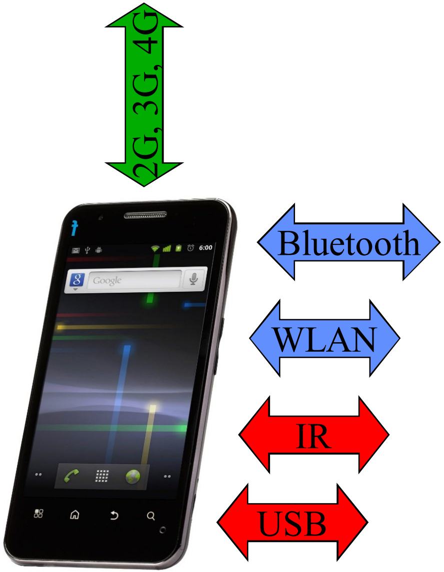
IEEE 802.11 WLAN and Security

Tomas Olovsson

Computer Science and Engineering

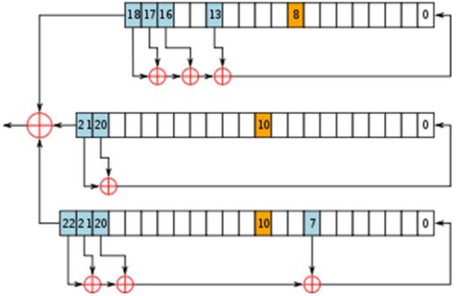
All links in a chain must be secured



- Modern devices communicate through different channels
- One weakness in one protocol is enough
- Smartphones have advanced IP stacks with bugs and “features”
- 2G, 3G, 4G, 5G and WLAN give the devices IP addresses on the networks
- WLAN and Bluetooth have their own security issues

Security in GSM

- Main security functions:
  - Ensuring the identity of the holder
    - Authentication using the SIM card (card requires PIN to do operations)
    - A3/A8 (operator dependent ciphers)
  - Encrypting the communication (for confidentiality)
    - A5/1 ciper used by most operators today
  - Also contains device integrity, secure boot, DRM etc.
- A5/1 is one of seven A5 ciphers (not all used)
  - Based on linear feedback ciphers
  - Designed 1987
- Tried to keep design secret
  - Leaked 1994
  - Broken 1998
  - Many academic papers exist, several vulnerabilities found
  - NSA routinely decrypt messages [Snowden 2013]



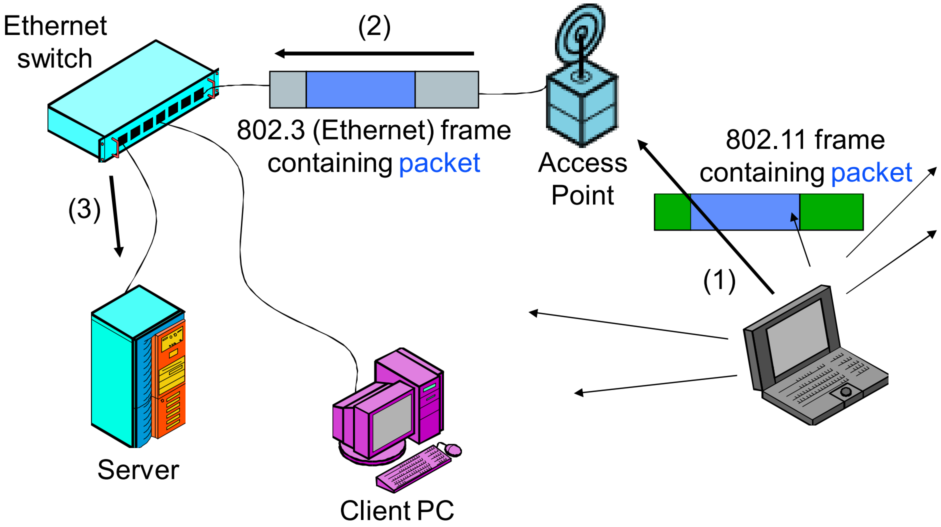
Don’t invent your own ciphers!

- 1998, Bruce Schneier wrote:
  ”Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break. It's not even hard.”

- 1864, Charles Babbage wrote:
  "One of the most singular characteristics of the art of deciphering is the strong conviction possessed by every person, even moderately acquainted with it, that he is able to construct a cipher which nobody else can decipher.“

- Bruce Schneier, again:
  What is hard is creating an algorithm that no one else can break, even after years of analysis. And the only way to prove that is to subject the algorithm to years of analysis by the best cryptographers around.”

