ArpGuard: Identify and Block Smartphones in Wi-Fi Using ARP Poisoning

Navya Babu [1], Tharun P Karun[2],, Vinitha V[3]
Department of Computer Application
[1,2] Project Scholar, College of Engineering, Trivandrum, Kerala, India
[3] Assistant Professor, College of Engineering, Trivandrum, Kerala, India

Abstract- *Handling people connecting to Wi-Fi Hotspots using their smartphones is a great issue these days, as these people can easily use up all the bandwidth that other users also need. The system identities mobiles through their Media Access Control address (MAC address). All mobiles from a single manufacturer will share a specific MAC address pattern and then kicks them out of the network through a technique called Address Resolution Protocol (ARP) Poisoning attack. An effective ARP poisoning attempt is undetectable to the user. The system is developed as a device which can be connected to the Wi-Fi network which is at risk and needs security*

Keywords- Address Resolution Protocol, Media Access Control, Raspberry, Raspbian operating system, smartphones, arping, gateway address, network interface, network address

I. INTRODUCTION

The risk of using a Wi-Fi network is very high. Nowadays network system show a lot of vulnerabilities which leads to loss of confidential data and causes other risks. It is mainly developed to avoid the unintentional connection of the smartphones which causes traffic and slow network connection to the intentionally connected devices. ArpGuard is a system that identifies the devices connected to a dedicated network and blocks all the Smartphones that are connected to the network. Nowadays network system show a lot of vulnerabilities which leads to loss of confidential data and causes other risks. The system is developed as a device i.e. Raspberry Pi. It can function as a proper desktop computer or be used to build smart devices

.

ArpGuard uses the technology Address Resolution Protocol (Arp). It is a protocol used by the Internet Protocol (IP) [RFC826], specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer.

II. THE PROPOSED BLOCKING SYSTEM

The blocking of specified devices are using a particular device is not a concept yet tried. The existing method to block a smartphone from a network is to manually input the MAC address to deny the access to the network. The proposed blocking system is developed as a device which is a Raspberry Pi that can be connected to any network and all Smartphones in the network is automatically identified and blocked.

ArpGuard uses the ARP poisoning technique to block Smartphones. First, find all the available interfaces and get all the information about the interfaces. Then find the gateway address for interface by extracting the required information from the interface details and hence generate network address. Finally, generate interface information dictionary. Identify all the devices connected to the network and generate a list of live devices on the network. Then we generate a list of devices to be attacked using the MAC Addresses of Smartphones that have been already collected manually and imported the program. In ARP Poisoning the target details and gateway details are specified for deciding which devices have to be blocked. The blocking is done by continuously sending packets to the target devices.

ArpGuard is a very easy to use system. It uses existing Linux subsystems as much as possible. It can work with any networking hardware supported by Linux. The clients on the network can successfully communicate over the network using their network interface. The Raspberry Pi uses the Raspbian operating system. The processor is Advanced RISC Machines Processor(ARM) and the Raspberry Pi has 512 MB.

The system uses different network interfaces like 'wlp13s0', 'wlan0', 'enlp0', 'eno0', 'eth0' etc. to communicate with the network devices and access the information.

The proposed system consists of mainly three functional modules. They are given below:

A. Generate Network Information

For generating network information, by the use of different python libraries list all the available interfaces and get all the information about the interfaces. There is a need to check the network address internally to avoid the local host address. After identifying the network address the gateway address is

identified and stored in the network interface dictionary. With this network information the all the live devices are identified by sending threads to each. Here multi-threading is uses so that multiple thread are parallelly send to devices. By this way the IP address, the MAC address and the status of all devices in the gateway is obtained.

B. Identify Target Devices

All the live devices and its details are already obtained from scanning the network. The target devices ie the smartphones have to be filtered from the list this is done with the help of Wi-Fi MAC address. All the smartphones have 48 bit Wi-Fi MAC address and the prefix of the MAC address shows its vendor. By comparing the list of MAC address of active devices and the list MAC address of Smartphones, the connected smartphones are identified and assign these as the target devices to be blocked from the network.

C. ARP Poisoning Attack

For ARP poisoning specifies the target details and gateway details for deciding which devices have to be attacked and blocked. The blocking is done by continuously sending packets to the target devices. The target device list is updated simultaneously, so that no new smartphones can be connected at any time the list gets updated at every five seconds.

