Database Security

CT069-3-3

Lecturer Information

- Lecturer– Dr. Kulothunkan Palasundram
- Email – kulothunkan@apu.edu.my

Learning Outcomes

At the end of this course, YOU should be able to :

- Explain the concepts and principles of secure database design, development and auditing.

- Analyze, design, build and audit a secure database system.

Topics we will cover

- Security Architecture
- Database Architecture
- Entity Relationship Diagram
- Relational Model
- SQL
- User Administration
- Encryption
- Triggers
- Auditing
- Backup

Module Assessments

- Group assignment – 60%
  - Form a team of 4 members from the same lab group to do your assignment
  - Has group and individual tasks
  - Demo your solution and submit 2 reports
- Class test – 40%

Reference Books

Essential Reading

- Stephen Morris, Peter Rob & Carlos Coronel (2013), *Database Principles: Fundamentals of Design, Implementation, and Management*, International 10th edition; CENGAGE Learning.

- Hassan Afyouni (2013), *Database Security and Auditing: Protecting Data Integrity and Accessibility*, 1st edition. CENGAGE Learning. ISBN-13:9780619215590

- Cherry Denny (2012), *Securing SQL Server: Protecting your database from attackers,* 2nd edition. Syngress. ISBN-13:978-1597499477

Important Note

- Lecture –
  - My sharing what you are expected/need to know/learn from this course
  - Pay attention, settle any doubts during lecture itself
- Tutorial/Lab –
  - Discussion of some sample problems
  - Discussion issues you are facing with your assignments

Lecture 1

Introduction to Database & Database Security

Learning Outcomes

At the end of this module, YOU should be able to explain:

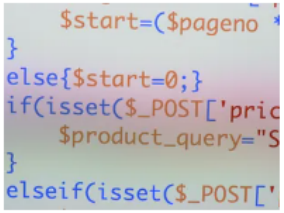
- What are the security problems affecting data and database

Key Terms you must be able to use

If you have mastered this topic, you should be able to use the following terms correctly :

- Information System
- Data, Database, DBMS
- Database Security
- Access control
- Data protection
- Auditing

Security News



Trigona Ransomware Trolling for 'Poorly Managed' MS-SQL Servers

Vulnerable MS-SQL database servers have external connections and weak account credentials, researchers warn.

by Dark Reading Staff, Dark Reading — April 21, 2023

REMOTE WORKFORCE | 1 MIN READ | ARTICLE

Western Digital Hackers Demand 8-Figure Ransom Payment for Data

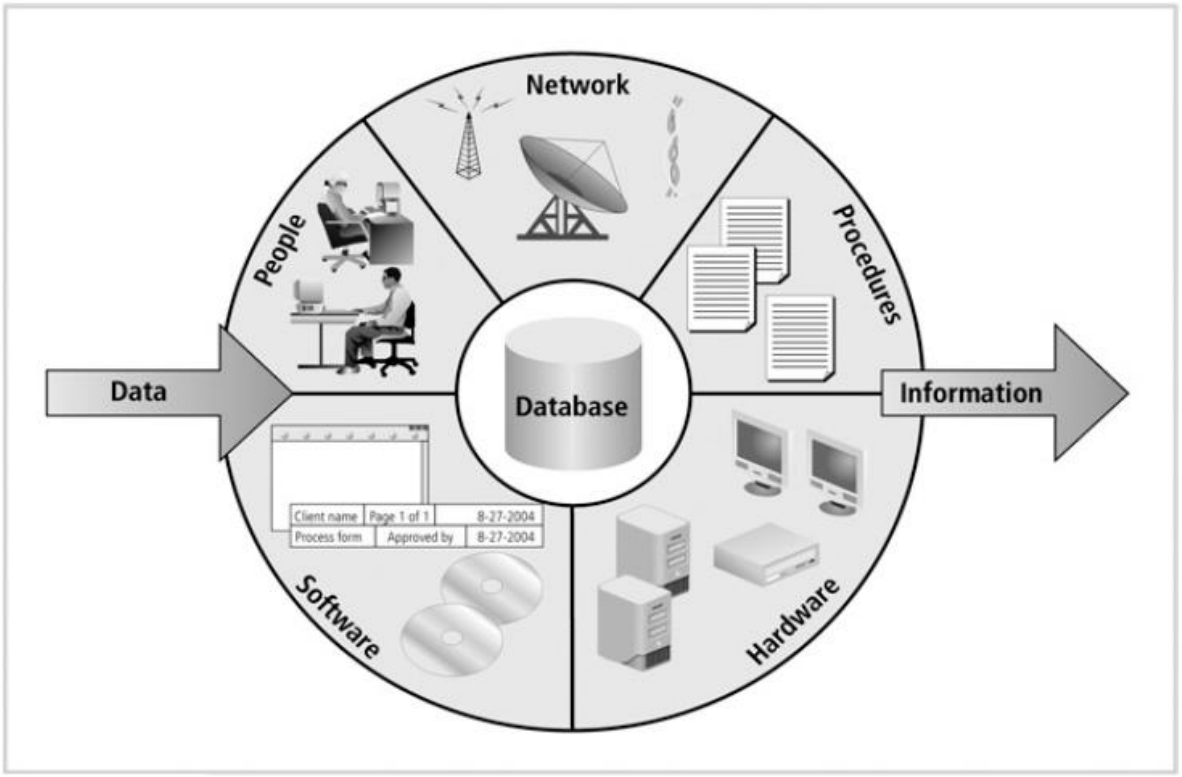
Western Digital has yet to comment on claims that the breach reported earlier this month led to data being stolen.

