两类：

- 静态恢复算法。即在系统恢复时不能处理新事务，它适用于对持续服务能力要求不高的数据库应用。
- 即时(on-the-fly)恢复算法。即在系统恢复时，数据库系统仍然能够处理新事务。

记录事务操作的日志信息对数据库系统恢复能否顺利实

现是不可或缺的，尤其是事务的读自依赖信息(read-from dependency information)。根据获取这些操作信息方法的不同，基于事务语法的数据库系统可靠恢复算法可以分成4类：在日志中记录事务读操作信息的静态系统恢复算法、在日志中记录事务读操作信息的即时系统恢复算法、从事务特征描述中获取读操作信息的静态系统恢复算法、从事务特征描述中获取读操作信息的即时系统恢复算法。

a)**恢复模型** 集合 $B=\{B_1,B_2,\cdots,B_m\}$表示历史[10~12]中已提交的恶意事务或者说是不期望事务的集合[16~18]。集合 $G=\{G_1,G_2,\cdots,G_n\}$表示历史中已提交的期望的事务或者说是非恶意攻击事务的集合。AG 表示受恶意攻击事务直接/间接影响的事务集合。

为了描述恶意事务和非恶意事务间的相互关系，定义了事务间的依赖关系和影响关系。如果事务 T_i 在事务 T_j 更新了数据项 x 后读取了 x，在 T_j 读取 x 之前 T_i 并没有夭折，且在事务 T_j 更新数据项 x 后到 T_j 读取 x 之前这一时间段内如果有任何事务更新了数据项 x，那么这些事务在 T_j 读取 x 之前均已夭折，满足上述条件，则称事务 T_j 依赖于 T_i。在依赖关系的传递闭包中，如果存在序偶(T_1,T_2)，则称事务 T_1 影响事务 T_2。如果某个非恶意攻击事务 G_i 受一些恶意攻击事务 B 影响，那么事务 G_i 为可疑事务。根据事务间的依赖关系和影响关系，又定义了事务依赖图 DG(S)。

虽然在历史中从恶意攻击事务开始到历史结束存在许多事务，但是只有受到恶意攻击事务直接/间接影响的非恶意攻击事务才需要撤消掉并重新执行。也就是说，只有集合 DG(B)中的事务需要撤消，只有 DG(B)中的非恶意事务需要在撤消后重新执行。

b)**基于在日志中记录事务读操作信息的静态数据库系统恢复** 在日志中记录事务读操作信息的静态系统恢复是基于传统的数据库系统恢复机制的[10~12]。其优点在于不需要完全重新设计数据库恢复算法。而且，标准的传统数据库恢复机制也不需要做很大修改。从本质上讲三趟恢复算法、两趟恢复算法、基于分离的读日志的数据库系统恢复算法都是静态数据库恢复算法。

静态数据库恢复算法的基本思想是在一组恶意攻击事务发现后，暂时停止新事务的处理，根据以日志或是以其它方式保存的事务读操作信息确定 DG(B)，据此得到需要撤消的恶意事务及受恶意攻击影响的其它事务。

三趟数据库恢复算法顾名思义由三趟组成。第一趟从日志中第一个恶意攻击事务提交的记录项开始向前扫描直到日志结束，获得第一个恶意事务提交以后所有提交事务的列表。这个列表中的某些非恶意攻击事务可能受恶意攻击事务影响成为可疑事务。第二趟从日志中第一个恶意攻击事务开始的记录项向前扫描，从第一趟扫描获得的已提交事务列表中抽取所有的恶意攻击事务和可疑事务。第三趟从日志的尾部向日志头部逐个撤消掉所有的恶意攻击事务和可疑事务。

三趟数据库恢复算法的缺点之一是需要三趟，在日志数量很大的情况下可能消耗掉太多的时间。通过增加内存空间的消耗，可以把三趟数据库恢复算法的前两趟合并成一趟，得到两趟数据库恢复算法。

