SIT327 - Network Forensics

Credit Task 2: WiFi Forensics Analysis

Overview

Task Overview:

In this task we will examine a forensics investigation an attack against wifi. Download the included pcap of the wifi capture. We will use two tools to investigate the pcap, tcpdump and tshark. As discussed in class, frames are transmitted in little endian order. The first byte of the frame contains the version/type/subtype, and the second byte contains flags, including a flag signaling the packet is encrypted. Research the frame format and use this to do a bitwise comparison to determine how many flags are encrypted in the data. Start with the following command.

```
tcpdump -nne -r wlan.pcap 'wlan[0] = X and wlan[1] OP Y = Y'
```

You will need to change X to indicate that this is a data frame, the OP to be the correct bitwise operation, and Y to indicate that this dataframe is an encrypted packet. Pipe the above to a unix command to count the number of encrpyted frames. Compare this to the number of frames transmitted in the clear. Pipe the output to a set of unix commands to count how many IVs we have. Do some research. Do you think this is should be enough IVs to attack WEP? Following this, determine a list of MACs that were transmitted. Which MACs transmitted to who? What was the general timeline of the transmission? What do you think happened?

Report Requirements:

- Detail your command for enumerating encrypted packets. Clarify your expectations regarding the appearance of the first two bytes in a raw encrypted data frame. Compare the tally of encrypted packets against those transmitted in plaintext.
- Provide an analysis of the data transmission, indicating which MAC addresses were involved, and offer a timeline and interpretation of the events.