

Ultra secret chat using Wi-Fi covert channel

Data exfiltration inside
802.11 protocol frames





About @yadox

Ethical hacker, expert in network engineering and system administration, with extensive experience in network infrastructures of all sizes. During his professional career, he has carried out international projects for large corporations in the banking, insurance, telecommunications, and Government security sectors among others.

In recent decades he has specialized extensively in wireless technologies, successfully leading numerous projects for security planning, implementation and auditing. With his company (WiFense), he has developed an interception system for one of the largest global intelligence corporations based in Israel. In the field of cybersecurity, he carries out regular interventions for the press, as well as lectures and training cycles in various universities and congresses.

Co-founder of Mundo Hacker, a team with which he has broadcasted programs on radio, streaming, podcast, conferences, as well as shows on public TV (Telecinco, Discovery Max, TVE La Dos and Channel Trece in Colombia). He published numerous publications and articles in specialized magazines, also collaborating with Ra-Ma editorial, through which he has written and published several books on computer security. For some years now, he has been a regular security trainer for intelligence, defense and national security services for many international governments.

Definitions



Data exfiltration: *defines the act of extracting and transferring information from computer systems without authorization of the owners.*

- *Requires physical access or network access*
- *Used to steal or leak information*
- *Requires strict data access prevention and DLP techniques*
- *In Governments and secure corporate environment is difficult to succeed*
- *Used in recent data leaks*
- *Traditional methods and more creative methods*

Definitions

Covert Channel *[Wikipedia]: a covert channel is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.*

- *When the main channels are secure, data exfiltration gets difficult*
- *Information hiding using overt channels. Hidden channels*
- *Shared resource for sender and receiver. Synchronization.*
- *Elude standard hardware, firmware, software (drivers)*
- *Taking advantage of technology and standards.*
- *Channel undetectable / un-interceptable*
- *Sniffing and recognizing patterns*
- *Data obfuscation and encryption*

Requirements

Hardware

Wi-Fi monitor mode adapter. ALFA AWUS-036NHA

OS

Linux OS, Kali Linux (recommended)



Python (2-3)

Hacking language for excellence

Scapy python library

Dot11 class

Packet manipulation library

DEMO

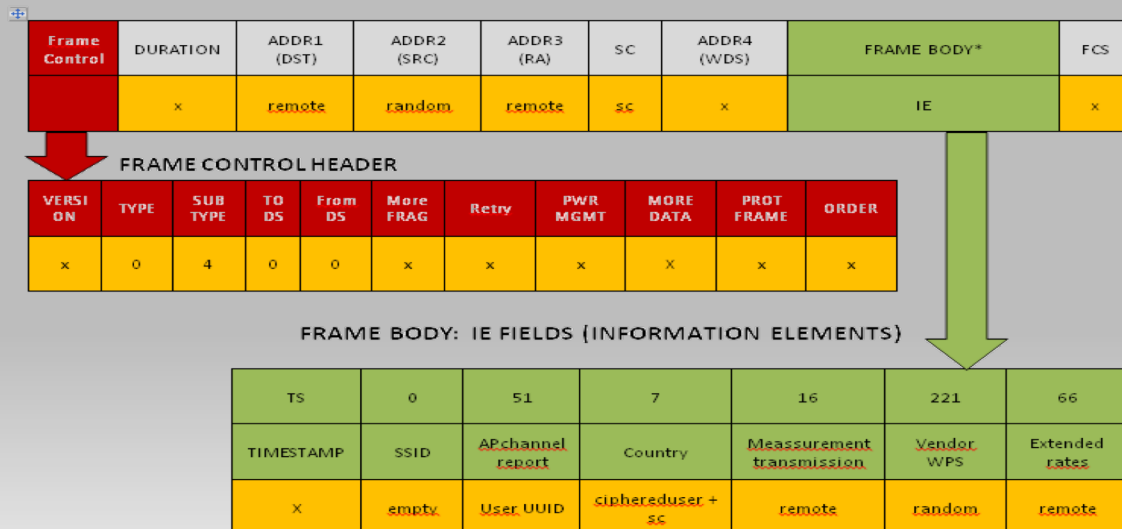
A bit of theory

802.11 PROTOCOL (description)

Layer 2 protocol

Network protocols structure (frame struct)

802.11 PROBE REQUEST FRAME



What is 802.11?



