Wireless security

or: How I Learned to Start Worrying and Love Hacking

Mateusz Maciejewski

This lecture's scope: Wi-Fi

More specifically:
security of IEEE 802.11*
(mainly OSI layer 2)

Why?

1. Most popular wireless medium
2. Very well documented/studied = good examples of various vulnerabilities of wireless protocols
3. Easiest to hack
    a. cheap customer-grade cards support all the advanced features we need

Cheap Wi-Fi card:

$9.61

(with free shipping!)

The only proper Bluetooth dongle:

$120.00

(excl. shipping)

UBERTOOTH ONE

$120.00

The Ubertooth One is an opensource Bluetooth test tool from Michael Ossmann. It is the world's first affordable Bluetooth monitoring and development platform and is a fully open source product (both hardware and software).

Commercial Bluetooth monitoring equipment starts at about $10,000. Project Ubertooth seeks to produce an affordable platform that can be used for Bluetooth monitoring and for the development of new Bluetooth and wireless technologies

Low-cost off-the-shelf Wi-Fi adapters have supported monitor mode for years, and the technique has found diverse uses in security research, troubleshooting, product development, intrusion detection, and more. Unfortunately, there has never been an equivalent tool for Bluetooth before Ubertooth One, a fully open source platform (both hardware and software).

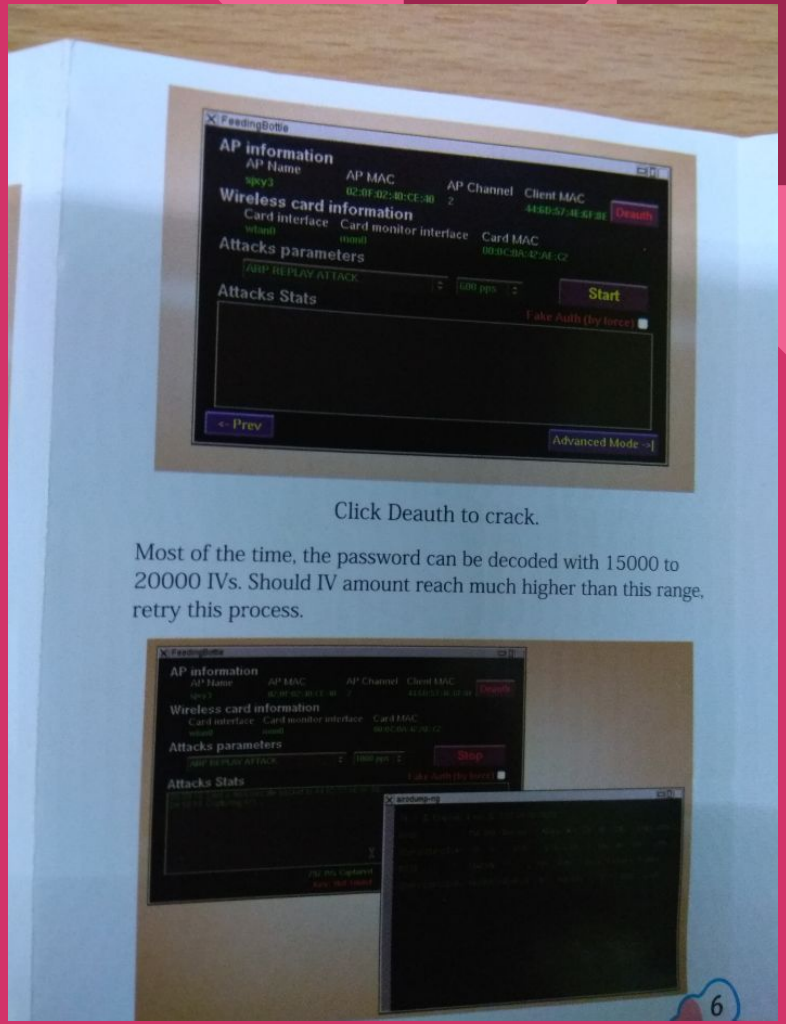
You can find out more about Project Ubertooth on my Michael Ossmann's blog and at the project web site.

QTY

1

ADD TO CART

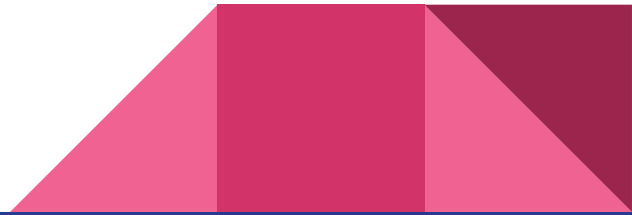
Free *Haxx0r LiveCD* included



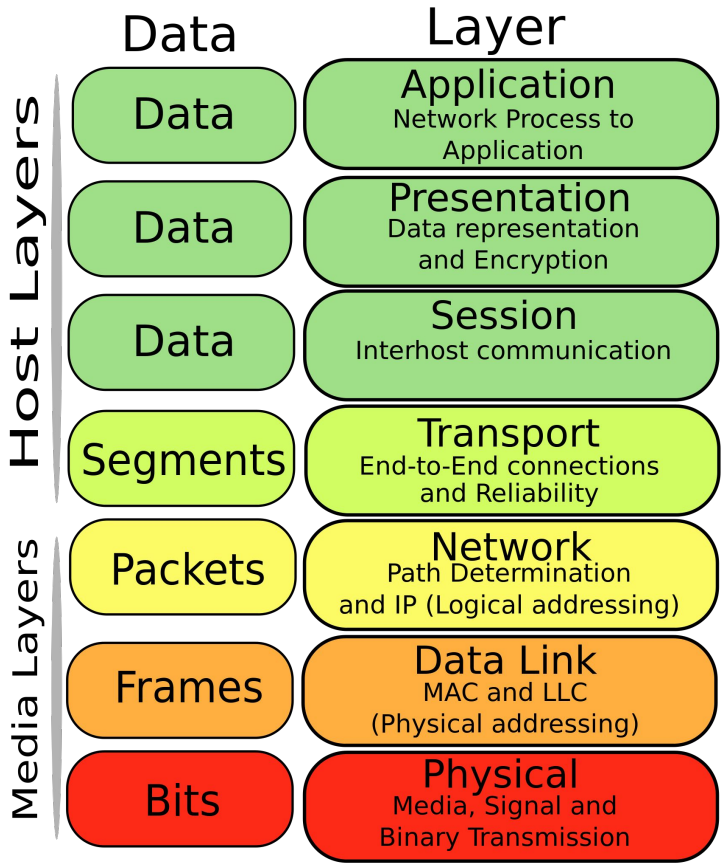
Basic problems with wireless

Problems

- All the problems with wired communication, but none of the protection
  - Physical security is impossible
    - No network ports to hide behind locked doors, RF leaks everywhere
  - No way to send to one device only - must rely on cryptography
    - Eavesdropping **raw packets** is inevitable
    - This also makes any kind of forgery a lot easier (assuming a weakness in crypto)
  - No builtin identity protection
    - Plugging a wire into your router vs connecting to a wireless network with a familiar name



OSI Model


Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data representation and Encryption
Data
Session
Interhost communication
Segments
Transport
End-to-End connections and Reliability
Packets
Network
Path Determination and IP (Logical addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal and Binary Transmission

IEEE 802.11

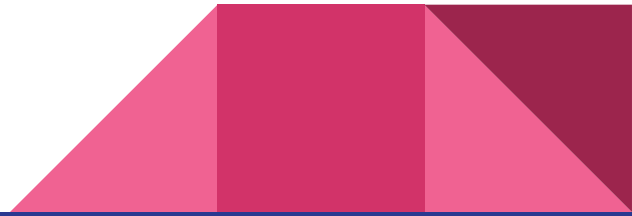
*is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and **60 GHz** frequency bands.*

7 Gbps - nice.

IEEE 802.11

Although there are about 18 different 802.11* protocols (or amendments), we are most interested in **802.11a(c)/b/g/n** - simply because they're most widely used and supported.

