



Welcome to

6. Wifi Security

Communication and Network Security 2024

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Codeberg
6-Wifi-Security.tex in the repo [security-courses](#)

Goals for today



It is not clear that the link layer is the right one for security. In a coffeeshop, the security association is terminated by the store: is there any reason you should trust the shopkeeper? Perhaps link-layer security makes some sense in a home, where you control both the access point and the wireless machines. However, we prefer end-to-end security at the network layer or in the applications.

Source: Cheswick-chap2.pdf Firewalls and Internet Security: Repelling the Wily Hacker , Second Edition, William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin

Today's goals:

- Introduce wireless networks and **security in them**
- Present the common security standards, and some tools used
- Discuss how to secure wireless best, infrastructure and/or encryption
- Wi-Fi security is more than just encryption

Plan for today



Subjects

- Wifi standarder IEEE 802.11
- Authentication Protocols RADIUS, PAP, CHAP, EAP
- Port Based Network Access Control IEEE 802.1x
- Security problems in wireless protocols
- Security problems in wireless encryption
- Hacking wireless networks

Exercises

- Wifi scanning, aka wardriving
- WPA hacking with a short password

Time schedule



- 17:00 - 18:15
Introduction and basics
- 30min break
- 18:45 - 19:30
- 15min break
- 19:45 -20:30 45min

Reading Summary



PPA chapter 12, 13 - 60 pages

Skim:

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

Reading Summary, continued



PPA chapter 12: Packet Analysis for Security

- Reconnaissance An attacker's first step
- SYN Scan and fingerprinting
- Traffic Manipulation ARP Cache Poisoning / spoofing
- Analyzing traffic from malware, exploit kits and ransomware

Reading Summary, continued



PPA chapter 13: Wireless Packet Analysis

- Sniffing channels
- Wireless card modes, Managed, Ad-hoc and Monitor mode
- 802.11 packet structure
- Wireless security

Wifi standarder IEEE 802.11



802.11 er arbejdsgruppen under IEEE

De mest kendte standarder idag indenfor trådløse teknologier:

- 802.11b 11Mbps versionen
- 802.11g 54Mbps versionen
- 802.11n endnu hurtigere
- 802.11i Security enhancements Robust Security Network RSN

New names soon:

Wi-Fi 6 to identify devices that support 802.11ax technology

Wi-Fi 5 to identify devices that support 802.11ac technology

Wi-Fi 4 to identify devices that support 802.11n technology

Kilde: <http://grouper.ieee.org/groups/802/11/index.html>

802.11 modes og frekvenser



Access point kører typisk i *access point mode* også kaldet infrastructure mode

- al trafik går via AP, mest typiske

Alternativt kan wireless kort oprette ad-hoc netværk

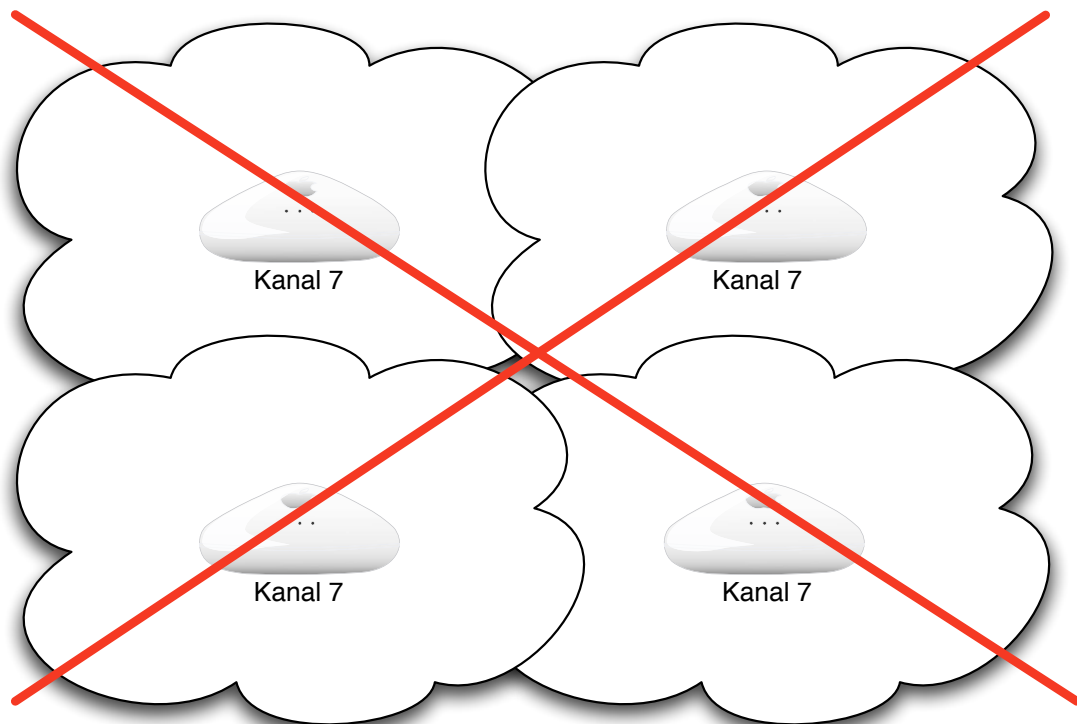
- hvor trafikken går direkte mellem netkort

Frekvenser op til kanal 11 og 12+13 i DK/EU

Helst 2 kanaler spring for 802.11b AP der placeres indenfor rækkevidde

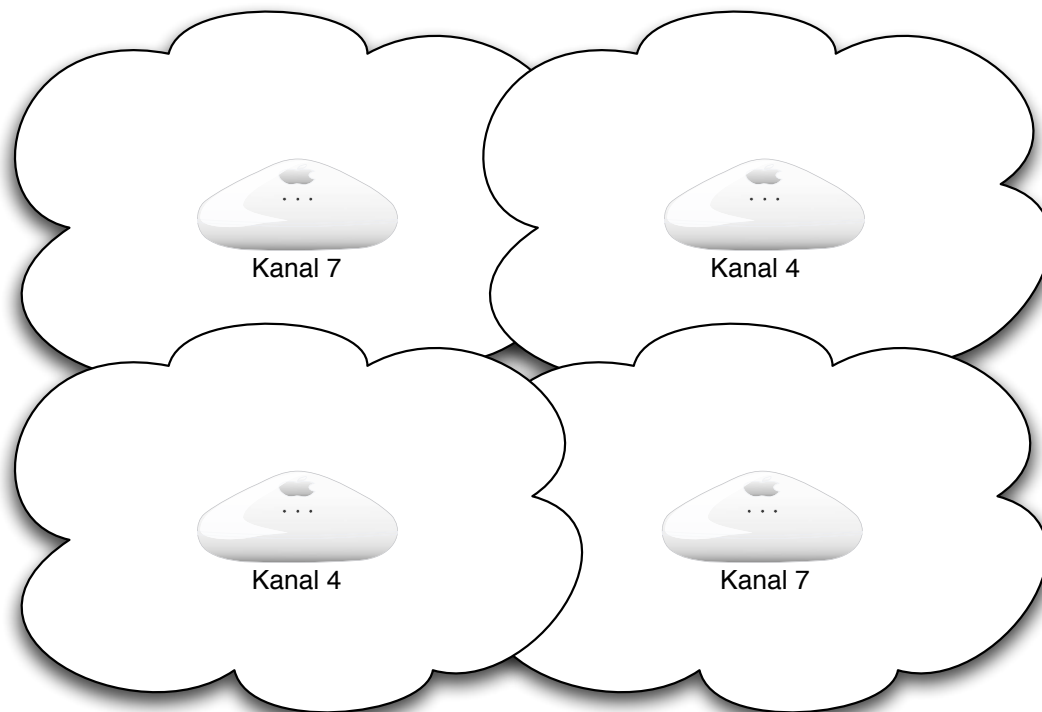
Helst 4 kanaler spring for 802.11g AP der placeres indenfor rækkevidde

Eksempel på netværk med flere AP'er



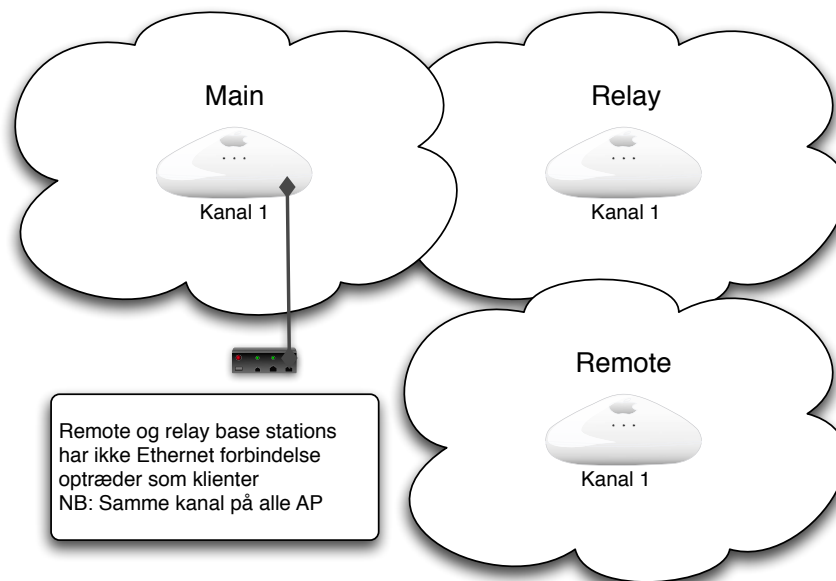
(802.11 uden WDS)

