CSIT115 Data Management and Security

Database Security

Dr Janusz R. Getta

School of Computing and Information Technology -
University of Wollongong

Database Security

Outline

- What is Database Security ?
- Threats
- Countermeasures
- Authorization and authentication
- Access Control
- Encryption

What is Database Security

Database security means protection of a database against unauthorized access, either intentional or unintentional

Database security requires the mechanisms that protect a database against the intentional or accidental threats

Such mechanisms affect hardware, software, people, and data

Database security protects against:

- Theft and fraud,
- Loss of confidentiality
- Loss of privacy
- Loss of integrity
- Loss of availability

Database Security

Outline

- What is Database Security ?
- Threats
- Countermeasures
- Authorization and authentication
- Access Control
- Encryption

Threats

A threat is any situation or event, whether intentional or accidental, that may adversely affect a system

Sample threats:

- Unauthorized amendment or copying of data
- Using another person's means of access
- Program alteration
- Wire tapping
- Illegal entry by hacker
- Blackmail
- Theft
- Failure of security mechanisms
- And the others ...

Database Security

Outline

- What is Database Security ?
- Threats
- Countermeasures
- Authorization and authentication
- Access Control
- Encryption

Countermeasures

Countermeasures range from physical controls to administrative controls

Security of Database Management System (DBMS) is as good as security of operating system running DBMS

We consider the following computer-based security controls in a multiuser environment:

- Authorization and authentication
- Access control
- Encryption
- Views
- Backup and recovery
- Integrity

Database Security

Outline

- What is Database Security ?
- Threats
- Countermeasures
- Authorization and authentication
- Access Control
- Encryption

Authorization and authentication

Authorization means granting a right or privilege to have a legitimate access to a system or resources operated by a system

Authorization is usually built into the software and it determines what system or object a user can access and what a user is allowed to do with it

In a process of authorization a subject representing a user or a program requests and obtains access to an object that represent relational table, relational view, etc

A process of authorization requires authentication of a subject

Authorization and authentication

Authentication is a mechanism that determines whether a user is who he or she claims to be

A system administrator is responsible for allowing users to have access to a computer system by creating individual user accounts

When account is created a user is given a unique identifier and a user picks a password associated with the identifier

To reduce the total number of user names and passwords it is possible to authenticate user's access to a database system through earlier authentication of access to an operating system

Database Security

Outline

- What is Database Security ?
- Threats
- Countermeasures
- Authorization and authentication
- Access Control
- Encryption

Access Control

A typical way to control access to a database system is based on granting and revoking privileges

A privilege allows a user to create, to drop, or to access in read or write mode some database objects like relational tables, relational views, index, etc or to perform certain operations

Privileges are granted to user to accomplish their task; excessive privileges can compromise security

A user who creates a database object becomes an owner of the object and he/she automatically gets all privileges on the object

DBMS keeps track of all granted privileges to ensure that only selected user can access and can perform operations on the database objects

Access Control

There are two different strategies of access control:

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)

In Discretionary Access Control each user is given access rights (privileges) on specific database objects

A user obtains privileges when he/she creates an object and access of other users to the object is at discretion of an owner

It is an effective system with some weaknesses, for example:

- user A creates a new relational table R and grants write access to such table to a user B
- user B owns a relational table S which is not accessible to user A
- user A modifies a software used by user B such that it copies the contents of a table S to a table R
- user A returns a software used by user B to its original state

Access Control

There are two different strategies of access control:

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)

Mandatory Access Control is based on system-wide policies that cannot be changed by individual users

