一种主动防御的数据库审计子系统①

王振铎[1], 王振辉[2], 陈绥阳[1], 王艳丽[2]

[1](西安思源学院 电子信息工程学院, 西安 710038)
[2](西安翻译学院 工程技术学院, 西安 710105)

摘 要: 针对数据库审计技术存在的缺陷, 提出利用数据库会话技术, 设计具有实时提醒和处理安全风险能力的数据库审计子系统. 系统详细记录用户的操作行为, 对非法入侵行为进行主动处理, 增加了审计系统的主动防预能力, 将“事后审计分析”提前到“事后及时处理”. 该系统应用证实有效提高了数据库的安全性, 保护了企业和用户的信息.

关键词: 数据库审计; 会话; 主动防御; 触发器

Development of Database Auditing Subsystem with Active Defense

WANG Zhen-Duo[1], WANG Zhen-Hui[2], CHEN Sui-Yang[1], WANG Yan-Li[2]

[1](School of Electronic & information, College of Siyuan, Xi'an 710038, China)
[2](School of Technology and Engineering, Xi'an Fanyi University, Xi'an 710105, China)

Abstract: According to the shortcomings of database audit technical, Put forward a method of designing a real time and security risk capacity database audit subsystem based on database sessions. The system records the user’s operation behavior, hand the illegal invasion behavior actively, adding the active prevention ability of the audit system, it can advance the"post audit analysis"to "after the timely processing ". The system proved effective in improving the security of databases, protect business and user information.

Key words: database audit; session; active defense; trigger

2012 年 5 月 17 日, WEB 应用防护与数据安全高峰论坛在杭州举行, 国家信息中心、中国科学院、中国人民银行及微软、安恒、新浪等单位的安全专家, 无不对 web 应用安全忧心重重[1].

随着外部攻击和内部数据偷窃的增加, 常用的认证、授权和访问控制等基本的数据库安全方法已经无法应对复杂的安全形式了. 事实上, 现在的信息泄漏和篡改事件大多是“内部人员”所为, 他们有合法的账号密码, 他们可以堂而皇之的窃取数据库信息, 根本不用任何攻击手段, 防火墙、入侵检测之类的传统安全系统根本发现不了. 因此, 对数据库系统的使用情况进行审计, 势在必行.

本文分析了目前数据库审计技术的发展和研究现状及不足, 结合实际项目, 提出了基于数据库会话技术, 准确捕获操作者, 实现细粒度的审计功能, 从用户的登陆、退出到用户对数据库实体和记录所做的任何更改进行详细记录, 并根据系统用户表中详细的注册记录, 对用户的非法行为进行主动提醒和处理, 将传统的“事后审计分析”提前到“事后及时处理”.

1 数据库审计技术的发展

数据库审计技术发展趋势经历了 4 个阶段[2]. 第一阶段: 流量行为审计技术, 主要对数据库访问行为进行分析和统计, 如 IP、端口、连接次数等; 第二阶段: 基于内容的审计技术, 主要对数据库访问行为实现内容记录, 如数据库登录账号、SQL 语句等; 用户可以利用该技术实现对 SQL 操作进行记录、分析和统计, 该阶段能够满足对数据库审计的基本需求, 但是在响应

① 基金项目:陕西省教育厅科研计划(12JK1055)
收稿时间:2013-02-16;收到修改稿时间:2013-04-15

和分析的精度上存在较大误差, 难以满足大中型用户对数据库审计的需求; 第三阶段: 实现对 SQL 语句的语义分析, 尽可能的将操作数据库的 SQL 语句进行细粒度解析, 比如账号名、数据库名、数据表名、字段名、字段值、返回码等, 以满足针对各种违规行为的精确检测、响应和审计; 第四阶段: 从工具转变为助手, 审计系统大大减少了系统管理员的工作量, 通过对数据库操作人员的事前、事中及事后的操作行为进行全面的审计, 及时发现问题, 避免造成更大的损失. 也就是说数据库审计系统对于用户来讲正在逐步从信息审计的工具转变为可靠易用的得力助手.

2 数据库审计技术的研究现状

各大型数据库厂商为了应对复杂的安全形式, 都提供了数据库审计功能和独立安装的数据库监控程序, 例如: Oracle 的 DBMonitor, MySQL 的 Monitor 等, 但均采用数据库日志文件进行事后审计, 存在诸多的弊端, 比如: 数据库审计功能的开启会影响数据库本身的性能、数据库日志文件本身存在被篡改的风险, 难于体现审计信息的真实性[3]. 并且日志审计功能并不能进行灵活的配置, 仅仅是简单的日志记录, 并不能帮助管理者及时发现问题, 快速定位问题; 并且不具有监测报警的功能, 不能在第一时间将异常信息报告给数据库管理者, 只能用于问题查证[4]. 数据库日志文件的作用不仅局限在审计方面, 更多的是用于数据库的故障修复, 并且该文件会占用过多的磁盘空间, 管理员在日志文件中查询数据的变更情况好比大海捞针.

