19CSE311 - COMPUTER SECURITY
UNIT-3- PART 3
Database Security

April 6, 2022

Dr.Remya S/ Mr. Sarath R

Assistant Professor

Department of Computer Science

AMRITA VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY
School of Engineering

Database Security and the Role of Cipher

- e-commerce data repositories is an attraction for attackers.
- Generally, conventional database security systems have some lose points that can be used by attackers to penetrate the database.
- Database security could be enhanced by encryption algorithm or ciphers to give protection to the database from various threat or hackers who target to get confidential information.
- The objective of database security is to prevent undesired modification of data and information disclosure moreover ensuring the availability of the necessary service.

- To protect data in databases unambiguous, consistent and multi-layered security policies must be followed.
- The mechanisms used to provide security could be:
  1. Security features of the operating system such as authentication, logging.
  2. Firewalls
  3. Access control

Encryption

- Developers have to consider many factors while developing a database encryption strategy.
  1. Where sensitive data resides in the organization and classify which data to encrypt?
  2. Where encryption should be performed; in the storage, in the database or in the application?
  3. What should be the cipher and mode of operation?
  4. Who should have access to the encryption keys?
  5. How to minimize the impact of database encryption on performance?
  6. Train users to use encryption appropriately.
- Depending on our security and performance requirements developer have to decide where the encryption will take place, as soon as it is assessed the data to be protected.
- In general, encryption could be implemented at any of the three levels; storage, database or application

Storage level

- Here data is encrypted in the storage subsystem therefore it is well suited for encrypting entire files and directories and protecting the data
- i.e. data is encrypted at the storage subsystem, either at the file level (NAS/DAS) or at the block level SAN.
- The storage subsystem has no knowledge of its users and the database scheme.
- The choice of data to be encrypted is limited to file granularity which may lead to increased overhead due to unnecessary data encryption.
- This type of encryption is well suited for encrypting files, directories, storage blocks, and tape media.

Database level

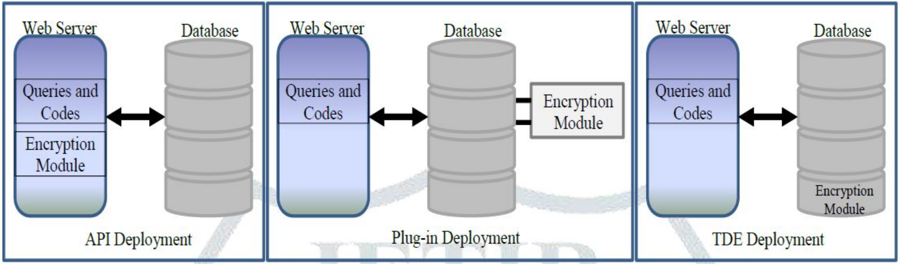
- Selective encryption is possible at database level and can be done at various granularities, such as tables, columns, rows.
- This type of deployment is usually done at the column level within a database table and, if coupled with database security and access controls, can prevent theft of critical data.

Application level

- Here encryption/decryption process is performed at the applications that generate the data.
- Encryption is performed within the application that introduces the data into the system, the data is sent encrypted, thus naturally stored and retrieved encrypted and then decrypted within the application.
- In this method the encryption keys never have to leave the application side and thus are separated from the encrypted data stored in the database. Depending

Encryption Module Deployment

There are three basic deployment methods namely API, plug-in, and TDE (Transparent Data Encryption)



API method

- This method requires the engineer to use a provided code change function (encryption agent) to edit relevant parts in the web server in order to apply the encryption.
- API method is applicable regardless of the database product types such as Oracle, MYSQL etc. and does not impose any additional burden on the DBMS.
- The encryption process could be time-consuming when there are large volumes of data.
- This is due to the fact that the encryption process happens before the data enter the database.

Plug-in Method

- In this method an encryption package (encryption module) is attached onto the DBMS.
- This encryption package works independently of the application and requires less modification to the query and code.
- It is easily applicable to both commercial DBMS and open source databases so is one of the most commonly used encryption method.
- The Plug-In method usually allows for index column-level encryption, access control, and auditing.

TDE Method

- This encryption method requires the installation of an encryption/decryption engine directly into the database engine.
- This method occurs at the lowest possible system level and requires no modification of the source code of the database environment or application.
- But this deployment is not so secure.