A new comparative study of database security

Daniel BĂRBULESCU, Adriana-Cristina ENACHE-DUCOFFE, Mihai TOGAN

Faculty of Computer Science, Military Technical Academy, Bucharest, Romania
danutbarbulescu@gmail.com, adryanaenache@gmail.com, mihai.togan@gmail.com

Abstract: Data is being stored electronically increasingly more, and the importance of databases has therefore increased significantly. Given that the data collected is used for various reasons and the sensitivity of the data can differ, the importance of database security is crucial. Although, database security has been on the "agenda" of security experts for a long time, technologies have changed and databases have evolved accordingly. In this paper, the aim is to offer a refreshed perspective of the security measures implemented in databases nowadays, with a comparison study of two popular databases: Oracle and Microsoft SQL. The comparison will provide the strengths and weaknesses of both database systems after analyzing the authentication, authorization, encryption, auditing and user management features provided by both, to help determine which Database Management System has a more comprehensive asset of tools to protect its internal data. Furthermore, this paper can also offer a guide for database administrators, to help them choose the best strategy and tools to secure their databases.

Keywords: Database security, DBMS, Oracle Database Server, Microsoft SQL Server.

Un nou studiu comparativ privind securitatea bazelor de date

Rezumat: Din ce în ce mai multe date sunt stocate electronic, prin urmare importanța bazelor de date a crescut în mod semnificativ. Întrucât datele colectate sunt folosite în diverse scopuri și sensibilitatea acestor date este diferită, securitatea bazelor de date are o importanță deosebită. Deși securitatea bazelor de date a fost pentru mult timp în "vizorul" experților de securitate, tehnologiile s-au schimbat și bazele de date au evoluat în concordanță. În această lucrare ne propunem să oferim o perspectivă actualizată a mecanismelor de securitate implementate la nivelul bazelor de date de astăzi, printr-un studiu comparativ a două dintre cele mai populare baze de date de astăzi: Oracle și Microsoft SQL. Studiul comparativ va oferi punctele forte și punctele slabe ale ambelor sisteme de baze de date, după analizarea mecanismelor de: autentificare, autorizare, criptare, auditare și gestionare a utilizatorilor, pentru a ajuta la determinarea sistemului de management al bazelor de date care are un set complex de instrumente pentru a-și proteja datele interne. Mai mult, această lucrare poate fi un ghid pentru administratorii de baze de date, pentru a-i ajuta să aleagă cele mai bune strategii și instrumente pentru a securiza bazele de date.

Cuvinte cheie: Securitatea bazelor de date, DBMS, Server de baze de date Oracle, Server Microsoft SQL.

1. Introduction

Data is the most important resource for any organization in today's digital era, making the security of the database that stores it a priority. Threats for a database can either come from inside or outside the organization, which means that security measures of a database must assess both internal and external sources of a potential attack. Therefore, the security measures cannot be overlooked, and the security protocols must be robust and comprehensive to avoid any loss or theft of data which can have a negative impact on the organization's economic state and its client's confidence, implicitly.

The goal of database security measures is to ensure confidentiality, integrity, availability, authentication, authorization and auditing. Confidentiality guarantees that sensitive data is accessible only to users that are authorized. Integrity ensures that data within the database has not been altered or removed without the consent of authorized users. Availability is the ability to bring data from a database responsive to authorized users. Authentication is responsible for the verification of the identity of the users and making sure that only authorized users have access to the database. Authorization means that a user has a limited number of actions which can be performed on the database, such as removing data, altering data, adding data etc. Auditing ensures

https://doi.org/10.33436/v33i3y202302

a log of actions performed by every user that impacted the database, so that every user is held responsible for its actions.

A database is securely managed through a Database Management System (DBMS). The most popular database management systems include Oracle, MySQL, Microsoft SQL Server, PostgreSQL, and MongoDB (DB-Engines, 2023). From these candidates, Oracle and Microsoft were chosen, as these are two different database providers (MySQL is developed by Oracle). Therefore, in this paper, the security measures of the Oracle Database server and Microsoft SQL Server will be compared, being two of the most popular database management systems. Both servers supply authentication, authorization, encryption, user management features and auditing to make the system secure against possible internal or external threats. It will be taken into consideration the efficiency of the features provided, but also the pliability of the features, for the reason that a vast variety of options can be suitable for a broad group of people. The differences between the approaches for each security measure will be analyzed to determine the advantages and disadvantages of the two. The purpose of this paper is to also give a comprehensive understanding of the security features provided by both servers to help guide organizations to choose the suitable system according to their needs and requirements. The hypothesis is that both servers have implemented the same security measures to be competitive with one another, but small differences are expected to reveal when the analysis is conducted.

