WISEflow
Europe/Copenhagen(CEST)
01 Jun 2018

Erhvervsakademi Sjælland

Specialiseringsprøve

Prædefineret information

Startdato:	16-03-2018 09:00	Termin:	jun 2018
Slutdato:	01-06-2018 13:00	Bedømmelsesform:	Dansk 7-trinsskala
Eksamensform:	Produkt, fremlægning + forsvar	ECTS:	30
SIS-kode:	259410 0618 ro16da2a4-4o 71224 - PRO EKS 7TRIN		
Intern bedømmer:	Mohammad Homayoon Faye		
Intern bedømmer:	Michael Claudius		

Deltager

Navn:	Paulius Klezys
Kandidatnr.:	
UNI-C ID:	
Alt. id:	
EASJ-id:	

Man-in-the-Middle Attack on the Link Layer

Student: Paulius Klezys

Supervisor: Mohammad Homayoon Fayez

Semester: 4th semester, IT security

Project period: 01-05-2018 – 01-06-2018

Erhvervsakademi Sjælland

Campus Roskilde

May 2018

Table of contents

Introduction

Motivation

I choose to write about this specific cyber-attack, because I find it to be very relevant to every person in this world, as privacy is the most important thing when it comes to browsing on the internet and elsewhere. More and more people start using communication devices to reach out to the world, consequently it is getting harder and harder to maintain privacy – most of the time they must rely on third party to keep their privacy. Not only that, cyber attacks bring huge losses to the companies and individuals. Many, including me, come to think, what does it take to protect from one?

To protect from the attack, you must know how it works. In this synopsis, I will be thoroughly explaining how Man-in-the-Middle attack, on the Data link layer of OSI model, works. My target will be my own Access point – my Wi-Fi router. To perform the attack, I will also need machine running Kali Linux and a special network card. I will be using Alfa AWUSO36NH network card.

Problem definition

How secure today's Wi-Fi access points are and how can we protect its traffic from being intercepted by the third party?

In addition, to answer the main question thoroughly, the following question arise:

1) Are today's cryptography techniques capable of making the data completely secure?

Planning

I have very strict week schedule and I know when I will be doing what, but I need to plan my work on synopsis, so I wouldn't fall back by procrastinating and later ending up not doing things the right way. I will plan what should be done each week, what is possible to be done in a week and when I should work.

The initial plan looks like this:

Week 1 (1 – 7 May)	Week 2 (7 – 14 May)	Week 3 (14 – 21 May)	Week 4 (21 – 31 May)
Introduction and planning	Writing about methods	Performing the attack again and taking screenshots	Writing synopsis conclusion
Setting up environment to perform attack on	Working on main body of the synopsis	Documenting the process of the attack	Making power point slides for oral exam
Gathering information for the best approach	Performing the attack to see if everything works	Finishing main body of the synopsis	Preparing in front of mirror or friends

Purpose and goal

The purpose and goal of this synopsis is for me to learn how to perform this attack and how to prevent it from happening, or at least lower the risks. For the one who reads this, to know how attack works and be aware of it, know how to protect from it. This synopsis should give a thorough understand of how data from Wi-Fi access point can be intercepted and decrypted from the beginning to the end.

Man-in-the-Middle (MitM) attack is an attack where the attacker possibly alters and relays the communication between two parties. These parties are not aware of an attack.

Methods

To conduct my research on this Man-in-the-Middle Attack, I will use the following methods:

1) Reading articles about tools necessary to perform MitM attack, how to use them and what functions do they provide. I need to know what they have to offer, because there are many variables that change approach to the attack.

