Security of a database and its data

Karen Christine Adviento

Harvard University Extension School

CS E-67: Oracle Database Administration

Prof. Patrick McGowan, ALM

November 29, 2020

Introduction

As we move forward to a more progressive future, the world is looking into the capitalization of data. From a World Economic Forum article, the world generates 500 million tweets, 294 billion emails sent, 5 billion searches made, and 65 billion messages sent through Whatsapp in a day. (Desjardins, 2019) This amount of data generated per day can create a tremendous amount of insight that can be used in a good way or, worse, in a bad way. Data can build a strong economy but also can psychologically manipulate your decision-making and appoint a person to sit in the highest office of a country. (Confessore, 2018, #) All of the data being collected is stored either in a data center or in the cloud. Regardless of the institution, may it be in the public or private sector, the frameworks, and technologies being used to collect, store, manipulate, and secure the data are similar. Non-technical people, and even some who have technical expertise and knowledge, are not aware of how much of their data are being shared and sold by institutions. It has come as no surprise that there are regulations in place and being authored to protect people's data. (Wharton, University of Pennsylvania, 2019)

With all these into account, organizations are heavily relying on information systems to support their businesses daily. Over the past decade, organizations have been vulnerable to data breaches, hacking, and other malicious cyber attacks. Having encryption alone is not enough to maintain the security posture of an organization. Security breaches are happening regardless of organization size. Thus, having these five areas would help protect an organization's data and databases: 1. Auditing and Monitoring refer to keeping track of all relevant actions issued by a database user and non-database user, 2. Authentication refers to the concept of verifying the identity of a user, 3. Updates and patches refer to updating the database with the latest security patch, 4. Data and Database encryption refers to encrypting data in motion and at rest, and lastly, 5. Access roles refer to the given roles to employees and/or staff in the organization. There are several ways on how to protect the data and databases of an organization, the areas mentioned are only a portion of what can be implemented. Also, these areas should supplement and/or align with the organization's standard operating procedures and policies.

Auditing and Monitoring

Auditing and monitoring are activities that strengthen your organization's security practices. It also helps the organization enforce and maintain compliance with existing regulations such as the Sarbanes-Oxley Act, HIPAA, etc. Some organizations would have clients who would request to run audits on information systems where their sensitive information resides and having an audit policy would show that the organization is serious about maintaining the security of their systems and databases.

Audit and Monitoring can be used to track the I/O performed in the database, investigate suspicious activity in the database, empower the DBA to make logical decisions on the database, gather evidence for compliance-related requirements, and detect problems on access control implementations.

Authentication and Passwords

Authentication can be defined as the concept of verifying the identity of a user that needs access to the relational database. Each user should identify himself before having access to data stored in the relational database system. Having a password management policy helps strengthen the security posture of an organization.

Password management should be implemented in the database and other systems connected to it. Passwords are usually the most valuable and vulnerable so, it is another layer where the organization should prioritize. Ensuring that the policies in place are well executed in the organization and its systems are crucial to maintaining the organization's security posture.

From a database perspective, when a database is created, there's usually a default password associated with it. There would also be accounts tied to it which also has a default password configured. Ensure that these passwords are changed. Passwords should have at least minimum requirements, should not be reused, hashed within the system, and should be changed periodically.

In terms of authentication of users from a database perspective, having a policy or solid process would also strengthen the security of the database. DBA or system teams can enforce a limit on failed login attempts, password lock times, password reuse, and password expiration. These are only a few out of the many settings DBA or system team could configure in a database.

Updates and Patches

Database updates and patches are also imperative in maintaining the security posture of the data and the database. Security patches address vulnerabilities in the software malicious cyber actors might use to gain unauthorized access to your data and your database. The DBA or team that maintains the database/s of an organization should apply security patches as soon as they become available. Updates and patches can be applied to the operating system where the relational database resides, in the database itself, and components added to the database.

With the growing interoperability of systems, having an outdated database may pose a risk to the business' ability to operate. There's also a probability that vulnerabilities are existing in the system thus, increasing the security risk of interconnected systems. It is important to have patch management in place for organizations to deal with the changes and updates of the systems and databases. The patch management should be included in the standard operating procedures and security policies of an organization.

Within the patch management process, the DBA and/or system team should keep themselves up to date with the security releases of their databases/systems. For example, always checking the Oracle Patch Updates, Security Alerts, and Bulletin resource. Also, a risk analysis that aligns with their organization's priorities would be beneficial in understanding which vulnerabilities need to be fixed.