III. THE NETWORK STRUCTURE

The device can be easily connected to the normal network which provides no security at all. After connecting the Raspberry Pi to the network it identifies all the active devices and itself becomes a device in the network structure.

A. Network Structure Without ArpGuard

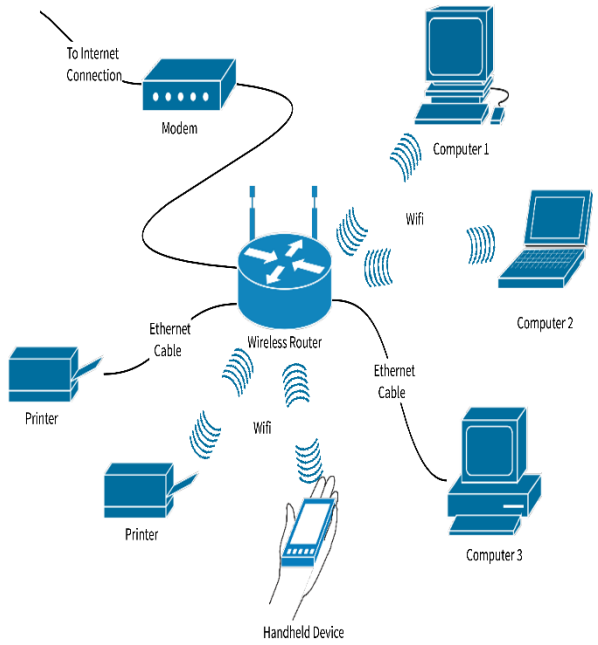

Fig 1.Network without ArpGuard

B. Network Structure With ArpGuard

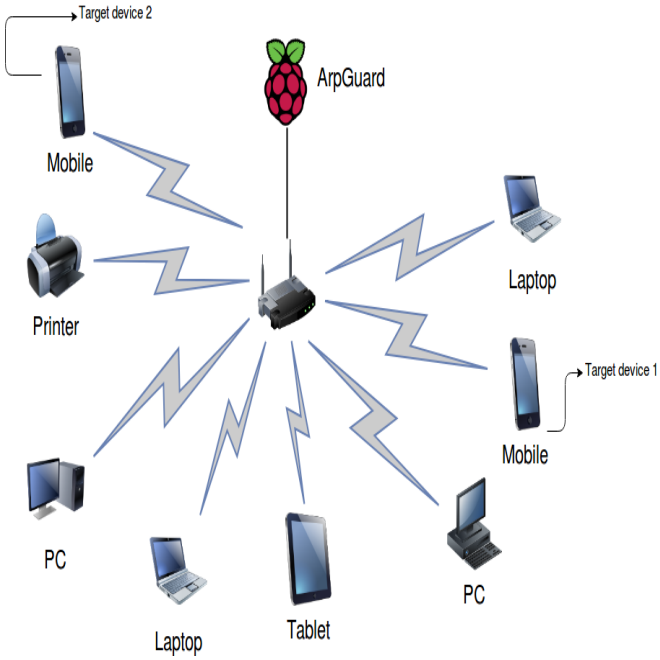

Fig 2. Network with ArpGuard.

