

Department of Computer Science

CSE 4820: Wireless and Mobile Security

5. WiFi Enumeration

Dr. Abdullah Aydeger

Location: Harris Inst # 310

Email: aaydeger@fit.edu

Outline

802.11 Enumeration

WiFi Sniffer

- A specific type of network analyzer or packet sniffer that is designed to work with wireless networks
- WiFi sniffing can be accomplished with a dedicated piece of electronic equipment or a software application
- Wireless network sniffing is akin to wiretapping a phone line, only without the court order that legalizes the activity

WiFi Sniffer

- There are valid and legal uses for a wireless sniffer tool to be used
 - An example is where a network administrator makes use of one to secure or monitor their network
 - E.g., home users may employ a sniffer to better understand how their network operates
- Unfortunately, a prime reason that WiFi sniffers are used by unscrupulous individuals is to attempt to collect information from, or gain access to, an unsecured network
 - A wireless sniffer allows someone to attack your network from a distance, making it hard to determine if there are attempts to compromise your data

How does WiFi Sniffer Work?

- WiFi sniffers come in two flavors: hardware and software
- They perform the same tasks, though the software route may be more popular in most cases
- You can obtain software WiFi sniffers for Windows, Mac, and mobile operating systems
- In the case of a mobile device, you are in essence turning it into a hardware sniffer when using it with a sniffing application

Hardware WiFi Sniffers

- No need any special level of technical expertise to operate a hardware WiFi sniffer
 - Most devices are small and portable, able to easily fit in your pocket or laptop bag
- You will be alerted by display lights when a wireless network is found within range of your device
- A WiFi sniffer for Android devices uses add-on tools and will offer a similar display when searching for networks
 - Will be able to detect a wireless signal in spite of interference from Bluetooth devices, microwaves or cell phones

Software WiFi Sniffers

- You can download these tools for just about any operating system
 - Some of these tools have advanced features that allow you to do more than just locate the nearest wireless network
- Tools such as Wireshark and Network Miner serve as WiFi sniffers for the Windows platform
- Users can download tools such as aircrack-ng or Zanti to perform WiFi sniffing on an Android device (or Linux/MAC)

KisMAC

- OS X passive scanner
- Has support for GPS
- Outdated

NetSpot

- NetSpot collects every detail about surrounding Wi-Fi networks and presents wireless data as an interactive table
- It lets you troubleshoot and improve your network's coverage, capacity, performance, APs configurations, signal level, interference, noise, etc.
 - Locate your busiest and least occupied channels

NetSpot Example Capture:

DISCOVER

SURVEY

EXPORT








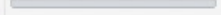
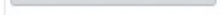
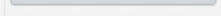
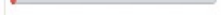
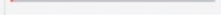
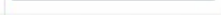
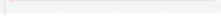



