

Welcome to

# Penetration testing III Wireless sikkerhed

Henrik Lund Kramshøj, internet samurai  
hlk@solido.net

<http://www.solidonetworks.com>



## Don't Panic!

At vise de sikkerhedsmæssige aspekter af trådløse netværk

At inspirere jer til at implementere trådløse netværk sikkert

At fortælle jer om nogle af mulighederne for sikring af de trådløse netværk



KI 17-21

Mindre foredrag mere snak

Mindre enetale, mere foredrag 2.0 med socialt medie, informationsdeling og interaktion

## Det korte svar - drop diskussionen

Det havde oprindeligt en anden betydning, men medierne har taget udtrykket til sig - og idag har det begge betydninger.

**Idag er en hacker stadig en der bryder ind i systemer!**

ref. Spafford, Cheswick, Garfinkel, Stoll, ... - alle kendte navne indenfor sikkerhed

Hvis man vil vide mere kan man starte med:

- *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Clifford Stoll
- *Hackers: Heroes of the Computer Revolution*, Steven Levy
- *Practical Unix and Internet Security*, Simson Garfinkel, Gene Spafford, Alan Schwartz

Eric Raymond, der vedligeholder en ordbog over computer-slang (The Jargon File) har blandt andet følgende forklaringer på ordet hacker:

- En person, der nyder at undersøge detaljer i programmerbare systemer og hvordan man udvider deres anvendelsesmuligheder i modsætning til de fleste brugere, der bare lærer det mest nødvendige
- En som programmerer lidenskabeligt (eller enddog fanatisk) eller en der foretrækker at programmere fremfor at teoretiserer om det
- En ekspert i et bestemt program eller en der ofte arbejder med eller på det; som i "en Unixhacker".

Kilde: Peter Makhholm, <http://hacking.dk>

Benyttes stadig i visse sammenhænge se <http://labitat.dk>

**Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling.**

Hacking kan betyde:

- At man skal betale erstatning til personer eller virksomheder
- At man får konfiskeret sit udstyr af politiet
- At man, hvis man er over 15 år og bliver dømt for hacking, kan få en bøde - eller fængselsstraf i alvorlige tilfælde
- At man, hvis man er over 15 år og bliver dømt for hacking, får en plettet straffeattest. Det kan give problemer, hvis man skal finde et job eller hvis man skal rejse til visse lande, fx USA og Australien
- Frit efter: <http://www.stophacking.dk> lavet af Det Kriminalpræventive Råd
- Frygten for terror har forstærket ovenstående - så lad være!

## wireless 802.11



Wireless er lækkert

Wireless er nemt

Wireless er praktisk

Alle nye bærbare leveres med wireless kort

Jeg bruger selv næsten udelukkende wireless på min laptop

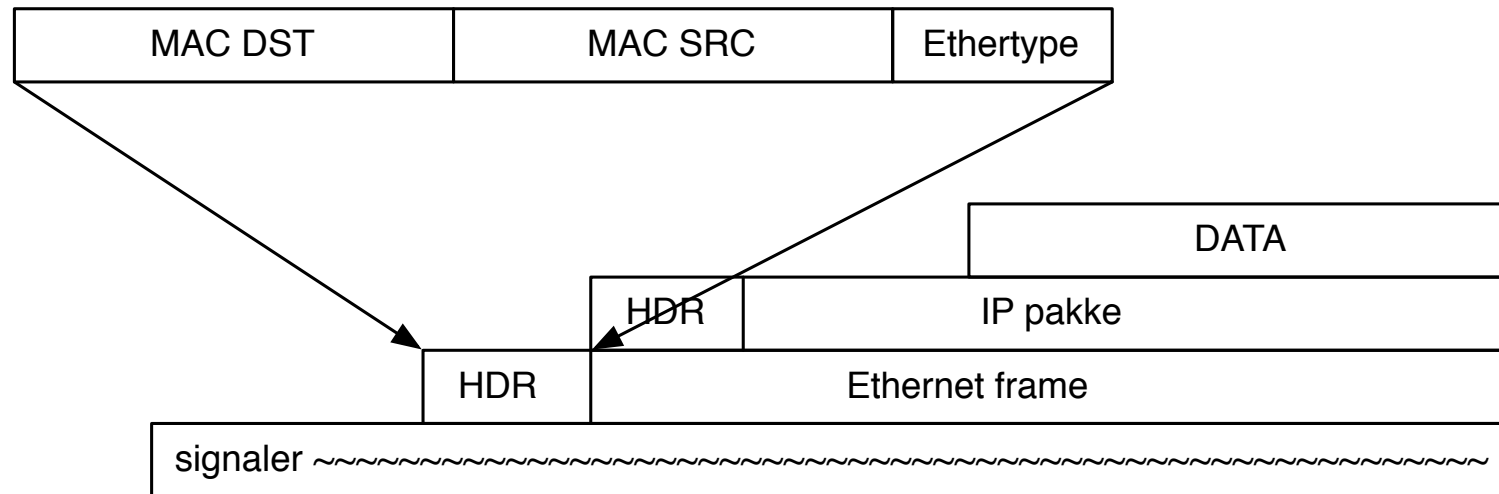


Hacking ligner indimellem magi





Hacking kræver blot lidt ninja-træning



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

Mange trådløse Access Points kan filtrere MAC adresser

Kun kort som er på listen over godkendte adresser tillades adgang til netværket ■

Det virker dog ikke ☺

De fleste netkort tillader at man overskriver denne adresse midlertidigt

Eksemplet med MAC filtrering er en af de mange myter

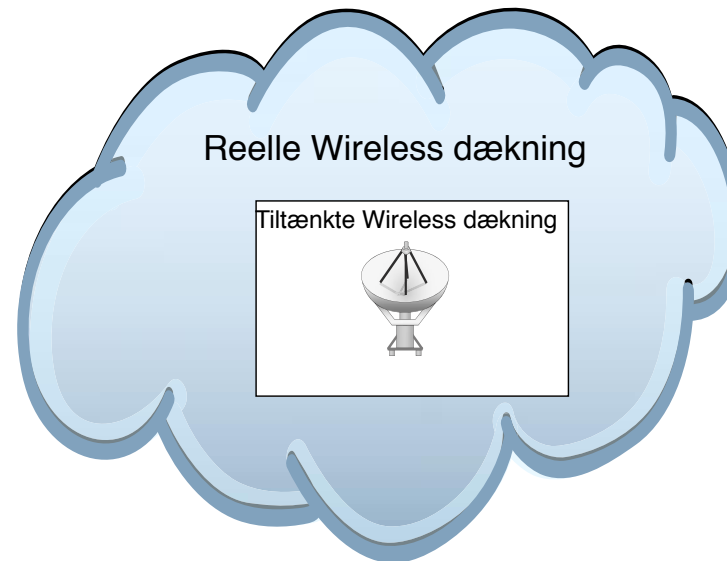
Hvorfor sker det?

- 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





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

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.

Kilde: [http://en.wikipedia.org/wiki/IEEE\\_802.11](http://en.wikipedia.org/wiki/IEEE_802.11)

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.

Kilde: [http://en.wikipedia.org/wiki/IEEE\\_802.11](http://en.wikipedia.org/wiki/IEEE_802.11)

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!

**Kilde:** [http://en.wikipedia.org/wiki/IEEE\\_802.11](http://en.wikipedia.org/wiki/IEEE_802.11)



Introduktion - begreber og teknologierne

Basal konfiguration af trådløst IEEE802.11 - wardriving

Hacking af trådløse netværk - portscanning, exploits

Sikkerhedsteknologier i 802.11b - WEP, forkortes, men stadig relevant

Sikkerhedsteknologier i 802.11i - WPA, WPA2

airodump og aircrack-ng

Packet injection med wireless værktøjer

Infrastrukturændringer, segmentering og firewall konfiguration

**Husk: trådløs sikkerhed er ikke kun kryptering**



Alle bruger nogenlunde de samme værktøjer, måske forskellige mærker

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

BackTrack <http://www.backtrack-linux.org/>

Laptop eller Netbook, typisk bruger jeg kort med Atheros chipset

**NB: de indbyggede er ofte ringe - så check før køb ;-)**

Access Points - jeg anbefaler Apple Airport

Bøger og Internet:

- *Metasploit The Penetration Tester's Guide* by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni <http://nostarch.com/metasploit>
- *Gray Hat Hacking: The Ethical Hacker's Handbook*, 3rd Edition, Shon Harris et al, Osborne
- *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses* (2nd Edition), Ed Skoudis, Prentice Hall PTR
- BackTrack <http://www.backtrack-linux.org/>
- Packetstorm wireless tools <http://packetstormsecurity.org/wireless/>
- *Beginner's Guide to Wireless Auditing* David Maynor  
<http://www.securityfocus.com/infocus/1877?ref=rss>

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/>
- Kismac <http://kismac-ng.org/>
- Aircrack-ng set of tools <http://www.aircrack-ng.org/>
- Bruteforge <http://masterzorag.blogspot.com/>
- Pyrit GPU cracker <http://code.google.com/p/pyrit/>
- OpenBSD operativsystem med fokus på sikkerhed <http://www.openbsd.org>

Tænk som en hacker

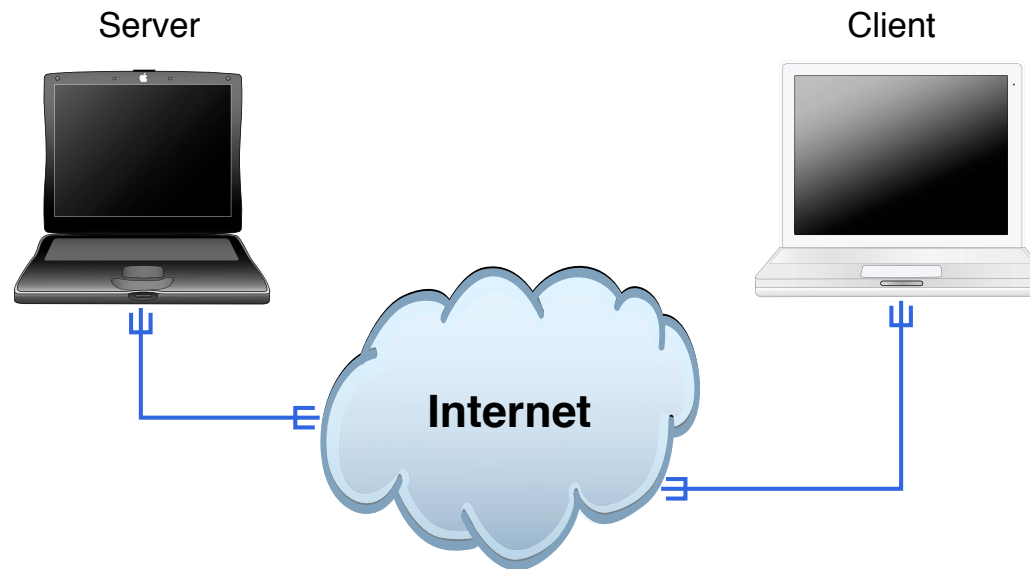
Rekognoscering

- ping sweep, port scan
- OS detection - TCP/IP eller banner grab
- Servicescan - rpcinfo, netbios, ...
- telnet/netcat interaktion med services

Udnyttelse/afprøvning: Nessus, nikto, exploit programs

Oprydning/hærdning vises måske ikke, men I bør i praksis:

**Vi går idag kun efter wireless**



Klienter og servere

Rødder i akademiske miljøer

Protokoller der er op til 20 år gamle

Meget lidt kryptering, mest på http til brug ved e-handel

OSI Reference  
Model

Application
Presentation
Session
Transport
Network
Link
Physical

Internet protocol suite

Applications  HTTP, SMTP, FTP, SNMP,	NFS
	XDR
	RPC
TCP UDP	
IPv4	IPv6 ICMPv6 ICMP
ARP RARP	
MAC	
Ethernet token-ring ATM ...	

