Security +
Wireless Access

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

Mobile Connection Standards

Cellular
- Group of protocols such as GSM, 3G, LTE, 4G, 5G
- Ranging from 800Mhz - 2600MHz

Wi-Fi
- The 802.11 protocol group
- 2.4GHz - 5GHz spectrum

SATCOM
- Frequency ranges of 1Ghz to 300Ghz
- Latency is the delay that happens in data communication
- Latency is the key concern when satellite WAN links are used
- Weather effects, such as rain fade, are another factor in satellite links

Bluetooth
- 2.4–2.5 GHz and 2.1 Mbit/s (normal) - 1 Mbit/s (BT low power)
- 100m (normal) and 50m (low power) max range

NFC - Near Field Communication
- Frequency range of 13.56 MHz
- About 20m maximum
- 424 kbit/s transfer rate

RFID
- 120–150 kHz (LF) 13.56 MHz (HF)
- Ranges of 10cm (LF) - 1m (HF)
- Used in supply-chain tracking, item-scanning, health-care, and passports

ANT / ANT+ Adaptive Network Technology
- Low speed, low power radio network technology (less than WIFI or Bluetooth)
- ANT is encrypted with AES
- Developed by Garmin

Infrared
- 850–900 nm wavelength
- Potential transfer rate range of 2.4 kbit/s to 1 Gbit/s

WiFi General Terms

USB tethering
- Connecting a mobile device into a computer with internet connectivity via USB and sharing the internet connection to other mobile devices via WiFi

Tethering / Phone as model (PAM)
- Sharing a devices internet connection to other mobile devices via WiFi

Wi-Fi Direct
- A direct ad-hoc WiFi network between devices

Beacon frames
- Broadcasts the presence of an AP
- Beacon frames are transmitted periodically, they serve to announce the presence of a wireless LAN and to synchronize the members of the service set
- Beacon frames are transmitted by the access point (AP) in an infrastructure basic service set (BSS)

Omnidirectional
- Broadcasts in all directions

Unidirectional
- Broadcasts in one directional

Antenna Power
- More power to the antenna will increase signal strength and increase the broadcast range

SIM Subscriber Identification Module
- Identifies which countries and networks the phone can use

SSID Service Set Identifier
- Text string which identifies the wireless network
- Can be broadcast or not broadcast
- Even if the AP is configured to hide the SSID, it can be sniffed from probe requests between trusted devices and the AP
- Attackers can disrupt the connection and then use a wireless protocol analyzer to listen for the probe response

Wireless Survey / Stumbler
- Tool that will see all wireless networks and grabs critical information such as GPS location
- WAP MAC address, detailed encrypted type, WPS enabled, etc

Fat AP (stand-alone, intelligent, autonomous AP)
- Includes all components to connect users to wireless network, routing NAT,

DHCP

Thin AP (controller based AP)

- Managed by a controller software that it connects with, must be connected to a router in order to communicate with an Internet protocol / modem

Wifi Band Selection

- 2 primary bands (2.4 GhZ and 5GhZ)
  - 802.11b - 2.4GHz - 22MHz
  - 802.11g - 2.4GHz - 20MHz
  - 802.11n - 2.4GHz and 5GHz - 20MHz and 40 MHz
  - 802.11ac - 5GHz - 22MHz - 20MHz, 40MHz, 80MHz, 160MHz

Mac Filtering

- Restricts devices that are allowed to connect to a whitelist of MAC addresses
- Not really effective since allowed MAC's can be intercepted / observed and used to attempt to connect

Wireless Architectural Zones

- **Wireless**
  - Can provide full network access
- **Guest Access / Guest Zone**
  - Provides internet / resource access to anyone who joins the network
- **Ad hoc**
  - Direct connections between devices such as hot-spot or laptops connecting via wireless antennal chipsets

Standards of Wifi Connection

WAP Wireless application protocol

- A technical markup standard for mobile devices
- **WAP** enhances **wireless** specification interoperability and facilitates instant connectivity between interactive **wireless** devices (such as **mobile** phones) and the Internet
- Most modern handset internet browsers now fully support HTML so they do not need to use WAP markup for web page compatibility

Open Wifi / Public hotspot

- Open wifi (not using a password) does not add an encryption layer between the AP and the devices, so communication is only protected by SSL/TLS, or any other application layer encryption
- Public Wireless internet leaves your communications open to a couple different threats like Man-In-The-Middle and sniffing attacks

WEP Wired Equivalent Privacy

- Insecure

- Uses a stream cipher based on RC4
- Improved to use **MIC Message Integrity Check** for integrity hashes that protect the header as well as the payload
- Can use TKIP to improve RC4 security

WPA and WPA2
- Replaced WEP as a newer standard
- Uses a stream cipher based on RC4
- Can use TKIP to improve RC4 security
- Susceptible to password attacks and disassociation attacks
- Uses MIC for integrity hashes
- **WPA-PSK Pre-Shared Key Mode**
  - Encryption is based on the IEEE 802.11i technology standard for data encryption
- **WPA2 (802.11i)**
  - WP2 can use CCMP (counter mode with cipher block chaining message authentication code protocol) which is provides the best security
  - WPA2 uses a block cipher not a stream cipher
  - Significant security improvement over WPA
- **WPA2 Enterprise**
  - Requires an authentication server and provides a PKI for better security

