Proposed Solutions of Oracle Sysdba Security Hole

A. E. M. Eljialy
Omdurman Islamic University, Information System Department, Khartoum, Sudan
Ccst.abubaker@gmail.com

***Abstract*—Sysdba security hole allows attacker to commit crimes in a database management system. Therefore, this research aims at proposing different alternative solutions. In this respect, the main objective is to clarify the sysdba security hole attacking methodologies. Moreover, the researcher in this work will maintains sysdba security hole by proposing alternative solutions in order to eradicate the loopholes. The researcher introduces new technique known as RCSRE to overcome the sysdba security hole. In this context, this database security hole affects all support of Oracle versions; relational database management system (RDBMS).**

***Index Terms*—crimes, RCSRE, solutions, SYSDBA, security, hole**

I. Introduction

A. Paul's Ideologies in this Attack [1]

It has been assumed that Pirate gains sysdba using orabrute, attackers are then can create their own sysdba user called in this case hacker, and this is illustrated as shown below:

1.
SQL> CREATE USER PIRATE IDENTIFIED BY PIRATE
USER CREATED
2.
SQL> GRANT CREATE SESSION TO PIRATE
GRANT SUCCEEDED
3.
SQL> GRANT SYSDBA TO PIRATE;
GRANT SUCCEEDED
4.
SQL> COMMIT;
COMMIT COMPLETE

In the above mentioned SQL clauses, the PIRATE user became the user with SYSDBA privilege. Therefore, the PIRATE user can do any SQL fraudulent clauses (DDL, DML and DCL commands).

B. Reveal of Attacker

The professional database security expert can reveal PIRATE user by checking different Oracle parameters to figure out the fraud. Furthermore, the reveal of PIRATE user can be done through the following SQL clauses:

SQL> SELECT NAME FROM SYS.USER$;
NAME
.....
ESOURCE
SCOTT
SYS
SYSTEM
PIRATE
HR
HS_ADMIN_ROLE

As indicated in the above SQL clauses SYS.USER$ reveals the PIRATE account. Therefore, the PIRATE account still hides from database administrator via the following fraudulent steps:

The attacker copies the current password file to a backup directory. Then Pirate deletes hacker sysdba account from the database. Also returns back the original password file and this fraudulent can be illustrated as shown below:

Locate the password file

[oracle@vmw] locate orapworcle
/u01/app/oracle/product/10.1.0/db_1/orapworcl

Backup the password file by copying the password file in a safe directory. Thus, it allows the attacker to delete the original file, this fraud can be indicated as demonstrated below:

Cp /u01/app/oracle/product/10.1.0/db_1/orapworcl
/u01/app/oracle/product/10.1.0/db_1/orapworclsu

Delete the PIRATE SYSDBA user by using the following SQL DML command as shown below:

SQL> DROP USER PIRATE CASCADE;
USER DROPED

The attacker Returns back the original password file from safe directory by copying. Hence, the attackers implements Linux command to retrieve back the original password file as illustrated below:

Cp /u01/app/oracle/product/10.1.0/db_1/orapworclsu
/u01/app/oracle/product/10.1.0/db_1/orapworcl

If the administrator selects user from sys.user$, it will be obvious that the Pirate user is vanished, moreover, it is

Manuscript received January 02, 2013; revised April 16, 2013.

doi: 10.12720/jiii.1.2.68-71

difficult for the administrator to detect the existence of Pirate user as shown below:

```
SQL> SELECT NAME FROM SYS.USER$
NAME
.....
RESOURCE
SCOTT
SYS
SYSTEM
HR
HS_ADMIN_ROLE
```

The attacker still has another problem, which exists in the parameter 'V$PWFILE_USERS'. In this respect, the professional database administrator can figure out the PIRATE USER. Nevertheless, the pirate user still exists in the above mentioned parameter. Thus, it can be illustrated as follows:

```
SQL> SELECT * FROM V$PWFILE_USERS;

    USERNAME     SYSDBA  SYSOP  SYSAS
SYS          TRUE    TRUE FALSE
 PIRATE
     TRUE    FALSE   FALSE
```

II. The Proposed Solution

The researcher has proposed different alternative solutions as follows:

(a) The protection of Oracle password file.
(b) Hardening of database security
(b) RCSRE Technical solution.

(a) The major vulnerability of sysdba due to the unprotected password file, this can be summarized from the above PIRATE user scenarios. Therefore, the hardening of database security is highly significant [2].

The hardening of database security can be implemented in order to prevent the database security, this can be done through the following steps as follows:

(b) Hardening of database security In UNIX environment:

Set the umask to 022.

(1) Lock software owner account.
(2) Set umask to 022.
(3) Set the adequate permission.
(4) Ensure limited file permission for init.ora
(5) Check default password file permission.
(6) Check the user sys got strong password
(7) Limit or disallow privilege for sys user.
(8) Limit user who have DBA granted role.
(9) Don't collect sysdba , osdba, sysoper into one role.
(10) Limit user with admin privilege.

