FIT3031 – Tutorial 6

WIRELESS NETWORK SECURITY

Q1 What is the basic building block of an 802.11 WLAN?

Q2 Define an extended service set.

Q3 Is a Distribution System a Wireless Network?

Q4 What security areas are addressed by IEEE 802.11i?

Q5 What is the difference between TKIP and CCMP?

Q6 What is the difference between an HTML filter and a WAP proxy?

Q7 List and briefly define all of the keys used in WTLS.

Q8 Describe three alternative approaches to providing WAP end-to-end security.

Problems:

1. In IEEE 80211, open system authentication simply consists of two communications. An authentication is requested by the client, which contains the station ID (typically a MAC address). This is followed by an authentication response from the AP/router containing the success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.
   a. What are the benefits of this authentication scheme?
   b. What are the security vulnerabilities of this authentication scheme

2. Watch the video "the WIFI scam" and discuss the implications.
   a. Could the Monash Wireless network be compromised using this technique? If so, what type of information could you hope to gain? If not, could you use social engineering to get the same effect?

b. Could this type of vulnerability be prevented?

You can access this video from a You Tube site:

http://www.youtube.com/watch?v=jV0Q_muo1wI