Security patches and updates also have some risks where systems and DBA teams should be aware of. Some patches cannot be done through hotfixes and this can be costly for the organization especially when the patch takes long. It can disrupt production schedules which could potentially affect SLAs to clients. Security patches can also be frequent depending on the software. It can also affect some of the system’s functionality. There might be some releases that could potentially break some codes and would need to be updated accordingly. There might be some performance issues on the new patch or updates. And lastly, it can also affect some devices which connect with the system and/or database. For implementation, planning the patch releases and testing them before deploying them would help mitigate or lower the risks in patching. Organizations should implement a solid process in patch management.

Data and Database Encryption

To understand which data needs to be protected, a *Data Dictionary* or *Data Asset Inventory* would be useful. The DBA or systems team together with the dev team should be able to assess which data assets they hold and where it is located. When organizations know what data they hold and where it is located, they are better equipped to protect sensitive information from leaks and malicious cyber attacks. One of the most important factors for an organization to prioritize is ensuring they are compliant with existing regulations on the data they hold. For example, if an organization holds health insurance information together with patient information and/or HCP information, they should legally comply with the HIPAA standards. All of this information should be documented in the standard operating procedures, security policy, and as well as the privacy policy of an organization.

With several leaks and data breaches over the years, all sensitive information should be protected regardless of the size of an organization. To lower these risks by implementing data and database encryption. Encryption should be implemented for data at rest, in motion, and use. There are several ways to do encryption but it’s always better to check which regulations the organization needs to comply with.

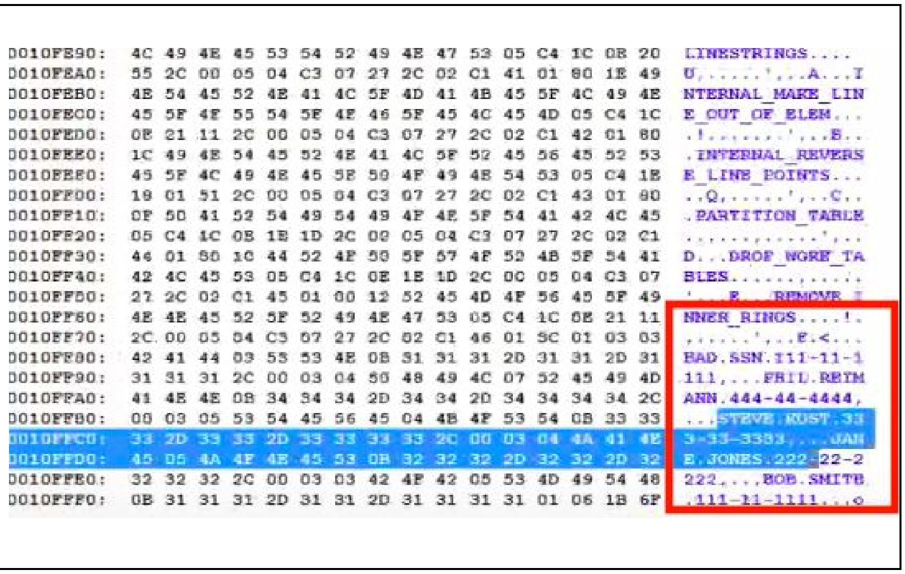
For Data at Rest

Transparent Data Encryption (TDE) can be used for Oracle Database encryption. It is an additional feature under the Advanced Security Option and has an associated cost. TDE stops unauthorized attempts from the operating system to access database data stored in files, without impacting how applications access the data using SQL. This is a solution only for data at rest and does not protect the organization from insider threats nor it can address access control requirements. (Integrigy, 2016)

