How to break into wireless LAN's enrypted with WEP/WPA

Giorgos (fedjo) Marinellis

Foss@Ntua

April 09 2012

Introduction

- **What's a wireless AP encryption?**
- A method to encrypt our network traffic and authenticate with APs and don't allow curious people see our packets
- **How is been achived?**
- In general ways the packet is encrypted with a secret key. Only users who have this key can decrypt packets.Other will see crap...

The old way of encryption - WEP 'encrypted' w-networks

- It's a very old encryption method based on cipher RC4 and CRC-32
- It is provided in to methods 64bit-WEP and 128bit-WEP (and 256-WEP) and they are recognized from a 40 bit or 104 bit key. These strings are concatenated with a 24bit Initialization Vector(IV) to form the RC4 key.

Authentication

- Two methods of authentication.Open System and Shared Key authentication
- In Open System auth. no auth. with the AP is done.Key is only for encrypting data frames
- In Shared Key auth. we have a 4-way handsake with the AP and then packet encryption
- The for steps are shown below

4-way authentication with AP

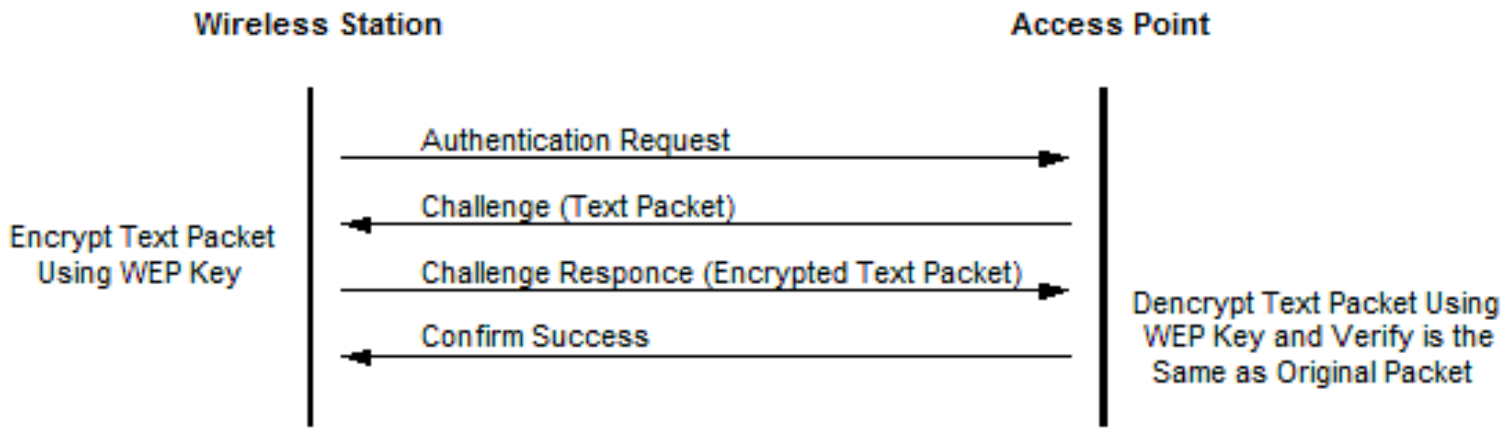


Figure 1: Example WEP Authentication

- Although it is not safer to use Shared Key auth. because keystream can be derived from the challenge packets

Protocol leakage...