Eksempel på netværk med flere AP'er



(802.11 uden WDS)

Wireless Distribution System WDS



(802.11 med WDS)

Se også: http://en.wikipedia.org/wiki/Wireless_Distribution_System

Jeg bryder mig ikke om Wi-Fi extenders generelt og systemer som WDS

Er trådløse netværk interessante?



wireless 802.11

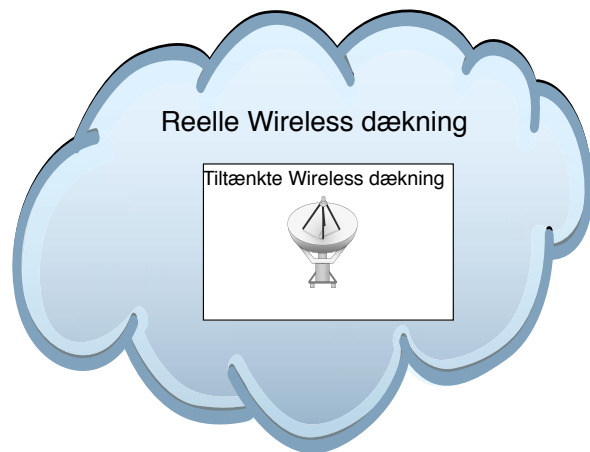


Sikkerhedsproblemer i de trådløse netværk er mange

- Fra lavt niveau - eksempelvis ARP, 802.11
- dårlige sikringsmekanismer - WEP
- dårligt udstyr - mange fejl
- usikkerhed om implementering og overvågning

Trådløst udstyr er blevet meget billigt!

Det er et krav fra brugerne - trådløst er lækkert



- Værre end Internetangreb - anonymt
- Kræver ikke fysisk adgang til lokationer
- Konsekvenserne ved sikkerhedsbrud er generelt større
- Typisk får man direkte LAN eller Internet adgang!



The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - [What's new ?](#)

KALI LINUX
"the quieter you become, the more you are able to hear"

**PENETRATION TESTING,
REDEFINED.**

A Project By Offensive Security

- Wirelessscanner - Kali og Airodump
- Wireless Injection - aireplay-ng
- Aircrack-ng pakken generelt
- Kali <http://www.kali.org/>

Konsulentens udstyr wireless, eksempel kort



Varenummer: 2225730

TP-Link TL-WN722N

Hi-Speed USB - 802.11b, 802.11g, 802.11n

På lager, 1-2 dages levering
(Billigste fragt: 0 kr.)
Ret land

4 stk på lager i Århus
0 stk på lager i Viborg
0 stk på lager i København

Køb

120,00 kr.
(96,00 kr.)

Laptop or Netbook, I typically use USB wireless cards

NB: de indbyggede er ofte ringe til wifi pentest - så check før køb ;-)

Access Points - get a small selection for testing

Books:

- Kali Linux Wireless Penetration Testing: Beginner's Guide Beginner's Guide, Vivek Ramachandran, Cameron Buchanan, March 2015

Also checkout his home page <http://www.vivekramachandran.com/>

Kali Nethunter



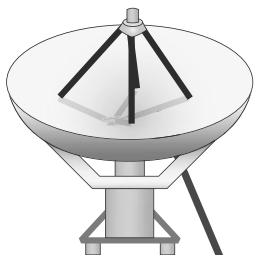
- **802.11 Wireless Injection** and **AP mode** support with multiple supported USB wifi cards.
- Capable of running **USB HID Keyboard attacks**, much like the **Teensy** device is able to do.
- **Supports BadUSB MITM attacks**. Plug in your Nethunter to a victim PC, and have your traffic relayed through it.
- Contains a **full Kali Linux toolset**, with many tools available via a simple menu system.
- **USB Y-cable support** in the Nethunter kernel – use your OTG cable while still charging your Nexus device!
- **Software Defined Radio support**. Use **Kali Nethunter** with your HackRF to explore the wireless radio space.

Source: <https://www.kali.org/kali-linux-nethunter/>



Der benyttes en del værktøjer:

- Nmap, Nping - tester porte, godt til firewall admins <http://nmap.org>
- Metasploit Framework gratis på <http://www.metasploit.com/>
- Wireshark avanceret netværkssniffer - <http://http://www.wireshark.org/>
- Kismet <http://www.kismetwireless.net/>
- Aircrack-ng set of tools <http://www.aircrack-ng.org/>
- Pyrit GPU cracker <http://code.google.com/p/pyrit/>
- Reaver brute force WPS <https://code.google.com/p/reaver-wps/>



Wireless Access Point



netværket - typisk Ethernet

et access point - forbindes til netværket

Basal konfiguration



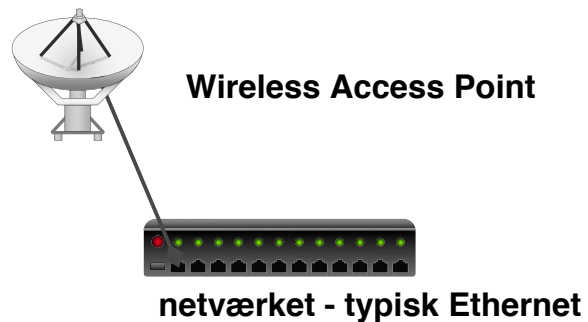
Når man tager fat på udstyr til trådløse netværk opdager man:

SSID - nettet skal have et navn

frekvens / kanal - man skal vælge en kanal, eller udstyret vælger en automatisk

der er nogle forskellige metoder til sikkerhed

Wireless networking sikkerhed i 802.11



Sikkerheden er baseret på nogle få forudsætninger

- SSID - netnavnet
- WEP *kryptering* - Wired Equivalent Privacy
- WPA kryptering - Wi-Fi Protected Access, SSID indgår i denne!
- måske MAC flitrering, kun bestemte kort må tilgå accesspoint

Forudsætninger



Til gengæld er disse forudsætninger ofte ikke tilstrækkelige ...

- WEP er nem at knække, lad helt være med at bruge WEP
- WPA PSK er baseret på en DELT hemmelighed som alle stationer kender
- nøglen ændres sjældent, og det er svært at distribuere en ny

SSID - netnavnet



Service Set Identifier (SSID) - netnavnet

32 ASCII tegn eller 64 hexadecimale cifre

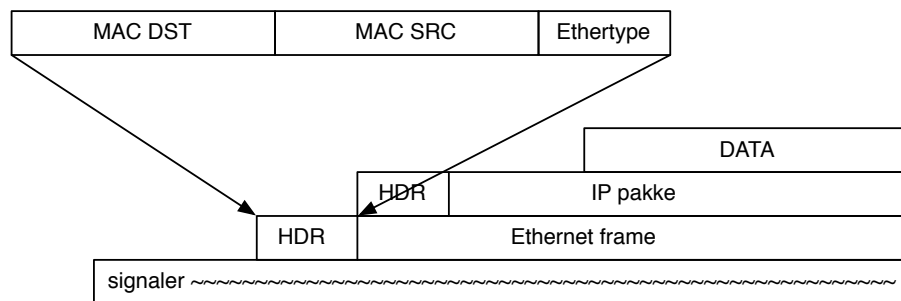
Udstyr leveres typisk med et standard netnavn

- Cisco - tsunami
- Linksys udstyr - linksys
- Apple Airport, 3Com m.fl. - det er nemt at genkende dem

SSID kaldes også for network id NWID

SSID broadcast - udstyr leveres oftest med broadcast af SSID

Hacking eksempel - det er ikke magi



MAC filtrering på trådløse netværk - Alle netkort har en MAC fra fabrikken

Kun godkendte kort tillades adgang til netværket

Netkort tillader at man overskriver denne adresse midlertidigt

MAC adressen på kortene er med i alle pakker der sendes

MAC adressen er aldrig krypteret, for hvordan skulle pakken så nå frem?

Myten om MAC filtrering



Eksemplet med MAC filtrering er en af de mange myter

Hvorfor sker det?

- Marketing - producenterne sætter store mærkater på æskerne
- Manglende indsigt - forbrugerne kender reelt ikke koncepterne
- Hvad er en MAC adresse egentlig
- Relativt få har forudsætningerne for at gennemskue dårlig sikkerhed

Løsninger?