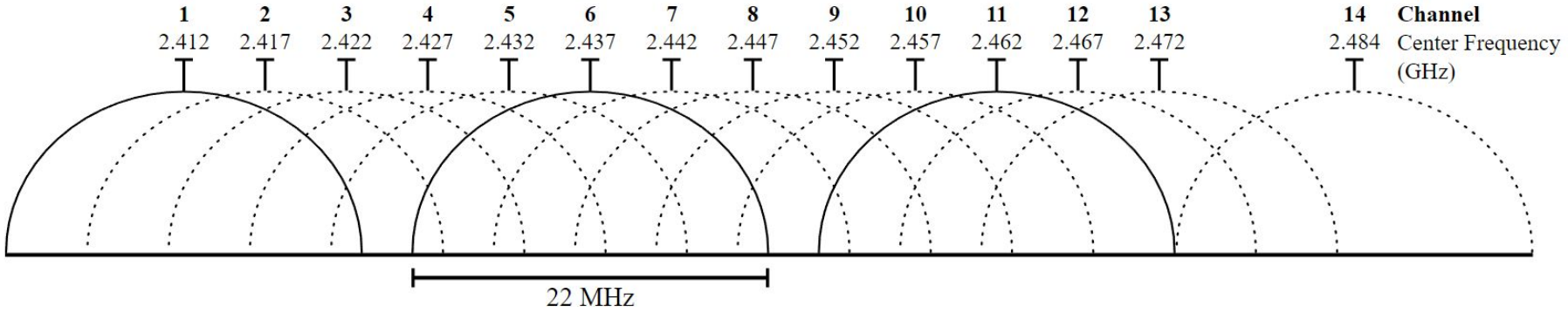
Actually, in this lecture's scope™ we can *almost* treat them the same. The major differences between them are in the layer 1 (physical) of OSI, which we won't exploit.



802.11 basics

- Electromagnetic waves as the medium duh
  - Frequency range divided into channels
- Half-duplex
  - Two-way communication, but only one device at once (per channel)
- Three types of layer 2 frames:
  - Management - association, authentication, probes
  - Control - ACK and stuff
  - Data - the actual data transmission (transporting higher OSI layers)

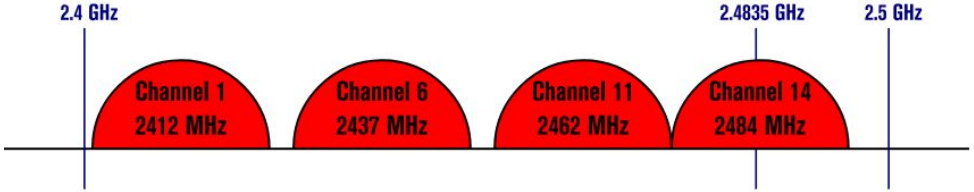
802.11b 2.4GHz 22 MHz channels



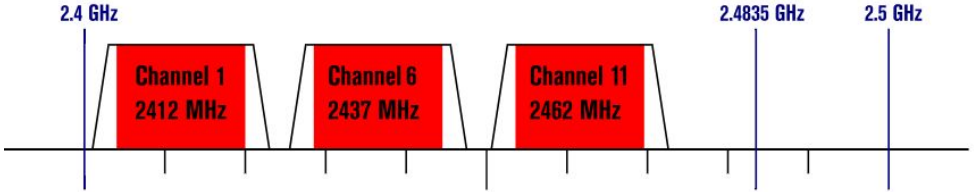
They overlap a lot!

Non-Overlapping Channels for 2.4 GHz WLAN

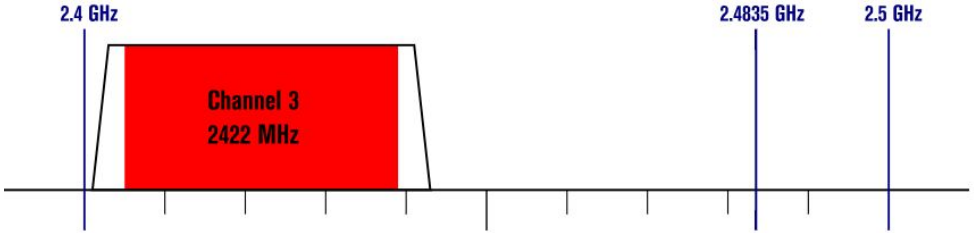
802.11b (DSSS) channel width 22 MHz



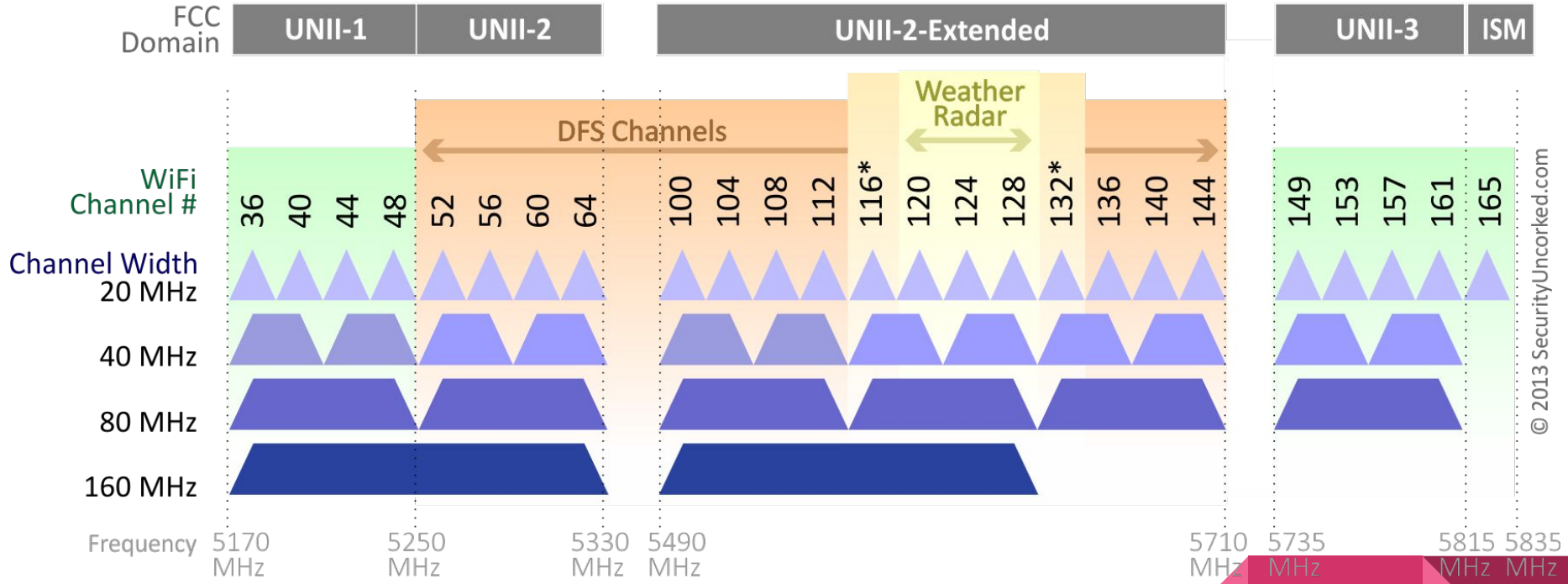
802.11g/n (OFDM) 20 MHz ch. width – 16.25 MHz used by sub-carriers



