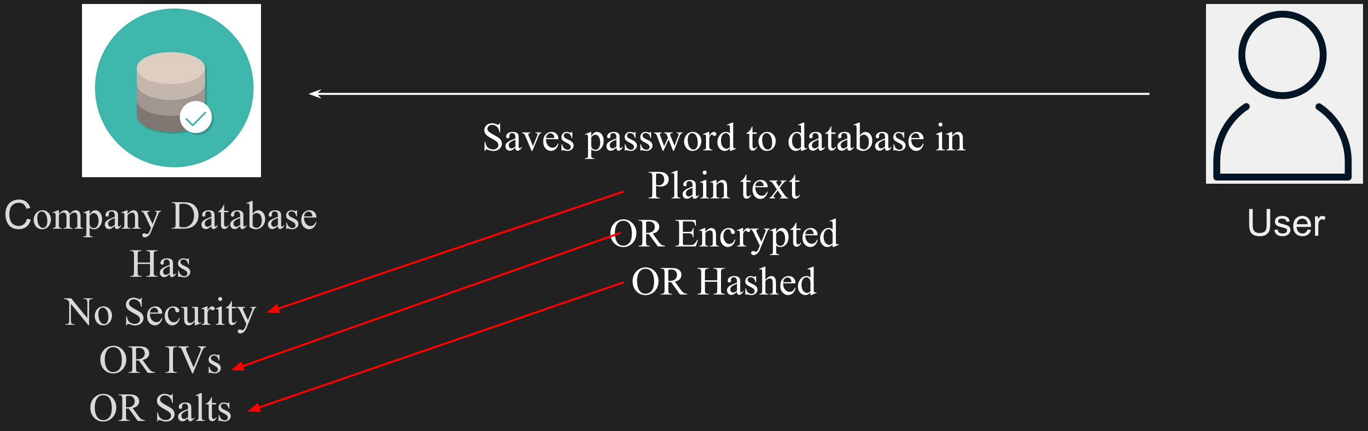
Introduction

In this series of videos, I will be demonstrating how the Wireless WPA2 Personal Password cracking works. To do that, We will discuss some common practices of How Password is Stored or Shared. How and Where to and not to Store Passwords. How to verify password and Authenticate by not sharing a password over the wire or wireless at all. We will be talking on a high level about Hashes, The differences between Hash and Encryption, Types of Hashes used in practice, Where to use what type of Hashes. And after that, We will see how each of the aforementioned concepts are used exactly to create a WPA2 Password. Then we will be able to deconstruct how exactly Wifi Hacking (WPA2 Personal) works ...

Password Storage



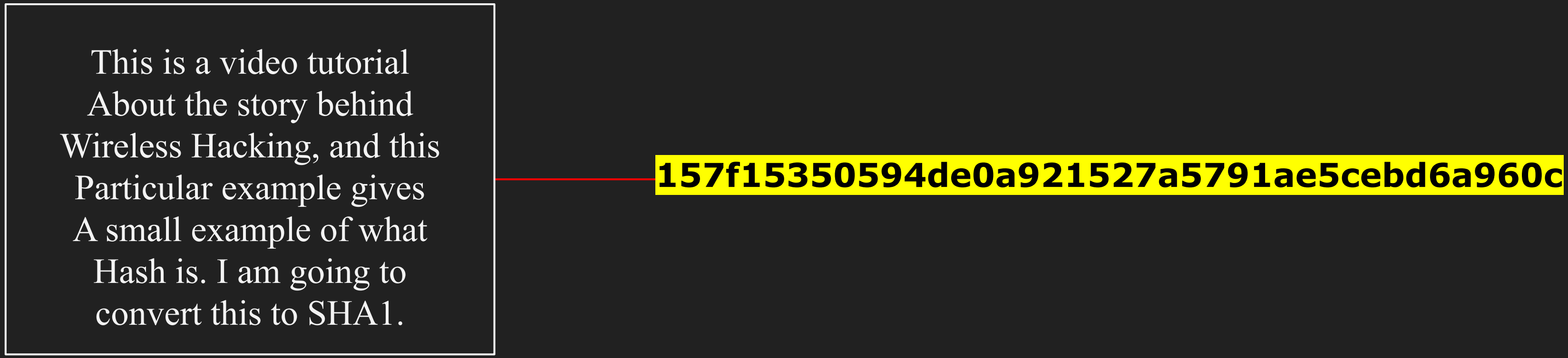
Saves password to database in
Plain text
OR Encrypted
OR Hashed

