Database Security

CT069-3-3

Security Architecture and Principles

Lecturer Information

- Lecturer– Dr. Kulothunkan Palasundram

- Email – kulothunkan@apu.edu.my

Learning Outcomes

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

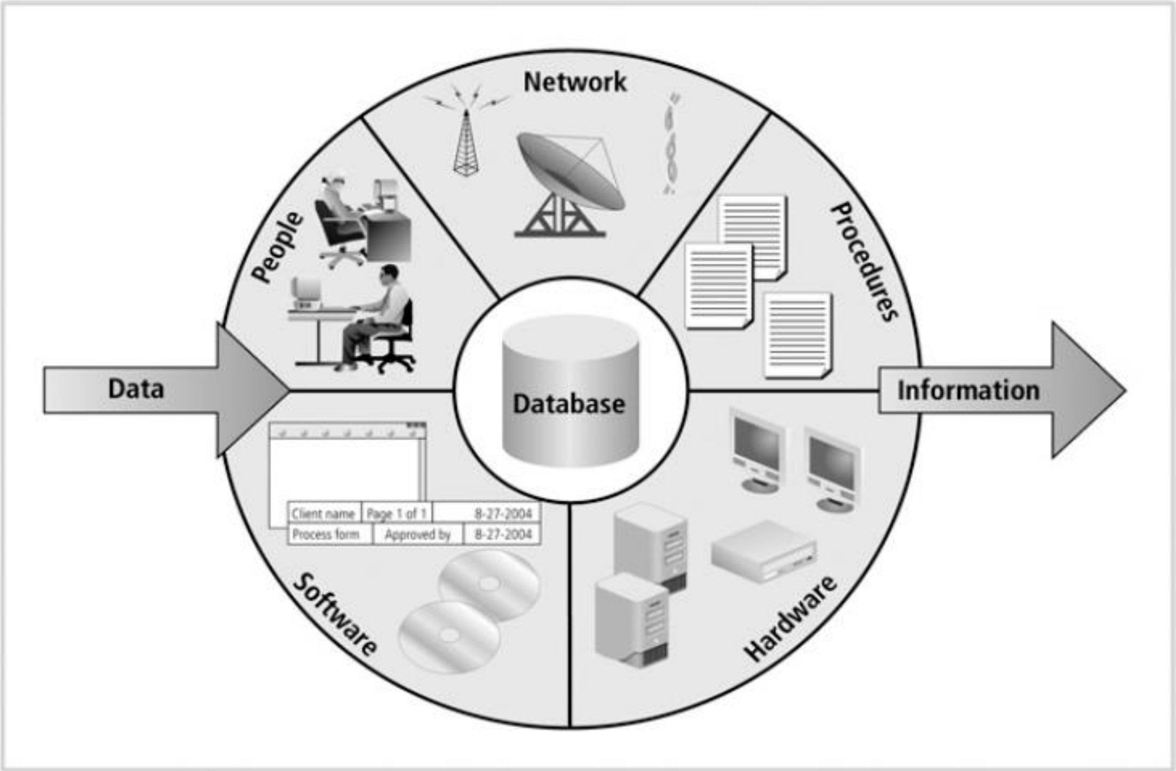
- Information security architecture
- Key information security principles to protect our data

Key Terms you must be able to use

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

- Security Architecture
- Security Principles

Recap: Information Systems (IS)



