FIT3031 – Tutorial 6 Solutions

WIRELESS NETWORK SECURITY

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

Ans: The basic building block of an 802.11 WLAN is the Basic Service Set which consists of wireless stations executing the same MAC protocol and competing for access to the same shared wireless medium.

Q2 Define an extended service set.

Ans: Two or more basic service sets interconnected by a distribution system is an extended service set.

Q3 Is a Distribution System a Wireless Network?

Ans: A Distribution System may or may not be. A DS can be a switch, a wired network or a wireless network.

Q4 What security areas are addressed by IEEE 802.11i?

Ans: IEEE 802.11i addresses four main security areas: authentication, key management, data confidentiality & data integrity.

Q5 What is the difference between TKIP and CCMP?

Ans: Both TKIP & CCMP (Counter Mode with Cipher Block Chaining MAC Protocol) protocols provide confidentiality, Data origin Authentication and Integrity and replay protection services for unicast user traffic of Robust Security Network (RSN). TKIP, Temporal Key Integrity Protocol is designed to require only software changes to devices that are implemented with the older wireless LAN security approach called Wired Equivalent Privacy (WEP).

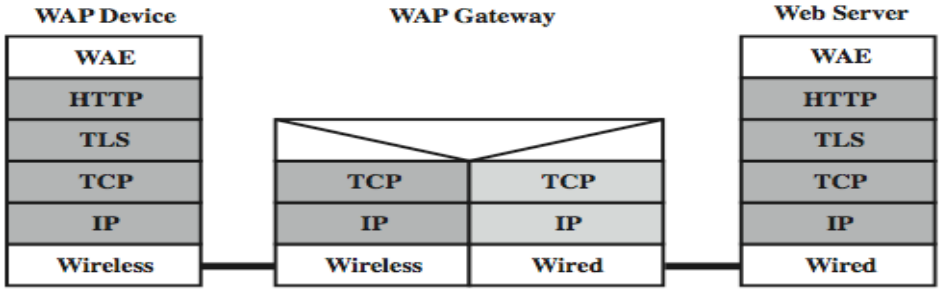
Q6 What is the difference between an HTML filter and a WAP proxy?

Ans: An HTML filter translates the HTML content into WML content. It may or may not be co-located with the WAP proxy. The proxy converts the WML to a more compact form known as binary WML and delivers it to the mobile user over a wireless network using the WAP protocol stack

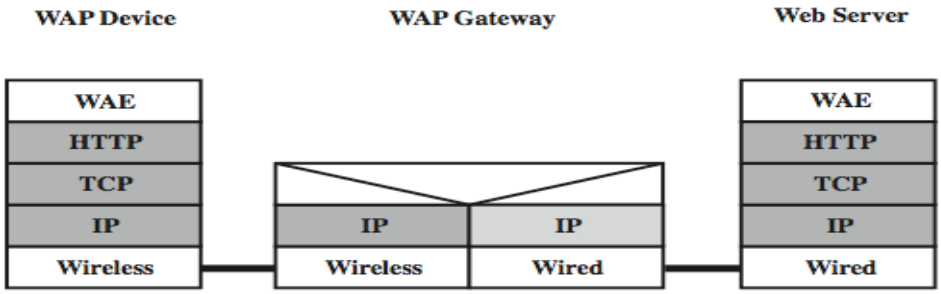
Q7 Describe three alternative approaches to providing WAP end-to- end security.

Ans: The **first** approach (Figure 6.20a) is to make use of TLS between client and server. A secure TLS session is set up between the endpoints. The WAP gateway acts as a TCP-level gateway and splices together two TCP connections to carry the traffic between the endpoints. However, the TCP user data field (TLS records) remains encrypted as it passes through the gateway and so end-to-end security is maintained.

Another possible **second** approach is shown in Figure 6.20b. Here we assume that the WAP gateway acts as a simple Internet router. In this case, end- to-end security can be provided at the IP level using IPsec.