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

**Kilder:** [http://en.wikipedia.org/wiki/IEEE\\_802.11](http://en.wikipedia.org/wiki/IEEE_802.11) <http://grouper.ieee.org/groups/802/11/index.html>



Access point kører typisk i *access point mode* også kaldet infrastructure mode - al trafik går via AP

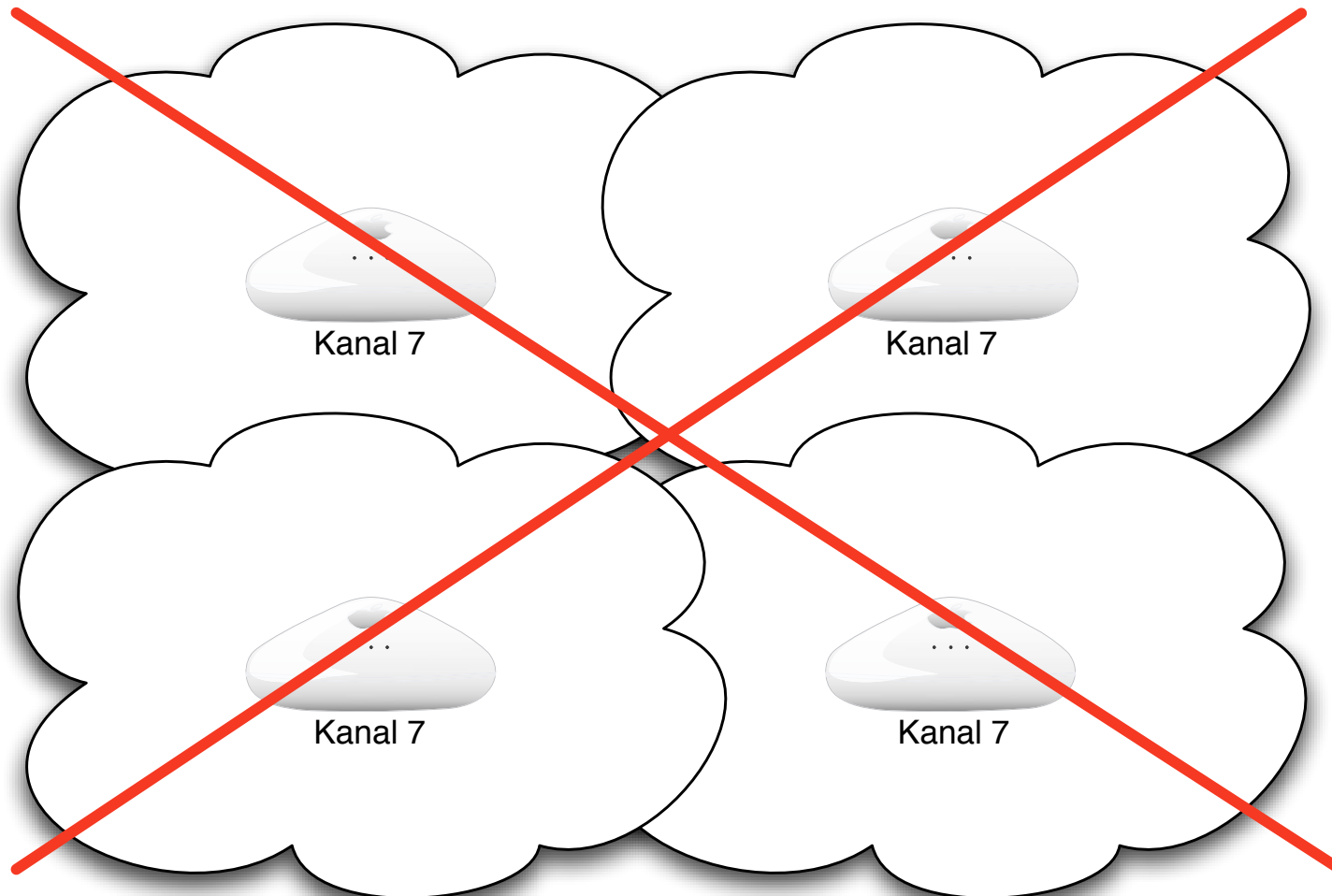
Alternativt kan wireless kort oprette ad-hoc netværk - hvor trafikken går direkte mellem netkort

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

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

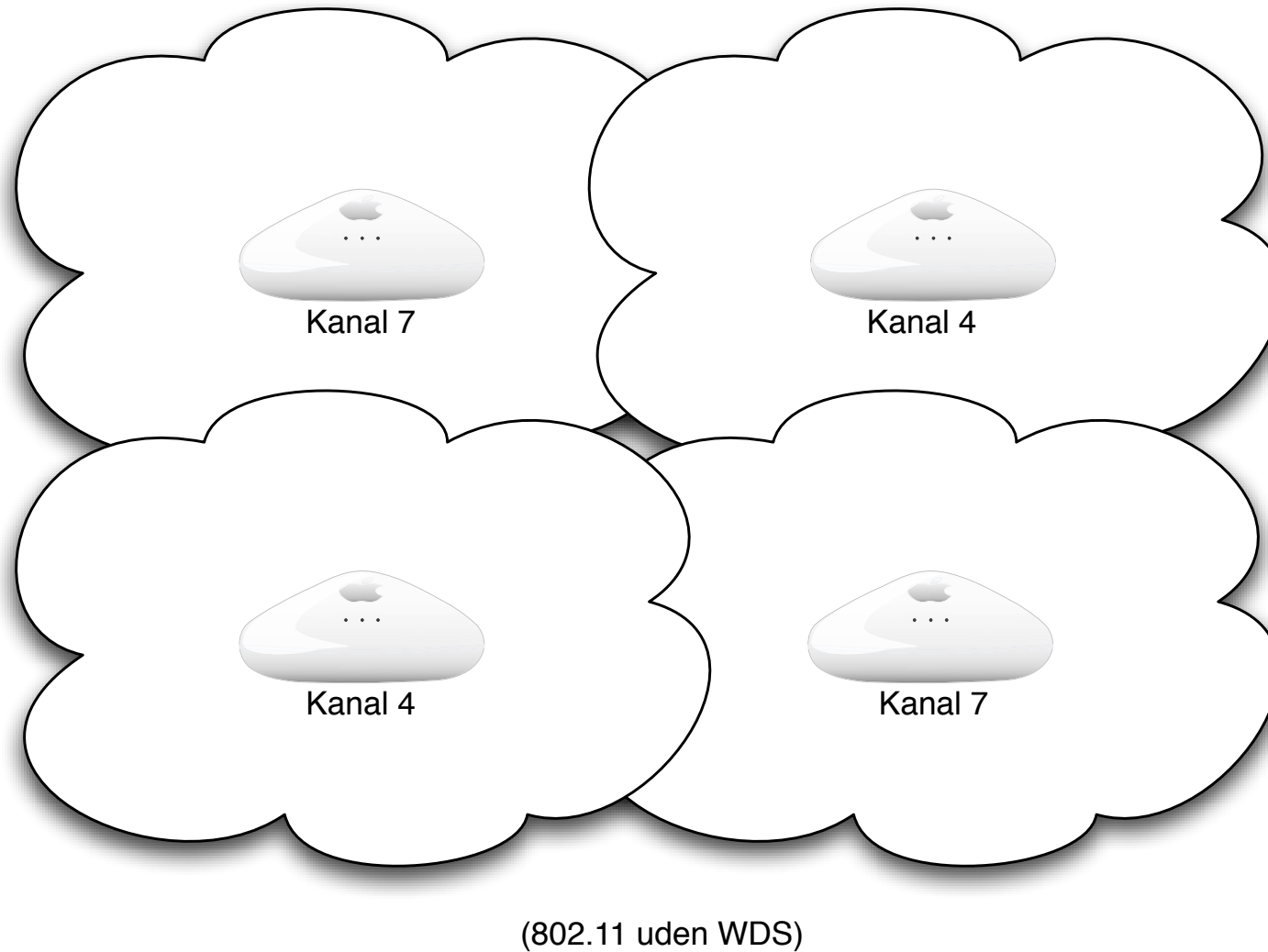
Helst 4 kanaler spring for 802.11g AP der placeres indenfor rækkevidde

