Welcome to

Wifi Security

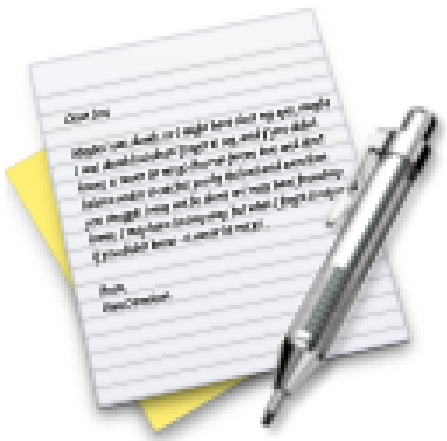
Communication and Network Security 2019

Henrik Lund Kramshøj hlk@zencurity.dk

Slides are available as PDF, kramse@Github

6-Wifi-Security.tex in the repo security-courses

Exercise



Now lets do the exercise

??

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

Trådløse teknologier 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, og draft
- 802.11i Security enhancements

Der er proprietære versioner 22Mbps og den slags
- det anbefales IKKE at benytte disse da det giver vendor lock-in - man bliver låst fast

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

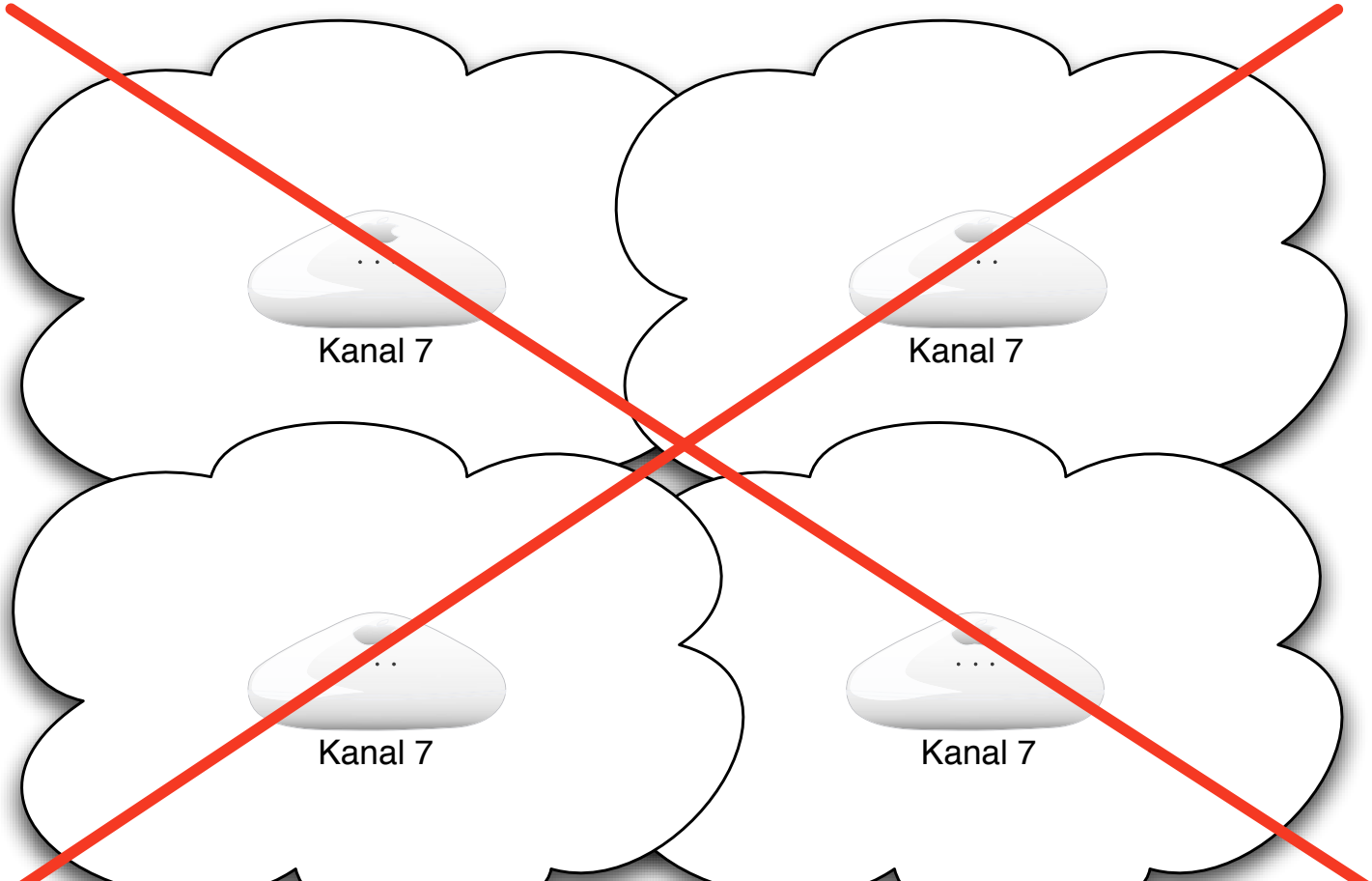
Alternativt kan wireless kort oprette ad-hoc netværk - hvor trafikken går direkte mellem netkort

