UNIVERSITY OF Ottawa
Faculty of Engineering and Computer Science
CSI 4139-CEG 4399 - SEC 5100 – Fall 2024

Assignment 1

Note

Some questions might be open-ended and require your own opinions and creativity, as the answers can vary considerably.

Question 1 (15%)

Based on the definitions we had for “Threats”, “Vulnerabilities”, and “Controls”, bring two different examples or scenarios, and indicate each of these three aspects in each scenario.

Question 2 (10%)

Using some sentences or examples, show how the four kinds of threats, “Interception”, “Interruption”, “Fabrication”, and “Modifications” relate to the three concepts, preserving “Confidentiality”, “Integrity”, and “Availability”.

Question 3 (10%)

Do you believe attempting to break into a computing system without authorization should be illegal? Why or why not? Bring at least two examples/scenarios to support your answer.

Question 4 (15%)

For each of the following two programs, answer the three questions followed:

1. A program that accepts and tabulates votes in an election.
2. A program that allows consumers to order products from the web.

- Who might want to attack the program?
- What type of harms might they want to cause?
- What kinds of vulnerabilities might they exploit to cause harm?

After completion, submit your answers as a single pdf file on Brightspace.

Question 5 (10%)

One-Time Pad is the only cryptosystem that provides ***Perfect Secrecy***.

- Describe the advantages and disadvantages of this cryptosystem.
- Bring one example in real-world applications, in which One-Time Pad is suitable to be used, and one example that is not. Justify your answers.

Question 6 (10%)

Rotor machines were used by Germany (Enigma) and Japan (Purple) in World War II. Watch this short clip on the Enigma rotor machine:

https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/case-study-ww2-encryption-machines

It consists of a set of independently rotating cylinders, each of which has 26 input pins and 26 output pins. Each input pin is connected to a unique output pin using internal wiring. You can see a related diagram in the following link, under the title "Rotor Machine":

http://sjsu.rudyrucker.com/~haile.eyob/paper/#3.%20Classic%20Cryptography

- A single-cylinder defines a mono-alphabetic substitution. Considering a 5-rotor machine, what would be the equivalent key length of a Vigenere cipher for this machine? Explain your answer.

- Humans are said to be the weakest link in any security system. Give two examples of human failure that could lead to compromise of encrypted data.

Question 7 (5%)

Based on the convention we use to represent the English alphabet using numbers 0 to 25, formulate Atbash Cipher by showing two mathematical expressions, one for encryption and one for decryption. Show the correctness of your expressions with one example.

After completion, submit your answers as a single pdf file on Brightspace.

Question 8 (5%)

Apply threat modeling to identify potential security flaws in a system:

- Choose a simple ecommerce web application and create a Data Flow Diagram (DFD) of the system.
- Using the STRIDE model, identify at least five threats that exist within the application.
- Propose specific mitigations for each threat and justify how these mitigations align with security design principles.
- Submit your DFD, a threat model table (Threats, Vulnerabilities, Mitigations), and a brief report explaining how the mitigations improve the security of the system.

Question 9 (10%)

Apply Secure SDLC principles to a practical example. Imagine you are part of a team developing an online payment system:

- Outline how you would integrate security practices into each phase of the SDLC:
  - Requirements
  - Design
  - Implementation
  - Testing
  - Deployment
- Submit a detailed report describing your security plan for each SDLC phase, along with a few real-world examples of how security failures could be avoided with proper SDLC practices.

Question 10 (10%)

- How would you test a ciphertext to quickly determine if it was likely the result of a simple **substitution**?
- How would you test a ciphertext to quickly determine if it was likely the result of a **transposition**?