COMPUTER SECURITY AND CYBER LAW (CSCL)

LECTURER: ROLISHA STHAPIT/ DIKSHYA SINGH

UNIT 9

Database Security LH5

- Issues regarding the right to access information, system related issues: system levels: physical hardware, Operating system, DBMS level, Multiple security level and categorization of data and users, Loss of integrity, Loss of availability, Loss of confidentiality, Access control, Inference control, flow control, data encryption.

Definition

- Database security is the protection of the database against intentional and unintentional threats that may be computer-based or non-computer-based.
- Database security is the business of the entire organization as all people use the data held in the organization's database and any loss or corruption to data would affect the day-to-day operation of the organization and the performance of the people.
- Therefore, database security encompasses hardware, software, infrastructure, people and data of the organization.

- It is concerned within information security control that involves the data protection, the database applications or stored functions protection, the database protection, the database servers and the associated network links protection.
- The main database security risks are unauthorized or unintended activity or misuse by authorized database users, database administrators, or network or system managers, or by unauthorized users or hackers inappropriate access to sensitive data or functions within databases, or inappropriate changes to database programs, structures or security configurations.
- Also the data corruption and loss caused by the entry of invalid data or commands, mistakes in database or system administration processes, criminal damage pose security problems in databases.

Issues regarding the right to access information

- Conflict with privacy.
- Right to access information is fundamental right of citizen
- According to Part 3, under Article 27 (Right to information) of constitution of Nepal, 2072

◦Every citizen shall have the right to seek information on any matters of concern to her/him or the public.

◦Provided that nothing shall be deemed to compel any person to provide information about which confidentiality is to be maintained according to law.

Importance of Data

- Bank/Demat accounts
- Credit card, Salary, Income tax data
- University admissions, marks/grades
- Land records, licenses
- Data = crown jewels for organizations

Identity Theft

- Pretend to be someone else and get credit cards/loans in their name
    - Identification based on “private” information that is not hard to obtain online
- Hurts victims even more than regular theft
    - Responsibility goes on innocent people to prove they didn’t get loans or make credit card payment
    - Credit history gets spoilt, making it harder to get future loans
    - And you may have been robbed without ever knowing about it.
- Increasing risk
    - PAN numbers, names available online

Levels of Data Security

- Human level: Corrupt/careless User
- Network/User Interface
- Database application program
- Database system
- Operating System
- Physical level

To protect the database, we must take security measures at several levels:

- **Physical:** The sites containing the computer systems must be secured against armed or surreptitious entry by intruders.

- **Human**: Users must be authorized carefully to reduce the chance of any such user giving access to an intruder in exchange for a bribe or other favors .

- **Operating System:** No matter how secure the database system is, weakness in operating system security may serve as a means of unauthorized access to the database.

- **Network:** Since almost all database systems allow remote access through terminals or networks, software-level security within the network software is as important as physical security, both on the Internet and in networks private to an enterprise.

• **Database System:** Some database-system users may be authorized to access only a limited portion of the database. Other users may be allowed to issue queries, but may be forbidden to modify the data. It is responsibility of the database system to ensure that these authorization restrictions are not violated.

Security at all these levels must be maintained if database security is to be ensured. A weakness at a low level of security (physical or human) allows circumvention of strict high level (database) security measures.

Physical/OS Security

Physical level

- Traditional lock-and-key security
- Protection from floods, fire, etc.
- Protection from administrator error

  E.g. delete critical files
- Solution

  □Remote backup for disaster recovery

  □Plus archival backup (e.g. DVDs/tapes)

Operating system level

- Protection from virus/worm attacks critical

Database Encryption

- E.g. What if a laptop/disk/USB key with critical data is lost?
- **Partial solution:** encrypt the database at storage level, transparent to application
- Main issue: key management

E.g. user provides decryption key (password) when database is started up

- Supported by many database systems

Standard practice now to encrypt credit card information, and other sensitive information

Network level: must use encryption to prevent

◦Eavesdropping: unauthorized reading of messages

◦Masquerading:

  □pretending to be an authorized user or legitimate site, or

  □sending messages supposedly from authorized users

Network Level

- All information must be encrypted to prevent eavesdropping
  - ◦Public/private key encryption widely used
  - ◦Handled by secure http - https://
- Must prevent person-in-the-middle attacks
  - ◦E.g. someone impersonates seller or bank/credit card company and fools buyer into revealing information
    - □Encrypting messages alone doesn’t solve this problem.

