Selecting Software Packages for Secure Database Installations

Afonso Araújo Neto, Marco Vieira

This document includes complementary information for the paper "Selecting Software Packages for Secure Database Installations" which was submitted to the *Fifth Latin-American Symposium on Dependable Computing*. It contains information regarding the full list of security best practices, the corresponding importance weights and the full gap analysis matrix.

Table 1. DBMS configuration security best practices devised from the analysis of the CIS documents

#	SECURITY BEST PRACTICE (CIS)	Recommendations in CIS documents			
		M	O8	O10	S
	ENVIRONMENT				
1	Use a dedicated machine for the database	1	1	1	28
2	Avoid machines which also run critical network services (naming, authentication, etc)	1	1	1	1
3	Use Firewalls: on the machine and on the network border	1	3	3	1
4	Prevent physical access to the DBMS machine by unauthorized people				1
5	Remove from the network stack all unauthorized protocols		1	1	1
6	Create a specific user to run the DBMS daemons	1	1	1	
7	Restrict DBMS user access to everything he doesn't need	1	4	4	3
8	Prevent direct login on the DBMS user account	2	1	3	3
	INSTALLATION SETUP				
9	Create a partition for log information	2	1	1	1
10	Only the DBMS user should read/write in the log partition	1			
11	Create a partition for DB data	1	1	1	2
12	Only the DBMS user should read/write in the data partition	1			
13	Separate the DBMS software from the OS files	1	2	2	2
	Remove/Avoid default elements:				
14	»»»Remove example databases	1			1
15	»»»Change/remove user names/passwords	1	4	4	2
16	»»»Change remote identification names (SID, etc...)		3	1	
17	»»»Change TCP/UDP Ports		1	1	1
18	»»»Do not use default SSL certificates	1			
19	Separate production and development servers		1	1	
20	No developer should have access to the production server		5	5	
21	Use different network segments for production and development servers		1	1	1
	Verify all the installed DBMS application files:				
22	»»»Check and set the owner of the files	1	2	3	
23	»»»Set read/running permissions only to authorized users	4	18	22	14
	OPERATIONAL PROCEDURES				
24	Keep the DBMS software updated	3		1	1
25	Make regular backups	1			4
26	Test the backups	1		1	
	SYSTEM LEVEL CONFIGURATION				
27	Avoid random ports assignment for client connections (firewall configuration)		1	1	
28	Enforce remote communication encryption with strong algorithms	1	1	11	3
29	Use server side certificate if possible	1		1	
30	Use IPs instead of host names to configure access permissions (prevents DNS spoofing)		1	1	
31	Enforce strong user level authentication	2	6	8	4
32	Prevent idle connection hijacking		2	2	
33	Ensure no remote parameters are used in authentication	1	2	1	
34	Avoid host based authentication		1	1	
35	Enforce strong password policies	1	2		2
36	Apply excessive failed logins lock		1	1	
37	Apply password lifetime control		1	1	

38	Deny regular password reuse (force periodic change)		2	2	
39	Use strong encryption in password storage	3			
40	Enforce comprehensive logging	1	2	1	
41	Verify that the log data cannot be lost (replication is used)		2	2	1
42	Audit sensible information		14	19	25
43	Verify that the audit data cannot be lost (replication is used)		1		1
	Ensure no "side-channel" information leak (don't create/restrict access):				
44	»»»From configuration files		2	1	
45	»»»From system variables	1			
46	»»»From core_dump/trace files		8	8	1
47	»»»From backups of data and configuration files		1	1	4
	Avoid the interaction between the DBMS users and the OS:				
48	»»»Deny any read/write on file system from DBMS used	2	3	2	
49	»»»Deny any network operation (sending email, opening sockets, etc...)		4	3	
50	»»»Deny access to not needed extended libraries and functionalities	1	11	11	54
51	»»»Deny access to any OS information and commands	2			
APPLICATION LEVEL CONFIGURATION AND USAGE					
52	Remove user rights over system tables	1	23	25	1
53	Remove user quotas over system areas		3	1	
54	Implement least privilege policy in rights assignments		9	10	6
55	Avoid ANY and ALL expressions in rights assignments	1	3	3	
56	Do not delegate rights assignments	1	3	3	3
57	No user should have rights to change system properties or configurations	3	4	4	2
58	Grant privileges to roles/groups instead of users		1	1	3
59	Do not maintain the DB schema creation SQL files in the DB server		1		
Total number of recomendations		**48**	**166**	**183**	**177**

