数据库安全在电力信息系统等级保护中的应用

梁智强，胡朝辉，江泽鑫，周强峰

（广东电网公司电力科学研究院 智能电网所，广东 广州 510080）

摘 要：简述了数据库安全，详细介绍了电力信息系统对数据库安全的要求，并介绍了在电力信息系统中用到的保障数据库安全的具体措施。

关键词：电力信息系统；数据库安全；MySql；Oracle；Sybase；SQL Server

中图分类号：TP311 **文献标识码**：A **文章编号**：1674-7720(2012)21-0079-03

Database security application for the classified protection of information system security in the power information system

Liang Zhiqiang, Hu Zhaohui, Jiang Zexing, Zhou Qiangfeng

(Electric Power Research Institute of Guangdong Power Grid Corporation, Guangzhou 510080, China)

Abstract: In this paper, we briefly introduce the database security technology, make a detailed description of the database security requirement for power information system, and at last we give the practical measures in the actual project.

Key words: power information system; database security technology; MySql; Oracle; Sybase; SQL Server

1 信息系统安全等级保护

随着信息技术的发展，越来越多的信息化、自动化设备被用于政府办公自动化和企业的生产经营活动，公用信息基础设施建设使得群众生活、生产日益依靠信息系统。信息系统在给政府、企业带来便利的同时，也引入了信息安全问题，黑客入侵和网络攻击的日益增多，信息系统中存在的漏洞、后门、运行维护人员信息安全知识的匮乏等使得部分关系到国计民生的关键系统受到了前所未有的安全挑战。特别是信息安全事件所引发的连锁安全事故，危害极大，如花旗集团受到黑客攻击导致36万多的客户账户信息被窃取，直接导致金融的混乱；四川某水电站无故全厂停机造成川西电网瞬间缺电80万千瓦引起的大面积停电事故等。这些均说明了信息安全的重要作用。

为此，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合颁布了关于印发《信息安全等级保护管理办法》的通知，要求公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》作为信息系统等级保护的国家标准，从物理安全、网络安全、主机安全、应用安全和管理安全等方面对其安全强度做出了具体的规定[1]。

电网企业、国家电力监管委员会、公安部等同样非常关注电力行业的信息系统安全等级保护，分别制定了相应的规范、作业指导书用于其等级保护测评。数据库是信息系统的重要组成部分，也是等级保护测评主要的测评实体之一。随着近年来智能电网研究的发展，数据库作为重要的技术之一在电力信息系统中得到越来越多的应用，如能量管理系统、调度自动化系统和配网自动化系统等广泛使用数据库来保存关键数据。因此，保证数据库的安全，防止敏感数据被窃取、被篡改有着十分重大的实现意义。

数据库威胁可以分为物理威胁和逻辑威胁。按照GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》，数据库物理威胁主要包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电等（其中物理位置的选择主要是指如数据库主机应该放置在防震、防风、防雨的建筑内[1]，物理访问控制主要是指数据库主机所在机房应该设置门禁等），具体的要求可以查看相应的国家标准。数据库物理威胁防护措施比较简单，主要通过机房建设得以保证。而逻辑威胁的防护内涵十分丰富，是本文研究的重点。

在电力信息系统中，经常使用的数据库包括 MySql、Oracle、SQL Server 和 Sybase 等。数据库的语法包括三类[2-3]：数据操作语言 DML（Data Manipulation Language），用于查询、插入、删除和修改数据库中的数据；数据控制语言 DCL（Data Control Language），用来控制存取许可、存取权限等；数据定义语言 DDL（Data Definition Language），用来建立数据库、数据库对象和定义其列，本文将根据电力信息系统中的数据库实际防护措施，选择相应的配置指令进行介绍。

2 数据库的身份鉴别

数据库的身份鉴别是数据库安全的第一道门槛，电力信息系统绝大部分是二级信息系统和三级信息系统，GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》对二/三级信息系统均要求："操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别"[1]。在实际数据库安全测评时，数据库所处机房的门禁系统可作为第一种鉴别技术，第二种身份鉴别技术主要通过数据库系统的登录密码来实现。数据库的身份鉴别技术主要包括用户名和密码验证、密码的定期更换、远程登录管理的数据防窃听三部分内容[4]。