Company Database
Has
No Security
OR IVs
OR Salts

User

Hashing

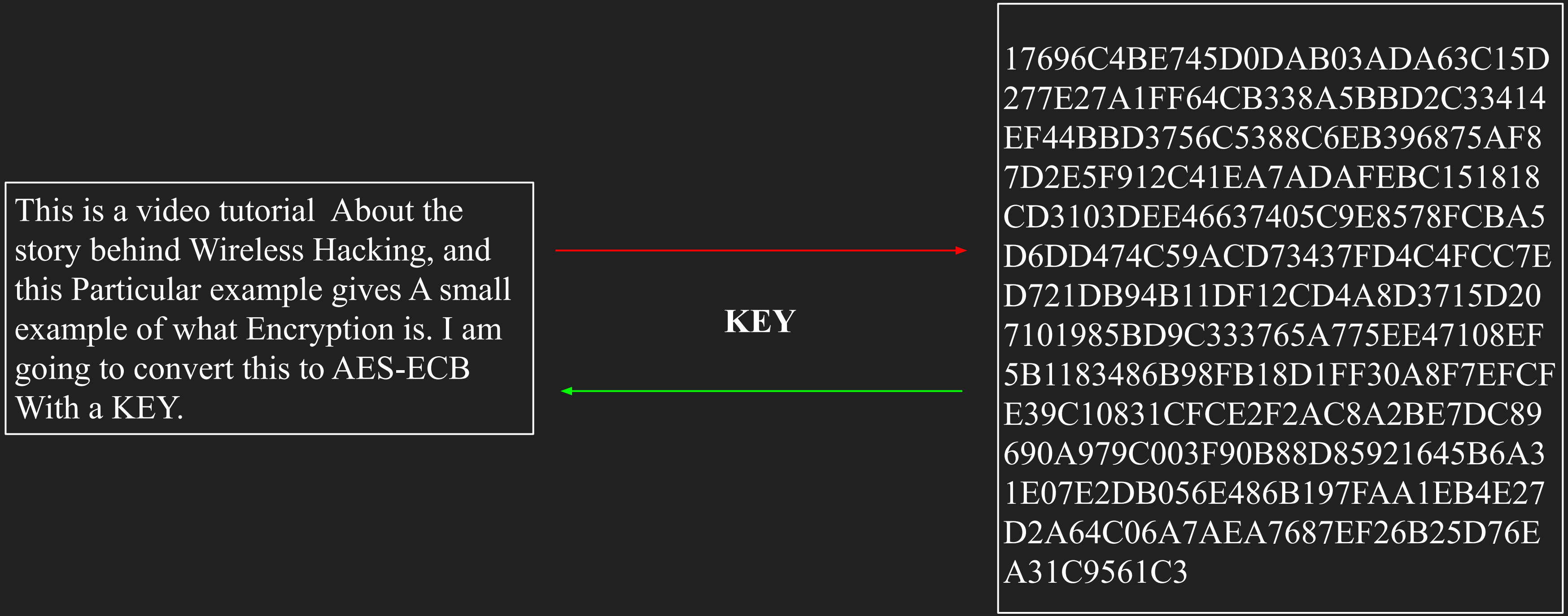
SHA1



This is a video tutorial About the story behind Wireless Hacking, and this Particular example gives A small example of what Hash is. I am going to convert this to SHA1.

157f15350594de0a921527a5791ae5cebd6a960c

Encryption
AES-ECB



This is a video tutorial About the story behind Wireless Hacking, and this Particular example gives A small example of what Encryption is. I am going to convert this to AES-ECB With a KEY.

