Summary

Between June 27 and July 6, SNS Global LLC conducted a program to determine what networks could be identified near the residences of several members of Congress whose Washington-area homes are pictured in Google's Street View database. The residences surveyed included those of House Energy and Commerce Committee Chairman Henry Waxman, Chairman Emeritus John Dingell, and Reps. Edward J. Markey, Rick Boucher, and Jane Harman.

The equipment used was two laptops running the Linux operating system and the Kismet wireless network detector, sniffer, and intrusion detection system.[1] Kismet is an open source program used by Google to collect information about residential wireless networks in the United States and more than two dozen other countries.

The Kismet application was using random access memory only and when the system was shut down any data captured was lost. Copies of the report files were moved to a USB drive prior to shutdown in order to retain the information required for this report. These are only text and image based files and no packets reside within them.

The KISMET application is an 802.11 wireless network, sniffer, and intrusion detection system. It identifies networks by passively collecting packets and detecting networks, which allows it to detect, and given time,

[1] To ensure proper procedures and assist in this research, SNS retained a Certified Information Systems Security Professional who holds a Master of Science in Information Security and Assurance.

expose the names of hidden networks and the presence of non-beaconing networks via data traffic.

Wireless internet data is transmitted in packets using the Transmission Control Protocol of the Internet Protocol technology suite. This suite is commonly referred to as TCP/IP.

TCP/IP packet reconstruction can be performed easily on any data packets captured using Kismet or similar programs. Once gathered, the packets can be presented to the appropriate packet reconstruction application and any files can be reconstructed to include word documents, email messages, and pictures.

Selected Results

The following networks were identified while parked on the public street in front of the addresses listed for approximately 5 minutes. This is only enough time to capture the information that identifies the networks, but not enough time to gather the amount of packets required for a full TCP/IP packet reconstruction analysis.

Jane Harman, CA. The following networks were detected. It is obvious that the two networks listed belong to the congresswoman. Neither one of them are utilizing the available security mechanisms built into the wireless access point. It would be a simple matter of setting and collecting the packets and then reconstructing any unencrypted content including documents, email or transmitted files.

Based on the various clients with various manufacturers of the wireless technology connected to the "harmantheater" network, it is very likely that this is an internet connected network used for various data types such as internet, email and internet telephony.

#	BSSID	SSID	Pkts	Encryption	Clients	
1	00:1E:E5:A1:4D:42	Harmanmbr	6	None	Client 1	00:1E:E5:A1:4D:42

2	00:23:69:78:65:AF	harmantheater	123	None	Client 1	00:18:3A:37:B9:0A
					Client 2	00:23:69:78:65:AF
					Client 3	00:26:24:16:4C:D0
					Client 4	00:26:82:4B:87:6F

John Dingell, MI, Chairman Emeritus. Based on the network information presented in Table 1 it is difficult to discern which one of the networks may be the former Chairman's. Many of the identified networks are WEP encrypted but eight were open.

#	BSSID	SSID	Pkts	Encryption	Client MAC	
1	00:0C:F1:46:38:EB	Home	1	None	Client 1	00:0C:F1:46:38:EB
2	00:12:0E:7A:66:A5	07B405917196	1	WEP	Client 1	00:12:0E:7A:66:A5
3	00:12:0E:8D:E4:52	07FX10125497	4	WEP	Client 1	00:12:0E:8D:E4:52
4	00:12:17:02:E7:F2	GMlink	230	none	Client 1	00:12:17:02:E7:F2
5	00:16:B6:F5:29:A4	Home	169	None	Client 1	00:0C:F1:46:38:EB
					Client 2	00:16:B6:F5:29:A4
6	00:18:39:41:C0:9B	Linksys	9	None	Client 1	00:18:39:41:C0:9B
7	00:18:F8:3D:AA:D3	Tamaki-Home	1	WEP	Client 1	00:18:F8:3D:AA:D3
8	00:1E:52:C9:6A:A9	<cloaked>	1	None	Client 1	00:1E:52:C9:6A:A9
9	00:1E:E5:73:4E:6F	jpfcbf	1	WPA	Client 1	00:1E:E5:73:4E:6F
10	00:1F:5B:87:87:3D	penguin	20	WPA	Client 1	00:1F:5B:87:87:3D
11	00:1F:90:B3:A3:5C	YAGI5	80	WEP	Client 1	00:1F:90:B3:A3:5C
					Client 2	00:23:EE:6B:2B:2A
					Client 3	00:23:EE:6B:2B:D3
12	00:1F:90:C8:4B:A8	IG135	5	WEP	Client 1	00:1F:90:C8:4B:A8
13	00:1F:90:C8:A0:48	KCZ15	4	WEP	Client 1	00:1F:90:C8:A0:48
14	00:1F:90:D4:AC:80	4LB94	21	WEP	Client 1	00:18:4D:CD:81:67
					Client 2	00:1F:90:D4:AC:80
15	00:1F:90:E2:C8:4D	3GG50	1	None	Client 1	00:1F:90:E2:C8:4D