国内各数据库厂商也做了相当多的研究, 有一些好的数据库审计产品[5], 但这些产品功能过于复杂, 操作不方便, 需要培训, 并且价格较高, 很难在众多 Web 系统中被采用.

3 数据库会话的重要性

会话是用户与数据库服务器的一种特定连接[6]. 当用户由数据库服务器验证时会话开始, 当用户退出或出现异常终止时会话结束. 它也是数据库服务器对连接数据库的用户进行记录的一种手段. 使用 SessionID(也称为审计会话标识符)记录每一个用户会话, 通过对会话标识符分析, 区分不同的会话过程, 对每个会话过程记录状态, 从会话中取得用户名和数据库名, 登录时间等记入会话信息中. 对于用户的后续会话过程, 数据库将会把已获取的用户名和数据库名填入审计记录中, 通过数据中存放的会话信息可以精确定位到具体操作用户. 故数据库会话是审计的基准, 利用它可以在第一时间查出具体操作人员的登录访问信息. 笔者长期从事 Web 项目开发, 在实际应用过程中, 对各种潜在的安全问题, 进行了深入的研究, 开发了一套通用的, 跨平台的数据库审计子系统, 有效实现了数据库操作动态监控的问题, 为数据库的安全增加最后一道防线.

4 审计子系统的设计

审计子系统的设计目标是对数据库系统中可能出现的问题进行事后审计. 该子系统主要解决的问题包括以下几个方面的内容:

(1) 身份的审计

(2) 操作内容的审计

(3) 操作时间的审计

(4) 发现问题, 限制非法访问

审计子系统以“何人、何时、何地、何种操作”为主要设计思想, 利用 jsp 编程技术, 监控程序可以很方便的获得连接数据库的远程客户的 IP 地址和 MAC 地址(这部分的内容属于安全系统中的安全登录子系统中记忆的, 详见[7]), 并和用户注册表中的地址进行比对, 如果不存在该地址, 监控程序以会话的方式自动断开该连接, 以防止用户进一步非法操作, 并将该地址和账号计入黑名单表中, 如果该地址有效, 则进一步记录该用户对数据表所做的操作, 记录到操作日志表中.

为此, 系统设计了两个数据表, 一个是操作日志表, 另一个是黑名单表, 日志表中主要记录操作账号、IP 地址、操作的数据表、操作类型、执行的 SQL 语句等; 黑名单表用于记录非法用户的账号、IP 地址等信息.

审计子系统的功能主要包括:

(1) 初始化: 由程序自动在数据库中创建日志表和黑名单表以及各个需要审计的数据表的触发器.

(2) 操作日志管理: 日志的查询, 非法账号的过滤, 非法 IP 的过滤, 加入黑名单和批量加入黑名单.

(3) 黑名单管理: 黑名单查询, 移出黑名单.

(4) 消息提醒和处理: 对非法用户和用户的非法操作进行消息提醒, 管理员可以主动进行处理.

5 关键技术

5.1 获得真实操作者

在 Web 系统开发中, 连接池作为优化数据库性能的一个方法已经广泛应用在系统中了, 例如, 在一个数据库账户下只有一个共享连接, 所有用户都使用这个共享连接更新客户信息, 当然用户并不知道他们使用的是同一个数据库账户, 从信息安全的角度来思考这种实现, 给我们提出了一个问题, 究竟谁才是这个连接的真正操作者[8]?

通过数据库会话, SessionID 可以获得数据库连接的客户端 IP, 会话时间等信息, 但是如果 Web 系统中用户通过代理服务器访问数据库, 这样在数据库会话中记录的就不是客户的真实 IP, 数据库审计就不准确了. 我们利用事前检测机制设计的安全登录子系统可以获取用户登录的真实 IP、帐号等信息, 并连同 SessionID 一并记录到用户登录表中, 以后用户所有的操作都会以这个 SessionID 记录, 这样前台登录和数据库会话技术的结合, 就获得了用户的真实身份.

5.2 触发器的应用

审计子系统使用触发器技术自动记录登录用户对数据表的操作行为. 在大型数据库中均提供触发器的功能, 触发器(trigger)是个特殊的存储过程[9], 它的执行不是由程序调用, 也不是手工启动, 而是由事件来触发, 比如当对一个表进行操作(insert, delete, update)时就会激活它执行. 触发器经常用于加强数据的完整性约束和业务规则等. 触发器有两种, DML 触发器和 DDL 触发器, 当数据库中表中的数据发生变化时, 包括 insert,update,delete 任意操作, 如果我们对该表写了对应的 DML 触发器, 那么该触发器自动执行. DDL 的活动审计一直很重要, 并且是最常使用的审计线索之一[10]. 从安全的观点来看, DDL 命令都是潜在的最具有破坏力的命令, 易被攻击者利用从而破坏系统.