KEY

```
17696C4BE745D0DAB03ADA63C15D
277E27A1FF64CB338A5BBD2C33414
EF44BBD3756C5388C6EB396875AF8
7D2E5F912C41EA7ADAFEBC151818
CD3103DEE46637405C9E8578FCBA5
D6DD474C59ACD73437FD4C4FCC7E
D721DB94B11DF12CD4A8D3715D20
7101985BD9C333765A775EE47108EF
5B1183486B98FB18D1FF30A8F7EFCF
E39C10831CFCE2F2AC8A2BE7DC89
690A979C003F90B88D85921645B6A3
1E07E2DB056E486B197FAA1EB4E27
D2A64C06A7AEA7687EF26B25D76E
A31C9561C3
```

HMAC

Hashed Keyed Message Authentication System

$$h(k \mid\mid h(k \mid\mid m))$$

A bit time consuming to break, and very secure means to verify authenticity and integrity of the message that the hash is representing.

PBKDF2

Password Based Key Derivation System

(PRF, word, salt, dklen, iterations)

The hash from the previous Loop (Not first time) is used as the Message for the next loops

PBKDF2 in WPA2

The birth of Pairwise Master Key

(HMAC - SHA1, Wpa2 Password, SSID, 256, 4096)

The result is what we call the Pairwise Master Key

The birth of Pairwise Transient Key

$$\mathrm{PTK} = \mathrm{HMAC} - \mathrm{SHA1}(\mathrm{PMK}, \mathrm{ANonce} \,||\, \mathrm{SNonce} \,||\, \mathrm{Amac} \,||\, \mathrm{STmac})$$

The result is what we call the Pairwise Transient Key

The birth of Message Integrity Code

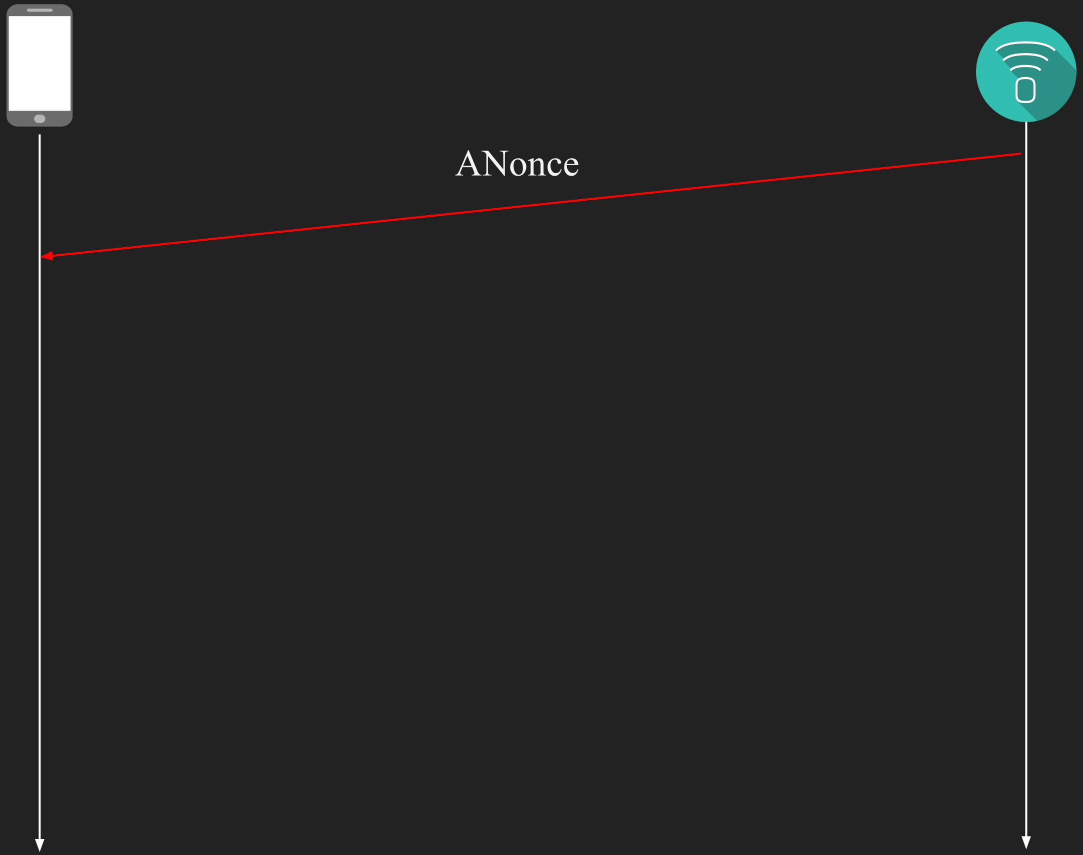
MIC = HMAC - SHA1(KCK, Payload(EAPOL - 2nd message and header info))