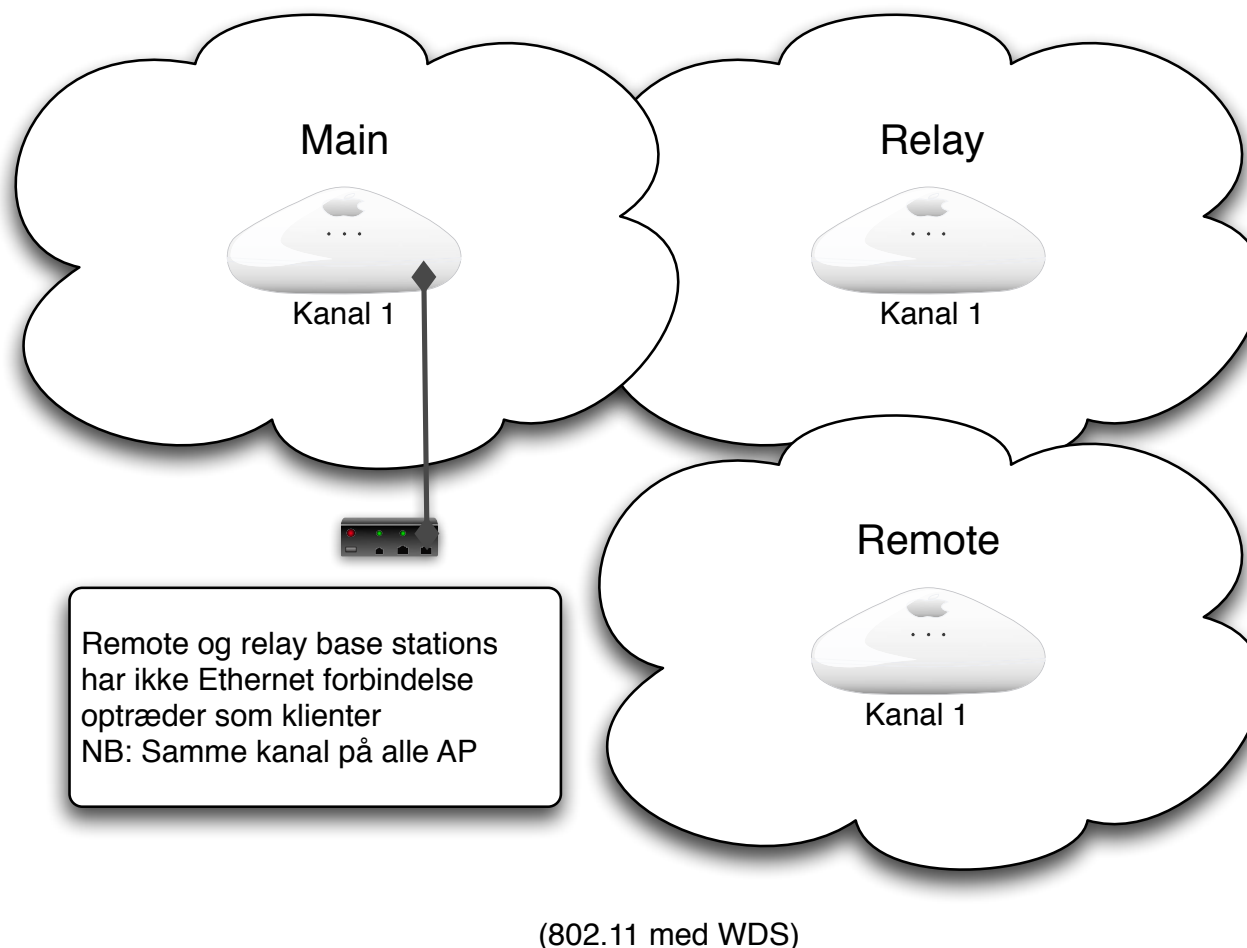
# Eksempel på netværk med flere AP'er



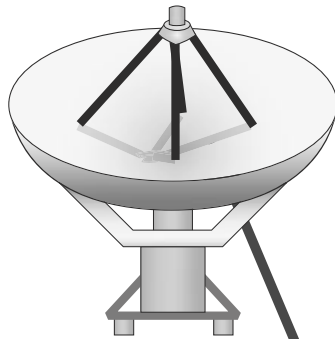
(802.11 uden WDS)

# Eksempel på netværk med flere AP'er

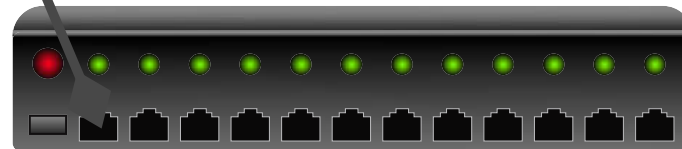




Se også: [http://en.wikipedia.org/wiki/Wireless\\_Distribution\\_System](http://en.wikipedia.org/wiki/Wireless_Distribution_System)



## Wireless Access Point



**netværket - typisk Ethernet**

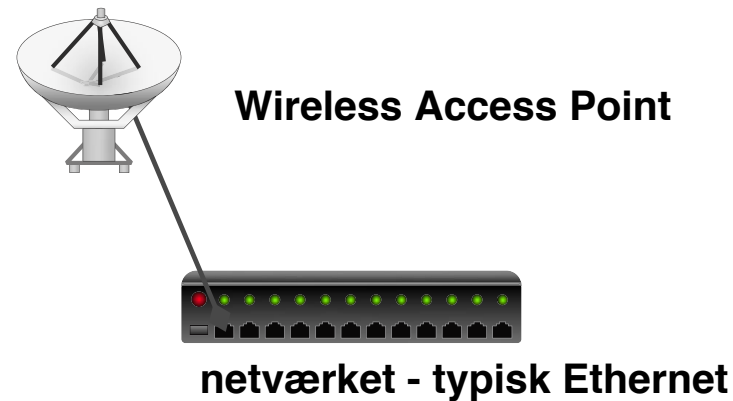
et access point - forbindes til netværket

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



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
- nøglen ændres sjældent, og det er svært at distribuere en ny

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



Service Set Identifier (SSID) - netnavnet

32 ASCII tegn eller 64 hexadecimale cifre

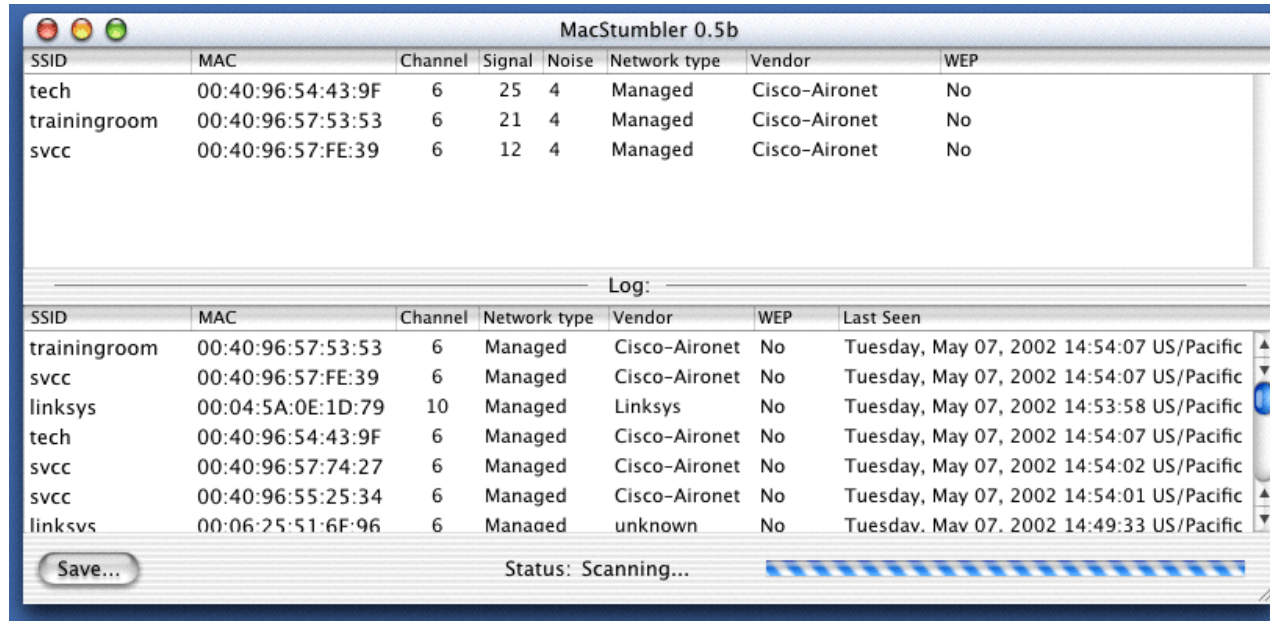
Udstyr leveres typisk med et standard netnavn

- 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



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

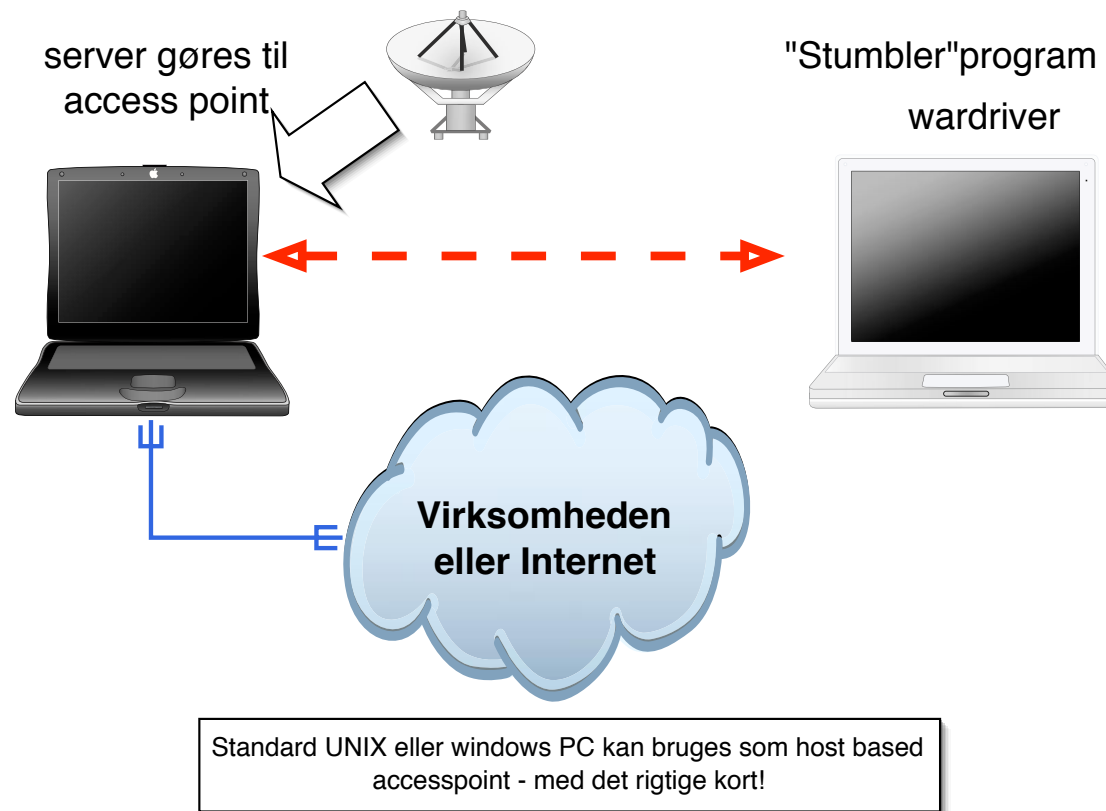
SSID	MAC	Channel	Network type	Vendor	WEP	Last Seen
trainingroom	00:40:96:57:53:53	6	Managed	Cisco-Aironet	No	Tuesday, May 07, 2002 14:54:07 US/Pacific
svcc	00:40:96:57:FE:39	6	Managed	Cisco-Aironet	No	Tuesday, May 07, 2002 14:54:07 US/Pacific
linksys	00:04:5A:0E:1D:79	10	Managed	Linksys	No	Tuesday, May 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	Tuesdav. May 07, 2002 14:49:33 US/Pacific

Save... Status: Scanning...

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/>
- Kismet ... mange andre

# Start på demo - wardriving



- Almindelige laptops bruges til demo
- Der startes et *access point*

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?