- Udbrede viden om usikre metoder til at sikre data og computere
- Udbrede viden om sikre metoder til at sikre data og computere

MAC filtrering



Demo: wardriving med airodump-ng



MacStumbler 0.5b							
SSID	MAC	Channel	Signal	Noise	Network type	Vendor	WEP
tech	00:40:96:54:43:9F	6	25	4	Managed	Cisco-Aironet	No
trainingroom	00:40:96:57:53:53	6	21	4	Managed	Cisco-Aironet	No
svcc	00:40:96:57:FE:39	6	12	4	Managed	Cisco-Aironet	No

Log:						
SSID	MAC	Channel	Network type	Vendor	WEP	Last Seen
trainingroom	00:40:96:57:53:53	6	Managed	Cisco-Aironet	No	Tuesday, May 07, 2002 14:54:07 US/Pacific
svcc	00:40:96:57:FE:39	6	Managed	Cisco-Aironet	No	Tuesday, May 07, 2002 14:54:07 US/Pacific
linksys	00:04:5A:0E:1D:79	10	Managed	Linksys	No	Tuesday, May 07, 2002 14:53:58 US/Pacific
tech	00:40:96:54:43:9F	6	Managed	Cisco-Aironet	No	Tuesday, May 07, 2002 14:54:07 US/Pacific
svcc	00:40:96:57:74:27	6	Managed	Cisco-Aironet	No	Tuesday, May 07, 2002 14:54:02 US/Pacific
svcc	00:40:96:55:25:34	6	Managed	Cisco-Aironet	No	Tuesday, May 07, 2002 14:54:01 US/Pacific
linksys	00:06:25:51:6F:96	6	Managed	unknown	No	Tuesday, May 07, 2002 14:49:33 US/Pacific

Save... Status: Scanning...

man tager et trådløst netkort og en bærbar computer og noget software:

- Tidligere brugte man diverse "stumbler", som MacStumbler eller Kismet
- Idag bruger vi Airodump-ng fra Aircrack-ng.org/Kali

Øvelse: airodump-ng



Vi afprøver nu airodump-ng

Lån eller køb et netkort, hvis jeg har flere

Brug dele af guiden

http://www.aircrack-ng.org/doku.php?id=simple_wep_crack

Exercise



Now lets do the exercise

i Wardriving Up to 60min

which is number **47** in the exercise PDF.

Resultater af wardriving

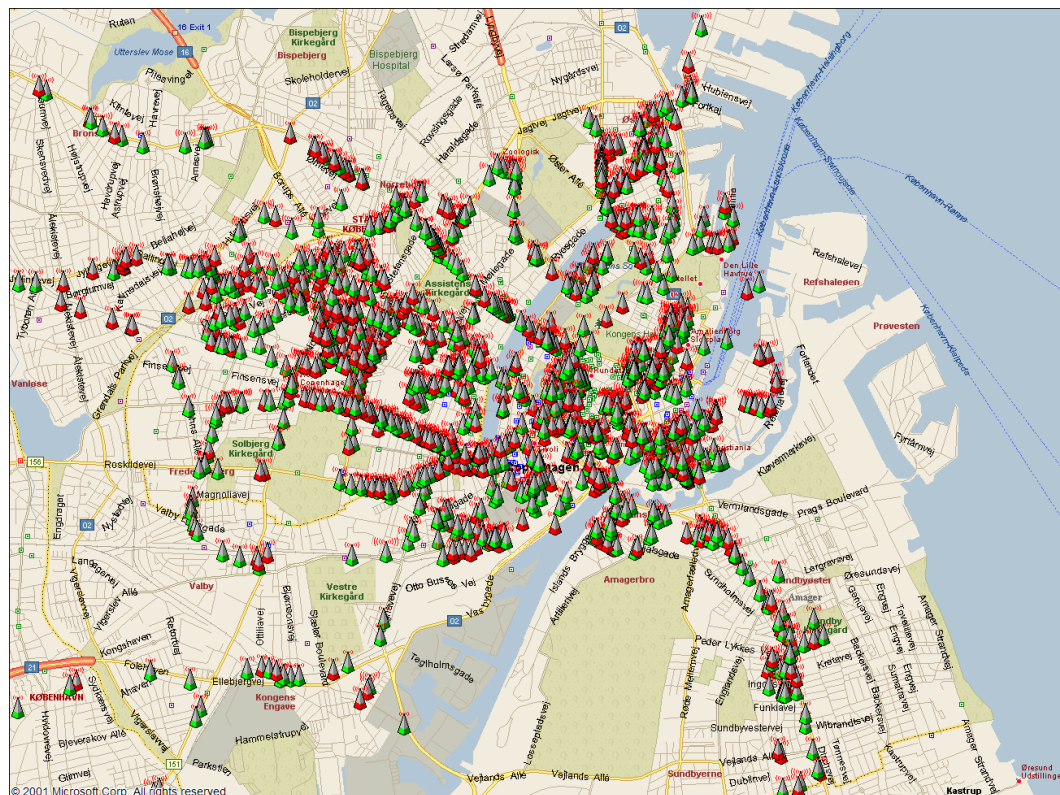


Hvad opdager man ved wardriving?

- at WEP/WPA IKKE krypterer hele pakken
- at alle pakker indeholder MAC adressen
- WPA/WEP nøglen skifter sjældent
- Mange wireless er fejlkonfigureret på forskellig vis

Man kan altså lytte med på et netværk med WEP/WPA,
genbruge en anden maskines MAC adresse
- og måske endda bryde krypteringen.

Storkøbenhavn





Det vi har udført er informationsindsamling

Indsamlingen kan være aktiv eller passiv indsamling i forhold til målet for angrebet

passiv kunne være at lytte med på trafik eller søge i databaser på Internet

aktiv indsamling er eksempelvis at sende ICMP pakker og registrere hvad man får af svar



Cryptography or cryptology is the practice and study of techniques for secure communication. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key, to ensure confidentiality, example algorithm AES.

Public-key cryptography (like RSA) uses two related keys, a key pair of a public key and a private key. This allows for easier key exchanges, and can provide confidentiality, and methods for signatures and other services.

Source: <https://en.wikipedia.org/wiki/Cryptography>



Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

Et succesfuldt angreb på en krypto-algoritme er enhver genvej som kræver mindre arbejde end en gennemgang af alle nøglerne

Nye algoritmer, programmer, protokoller m.v. skal gennemgås nøje!

Se evt. Snake Oil Warning Signs: Encryption Software to Avoid

<http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>

IEEE 802.11 Security fast forward



In 2001, a group from the University of California, Berkeley presented a paper describing weaknesses in the 802.11 Wired Equivalent Privacy (WEP) security mechanism defined in the original standard; they were followed by **Fluhrer, Mantin, and Shamir's** paper titled "Weaknesses in the Key Scheduling Algorithm of RC4". Not long after, Adam Stubblefield and AT&T publicly announced the first **verification of the attack**. In the attack, they were able to intercept transmissions and gain unauthorized access to wireless networks.

Source: http://en.wikipedia.org/wiki/IEEE_802.11

IEEE 802.11 Security fast forward



The IEEE set up a dedicated task group to create a replacement security solution, **802.11i** (previously this work was handled as part of a broader 802.11e effort to enhance the MAC layer). The Wi-Fi Alliance announced an **interim specification called Wi-Fi Protected Access (WPA)** based on a subset of the then current IEEE 802.11i draft. These started to appear in products in **mid-2003**. **IEEE 802.11i (also known as WPA2)** itself was ratified in **June 2004**, and uses government strength encryption in the **Advanced Encryption Standard AES**, instead of RC4, which was used in WEP. The modern recommended encryption for the home/consumer space is **WPA2 (AES Pre-Shared Key)** and for the Enterprise space is **WPA2 along with a RADIUS authentication server** (or another type of authentication server) and a strong authentication method such as EAP-TLS.

Source: http://en.wikipedia.org/wiki/IEEE_802.11

IEEE 802.11 Security fast forward



In January 2005, the IEEE set up yet another task group "w" to protect management and broadcast frames, which previously were sent unsecured. Its standard was published in 2009.[24]

In **December 2011**, a security flaw was revealed that affects wireless routers with the **optional Wi-Fi Protected Setup (WPS)** feature. While WPS is not a part of 802.11, **the flaw allows a remote attacker to recover the WPS PIN and, with it, the router's 802.11i password in a few hours.**

WPS WTF?! - det er som om folk bevidst saboterer wireless sikkerhed!

Source: http://en.wikipedia.org/wiki/IEEE_802.11



WEP *kryptering* - med nøgler der specificeres som tekst eller hexadecimale cifre
typisk 40-bit, svarende til 5 ASCII tegn eller 10 hexadecimale cifre eller 104-bit 13 ASCII tegn eller 26 hexadecimale cifre

WEP er baseret på RC4 algoritmen der er en *stream cipher* lavet af Ron Rivest for RSA Data Security

De første fejl ved WEP



Oprindeligt en dårlig implementation i mange Access Points

Fejl i krypteringen - rettet i nyere firmware

WEP er baseret på en DELT hemmelighed som alle stationer kender

Nøglen ændres sjældent, og det er svært at distribuere en ny



WEP bør ikke bruges overhovedet mere

WEP er for simpel til et større netværk - eksempelvis 20 brugere

Firmaer bør efter min mening bruge andre sikkerhedsforanstaltninger

Hvordan udelukker man en bestemt bruger?



