Wireless Client Device Finger printing

B A Sujathakumari (sujathakumari@sjce.ac.in), Abhishek P (abhishekprabhu6@gmail.com)

Abstract: Client device finger printing is method of identifying the client device type, operating system, Device vendor and other types of information which is connected to the wireless network. Also, it is the action of gathering device information to characterize it. This process generates a signature, also called a fingerprint, that describes the observed features of a device in a compact form. If the generated signature is distinctive enough, it may be used to identify a device. In the present developments where they are talking about internet of everything and bring your own device (BYOD) it is required for the enterprise to identify the devices connected to the network and mark them accordingly which may help the enterprise to avoid data leakage, unauthorized device connections and some other security violations. This paper gives the client fingerprinting types and new developed techniques to obtain the device details like device vendor, device operating system and device type.

Key words: Access Point, Mac Address, DHCP, WLAN, User Equipment

Introduction: Wi-Fi is emerging as the primary medium for wireless Internet access. Cellular carriers are increasingly offloading their traffic to Wi-Fi Access Points (APs) to overcome capacity challenges, limited RF spectrum availability, cost of deployment, and keep up with the traffic demands driven by user generated content.

The explosive growth of mobile devices has challenged the network IT staff because mobile devices lack the option to connect using Ethernet, which is the dominant wired access technology. Leading industry analyst forecasts predict that only 15% of the devices will have built-in Ethernet capability. As more of these devices connect using the enterprise wireless LAN, network administrators have noted that an employee typically has gone from using a single device to using three or more devices.

As network engineers get ready to support large numbers of smartphones and tablets in addition to laptops and desktops, they are realizing the importance of reliably identifying mobile devices. Gaining visibility into mobile device types is essential for network engineers to build granular access policies to maintain security and quality of service (QoS) for critical enterprise applications

About Wi-Fi: Wi-Fiis a technology for wireless local area networking with the IEEE 802.1x standard devices, Wi-Fi Access Point, Cloud or Virtual Wireless Lan Controller and Graphical User Interface are the components of Wi-Fi

Wi-Fi Access Point: It is networking equipment that involves

gadgets which are remote and connected with systems using Wi-Fi. Wi-Fi Access Points uses IEEE 802.11x guidelines and gives associations with one or various remote gadgets. Wi-Fi AP depends on embedded chip set. Wi-Fi AP is overseen and arranged by means of CWLC. CWLC gives concentrated administration to countless Wi-Fi APs. Apart from overseeing Wi-Fi AP, controller additionally empowers system improvement elements to give more prominent RF proficiency furthermore gives better end client experience. Wi-Fi Controller (CWLC) is a cloud based Wi-Fi controller which brought together administration to an extensive number of Wi-Fi APs. CWLC uses Open Stack based cloud. One CWLC can manage numerous APs and STA gadgets. Number of APs and STA gadgets upheld by a CWLC relies on upon number of centers accessible to run CWLC application. The cloud based **Methodology:** There are three typesfinger printing discussed in this paper, they are identifying vendor type using MAC address finger printing, identifying Device type and Operating system type of connected devices using DHCP message requests.

MAC Address finger printing: Every device has a physical address which is different for every device called Media access control, these mac addresses are provided uniquely for vendors by IEE 802 standards, mac address consists of 6 octets separated by semicolon, the first three octets are specifically called as Organizationally Unique Identifier and the next three octets are identified as Network Interface controller specific.

CWLC will have different Virtual Machines. The 4 fundamental Virtual machines are: Load Balancer VM, Controller VM, GUI/CLI/NAT VM, DB VM, The Controller (cWLC) provides GUI for the management of Access Points and the controller itself including the monitoring of Wireless Clients.