Site Authentication

- Digital certificates are used in https to prevent impersonation/man-in-the middle attack

◦Certification agency creates digital certificate by encrypting, e.g., site’s public key using its own private key

- Verifies site identity by external means first!

◦Site sends certificate to buyer

◦Customer uses public key of certification agency to decrypt certificate and find sites public key

□Man-in-the-middle cannot send fake public key

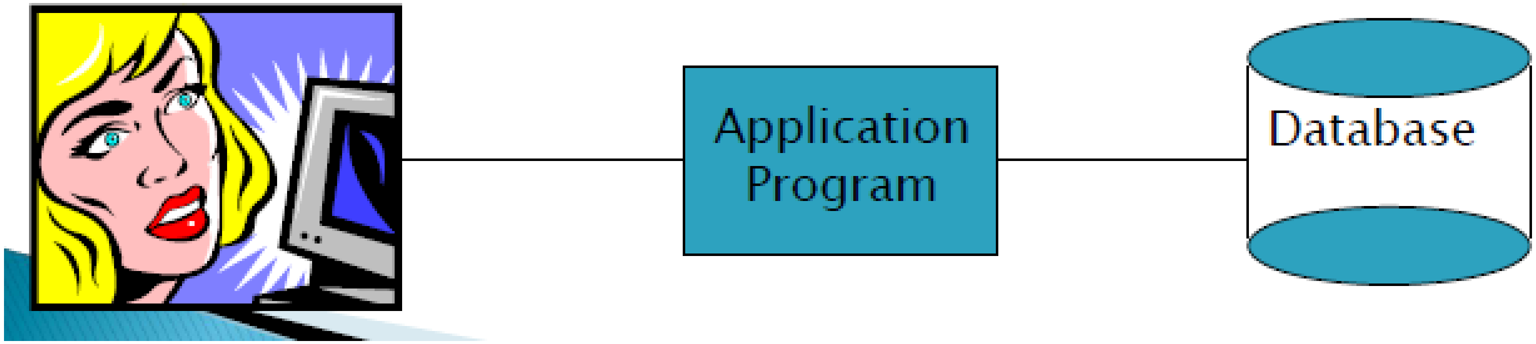
◦Sites public key used for setting up secure communication

Security at Database/Application Program

- Authentication and authorization mechanisms to allow specific users access only to required data
- Authentication: who are you? Prove it!
- Authorization: what you are allowed to do

Application vs Database

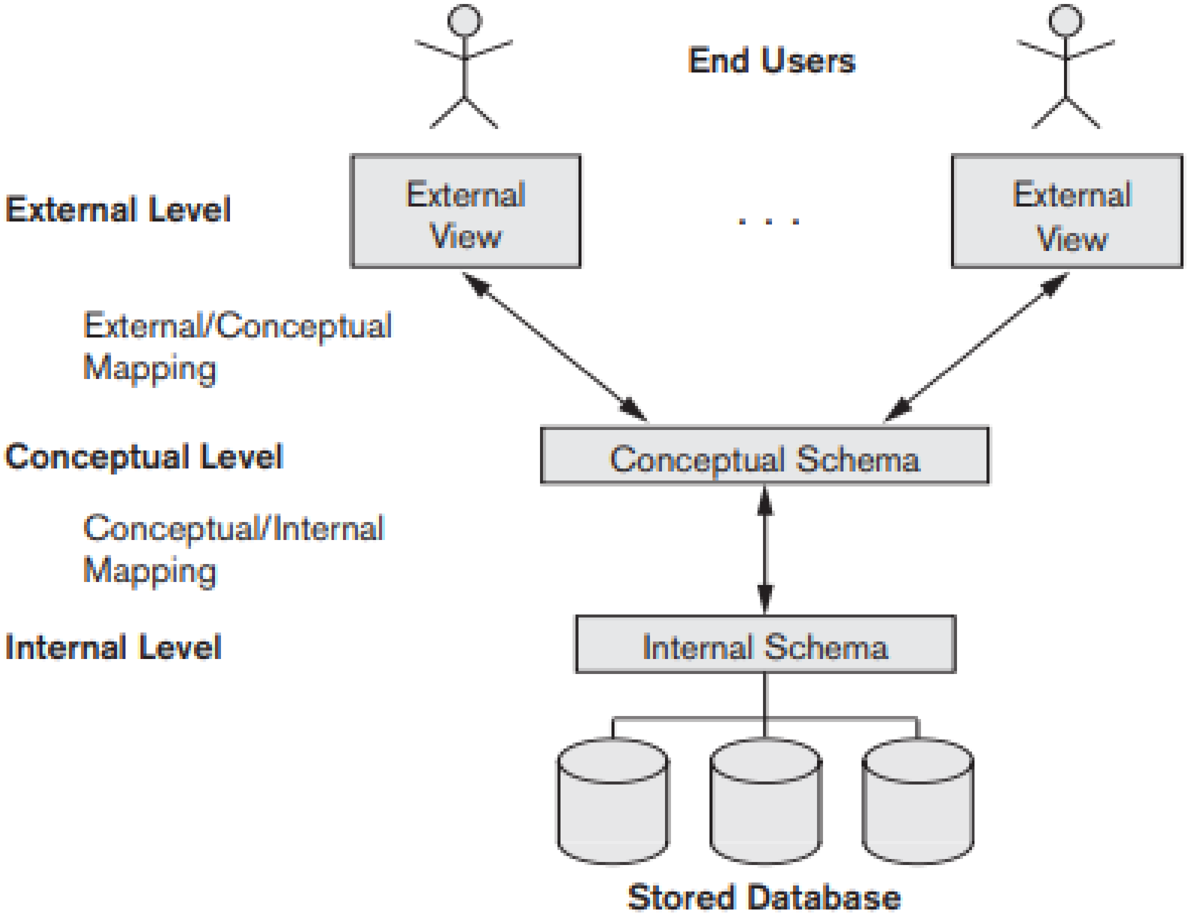
- Application authenticates/authorizes users
- Application itself authenticates itself to database
    - Database password