AirSnort Homepage



AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. <https://github.com/kramse/conference-open-8021x> 802.11b, using the Wired Equivalent Protocol (WEP), is crippled with numerous security flaws. Most damning of these is the weakness described in "Weaknesses in the Key Scheduling Algorithm of RC4 "by Scott Fluhrer, Itsik Mantin and Adi Shamir. Adam Stubblefield was the first to implement this attack, but he has not made his software public. AirSnort, along with WEPCrack, which was released about the same time as AirSnort, are the first publicly available implementations of this attack. <http://airsnort.shmoo.com/>

major cryptographic errors



weak keying - 24 bit er allerede kendt - $128\text{-bit} = 104\text{ bit}$ i praksis

small IV - med kun 24 bit vil hver IV blive genbrugt oftere

CRC-32 som integritetscheck er ikke *stærkt* nok kryptografisk set

Authentication gives pad - giver fuld adgang - hvis der bare opdages *encryption pad* for en bestemt IV. Denne IV kan så bruges til al fremtidig kommunikation

Konklusion: Kryptografi er svært

WEP cracking - airodump og aircrack



airodump - opsamling af krypterede pakker

aircrack - statistisk analyse og forsøg på at finde WEP nøglen

Med disse værktøjer er det muligt at knække *128-bit nøgler*!

Blandt andet fordi det reelt er 104-bit nøgler 😊

tommelfingerregel - der skal opsamles mange pakker ca. 100.000 er godt

Links:

<http://www.cr0.net:8040/code/network/aircrack/> aircrack

<http://www.securityfocus.com/infocus/1814> WEP: Dead Again

airodump opsamling



BSSID	CH	MB	ENC	PWR	Packets	LAN IP / # IVs	ESSID
00:03:93:ED:DD:8D	6	11		209	801963	540180	wanlan

Når airodump kører opsamles pakkerne

Lås airodump fast til een kanal, -c eller --channel

Startes med airmon og kan skrive til capture filer:

```
airmon-ng start wlan0
```

```
airodump-ng --channel 6 --write testfil wlan0mon
```

aircrack - WEP cracker



```
$ aircrack -n 128 -f 2 aftendump-128.cap
aircrack 2.1
* Got 540196! unique IVs | fudge factor = 2
* Elapsed time [00:00:22] | tried 12 keys at 32 k/m
KB    depth  votes
0     0/ 1    CE( 45) A1( 20) 7E( 15) 98( 15) 72( 12) 82( 12)
1     0/ 2    62( 43) 1D( 24) 29( 15) 67( 13) 94( 13) F7( 13)
2     0/ 1    B6( 499) E7( 18) 8F( 15) 14( 13) 1D( 12) E5( 10)
3     0/ 1    4E( 157) EE( 40) 29( 39) 15( 30) 7D( 28) 61( 20)
4     0/ 1    93( 136) B1( 28) 0C( 15) 28( 15) 76( 15) D6( 15)
5     0/ 2    E1( 75) CC( 45) 39( 31) 3B( 30) 4F( 16) 49( 13)
6     0/ 2    3B( 65) 51( 42) 2D( 24) 14( 21) 5E( 15) FC( 15)
7     0/ 2    6A( 144) 0C( 96) CF( 34) 14( 33) 16( 33) 18( 27)
8     0/ 1    3A( 152) 73( 41) 97( 35) 57( 28) 5A( 27) 9D( 27)
9     0/ 1    F1( 93) 2D( 45) 51( 29) 57( 27) 59( 27) 16( 26)
10    2/ 3    5B( 40) 53( 30) 59( 24) 2D( 15) 67( 15) 71( 12)
11    0/ 2    F5( 53) C6( 51) F0( 21) FB( 21) 17( 15) 77( 15)
12    0/ 2    E6( 88) F7( 81) D3( 36) E2( 32) E1( 29) D8( 27)
KEY FOUND! [ CE62B64E93E13B6A3AF15BF5E6 ]
```

Hvor lang tid tager det?



Opsamling a data - ca. en halv time på 802.11b ved optimale forhold

Tiden for kørsel af aircrack fra auditor CD på en Dell CPi 366MHz Pentium II laptop:

```
$ time aircrack -n 128 -f 2 aftendump-128.cap
...
real    5m44.180s    user    0m5.902s      sys    1m42.745s
```

Tiden for kørsel af aircrack på en VIA CL-10000 1GHz CPU med almindelig disk OpenBSD:

```
25.12s real    0.63s user    2.14s system
For 10 år siden :-P
```

Erstatning for WEP- WPA



Det anbefales at bruge:

Kendte VPN teknologier eller WPA

baseret på troværdige algoritmer

implementeret i professionelt udstyr

fra troværdige leverandører

udstyr der vedligeholdes og opdateres

Man kan måske endda bruge de eksisterende løsninger - fra hjemmepc adgang, mobil adgang m.v.

Erstatninger for WEP



Der findes idag andre metoder til sikring af trådløse netværk

802.1x Port Based Network Access Control

WPA - Wi-Fi Protected Access)

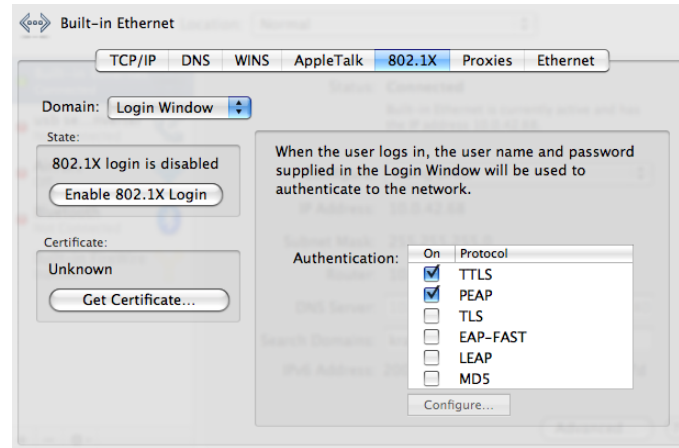
WPA = 802.1X + EAP + TKIP + MIC

nu WPA2

WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance.

Kilde: http://www.wifialliance.org/OpenSection/protected_access.asp

IEEE 802.1x Port Based Network Access Control



- Nogle switche tillader at man benytter 802.1x
- Denne protokol sikrer at man valideres før der gives adgang til porten
- Når systemet skal have adgang til porten afleveres brugernavn og kodeord/certifikat
- Denne protokol indgår også i WPA Enterprise

802.1x og andre teknologier



802.1x i forhold til MAC filtrering giver væsentlige fordele

MAC filtrering kan spoofes, hvor 802.1x kræver det rigtige kodeord

Typisk benyttes RADIUS og 802.1x integrerer således mod både LDAP og Active Directory

WPA eller WPA2?



WPA2 is based upon the Institute for Electrical and Electronics Engineers (IEEE) 802.11i amendment to the 802.11 standard, which was ratified on July 29, 2004.

Q: How are WPA and WPA2 similar?

A: Both WPA and WPA2 offer a high level of assurance for end-users and network administrators that their data will remain private and access to their network restricted to authorized users. Both utilize 802.1X and Extensible Authentication Protocol (EAP) for authentication. Both have Personal and Enterprise modes of operation that meet the distinct needs of the two different consumer and enterprise market segments.

Q: How are WPA and WPA2 different?

A: WPA2 provides a **stronger encryption mechanism** through **Advanced Encryption Standard (AES)**, which is a requirement for some corporate and government users.

Kilde: <http://www.wifialliance.org> WPA2 Q and A

WPA Personal eller Enterprise



Personal - en delt hemmelighed, preshared key

Enterprise - brugere valideres op mod fælles server

Hvorfor er det bedre?

- Flere valgmuligheder - passer til store og små
 - WPA skifter den faktiske krypteringsnøgle jævnligt - TKIP
 - Initialisationsvektoren (IV) fordobles 24 til 48 bit
 - Imødekommer alle kendte problemer med WEP!
 - Integrerer godt med andre teknologier - RADIUS
-
- EAP - Extensible Authentication Protocol - individuel autentifikation
 - TKIP - WPA Temporal Key Integrity Protocol - nøgleskift og integritet
 - MIC - Message Integrity Code - Michael, ny algoritme til integritet
 - CCMP - WPA2 AES / Counter Mode CBC-MAC Protocol

Authentication Protocols RADIUS, PAP, CHAP, EAP



- Used for verifying credentials, typically username and password
- Extensible Authentication Protocol EAP
https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
- Challenge-Handshake Authentication Protocol
https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol
- Password Authentication Protocol
https://en.wikipedia.org/wiki/Password_Authentication_Protocol

Remote Authentication Dial-In User Service RADIUS



RADIUS er en protokol til autentificering af brugere op mod en fælles server

Remote Authentication Dial In User Service (RADIUS)

RADIUS er beskrevet i RFC-2865

RADIUS kan være en fordel i større netværk med

- dial-in
- administration af netværksudstyr
- trådløse netværk
- andre RADIUS kompatible applikationer

<https://en.wikipedia.org/wiki/RADIUS>

Hint: Jeg har publiceret en RADIUS konfiguration der giver WPA Enterprise - med vilkårligt brugernavn og kode!