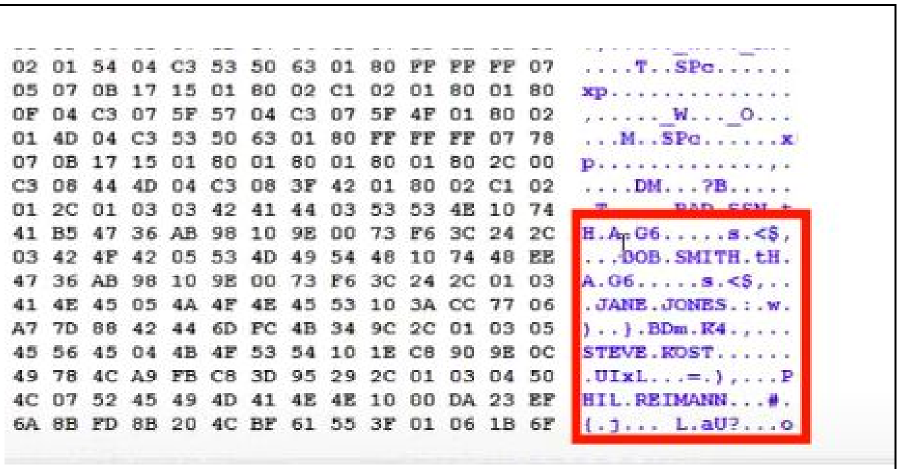
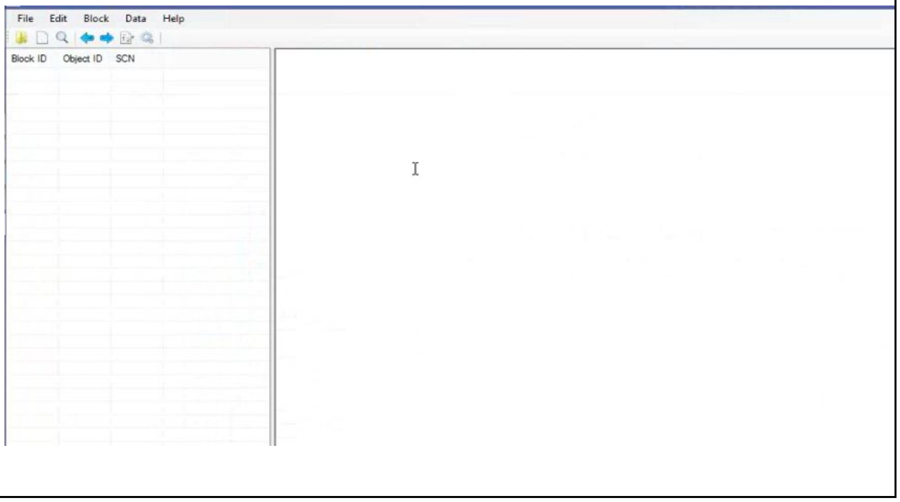
There are two ways to implement TDE, column encryption, and tablespace encryption. Column encryption from the title itself is applied only on the column level. Encryption is done using the Alter Table command. This type of encryption is used for standard application columns. While tablespace encryption provides datafile encryptions for version 12c and above. Implementation of this type of encryption is by exporting and importing the tablespace. This is used for custom tablespaces or even the entire database.

It is recommended to use TDE Tablespace encryption instead of the column level encryption. There are several benefits for this type of encryption: it protects during SQL operations using join and sort, the data is safe when being moved to the temporary tablespace, it allows index range scans wherein column level encryption can't, but what stands out the most is data file encryption.

Looking more closely at the capability of column and tablespace encryption, there's a test conducted by *Integrigy* (Integrigy, 2016) on the strength of encryption. They are assuming that there was a data breach and data got into the hands of malicious cyber actors. They used technology software that reads *.dbf* files. This tool is freely available online. They have three sets of data files which hold the first name, last name, and SSN; There's one file that doesn't have any encryption, another one with column level encryption, and finally a datafile with tablespace encryption. In the column level encryption datafile, they encrypted only the SSN column. The table below shows the results of the test.