by Dark Reading Staff, Dark Reading — April 15, 2023

VULNERABILITIES/THREATS | 1 MIN READ | ARTICLE

Source: https://www.darkreading.com/database-security, accessed on 27-April-2023

Information Systems (IS)



Information system components

- Information system - comprised of components working together to produce and generate accurate information
- Central to any Information System is the **database** that contains all the required data and **information** that the organization acquires, processes, generates, stores and uses to run its business

Data vs Database vs DBMS

- Data
  - Data or Information –
    - is one of an organization's most valuable assets
    - critical for all individuals and organizations (government, SME and corporations) to function properly
- Database
  - An organized collection of structured data to make it easily accessible, manageable and updatable
- DBMS
  - Typically, a Database Management System or **DBMS** such as **MS-SQL** or Oracle is used to manage the databases
- Organizing data in database using DBMS provides:-
  - Better control on access and security such as encryption
  - Better activity tracing and auditing capabilities
  - Efficient backup and recovery management
  - Reduced data redundancy and increased consistency.

Database Security Problems/Breaches

- Since data is very valuable, it is subject to misuse, damage or loss or can be stolen – by whom ?
- Problems can come in many ways
  - Unauthorized access to steal valuable data – How can this happen ? What is impact ?
  - Intentional damage caused by unauthorized persons – How can this happen ? What is impact ?
  - Accidental damage caused by authorized persons or application – How can this happen ? What is impact ?
  - Other damages caused by power interruptions, hardware, OS or software failure etc

Database Security Vulnerabilities

Vulnerability refers to the weakness in the system

- Network vulnerabilities
  - Weaknesses within an organization's software and access infrastructure that allow cyber attackers to gain access and cause harm.
- Operating system (OS) vulnerabilities
  - Caused by exposures within an OS typically unpatched and outdated OS
- Process vulnerabilities
  - Occurs when security procedures are inadequate or nor strictly followed such as use weak passwords, sharing password etc
- Human mistakes - insufficient training, careless

