Welcome to

3. Network spoofing and Cracking Passwords

KEA Kompetence Penetration Testing

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github

3-network-spoofing-password-cracking.tex in the repo security-courses

Plan for today

Subjects

- Network spoofing and Cracking Passwords
- Some sniffing, some wireless
- ARP spoofing, ICMP redirects, the classics
- Person in the middle attacks
- Brute force attacks
- Powershell - we really should, but sorry. Home exercise

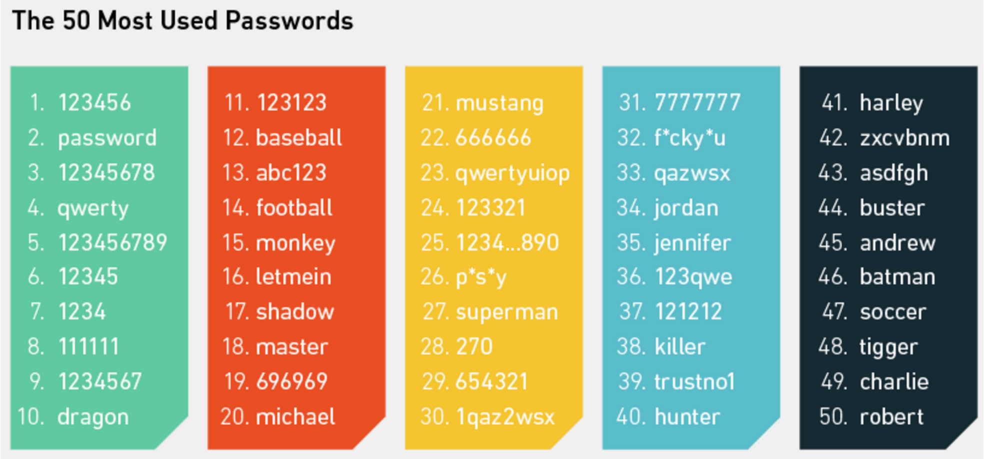
Exercises

- ARP spoofing and ettercap
- EtherApe
- Pcap-diff

Reading Curriculum:

- Grayhat chapters 10,15

Goals for today: Non-exploit methods

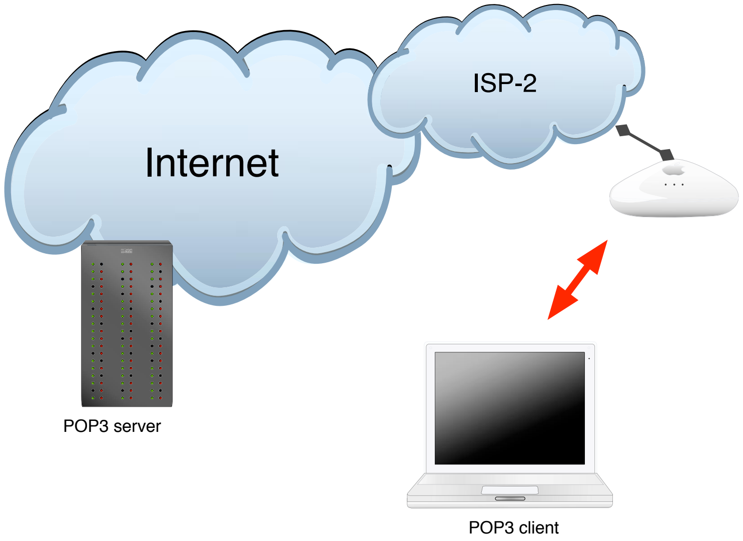


The 50 Most Used Passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 111111
9. 1234567
10. dragon
11. 123123
12. baseball
13. abc123
14. football
15. monkey
16. letmein
17. shadow
18. master
19. 696969
20. michael
21. mustang
22. 666666
23. qwertyuiop
24. 123321
25. 1234...890
26. p*s*y
27. superman
28. 270
29. 654321
30. 1qaz2wsx
31. 7777777
32. f*cky*u
33. qazwsx
34. jordan
35. jennifer
36. 123qwe
37. 121212
38. killer
39. trustno1
40. hunter
41. harley
42. zxcvbnm
43. asdfgh
44. buster
45. andrew
46. batman
47. soccer
48. tigger
49. charlie
50. robert

- Getting shells without exploits - Living of the land - use existing features and programs
- Badly configured systems exist
- Using passwords like admin/admin or SNMP with community string public or private

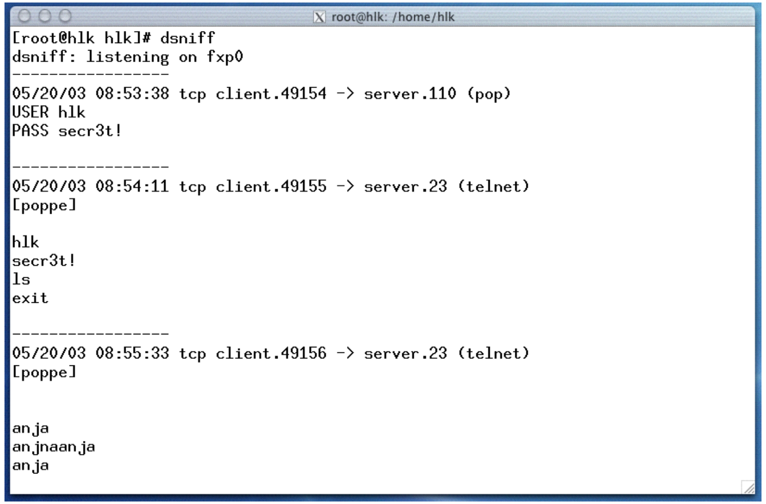
POP3 - trådløst



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

Deler man et netværksmedium med andre?

POP3 netværk



```
[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]


anja
anjnaanja
anja
```

Dsniff screenshot, vi viser måske tilsvarende i Wireshark

Dsniff er et godt demo program til arpspoofing mv., Ettercap er mere moderne

Person in the middle attacks

ARP spoofing, ICMP redirects, the classics

Used to be called Man in The Middle MiTM

- ICMP redirect
- ARP spoofing
- Wireless listening and spoofing higher levels like airpwn-ng `https://github.com/ICSec/airpwn-ng`

Usually aimed at unencrypted protocols

Today we only talk about getting the data, not how to perform higher level attacks

ICMP redirect

Routere understøtter ofte ICMP Redirect

Med ICMP Redirect kan man til en afsender fortælle en anden vej til destination

Den angivne vej kan være smartere eller mere effektiv

Det er desværre uheldigt, idet der ingen sikkerhed er

Idag bør man ikke lytte til ICMP redirects, ej heller generere dem

Det svarer til ARP spoofing, idet trafik omdirigeres

New Loki - ikke alt er layer 7

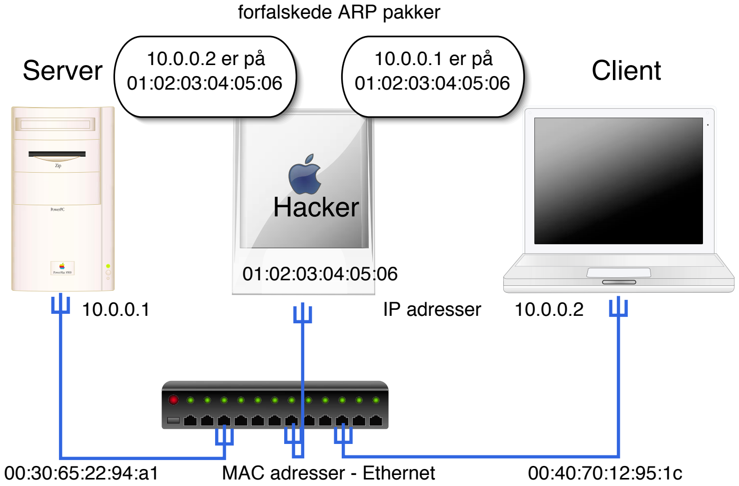
> At the beginning LOKI was made to combine some stand-alone **command line tools**, like the `bgp_cli`, the `ospf_cli` or the `ldp_cli` and to give them a **user friendly, graphical interface**. In the meantime LOKI is more than just the comb ination of the single tools, it gave its modules the opportunity to base upon each other (like **combining ARP-spoofing from th e ARP module with some man-in-the-middle actions, rewriting MPLS-labels for example)** and even inter operate with each other. (Fre mh<E6>vning: HLK)

`https://www.c0decafe.de/loki.html` Loki

`http://www.packetstan.com/2011/02/running-loki-on-backtrack-4-r2.html`

"Yersinia is a network tool designed to take advantage of some weakeness in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems."`http://www.yersinia.net/`

Hvordan virker ARP spoofing?



Hackeren sender forfalskede ARP pakker til de to parter

De sender derefter pakkerne ud på Ethernet med hackerens MAC adresse som modtager - som får alle pakkerne

Forsvar mod ARP spoofing

Hvad kan man gøre?

låse MAC adresser til porte på switche

låse MAC adresser til bestemte IP adresser

Efterfølgende administration!