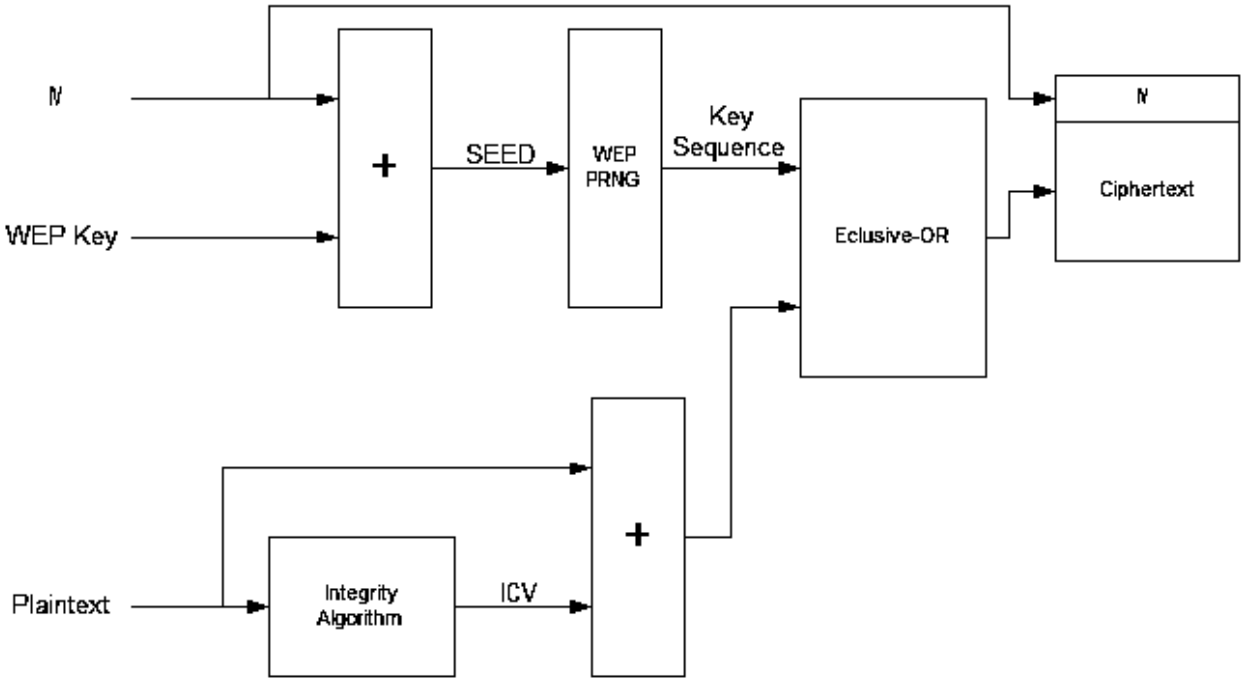


Figure 2: WEP Encryption

- Because RC4 is a stream cipher IV must not be repetead but for an 24bit IV there is a 50% probability the IV will repeat every 5000 packets.
- And this is where the party starts. Grabbing as many IVs from packets we can then crack the WEP key

Let's get started...

- **What we will need:**

Let's get started...

- **What we will need:**
- A wireless NIC with monitor mode

Let's get started...

- **What we will need:**
- A wireless NIC with monitor mode
- A packet sniffer

Let's get started...

- **What we will need:**
- A wireless NIC with monitor mode
- A packet sniffer
- Aircrack-ng

Enable monitor mode

Enable monitor mode

- **#: airmon-ng wlan0 start** as root
  (maybe a new virtual interface will appear)

Explore wireless networks and grab IV's

Explore wireless networks and grab IV's

- **$: airodump mon0** to see networks

Explore wireless networks and grab IV's

- **$: airodump mon0** to see networks
- **$: airodump mon0** $< output > < channel >$ **1** to start grab IV's

The procedure...

- As we can see airodump gives as a lot info about the network
- We can to collect at least 100.000 packets (under # Data)

```
BSSID              PWR  Beacons    # Data  CH  MB  ENC   ESSID

00:23:1F:55:04:BC   76    21995    213416   6  54. WEP   hackme

BSSID              STATION            PWR  Packets  Probes

00:23:1F:55:04:BC  00:12:5B:4C:23:27  112     8202  hackme
00:23:1F:55:04:BC  00:12:5B:DA:2F:6A   21     1721  hackme
```

Cracking procedure

Cracking procedure

- **$: aircrack-ng -a 1 -b** $< bssid >$ **-n** $< key - length >$ $< output.ivs >$
- There are several options you can use

Traffic problems

Traffic problems

- Because we may suffer from packet untraffic WE have to generate more traffic

Traffic problems

- Because we may suffer from packet untraffic WE have to generate more traffic
- That's why we use **aireplay**

ARP Injection

ARP Injection

- **$: aireplay -3 -b** $< APMAC >$ **-h** $< ClientMAC >$ **mon0**

Re-send all data attack

Re-send all data attack

- Ask AP to resend all packets. Some AP's re-encrypt them some use the same IV's

Re-send all data attack

- Ask AP to resend all packets. Some AP's re-encrypt them some use the same IV's
- **$: aireplay -2 -b** $< APMAC >$ **-h** $< ClientMAC >$ **-n 100 -p 0841 -c FF:FF:FF:FF:FF:FF mon0**

Fake Authentication

Fake Authentication

- Won't generate more traffic but it is uselful if there are no connected clients and we need to apply latter attacks

Fake Authentication

- Won't generate more traffic but it is uselful if there are no connected clients and we need to apply latter attacks
- It's easier if we have another station otherwise we must spoof ou MAC

Fake Authentication

- Won't generate more traffic but it is uselful if there are no connected clients and we need to apply latter attacks
- It's easier if we have another station otherwise we must spoof ou MAC
- **$: aireplay -1 30 -e** $<$ *ESSID* $>$ **-b** $<$ *BSSID* $>$ **-h** $<$ *NewMAC* $>$ **mon0**

The new trend WPA/WPA2-PSK

The new trend WPA/WPA2-PSK

- We'll talk about the PSK(Pre Shared Key) Personal edition

The new trend WPA/WPA2-PSK

- We'll talk about the PSK(Pre Shared Key) Personal edition
- There is a 2-way handsake authentication with the AP based on a secret key that each client must know

Let's go deep

Let's go deep

- The AP generates PMK(Pairwise Master Key) from PSK and ESSID and ESSID length hashed 4096 times with SHA-1

