ICCECIP 2020
2nd International Conference on Central European Critical Infrastructure Protection
November 16-17, 2020. Budapest, Hungary

ÓBUDA UNIVERSITY
BÁNKI DONÁT FACULTY OF MECHANICAL AND SAFETY ENGINEERING

• Disabling a Wi-Fi Security Camera with Kali linux

[1]Pinter Robert, [2]Sanja Maravić Čisar[3]Furstner Igor

1 Subotica Tech
pinter.robert@vts.su.ac.rs

2 Subotica Tech
sanjam@vts.su.ac.rs

3 Subotica Tech
ifurst@vts.su.ac.rs

Introduction

This work will present an option to attack a Wi-Fi camera. The goal is to disable it in a way that it cannot send any data. This attack will use the deauther method. The deauther does not interfere with any frequencies, it is just sending a few Wi-Fi packets that let certain devices disconnect.
So the focus is only on one device, not blocking or disabling the whole network. For attack we will use Kali Linux and its tools for attacking Wi-Fi network and devices.
While a jammer just creates noise on a specific frequency range (i.e. 2.4GHz), a deauthentication attack is only possible due to a vulnerability in the WiFi (802.11) standard. The deauther does not interfere with any frequencies, it is just sending a few WiFi packets that let certain devices disconnect. That enables you to specifically select every target. A jammer just blocks everything within a radius and is therefore highly illegal to use.

Experimental study

For disabling the IP camera we will use the **aireplay-ng** linux tool. The **aireplay-ng** is used to inject frames. The primary function is to generate traffic for the later use in aircrack-ng for cracking the WEP and WPA-PSK keys.
There are different attacks which can cause deauthentications for the purpose of capturing WPA handshake data, fake authentications, Interactive packet replay, hand-crafted ARP request injection and ARP-request reinjection. With the packetforge-ng tool it's possible to create arbitrary frames.
It works with any wireless network interface controller whose driver supports raw monitoring mode and and sniff 802.11a, 802.11b and 802.11g traffic.

Performing this attack, we have to be on the same network as camera. To find the MAC address we use **arp-scan** (Fig. 1.):

```
root@sif:/home/probii# arp-scan -l
Interface: wlan0, type: EN10MB, MAC: 00:13:02:e3:12:df, IPv4: 192.168.1.15
Starting arp-scan 1.9.7 with 32 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     e0[redacted]f0          [redacted] Ltd.
192.168.1.6     1[redacted]34           ASUSTek COMPUTER INC.
192.168.1.10    [redacted]              [redacted]
192.168.1.14    10[redacted]f:5b        SHENZHEN BILIAN ELECTRONIC CO., LTD
192.168.1.16    90:[redacted]17         Samsung Electronics Co.,Ltd
192.168.1.8     6[redacted]             [redacted] Company
192.168.1.7     a[redacted]c9           [redacted] Co Ltd

7 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 32 hosts scanned in 1.719 seconds (18.62 hosts/sec). 7 resp
onded
```

Fig. 1. *Scannig IP and MAC addresses*

The **arp-scan** tool gives us a simple view of devices IP and MAC addresses attached to the network. Also we can find data about the manufacturer. This can help us to find which devices is a camera. In this example we use cheap IP camera manufactured in China: ACME indoor camera IP1202 model.Fig.1.:device which was manufactured in Shenzen Bilian Electronic is highly possible our IP camera.

We need additional information to be sure that the we found the camera, and to attack it. For this purpose the kismet tool is used.