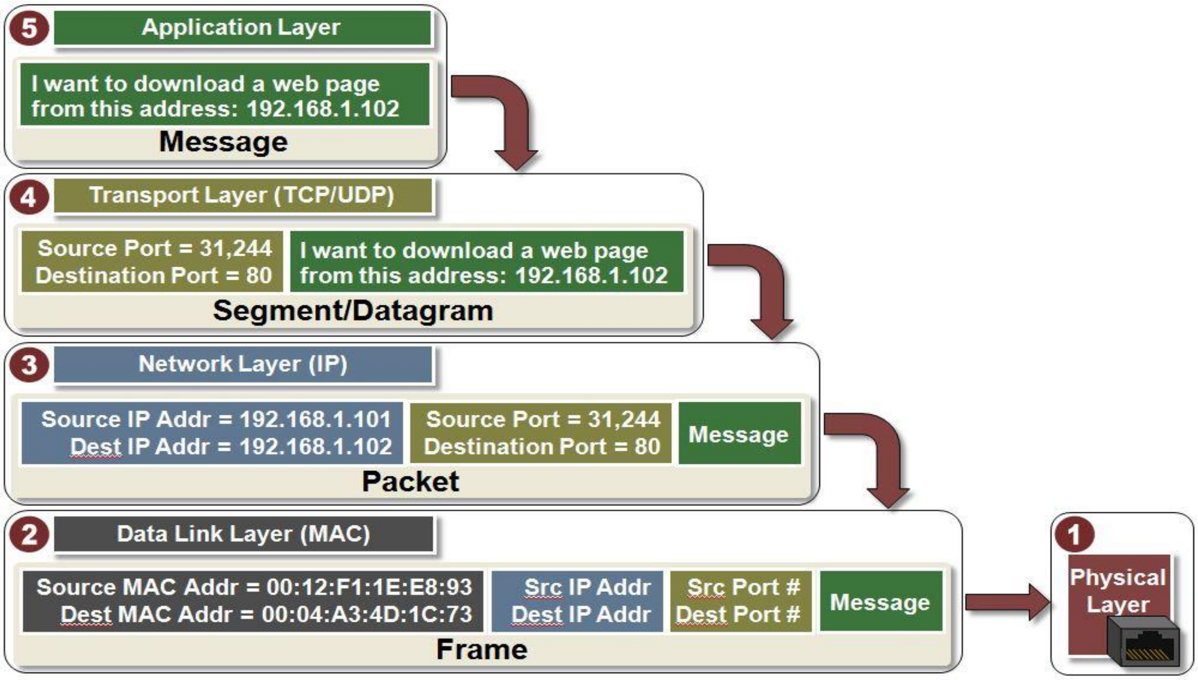
2) Setting up testing environment for the attack, as doing so on any other network without permission is illegal. Also, in the end, data from the attacker's machine and testing environment must be compared to see if attack was successful.

3) Performing live attack on my own testing environment. Learning by doing.

Answer to a problem

Understanding frames

The attack will be mostly focusing on the second layer of OSI model – Data Link Layer. Data Link Layer Encapsulates every other layer and its Protocol Data Units: messages, segments/datagrams, packets and then puts it into the frames. After that, frames are sent and received between the router and a client connected to it.


5
Application Layer
I want to download a web page from this address: 192.168.1.102
Message
4
Transport Layer (TCP/UDP)
Source Port = 31,244
Destination Port = 80
I want to download a web page from this address: 192.168.1.102
Segment/Datagram
3
Network Layer (IP)
Source IP Addr = 192.168.1.101
Dest IP Addr = 192.168.1.102
Source Port = 31,244
Destination Port = 80
Message
Packet
2
Data Link Layer (MAC)
Source MAC Addr = 00:12:F1:1E:E8:93
Dest MAC Addr = 00:04:A3:4D:1C:73
Src IP Addr
Dest IP Addr
Src Port #
Dest Port #
Message
Frame
1
Physical Layer

OSI 5 LAYER MODEL

There are various multi-stage attacks that must be done in order to get and decrypt the data from a client connected to the access point. First of all, there are very strict functional restrictions in Wi-Fi networks. To get most control over it, a special network card is required. This special card has custom firmware and chipset, which allows us to enter monitor mode and do packet injection.

