DOI:10.3969/j.issn.1000-1565.2014.03.018

自律式容侵安全数据库模型

齐耀龙[1],刘慧君[2],邓娜[1]

(1. 河北大学 计算中心,河北 保定 071002;2. 河北大学 实验室管理办公室,河北 保定 071002)

摘 要:针对当前入侵容忍的数据库系统缺乏自适应能力的问题,采用了将自律计算、入侵容忍与传统数据库安全相结合的方法,提出了一个自律式容侵安全数据库模型.通过对数据库运行状态集的实时监测,自主评价访问可信度并对可疑访问进行自适应分流,并将高危访问进行特征分析并施加安全策略,最终保障数据库的安全运行.实验数据表明,该模型对本地和网络攻击可以实现有效稳定抵御,对于国家机构的数据管理、大型企业的管理控制等安全级别要求较高的领域有着重要的意义和价值.

关键词:数据库;自律计算;入侵容忍

中图分类号:TP309.2 **文献标志码**:A **文章编号**:1000-1565(2014)03-0312-05

An intrusion tolerance model of database security based on autonomic computing

QI Yaolong[1], LIU Huijun[2], DENG Na[1]

(1. Computer Center, Hebei University, Baoding 071002, China; 2. Laboratory Management Office, Hebei University, Baoding 071002, China)

Abstract: Concerning lack of self-adaptation ability on existent intrusion tolerance database systems, this paper proposed an intrusion tolerance model of database security based on autonomic computing. By defending the attacks effectively, keeping the security of database system, and providing users with continuous service, the simulation results show that the model has great significance for the data management in national organization or large enterprises.

Key words: database; autonomic computing; intrusion tolerance

---

当前,网络安全严重威胁着国家机关和企事业单位的信息安全,网络安全作为影响国家安全和经济发展的重大问题已经刻不容缓.实现网络安全的核心环节是保障数据库系统安全,其目标是从数据完整、数据机密和数据有效层面进行有效保障.现有的防火墙、身份认证、权限控制、数据加密和入侵检测等数据库安全手段并不能实现完全防御.因此数据库系统安全研究的核心问题就集中在当传统防御技术失效的状况下如何对数据库安全进行保障.

作为第 3 代信息系统安全的核心技术,入侵容忍提出系统全局在特定局部遭受破坏或恶意控制时仍然

收稿日期:2013-10-30

基金项目:河北大学自然科学研究计划项目(2008Q50);河北省科技厅软科学项目(12450328)

第一作者:齐耀龙(1978-),男,河北保定人,河北大学讲师,主要从事网络及数据库应用方向研究.

E-mail: dragon@hbu.cn

可以向客户提供稳定不间断的服务,并维持数据完整和数据机密[1]. 入侵容忍技术是上述安全问题的可行方案,令数据库系统具备了一定程度的攻击弹性和服务不间断性特征. 1986 年,Dobson 等人[2]进行了初步的入侵容忍技术研究,其思路是借助非可靠性、非安全性的组件以搭建具备可靠性和安全性的系统. 之后斯坦福大学将门限密码技术用于网络容侵的研究中[3],随后康奈尔大学研究建立了秘密健壮的数据分布项目[4],并在容侵重现认证项目中使用了加密共享技术[5]. Rabint[6]在 RSA 加密门限策略的研究中采用了自适应的安全策略,之后一些具备自适应特征的门限策略相继被提出[7~8],但上述研究仅限于设计加密共享策略或门限密码技术研究,并没有将其应用到具备自适应特征的容侵系统中. 美国国防部先进研究项目局的资助项目 ITUA 借助冗余管理思想完成令攻击方难以预测的资源动态配给和系统容错响应[9],但缺乏自适应特征即无法对容侵系统的运行配置参数实施动态矫正. 国内,王慧强等人[10]于 2010 年提出一个关键任务系统下的自律可信性模型和其相应的量化分析算法,基于稳态概率的思想设计了一个度量自律可信性的方法,但研究仅针对大型分布式的关键任务系统;2011 年,吴庆涛等人[11]构建了一个针对计算机网络的基于自律反馈机制的入侵容忍模型,在实时分析网络访问的可信程度时引入了自律机制,但这些研究都未针对数据库安全体系进行研究,且未涉及自适应事务自适应分级策略. 此外,国防科技大学等单位也都进行了入侵容忍系统相关技术的尝试和研究并应用到数据库领域,但是上述研究主要讨论面向状态的入侵容忍、面向服务的入侵容忍和对数据库事务级的容忍,多采用分级容侵策略、秘密共享策略或门限密码理论将一些异常的事务隔离,对已破坏的数据进行恢复,缺乏自适应能力.