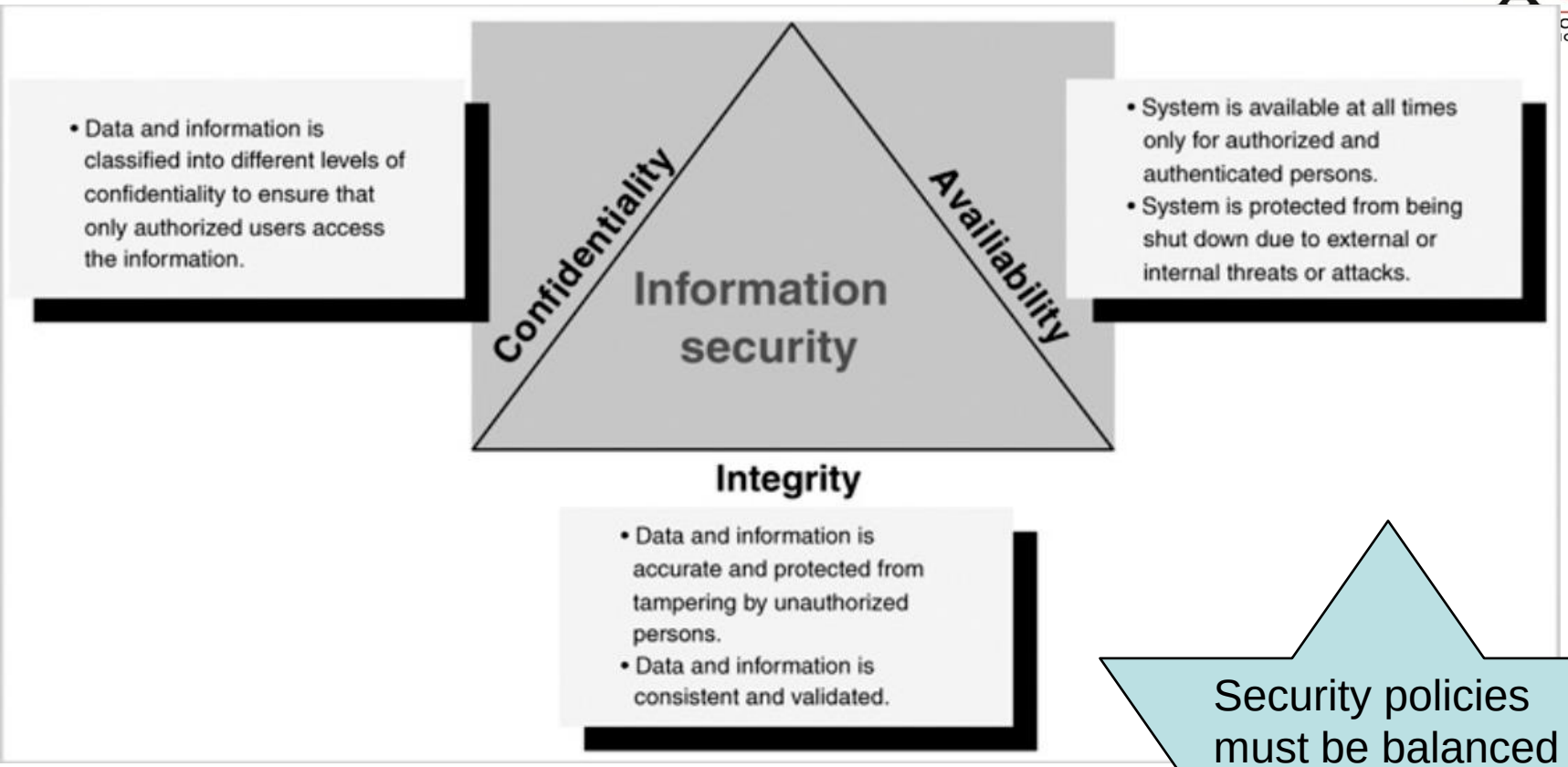
Database Security

Definition

Database security is a discipline that seeks to protect data stored into a DBMS from intrusions, improper modifications, theft, and unauthorized disclosures. This is realized through a set of *security services*, which meet the security requirements of both the system and the data sources. Security services are implemented through particular processes, which are called *security mechanisms*.

- DB Security is a complex and challenging endeavor that involves all aspects of information security technologies and practices
- DB Security refers to the range of tools, controls, and measures designed to establish and preserve database **confidentiality, integrity, and availability**
- DB Security enforces security at all database levels
- To achieve highest level of protection, data access point must be small

