CS-3002 Information Security

Assignment 01

Submission Deadline: 20 February 2025 (11:59 p.m.)

Section-I Principles of Secure Design (50 Points)

Question 1

Show a code example of each of the following principles, i.e. one piece of code that follows each principle and one piece of code that does not:

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of separation of privileges
6. Principle of least common mechanism

Write a short explanation of what the code does and how you enforced the principle, and what exactly in your code was causing the principle not to be followed.

Question 2

For the following security mechanisms, explain which principle(s) are being enforced. Write a short explanation to justify your answer – do not just name the principle(s).

1. Hardware security module
2. Cuckoo sandbox for malware analysis
3. Access control list in an operating system
4. Image Captcha on Flex
5. Password strength indicator on Google or similar websites when you create an account
6. Biometric authentication required before using banking app
7. The way encryption ciphers like AES were designed (look at the history of AES first)
8. Atomicity in database transactions
9. Intrusion detection systems in front of public facing servers of an organization

Question 3

Explain how the principle of least common mechanism violated or enforced in the following scenarios:

1. Air-gapping of important machines/servers in companies
2. Cloudflare protection for websites
3. The Colonial Pipeline ransomware attack
4. Multi-tenancy in cloud computing (e.g., AWS, Azure, Google Cloud)
5. Shared authentication services (e.g., Single Sign-On using Google or Microsoft accounts)
6. Log4Shell vulnerability in Log4j affecting multiple applications

Section-II Product Ciphers Using Classical Ciphers (50 Points)

Question 4:

Design and implement a product cipher that combines at least one substitution cipher (e.g., Caesar, Vigenère) with a transposition cipher (e.g., Rail Fence, Columnar).

a. Clearly define the encryption and decryption steps.
b. Provide a sample plaintext and show the step-by-step encryption process.
c. Demonstrate how decryption recovers the original plaintext.

Implement your designed product cipher in a programming language of your choice (Python, C++, Java, etc.). Submit the code along with test cases.

Question 5:

Compare the security of your implemented product cipher with individual classical ciphers strength and answer the following:

a. Does your product cipher resist frequency analysis better than a simple substitution cipher?
b. How does the transposition layer impact the security of the ciphertext?
c. What are the potential weaknesses of your product cipher?

Question 6:

Perform a cryptanalysis experiment:

a. Try breaking your product cipher using frequency analysis, brute-force, or known-plaintext attacks.
b. Describe the challenges faced in attacking your cipher compared to attacking a standalone classical cipher.

Provide an analysis of results and security insights.

Submission Guidelines:

1. Submit your work as a single PDF document in Google Classroom.
2. Submit a detailed report (Max 8-10 pages) covering your responses to the questions.
3. The cover page should mention the names and roll numbers of both group members. The maximum length of the document is 8 pages, in Times size 12 font with line spacing = 1.0.
4. Your submission must follow the naming convention as follows: ROLLNUMBER1_ROLLNUMBER2.pdf (e.g. R_i22xxxx_i22xxxx.pdf). Please note that your submission will NOT be considered if the naming convention is not followed.
5. Include source code and screenshots of encryption/decryption output.
6. Late submission is not allowed and will not be considered.
7. If plagiarism is detected, you will be marked zero for this assignment.

Evaluation Rubric:

Each of the assignment questions will be evaluated on the following:

1. Technical correctness, i.e. the principle is applied correctly and correct understanding is demonstrated. (70% weightage)
2. Clarity of explanation – brief and clear explanation of how the principle is being followed/violated. (25% weightage)
3. Following page limit and formatting requirements. (5% weightage).