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

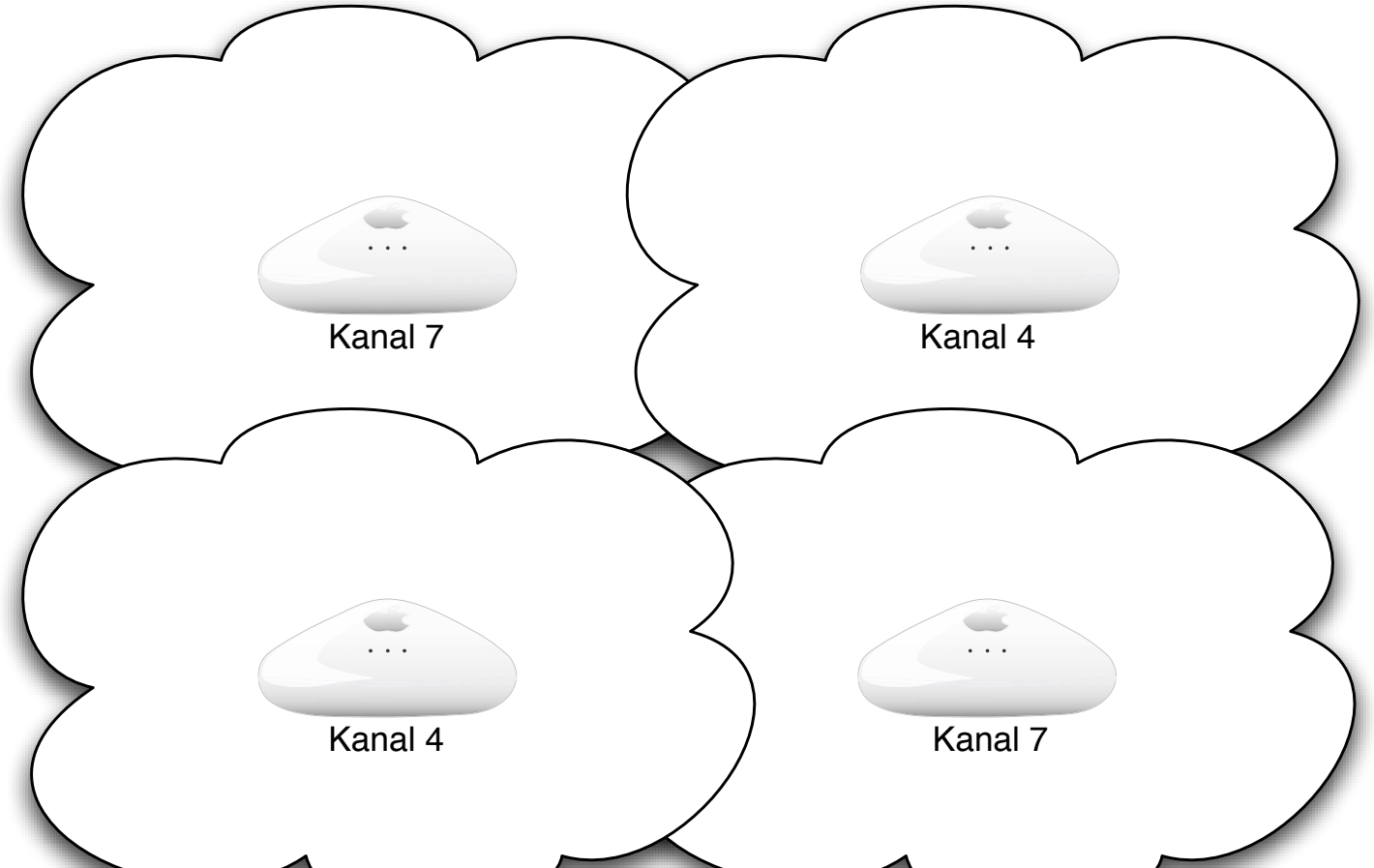
Helst 2 kanaler spring for 802.11b AP der placeres indenfor rækkevidde

