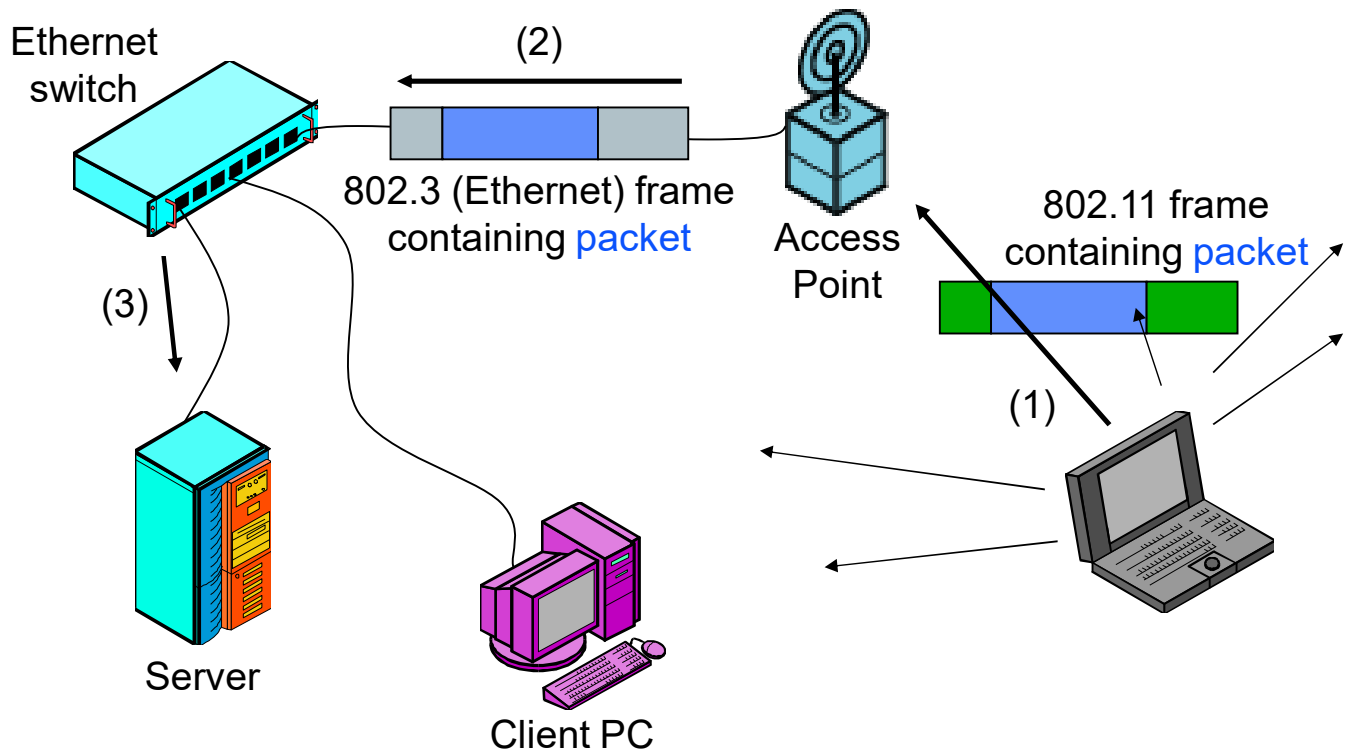
IEEE 802.11 WLAN Security

WEP, WPA, WPA2, WPA3

802.1x

Chapter 18

IEEE 802.11 Wireless LAN (WLAN)



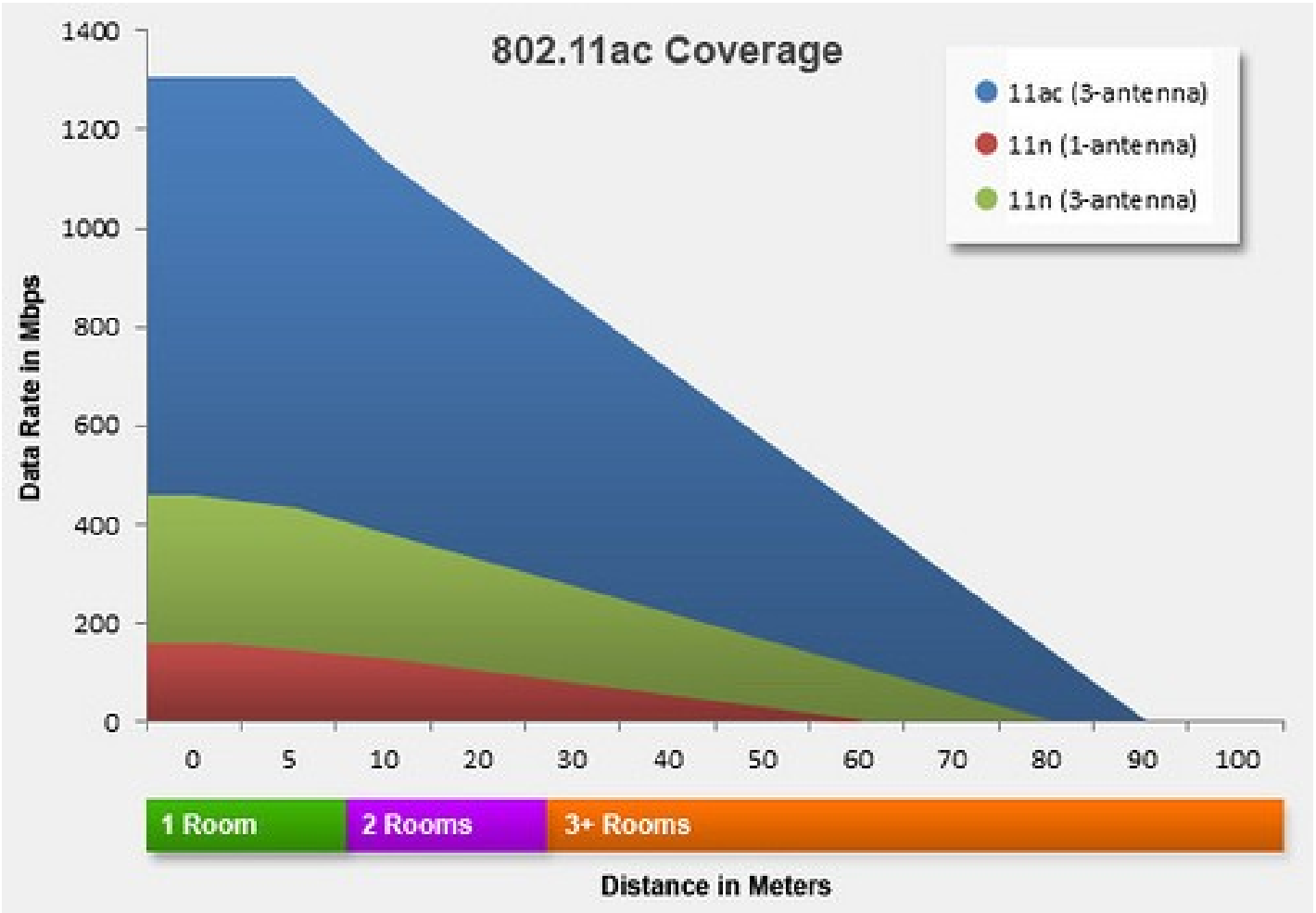
The 802.11 standard

- IEEE standard 1997
- Extensions constantly arrive, mainly in four areas:
  - Performance
  - Functionality (qos)
  - Security
  - Usability (frequency, ranges, …)
- Extensions have a suffix:
  - 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax, … (modulation, frequencies, …)
  - 802.11i for enhanced security (defines WPA and WPA2)
  - 802.11r for secure and fast handover between APs (roaming)
  - etc.

802.11 sub-standards

Wi-Fi Alliance: https://www.wi-fi.org

- Wi-Fi 1: 802.11**a** [1999] – primarily used in the US
  - 54 Mbps, 5 GHz band (forbidden band in most countries at that time)
- Wi-Fi 2: 802.11**b** [1999] – popular in Europe
  - 11 Mbps, 2.4 GHz
- Wi-Fi 3: 802.11**g** [2003] – old but still sometimes used
  - 54 Mbps, 2.4 GHz
- **Wi-Fi 4**: 802.11**n** [2009]
  - 2.4 and 5 GHz, Up to **600 Mbps** theoretical speed with 4 parallel streams (4x4 antennas)
  - Most common: 2 streams → 270 Mbps under perfect conditions
- **Wi-Fi 5**: 802.11**ac** [2014]
  - 867 Mbps (1x1) to 6.77 Gbps (8x8, rare)
- **Wi-Fi 6**: 802.11**ax** [2019] – WPA3 support mandatory now
  - Up to 10 Gbps (in reality about 30% faster than WiFi 5)
  - Better modulation (1024 QAM) for 25% increased speed
  - 4 times as many connected units, lower latency, sleep mode for devices (Target Wakeup Time)
- **Wi-Fi 7**: 802.11**be** [2024]
  - Up to 40 Gbps (16x16)
  - Adds **6 GHz** band, multilink support (parallel usage of multiple channels)
- **Wi-Fi 8**: 802.11**bn** [202?]
  - With a focus on low latency and high reliability



https://www.broadcom.com/

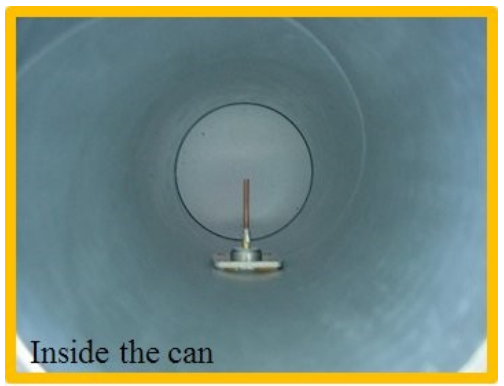
Modes of operation

- Two modes of operation:
  - Ad-hoc mode – computers talk directly to each other
  - Infrastructure mode – traffic goes through an access point (AP)
    - Most common
    - Clients (stations, STA) must form an association with the AP
    - Security mechanisms are WEP, WPA, WPA2 and WPA3
- Several APs can work together
  - Basic Service Set (BSS) = one AP
  - Extended Service Set (ESS) = multiple APs
  - One master controls the other
  - Roaming = re-association with other APs (re-authentication not needed)
  - Example: Eduroam at Chalmers with lots of APs
- The network is identified by a BSSID – Basic Service Set ID
  - The name of the network (“eduroam”, …)

An external antenna can increase range

"A 12 dB can-to-can shot should be able to carry an 11Mbps link well over ten miles."

Note that standard network equipment is used!



