MiniProject 2: Internet Security Protocols

October 4, 2023

Hand-in

Write a report that summarises your results, the steps you took to achieve the correct result and your source code. Upload the .pdf and a .zip file containing your files to Learnit. You submit in groups.

Assignment 1: Secure Communication

1. Write a client and a server that communicate over a network. Your client should accept the following arguments: message, ip address for server, port for server. Your server should not take any arguments, but should be running at a static port (7007). You can choose the programming language yourself.

2. Next, ensure that the communication between the client and server is confidential and ensure integrity for the messages. You'll need to make a self-signed certificate for this. Perhaps look into TLS and ServerSocket if you are using Java *Assume that no preshared secret exists between the client and server, hence public key cryptography and certificates are needed. DO NOT just access the key in a shared folder*. After implementing this, the following must hold:

   - (Confidentiality) Messages between the server and the client are encrypted and unreadable by third parties, except for any handshake messages and any metadata about the encrypted data (length, fragmentation, etc.).
   - (Integrity) Corruption of messages, or messages originating from a third party, are detectable as being such.

3. Write a short (less than a page) documentation on how your client/server works. If there is any other setup than just compiling, you need to explain how to do this setup. Explain how you achieve confidentiality/integrity and if not, what your challenges were. Submit the code and a .pdf in a zipped archive.

Assignment 2: Man-in-the-Middle

In this part of the miniproject you will be using the virtual machine mallory to eavesdrop (capture) network data sent between the virtual machines alice and bob. Following the instructions below, bob will log in to alice using the remote management tool *telnet* and alice will log in to bobs web shop, all while mallory is eavesdropping on their traffic.

Part A

Alice and Bob are using the telnet protocol to administrate their web shop on https://bob/. Mallory is having a bad day. It's the end of the month, she's out of money and forgot to by that hammer that she needed to hang pictures of cute cats in her new apartment. She decides to try eavesdropping on the communication between Alice and Bob in an effort to alter the prices on the web shop.

1. Launch the three Virtual Machines alice, bob and mallory.
2. Start a sniffer on mallory e.g. wireshark.
3. Connect and log in to bob via telnet from alice using bobs credentials.
4. Once logged in, run the ls command, listing the directories on alice
5. Logout from bob.
6. Stop capturing traffic on mallory and save the capture as capture1.pcap.

Part B

Alice and Bob noticed Mallory's efforts, and took measures to prevent further attacks on telnet. But this doesn't stop Mallory. She is determined to hang her pictures before her parents visit this weekend. Mallory needs that hammer. Perhaps she can eavesdrop another person's access credentials, and use their credit card to pay for her hammer?

1. Start capturing traffic with wireshark on mallory again.
2. Open up a web browser on alice and go to the TLS secure web site http**s**://bob/.
3. In the web shop at https://bob/, log in as alice using the following credentials:

   Username: alice

   Password: alice123
4. Stop capturing traffic on mallory and save the capture as capture2.pcap.

Part C

Mallory does not give up easily, and decides to try a Mallory-in-the-middle attack. The best approach is social engineering, so she visits their physical store, and asks the cashier (Alice) if they have cotton candy mixture. Alice goes to the stockroom to check, which is a perfect opportunity for Mallory to set up her own server as a proxy on Alice's computer.

1. Start SSLKEYLOGFILE=$HOME/mallory/sslkeylogfile.txt mitmproxy --ssl-insecure on mallory.

2. In another terminal on mallory, start capturing traffic with wireshark on again.
3. On alice, set mallory as proxy server.
4. Open up a web browser on alice and go to the TLS secure web site https://bob/.
5. In the web shop at https://bob/, log in as alice using the following credentials:

   Username: alice

   Password: alice123
6. Stop capturing traffic on mallory and save the capture as capture3.pcap.

Report

Analyse your captures in wireshark. Suppose you are the adversary, eavesdropping and tampering on Alices and Bobs connections. Inspect the traffic. What do you learn? Summarise your findings in a brief (10 paragraph max) report. Submit the report as a PDF.