三趟数据库恢复算法和两趟数据库恢复算法所需的事务读操作信息都是和事务写操作信息记录在同一个日志中，这需要对传统的数据库日志作修改。也可以用一个日志单独记录事务的读操作，这样就不必修改原来的数据库日志。这个单独记录读操作的日志称为读日志，而原来记录事务写操作的日志称为更新日志。实际上只要保证单独的读日志和更新日志上的扫描顺序能正确同步，就能把前面提到的两趟数据库恢复算法用到这种分离的日志结构上。这也就是基于分离的读操作日志的数据库系统恢复算法的思想。

c)**基于在日志中记录事务读操作信息的即时数据库系统恢复** 三趟恢复算法、两趟恢复算法、基于分离的读操作日志的数据库系统恢复算法都是静态恢复算法，在对数据库系统进行恢复时，新的事务不能得到系统响应。在某些数据库应用中，要求系统能够在进行恢复的同时并发执行新的事务，这就要求即时修复(on-the-fly repair)。即时修复的缺点在于新事务可能无意中读取受到攻击破坏的数据，并通过它对其它数据项的操作造成数据破坏范围的扩大。普通关系数据库管理系统的事务管理体系结构完全能够实现数据库的即时恢复。

在即时数据库恢复算法中，新的事务不断提交到操作调度器，所以日志在动态增长，因此，即时数据库恢复算法的一个重要问题就是“恢复过程是否会终止？怎么判断恢复已经结束？”恢复过程是否终止取决于恢复的速度，新事务的到达速度，以及新到达事务本身的特点。在文[18]中给出了一组条件，满足它们就可以判定即时数据库恢复过程终止。

即时数据库恢复算法要求恢复管理器为每个恶意攻击事务和可疑事务建立撤消事务。由于日志在不停地增长，对恶意事务和可疑事务的撤消操作只能从恶意事务开始的地方往历史尾部做。这一点与静态数据库恢复算法不同。

当新事务和系统恢复过程并发进行时，为了获得正确的结果，需要用一个特殊算法[18]建立撤消事务。操作调度器调度用户操作以及撤消(undo)操作对系统进行恢复。操作调度器的一个重要任务就是控制用户操作的提交速度，使数据库恢复过程能够结束。

即时数据库恢复算法分成三个部分，分别由修补管理器、操作调度器和恢复管理器执行。修补管理器从第一个恶意攻击事务开始的地方扫描日志，得到所有需要撤消的恶意攻击事务和可疑事务，并建立相应的撤消事务，然后把撤消事务提交到操作调度器。操作调度器对用户操作和由修补管理器提交的撤消操作进行调度。恢复管理器对数据进行恢复。

d)**从事务特征描述中获取读操作信息的数据库系统恢复** 和读日志方法比较，采用从事务特征描述(transaction profiles)和输入参数获取事务读操作信息的方法有下列优点。第一，每个事务只需要存储它的输入参数，大大降低了存储空间的消耗。第二，由于是把输入参数放在一个专门的用户数据库中，而不是记录在日志中，所以数据库管理系统的恶意攻击恢复模块能够和传统数据库的原有事务恢复模块完全隔离。这样，就能在现有数据库管理系统之上实现入侵容忍数据库恢复模型，而且可以避免影响数据库管理系统的原有系统恢复机制的性能。这个方法的缺点在于，它可能撤消掉未受影响的事务，或是在即时数据库系统恢复时延迟恢复终止的判定；而且应用程序的编写者在编写应用时必须改变事务代码，使数据库恢复获得必要的支持。

从事务特征描述中获取事务读操作信息的数据库恢复算法与前面提到的两种数据库恢复算法的差异在于获取读操作信息的方法。在许多联机事务处理(OLTP)应用中为了满足实时性，不能在事务执行时通过即时分析事务代码获取读操作信息。因此，提出了事务读集模板的概念。为每种事务设置一个类型，它描述了事务的特点。当事务 T 提交到调度器后，

与 T 的类型相关联的读集模板就用 T 的参数来物化(materialized)。这样就获得了事务 T 的读集。

同样给出了静态数据库系统恢复算法、即时数据库系统恢复算法。

2)基于事务语义重写事务历史的破坏范围自动确定与恢复。Peng Liu 还提出了基于事务语义,通过对事务的执行历史进行重写,实现数据库入侵容忍的方法[17,18]。

