The University of Sydney
School of Computer Science
Dr Suranga Seneviratne
Senior Lecturer - Security

THE UNIVERSITY OF SYDNEY

INFO3616/CSEC3616/CSEC5616 — S2 2025
Assignment - 1

This is an **individual** assignment.

This assignment worths 10% of the final marks of the course. It covers Weeks 1-3 (inclusive).

Submit your final report as a `PDF` and codes as a `zip` file in Canvas. In Canvas, under Assignment 1, you will find two links to submit your report and code separately.

You should explain any details of how to run your code in the report.

Please read the below instructions carefully.

***** IMPORTANT *****

1) **Note the answer release date:** Please note the answer release date mentioned below. Any submission after that will get zero marks, instead of a late penalty.

2) **Typeset reports only:** We accept only typeset answers. Any hand written answers will get zero marks. This is because we can't do plagiarism checks for hand written answers.

3) **DO NOT repeat questions in the report:** Simply include the question number and your answer only. If you include question text in your answer sheet, your TurnItIn score will be high and there will be additional checks. This will cause a delay in releasing your marks. **We will also impose a penalty of 10% of the total marks.**

3) **Cite your sources:** If you are referring to any internet sources include them as citations. We do not expect any specific citation style. You are free to select a style you think as appropriate. As mentioned in class announcements you are free to use GenAI. If you do so, make declaration in the report.

***** SUBMISSION *****

Final Report & Code: Due by Week 5, Sunday the 07th of September, 2025 11:59PM

Simple Extensions: For this assignment, you can apply for simple extensions following the university process. If your request is **approved**, the revised deadline will be **12th of September, 2025 11:59 PM**. Please note that you have do it yourself and no need to contact the unit of study co-ordinator for this. We will get an automatic email from the system if your request was approved. Also note that, this system is not connected with Canvas, therefore it is normal for you to see the old deadline in Canvas, even if your simple extension was approved.

Answer release: The answers to this assignment will be automatically released on the **15th of September 00:00 AM**. Any submissions after that will get **zero marks**. If you have a legitimate reason that requires an extension beyond that you will need to go through the university special considerations process. If approved, what you will be grant is a mark adjustment not an extension.

1 Fundamentals of Security Engineering (25 marks)

a) Definitions (5 marks)

Define safety engineering and reliability engineering, and explain how security engineering differs from them.

b) Conceptual Framework (10 marks)

i List and explain the four components of the conceptual framework for security, that we are using in this class. **(2 marks)**

ii Given the scenario below, extract and explain the various components of the **conceptual framework for security**. **(8 marks)**

A company that recently secured several healthcare contracts is designing a secure system for employees to access valuable client health data remotely. The company mandates that only employees with multi-factor authentication (MFA) enabled can access the data. The system uses a combination of password-based authentication and biometric scans for identity verification. Employees who maintain good security practices, such as regularly updating passwords and enabling MFA, are rewarded with bonuses.

However, attackers are highly motivated to gain unauthorised access to the system. Access to sensitive healthcare data could allow ransom calls or the sale of private information on black markets. The company is aware of these risks and takes steps to prevent attackers from exploiting weak passwords or spoofing biometric data.

To ensure the security of the system, the company conducts regular security audits, monitors access logs, and relies on the high accuracy of the biometric system, which has a False Acceptance Rate (FAR) of 0.001% and a False Rejection Rate (FRR) of 0.5%. Combining both biometric authentication and passwords improves security by at least 100 times compared to using passwords alone.

c) Security Goals (10 marks)

Analyse the following real-world IT-related incidents and data breaches where specific security goals were compromised. For each scenario, identify the compromised security goal (e.g., Confidentiality, Data/Message Integrity, Authenticity, Authorisation, Accountability, Non-repudiation, Deniability, Availability, Privacy) and explain how the incident compromised that goal.

You will have to do your research by referring to various news articles and incident reports to understand what happened in each incident. We have given some sample links to get you started but feel free to investigate more and understand what happened in each incident. *Most of the questions will have more than one correct answer, depending on how you look at them. We will accept them if your explanation is correct and related to the incident. However, you should only pick one, i.e., one you think as most appropriate, and explain it. Attempts to list multiple answers will result in zero marks.*

Provide clear and concise explanations for each scenario, as shown in the example.

Example 1 - CrowdStrike Falcon update failure 2024 - Link

Compromised Security goal: Availability

Explanation: Windows machines with the CrowdStrike Falcon Sensor installed went into the boot loop with BSOD (Blue Screen of Death), making them unusable and compromising availability.

Example 2 - Optus data breach 2022 - Link

Compromised Security goal: Confidentially

Explanation: Personal information of the Optus customers, such as driver's licence number, passport number, and address, was harvested by an attacker using an unauthenticated API endpoint. Optus was in breach of keeping their customer's data confidential. Here, arguments can be made for security goals such as authorisation and privacy - but they are secondary to confidentiality.

2 marks for each. 1 mark for correctly naming the security goal and one mark for the explanation.

i MOVEit Breach, 2023 Link

ii Okta Support System Breach, 2023 Link 1, Link 2

iii MGM Resorts Cyberattack, 2023 Link 1 Link 2

iv Medibank Breach, 2022 Link 1 Link 2

v SolarWinds Supply Chain Attack, 2020, Link.

2 Social Engineering in Practice (25 marks)

You are a given a X (formerly Twitter) profile of a fictitious person.

https://x.com/EmilyB62363

A pdf export of the profile is also given, in case you can't access the link.

