Lab1 COMS20012 Computer System B
Message Analysis using Wireshark

- **Objectives:**

Hi class, welcome to your first lab. Hope you will enjoy and have fun!

Today, your task is to engage in group discussions to explore the following problems. Each team will have 45 minutes to delve into the issues and collectively draw conclusions. Following the discussion, select one representative from your team to present the identified problem and the conclusions reached. Ensure that your representative provides strong arguments supporting these conclusions. This exercise aims to foster collaborative problem-solving and effective communication within your teams and to expend understanding of CIA principle in the real world scenario.

- Please read before solving any questions!

Problem 1!

Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash.

a. Give examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement.

b. Would it be the same requirements for a payment gateway system where a user pays for an item using their account via the payment gateway?

c. If these systems involve third-party integrations, analyze the security implications.

d. Consider how the confidentiality, integrity, and availability requirements extend to external entities.

e. Explore the impact of different user authentication methods on the security requirements.

1. **Deliverable**: Report (Answers to the questions)

Problem 2!

Consider a financial report publishing system used to produce reports for various organizations.

a. Give an example of a type of publication in which confidentiality of the stored data is the most important requirement.
b. Give an example of a type of publication in which data integrity is the most important requirement.
c. Give an example in which system availability is the most important requirement.
d. Explain the importance of user authentication in maintaining the security of the financial report publishing system.
e. Consider the impact of distributed denial-of-service (DDoS) attacks on system availability and suggest mitigation strategies.
f. How would you handle confidentiality concerns if the financial report publishing system interacts with third-party analytics tools or services?

1. **Deliverable**: Report (Answers to the questions)

Problem 3!

For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.

a. A student maintaining a blog to post public information.
b. An examination section of a university that is managing sensitive information about exam papers.
c. An information system in a pathological laboratory maintaining the patient's data.
d. A student information system used for maintaining student data in a university
e. that contains both personal, academic information and routine administrative in- formation (not privacy related). Assess the impact for the two data sets separately and the information system as a whole.

f. A University library contains a library management system which controls the distribution of books amongst the students of various departments. The library management system contains both the student data and the book data. Assess the impact for the two data sets separately and the information system as a whole.

g. Consider a scenario where budget constraints limit the implementation of certain security measures. Prioritize the implementation of security controls based on the potential impact.

1. **Deliverable**: Report (Answers to the questions)

Problem 4!

You are part of a team designing a smart home automation system that connects various devices, including security cameras, door locks, and thermostats, to enhance home management.

a. Give examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement.

b. In the event of a device failure or network disruption, how can the system maintain critical functionalities, ensuring continued availability?

c. How can the system address privacy concerns related to the data collected by security cameras, and what measures are in place to prevent unauthorized access to users' private spaces?

d. Consider scenarios where external attacks, such as denial-of-service, may impact the availability of critical home automation services. How would you mitigate such threats?

e. Discuss measures to guarantee the integrity of commands sent between devices, preventing tampering or manipulation.

2. **Deliverable**: Report (Answers to the questions)

Good Luck ☺