Swapnil Samant
80073690

Objective

The objective of this project is to determine the type of devices connected to 802.11 WiFi Network.

Background

There are various approaches to determine wireless devices types connected to a WiFi network. Each one of these approaches provides different levels of details about the connected devices. The approach used in this project is a combination of Wifi MAC Layer Management Entity (MLME) along with requested options during a DHCP request and the MAC ID of the wireless device. The MLME approach is influenced by the paper listed in [1] and the talk listed in [2].

Each WiFi device has a unique MAC address, a MAC address is a 48-bit number. The first 24 bits can be used to identify the manufacturer of the device. The first 24 bits might also represent the manufacturer of the WiFi card in some cases. A list for the first 24-bits (Organizationally Unique Identifier OUI) and the manufacturer name is available from IEEE.

When a WiFi device connects to an access point, the DHCP server can query the device for the type of device, manufacturer name, host name and OS of the client device. The options are detailed in RFC 2132. The options can be used to create a fingerprint for the device type. Fingerbank (https://fingerbank.org) has a huge database of such fingerprints for a variety of wired and wireless devices. Fingerbank also provides and API to query these finger prints.

MLME consists of a number of different types of packets used in the operation of a Wifi network. Most Wifi MLME frames consist of a set of Fixed Parameters which are always present followed by Tagged parameters, optional fields which are implemented as Type-Length-Value tuples. The standards documents define many parameters, and there is a vendor extension mechanism for private entities to add their own parameters [1]. In our approach we have focused on Probe Requests, Probe Responses and Association frames. Examples of other types of frames are QoS Data Frames, Acknowledgement frames, Request-to-send frames, Clear-to-send frames.

Example of a probe request frame captured from Apple iPhone SE is listed in Figure 1.

```
▶ Frame 88466: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface 0
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▶ IEEE 802.11 Probe Request, Flags: ........C
▼ IEEE 802.11 wireless LAN
  ▼ Tagged parameters (138 bytes)
    ▶ Tag: SSID parameter set: mifi
    ▶ Tag: Supported Rates 1, 2, 5.5, 11, [Mbit/sec]
    ▶ Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 4
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: Extended Capabilities (8 octets)
    ▶ Tag: Interworking
    ▶ Tag: Vendor Specific: Apple
    ▶ Tag: Vendor Specific: Epigram: HT Capabilities (802.11n D1.10)
    ▶ Tag: Vendor Specific: Microsof: Unknown 8
    ▶ Tag: Vendor Specific: Broadcom
```

Figure 1: Summary of iPhone SE Probe Request Frame

The management entity in an Access Point handles processing of MLME frames received from other stations. As part of its handling of Probe Request and Association Request frames, the AP examines the series of Tagged

Parameters seen from each client, extracting information which is used to make a signature. This information is concatenated into a simple text string.

An example signature for an iPhone SE is:

wifi4|probe:0,1,50,3,45,127,107,221(0017f2,10),221(0050f2,8),221(001018,2),htcap:4021,htagg:17,htmcs:000000ff,extcap:0400088400000040|assoc:0,1,50,33,36,127,221(0017f2,10),221(001018,2),txpow:1402,extcap:0000000000000040

Authors in [1] have created a database of these WiFi fingerprints which is available at [3]. This database is still a work in progress and does not include all wireless devices.

Methodology

The following hardware was used for this project:

- Raspberry pi model B+
- Alfa network adapter AWUS036NH

The softwares used for this project are:

- hostapd – a user space daemon for access point and authentication servers
- Dnsmasq – DNS and DHCP server.
- raspbian stretch lite – operating system based on Debain Stretch.

Dnsmasq provides a DNS and a DHCP server which can be used with hostapd to create an open access point. WiFi devices can see the SSID created using this setup and connect to the access point. If WiFi device has connected to an open network with the same SSID. In the past, then the device connects to this access point automatically without any user intervention.

Dnsmasq was selected as a DHCP and DNS server for the following reasons:

- Dnsmasq provides a DHCP fingerprint of clients connected through an environment variable(DNSMASQ_REQUESTED_OPTIONS) which can be access through user scripts. Other attributes of the connected clients such as MAC Address, IP Address, host name and device vendor class are also available from Dnamasq.
- Dnsmasq provides a mechanism to run a script on any client activity such as connect or disconnect through a run time setting(dhcp-script).

hostapd was selected as the access point software because of the following reason:

- hostapd provides a mechanism to broadcast multiple SSIDs at the same time.
- hostapd provides a compile time flag(CONFIG_TAXONOMY) which can be used to retrieve the WiFi signature of connected clients through the hostapd_cli command with the signature option.

In our setup an open WiFi SSID was setup using hostapd and network setting were provided by Dnsmasq. A client script was written which runs when client connects through Dnsmasq, this script gets the clients MAC address, DHCP fingerprint, host name and vendor class and writes them to a text file.