<https://github.com/kramse/conference-open-8021x>



Nu skifter vi så til WPA og alt er vel så godt?

Desværre ikke!

Du skal vælge en laaaaang passphrase, ellers kan man sniffe WPA handshake når en computer går ind på netværket!

Med et handshake kan man med aircrack igen lave off-line bruteforce angreb!

Nye angreb gør at man ikke engang behøver et klient handshake, men kan snakke med AP alene!

WPA cracking demo



Vi konfigurerer AP med Henrik42 som WPA-PSK/passhrase

Vi finder netværk kismet eller airodump

Vi starter airodump mod specifik kanal

Vi spoofer deauth og opsamler WPA handshake

Vi knækker WPA :-)

Brug manualsiderne for programmerne i aircrack-ng pakken!

WPA cracking med aircrack - start



```
slax ~ # aircrack-ng -w dict wlan-test.cap  
Opening wlan-test.cap  
Read 1082 packets.
```

#	BSSID	ESSID	Encryption
1	00:11:24:0C:DF:97	wlan	WPA (1 handshake)
2	00:13:5F:26:68:D0	Noea	No data - WEP or WPA
3	00:13:5F:26:64:80	Noea	No data - WEP or WPA
4	00:00:00:00:00:00		Unknown

```
Index number of target network ? 1
```

WPA cracking med aircrack - start



[00:00:00] 0 keys tested (0.00 k/s)

KEY FOUND! [Henrik42]

```
Master Key      : 8E 61 AB A2 C5 25 4D 3F 4B 33 E6 AD 2D 55 6F 76
                  6E 88 AC DA EF A3 DE 30 AF D8 99 DB F5 8F 4D BD
Transcient Key  : C5 BB 27 DE EA 34 8F E4 81 E7 AA 52 C7 B4 F4 56
                  F2 FC 30 B4 66 99 26 35 08 52 98 26 AE 49 5E D7
                  9F 28 98 AF 02 CA 29 8A 53 11 EB 24 0C B0 1A 0D
                  64 75 72 BF 8D AA 17 8B 9D 94 A9 31 DC FB 0C ED

EAPOL HMAC      : 27 4E 6D 90 55 8F 0C EB E1 AE C8 93 E6 AC A5 1F
```

Min Thinkpad X31 med 1.6GHz Pentium M knækker ca. 150 Keys/sekund

Encryption key length



Encryption key lengths & hacking feasibility

<i>Type of Attacker</i>	<i>Budget</i>	<i>Tool</i>	<i>Time & Cost/Key 40 bit</i>	<i>Time & Cost/Key 56 bit</i>
Regular User	Minimal \$400	Scavenged computer time FPGA	1 week 5 hours (\$.08)	Not feasible 38 years (\$5,000)
Small Business	\$10,000	FPGA ¹	12 min. (\$.08)	556 days (\$5,000)
Corporate Department	\$300,000	FPGA ASIC ²	24 sec. (\$.08) 0.18 sec. (\$.001)	19 days (\$5,000) 3 hours (\$38)
Large Corporation	\$10M	ASIC	0.005 sec. (\$.001)	6 min. (\$38)
Intelligence Agency	\$300M	ASIC	0.0002 sec. (\$.001)	12 sec. (\$38)

Old, but think about your attackers and their budgets!

Kilde: http://www.mycrypto.net/encryption/encryption_crack.html

New attack on WPA/WPA2 using PMKID



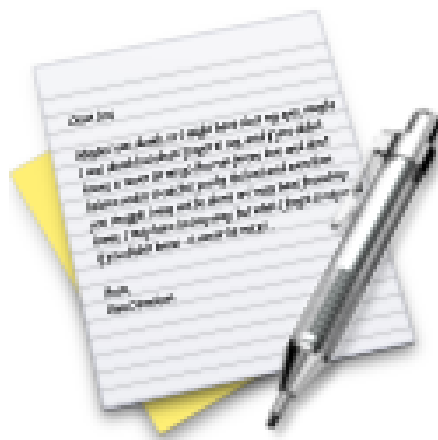
This attack was discovered accidentally while looking for new ways to attack the new WPA3 security standard. WPA3 will be much harder to attack because of its modern key establishment protocol called "Simultaneous Authentication of Equals"(SAE). The main difference from existing attacks is that in this attack, capture of a full EAPOL 4-way handshake is not required. The new attack is performed on the RSN IE (Robust Security Network Information Element) of a single EAPOL frame.

At this time, we do not know for which vendors or for how many routers this technique will work, but we think it will work against all 802.11i/p/q/r networks with roaming functions enabled (most modern routers).

The main advantages of this attack are as follow: No more regular users required - because the attacker directly communicates with the AP (aka "client-less" attack) No more waiting for a complete 4-way handshake between the regular user and the AP No more eventual retransmissions of EAPOL frames (which can lead to uncrackable results) No more eventual invalid passwords sent by the regular user No more lost EAPOL frames when the regular user or the AP is too far away from the attacker No more fixing of nonce and replaycounter values required (resulting in slightly higher speeds) No more special output format (pcap, hccapx, etc.) - final data will appear as regular hex encoded string

- <https://hashcat.net/forum/thread-7717.html> New attack on WPA/WPA2 using PMKID
- <https://www.evilssocket.net/2019/02/13/Pwning-WiFi-networks-with-bettercap-and-the-PMKID-client-less-attack/>

Exercise



Now lets do the exercise

! Aircrack-ng 30 min

which is number **48** in the exercise PDF.

WPA2 cracking med Pyrit



Pyrit takes a step ahead in attacking WPA-PSK and WPA2-PSK, the protocol that today de-facto protects public WIFI-airspace. The project's goal is to estimate the real-world security provided by these protocols. *Pyrit* does not provide binary files or wordlists and does not encourage anyone to participate or engage in any harmful activity. **This is a research project, not a cracking tool.**

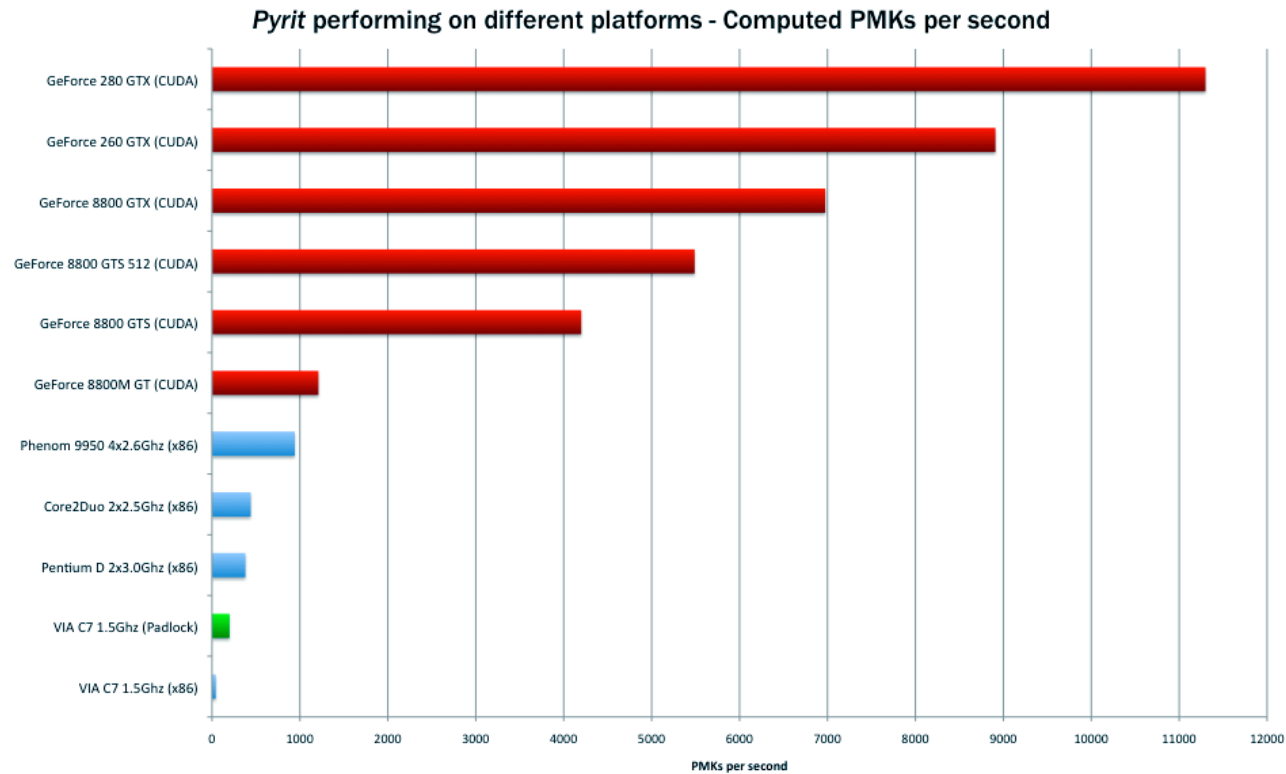
Pyrit's implementation allows to create massive databases, pre-computing part of the WPA/WPA2-PSK authentication phase in a space-time-tradeoff. The performance gain for real-world-attacks is in the range of three orders of magnitude which urges for re-consideration of the protocol's security. Exploiting the computational power of GPUs, *Pyrit* is currently by far the most powerful attack against one of the world's most used security-protocols.

sloooow, plejede det at være - 150 keys/s på min Thinkpad X31

Kryptering afhænger af SSID! Så check i tabellen er minutter.