No Encryption Sensitive Information can be viewed using the tool	

```
D010FE90:  4C 49 4E 45 53 54 52 49 4E 47 53 05 C4 1C 0B 20  LINESTRINGS....
D010FEA0:  55 2C 00 05 04 C3 07 27 2C 02 C1 41 01 80 1E 49  U,.....',..A...I
D010FEB0:  4E 54 45 52 4E 41 4C 5F 4D 41 4B 45 5F 4C 49 4E  NTERNAL_MAKE_LIN
D010FEC0:  45 5F 4F 55 54 5F 4F 46 5F 45 4C 45 4D 05 C4 1C  E_OUT_OF_ELEM...
D010FED0:  0E 21 11 2C 00 05 04 C3 07 27 2C 02 C1 42 01 80  .!.,.....',..B..
D010FEE0:  1C 49 4E 54 45 52 4E 41 4C 5F 52 45 56 45 52 53  .INTERNAL_REVERS
D010FEF0:  45 5F 4C 49 4E 45 5F 50 4F 49 4E 54 53 05 C4 1E  E_LINE_POINTS...
D010FF00:  18 01 51 2C 00 05 04 C3 07 27 2C 02 C1 43 01 80  ..Q,.....',..C..
D010FF10:  0F 50 41 52 54 49 54 49 4F 4E 5F 54 41 42 4C 45  .PARTITION_TABLE
D010FF20:  05 C4 1C 0B 1E 1D 2C 00 05 04 C3 07 27 2C 02 C1  ......,.....',..
D010FF30:  44 01 80 1C 44 52 4F 50 5F 57 4F 52 4B 5F 54 41  D...DROP_WORK_TA
D010FF40:  42 4C 45 53 05 C4 1C 0E 1E 1D 2C 00 05 04 C3 07  BLES......,.....
D010FF50:  27 2C 02 C1 45 01 00 12 52 45 4D 4F 56 45 5F 49  ',..E...REMOVE_I
D010FF60:  4E 4E 45 52 5F 52 49 4E 47 53 05 C4 1C 0E 21 11  NNER_RINGS....!.
D010FF70:  2C 00 05 04 C3 07 27 2C 02 C1 46 01 3C 01 03 03  ,.....',..F.<...
D010FF80:  42 41 44 03 53 53 4E 0B 31 31 31 2D 31 31 2D 31  BAD.SSN.111-11-1
D010FF90:  31 31 31 2C 00 03 04 50 48 49 4C 07 52 45 49 4D  111,...PHIL.REIM
D010FFA0:  41 4E 4E 0B 34 34 34 2D 34 34 2D 34 34 34 34 2C  ANN.444-44-4444,
D010FFB0:  00 03 05 53 54 45 56 45 04 4B 4F 53 54 0B 33 33  ...STEVE.KOST.33
D010FFC0:  33 2D 33 33 2D 33 33 33 33 2C 00 03 04 4A 41 4E  3-33-3333,...JAN
D010FFD0:  45 05 4A 4F 4E 45 53 0B 32 32 32 2D 32 32 2D 32  E.JONES.222-22-2
D010FFE0:  32 32 32 2C 00 03 03 42 4F 42 05 53 4D 49 54 48  222,...BOB.SMITH
D010FFF0:  0B 31 31 31 2D 31 31 2D 31 31 31 31 01 06 1B 6F  .111-11-1111...o
```

Column Encryption Since the SSN column is encrypted, when the file was viewed using the tool, it did not show the SSN details but it still shows other information in the datafile like first name and last name	
Tablespace Encryption The tool couldn't even identify the data blocks in a datafile with tablespace encryption	 File Edit Block Data Help Block ID Object ID SCN

```
02 01 54 04 C3 53 50 63 01 80 FF FF FF 07   ....T..SPc......
05 07 0B 17 15 01 80 02 C1 02 01 80 01 80   xp..............
0F 04 C3 07 5F 57 04 C3 07 5F 4F 01 80 02   ,....._W..._O...
01 4D 04 C3 53 50 63 01 80 FF FF FF 07 78   ...M..SPc......x
07 0B 17 15 01 80 01 80 01 80 01 80 2C 00   p.............,.
C3 08 44 4D 04 C3 08 3F 42 01 80 02 C1 02   ....DM...?B.....
01 2C 01 03 03 42 41 44 03 53 53 4E 10 74   .T....BAD.SSN.t
41 B5 47 36 AB 98 10 9E 00 73 F6 3C 24 2C   H.A.G6.....s.<$,
03 42 4F 42 05 53 4D 49 54 48 10 74 48 EE   ...DOB.SMITH.tH.
47 36 AB 98 10 9E 00 73 F6 3C 24 2C 01 03   A.G6.....s.<$,..
41 4E 45 05 4A 4F 4E 45 53 10 3A CC 77 06   .JANE.JONES.:.w.
A7 7D 88 42 44 6D FC 4B 34 9C 2C 01 03 05   )..}.BDm.K4.,...
45 56 45 04 4B 4F 53 54 10 1E C8 90 9E 0C   STEVE.KOST......
49 78 4C A9 FB C8 3D 95 29 2C 01 03 04 50   .UIxL...=.),...P
4C 07 52 45 49 4D 41 4E 4E 10 00 DA 23 EF   HIL.REIMANN...#.
6A 8B FD 8B 20 4C BF 61 55 3F 01 06 1B 6F   {.j... L.aU?...o
```

From the results, it shows how important encrypting sensitive information but most especially an organization can choose tablespace encryption to be able to fully protect their data assets. In implementing the TDE solution, the team should ensure that the key wallet is not backed up together with the database files. The team should back up the wallet separately. When encrypting a large volume of data, the team should create a new tablespace and shred the old one. There may be some data remaining in the tablespace blocks, ensuring that the team performs a disk wipe to remove them. Key Management tools also help in strengthening security.