802.11n (OFDM) 40 MHz ch. width – 33.75 MHz used by sub-carriers

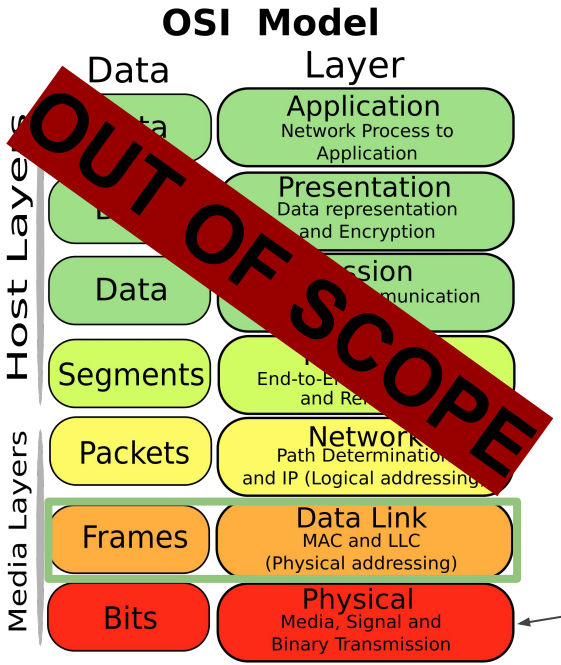


802.11ac Channel Allocation (N America)

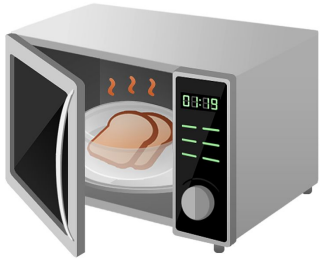


*Channels 116 and 132 are Doppler Radar channels that may be used in some cases.

Moving on and why layer 1 is boring:



We limit ourselves to the data link layer, as it implements all the protocols needed for establishing *secure* connections between Wi-Fi devices.



Deauthentication attack

Frames are not encrypted!

This includes management frames, which includes the deauthentication frames. By forging the origin MAC address one can impersonate any station and terminate a connection with another station on its behalf. Even better, it is possible* to use a broadcast destination address, which will be received by all clients connected to a given AP.

This issue has been fixed in 802.11w-2009, which introduces *Protected Management Frames*, but in reality it's rarely used in b/g/n networks. It is, however, required in 802.11ac.

*In my experience, many PC cards ignore broadcast deauth frames, while Android phones happily receive them and disconnect from the network.

10:35
6/10/2014

Hotel Marriott zagłuszał hostpoty klientów aby nakłonić ich do płacenia za hotelowe Wi-Fi

Autor: igH | Tagi: Best Western, hotel, jamming, Marriott, Wi-Fi

Sieci hotelowej Marriott przyjdzie zapłacić 600 000 dolarów kary po tym, jak została przyłapana na celowym zagłuszaniu sygnału mobilnych hotspotów stawianych przez klientów. Chodzi o tzw. tethering przy użyciu sieci GSM, a realizowany np. przy pomocy iPhonów lub smartphonów z Androidem oraz urządzeń Mi-Fi.

Marriott wymuszał wykupienie dostępu do internetu

Marriott w Nashiville zagłuszał urządzenia klientów tylko i wyłącznie w jednym celu — aby zdesperowani musieli zakupić hotelową usługę dostępu do internetu. Co interesujące, jej koszt wynosił między **250 a 1000 dolarów (od urządzenia)**. To dużo, ale rozumiemy, że kadra managerska, która płaci firmową kartą kredytową i koniecznie musi odebrać ważnego e-maila od kontrahenta jest w stanie zaakceptować taką ofertę (czyżby w pobliżu nie było żadnego Starbucksa?).

Practical example [demo time]

A

Regular traffic

B

From: A - To: B

Terminate this connection **NOW**

802.11 Probes & Beacons

Beacon frames broadcasting

My name is …
I can transmit using rates such as ...
I use … encryption

`ff:ff:ff:ff:ff:ff`

Probe request

I am looking for SSID … (can be a wildcard!)

`ff:ff:ff:ff:ff:ff`

Probe response

<Same information as a Beacon +
answers to detailed questions>

Example

Pac...	Transmitter	Receiver	Flags	Ch...	Signal	Data ...	Size	Protocol	Size Bar
453	B8:38:61:99:1A:AF	Ethernet Broadcast	*	149	54%	24.0	262	802.11 Beacon	802.11 Beacon
454	84:38:38:5B:63:D5	Ethernet Broadcast	*	149	48%	6.0	118	802.11 Probe Req	802.11 Probe Req
455	B8:38:61:99:1A:AF	84:38:38:5B:63:D5	*+	149	56%	24.0	253	802.11 Probe Rsp	802.11 Probe Rsp
456		B8:38:61:99:1A:AF	#	149	45%	24.0	14	802.11 Ack	
457	B8:38:61:99:1A:AE	84:38:38:5B:63:D5	*P+	149	56%	24.0	288	802.11 Probe Rsp	802.11 Probe Rsp
458		B8:38:61:99:1A:AE	#	149	46%	24.0	14	802.11 Ack	
459	B8:38:61:99:1A:AE	Ethernet Broadcast	*P	149	54%	24.0	297	802.11 Beacon	802.11 Beacon
460	84:38:38:5B:63:D5	Ethernet Broadcast	*	149	48%	6.0	118	802.11 Probe Req	802.11 Probe Req
461	B8:38:61:99:1A:AF	84:38:38:5B:63:D5	*+	149	57%	24.0	253	802.11 Probe Rsp	802.11 Probe Rsp
462		B8:38:61:99:1A:AF	#	149	46%	24.0	14	802.11 Ack	
463	B8:38:61:99:1A:AE	84:38:38:5B:63:D5	*P+	149	55%	24.0	288	802.11 Probe Rsp	802.11 Probe Rsp
464		B8:38:61:99:1A:AE	#	149	46%	24.0	14	802.11 Ack	
465	84:38:38:5B:63:D5	B8:38:61:99:1A:AF	C	149	45%	24.0	30	802.11 Null Data	802.11 Data

Beacon flood attack - [demo]

My name is **A**
I can transmit using rates such as ...
I use … encryption

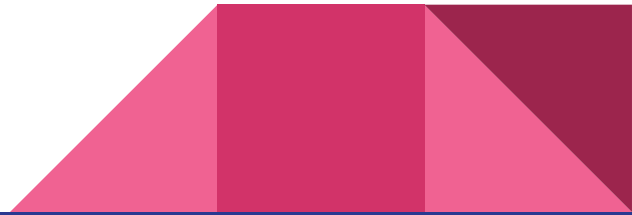
ff:ff:ff:ff:ff:ff

My name is **A**
My name is **A**
My name is **A**
My name is **A**
My name is **A**
My name is **A**