Adskilte netværk - brug IEEE 802.1q VLANs

arpwatch er et godt bud - overvåger ARP

bruge protokoller som ikke er sårbare overfor opsamling

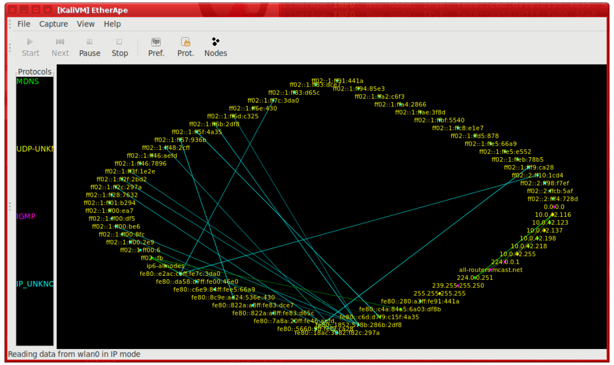
Lufthavns wifi

Åbne trådløse netværk er dejlige, vi bruger dem allesammen.

```
http://wifi.aal.dk/fs/customwebauth/login.html?
switch_url=http://wifi.aal.dk/login.html&ap_mac=70:db:98:73:e5:a0&
```
client_mac=30:10:b3:XX:YY:ZZ&wlan=AALfree&redirect=www.gstatic.com/generate_204

- Når du forbinder til netværket, bruger din enhed sin MAC adresse
- Denne indeholder en OUI som er den første halvdel af de 48-bit
- Dette ID er gemt i din enhed, fra fabrikken, kan sjældent ændres
- Alle i nærheden kan se denne MAC, og dermed din enheds unikke hardwareadresse.
- Kendere ved at man kan skifte sin MAC midlertidigt, og det gør telefoner ofte når de scanner efter netværk idag - hvis de overhovedet scanner

Demo Attacks fun with nodes



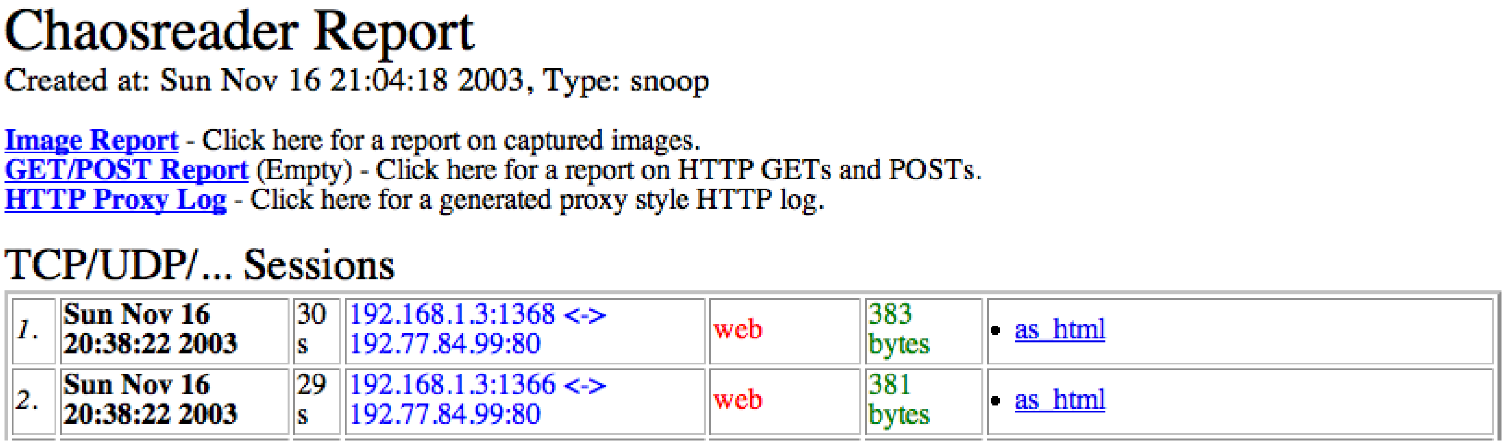
Reading data from wlan0 in IP mode

EtherApe is a graphical network monitor for Unix modeled after etherman. Featuring link layer, IP and TCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Color coded protocols display.

How do we find nodes to perform ARP spoofing?

The main page for the tool is: `https://etherape.sourceforge.io/`

Chaosreader



Chaosreader Report

Created at: Sun Nov 16 21:04:18 2003, Type: snoop

Image Report - Click here for a report on captured images.
GET/POST Report (Empty) - Click here for a report on HTTP GETs and POSTs.
HTTP Proxy Log - Click here for a generated proxy style HTTP log.

TCP/UDP/... Sessions

1.	**Sun Nov 16 20:38:22 2003**	30 s	192.168.1.3:1368 <-> 192.77.84.99:80	web	383 bytes	• as_html
2.	**Sun Nov 16 20:38:22 2003**	29 s	192.168.1.3:1366 <-> 192.77.84.99:80	web	381 bytes	• as_html

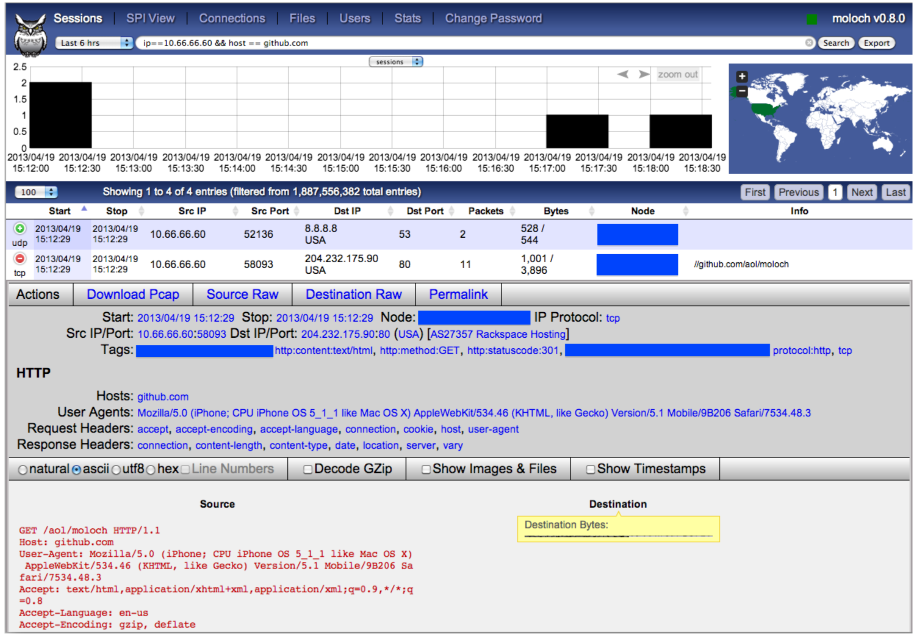
Simple but illustrative program

Read a pcap - packet capture into this tool chaosreader

Output HTML with nice index - usefull for quick demos

`http://chaosreader.sourceforge.net/`

Big data example Moloch



ip==10.66.66.60 && host == github.com

Showing 1 to 4 of 4 entries (filtered from 1,887,556,382 total entries)

	Start	Stop	Src IP	Src Port	Dst IP	Dst Port	Packets	Bytes	Node	Info
udp	2013/04/19 15:12:29	2013/04/19 15:12:29	10.66.66.60	52136	8.8.8.8 USA	53	2	528 / 544	[redacted]	
tcp	2013/04/19 15:12:29	2013/04/19 15:12:29	10.66.66.60	58093	204.232.175.90 USA	80	11	1,001 / 3,896	[redacted]	//github.com/aol/moloch

Actions | Download Pcap | Source Raw | Destination Raw | Permalink

Start: 2013/04/19 15:12:29 Stop: 2013/04/19 15:12:29 Node: [redacted] IP Protocol: tcp
Src IP/Port: 10.66.66.60:58093 Dst IP/Port: 204.232.175.90:80 (USA) [AS27357 Rackspace Hosting]
Tags: [redacted] http:content:text/html, http:method:GET, http:statuscode:301, [redacted] protocol:http, tcp

HTTP

Hosts: github.com
User Agents: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3
Request Headers: accept, accept-encoding, accept-language, connection, cookie, host, user-agent
Response Headers: connection, content-length, content-type, date, location, server, vary

○ natural ● ascii ○ utf8 ○ hex □ Line Numbers | □ Decode GZip | □ Show Images & Files | □ Show Timestamps

Source

```
GET /aol/moloch HTTP/1.1
Host: github.com
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1_1 like Mac OS X)
 AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Sa
fari/7534.48.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q
=0.8
Accept-Language: en-us
Accept-Encoding: gzip, deflate
```

Destination

Destination Bytes:

Picture from `https://github.com/aol/moloch`

Be your own GCHQ … capture all, index all, search all

Exercise

Now lets do the exercise

Zeek on the web 10min

which is number **6** in the exercise PDF.