基于事务语义,定义了事务 T 和事务序列 R 之间的能跟随(can follow)关系。如果事务序列 R 中的任何一个事务都不从事务 T 的写集中读,那么称事务 T 能够跟随事务序列 R。根据 can follow 关系,可以通过把 G-AG 中的事务移到历史头部的方式对事务历史进行重写。

Can-Follow Rewriting 算法的输入是需要重写的可串行化历史 H' 和恶意攻击事务集合 B。它从历史中记录的第一个恶意攻击事务 B_1 后的第一个非恶意攻击事务开始向需要重写的可串行化历史 H' 的尾部扫描。对遇到的每个事务 T,如果 T 是已经发现的恶意攻击事务就跳过它,如果 T 是一个非恶意攻击事务,只要从 B_1(包括 B_1 在内)到 T 之间的事务序列和 T 之间满足 can follow 关系,就把 T 移动到 B_1 的直接前驱位置上。对重写后的事务历史直接通过 undo 操作就能够撤消掉恶意攻击事务和可疑事务对数据库的影响。

通过把 Can Follow Rewriting 算法和两个事务 T_1 和 T_2 之间的能先于(can precede),或是两个事务序列 P 和 Q 之间的互逆(invert)和覆盖(cover)关系结合[20,21],数据库管理系统恢复时不仅能够保留 G-AG 中的事务,而且能够保留 AG 中某些实际未受恶意攻击事务影响的非恶意攻击事务。这就是 Can-Follow and Can-Precede Rewriting 算法和 Can-Follow,Can-Precede,Cover,and Invert Rewriting 算法的思想。

这组算法通过重写数据库系统中事务的执行历史,使重写后获得的历史的前缀(prefix)中只保留了未受恶意攻击影响的非恶意攻击事务,且保持事务之间的相对顺序与重写之前的事务执行历史中的顺序一致;而重写后获得的事务历史的后缀(suffix)中包含了恶意攻击事务和受其影响的可疑事务以及用来描述恶意攻击事务和受其影响的可疑事务的数据库状态信息。通过利用事务的语义信息,能够从重写后获得的事务执行历史后缀中提取额外的未受攻击事务影响的事务。正是这一处理,使基于事务语义重写事务历史的方法比基于事务语法的方法,在恢复受破坏的数据库系统时能保留更多的未受恶意攻击事务影响的事务。Peng Liu 基于 SAGAS 事务处理模型,论证了他所提出的数据库管理系统恢复算法的可行性。

2.2.2 *基于数据依赖的数据库系统恢复* Brajendra Panda 等提出基于数据依赖使数据库从恶意攻击中恢复的方法[20],而不是基于事务的方法。他们的方法不是把受恶意攻击事务直接/间接影响的那些事务的所有操作都撤消掉,然后重新执行这些受影响的事务;而是只把这些受影响的事务中的受影响的操作撤消掉并重做。

Sani Tripathy 等针对日志数据增长迅速,查找耗时的特点,作了改进[21],提出基于数据依赖把数据库日志分成多个日志块(multiple log segments),每个日志块只包含存在数据依赖的操作。它根据操作所涉及到的数据项来判定操作是否存在依赖,只有相互间存在依赖关系的操作才放在一个日志块中,相互间独立的操作放在不同的日志块里。在对系统被破坏程度进行评估和系统恢复时,就可以只扫描包含恶意操作和相关操作的那些日志块。这大大减少了日志扫描时间,加速了数据库系统的恢复。

它是基于这样一个事实:在一个事务中,某些操作相互之间完全可能是独立的。因此,在受到恶意事务攻击的情况下,对一个受到影响的事务而言,不是它包含的所有操作都一定受到恶意事务的影响。所以,在系统恢复时,就不必撤消并重新执行受影响事务的所有操作,只需要撤消并重新执行该事务中受到影响的那部分操作。

基于数据依赖的数据库恢复方法的另一个优点在于能够及时判定未受到恶意事务影响的数据项的最大集合,从而使它们尽可能快地为系统正在和将要处理的事务所用。这样就降低了拒绝服务攻击的风险,提高了系统的可用性。

2.3 对抗数据库管理系统本身潜藏的恶意功能

国内浙江大学计算机系蔡亮、杨小虎、董金祥等的研究[22]重点是在信息战语义下,如何防止从国外进口的数据库管理系统本身可能潜藏的恶意功能。由于引进的商用数据库管理系统不提供源代码,不能进行代码分析、评审,无法进行可信计算基(Trusted Computing Base)分析。更为严重的是在信息战语义下,潜在的敌人完全可能在我国引进的数据库管理系统中事先通过修改标准数据库管理系统的代码,注入各种隐藏的恶意功能,在信息战时启动它们。这些恶意功能主要包括:在数据库管理系统的身份认证机制上留下后门,从而使敌人能够绕过身份认证;在授权机制上留有后门,从而敌人的某些操作可以绕过正常的访问控制;在数据处理模块中添加恶意功能,在必要时启动,对数据进行隐蔽的自动修改和破坏;在审计功能上留下后门,篡改审计数据,将攻击活动伪造成正常活动,或者不记录某些攻击活动,甚至可能通过伪造审计数据,陷害无辜,制造系统受攻击的假象。他们提出了相应的对抗措施,并初步实现了一个提供数据库安全保护的原型系统。它是一个在数据库管理系统可能具有暗藏的恶意功能的情况下,用来保证数据库安全的外挂式多级数据库安全平台。它的思想是使数据库管理系统和应用隔离,两者之间的通信都必须通过这个外挂式数据库安全平台,从而使引进的数据库管理系统可能暗藏的恶意功能难以发挥作用,它实现了独立的身份认证、访问控制和审计功能。

2.4 评论

从数据库管理系统入侵容忍技术的角度来看,对可疑入侵行为的入侵隔离的方法适合于在可疑行为没有得到确认之前使用。而基于事务的和基于数据依赖的对受到攻击破坏的系统自动进行破坏范围评估和恢复的方法属于事后补救措施。基于事务的静态数据库恢复算法可以实现精确恢复,但是在恢复时不能响应新的事务处理请求,不适合要求连续提供服务的应用。而基于事务的即时数据库恢复算法在恢复时可以响应新的事务,适合需要提供不间断服务的场合,虽然可能撤消掉实际不必撤消的事务,但是并不会影响系统恢复的正确性,是一种比较理想的数据库入侵容忍技术。基于事务语义的数据库恢复算法能够比基于事务语法的数据库恢复算法在系统恢复时保留更多的未受恶意攻击影响的事务,但是精确语义信息的获取比较困难。与传统的数据库恢复算法相比,基于事务的数据库恢复算法在系统恢复时能够保留较多的未受攻击影响的事务,而且在即时恢复时能够提供不间断的服务。基于数据依赖的数据库入侵容忍技术由于采用了日志分块算法,在系统恢复时能够提高效率,减少不必要的扫描时间耗

费，但是在进行日志分块时需要判断数据依赖，因此有一定的服务时间延迟。国外的数据库管理系统入侵容忍技术研究的重点是如何解决由恶意授权用户的行为造成的系统破坏，而国内浙江大学的研究则着眼于解决数据库系统本身可能存在的恶意功能。从入侵容忍技术的角度来说，它是通过切断用户和数据库系统之间的直接通讯达到对抗那些隐藏的恶意功能的目的，比较适合我国目前的国情。

3 需要进一步研究的问题

作为信息系统可生存性研究的一个重要内容，数据库管理系统的入侵容忍技术已成为一个新的数据库安全研究热点。它使数据库系统具有抗恶意内部攻击能力，增强了系统防止拒绝服务攻击(Denial of Services)的能力，尽管已有了一些初步研究成果和原型系统[17]，但是仍有许多问题亟待解决。

首先，需要研究发现恶意攻击的有效方法。这是因为，随着恶意攻击从实施到被发现的延迟时间的增加，对数据库系统进行恢复的代价就变得越来越高，难度也不断增大。不能发现恶意攻击，实现数据库系统的入侵容忍也就无从谈起。这方面的研究可以分成两个部分，一是研究如何解决内部安全威胁；二是提高入侵检测和攻击检测的效率及准确性。

其次，在数据库系统受到恶意攻击时，如何实现系统状态的自稳定，保证一定的服务质量也值得深入研究。如果能够度量系统的自稳定性，在一些紧急情况下就能保证最重要的任务得到优先服务。

再次，在遭受到恶意攻击时，数据库系统如何在保护重要资源的同时对攻击者进行信息欺骗和攻击取证也是一个有意思的话题。这里还涉及到法律方面的问题。

另外，在分布式数据库管理系统、多版本数据库管理系统、多级安全数据库管理系统等数据库模型中如何实现入侵容忍也需要深入研究。

参 考 文 献

1 Jones A. Information Warfare--What is it?: [Information Security Technical Report]. Elsevier, 1999, 4(3): 12～19

2 Waltz E. Information Warfare: Principles and Operations. Boston London, USA. Artech House, 1998

3 Graubart R, Schlipper L, McCollum C. Defending Database Management Systems Against Information Warfare Attacks: [Technical Report]. The MITRE Corporation, 1996

4 Jajodia S, Ammann P, McCollum C D. Surviving information warfare attacks. IEEE Computer, 1999, 32(4): 57～63

5 Bell D E, LaPadula L J. Secure Computer System: Unified Exposition and Multics Interpretation: [Technical Report MTR-2997]. MITRE, Bedford Masschusetts., HQ Electron. Syst. Dov., Hanscom AFB, MA: [ech. Rep. ESD-TR-75306]. June 1975, 1976

6 Anderson R H. Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems: Results of a Three-Day Workshop. RAND CF-151-OSD, 1999

7 Insider Threat Integrated Process Team, Department of Defense (DoD-IPT), 2000. Available at http://www.c3i.osd.mil

8 DoD Insider Threat Mitigation, U. S. Department of Defense, 2000. Available at http://www.c3i.osd.mil

9 Lee P A, Anderson T. Fault Tolerance: Principles and Practice. Springer-Verlag, Wien, Austria, second edition, 1990

10 Bernstein P A, Hadzilacos V, Goodman N. Concurrency Control and Recovery in Database Systems. Addison-Wesley, Reading, MA, 1987

11 Gray J, Reuter A. Transaction Processing: Concepts and Techniques. Morgan Kaufmann, San Mateo, CA, 1993

12 Weikum G, Vossen G. Transactional Information Systems: Theory, Algorithms, and the Practice of Concurrency Control and Recovery. Morgan Kaufmann Publishers, 2001

13 Ammann P, Jajodia S, Liu P. A Fault Tolerance Approach to Survivability. In: Proc. of the Computer Security, Dependability, and Assurance: From Needs to Solutions, York , England and Washington DC, USA, 1998

14 Jajodia S, Liu P, McCollum C D. Application-Level Isolation to Cope With Malicious Database Users. In: Proc. 14th Annual Computer Security Applications Conference, Phoenix, AZ, 1998. 73～82

15 Fayad A, Jajodia S, McCollum C D. Application-Level Isolation Using Data Inconsistency Detection. In: 15th Annual Computer Security Applications Conf. Phoenix, Arizona, 1999. 119～126

16 Ammann P, Jajodia S, Liu P. Recovery from malicious transactions. IEEE Transactions on Knowledge and Data Engineering, 2002, 14(5): 1167～1185

17 Liu P, Ammann P, Jajodia S. Rewriting histories: recovering from malicious transactions. Distributed and Parallel Databases, 2000, 8(1): 7～40

18 Liu P. Trusted Recovery from Malicious Attacks: [Ph. D. Dissertation]. George Masson University, U. S. A, 1999

19 Panda B, Giordano J. An Overview of Post Information Warfare Data Recovery. In: Proc of the 1998 ACM Symposium on Applied Computing, Atlanta, GA, Feb. 1998

20 Panda B, Giordano J. Reconstructing the Database after Electronic Attacks. in Database Security XII: Status and Prospect, S. Jajodia(editor), Kluwer Academic Publishers, 1999. 143～156

21 Tripathy S, Panda B. Post-Intrusion Recovery Using Data Dependency Approach. In: Proc. of the 2001 IEEE Workshop on Information Assurance and Security. United States Military Academy, West Point, NY, June, 2001

22 蔡亮，杨小虎，董金祥. 信息战下的数据库安全--我国的特殊需求分析和对策. 计算机研究与发展，2002，39(5)：568～573

23 Leonard J. Lapadula State of the Art in Anomaly Detection and Reaction: [Technical report]. MITRE, Bedford, Massachusetts, 1999