- Not legal as transmitter – disturbs other networks
- But eavesdropping can be done far away

A commercial solution

D-Link

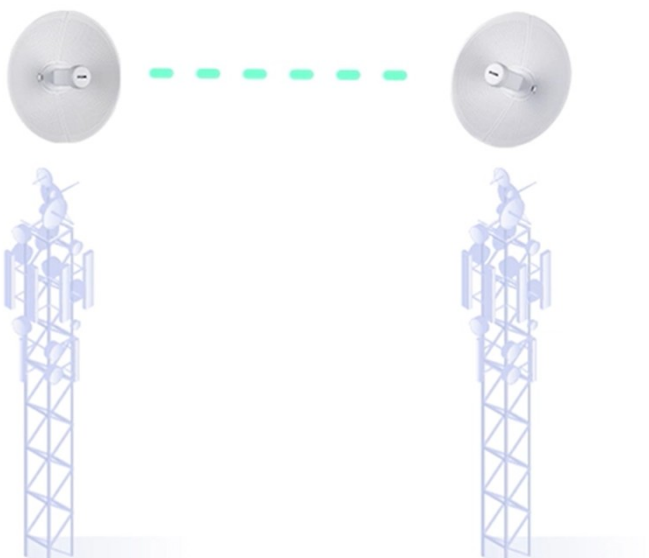
5 km / 20 km Long Range Wireless AC Bridges

Resilient solutions that overcome the challenges of rural areas and tricky terrain to supply stable, high-speed connectivity over vast distances

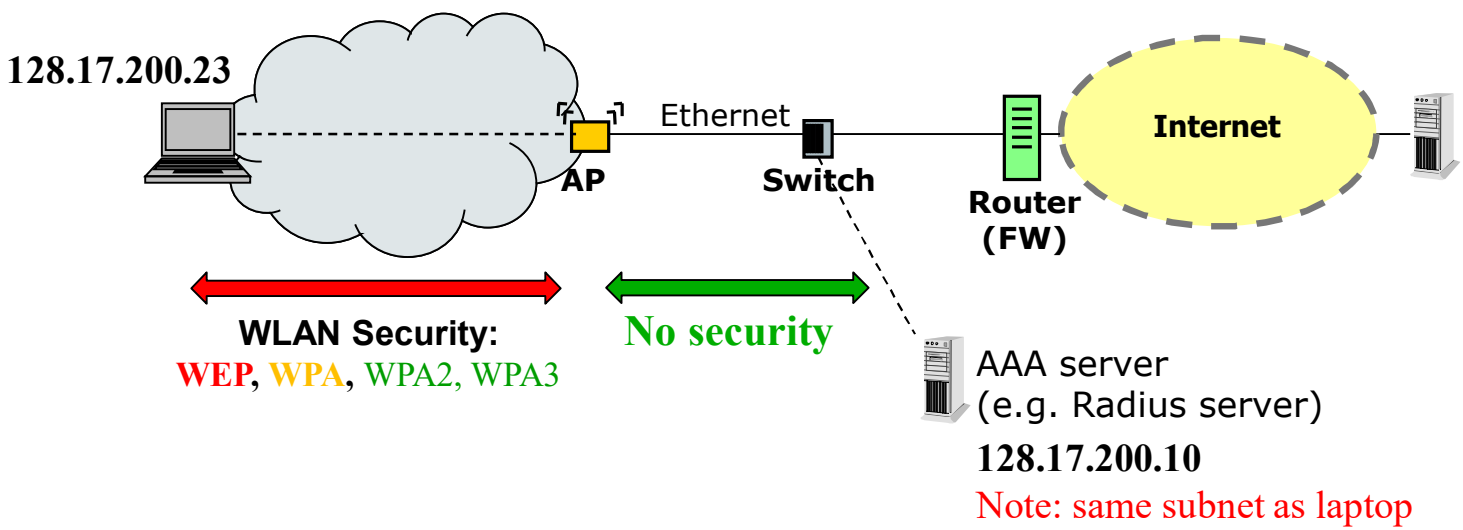
DAP-3711 / DAP-3712

- The DAP-3711 & DAP-3712 feature high-gain 15 and 23 dBi directional antennas, respectively, supplying high-speed, stable coverage to up to 20 km away
- Integrated TDMA Technology cuts through interference to ensure high-speed, consistent coverage
- Superior throughput with single-band transfer speeds of up to 867 Mbps
- Refined design effortlessly blends into any setting
- Stay secure with 128-bit personal and enterprise wireless encryption
- Support for Power over Ethernet means fewer wires, for cleaner and easier deployment
- IP66-rated water-resistant and dust-tight housing means the DAP-3711 & DAP-3712 are suitable for harsh outdoor environments

3,000 SEK



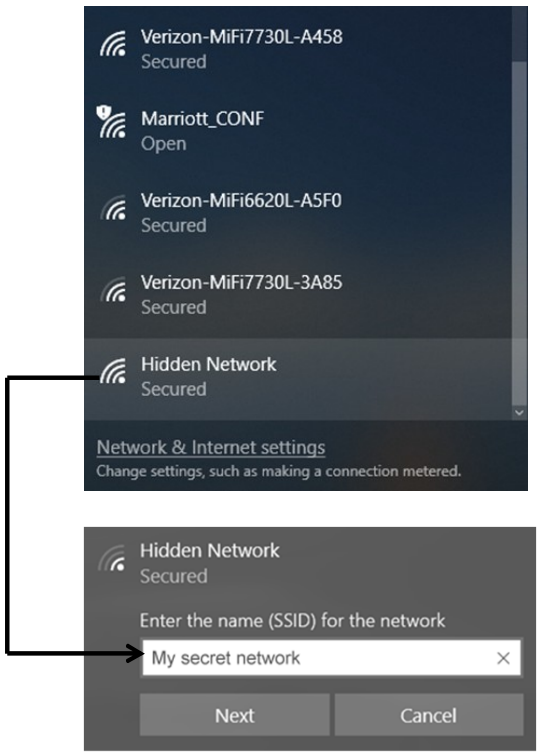
WLAN Security Scope



The AP works on link level. This means that ARP is used to find other hosts on the WLAN + LAN

802.11 WLAN – Basic security

- Must know SSID to connect
  - Frequently broadcasted by the access point to ease discovery
  - SSID broadcasts can be disabled – shown as “Hidden Network” in Windows →
    - But SSID is revealed when devices connect
    - Makes it (a little) harder to discover the network
- Many devices can filter on MAC addresses
  - Only specified devices can connect
  - Hard to do in larger environments
  - MAC addresses can easily be spoofed
- WEP (Wired Equivalent Privacy) was designed to offer good security
  - Confidentiality, Access control and Data integrity
  - But algorithms and implementation were done by cryptographic amateurs
- WPA, WPA2 and WPA3 newer security standards
  - WPA was only intended to be used during a transition period



Connections and faked APs

- Faked AP (e.g. a PC) can be used to fool users to connect
  - Easy to fake any SSID name and become MITM
  - Open access points, for example at airports and hotels, trivial to spoof
  - Someone may fake a previously known AP and “offer” Internet access
  - If encryption was expected by the client, the connection will fail
- Protection can be made on higher level for open APs
  - Use SSH and TLS to encrypt traffic to home networks and own servers
  - The network is just used to transport encrypted network packets
- Clients often search for previously accessed networks
  - If client sees a known network name: it may automatically try to connect
  - Many devices store long lists of previously associated networks
- Some devices constantly send out network probes (e.g. smartphones)
  - Can be used to identify phones, e.g. by shops to discover returning customers

I am Marriott Hotel
and SJ
and Landvetter Airport
and …

Please connect and
you will get Internet access!

Client support

```
> netsh wlan show drivers
Interface name: Wi-Fi

    Driver                     : Intel(R) Wi-Fi 6 AX201 160MHz
    Vendor                     : Intel Corporation
    Type                       : Native Wi-Fi Driver
    Radio types supported      : 802.11b 802.11g 802.11n 802.11a
                                 802.11ac 802.11ax
    FIPS 140-2 mode supported : Yes
    Authentication and cipher supported in infrastructure mode:
                                 Open            None
                                 Open            WEP-40bit
                                 Open            WEP-104bit
                                 Open            WEP
                                 WPA-Enterprise  TKIP
                                 WPA-Enterprise  CCMP
                                 WPA-Personal    TKIP
                                 WPA-Personal    CCMP
                                 WPA2-Enterprise TKIP
                                 WPA2-Enterprise CCMP
                                 WPA2-Personal   TKIP
                                 ...
                                 WPA3-Personal   CCMP
                                 WPA3-Enterprise GCM-256
                                 ...
```

Networks

```
C:>netsh wlan show networks

Interface name : Wireless Network Connection
There are 2 networks currently visible.

SSID 1 : eduroam
    Network type            : Infrastructure
    Authentication          : WPA2-Enterprise
    Encryption              : CCMP

SSID 2 : NOMAD
    Network type            : Infrastructure
    Authentication          : Open
    Encryption              : None
```

File View Help

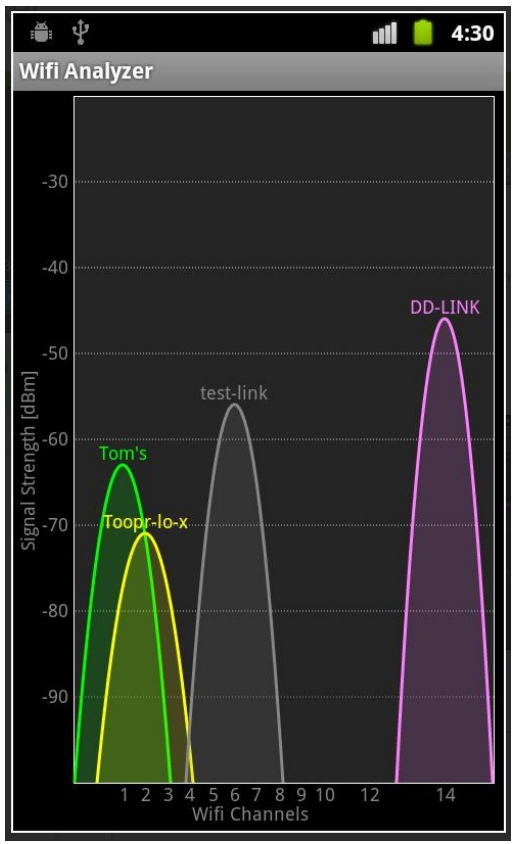
Start GPS | Intel(R) Wireless WiFi Link 4965AGN | Stop

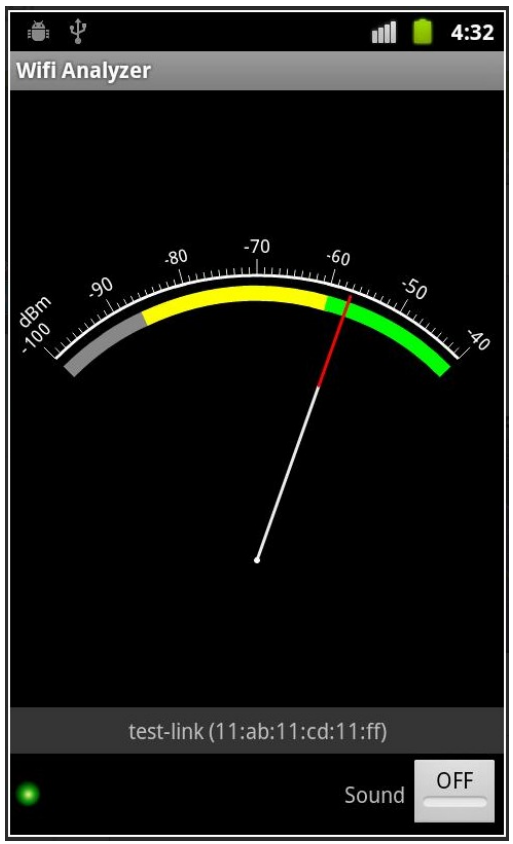
MAC Address	SSID	RSSI	Channel	Vendor	Privacy	Max Rate	Network Type	First Seen	Last Seen	Latitude	Longitude
00:1F:6C:CB:25:01	NOMAD	-78	11	Cisco Systems	None	54	Infrastructure	11:41:40	11:48:07	0,000000	0,000000
00:1F:6C:CB:25:02	eduroam	-70	11	Cisco Systems	RSNA-CCMP	54	Infrastructure	11:41:40	11:48:07	0,000000	0,000000
00:18:4D:99:D5:90	ECT	-65	11	Netgear Inc.	RSNA-CCMP	54	Infrastructure	11:41:40	11:48:07	0,000000	0,000000
00:22:3F:A7:E2:9F	indian	-72	2	Netgear Inc.	RSNA-CCMP	150 (N)	Infrastructure	11:41:40	11:47:55	0,000000	0,000000
14:D6:4D:27:9E:D4	SnelHest	-84	1		RSNA-CCMP	270 (N)	Infrastructure	11:41:40	11:48:07	0,000000	0,000000
F8:1E:DF:F9:20:B5	CLT	-83	6	Apple, Inc	RSNA-CCMP	216 (N)	Infrastructure	11:41:40	11:48:07	0,000000	0,000000
00:02:CF:CA:B9:BE	S.sound	-87	6	ZyGate Commu...	WPA-TKIP	54	Infrastructure	11:41:40	11:48:07	0,000000	0,000000
00:3A:98:3E:B5:6D	eduroam	-85	100	Cisco Systems	RSNA-CCMP	54	Infrastructure	11:41:40	11:48:07	0,000000	0,000000
00:3A:98:3E:B5:6E	NOMAD	-85	100	Cisco Systems	None	54	Infrastructure	11:41:40	11:48:07	0,000000	0,000000
00:1F:6C:CB:25:0E	NOMAD	-85	112	Cisco Systems	None	54	Infrastructure	11:41:40	11:48:03	0,000000	0,000000
00:1E:F7:56:0B:51	NOMAD	-83	6	Cisco Systems	None	54	Infrastructure	11:41:40	11:48:03	0,000000	0,000000
00:1F:6C:CB:25:0D	eduroam	-83	112	Cisco Systems	RSNA-CCMP	54	Infrastructure	11:41:40	11:47:28	0,000000	0,000000
00:3A:98:3E:B5:62	eduroam	-86	6	Cisco Systems	RSNA-CCMP	54	Infrastructure	11:41:51	11:47:55	0,000000	0,000000
00:1E:F7:56:0B:52	eduroam	-80	6	Cisco Systems	RSNA-CCMP	54	Infrastructure	11:41:57	11:48:03	0,000000	0,000000
00:3A:98:3E:B5:61	NOMAD	-86	6	Cisco Systems	None	54	Infrastructure	11:42:06	11:47:45	0,000000	0,000000