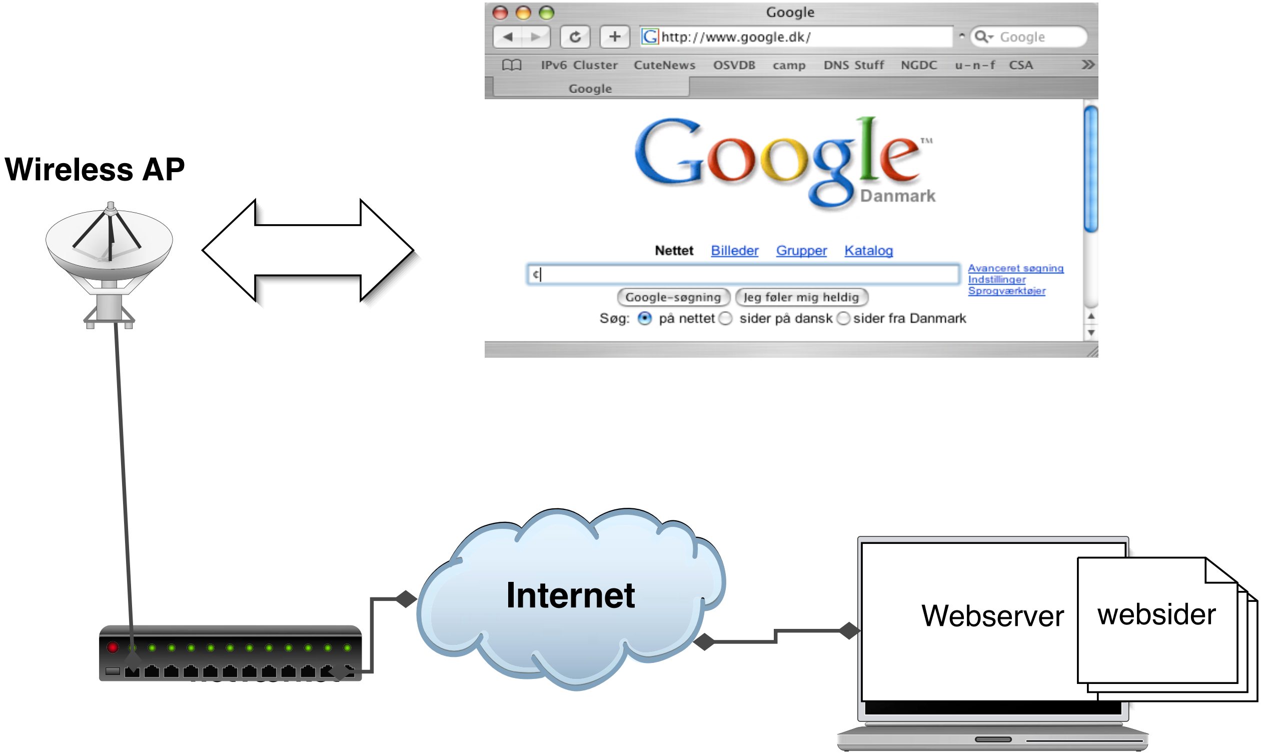
Exercise

Now lets do the exercise

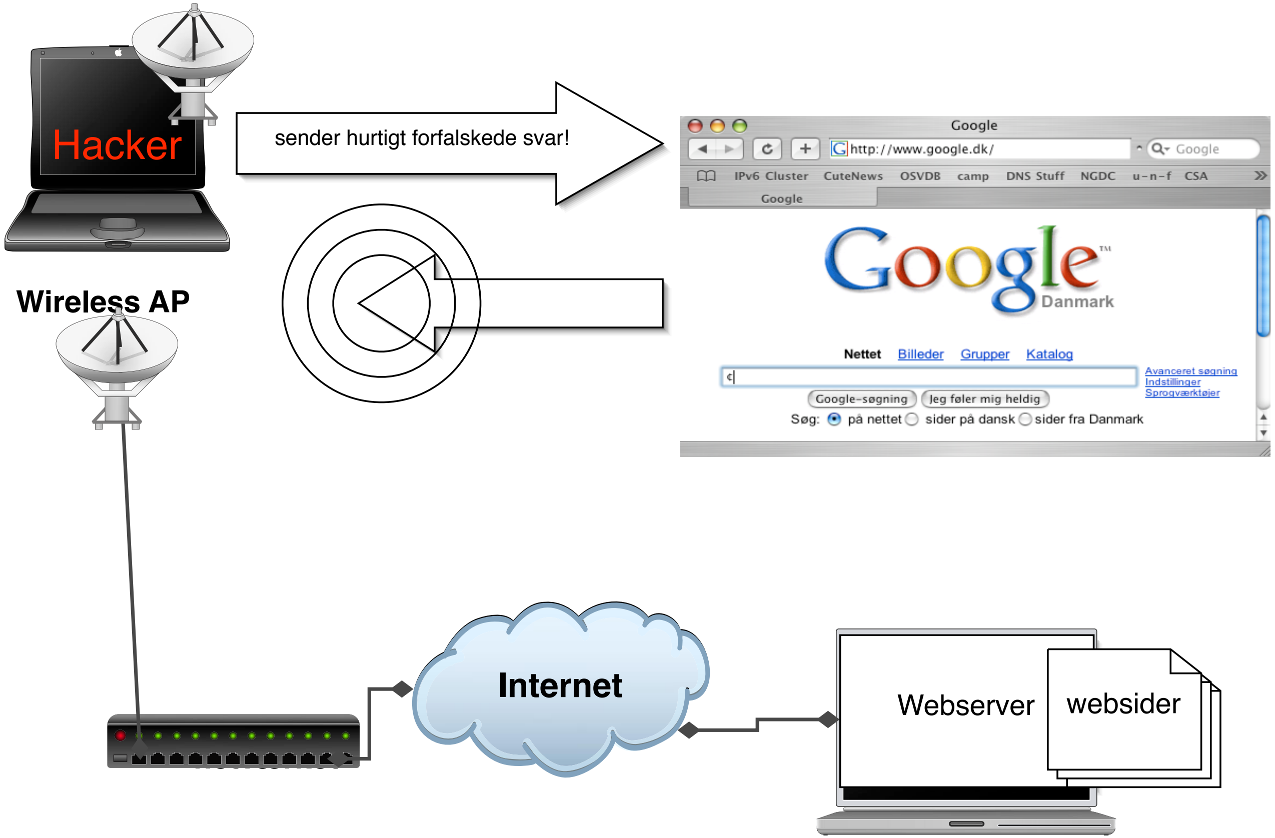
Bonus: Configure Mirror Port 10min

which is number **7** in the exercise PDF.

Normal WLAN brug



Packet injection - airpwn


sender hurtigt forfalskede svar!

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 måske 20-50ms
- Airpwn kan svare på omkring 1ms angives det
- Airpwn har alle informationer til rådighed

Airpwn source findes på Sourceforge
`http://airpwn.sourceforge.net/`

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

Mange Wireless netværk idag er ukrypterede og samme teknikker kan bruges idag

Ja, de **samme metoder** oprindeligt fra **2004** kan bruges idag!

Exercise

Now lets do the exercise

Wardriving Up to 30min

which is number **8** in the exercise PDF.

Cryptography

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`

Kryptografiske principper

Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

Et successfuldt 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`

DES, Triple DES og AES

AES

Advanced Encryption Standard

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

Der blev i 2001 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.

Se også `https://en.wikipedia.org/wiki/Advanced_Encryption_Standard`

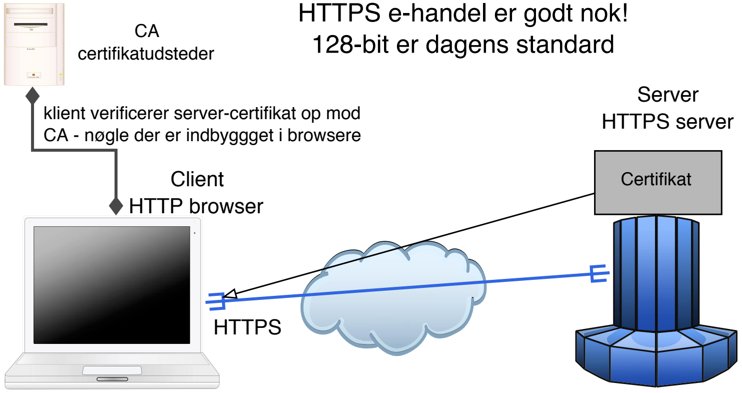
Formålet med kryptering

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet

SSL og TLS


CA
certifikatudsteder
HTTPS e-handel er godt nok!
128-bit er dagens standard
klient verificerer server-certifikat op mod
CA - nøgle der er indbyggget i browsere
Server
HTTPS server
Certifikat
Client
HTTP browser
HTTPS

Oprindeligt udviklet af Netscape Communications Inc.

Secure Sockets Layer SSL er idag blevet adopteret af IETF og kaldes derfor også for Transport Layer Security TLS TLS er baseret på SSL Version 3.0

RFC-2246 The TLS Protocol Version 1.0 fra Januar 1999

RFC-3207 SMTP STARTTLS

SSL

> The 'S' in HTTPS stands for 'secure' and the security is provided by SSL/TLS. SSL/TLS is a standard network protocol which is implemented in every browser and web server to provide confidentiality and integrity for HTTPS traffic.

Nu vi snakker om kryptering - SSL overalt?

Kan vi klare det på vores servere?

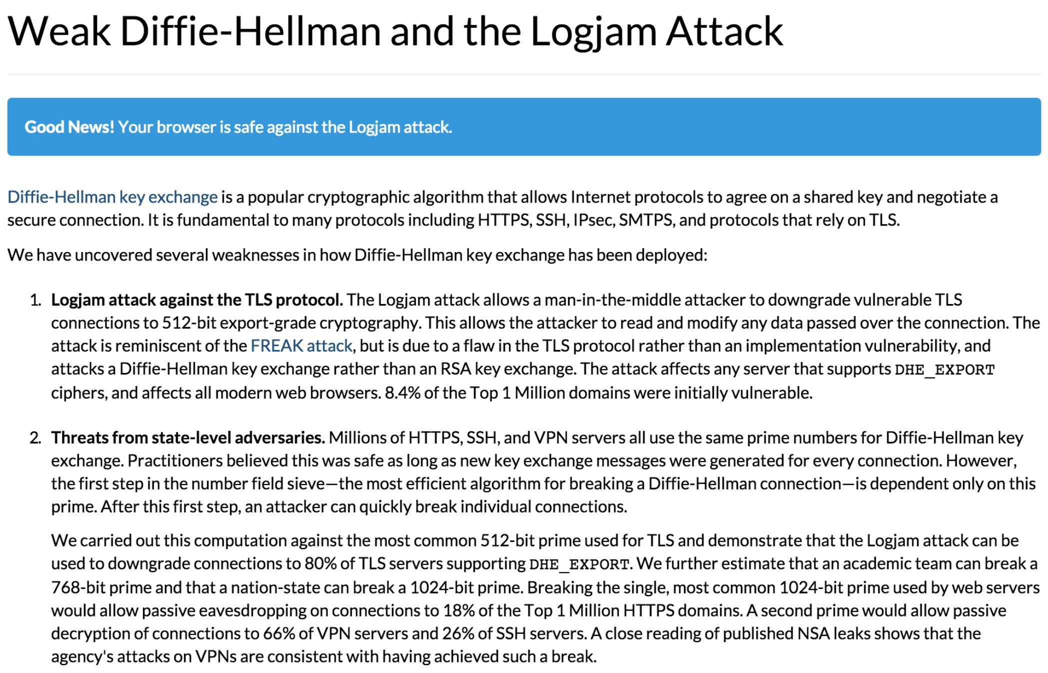
Google kan:

`http://www.imperialviolet.org/2010/06/25/overclocking-ssl.html`

Men alt for få gør det

Næste spørgsmål er så hvilke rod-certifikater man stoler på ...

Weak DH paper



Weak Diffie-Hellman and the Logjam Attack

Good News! Your browser is safe against the Logjam attack.

Diffie-Hellman key exchange is a popular cryptographic algorithm that allows Internet protocols to agree on a shared key and negotiate a secure connection. It is fundamental to many protocols including HTTPS, SSH, IPsec, SMTPS, and protocols that rely on TLS.