IEEE 802.11 Wireless LAN (WLAN)



The 802.11 standard

- 802.11 ready 1997, became ISO standard 1999
  - 2 Mbps
- 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
  - 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: 802.11a – Very old, was rare in Sweden [1999]
  - 54 Mbps (max, speed depends on signal quality), 5 GHz
- WI-FI 2: 802.11b – Very old [1999]
  - 11 Mbps, 2.4 GHz
- WI-FI 3: 802.11g – Old but still used [2003]
  - 54 Mbps, 2.4 GHz
- **WI-FI 4**: 802.11**n** – Most popular today [2009]
  - 2.4 and 5 GHz, Up to 600 Mbps (theoretical speed)
  - MIMO technique: multiple antennas for simultaneous data stream transmission
  - 4 streams allowed: 4 transmit and 4 receive antennas (4x4)
  - Most common: 2 streams → 270 Mbps (under perfect conditions)
- **WI-FI 5**: 802.11**ac** – Adopted by most new equipment [2014]
  - 867 Mbps (1x1) to 6.77 Gbps (8x8, rare)
- **WI-FI 6**: 802.11**ax** – Newest standard [2019]
  - Up to 10 Gbps
  - 2.4 and 5 GHz band used simultaneously – other frequencies possible (1-7 GHz)
  - Better modulation (1024 QAM) for 25% increased speed

What is security?

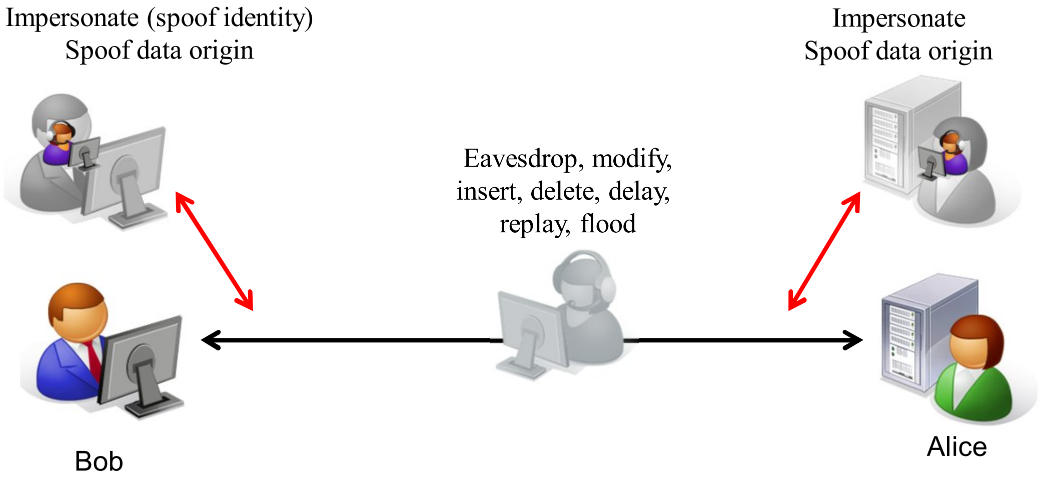
- **Confidentiality**
  - Protection against eavesdropping (ability to keep secrets)
- **Integrity**
  - Protection against unauthorized packet/data modification, removal, forgery, …
- **Availability**
  - System is able to serve its authorized users

CIA

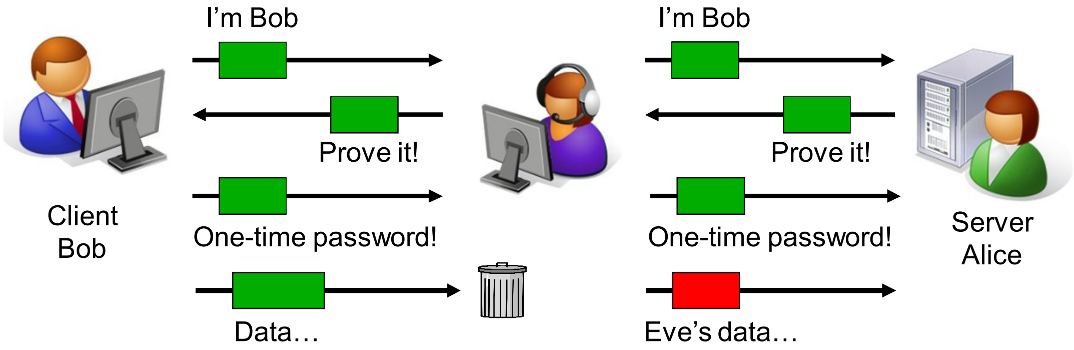
Some standards and publications add more attributes:

- Privacy
- ARM/RAM/RMA: Availability, Reliability, Maintainability
- Accountability and Traceability
  - Possibility to trace back actions to an entity – important after and incident
- Authenticity (or Non-repudiation)
  - Possibility to check if contents, sender or transmission is genuine