News | Time Graph | 2.4 GHz Channels | 5 GHz Channels | Filters | GPS

15 / 15 AP(s) GPS: Off Logging: Off https://www.metageek.net/products/inssider/

WiFi Analyzer for Android



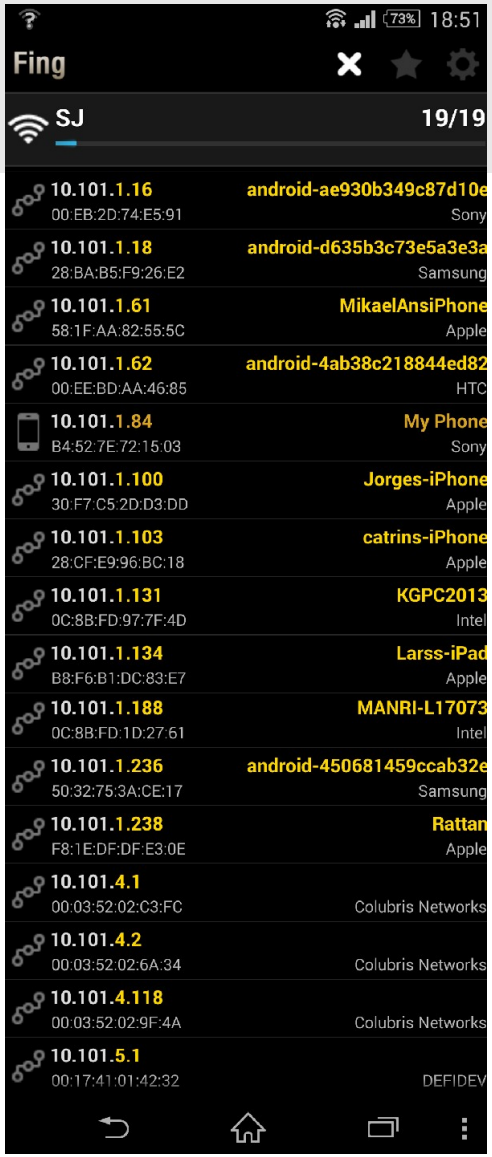


FING

Just one example of on app:

shows all devices connected
to an access point, IP addresses
MAC addresses and brand

Can be used to discover illegal use of own WLANs.
Other apps exist that also warns when new devices are seen on the network!



The law – a reminder

- Swedish law:
  - Not illegal to connect to an open network
  - But may be possible to sue for damages/costs
  - It's illegal to connect to a protected network
- Internet operators don't allow open networks
  - Broadband connections intended for one customer
- If an outsider uses your network for illegal activities, the owner (you?) will be the first to suspect

WEP – Wired Equivalent Privacy

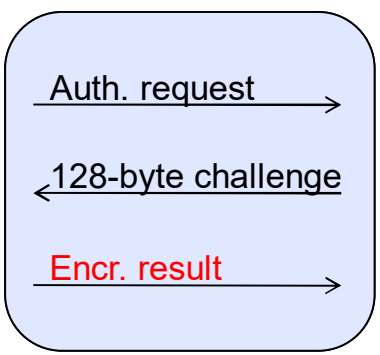
A quick summary can be found in this paper,
What's wrong with WEP?

https://www.opus1.com/www/whitepapers/whatswrongwithwep.pdf

Client Authentication

- Open System Authentication
  - Default, it's a NULL process
  - Wide open even if WEP enabled

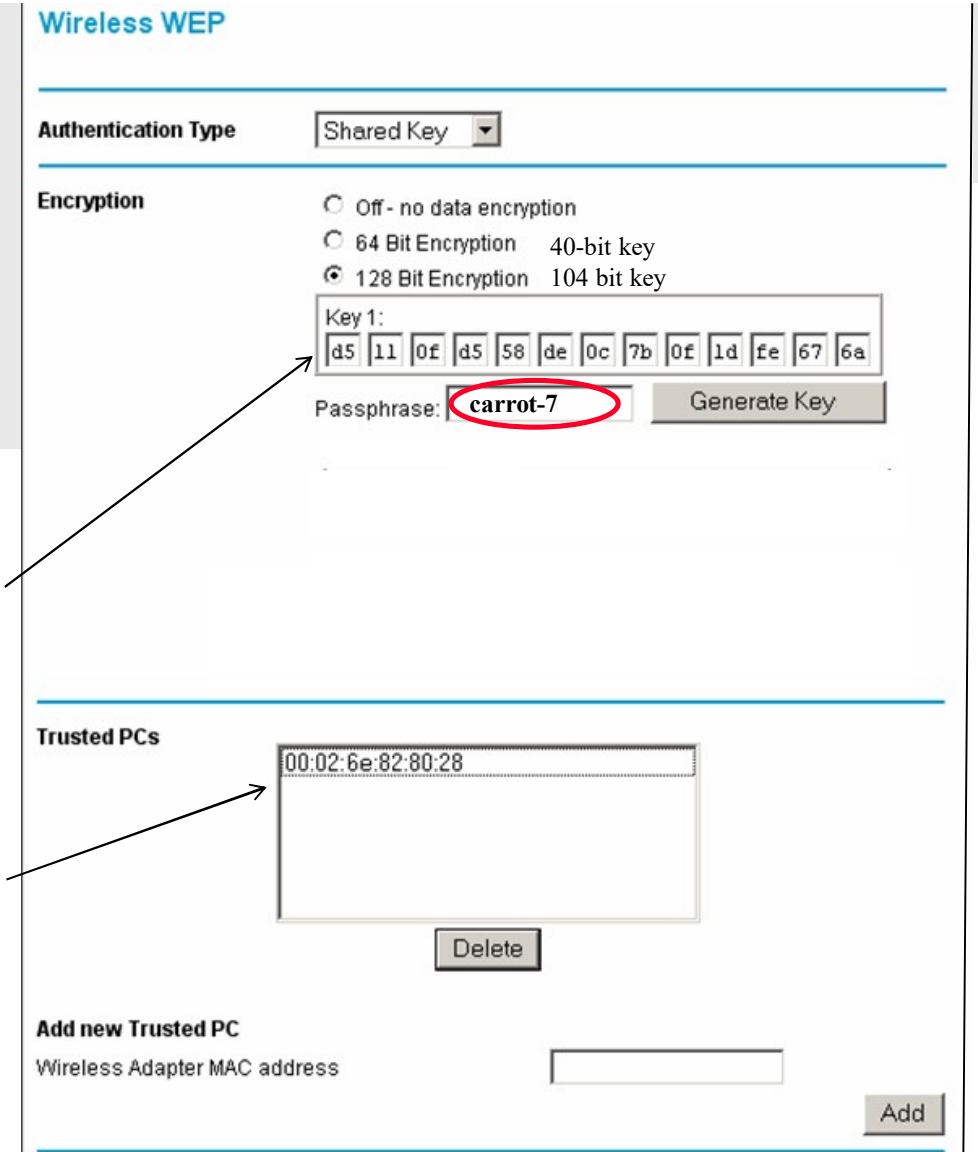
- Shared key Authentication (WEP)
  - Shared key = all devices/users have the same session key
  - Client sends Authentication Request to AP
  - AP sends frame with 128-byte challenge text to client
  - Challenge is encrypted with RC4 using a shared secret and a newly selected IV by the client
  - AP decrypts response and verifies it



Configuring an AP for WEP Shared Key authentication

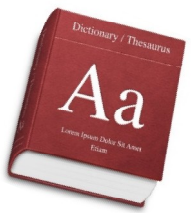
Wep keys Generated from MD5(passphrase) or entered manually

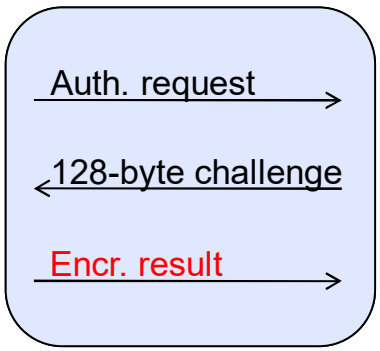
MAC addresses filtering enabled



Dictionary attacks

- WEP: APs use MD5 to generate a key from a user's password
- If both clear-text and cipher-text known:
  - Easy to do dictionary based attacks
  - >100,000 (off-line) guesses per second with a normal CPU
    - If key not random, we get approx. 4-5 bits per character in a password
    - 5 characters: 21 seconds to search all keys
    - 9 characters: 127 days
    - Truly random 104-bit key → Brute force not realistic (10^{19} times harder)

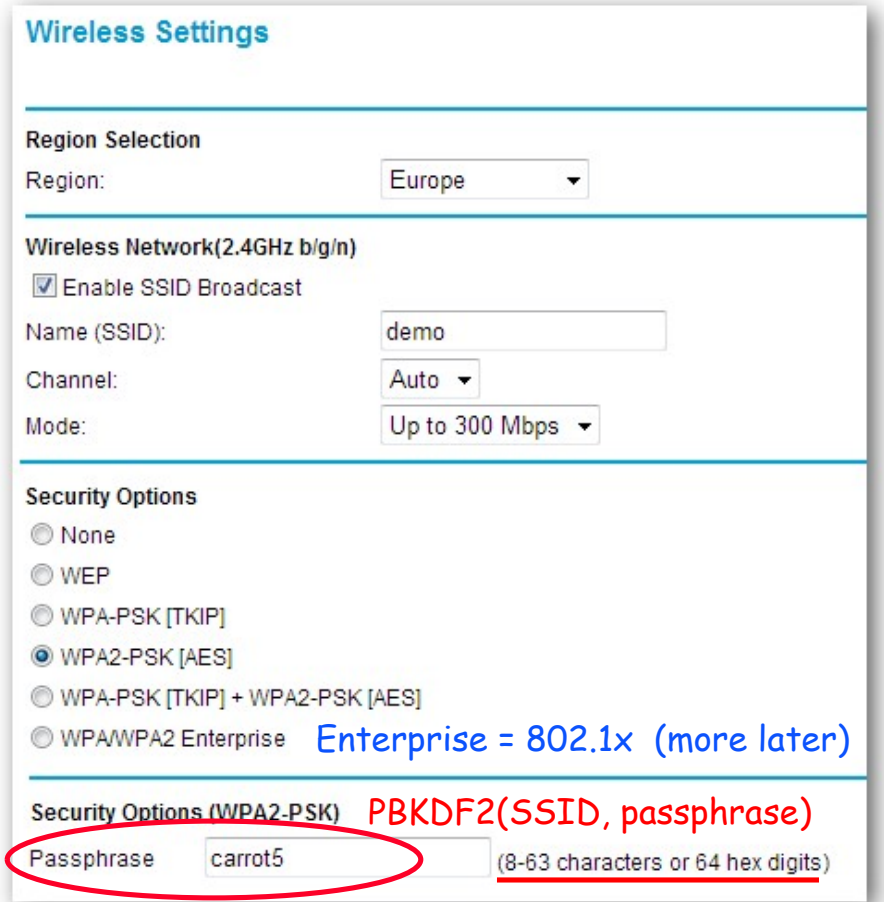




- GPUs, can do this >1000 times faster
  - All 40 bit keys searched in 3 hours [=9 characters]
- Pre-generated dictionaries (rainbow tables) can be created = even faster

- WPA2 better: requires one table per SSID (name)
  - Also performs 4,096 (HMAC) rounds, not just one hash: HMAC(password, SSID)
  - But pre-calculated Rainbow tables exist for well-known network names (dlink, netgear, eduroam, …)
  - Select an uncommon name!