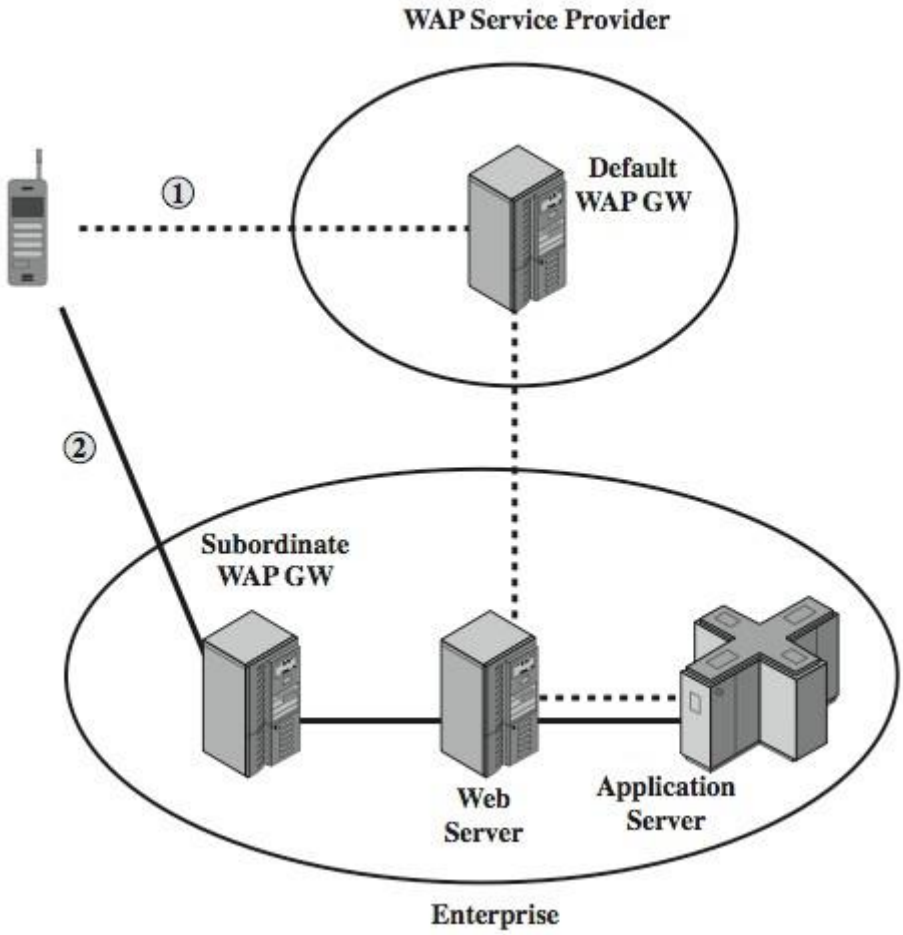
(a) TLS-based security



(b) IPSec-based security

Yet another **third** approach, somewhat more complicated, approach has been defined in more specific terms by the WAP forum in specification entitled "WAP Transport Layer End-to-End Security." This approach is illustrated in Figure 6.21. In this scenario, the WAP client connects to its usual WAP gateway and attempts to send a request through the gateway to a secure domain. The secure content server determines the need for security that requires that the mobile client connect to its local WAP gateway rather than its default WAP gateway. The Web server responds to the initial client request with an HTTP redirect message that redirects the client to a WAP gateway

that is part of the enterprise network. This message passes back through the default gateway, which validates the redirect and sends it to the client. The client caches the redirect information and establishes a secure session with the enterprise WAP gateway using WTLS. After the connection is terminated, the default gateway is reselected and used for subsequent communication to other Web servers. Note that this approach requires that the enterprise maintain a WAP gateway on the wireless network that the client is using.



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?

Ans: This scheme is extremely simple and easy to implement. It does protect against very simple attacks using an off-the-shelf Wi- Fi LAN card, and against accidental connection to the wrong network.

b. What are the security vulnerabilities of this authentication scheme

Ans: This scheme depends on all parties behaving honestly. The scheme does not protect against MAC address forgery.

2. Watch the video “the WIFI scam” and discuss the implications.

You can access this video from a You Tube site:

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

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?

Ans: This is an example of a Rogue AP attack.
First of all the setup of this scam requires either a rogue access point bridged to a wireless 802.16 broadband connection or an ad-hoc network which is working in a peer-to-peer setup. It's possible.The attacker may set a ad hoc network named like 'monash network' in his/her laptop, and his/her laptop has connected to internet (like via legal monash username/passsword to monash network). He/she allows the victims to browse internet via his/her connections. Next step the attacker sets up a fake web page which asks you to input some information like monash user name/password. Then the attacker waits for victims to connect his/her network and enter their details. (In this university scenario, it's not possible to ask victims to enter their personal information about credit card, but in some scenarios like airports and cafes, such information can be considered legitimate. However, the attacker may set up

more false web pages, when he ascertains the users want to purchase something online (e.g. ebay), he/she can transfer the links to the forged pay link to steal their credit card information. But this is a more advanced attack).

b. Could this type of vulnerability be prevented?

Ans: It's hard to prevent this type of vulnerability. The best way is not to connect to such ad hoc networks and never enter private information in free public networks (The attacker may setup a rogue AP by a router rather than just a laptop). The existing techniques like rogue AP detection cannot fully prevent this attack.

There is a useful article about wifi scam http://www.computerworld.com/s/article/9008399/Don_t_fall_victim_to_the_Free_Wi_Fi_scam?taxonomyId=16&pageNumber=1

BTW, wifi is secure only if during authentication phase the IEEE 802.1x, port based network access control protocol is implemented. Small /home WLANs based on only passwords are never secure, any other legal users in such a WLAN may reveal your information because such WLANs are based on symmetric ciphers.

Comment: *The problem is an open problem and is meant to stimulate a debate on WIFI networks that require web based authentication.Are they safe, can you make them safe? The video discusses some solutions, but are these really solutions?*