Hands-on Session: Simple Attacks on Wi-Fi Networks

Group Size: 3

Task-1: DoS attacks on a victim's Wi-Fi STA

S1: Configure one STA (laptop or smartphone) as a client and connect it to IITH-Guest Wi-Fi AP

S2: Sniff traffic between STA and IITH-Guest Wi-Fi AP using a Wi-Fi sniffer (configure another laptop in monitor mode to listen to packets exchanged between STA and AP by using airmon-ng and airodump-ng tools. You can also use wireshark/tcpdump with appropriate filters on the sniffer laptop to observe the traffic once you keep Wi-Fi radio of the sniffer laptop in monitor mode using airmon-ng or iw command)

S3: Use aireplay-ng to launch DoS attacks on the victim (STA) e.g., by injecting fake DEAUTH messages towards the victim STA

S4. Repeat S2 to observe that the DoS attack is indeed successful.

Deliverables: Detailed steps followed to complete S1-S4 and screenshots of key observations/activities and pcap.

References:

1. https://sandilands.info/sgordon/teaching/its332y14s2/
2. https://wireless.wiki.kernel.org/en/users/documentation/iw
3. https://www.aircrack-ng.org/doku.php

Task-2: Snoop into HTTP traffic of a victim Wi-Fi STA

S1: Same as S1 of Task-1

S2: Same as S2 of Task-1 except that the victim STA visits example.com over http. So, no encryption of application traffic by TLS, but we have link level encryption as IITH-Guest is a protected Wi-Fi network. Save the sniffed traffic between victim STA and example.com as a pcap file.

S3: Open this pcap in wireshark to check whether you could see any HTTP traffic between victim STA and example.com

S4. Open wireshark again and key in IITH-Guest password (refer to https://wiki.wireshark.org/HowToDecrypt802.11) for decrypting the pcap file. Now check for presence of any HTTP traffic due to automatic decryption of link-level encrypted L2 packets.

Deliverables: Detailed steps followed to complete S1-S4 and screenshots of key observations/activities and pcap.

Task-3: MITM attacks on a Wi-Fi Network

S1: Implement one of the four MITM attacks on Wi-Fi networks; a) MITM by creating an open Wi-Fi network, b) MITM by creating an evil twin hotspot (rogue AP) on a genuine Wi-Fi network, c) Multi-channel MITM by creating an evil twin hotspot (rogue AP) on a genuine Wi-Fi network, and d) MITM by ARP poisoning of two clients (Alice and Bob) on a genuine Wi-Fi network

S2: Let the victim client visit example.com over http and show that MITM attacker observes (passive attacker) into http traffic between the victim and remote webserver.

S3: Active MITM attacker: Show how MITM attacker could modify HTTP responses from example.com by injecting custom HTML code or javascript.

Deliverables: Detailed steps followed to complete S1-S3 and screenshots of key observations/activities and pcap.

References:

- https://thecybersecurityman.com/2018/08/11/creating-an-evil-twin-or-fake-access-point-using-aircrack-ng-and-dnsmasq-part-2-the-attack/
- https://anooppoommen.medium.com/create-a-wifi-hotspot-on-linux-29349b9c582d
- https://witestlab.poly.edu/blog/conduct-a-simple-man-in-the-middle-attack-on-a-wifi-hotspot/
- https://askubuntu.com/questions/318973/how-do-i-create-a-wifi-hotspot-sharing-wireless-internet-connection-single-adap/324785#324785
- https://wiki.archlinux.org/title/software_access_point#Wireless_client_and_software_AP_with_a_single_Wi-Fi_device
- https://w1.fi/hostapd/
- https://wiki.archlinux.org/title/Network_configuration/Wireless
- https://www.howtogeek.com/214080/how-to-turn-your-windows-pc-into-a-wi-fi-hotspot/