Another script runs on the machine, which read the file which has the details about connected clients. This script is written in Python. The Python script queries the IEEE OUI database to get the clients manufacturer using its MAC address. Then the Python script uses the DHCP fingerprint and MAC address to query Fingerbank using API to retrieve the device type, operating system and the class of the device. Finally, the Python script looks up the WiFi fingerprint in the WiFi Taxonomy database to retrieve the device model. These details are then displayed to the user.

Results

A limited testing of the setup was performed with six devices. The devices are as follows:

- Apple iPhone SE
- Apple iPad Pro 9''
- Moto E 2nd gen
- Kyocera Hydro
- Blackberry Q10

The complete results are listed in Appendix A.

Out of the six devices that were used for testing, the setup was able to identify the manufacturer, operating system and device type (mobile, tablet etc.) for five of the six devices. The setup was not able to identify the exact model for any of the devices, this might because the WiFi taxonomy database listed in [3] is still a work in progress and is missing the fingerprints of the devices that were tested.

Conclusions

Looking at the results it can be concluded that it is possible to identify the manufacturer, OS and device type for most of the devices. However, to identify the exact model of older devices, the WiFi taxonomy database needs to be updated with the fingerprints of all possible devices. The WiFi taxonomy database could benefit if there was a better way to collect the fingerprints of devices.

Bibliography

[1] D. Gentry and A. Pennarun, "Passive Taxonomy of Wifi Clients using MLME Frame Contents," Google, Inc., 2016.

[2] DEFCONConference, "DEF CON 25 Conference - Denton Gentry - I Know What You Are By the Smell of Your Wi-Fi - YouTube," Google Inc., 19 Jan 2018. [Online]. Available: https://www.youtube.com/watch?v=n_gSJkswdhU. [Accessed 23 4 2018].

[3] DentonGentry, "GitHub - NetworkDeviceTaxonomy," [Online]. Available: https://github.com/NetworkDeviceTaxonomy/wifi_taxonomy. [Accessed 29 4 2018].

Swapnil Samant
80073690

Appendix A

MAC Addresses have been anonymized to protect privacy.

Testing output:

{'24:da:9b:xx:xx:xx': {'fingerbank_response':
{u'version': None,
u'created_at': u'2018-04-29T03:33:13.000Z',
u'updated_at': u'2018-04-29T03:33:13.000Z',
u'score': 50,
u'device': {u'name': u'Generic Android',
u'mobile': True,
u'created_at': u'2014-09-09T15:09:52.000Z',
u'updated_at': u'2015-02-06T15:53:25.000Z',
u'inherit': False,
u'parent_id': 11,
u'parents': [{u'name': u'Smartphones/PDAs/Tablets',
u'tablet': False,
u'mobile': True,
u'created_at': u'2014-09-09T15:09:50.000Z',
u'updated_at': u'2016-11-23T03:41:40.000Z',
u'inherit': False,
u'submitter_id': None,
u'parent_id': None,
u'details': None,
u'devices_count': 23,
u'id': 11,
u'approved': True}],
u'id': 202},
u'id': 20592212},
'wifi_taxonomy':
'wifi4|probe:0,1,50,3,45,221(0050f2,8),htcap:012c,htagg:03,htmcs:000000ff|assoc:0,1,50,45,127,htcap:012c,htagg:03,htmcs:000000ff,extcap:00000a0200000000',
'dhcp_finger_print': '1,33,3,6,15,28,51,58,59',
'vendor_class': 'dhcpcd-5.5.6',
'host_name': 'android-1111b7a5cebbd0d5',
'manufacturer': 'Motorola Mobility LLC, a Lenovo Company'
},

'78:4f:43:xx:xx:xx': {'fingerbank_response':
{u'version': None,
u'created_at': u'2016-11-29T12:17:54.000Z',
u'updated_at': u'2016-11-29T12:17:54.000Z',
u'score': 50,
u'device': {
u'name': u'Mac OS X',
u'mobile': False,
u'created_at': u'2014-09-09T15:09:51.000Z',
u'updated_at': u'2015-03-24T11:44:09.000Z',
u'inherit': False,
u'parent_id': 2,
u'parents': [{u'name': u'Macintosh',

u'tablet': False,
u'mobile': False,
u'created_at': u'2014-09-09T15:09:50.000Z',
u'updated_at': u'2014-09-09T15:09:50.000Z',
u'inherit': False,
u'submitter_id': None,
u'parent_id': None,
u'details': None,
u'devices_count': 2,
u'id': 2,
u'approved': True}],
u'id': 38},
u'id': 5689554},
'wifi_taxonomy': '',
'dhcp_finger_print': '1,121,3,6,15,119,252,95,44,46',
'vendor_class': '',
'host_name': 'Swapnils-MBP',
'manufacturer': 'Apple, Inc.'
},