Monitor mode allows to listen to any communication in the air, but it doesn't allow to send data at the same time. However, packet injection allows us to send the data[1]. Combining monitor mode with packet injection let us capture and send the data at the same time.

The usage of my Alfa AWUSO36NH network card will be to intercept frames that are not meant for my network card. That is frames, that possess encapsulated data being sent to someone else.

[1] https://security.stackexchange.com/questions/76983/what-is-the-need-and-purpose-of-packet-injection-within-wifi-attacks?utm_medium=organic&utm_source=google_rich_qa&utm_campaign=google_rich_qa

802.11 IEEE

To be able to send data to the router one must authenticate and associate with it by exchanging 802.11 management frames. 802.11 IEEE wireless LAN standard specifies an over-the-air interface (communication link) between a wireless client and a base station or between two wireless clients.

Authentication frame

When it comes to authentication, there 2 types of authentications: open system authentication and shared key authentication (PSK). Open system authentication does not require a key; therefore, it does not support data encryption. Shared key authentication requires a key, which is manually set on router and connecting client – it is Wi-Fi passphrase. This Wi-Fi passphrase will later be used by the algorithm to make encryption key during the handshake process when the client is connecting to the router.

Association frame

After authentication, to gain full access to the network client must associate. Association guarantees proper frame delivery from router to associated clients.[2]

Preparation for the attack

Before launching MitM attack, I must analyze the Access Point and its network to see how secure it is, and which attack against it would be the most time-efficient. The main purpose to attack the router is to retrieve the passphrase used to connect to the Wi-Fi network. This passphrase is used by the encryption algorithm to make encryption key and encrypt the data sent between the client and the router. The router's passphrase security will depend on the strength of an algorithm.

Encryption algorithm depends on used network authentication method and there are quite a few of them. Some of them are considered to be outdated due to their inability to provide strong encryption, which leads security issues such as compromised router.[3]

[2] https://www.intel.com/content/www/us/en/support/articles/000006508/network-and-i-o/wireless-networking.html

[3] https://www.cisco.com/c/en/us/support/docs/wireless-mobility/80211/200527-Fundamentals-of-802-11-Wireless-Sniffing.html

Short overview of existing Wi-Fi security protocols, their authentication methods and its encryption algorithms:

Wired Equivalent Privacy (WPA). Uses RC4 stream cipher and 64-bit or 128-bit keys – It is very insecure because of its 24-bit initialization vector used in encryption and weak authentication. Can be easily hacked in under 2 minutes.

Wi-Fi Protected Access (WPA). Uses the same RC4 based cryptosystem – It is more or less the same us WPA but adds longer initialization vectors and 256-bit keys. Each client gets new unique key with TKIP. TKIP implements key mixing function combined from the secret root key before passing it to the RC4 cipher initialization. As of today, it is outdated and not very secure.

Wi-Fi Protected Access 2 (WPA2). Uses AES (Advanced encryption standard) and CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) – Replaces old RC4 and TKIP with much stronger and efficient CCMP and AES algorithms for stronger authentication. AES is for encryption and CCMP is designed for data confidentiality. AES offers 128, 192 or 256-bit encryption. Even 128-bit is theoretically being unbreakable.

Wi-Fi Protected Access 3 – To be released in 2018 as WPA2 is no longer that secure to be reliable.