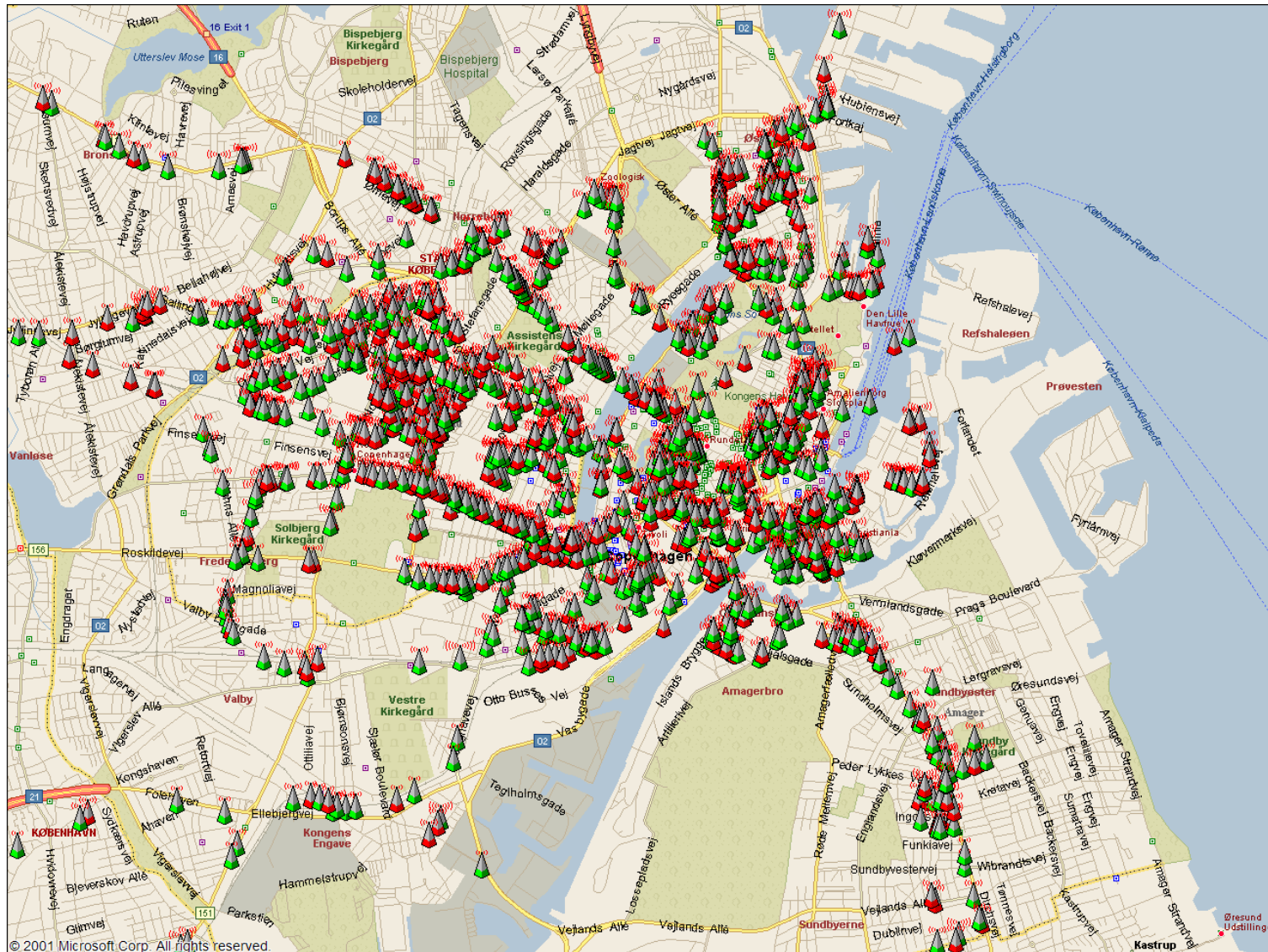
MAC adressen kan derfor overtages, når en af de tilladte stationer forlader området ...

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.



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

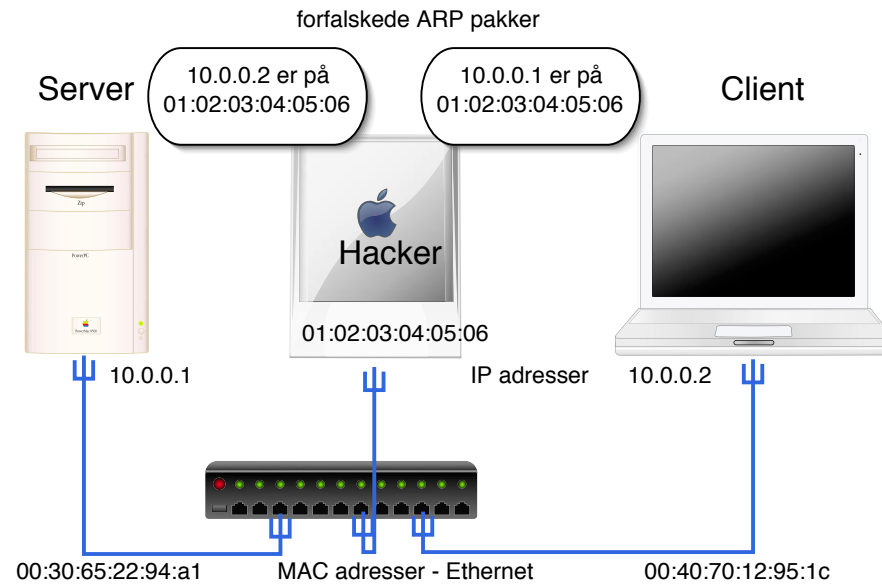
en sniffer til mange usikre protokoller

inkluderer **arpspoof**

Lavet af Dug Song, [dugsong@monkey.org](mailto:dugsong@monkey.org)

dsniff is a password sniffer which handles FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL\*Net, Sybase and Microsoft SQL protocols.

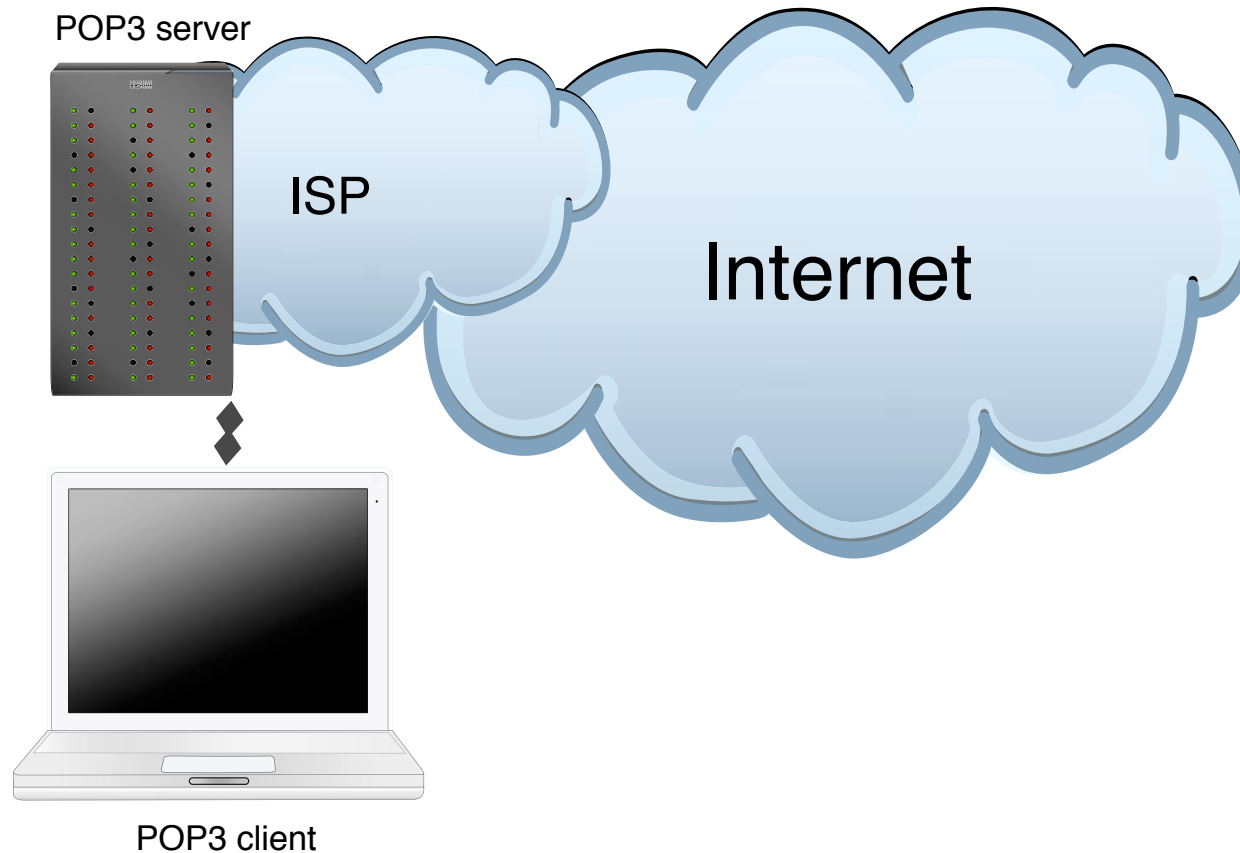




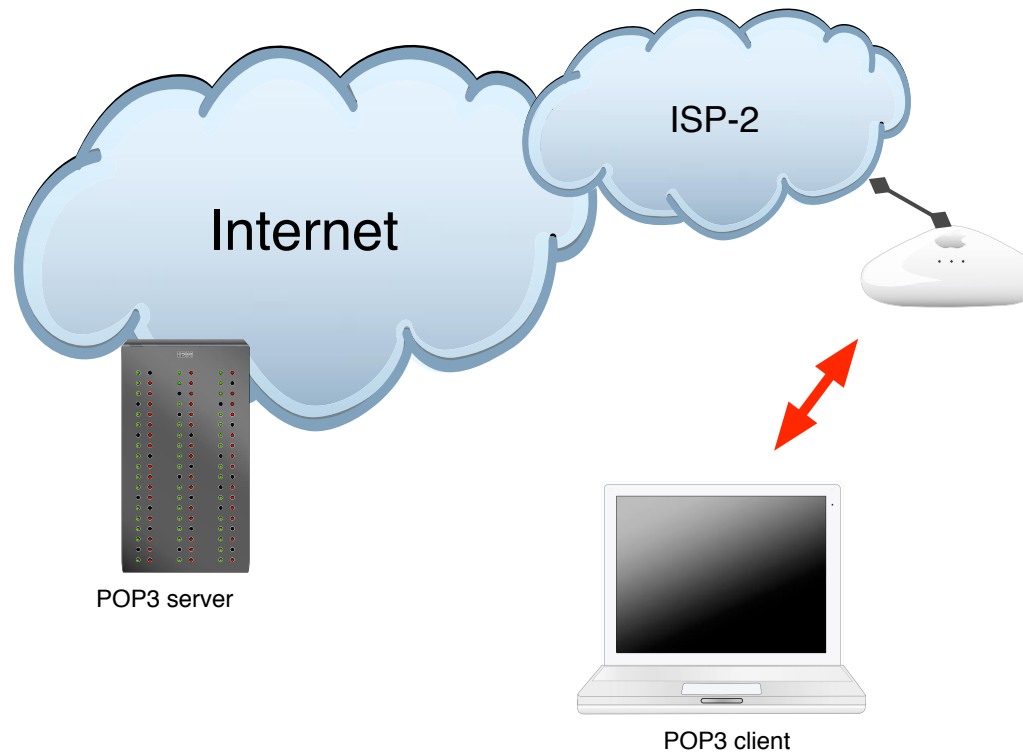
Aflæsning af hemmeligheder - kodeord m.v.