Wireshark reviewing packets

Using specific packet filters

Dissecting protocol

Checking for errors

The screenshot shows the Wireshark interface with a packet capture of IEEE 802.11 traffic. The packet list pane shows four packets, all of type 802.11. Packet 113 is selected, and the packet details pane shows the structure of the IEEE 802.11 wireless LAN management frame, including the Tagged parameters section. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
111	7.405818	2d:f4:1d:d2:96:4e	68:69:61:6c:6c:68	802.11	123	Probe Request, SN=41, FN=8, Flags=....., SSID=Broadcast
112	7.407008	c3:01:46:ed:81:70	68:69:61:6c:6c:68	802.11	123	Probe Request, SN=41, FN=8, Flags=....., SSID=Broadcast
113	7.409551	b9:19:3c:73:d1:60	68:69:61:6c:6c:68	802.11	123	Probe Request, SN=41, FN=8, Flags=....., SSID=Broadcast
114	7.410802	cc:2a:06:a8:e1:cd	68:69:61:6c:6c:68	802.11	123	Probe Request, SN=41, FN=8, Flags=....., SSID=Broadcast

Frame 113: 123 bytes on wire (984 bits), 123 bytes captured (984 bits)

- Radiotap Header v0, Length 8
- IEEE 802.11 Probe Request, Flags:
- IEEE 802.11 wireless LAN management frame
 - Tagged parameters (91 bytes)
 - Tag: SSID parameter set: Broadcast
 - Tag: AP Channel Report: Operating Class 52, Channel List :
 - Tag: Country Information: Country Code Na, Environment Unk
 - Tag: Challenge text
 - Tag: Vendor Specific: 36:69:35
 - Tag: Measurement Pilot Transmission: Undecoded

```
0000 00 00 08 00 00 00 00 40 00 00 00 68 69 61 6c ..... @..hial
0010 6c 68 b9 19 3c 3a ce 60 68 69 61 6c 6c 68 98 02 lh.<.: hiallh..
0020 00 00 33 07 34 65 39 65 30 65 36 07 18 4e 61 79 ..3.4e9e 0e6..Nay
0030 69 37 6e 50 7a 71 2b 77 2b 58 6f 58 45 5a 68 65 17nPzqt+w +XoXEZhe
0040 73 4e 51 3d 3d 10 18 72 64 70 63 51 70 33 62 44 sNQ==..r dpcQp3bD
0050 52 68 5a 47 47 33 56 67 49 76 73 61 77 3d 3d dd RhZGG3Vg Ivsaw==.
0060 18 36 69 35 56 38 47 66 74 79 38 39 78 46 78 51 .6i5V8Gf ty89xFxQ
0070 48 48 56 50 33 67 77 3d 3d 42 00 HHVP3gw= =B.
```

DEMO

Tipos de trama	Filtro Wireshark
Tramas de gestión	wlan.fc.type eq 0
Tramas de control	wlan.fc.type eq 1
Tramas de datos	wlan.fc.type eq 2
Association request	wlan.fc.type_subtype eq 0
Association response	wlan.fc.type_subtype eq 1
Reassociation request	wlan.fc.type_subtype eq 2
Reassociation response	wlan.fc.type_subtype eq 3
Probe request	wlan.fc.type_subtype eq 4
Probe response	wlan.fc.type_subtype eq 5
Beacon	wlan.fc.type_subtype eq 8
Disassociate	wlan.fc.type_subtype eq 10
Authentication	wlan.fc.type_subtype eq 11
Deauthentication	wlan.fc.type_subtype eq 12
WPA handshake	eapol

Code revision

Protocol manipulation with Scapy

Type of frames to use

Channel, MAC, encryption key calculation

try:

```
print "===== "  
print "    SECRET AND HIDDEN CHAT VIA WI-FI COVERT CHANNEL    "  
print "===== "  
print "Welcome to Hidden Wi-Fi Chat! Enter :exit: to exit if you wish!"  
print "===== "  
  
# Ask for monitor mode interface  
interface = raw_input("Enter your Wi-Fi interface [%s]: " %defaultinterface)  
if interface == "": interface=defaultinterface  
if not InitMon(interface): exit(-1)  
  
# Asks for the alias of the user  
username = raw_input("Enter your User name or alias: ")  
if username == "": exit()  
if username[0] == " ": exit()  
uuid = md5(getmac(intfmon))[7:14]  
userlist[uuid]=username
```


Demo time

<https://github.com/yadox666/>

```
root@laptop386:/home/yadoxusr/Descargas/raspberry/WiFi_CCC# python wifichat.py
=====
SECRET AND HIDDEN CHAT VIA WI-FI COVERT CHANNEL
=====
Welcome to Hidden Wi-Fi Chat! Enter :exit: to exit if you wish!
=====
Enter your Wi-Fi interface [wlan0]: wlan0
Enter your User name or alias [yadox]: yadox
Define private IRC channel name [yadox]: yadox
Setting mon1 to channel: 9 (5)
Just write and press enter to send!

bob: hi
bob: how are you
█
```

DEMO

Conclusions & Questions

- Detection and avoidance
- Difficulties
 - Hardware, Drivers, Monitor mode, encryption
- Anti detection techniques
- Want more info?
 - Ask for Python Scapy Dot11 book.



Don't forget
to visit our **stand**
in the hacking
armory section.

You'll discover
all the
Hacking tools
you need