We have uncovered several weaknesses in how Diffie-Hellman key exchange has been deployed:

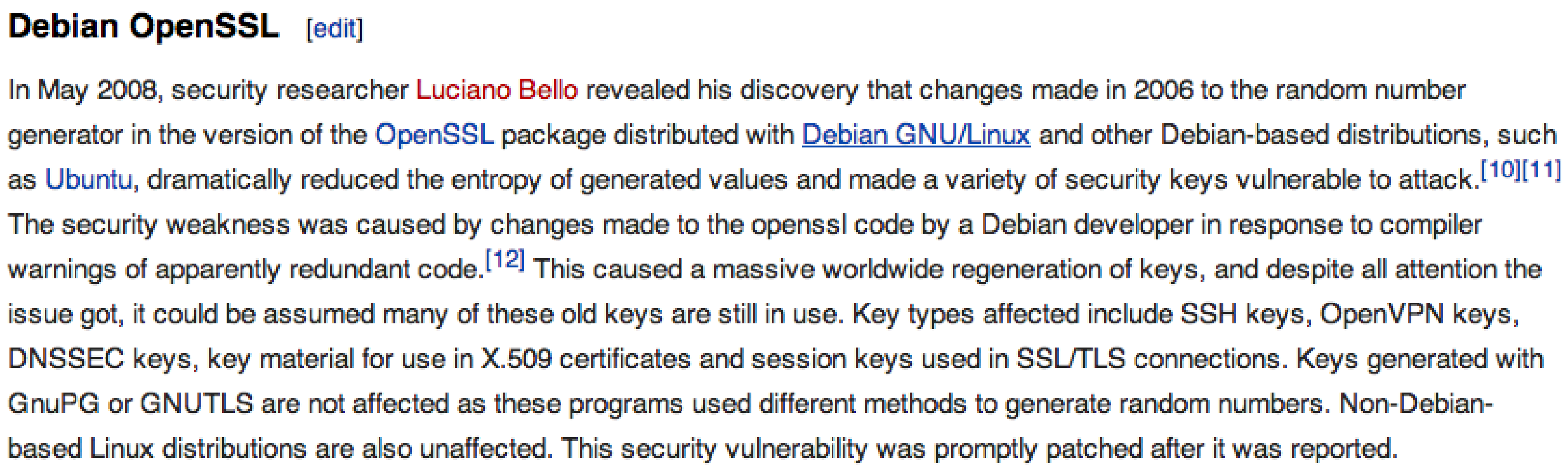
1. **Logjam attack against the TLS protocol.** The Logjam attack allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography. This allows the attacker to read and modify any data passed over the connection. The attack is reminiscent of the FREAK attack, but is due to a flaw in the TLS protocol rather than an implementation vulnerability, and attacks a Diffie-Hellman key exchange rather than an RSA key exchange. The attack affects any server that supports `DHE_EXPORT` ciphers, and affects all modern web browsers. 8.4% of the Top 1 Million domains were initially vulnerable.

2. **Threats from state-level adversaries.** Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve—the most efficient algorithm for breaking a Diffie-Hellman connection—is dependent only on this prime. After this first step, an attacker can quickly break individual connections.

   We carried out this computation against the most common 512-bit prime used for TLS and demonstrate that the Logjam attack can be used to downgrade connections to 80% of TLS servers supporting `DHE_EXPORT`. We further estimate that an academic team can break a 768-bit prime and that a nation-state can break a 1024-bit prime. Breaking the single, most common 1024-bit prime used by web servers would allow passive eavesdropping on connections to 18% of the Top 1 Million HTTPS domains. A second prime would allow passive decryption of connections to 66% of VPN servers and 26% of SSH servers. A close reading of published NSA leaks shows that the agency's attacks on VPNs are consistent with having achieved such a break.

Source: `https://weakdh.org/` and
`https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf`

PRNG



Debian OpenSSL [edit]

In May 2008, security researcher Luciano Bello revealed his discovery that changes made in 2006 to the random number generator in the version of the OpenSSL package distributed with Debian GNU/Linux and other Debian-based distributions, such as Ubuntu, dramatically reduced the entropy of generated values and made a variety of security keys vulnerable to attack.[10][11] The security weakness was caused by changes made to the openssl code by a Debian developer in response to compiler warnings of apparently redundant code.[12] This caused a massive worldwide regeneration of keys, and despite all attention the issue got, it could be assumed many of these old keys are still in use. Key types affected include SSH keys, OpenVPN keys, DNSSEC keys, key material for use in X.509 certificates and session keys used in SSL/TLS connections. Keys generated with GnuPG or GNUTLS are not affected as these programs used different methods to generate random numbers. Non-Debian-based Linux distributions are also unaffected. This security vulnerability was promptly patched after it was reported.

`https://en.wikipedia.org/wiki/Random_number_generator_attack#Debian_OpenSSL`

The random number generator is VITAL for crypto security

Check out modern CPUs and Linux response to this
`https://en.wikipedia.org/wiki/RdRand`

sslscan

```
root@kali:~# sslscan --ssl2 web.gratisdns.dk
Version: 1.10.5-static
OpenSSL 1.0.2e-dev xx XXX xxxx

Testing SSL server web.gratisdns.dk on port 443
...
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  *.gratisdns.dk
Altnames: DNS:*.gratisdns.dk, DNS:gratisdns.dk
Issuer:   AlphaSSL CA - SHA256 - G2
```

Source: Originally sslscan from http://www.titania.co.uk but use the version on Kali

IPsec IKE-SCAN

Scan IPs for VPN endpoints with ike-scan:

```
root@kali:~# ike-scan 91.102.91.30
Starting ike-scan 1.9 with 1 hosts
(http://www.nta-monitor.com/tools/ike-scan/)
91.102.91.30 Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=f0d6043badb2b7bc, msgid=f97a7508)

Ending ike-scan 1.9: 1 hosts scanned in 1.238 seconds (0.81 hosts/sec).
0 returned handshake; 1 returned notify
```

Source:

http://www.nta-monitor.com/tools-resources/security-tools/ike-scan

crack IKE psk?

http://ikecrack.sourceforge.net/

https://www.trustwave.com/Resources/SpiderLabs-Blog/Cracking-IKE-Mission-Improbable-(Part-1)/

ike-scan network scanning

```
hlk@cornerstone03:~$ sudo ike-scan -M 91.102.91.0/24
Starting ike-scan 1.9 with 256 hosts
(http://www.nta-monitor.com/tools/ike-scan/)
91.102.91.14 Notify message 14 (NO-PROPOSAL-CHOSEN)
 HDR=(CKY-R=94dd41cf44da082b, msgid=602c35c1)
91.102.91.30 Notify message 14 (NO-PROPOSAL-CHOSEN)
 HDR=(CKY-R=e21e89d16f898aa5, msgid=ff41d51c)
91.102.91.70 Notify message 14 (NO-PROPOSAL-CHOSEN)
 HDR=(CKY-R=e882d9b4477b847b, msgid=55be4339)
91.102.91.78 Notify message 14 (NO-PROPOSAL-CHOSEN)
 HDR=(CKY-R=1fc54d8c3042daa3, msgid=ea705f39)
91.102.91.150 Notify message 14 (NO-PROPOSAL-CHOSEN)
 HDR=(CKY-R=d5470f881de6d2d9, msgid=2bf5f5ef)
91.102.91.158 Notify message 14 (NO-PROPOSAL-CHOSEN)
 HDR=(CKY-R=9f7af04bcb0152a9, msgid=44f26f01)
Ending ike-scan 1.9: 256 hosts scanned in 40.465 seconds (6.33 hosts/sec).
0 returned handshake; 6 returned notify
```

Exercise

Now lets do the exercise

SSL/TLS scanners 15 min

which is number **9** in the exercise PDF.

Exercise

Now lets do the exercise

Try pcap-diff 15 min

which is number **10** in the exercise PDF.

Exercise

Now lets do the exercise

Bonus: EtherApe 10 min

which is number **11** in the exercise PDF.

Exercise

Now lets do the exercise

ARP spoofing and ettercap 20min

which is number **12** in the exercise PDF.

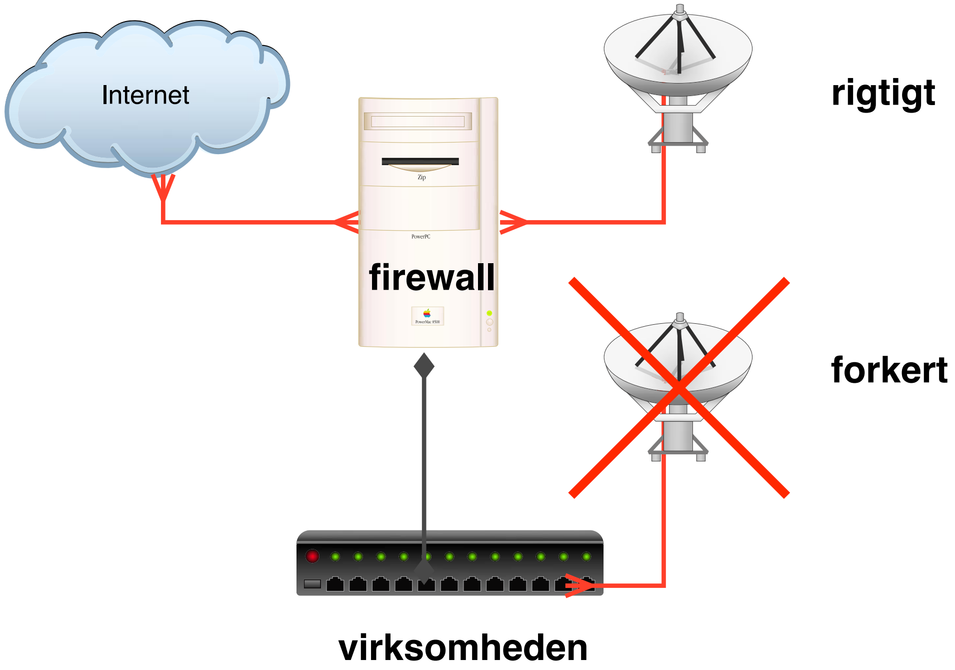
Når adgangen er skabt

Så går man igang med de almindelige værktøjer

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

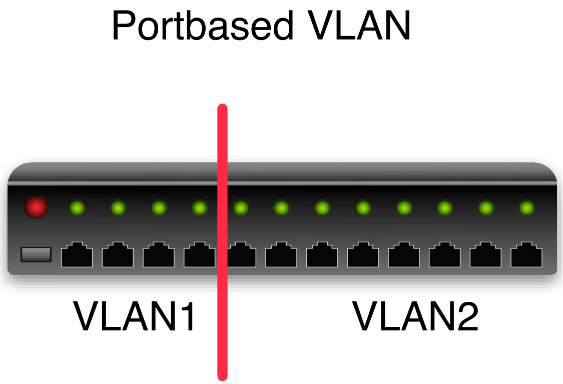
Forsvaret er som altid - flere lag af sikkerhed!