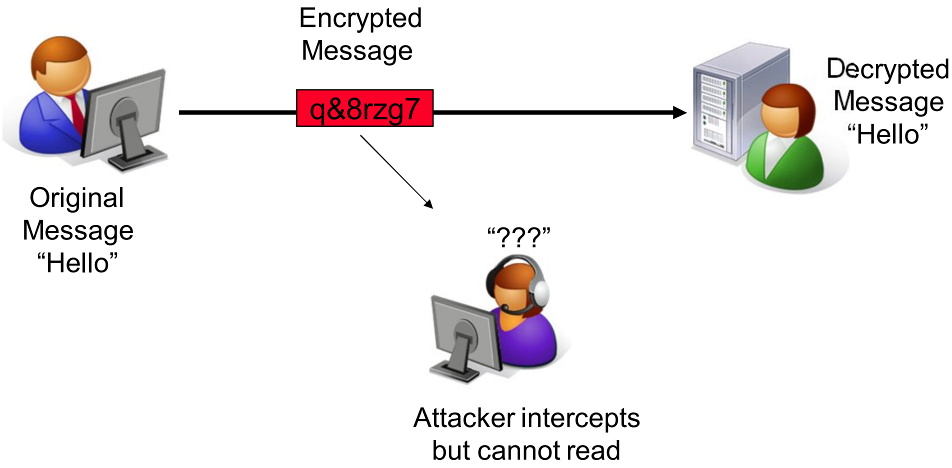
Communication threats



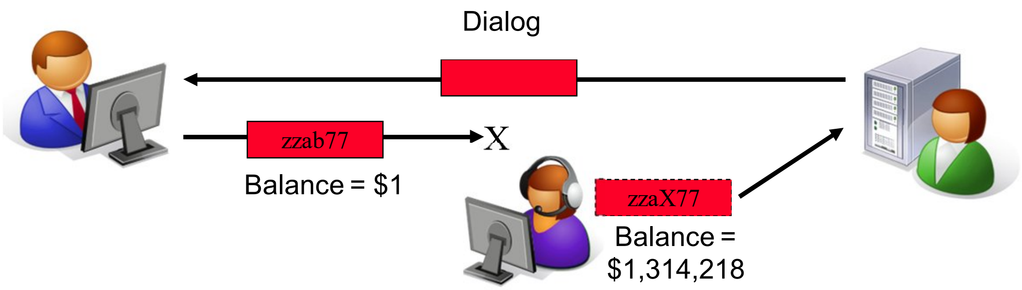
Man in-the-middle (MITM) attacks



Encryption for Confidentiality



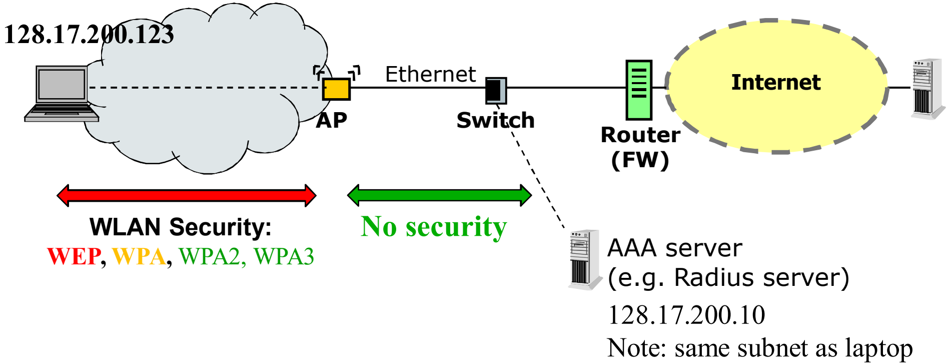
Encryption ≠ Integrity protection



Attacker intercepts and
alters encrypted messages

Eve may not understand the contents. But it has changed…

WLAN Security Scope

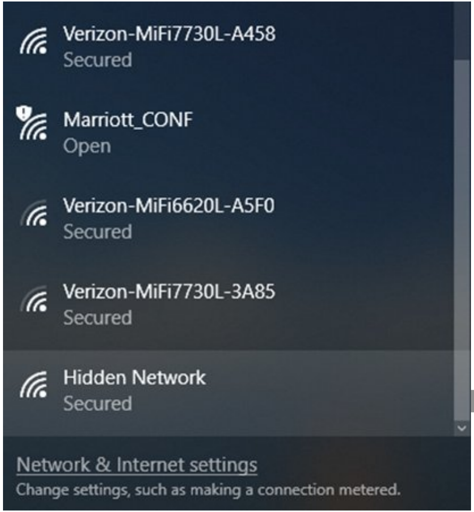


The AP works on link level. This means that ARP is used to find other hosts on the WLAN + LAN.

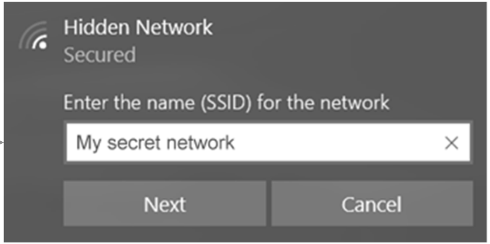
802.11 WLAN – Basic security

- Must know SSID to connect
  - Frequently broadcasted by the access point to ease discovery
  - SSID broadcasts can be disabled
    - But SSID is still sent in the clear 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

Connecting to a non-broadcasted network



No real security, "just" obfuscation



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
  - If encryption was expected by the client, the connection will fail
    - Static password
    - WPA2 Enterprise mode: rogue AP cannot talk to Radius server and get the key
- Protection can be made on higher level
  - Use SSH and TLS to encrypt traffic to home networks and own servers
- 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
  - Someone may fake a previously known AP and "offer" Internet access
- Some devices constantly send out network probes (e.g. smartphones)
  - Can be used to identify phones, e.g. by shops to discover returning customers

Auth. methods

```
C:>netsh wlan show drivers
    Driver                     : Intel Dual Band AC 7260
    …
    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
                               WPA2-Personal   CCMP
                               Open            Vendor defined
                               Vendor defined  Vendor defined
                      cipher supported in ad-hoc mode:
                               Open            None
                               Open            WEP-40bit
                               Open            WEP-104bit
                               Open            WEP
                               WPA2-Personal   CCMP
```

