Database Security &Threats

- **Database**
  - An essential corporate resource
- Data
  - is a valuable resource
  - Must be strictly controlled, managed and secured
  - May have strategic importance
  - Should be kept secure and confidential

Threat

- A threat may be caused by a situation or event involving a person, action, or circumstance that is likely to bring harm to an organization. The harm may be tangible, such as loss of HW, SW or data, or intangible harm, such as loss of credibility or client confidence.
- Any threat must be viewed as a potential breach of security which, if successful, will have a certain impact.
- We consider database security in relation to the following situations, that broadly represent areas which the organization should seek to reduce risk.

Threat types

- Theft and fraud
  - Effect the database environment and also the organization
- Loss of confidentiality
  - Compromises the secrecy of critical organizational data
- Loss of privacy
  - Lead to legal action being taken against the organization
- Loss of integrity
  - Results in invalid or corrupt data, which may seriously affect the operation of an organization
- Loss of availability
  - The data, system, or both cannot be accessed, which can seriously affect an organizations financial performance.

Threat

- The extent that an organization suffers as a result of a threat’s succeeding depends upon a number of factors, such as:
  - The existence of countermeasures
  - Contingency plans.
- For example
  - When the last backups were taken
  - The time needed to restore the system

Threat A deeper look

- A good overview is given here
- https://micl-easj.dk/IT%20Security/Overheads/Database%20Security%20Threats.pdf
- DBMS server behind a firewall is responsible:
    - Authentication (User, password)
    - Authorization (Roles, user priviligies)
    - Back up (RAID system)
    - Integrity (PK, FK,)
    - Recovery (UNDO, REDO)

Integrity Types

- Entity integrity
  - Primary Key (PK) is NOT NULL
- Referential Integrity
  - Foreign Key (FK) refers to a PK OR
  - Totally NULLS
- Constraints
  - Default values given OR
  - Check of value set (6 letters , 10-90)

Countermeasures

- Views
- Backup and recovery
  - A DBMS should provide backup facilities to assist with the recovery of a database following failure. The backup copy and the details captured in the log file are used to restore the database to the latest possible consistent state.
  - Journaling
- Integrity
  - Preventing data from becoming invalid
- Encryption

Countermeasures

- **Computer based security controls**
  - The security of a DBMS is only as good as that of the operating system.
- **Authorization**
  - Authentication, Privileges
  - Ownership and privileges
    - Each privilege has a binary value associated with it for example

SELECT	UPDATE	INSERT	DELETE	ALL
0001	0010	0100	1000	1111

- Access Control Matrix

User/attr.	property	type	price	ownerNo	staffNo	Branch	Row limit
Sales	0001	0001	0001	0000	0000	0000	15
SG37	0101	0101	0111	0101	0111	0000	200
SG5	1111	1111	1111	1111	1111	1111	none

Backup facilities

- 5 units
  - DB Cache with the transaction changes
  - Log file with coming transaction changes
  - DB with tables
  - Backup of Log file
  - Backup of DB

Transaction life cycle

- A transaction arrives and registers in Log file (BEGIN T)
- Necessary data loads to DB cache
- Actions done in DB cache COMMIT written in Log file
- Checkpoint DB cache writes to DB (by COMMIT, FLUSH (10 minutes))

- Backup taken of Log file (RAID 5)
- Backup taken of DB (RAID 1/0)

Countermeasures

- RAID levels
  - RAID 0
    - Nonredundant
  - RAID 1
    - Mirrored
  - RAID 0+1
    - Nonredundant and Mirrored
  - RAID 5
    - Uses parity data for redundancy

RAID Examples

- **4 disks (D1,D2,D3,D4), 8 blocks (1,2,3,4,5,6,7,8) to be written**

Disk	RAID 0	RAID 1/0	RAID 5
D1	1 6	1 6 5 2	1 6 *
D2	2 5	1 6 5 2	2 * 5
D3	7 3	4 8 7 3	7 3 *
D4	4 8	4 8 7 3	4 8 *

  - The * is the parity bit file based on the 3 other disk bit pattens
  - Lets do calculation together together !

RAID Advantages

- **Discuss in groups for the RAID types:**
- **Redundancy**
- **Speed of read**
- **Speed of write**