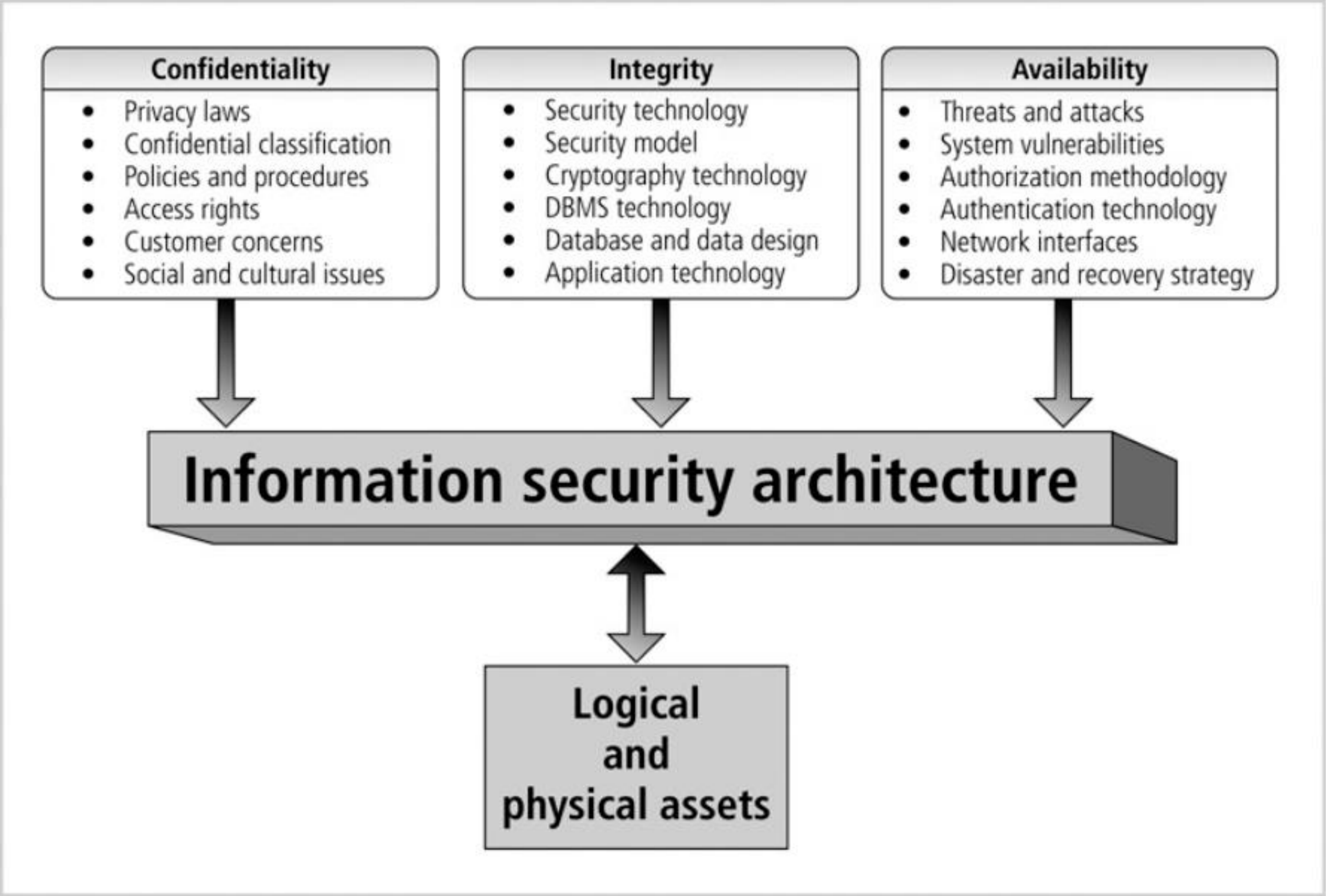
Information system components

- Information system - comprised of components working together to produce and generate accurate information
- All components are **integrated** to function properly

Recap: Database Security Vulnerabilities

- 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  - Caused by exposures within an OS typically unpatched and outdated OS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 vulnerabilities - insufficient training, careless

Security Architecture



Confidentiality

- Privacy laws
- Confidential classification
- Policies and procedures
- Access rights
- Customer concerns
- Social and cultural issues

Integrity

- Security technology
- Security model
- Cryptography technology
- DBMS technology
- Database and data design
- Application technology