2. Literature review

Previous papers have covered major attacks directed at database servers and the security measures of the Microsoft SQL Server and Oracle Server, but a comparison between the two approaches has not been conducted. Therefore, this literature review will analyze the security measures described before. According to (King & Collmeyer, 1973), database sharing refers to the granting of simultaneous access to a database. Conforming to (Ilić et al., 2021) Oracle users can share databases, while SQL Server does not have this capability, thus having better protection. As reported by (MS SQL Server 2022, 2022), in the official documentation of the SQL Server, database sharing is possible and it's described on how to do so explicitly, consequently, both systems have the same vulnerability from this stand of view.

Cloud computing has become a relevant field because it brings several advantages to digital era such as scalability, cost savings, disaster saving and many more. That being the case, both Oracle Server and Microsoft SQL Server have a cloud alternative based on the two engines described realising the importance of cloud coverage. The most important technique for securing cloud databases is encryption, according to (Soofi, Khan & Amin, 2017), the results show that the majority of approaches are based on encryption (45%) out of which 71% of encryption techniques results are validated. Conforming to (Kulkarni & Urolagin, 2012), the major attacks on databases can be categorized as inference, passive, active and SQLIA. Inference refers to the use of legitimate data to infer unknown information without having right to directly retrieve that information (Murray, 2010). As said by (Kulkarni & Urolagin, 2012): passive attack, the attacker only observes data present in the database and regarding to an active attack, actual database values are modified. SQLIA (SQL Injection Attack) occurs when an attacker changes the intended effect of an SQL query by inserting new SQL keywords or operators into the query (Halfond, Viegas & Orso, 2006). All the security measures assessed in this paper, if configured properly, are efficient steps against the attacks mentioned.

3. Comparison among found vulnerabilities

In a previous paper (Litchfield, 2006), the comparison between the security of the two products focused only on the number of security flaws found and fixed from December 2000 until November 2006. The latest vulnerability statistics (CVE MS SQL Server, 2023) (CVE Oracle Server, 2023) on Microsoft SQL Server and Oracle Server offer a better overview.

Figure 1 displays clearly that more vulnerabilities have been found over the years in the Oracle Database Server. More vulnerabilities do not necessarily mean that the Oracle Database Server is less secure than Microsoft SQL Server, it must be taken into consideration what vulnerabilities have been found to determine the gravity of a vulnerability. Many vulnerabilities were found to suggest that Oracle Server has been better tested, therefore more secure.

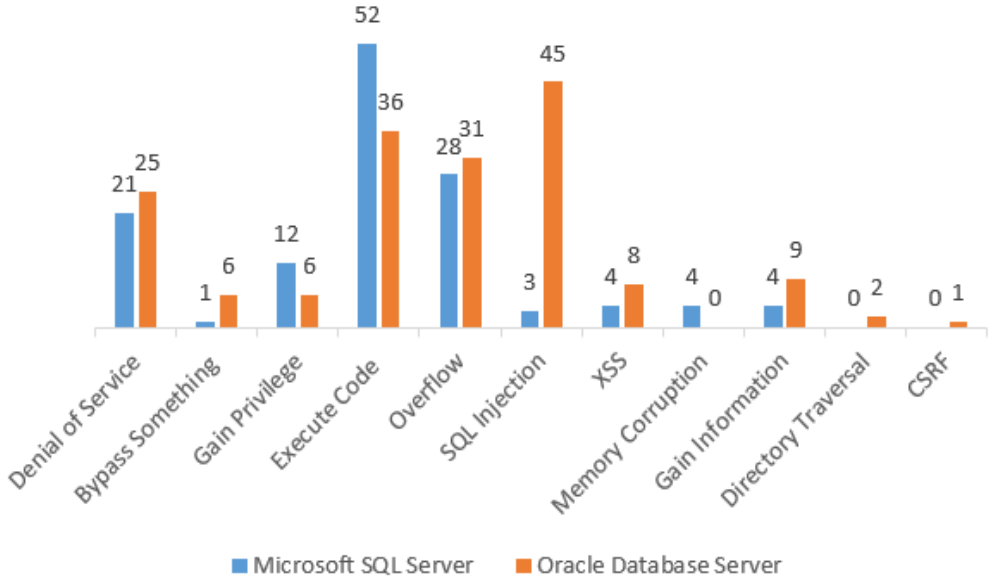

Figure 1. Vulnerabilities by year (Graphic obtained by the author from public extracted data)