WPS WI-fi Protected Setup
- Uses a **PIN number** instead of a password
- Susceptible to **WPS PIN brute force**
- AP handles the first 4 and next 3 digits separately which limits the possibilities to 10,000 for the first 4 digits
- PIN is easily brute-forced

TKIP Temporal Key Integrity Protocol
- TKIP is **insecure**
- An older encryption protocol used with **WPA** and **WPA2**
- Not recommended by IEEE due to security issues
- Later an **AES** implementation for WPA and WPA2 (CCMP) provided an improved encryption standard to replace TKIP

CCMP Counter Mode with Cipher Message Authentication Code Protocol
- A newer encryption protocol used with WPA2
- Recommended by IEEE

PSK Pre-shared Key mode
- Users access the wireless network anonymously with a PSK or passphrase
- This provides authorization without identification
- The max pre-shared key (password) length is 63 characters

Enterprise Mode
- Forces users to authenticate with unique credentials using **802.1x** protocol
- Enterprise mode often uses RADIUS server

- **802.1x** can use certificates in the authentication process

RADIUS with Enterprise Mode
- Need to configure the IP address assigned to the RADIUS 802.1x server
- Need to configure RADIUS port 1812
- The pre-shared key (password)
- **802.1x** authentication reduces likeliness of successful access attack

Wireless Authentication Protocols
- List of common wireless authentication protocols
- **EAP Extensible Authentication Protocol**
  - RFC 5247
  - Is a group of wireless authentication protocols configured for several different network authentication protocols such as **Kerberos**, **MS-CHAP**, **RADIUS**, **SAML**, etc.
  - Authentication is manged by a **Network Access Server (NAS)**
  - **Lightweight EAP (LEAP)**
    - Proprietary to **Cisco**
    - Based on **MS-CHAP** and therefore has security problems
    - Only passwords are required
    - No certificates
  - **Protected EAP (PEAP)**
    - Created by Cisco, RSA Security, and Microsoft
    - Uses **TLS encryption** tunnel for data-in-transit
    - Certificate on the server for encryption
  - **EAP Flexible Authentication vis Secure Tunnelling (EAP-FAST)**
    - Supports digital certificates but they are optional
  - **EAP-Tunnelled TLS (EAP-TTLS)**
    - RFC 5281
    - Require X.509 certificates on the sever
    - The client does not require X.509 certificate to authenticate to the server
  - **EAP-TLS**
    - RFC 5216
    - Requires X.509 certificates on both server and clients
  - **EAP-Password EAP-PWD**
    - RFC 5931
    - Uses a shared password for authentication
    - The underlying key exchange is resistant to active attack, passive attack, and dictionary attack
  - **RADIUS Federation**

Captive Portals
- Require uses to or complete another specific process before giving internet / network access
- Free Internet Access - EULA or AUP
- Paid Internet Access - add credit card information and contract agreements
- Alternative to IEEE 802.1x for identification and authentication

MDM Mobile Device Management

Ensures devices are up-to-date with patches, etc before allowing connections

Application management
- Can whitelist and blacklist applications

Device Identification
- Can assign a unique ID to devices to allow mangement

Full device encryption
- Ensure confidentiality of data if device is lost, stolen, or breached

Storage segmentation
- Can isolate data to apply different policies to different classes of data

Content management
- Can separate data to different storage segments based on the classification of the data

Containerization
- Isolates a mobile application to a container
- Useful when using a BYOD mobile device policy

Passwords and PINS
- Provide authentication for applications

Biometrics
- Provides 3rd factor authentication

Screen locks
- Can limit access to the phone if lost or stolen

Remote wipe
- Ability to wipe the data from a lost or stolen device

Geolocation
- Can report the physical location of the device, locate lost devices, etc.

Geofencing
- Can limit services to within a specific physical location

GPS tagging
- Can tag photos and videos with GPS location

Context Aware Authentication
- Combines elements when authenticating a user

Push notification services

- Notify mobile users of compliance with policy requirements, etc.

Mobile Device Enforcement and Monitoring

- Monitor device for security compliance and
- block access if unhealthy (NAC)

Unauthorized software

- **Third party app stores**
- **Jail-braking** removing security features from the device OS. The device an be transferred to another mobile provider out of contract, or 3rd party applications can be installed
  - **Rooting** giving the user root level access to an Android device OS
  - **Side-loading** directly copy the application to the device and install
  - **OTA over the air** updates are available OTA
  - **Carrier unlocking** device an be transferred to another mobile provider
  - **USB-OTG (on the go)** devices can act as hosts and allow USB thumb-drives to be plugged into them

Additional Security Concerns related to Mobile Devices

- Mobile devices can also:
  - Record or stream video
  - Take pictures
  - Record or stream audio