COM106: Introduction to Databases

Database Management - Security

Database Management - Security

See Chapter 20 & 21 of Connolly & Beggs (6th ed)
(or similar chapters in other textbooks.)
and Lesson 5.1 in Database Administration Fundamentals

Some Background – Why is Security Important?:

- Data is a valuable resource that must be strictly controlled and managed, as with any corporate resource.
- Part or all of the corporate data may have strategic importance and therefore needs to be kept secure and confidential.
- Depending on the nature of the data, there may be legal, ethical and/or regulatory requirements to keep data secure.

Definition of Database Security

The protection of the database against intentional or unintentional threats using computer-based or noncomputer-based controls

Measures should be in place to guard against:

Theft and fraud

Loss of privacy (data about individuals)

Loss of availability (available for use)

Loss of confidentiality (organisational secrecy)

Loss of integrity (correctness of data)

Database Security Threats

Any situation or event, whether intentional or accidental, that may adversely affect a system and consequently the organisation, must be identified and steps taken to reduce or remove the impact.

- Organisations will have a Business Continuity Plan and a Disaster Recovery Plan in place.
- Given their fundamental importance, Databases are a crucial aspect of such plans.

Types of threat:

Hardware
- Fire/Flood/Disaster
- Power Supply Failure/Surge
- Physical Security Failure (Loss/Damage)

Software
- Virus/Trojan /Worm/ Malware etc

Communication
- Message interception

Users
- Unauthorised Access (Industrial Espionage/Data Protection)

See also Table 20.1 Connolly & Beggs for further examples.

Database Security – Legal Requirements

IT professionals must be aware of the laws and regulations that affect how data may be collected, processed, stored and distributed.

Each country, jurisdiction and/or organisation will have their own requirements.

In the UK, the legal requirements include compliance with:

*Data which allows **anyone** to link info to a specific person.*

EU General Data Protection Regulation (GDPR)

- Dealing with the protection of individuals with regard to the processing of personal data and on the gathering, storage and movement of such data.
- Based on seven principles, dealing with:

Any manual or automatic operation on personal data

Lawfulness, fairness and transparency, Purpose limitation, Data minimisation, Accuracy, Storage limitation, Integrity and confidentiality, Accountability

Data Protection Act (2018)

- The UK's implementation of the GDPR
- Together with GDPR, forms part of the data protection regime in the UK

Freedom of Information Act

Some sectors are subject to regulation that has implication for how data is managed – eg:

- As a result of major fraud incidents, Banks and Financial Services organisations must be able to provide detailed financial records to regulators on request.

GDPR – The Seven Key Principles

Article 5(1) of the GDPR requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ***('lawfulness, fairness and transparency')***;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ***('purpose limitation')***;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ***('storage limitation')***;

GDPR – The Seven Key Principles

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality')***."

Article 5(2) adds that:

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ***('accountability')***.

GDPR & DPA (2018) – Database Implications

These Principles have fundamental implications for database designers and administrators.

The principles of accuracy and storage limitation have implications for:

- Data Input verification and validation
- Transaction Management
- Database backup/recovery
- Archiving policy – what should be kept, and for how long?

The Principle of Integrity and Confidentiality means that:

- Database security should be **designed** and **organised** to fit the nature of the personal data held and the harm that may result from a security breach.
- There should be **clarity on who is responsible** in the organisation for ensuring information security.
- Appropriate physical and technical security should be in place (**eg, authorisation and access controls, encryption, etc**), backed up by robust **policies and procedures** and reliable, **well-trained staff**.
- Processes should be in place to respond to any breach of security swiftly and effectively.

General Data Protection Regulation - GDPR

Before 25 May 2018 each member state in the EU operated under the EU Directive on Data Protection (1995) as implemented under its own national laws.

- In the UK, the Data Protection Act 1998.

The **European General Data Protection Regulation** (**GDPR**) came into force on **25 May 2018** to replace the 1995 directive.

The UK has implemented a new **Data Protection Act 2018** which, although there are some small changes, largely includes all the provisions of the GDPR.

GDPR (and the Data Protection Act) aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

- Strengthens and unifies data protection for all individuals within the EU.
- Addresses the export of personal data outside the EU and applies to foreign companies processing data of EU residents.
- Includes a 'right to be forgotten'
- Implements a strict data protection compliance regime with severe penalties of up to €20 million or 4% of worldwide turnover (whichever is greater).
- And more – see the following for detail:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

General Data Protection Regulation - GDPR

The Data Protection Act 2018 is a significant evolution of the Data Protection Act 1998, not a step change.