Hvilke forudsætninger er der for at bruge Dsniff?

dsniff skal have adgang til trafikken ...

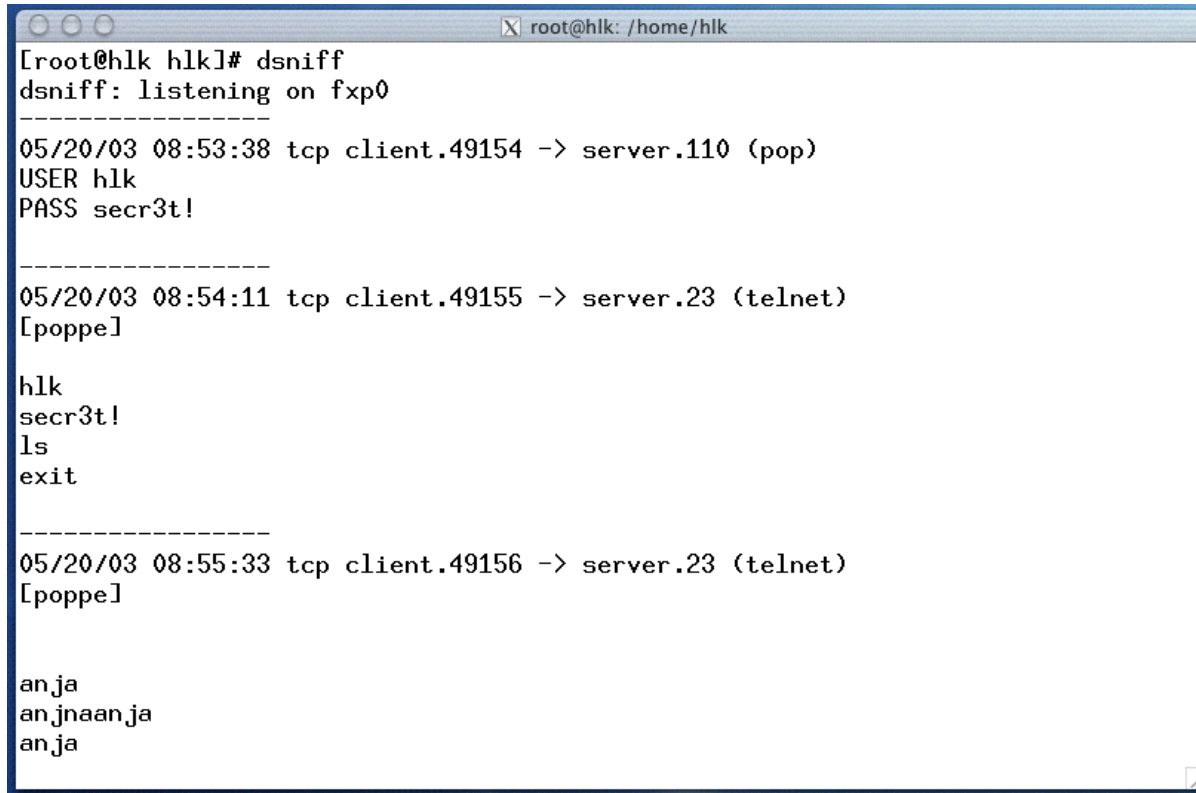


Man har tillid til sin ISP - der administrerer såvel net som server



Har man tillid til andre ISP'er? Alle ISP'er?

Deler man et netværksmedium med andre?



```
root@hlk: /home/hlk
[root@hlk hlk]# dsniff
dsniff: listening on fxp0
-----
05/20/03 08:53:38 tcp client.49154 -> server.110 (pop)
USER hlk
PASS secr3t!
-----
05/20/03 08:54:11 tcp client.49155 -> server.23 (telnet)
[poppe]

hlk
secr3t!
ls
exit
-----
05/20/03 08:55:33 tcp client.49156 -> server.23 (telnet)
[poppe]

an ja
an jnaan ja
an ja
```

Dsniff screenshot, vi viser måske Ethereal

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

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 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?

Kryptografi er læren om, hvordan man kan kryptere data

Kryptografi benytter algoritmer som sammen med nøgler giver en ciffertekst - der kun kan læses ved hjælp af den tilhørende nøgle

privat-nøgle kryptografi (eksempelvis AES) benyttes den samme nøgle til kryptering og dekryptering

offentlig-nøgle kryptografi (eksempelvis RSA) benytter to separate nøgler til kryptering og dekryptering



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>

## AES

Advanced Encryption Standard

DES kryptering baseret på den IBM udviklede Lucifer algoritme har været benyttet gennem mange år.

Der er vedtaget en ny standard algoritme Advanced Encryption Standard (AES) som afløser Data Encryption Standard (DES)

Algoritmen hedder Rijndael og er udviklet af Joan Daemen og Vincent Rijmen.

Kilde: <http://csrc.nist.gov/encryption/aes/>  
<http://www.esat.kuleuven.ac.be/~rijmen/rijndael/>

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet

## Kryptering af e-mail

- Pretty Good Privacy - Phil Zimmermann
- PGP = mail sikkerhed

## Kryptering af sessioner SSL/TLS

- Secure Sockets Layer SSL / Transport Layer Services TLS
- krypterer data der sendes mellem webservere og klienter
- SSL kan bruges generelt til mange typer sessioner, eksempelvis POP3S, IMAPS, SSH m.fl.

Sender I kreditkortnummeret til en webserver der kører uden https?



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 implementations of this attack. <http://airsnort.shmoo.com/>

weak keying - 24 bit er allerede kendt - 128-bit = 104 bit i praksis

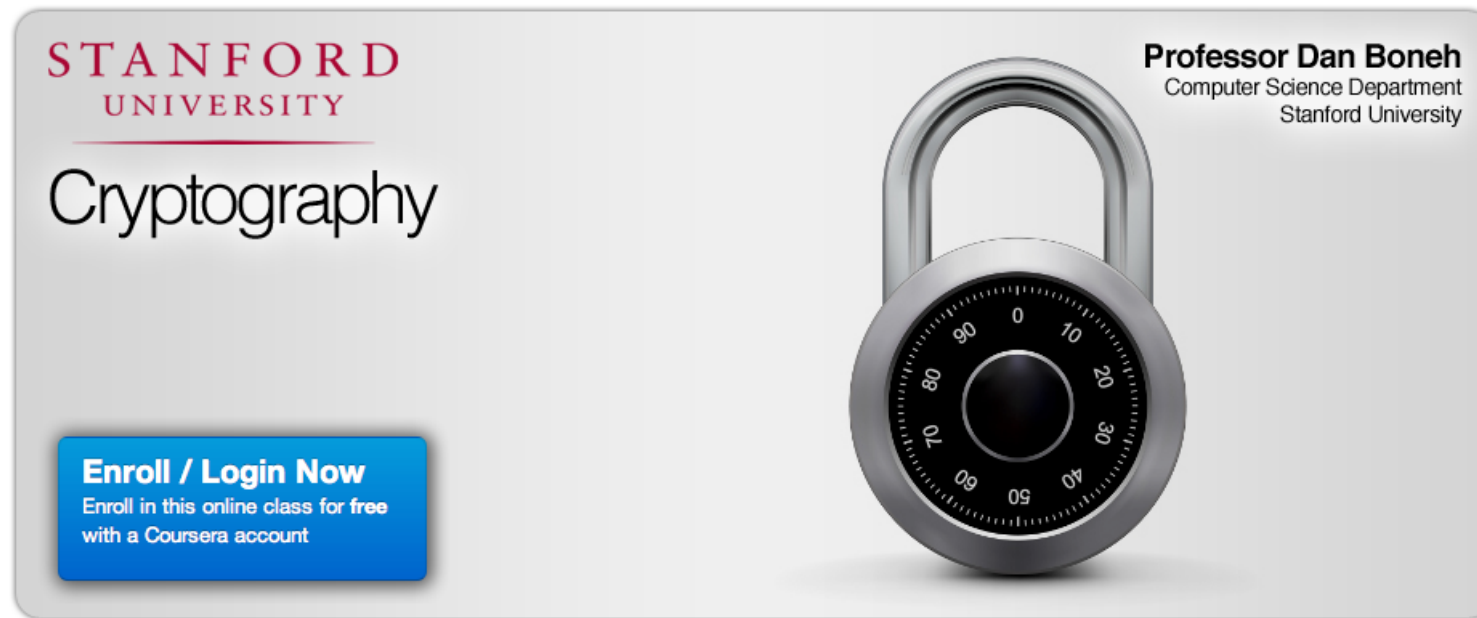
small IV - med kun 24 bit vil hver IV blive genbrugt oftere

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

Kilde: *Secure Coding: Principles and Practices*, Mark G. Graff og Kenneth R. van Wyk, O'Reilly, 2003

# Konklusion: Kryptografi er svært



Åbent kursus på Stanford er startet Marts 2012, slut ca. Maj  
<http://crypto-class.org/>



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. 500.000 er godt, og ofte kan der knækkes med lang færre

Links:

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

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



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	<b>801963</b>	<b>540180</b>	wanlan

NB: dataopsamlingen er foretaget på 100% opdateret Mac udstyr

```
$ 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 ]**

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
```

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 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

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](http://www.wifialliance.org/OpenSection/protected_access.asp)

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

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



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!