WPA2 requires more work

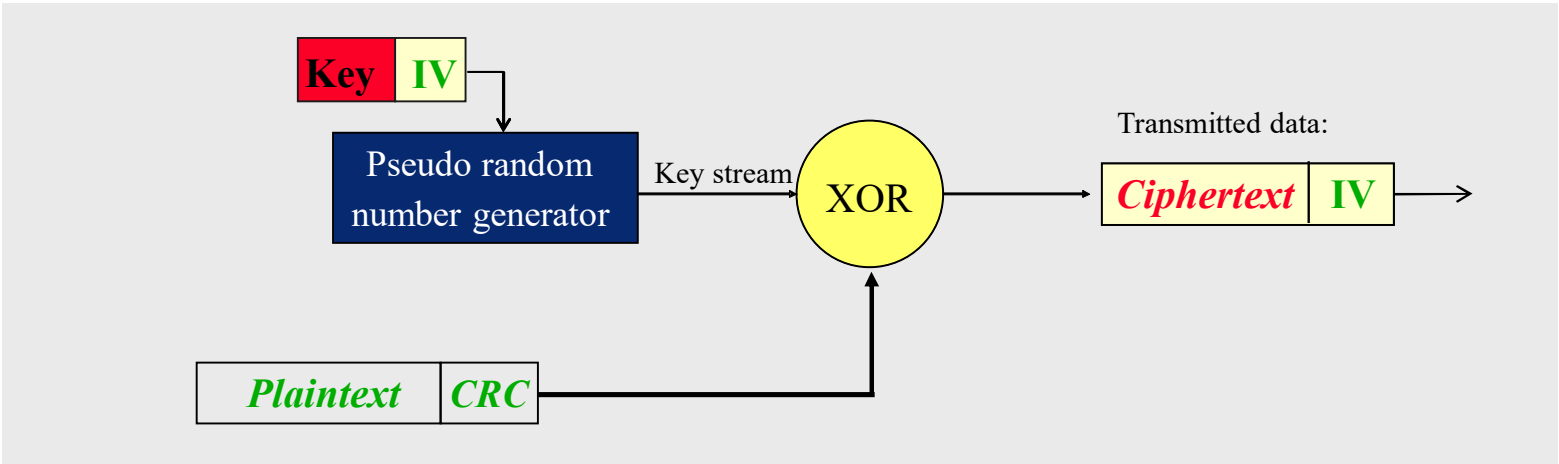


- PBKDF2 = Password-Based Key Derivation Function 2.0
- Uses 4,096 HMAC rounds
- This key is only used to generate session keys (more later)

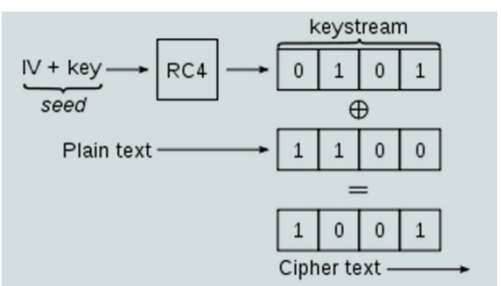
The first attacks against WEP were cryptographic

- WEP standardized 1999
- 2001 - The insecurity of 802.11, N. Borisov, I. Goldberg and D. Wagner: found problems with CRC and reuse of IV:s
- 2001 - Weaknesses in the key scheduling algorithm of RC4. S. Fluhrer, I. Mantin, A. Shamir
- 2002 - Using the (Fluhrer, Mantin, and Shamir) **FMS Attack** to Break WEP: A. Stubblefield, J. Ioannidis, A. Rubin. Requires 4 million packets to crack WEP key through weak keys.
- 2004 - **KoreK**, reduces the complexity of WEP cracking to not need weak keys to require only around 500,000 packets. Today, only around 50,000 packets are needed to break the WEP key. (100 Mbps → 10,000–100,000 packets/s)

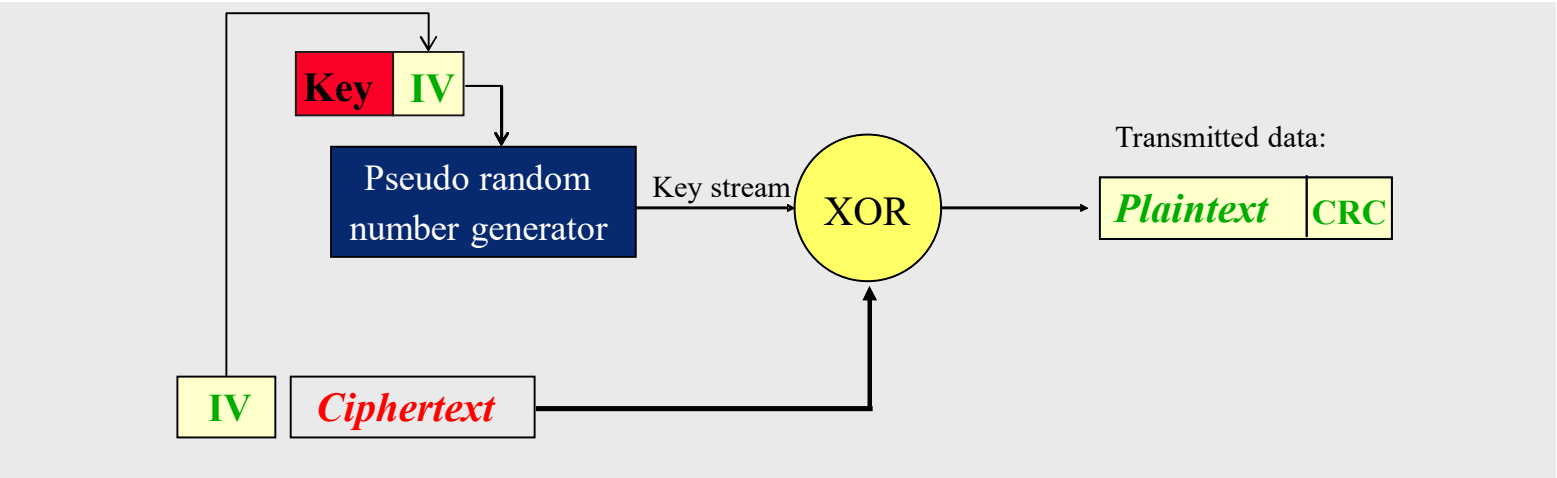
Encryption



- All devices use the same shared key (40 or 104 bits)
- 40 bit key + 24 bit Initialization Vector (IV) = 64 bits input to PRNG
  - Or 104 bit key + 24 bit IV = 128 bits input
  - IV unique for each packet and randomly selected at connection time
  - IV is sent in clear together with encrypted data
- 9,000 IV:s are weak with RC4 (part of the key)
  - Some devices filter them out, most don't

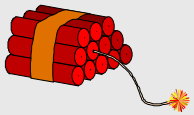


Decryption



- Decryption: same procedure
  - Secret key is shared, IV is found in packet
  - The same key stream is generated by the random number generator
- CRC = Cyclic Redundancy Check = checksum to detect modifications, CRC often used in hardware to detect transmission errors
- 104 bit keys should mean 2^{64} times as hard to crack
  - In reality its about as secure as 40-bit keys

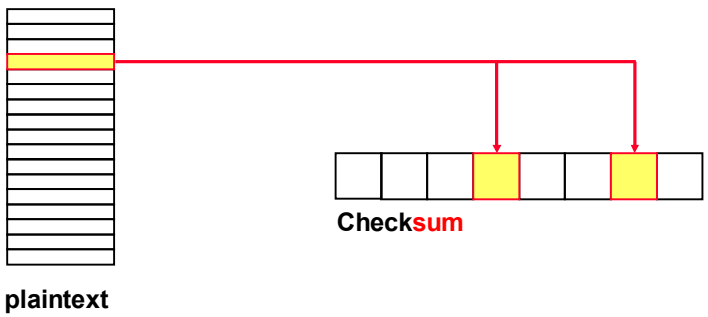
Data encryption in WEP



- Key and IV used to generate an infinite pseudo-random stream to be XORed with the plaintext
- What if two plaintexts encrypted with same stream ***b*** are XOR:ed?
- Then the result is *plaintext1* ⊕ *plaintext2:*
  - ***c***1 ⊕ ***c***2 = (***p***1 ⊕ ***b***) ⊕ (***p***2 ⊕ ***b***) = ***p***1 ⊕ ***p***2 ⊕ ***b*** ⊕ ***b*** = ***p***1 ⊕ ***p***2
  - Now p1 and p2 can be found with statistical analysis of plaintexts (xor is not a cipher…)
- This is why IV is present: to create different streams for similar data
- Many devices started sessions with IV=0, 1, 2, 3, … to guarantee they were unique
  - Problem: With 2 or more devices connected, IV:s will immediately be reused/duplicated
  - Manufacturers were unaware of **why** the IV was used
- A busy AP (54 Mbps for 802.11g → 1000 bytes/packet = 5,000 packets/s) which exhausts the IV space (24 bits = 16M) in less than 1 hour
  - 50% chance of IV collision after only 4,823 packets (<1 second)
  - 99% collision risk after 12,430 packets (2 seconds)

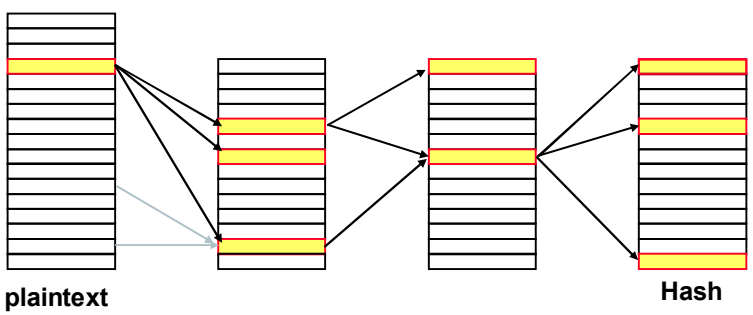
CRC versus Hash functions

CRC:



CRC: When one bit in plaintext is modified, we know exactly what bits to change in the checksum.

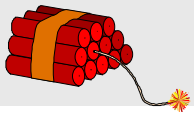
Hash:



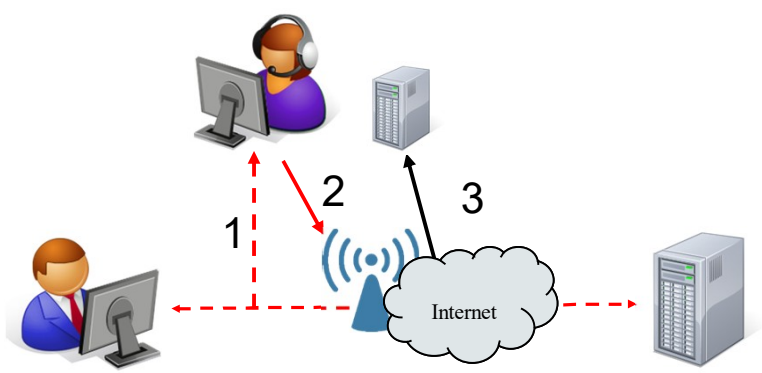
Hash: One modified bit affects more bits in the next step → chaos/avalanche effect.

Impossible to predict result of a change without redoing calculation from the beginning.