The result is what we call the Message Integrity Code

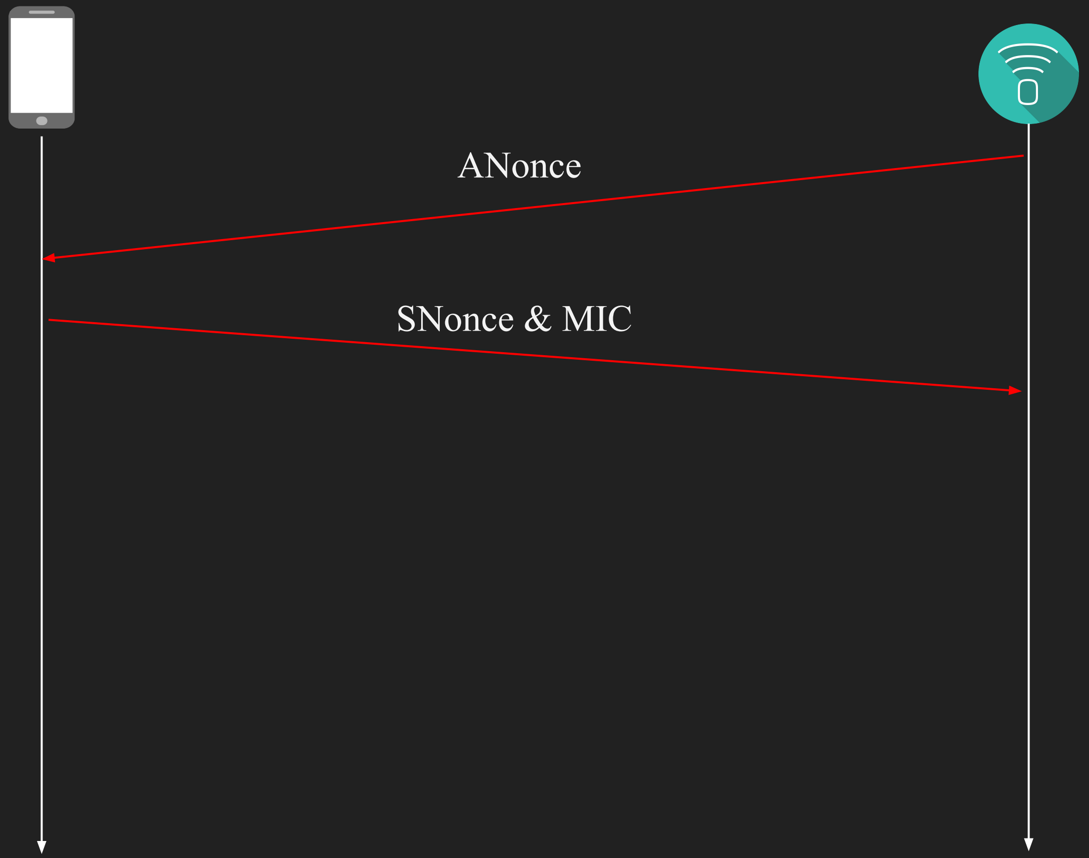
The 4 way handshake

In this segment, we are going to talk about the few key ingredients among many of them that occurs when we first type in our WiFi Password and click ‘Connect’. The same concept is broken down and used when we perform an attack to get the WPA2 Password as well. So understanding this part is pretty important. We will go from message 1 to 4 on the following pages respectively.

