Man in the Middle Threat in Public Wi-fi: Sniffing

Dimas Putra Anugerah

Tutorial H11A

z5520430

COMP6441

Results

1. Packet Sniffer program (Index 0)
   C program that captures network packets and print information regarding it (Source and destination port, payload, etc.). It first takes in 2 parameters: Network device to capture packet on and number of packets to capture. The captured packet's layers will be dissected to obtain the header information and payload itself. It is printed in a JSON format to increase readability and allow other programs to easily consume the data.

2. Man in the Middle Threats in Public Wi-fi Presentation (Index 1)
   A short presentation that provides background on Man in the Middle attacks in public wi-fi usage.

What I Did

My aim of this project was to research into the threat of man in the middle attacks when we use public wi-fi, and to demonstrate one such threat of eavesdropping / sniffing by creating a packet sniffer program in C.

I spent the first week into researching public wi-fi threats and decided to focus on sniffing. I knew about Wireshark but I wanted to understand and implement a custom packet capture program myself. The next weeks were spent on creating the packet sniffer program. I found an online resource that goes over using the libpcap module to capture network packets, and so I studied it thoroughly and slowly implemented the program. The first part was understanding network layers and how packets are structured. After gaining a solid understanding, I started creating the packet structs, trial and erroring obtaining the network parts, and finally creating functions to output information. Once the program is done I summarized my research into a presentation.

Challenges I Faced

There were other courses which had big projects that happens at the same time as this project, which took up a lot more time than I would like to. Feeling I needed more time, I asked for an extension to prevent me from rushing my work. As time went on I realized my project was less exciting than I thought it would be and lost some motivation. Initially I had an idea to create a program that sniffs packets and be able to display the plain network content, device names, and websites involved, but it turns out either is not possible or requires more time than I had. In spite of this, I remind myself that I still can learn a lot from the project such as being more familiar with C programming and reinforcing my network understanding. This is an opportunity to upskill myself and it was what kept me going. Even though learning networking programming is tricky, I feel like it's an important topic to learn and hence why I did it.

Overall, I felt like this project had more potential than what was done. It could have been a lot cooler if I had done more to display the packet information in a meaningful way, such as creating a front-end app to list the network packets or attempt to decode the encrypted payload. I still needed to manage my time better as my other commitments slowed down this project's progress. I also wished I had consulted more because at times I was unsure of what to do or where I'm going with the project, so it would have provided me with better direction. However, I'm still happy I got to gain a deeper understanding on networking concepts and code in C. I'm definitely interested to continue this project afterwards.