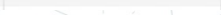
USER GUIDE

ASK A QUESTION

UPGRADE NOW

SSID	BSSID	Alias	Channel	Band	Security	Vendor	Mode	Level (SNR)	Signal	Signa...	Avg	Max	Min	Noise	Noi...	Last seen
<input type="checkbox"/> ATTFHV8Cwa	02:30:44:21:5C:8F		6	2.4GHz	WPA2 Personal	02:30:44	b/g/n		-	0%	-91	-84	-94	-	0%	1min 13s ago
<input type="checkbox"/> ExpressPress#2	02:30:44:21:5C:...		6	2.4GHz	WPA2 Personal	02:30:44	b/g/n		-92	8%	-91	-82	-94	-94	6%	now
<input type="checkbox"/> BLINK-4SFM	AC:CC:FC:AF:76:...		6	2.4GHz	Open	AC:CC:FC	b/g/n		-	0%	-47	-24	-65	-	0%	7h 2min 48s...
<input type="checkbox"/> MySpectrumWiFiE4-2G	98:F7:81:B8:C7:E5		6	2.4GHz	WPA2 Personal	ARRIS	ac		-	0%	-82	-75	-85	-	0%	59s ago
<input type="checkbox"/> Poncho	E4:F7:5B:13:FC:20		1	2.4GHz	WPA2 Personal	ARRIS	b/g/n		-	0%	-91	-91	-93	-	0%	6h 50min 11...
<input type="checkbox"/> Drasha33	2C:00:AB:40:2D:...		6	2.4GHz	WPA2 Personal	ARRIS	b/g/n		-	0%	-92	-89	-94	-	0%	59s ago
<input type="checkbox"/> MySpectrumWiFi3A-2G	84:BB:69:CC:B...		6	2.4GHz	WPA2 Personal	ARRIS	ac		-94	6%	-92	-90	-94	-94	6%	now
<input type="checkbox"/> The_Travers	10:93:97:19:D4:70		1	2.4GHz	WPA2 Personal	ARRIS	b/g/n		-	0%	-92	-91	-93	-	0%	6h 47min 48...
<input type="checkbox"/> ATTFHV8Cwa	B0:DA:F9:7B:8...		1	2.4GHz	WPA2 Personal	ARRIS	b/g/n		-92	8%	-89	-87	-93	-94	6%	now
<input type="checkbox"/> ATTQH4bXys_2.4	FC:AE:34:A4:4F:...		1	2.4GHz	WPA2 Personal	ARRIS	b/g/n		-	0%	-93	-93	-93	-	0%	7h 3min 6s...
<input type="checkbox"/> chittum2014	AC:B3:13:A7:C8:10		1	2.4GHz	WPA2 Personal	ARRIS	b/g/n		-	0%	-93	-92	-95	-	0%	1min 27s ago
<input type="checkbox"/> MySpectrumWiFi73-2G	7C:DB:98:E7:F5...		11,-1	2.4GHz	WPA2 Personal	ASKEY	ac		-73	27%	-72	-58	-75	-93	7%	now
<input type="checkbox"/> MySpectrumWiFi73-5G	7C:DB:98:E7:F5...		161	5GHz	WPA2 Personal	ASKEY	ac		-79	21%	-77	-71	-81	-94	6%	now
<input type="checkbox"/> SpectrumSetup-55	F4:69:42:8A:C7:53		11,-1	2.4GHz	WPA2 Personal	ASKEY	ac		-	0%	-89	-88	-90	-	0%	6h 47min 49...
<input type="checkbox"/> Amandas network	F4:69:42:25:BD:45		6,+1	2.4GHz	WPA2 Personal	ASKEY	ac		-	0%	-91	-89	-91	-	0%	6h 48min 3...
<input type="checkbox"/> BLINK-76VS	4C:53:FD:37:EA:78		6	2.4GHz	Open	Amazon	b/g/n		-	0%	-63	-63	-63	-	0%	7h 4min 43s...
<input type="checkbox"/> NTGR_VMB_9395471872	A4:11:62:4B:E3:66		8	2.4GHz	WPA2 Personal	Arlo	b/g/n		-	0%	-92	-86	-93	-	0%	6h 51min 7s...
<input type="checkbox"/> SpectrumSetup-07	88:DE:7C:C5:85:...		6	2.4GHz	WPA2 Personal	Askey	ax		-	0%	-88	-86	-91	-	0%	46s ago
<input type="checkbox"/> myBuick	BA:9F:09:44:20:...		1	2.4GHz	WPA2 Personal	BA:9F:09	g/n		-	0%	-85	-85	-85	-	0%	6h 48min 3...
<input type="checkbox"/> Hotspot7918	00:54:AF:52:79:18		8	2.4GHz	WPA/WPA2 Personal	Continental	b/g/n		-	0%	-82	-77	-88	-	0%	7h 12s ago
<input type="checkbox"/> Hotspot5631	00:54:AF:7B:56:31		4	2.4GHz	WPA/WPA2 Personal	Continental	b/g/n		-	0%	-93	-93	-93	-	0%	7h 18min 12...
<input type="checkbox"/> Hotspot2026	00:54:AF:72:20:26		7	2.4GHz	WPA/WPA2 Personal	Continental	b/g/n		-	0%	-82	-82	-82	-	0%	7h 2min 34s...

NetSpot Example Capture:

