# SIL765: Networks and System Security

# Semester II, 2023-2024

# Assignment-3

March 22, 2024

## Problem: Message Handling System (100 Marks)

### Background

In this problem, you will perform the security analysis of the IITD email message handling system (MHS). This will be a black-box analysis, i.e., it has to be carried out only by interacting (e.g., sending and receiving emails) with the IITD MHS. You cannot ask IITD CSC folks about its internal working mechanisms. However, you can infer the internal working mechanisms by reading about it or through any tool. For instance, to get help in understanding the IITD MHS, you can refer to the information provided at this link. Considering this assignment, the most useful information is available in the following sentence.

*"In their favorite email clients the users will need to set mailstore.iitd.ac.in as their IMAP server (incoming) and smtp.iitd.ac.in as their SMTP server (outgoing). They will need to set IMAP to use port 993 (SSL) and enable authentication for outgoing mails (SMTP) over TLS (either starttls over port 25, or SSL/TLS over port 465)."*

### Part-1: System Setup (30 Marks)

In this part, you need to write the following scripts.

- `my_sender`: This can be utilized to send an email. For any email, the body/content should be "The OTP for transferring Rs 1,00,000 to your friend's account is 256345." This will utilize your IITD credentials (login and password).
- `my_receiver`: This can be utilized to fetch the most recently received email from your inbox. The fetched data should contain all the headers (specifically those containing information about the utilized security protocols). This will also utilize your IITD credentials (login and password).
- `my_parser`: This can be utilized to extract information about the security protocols employed in a received email.

### Part-2: Security Evaluation (70 Marks)

For this part, send an email to your own inbox using `my_sender`, send another email to your inbox using a Gmail account, retrieve the two emails along with their headers using the `my_receiver` script, and finally execute your `my_parser` script on them. Thereafter, perform the following analysis.

- Basic Analysis (20 Marks): From the `my_sender` and `my_receiver` scripts, what can you tell about the security protocols utilized in the IITD MHS. Discuss their effectiveness against state-of-the-art attacks.

- Advanced Analysis (30 Marks): Discuss the step-by-step methodology to authenticate the DKIM signature in the email. Note that the DKIM signatures are not typically verified by the client. Hence, you may have some missing information in the headers, and you will have to think about how to obtain the missing information.

- Comparative Analysis (20 Marks): Discuss the similarities and differences between the security protocols employed by Gmail and IITD by parsing the received emails. Explain which one handles the security better. Further, you should find out the number of DKIM signatures in the email from IITD server and Gmail. Explain the reason for those differences.

## Submission

- You should submit a single folder that should contain all the files related to this assignment.

- The folder should be named as: ⟨Your Entry Number⟩-assignment-⟨Assignment Number⟩. *Example:* 2020EE10350-assignment-4

- You are free to use any programming language (preferably, C++ or Python).

- Please submit the following files. Each file should be named as specified in the problem.

  - `my_sender:` This should contain the sender's source code.
  - `my_receiver:` This should contain the receiver's source code.
  - `my_parser:` This should contain the source code which can be utilized to analyze the email contents.
  - `readme:` This should be the pdf file containing all the necessary details about your solution. For instance, it should explain the steps to build and execute your code. It should have screenshots of terminals to demonstrate that your code works as desired. It should contain discussions about the analysis conducted by you.