ORACLE 数据库存储过程应用安全①

刘伟祥, 周建宁, 张 捷

(公安部交通管理科学研究所, 无锡 214151)

摘 要: 针对目前各行业管理信息系统应用过程中存在的通过反编译存储过程擅自修改存储过程中的业务逻辑或破解数据库加密校验位算法违规办理业务的情况, 提出了一种 oracle 数据库存储过程反编译和异常使用的检测方法, 给出了数据库存储过程安全应用监控平台的系统设计原理和实现方案, 并给出了系统具体实现的关键技术.

关键词: 应用安全; 数据库存储过程反编译

Application Security of Oracle Databas Stored-Procedure

LIU Wei-Xiang, ZHOU Jian-Ning, ZHANG Jie

(Traffic Management Research Institute, Ministry of Public Security, Wuxi 214151, China)

Abstract: In the process of management information system applications, a small number of non-compliance staff without authorization to modify the stored procedure decompile the business logic in stored procedures or crack the database cryptographic checksum algorithm illegal to conduct business. This paper presents an oracle database stored procedure decompile and abnormal detection methods to solve these problems, it given the system design principles and implementation of a database stored procedure security application monitoring platform and gives a concrete realization of the key technologies.

Key words: application security; database stored procedure decompile

随着信息化建设的不断发展, 基于 B/S(Browser/Server)模式, 或者基 WebService 的模式的网络服务已成为信息系统发展的主流. Web 的开放性、易用性和 Web 应用的易于开发性使得 Web 应用的安全问题日益突出[1], 解决 WEB 应用的安全性问题无论在理论上还是工程上都是热点问题. Web 安全是一个系统问题, 包括 Web 服务器安全、Web 应用服务器安全、Web 应用程序安全、数据传输安全和应用客户端安全[2]. 在现实应用中逐步建立了发布安全管理、运行安全监控[3]、Web 应用安全[4]、主要业务逻辑采用数据库存储过程实现[5]等方面的多层次全方位的安全防护体系, 但这些都是建立在 oracle 数据库不被攻击、存储过程加密文件不能被反编译的基础上. 在实际的应用中也陆续发现了一些违反信息系统安全的做法, 主要包括以下四种方式: ①通过反编译统一下发的数据库存储过程, 修改里面的业务逻辑, 重新加密后再更新至工作数据库中. ②反编译统一下发的数据库存储过程后, 通过分析存储过程业务判断逻辑寻找系统的漏洞进行违规操作. 比如通过获取加密校验位算法后自行修改工作数据库记录, 再将记录的校验位更新为正常校验位. ③在工作数据库上编写自行开发的存储过程操作数据库, 办理违规业务. ④在工作数据库上非法建立触发器, 影响系统的安全运行.

1 方案设计

现阶段 Oracle 数据库存储过程加密文件能被反编译无法避免, 但是如果作为监管者如果能够及时发现和制止违规操作, 对不法分子将是一个极大的威慑.

① 收稿时间:2012-07-01;收到修改稿时间:2012-08-27

解决上述问题的关键是能有效判定工作数据库的存储过程是否被篡改或非法调用、用户自定义的存储过程是否有违规操作. 解决办法包括以下四个方面: ①通过比较加密存储过程的行数和长度判断存储过程是否被修改. ②通过数据库审计系统收集非法调用存储过程的情况并进行分析, 判定违规操作. ③通过比较当前用户下的存储过程包和统一下发的存储过程包的一致性来检测用户自定义存储过程的使用情况, 并将自定义存储过程发送到监管系统中进行后续处理. ④调整存储过程中加密算法的生成模式, 避免直接调用存储过程加密算法修改数据校验位的情况发生.

1.1 系统结构

根据系统的功能要求及数据交换需求, 系统涉及到存储过程发布更新软件, 业务管理信息系统和信息系统安全运行监控软件(以下简称监管软件)三个系统, 存储过程安全发布更新软件为独立的 C/S 程序、存储过程检测系统作为功能模块嵌入到交通管理信息系统中、数据库审计系统通过数据库本身审计功能实现.