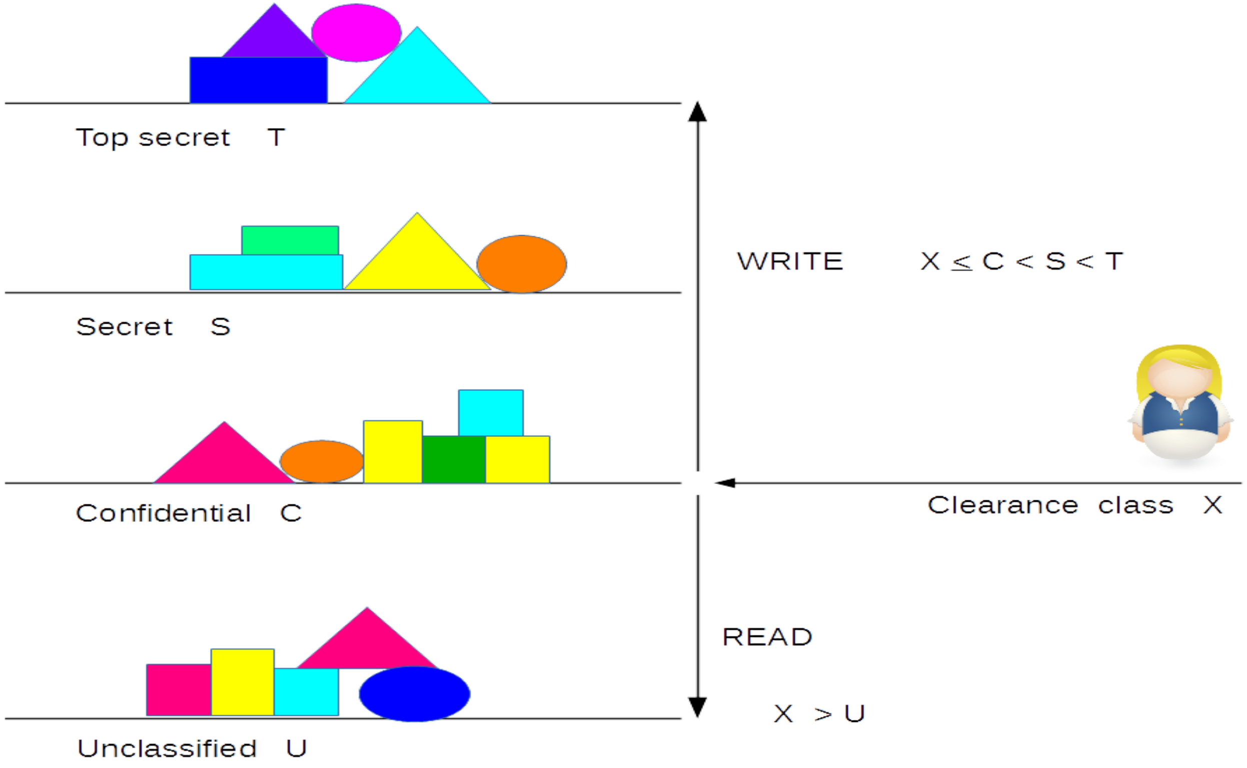
Each database object is assigned a security class and each user is assigned a clearance for a security class and rules are imposed on reading and writing database objects by users

DBMS determines whether a user can read or write a database object based on certain rules that involve security level of the object and clearance of the user

Access Control

A popular model for MAC is Bell-LaPadula model (Bell and LaPadula 1974)

The model uses the terms of objects (relations, views, indexes, etc), subjects (users and programs), and security classes and clearances



Access Control

The principles of Bell-LaPadula model are the following:

- Each database object is assigned a security class
- Each subject is assigned clearance class
- The security classes are ordered, with a most secure class and a least secure class, e.g. top secret (TS), secret (S), confidential (C), and unclassified (U)
- TS > S > C > U
- Simple Security Property: Subject S is allowed to read object O only if class of subject S > class of O
- * Property: Subject S is allowed to write object O only if class of S <= class of O

Database Security

Outline

What is Database Security ?

Threats

Countermeasures

Authorization and authentication

Access Control

Encryption

Encryption

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

Sensitive data can be encoded to protect it against external threats or access

Some DBMS provide special facilities to encrypt data and to access encrypted data after decoding it

Usually there is a degradation in performance because of time needed to decode data

A typical cryptosystem includes:

- An encryption key to encrypt data (plaintext)
- An encryption algorithm that with the encryption key transfroms plaintext into ciphertext
- A decryption key to decrypt the ciphertext
- A decryption algorithm to use decryption key with cipher text and to create the original plaintext

References

T. Connoly, C. Begg, Database Systems, A Practical Approach to Design, Implementation, and Management, Chapters 20.1 Database Security, 20.2 Countermeasures - Computer-Based Controls (except 20.2.7), Pearson Education Ltd, 2015