You are also given a data dump from a data breach that happened in a website where Emily is a registered user (i.e., `email_md5_dataset.txt`). It contained email addresses of the registered user and the unsalted MD5 hashes.

Your task is to conduct reconnaissance on the profile, guess the password (which is a combination of keywords/information that can be extracted from the profile), and find the target's email address from the given list. Write a Python program that does the following:

- Given a set of keywords, generate all possible permutations of keyword combinations to be used as potential passwords (see the example below).
- For each generated password, compute its MD5 hash and check whether it is present in the given file.

- If there is a match, print the corresponding email address.

For example, if you identify the possible keywords as "blue" and "car," the Python program should generate a list of permutations as below.
blue
car
blueblue
bluecar
carblue
carcar

Hint: The correct password contains only lowercase letters, digits, and **a** special character. The length of the password is less than 20 characters.

Include details on how to run your code, along with the email address, plaintext password, and the MD5 hash of the password, in the `PDF` report. Submit your code using the code submission link provided in Canvas.

3 Access Control (25 marks)

a) Basics

i Access control is often categorised into two general forms (which we called two ends of a spectrum). What are they, and how are they different from each other? **(4 marks)**

ii Which form of access control, from the options above, do cloud-based storage solutions like Google Drive or Microsoft OneDrive use? Explain your answer. **(3 marks)**

iii Modern CPUs have support for access control. Explain two key ideas of the common x86 architecture. **(4 marks)**

iv In class, we learned about role-based access control (RBAC) and discussed its primary use in databases. However, there are other forms of access control. Conduct your own research on the following access control methods and explain them briefly (3-5 sentences each). For each method, provide an application case where it might be useful. **(4 marks)**

a Rule-based access control

b Attribute-based access control

b) Security Policy Models - Definitions

Explain the key difference between the Bell-LaPadula and Biba models. **(2 marks)**.

c) Security Policy Models - Example

Table 1 and Table 2 show mappings between users and clearances, and between required clearances and objects, respectively. The clearance level increases as Basic, Internal, Confidential, Secret and Top Secret, in increasing level of security. Only these mappings are defined; no other rule sets exist. State if the following statements are True or False, and explain why.

i "In a Bell LaPadula model, Sarah can read the file financial_report.txt." **(2 marks)**

User	Clearance
John	Basic
Sarah	Internal
Michael	Confidential
Emma	Secret
Thomas	Top Secret

Table 1: User Clearance Levels

Object	Required Clearance
company_memo.txt	Internal
financial_report.txt	Confidential
research_proposal.txt	Secret
strategic_plan.txt	Top Secret

Table 2: Object Clearance Requirements

ii "In a Biba model, Michael can edit company_memo.txt." **(2 marks)**

iii "In a Bell LaPadula model, Thomas can help John access strategic_plan.txt by writing its content to company_memo.txt." **(2 marks)**

iv "In a Biba model, Emma can modify strategic_plan.txt." **(2 marks)**

4 Linux Access Control (25 marks)

Below questions are associated with the provided Azure VM.

a) Basic Access Control

Below questions can be answers by Linux One liners. Provide the **answer to each question** and **include the command you used**. Make sure that you include the command as letters/characters in the report (than screenshots/images), so that the markers can copy/paste command and check whether it is working.

i What is the `User ID (UID)` of the user `sheppard`. **(1 mark)**

ii What is the `Group ID (GID)` of the group `scientists`. **(1 mark)**

iii Find which group(s) the user `carter` belongs to. **(1 mark)**

iv Find all the users in the group `humans`. **(1 mark)**

v Does the user `ronan` have `sudo` access? There are multiple ways to do this. Answers requiring more than one command is also accepted. **(1 mark)**

vi Does the user `carter` have `sudo` access? There are multiple ways to do this. Answers requiring more than one command is also accepted. **(1 mark)**

b) File Permissions

For i-iii, use the linux `find` command with correct options and make sure that you command do not generate any permission denied messages or other error messages. Include the commands you used in your answer. You must include the full paths of the files.

i Find all the non hidden **files** owned by user `teyla`. **(1 mark)**

ii Find all the files owned by `teyla` and associated with the group `ancients`. **(1 mark)**

iii Locate a file owned by `mckay`. Can `carter` write to this file? Can `ladon` write to this file? Explain your answer. **(2 marks)**

iv In user `kolya`'s home directory, you will find two files `genii_launch.sh` and `genii_pre_launch.sh`.

Can the user `kolya` execute either of these files?

Can the user `ladon` execute either of these files?

Can the user `todd` execute either of these files?

Explain your answers. **(6 marks)**

c) Directory Permissions

i Locate the `/mission_reports` directory. Identify its owner and associated group. **(1 marks)**

ii Become user `ladon`. You should be able to do this even without knowing user `ladon`'s password. Try deleting a file in `military_reports`. Are you allowed to delete a file? You can select yes to any warnings you get. **(2 marks)**

iii Still remaining as user `ladon` try deleting a file in `science_reports`. Is it successful? **(2 marks)**

iv If you check the permissions of the directories `military_reports` and `science_reports`, you will see that the owner, group, and others all have full permissions on each directory. Even so, the user `ladon` can delete files only in one of them. Explain why. **(2 marks)**

v You will see that the `/tmp` directory on Ubuntu has a similar setup to the `science_reports` directory in the previous question. Explain why this setup is important for a directory like `/tmp` that is writable by all users. What problems might arise if this setup were not in place? **(2 marks)**