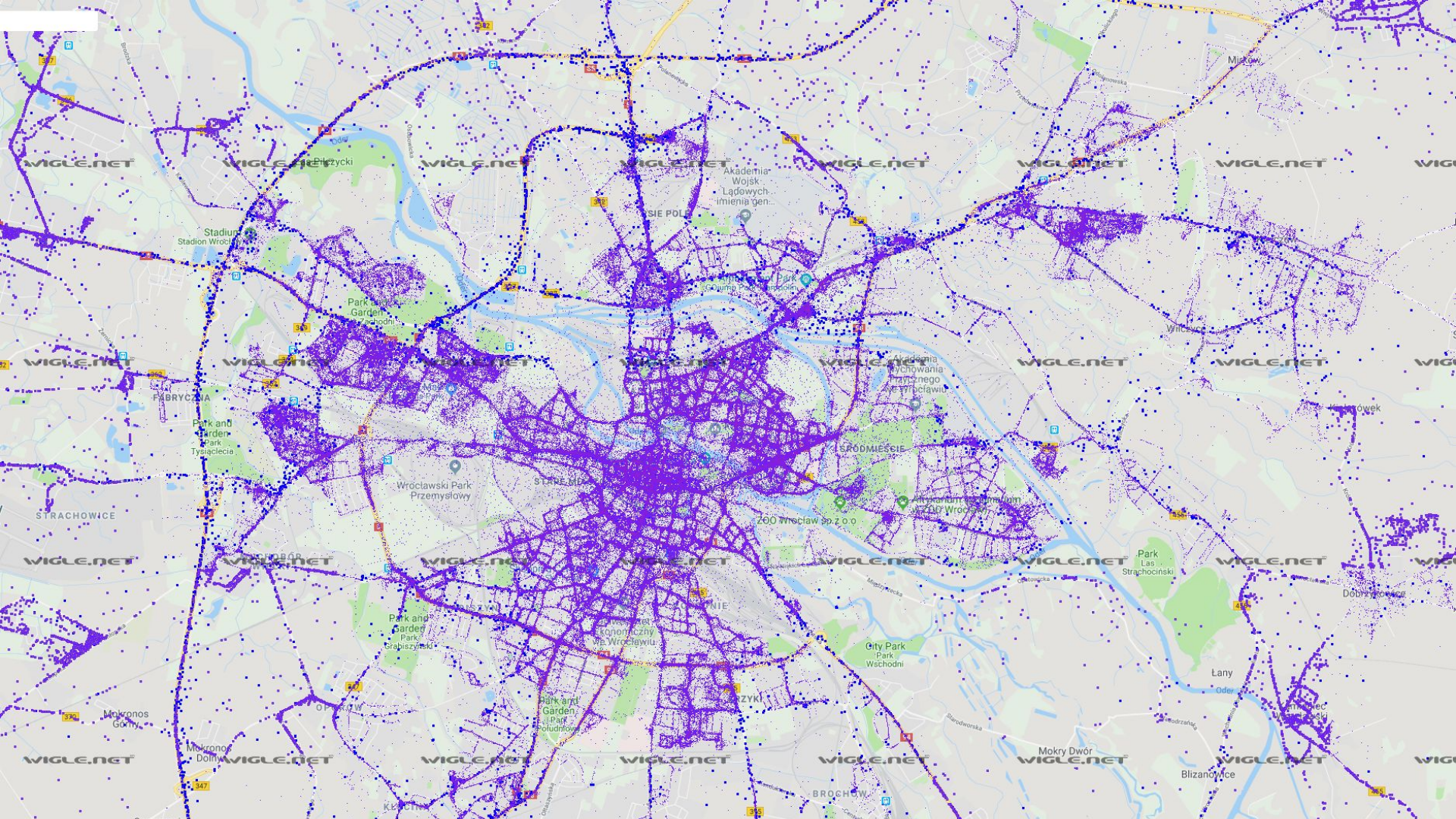
KARMA and MANA attacks (Wi-Fi Pineapple)

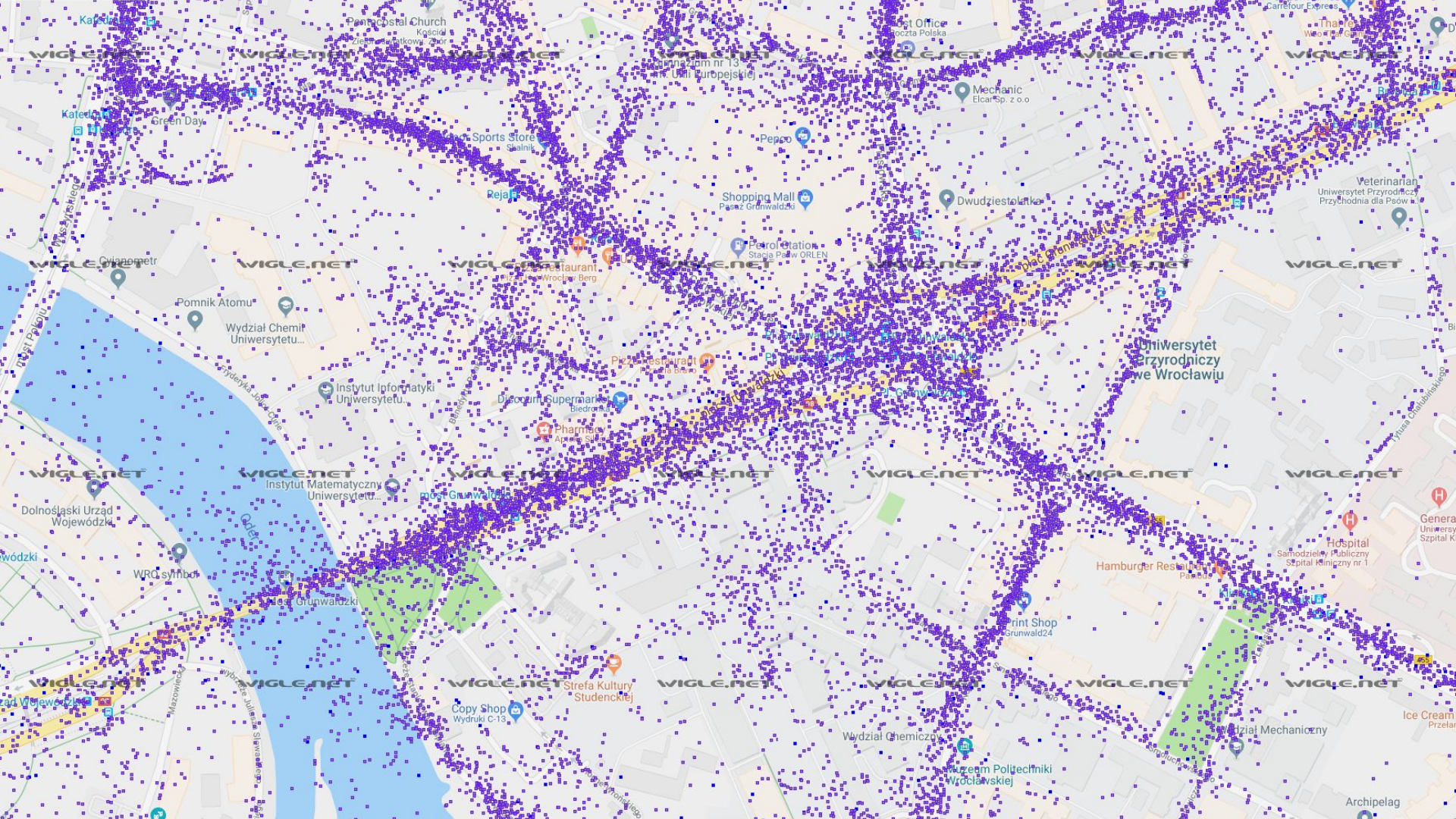
By responding to probe request a malicious actor can impersonate other APs and convince supplicants to connect to them, which is usually a setup for a MitM attack - this is the classic KARMA attack (2004).