Database/Application Security

- Ensure that only authenticated users can access the system
- And can access (read/update) only data/interfaces that they are authorized to access

DBMS level


End Users
External Level
External View
. . .
External View
External/Conceptual Mapping
Conceptual Level
Conceptual Schema
Conceptual/Internal Mapping
Internal Level
Internal Schema
Stored Database

1. The **internal level** has an internal schema, which describes the physical storage structure of the database. The internal schema uses a physical data model and describes the complete details of data storage and access paths for the database.

2. The **conceptual level** has a conceptual schema, which describes the structure of the whole database for a community of users. The conceptual schema hides the details of physical storage structures and concentrates on describing entities, data types, relationships, user operations, and constraints. Usually, a representational data model is used to describe the conceptual schema when a database system is implemented. This implementation conceptual schema is often based on a conceptual schema design in a high-level data model.

3. The **external or view level** includes a number of external schemas or user views. Each external schema describes the part of the database that a particular user group is interested in and hides the rest of the database from that user group. As in the previous level, each external schema is typically implemented using a representational data model, possibly based on an external schema design in a high-level data model.

The three-schema architecture is a convenient tool with which the user can visualize the schema levels in a database system. Most DBMSs do not separate the three levels completely and explicitly, but support the three-schema architecture to some extent.

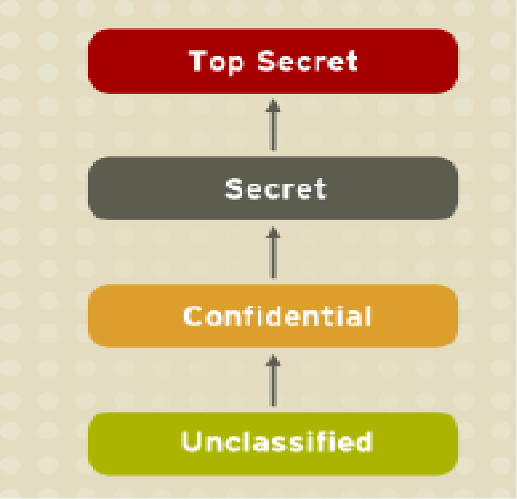
- The three schemas are only descriptions of data; the stored data that actually exists is at the physical level only.
- In a DBMS based on the three-schema architecture, each user group refers to its own external schema.
- Hence, the DBMS must transform a request specified on an external schema into a request against the conceptual schema, and then into a request on the internal schema for processing over the stored database.
- If the request is a database retrieval, the data extracted from the stored database must be reformatted to match the user's external view. The processes of transforming requests and results between levels are called **mappings.**
- These mappings may be time-consuming, so some DBMSs—especially those that are meant to support small databases—do not support external views. Even in such systems, however, a certain amount of mapping is necessary to transform requests between the conceptual and internal levels.