<http://pyrit.wordpress.com/about/>

Tired of WoW?



Kilde: <http://code.google.com/p/pyrit/>

Hashcat Cracking passwords and secrets



- Hashcat is the world's fastest CPU-based password recovery tool.
- oclHashcat-plus is a GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.
- oclHashcat-lite is a GPGPU cracker that is optimized for cracking performance. Therefore, it is limited to only doing single-hash cracking using Markov attack, Brute-Force attack and Mask attack.
- John the Ripper password cracker old skool men stadig nyttig

Source:

<http://hashcat.net/wiki/>

<http://www.openwall.com/john/>

http://hashcat.net/wiki/doku.php?id=cracking_wpawpa2

Wi-Fi Protected Setup, WPS hacking - Reaver



Reaver Open Source Reaver implements a brute force attack against Wifi Protected Setup (WPS) registrar PINs in order to recover WPA/WPA2 passphrases, as described in http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.

Reaver has been designed to be a robust and practical attack against WPS, and has been tested against a wide variety of access points and WPS implementations.

On average Reaver will recover the target AP's plain text WPA/WPA2 passphrase in 4-10 hours, depending on the AP. In practice, it will generally take half this time to guess the correct WPS pin and recover the passphrase.

Hvad betyder ease of use?

Source:

<https://code.google.com/p/reaver-wps/>

<http://lifehacker.com/5873407/how-to-crack-a-wi-fi-networks-wpa-password-with-reaver>

WPS Design Flaws used by Reaver



Design Flaw #1

Option / Authentication	Physical Access	Web Interface	PIN
Push-button-connect	X		
PIN – Internal Registrar		X	
PIN – External Registrar			X

WPS Options and which kind of authentication they actually use.

As the External Registrar option does not require any kind of authentication apart from providing the PIN, it is potentially vulnerable to brute force attacks.

Pin only, no other means necessary

Source:

http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

WPS Design Flaws used by Reaver



IEEE 802.11/EAP Expanded Type, Vendor ID: WFA (0x372A), Vendor Type: SimpleConfig (0x01)			
M1	Enrollee → Registrar	N1 Description PK _E	Diffie-Hellman Key Exchange
M2	Enrollee ← Registrar	N1 N2 Description PK _R Authenticator	
M3	Enrollee → Registrar	N2 E-Hash1 E-Hash2 Authenticator	
M4	Enrollee ← Registrar	N1 R-Hash1 R-Hash2 E _{KeyWrapKey} (R-S1) Authenticator	proove posession of 1 st half of PIN
M5	Enrollee → Registrar	N2 E _{KeyWrapKey} (E-S1) Authenticator	proove posession of 1 st half of PIN
M6	Enrollee ← Registrar	N1 E _{KeyWrapKey} (R-S2) Authenticator	proove posession of 2 nd half of PIN
M7	Enrollee → Registrar	N2 E _{KeyWrapKey} (E-S2 ConfigData) Authenticator	proove posession of 2 nd half of PIN, send AP configuration
M8	Enrollee ← Registrar	N1 E _{KeyWrapKey} (ConfigData) Authenticator	set AP configuration

<p>Enrollee = AP Registrar = Supplicant = Client/Attacker</p> <p>PK_E = Diffie-Hellman Public Key Enrollee PK_R = Diffie-Hellman Public Key Registrar Authkey and KeyWrapKey are derived from the Diffie-Hellman shared key.</p> <p>Authenticator = HMAC_{AuthKey}(last message current message)</p> <p>E_{KeyWrapKey} = Stuff encrypted with KeyWrapKey (AES-CBC)</p>	<p>PSK1 = first 128 bits of HMAC_{AuthKey}(1st half of PIN) PSK2 = first 128 bits of HMAC_{AuthKey}(2nd half of PIN)</p> <p>E-S1 = 128 random bits E-S2 = 128 random bits E-Hash1 = HMAC_{AuthKey}(E-S1 PSK1 PK_E PK_R) E-Hash2 = HMAC_{AuthKey}(E-S2 PSK2 PK_E PK_R)</p> <p>R-S1 = 128 random bits R-S2 = 128 random bits R-Hash1 = HMAC_{AuthKey}(R-S1 PSK1 PK_E PK_R) R-Hash2 = HMAC_{AuthKey}(R-S2 PSK2 PK_E PK_R)</p>
---	--

1	2	3	4	5	6	7	0
1 st half of PIN				checksum			
				2 nd half of PIN			

Reminds me of NTLM cracking, crack parts independently

Source:

http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

WPS Design Flaws used by Reaver



Design flaw #2

An attacker can derive information about the correctness of parts the PIN from the AP's responses.

- If the attacker receives an EAP-NACK message after sending M4, he knows that the 1st half of the PIN was incorrect.
- If the attacker receives an EAP-NACK message after sending M6, he knows that the 2nd half of the PIN was incorrect.

This form of authentication dramatically decreases the maximum possible authentication attempts needed from 10^8 (=100.000.000) to $10^4 + 10^4$ (=20.000).

As the 8th digit of the PIN is always a checksum of digit one to digit seven, there are at most $10^4 + 10^3$ (=11.000) attempts needed to find the correct PIN.

100.000.000 is a lot, 11.000 is not

Source:

http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

Reaver Rate limiting



```
Kali 64-bit
Applications Places Thu May 30, 11:54 AM root
root@kali01: ~
File Edit View Search Terminal Help
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M3 message
[+] Received M3 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] 0.05% complete @ 2013-05-30 11:49:58 (7 seconds/pin)
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
root@kali01: ~
```

Make no mistake, it will work!



WPA3

In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2.[12][13] Certification began in June 2018,[14] and WPA3 support has been mandatory for devices which bear the "Wi-Fi CERTIFIED™" logo since July 2020.[11]

The new standard uses an equivalent 192-bit cryptographic strength in WPA3-Enterprise mode[15] (AES-256 in GCM mode with SHA-384 as HMAC), and still mandates the use of CCMP-128 (AES-128 in CCM mode) as the minimum encryption algorithm in WPA3-Personal mode.

The WPA3 standard also replaces the pre-shared key (PSK) exchange with Simultaneous Authentication of Equals (SAE) exchange, a method originally introduced with IEEE 802.11s, resulting in a more secure initial key exchange in personal mode[16][17] and forward secrecy.[18] The Wi-Fi Alliance also says that WPA3 will mitigate security issues posed by weak passwords and simplify the process of setting up devices with no display interface.[2][19]

Protection of management frames as specified in the IEEE 802.11w amendment is also enforced by the WPA3 specifications.

Source: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

- Does not seem to be used much, in Denmark, yet – but coming

IS WPA3 supported?



A wireless network adapter that supports Wi-Fi 6. To see if your PC supports it, check the documentation that came with it or check the PC manufacturer's website. Tip: You can also check to see if your router supports Wi-Fi 6 by opening the Command Prompt, and then typing the command `netsh wlan show drivers`. Look next to Radio types supported and see if it includes 802.11ax.

Source: <https://support.microsoft.com/en-us/windows/faster-and-more-secure-wi-fi-in-windows-26177a28-38ed-1a8e-7e>

- Your devices must support both WPA3 in both operating system and Wi-Fi drivers!
- Windows 10 and 11 does, so try upgrading drivers
- Android does since Android 10 – pretty new still
- Apple devices have support in recent versions

WPA3 on Apple Devices



- iPhone 7 or later.
- iPad 5th generation or later.
- Apple TV 4K or later.
- Apple Watch series 3 or later.
- Mac computers (late 2013 or later, with 802.11ac or later)

Source: <https://support.apple.com/da-dk/guide/security/sec8a67fa93d/web>



WPA3™ provides cutting-edge security protocols to the market. Building on the widespread success and adoption of Wi-Fi security, WPA3 adds new features to simplify Wi-Fi security, enable more robust authentication, deliver increased cryptographic strength for highly sensitive data markets, and maintain resiliency of mission critical networks. All WPA3 networks:

- Use the latest security methods
- Disallow outdated legacy protocols
- Require use of Protected Management Frames (PMF)

Since Wi-Fi networks differ in usage purpose and security needs, WPA3 includes additional capabilities specifically for personal and enterprise networks. Users of WPA3-Personal receive increased protections from password guessing attempts, while WPA3-Enterprise users can now take advantage of higher-grade security protocols for sensitive data networks.

WPA3 is a mandatory certification for Wi-Fi CERTIFIED™ devices.

