MiniProject I: Internet Security Protocols

September 28, 2018

Deadline: Friday 11. October 2018.

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

Part A

1. Write a client and a server that communicate over a network. Your client should only accept: message, ip address and port for where to send that message as input. Your server should be running at a static port (7007).

2. Next, ensure that the communication between the two programs are confidential and ensure integrity for the messages. You'll likely need to make a self-signed certificate for this exercise. *Assume that no preshared secret exists between the client and server, hence public key cryptography and certificates are needed.*

3. *(Optional)* Make the communication scheme replay-resistant.

Assignment 2: Man-in-the-Middle

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

VM Name	Username	Password
Alice	alice	alice
Bob	bob	bob
Mallory	mallory	mallory

Part A

Alice and Bob are using the telnet protocol to administrate their webshop 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 webshop.

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 `bob`'s credentials.
4. Once logged in, run the `ls` command, listing the directories on `bob`
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 https://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 candyfloss 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 (ip: 192.168.1.3, port: 8080).
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 Mallory, eavesdropping and tampering on Alice's and Bob's connections. Inspect the traffic. What do you learn? Did Mallory get her hammer in the end? Summarise your findings in a brief (10 paragraph max) report. Submit the report as a PDF.