Infrastrukturændringer



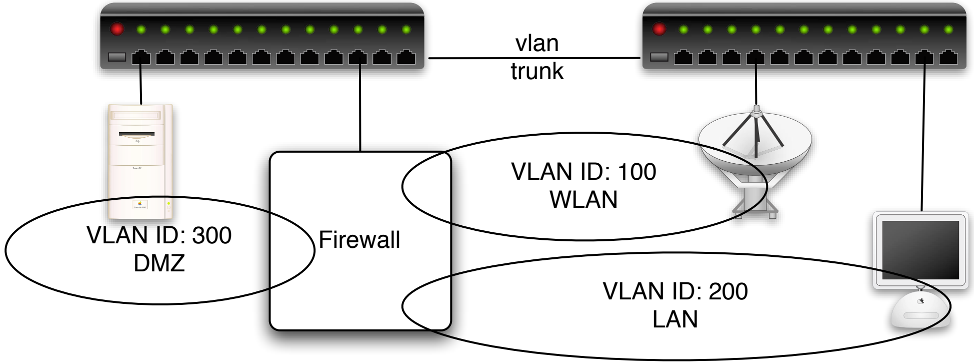
Sådan bør et access point logisk forbindes til netværket

VLAN Virtual LAN



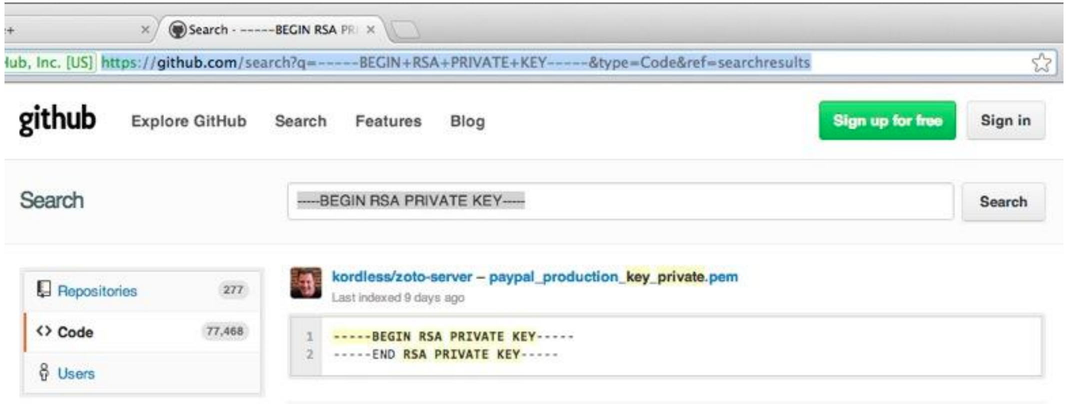
- Nogle switche tillader at man opdeler portene
- Denne opdeling kaldes VLAN og portbaseret er det mest simple
- Port 1-4 er et LAN
- De resterende er et andet LAN
- Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2

IEEE 802.1q



- 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 værktøjer der måske kan lette dette arbejde management værktøjer, provisioneringsværktøjer osv. Network Automation with Python

Github Public passwords?



https://github.com/search?q=-----BEGIN+RSA+PRIVATE+KEY-----&type=Code&ref=searchresults

-----BEGIN RSA PRIVATE KEY-----

kordless/zoto-server – paypal_production_key_private.pem

Last indexed 9 days ago

```
-----BEGIN RSA PRIVATE KEY-----
-----END RSA PRIVATE KEY-----
```

Sources:

`https://twitter.com/brianaker/status/294228373377515522`

`http://www.webmonkey.com/2013/01/users-scramble-as-github-search-exposes-passwords-security-details/`

`http://www.leakedin.com/`

`http://www.offensive-security.com/community-projects/google-hacking-database/`

Use different passwords for different sites, yes - every site!

Simple Network Management Protocol

SNMP er en protokol der supporteres af de fleste professionelle netværksenheder, såsom switche, routere

hosts – skal slås til men følger som regel med

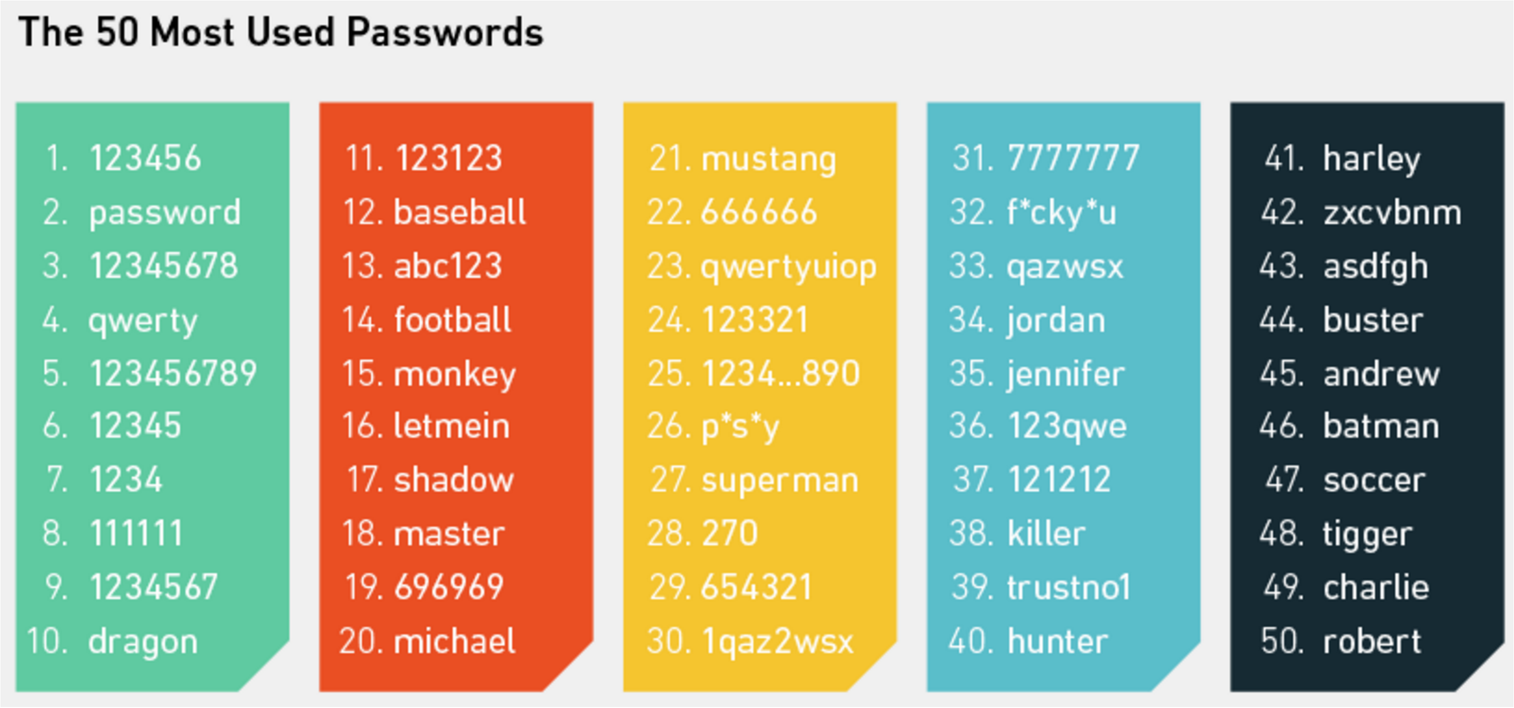
SNMP bruges til:

- *network management*
- statistik
- rapportering af fejl – SNMP traps

Sikkerheden baseres på community strings der sendes som klartekst ...

Det er nemmere at brute-force en community string end en brugerid/kodeord kombination

Passwords vælges ikke tilfældigt



The 50 Most Used Passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 111111
9. 1234567
10. dragon
11. 123123
12. baseball
13. abc123
14. football
15. monkey
16. letmein
17. shadow
18. master
19. 696969
20. michael
21. mustang
22. 666666
23. qwertyuiop
24. 123321
25. 1234...890
26. p*s*y
27. superman
28. 270
29. 654321
30. 1qaz2wsx
31. 7777777
32. f*cky*u
33. qazwsx
34. jordan
35. jennifer
36. 123qwe
37. 121212
38. killer
39. trustno1
40. hunter
41. harley
42. zxcvbnm
43. asdfgh
44. buster
45. andrew
46. batman
47. soccer
48. tigger
49. charlie
50. robert

Source: `https://wpengine.com/unmasked/`

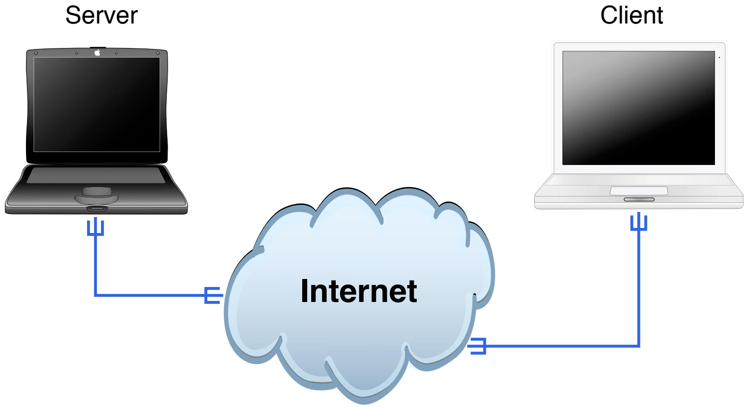
Brute force

Hvad betyder bruteforcing?
afprøvning af alle mulighederne

```
Hydra v2.5 (c) 2003 by van Hauser / THC <vh@thc.org>
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]]
[-o FILE] [-t TASKS] [-g TASKS] [-T SERVERS] [-M FILE] [-w TIME]
[-f] [-e ns] [-s PORT] [-S] [-vV] server service [OPT]

Options:
  -S         connect via SSL
  -s PORT    if the service is on a different default port, define it here
  -l LOGIN   or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS    or -P FILE try password PASS, or load several passwords from FILE
  -e ns      additional checks, "n" for null password, "s" try login as pass
  -C FILE    colon seperated "login:pass" format, instead of -L/-P option
  -M FILE    file containing server list (parallizes attacks, see -T)
  -o FILE    write found login/password pairs to FILE instead of stdout
...
```

Demo: snmpwalk og Hydra



snmpwalk og Hydra

Vi laver sammen noget SNMP scanning og bruteforcing, derefter er det jeres tur

Exercise

Now lets do the exercise

SNMP walk 15min

which is number **16** in the exercise PDF.

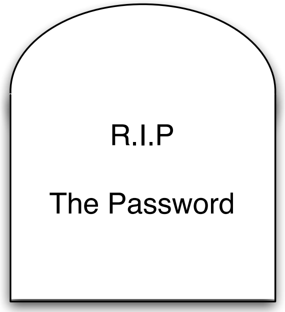
Exercise

Now lets do the exercise

Try Hydra brute force 30min

which is number **17** in the exercise PDF.

Are passwords dead?



Can we stop using passwords?