2.1 用户名和密码的验证

数据库安全防护的第一步是检查数据库是否采取用户名+密码形式的登录验证方式[3,5]。数据库的安全配置及网络登录必须采取用户名+密码的验证形式；密码在数据库当中以密文的形式保存；且需要及时修改数据库默认帐号的默认密码。

在 MySql 数据库中，使用如下指令查看数据库中的用户权限信息（包含是否采用用户名+密码的验证方式登录）：

```
Use Mysql;(选择数据库，数据库的用户权限列表保存在 Mysql 数据库中的 user 表中)
Select*from user;(查询用户权限列表)
```

根据查询的结果检查相应用户是否设置了密码，并通知未设置密码的用户设置密码。

Oracle 数据库带有很多默认账户，如 sys、system、sysman、scott、aqadm 和 dbsnmp，其默认的密码分别为 change_on_install、Manager、oem_temp、tiger、aqadm、dbsnmp。需要及时修改这些默认账户及相关密码，防止非授权用户通过默认账户登录数据库系统窃取、篡改数据等。

2.2 密码的定期更换

按照等级保护的要求，系统运维人员需要对数据库的登录密码进行定期更换。

MySql 数据库使用 SET PASSWORD FOR root = PASSWORD('new_password') 指令更换密码（注：在该模式下需再次使用 FLUSH PRIVILEGES 指令告诉服务器再次读入授权表，使密码更换生效），如在 shell 模式下，可采用 mysqladmin-u root password new_password 指令更换密码。

如果使用 Oracle 数据库[6]，则可以使用 select*from dba_profiles 指令查看数据库用户密码策略，其查询结果 PASSWORD_GRACE_TIME XX 表示账户密码的生命周期（单位为"天"）。

2.3 远程登录管理的数据防窃听

电力信息系统一般要求数据库不开放远程登录功能，但并未是强制性要求。如果开放了远程管理的功能，则需采取必要的网络防护措施对网路通信进行加密，如采用加密模式对网络通信进行加密或开启数据库的 OpenSSL 功能等。

在 SQL Server 数据库当中，可以采用 exec sp_configure "remote access" 指令来查看是否可以对数据库进行远程连接，其结果：1 表示容许远程访问，0 表示不容许远程访问。

3 数据库的访问控制

电力信息系统要求数据库启用访问控制功能，其主要包括：用户的权限管理、权限最小原则等。

3.1 用户权限管理

数据库的用户权限管理主要是指对不同的用户分配不同的权限，不使用特权用户对数据库操作及配置。

以 MySql 数据库为例，数据库的用户权限查看及修改指令如下：

```
Use Mysql;(选择数据库)
Select * from user;(查询用户权限列表)
```

根据查询到的用户权限结果，使用 GRANT 和 REVOKE 指令对用户的权限进行修改，语法如下：

```
GRANT priv_type[(column_list)]
                [,priv_type[(column_list)]...]
ON {tbl_name|*|*.*|db_name.*}
    TO user_name [IDENTIFIED BY 'password']
    [,user_name [IDENTIFIED BY 'password'] ...]
    [WITH GRANT OPTION]
```

其中，GRANT 代表对用户进行授权操作，可用于授权及创建用户；priv_type 指的是数据库操作权限，可以从如下集合中取值{ALL PRIVILEGES，FILE，RELOAD，ALTER，INDEX，SELECT，CREATE，INSERT，SHUTDOWN，DELETE,PROCESS,UPDATEDROP,REFERENCES,USAGE}；参数 ON {tbl_name|*|*.*|db_name.*} 为用户权限的使用范围，*.* 代表用户权限范围为所有数据库的所有表，db_name.* 代表 db_name 数据库的所有表。

3.2 权限最小原则

权限最小原则是指针对不同的用户，为其分配使用数据库的最小权限，若使用 MySql 数据库，其指令如下：

```
REVOKE priv_type[(column_list)]
```

[,priv_type[(column_list)]...]
ON{tbl_name|*|*.*|db_name.*}
FROM user_name[,user_name...]