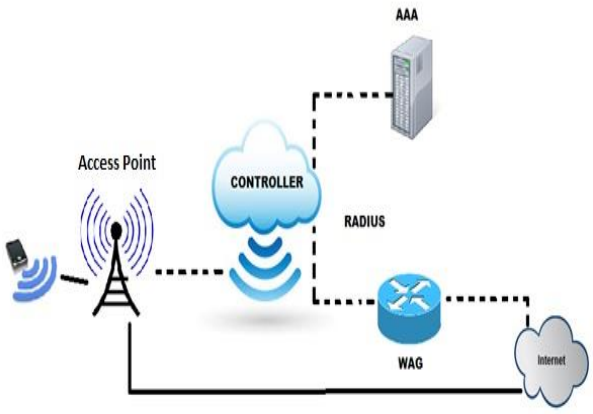

Figure 1.1 W-Fi Network diagram

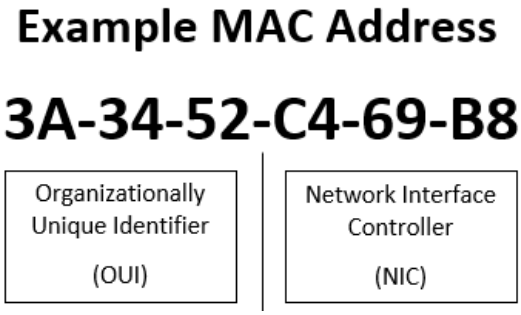

Fig :1.2 MAC Address representation

When a mobile device is connected to Wi-Fi network during the initial connection establishments the controller obtains the mac address of the device connected, this mac address is copied to one of the database. A database is added in the controller which will have the complete data of the vendors with corresponding mac addresses obtained from http://standards-oui.ieee.org/oui/oui.txt.
The vendor description is displayed in user

interface with respect to connected SSID, these information's are used for further blacklisting or whitelisting vendors.

Operating System and Device typeIdentification: In recent operating systems related threats are very risky and are prevented using OS hardening and updating to latest versions of operating systems, in order to apply above all policies, the controller should be knowing the operating system of the client device which is connected to the Wi-Fi system via SSID's radiated by wi-fi Access Point. DHCP abbreviated as Dynamic Host Configuration Protocol is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network. When a device tries to access wi-fi it first undergoes authentication processes using Authentication, authorization, and accounting (AAA) after successful authenticity of the device it requests for IP Address from DHCP server during this IP Address there will lot of other DHCP messages request will be taking place, one of the DHCP message is DHCP option 60 which is used todetermine the operating system of the connected device, DHCP option 60 is represented by Figure 1.3 here code is 60 and n represents the option codes length which is already stored in context library and c1 gives the appropriate DHCP message option 60 for connected wireless device to controller c2 gives end of the DHCP option 60 message, through this message controller fetches the client device operating system details.

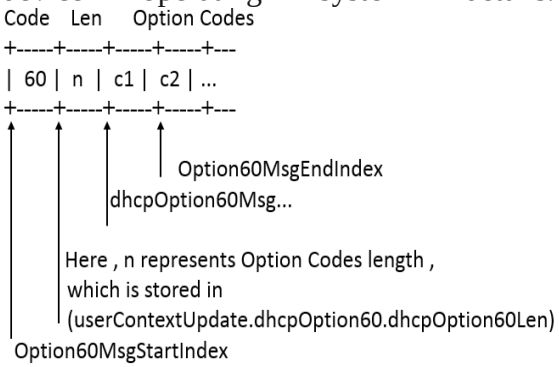

Figure1.3:DHCP Option 60 Message format

Below diagram shows the initial message flow between client device and the Access Point. A client finger print flag is added at the WLAN level to enable or disable client device finger printing of the radiating WLAN, the CFP Flag enable or disable flow goes as the message flow diagram **(Fig 1.4)**