C. The Work Flow of the System

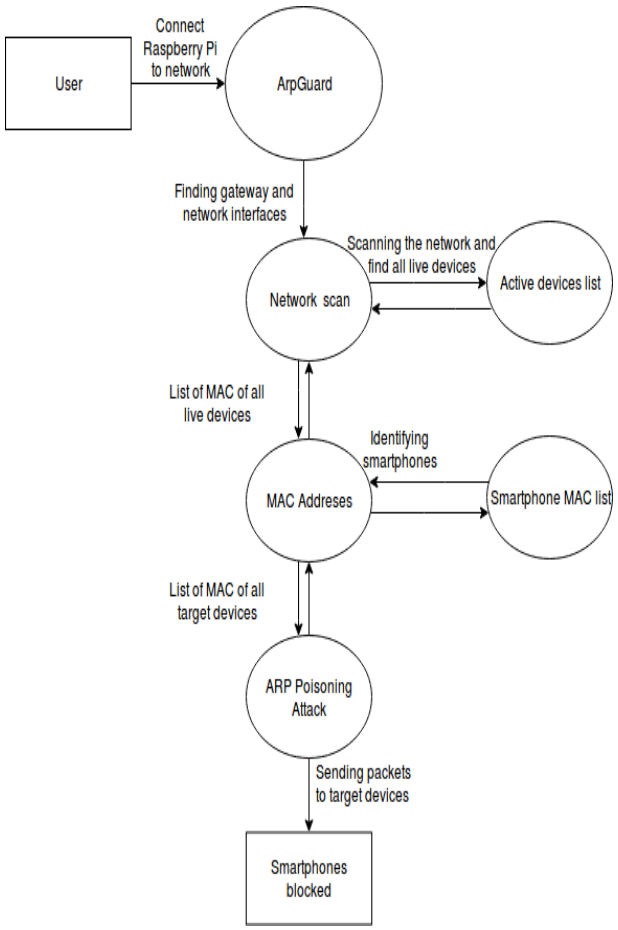

Fig 3.Work Flow Diagram

IV. IMPLEMENTATION

To achieve the best performance by the system instead of normal scanning threads are sent to each device. From all the identified devices exactly the Smartphones are blocked and there is no confusion in blocking the target devices. The system is implemented as a pure portable device. The program is loaded and executed in the Raspberry Pi and then connected the device to the desired network. The network can either be an LAN or WLAN.

The working of ArpGuard is divided into three modules, the network scanning module, the smartphone identification module and the ARP Poisoning attack module.

The three of them has distinct functions. Therefore three different algorithms are used to implement these functions effectively

A. Algorithm 1: Algorithm for Network scanning

Step 1: Initialize the system.
Step 2: Get all the information about the interface.
Step 3: Get gateway address for the interface.
Step 4: Extract required information from interface details.
Step 5: Generate network address.
Step 6: Generate interface information dictionary.
Step 7: Start scanning for live devices.
Step 8: Get information about the live devices.

B. Algorithm 2: Algorithm for Smartphone identification is as follows:

Step 1: Initialize the system.
Step 2: Generate a list of live devices on the network.
Step 3: Generate a list of devices to be attacked.
Step 4: Check the status of devices.
Step 5: Identify the MAC of smartphones and assign it as the target.

C. Algorithm 3: Algorithm for ARP Poisoning attack is as follows:

Step 1: Initialize the system.
Step 2: Specify target details.
Step 3: Specify gateway details.
Step 4: Start ARP Poisoning.
Step 5: Send packets to the target devices.

The proposed system consists of several advantages compared with other existing security measures in networking. The main advantage is that the proposed system is a compatible device that can be easily connected and disconnected whenever needed by the user.

The advantages of the system are

- It will identify all the devices in the network.
- Block all the Smartphones identified.
- Reduce time and effort for securing a network.
- It is developed as an easy to use the device.
- Provide consistency and efficiency.
- It can be connected and disconnected from the network anytime.

The limitations of the system are

- Manual configuration of the network interface when the device is moved from one network to another network.
- Block all the Smartphones identified; hence the intentional connection of Smartphone is also not possible.
- Need to update the Smartphone MAC list whenever a new mobile company is introduced with a new MAC prefix.

V. CONCLUSION

A system has been developed to handling people connecting to Wi-Fi Hotspots using their smartphones. The system identifies mobiles through their MAC IDs (Media Access Control address, all mobiles from a single manufacturer will share a specific MAC address pattern) and then kicks them out of the network through a technique called ARP poisoning attack. An effective ARP poisoning attempt is undetectable to the user. The program will run on a computer which is connected to the Wi-Fi Network in question. It is developed as a connectable device to the network using Raspberry Pi with Raspbian operating system.

VI. FUTURE EXTENSION

The proposed system can be extended. We can create a user interface to momentary disarm the system. In the proposed system there no possibilities to re-correct the network interface when the connected network is changed. This will be very useful while moving the device from one type of network to another network

REFERENCES

[1] Doug Hellman,(2018), "Multiprocessing Basic", [online]: https://pymotw.com/3/multiprocessing/basics.html

[2] Mariia Yakimova ,(2017) , "Guide to async programming in Python" [available at]: https://medium.freecodecamp.org/a-guide-to-asynchronous-programming-in-python-with-asyncio-232e2afa44f6

[3] Python Software Foundation ,(2019), "Subprocess Managmement" [available at]: https://docs.python.org/3.5/library/subprocess.html

[4] Python Software Foundation,(2019), "Flask - Quickstart ", [available at]:http://ask.pocoo.org/docs/1.0/quickstart/

[5] Python Software Foundation,(2019), "Low level networking interface"