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

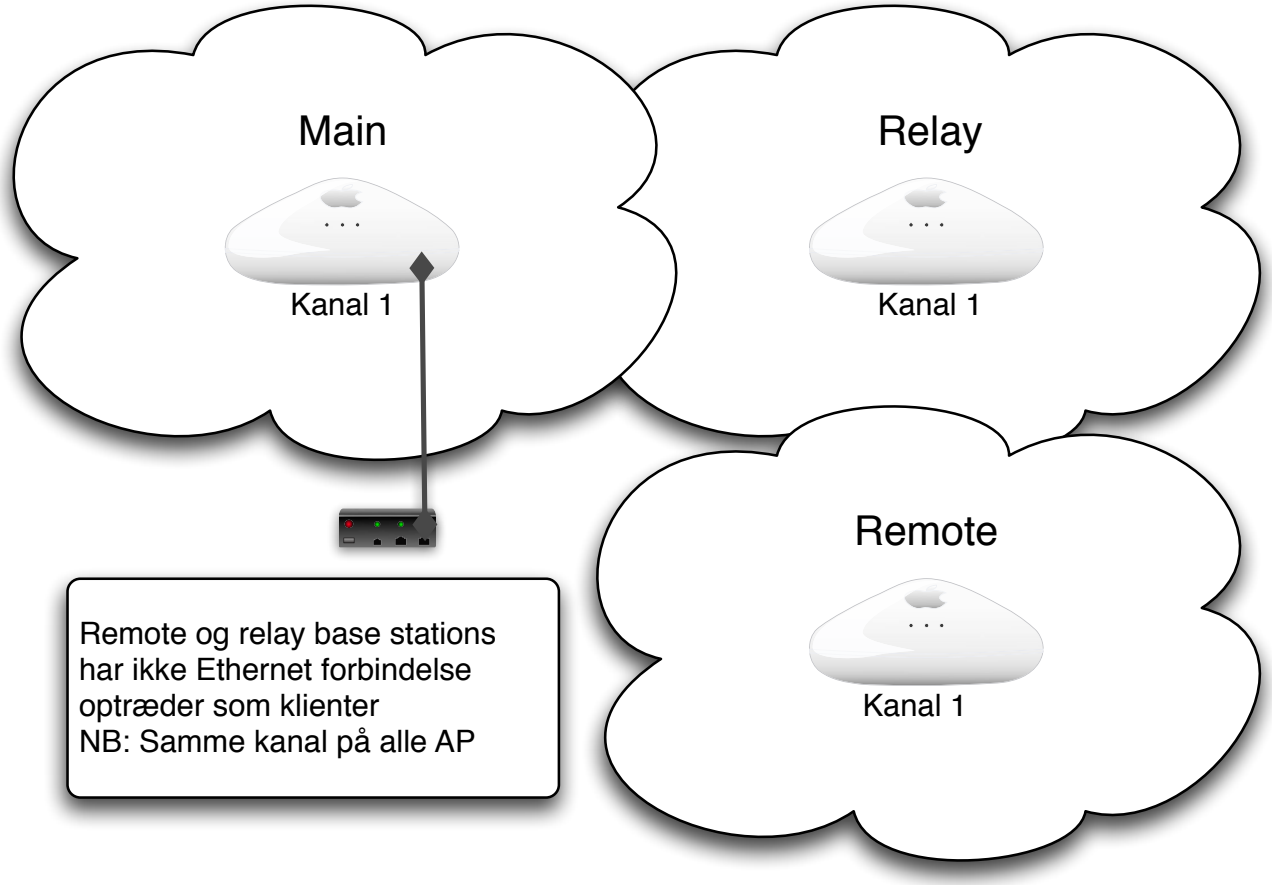
Eksempel på netværk med flere AP'er



Eksempel på netværk med flere AP'er



Wireless Distribution System WDS



(802.11 med WDS)

Er trådløse netværk interessante?

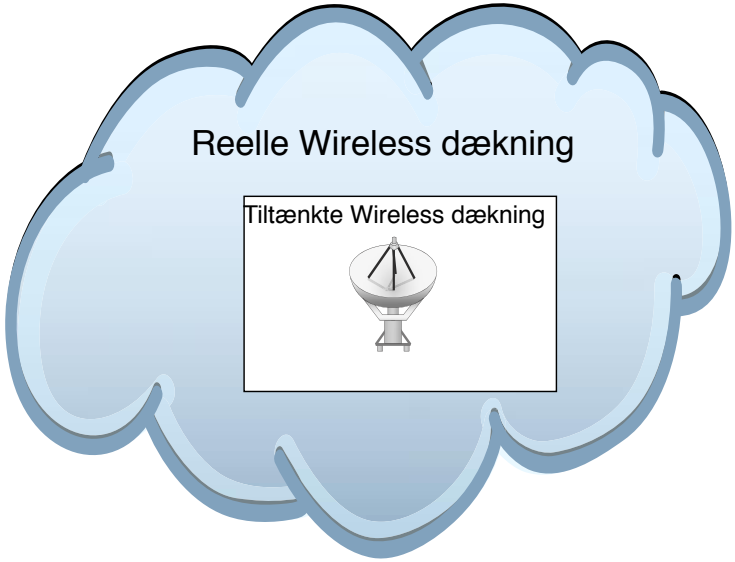
Sikkerhedsproblemer i de trådløse netværk er mange

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

Trådløst udstyr er blevet meget billigt!

Det er et krav fra brugerne - trådløst er lækkert

Konsekvenserne



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

Værktøjer

Alle bruger nogenlunde de samme værktøjer, måske forskellige mærker

- Wirelessscanner - Kismet og netstumbler
- Wireless Injection - typisk på Linux
- ...
- Aircrack-ng

Jeg anbefaler Auditor Security Collection og BackTrack boot CD'erne

Konsulentens udstyr wireless

Laptop med PC-CARD slot

Trådløse kort Atheros, de indbyggede er ofte ringe ;-)

Access Points - jeg anbefaler Airport Express

Antenner hvis man har lyst

Bøger:

- *Real 802.11 security*
- Se oversigter over bøger og værktøjer igennem præsentationen:

Internetressourcer:

- BackTrack - CD image med Linux+værktøjer
- Packetstorm wireless tools `http://packetstormsecurity.org/wireless/`
- *Beginner's Guide to Wireless Auditing* David Maynor `http://www.securityfocus.com/infocus/1877?ref=rss`

Typisk brug af 802.11 udstyr

Wireless Access Point

netværket - typisk Ethernet

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

Trådløs sikkerhed

- Trådløs sikkerhed - WPA og WPA2

Wireless networking sikkerhed i 802.11b

Sikkerheden er baseret på nogle få forudsætninger

- SSID - netnavnet
- WEP *kryptering* - Wired Equivalent Privacy
- måske MAC flitrering, kun bestemte kort må tilgå accesspoint

Til gengæld er disse forudsætninger ofte ikke tilstrækkelige ...

- WEP er måske *ok* til visse små hjemmenetværk
- WEP er baseret på en DELT hemmelighed som alle stationer kender

Forudsætninger

Til gengæld er disse forudsætninger ofte ikke tilstrækkelige ...

Hvad skal man beskytte?

Hvordan kan sikkerheden omgås?

Mange firmaer og virksomheder stille forskellige krav til sikkerheden - der er ikke en sikkerhedsmekanisme der passer til alle