Table 2. Complementary DoD configuration best practices

#	COMPLEMENTARY BEST PRACTICES (DoD)	Group
1A	Monitor de DBMS application and configuration files for modifications	Operational Procedures
2A	Do not use self signed certificates	System Level Config.
3A	Protect/encrypt application code	Appl. Level Config./Usage
4A	Audit application code changes	Appl. Level Config./Usage
5A	Employ stored procedures and views instead of direct table access	Appl. Level Config./Usage

Best practices weights

The following table presents the individual weights given by the experts, the relative importance to the attack surface and the cumulative importance for each best practice. For each contributor, E stands for engineer and A for academic.

Best Practice	E1	E2	A3	A4	E5	A6	E7	A8	A9	Relative Weight	Cumul. Weight
4	4	4	4	4	4	4	4	4	4	5,26%	5,26%
3	4	4	4	4	4	4	4	3	4	4,73%	9,99%
19	4	4	4	3	4	4	4	4	3	4,21%	14,19%
28	3	4	4	3	4	4	4	4	4	4,21%	18,40%
57	3	4	4	3	4	4	4	4	4	4,21%	22,60%
2	3	4	3	3	4	4	4	4	4	3,68%	26,28%
24	3	3	4	4	3	4	4	4	4	3,68%	29,96%
39	4	3	4	3	3	4	4	4	4	3,68%	33,64%
35	4	3	4	2	3	4	4	4	4	3,63%	37,27%
15	4	3	4	4	3	3	3	4	4	3,15%	40,42%
1	3	4	3	2	4	4	4	3	4	3,10%	43,52%
6	2	4	4	2	4	4	4	2	3	3,00%	46,52%
52	2	3	4	3	3	4	3	4	4	2,58%	49,10%
25	4	4	3	3	1	4	4	3	2	2,52%	51,61%
20	3	4	3	3	4	3	4	3	3	2,10%	53,72%
23	3	3	4	3	3	3	4	3	4	2,10%	55,82%

