CM2025 Computer Security: Midterm Coursework

October 2022 version 1

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: Bank Security

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

You are chief security manager for one of the biggest private banks in your city. Many customers including people and companies have accounts there and rely to these accounts financially. Computer security for banks is very important because banks are frequently targeted by hackers and adversaries. If hackers can hack the bank's network and find the private information of customers or if they can prevent customers from accessing their accounts, they will lose their trust in the bank and will close their accounts and withdraw their monies.

Computer security for banks is also complex because a lot of different types of people and organizations use their network and services:

- Customers use different apps and online banking websites to access their accounts. Additionally, they may need onsite services.
- Bankers and bank staffs that have directly access to the core banking systems
- Companies that need the services provided by the bank (such as online payment services)
- Other banks and branches, the bank should be able to work with other banks and branches to send or receive data about its customers
- ATMs are also a part of the system

Many of the systems used by these different stakeholders will be different from each other (e.g. a mobile app for managing accounts by customers or a SWIFT service which is used for the execution of financial transactions and payments between banks worldwide), but there are services, such as the online banking services, though in different forms and with different levels of access.

As a security manager you need to keep up to date on possible threats to the bank. For this coursework, you should research 3 specific threats that could affect a bank (e.g. a specific piece of malware or a specific type of DDoS attack), describe that threat and suggest a security mechanism to protect against it, and explain how it will defend against the attack.

You could, for example use articles in the Online library for your research. All sources must be fully referenced.

Here are some starting points for your research:

Quarterly reports of threat statistics from Kaspersky https://web.archive.org/web/20200912123817/https://securelist.com/all/?category=919

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

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

Marking criteria for Part A:

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

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 defenses, 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.

Search the Internet and learn about the Elliptic Curve Cryptography (**ECC**).

Then, based on the **RSA** and **ECC** answer the following questions:

1) What is the concept of one-way function in cryptography? **[2 marks]** Describe the one-way functions which are used in **RSA [2 marks]** and **ECC [2 marks]**.

2) Explain how the private and public keys are defined in **ECC [4 marks]**

3) Compare the **RSA** with **ECC** in terms of the key size and encryption strength **[4 marks]**

4) Bob uses **RSA** and chooses the pair ***(N=713, e=7)*** as his public key. Using this public key, encrypt the message **M=59**. Show your work step-by-step. **[4 marks]**

5) Using the public key in part (4), Alice has encrypted a message (we do not know what was the original message), and sends it to Bob through a public channel. Assume the encrypted message sent by Alice is **16**. Eve also has the Bob's public key and receives the encrypted message (sent by Alice). Eve claims that using a simple program (as shown in the following) can find the prime numbers ***p*** and ***q*** which are used by **RSA** to calculate **N** (i.e. **N=p.q**), thus the original message is 35. Check the program and verify her claim? **[2 marks]** Show your work step-by-step. What is the output of the program? **[2 marks]** Explain how she decrypted the message without having Alice's private key? **[2 marks]**

```
i=2
N=713
while i<N/2:
        if N%i==0:
                print(“p=”,i, “q=”,N/i)
                break;
```

6) Explain how Eve could find the decrypted message using ***p*** and ***q*** in part (5). **RSA** algorithm is not strong enough or Bob missed something? **[4 marks]**

7) Write a simple program (as a pseudocode or any programming language) to show how one can use it to try to find the private key in **ECC** (having two points ***P*** and ***Q***). Assume the starting point on the curve is ***P*** and the public key is ***Q*** which is another point on the curve, additionally, in your pseudocode or program assume the operation "." (in some documents it is shown by "+") has been defined so you can simply apply it on two points on the curve. **[4 marks]** Explain in which circumstances such a program can find the private key. **[2 marks]**

8) Having ***k*** (a private key) in **ECC** and the starting point ***P*** on the curve, write a simple program (as a pseudocode or any programming language) to ***<u>efficiently</u>*** (i.e. in terms of computability) calculate the public key. Again, in your pseudocode or program assume the operation "." (in some documents it is shown by "+") has been defined so you can simply apply it on two points on the curve. **[6 marks]**

Total available marks: 40 marks