# COS30041 Creating Secure and Scalable Software

Lecture 07b Building Secure Enterprise Applications

SWINBURNE UNIVERSITY OF TECHNOLOGY

# Learning Objectives

- After studying the lecture material, you will be able to
  - Discuss the security issues in Enterprise Application
  - Mitigate those security issues in building secured enterprise applications

# Pre-requisite

- Basic Security considerations
  - Authentication
  - Authorization
  - Confidentiality
  - Data Integrity

# Case Study – EMS – Background

SECURE is a company proud of developing secure enterprise applications. The company uses an online system called Employee Management System (or EMS in short) to perform the CRUD operations of its employee records. At the moment, only administrators can perform these operations.

However, the company is now considering extending EMS to allow its employees to maintain their own information by adding the following features.

# Case Study – EMS extension (cont’d)

The requirements of the new features are as follows:

1. Employees can review their own individual information (except the password) but not others
2. Employees can change their own individual information (including password) but not others. See the business logic for employees to change their own passwords for details. [In case, when employees forget their own passwords, they can ask the administrators to reset their passwords via phone or email.]

# Case Study – Design decision 1

Context: Business logic – user login

- The company choose to send the existing password to the web tier for authentication

Questions:

- Is there a problem with this?
- What is the reason behind this?
- Is this a good practice? Why or Why not? If not, propose an alternative and justify your choice.

# Case Study – Design decision 2

Context: Changing employee’s record by individual employee

- What information can be changed by the employee?
- What cannot?
- Why?

# Case Study – Design decision 3

Context: Business logic – employees updating their personal details

- The company decides to do the actual updating at the data layer, that is, after the relevant business objects have checked the relevant information are valid, then perform the updating

Questions:

- What is the reason behind this?
- Is this a good practice? Why or Why not? If not, propose an alternative and justify your choice.

# Case Study – Design decision 4

Context: Changing employee's password by individual employee (employee keys in **old**, **new** and **reconfirm**)

- The company choose to send the existing password to the web tier for authentication purposes and then send the new password to the business tier for updating after checking the new password is the same as the reconfirmed password.

Questions:

- Is there a problem with this?
- Is this a good practice? Why or Why not? If not, propose an alternative and justify your choice.

# Case Study – Design decision 5

Context: Display employee's personal details by individual employee

- The company choose to implement a DTO, EmployeeDTO, which contains all information of the employee except the password

Questions:

- Is there a problem with this?
- Is this a good practice? Why or Why not? If not, propose an alternative and justify your choice.

# Case Study – Design decision 6

Context: Storing password

- The company choose to store the password as plain text

Questions:

- Is there a problem with this?
- Is this a good practice? Why or Why not? If not, propose an alternative and justify your choice.

# Overall

- Is the application secure at the moment?
- Is the application secure after making all the changes as suggested?
  - What needs to be done to secure the online application? [REMEMBER – this is not about protecting from hacking]