SSID - netnavnet

Service Set Identifier (SSID) - netnavnet

32 ASCII tegn eller 64 hexadecimale cifre

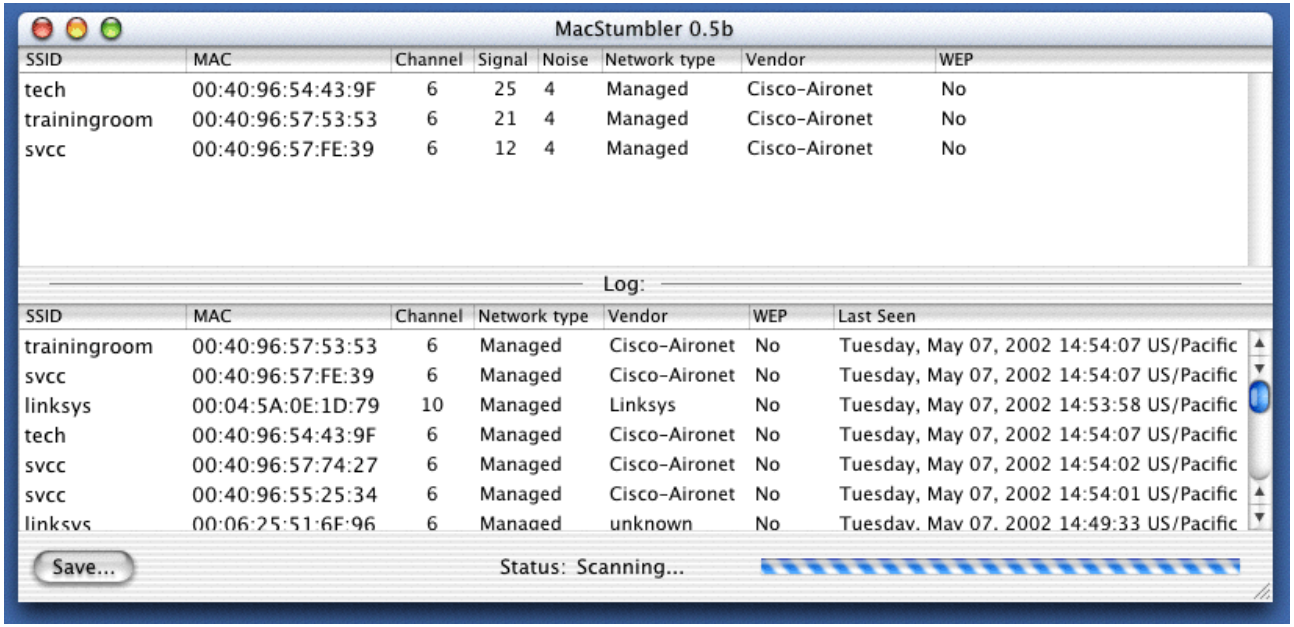
Udstyr leveres typisk med et standard netnavn

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

SSID kaldes også for NWID - network id

SSID broadcast - udstyr leveres oftest med broadcast af SSID

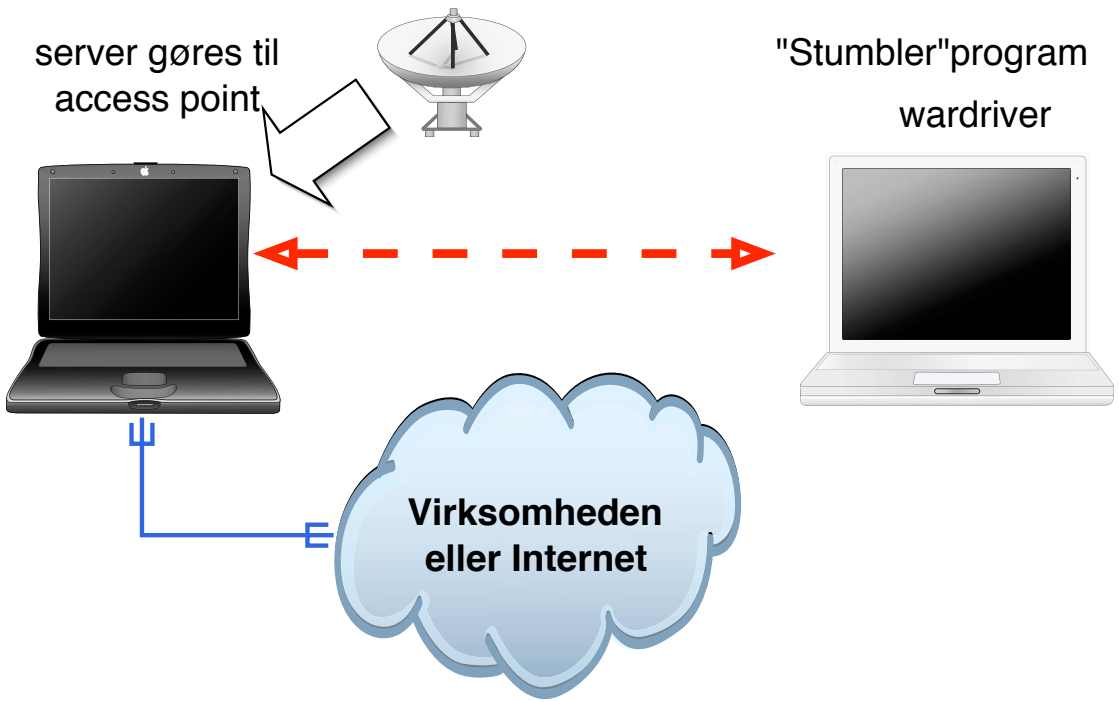
Demo: wardriving med stumbler programmer



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

- Netstumbler - Windows `http://www.netstumbler.com`
- dstumbler - UNIX `http://www.dachb0den.com/projects/dstumbler.html`
- iStumbler - Mac `http://www.istumbler.net/`

Start på demo - wardriving



Standard UNIX eller windows PC kan bruges som host based accesspoint - med det rigtige kort!

MAC filtrering

De fleste netkort tillader at man udskifter sin MAC adresse

MAC adressen på kortene er med i alle pakker der sendes

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

MAC adressen kan derfor overtages, når en af de tilladte stationer forlader området ...