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**

```
[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 lengths & hacking feasibility**

<i>Type of Attacker</i>	<i>Budget</i>	<i>Tool</i>	<i>Time &amp; Cost/Key 40 bit</i>	<i>Time &amp; 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 <sup>1</sup>	12 min. (\$.08)	556 days (\$5,000)
Corporate Department	\$300,000	FPGA  ASIC <sup>2</sup>	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)

Kilde: [http://www.mycrypto.net/encryption/encryption\\_crack.html](http://www.mycrypto.net/encryption/encryption_crack.html)

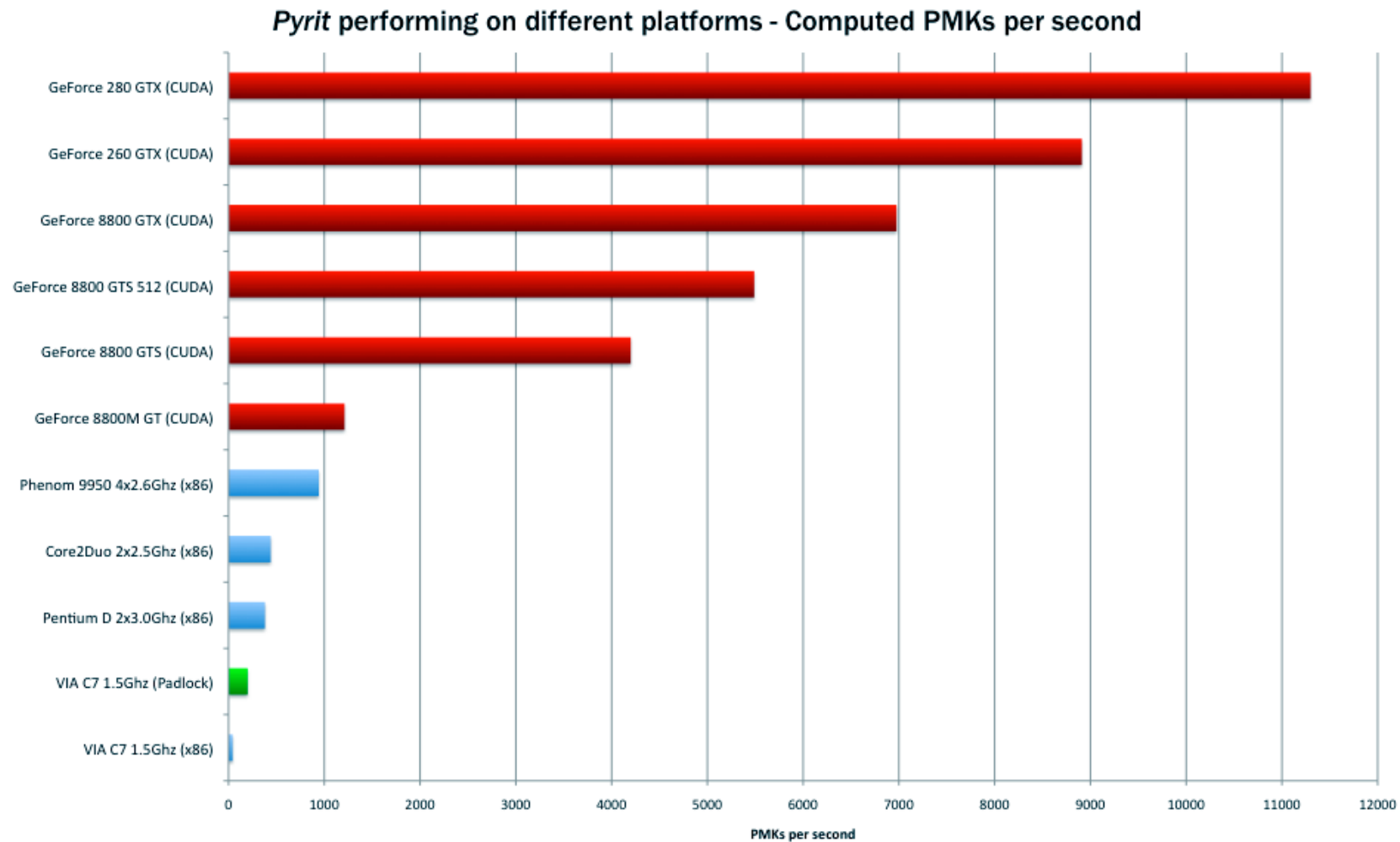
*Pyrit* takes a step ahead in attacking WPA-PSK and WPA2-PSK, the protocol that today de-facto protects public WIFI-airspace. The project's goal is to estimate the real-world security provided by these protocols. Pyrit does not provide binary files or wordlists and does not encourage anyone to participate 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 - ca 150 keys/s på min Thinkpad X31

Kryptering afhænger af SSID!.

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



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

How Reaver Works Now that you've seen how to use Reaver, let's take a quick overview of how Reaver works. The tool takes advantage of a vulnerability in something called Wi-Fi Protected Setup, or WPS. It's a feature that exists on many routers, intended to provide an easy setup process, and it's tied to a PIN that's hard-coded into the device. Reaver exploits a flaw in these PINs; the result is that, with enough time, it can reveal your WPA or WPA2 password.

Hvad betyder ease of use?

Kilde: nice tutorial med BackTrack - husk Reaver er med på BT5 idag

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



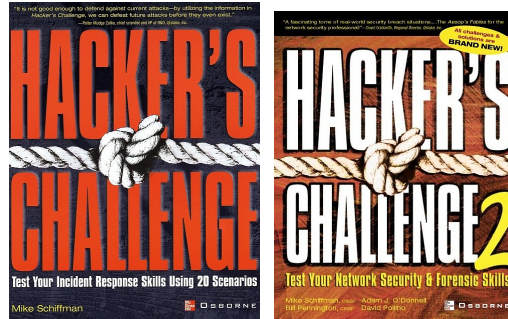
De fleste trådløse enheder leveres med en standard konfiguration som er helt åben!

det første man kan gøre er at slå noget kryptering til

Brug ikke WEP men *noget andet* - WPA, Cisco LEAP, VPN, IPsec, ...

Derudover kan en del access points filtrere på MAC adresser glem det

på visse AP er der mulighed for opslag på RADIUS servere - Remote Authentication Dial In User Service (RADIUS)



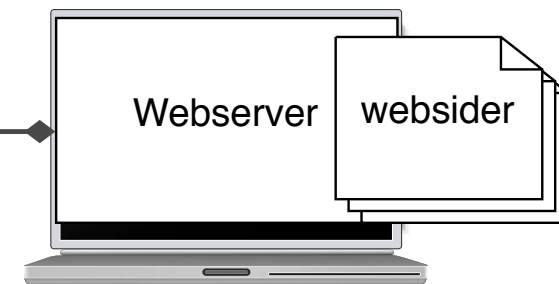
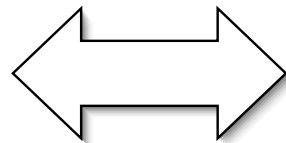
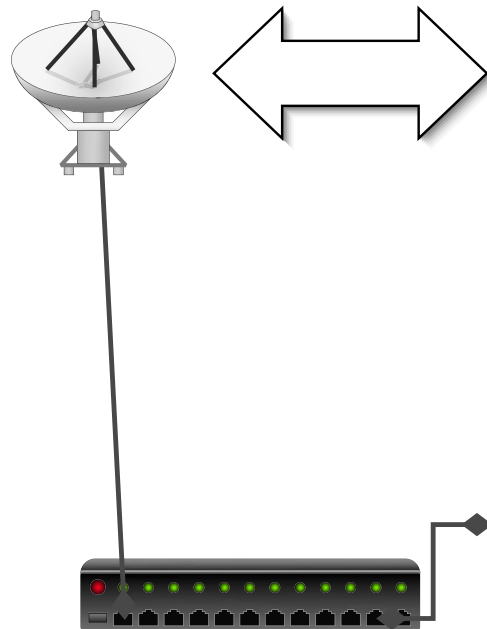
## Hackers Challenge 2 - disassociate attack

OpenBSD program - fremprovokere trafik så der kan knækkes WEP findes på Packetstorm med navnet wnet.tgz lavet til OpenBSD 3.2

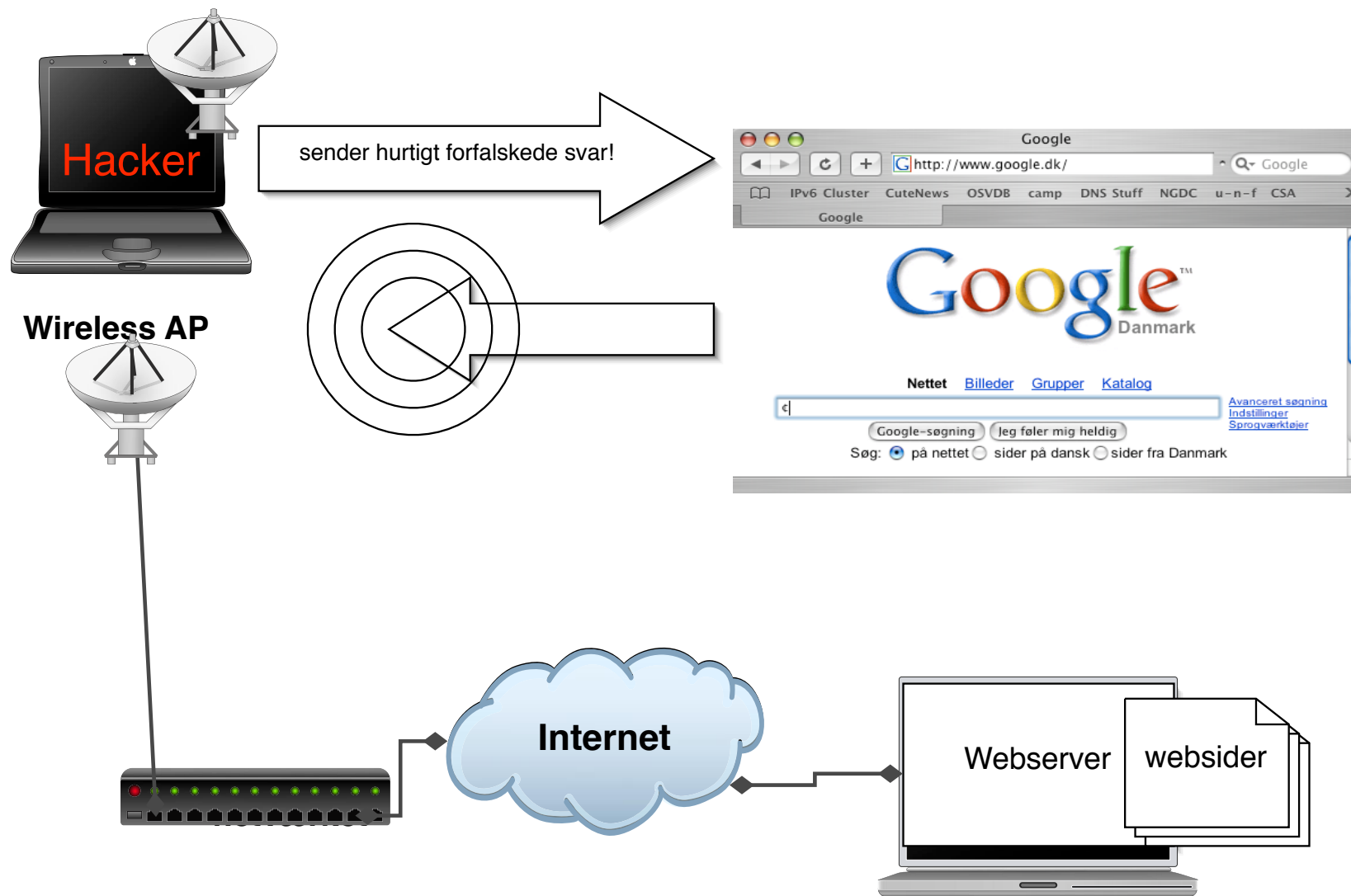
*Hacker's Challenge : Test Your Incident Response Skills Using 20 Scenarios af Mike Schiffman*

*Hacker's Challenge II : Test Your Network Security and Forensics Skills af Mike Schiffman*

**Wireless AP**



# 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

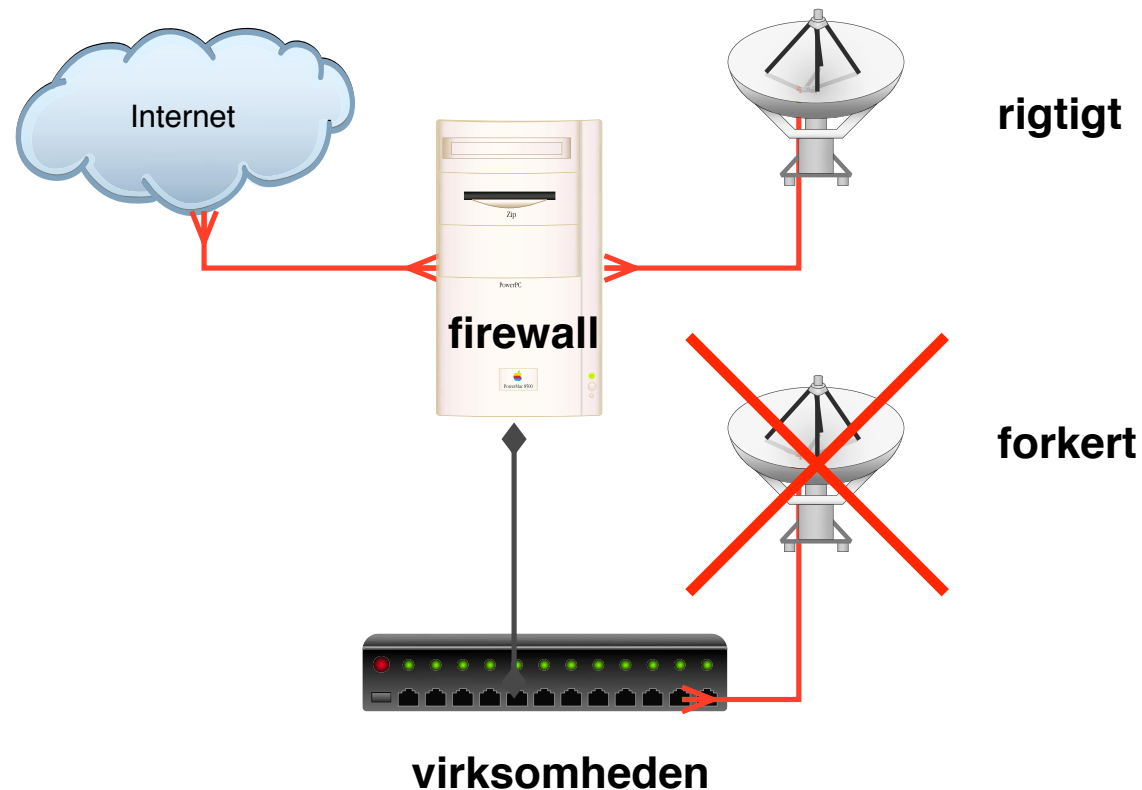
<http://airpwn.sourceforge.net/>

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

Så går man igang med de almindelige værktøjer

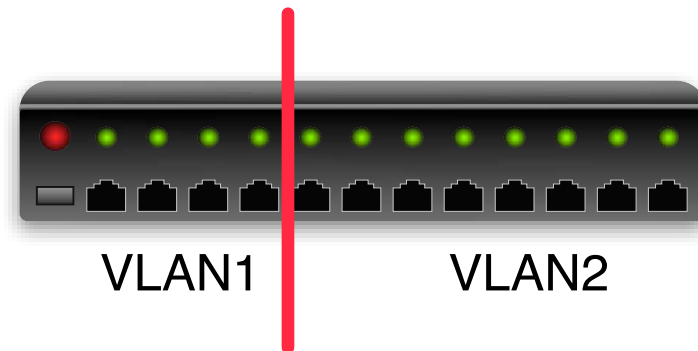
SecTools.Org: Top 125 Network Security Tools <http://www.sectools.org>

**Forsvaret er som altid - flere lag af sikkerhed!**



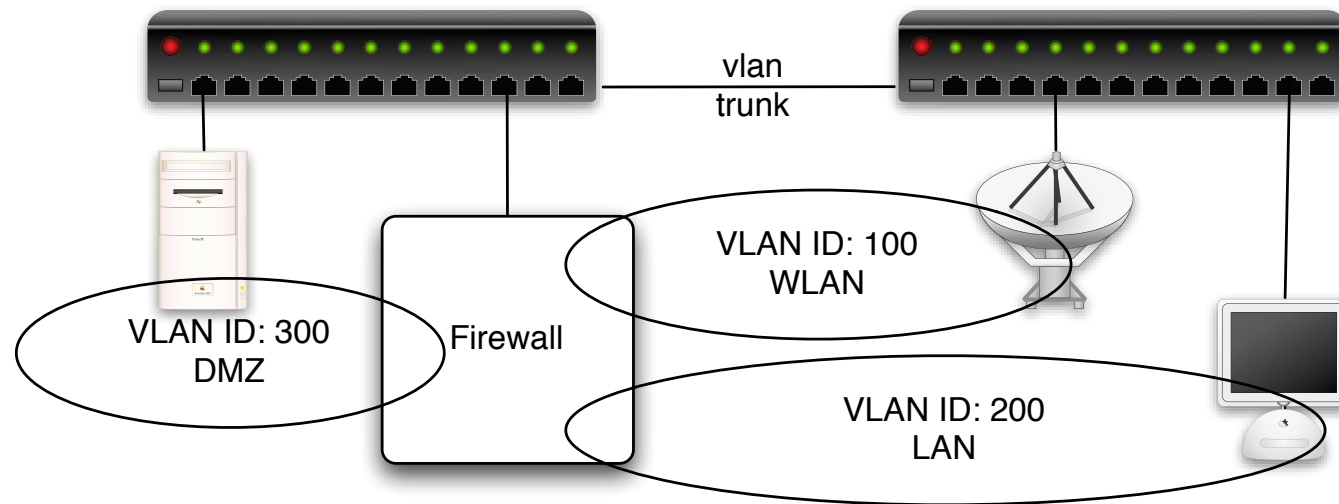