<input type="checkbox"/> Caballete0071	EA:9F:80:21:D4:60	8	2.4GHz	WPA2/WPA3 Personal	EA:9F:80	ax		-	0%	-93	-93	-93	-	0%	7h 41min 8s...
<input type="checkbox"/> 919 wifi	CC:F4:11:77:6D...	11	2.4GHz	WPA2 Personal	Google	b/g/n		-87	13%	-86	-80	-91	-94	6%	now
<input type="checkbox"/> 919 wifi	CC:F4:11:8F:09...	1	2.4GHz	WPA2 Personal	Google	b/g/n		-91	9%	-89	-80	-91	-93	7%	now
<input type="checkbox"/> 919 wifi	B0:E4:D5:0A:3...	1	2.4GHz	WPA2 Personal	Google	b/g/n		-86	14%	-81	-70	-87	-94	6%	now
<input type="checkbox"/> 919 wifi	CC:F4:11:8F:09:DD	149	5GHz	WPA2 Personal	Google	ac		-	0%	-92	-91	-94	-	0%	19min 23s a...
<input type="checkbox"/> Private Access V3	94:A6:7E:43:C6:7B	7	2.4GHz	WPA2 Personal	NETGEAR	ax		-	0%	-90	-85	-93	-	0%	14s ago
<input type="checkbox"/> Private Access V3	3C:37:86:C8:0...	7	2.4GHz	WPA2 Personal	NETGEAR	ax		-87	13%	-89	-84	-92	-94	6%	now
<input type="checkbox"/> ATTfHV8Cwa_2GEXT	94:A6:7E:2D:F0:41	1	2.4GHz	WPA2 Personal	NETGEAR	b/g/n		-	0%	-92	-91	-92	-	0%	6h 55min 51...
<input type="checkbox"/> NETGEAR93	14:59:C0:C1:19:BD	2	2.4GHz	WPA2 Personal	NETGEAR	ac		-	0%	-92	-92	-92	-	0%	7h 41min 50...
<input type="checkbox"/> SpectrumSetup-FE	4C:19:5D:3C:86:...	6	2.4GHz	WPA2 Personal	Sagemcom	ax		-	0%	-82	-76	-90	-	0%	14s ago
<input type="checkbox"/> SpectrumSetup-FE	4C:19:5D:3C:8...	44	5GHz	WPA2 Personal	Sagemcom	ax		-89	11%	-88	-84	-91	-91	9%	now
<input type="checkbox"/> SpectrumSetup-90	4C:19:5D:0E:97...	6	2.4GHz	WPA2 Personal	Sagemcom	ax		-92	8%	-91	-90	-94	-93	7%	now
<input type="checkbox"/> SpectrumSetup-A3	58:2F:F7:EE:93:A9	6	2.4GHz	WPA2 Personal	Sagemcom	ax		-	0%	-92	-90	-93	-	0%	7h 5s ago
<input type="checkbox"/> MySpectrumWiFic8-2G	A8:9A:93:9E:2...	6, -1	2.4GHz	WPA2 Personal	Sagemcom	b/g/n		-93	7%	-93	-92	-94	-94	6%	now
<input type="checkbox"/> dashcam	58:70:C6:CF:63:B2	5	2.4GHz	WPA2 Personal	Shanghai	b/g/n		-	0%	-70	-70	-70	-	0%	6h 58min ago
<input type="checkbox"/> tl61974e	00:25:F0:61:97:4E	11	2.4GHz	WPA2 Personal	Suga	g/n		-	0%	-92	-91	-92	-	0%	7h 29min 1s...
<input type="checkbox"/> TP-Link_73B0	CC:32:E5:64:73:...	2	2.4GHz	WPA/WPA2 Personal	TP-LINK	b/g/n		-	0%	-91	-89	-94	-	0%	15min 39s a...
<input type="checkbox"/> ARCNET5G	68:D7:9A:2A:60:...	6	2.4GHz	WPA2 Personal	Ubiquiti	b/g/n		-	0%	-86	-86	-89	-	0%	9min 53s ago

NetSpot Surveys

- Wi-Fi surveys are the key feature of NetSpot
 - You run a survey by walking, marking your position on the map, giving NetSpot a few seconds to collect data samples, watching Wi-Fi networks being detected and visualized
 - 15+ heatmap coverage graphs are available with powerful customizable reports