Before analyzing the statistics, a brief explanation of the vulnerabilities above is due. According to (Elleithy et al., 2006), a Denial of Service (DOS) attack is any type of attack on a networking structure to disable a server from servicing its clients. Bypass vulnerability indicates that an attack managed to get around an authentication method. Gain Privilege refers to an attacker getting access to forbidden resources. Overflow vulnerability occurs when data written in a buffer exceeds its limits. SQL Injection occurs when an attacker changes the intended effect of an SQL query by inserting new SQL keywords or operators into the query (Halfond, Viegas & Orso, 2006). XSS (Cross-Site Scripting) materializes most often through web requests and has the purpose of introducing data in a web application. Directory traversal gives access to an attacker to files on the server. CSRF (Cross-Site Request Forgery) refers to an attacker executing actions under the mask of a legitimate user.

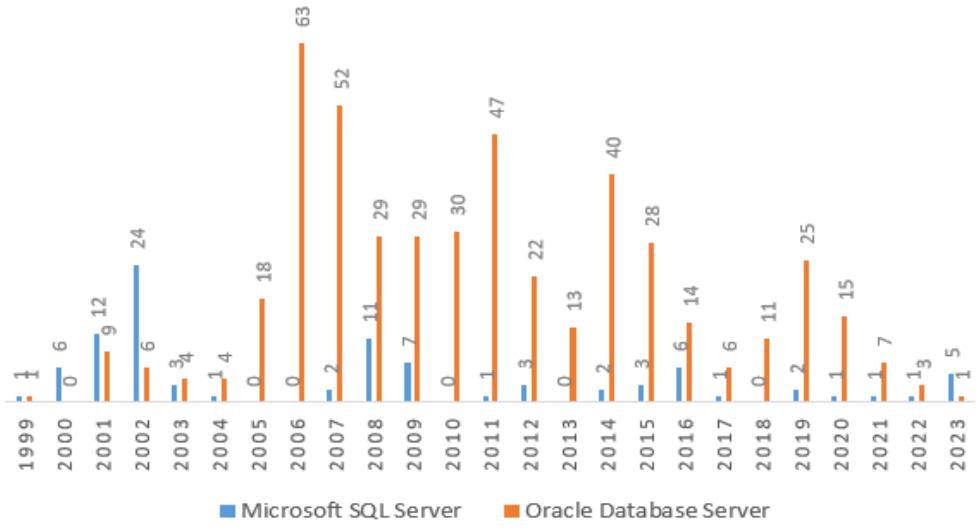

Figure 2. Vulnerabilities by type (Graphic obtained by the author from public extracted data)

The biggest discrepancy in the statistics shown in Figure 2 is for the SQL Injection vulnerability, this indicates that Microsoft SQL Server has taken better care of the users by sanitizing queries before executing them. According to (CVE MS SQL Server, 2023) and (CVE Oracle Server, 2023) no SQLIA has been found in the Oracle Server since 2012, which indicates that in later patches of the server, more tools were developed to defend against this attack, whereas Microsoft SQL Server has been vulnerable to SQLIA up to 2021. The rest of the statistics are roughly even and do not signal any major differences between the two systems proposed to be compared.

4. Security measures comparison

4.1. Authentication

Authentication has the purpose of denying unauthorized access to the database using different access methods. Both Oracle and Microsoft have developed password-based authentication, this method implies to use a combination of a username and password to gain access to the database, this is the default authentication method for Oracle Servers. Microsoft's default authentication method is *Windows Authentication* which implies that the user has a valid Windows user account to access the SQL Server, this method is also available for Oracle using the Oracle Native Authentication Module (O.N.A.M) for Windows.

Table 1. Authentication methods supported

Authentication Method	**Microsoft SQL Server**	**Oracle Database Server**
Password-based	Yes (default)	Yes
Windows Authentication	Yes	Yes (default)
Kerberos	Yes	Yes
SSL	Yes	Yes
Certificate-based	Yes	Yes
Active Directory	Yes	Yes
Azure Active Directory	Yes	Yes

Both servers offer *Kerberos authentication*, Oracle supports Kerberos authentication out of the box using Oracle Advanced Security Kerberos Authentication. Kerberos is a network authentication protocol that uses tickets to grant access to users using encrypted communication. *Secure Sockets Layer (SSL) authentication* is a method implemented by both servers, SSL is a cryptographic protocol used to send data securely and encrypted between two entities. *Certificate-based authentication* uses digital certificates issued by a Certificate Authority (CA), this method is also supported by both database servers. *Active Directory Authentication* and *Azure Active Directory Authentication* are supported by a pair of systems, the first one is beneficial when a centralized authentication method is used, while the last one is used for cloud-based authentication.