其中 REVOKE 用于用户权限的收回，其他参数的含义同 GRANT 指令参数。

对于数据库的多余用户账户，应及时删除。在 MySql 数据库中，可以使用 Delete user where User='username' 指令删除多余账户。在 Oracle 数据库中，可以使用指令 select*from dba_users；select*from dba_users t where t.expiry_date <sysdate；select LOCK_DATE，username from dba_users；来查看数据库中是否有多余、过期或被锁定的账号。

4 安全审计

除了数据库的身份鉴别、访问控制以外，还需对数据库进行安全审计。审计的范围包括服务器及重要的客户端，审计的内容包括用户行为、系统资源的使用情况和重要系统指令的使用情况等。

以 Oracle 数据库为例，数据库安全审计的检查应该包含如下内容：

(1)检查数据库是否开启了审计功能：

show parameter audit_trai；

(2)检查数据库中的日志使用情况：

select*from V$LOG

(注：检查结果中的 group 表示日志组号，bytes 显示日志文件大小，ARC 显示日志文件是否归档，status 表示日志有状态)

(3)检查数据库的审计级别：

select*dba_stmt_audit_opts

(4)根据数据库的审计级别查看审计内容：

select*from dba_stmt_audit_opts；

select privilege，user_name from dba_priv_audit_opts；

select owner，object_name，object_type，INS，SEL from dba_obj_audit_opts；

5 资源控制功能

除了对数据库本身的访问控制以外，还需对安装数据库的服务器进行资源控制，包含对服务器的 CPU、硬盘、内存和网络资源使用情况进行监视，设置客户端操作超时锁定等[7]。

6 入侵防范及网络数据安全传输

如同大部分网络服务器一样，在装有数据库的服务器上需要部署入侵防范措施。在电力信息系统中，通常在网络边界上部署防火墙或者其他 IDS 设备实现服务器的保护。在实际应用中，可以结合网络 SSL 协议、IPSec 协议和 HTTPS 协议等保护数据的安全传输。

还可以使用在数据库表中加入校验字段的方式实现数据加密[7-8]，客户端在对服务器数据库数据进行操作之前，使用加密算法，将需要传输的数据由明文转化为密文；在服务器端，使用特定的程序将密文转化为明文，并通过校验字段的检查来判断通信的数据是否被修改。此外，对于特别重要的数据还可以采用硬件加密的形式对其加密等。

本文主要讨论了电力信息系统中数据库安全防护的具体措施，总结了电力信息系统中使用的数据库安全技术，并给出了相应操作的代码。在实际的工作中，需根据实际情况采取相应的防护措施，及时形成电力信息系统数据库安全防护规范，以便在实际应用中开展安全防护工作。

参考文献

[1] GB-T 22239-2008. 信息安全技术 信息系统安全等级保护基本要求.2008.

[2] 王珊，萨师煊.数据库系统概论[M].北京：高等教育出版社，2010.

[3] 朱良根，雷振甲，张玉清.数据库安全技术研究[J].计算机应用研究，2004(9)：127-138.

[4] 王静，易军凯.基于入侵检测的数据库安全模型研究[J].微计算机信息，2006，22(9-3)：84-86.

[5] 马鲜艳.数据库安全技术探析[J].西安邮电学院学报，2008，13(3)：99-102.

[6] 李东风，谢昕.数据库安全技术研究与应用[J].计算机安全，2008(1)：42-44.

[7] 胡志奇.数据库安全与加密技术研究[J].计算机与现代化，2003(11)：58-61.

[8] 张剡，夏辉，柏文阳.数据库安全模型的研究[J].计算机科学，31(1)：101-104.

(收稿日期：2012-06-11)

作者简介：

梁智强，男，1983 年生，硕士研究生，高级工程师，主要研究方向：信息安全，电力调度自动化。