**Module 6 Cryptography & PKI**

**6.3 Wi-Fi Security**

**Wireless Access Methods**

* Open Authentication

1. Only need to know network name/SSID
2. Captive portal – web page that is launched 1st when connecting through network

* Shared Authentication

1. Client & wireless access point must negotiate & share key prior to initiating communications
2. Pre-shared key (PSK) – each user uses same key to connect to Wi-Fi network

* Enterprise

1. Server handles distribution of cryptographic keys &/or digital certificates
2. Extensible Authentication Protocol (EAP)

**Wi-Fi Protected Setup (WPS)**

* Standard to simplify Wireless Access Point (WAP) set-up for home users
* 3 modes

1. PIN entry
2. Push-Button Configuration (PBC)
3. Near Field Communication (NFC)

**Wireless Cryptographic Protocols**

* Wired Equivalent Privacy (WEP) – original wireless encryption standard that shouldn’t be used today
* Wi-Fi Protected Access (WPA) – developed in response to security concerns over WEP
* Wi-Fi protected Access Version 2 (WPA2)

1. Required for Wi-Fi certified devices
2. Uses AES for encryption
3. Based on IEEE 802.11i standard

**Wi-Fi Protected Access (WPA)**

* WPA-Personal (WPA-PSK) – uses pre-shared key to authenticate & validate users on wireless LAN (WLAN)/Wi-Fi connection
* WPA-Enterprise (WPA-802.1X)

1. Increased security for larger organisations
2. Requires RADIUS authentication server

* Temporal Key Integrity Protocol (TKIP)

1. Based on RC4
2. Uses unique key with each packet
3. Considered depreciated

**Wi-Fi Protected Access 2 (WPA2)**

* Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

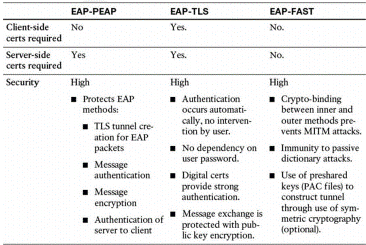
1. Replaced TKIP
2. Based on AES encryption cipher
3. Combines CTR for confidentiality & CBC-MAC for authentication & integrity

* Fully implements IEEE 802.11i-2004 Wi-Fi security standards

**Authentication Protocols – EAP (Extensible Authentication Protocol)**

* Requires authentication server
* Allows authentication methods beyond username/passwords
* Provides support for public certificates
* 4 modes

1. PEAP – Protected EAP
2. EAP-TLS – EAP-Transport Layer Security
3. EAP-TTLS – EAP Tunnelled Transport Layer Security
4. EAP-FAST – EAP Flexible Authentication via Secure Tunnelling



**Authentication Protocols**

* IEEE 802.1x – IEEE standard for port-based network access control
* RADIUS Federation

1. Using RADIUS to authenticate between entities
2. As part of PEAP negotiation, client establishes TLS session with RADIUS server
3. Client authenticates with RADIUS server