Both systems have developed over the years methods to authenticate users using a variety of methods to be suitable for more situations for developers.

4.2. Authorization

Authorization is a database security measure responsible for denying or granting access to different resources to users, based on what authorization the account used has received. Object permissions are implemented by both systems and refer to allowing users to have access to specific database objects such as views, tables or stored procedures. An even more granular permission type is the *Row-Level Security* (RLS) mechanism that allows controls access over rows or columns from

the tables in the database, this method is implemented by Microsoft SQL Server. Oracle Database Server also offers this mechanism, the only difference is the terminology, Virtual Private Database (VPD) is how Oracle has named its RLS mechanism. Both servers have enabled *Context-based access control*, an authorization method that permit users based on their IP Address, location or time of day. This method is implemented by Microsoft SQL Server under the name Dynamic Access Control (DAC). A schema is a container for database objects, *Schema Permission* offers control over all the objects contained in the schema. This authorization is available on both database servers.

Table 2. Authorization methods supported

Authorization methods	**Microsoft SQL Server**	**Oracle Database Server**
Object Permissions	Yes	Yes
Row-Level Security	Yes	Yes (VPD)
Context-Based Access Control	Yes (DAC)	Yes
Schema Permissions	Yes	Yes

Overall, both database servers provide a wide range of authorization methods of different granularity which offers the users great coverage of the database.

4.3. Encryption

Encryption is the database security measure that ensures that data stored is not saved in plain text but altered using an algorithm with a key to make it unreadable or unrecognizable for unauthorized users. Encryption is most frequently used over sensitive data stored in the database such as credit cards, medical information, passwords or personal identifying information. Both Microsoft SQL Server and Oracle Database Server have implemented Transparent Data Encryption (TDE), this mechanism provides encryption when data is entered into the database and appropriate decryption when data is read from the database with little to no overhead. The advantages of using TDE are that it doesn't require changes to the code of the applications connected to the database and that it provides more security for the data stored because even if an attacker has access to the database files, without the decryption key, the data is unreadable. Conforming to (Sharma & Johnson, 2014), TDE Column Encryption can be used to encrypt specific data, this approach is useful when database tables are large, only a small number of columns must be encrypted, and the columns are known. TDE Tablespace Encryption is suitable when the database contains a large amount of sensitive data to be encrypted and the columns reside in many different locations (Sharma & Johnson, 2014). Both servers offer in *Transit Encryption* using Transport Layer Security (TLS) and *Backup Encryption*, Oracle through Oracle Recovery Manager (RMAN) and Microsoft through SQL Server Backup Encryption.

According to (Baba et al., 2014) and (Basharat & Azam, 2012), the execution time depends on the algorithm used and the comparison between the execution times shows an average of 0.841 - second delay for data to be read from an encrypted table compared to a plain text table of the same size (665060 bytes). The experiment shows that the slowest algorithm was 3DES 168, therefore the importance of the algorithm used was shown. Both systems support the same hash algorithms SHA-1, SHA-2, and SHA-3.

Table 3 shows the encryption algorithm supported natively by the two database servers compared. Blowfish is deprecated and not recommended to use, but ChaCha20 is a notable loss for Oracle Database Server. This exclusion may be based on the fact that ChaCha20 is not on the list of FIPS (Federal Information Processing Standards) compliant cipher suites (FIPS 140-2, 2021).

Table 3. Encryption Algorithms supported

Encryption Algorithm	**Microsoft SQL Server**	**Oracle Database Server**
AES-128/192/256	Yes	Yes
RSA	Yes	Yes
DES	Yes	Yes
3DES	Yes	Yes
ChaCha20	Yes	No
Blowfish	No	Yes

4.4. Auditing

Auditing is the database security measure that logs and keeps track of all the activity conducted by users such as creating other users, creating tables, altering data and deleting data. *Extended Events Auditing* is a method of auditing specific data access events such as select, insert, update and delete. Both servers have this method of auditing implemented, but for Oracle, the terminology is Fine-Grained Auditing (FGA). The two systems also have implemented Transparent Data Encryption Auditing which implies that the access to any encrypted data or TDE keys is monitored. *Firewall Auditing* is implemented to log any firewall changes or traffic. Dynamic Management Views (DMVs) are a method of auditing performance data such as memory usage, I/O operations and CPU usage. This data is stored by Microsoft SQL Server in the error log. The equivalent of DMVs for Oracle is Automatic Workload Repository (AWR).