- As such, the design, operation, management and security of the database becomes even more important.

Some Definitions:

Data Controller - determines the purposes and means of processing personal data.

Data Processor - responsible for processing personal data on behalf of a controller.

Data Subject - a person whose personal data is processed by a controller or processor

Personal Data - any information related to a Data Subject, that can be used to directly or **indirectly** identify the person

Sensitive Personal Data -special categories of personal data that are subject to **additional protections**, including: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

General Data Protection Regulation - GDPR

Personal Data Breach - a **breach of security** leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data. GDPR **requires that data breaches are reported** to the Information Commissioner; previously, the DPA 1998 did not.

Data Protection Officer - employed by an organisation and responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements. **Legal requirement** in some organisations

Information Commissioner's Office (ICO) - the independent regulatory office (national data protection authority) dealing with the DPA 2018 and GDPR.

General Security Measures

Organisational Measures

Security Policy

- User responsibility for security
- Defining who should be authorised to do what
- Security measures taken must be proportionate to risk cost estimates
- Plan for handling security breaches (contain, assess, notify and respond)

User Training

- Good practice (e.g. computer screen issues)
- Staff vetting and authorisation

Physical, Hardware and Software Measures

Physical Access restriction

- Room locking, physical access restriction through user identity

Hardware issues

- IT asset disposal

Software issues

- Passwords & user authorisation hierarchy
- Firewalls, Anti-virus & anti-malware software
- Encryption software

Database Auditing

Database Security Measures

Concerned with physical controls to administrative procedures and includes:

- User IDs and Passwords
- Authorisation levels (retrieve, append, delete, update)
- Views

  Defining a subset of tables to refine access to data
- Backup and recovery

  Strategy for backup/recovery
- Integrity Maintenance

  Data validation

  Transaction mechanism
- Encryption

SQL & DB Security – Users and Authorisation

CREATE USER 'brian'@'localhost' identified by 'bananas';

- Creates username with password

GRANT *Privilege* ON Table TO *User*

- Assumes that user accounts are defined
- Privileges (permissions) are:- SELECT/INSERT/DELETE/UPDATE/ALL

  e.g. GRANT SELECT ON test.emp TO 'brian'@'localhost'

  GRANT ALL on Emp_NoSalaries TO Public;
- Privileges should only be granted as required, unnecessary privileges should be revoked

  e.g. REVOKE UPDATE ON Emp_NoSalaries FROM Public;

Database Security Measures

SQL & DB Security – Views

CREATE VIEW *viewname* (<new attribute list>)
AS SELECT *<attribute list>* FROM *<table list>*
[other clauses];

For Example, given a table - EMP (empnum, ename, salary, deptnum)

CREATE VIEW Emp_NoSalaries AS SELECT empnum, ename, deptnum FROM Emp;

Views are treated as normal tables for SQL queries, for example:

SELECT * FROM Emp_NoSalaries; - *displays EMP table without salaries*

INSERT INTO Emp_NoSalaries VALUES (1011, 'Smith', 2); - *adds record into EMP with no salary value*

Views are *virtual tables* (not materialised until used) and allow a subset of data to be used

- For example, statistical databases can be created to allow retrieval of summary information from a database without allowing individual records to be viewed - hence maintaining data protection (e.g. on census data).

When combined with authorisation, Views can be used to refine DB security

- Allows limitation of attributes or records to be available
- Permission can be granted to allow only some users to use the view for retrieval and limit insert, update or delete to a smaller subset of users.

Database Security Measures

SQL & DB Security – Using SQL over a network

SQL Injection Attack

Can arise because of improperly validated user value entry
(e.g. logins, forms, user text entry which is ultimately used in SQL selection clause values)

Consider the SQL statement:

"SELECT * FROM users WHERE name = '" . $userName . "'";

If a malicious user enters **x' or '1** then the SQL statement becomes:

SELECT * FROM users WHERE name = '**x' or '1**'

Note: *- for a Logical OR term to be true, one OR other of the arguments must be true.*
In this case, anything OR 1 is always true

Once access is gained, malicious use of similar techniques can delete tables, access sensitive information and change table values

Solutions include:

Strong validation of user input

- Limiting size of input and excluding certain characters
- Use pattern matching to ensure expected input – regular expressions

Use of precompiled SQL statements (prepared statements and stored procedures)

Database Security Measures

SQL & DB Security – Backup Issues *(more in Transaction Management)*

Backup

Periodic copying of the database and log file to offline storage media.