Networks

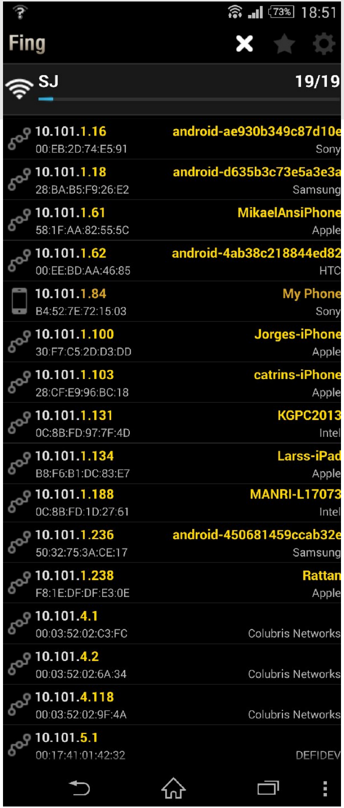
```
C:>netsh wlan show networks

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
```

FING

Example of an Android 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

- 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

The Final Nail in WEP's Coffin:
https://ieeexplore.ieee.org/document/1624028?arnumber=1624028

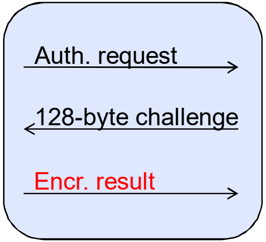
Very good paper explains many attacks, new and old in detail

A quick summary can be found at
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

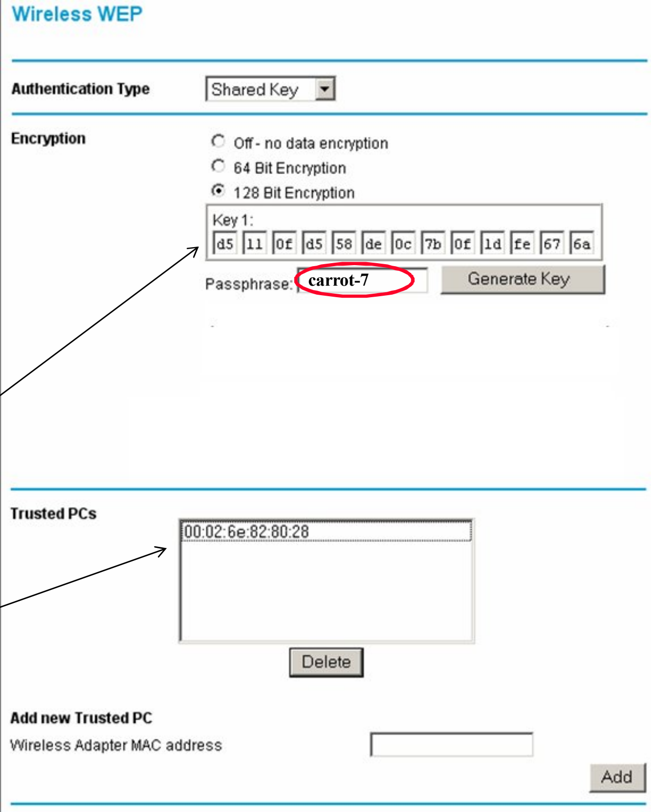
- Shared key Authentication (WEP)
  - Client sends Authentication Request to AP
  - AP sends frame with 128-byte challenge text to client
  - Challenge is encrypted with RC4 using a shared secret and a newly selected IV by the client
  - AP decrypts response and verifies it



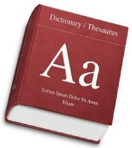
Configuring an AP for WEP Shared Key authentication

Wep keys
Generated from
MD5(passphrase)
or entered manually

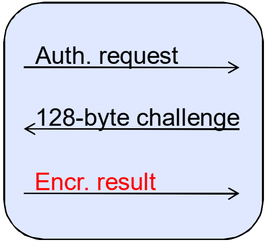
MAC addresses
filtering enabled



Dictionary attacks

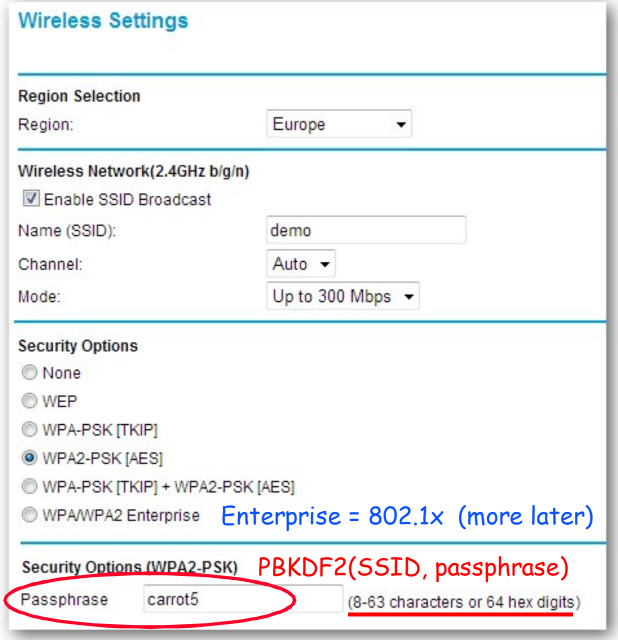


- WEP: APs use MD5 to generate a key from a user's password
- If clear text and cipher text known…
  - Easy to do dictionary based attacks
  - 100,000 (off-line) guesses per second with a normal CPU
    - If not random key, we get approx. 4-5 bits per character
    - 21 bit keys → 21 seconds to search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