18	3	3	3	2	3	3	4	4	4	2,05%	57,87%
31	4	4	3	2	4	3	3	3	3	2,05%	59,92%
8	2	3	2	3	3	4	4	3	4	2,00%	61,92%
29	2	4	3	2	4	3	4	3	3	2,00%	63,91%
51	2	4	3	2	4	3	3	3	4	2,00%	65,91%
32	3	4	2	1	4	3	3	4	3	1,99%	67,90%
36	3	3	3	2	3	3	4	3	4	1,52%	69,43%
54	3	3	4	3	3	2	3	4	3	1,52%	70,95%
33	4	3	3	2	3	4	3	2	3	1,47%	72,42%
37	3	2	3	1	2	3	4	3	4	1,41%	73,84%
10	2	3	3	1	3	4	4	3	1	1,41%	75,25%
12	2	3	3	1	3	4	4	3	1	1,41%	76,66%
42	2	2	3	2	2	4	4	3	3	1,37%	78,02%
41	3	1	1	1	1	4	4	2	2	1,24%	79,26%
22	3	3	4	2	3	3	3	3	3	1,00%	80,26%
34	3	3	4	2	3	3	3	3	3	1,00%	81,26%
5	3	3	2	2	3	3	4	3	3	0,95%	82,21%
48	2	3	4	2	3	3	3	3	3	0,95%	83,15%
21	3	3	2	3	3	3	4	1	3	0,94%	84,09%
47	2	2	4	3	2	3	3	3	3	0,89%	84,99%
38	3	2	3	1	2	3	4	3	3	0,89%	85,88%
55	3	3	4	1	3	1	3	3	2	0,88%	86,76%
46	2	2	4	3	2	3	3	2	3	0,84%	87,60%
50	2	2	4	2	2	3	3	3	3	0,84%	88,44%
7	2	2	3	2	2	3	4	2	3	0,79%	89,23%
44	2	2	2	3	2	4	3	2	3	0,79%	90,02%
45	2	2	2	3	2	4	3	2	3	0,79%	90,81%
49	2	2	4	2	2	3	3	2	3	0,79%	91,59%
26	3	3	2	2	1	2	4	2	3	0,78%	92,38%
40	4	1	1	2	1	3	3	3	2	0,77%	93,15%
43	2	2	3	1	2	3	4	2	2	0,73%	93,88%
9	3	1	1	2	2	3	4	2	1	0,72%	94,60%
4A	1	1	4	1	1	3	3	2	2	0,71%	95,32%
11	2	1	1	2	2	3	4	2	1	0,67%	95,98%
17	2	1	2	1	1	2	4	2	2	0,62%	96,60%
13	1	1	1	1	1	2	4	1	2	0,60%	97,20%
56	3	3	3	2	3	3	3	3	3	0,47%	97,67%
30	2	3	2	1	3	3	3	3	2	0,31%	97,98%
1A	2	3	2	2	3	2	3	3	2	0,26%	98,24%
53	2	2	3	2	2	1	3	3	3	0,26%	98,50%
58	3	2	1	3	2	2	3	2	3	0,26%	98,76%
27	2	3	1	1	1	3	3	1	3	0,24%	99,00%
2A	2	2	3	1	2	1	3	3	2	0,20%	99,20%
14	1	1	2	3	1	3	3	2	1	0,19%	99,39%
5A	2	2	2	3	2	2	3	2	2	0,16%	99,55%
16	2	2	2	1	2	3	3	2	2	0,15%	99,70%
59	2	2	1	2	2	3	3	2	2	0,15%	99,85%
3A	3	2	2	1	2	2	3	1	2	0,15%	100,00%

Overall results of the experimental evaluation of 7 different software packages.

DBMS Engine	Operating system	Package N.	MP	NSMC	%
SQL Server 2005	Windows XP	1	79	131,5	76%
Oracle 10g	Red Hat Enterprise Linux 5	2	74	118,5	68%
	Windows XP	3	73	118	68%
PostgreSQL 8	Red Hat Enterprise Linux 5	4	73	123	71%
	Windows XP	5	68	114,5	66%
MySQL Community Edition 5	Red Hat Enterprise Linux 5	6	66	110	64%
	Windows XP	7	66	110,5	64%

GAP ANALISYS MATRIX

The following table presents the complete gap analysis matrix of the 7 packages, not included in the paper.