CIA Triangle



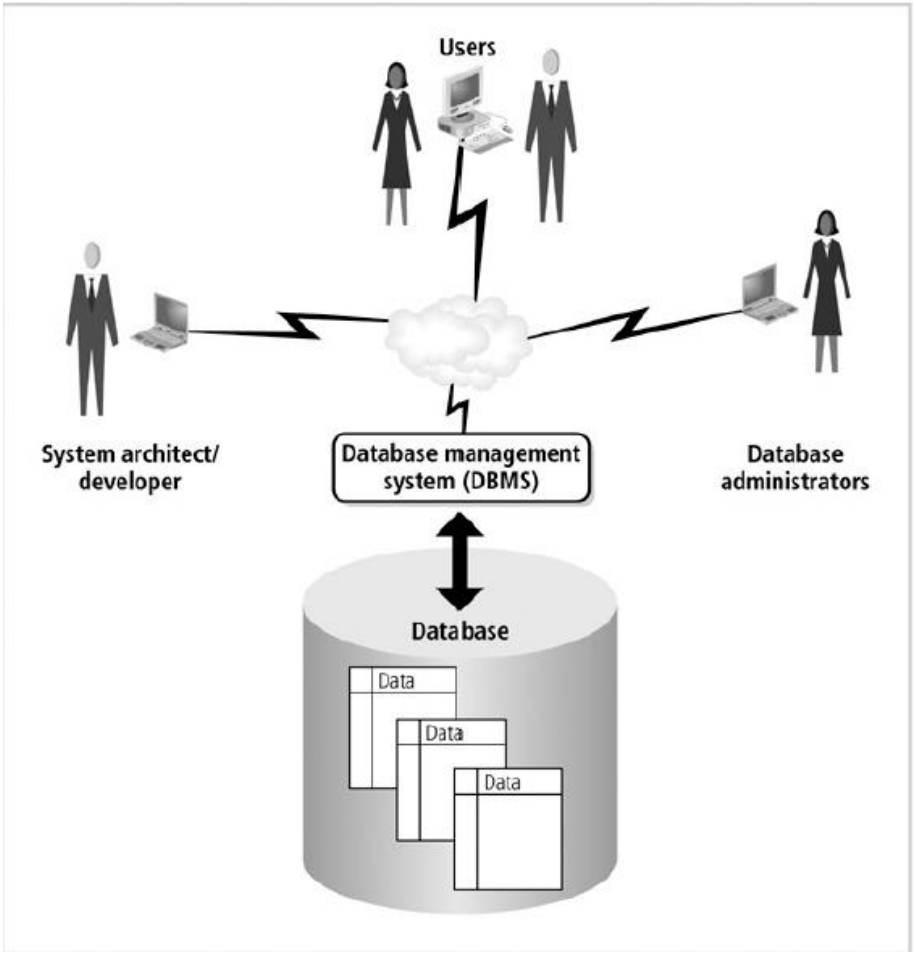
Security policies must be balanced according to the C.I.A. triangle

C.I.A

Confidentiality	Integrity	Availability
What?		
• Data loss can cause huge monetary and image loss. • **Information is safe from accidental or intentional disclosure.** • Keeping the identity of authorized parties involved in sharing and holding data private and anonymous.	• Data only has value if it is accurate. • **Information is safe from accidental modification or intentional unauthorized modification** • It is a requirement that information and programs are changed only in a specified and authorized manner.	• Data only has value if the right people can access it at the right time. • **Information is available to the authorized users when needed**
How ? Best Practices		

• Permission Control (Authentication & Authorization)
• Encryption
  • Database, Column, Backup
  • Symm , Asymm, Cert, Pwd
• Views
	• Good database design & implementation – constraints (entity, relationships, data type, data length, valid values, default values etc)
	• Trigger (automation & protection, auditing)
	• Auditing (what happened or what could happen, who did it, when it happened)
		• Backup – up-to-date backups in external location to protect against theft or destruction
		• Access control – limit users & timing to ensure server is in optimal condition (protect against Denial-Of-Service attack)

Types of Users



What role do you play here ?

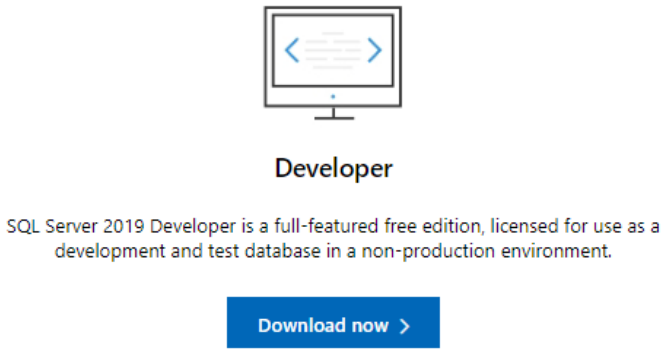
DB Security Best Practices

A·P·U
ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

- Access Control (User/Permission Management)
  - Authentication
  - Authorization/Privileges
  - Password Policies
  - Role
- Data protection
  - Encryption
  - Backup
  - User action validation to protect against accidental or intentional data loss
- Auditing
  - Try to identify what could happen (potential risk) - *future*
  - Keeping track of is happening (monitoring) - *present*
  - Investigating security breach (What happened, Who did it, When it happened) - *past*

Homework

- Download and install
  - MS SQL Server – Developer Edition
  - Management Studio



  - Source: https://www.microsoft.com/en-us/sql-server/sql-server-downloads