DDL 触发器主要用于审核与规范对数据库中表、触发器、视图等结构上的操作. 比如在修改表, 修改列, 新增表, 新增列等. 它在数据库结构发生变化时执行, 我们主要用它来记录数据库的修改过程, 以及限制程序员对数据库的修改, 比如不允许删除某些指定表等.

例如, 为了防止恶意攻击者, 对数据库中的表、存储过程等实体进行修改和删除, 特别是创建新的数据表, 我们可以编写 DDL 触发器, 用于禁止用户创建、删除、修改数据表和存储过程.

```
create trigger deny_delaltertable_delproc
on database
for
create_table, drop_ table, alter_ table,
create_procedure,alter_procedure,
drop_procedure
as
print '您不能创建数据表, 删除表和其它可编程对象'
rollback;
```

同时, 为了方便管理员操作审计子系统, 触发器不需要手工创建, 管理员可以通过系统中提供的功能, 选择需要进行审计的数据表, 系统自动为该表创建日志管理的触发器. 例如: 用户登录系统后, 系统记录登录信息的同时, 将信息同时写入操作日志表的触发器代码, 如下:

```
create trigger insert_audio
on tbl_user_login
for insert,update,delete
as
begin
declare @UserID      AS bigint
declare @UserIP      AS varchar(20)
declare @UserKind AS varchar(20)
declare @UserIP      AS varchar(20)
if exists (select 1 from inserted) AND NOT exists
   (select 1 from deleted)
   set @UserKind = ‘插入数据’
if exists (select 1 from inserted) AND exists (select
   1 from deleted)
   set @IsUpdate =  ‘修改数据’
if not exists (select 1 from inserted) and exists(select
   1 from deleted)
set @IsDelete = ‘删除数据’
select @UserIP=userIp from tbl_login where
      Session_id=@@spid
select @UserID = Session_id,
        from sys.dm_exec_connections where
      Session_id=@@spid
insert into tbl_audio(session_id, session_ip,
      session_time, session_table,session_kind)
```

```
        values(@UserID,@UserIP,getdate(),
                'tbl_user_login', @UserKind)
    end
```

5.3 查询操作的审计

如上所述，利用触发器仅仅能够实现对数据的插入、修改、删除进行审计，但无法实现对查询操作的审计，而数据库中大量的操作对数据的查询，一些表中的关键数据只能有权限的用户才能查询，否则会造成数据泄密，这对于金融、政府等关键部门是难以接受的，所以对查询操作的审计同样至关重要.

为此，对各大型数据库，进行了细致的研究，发现数据库查询操作存放在系统数据库的表中，以 SQL Server 数据库为例，各会话的操作存放在 master 数据库的 sysprocesses 表中[11]，该表详细记录了各会话对数据库的操作，故我们可以方便地通过程序对用户的查询操作进行审计，防止无权限的用户看到重要数据.

5.4 执行 SQL 语句的详细审计

在审计子系统中，日志表中不仅记录用户对数据表的操作类型，而且可以详细记录用户所执行的 Sql 命令，在图 1 中的详情连接即可帮助管理员详细了解用户执行的数据情况.

图 1　审计子系统审计功能界面图

详细的 Sql 语句也依靠系统表中记录的会话缓存记录，例如 Sqlserver 数据库存放在 sys.syscacheobjects 中，如图 2 所示:

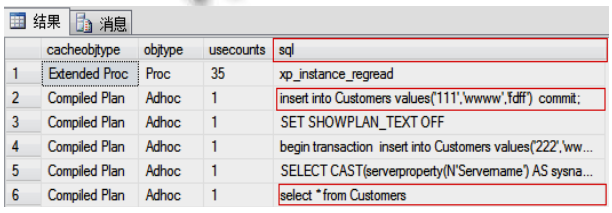

图 2　SQL 语句执行记录图

5.5 动态消息提醒

该功能在触发器触发记录用户操作行为的同时，会根据自动进行非法操作检测，并浮动出一个消息窗口，及时提醒管理人员，询问是否对风险进行处理，是继黑名单后审计系统中增加的又一个主动防御的功能，类似于杀病毒软件的提醒框. 采用 Jquery 的 dialog 对话框技术实现. 如图 3 所示:

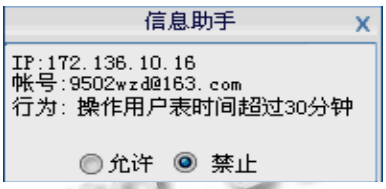

图 3　风险预警消息图

6　实验及性能优化

为了验证该系统的准确性，将系统加入到已使用的 Web 系统中，系统环境为 Sqlserver2005 和 MySql5.0.2，证明审计结果真实可信，并能达到主动防御的功能. 经过 Web 自动化测试工具和 DataFactory 数据库测试工具的使用发现，审计子系统的操作日志表的数据量日益增大，为了提高其操作性能，主要采用了三种技术进行优化. 第一，设计了分页的存储过程提高数据检索效率；第二，操作日志数据要不断的产生，该页面也要能够显示最新的日志数据，采用了 Ajax 技术自动刷新页面数据的功能，减轻服务器的负载；第三，为了提高 SQL 的性能，利用阿里巴巴开源平台上的一个项目 Druid 插件，创建数据库连接池，编写程序，扩展 JDBC 数据库的功能和提高 SQL 执行的性能.

7　结论

本文利用数据库会话结合应用层用户注册和登录信息，实现了操作者真实身份的获取，核实用户的权限，并利用触发器技术，实现了数据库操作行为的细粒度审计. 同其它系统相比，系统界面友好，操作简便，支持 Sqlserver、Oracle、MySQL 数据库，功能实用，审计内容详细，并且增加了主动防御、过滤和阻止非法用户的功能，同时该系统基于 java 语言开发计的，支持跨平台使用. 经过在 Web 项目中应用，证明该系统占用资源少，可以满足数据审计和动态防御的要求. 在后期的研究中，还将进一步扩展主动监控和防御的功能，以减少事后审计的情况.

参考文献

1 中国计算机安全.2012WEB 应用防护与数据安全高峰论坛杭州举行. [2012-05-24]. http://sec.chinabyte.com/406/12342906.shtml.

2 中国软件网.慧眼数据库审计系统的技术原理[2011-04-26].http://www.soft6.com/v9/2011/pldj_0426/150594.html.

3 瑞星网.数据安全防“脱库”解决方案[2012-01-13].http://www.rising.com.cn/newsletter/news/2012-01-13/9744.html.

4 CIO 时代网.浅析数据库安全现状及其安全审计[2011-05-17].http://www.ciotimes.com/infrastructure/sjk/49737.html.

5 计世网.慧眼数据库审计系统浮出的内幕[2011-04-25].http://soft.ccw.com.cn/news/htm2011/20110425_925262.shtml

6 赛迪网.数据库信息安全需求紧迫面临严峻挑战[2010-02-01].http://tech.ccidnet.com/art/1105/20100201/1991923_1.html.

7 王振辉,王振铎.一种安全登录子系统的设计与实现.科学技术与工程,2012,12(22):1671−1815.

8 陈晨,陈怀楚,高国柱,等.基于oracle数据库的数据审计系统的设计与实现.实验技术与管理.2005,22(12):76−79.

9 魏权利,李丽萍.数据库触发器技术在 Web 软件中的应用.微型机与应用,2011,30(9):3−5.

10 TechTarget 数据库网站.数据库安全审计手册[2012-05-14].http://www.searchdatabase.com.cn/guide/databaseaudit.htm.

11 MSDN.SQL Server 系统表.http://msdn.microsoft.com/zh-cn/library/ms179932(v=SQL.90).aspx.

12 唐小丹.基于中心节点的数据库跟踪审计系统.计算机应用与软件,2011,28(10):159−162.

13 李亿红,徐韧,程祥圣.基于 XML 和 WebService 的数据库审计系统.计算机应用与软件,2010,27(1):198−200.

14 李晶媛,韩慧莲.一个基于误用检测的数据库安全审计系统.计算机与数字工程,2009,37(10):116−119.

15 陈海东.ORACLE 数据库审计功能和触发器在医院数据监管中的应用.中国医疗设备,2008,23(7):43−44.

(上接第 233 页)

5 Dai XZ, Xu J, Peng YN, et a1. A new Method of Improving the Weak Target Detection Performance Based on the M IMO Radar, 2006 CIE International Conference on Radar. Shanghai, 2006:24−27.

6 Haimovich AM, Blum RS, Cimini LJ. MIMO Radar with Widely Separated Antennas. IEEE Trans. Signal Processing, January, 2008:116−129.

7 Toica P, Li J, Xie Y. On Probing Signal Design For MIMO Radar. IEEE Trans. Signal Processing August, 2007,55(8):4151−4161.

8 Chang S, Li H, Xu CH. MIMO radar detection performance analysis. Materials Science and Information Technology. Trans Tech Publications, 2012.

9 常帅,李宏,徐长辉.MIMO 雷达检测性能分析.电子设计工程,2011,24:90−93.

10 曾涛,龙腾,王洪波.准连续波跟踪雷达信号处理机的设计与实现.北京理工大学学报,1999,19(5):604−607.