Wi-Fi Protected Setup – this is just authentication method on top of already existing authentication method. There is a serious flaw found, where its PIN can be brute-force attacked and retrieved within a couple of hours. From this PIN, Wi-Fi passphrase can be easily retrieved

For authentication there can be 2 types: PSK (Pre-Shared Key) or Open System – PSK is manually set on the router and the client and it is used to make unique, temporary encryption keys for each session. Open system requires no keys, can only use WEP encryption, or no encryption at all.[4]

As new encryption algorithms, authentication methods are being created, the problem of legacy support appears. Not all devices support newest authentication methods or encryption methods. Nowadays most of the routers have mixed modes like WPA-AES, WPA2-TKIP and so on. Also, it is known that using TKIP will slow down network to ensure compatibility with older devices.[5]

[4] https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/

[5] https://www.makeuseof.com/tag/wpa2-wep-and-friends-whats-the-best-way-to-encrypt-your-wi-fi/

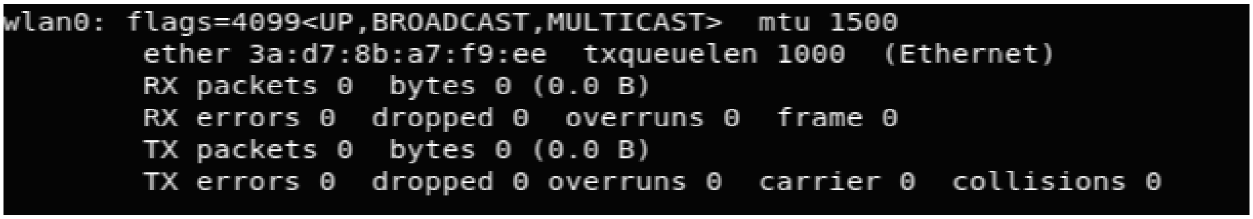
Performing the attack

I will begin the attack by attacking my own router to retrieve its Wi-Fi passphrase.

Entering monitor mode

The first step is to is to run Alfa AWUSO36NH network card into monitor mode on Kali Linux to see all routers and access points that are nearby and what authentication and encryption method they are using.

I will have to find the name of the network card that will be used. To do that, I have to type in the terminal window: ***ifconfig***. In my case, it is ***wlan0*** – it's the network card that I will have to turn into monitor mode. It is done by running the following command: ***airmong-ng start wlan0***. Airmong-ng is a tool that helps managing Wi-Fi network devices and its drivers.



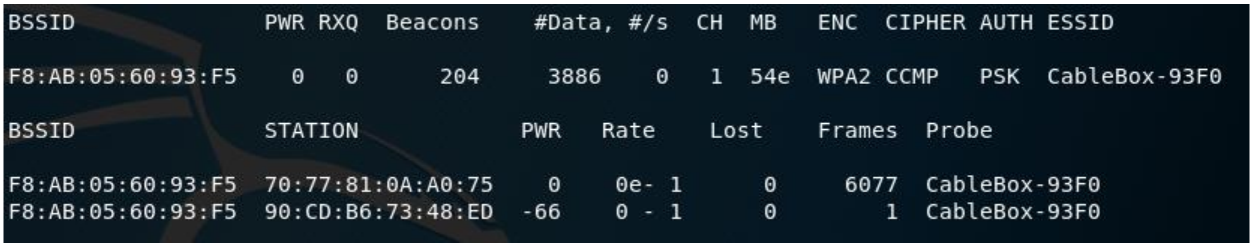
```
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 3a:d7:8b:a7:f9:ee  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Monitoring the traffic

Now it is possible to monitor the traffic and capture raw 802.11 frames from which Wi-Fi passphrase will be extracted during the handshake process of one connecting client.

After typing: **airodump-ng wlan0mon** we can see a list of nearby routers and information about them, such as: ***BSSID*** - MAC address of the router, ***PWR*** – strength of the signal, the bigger it is, the closer the router is. ***Beacons*** – number of announcement packets sent by the router. It announces the clients about its existence, and that they can connect to it. ***Data*** – number of captured data packets from this router. ***/s*** – number of data packets per second. ***CH*** – channel number on which router is operating (this info is taken from beacon announcement packet). ***MB*** – indicates the maximum speed supported by the router. ***ENC*** – indicates what encryption algorithm is used. ***CIPHER*** – cipher used by the router. ***AUTH*** – authentication method. ***ESSID*** – the name of the wireless network.

Then I select to capture frames from my own router by typing into the terminal:
airodump-ng –bssid F8:AB:05:60:93:F5 -c 1 -w capture wlan0mon



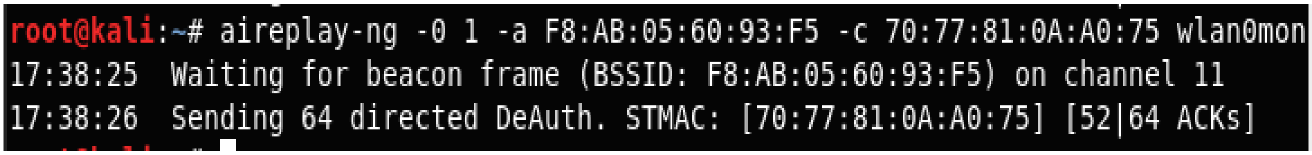
```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F8:AB:05:60:93:F5    0   0      204     3886    0   1  54e  WPA2 CCMP   PSK  CableBox-93F0