Source: <https://www.wi-fi.org/discover-wi-fi/security>

WPA3-Personal



WPA3-Personal brings better protections to individual users by providing more robust password-based authentication, even when users choose passwords that fall short of typical complexity recommendations. This capability is enabled through Simultaneous Authentication of Equals (SAE). The technology is resistant to offline dictionary attacks where an adversary attempts to determine a network password by trying possible passwords without further network interaction.

- **Natural password selection:** Allows users to choose passwords that are easier to remember
- **Ease of use:** Delivers enhanced protections with no change to the way users connect to a network
- **Forward secrecy:** Protects data traffic even if a password is compromised after the data was transmitted

Source: <https://www.wi-fi.org/discover-wi-fi/security>

WPA3-Enterprise



WPA3-Enterprise builds upon the foundation of WPA2-Enterprise with the additional requirement of using Protected Management Frames on all WPA3 connections.

- **Authentication:** multiple Extensible Authentication Protocol (EAP) methods
- **Authenticated encryption:** minimum 128-bit Advanced Encryption Standard Counter Mode with Cipher Block Chaining Message Authentication (AES-CCMP 128)
- **Key derivation and confirmation:** minimum 256-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA256)
- **Robust management frame protection:** minimum 128-bit Broadcast/Multicast Integrity Protocol Cipher-based Message Authentication Code (BIP-CMAC-128)

Source: <https://www.wi-fi.org/discover-wi-fi/security>

WPA3-Enterprise with 192-bit mode



WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data.

- **Authentication:** Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) using Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
- **Authenticated encryption:** 256-bit Galois/Counter Mode Protocol (GCMP-256)
- **Key derivation and confirmation:** 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
- **Robust management frame protection:** 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

The 192-bit security mode offered by WPA3-Enterprise ensures the right combination of cryptographic tools are used and sets a consistent baseline of security within a WPA3 network.

Source: <https://www.wi-fi.org/discover-wi-fi/security>

2020: Dragonblood



April 2019 — Modern Wi-Fi networks use WPA2 to protect transmitted data. However, because **WPA2 is more than 14 years old**, the Wi-Fi Alliance recently announced the new and more secure WPA3 protocol. One of the supposed advantages of WPA3 is that, thanks to its underlying **Dragonfly handshake**, it's **near impossible to crack the password** of a network. Unfortunately, we found that even with WPA3, an **attacker within range of a victim can still recover the password**. If the victim uses no extra protection such as HTTPS, this allows an attacker to steal sensitive information such as passwords and emails. We hope our disclosure motivates vendors to mitigate our attacks before WPA3 becomes widespread.

...

Fortunately, as a result of our research, both the Wi-Fi standard and EAP-pwd are being updated with a more secure protocol. Although this update is not backwards-compatible with current deployments of WPA3, it does prevent most of our attacks.

Source: <https://wpa3.mathyvanhoef.com/>

- Side-channel leaks
- Full paper Mathy Vanhoef and Eyal Ronen. 2020. *Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd*. In IEEE Symposium on Security & Privacy (SP). IEEE. <https://eprint.iacr.org/2019/383>

2021: Fragment and Forge



Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation

Abstract In this paper, we present three design flaws in the **802.11 standard that underpins Wi-Fi**. One design flaw is in the frame aggregation functionality, and another two are in the frame fragmentation functionality. These design flaws enable an adversary to **forge encrypted frames** in various ways, which in turn enables **exfiltration of sensitive data**. We also discovered common implementation flaws related to aggregation and fragmentation, which further worsen the impact of our attacks. Our results **affect all protected Wi-Fi networks, ranging from WEP all the way to WPA3**, meaning the discovered flaws have been part of Wi-Fi **since its release in 1997**. In our experiments, all devices were vulnerable to one or more of our attacks, confirming that **all Wi-Fi devices are likely affected**. Finally, we present a tool to test whether devices are affected by any of the vulnerabilities, and we discuss countermeasures to prevent our attacks.

Source: Mathy Vanhoef <https://eprint.iacr.org/2021/763.pdf> (bold by me)

Når adgangen er skabt

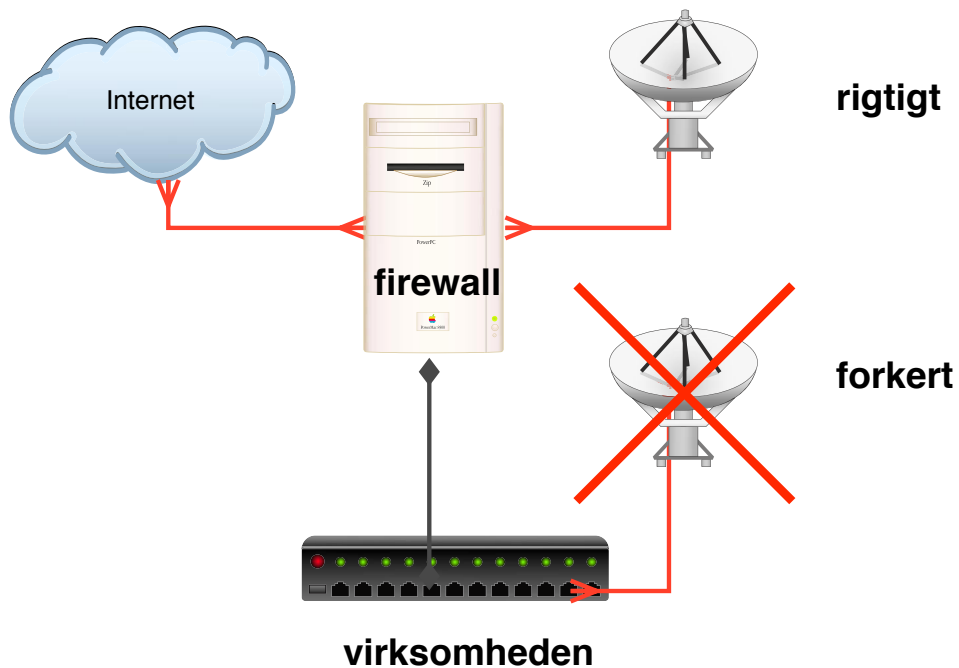


Så går man igang med de almindelige værktøjer

Fyodor Top Network Security Tools <http://www.sectools.org>

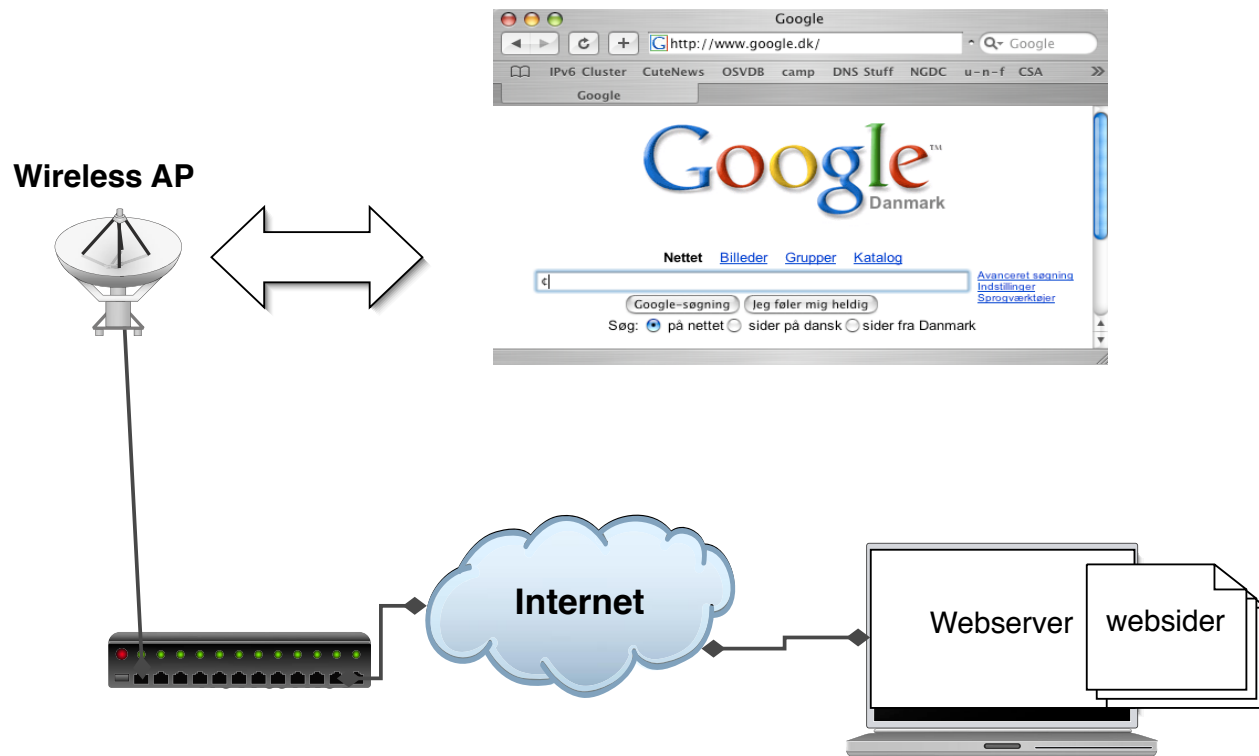
Forsvaret er som altid - flere lag af sikkerhed!