4.5. User management

Both database systems have implemented the most common user management measures such as user accounts, privileges or permissions, roles, password management or policy. Privileges or permissions are used to give access to a specific resource from the database or to a specific action that can impact the server. Roles are used to group multiple privileges for multiple users. The password management or policy applies specific rules to users' passwords, thus ensuring the use of high-security passwords.

5. Practical comparative analysis of encryption performance

As previously stated, a comparison regarding encryption time has been conducted (Baba et al., 2014). But in this chapter, the aim is to show the differences between the optimizations of the two database servers regarding encryption. The data on which the encryption tests will be conducted is 68910124 bytes long.

The comparison will watch the encryption and decryption time difference between the two, but most importantly the difference of the overhead added by the decryption happening during select statements.

In all of the tables to come the average has been calculated without the fastest and slowest time (marked by *) to have a more accurate average time. In Table 4 the times registered are from a simple select statement on the tables without being encrypted to have a solid startup point to compare against the select for encrypted data.

Table 4. Time needed to fetch all 507802 rows

Test No.	Time for Microsoft SQL Server to complete (ms)	Time for Oracle Database Server to complete (ms)
1	6974	18019*
2	6499*	16579
3	6837	16164*
4	10286*	17254
5	7979	17295
Average	7263.3	17042.6

Table 5. Time needed to encrypt and decrypt data using AES128

Test No.	Time for Microsoft SQL Server to complete (ms)		Time for Oracle Database Server to complete (ms)	
	Enc	Dec	Enc	Dec
1	16973	7626*	49992	30374
2	18197*	9214	35450*	94569*
3	17126	8352	78642*	27284*
4	16485	9377	37512	87377
5	16433*	11439*	69002	63165
Average	16861.3	8981	52168.6	60305.3

Table 6. Time needed to encrypt and decrypt data using AES192

Test No.	Time for Microsoft SQL Server to complete (ms)		Time for Oracle Database Server to complete (ms)	
	Enc	Dec	Enc	Dec
1	16025*	10364	28971*	46286*
2	16496	8817*	85394*	70087
3	16777	10490	42920	89765*
4	17333*	11846*	78603	72806
5	17284	9225	58417	59164
Average	16852.3	10026.3	59980	67352.3

Microsoft SQL Server is clearly the faster server for encrypting and decrypting data using AES128, with a very fast decryption time, half the time it takes to encrypt data. Oracle Database Server is slower on average when decrypting than when encrypting.

For AES192 encryption and decryption of the 68910124 byte column, the same observations come across. Microsoft SQL Server is faster when decrypting, while Oracle Database Server's encryption time is faster.

Table 7. Time needed to encrypt and decrypt data using AES256

Test No.	Time for Microsoft SQL Server to complete (ms)		Time for Oracle Database Server to complete (ms)	
	Enc	Dec	Enc	Dec
1	19026*	9722	66364	41088*
2	17168*	9965	71430	114159*
3	17695	9037*	73470*	85715
4	17823	10163	58441*	65508
5	17996	10805*	67501	54454
Average	17838	9950	68431	68559

After comparing the average time from all three encryption algorithms used (AES128 from Table 5, AES192 from Table 6 and AES256 from Table 7), the main takeaway is that AES128 is the fastest algorithm to use for both servers when both encryption and decryption are taken into consideration. Microsoft SQL Server is the faster server when it comes to encrypting and decrypting data with all the algorithms tested when compared to Oracle Database Server.