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

F8:AB:05:60:93:F5  70:77:81:0A:A0:75    0    0e- 1      0     6077  CableBox-93F0
F8:AB:05:60:93:F5  90:CD:B6:73:48:ED  -66    0 - 1      0        1  CableBox-93F0
```

This will capture the frames that are in the air and write them into the capture file named capture. The whole point of capturing frames is to capture 4-way handshake of a client when connection is being established between the client and the router. During 4-way handshake process, a temporary encryption key is made to encrypt the data being passed between them. If its PSK authentication method – Wi-Fi passphrase derived and part of it is used in creation of temporary encryption key.

Capturing the handshake

While ***airodump-ng –bssid F8:AB:05:60:93:F5 -c 1 -w capture wlan0mon*** is running, one of the clients must be DeAuthenticated in order to capture the 4-way handshake and get the key. [6]

In another terminal window I type: ***aireplay-ng -0 1 -a F8:AB:05:60:93:F5 -c 70:77:81:0A:A0:75 wlan0mon*** to send DeAuthentication frame. ***-0*** means DeAuthentication, ***1*** means send 1 DeAuth frame, ***-a*** and MAC address of the access point to which client is connected, ***-c*** is the MAC address of the connected client which will be DeAuthenticated and wlan0mon is the name of my network card (network interface name).



