SIL765: Networks and System Security
Semester II, 2024-2025
Assignment-5

April 10, 2025

Problem-1: Transport Layer security (40 marks)

In this assignment we focus on TLS handshake protocol implemented on the client side.

```python
#!/usr/bin/python3
import socket, ssl, sys, pprint

hostname = sys.argv[1]
port = 443
cadir = '/etc/ssl/certs'

# Set up the TLS context
context = ssl.SSLContext(ssl.PROTOCOL_TLS_CLIENT)
context.load_verify_locations(capath=cadir)
context.verify_mode = ssl.CERT_REQUIRED
context.check_hostname = True

# Create TCP connection
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect((hostname, port))
input("After making TCP connection. Press any key to continue ...")

# Add the TLS
ssock = context.wrap_socket(sock, server_hostname=hostname,
do_handshake_on_connect=False)
ssock.do_handshake() # Start the handshake
pprint.pprint(ssock.getpeercert())
input("After handshake. Press any key to continue ...")

# Close the TLS Connection
ssock.shutdown(socket.SHUT_RDWR)
ssock.close()
```

Task 1 : TLS Handshake

The above client program initiates a TLS handshake with a TLS server (the name of the server needs to be specified as the first command line argument). In this task, you can use this code to communicate with a real HTTPS-based web server and perform the following. Note that some additional code may need to be added to complete the task.

- What is the cipher used between the client and the server?
- Print out the server certificate in the program.
- Explain the purpose of ***/etc/ssl/certs*** certs.
- Use Wireshark to capture the network traffics during the execution of the program, and explain your observation. In particular, explain which step triggers the TCP handshake, and which step triggers the TLS handshake. Explain the relationship between the TLS handshake and the TCP handshake.

Taks-2: CA's Certificate

In the client program, we use the certificates in the **/etc/ssl/certs** folder to verify server's certificates. In this task, you will create your own certificate folder.

- Create a folder called certs, and assign the **cadir** to **./certs**. Run the client program. Since the folder is empty, the program will throw an error. Report your observation and the potential cause.
- Figure out how you can resolve this issue, then run your client program again, report your steps to solve the issue and your observations.

Task-3: Hostname

The objective of this task is to make you understand the importance of hostname checks at the client side. Please conduct the following steps using the client program.

- Get the IP address of the server using the **dig** command.
- Modify the **/etc/hosts** file, add the IP address along with host name to the end of file.

```
    127.0.0.1 anything.com
```

- Switch following line in your client program between **True** and **False**, Describe abd explain your observation in both cases.

```
        context.check_hostname = False
```

Based on the above experiment, explain the importance of hostname check. If the client program does not perform the hostname check, explain the security consequences.

Task-4: Communicating Data

In this task, we will send data to the server and get its response. Since we choose to use HTTPS servers, we need to send HTTP requests to the server; otherwise, the server will not understand our request. The following code example shows how to send HTTP requests and how to read the response.

```python
# Send HTTP Request to Server
request = b"GET / HTTP/1.0\r\nHost: " + \
    hostname.encode('utf-8') + b"\r\n\r\n"
ssock.sendall(request)

# Read HTTP Response from Server
response = ssock.recv(2048)
while response:
    pprint.pprint(response.split(b"\r\n"))
    response = ssock.recv(2048)
```

- Please add the data sending/receiving code to your client program, and report your observation.
- Please modify the HTTP request, so you can fetch an image file of your choice from an HTTPS server.

Submission

- **tls_client.py** : python file containing your client code.
- **Report_part1** : This should be the pdf file containing all the necessary details about your solution. For instance, it should explain the steps to execute your code. It should have the screenshots of terminals to emonstrate that your code works as desired. It should contain discussions about the security and efficiency of the protocol.

1 Problem 2 : Website Security Analysis (60 Marks)

A website is a crucial component of any digital e-commerce business. It can also be simply used as a digital representation of an organization, and a platform where visitors can obtain information about the organization. However, with increasing technology usage, websites have become vulnerable to various cyber threats.In this assignment you will peroform VAPT(Vulnerability assessment and Penetration Testing) to find vulnerabilities on websites of your choice. **Note** - Please do not perform penetration testing on any security-sensitive website as the source of the test can be traced back to you.

Testing Tools You can choose any tool that is avilable online, few examples are :

- **Metasploit** - `https://www.metasploit.com`
- **Nmap** - `https://nmap.org`
- **Burp Suit** - `https://portswigger.net/burp`

Exploring tools other than above mentioned is highly encouraged.

Security evalution and report submission

In this assignment, you need to analyze any popular websites for security vulnerabilities using any two testing tools.

- For each tool explain at least four vulnerabilities you tried to find using the tool. Explain the functionality of the tool, i.e., how the tool tested the vulnerabilities. (10 Marks)
- For at least two critical vulnerabilities tested by each tool, but not found on the website, explain the security measures deployed on the website which mitigate those vulnerabilities. (2 x 2 x 5 =20 Marks)
- For at least two critical vulnerabilities found by each tool on websites, explain how those vulnerabilities can be used to launch attacks and validate that the vulnerabilities can be practically exploited. (2 x 2 x 5 = 20 marks)
- For the discovered vulnerabilities, suggest mitigation techniques that could be deployed by the website. (10 marks)

Submission

- **Report_part2:**This document should be a detailed PDF that includes screenshots of all terminal sessions or tools used throughout the process. It must clearly show the commands executed along with their respective outputs. Each step should be thoroughly explained, providing both the procedure and the underlying rationale.