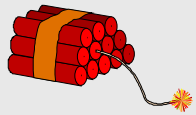
Integrity check in WEP



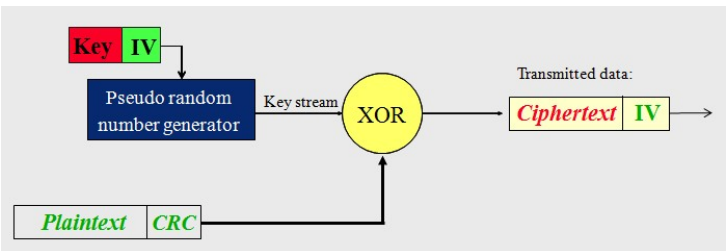
- Observation: Flipping one bit in the Ciphertext, flips the same bit in the plaintext
  - Changing one bit in the input results in a predictable change of the CRC
  - So we can change the checksum to match even if it is encrypted!
- The IP address is normally known or can be guessed
  - Opens up for address modifications (we know where it is located in a datagram)
- Attackers can redirect packets to another computer:
  1. Capture one datagram (encrypted)
  2. Modify IP address – we may have to try a while, but addresses are not random, and send it to the AP
  3. When address is correct, we will receive the datagram in cleartext since encryption ends in the AP
- WEP should have used a non-linear checksum, a hash

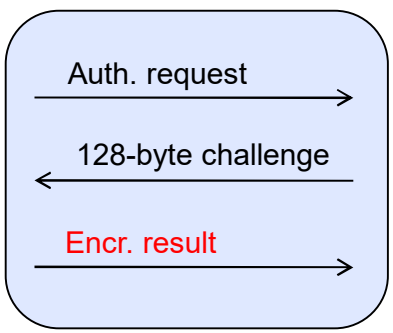


Sending data without the key



- Observations:
  - If plaintext and ciphertext is known, an XOR operation reveals the key stream
  - Knowing a key stream, arbitrary data can be sent
  - WEP allows the same IV, i.e. keystream, to be reused
- How can plaintext data be found?
- In shared key authentication, the AP transmits a 128 byte challenge
  - The client encrypts the data and replies with the ciphertext
  - The same method (IV, key, algorithm) as for data encryption…
- So: challenge ⊕ encrypted_result = key stream for one IV
  - We now have a key stream of 128 bytes to use, to be reused forever
- Knowing n bytes of a keystream, byte n+1 can be found
  - Send a ping with 256 variations of byte n+1 in key stream until success. This can be repeated with n+2, …





Injecting traffic with WEPWedgie

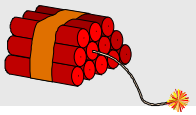
```
wifitest / # prgasnarf -c 1
Auth Frame:  Auth Type: Shared-Key - 00 01:00:01:00
Auth Frame:  Auth Type: Shared-Key - 01 01:00:02:00 :seq = 02 : Challenge Frame?
Auth Frame:  [3]Encrypted Auth Response
Auth Frame:  [4]responder OK with auth

BSSID: 0023ef3f202f     SourceMAC: 0060c10bb76e
Created 136byte PRGA for IV: b9:00:95
Created prgafile.dat in current directory
wifitest / # wepwedgie -h c0:a8:00:be -t c0:a8:00:01 -S 2 -c 1
Pingscanning Selected
Reading prgafile.dat
BSSID:      00:23:ef:3f:20:2f
Source MAC: 00:60:c1:0b:b7:6e
IV:         b9:00:95:00
Pingscan
Setting last byte of target IP to 0 -- scanning 192.168.0.0-192.168.0.255
Injecting Ping....192.168.0.190->192.168.0.0
Injecting Ping....192.168.0.190->192.168.0.1
Injecting Ping....192.168.0.190->192.168.0.2
Injecting Ping....192.168.0.190->192.168.0.3
Injecting Ping....192.168.0.190->192.168.0.4
Injecting Ping....192.168.0.190->192.168.0.5
```

Wait for challenge string and the encrypted result

Use key stream to send an ICMP Echo message!

The FMS and Chopper attacks



- Attacks aiming for the keys (the ultimate goal)
- Fluhrer-Mantin-Shamir attacks (FMS) discovered **2001**
  - Must know one byte of plaintext to work
  - Not a problem since the link layer header has a constant byte
  - 10^6 packets must be collected (= 10-20 minutes)
  - Some Key+IV:s are weak, if found, only 20,000 packets needed = 10 seconds
  - Tools are publicly available: Airsnort and WEPCrack
- Chopper attack (**2004**)
  - Requires collection of unique IV:s
  - Requires 200,000 packets (40-bit keys)
  - And (only) 500,000 packets for 104 bit keys
  - Typically 95% of packets are useful
  - Cracking the key takes from a few seconds to a couple of hours

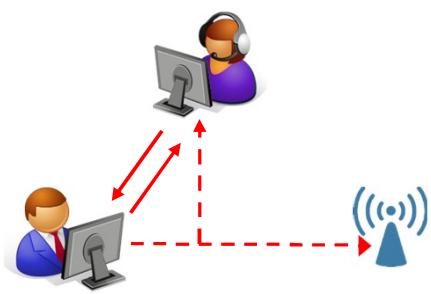
Speeding up the collection of packets

There are now even better attacks against WEP:

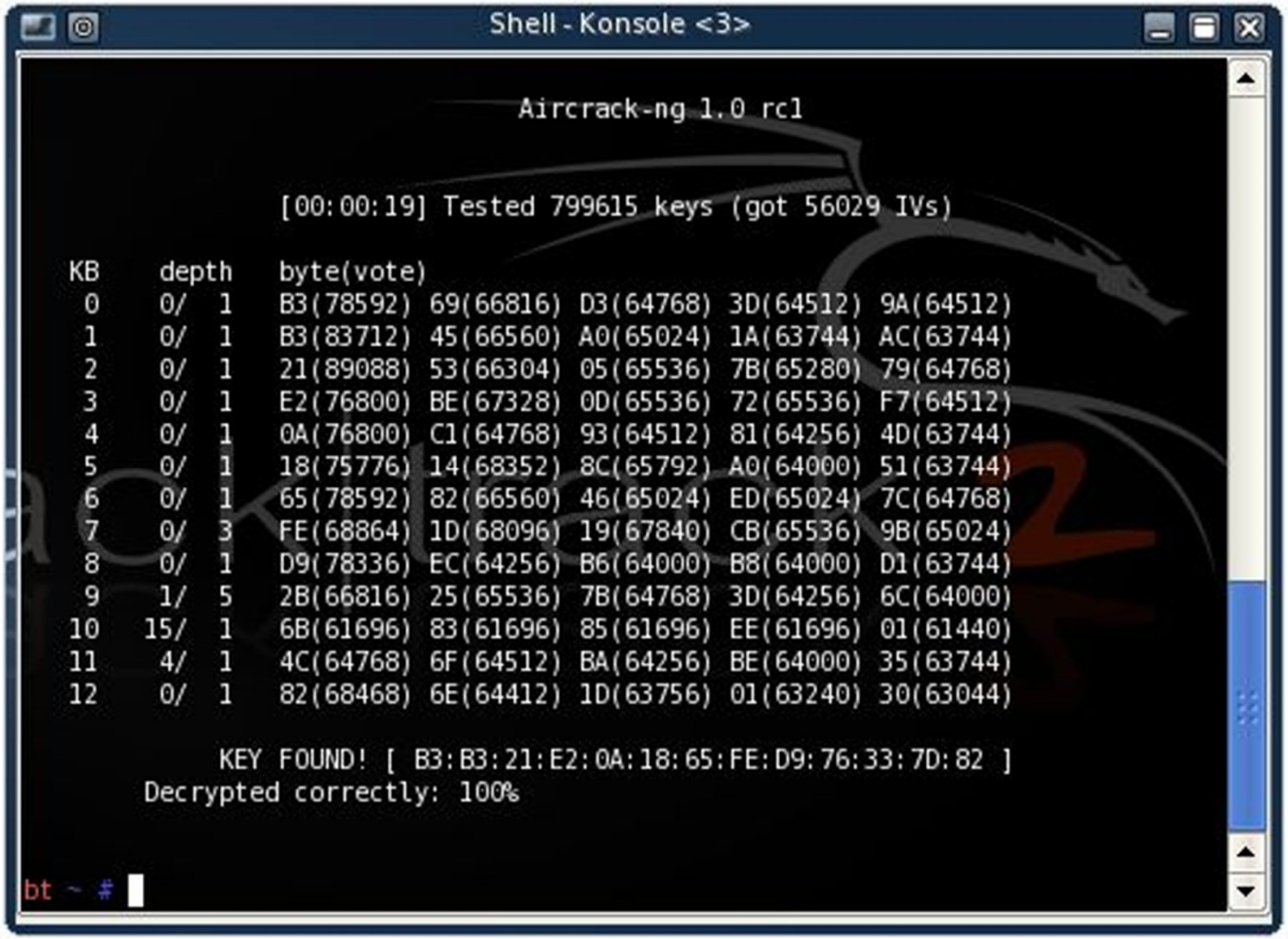
- Bittau, Handley, Lackey: Breaking WEP in less than 60 seconds 2007, University College, London

Idea:

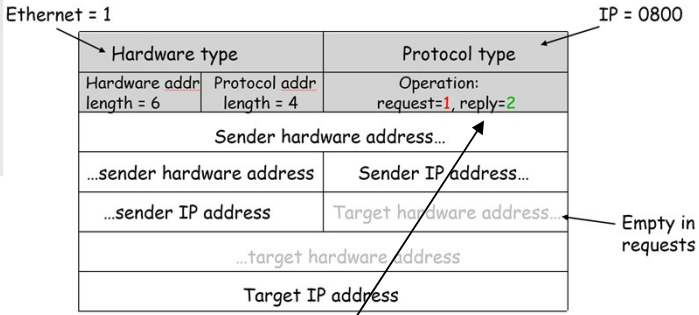
- Speed up the process to get IVs:
  - ARP packets (link-layer protocol) have 16 known bytes in the header (8 bytes in logical link control (LLC) header + 8 bytes ARP header)
  - They are easy to identify due to their unusual length and use of broadcast address
- We can re-inject old ARP requests to get replies – with new IVs
- Tools developed that extract the key given enough packets
  - Takes 53 seconds to gather enough data (40,000 packets)
  - And 3 seconds to calculate the 104-bit key…



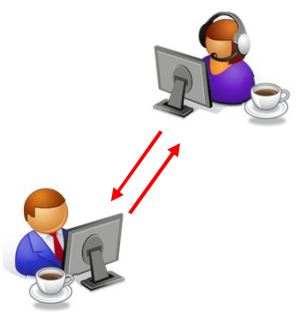
https://eprint.iacr.org/2007/120.pdf


Shell - Konsole <3>
Aircrack-ng 1.0 rc1
[00:00:19] Tested 799615 keys (got 56029 IVs)
KB depth byte(vote)
0 0/ 1 B3(78592) 69(66816) D3(64768) 3D(64512) 9A(64512)
1 0/ 1 B3(83712) 45(66560) A0(65024) 1A(63744) AC(63744)
2 0/ 1 21(89088) 53(66304) 05(65536) 7B(65280) 79(64768)
3 0/ 1 E2(76800) BE(67328) 0D(65536) 72(65536) F7(64512)
4 0/ 1 0A(76800) C1(64768) 93(64512) 81(64256) 4D(63744)
5 0/ 1 18(75776) 14(68352) 8C(65792) A0(64000) 51(63744)
6 0/ 1 65(78592) 82(66560) 46(65024) ED(65024) 7C(64768)
7 0/ 3 FE(68864) 1D(68096) 19(67840) CB(65536) 9B(65024)
8 0/ 1 D9(78336) EC(64256) B6(64000) B8(64000) D1(63744)
9 1/ 5 2B(66816) 25(65536) 7B(64768) 3D(64256) 6C(64000)
10 15/ 1 6B(61696) 83(61696) 85(61696) EE(61696) 01(61440)
11 4/ 1 4C(64768) 6F(64512) BA(64256) BE(64000) 35(63744)
12 0/ 1 82(68468) 6E(64412) 1D(63756) 01(63240) 30(63044)
KEY FOUND! [B3:B3:21:E2:0A:18:65:FE:D9:76:33:7D:82]
Decrypted correctly: 100%
bt ~ #

The Caffe Latte Attack



- The Caffe Latte Attack (Vivek, Sohail) 2007
  - Should be quick enough to work when the owner stops for a cup of coffee…
- Works even if clients are not connected to an AP !!
  - Clients are fooled to connect to a fake AP
  - Fake the name of the AP for which we want the key
- Observation: when connecting, a client sends several (although encrypted) gratuitous ARP messages
  - Attacker fakes the requested AP's SSID and waits for client to connect
  - Client will reuse it's old IP address and sends (an encrypted) gratuitous ARP*: I'm here, my IP address is 11.22.33.44
  - Using the WEP authentication challenge, a 128 bit keystream can be obtained, and with a small modification the ARP reply can become an ARP request
  - Flipping bits in WEP is trivial due to the CRC
  - Now send lots of requests to the client ("who has IP address 11.22.33.44 ?")
  - In 4-5 minutes, 80 000 packets can be received, and it is possible to calculate the key, for example to the user's home network
- Solution: don't use WEP or at least disable "automatic connect"