Multi – Level Security (MLS)

- Protecting sensitive or confidential data is paramount in many businesses. In the event such information is made public, businesses may face legal or financial ramifications. At the very least, they will suffer a loss of customer trust. In most cases, however, they can recover from these financial and other losses with appropriate investment or compensation.
- The same cannot be said of the defense and related communities, which includes military services, intelligence organizations and some areas of police service. These organizations cannot easily recover should sensitive information be leaked, and may not recover at all. These communities require higher levels of security than those employed by businesses and other organizations.
- Having information of different security levels on the same computer systems poses a real threat. It is not a straight-forward matter to isolate different information security levels, even though different users log in using different accounts, with different permissions and different access controls.
- Some organizations go as far as to purchase dedicated systems for each security level. This is often prohibitively expensive, however. A mechanism is required to enable users at different security levels to access systems simultaneously, without fear of information contamination.

Why Multi Level?

- The term multi-level arises from the defense community's security classifications: Confidential, Secret, and Top Secret.
- Individuals must be granted appropriate clearances before they can see classified information. Those with Confidential clearance are only authorized to view Confidential documents; they are not trusted to look at Secret or Top Secret information. The rules that apply to data flow operate from lower levels to higher levels, and never the reverse.



- Multilevel security or multiple levels of security (MLS) is the application of a computer system to process information with incompatible classifications (i.e., at different security levels), permit access by users with different security clearances and needs-to-know, and prevent users from obtaining access to information for which they lack authorization.
- Multilevel security is a security policy that allows you to classify objects and users based on a system of hierarchical security levels and a system of non-hierarchical security categories.
- Multilevel security provides the capability to prevent unauthorized users from accessing information at a higher classification than their authorization, and prevents users from declassifying information.

Types of Security

Database security is a broad area that addresses many issues, including the following:

- Various legal and ethical issues regarding the right to access certain information — for example, some information may be deemed to be private and cannot be accessed legally by unauthorized organizations or persons. In the United States, there are numerous laws governing privacy of information.
- Policy issues at the governmental, institutional, or corporate level as to what kinds of information should not be made publicly available— for example, credit ratings and personal medical records.

- System-related issues such as the system levels at which various security functions should be enforced— for example, whether a security function should be handled at the physical hardware level, the operating system level, or the DBMS level.
- The need in some organizations to identify multiple security levels and to categorize the data and users based on these classifications— for example, top secret, secret, confidential, and unclassified. The security policy of the organization with respect to permitting access to various classifications of data must be enforced.

Threats to Database

- Threats to databases can result in the loss or degradation of some or all of the following commonly accepted security goals: integrity, availability, and confidentiality.
- **Loss of integrity:**

□Database integrity refers to the requirement that information be protected from improper modification. Modification of data includes creation, insertion, updating, changing the status of data, and deletion. Integrity is lost if unauthorized changes are made to the data by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions.

- **Loss of availability:**

□Database availability refers to making objects available to a human user or a program to which they have a legitimate right.

- **Loss of confidentiality:**

Database confidentiality refers to the protection of data from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from violation of the Data Privacy Act to the jeopardization of national security. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Database Security Mechanism

- A DBMS typically includes a database security and authorization subsystem that is responsible for ensuring the security of portions of a database against unauthorized access. It is now customary to refer to two types of database security mechanisms:
- Discretionary Security Mechanism
- Mandatory Security Mechanism

- **Discretionary security mechanisms:**

□These are used to grant privileges to users, including the capability to access specific data files, records, or fields in a specified mode (such as read, insert, delete, or update).