存储过程版本控制系统、存储过程异常监测系统、数据传输管理作为功能模块内嵌于信息系统安全运行监控软件中, 其系统结构如图 1 所示:

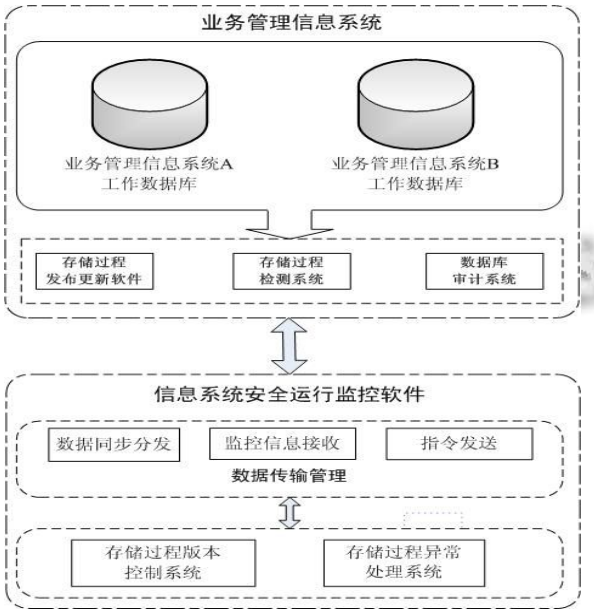

图 1 系统结构图

① 存储过程发布更新软件. 提供存储过程加密/解密、存储过程安全发布、存储过程资料管理等功能, 实现数据库存储过程的安全发布管理.

② 存储过程检测系统. 提供存储过程定期扫描、存储过程异常信息收集上传、存储过程异常信息报警等功能, 实现对存储过程发布和使用的动态监控管理.

③ 数据库审计系统. 通过开启数据库审计功能, 对可能导致违规操作的功能点进行审计, 重点审计调用存储过程加密校验位算法、手工修改数据库记录等的数据库操作.

④ 统计监管软件. 存储过程监控及异常处理作为功能模块内嵌在统计监管系统中, 提供存储过程异常处理、存储过程版本控制、预警信息发布等功能, 实现对存储过程异常情况的后续管理功能.

1.2 流程设计

存储过程保护在分发过程中必须解决三个问题: ①存储过程的发布必须在指定的合法的数据库上执行. ②存储过程的非法异常使用能及时进行预警和监控. ③系统能及时收集违规证据并进行分析处理. ④数据库加密校验位算法不能直接调用. 因此系统的升级维护在流程上有严格的要求. 其业务流程分为四个环节: 存储过程加密、存储过程发布、存储过程检测、存储过程监控机异常处理, 如图 2 所示:

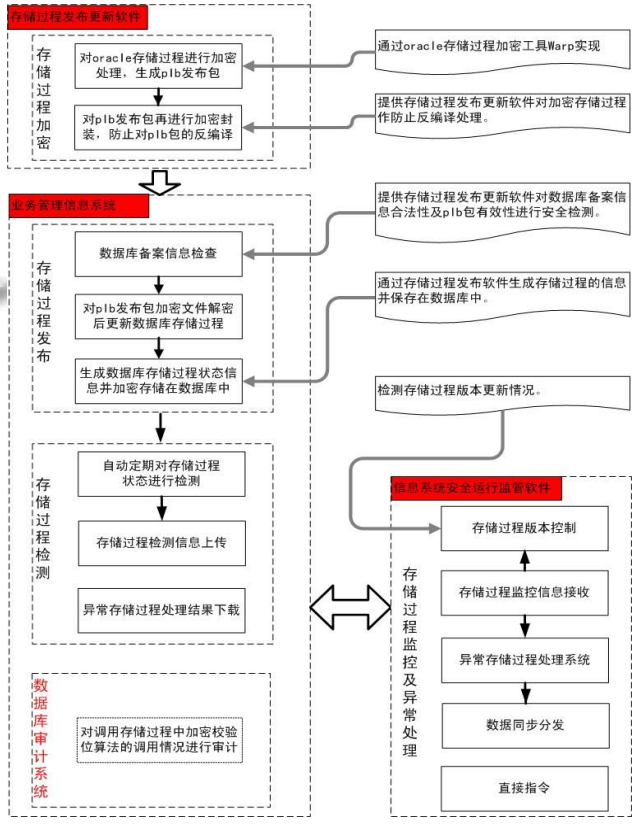

图 2 业务流程图

1.2.1 存储过程加密

软件在发布和升级前需要对数据库存储过程进行加密处理，避免非法用户直接反编译统一下发的存储过程. 其措施分为两个方面:

①通过 oracle 的 warp 工具对数据库存储过程明文进行加密，生成 plb 发布包.