*Simplified, for more details: https://www.esecurityplanet.com/wireless-security/The-Caffe-Latte-Attack-How-It-Works-and-How-to-Block-It-3716656.htm

Summary of WEP insecurity

- Major weaknesses – lacks most of the features we saw in TLS:
  - No **negotiation** of capabilities
  - **Same key** for authentication and encryption
  - All sessions and devices use the same key (no unique session keys)
  - **No master secret** and no regular key changes (time or amount)
  - **CRC**, not HMAC, with stream cipher allows modification
  - **RC4** with weak keys. After collecting enough traffic, key search is possible
  - **No nonces**, no sequence numbers, replays possible
  - An IV that can be, and will be, reused

- Authentication
  - Shared keys commonly used
  - Entropy in passwords are generally low, dictionary or exhaustive searches possible

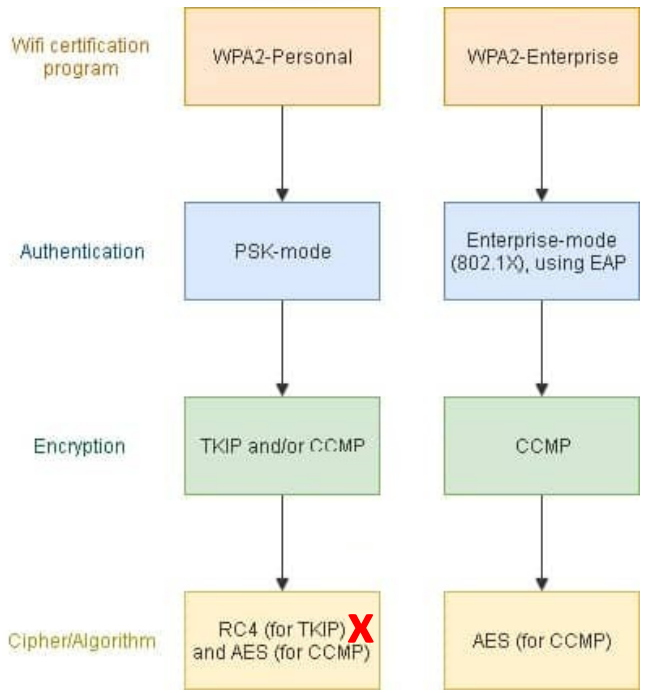
- IV space and design is really bad
  - Too short **IV space**: collisions
  - **Duplicates allowed** - reuse (replays) possible
  - Reused IVs can be used to decrypt data: p1 ⊕ p2
  - **One known plaintext/ciphertext reveals key stream** for IV which can be used forever to transmit data

WPA, WPA2, WPA3

Chapter 18.4

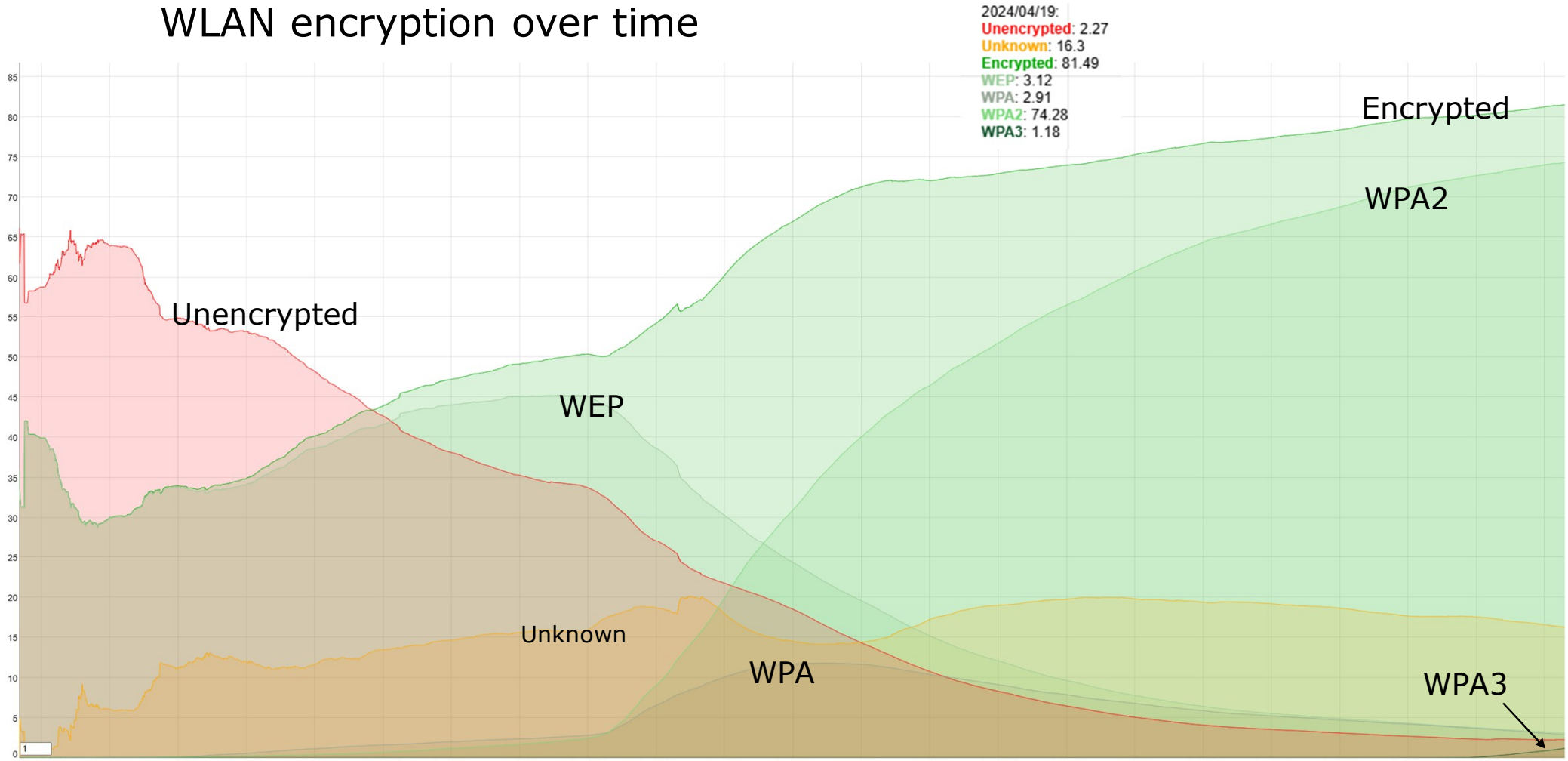
WiFi Protected Access

- **WPA**, Wi-Fi Protected Access – old temporary solution
  - Uses RC4 to allow old hardware to be upgraded to WPA
  - Basic technology in WPA: 802.1x, TKIP
  - TKIP: the temporal key is changed every 10,000 packets and normally also every hour
  - Still uses the insecure RC4 cipher – don't use!
- **WPA2**
  - All certified devices manufactured after 2006 support WPA2
  - Uses 802.1x and CCMP (AES **C**ounter mode with **C**BC **M**AC **P**rotocol)
    - For backward compatibility, TKIP may be supported (and RC4)
  - Personal mode with Pre-shared keys (**PSK**)
  - **Enterprise mode** with Radius for authentication – all stations receive a unique session key created by the Radius server
  - Individual session keys negotiated – stations cannot read each others traffic
  - BUT the session key is derived from the PSK…
- WPA3
  - Released 2018



https://www.comparitech.com/blog/information-security/wpa2-aes-tkip/

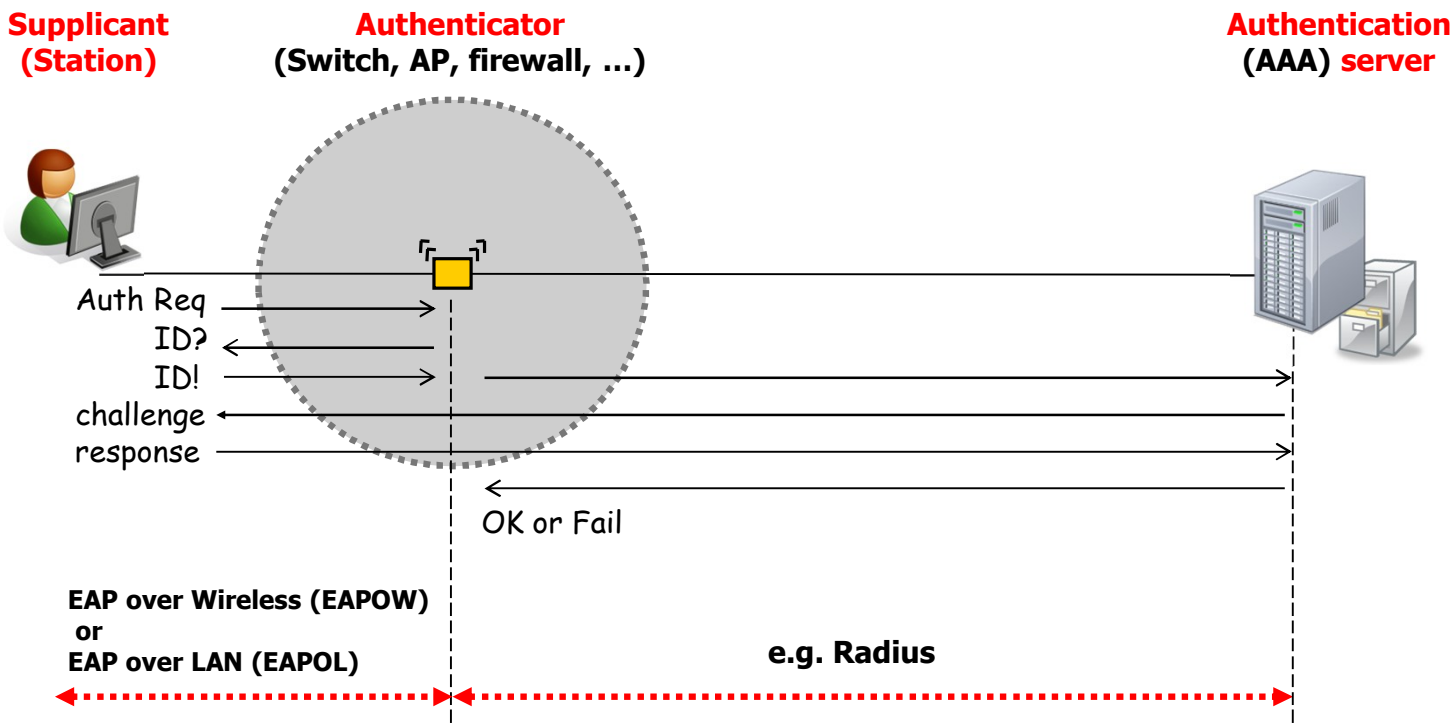
WLAN encryption over time



WIGLE.NET

https://www.wigle.net

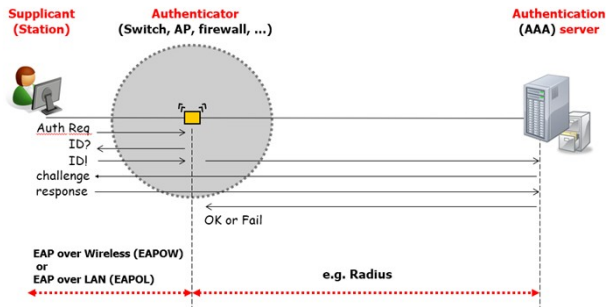
802.1x Port-based access control



After User Authentication, the port is opened
All traffic is now allowed from this port (all MAC addresses)

802.1x Port-based network access control

- Link-level protocol, active before a device gets an IP address
  - For all 802 standards, wired and wireless
- No access unless authenticated
- Provides centralized authentication and dynamic key distribution
  - Supported by all major operating systems today
  - Supports many authentication methods, including certificates at both sides
  - Uses EAP – extensible authentication protocol [RFC 4017]
  - Has names like EAP-OTP (one-time passwords), EAP-TLS (TLS with server and client certificates), EAP-TTLS (Tunneled TLS with server certificates and client passwords), etc.
- No encryption of network traffic
  - No big problem when having a wired connection (see link-level lecture)
  - In WLANs encryption is handled by WPA/WPA2/WPA3
- In WLAN, the use of 802.1x with Radius authentication is called Enterprise Mode
  - The Authenticator (AP) can receive a user-unique session key from the AAA server
  - In Personal Mode when pre-shared keys (PSK) are used, 802.1x is not used