Resultater af wardriving

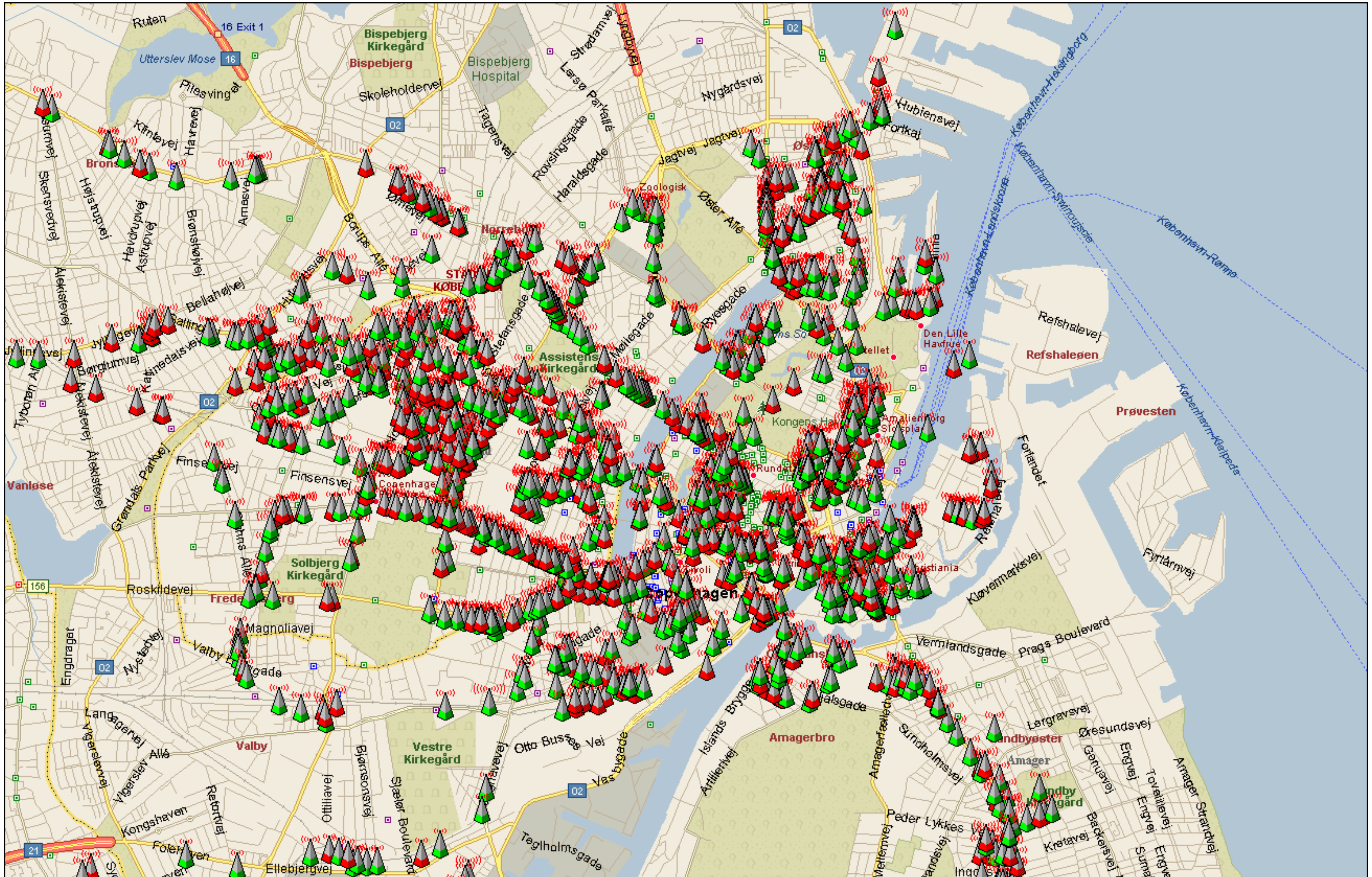
Hvad opdager man ved wardriving?

- at WEP IKKE krypterer hele pakken
- at alle pakker indeholder MAC adressen
- WEP nøglen skifter sjældent
- ca. 2/3 af de netværk man finder har ikke WEP slået til - og der er fri og uhindret adgang til Internet

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

Medmindre man kender virksomheden og WEP nøglen ikke er skiftet ... det er besværligt at skifte den, idet alle stationer skal opdateres.

Storkøbenhavn



Informationsindsamling

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

WEP kryptering

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 som sikkerhed

WEP er *ok* til et privat hjemmenetværk

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?

WEP sikkerhed

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.

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 implementaions of this attack. `http://airsnort.shmoo.com/`

major cryptographic errors

weak keying - 24 bit er allerede kendt - 128-bit = 104 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 afvikling

Når airodump kører opsamles pakkerne
samtidig vises antal initialisationsvektorer IV's:

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

NB: dataopsamlingen er foretaget på 100% opdateret Mac udstyr

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! [ CF62B64F03F13B6A3AF15BF5F6 ]
```

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 moderne 1.6GHz CPU med almindelig laptop disk tager typisk mindre end 60 sekunder

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.

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

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

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 - Temporal Key Integrity Protocol - nøgleskift og integritet
- MIC - Message Integrity Code - Michael, ny algoritme til integritet

WPA cracking

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!

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

Type of Attacker	*Budget*	Tool	*Time & Cost/Key 40 bit*	*Time & Cost/Key 56 bit*
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.($0.001)	6 min. ($38)
Intelligence Agency	$300M	ASIC	0.0002 sec.($0.001)	12 sec. ($38)

WPA 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.**

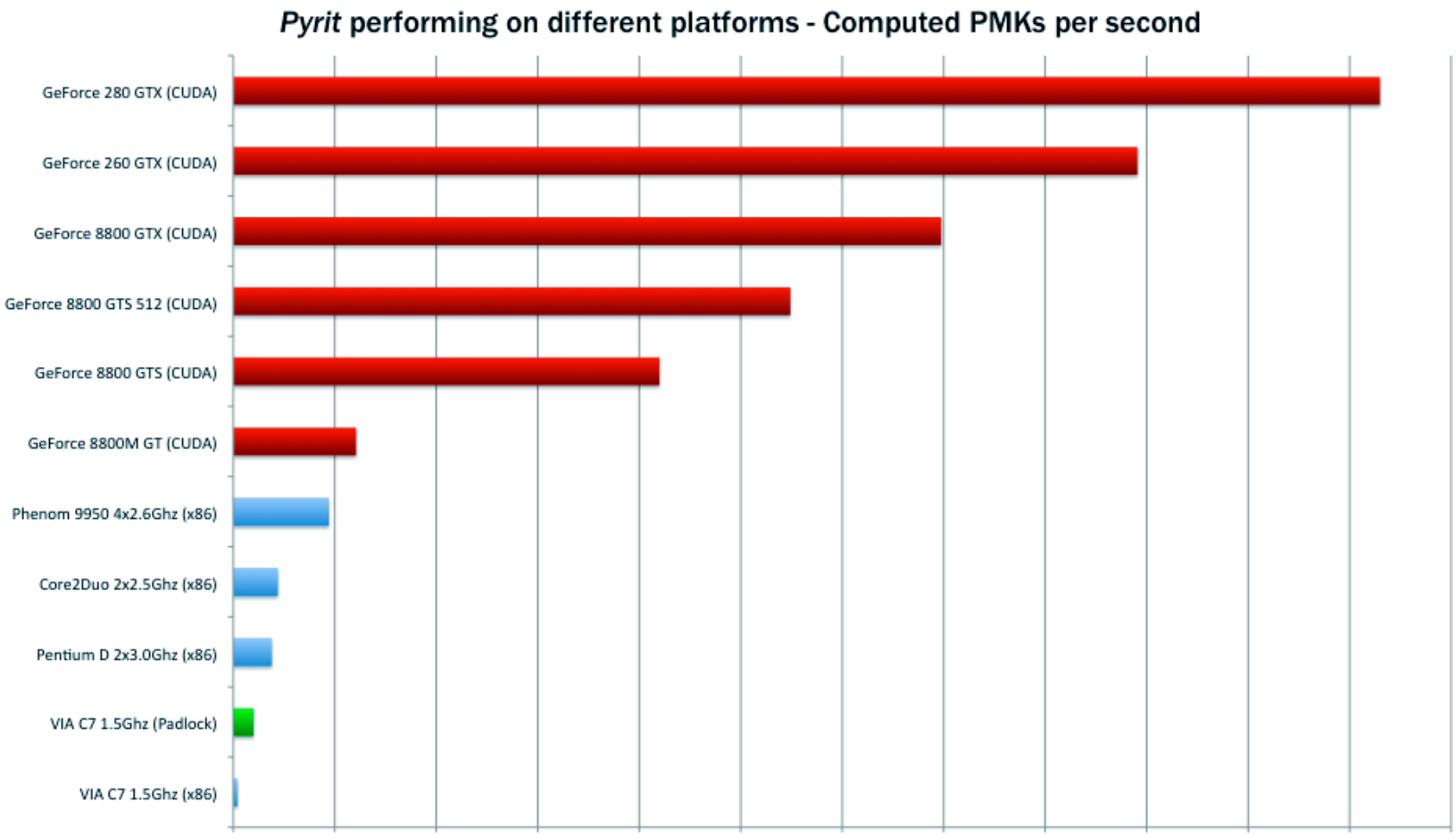
Pyrit's implementation allows to create massive databases, pre-computing part of the WPA/WPA2-PSK authentication phase in a space-time-tradeoff. The performance gain for real-world-attacks is in the range of three orders of magnitude which urges for re-consideration of the protocol's security. Exploiting 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?