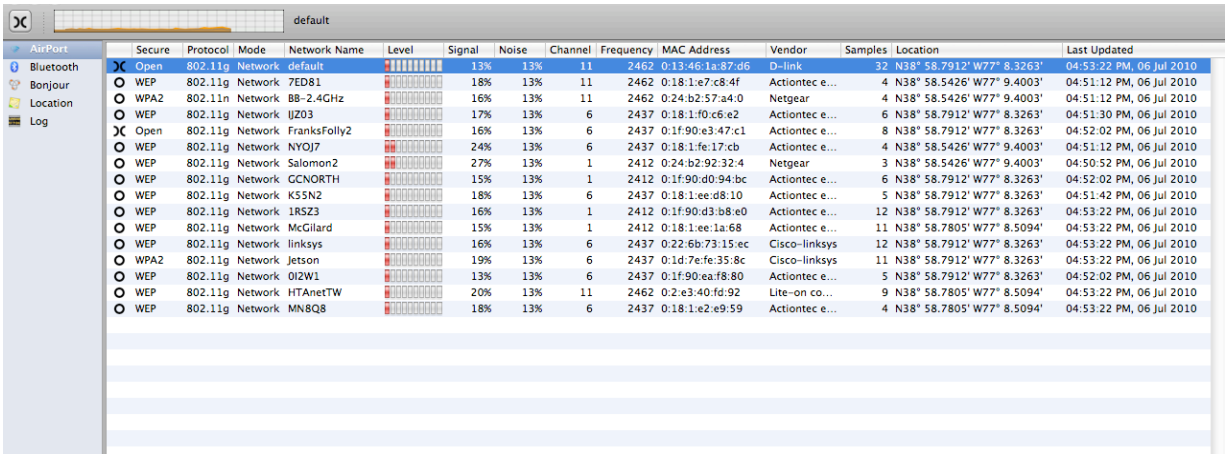
16	00:1F:90:F7:38:74	TIWH3	169	WEP	Client 1	00:1F:90:F7:38:74
					Client 2	00:1F:C4:96:19:EC
					Client 3	00:22:10:7A:85:6F
17	00:22:3F:2C:01:AE	WuNet	79	WPA	Client 1	00:22:3F:2C:01:AE
					Client 2	00:25:D3:44:DB:00
18	00:23:7A:08:FB:D0	bay2	1	None	Client 1	00:23:7A:08:FB:D0
19	00:25:3C:BD:56:41	Kalyani	3	WEP	Client 1	00:25:3C:BD:56:41
20	00:25:D3:44:DB:00	<cloaked>	1	None	Client 1	00:25:D3:44:DB:00
21	00:26:62:E0:5C:AC	NV356	238	WEP	Client 1	00:1E:C2:0A:14:20
					Client 2	00:23:EE:42:F2:8D
					Client 3	00:23:EE:A6:84:3F
					Client 4	00:26:62:E0:5C:AC

Edward J. Markey. Based on the network information listed in the table below it is difficult to discern which one of these networks belongs to the congressman. Many of the identified networks are WEP encrypted but two are open.

#	BSSID	SSID	Pkts	Encryption	Clients	
1	00:12:0E:63:85:2F	07B402673980	187	WEP	Client 1	00:12:0E:63:85:2F
2	00:18:01:EA:D5:D4	MMTO1	30	WEP	Client 1	00:18:01:EA:D5:D4
3	00:18:01:EE:D8:50	1V8N2	30	WEP	Client 1	00:18:01:04:B5:4C
					Client 2	00:18:01:EE:D8:50
					Client 3	00:23:EE:2C:BC:D5
4	00:18:01:F1:1F:82	D OFC	12	WEP	Client 1	00:18:01:4D:83:89
					Client 2	00:18:01:F1:1F:82
5	00:1A:70:34:5F:AA	Linksys	38	None	Client 1	00:0E:A6:9A:BD:FC
					Client 2	00:18:01:1E:E8:E7
					Client 3	00:19:7D:18:EF:98
					Client 4	00:1A:70:34:5F:AA
6	00:1F:33:F8:D2	NETGEAR	160	None	Client	00:1F:33:F8:D

	:BE				1	2:BE
					Client 2	00:24:8C:9C:50:4E
7	00:1F:90:CB:46:A8	4II35	174	WEP	Client 1	00:1F:90:CB:46:A8
					Client 2	00:23:ED:85:1A:54
8	00:1F:90:F1:51:06	2SD43	63	WEP	Client 1	00:1F:90:5F:6D:E5
					Client 2	00:1F:90:F1:51:06
9	00:26:62:F3:3C:28	TC042	1	WEP	Client 1	00:26:62:F3:3C:28
10	00:30:BD:F7:03:E9	I OFC	104	WEP	Client 1	00:30:BD:F7:03:E9

Henry Waxman, CA The following networks were detected. A total of 16 networks were picked up at this location but an analysis of the networks did not reveal an obvious match to Rep. Waxman. However, his network may be in the compiled list of network names. Two of these networks were unencrypted.



Rick Boucher, VA The following networks were detected. A total of 93 networks were picked up at this location but an analysis of the networks did not reveal an obvious match to Rep. Boucher. However, his network may be in the compiled list of network names. Some of these networks were unencrypted.

DD's, 3DPU9, Telvar, 06B404674078, 09FX05078710, 09FX10019023, 09FX10089705, the best, markbert, Learn, KMB, Cedric, Learn, JMG2009, Home, 06B404673231, Korach, YIKES, GMS, NETGEAR, BAYS, slick1, Pucktopuck, Mishelle Outlaw's Network, Plainview1, ChitNet, Abingdon House, DillyNet8, Megan, Jill, AlandTrooper, JW0824, Apple Network 9a55ef, DCA-SW, kay, Ideas, lost, Fleming, DZHU1, 137 Duddington, linksys, Lucy Luck, Lucy Luck, Amanda, Mr. Smith, 09FX10041345, 09FX12050068, 71423030, Buddy, SAM, denholm Elliott, mike1, Chase, LeoLuberecki, SMCnet, networkLW, LowDudd, Jay's lament, 3LJX9, Melrose, PeteNet, John & Pam Kirby's Network, hoffman2, Pupo, El Network, DCRican's Guest Network, Customer ID, pj44, Lauras Network, happydog, attwifi, Drew Sweat\342\200\231s MacBook, SON-Jefferson@Capitol Yards, mpm1215, 05B401891404