自律计算的构想是由 IBM 公司提出的,自律计算环境的核心目标是使计算机系统具备高可靠性、高可用性和高服务性. 由自律计算策略建构的系统具备自主配置、自主优化、自主保护和自主修复 4 大特征. 而现有的容侵数据库系统恰恰缺少这 4 类特征,本文据此提出将入侵容忍技术、传统数据库安全策略与自律计算相结合的方法,研究了一个具有自适应特征的自律式容侵安全数据库模型,对本地和网络攻击可以实现有效稳定抵御,使得数据库系统始终处于安全和稳定运行的状态.

1　自律式容侵安全数据库模型

本模型具备自律计算特征,因此可以在无需外力参与的情况下,对数据库系统的资源占用、网络占用、连接请求、响应时间、数据吞吐量及系统运行环境进行实时数据采样,并对数据库连接信度进行主动评估,之后将非可信连接导向虚拟数据库系统进行特征分析,并根据安全策略对其实施处理,最终维持或还原数据库的稳定安全状态. 自律式容侵安全数据库模型划分为 4 层,如图 1 所示.

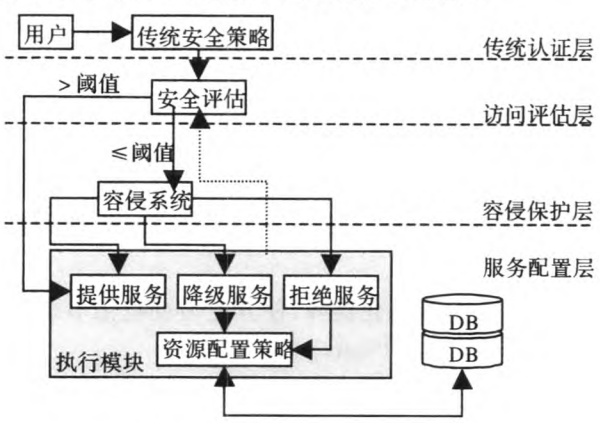

图 1　自律式容侵安全数据库模型框架

Fig. 1　Module architecture

a)传统认证层. 包括身份认证、数据加密、权限控制、防火墙等策略. 客户发起的连接请求通过防火墙之后,系统对其进行身份认证与权限控制,如有必要则对敏感信息加密处理.

b)访问评估层.评价模块对数据库本体、运行环境和数据请求进行实时数据采样并传输给安全评估模块;访问请求的信度计算由经验数据库、专家数据库和采样数据经由多属性决策分析得出,为了维持系统的并发性能和吞吐性能,应当立即对信度数值达到阈值的连接提供服务.

c)容侵保护层.对非可信访问的容侵和数据库系统的保护由事务自适应分级子系统和虚拟数据库系统共同实现.被判定为非可信的访问请求将被交由事务自适应分级子系统,分级结果由该访问发起的数据库事务的重要性和对数据库的影响程度得出,可以划分成关键性事务和非关键性事务,如有必要则对关键性事务进行冗余配置.然后将事务自适应分级信息、非可信访问连同其请求的数据库资源的副本同时传输至虚拟数据库系统,进一步实现对非可信访问请求的行为判析和处置策略.

d)服务配置层.根据行为判析的结论,采取对应的服务策略或复原策略使数据库自行保持安稳运行状态.

2 访问评估

首先对到达的访问请求进行初始化可信程度评估,然后基于阈值策略分流可信访问和非可信访问.访问评估模块的工作原理见图 2.

访问评估采样器负责采集系统资源信息 LS、网络资源信息 NS、会话特征信息 SS 和响应能力信息 SP.其中系统资源信息表现了本地系统资源占用情况,LS={CPU 占用信息,数据库缓存占用信息,内存占用信息,IO 命中率,表空间占用信息,数据库锁使用信息};响应能力信息表示当前数据库配合操作系统对客户端提供正常数据库服务的能力,SP={每秒事务处理量,事务平均响应率,查询平均命中率,死锁率,网络资源利用率,数据吞吐率};网络资源信息体现了各种网络事件和资源占用,NS={会话数量,连接状态,发送数据包数量,接收数据包数量,平均会话耗时};会话特征信息代表了访问请求的自身信息,SS={源 IP,目标 IP,被访问数据库对象,带宽占用,请求频度}.所以采样数据 SD={LS,SS,NS,SS}.其中:LS={LS_i | $i=1,\cdots,6$};SS={SS_j | $j=1,\cdots,5$};NS={NS_k | $k=1,\cdots,5$};SP={SS_l | $l=1,\cdots,6$}.专家数据库 ED 包含知识推理数据 kd 和系统特征数据 tt.知识推理数据即领域知识 tk 和采样数据 SD 对于数据库状态 ds 的推论.系统特征数据即数据库系统应当达到的目标状态,tt={数据完整,数据有效,数据保密,运转保障,数据吞吐量,事务处理量},所以 ED={kd,tt},其中 $kd=\{f^{(l)}(tk_l,SD_l)\rightarrow ds_j \mid l=1,\cdots,n,j=1,\cdots,m\}$;$tt=\{tt_k \mid k=1,\cdots,6\}$.经验数据库 TD 包括会话数据 SD 和成因数据 ID.会话数据表现了会话的资源占用特征,SD={会话类别,开始时间,结束时间,源 ID,目标 ID,持续时间}.成因数据表现数据库系统从稳定态变为不稳定态的进程及规律,可以用一个 SD 对 ds 的函数关系表示,即 TD={SD,ID},其中 SD={SD_i | $i=1,\cdots,6$};$ID=g(SD_{Tj}\rightarrow ds_k \mid j=1,\cdots,n,k=1,\cdots,m)$.