Table 8. Time needed to fetch data and decrypt it for the user for each algorithm

Time for Microsoft SQL Server to complete (ms)			
Test No.	Encrypted with AES 128	Encrypted with AES 192	Encrypted with AES 256
1	10935*	8425*	8761
2	9480	9399	8352*
3	8304*	10084*	9757
4	8559	8873	9561
5	8340	8934	10570*
Average	8793	9068.6	9359.3

Table 9. Time needed to fetch data and decrypt it for the user for each algorithm

Time for Oracle Database Server to complete (ms)			
Test No.	Encrypted with AES 128	Encrypted with AES 192	Encrypted with AES 256
1	18138	19737	24389*
2	18634	20472	21359
3	25406*	20308	18607*
4	18931	18857*	20310
5	16748*	20876*	20855
Average	18567.6	20172.3	20841.3

Analyzing Tables 8 and 9 a significant overhead is observed for both Database Servers. For Microsoft SQL Server, the increase for fetching all rows when data is encrypted, percentage wise, is by 21% when AES128 is used, by 24% for AES192 and by 28% when AES256 is used. Regarding Oracle Database Server, the overhead induced by the encryption used is as follows:

8% overhead for AES128, 18% when AES192 is used and 22% for AES256. When comparing the two performances percentage wise, Oracle Database Server is the more efficient of the two when it comes to fetching encrypted data.

6. Discussion

The vulnerability statistics provided in this paper show that over the years Oracle has struggled more against different attacks, but as of 2021, the vulnerabilities found have not been alarming for either of the database servers. The biggest difference in vulnerabilities found when splitting them per type has been for the SQL Injection Attacks, where Oracle struggled, due to the 27 findings in 2006 (CVE Oracle Server, 2023). Since 2012 no SQLI vulnerabilities have been reported for the Oracle Database Server. SQLI occurs due to bad configuration such as not verifying or sanitizing queries before executing them, not using parameterized queries or bad coding practices. Therefore, this makes database servers responsible for offering easy-to-configure built-in tools against this attack and the need for patches for the vulnerabilities signalled is highly important.

The comparison between the security measures confirmed that both database servers have a comprehensive asset of efficient and useful tools to defend against the most common threats. The notable difference between the two security measures developed was in the encryption analysis, where the missing native ChaCha20 algorithm for the Oracle Database Server was unexpected. In all of the other comparisons, the Microsoft SQL Server and Oracle Database Server have been a good match for each other, having implemented the same security methods, some of them under a different name, but the functionality being the same.

Looking at security incidents in recent years, both Oracle and Microsoft have their own set of security incidents, and it is not a surprising fact, as the plethora of cyber attacks evolve daily. As a response to these security incidents, both Oracle and Microsoft release update patches to fix the bugs in their software. In the next part, some security incident scenarios are presented.

Looking at recent cyber attacks addressing MS SQL Server, it is worth mentioning: CobaltStrike, (BleepingComputer ColbaltStrike, 2022) or Fargo ransomware (BleepingComputer TargetCompany, 2022). The most recent cyber attack, deploying the Trigona ransomware, exploits poorly secured MS SQL Server (BleepingComputer, 2023), via brute-force or dictionary attacks of account credentials. Thus, after connecting to the server, attackers can deploy CRL Shell and by exploiting the vulnerability in Windows Secondary Logon Service they can manage to escalate privileges to LocalSystem. This attack can be conducted only if two conditions are met poor security configuration of the MS SQL Server (ex. poor passwords as there are no password complexity mechanisms implemented by the administrator allows brute-force attacks without permanently blocking an account after several password tries, no audit mechanisms to alert etc.) and vulnerability CVE-2016-0099 in the Operating System (Microsoft MS16-032, 2023).

In the case of Oracle Database Server, there could not be found recent major cyber attacks examples, most of them include their Cloud Infrastructure (Mascellino, 2022), but many scenarios can be conducted, such as database administrators tampering with data and the auditing mechanisms to counter fake information, human error to share their password etc. Many such examples of scenarios can be found in (Burleson, 2023).

7. Conclusion

The importance of a secure database has increased in digital era due to the sensitive data that is being more and more stored electronically. Therefore, it is no surprise that valuable data stored in databases today can become the target of malicious actors. To have a secured database, security experts and database administrators should be aware of all the security mechanisms that databases offer today.

In this paper, the security measures that are the most common and have the purpose of increasing the strength against theft or loss of data were analysed and compared. It started with a