Muffett on Passwords has a long list of password related information, from the author of crack `http://en.wikipedia.org/wiki/Crack_(password_software)`

`http://dropsafe.crypticide.com/muffett-passwords`

NT hashes

NT LAN manager hash værdier er noget man typisk kan samle op i netværk

det er en hash værdi af et password som man ikke burde kunne bruge til noget - hash algoritmer er envejs

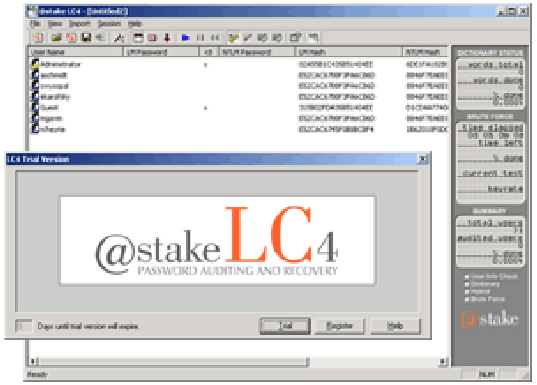
opbygningen gør at man kan forsøge brute-force på 7 tegn ad gangen!

en moderne pc med l0phtcrack kan nemt knække de fleste password på få dage!

og sikkert 25-30% indenfor den første dag - hvis der ingen politik er omkring kodeord!

ved at generere store tabeller, eksempelvis 100GB kan man dække mange hashværdier af passwords med almindelige bogstaver, tal og tegn - og derved knække passwordshashes på sekunder. Søg efter rainbowcrack med google

l0phtcrack LC4



Consider that at one of the largest technology companies, where policy required that passwords exceed 8 characters, mix cases, and include numbers or symbols...

L0phtCrack obtained 18% of the passwords in 10 minutes
90% of the passwords were recovered within 48 hours on a Pentium II/300
The Administrator and most Domain Admin passwords were cracked
http://www.atstake.com/research/lc/

Pass the hash

Lots of tools in pentesting pass the hash, reuse existing credentials and tokens *Still Passing the Hash 15 Years Later* `http://passing-the-hash.blogspot.dk/2013/04/pth-toolkit-for-kali-interim-status.html`

> If a domain is built using only modern Windows OSs and COTS products (which know how to operate within these new constraints), and configured correctly with no shortcuts taken, then these protections represent a big step forward.

Source:
`http://www.harmj0y.net/blog/penetesting/pass-the-hash-is-dead-long-live-pass-the-hash/` `https://samsclass.info/lulz/pth-8.1.htm`

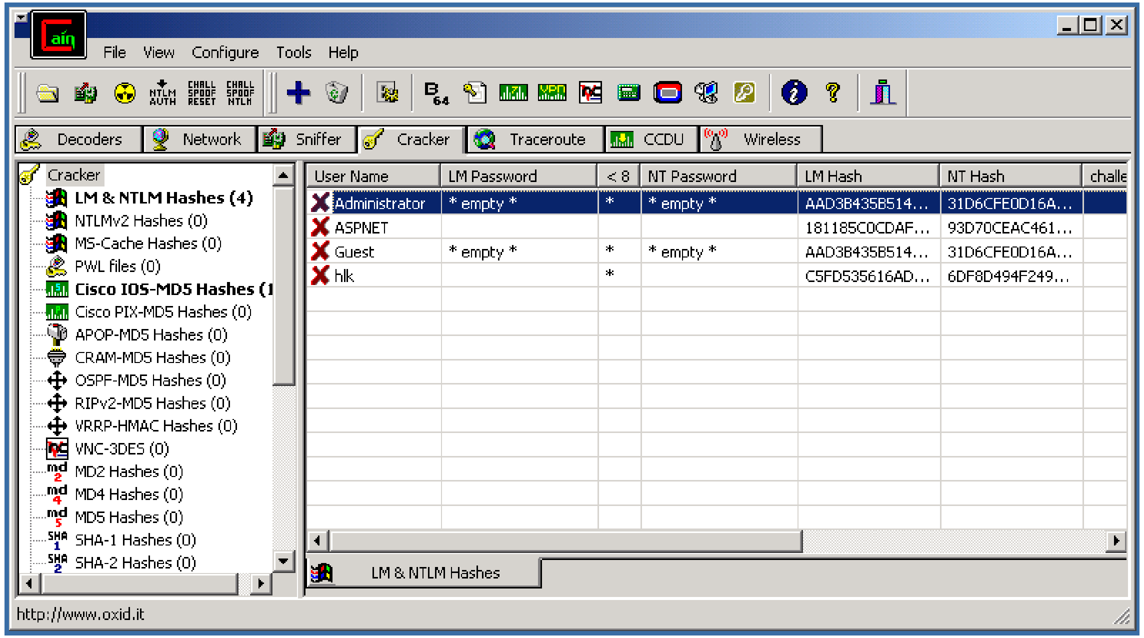
Mimikatz

> mimikatz is a tool I've made to learn C and make somes experiments with Windows security.
>
> It's now well known to extract plaintexts passwords, hash, PIN code and kerberos tickets from memory. mimikatz can also perform pass-the-hash, pass-the-ticket or build Golden tickets.

- Understatement of the year, candidate
- Proof of concept code, that is abused a lot by everyone, malware to pentesters
- `https://github.com/gentilkiwi/mimikatz`

Your anti-virus application SHOULD catch mimikatz

Cain og Abel



User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challe
Administrator	* empty *	*	* empty *	AAD3B435B514...	31D6CFE0D16A...	
ASPNET				181185C0CDAF...	93D70CEAC461...	
Guest	* empty *	*	* empty *	AAD3B435B514...	31D6CFE0D16A...	
hlk		*		C5FD535616AD...	6DF8D494F249...	

Cain og Abel *anbefales til demoer* `http://www.oxid.it`

Bruger selv John the Ripper eller Hashcat hvis jeg skal lave brute forcing

John the Ripper

> John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches.

Unix passwords kan knækkes med alec Muffets kendte Crack program eller eksempelvis John the Ripper `http://www.openwall.com/john/`

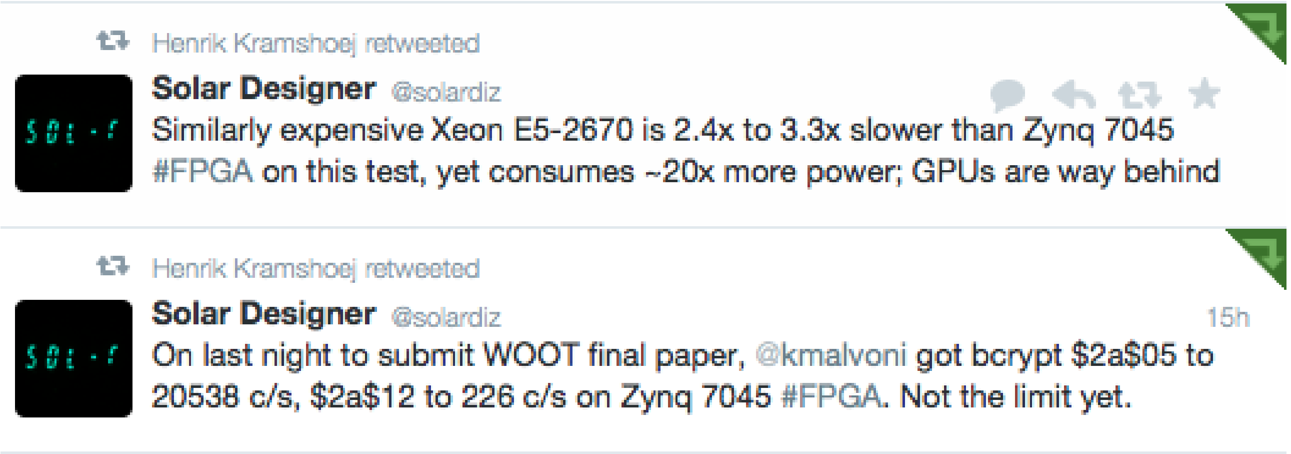
Jeg bruger selv John the Ripper

Cracking passwords

- 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:
`https://hashcat.net/wiki/`
`http://www.openwall.com/john/`

Parallella John



Henrik Kramshoej retweeted

Solar Designer @solardiz

Similarly expensive Xeon E5-2670 is 2.4x to 3.3x slower than Zynq 7045 #FPGA on this test, yet consumes ~20x more power; GPUs are way behind

Henrik Kramshoej retweeted

Solar Designer @solardiz 15h

On last night to submit WOOT final paper, @kmalvoni got bcrypt $2a$05 to 20538 c/s, $2a$12 to 226 c/s on Zynq 7045 #FPGA. Not the limit yet.

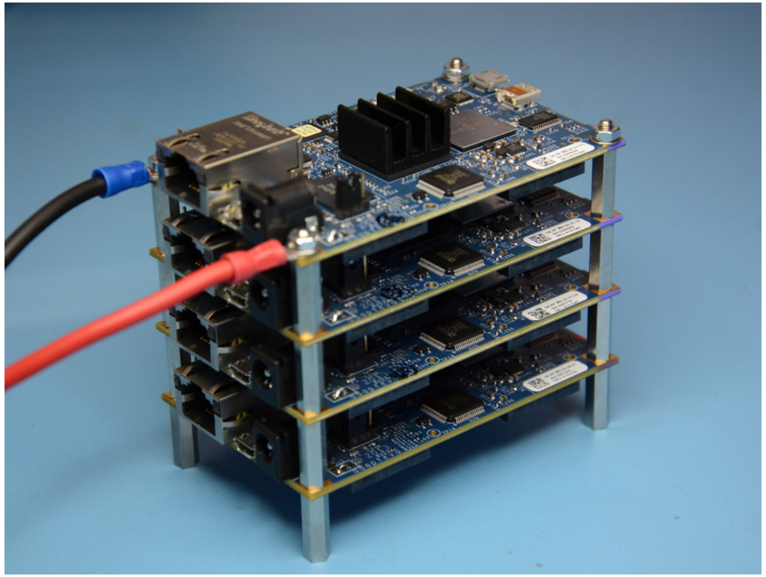
`https://twitter.com/solardiz/status/492037995080712192`