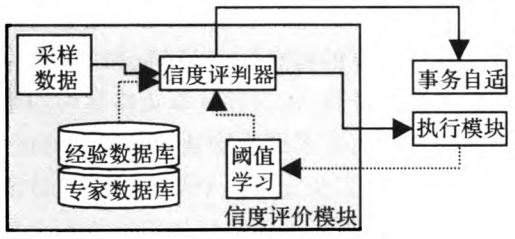

图 2 访问评估模块

Fig. 2 confidence evaluation module

采样数据、专家数据库和先验数据库作为评定当前数据库访问可信度的 3 类输入,直接影响到评估结果的准确度,但是其权重系数尚不能明确定义.因此数据库访问的可信程度值可以利用多属性决策,并结合离差最大化来演算得出.

首先建立决策矩阵,然后对此矩阵进行规范化演算,使其变为规范化形式

$$R_k^{(3)}=(r_{ij})n\times m. \tag{1}$$

假定参数权重向量定义为

$$\omega_k^{(3)}=(\omega_{k1}^{(3)},\omega_{k2}^{(3)},\cdots,\omega_{kn}^{(3)}),\omega_{ki}^{(3)}\geqslant 0,i\in M, \tag{2}$$

对其求解并施加归一化操作得到

$$\omega_{kj}^{(3)}=\frac{\sum_{i=1}^{n}\sum_{x=1}^{n}\mid r_{kij}^{(3)}-r_{krj}^{(3)}\mid}{\sum_{j=1}^{m}\sum_{i=1}^{n}\sum_{x=1}^{n}\mid r_{kij}^{(3)}-r_{xj}^{(3)}\mid},j\in M. \tag{3}$$

因此三阶参数的属性值就可以演算得出,将计算结果当做属性值代入二阶参数,那么一阶参数对应的属性值就可以通过重复上述决策过程演算得出.

在此基础上计算得出数据库访问请求的可信程度值

$$C=\sum_{l=1}^{3}\left(\sum_{k=1}^{9}\left(\sum_{j=1}^{m}r_{kij}^{(3)}\omega_{kj}^{(3)}\right)\omega_{kj}^{(3)}\right)\omega_{ij}^{(3)}. \tag{4}$$

然后基于阈值策略分流可信访问和非可信访问,可信程度阈值数据将在系统运行时根据执行模块反馈的相关结果进行自主调整.当系统运行时间到达预设检查点时,假定容侵保护子系统将非可信访问识别为可信访问的比率偏高,即误判率偏高,则自动降低可信程度阈值数据,否则将其自动上调.

3　容侵保护

为了防止数据库遭受非可信访问的攻击,必须实时断开非可信请求对真实数据库的连接,并使攻击方难以察觉,然后分析与鉴别攻击者的访问请求,将访问请求界定为非可信访问、可信访问或可疑访问,从而为数据库提供可靠的访问请求.

a)虚拟数据库系统.利用诱骗网络并结合入侵重定向技术,本文基于虚拟化技术搭建虚拟网络环境中的数据库系统,用于无缝承接非可信访问请求,从而对攻击方实施诱骗和监控,并且对访问行为进行特征分析,并且防止真实数据库遭受攻击.

b)访问重定向.为了提高数据库系统的容侵能力和保障运行安全,此模块将非可信访问请求实时重定向到虚拟数据库系统,并及时断开非可信访问对真实数据库的连接.

c)特征分析.通过命令分析、多模式匹配算法等方法判别该访问的真实意图及行为导致的结果.

d)自律学习.如果某次非可信访问在经过了访问评估模块的分析后,被判定属于攻击行为范畴,就将此攻击呈现出的行为特征联合现有知识库的数据进行整体分析,找到攻击行为在初期状态下的访问特征.然后对安全问题的产生条件和早期征兆进行预测,基于智能决策支持技术对攻击特征进行自律学习,并将结果数据更新至现有知识库.