Limit access to sys.user$, sys.user_history, sys.link$ perfstate.stat$sql_summary, all_source, dba_roles, dba_sys_privs, dba_users, user_tab_ privs and user_role_privs.

(11) Revoke connect and resource roles from all users.
(12) Enable auditing.

Oracle enterprise should do well if monitor all sys DBA user by implementing database security.

Don't collapse OSDBA/SYSDBA, OSOPER/SYSOPER and database administrator into one role. Groups mapping to OSDBA role, the OSOPER role, and the software owner should be distinct [3].

Limit users who have with admin privileges this will limit users who can change schema and other system attributes [4].

Limit with grant options these create privilege chains in which a user is allowed to grant access to other users.

Fully understand, monitor, and review system privileges assigned to users and roles [5]. These are stored in dba_sys_privs. Remember the list of both users and roles and that there is a hierarchical role structure [6].

III. RCSRE Solution

A. Implementation of Interprocess Communication:

Depending on the concept of inter process communication (IPC), the researcher proposes implementation of this concepts in order to overcome SYSDBA security back door [7].

[8] This interprocess communication (IPC) concept allows the database administrator to monitor the Pirate user efficiently through conducting a background process technique [9], rather than directly tracing database user by keeping their log information in a synonymous. Whereas the researcher considers this concept that mentioned above, the database will reveal any modification of log information and alteration of privileges as well.

This proposed solution is performed by activating the role of business owner ,because the business owner is the stake holder of the firm, moreover, any database fraudulent actions affect business firms , so the business owner is usually the prime figure of the value organization assets.

The implementation of (RCSRE, i.e., Read, Create, Send, Receive and Email) can be categorised as follows:

(a) Read log information.
(b) Create processes.
(c) Send log information.
(d) Receive log information.
(e) Email to business owner.

B. Read Log Information

The researcher assumes that the pirate reaches the SYSDBA privileges via orabrute [10]. So, this is the major problem of this technique and in order to solve such a problem, computer professional could not protect database from orabrute, in spite of the progressive development in new technologies and innovations whereas database enterprises frequently offer.

In the first step, the database will read the log information from database SQL processor and actually in this step SQL reads all log information through special VIEW.

The RCSRE is similar to the auditing feature that has already been exhibited in Oracle within the familiar parameter on the init.ora file. In this respect, the researcher

tends to clarify the impossible solution of orabrute. Hence, it is better to monitor or trace the suspicious activities than overlooking fraudulent incidents.

Even the database security is offensive and self protective, the researcher introduces RCSRE techniques that make Oracle lags behind. In fact oracle deals with background processes. Moreover, Fig. 1 illustrates RCSRE reading log information below:

C. Create processes

According to interprocess communication concepts, it is very significant to create two processes in order to establish communication links between them. The researcher recommends RCSRE solution technique to be adopted in an Oracle product [7].

If the reader returns back to the architecture for external audit system (Ron Ben Natan, "implementing database security and auditing", 2005) , the reader will get a better way to trace a database fraudulent incidences[2].

The researcher of this work relies on Natan's concept in implementing interprocess concept in database auditing and this can be described as follows in the RCSRE solution technique:

D. Send log information from process 1 to process 5 as it has been shown in Fig. 2.

E. Process 5 receives the log information via inter process communication message queue identifier, which basically acts as a symmetric key.

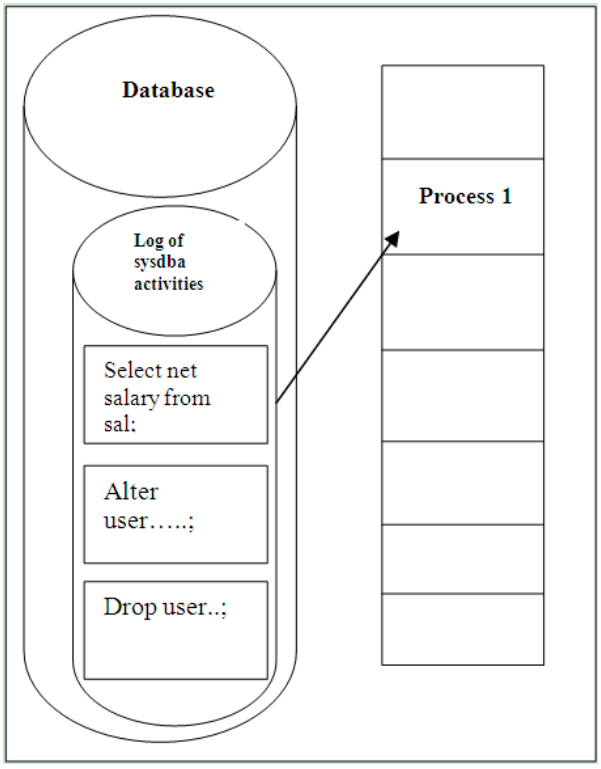

Figure 1. Reading of Log Information

F. Sending email to business owner in case of any SYSDBA suspicious activities. There are a lot of arguments about the size of email spool.

