CM2025 Computer Security: Midterm Coursework

April 2022 version 3

Introduction

This coursework aims to assess the first five topics on the Computer Security course. The coursework consists of two parts: a written report and some short answer questions. You should complete both parts.

PART A: Securing the computer network of a local school

This part is worth **60%** of the mark for the mid-term.

You are in charge of the security for a computer network for a large local high-school. The school has several requirements and constraints for the computer system:

- The data and user account system is based on servers running on-site at the school as the school has a very strict data protection policy prohibiting the use of cloud-based servers.
- The network needs to be lockdown-ready in case there is a flare-up of a disease-causing virus such as Covid-19. That means users should be able to access the network remotely (off-site) as well as locally (on-site).
- There are at least three types of users, namely, administrator, teacher and students. Different users have differing levels of access.
- Users need access in different ways, using tablets, mobile phones, desktop computers and laptops.

You are trying to convince the school's governors to spend more money and staff time on computer security. You have decided that you are going to try to paint them a frightening picture of the computer security landscape.

Your submission to the school will be in the form of a report of up to 1500 words. In the report, you should (1) identify THREE threats and (2) explain what might happen if the school's network is attacked in that way. You should then (3) suggest what they should do to defend against that specific attack and why that defence works.

Here are some places you might find information about common threats and solutions:

IEEE Security & Privacy
https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013
IEEE Access
https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639

Kaspersky SecureList:
https://web.archive.org/web/20220527080756/https://securelist.com/it-threat-evolution-in-q1-2022-non-mobile-statistics/106531/

https://web.archive.org/web/20220527080734/https://securelist.com/it-threat-evolution-in-q1-2022-mobile-statistics/106589/

Marking criteria for Part A:

Has the student explained the attack and how it would affect the school?

- 0: No, or the explanation is incorrect
- 4: Yes, but the explanation is missing elements, or has minor errors or the attack is not relevant to the situation
- 5: Yes, but the explanation shows little evidence of independent research
- 7: Yes, the explanation is clear and correct as far as I can tell, and include good evidence of independent research
- 8: Yes, the explanation is clear and correct as far as I can tell, and include evidence of deep independent research and important insights
- 10: Wow, this is a professional level analysis of a security threat citing many sources and adding new insights to the research

Has the student suggested realistic defences, and explain how they protect against the attack?

- 0: No, or the explanation is incorrect
- 4: Yes, but the explanation is missing elements, or has minor errors, or is not fully appropriate to the attack
- 5: Yes, but the explanation shows little evidence of independent research
- 7: Yes, the explanation is clear and correct as far as I can tell, and include good evidence of independent research
- 8: Yes, the explanation is clear and correct as far as I can tell, and include evidence of deep independent research and important insights
- 10: Wow, this is a professional level analysis of the application of a defensive technique citing many sources and adding new insights to the research

Total available marks: 60 marks (20 for each threat you describe)

PART B: Cryptography

This part is worth **40%** of the mark for the midterm coursework.

1. Why are prime numbers important in cryptography? **[4 marks]**

2. Are 150 and 175 co-prime? Justify your answer. **[4 marks]**

3. State Euler's Phi function and show the result of applying Euler's Phi function to the number 10. Show your working. **[6 marks]**

4. Explain why Euler's Phi function is important for cryptography. **[6 marks]**

5. Write a pseudo-code algorithm that implements the modulo function. **[6 marks]**

6. Alice is sending a message to Bob. Bob wants Alice to encode the message using RSA. Bob thinks that the following elements are necessary in order for Alice to encode the message:

- two prime numbers multiplied together to make *N*

- a value called *e* which is co-prime with *phi(N)*

i. . State the formula that will allow Alice to take message M and encrypt it to E using e and N. **[4 marks]**

ii. Given an N of 21, select a value for e. Show your working. Do you agree that this forms Bob's public key? **[4 marks]**

iii. Alice wants to send a message which is just a number to test the encryption is working. Choose a small number for Alice's message (M<20) and encrypt it with Bob's public key. Show your working. Make it clear what your chosen M is. **[6 marks]**

Total available marks: 40