theoretical point of view and deepened into a more practical comparison of the two most popular database solutions used today: Oracle and Microsoft SQL. The main contributions of this paper include a framework with the main security mechanisms to take into account (authorization, authentication, encryption, auditing, user management), with concrete examples of security tools offered by the two database providers and an up-to-date analysis of the vulnerabilities discovered over the recent years in the two databases. Furthermore, a practical test to compare the encryption and decryption speed of the most recent database versions of Oracle (version 19c - long-term release) and MS SQL Server (version 2022) was conducted, from which the result is that for the same amount of data and the same cryptographic algorithm, MS SQL Server is faster at encrypting and decrypting. There is evidence that both database servers are reliable, with a downward trend in the number of vulnerabilities discovered. In addition, the comparison study strengthens the downward trend observed, having found that both Microsoft SQL Server and Oracle Database Server have successfully implemented the same and most effective security measures, therefore if configured correctly and having up-to-date patches both servers should be equally secure. On the other hand, the most recent cyber attacks of MS SQL and Oracle were noted and concluded that there is a recent rise in the attacks addressing MS SQL Servers, most of them being coupled with vulnerabilities found in the Microsoft Operating System. Furthermore, it is worth mentioning that Oracle did not include ChaCha20, which is not a FIPS-compliant cryptographic algorithm. This can suggest that Oracle is more natively inclined to be secure, while MS SQL might include mechanisms which are not necessarily secure. However, this last affirmation requires further research and testing of the two database systems.

For future works, an ampler palette of database providers, including NoSQL databases (Nicolau, 2018) is left to be compared using the same security framework mechanisms.

REFERENCES

Baba, M. A., Yusuf, A., Ahmad, A. & Maijamaa, L. (2014) Performance Analysis of the Encryption Algorithms as Solution to Cloud Database Security. *International Journal of Computer Applications*. 99(14), 24-31. doi: 10.5120/17442-8228.

Basharat, I. & Azam, F. (2012) Database Security and Encryption: A Survey Study. *International Journal of Computer Applications*. 47, 28-34. doi: 10.5120/7242-0218.

BleepingComputer (2023) *Microsoft SQL servers hacked to deploy Trigona ransomware*. https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/ [Accessed: 19th July 2023].

BleepingComputer CobaltStrike (2022) *Vulnerable Microsoft SQL Servers targeted with Cobalt Strike.* https://www.bleepingcomputer.com/news/security/vulnerable-microsoft-sql-servers-targeted-with-cobalt-strike/ [Accessed 19th July 2023].

BleepingComputer TargetCompany (2022) *Microsoft SQL servers hacked in TargetCompany ransomware attacks*. https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-in-targetcompany-ransomware-attacks/ [Accessed 19th July 2023].

Burleson, D. (2023) *Oracle hackers horror stories*. http://www.dba-oracle.com/t_ hackers_breaches_horror_stories.htm [Accessed 19th July 2023]

CVE MS SQL Server (2023) *Microsoft SQL Server Vulnerability Statistics*. https://www.cvedetails.com/product/251/Microsoft-Sql-Server.html?vendor_id=26 [Accessed: 4th April 2023].

CVE Oracle Server (2023) *Oracle Server Vulnerability Statistics*. https://www.cvedetails. com/product/467/Oracle-Database-Server.html?vendor_id=93 [Accessed 4th April 2023].

DB-Engines (2023) *DB-Engines Ranking*. https://db-engines.com/en/ranking [Accessed 19th July 2023].

Elleithy, K., Blagovic, D., Cheng, W. & Sideleau, P. (2006) Denial of Service Attack Techniques: Analysis, Implementation and Comparison. *Journal of Systemics, Cybernetics and Informatics*. 3(1), 66-71.

FIPS 140-2 (2021) *Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*. https://csrc.nist.gov/files/pubs/fips/140-2/upd2/final/docs/fips1402annexa.pdf [Accessed 19th July 2023].

Halfond, W. G., Viegas, J. & Orso, A. (2006) A classification of SQL-injection attacks and countermeasures. *Proceedings of the IEEE international Symposium on Secure Software Engineering*. 1. IEEE, pp. 13-15.

Ilić, M., Kopanja, L., Zlatković, D., Trajković, M. & Ćurguz, D. (2021) Microsoft SQL Server and Oracle: Comparative performance analysis. In *The 7th International conference Knowledge management and informatics, June 2-4, 2021, Vrnjacka Banja, Serbia*. pp. 33-40.

King, P. F. & Collmeyer, A. J. (1973) Database sharing: an efficient mechanism for supporting concurrent processes. *Proceedings of the June 4-8, 1973, national computer conference and exposition (AFIPS '73).* Association for Computing Machinery, New York, NY, USA. pp. 271–275. doi: 10.1145/1499586.1499661.

Kulkarni, M. S. & Urolagin, D. S. (2012*)* Review of Attacks on Databases and Database Security Techniques. *International Journal of Emerging Technology and Advanced Engineering*. 2(11), 253-263.