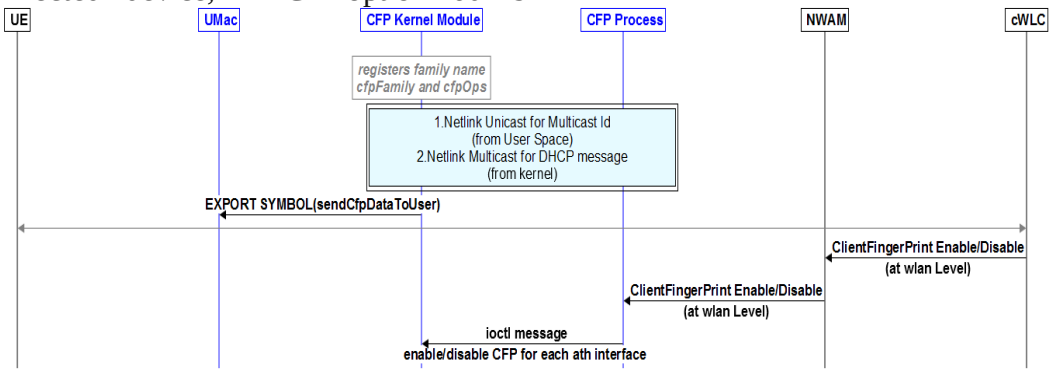

Fig: 1.4Initial call flow of cf process

A kernel module is added in Access point such that it is developed with Netlink modules such that User space will be the client ID which is awaited in kernel space with Netlink Multicastfor DHCP message to be received by the controller. The initial call flow for cfp process described as follows, from Graphical user interface cfp flag is enabled the ack message is sent to cloud controller from cloud controller thecfp enable request message is forwarded to Network manager input output control message is sent from controller to kernel module in Access Point it contains enable or disable cfp for each ath interface for every WLAN, cfp multicasts id message is sent to connected mobile device.It also uses Uthash to handle duplicacy for multiple DHCP coming from single UE, from the received message first DHCP message discover or request received from kernel is processed.The completeDHCP cfp request call flow is given in the **fig.1.4** User equipment is the wireless device which is to be connected to the Wi-Fi Access Point it is connected to wifi AP using WLAN with cfp flag enabled, when it starts connecting to wifi Access point first DHCP Discover/Request message is sent this message is first received by cfp process at this stage UE mac address is added to the Hash table to avoid duplicacy during the DHCP request DHCP option 55 and 60 is extracted and these DHCP options context messages are sent to controller (cWLC) which also includesWlan id of the connected wlan mac id of the connected Access point pre provisioned zone id and the wlan mac the received context is acknowledged by hostApd manager to the cfp process module user context update is sent from cfp process module these data is sent to AAA server where it verifies the authenticity of connected wireless device and also the provided credentials for the security purposes , AAA server also starts accounting server for the connected session of theclient device, than the cfp info is added to the gui in user sessions. When the UE is disconnected accounting is stopped and the user dession is moved to archive list. DHCP option 55 is used to decode the OS Type of the connected device and DHCP option 60 is used to decode the device type these may be Mobile Phones, Laptops or Notepads.RFC 2132 allows server to query additional information from device, DHCP option 55 (Parameter Request List) and option 60 (Vendor class identifier) can be used to find device OS and device type.DHCP Option 55 - This option is used by a DHCP client to request values for specified configuration parameters. The list of requested parameters is specified as a list and the client may list the options in order of preference.The order in which options are added in parameter list is fairly unique and can be used to fingerprint end device.DHCP Option 60 – This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. If DHCP option 60 is