FPGA hacking er populært

Dog mange forskellige hardware systemer/modeller

Ringere support for algoritmer

Stacking Parallella boards

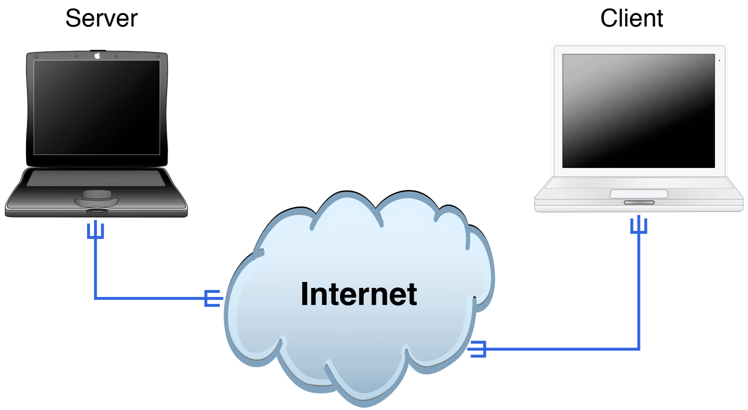


FPGA og ASICS må vi forvente at eksempelvis NSA bruger

https://www.parallella.org/

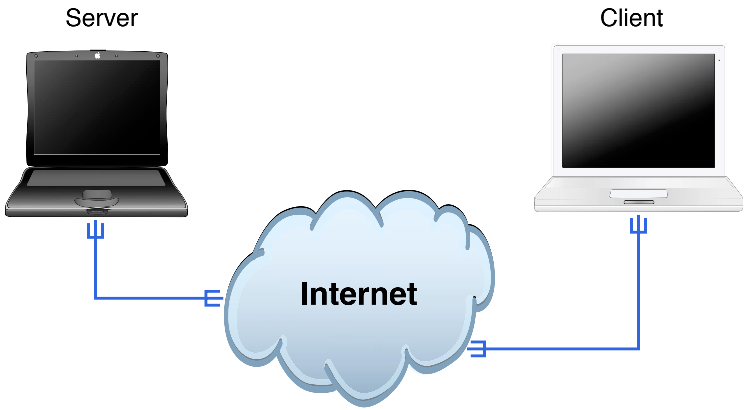
https://en.wikipedia.org/wiki/Application-specific_integrated_circuit

Demo: Playtime - speed test openssl speed, John speed



Playtime - speed test openssl speed, John speed

Demo: Cain/Abel, hashcat or John the Ripper

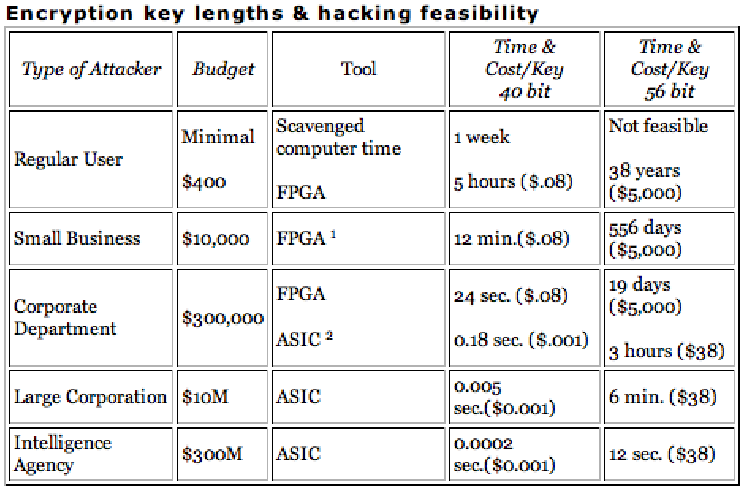


Cain/Abel, hashcat or John the Ripper

Try as many as you like

Grab sample hashes from your local system or
`https://hashcat.net/wiki/doku.php?id=example_hashes`

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)

Source: `http://www.mycrypto.net/encryption/encryption_crack.html`

More up to date: In 1998, the EFF built Deep Crack for less than $250,000

`https://en.wikipedia.org/wiki/EFF_DES_cracker`

FPGA Based UNIX Crypt Hardware Password Cracker - 100 EUR in 2006

`http://www.sump.org/projects/password/`

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

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

Konklusion: Kryptografi er svært

STANFORD UNIVERSITY

Cryptography

Professor Dan Boneh
Computer Science Department
Stanford University

Enroll / Login Now
Enroll in this online class for free with a Coursera account
0
10
20
30
40
50
60
70
80
90

Åbent kursus på Stanford
`http://crypto-class.org/`

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 ☺

Links:
Tutorial: Simple WEP Crack
`http://www.aircrack-ng.org/doku.php?id=simple_wep_crack`

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
```

Exercise

Now lets do the exercise

Aircrack-ng 30 min

which is number **18** in the exercise PDF.

RADIUS

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

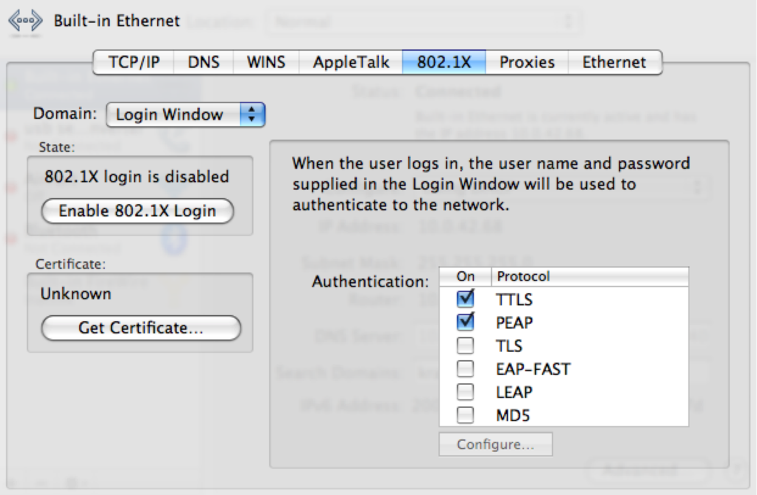
Remote Authentication Dial In User Service (RADIUS)

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

IEEE 802.1x Port Based Network Access Control



Domain: Login Window

State:

802.1X login is disabled

Certificate:

Unknown

When the user logs in, the user name and password supplied in the Login Window will be used to authenticate to the network.

Authentication:

On	Protocol
☑	TTLS
☑	PEAP
□	TLS
□	EAP-FAST
□	LEAP
□	MD5

- 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

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 = 802.1X + EAP + CCMP

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

Source: 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.

Source: 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

WPA cracking

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

Desværre ikke!

Du skal vælge en laaaaang passphrase

Hvis koden til wifi er for kort kan man sniffe WPA handshake når en computer går ind på netværket, og knække den!

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 med 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