MANA attack is an updated version (2015), which accounts for various fixes implemented in the popular OSs (especially Android and iOS) since 2004.



Let’s go *wardriving*


Stadion Wrocław
Park and Garden Tysiąclecia
Wrocławski Park Przemysłowy
Park and Garden Grabiszyński
Park and Garden Południowy
Akademia Wojsk Lądowych imienia gen...
Akademia Wychowania Fizycznego we Wrocławiu
Aquarium Wrocławskie
ZOO Wrocław sp.z o.o
Park Las Strachociński
City Park Park Wschodni
Mokronos Górny
Mokronos Dolny
Mokry Dwór
Blizanowice
Łany
Miłów
STRACHOWICE
BROCHÓW


Pentecostal Church
Post Office
Poczta Polska
Mechanic
Elcar Sp. z o.o
Green Day
Sports Store
Pepco
Shopping Mall
Pasaż Grunwaldzki
Dwudziestolatka
Veterinarian
Uniwersytet Przyrodniczy
Przychodnia dla Psów
Petrol Station
Stacja Paliw ORLEN
Restaurant
Cytanometr
Pomnik Atomu
Wydział Chemii Uniwersytetu...
Instytut Informatyki Uniwersytetu...
Uniwersytet Przyrodniczy we Wrocławiu
Pharmacy
Instytut Matematyczny Uniwersytetu...
Dolnośląski Urząd Wojewódzki
WRC symbol
Hospital
Samodzielny Publiczny Szpital Kliniczny nr 1
Hamburger Restaurant
Print Shop
Grunwald24
Strefa Kultury Studenckiej
Copy Shop
Wydruki C-13
Wydział Chemiczny
Wydział Mechaniczny
Archipelag


Kieleczewska
Zielna
Malborska
Nowogrodzka
Grodzieńska
Sławatycka
Image © 2018 DigitalGlobe
© 2018 Google
Image © 2018 CNES / Airbus

I even managed to find some WEP APs

18:46
10/5/2010

Samochody Google zbierają dane na temat sieci Wi-Fi

Autor: Piotr Konieczny | Tagi: Google, GSM, hardware, inwigilacja, prywatność, Wi-Fi

Google Car to samochód przystosowany do fotografowania ulic. Zdjęcia z Google Cara wykorzystywane są w produktach takich jak Google Maps (Street View) i Google Earth. Niedawno okazało się, że samochody Google'a oprócz zdjęć budynów, zbierają również dane na temat sieci Wi-Fi, których sygnał odbierają w trakcie jazdy po mieście.

Analizując sygnał sieci Wi-Fi można wyciągnąć wnioski co do jej bezpieczeństwa (algorytmy szyfrowania, wykorzystany sprzęt, wersja oprogramowania) — czasem, nawet po samej nazwie sieci można wiele wywnioskować...

Geolokalizacja przy pomocy Wi-Fi

Google zbiera dane dotyczące Access Pointów najprawdopodobniej w celu ulepszenia geolokalizacji urządzeń, które nie posiadają odbiornika GPS, ale są wyposażone w Wi-Fi.

INDOOR TRAX

To unikatowe narzędzie oparte na wieloletnich praktykach w analizie danych konsumenckich. Daje niespotykane dotąd możliwości analizy i optymalizacji procesów biznesowych.

Monitorujemy ruch klientów

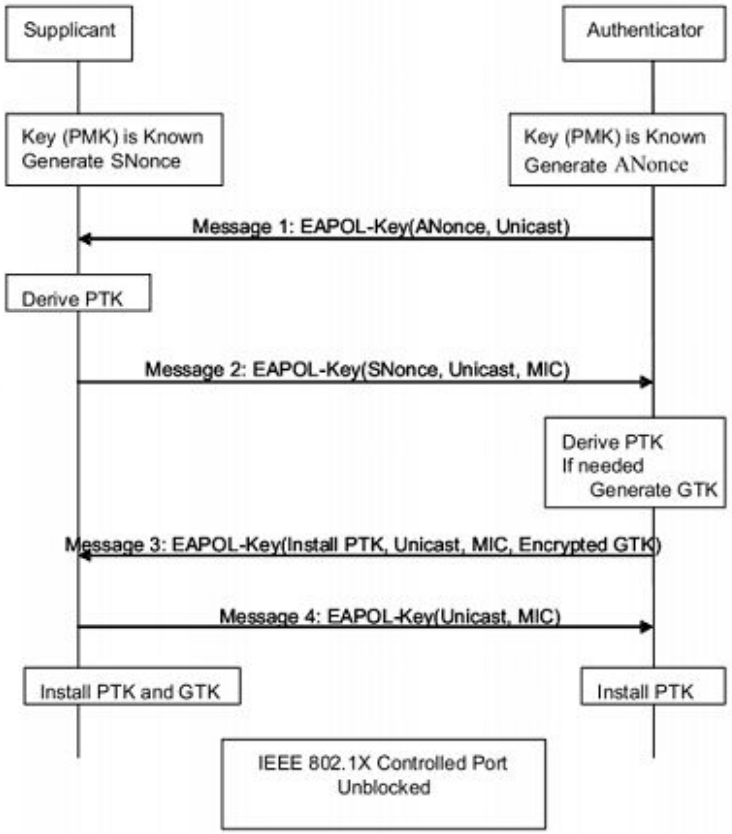
Kluczowym źródłem danych wejściowych są informacje pochodzące z monitoringu ruchu klientów placówki handlowej. Wykorzystujemy i integrujemy dane ze wszystkich źródeł – sieci WIFI, dedykowane sensory, kamery 3D. Ogromne zasoby surowych danych dzięki zaawansowanej technologii przekształcane są do postaci, która może podlegać dalszej obróbce.

iOS 11: toggling wifi and Bluetooth in Control Centre doesn't actually turn them off