Availability

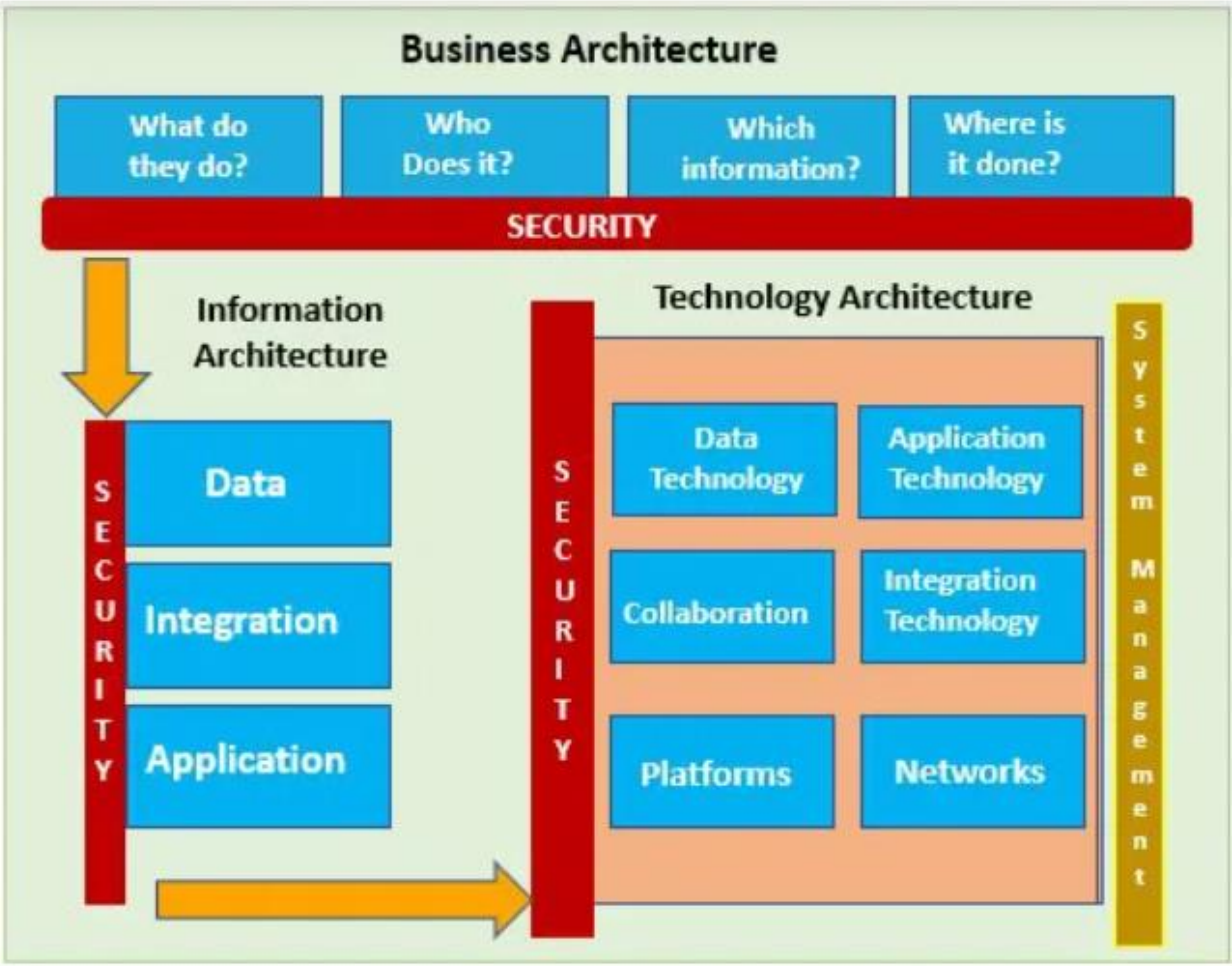
- Threats and attacks
- System vulnerabilities
- Authorization methodology
- Authentication technology
- Network interfaces
- Disaster and recovery strategy

Information security architecture

Logical and physical assets

What is a Security Architecture ?

A Security Architecture refers to an integrated set of **tools, procedures and users/roles** which is developed and deployed to protect the system from unauthorized access, modification or destruction.