```
root@kali:~# aireplay-ng -0 1 -a F8:AB:05:60:93:F5 -c 70:77:81:0A:A0:75 wlan0mon
17:38:25  Waiting for beacon frame (BSSID: F8:AB:05:60:93:F5) on channel 11
17:38:26  Sending 64 directed DeAuth. STMAC: [70:77:81:0A:A0:75] [52|64 ACKs]
```

AIREPLAY ATTACK. SENDING DEAUTH FRAME

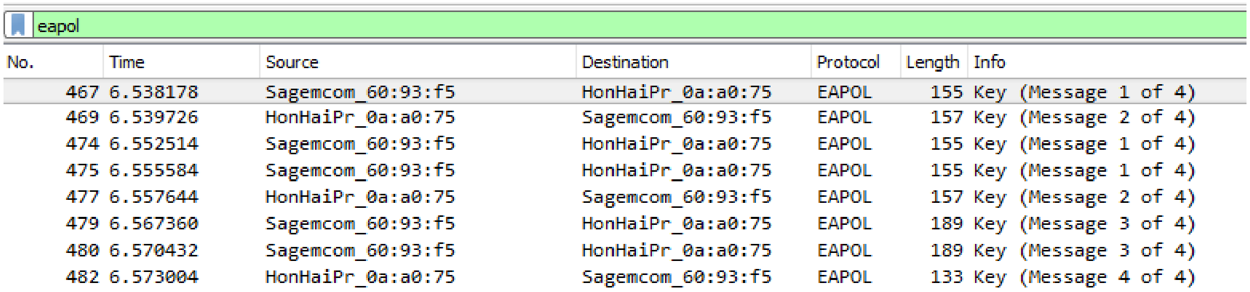
After this point, all the data that is going to be sent or received by this specific MAC address, will be captured and written into the file called capture.cap, it can be opened by using Wireshark to decrypt and inspect packets (captured data).

Inspecting packets and the data

Opening the capture file and filtering for EAPOL (authentication protocol) packets yields 4-way handshake messages which contains parts of the keys used together with Wi-Fi passphrase to encrypt and decrypt the data. Some of the messages were captured multiple times.[7]

[6] https://security.stackexchange.com/questions/17767/four-way-handshake-in-wpa-personal-wpa-psk?utm_medium=organic&utm_source=google_rich_qa&utm_campaign=google_rich_qa

[7] http://www.wi-fiplanet.com/tutorials/article.php/1447501/Understanding-80211-Frame-Types.htm



eapol

No.	Time	Source	Destination	Protocol	Length	Info
467	6.538178	Sagemcom_60:93:f5	HonHaiPr_0a:a0:75	EAPOL	155	Key (Message 1 of 4)
469	6.539726	HonHaiPr_0a:a0:75	Sagemcom_60:93:f5	EAPOL	157	Key (Message 2 of 4)
474	6.552514	Sagemcom_60:93:f5	HonHaiPr_0a:a0:75	EAPOL	155	Key (Message 1 of 4)
475	6.555584	Sagemcom_60:93:f5	HonHaiPr_0a:a0:75	EAPOL	155	Key (Message 1 of 4)
477	6.557644	HonHaiPr_0a:a0:75	Sagemcom_60:93:f5	EAPOL	157	Key (Message 2 of 4)
479	6.567360	Sagemcom_60:93:f5	HonHaiPr_0a:a0:75	EAPOL	189	Key (Message 3 of 4)
480	6.570432	Sagemcom_60:93:f5	HonHaiPr_0a:a0:75	EAPOL	189	Key (Message 3 of 4)
