CMSC 426
Principles of Computer Security

Wireless Hacking and Security

Last Class We Covered

- Important info you need to know
  - Cookies
  - HTML
  - GET and POST
  - JavaScript
- Cross-Site Scripting
- SQL Injection

Any Questions from Last Time?

Today's Topics

- 802.11 Standard
  - Basic information
  - Sessions and security

- Wireless Hacking

802.11 Standard

802.11 Standard

- Specification for how WLANs are implemented
  - Wireless Local Area Networks
- Provides the basis for Wi-Fi technology

- Standard put out by IEEE
  - 802 covers anything dealing with area networks (local or metro)
  - 11 is specifically for WLANs
  - Multiple amendments have been released, including a, b, g, and n

Information from Hacking Exposed 7 (McClure, Scambray, Kurtz)

802.11 Frequencies and Channels

- 802.11 operates within the radio spectrum, specifically the industrial, scientific, and medical (ISM) radio bands
  - Can operate in 2.4-GHz or 5-GHz ISM bands

- Each spectrum is divided up into channels
  - 2.4-GHz is channels 1-14, which overlap slightly with their neighbors
    - Overlapping can cause interference, but 1, 6 and 11 are non-overlapping
  - 5-GHz is channels 36-165 (in the US) and they don't overlap

Information from Hacking Exposed 7 (McClure, Scambray, Kurtz)

Wireless Access Point

- Hardware device that allows a Wi-Fi device to connect to a wired network
  - Connected directly to a WLAN, typically Ethernet
  - Access point provides wireless connections so that other devices may use the wired network
  - Multiple wireless devices can connect thru a single wired connection

- Networks with access points are referred to as ***infrastructure***, while those that are peer-to-peer are called ***ad hoc***
  - We'll be focusing on infrastructure networks

Service Set Identifier

- Also known as SSID
- The network's "name," often set by the network admin
  - UMBC has eduroam, UMBC Campus, and UMBC Visitor
- Possible to have two networks with the same SSID within the same broadcasting range
  - Some devices try to connect to the one with the stronger signal
  - Some devices try to connect to the first one they see

802.11 Sessions and Security

Establishing an 802.11 Session

- Before establishing a connection, client must identify if a wireless network is actually present
  - Sends out a ***probe request*** asking the network to identify itself
  - Uses SSID, and broadcasts on each channel it supports
  - If present, access point (AP) responds with a ***probe response***

- Next, client sends out an ***authentication request***
  - Separate from any security measures or encryption
  - Most APs are configured to accept any connection, and will only reject the connection when incorrectly encrypted data comes through

Information from Hacking Exposed 7 (McClure, Scambray, Kurtz)

Establishing an 802.11 Session (Continued)

- Final step is an ***association request***, sent by the client
  - Begins the record-keeping process of association
- AP sends out an ***association response***
  - Indicates that the AP is keeping track of the wireless client
- At this point, client *should* be able to communicate with AP
  - Depending on the level of security, may require further steps

Information from Hacking Exposed 7 (McClure, Scambray, Kurtz)

802.11 Security Mechanisms

- MAC filtering
  - Some APs will deny a client connection if their MAC address does not match an address in a preconfigured list
- "Hidden" wireless networks
  - APs send out ***beacon*** announcements with info on connecting
  - Beacon may be configured so that SSID is omitted
    - Client cannot join the network without knowing the SSID
- Ignoring broadcast probe requests
  - Clients can discover nearby wireless network through a broadcast probe request, without knowing the SSID; simply ignore these

Information from Hacking Exposed 7 (McClure, Scambray, Kurtz)

Security Protocols

- WEP (Wired Equivalency Privacy)
  - Uses RC4, a stream cipher
  - 40-bit encryption key, 24-bit initialization vector
    - Really small size, makes it easy to crack!
- WPA (Wi-Fi Protected Access)
  - Interim standard released because WEP was so flawed
  - Also uses RC4, but with a 256-bit key, and a 48-bit IV
  - Adopted TKIP (Temporal Key Integrity Protocol) to increase security
    - Generates a new 128-bit key for each packet

Information from https://searchnetworking.techtarget.com/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

Security Protocols (Continued)

- WPA2 (Wi-Fi Protected Access 2)
  - Current standard
- Uses AES-CCMP instead of TKIP
  - TKIP was designed to not have additional hardware requirements
  - AES: Advanced Encryption Standard
  - CCMP: Counter Mode Cipher Block Chaining Message Authentication Code Protocol
    - CCMP allows only authorized network users to receive data, and uses cipher block chaining MAC to ensure message integrity
  - WPA2 can also use TKIP as a fallback if CCMP isn't supported

Information from https://searchnetworking.techtarget.com/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

Wireless Hacking

Wireless Hacking: aircrack-ng suite

- Software suite of tools to assess Wi-Fi network security
  - Contains WEP and WPA crackers
  - Allows monitoring and capture of transmitted packets
  - Can be used to perform attacks
    - Replay, de-authentication, fake access points, packet injection, etc.

- Available on the Kali Linux VM!

Information from https://en.wikipedia.org/wiki/Aircrack-ng and https://www.aircrack-ng.org/

Wireless Hacking: Sniffing Traffic

- Many networks are unencrypted at the 802.11 layer
  - Makes it trivially easy to “sniff” transmitted packets, listening in
  - Note: depending on local laws, this may be straight-up illegal
- Wireshark is a packet analysis tool for live or captured data
- Simplest defense is to enable an 802.11 layer encryption
  - If that’s not possible, higher level encryption can also be used

Information from Hacking Exposed 7 (McClure, Scambray, Kurtz)

Wireless Hacking: De-Auth. Attacks

- Spoofs de-authentication frames from the client to the AP and vice versa to force a disconnect
  - May send multiple frames, as some clients try to reconnect immediately
- Can use the aireplay-ng tool (within aircrack-ng) to perform this
  - Sends out 128 frames (64 to client, 64 to AP) for every deauth
- Difficult to thwart without going outside the 802.11 standards
  - As a solution, some drivers will disconnect and quickly try to reconnect elsewhere when they see a de-auth frame, but this can be countered

Information from Hacking Exposed 7 (McClure, Scambray, Kurtz)

Wireless Hacking: WEP Cracking

- Good demonstration and explanation:

- https://youtu.be/RydsjNhUjdg

Information from Hacking Exposed 7 (McClure, Scambray, Kurtz)

Wireless Hacking: Wardriving

- Driving around, using a laptop or smartphone to search for Wi-Fi wireless networks
  - Can be used to map out the location of networks
  - Seattle was mapped by 100 undergrads in 2004, who found 5200 access points, including one called “Open to share, no porn please”
  - There’s also warbiking and warcycling, but it’s not as cool sounding
- Wardriving is technically legal, although when Google admitted to doing it with the StreetView vans, people weren’t happy
  - It’s okay – they just use your Android mobile device to do it now

Information from https://en.wikipedia.org/wiki/Wardriving

Wireless Hacking: Wi-Fi Pineapples

- https://youtu.be/I4f47q7fNZk

Image Sources

- Wireless access point:
  - https://en.wikipedia.org/wiki/File:Cisco_Aironet_1131AG_-_Close.jpg