Pyrit performing on different platforms - Computed PMKs per second
GeForce 280 GTX (CUDA)
GeForce 260 GTX (CUDA)
GeForce 8800 GTX (CUDA)
GeForce 8800 GTS 512 (CUDA)
GeForce 8800 GTS (CUDA)
GeForce 8800M GT (CUDA)
Phenom 9950 4x2.6Ghz (x86)
Core2Duo 2x2.5Ghz (x86)
Pentium D 2x3.0Ghz (x86)
VIA C7 1.5Ghz (Padlock)
VIA C7 1.5Ghz (x86)

Tools man bør kende

- Aircrack http://www.aircrack-ng.org/
- Kismet `http://www.kismetwireless.net/`
- Airsnort `http://airsnort.shmoo.com/` læs pakkerne med WEP kryptering
- Airsnarf `http://airsnarf.shmoo.com/` - lav dit eget AP parallelt med det rigtige og snif hemmeligheder
- Wireless Scanner `http://www.iss.net/` - kommercielt krypteringen i WEP
- Dette er et lille uddrag af programmer
  Se også `http://packetstormsecurity.org/wireless/`

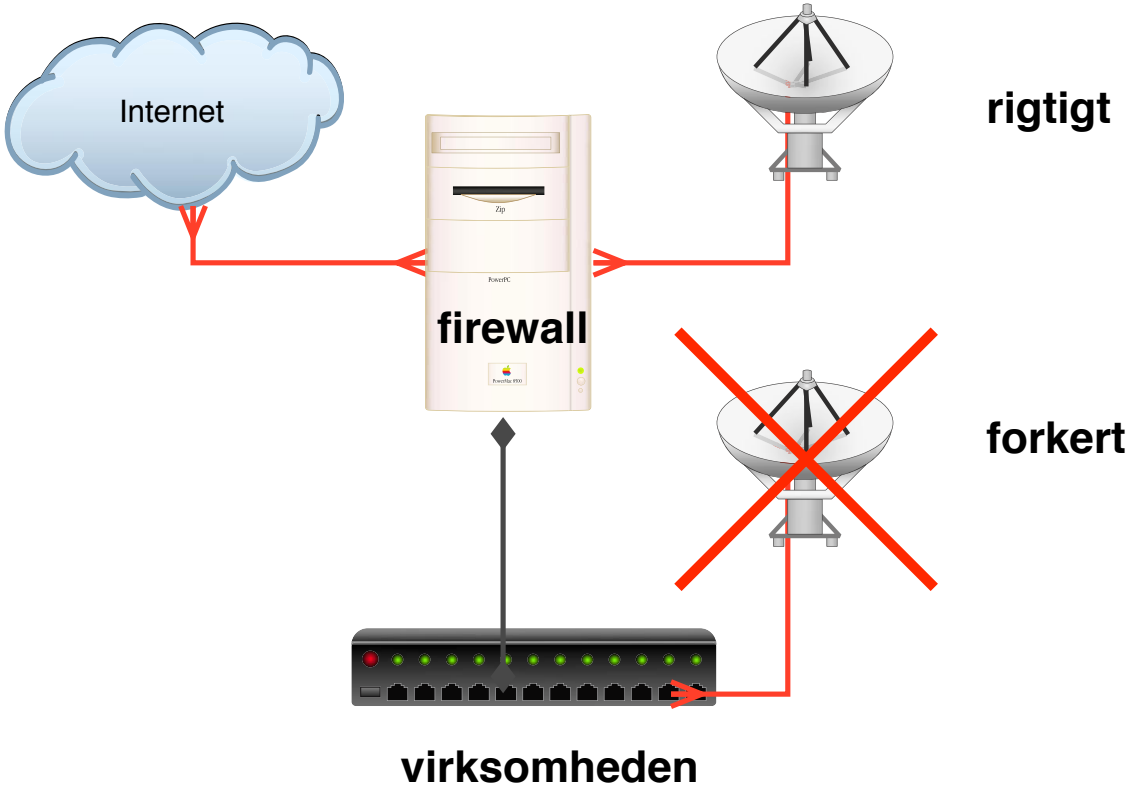
Når adgangen er skabt

Så går man igang med de almindelige værktøjer

Fyodor Top 100 Network Security Tools `http://www.sectools.org`

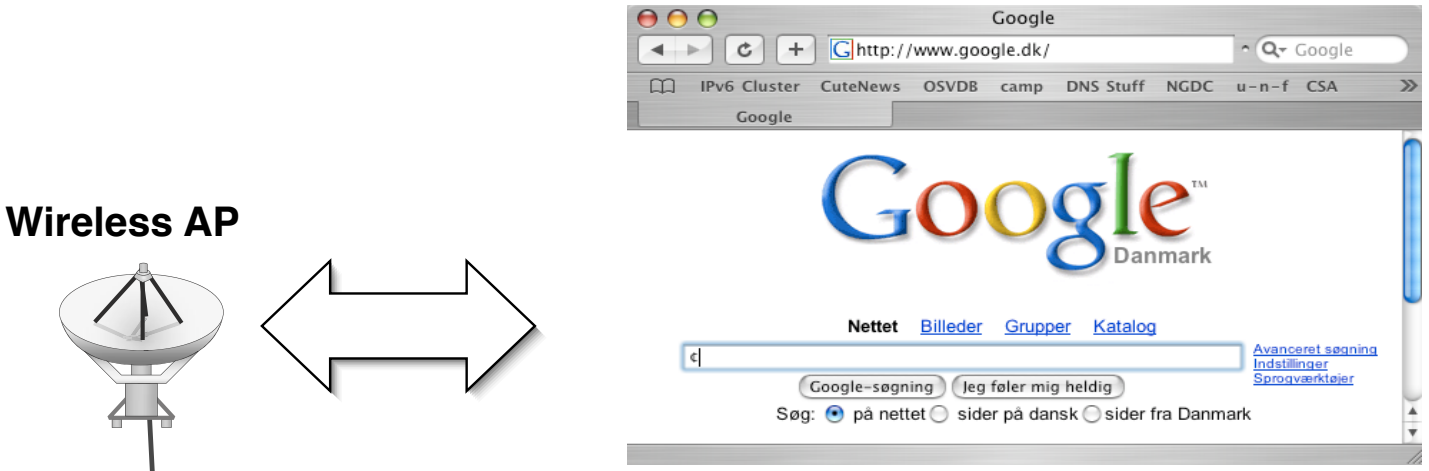
Forsvaret er som altid - flere lag af sikkerhed!

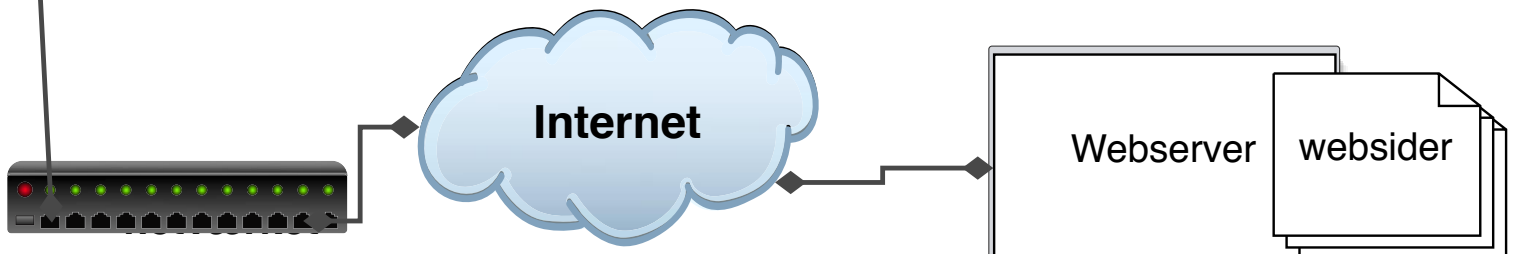
Infrastrukturændringer



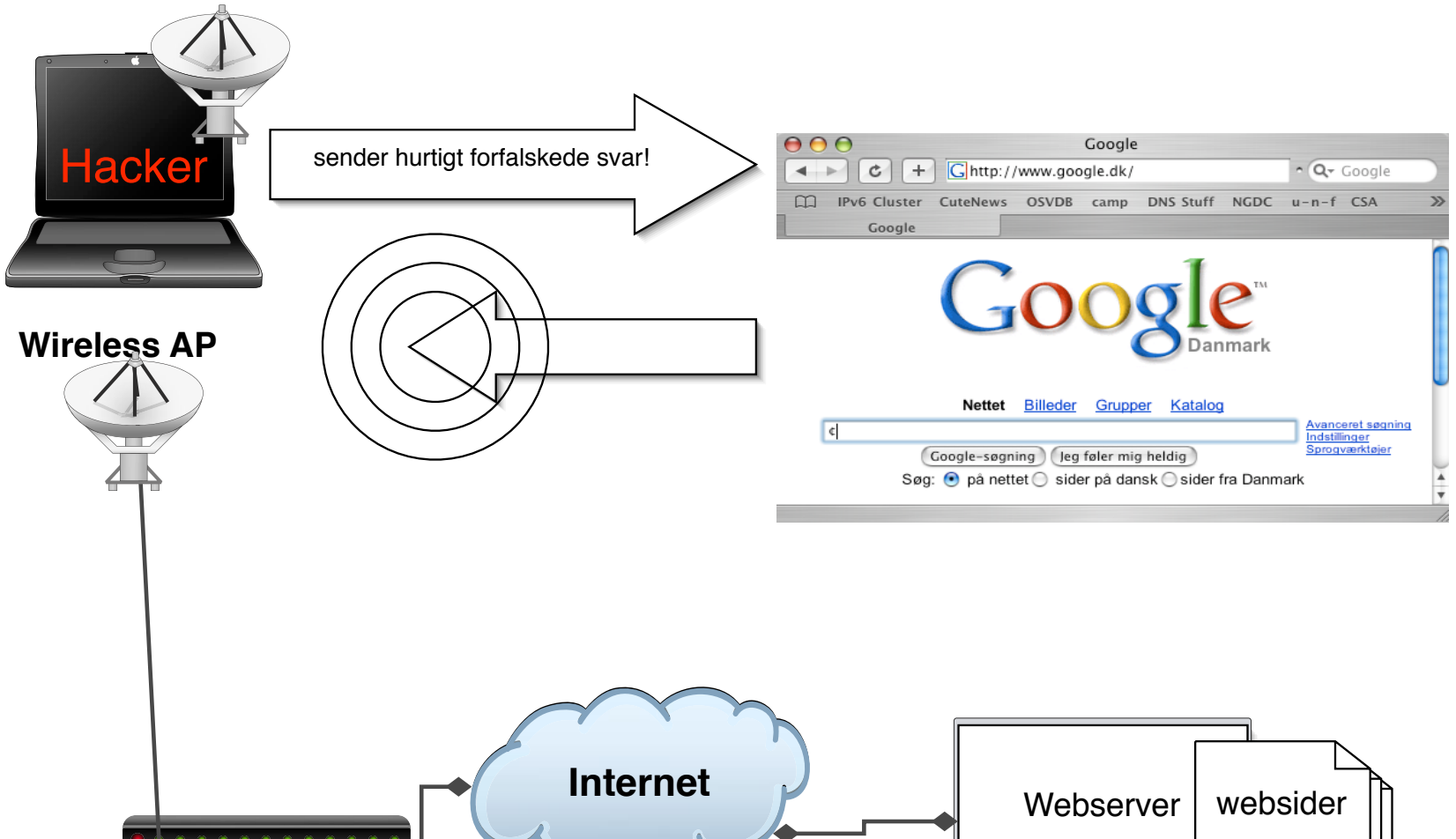