Infrastrukturændringer

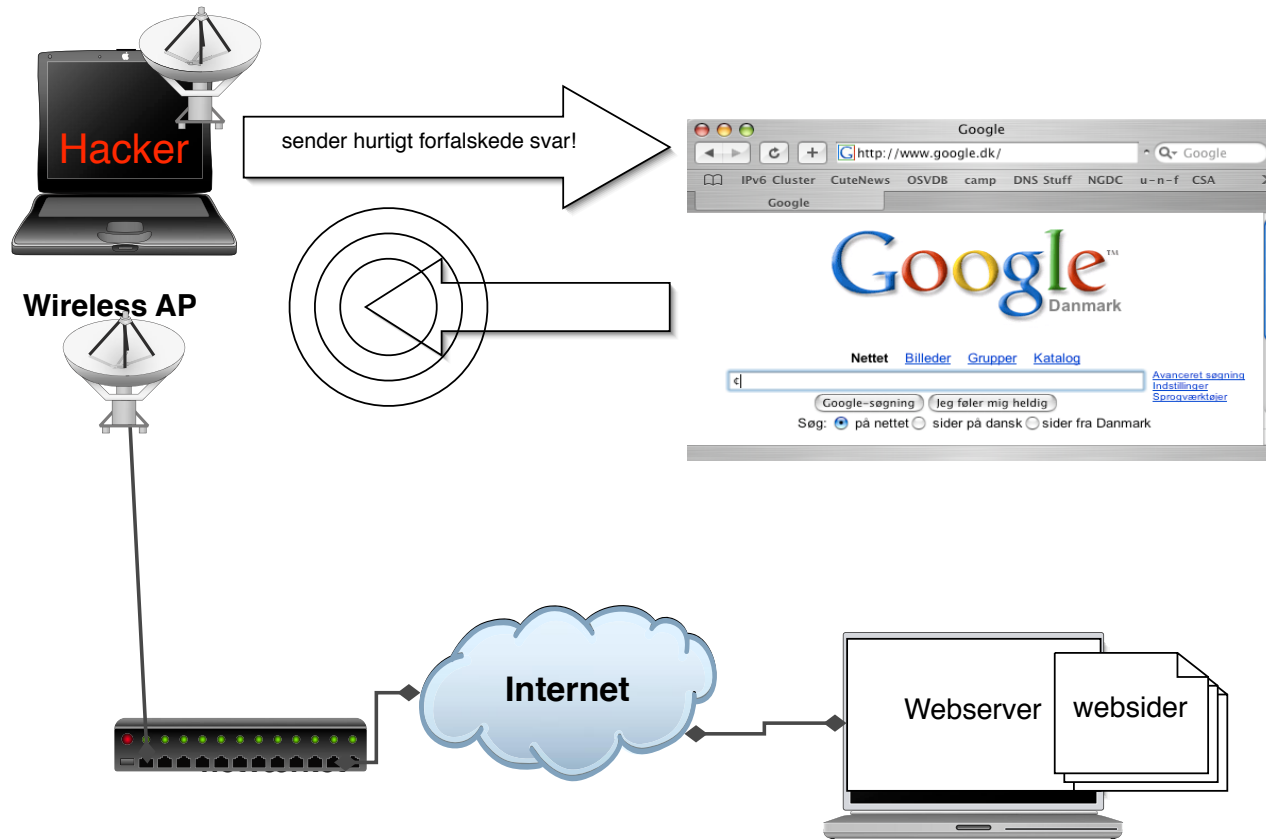


Sådan bør et access point logisk forbindes til netværket

Normal WLAN brug



Packet injection - airpwn





Klienten sender forespørgsel

Hackerens program airpwn lytter og sender så falske pakker

Hvordan kan det lade sig gøre?

- Normal forespørgsel og svar på Internet tager 50ms
- Airpwn kan svare på omkring 1ms angives det
- Airpwn har alle informationer til rådighed

Airpwn på Defcon 2004 - findes på Sourceforge

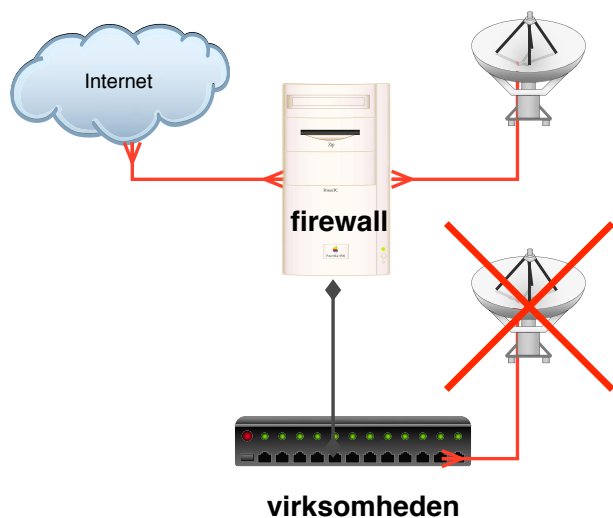
<http://airpwn.sourceforge.net/>

NB: Airpwn som demonstreret er begrænset til TCP og ukrypterede forbindelser



Lad være med at bruge et wireless-kort i en PC til at lave AP, brug et AP
Husk et AP kan være en router, men den kan ofte også blot være en bro
Brug mindst WPA2 og overvej at lave en decideret DMZ til WLAN
Placer AP hensigtsmæssigt og gerne højt, oppe på et skab eller lignende

Recommendations for wireless networks

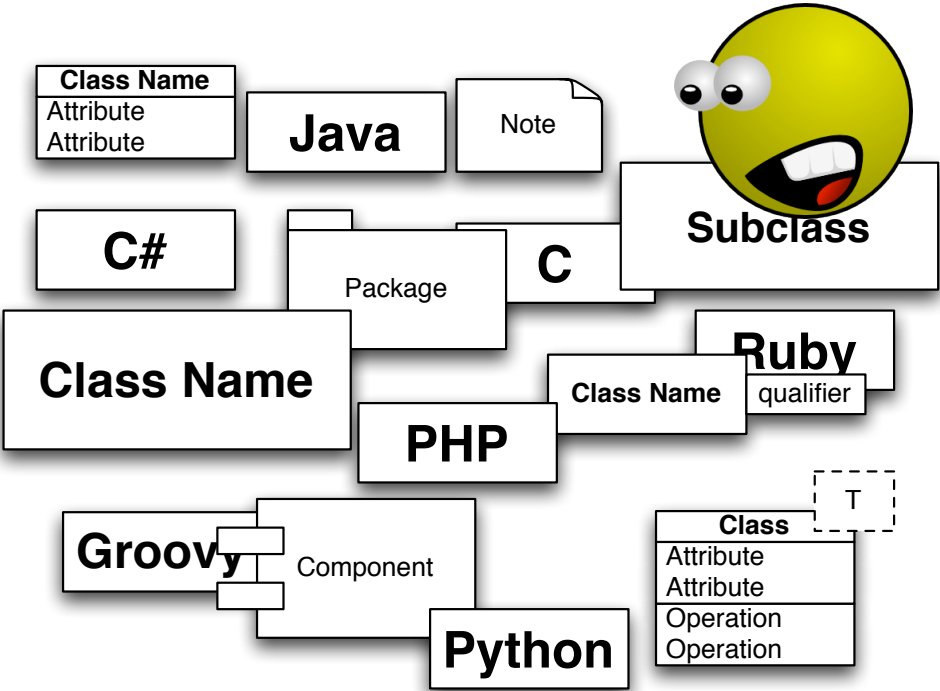


- Use a specific SSID - network name, influences the WPA PSK keying
- Never use WEP
- Use WPA PSK or Enterprise, or at least some VPN with individual user logins
- When using WPA Personal/PSK passphrase must be long, like +40 chars!
- Place network Access Points on the network where they can be monitored. Separate VLAN, isolated from the cabled LAN
- Have rules for the use of wireless networks, also for persons travelling - "Always use VPN when using insecure wireless in hotels, airports etc."

rigtig

forkert

Bonus: Next step, software sikkerhed



Wireless AP implementerer protokoller med hardware+software

Sårbare AP'er - 1



Hvordan bygger man et billigt Access Point?

- En embedded kerne
- En embedded TCP/IP stak
- Noget 802.11 hardware
- Et par Ethernet stik
- eventuelt et modem
- Tape ...

Hvad med efterfølgende opdatering af software?

Sårbare AP'er - 2



Eksempler på access point sårbarheder:

Konfigurationsfilen kan hentes uden autentificering - inkl. WEP nøgler

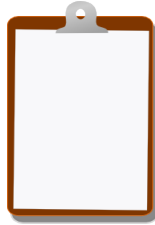
Konfigurationen sker via SNMP - som sender community string i klar tekst

Wi-Fi Protected Setup,(WPS) kan ikke slås helt fra

...

Konklusionen er klar - hardwaren er i mange tilfælde ikke sikker nok til at anvende på forretnings-kritiske LAN segmenter!

For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools