文章编号:1001 - 9081(2006)02 - 0383 - 02

用于入侵容忍数据库系统的多阶段控制技术

李文才,孟丽荣,于常辉
(山东大学 计算机科学与技术学院,山东 济南 250061)
(xiaoxinlwc@ mail. sdu. edu. cn)

摘 要:传统入侵容忍数据库系统的破坏控制是一阶的,对象直到破坏评估器确认其受到破坏才被控制,时间延迟导致破坏的扩散而影响数据库系统的可用性,针对这个问题提出了多阶段破坏控制方案。给出了多阶段破坏控制技术模型,及多阶段破坏控制方案中各阶段的任务。最后,给出了多阶段破坏控制各阶段的效率分析。多阶段破坏控制方案有效地拒绝了破坏扩散,保证了数据库系统的可用性。

关键词:入侵容忍;多阶段控制;破坏控制
中图分类号: TP311.13 **文献标识码**:A

Multiphase confinement for intrusion tolerant database system

LI Wen-Cai, MENG Li-rong, YU Chang-hui
(*School of Computer Science and Technology, Shangdong University, Jinan Shandong* 250061, *China*)

Abstract: Traditional damage confinement of intrusion tolerant database systems is one phase. Damaged objects are confined until damage assessor finds they are damaged. However, time latency causes damage spread. Serious damage spread usually causes the unavailability of database systems. To solve the problem, multiphase confinement solution was given. The model of multiphase confinement solution was defined. The functions of the phases of multiphase confinement solution were described. Finally, the model was evaluated and analyzed through experiments. Multiphase confinement solution can defuse time latency and avoid damage spread , so it can confirm the availability of database systems effectively.

Key words: intrusion tolerance; multiphase confinement; damage confinement

数据库的安全性包括数据库中数据的机密性、完整性、可用性。一般的研究强调将攻击者拒之门外,通过加密和严格的存取控制保护信息的保密和完整。像信用卡支付、银行、飞机交通控制、后勤管理、在线期货交易等大量用到数据的系统中,正在面临着一些恶意的攻击。从某种程度上说,这些攻击是不可避免的,这就需要建立具有抵抗力的数据库系统。目前一阶的入侵容忍数据库系统,由于检测延迟、评估延迟、恢复延迟可能会导致严重的破坏扩散,使数据库变得不可用。为此引入多阶段控制的入侵容忍数据库系统,在面临恶意攻击带来的损害时,首先控制所有可能受到损害的对象,避免了破坏扩散,然后分阶段的恢复直到数据库恢复到正常的状态。

1 一般入侵容忍系统的架构

这个架构在 COTS(Commercial Off The Shelf)DBMS 上实现。具有入侵容忍能力的数据库通过把入侵检测和攻击恢复结合起来达到入侵容忍的目标。入侵容忍数据库系统架构如图 1 所示[3],它包括:

入侵检测器: 负责实时的监控和分析数据库中的日志以尽可能早的发现恶意事务;

破坏评估器: 负责发现恶意事务并定位遭受破坏的位置,通知破坏修复器;

破坏修复器: 采用回滚操作修复恶意事务造成的破坏;

策略执行管理器(PEM): 对普通用户的事务和回滚操作起代理的作用,执行系统范围内的入侵容忍策略;

破坏控制管理器: 负责限制那些对已经被损害的对象的访问。

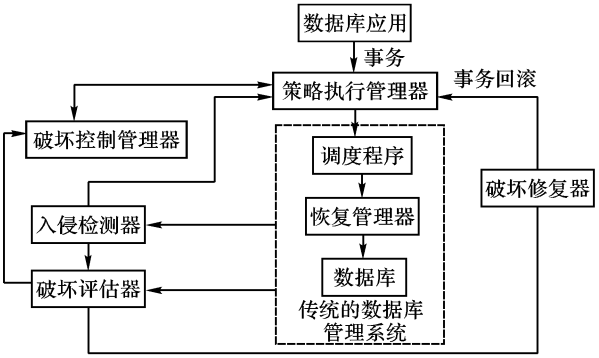

图 1 入侵容忍数据库系统的结构

这样的系统存在以下的问题:

1) 检测延迟

发生检测延迟的原因主要有:1)多数情况下检测需要人的交互;2)为了减少误报率,很多情况下需要对连续的行为进行分析。因此,检测延迟几乎是不可避免的。

2) 评估延迟

发生评估延迟的原因主要有:1)检测延迟可能会导致评估延迟。当发现一个恶意事务 B_i 时,可能已经有许多事务直接或间接的受到了 B_i 的影响。这时对事务进行评估,评估延迟几乎是不可避免的。2)破坏评估往往需要一定的计算时间,其往往和历史日志的长度成正比。系统需要查询历史日志察看哪些事务受到了影响,哪些没有受到影响,这些又会导

收稿日期:2005 - 08 - 05;**修订日期**:2005 - 10 - 27

作者简介:李文才(1983 -),男,山东阳谷人,硕士研究生,主要研究方向:网络安全; 孟丽荣(1946 -),女,黑龙江哈尔滨人,教授,主要研究方向:软件工程、网络安全等; 于常辉(1977 -),男,山东海阳人,硕士研究生,主要研究方向:网络安全.

致评估延迟。

3）修复延迟

当一个受影响的事务被定位时，破坏修复器构造一个特定的清理事务来恢复被破坏的对象，这需要时间，就容易产生恢复延迟。

4）破坏扩散

恶意的事务可能会通过破坏扩散严重损坏一个数据库。在一个数据库中，一个事务的执行结果会影响其他的事务。例如，当一个事务 T_i 读取一个数据对象 x，而 x 被另一个事务 T_j 所更新，我们称 T_i 被 T_j 所直接影响；如果第三个事务 T_k 被 T_i 直接影响，但没有被 T_j 所直接影响，我们称 T_k 被 T_j 所间接影响。容易看到，如果一个更新 x 的事务 B_i 被确认为恶意的，那么在恶意的事务被修复前，对 x 造成的破坏能扩散到每一个被 B_i 所直接或间接影响的好的事务所更新的对象。入侵检测器、破坏评估器和破坏修复器负责定位并修复那些受到破坏的对象。但是在一阶系统中，对象直到破坏评估器确认其受到破坏才被控制。检测延迟、评估延迟、恢复延迟往往会导致破坏扩散使整个系统将会变得不可用。在多阶段控制技术模型中，一旦入侵被发现，将会控制所有可能被破坏的对象，保证直到系统恢复之前没有破坏扩散，在此基础上，实现数据库的入侵容忍。

2 多阶段控制技术模型

当发现了恶意攻击时，要对可能遭到破坏的对象进行隔离。将受到隔离的对象定义为 A，实际上遭到破坏的对象为 B。如果 $A = B$ 称之精确控制。精确控制是我们的目标，但很难实现。如果 $A \geqslant B$ 称之为过量控制，如果 $A \leqslant B$ 称之为不足控制。多阶段控制技术主要是通过过量控制来实现。当发现入侵时，立即控制所有可能受到破坏的对象，然后通过回滚逐渐恢复未被破坏的对象。已经损害对象通过破坏修复器进行修复，实现破坏控制和恢复。多阶段控制系统的结构如图 2 所示。

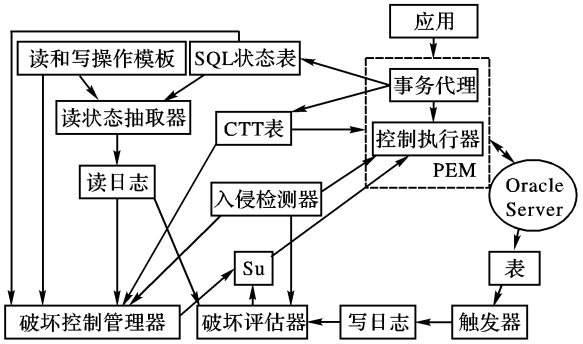

图 2 多阶段控制系统的结构

时间戳，用来记录对象被事务更新的时间；CTT 表（Committed Transaction Table）包括：1）事务 ID，用来唯一的标示一个事务；2）提交时间，记录事务是什么时候提交的；3）事务类型，记录事务的类型。Su，用来记录所有被控制然后恢复的对象；DG(B_i)，所有被恶意事务 B_i 影响的对象的关系图；历史日志，用来记录所有的读操作和写操作；入侵检测器，负责检测恶意事务；PEM（Policy Enforcement Manager），负责执行破坏控制的策略管理。

多阶段控制的工作原理：

初始控制阶段：时间戳记录对象最后被更新的时间。当一个恶意事务 B_i 被确定时，所有时间戳晚于 B_i 的开始时间的对象都要被控制。在第一阶段所有操作被恶意事务影响的对象的活动都要被中断。因此就不会存在破坏遗漏。但并不包括在这一阶段之后受到更新的对象，保证了不影响这一阶段之后正常的操作。

第一恢复阶段：扫描日志察看哪些事务直接受到 B_i 的影响。如果事务 G 没有直接受到 B_i 影响，所有时间戳早于 G 的提交时间的被 G 更新的对象将会被恢复。但是需要注意的是，这些对象可能在以后的时间里可能被其他恶意事务更新而遭到破坏。

第二恢复阶段：从 CTT 表中读取事务的类型，以及事务之间的关系图 DG(B_i)。将这一阶段将被恢复的对象暂时放入对象集 Q 中。分析关系图 DG(B_i)，如果一个事务 G 没有直接或间接受到恶意事务 B_i 的影响，那么事务 G 操作的对象将会被暂时放入 Q 中；如果事务 G 受到恶意事务影响，那么从 Q 中减去 Q 和 G 操作的对象的交集，然后将 Q 放入 S_u 中。本阶段从读和写操作模板以及 SQL 状态表中获得操作事务之间的关系图 DG(B_i)。使用事务代理来代理每一次的 SQL 操作。本阶段在破坏控制管理器执行。

第三恢复阶段：将关系图 DG(B_i) 实例化，按照假设的实际执行的情况进行实例化。有时一些在关系图上间接受到影响的事务实际上并没有受到影响，我们将按假设的实际操作一次，如果没有受到影响，将其放入 S_u 中。由于进行事务的实例化要比破坏评估快捷的多。因此，可以从很大程度上减少恢复延迟。问题是如何得到实际的读和写的操作信息。由于在 Oracle 数据库中，写操作的信息是保密的。因此，我们使用触发器来获得删除、更新、插入的信息。本阶段在破坏评估器执行。

第四恢复阶段：对那些受到损害的对象，通过回滚进行恢复，并去除时间戳的限制完成整个多阶段控制。

3 效率分析

初始控制阶段可能会控制一些实际上没有受到损害的对象，但是不会导致破坏扩散，保证了数据库的完整性。系统在第一恢复阶段要对读日志和写日志进行大量扫描，所以第一阶段最慢。除了进行损害修复的第四恢复阶段，其他阶段都是独立的，因此可以进行并发处理，有效地避免评估延迟。支持灵活地损害控制，既可以以牺牲资源为代价保证没有遗漏，也可以最大限度的实现可用性。系统可以实时地实现入侵容忍，而不需要中断正常的操作。系统具有灵活的可用性，可以无缝地移植到现有损害评估和修复系统。

4 结语

本文提出实现破坏控制和破坏恢复的多阶段控制解决方案，保证了在入侵检测期间没有破坏扩散。尽管由于过量控制而损失了一些可用性，但是由于支持灵活的破坏控制，因此方案是灵活、高效、实用的，对实现现有数据库的改进有很大的帮助。

参考文献：

[1] LIU P, WANG Y. DDCS: A Multiphase Database Damage Confinement Prototype System [J]. In Proceedings of the 2002 IFIP WG 11.3 Working Conference on Data and Application Security, 2002.

[2] LIU P, JAJODIAL S. Multiphase Confinement In Database System For Intrusion Tolerance [A]. 14th IEEE Computer Security Foundations Workshop (CSFW'01) [C]. 2001.11 - 13.

[3] LIU P, JAJODIAL S. Multiphase Damage Confinement In Self-Healing Database System[J]. Technical report, George Mason University, Fairfax, VA, 1998.