Sådan bør et access point forbindes til netværket

Normal WLAN brug





Packet injection - airpwn



Airpwn teknikker

Klienten sender forespørgsel

Hackerens program airpwn lytter og sender så falske pakker

Hvordan kan det lade sig gøre?

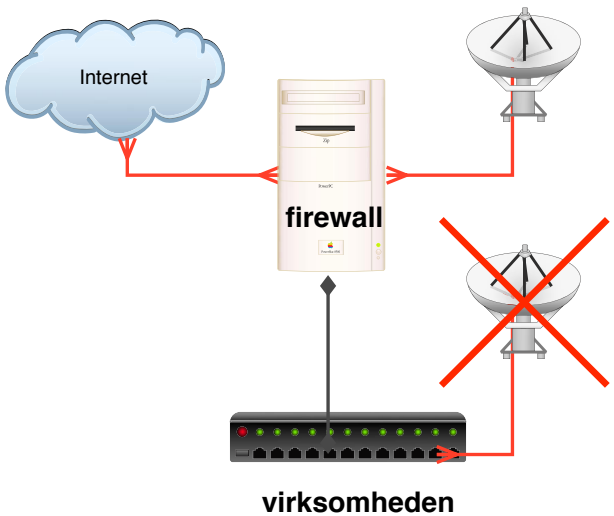
- Normal forespørgsel og svar på Internet tager 50ms
- Airpwn kan svare på omkring 1ms angives det
- Airpwn har alle informationer til rådighed

Airpwn på Defcon 2004 - findes på Sourceforge

`http://airpwn.sourceforge.net/`

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

Anbefalinger mht. trådløse netværk



rigtigt

- Brug noget tilfældigt som SSID - netnavnet
- Brug ikke WEP til virksomhedens netværk
  - men istedet en VPN løsning med individuel autentificering eller WPA
- NB: WPA Personal/PSK kræver passphrase på +40 tegn!

forkert

- Placer de trådløse adgangspunkter hensigtsmæssigt i netværket - så de kan overvåges
- Lav et sæt regler for brugen af trådløse netværk - hvor må medarbejdere bruge det?
- Se eventuelt pjecerne *Beskyt dit trådløse Netværk* fra Ministeriet for Videnskab, Teknologi og Udvikling
  `http://www.videnskabsministeriet.dk/`

Hjemmenetværk for nørder

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 WPA og overvej at lave en decideret DMZ til WLAN

Placer AP hensigtsmæddigt og gerne højt, oppe på et skab eller lignende