482	6.573004	HonHaiPr_0a:a0:75	Sagemcom_60:93:f5	EAPOL	133	Key (Message 4 of 4)

CAUGHT 4-WAY HANDSHAKE MESSAGE

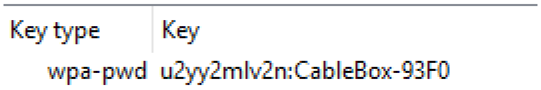
Cracking Wi-Fi passphrase

The router's Wi-Fi passphrase on which I'm performing this Man-in-the-Middle attack is secured with WPA2. The final step is to get Wi-Fi passphrase. This can be done by either brute-forcing using dictionary attack on the capture.cap file. However, this takes a lot of time. The easiest way to get the Wi-Fi passphrase by exploiting weakness in WPS (Wi-Fi Protected Setup).

As I already know the Wi-Fi passphrase, I will be skipping this step and continue decrypting the data in this final step.

Decrypting the data

Open the capture.cap file with Wireshark, go to: ***Edit*** > ***Preferences...*** > ***Protocols*** > ***IEEE 802.11*** > ***Decryption keys*** > check "***Enable decryption***" box and click "***Edit...***" > press ***+*** sign and add these in the following format:



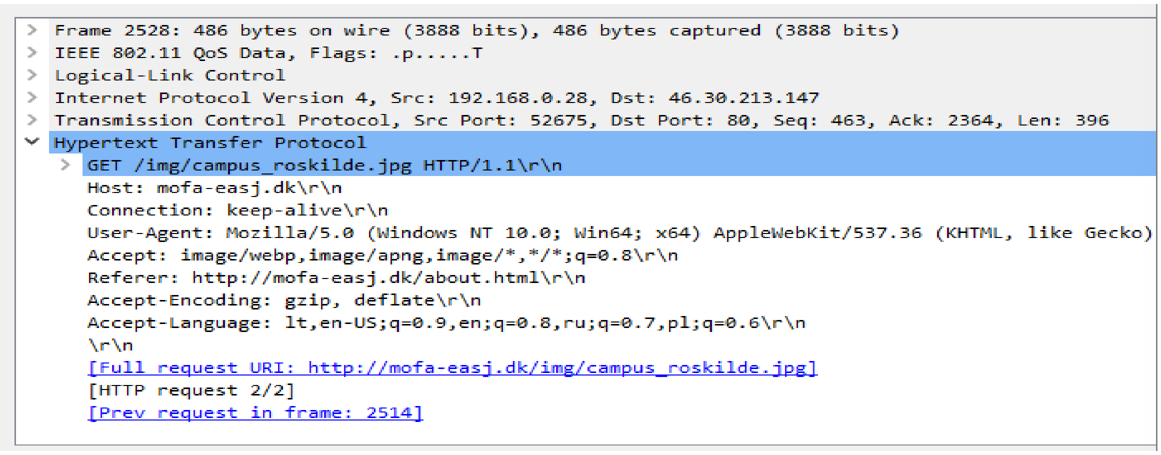
Key type	Key
wpa-pwd	u2yy2mlv2n:CableBox-93F0

Key contains Wi-Fi passphrase (the on you enter to use Wi-Fi) and the name of the Wi-Fi network (SSID). After this, Wireshark automatically decrypts all the data if the 4-way handshake is present. In my case it is, as I have seen 4 EAPOL messages.

End result

We can see that the attack was successful. TCP packets contain HTTP protocol, it means the victim was browsing on the internet. Visited websites, destination IP and port and even the content of the website can be seen, like images. If I was to fill log-in form, it would also be visible to the attacker in plain-text.

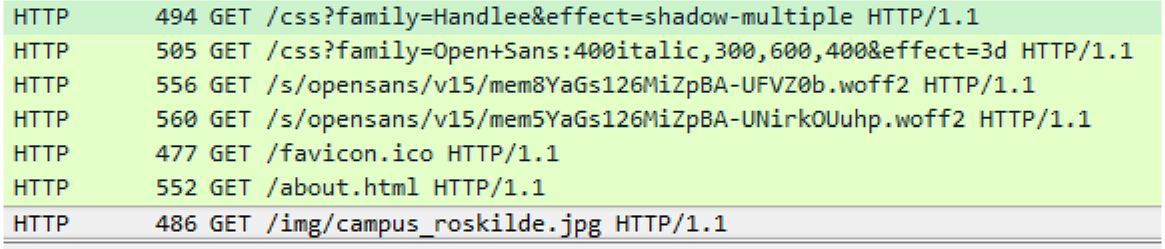
As I was visiting HTTP websites, the data on transport layer has not been encrypted, therefore we can see all the data in plain text.