②通过存储过程发布更新软件对 plb 文件进行对称加密处理，避免不通过存储过程发布更新软件而在数据库上直接执行存储过程包.

③存储过程发布更新软件根据要下发的存储过程包，生成 plb 发布包的配置信息并和发布软件一起下发.

1.2.2 存储过程发布

存储过程的更新发布必须通过存储过程发布更新软件进行操作，根据存储过程发布的处理流程，其工作原理如下:

①存储过程发布更新软件对业务工作数据库的备案信息进行检查，确保数据库是已经在监管软件进行过安全备案.

②数据库备案信息检查通过后，存储过程发布更新软件对下发的 plb 包进行解密，并验证 plb 的合法性.

③存储过程发布更新软件将解密后的 plb 发布包更新至业务工作数据库中.

④存储过程更新完成后，存储过程发布更新软件读取 plb 发布包配置信息，生成存储过程的检测信息.

1.2.3 存储过程检测

存储过程检测系统作为功能模块内嵌入业务管理信息系统中，通过对存储过程进行定期扫描，检查和发现存储过程的异常情况. 其工作机制如下:

①系统定期对存储过程进行体检，发现异常及时将信息上传至监管软件进行后续处理.

②系统定期将存储过程的信息上传至监管软件，便于监督者对存储过程的版本进行管理.

③如发现异常存储过程，由监管者在监管软件处理后下载到业务工作数据库中. 系统通过读取处理结果信息进行实时预警或停止部分业务功能.

④数据库审计系统功能由数据库本身实现，通过定制审计内容实现对非法操作敏感数据或函数的实时监控.

⑤定期检查业务工作数据库上触发器的情况，并上传至监管软件.

1.2.4 存储过程监控异常处理.

存储过程监控异常处理的功能模块在监管软件中实现，主要包括以下几个方面:

①接收各地上传的存储过程监控信息，并进行分类存储.

②对上传的有异常嫌疑的存储过程进行解密为明文后进行分析，如确认异常则通过短信方式告知系统管理员；如确认正常则将处理结果写入下载信息表中.

③存储过程版本控制: 统计各地升级情况，根据情况可强制要求进行升级.

④数据同步分发: 将处理结果信息分发到各地业务工作数据库中.

⑤直接指令: 如需要直接停止存储过程或对存储过程在业务系统中进行预警，至直接发送指令生效. 控制未按时升级存储过程的使用期限.

1.3 功能设计

按照软件分布，业务管理信息系统工作数据库存储过程应用安全的由存储过程发布更新软件、存储过程检测系统和存储过程控制及异常处理模块组成，其系统功能如下图 3 所示:

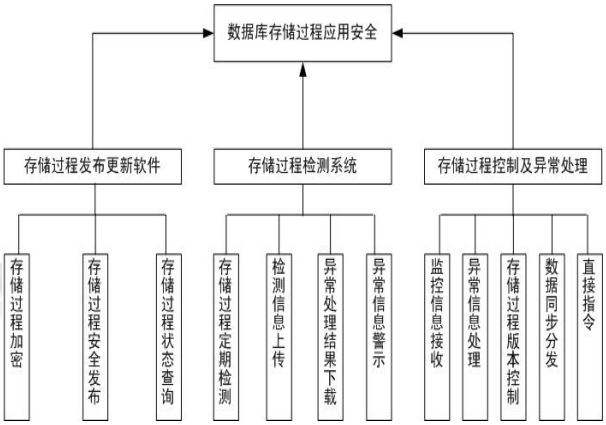

图 3　系统功能图

①存储过程发布更新软件采用 C/S 模式，存储过程机密通过对称算法实现;

②存储过程定期检测的的内容包括存储过程行数、存储过程大小、创建时间、执行时间、编译时间、版本号、是自定义存储过程还是统一下发存储过程等信息;

③异常信息处理包括异常存储过程明文的查询功能、异常信息短信告知. 告知类型分为 A021-存储过程非法修改、A022-存在异常存储过程包、A023-存储过

程状态信息非法修改. 异常描述信息未存储过程包名+异常情况.