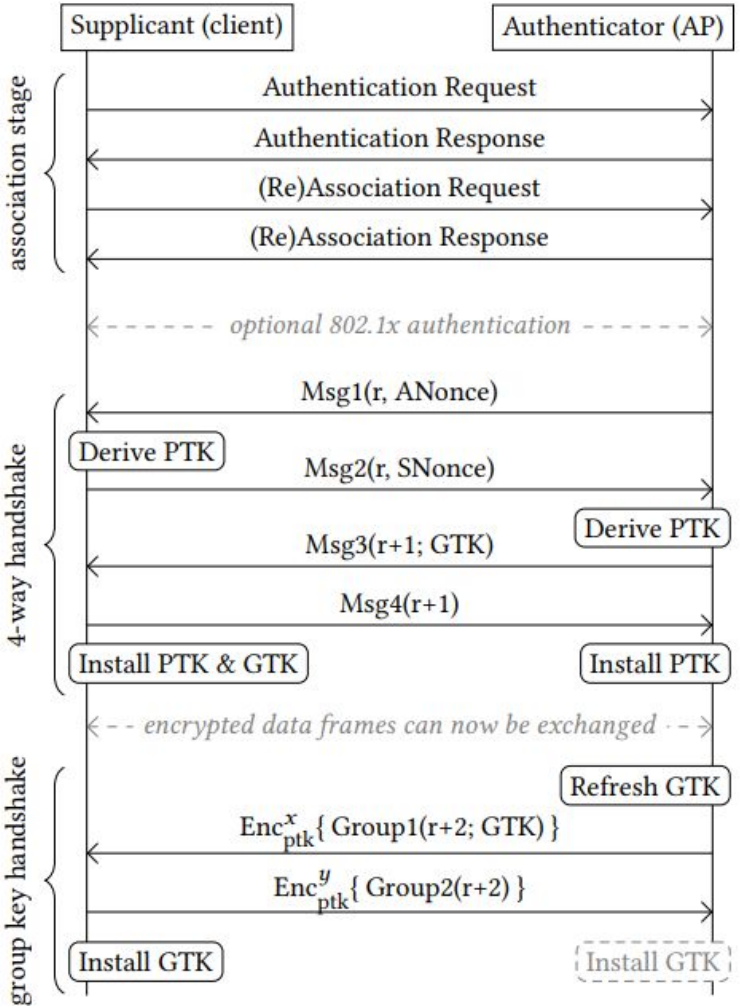
Quick switch simply disconnects phone from access points and devices rather than turning off the radios, in move criticised by security researchers

▲ The wifi toggle disconnects Apple's iPhone or iPad from any wifi networks, but leaves the wireless radio available for use. Photograph: Samuel Gibbs for the Guardian

Basics of 802.11 security


Supplicant
Authenticator
Key (PMK) is Known
Generate SNonce
Key (PMK) is Known
Generate ANonce
Message 1: EAPOL-Key(ANonce, Unicast)
Derive PTK
Message 2: EAPOL-Key(SNonce, Unicast, MIC)
Derive PTK
If needed
Generate GTK
Message 3: EAPOL-Key(Install PTK, Unicast, MIC, Encrypted GTK)
Message 4: EAPOL-Key(Unicast, MIC)
Install PTK and GTK
Install PTK
IEEE 802.1X Controlled Port
Unblocked

4-way handshake

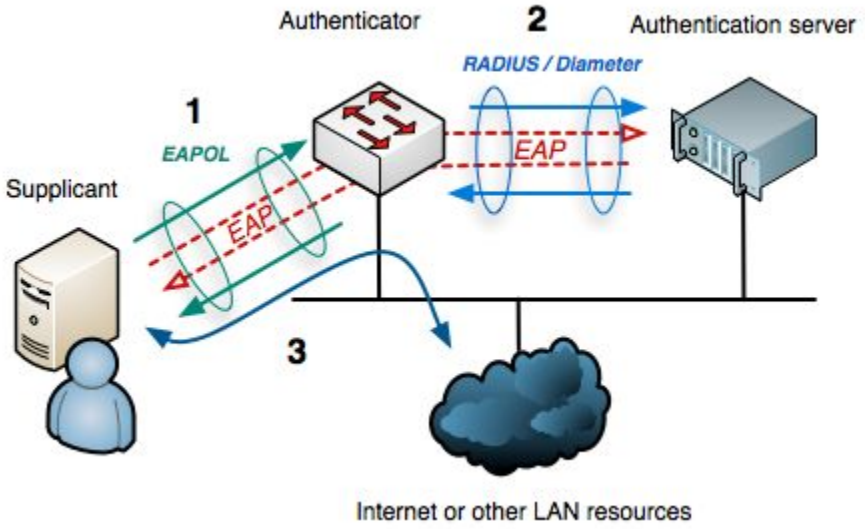


Quick summary of Wi-Fi encryption weaknesses

- WEP:
  - Broken because of IV collisions, key reuse with RC4 (streaming) cipher
- WPA-TKIP (2002):
  - Designed as a quick patch for WEP hardware - essentialy WEP with fancier key mixing routine, packet counter (to prevent replays) and MIC (“protected hash”) to prevent forgery
  - Deprecated as of 2012
- WPA2-AES-CCMP (2004):
  - Current standard, considered to be safe*
  - (2017) “Krack” Key Reinstallation Attack
    - Attacking 4WH allows the attacker to decypt CCMP packets
    - **The same can be used to forge and inject TKIP / GCMP packets**
    - Can be fixed with software patch

802.1X Access Control

Principles

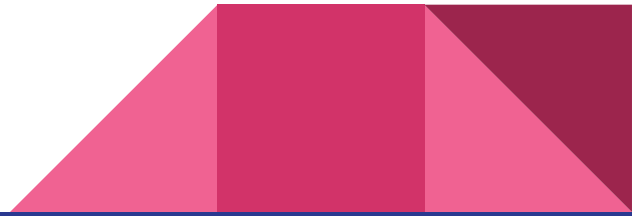

Authenticator
2
Authentication server
RADIUS / Diameter
1
EAPOL
EAP
Supplicant
EAP
3
Internet or other LAN resources

Case study: eduroam

Let’s say you’re a CS freshman...

...and want to connect to the free Wi-Fi - it’s only natural you seek help on your faculty’s website.

One quick Google query yields the following page



New research grants

FOR STUDENTS

- Timetable
- For candidates
- For students
- Our studies
- Services
- Employment and internships
- Student Exchange Programs
- Labs and networks
- Contests
- Questions

LABS AND NETWORKS

Instytut Informatyki posiada 5 pracowni komputerowych. W pracowniach są zainstalowane systemy Windows 7 (pracownie 7, 107, 108, 110) oraz Linux (7, 107, 108, 110, 137). Z pracowni może korzystać każdy student Instytutu Informatyki. Klucz do pracowni można pobrać na portierni po zostawieniu legitymacji lub indeksu.

Na terenie instytutu dostępna jest sieć wifi *eduroam*, do której mają dostęp wszyscy studenci. Szczegóły pod adresem http://dui.uni.wroc.pl/instrukcje-instalacji/.