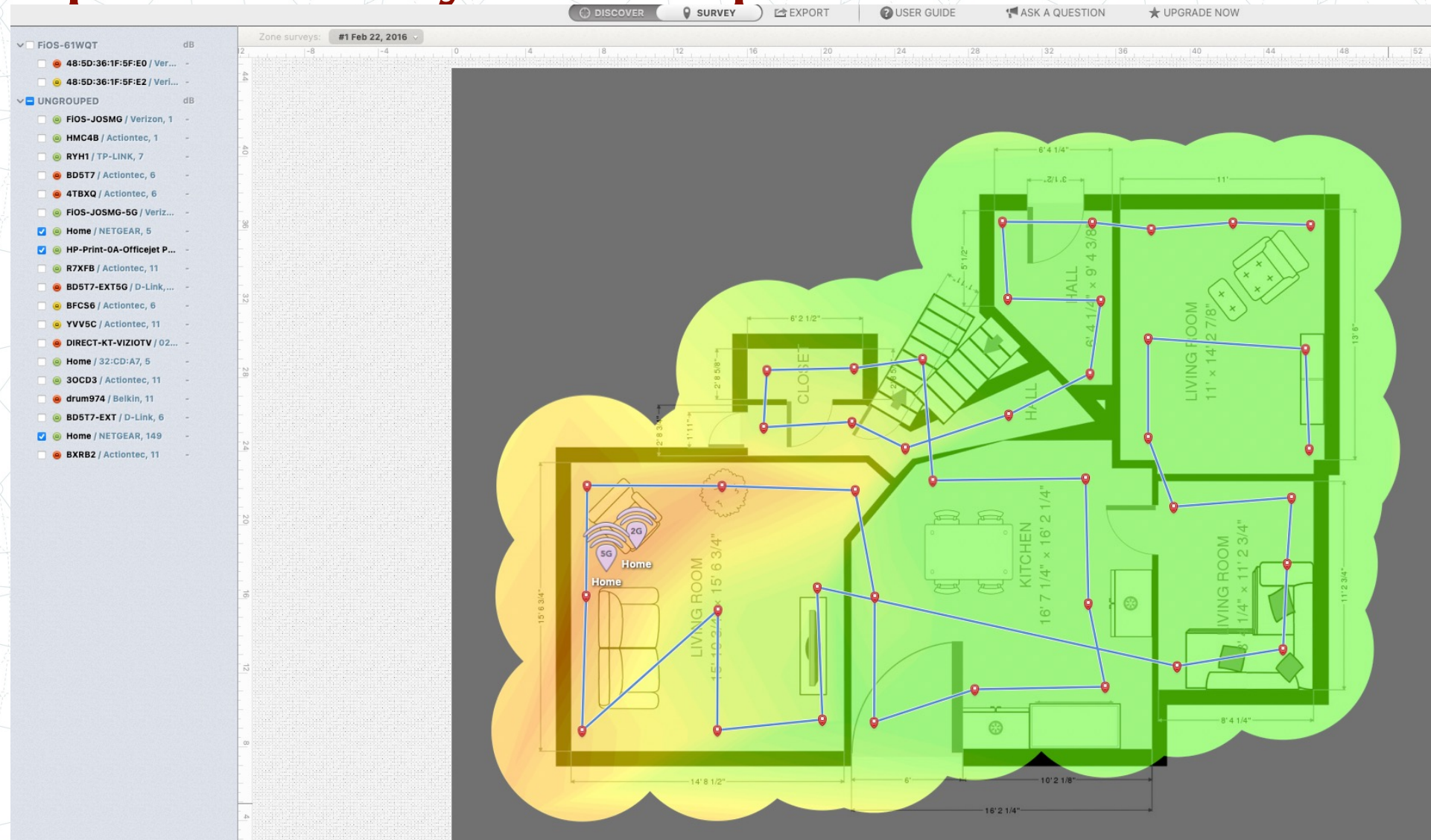
NetSpot Passive Surveys

- Signal-to-noise ratio
- Signal level
- Quantity of access points
- Noise level
- Signal-to-interference ratio
- Frequency band coverage
- PHY mode coverage

NetSpot Active Surveys

- Throughput testing with Iperf 3 or custom speed test servers
- Upload and download speed
- Wireless transmit rate
- Iperf upload, download and jitter

NetSpot Survey Example:



Airodump-ng

- Airodump-ng is used for packet capture, capturing raw 802.11 frames
- It is particularly suitable for collecting WEP IVs (Initialization Vector) or WPA handshakes for the intent of using them with aircrack-ng
- If you have a GPS receiver connected to the computer, airodump-ng is capable of logging the coordinates of the found access points

Kismet

- A wireless network and device detector, sniffer, wardriving tool, and WIDS (wireless intrusion detection) framework
- Kismet works with Wi-Fi interfaces, Bluetooth interfaces, some SDR (software defined radio)
- Kismet works on Linux, OSX, and Windows 10
 - On Linux it works with most Wi-Fi cards, Bluetooth interfaces, and other hardware devices
 - On OSX it works with the built-in Wi-Fi interfaces, and on Windows 10 it will work with remote captures

Thank you. Questions?

Dr. Abdullah Aydeger