Message 1/4



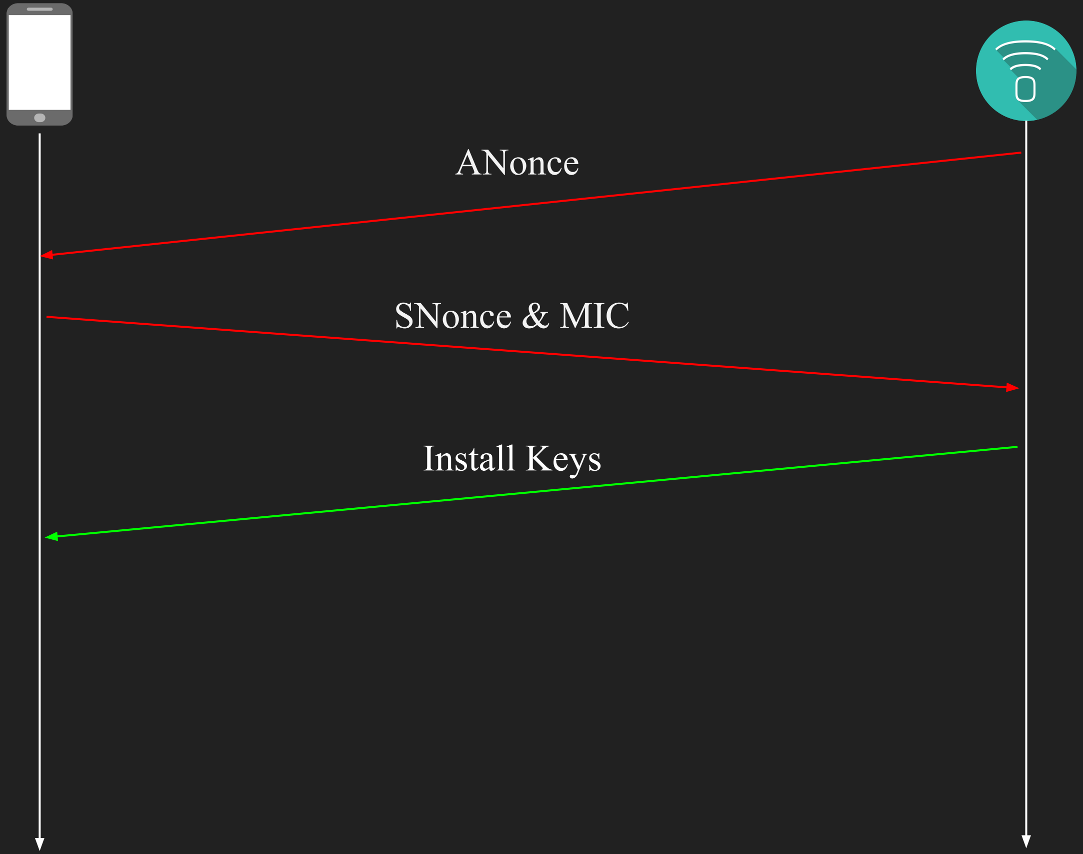
Message 2/4



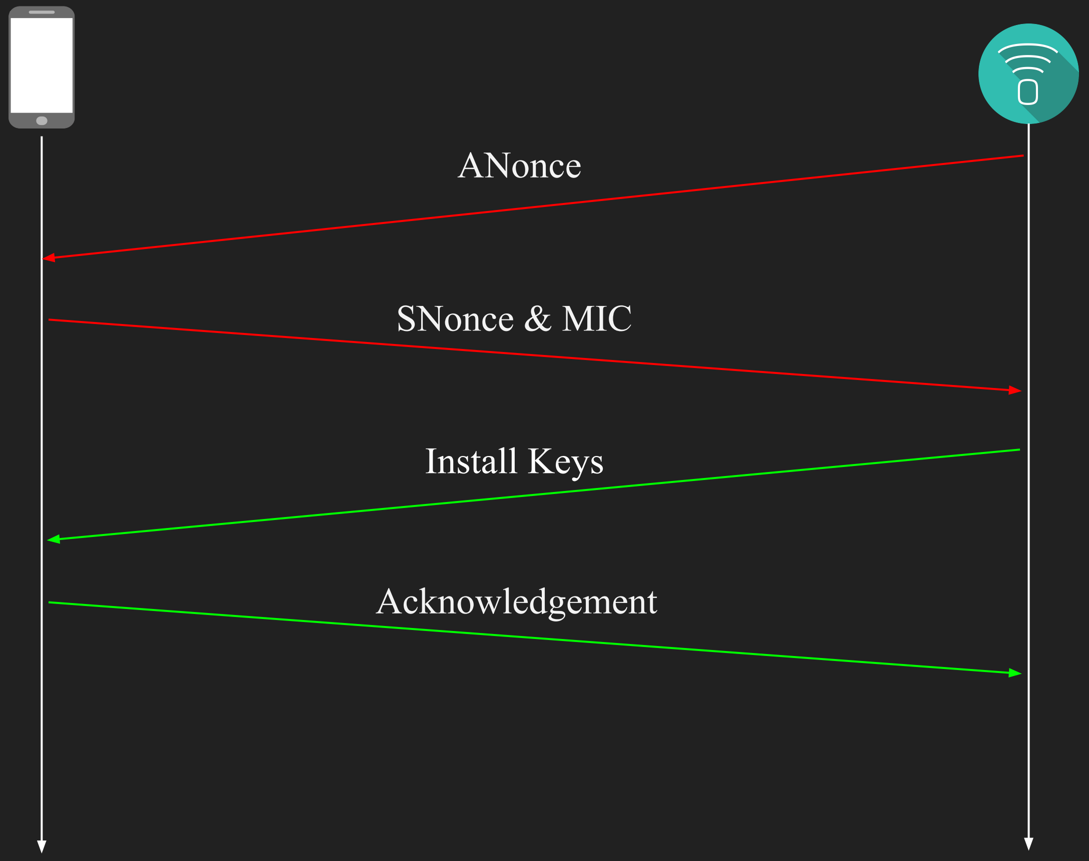
ANonce

SNonce & MIC

Message 3/4



Message 4/4



ANonce

SNonce & MIC

Install Keys

Acknowledgement

Cracking WPA2 Practicals

Now we will move on to the Practicals, where I show you the handshake, and break the Key using the concepts explained earlier. An overview of the command as follows.

airmon-ng - Puts the wireless adapter into Monitor mode
airodump-ng - Used to sniff out the Air and for Targeted sniffing
aireplay-ng - Used for replay and deauthentication attacks
aircrack-ng - Used to actually perform the Bruteforce Attack
airbase-ng - Used to create a fake Access Point
Wireshark - Used to analyze the traffic with naked eyes

AP less Attacks (Assignment)

Like we discussed all the processes before, The same would be used if you wanted to do the same attacks without even the Access Point present. The way you can do that is by Creating a fake access point with ‘airbase-ng’ with the same SSID as the client was previously connected. The rest of the process is exactly identical. You can fetch the name of the AP by sniffing the probe requests from the un associated target supplicant for trying to connect with the previous AP.

The End

In a nutshell, We have learnt about a bit of Encryption, Hashing, HMACs, Key Derivation, How all of these mechanisms are used in WPA2 handshake process, And how to break it. I hope you have come to know the knitty bitty bits of the whole process instead the very high level abstracts of the actual process.
This concludes the “Behind The Scenes” of WPA2 hacking. Hope to see you in the future.

Thank You