'00:1f:bd:xx:xx:xx': {'fingerbank_response':
{u'version': None,
u'created_at': u'2018-04-29T03:33:14.000Z',
u'updated_at': u'2018-04-29T03:33:14.000Z',
u'score': 50,
u'device': {u'name': u'Generic Android',
u'mobile': True,
u'created_at': u'2014-09-09T15:09:52.000Z',
u'updated_at': u'2015-02-06T15:53:25.000Z',
u'inherit': False,
u'parent_id': 11,
u'parents': [{u'name': u'Smartphones/PDAs/Tablets',
u'tablet': False,
u'mobile': True,
u'created_at': u'2014-09-09T15:09:50.000Z',
u'updated_at': u'2016-11-23T03:41:40.000Z',
u'inherit': False,
u'submitter_id': None,
u'parent_id': None,
u'details': None,
u'devices_count': 23,
u'id': 11,
u'approved': True}],
u'id': 202},
u'id': 20592213},
'wifi_taxonomy':
'wifi4|probe:0,1,50,3,45,221(0050f2,8),htcap:012c,htagg:03,htmcs:000000ff|assoc:0,1,50,45,htcap:012c,htagg:03,
htmcs:000000ff',
'dhcp_finger_print': '1,33,3,6,12,15,28,51,58,59,119',
'vendor_class': 'dhcpcd-5.2.10:Linux-3.0.8-perf:armv7l:QCT MSM8X55 SURF',
'host_name': 'android-5fb772b6c03d8d5a',
'manufacturer': 'Kyocera Wireless Corp.'
},

Swapnil Samant
80073690

'1c:91:48:xx:xx:xx': {'fingerbank_response':
{u'version': None,
u'created_at': u'2016-04-18T17:12:08.000Z',
u'updated_at': u'2016-04-18T17:12:09.000Z',
u'score': 50,
u'device': {u'name': u'Apple iPod, iPhone or iPad',
u'mobile': True,
u'created_at': u'2014-09-09T15:09:52.000Z',
u'updated_at': u'2015-02-04T15:53:52.000Z',
u'inherit': False,
u'parent_id': 11,
u'parents': [{u'name': u'Smartphones/PDAs/Tablets',
u'tablet': False,
u'mobile': True,
u'created_at':
u'2014-09-09T15:09:50.000Z',
u'updated_at': u'2016-11-23T03:41:40.000Z',
u'inherit': False,
u'submitter_id': None,
u'parent_id': None,
u'details': None,
u'devices_count': 23,
u'id': 11,
u'approved': True}],
u'id': 193},
u'id': 3172872},
'wifi_taxonomy':
'wifi4|probe:0,1,50,3,45,127,107,221(0017f2,10),221(0050f2,8),221(001018,2),htcap:4021,htagg:17,htmcs:000000ff,extcap:0400088400000040|assoc:0,1,50,33,36,127,221(0017f2,10),221(001018,2),txpow:1402,extcap:0000000000000040',
'dhcp_finger_print': '1,121,3,6,15,119,252',
'vendor_class': '',
'host_name': 'iPhone',
'manufacturer': 'Apple, Inc.'},

'98:01:a7:xx:xx:xx': {'fingerbank_response':
{u'version': None,
u'created_at': u'2016-06-13T03:28:32.000Z',
u'updated_at': u'2016-06-13T03:28:33.000Z',
u'score': 50,
u'device': {u'name': u'Apple iPod, iPhone or iPad',
u'mobile': True,
u'created_at': u'2014-09-09T15:09:52.000Z',
u'updated_at': u'2015-02-04T15:53:52.000Z',
u'inherit': False,
u'parent_id': 11,
u'parents': [{u'name': u'Smartphones/PDAs/Tablets',
u'tablet': False,
u'mobile': True,
u'created_at': u'2014-09-09T15:09:50.000Z',
u'updated_at': u'2016-11-23T03:41:40.000Z',
u'inherit': False,

Swapnil Samant
80073690

u'submitter_id': None,
u'parent_id': None,
u'details': None,
u'devices_count': 23,
u'id': 11,
u'approved': True}],
u'id': 193},
u'id': 3776681},
'wifi_taxonomy': '',
'dhcp_finger_print': '1,121,3,6,15,119,252',
'vendor_class': '',
'host_name': 'Swapnils-iPad',
'manufacturer': 'Apple, Inc.'},

'94:eb:cd:xx:xx:xx': {'fingerbank_response':
{u'fixed': False,
u'user_agent_id': 0,
u'score': 0,
u'created_at':
u'2018-04-30T01:35:43.895Z',
u'dhcp6_fingerprint_id': 0,
u'updated_at': u'2018-04-30T01:35:43.913Z',
u'mac_vendor_id': 15665,
u'dhcp6_enterprise_id': 0,
u'version': None,
u'dhcp_vendor_id': 0,
u'dhcp_fingerprint_id': 898,
u'submitter_id': 5808,
u'id': 20632478,
u'device_id': None},
'wifi_taxonomy': '',
'dhcp_finger_print': '1,28,2,3,15,6,12,119',
'vendor_class': 'BlackBerry OS 10.3.3.2205',
'host_name': 'BLACKBERRY-36C5',
'manufacturer': 'BlackBerry RTS'
}

}