received, vendor information will be identified

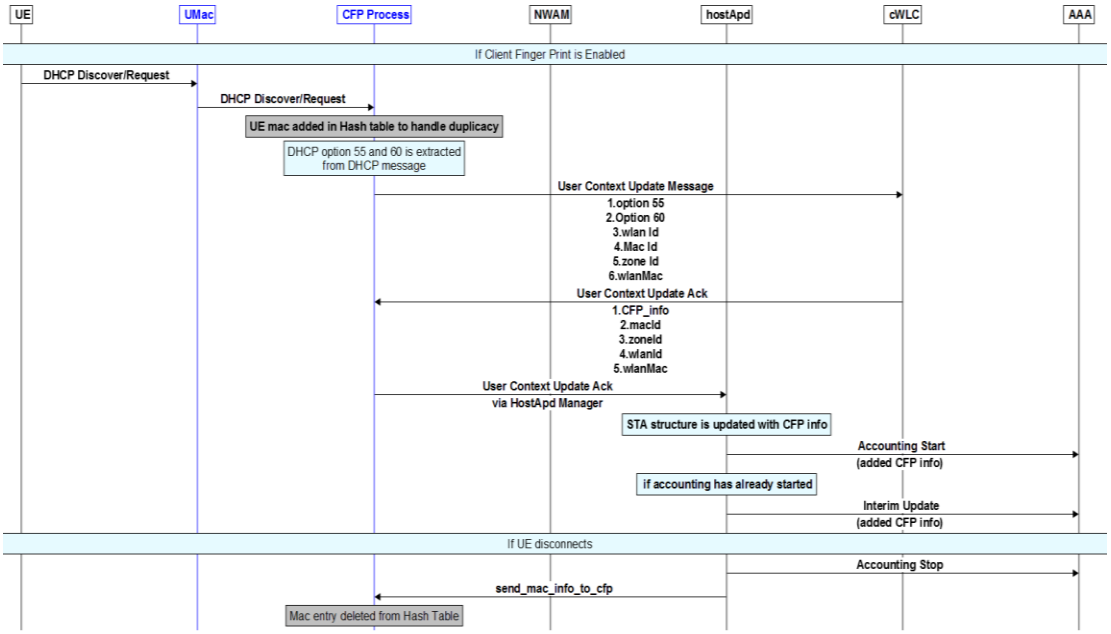

Figure 1.4 Complete call flow diagram of cfp process

Advantages and Disadvantages: The client finger print helps to get the client information without the knowledge of the client by passive accessing internally so that the company can access user data without the knowledge of client. The only disadvantage is if IP Address is assigned statically to user device client fingerprinting is a failed phenomenon for such a process, however most of the client connections to Access point is of dynamic DHCP IP request and makes client finger printing easier,

0	/'Galaxy S [....]	Smartphone [....]	Samsung El [....]
0	/'iPhone 6 [....]	Smartphone [....]	Apple, Inc [....]
0	/'iPhone 6 [....]	Smartphone [....]	Apple, Inc [....]
0	/'OnePlus [....]	Smartphone [....]	OnePlus Te [....]
0	/'Xperia Z [....]	Smartphone [....]	Sony Mobil [....]
0	/'Moto E ([....]	Smartphone [....]	Motorola M [....]
0			
0	/'HTC One [....]	Smartphone [....]	HTC Corpor [....]
0	/'Galaxy S [....]	Smartphone [....]	Samsung El [....]
0	/'OnePlus [....]	Smartphone [....]	OnePlus Te [....]
0	/'iPhone 5 [....]	Smartphone [....]	Apple, Inc [....]
0			
0	/'iPhone 5 [....]	Smartphone [....]	Apple, Inc [....]
0	/'Galaxy S [....]	Smartphone [....]	Murata Man [....]
0	Unknown	Unknown	Microsoft [....]
0	/'Xperia E [....]	Smartphone [....]	Sony Mobil [....]
0	Unknown	Unknown	Microsoft [....]

Fig 1.5 :cfp data of client user equipment

Results: The cfp finger printing is performed with the Access point with the latest database in the controller and satisfied with the results, however database should be upgraded whenever the latest devices are released to the market.

Future enhancements: This is practically used for organizations and future enhancement may include blacklisting or whitelisting the devices with the allowed operating system, device type and the vendor information

Conclusion: A new process named Client Fingerprint is added, Cfp successfully fetches the device type, vendor type and device Operating system, The results are successfully verified with live Access point

References:

[1] K. Gao, C. Corbett, and R. Beyah, "A passive approach to wireless device fingerprinting," in Proc. IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Chicago, Illinois, USA, Aug. 2010, pp. 383–392.

[2] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting," Canadian Journal of Electrical and Computer Engineering, vol. 32, no. 1, pp. 27–33, 2007.

[3] K. Gao, C. Corbett, and R. Beyah, "A passive approach to wireless device fingerprinting," in Proc. IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Chicago, Illinois, USA, Aug. 2010, pp. 383–392.

[4] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in Proc. The 14th ACM International Conference on Mobile Computing and Networking, ser. MobiCom '08, San Francisco, USA, Sep. 2008, pp. 116–127.

[5] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting," Canadian Journal of Electrical and Computer Engineering, vol. 32, no. 1, pp. 27–33, 2007.

[6] C. Neumann, O. Heen, and S. Onno, "An empirical study of passive 802.11 device fingerprinting," in Proc. The 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), Macau, China, Jun. 2012, pp. 593– 602.

[7] M. Barbeau, J. Hall, and E. Kranakis, "Detecting impersonation attacks in future wireless and mobile networks," in Proc. The First International Conference on Secure Mobile Ad-hoc Networks and Sensors, ser. MADNES'05, Singapore, 2006, pp. 80–95.