Security Mechanism (*The package offers support for...*)	Component Target	Package 1	Package 2	Package 3	Package 4	Package 5	Package 6	Package 7
Disabling access to extended stored procedures and functions	DB	X	X	X	X	X	X	X
Config. the system to always encrypt a remote connection to the DBMS	DB	X	X	X	X	X	X	X
Encrypting the connection of developer applications	DB	X	X	X	X	X	X	X
Removing system privileges of DBMS userids	DB	X	X	X	X	X	X	X
Restricting read/write privileges of a partition to a specific userid	OS	X	X	X	X	X	X	X
Automated installation of DBMS pending patches	DB	X						
Automated installation of OS pending patches	OS	X	X	X	X	X	X	X
Configuring the DBMS to store credential information using a reliable encryption scheme	DB	X	X	X	X	X	X	X
Configuring the OS to store credential information using a reliable encryption scheme	OS	X	X	X	X	X	X	X
Defining all DBMS passwords during the installation phase	DB	X	X	X	X	X	X	X
Defining all DBMS userids in the installation phase	DB	X						
Defining all OS passwords during the installation phase	OS	X	X	X	X	X	X	X
Defining all OS userids during the installation phase	OS							
Relying the DBMS on an outside specialized authentication mechanism	DB	X	X	X	X	X		
Relying the OS on an outside specialized authentication mechanism	OS	X	X	X	X	X	X	X
Removing all privileges of users over all systems tables.	DB							
Warning DBMS users, in a password change operation, that their new passwords are weak and cannot be accepted	DB				X			
Warning OS users, in a password change operation, that their new passwords are weak and cannot be accepted	OS	X	X	X	X	X	X	X
A DBMS authentication procedure that requests only credential information to the remote users	DB	X	X	X	X	X	X	X
An authentication procedure for remote clients that identify individual end users instead of individual applications	DB	X						
An OS authentication procedure that requests only credential information to the remote users	OS	X	X	X	X	X	X	X
Configuring the DBMS so only administrators have access to log	DB	X	X	X	X	X	X	X

information								
Configuring the OS so only admins. have access to log information	OS							
Configuring the system to drop idle connections after a specific period of inactivity	DB		X	X	X	X	X	X
Configuring the system to require that remote clients have the correct server certificate installed	DB	X			X	X	X	X
Denying login into the DBMS from a credential with more than a specified number of failed authentication attempts	DB				X			
Denying login into the OS from a credential with more than a specified number of failed authentication attempts	OS		X		X		X	
Forcing the DBMS users to change their passwords when they're older than a specified time frame	DB				X			
Forcing the OS users to change their passwords when they're older than a specified time frame	OS		X		X		X	
Identifying systems privileges of DBMS userids	DB	X	X	X	X	X	X	X
Setting read/write/execution privileges over files	OS	X	X	X	X	X	X	X
Setting that a userid cannot login	OS	X	X	X	X	X	X	X
Setting who can change configuration files	OS	X	X	X	X	X	X	X
Setting who can change environment variables	OS	X	X	X	X	X	X	X
Specifying privileges in a row/value level	DB		X	X				
Using custom defined SSL certificates for encrypted connections	DB	X	X	X	X	X	X	X
Changing DBMS userids already in use	DB	X			X	X	X	X
Changing OS userids already in use	OS	X	X	X	X	X	X	X
Changing passwords of DBMS userids already in use	DB	X	X	X	X	X	X	X
Changing passwords of OS userids already in use	OS	X	X	X	X	X	X	X
Creating an OS userid with limited privileges	OS	X	X	X	X	X	X	X
Creating file systems partitions	OS	X	X	X	X	X	X	X
Identifying DBMS userids with default passwords	DB							
Identifying default DBMS userids	DB							
Identifying default OS userids	OS							
Identifying OS userids with default passwords	OS							
Identifying users with privileges over systems tables	DB	X	X	X	X	X	X	X
Making a backup copy of the database	DB	X	X	X	X	X	X	X
Making a backup copy of the OS which can be used to restore the environment to its current state	OS	X		X		X		X
Storing the backup in a custom storage place	DB	X	X	X	X	X	X	X
Testing the installation of DBMS new patches	DB							
Testing the installation of OS new patches	OS							
Using a privilege limited userid to successfully install the DBMS.	OS		X		X		X	
Using a privilege limited userid to successfully load a DBMS process.	OS	X	X	X	X	X	X	X
Warning the admin that the last data backup is not up-to-date anymore	DB	X						
Warning the administrator that the last OS backup is not up-to-date anymore	OS							
Warning the administrator that there are DBMS vendor patches remaining to be applied	DB	X						
Warning the administrator that there are OS vendor patches remaining to	OS	X	X	X	X	X	X	X