Litchfield, D. (2006) *Which database is more secure? Oracle vs. Microsoft*. *NGSSoftware InsightSecurity Research.* http://www.databasesecurity.com/dbsec/comparison.pdf. [Accessed 4th April 2023].

Mascellino, A. (2022) *Critical Vulnerability in Oracle Cloud Infrastructure Allowed Unauthorized Access, Security Magazine*. https://www.infosecurity-magazine.com/news/flaw-in-oracle-cloud-unauthorized/ [Accessed 19th July 2023].

Microsoft MS16-032 (2023) *Microsoft Security Bulletin MS16-032-Important.* https://learn.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-032 [Accessed 19th July 2023].

MS SQL Server 2022 (2022) *Configure the user connections Server Configuration Option*. https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/configure-the-user-connections-server-configuration-option?view=sql-server-ver16 [Accessed: 4th April 2023].

Murray, M. C. (2010) Database security: What students need to know. *Journal of Information Technology Education: Innovations in Practice*. 9, 061-077. doi: 10.28945/1132.

Nicolau, D. (2018) Considerations on NoSQL Databases. *Romanian Journal of Information Technology and Automatic Control (Revista Română de Informatică și Automatică)*. 28(3), 53-62.

Sharma, A. & Johnson, S. (2014) Oracle Database Security. *International Journal of Engineering Research & Technology.* 2 (3). doi: 10.17577/IJERTCONV2IS03035.

Soofi, A.A., Khan, M.I. & Amin, F.E. (2017) A review on data security in cloud computing. *International Journal of Computer Applications*. 94(5), 975-8887. doi: 10.5120/16338-5625.

Daniel BĂRBULESCU is a Bachelor student in Computer Science at the Military Technical Academy, in his final years of study. He aims to pursue his studies with a Master's degree in Computer Science.

Daniel BĂRBULESCU este student în ultimul an de licență în domeniul Științei Calculatoarelor din cadrul Academiei Tehnice Militare „Ferdinand I" din București. Își propune să urmeze studiile de Master în domeniul Științei Calculatoarelor.

Adriana-Cristina ENACHE-DUCOFFE has a Master's degree in Computer Science from the Military Technical Academy and a Ph.D. in Automatics from the Polytechnic University of Bucharest. She is the author of 14 scientific papers in international conferences and journals. Her main research areas include artificial intelligence, particularly bio-inspired algorithms, defensive security mechanisms and modern cryptographic systems.

Adriana-Cristina ENACHE-DUCOFFE deține o diplomă de Master în domeniul Științei Calculatoarelor obținută la Academia Tehnică Militară „Ferdinand I" din București și titlul de Doctor în domeniul Automaticii obținută la Universitatea Politehnica din București. Este autoarea a 14 articole științifice publicate în conferințe și jurnale internaționale. Principalele sale domenii de cercetare includ: inteligența artificială, în special algoritmii inspirați biologic sau algoritmii de inspirație biologică, mecanisme defensive pentru asigurarea securității și sisteme moderne de criptare.

Mihai TOGAN is a professor and Head of the Computer Science Department at the Military Technical Academy. With more than 50 scientific papers in international conferences and journals, technical or program committee member of international conferences, project director or responsible for four national research projects, his main research contributions include polyvalent areas of information security aspects such as modern cryptographic systems, cloud security, hardware mechanisms for optimizing cryptographic operations, electronic identity cards and public key infrastructures (PKI). He is a committee member of COST Association COST Action CA15127, a member of the NATO IST Information Systems Technology Panel and a member of the Technical Committee of the Romanian Standards Association, Techniques for Informatics Security Panel.

Mihai TOGAN este profesor și șeful Departamentului de Știința Calculatoarelor din cadrul Academiei Tehnice Militare „Ferdinand I" din București. Are peste 50 de articole științifice publicate în reviste și jurnale internaționale și este membru în comitetul tehnic pentru conferințe internaționale, director și responsabil de proiect pentru patru proiecte naționale, iar principalele sale contribuții științifice includ domenii polivalente din securitatea informației, precum: sisteme moderne de criptare, securitatea în cloud, mecanisme hardware pentru optimizarea operațiilor criptografice, carduri pentru identitatea electronică sau infrastructurile cu chei publice (PKI). Domnul profesor Mihai Togan este membru în Comitetul COST Association COST Action CA15127, membru în Comisia pentru Tehnologie al Sistemelor Informaționale NATO IST și membru al Comitetului tehnic din Comisia pentru Tehnici pentru Securitate în Informatică, al Asociației de Standardizare din România.