For Data in Use

In application, the team should ensure that it encrypts and decrypts when reading and writing data. The team should also use standard and custom encryption routines and check its security status. For Databases, there are views and triggers encryption solutions. The view is for reading the data and trigger is used when writing data. Oracle has **DBMS_CRYPTO** which supports most major encryption and hash algorithms but it does not have key management available.

For Data in Motion

In Oracle, the use of SQLNet Encryption where it encrypts traffic between the client and DB listener is recommended. This is available in the database and can be configured in the sqlnet.ora file. All data transmitted between the client and the server will be encrypted. The organization should again identify which type of algorithm they would need to use to ensure compliance with existing regulations that applies to them.

Access Control and Roles

Preventing unauthorized access to the database is the main goal in implementing a secure database management system. Access controls are procedures that are defined to manage authorizations of the data in the relational database. Most database users wouldn't need the entire access to the database, they would only need specific permissions. DBA or system team should only grant privileges to users on a need-to-know basis and when it's required for their jobs. There are three ways of granting privileges, discretionary access control (DAC), mandatory access control (MAC), and role-based access control.

Discretionary access control (DAC) is based on granting and revok-ing privileges for the usage of system objects. It is called discretionary in the sense that the owner of data has complete discretion regarding granting/revoking access privileges to his data. Before implementing DAC, an organization should assess if it is aligned with their existing security policy.

Mandatory access control (MAC) depends on the security level associated with each object in the database and each user. A security level on an object is defined as a security classification, while the security level on a user is defined as a security clearance. MAC is also defined as a multilevel security. Multilevel security is formalized in these two rules:

No Read Up	A subject is allowed to read an object if the subject's security clearance level is greater than or equal to the object's security classification level
No Write Down	A subject is allowed to write to an object if the object's security classification level is greater than or equal to the subject's security clearance level.

A role-based control is a named group of related privileges that DBA could grant as a group to users or other roles. Managing and controlling the privileges is easier when Access Roles are configured in a database. Roles are useful for quickly granting access to users. It can be granted system or object privileges, any role can be granted to any database user, and roles can either be enabled or disabled. (Oracle, 2020) Role based access control has the following security principles:

Least Privilege	RBAC allows a user to access objects with the least privilege required for the specific task that is needed to be performed. This minimize Trojan horses attack
Separation of duties	RBAC ensures that no user has enough privileges to misuse the system on his own
Data abstraction	This is supported by means of abstract priv-ileges such as credit and debit for an account

On another note with a role-based access control, an administrator role should have a much thorough process when being granted. A background check which covers criminal check should be a requirement. For a much sensitive database like those in hospitals and military, a more detailed background check and personality check should be required. Only those who are considered trusted users should be granted administrative privileges.

Conclusion

The five areas stated in this paper are just a subset of what could be implemented in the database to strengthen its security. It should work together with the existing security policy, privacy policy, and other standard operating procedure of an organization. It's crucial to understand the organization's assets and all the security controls in place to protect them. For the DBAs and Network and Security teams, it would be beneficial to develop a more robust security and privacy program technologies continuous to upgrade and malicious cyber attacks are getting more rampant.

Bibliography

Bertino, E., & Sandhu, R. (2005). Database Security—Concepts, Approaches, and Challenges. *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, *2*(1), 18. Harvard Library. 10.1109/tdsc.2005.9

Callan, S. (2015, June 27). *Database Security Patches - Part One*. Burleson Consulting. http://www.dba-oracle.com/t_callan_db_security_patches1.htm

Carfagno, D. (2019, August 19). *What Is a Security Patch?* CyberShark. https://www.blackstratus.com/what-is-a-security-patch/#:~:text=Security%20patches%20address%20vulnerabilities%20in,can%20have%20far%2Dreaching%20implications.

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Desjardins, J. (2019, April 17). *How much data is generated each day?* World Economic Forum. https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

Faragallah, O., El-Rabaie, E.-S., El-Samie, F., Sallam, A., & El-Sayed, H. (2015). *Multilevel Security for Relational Databases*. Auerbach Publications. 10.1201/b17719

Integrigy. (2016, January 22). *All Things Oracle Database Encryption*. YouTube. https://www.youtube.com/watch?v=s_swBezkNW8&ab_channel=Integrigy

Oracle. (2020). *Oracle Database Security Guide, 19c*. Oracle. E96299-10

Oracle. (2020, November 16). *Oracle Critical Patch Update Advisory - October 2020*. Oracle. https://www.oracle.com/security-alerts/cpuoct2020.html

Wharton, University of Pennsylvania. (2019, October 28). *Your Data Is Shared and Sold…What's Being Done About It?* Knowledge@Wharton. https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/