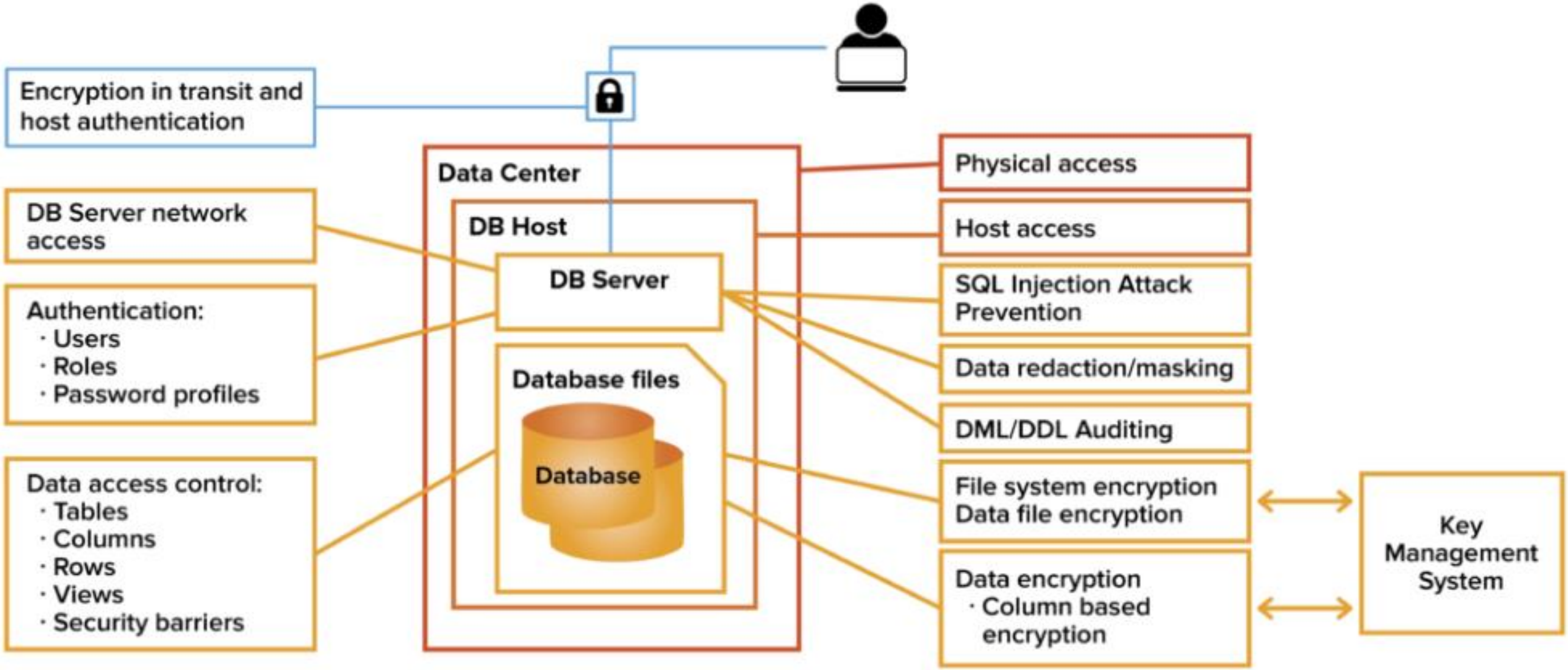
Security Architecture - examples

- **People/Roles** – *players in the system*
  - Management
  - DBA
  - Users
  - Customers

What is their roles and responsibilities? What can they do ? What cannot they do ? Who manages the users ? etc

- **Procedures** – *how to do things in this system*
  - Must separate web and database servers
  - Take backup every night
  - Users must be authenticated using 2FA authentication
- **Tools** - *what are the technologies that we can use to achieve high level security? What devices or software that are prohibited from being used ? etc*
  - Use only the latest version of browser, os, application
  - Old versions not allowed and must be un-installed
  - Cannot use thumb drive

DB Security Architecture



Security Principles

- To address the vulnerabilities and better protect our data, we need to adopt and apply IS security principles
- In other words, a good security architecture will implement a good set of security principles
- Security principles provides guideline on how we develop, implement and operate IS components to be highly secure

Security Principles

- **Economy of mechanism**
  - This basically means keep your system as simple as possible. Simpler systems have fewer bugs and easier to debug and protect.
- **Confidentiality**
  - Permission control – authentication and authorization
  - Encryption to protect the data on transit or at rest
  - Data hiding (SQL Views)
- **Integrity**
  - Audit trail - We can trace all changes to data changes from the time it was acquired to even after it was disposed (timeline subject to laws etc).
  - Assurance that the data that we have is accurate (up-to-date, not illegally modified etc)
  - Continuous monitoring to ensure there is no security breach

Security Principles

- **Least privilege**
  - – Give a user the <u>minimum privileges </u>required to perform their work. The more privileges you give to a party, the greater the danger that they will abuse those privileges or mistakenly cause more damage.
- **Availability**
  - – Access control – control how many users can access at a certain time, when system can be accessed etc
  - – Ensuring system/data is available to authorized users anytime they need it without any interruptions
- **Password Policies**
  - – A good password policy is the first line of defense against the unwanted accessing of an operating system. In most cases hackers utilize tools that use the dictionary method to crack passwords. These tools use the permutations of word in the dictionary to guess the password.

Security Principles

- **Fail-safe defaults**
  - Default to security, not insecurity. If policies can be set to determine the behavior of a system, have the default for those policies be stricter (more secure), not less.

- **Separation of duty and privilege**
  - Require multiple (MFA ?) and separate authentications to perform critical actions - such user account to access emails; admin account to manage database

Recap: 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 ?		
• 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)