4　仿真实验

为了测试本模型的容侵性能,仿真实验在 ORACLE 11*g* 数据库服务器上,在 24 h 内高频度随机施加了入侵和攻击行为.为了降低实验结果误差,使用开源的 ORACLE 性能测试工具 ORABM 进行 24 h 不间断性能测试,并计算单位时间的性能均值,数据库系统在遭受攻击状态下,系统的容侵能力见图 3.通过仿真实验结果可以得出,应用了本安全模型的数据库系统的每秒事务处理量(transaction per second,TPS)表现比较正常,经计算均值为 2 101.根据目标数据库正常运行情况下的 TPS 计算均值为2 110可以得出,在被施加

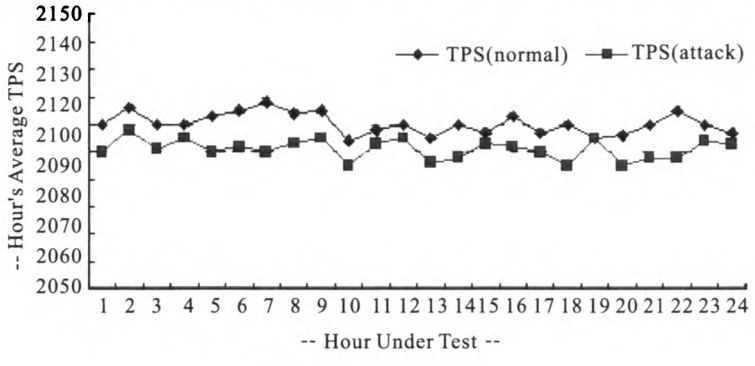

图 3　TPS 测试对比

Fig. 3　TPS evaluation

了入侵和攻击行为之后,应用了本安全模型的数据库系统可以稳定不间断地提供服务,从而对自律式容侵安全数据库模型的容侵性能在实际运行中进行了验证.

5 结论

针对现有的容侵数据库系统普遍存在自适应性不足的问题,提出了一个自律式容侵安全数据库模型.该模型采用分层模式,关键模块包括了数据库访问请求的可信程度评估和非可信访问的主动容侵保护,能够自主完成信度阈值数据和容侵知识库的自适应和自学习过程,从而达到了对非可信访问的有效容侵,令数据库系统具备较高的自修复和自优化特征,保障了高安全性和高可靠性领域的数据库系统安全.

参 考 文 献:

[1] FRAG A J S,POWELL D. A fault and intrusion tolerant file system[Z]. Proc of the 3rd International Conference on Computer Security,Washington DC,1985

[2] DOBSON J E,RANDELL B. Building reliable secure systems out of unreliable insecure components[Z]. Proc of IEEE Symposium On Security and Privacy,Oakland,1986.

[3] WU T,MALKI N M,BONEH D. Building intrusion tolerant applications[Z]. Proc of the 8th Conference on USENIX Security Symposium, Berkeley,1999.

[4] MARSH M A,SCHNEIDER F B. CODEX: a robust and secure secret distribution system[J]. IEEE Trans on Dependable and Secure Computing, 2001, 1(1): 34 - 47.

[5] ZHOU L,FRED B S,RENESSE R. COCA: a secure distributed on-line certification authority[J]. ACM Trans on Computer Systems, 2002, 20(4): 329 - 368.

[6] RABIN T. A simplified approach to threshold and proactive RSA[Z]. Proc of the 18th Annual International Cryptology Conference on Advances in Cryptology,London,1998.

[7] JARECKI S,LYSYANSKAYA A. Adaptively secure threshold cryptography: introducing concurrency, removing erasures[Z]. Proc of Advances in Cryptology-EUROCRYPT,Berlin,2000.

[8] CANETTI R,GENNARO R,JARECKI S. Adaptive security for threshold crypto systems[Z]. Proc of the 19th Annual International Cryptology Conference on Advances in Cryptology, London,1999.

[9] CUKIER M,COURTNEY T,LYONS J. Providing intrusion tolerance with ITUA[Z]. Proc of International Conference on Dependable Systems and Net works (DSN), Washington DC, 2002.

[10] 王慧强,吕宏武,赵倩,等. 一种关键任务系统自律可信性模型与量化分析[J].软件学报,2010,21(2)344 - 358.
WANG Huiqiang,LÜ Hongwu,ZHAO Qian,et al. Model and quantification of autonomic dependability of mission-critical systems[J]. Journal of Software,2010,21(2):344 - 358.

[11] 吴庆涛,华彬,郑瑞娟. 基于自律反馈机制的入侵容忍模型[J].微电子学与计算机,2011,28(4):99 - 102.
WU Qingtao,HUA Bin,ZHENG Ruijuan. Intrusion tolerance model based on autonomic feedback mechanism[J]. Microelectronics & Computer,2011,28(4):99 - 102.

(责任编辑:孟素兰)