

Laboratory 2: Unauthorized Access in Wireless Networks

Niclas Scheuing and Vasileios Dimitrakis

November 5, 2015

1 Introduction

In this laboratory exercise, we learn about and experiment on the weakness in various wireless security mechanisms. More specifically, in the first chapter, we hack the MAC filtering, in the second one, we crack the WEP encryption and in the last part, we break the WPA2 Personal Passwords.

2 Materials and Methods

Throughout the lab exercise 2 we used different materials and methods, that are presented below:

- *ifconfig*: Is used to configure the network interfaces.
- *hostapd*: Is a user space daemon for Access Point and authentication servers.
- *iwconfig*: Is used to configure the wireless network interfaces.
- *iwlist*: Is used to display some additional information from a wireless network interface that is not displayed by *iwconfig*
- *wireshark*: Is an open source packet analyser.
- *macchanger*: Is a Linux command that changes the MAC address of a network interface.
- *airodump-ng*: Is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with *aircrack-ng*.

- *aircrack-ng*: Is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured.
- *ping*: Is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer and back.
- *wpa_supplicant*: Is a cross-platform supplicant with support for WEP, WPA and WPA2.
- *aireplay-ng*: Inject ARP-request packets into a wireless network to generate traffic.

3 Terminology

The machine serving as wireless nodes is denoted by *User* and the machine used to attack the communication by *Attacker*. The machine used as access point is called *AP* in the following.

4 Experiments

In the following we will go through the experiments one by one and introduce the corresponding theory, setup and results.

4.1 Hacking MAC Filtering

MAC filtering is a security technique to prevent unauthorized users from accessing a wireless network. All network devices have a unique 48bit *MAC* address. The access-point grants or denies access to devices based on the *MAC* address communicated by the device itself. This is why a device can spoof the *MAC* address. For filtering black-lists and white-lists are used, granting access to devices contained in the white-list and denying access to those in the black-list.

4.1.1 Running the Experiment

AP used a white-list containing the *User's MAC* address, but not the *Attacker's*. The *AP* and the *User* were transmitting data.

To find the channel and *AP's MAC*, the *Attacker* used the *iwlist* tool. The *Attacker* is observing the communication running its Wifi adapter in

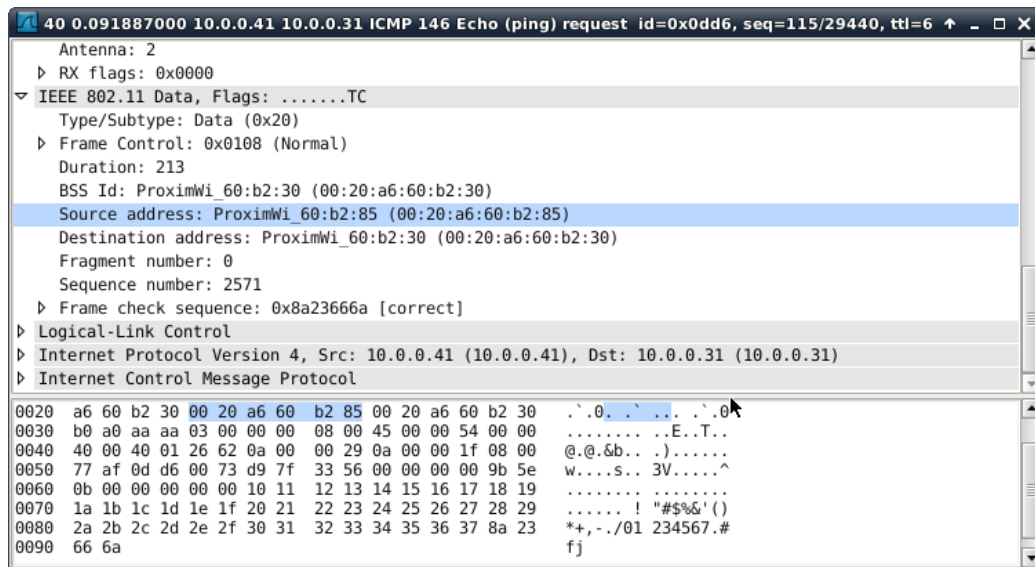


Figure 1: Finding the *User's* MAC address using *Wireshark*.

monitor mode and capturing the observed traffic with *Wireshark*. This way he was able to extract the *User's* MAC. See Figure 1

Knowing this *MAC*, the *Attacker* sets his own *MAC* address to the *User's* address using the *macchanger* tool. See Figure 2.

4.2 Cracking WEP Encryption

4.2.1 Setup

4.2.2 Results

4.3 Breaking WPA2 Personal Passwords

4.3.1 Theory

4.3.2 Setup

4.3.3 Results

5 Analysis

References

```
Terminal - station4@station4: ~
File Edit View Terminal Go Help

Channel:112
Frequency:5.56 GHz (Channel 112)
Quality=21/70 Signal level=-89 dBm
Encryption key:off
ESSID:"public-5"
Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
          36 Mb/s; 48 Mb/s; 54 Mb/s
Mode:Master
Extra:tsf=0000002780a5991b0
Extra: Last beacon: 1532ms ago
IE: Unknown: 00087075626C69632D35
IE: Unknown: 01088C129824B048606C
IE: Unknown: 050400010000
IE: Unknown: 070C43484924080F640510840310
IE: Unknown: 2D1AEE1103FFFFFF000000000000000000000000000000000000
0000000000
0
22F00
00000000000000000000
0000000000
IE: Unknown: 3D16700F0400000000000000000000000000000000000000000000
IE: Unknown: DD180050F2020101800003A4000027A4000042435E00623
IE: Unknown: DD1E00904C33EE1103FFFFFF0000000000000000000000000000
IE: Unknown: DD1A00904C34700F040000000000000000000000000000000000
root@station4:/home/station4# ifconfig wlan0 down
root@station4:/home/station4# macchanger wlan0 -m 00:20:a6:60:b2:85
Permanent MAC: 00:20:a6:60:b2:8c (Proxim Wireless)
Current MAC: 00:20:a6:60:b2:8c (Proxim Wireless)
New MAC: 00:20:a6:60:b2:85 (Proxim Wireless)
root@station4:/home/station4#
```

Figure 2: Changing the *Attacker's* MAC address using *macchanger*.