```
# 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
```

Aircrack-ng er en god måde at checke om der er et handshake i filen

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

En mere moderne CPU kommer stadig ikke særligt højt, med WPA cracking, Hint: GPU

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.

`http://pyrit.wordpress.com/about/`

Also check out the Reaver brute force WPS

`https://code.google.com/p/reaver-wps/`

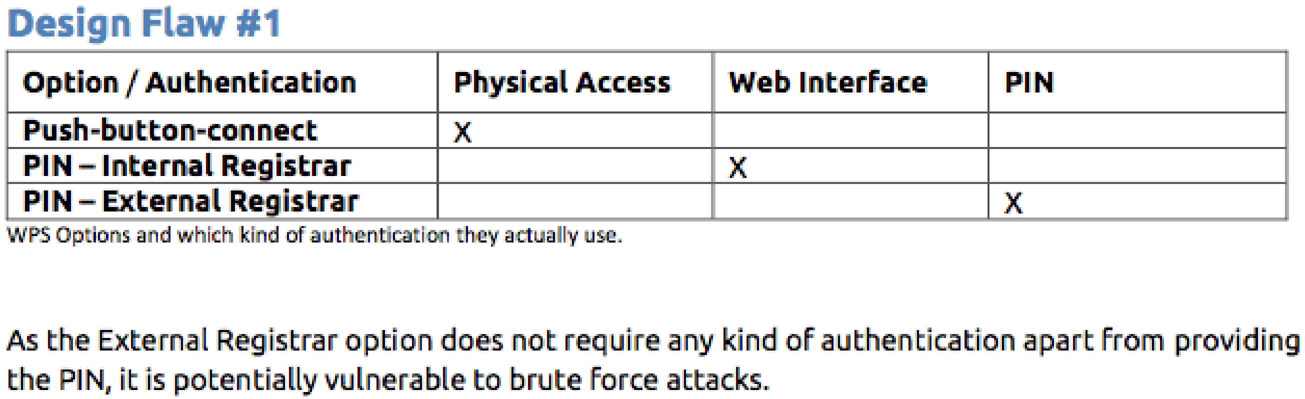
Wi-Fi Protected Setup, WPS hacking - Reaver

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?

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

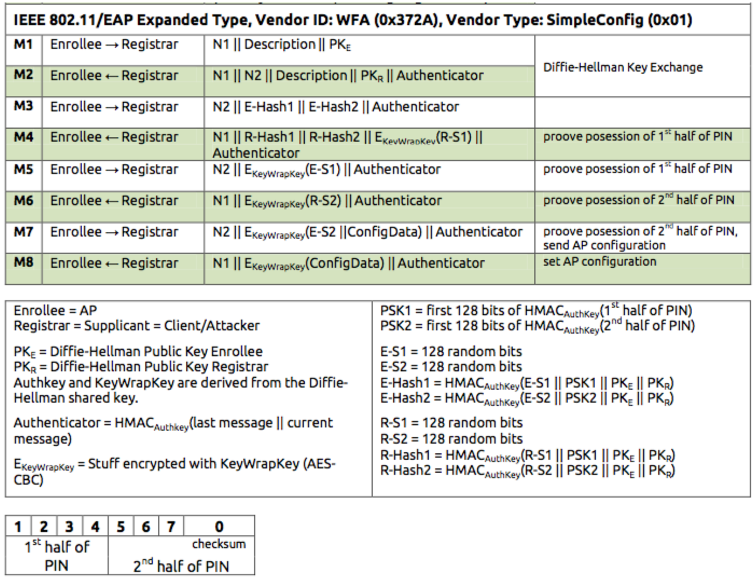
WPS Options and which kind of authentication they actually use.

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 || $E_{KevWrapKev}$(R-S1) || Authenticator	proove posession of 1st half of PIN
M5	Enrollee → Registrar	N2 || $E_{KeyWrapKey}$(E-S1) || Authenticator	proove posession of 1st half of PIN
M6	Enrollee ← Registrar	N1 || $E_{KeyWrapKey}$(R-S2) || Authenticator	proove posession of 2nd half of PIN
M7	Enrollee → Registrar	N2 || $E_{KeyWrapKey}$(E-S2 ||ConfigData) || Authenticator	proove posession of 2nd half of PIN, send AP configuration
M8	Enrollee ← Registrar	N1 || $E_{KeyWrapKey}$(ConfigData) || Authenticator	set AP configuration

Enrollee = AP
Registrar = Supplicant = Client/Attacker

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.

Authenticator = $HMAC_{Authkey}$(last message || current message)

$E_{KeyWrapKey}$ = Stuff encrypted with KeyWrapKey (AES-CBC)

PSK1 = first 128 bits of $HMAC_{AuthKey}$(1st half of PIN)
PSK2 = first 128 bits of $HMAC_{AuthKey}$(2nd half of PIN)

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)

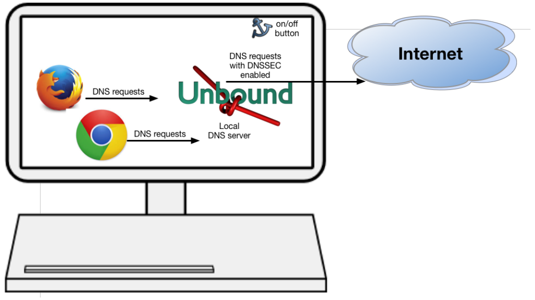
R-S1 = 128 random bits
R-S2 = 128 random bits
R-Hash1 = $HMAC_{AuthKey}$(R-S1 || PSK1 || PK_E || PK_R)
R-Hash2 = $HMAC_{AuthKey}$(R-S2 || PSK2 || PK_E || PK_R)

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

Reminds me of NTLM cracking, crack parts independently

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

DNSSEC trigger



Lots of DNSSEC tools, I recommend DNSSEC-trigger a local name server for your laptop

- DNSSEC Validator for firefox https://addons.mozilla.org/en-us/firefox/addon/dnssec-validator/
- OARC tools https://www.dns-oarc.net/oarc/services/odvr
- http://www.nlnetlabs.nl/projects/dnssec-trigger/

DNSSEC NSEC walk the zone

DNSSEC:NSEC vs. NSEC3

The Domain Name System Security Extensions(DNSSEC) provide two different records for securely handling non-existent names in DNS, NSEC and NSEC3. They are mutually exclusive, so operators need to pick one when deploying DNSSEC.

The problem both NSEC and NSEC3 solve is knowing when a name exists within a given zone. This is required to prevent malicious actors from sending fake negative responses to queries.

... the challenge with the plain NSEC record is that someone could use the NSEC responses to "walk the zone" and build a list of all of the records in a DNS zone.

Source:
`http://www.internetsociety.org/deploy360/resources/dnssec-nsec-vs-nsec3/`

Perhaps try `http://josefsson.org/walker/`

DANE

Objective:

Specify mechanisms and techniques that allow Internet applications to establish cryptographically secured communications by using information distributed through DNSSEC for discovering and authenticating public keys which are associated with a service located at a domain name.

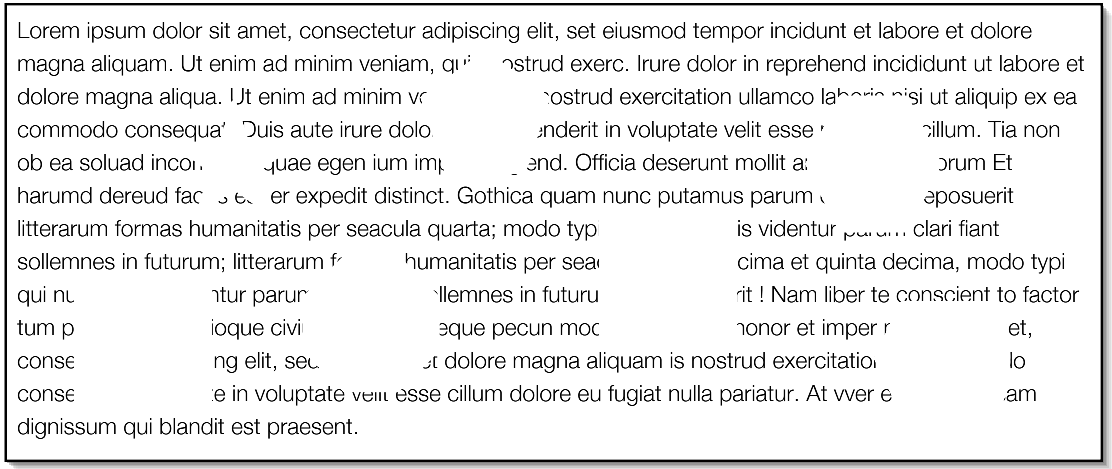
DNS-based Authentication of Named Entities (dane)
`https://datatracker.ietf.org/wg/dane/charter/`

`http://googleonlinesecurity.blogspot.dk/2011/04/improving-ssl-certificate-security.html`

DNSSEC er ved at være godt udbredt - undtagen i DK

(findes på .dk zonen, men næsten ingen resolvere)

Are your data secure - data at rest



Lorem ipsum dolor sit amet, consectetur adipiscing elit, set eiusmod tempor incidunt et labore et dolore
magna aliquam. Ut enim ad minim veniam, qu ostrud exerc. Irure dolor in reprehend incididunt ut labore et
dolore magna aliqua. Ut enim ad minim v ostrud exercitation ullamco lab isi ut aliquip ex ea
commodo consequa Duis aute irure dolo nderit in voluptate velit esse cillum. Tia non
ob ea soluad inco quae egen ium im end. Officia deserunt mollit a orum Et
harumd dereud fac er expedit distinct. Gothica quam nunc putamus parum eposuerit
litterarum formas humanitatis per seacula quarta; modo typi is videntur clari fiant
sollemnes in futurum; litterarum f humanitatis per sea cima et quinta decima, modo typi
qui nu ntur parur llemnes in futuru rit ! Nam liber te conscient to factor
tum p ioque civi eque pecun moc honor et imper et,
conse ng elit, sec t dolore magna aliquam is nostrud exercitatio lo
conse e in voluptate velit esse cillum dolore eu fugiat nulla pariatur. At vver e am
dignissum qui blandit est praesent.

Stolen laptop, tablet, phone - can anybody read your data?

Do you trust ”remote wipe”

How do you in fact wipe data securely off devices, and SSDs?

Encrypt disk and storage devices before using them in the first place!

Circumvent security - single user mode boot

Unix systems often allows boot into singleuser mode
press command-s when booting Mac OS X

Laptops can often be booted using PXE network or CD boot

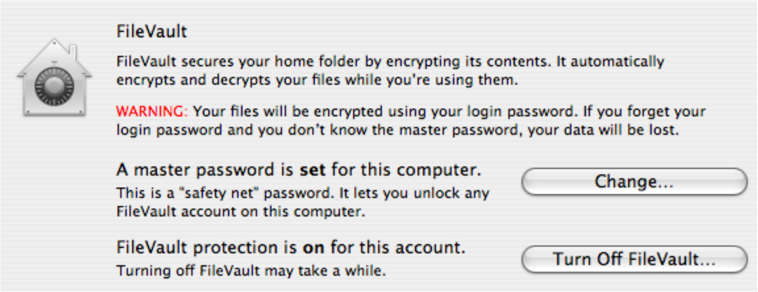
Mac computers can become a Firewire disk
hold t when booting - firewire target mode

Unrestricted access to un-encrypted data

Moving hard drive to another computer is also easy

Physical access is often - **game over**

Encrypting hard disk



FileVault

FileVault secures your home folder by encrypting its contents. It automatically encrypts and decrypts your files while you're using them.

WARNING: Your files will be encrypted using your login password. If you forget your login password and you don't know the master password, your data will be lost.

A master password is **set** for this computer.
This is a "safety net" password. It lets you unlock any FileVault account on this computer.

FileVault protection is **on** for this account.
Turning off FileVault may take a while.

Becoming available in the most popular client operating systems

- Microsoft Windows Bitlocker - requires Ultimate or Enterprise
- Apple Mac OS X - FileVault og FileVault2
- FreeBSD GEOM og GBDE - encryption framework
- Linux LUKS distributions like Ubuntu ask to encrypt home dir during installation
- PGP disk - Pretty Good Privacy - makes a virtuel krypteret disk
- TrueCrypt - similar to PGP disk, a virtual drive with data, cross platform
- Some vendors have BIOS passwords, or disk passwords

Attacks on disk encryption

Firewire, DMA & Windows, Winlockpwn via FireWire
Hit by a Bus: Physical Access Attacks with Firewire Ruxcon 2006

Removing memory from live system - data is not immediately lost, and can be read under some circumstances
Lest We Remember: Cold Boot Attacks on Encryption Keys
`http://citp.princeton.edu/memory/`

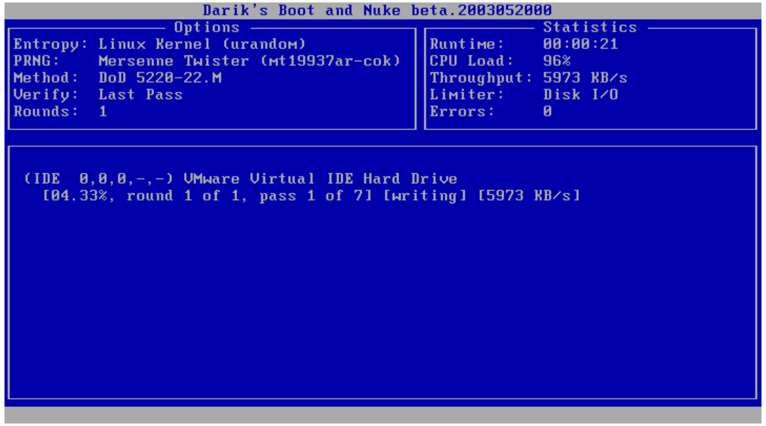
This is very CSI or Hollywoord like - but a real threat

VileFault decrypts encrypted Mac OS X disk image files
`https://code.google.com/p/vilefault/`

FileVault Drive Encryption (FVDE) (or FileVault2) encrypted volumes
`https://code.google.com/p/libfvde/`

So perhaps use both hard drive encryption AND turn off computer after use?

… and deleting data



```
                  Darik's Boot and Nuke beta.2003052000
 ─────────────── Options ───────────────  ──────── Statistics ──────
 Entropy: Linux Kernel (urandom)           Runtime:    00:00:21
 PRNG:    Mersenne Twister (mt19937ar-cok)  CPU Load:   96%
 Method:  DoD 5220-22.M                    Throughput: 5973 KB/s
 Verify:  Last Pass                        Limiter:    Disk I/O
 Rounds:  1                                Errors:     0

  (IDE  0,0,0,-,-) VMware Virtual IDE Hard Drive
   [04.33%, round 1 of 1, pass 1 of 7] [writing] [5973 KB/s]
```

Getting rid of data from old devices is a pain

Some tools will not overwrite data, leaving it vulnerable to recovery

Even secure erase programs might not work on SSD - due to reallocation of blocks

I have used Darik's Boot and Nuke ("DBAN") `http://www.dban.org/`

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