```
> Frame 2528: 486 bytes on wire (3888 bits), 486 bytes captured (3888 bits)
> IEEE 802.11 QoS Data, Flags: .p.....T
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.0.28, Dst: 46.30.213.147
> Transmission Control Protocol, Src Port: 52675, Dst Port: 80, Seq: 463, Ack: 2364, Len: 396
v Hypertext Transfer Protocol
   > GET /img/campus_roskilde.jpg HTTP/1.1\r\n
     Host: mofa-easj.dk\r\n
     Connection: keep-alive\r\n
     User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
     Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
     Referer: http://mofa-easj.dk/about.html\r\n
     Accept-Encoding: gzip, deflate\r\n
     Accept-Language: lt,en-US;q=0.9,en;q=0.8,ru;q=0.7,pl;q=0.6\r\n
     \r\n
     [Full request URI: http://mofa-easj.dk/img/campus_roskilde.jpg]
     [HTTP request 2/2]
     [Prev request in frame: 2514]
```

HTTP WEBSITE'S DECRYPTED PACKET

It shows what HTTP request methods where called for each packet and what resources where given. A packet contains around 1450 bytes of data.[8]



```
HTTP      494 GET /css?family=Handlee&effect=shadow-multiple HTTP/1.1
HTTP      505 GET /css?family=Open+Sans:400italic,300,600,400&effect=3d HTTP/1.1
HTTP      556 GET /s/opensans/v15/mem8YaGs126MiZpBA-UFVZ0b.woff2 HTTP/1.1
HTTP      560 GET /s/opensans/v15/mem5YaGs126MiZpBA-UNirkOUuhp.woff2 HTTP/1.1
HTTP      477 GET /favicon.ico HTTP/1.1
HTTP      552 GET /about.html HTTP/1.1
HTTP      486 GET /img/campus_roskilde.jpg HTTP/1.1
```

PACKETS WITH HTTP PROTOCOL

It is possible to intercept all HTTP request methods, including POST, which can yield user’s log-in data such us username and/or password.

[8] https://stackoverflow.com/questions/2613734/maximum-packet-size-for-a-tcp-connection?utm_medium=organic&utm_source=google_rich_qa&utm_campaign=google_rich_qa

Conclusion

In conclusion, I would like to say that I have learned a lot not only about Wi-Fi attacks and its security, but I also dove very deep to see how communication on the lowest layers of networks is happening. Reading about Wi-Fi security, I have learned what are the best ways to protect my own network, how to configure router properly and make the best out of it.

From the attacker's perspective it was quite hard to perform such attack. It is very sophisticated, multi-stage attack, requiring one to be knowledgeable about many aspects of information technology and information security. Performing the attack taught me many things, such as how a change in encryption algorithm could change attack time drastically, if not making it impossible to perform such attack at all.

For people who are not that tech-savvy it is very important to understand that the length and complexity of the Wi-Fi passphrase/password is what makes it very hard or easy for the attacker to crack it. As of today, the safest, yet still exploitable authentication method and encryption algorithm is WPA2-PSK – this is what I recommend using for home or other small networks.

Today's routers provide high security standards and they are reliable. Even though data can be dumped very easily, cryptography techniques used by the routers, most of the time, are sufficient to protect the data even if it is intercepted. It is very hard to decrypt it. However, today's encryption algorithms are not able to make the data completely safe.

Reflection

Overall, I'm happy with the work that I have done. I had to read a lot, and this is what took most of my time. Now that is okay, but I didn't mention it on my plan, therefore I didn't expect to spend that much of my time reading.

The title of the synopsis could've been better, emphasizing more on Wi-Fi security rather than the attack itself.

Another thing that I could have improved is that I could have referenced the pictures and text in my synopsis while I'm in the progress and not in the end, when all the work has been done. This way I had to go through everything again and again and put references to appropriate links.

Full list of references:

https://www.intel.com/content/www/us/en/support/articles/000006508/network-and-i-o/wireless-networking.html

https://security.stackexchange.com/questions/17767/four-way-handshake-in-wpa-personal-wpa-psk?utm_medium=organic&utm_source=google_rich_qa&utm_campaign=google_rich_qa

https://security.stackexchange.com/questions/76983/what-is-the-need-and-purpose-of-packet-injection-within-wifi-attacks?utm_medium=organic&utm_source=google_rich_qa&utm_campaign=google_rich_qa

http://microchipdeveloper.com/tcpip:tcp-ip-five-layer-model

https://www.makeuseof.com/tag/wpa2-wep-and-friends-whats-the-best-way-to-encrypt-your-wi-fi/

https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/

http://www.wi-fiplanet.com/tutorials/article.php/1447501/Understanding-80211-Frame-Types.htm

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-using-aircrack-ng-0148366/

https://www.aircrack-ng.org/doku.php?id=cracking_wpa