WPA and WPA2 Phases – Overview

1. Discovery phase - agree on capabilities
   - Cipher suite: TKIP (WPA), CCMP (WPA2), …
   - Authentication and key management: PSK, 802.1x (Radius)
2. Authentication phase
   - This phase skipped if PSK used
   - *Derive a (pairwise) master key* (**PMK**) between station and AP
   - PMK can also be received from Radius server (AS)
3. Key management phase
   - "Four way handshake" (see later)
   - Derive *pairwise transient keys* (**PTK**) for encryption (session keys)
   - Receive *group transient key* (**GTK**) from AP for broadcast messages, e.g. ARP
4. Protected data transfer phase
   - TKIP for WPA
   - AES CCMP – Counter mode with CBC (Cipher Block Chaining) MAC Protocol, for WPA2

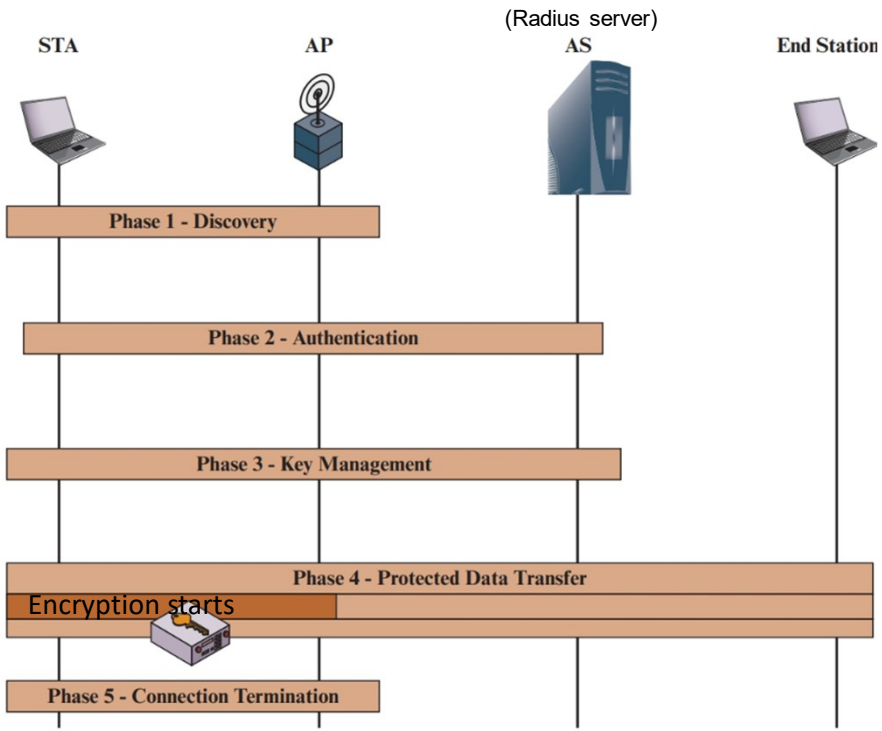


Fig. 18.7

https://tldp.org/HOWTO/html_single/8021X-HOWTO/#what8021x

1. Discovery phase

Agree on security capabilities

2. Authentication phase (802.1x protocol)

Many authentication methods supported

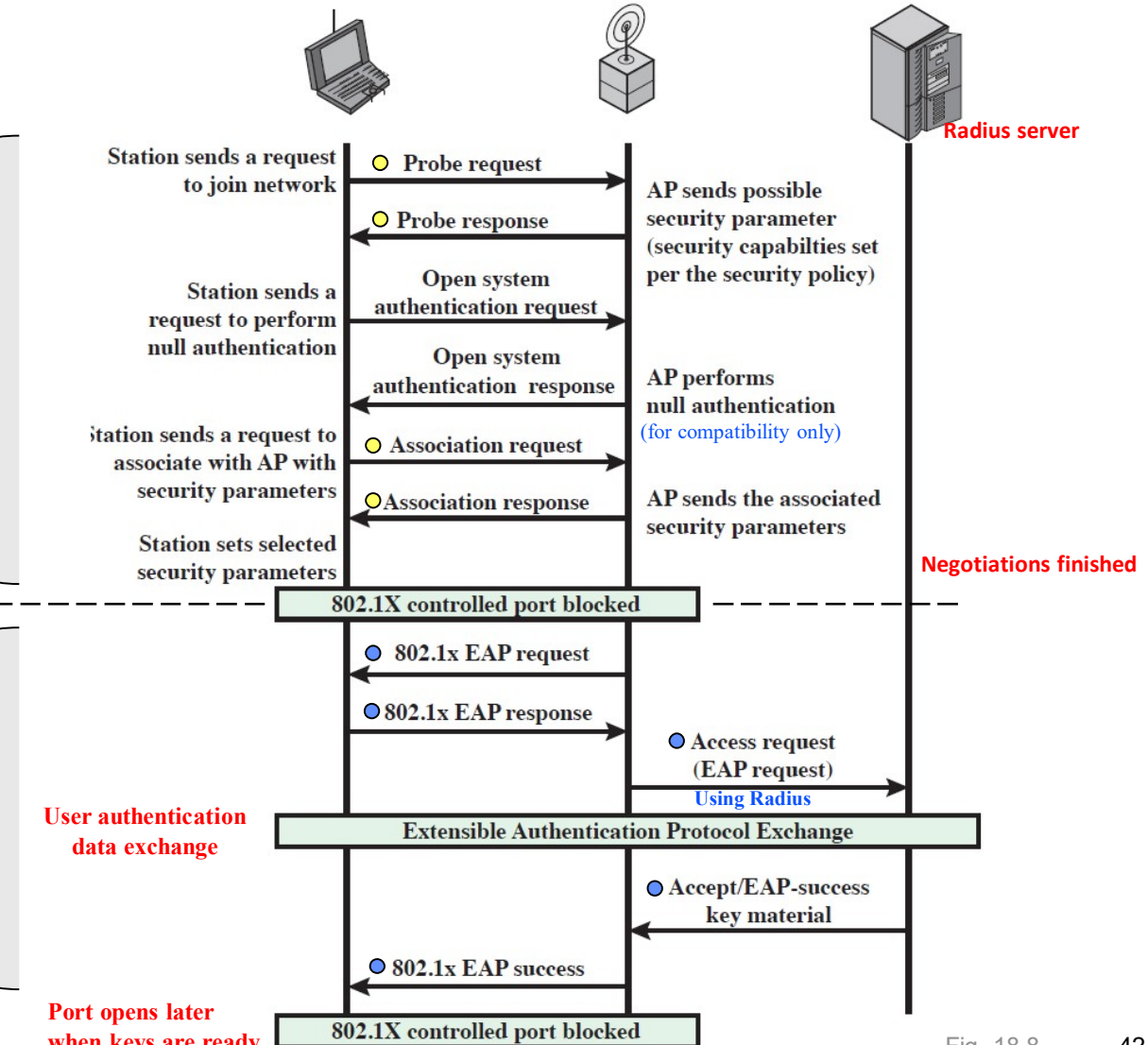


Fig. 18.8

3. Key management phase

Some simplifications done here, see standard for details

256-bit Pairwise master key (**PMK**) is either:

- If a pre-shared key (PSK) used:
  PMK = HMAC-SHA-1 (PSK, SSID) 4,096 rounds
- Enterprise mode: a **random PMK is derived from secret info** the Supplicant and the Radius server share (secret unknown to Authenticator)

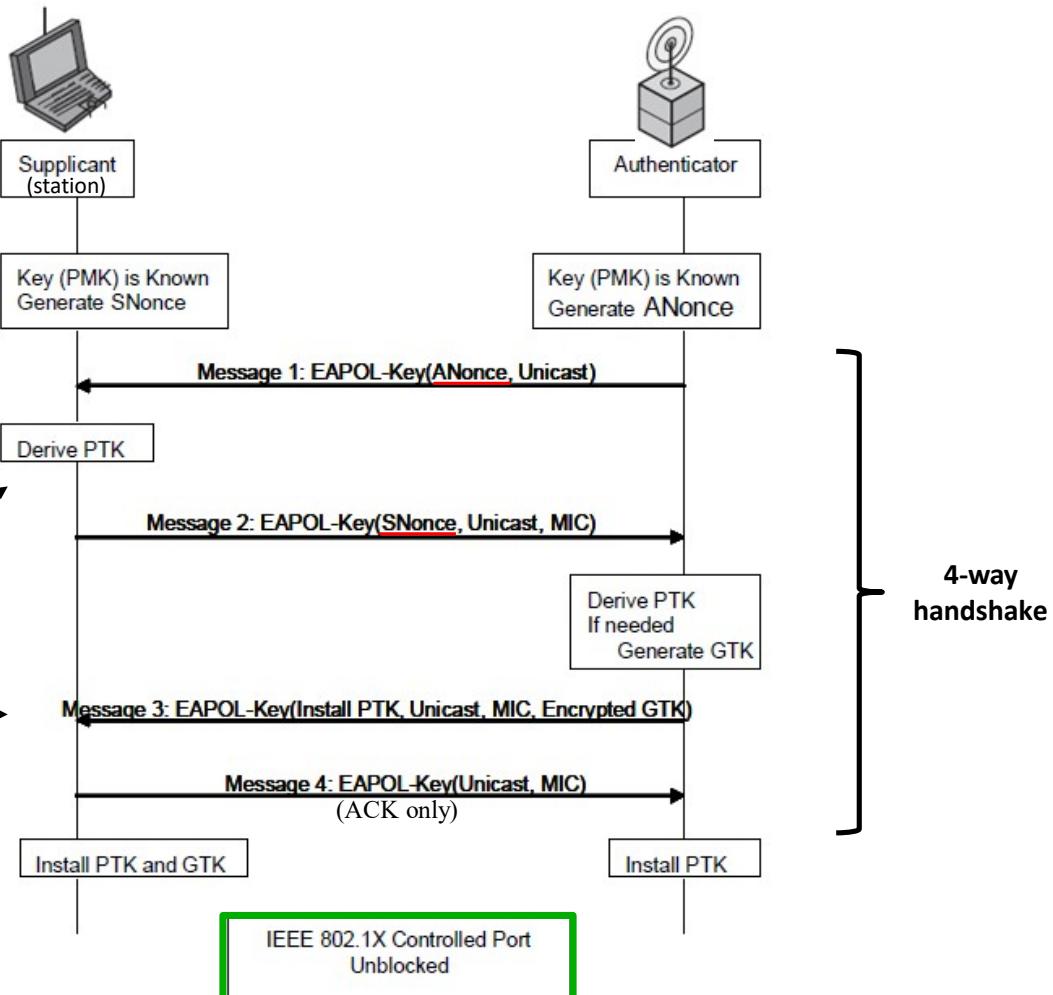
Pairwise transient key
PTK = HMAC-SHA-1(nonces, MACs, PMK)

GTK = Group transient key used for broadcasts. New key is created when a client leaves the group (de-authenticates)

Both sides participate in key generation

Both sides demonstrate that they are live and know the PMK (MIC in message 2 and 3)

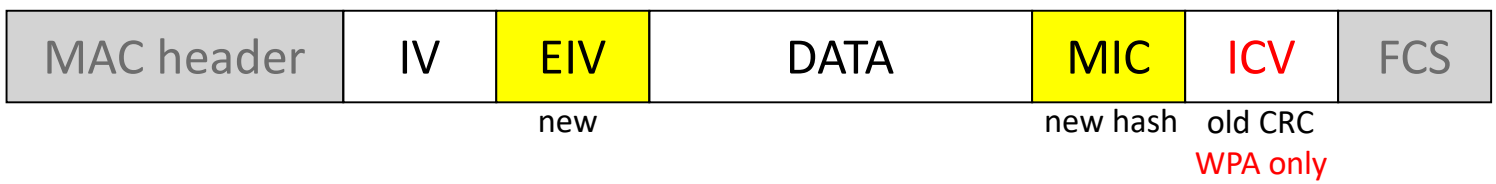
A station knowing the PSK can also derive other stations PTKs since they know the PMK and can see the Nonces!
Wireshark will do this if it knows the PSK…



EAPOL = EAP over LAN
MIC = Message Integrity Check (≈keyed hash/HMAC)

Fig. 18.10

Packet format: WPA and WPA2



MAC header = link-level addresses, etc.
FCS = Frame Check Sequence (link level to detect bit errors in transmission)

IV = Initialization Vector (same as in WEP, 24 bits) 2^{24} = 16,777,216
EIV = Extended IV (24 bits)
MIC = new Message Integrity Code (hash) which also covers MAC addresses
ICV = Integrity Check Value = old WEP CRC used for compatibility by WPA (only)

More about keys

- Each packet has a unique sequence number
  - The ***Nonces*** are incremented for each transmitted package
  - Packets must be received in order (no replays)
  - Packets are encrypted with *f(PTK, sender_MAC_address, nonce)*
  - Nonce makes sure each packet is encrypted differently
- Personal mode: 256-bit Pre-shared keys are used
  - WPA2: hash is 4,096 iterations of HMAC-SHA-1
  - No forward secrecy: PTK = f(nonces, MAC, psk, SSID)
  - Pre-generated rainbow tables exist
  - Don't use popular SSID names (e.g. top 1,000)
  - Routers start to use more random SSID names e.g. "linksys_24a8f9"
- To be even more secure: use Enterprise mode !