Instrukcje instalacji – Eduroam

Lista instrukcji instalacji dla kont w domenie:

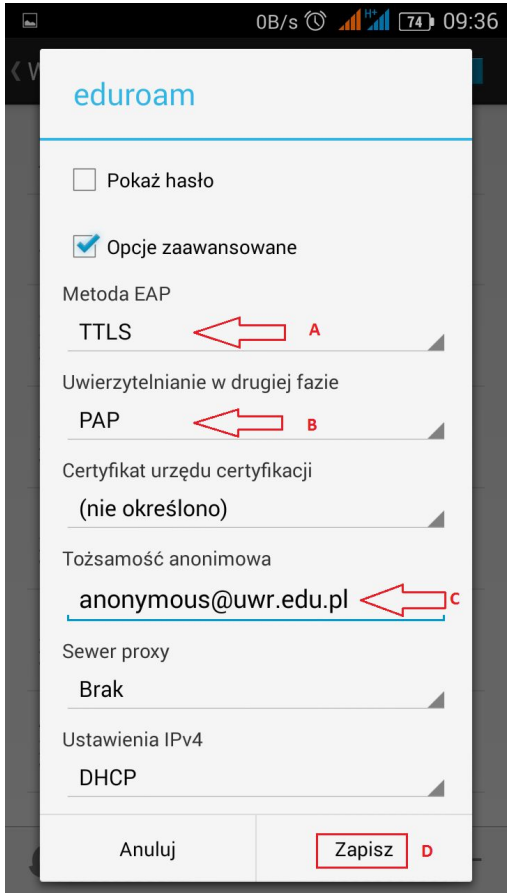
- Windows 10
- Windows 8 i 8.1
- Windows 7
- Windows Vista
- iOS
- Android 4.4.2
- MacOS
- Linux
- Windows Phone

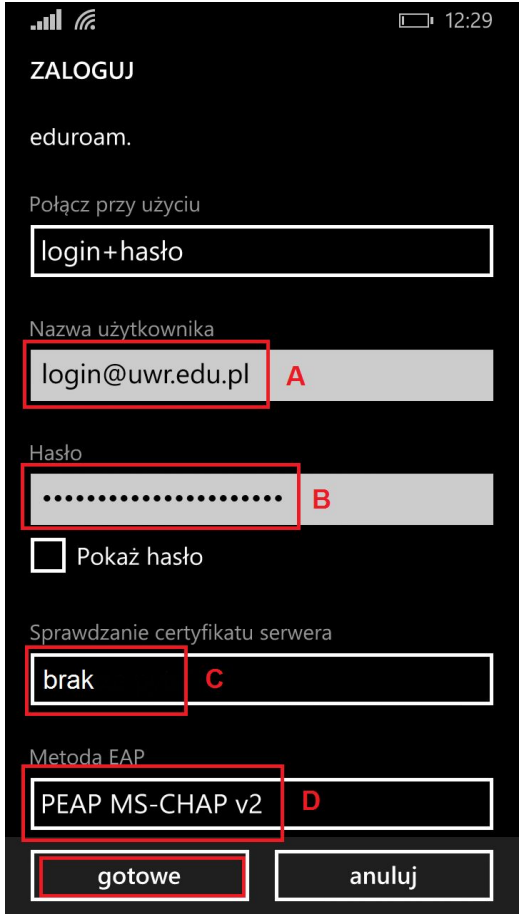
This is where things get interesting

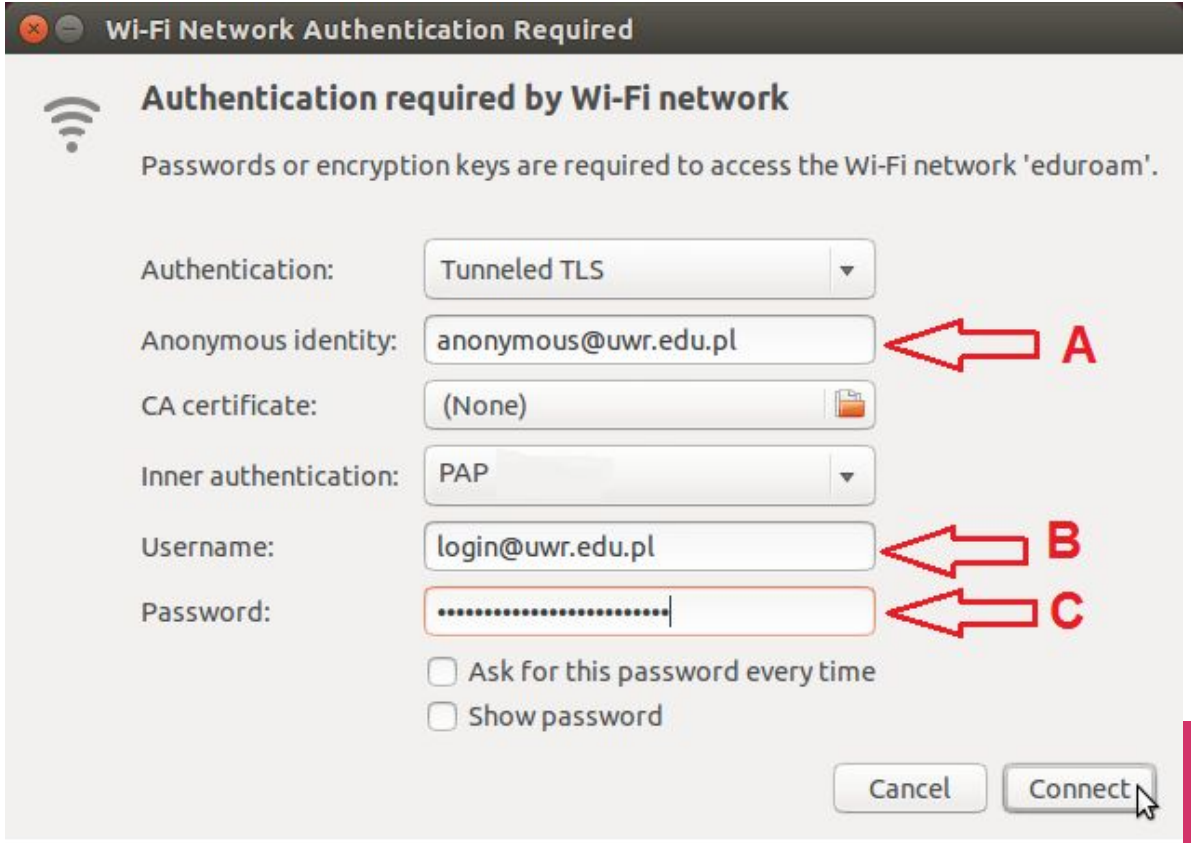
For Windows, iOS and Mac OS X the guide recommends downloading the official eduroam installer, which takes care of the proper configuration and **installing the necessary certificates.**

Unfortunately, in case of Linux, Android and Windows Phone, the author decided to try and present their unique solution - with poor results.

Pay close attention to the second phase/inner authentication and certificate settings!