- GPUs, can do this >1000 times faster (10 bits or 2-3 characters)
- Pre-generated dictionaries (rainbow tables) can be created
- WPA2 requires one table per SSID name
  - Also uses 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



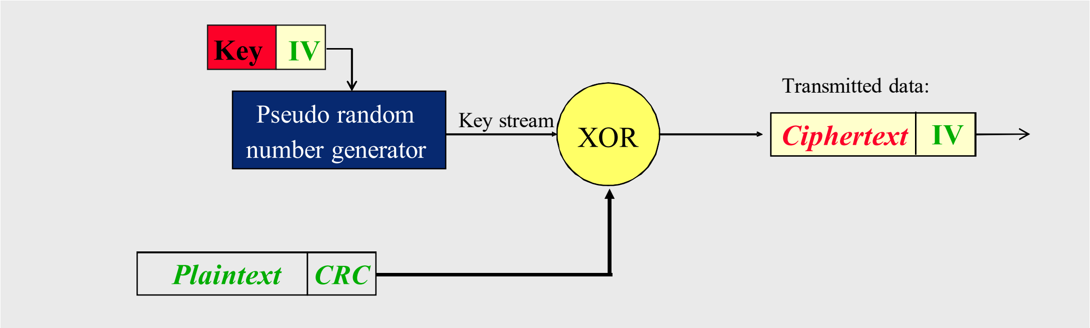
- PBKDF2 = Password-Based Key Derivation Function 2.0
- Described in PKCS#5 standard
- Uses 4,096 HMAC rounds
- This key is only used to generate session keys – each session will have a unique crypto key!

Rainbow tables – by SSID popularity

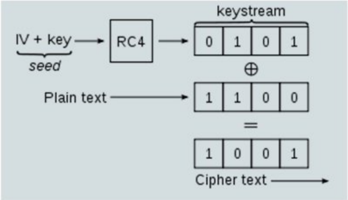
SSID	Total	Percent
linksys	2781573	2.949%
<no ssid>	2331805	2.472%
NETGEAR	1234930	1.309%
default	734576	0.779%
dlink	661229	0.701%
hpsetup	479933	0.508%
belkin54g	364819	0.386%
wireless	298279	0.316%
BTFON	278898	0.295%
FreeWifi	251685	0.266%
BTWIFI	248950	0.264%
BTOpenzone	241718	0.256%
no_ssid	224097	0.237%
BTWiFi-with-FON	222212	0.235%
Home	213190	0.226%
WLAN	181210	0.192%
SFR WiFi Public	172655	0.183%
BTOpenzone-H	156787	0.166%
" (Cloaked)	135631	0.143%
FRITZ!Box Fon WLAN 7170	130513	0.138%
FRITZ!Box Fon WLAN 7112	127927	0.135%
FreeWifi_secure	126825	0.134%
eduroam	125464	0.133%
Free Public WiFi	120558	0.127%
attwifi	104854	0.111%
ACTIONTEC	103128	0.109%
TELENETHOMESPOT	101670	0.107%
Guest	101436	0.107%
FRITZ!Box Fon WLAN 7270	99239	0.105%
(null)	97222	0.103%
ZyXEL	96867	0.102%
freephonie	93844	0.099%
SFR WiFi Mobile	88242	0.093%
SMC	82410	0.087%
setup	77760	0.082%
VOIP	76104	0.080%
asus	75686	0.080%
Tp-link	74045	0.078%
FRITZ!Box Fon WLAN 7113	73735	0.078%
internet	73457	0.077%
<hidden ssid>	71297	0.075%
Sitecom	70010	0.074%
FON_BELGACOM	68627	0.072%
Motorola	65736	0.069%
orange	61016	0.064%
hhonors	60470	0.064%
FON_ZON_FREE_INTERNET	59461	0.063%
FON_FREE_INTERNET	54674	0.057%
AndroidAP	52353	0.055%
BELTELECOM WIFI	52065	0.055%
0001softbank	51588	0.054%
MyPlace	51400	0.054%
airportthru	49373	0.052%
MSHOME	49099	0.052%
orange12	49062	0.052%
wlan-ap	48527	0.051%