Hotmail, Yahoo and Gmail,...etc. In this situation, UNIX exchange server is capable of holding a high volume of emails.

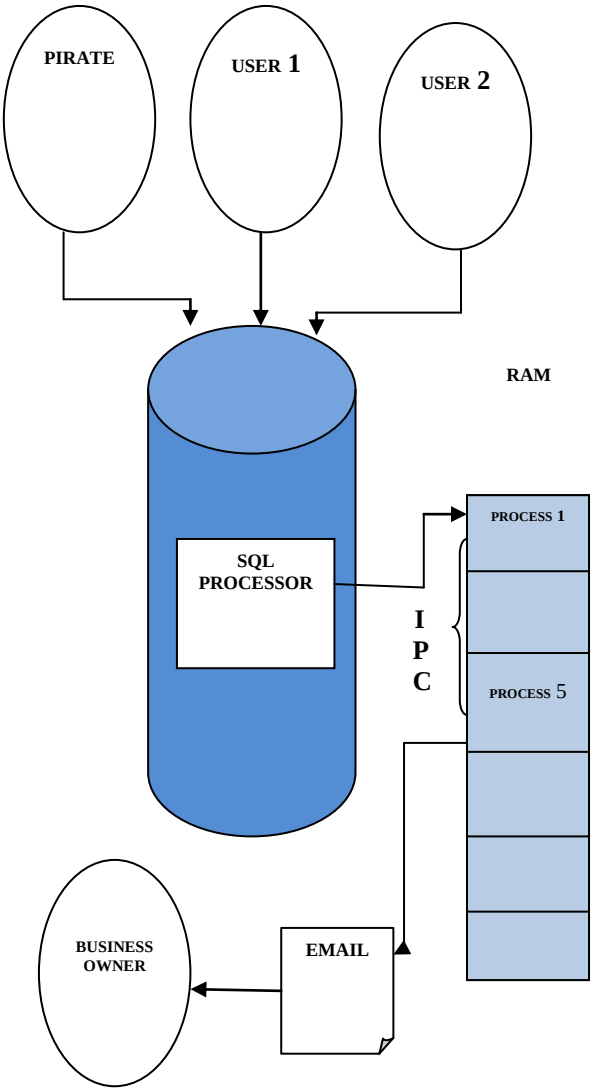

Figure 2. RCSRE technical solution.

IV. Conclusion

- SYSDBA attack methodologies have been identified.
- It has been proven that the database security hole starts with common SQL ORABRUTE attacks.
- The researcher introduces a number of proposed practical solutions.
- Oracle has to protect password file in order to avoid this database security hole.
- RCSRE solution technique applies business owner email as forensic stock, as it is of significance to be used in case of crime.

It has been proven that the SYSDBA security hole is a very hazardous security hole, therefore, the researcher introduces technical solution to eradicate the security problem.

As it has been shown in the research work the RCSRE technique is a feasible solution, thus database developer should consider.

In the light of database forensics, it is very difficult to reveal SYSDBA security hole. It is highly recommended to protect the database against any mischievous actions

through a continuous database auditing and applying of RCSRE technique. Therefore, the database management system must be protected because it's cost doing business.

ACKNOWLEDGMENT

Acknowledgment is extended to Dr. Salah Awad Elkarim for his technical assistance.

REFERENCES

[1] P. M. Wright. (October 2007). Oracle Sysdba Backdoor, SANS Organization. [Online]. Available: http://www.sans.org/resource/glossary.pdf
[2] R. B. Natan, "Implementing database security & auditing," *Elsevier*, 2005, pp. 6-16.
[3] Oracle Advanced Security with Oracle 11g release 2. Oracle Enterprise. (October 2011). [Online]. Available: http://www.oracle.com/us/products/database/security/overview
[4] P. M. Wright. (October 2012). Sys-throttle and Distributed Database Forensics. [Online]. Available: https://www.oracleforensics.com/wordpress/index.php/2012/10/
[5] Burleson. (December 2009). Oracle Security Auditing for Sys Connections. [Online]. Available: https://www.dba-oracle.com/security/auditing-sys-connections.htm
[6] B. Faroug. (December 2012). SQL Server 2012 Security. [Online]. Available:http://searchsqlserver.techtarget.com/feature/SQL-Server-2012-security-Changes-for-the-newest-version
[7] D. Boneh. (May 2010). SQL Injection Attacks & Defenses. Standford University. [Online]. Available: http://www.crypto.standford.edu/cs142/lectures/16-sql-inj.pdf
[8] Ryutov *et al.*, "The specification and enforcement of advanced security polices," U.S. Patent , 2006.
[9] H. Ramankutty. Interprocess communication. [Online]. Avialable: http://linuxgazette.net/104/ramankutty.html
[10] P. M. Wright. (June 2012). Burleson Consulting. [Online]. Available:http://www.dba-oracle.com/forensics/t-forensics-orabrute.htm

Dr. A.E.M. Eljialy
Assistant Professor - Omdurman Islamic University
PhD in Information Technology
M.Sc. in Computer Science
B.Sc. in Information Technology