2 关键技术

2.1 存储过程合法性验证

通过 oracle 的 warp 工具加密后的数据库存储过程的行数和大小是固定的, 如篡改存储过程则很难保证和原存储过程行数和大小保持一致. 通过检测存储过程的行数和大小可以监控到加密后的存储过程是否被修改. 具体方法如下:

① 读取存储过程的行数语句一下:

select max(LINE) from user_source where name= 'ADMIN_CHECK_PKG'

② 读取存储过程的大小的语句如下:

select sum(length(text)) from user_source where name='ADMIN_CHECK_PKG'

③ 读取存储过程状态信息

select t.object_name"名称",t.last_ddl_time"执行日期",t.timestamp"编译日期"from user_objects t

其中 “'ADMIN_CHECK_PKG”为存储过程名称.

2.2 数据库加密校验位算法

Oracle 调用 jar 包的 java 加密算法, java 算法里增加时间戳判定, 避免模拟存储过程调用 java 加密算法的问题, 作为内部函数或私有方法是用. 具体方法如下:

① 加载 class 进 oracle loadjava 在 oracle 的 bin 目录下

loadjava -u trff_app/trff_admin -r -f -v f:\oscar.class

② 建立存储过程

create or replace function oscar_quote2(string varchar2) return varchar2 as language java name 'oscar.aa(java.lang.string) return java.lang.string';

③ 加密机制

a)在 J2EE 层通过 Oscar 中的 dd 方法将当前数据库时间经 AES 加密后生成密文.

b)密文传到存储过程中, 由存储过程将密文与需加密的字符串一同传送至 JAVA 存储过程中.

c)Java 存储过程校验时间密文, 如果送过来的时间与当前数据库时间在 60 秒以内的, 系统将允许调用算法. 否则禁止调用. 存储过程入口为 gg(key,content). 内容字串加密的规则为, 先通过 AES 进行加密, 随后通过 MD5 压缩编码长度. 返回压缩后编码.

2.3 预警机制建立

预警信息通过短信、系统提示方式告知系统管理员和监管者数据库存储过程的异常违法调用情况. 定义三类消息模式, 其格式如下:

① A021-存储过程非法修改. 消息内容: xtlb+azdm, 存储过程包名被非法修改.

② A022-存在异常存储过程包. 消息内容: xtlb+azdm, 存储过程包名+异常.

③A023-存储过程状态信息非法修改. 消息内容: xtlb+azdm, 存储过程包名+记录非法修改

3 结语

通过对数据库存储过程异常使用情况的监测和分析方法的使用, 提供了技术手段和管理机制避免了违规情况的发生, 极大地威慑了不法分子的违规违法行为. 通过对业务信息系统使用过程中异常情况的网上监管, 为信息系统的应用安全提供了重要的技术保障. 但也存在一些不足, 例如通过 Java 混淆机制对关键加密算法进行保护, 虽然增加了不法分子的违法难度, 但也存在被攻破的可能. 下一步将从如何更加有效防止 Java 反编译等安全防护手段等方面进一步提高 Web 应用系统的安全等级.

参考文献

1 丁妮.WEB 应用安全研究[硕士学位论文].南京:南京信息工程大学,2007.

2 包勇强,江海龙,邵志骅,是建荣.交通管理信息系统软件安全设计与应用.智能交通,2009,17(4):106–110.

3 江海龙,季君,邹伟.公安交管信息系统 Web 应用安全研究.中国公共安全,2011,24(3):84–87.

4 孙娜,曹君.存储过程的数据库安全性应用研究.计算机与数字工程,2009,233(3):154–156.