be applied								
Allowing the DBA to not use ANY and ALL expressions	DB	X	X	X	X	X	X	X
Allowing to explicitly state that a particular privilege cannot be delegated	DB	X	X	X	X	X	X	X
Auditing a variety of important DBMS events	DB	X	X	X				
Auditing data changes	DB	X	X	X				
Blocking non-DBAs from delegating their privileges	DB							
Blocking privileges not inherited from groups/roles	DB							
Blocking the usage of ANY and ALL expressions in privileges granting	DB							
Changing listening TCP/UDP ports	DB	X	X	X	X	X	X	X
Changing remote identification information already in use. (e.g., SID)	DB	X	X	X	X	X	X	X
Config. the DBMS so only DBAs have access to audited information	DB	X	X	X				
Configuring the system to always establish connections through the same TCP/UDP ports during the installation phase.	DB	X			X	X	X	X
Configuring the system to always establish connections through the same TCP/UDP ports.	DB	X	X	X	X	X	X	X
Defining all remote identification information during the installation phase	DB	X	X	X	X	X	X	X
Defining listening TCP/UDP ports during the installation phase	DB		X	X	X	X		X
Disabling the generation of core_dump files	OS	X	X	X	X	X	X	X
Disabling the generation of trace files	DB	X	X	X	X	X	X	X
Encrypting backups with a reliable encryption algorithm	OS							
Identifying available functions that interact with the operating system	DB							
Preventing specifying sensitive information in configuration files. (e.g., not require specifying password in configuration files, etc.)	OS	X	X	X	X	X	X	X
Preventing the general use of sensitive information in systems variables	OS	X	X	X	X	X	X	X
Preventing the installation of a database example during installation	DB		X	X	X	X	X	X
Removing quotas over systems areas	DB	X	X	X				
Setting and discarding a complex password for a userid	OS	X	X	X	X	X	X	X
Setting privileges to groups or roles	DB	X	X	X	X	X		
Setting the owner of files	OS	X	X	X	X	X	X	X
Specifying important events which occur in the DBMS that should generate a finger print	DB	X	X	X				
Specifying important events which occur in the OS that should generate a finger print	OS	X	X	X	X	X	X	X
Specifying privileges in a column level	DB	X						
Specifying privileges in a database level	DB	X	X	X	X	X	X	X
Specifying privileges in a table level	DB	X	X	X	X	X	X	X
Warning DBMS users that their passwords are older than a specified time frame	DB				X			
Warning OS users that their passwords are older than a specified time frame	OS	X	X	X	X	X	X	X
Warning the administrator if any important configuration or file was modified	OS							
Writing procedures that generate a trace for data changes	DB	X	X	X	X	X	X	X
Creating stored procedures	DB	X	X	X	X	X	X	X
Creating views	DB	X	X	X	X	X	X	X
Disabling a network protocol	OS	X	X	X	X	X	X	X

Identifying active protocols in the network stack	OS	X	X	X	X	X	X	X
Identifying available extended functions in general	DB							
Identifying available functions that can be used to perform network operations	DB							
Identifying available functions that can be used to read/write in the file system	DB							
Identifying example databases	DB							
Identifying users with quotas over systems areas	DB	X	X	X				
Removing a database	DB	X	X	X	X	X	X	X
Selecting a different partition for OS log information	OS	X	X	X	X	X	X	X
Selecting a different partition than the main OS partition for auditing info	DB	X	X	X				
Selecting a different partition than the main OS partition for DBMS log information	DB	X	X	X	X	X	X	X
Selecting a different partition than the main OS partition for the data files	DB	X	X	X	X	X	X	X
Setting/unsetting access privileges over peripherals	OS		X		X		X	
Setting/unsetting read/write/execute privileges over files	OS	X	X	X	X	X	X	X
Testing if a recently created backup correctly restores the database data to its corresponding state	DB							
Testing if a recently created backup correctly restores the system to its corresponding state	OS							
Warning administrators of ANY and ALL expressions used in privileges assignments	DB							
Warning admin of users with the power of delegating their privileges	DB							