All transactions backed up in log file

If the database is corrupted it can be restored from the backup copy and all subsequent transactions rerun.

This restores the database to its correct state at the time of failure

In the event of a major incident (fire, earthquake, etc), the backed up database and log file are crucial for Business Continuity and Disaster Recovery

The backup copy of the database and log file must be held securely.

Journaling (Logging)

Process of keeping and maintaining a log file (or journal) of all changes made to database to enable effective recovery in event of failure (e.g. before and after values of update)

Database Security Measures

SQL & DB Security – Encryption

Encryption - The encoding of data by a special algorithm that renders the data unreadable by any program without the decryption key.

The algorithms (programs) for encrypting or decrypting are normally made public, but the keys for encryption and decryption are kept secret

Used for encryption of:

- Data
- Messages (Message Authentication/Non-Repudiation)
- Digital Signatures (e.g. Website Authentication)

Asymmetric Encryption (also known as Public Key Encryption)

In asymmetric encryption, the encryption and decryption keys are different.

Used to enforce confidentiality - encryption key is public, decryption key kept secret

Used to enforce authenticity (e.g. digital signatures) – encryption key kept secret, decryption key made public to allow checking.

Used to validate websites – digital security certificate issued by a certificate authority (variation on digital signature)

Examples include algorithms such as **RSA** and protocols such as **SSH** (Secure Shell)

Symmetrical Encryption algorithms use the same keys for encryption and decryption. They are faster, but less secure and are often used in conjunction with asymmetric algorithms.

SQL Server Security Model

Login Authentication

- Windows Authentication - Better for Windows environment
- SQL Server Authentication - Better for mixed environment (e.g. Windows/Novell)

Tiered Security Model

A tiered approach allows a layered security model to be constructed:

- Login security—Connecting to the server
- Database security—Getting access to the database
- Database objects—Getting access to individual database objects and data

Within the model:

- login privilege does not automatically grant DB access
- DB access does not automatically grant access to individual DB objects (table, view, etc)

Roles are a part of the tiered security model

Server Roles specify the authority necessary to grant other users access to system areas/objects:

SysAdmin – any action performed on server

ServerAdmin – config options can be set on server

SetupAdmin – can manage startup options & tasks

SecurityAdmin – can manage server security

ProcessAdmin – can kill processes running on server

DbCreator – can create, alter, drop & restore DBs

DiskAdmin – can manage SQL server disk files

BulkAdmin – can run bulk insert commands

SQL Server Security Model

Predefined Database Roles include:

- **db_owner**: Members have full access (dbo)
- **db_accessadmin**: Members can manage Windows groups and SQL Server logins.
- **db_datareader**: Members can read all data.
- **db_datawriter**: Members can add, delete, or modify data in the tables.
- **db_ddladmin**: Members can run dynamic-link library (DLL) statements.
- **db_securityadmin**: Members can modify role membership and manage permissions.
- **db_bckupoperator**: Members can back up the database.
- **db_denydatareader**: Members can’t view data within the database.
- **db_denydatawriter**: Members can’t change or delete data in tables or views.

New roles can be created if required.

SQL Commands in Security

SQL commands can be run in SQL server - although many are created in **stored procedures**

CREATE/DROP LOGIN

CREATE LOGIN *login_name* WITH PASSWORD = '*Password*';

CREATE/DROP USER

CREATE USER *username* FOR LOGIN *login_name* [WITH DEFAULT_SCHEMA *schema_name*];

Schema could be a database or part of a database

GRANT/REVOKE

GRANT *privilege* ON *object user* [WITH GRANT OPTION];

Objects could be tables, views etc - Privileges could be SELECT, INSERT, DELETE, UPDATE

Summary of Database Administrator (DBA) Responsibility:

- Create a login for a person (either Windows or SQL Server login)
- Map this login to a user with the same name in those databases that person needs to access. **Only pick those databases needed**, not all databases.
- Create a **role** in each database for each group of users/permissions.
- **Add the users** to this role
- **Grant permissions** on the objects needed to these roles.