http://www.wigle.net

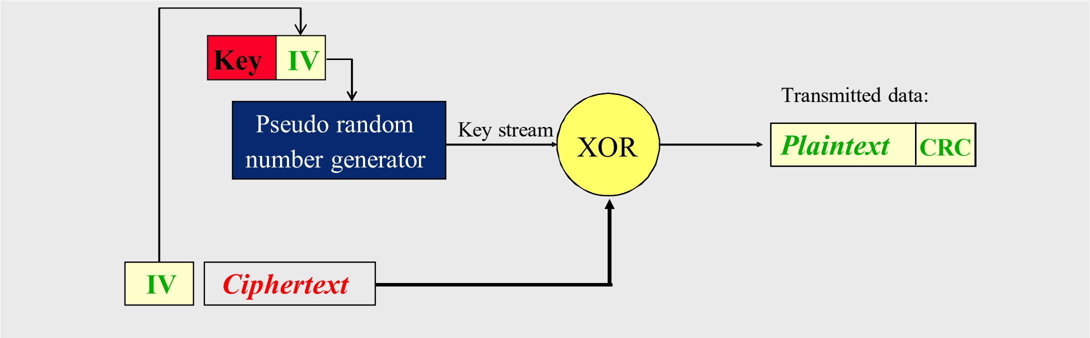
Encryption



- 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

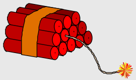


Decryption



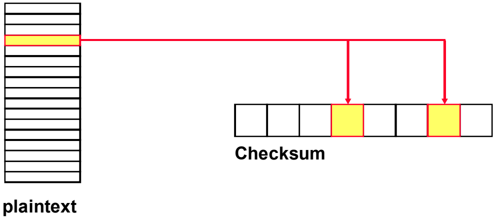
- Decryption: same procedure
  - Secret key is shared, IV is found in packet
  - The same key stream is generated by the random number generator
- CRC = Cyclic Redundancy Check = checksum to detect modifications, often used in hardware to detect transmission errors
- 104 bit keys should mean 2^{64} times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

Data encryption in WEP

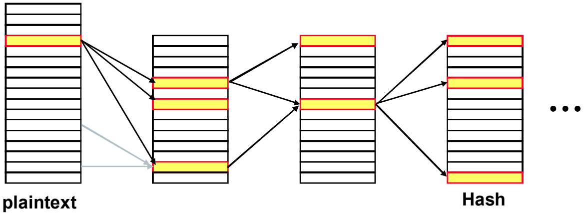


- Key and IV used to generate an infinite pseudo-random stream to be XORed with the plaintext
- What if two plaintexts are encrypted with same stream ***b*** are XOR:ed?
- Then the result is *plaintext1* $\oplus$ *plaintext2:*
  - $c1 \oplus c2 = (p1 \oplus b) \oplus (p2 \oplus b) = p1 \oplus p2 \oplus b \oplus b = p1 \oplus p2$
  - 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
- Many (older) devices started sessions with IV=0, 1, 2, 3, … to guarantee they were unique
  - Problem: With 2 or more devices connected, all 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 packets) in less than 1 hour
  - 50% chance of IV collision after only 4,823 packets (<1 second)
  - 99% collision after 12,430 packets (2 seconds)

CRC versus Hash functions

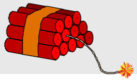


CRC: When one bit in plaintext is modified, we know exactly what bits to change in the checksum.



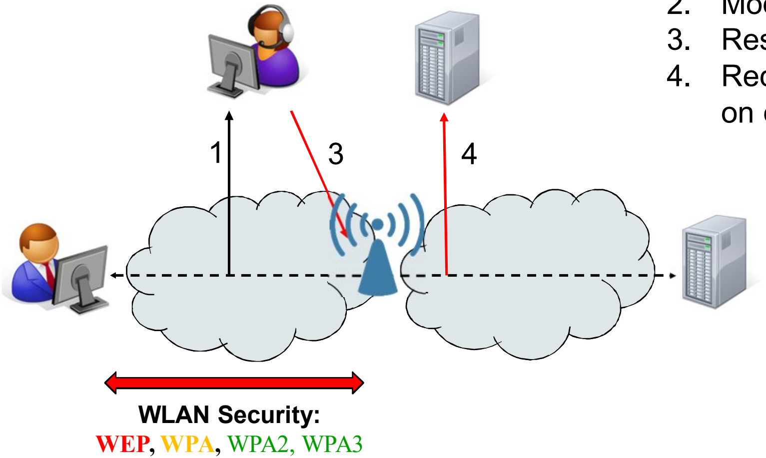
Hash: One modified bit affects more bits in the next step – chaos/avalanche effect. Impossible to predict change without redoing calculation from clear text.

Integrity check in WEP



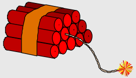
- Observation: Flipping one bit in the Ciphertext, flips the same bit in the plaintext
- WEP uses a linear CRC (a checksum) and a stream cipher
  - Changing a bit in the input results in a predictable change of the CRC
  - So we can change the checksum to match even if it is encrypted!
- The IP address is normally known or can be guessed
  - Opens up for address modifications (we know where it is located in a datagram)
  - Attacker may be able to redirect packets to another computer
- Modified packets will be sent in clear to a remote destination [next page]
  - Encryption ends in AP
  - Method:
    - Capture one datagram (encrypted)
    - Modify address – we may have to try a while, but addresses are not random
    - When address is correct, we will receive the datagram in cleartext
- WEP should have used a non-linear checksum, a hash (SHA-256, …)