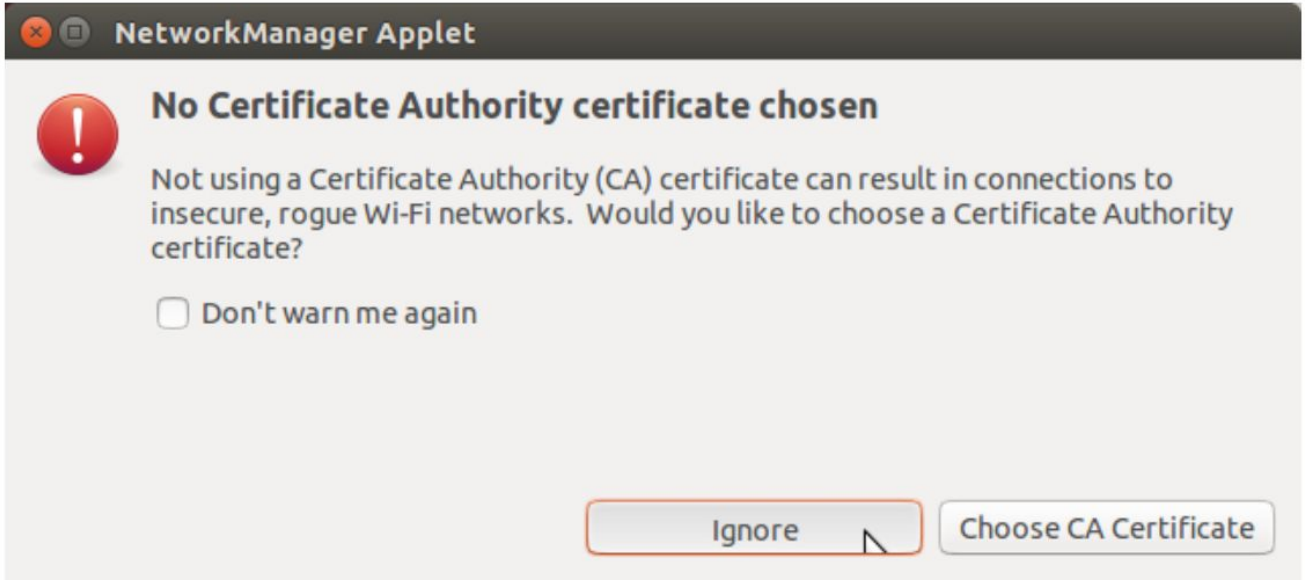

0B/s
74
09:36
eduroam
Pokaż hasło
Opcje zaawansowane
Metoda EAP
TTLS
A
Uwierzytelnianie w drugiej fazie
PAP
B
Certyfikat urzędu certyfikacji
(nie określono)
Tożsamość anonimowa
anonymous@uwr.edu.pl
C
Sewer proxy
Brak
Ustawienia IPv4
DHCP
Anuluj
Zapisz
D


12:29
ZALOGUJ
eduroam.
Połącz przy użyciu
login+hasło
Nazwa użytkownika
login@uwr.edu.pl
A
Hasło
••••••••••••••••••••••
B
Pokaż hasło
Sprawdzanie certyfikatu serwera
brak
C
Metoda EAP
PEAP MS-CHAP v2
D
gotowe
anuluj

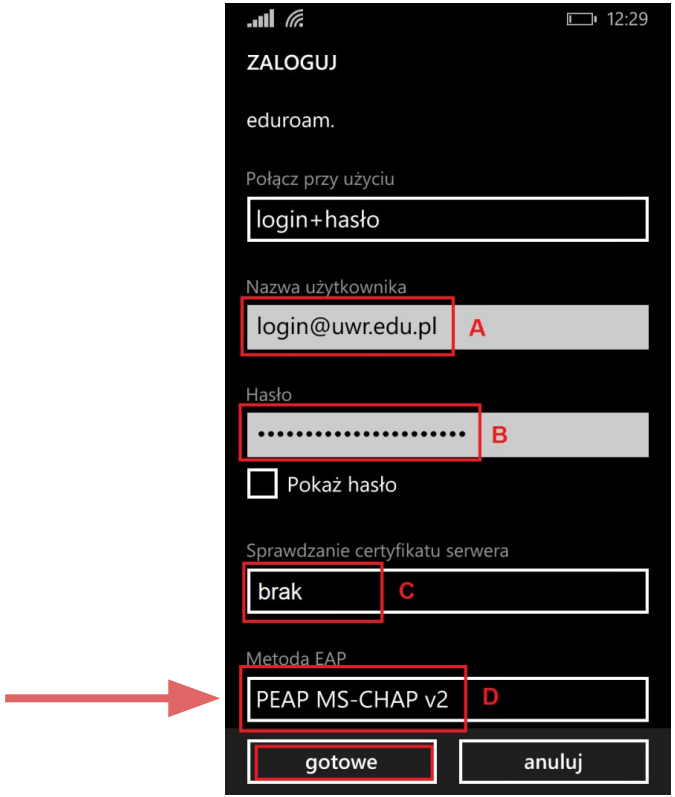

Wi-Fi Network Authentication Required
Authentication required by Wi-Fi network
Passwords or encryption keys are required to access the Wi-Fi network 'eduroam'.
Authentication:
Tunneled TLS
Anonymous identity:
anonymous@uwr.edu.pl
A
CA certificate:
(None)
Inner authentication:
PAP
Username:
login@uwr.edu.pl
B
Password:
C
Ask for this password every time
Show password
Cancel
Connect

When presented with a warning… ignore!

3. Kolejne okno informuje nas o braku certyfikatu, wybieramy „Ignore” by móc się połączyć z siecią.

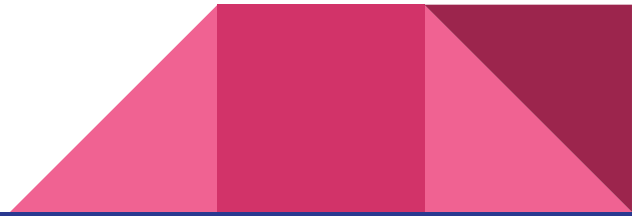


For some reason, Windows Phone is special



What is EAP-PEAP-MSCHAPv2

- Use 802.1x
- Encrypt using server-side certificate (SSL/TLS)
- Use MS-CHAPv2: challenge-response mode, effectively using password hashes



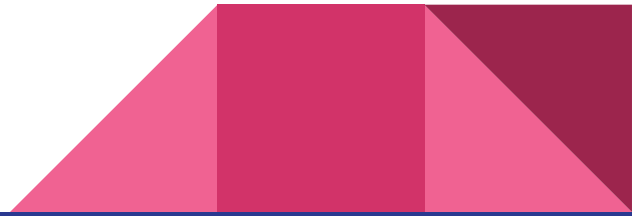
What is EAP-TTLS-PAP

- Use 802.1x
- Tunnel the EAP communication through TLS
- Use plaintext username:password for authentication

Why using certificates is vital

Without the certificate the supplicant has no way to check the identity of the access point, which makes the EAP tunneling worthless. Using an evil twin attack it is trivial to obtain either the plaintext passwords, or at least the hashes.

Considering the fact that eduroam is authenticated against the Office365 service and people love reusing passwords, the reward is high.



Practical aspect [demo ;)]

Evil twin attack on EAP is well known, and the tools are widely available.

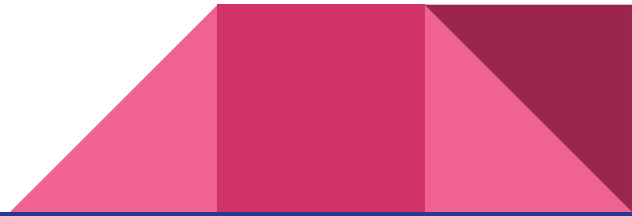
Using Kali Linux and eaphammer it is possible to perform the attack with only two simple commands:

```
# generate certificates
./eaphammer --cert-wizard

# launch attack
./eaphammer -i wlan0 --channel 4 --auth wpa --essid CorpWifi --creds
```

Key takeaways

- Keep all your (Wi-Fi) deviced updated
- Use WPA2 (CCMP) with a complex password
- Turn off Wi-Fi when not in use
- Try switching to 802.11ac (5 GHz)
- **Install the eduroam cert and don’t use PAP!**



Bonus links (software and hardware)

ESP8266 deauther project, "Official" deauther store (clones are cheaper), Alfa AWUS036NHA Wi-Fi card, List of the best Wi-Fi cards (chipset model is what matters), Kali Linux project