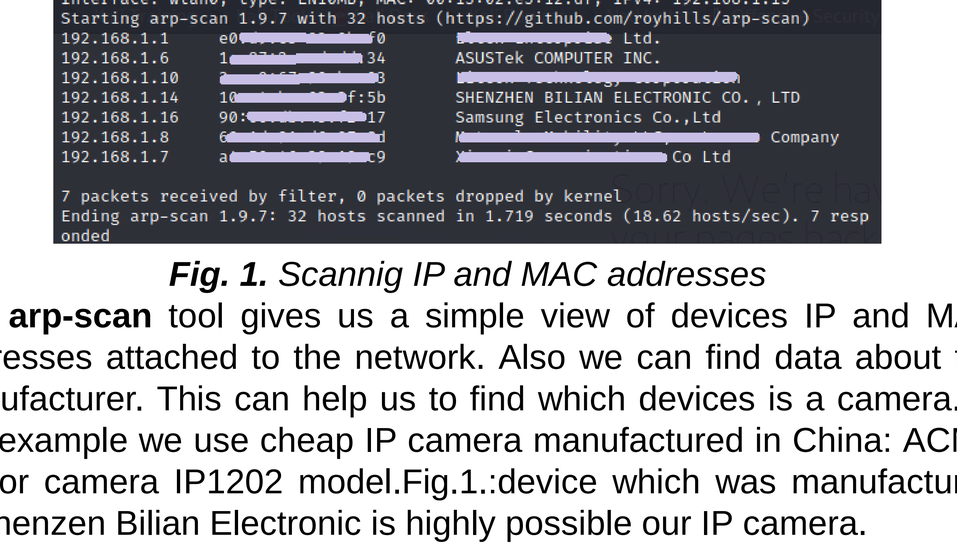

Fig. 2. *kismet tool*

In the terminal window type: **kismet -c wlan0mon**. NB: the wireless adapter should be in the monitoring mode (airmon-ng start wlan0). Open the http://localhost:2501 address in the browser to see data collected by the kismet, see Fig.2.

From data displayed by kismet, we can find which device is the camera and which is the access point, see Fig.3.

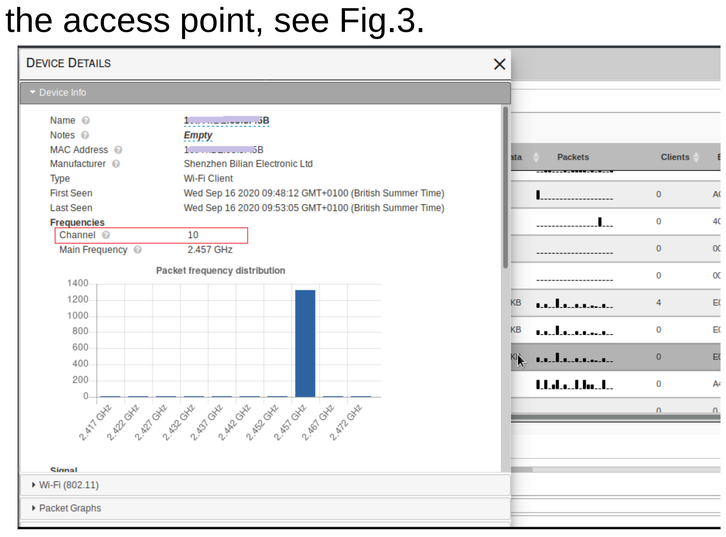

Fig. 3. *Data provided by kismet*

The data shows that the camera use channel 10 to communicate with the AP. The next figure shows an option when we filtered devices by MAC address. To attack only the camera, we must lock wlan0mon to focus on channel 10:

```
root@sif:/home/probii# airmon-ng start wlan0mon 10

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  400 NetworkManager
  511 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0mon        iwl3945         Intel Corporation PRO/Wireless 3945ABG [Go
lanl (rev 02)
```

Fig. 4. *Set wlan0mon to channel 10*

We will disable the camera, by send continuous stream of authentication packets (option -0 0):

```
aireplay-ng -0 0 -a B[redacted]F2 -c 1[redacted]5b wlan0mon
```

Fig. 5. *Attack the camera*

The first blured data is the MAC address of the Access Point, the second blured data is camera's MAC address. The stream of packets will disable the camera, and it will send only one (freeze) frame. Pressing CTL+C will stop the attack. It is also possible that the camera become operational again if it realize that it could communicate again with the network. Our camera didn't come back online. Reset was needed.

Conclusion

In kali linux there are tools which can be used for performing simple and effective attacks on the device which is on the same network as the attacker. We attacked an IP camera, by sending continuous stream of authentication packets. Because of authentication packets the camera was disabled, and it couldn't sent continuous frames.

Acknowledgement

We acknowledge the financial support of this work by the 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP Information Security Services Education in Serbia(ISSES)