SIL765: Networks and System Security
Semester II, 2020-2021
Assignment-4

April 15, 2021

Submission Instructions

1. You will submit the assignment on Moodle.
2. You can use Piazza for any queries related to the assignment.
3. You should submit a single folder which should contain all the files related to this assignment.
4. The folder should be named as: ⟨Your Entry Number⟩-assignment-⟨Assignment Number⟩.
   Example: 2020EE10350-assignment-4
5. Each file should be named as specified in the problem.
6. You are free to use any programming language (preferably, C++ or Python).
7. Failure to strictly follow the instructions will adversely affect the grades.

Problem: Message Handling System (100 Marks)

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 sending emails and receiving emails using your own IITD email account. For any email, the body/content should be "The OTP for transferring Rs 1,00,000 to your friend's account is 256345."

Part-1 (40 Marks)

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 favourite 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)."

In this part of the assignment, you need to perform the following.

- Scripts (20 Marks): You will write the following two scripts that will utilize your IITD credentials (login and password) to send and receive emails.
  - `my_sender`: This can be utilized to send an email.
  - `my_receiver`: This can be utilized to fetch the first email from your inbox. The fetched data should contain all the headers (specifically those containing information about the utilized security protocols).
- 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 the state-of-the-art attacks.

Part-2 (60 Marks)

In this part, you need to perform the following.

- Send an email to your own inbox using `my_sender`. Send another email to your inbox using a Gmail account. Then, retrieve the two emails along with their headers using the `my_receiver` script.
- Parsing (15 Marks): Write a script, `my_parser`, to extract information about the security protocols employed the email received from IITD server and the one received from Gmail.
- Analysis (15 Marks): Discuss the similarities and the differences between the security protocols employed by Gmail and IITD. Explain which one handles the security better.
- DKIM (15 Marks): You should find out that although there is only one DKIM signature in the email from IITD server, there are multiple DKIM signatures in the email received from Gmail. Explain the reason for those numbers.
- Verification (15 Marks): Discuss the step-by-step methodology to authenticate these DKIM signatures. Note that the DKIM signatures are not typically verified at 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.

Submission

- 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 the screenshots of terminals to demonstrate that your code works as desired. It should contain discussions about the analysis conducted by you.