Attacks and Weaknesses

Dictionary attacks always possible

- Hashcat or another tool can then be used to spawn dictionary attacks against the pre-shared key (PSK):
  PMK = **HMAC-SHA-1** (PSK, SSID)   4,096 rounds
  PTK = **HMAC-SHA-1** (nonces, MACs, PMK)

- -

- Hacking WPA Passwords with Cowpatty:
  https://www.youtube.com/watch?v=GAuiXr8mwOE&feature=fvwrel

- Watch 6:45 – 14:15

Each of the following links below are to a .torrent file which enables you to download a Cowpatty WPA Rainbow Table using BitTorrent. All of the tables are SSID specific and use a 49 million WPA optimised password dictionary file. Please take note that each of the tables is 1.9 GB in size. We ask that you help in seeding these torrents when you are finished downloading them.

1. 101.WPA
2. 130.WPA
3. 188.WPA
4. 2WIRE236.WPA
5. 2WIRE631.WPA
6. 3BLINDMICE.WPA
7. 3COM.WPA
8. 5ECUR3W3P5TOR3.WPA
9. ACTIONTEC.WPA
10. ADSL_WIFI.WPA
11. AIRPORTTHRU.WPA
12. AIRPORT.WPA
13. ALICE_WLAN.WPA
14. ALICE-WLAN.WPA
15. AMD_IBSS.WPA
16. ANY.WPA
17. ARESCOM.WPA
18. ATTWIFI.WPA
19. BELKIN54G.WPA
20. BELKIN.WPA
21. BESTBUY.WPA
22. BLITZZ.WPA
23. BOB.WPA
24. BUFFALO.WPA
25. CHRIS.WPA
26. COMCAST.WPA
27. CONEXANT.WPA
28. CONNECTIONPOINT.WPA
29. UNIVERSITY_OF_WASHINGTON.WPA

1. GOLDENTREE.WPA
2. GUEST.WPA
3. HARVARD_UNIVERSITY.WPA
4. HAWKING.WPA
5. HHONORS.WPA
6. HOLIDAYINN.WPA
7. HOME1.WPA
8. HOME_NETWORK.WPA
9. HOMENETWORK.WPA
10. HOMENET.WPA
11. HOMEOFFICE.WPA
12. HOMERUN.WPA
13. HOME_WIRELESS.WPA
14. HOMEWIRELESS.WPA
15. HOME.WPA
16. HOUSE.WPA
17. HPSETUP.WPA
18. IBAHN.WPA
19. IBM.WPA
20. INFIDEL.WPA
21. INTERMEC.WPA
22. INTERNET.WPA
23. IU_WIRELESS.WPA
24. KABELINTERNET.WPA
25. LAQUINTA.WPA
26. LINKSYS1.WPA
27. LINKSYS2.WPA
28. LINKSYS_G.WPA

WPA Rainbow tables for AP:s in alphabetical order (list truncated)

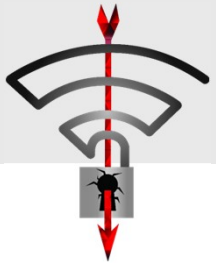
Hash (password, SSID)

Rainbow tables by SSID popularity

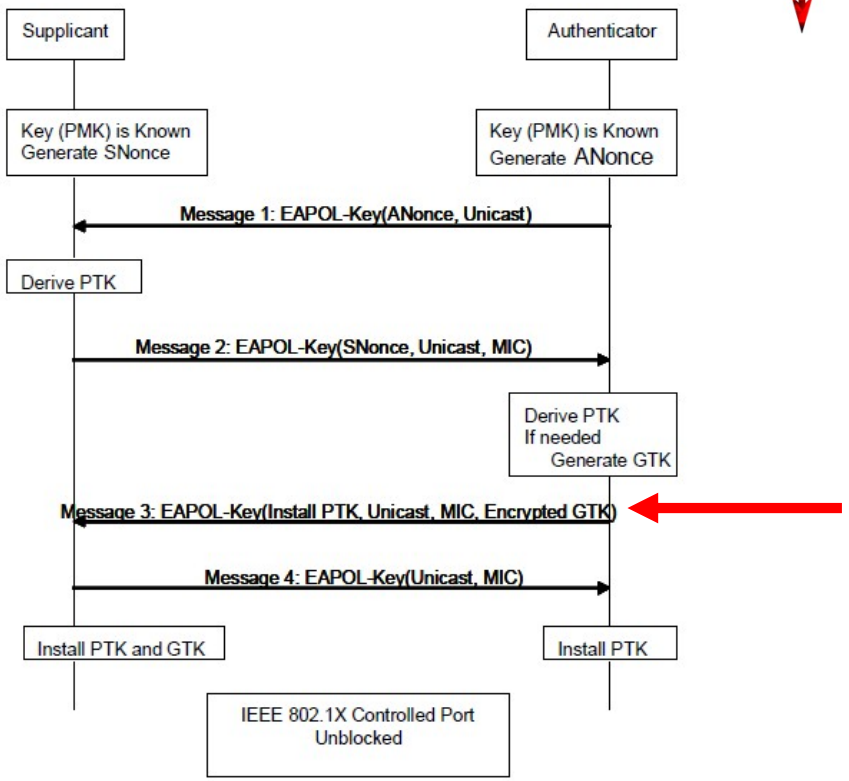
SSID	total	%
xfinitywifi	13,717,239	2.14%
XFINITY	3,192,885	0.50%
BTWiFi-with-FON	3,115,074	0.49%
linksys	3,114,223	0.49%
<no ssid>	2,590,873	0.40%
BTWifi-X	2,517,149	0.39%
AndroidAP	2,113,127	0.33%
UPC Wi-Free	2,095,575	0.33%
Ziggo	1,672,108	0.26%
NETGEAR	1,556,924	0.24%
Telekom_FON	1,453,876	0.23%
eduroam	1,381,070	0.22%
FreeWifi	1,235,920	0.19%
optimumwifi	1,132,432	0.18%
FreeWifi_secure	1,131,057	0.18%
dlink	1,060,689	0.17%
cablewifi	996,636	0.16%
FRITZ!Box 7490	897,982	0.14%
iPhone	885,952	0.14%
KPN Fon	872,488	0.14%
hpsetup	858,584	0.13%
Virgin media	844,051	0.13%
default	839,363	0.13%
TelenetWiFree	717,623	0.11%
asus	700,243	0.11%
Vodafone Hotspot	698,945	0.11%
orange	664,046	0.10%
" (Cloaked)	615,206	0.10%
SFR WiFi Mobile	610,432	0.10%
TELENETHOMESPOT	606,200	0.09%
BTWIFI	589,686	0.09%
Unitymedia WifiSpot	564,054	0.09%
Vodafone Homespot	545,989	0.09%
Guest	537,501	0.08%
Telstra AIR	529,601	0.08%
Fon WiFi	524,438	0.08%

https://www.wigle.net

KRACK – The key reinstallation attack

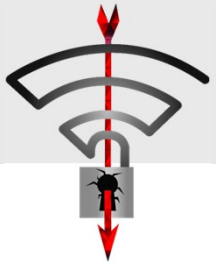


- Tricks the victim to reinstall the crypto keys
- Receivers will accept Message 3 at arbitrary times – not good ☹
  - Causes the transmit and receive packet numbers (nonces) to be reset to their initial values
- As a result, the same encryption key is used which has been used in the past
  - This causes WPA2 to reuse the keystream when encrypting packets
  - Compare with WEP!
- Even worse: Linux and Android installs an all-zero encryption key
  - The Wi-Fi standard suggests to clear the encryption key from memory once it has been installed the first time… ☹
  - See https://youtu.be/Oh4WURZoR98



Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake

KRACK FAQ



How did you [Mathy Vanhoef] discover these vulnerabilities?

– It was at that time that a particular call to *ic_set_key* caught my attention. This function is called when processing message 3 of the 4-way handshake, and it installs the pairwise key to the driver.

  While staring at that line of code I thought *"Ha. I wonder what happens if that function is called twice"*. At the time I (correctly) guessed that calling it twice might reset the nonces associated to the key.

The 4-way handshake was mathematically proven as secure. How is your attack possible?

– The formal models did not define when a negotiated key should be installed. In practice, this means the same key can be installed multiple times, thereby resetting nonces and replay counters used by the encryption protocol

WPA 3 (2018)

WPA3 at a glance

WPA3-Personal

- WPA3 mandatory for WiFi 6 certified devices
- 128-bit encryption keys with **forward secrecy!**
  - WPA2 has no forward secrecy:
    SSID + password -> master key -> session key
- Encryption also in open networks lacking authentication ("Opportunistic Wireless Encryption")
- Simultaneous Authentication of Equals (SAE)
  - New handshake using Diffie-Hellman
    master_key = f(D-H, password, MAC address)
  - Makes PSK resistant to offline dictionary attacks
  - Both sides know the other is in possession of the key
  - Based on Dragonfly key exchange (RFC 7664)
- Wi-Fi Easy connect: Support for IoT devices without user interface
  - QR code or printed number support
  - Uses "Device Provisioning Protocol (DPP)" – mobile phones can be used to pair or connect other devices

WPA3-Enterprise

- Strong enough to protect corporate networks
- 192-bit minimum-strength keys and HMAC-SHA384
- Elliptic Curve Diffie-Hellman (ECDH) key exchange
- Elliptic Curve Digital Signature Algorithm (ECDSA) for **authentication**
- **Encryption**: 256-bit Galois/Counter Mode Protocol (GCMP-256)

https://www.wi-fi.org/discover-wi-fi/security

Dragonblood – April 2019

- Researchers found problems in WPA3's secure handshake (SAE/Dragonfly)
  - Affected by password partitioning attacks (dictionary attacks abusing timing or cache-based side-channel leaks)
  - Brute-forcing all 8-character lowercase password requires less than 125$ in Amazon cloud instances
- "We believe that WPA3 does not meet the standards of a modern security protocol. Moreover, we believe that our attacks could have been avoided if the Wi-Fi Alliance created the WPA3 certification in a more open manner."
- The standard has been updated with proper defenses ☺

https://papers.mathyvanhoef.com/dragonblood.pdf

Summary and Recommendations

- **Goal: the only possible attack should be an exhausted search with passwords**
- Enable and use WPA3, WPA2, WPA and WEP in this order (WEP is still better than nothing)
- Change the default SSID to something difficult not commonly used (PSK)
- Disable SSID? Forces attackers to wait until someone connects to see SSID
- Use MAC address filtering?
- Use a virtual private network (VPN) if possible (IPsec, SSH or TLS) to encrypt traffic
- Link-level attacks are possible between all connected devices
- Scan regularly for rogue access points
- Make sure passphrase is random and long enough!
- Use a Radius server (Enterprise mode) instead of pre-shared keys
- Treat all WLAN systems as external – send traffic to internal LAN through firewall