- **Mandatory security mechanisms.**

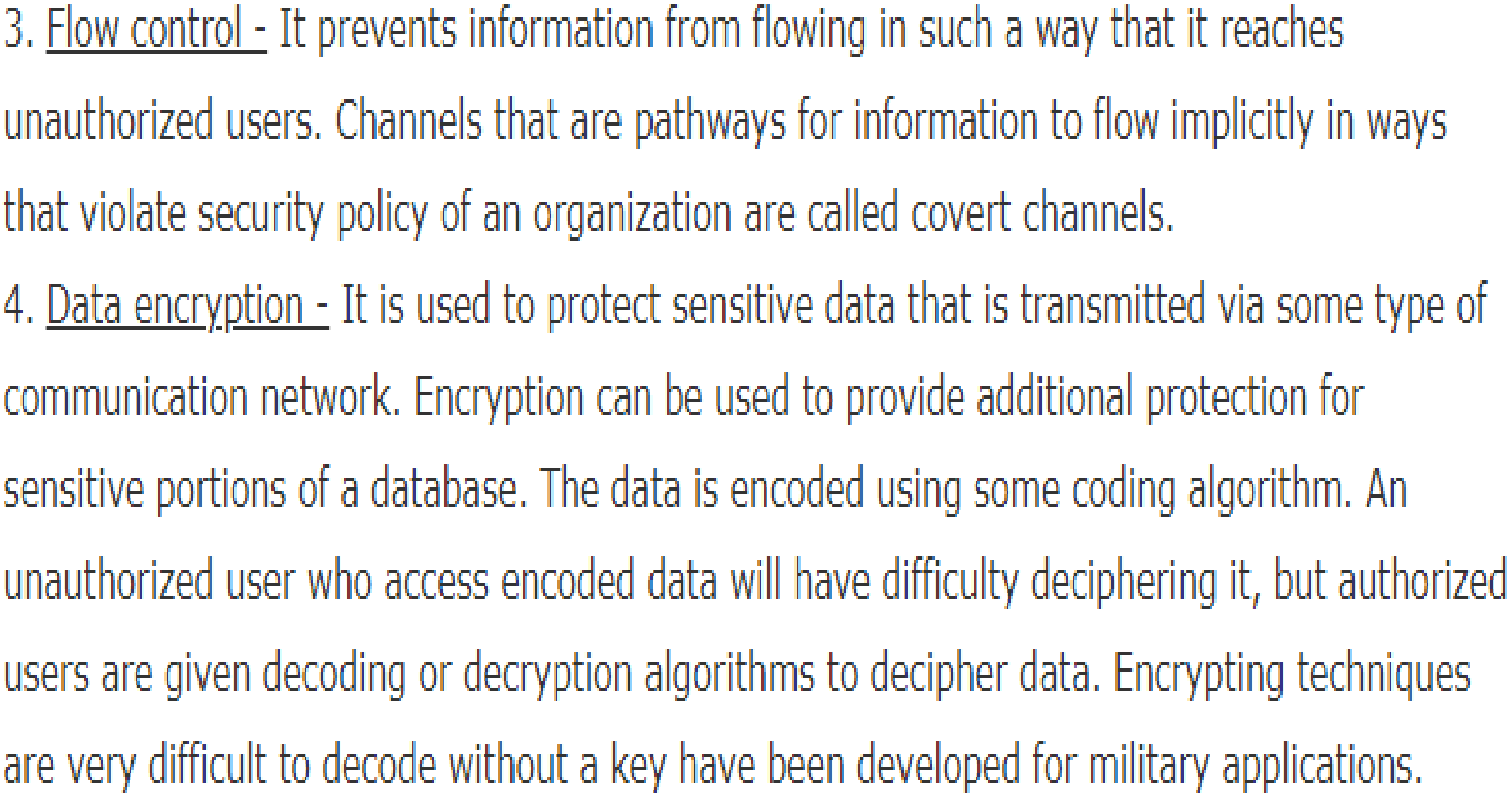
□These are used to enforce multilevel security by classifying the data and users into various security classes (or levels) and then implementing the appropriate security policy of the organization. For example, a typical security policy is to permit users at a certain classification (or clearance) level to see only the data items classified at the user’s own (or lower) classification level. An extension of this is role-based security, which enforces policies and privileges based on the concept of organizational roles.

Control Measures

Four main control measures are used to provide security of data in databases:

- Access control
- Inference control
- Flow control
- Data encryption

1. Access control - The security mechanism of a DBMS must include provisions for restricting access to the database as a whole. This function is called access control and is handled by creating user accounts and passwords to control the login process by the DBMS.
2. Inference control - Statistical databases are used to provide statistical information or summaries of values based on various criteria. Security for statistical databases must ensure that information about individuals cannot be accessed. It is possible to deduce or infer certain facts concerning individuals from queries that involve only summary statistics on groups, consequently this must not permitted either. This problem called statistical database security and corresponding control measures are called inference control measures.



3. Flow control - It prevents information from flowing in such a way that it reaches unauthorized users. Channels that are pathways for information to flow implicitly in ways that violate security policy of an organization are called covert channels.

4. Data encryption - It is used to protect sensitive data that is transmitted via some type of communication network. Encryption can be used to provide additional protection for sensitive portions of a database. The data is encoded using some coding algorithm. An unauthorized user who access encoded data will have difficulty deciphering it, but authorized users are given decoding or decryption algorithms to decipher data. Encrypting techniques are very difficult to decode without a key have been developed for military applications.

Assignment

- What is database security? Explain with levels of it.
- Explain DBMS level.
- Explain the threats of database.
- Explain the control measures of the threats of database.