Capturing and decrypting traffic

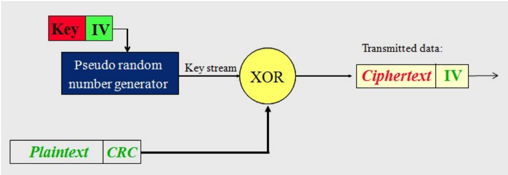


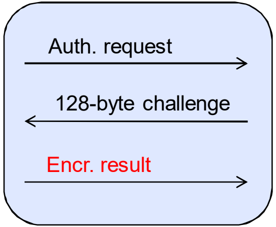
1. Capture encrypted packet
2. Modify IP address field
3. Resend it to AP
4. Receive unencrypted packet on own system

Sending data without the key



- Observation: 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 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, this IV can be reused forever



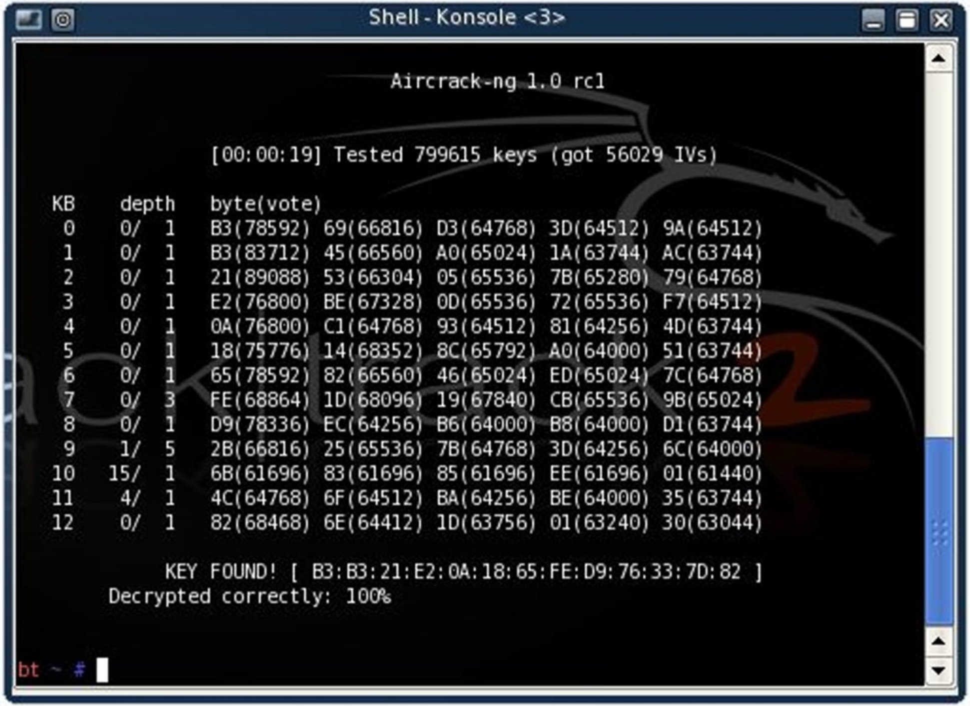


Injecting traffic with WEPWedgie

```
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!


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 ~ #

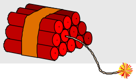
Dictionary attacks always possible

Homework

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

Watch 6:45 – 14:15

The story continues…



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
  - 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

Summary of WEP insecurity

- Major weaknesses – lacks most of the features we saw in TLS:
  - No negotiation of capabilities
  - Same key used for both 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

802.11i Framework (WPA, WPA2, WPA3)

Chapter 18.4

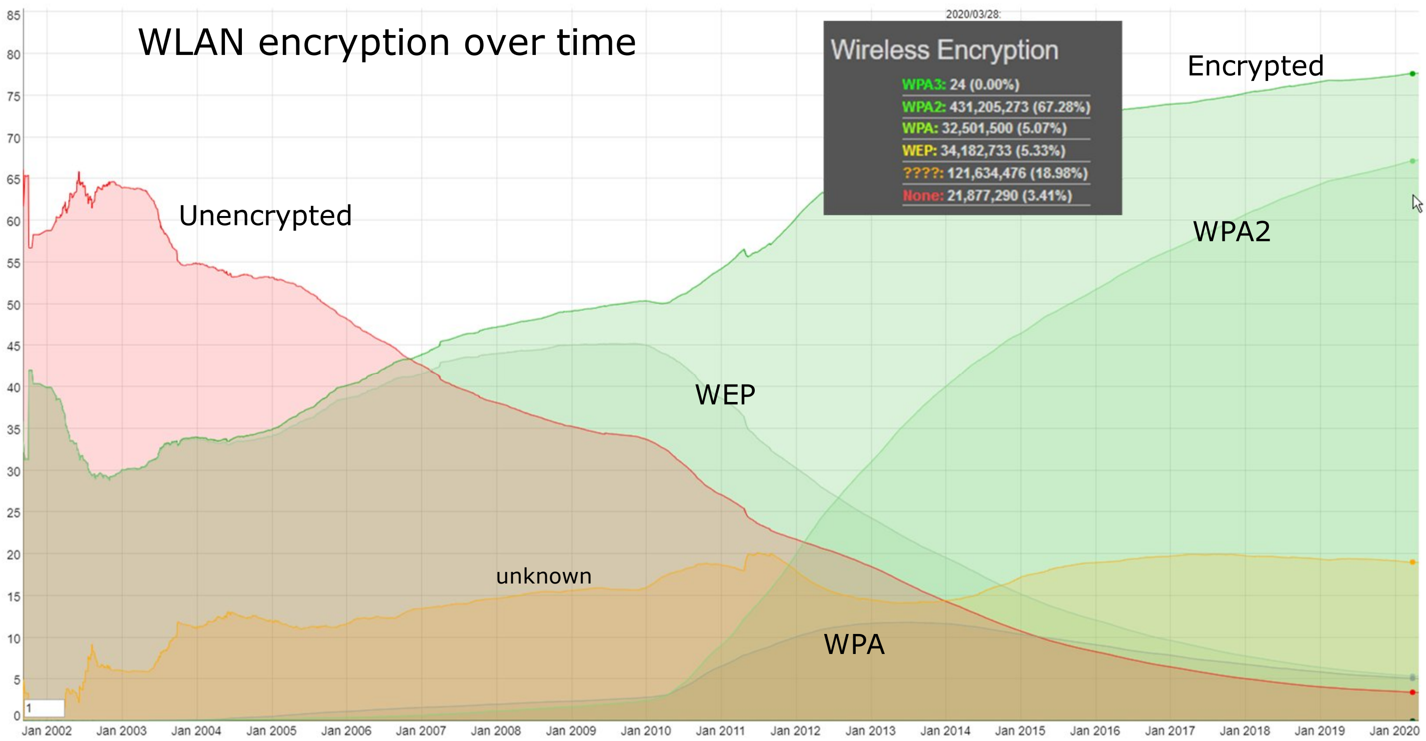
802.11i

- 802.11i the standard to be used for WLAN security (**2004**)
  - Framework for security, specifies WPA and WPA2
- **WPA**, Wi-Fi Protected Access – temporary solution!
  - First step towards 802.11i – better than WEP
  - Uses RC4 to allow old hardware to be upgraded to WPA
  - Basic technology in WPA: 802.1x, TKIP, MIC (message integrity check)
  - Now insecure due to RC4 – **don't use!**
- **WPA2** implements 802.11i
  - Uses 802.1x and CCMP (AES counter mode with CBC MAC protocol)
  - All certified devices manufactured after **2006** support WPA2
  - Personal mode with Pre-shared keys (PSK)
  - Enterprise mode with Radius for authentication
  - Session keys negotiated – stations cannot read each others traffic

802.11i

- Each packet has a unique sequence number
  - IV+EIV incremented for each transmitted package
  - Packets must be received in order (no replays)
- 256-bit Pre-shared keys are used in home environments (personal mode)
  - WPA: Hash (SSID, password) unique per station name
  - WPA2: hash is 4,096 iterations of HMAC-SHA-1 (RFC 2898)
  - Pre-generated rainbow tables exist
  - Don’t use the most popular SSID names (top 1,000)