Sådan bør et access point forbindes til netværket

## Portbased VLAN

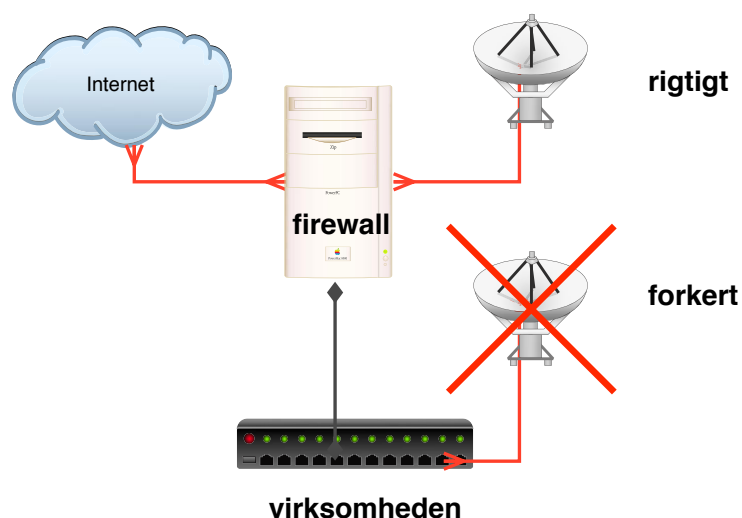


- Nogle switche tillader at man opdeler portene
- Denne opdeling kaldes VLAN og portbaseret er det mest simple
- Port 1-4 er et LAN
- De resterende er et andet LAN
- Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2





- Nogle switche tillader at man opdeler portene, men tillige benytter 802.1q
- Med 802.1q tillades VLAN tagging på Ethernet niveau
- Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2
- VLAN trunking giver mulighed for at dele VLANs ud på flere switches
- Der findes administrationsværktøjer der letter dette arbejde: OpenNAC FreeNAC, Cisco VMPS



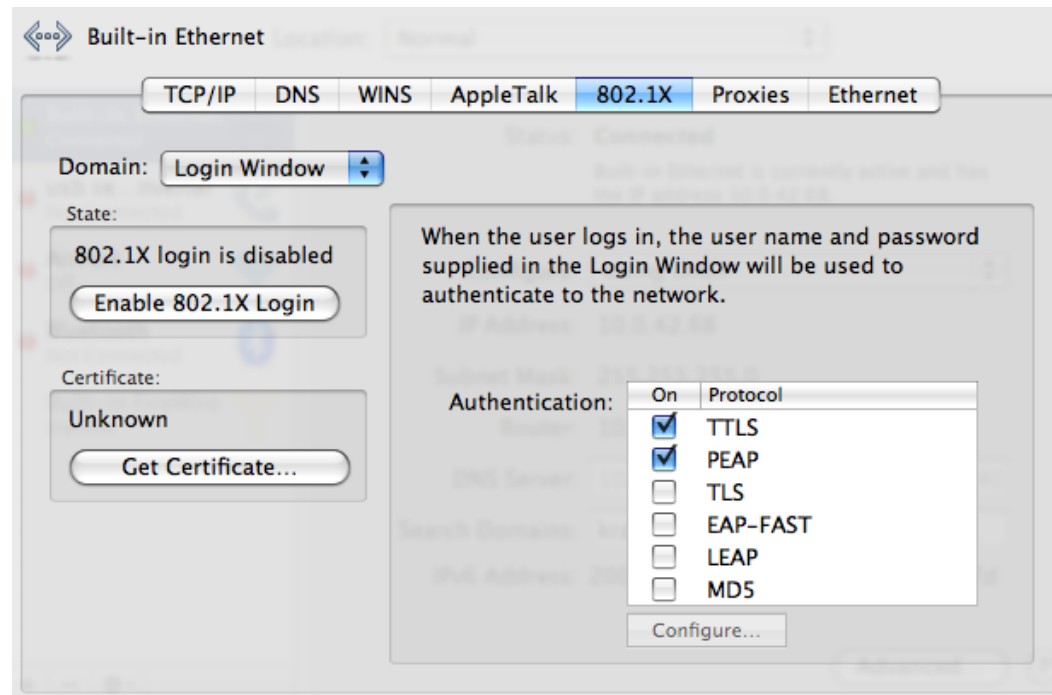
- Brug noget tilfældigt som SSID - netnavnet
- Brug ikke WEP til virksomhedens netværk  
- men istedet en VPN løsning med individuel autentificering eller WPA
- NB: WPA Personal/PSK kræver passphrase på mange tegn! +40?
- Placer de trådløse adgangspunkter hensigtsmæssigt i netværket - så de kan overvåges
- 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/>

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



- 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 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

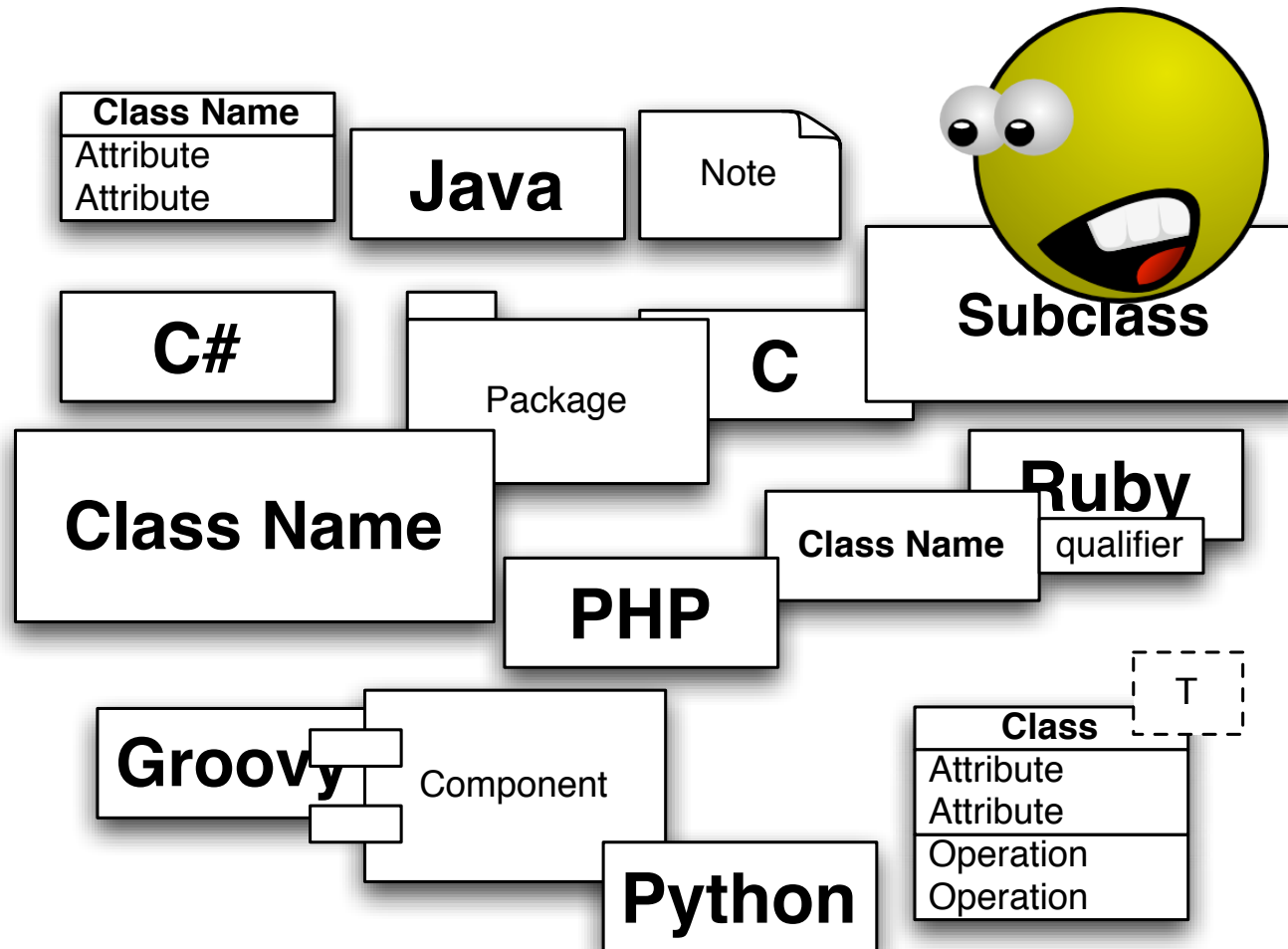
når vi scanner efter services går det nemt med at finde dem

Giv jer selv mere tid til at omkonfigurere og opdatere ved at undgå standardindstillinger

Tiden der går fra en sårbarhed annonceres til den bliver udnyttet er meget kort idag!

Ved at undgå standard indstillinger kan der måske opnås en lidt længere frist - inden ormene kommer

NB: ingen garanti - og det hjælper sjældent mod en dedikeret angriber



Wireless AP implementerer protokoller med hardware+software

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?



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 forretningskritiske LAN segmenter!

# Hvordan finder man buffer overflow, og andre fejl

Black box testing

Closed source reverse engineering

White box testing

Open source betyder man kan læse og analysere koden

Source code review - automatisk eller manuelt

Fejl kan findes ved at prøve sig frem - fuzzing

Exploits virker typisk mod specifikke versioner af software

Bemærk: alle angreb har forudsætninger for at virke

Et angreb mod Telnet virker kun hvis du bruger Telnet

Et angreb mod Apache HTTPD virker ikke mod Microsoft IIS

Kan du bryde kæden af forudsætninger har du vundet!

**Et buffer overflow** er det der sker når man skriver flere data end der er afsat plads til i en buffer, et dataområde. Typisk vil programmet gå ned, men i visse tilfælde kan en angriber overskrive returadresser for funktionskald og overtage kontrollen.

**Stack protection** er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.

# Wireless buffer overflows beware of the BLOB



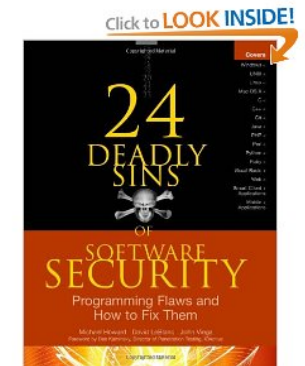
exploit/exploitprogram programmer rettet mod drivere

# 24 Deadly Sins of Software Security

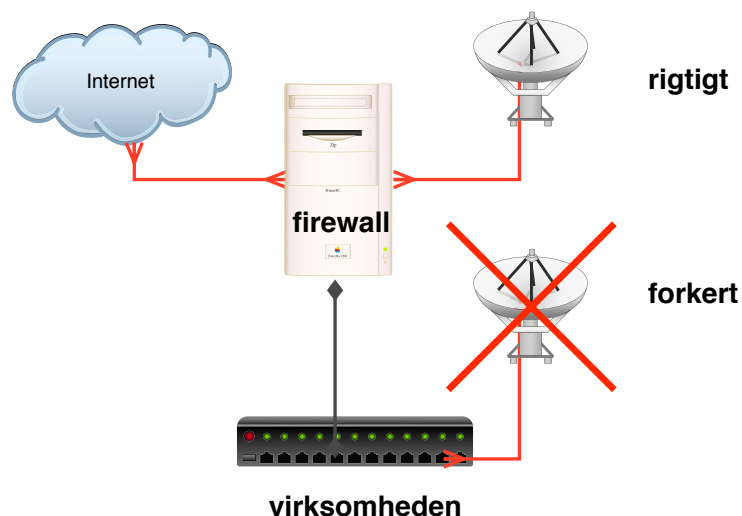
*24 Deadly Sins of Software Security* af Michael Howard, David Leblanc, John Viega 2009

## Obligatorisk læsning for alle udviklere

Denne bog er præcis og giver overblik på kun 432 sider