Let's go deep

- The AP generates PMK(Pairwise Master Key) from PSK and ESSID and ESSID length hashed 4096 times with SHA-1
- Each time a client going to associate with the AP generates it's PMK

The handshake

The handshake

- The AP sends to the client a random number called ANonce

The handshake

- The AP sends to the client a random number called ANonce
- The client also generate it's random number called SNonce and mixes the PMK, ANonce, SNonce, MAC_AP, MAC_Client and generates a 512 byte number called PTK

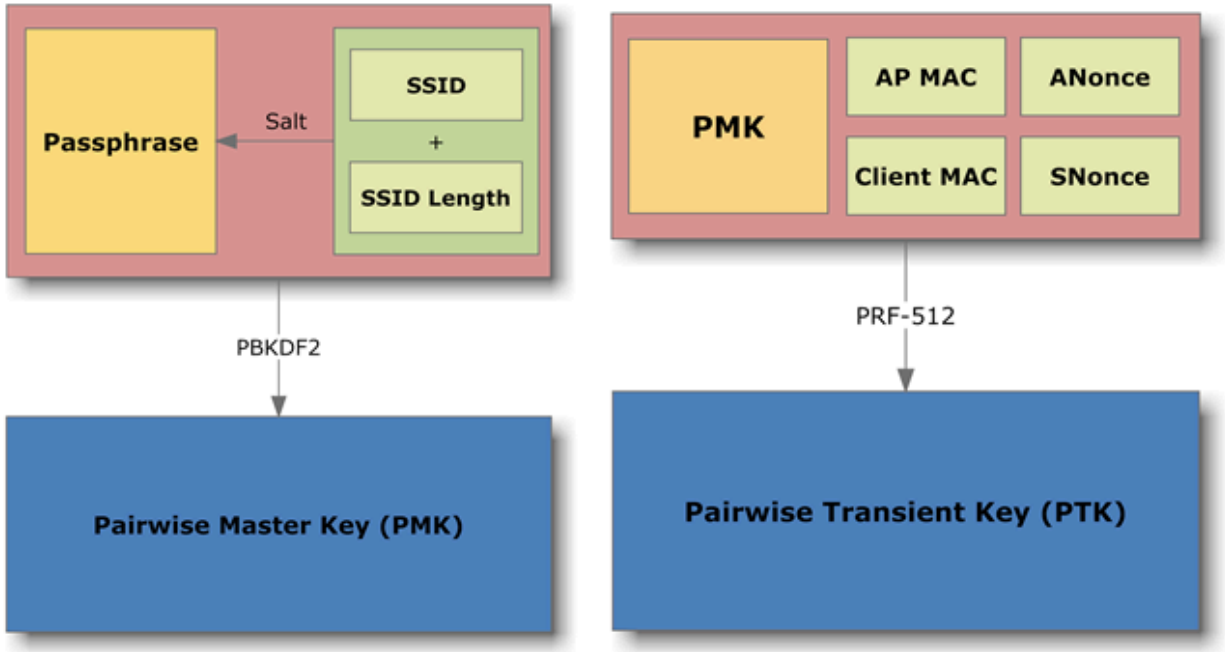
The handshake

- The AP sends to the client a random number called ANonce
- The client also generate it's random number called SNonce and mixes the PMK, ANonce, SNonce, MAC_AP, MAC_Client and generates a 512 byte number called PTK
- Then encrypts SNonce with PTK(MIC digital sign) and sends both SNonce and MIC to AP

The handshake

- The AP sends to the client a random number called ANonce
- The client also generate it's random number called SNonce and mixes the PMK, ANonce, SNonce, MAC_AP, MAC_Client and generates a 512 byte number called PTK
- Then encrypts SNonce with PTK(MIC digital sign) and sends both SNonce and MIC to AP
- If the AP can match this 2 numbers then we have authentication

The new trend WPA/WPA2-PSK



Where is the problem...?

Where is the problem...?

- We can sniff during authentication SNonce, ANonce, MIC

Where is the problem...?

- We can sniff during authentication SNonce, ANonce, MIC
- Then with bruteforcing we can use all available passphrases to check...!

Where is the problem...?

- We can sniff during authentication SNonce, ANonce, MIC
- Then with bruteforcing we can use all available passphrases to check...!
- But this is an extremely long procedure

For instance

For instance

- We can use rainbow tables with precomputed PMK's for each different ESSID

For instance

- We can use rainbow tables with precomputed PMK's for each different ESSID
- This is also a very heavy procedure but...

For instance

- We can use rainbow tables with precomputed PMK's for each different ESSID
- This is also a very heavy procedure but...
- we can base on peoples awareness not changing the default SSID and PSK

For instance

- We can use rainbow tables with precomputed PMK's for each different ESSID
- This is also a very heavy procedure but...
- we can base on peoples awareness not changing the default SSID and PSK
- There are rainbow tables free on the internet which you can use