  - Routers start to use more random SSID default names: e.g. “linksys_24a8f9”
- WPA uses 802.1x, TKIP, MIC (message integrity check)
  - Better than WEP, not as good as WPA2
  - WPA only intended for older devices not capable of WPA2
- TKIP: the temporal key is changed every 10,000 packets and normally also every hour
- TKIP uses a cryptographic message integrity check (MIC)
  - Not linear CRC as in WEP
  - Uses RC4-based one-way function and encryption algorithm called Michael
  - In 2004, an inverse function to MIC was found → key can be calculated if the same key is used twice...

WLAN encryption over time



WIGLE.NET

https://www.wigle.net

WPA3

- WEP 1997, WPA 2003, WPA2 2004, WPA3 2018
  - Software update WPA2 → WPA3 possible (but likely?)
- Easier to connect smaller IoT devices
- Addresses some problems in WPA2
  - KRACK – key reinstallation attack biggest problem (although patches exist)
  - Brute force password guessing
- DiffieHellman will be used for each station
  - Means that all session crypto-keys will be unique and never reused!
  - Possible also between two devices in the network!

WPA3 at a glance

WPA3-Personal

- **More robust password-based authentication**, even when users choose weak passwords.
  - Simultaneous Authentication of Equals (SAE) replaces Pre-shared Key (PSK) in WPA2-Personal - resistant to offline dictionary attacks
  - Based on IETF Dragonfly key exchange: Both sides know that the other knows the password ("proof of knowledge")
- **Enhanced open**: Encryption also in open networks lacking authentication ("Opportunistic Wireless Encryption")
- **Forward secrecy**: Protects data traffic even if a password is compromised (D-H)
- Wi-Fi Easy connect: Support for IoT devices without user interface: QR code or printed number
  - Uses "Device Provisioning Protocol (DPP)" – mobile phones can be used to connect other devices (configurator for enrollees).

WPA3-Enterprise

- Offers an optional 192-bit minimum-strength keys to better protect sensitive data
- **Authenticated encryption**: 256-bit Galois/Counter Mode Protocol (GCMP-256)
- **Key establishment and authentication**: Elliptic Curve Diffie-Hellman (ECDH) key exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)
- **Key derivation and confirmation**: HMAC-SHA384

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