Buffer Overruns, Format String Problems, Integer Overflows, SQL Injection, Command Injection, Failing to Handle Errors, Cross-Site Scripting, Failing to Protect Network Traffic, Magic URLs Hidden Form Fields, Improper Use of SSL and TLS, Weak Password-Based Systems, Failing to Store and Protect Data Securely, Information Leakage, Improper File Access, Trusting Network Name Resolution, Race Conditions, Unauthenticated Key Exchange, Cryptographically Strong Random Numbers, Poor Usability



- 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!
- 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/>

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 hensigtsmæssigt og gerne højt, oppe på et skab eller lignende



Brug alt hvad I kan overkomme:

- Firewalls: IPfilter, IPtables, OpenBSD PF
- Kryptografi
- Secure Shell - SSH
- betragt Telnet, Rlogin, Rsh, Rexec som døde!
- FTP bør kun bruges til anonym FTP
- Intrusion Detection - Snort
- Sudo
- Tripwire, mtree, MD5

Sikkerhedspolitikken er din "plan" for sikkerheden - og er med til at sikre niveauet er ens

Firewalls hjælper ikke mod alle trusler

Husk følgende:

- Husk: IT-sikkerhed er ikke kun netværkssikkerhed!
  - Sikkerhed kommer fra langsigtede initiativer
- Vi håber I kan genkende de problemer vi har talt om, og finde information om nye problemer i netværk som bliver kendt**
- eksempelvis nye metoder til scanning eller omgåelse af firewalls**
- Hvad er informationssikkerhed?
  - Data på elektronisk form
  - Data på fysisk form
  - Social engineering er måske overset - *The Art of Deception: Controlling the Human Element of Security* af Kevin D. Mitnick, William L. Simon, Steve Wozniak

Computer Forensics er reaktion på en hændelse

**Informationssikkerhed er en proces**

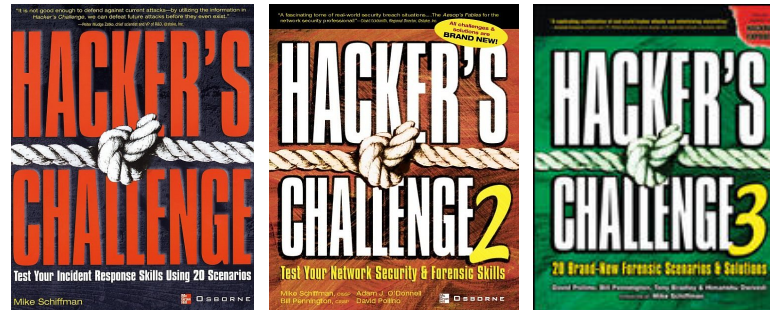
Henrik Lund Kramshøj, internet samurai  
hlk@solido.net

`http://www.solidonetworks.com`

You are always welcome to send me questions later via email

Følgende kurser afholdes med mig som underviser

- IPv6 workshop - 1 dag  
Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk.
- Wireless teknologier og sikkerhed workshop - 1-2 dage  
En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk, samt integration med hjemmepc og virksomhedsnetværk.
- Hacker workshop 2 dage  
Workshop med detaljeret gennemgang af hackermetoderne angreb over netværk, exploitprogrammer, portscanning, Nessus m.fl.
- Forensics workshop 2 dage  
Med fokus på tilgængelige open source værktøjer gennemgås metoder og praksis af undersøgelse af diskimages og spor på computer systemer
- Moderne Firewalls og Internetsikkerhed 2 dage  
Informere om trusler og aktivitet på Internet, samt give et bud på hvorledes en avanceret moderne firewall idag kunne konfigureres.



*Hacker's Challenge : Test Your Incident Response Skills Using 20 Scenarios* af Mike Schiffman McGraw-Hill Osborne Media; (October 18, 2001) ISBN: 0072193840

*Hacker's Challenge II : Test Your Network Security and Forensics Skills* af Mike Schiffman McGraw-Hill Osborne Media, 2003 ISBN: 0072226307

Bøgerne indeholder scenarier i første halvdel, og løsninger i anden halvdel - med fokus på relevante logfiler og sårbarheder