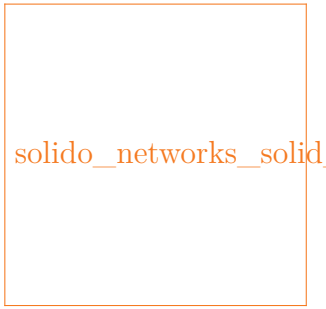



Welcome to

# Hacking - protect yourself

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

# Goal of this presentation

solido_networks_solid_RGB

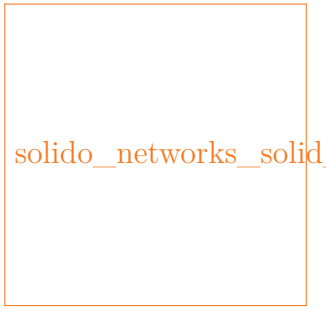
Don't Panic!

Introduce hacking and a couple of hacker tools

List some tools that can be used to protect your computer and data

PS Sorry about the many TLAs ... og danglish

# Plan for foredraget



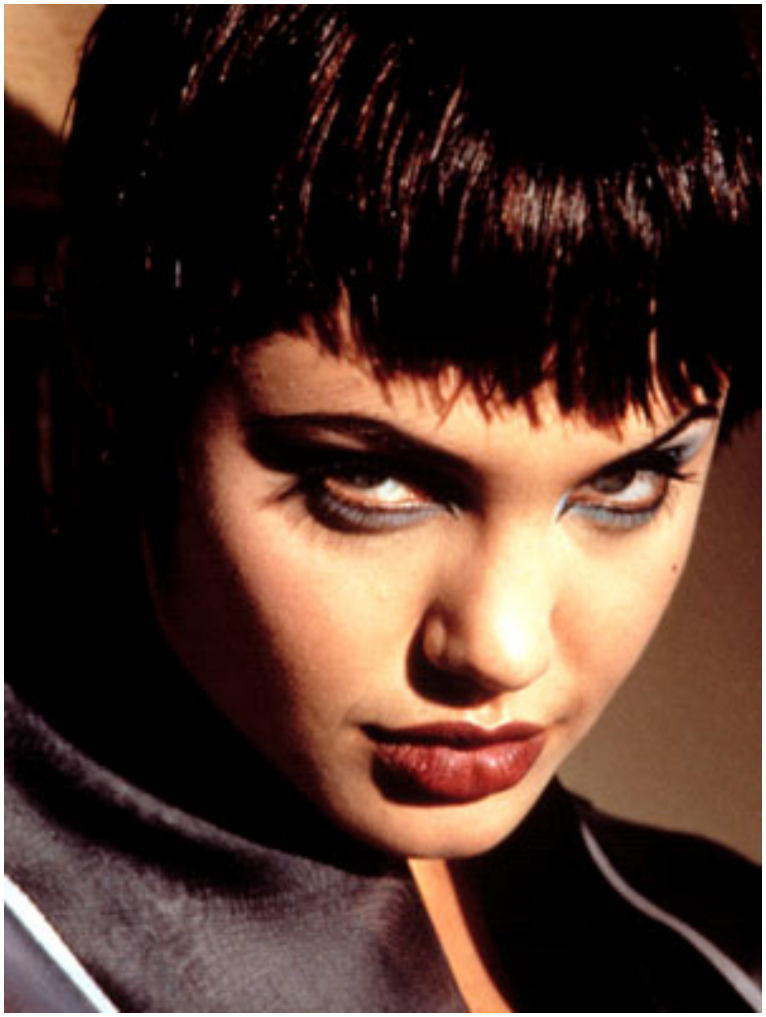

Hvad er hacking - introduktion

Teknisk hacking opsamling af hemmeligheder m.v.

Linger og demoer: kryptering, add-ons til browsere m.v.

prntationen er meget teknisk, men foredraget behr ikke at blive det ☺

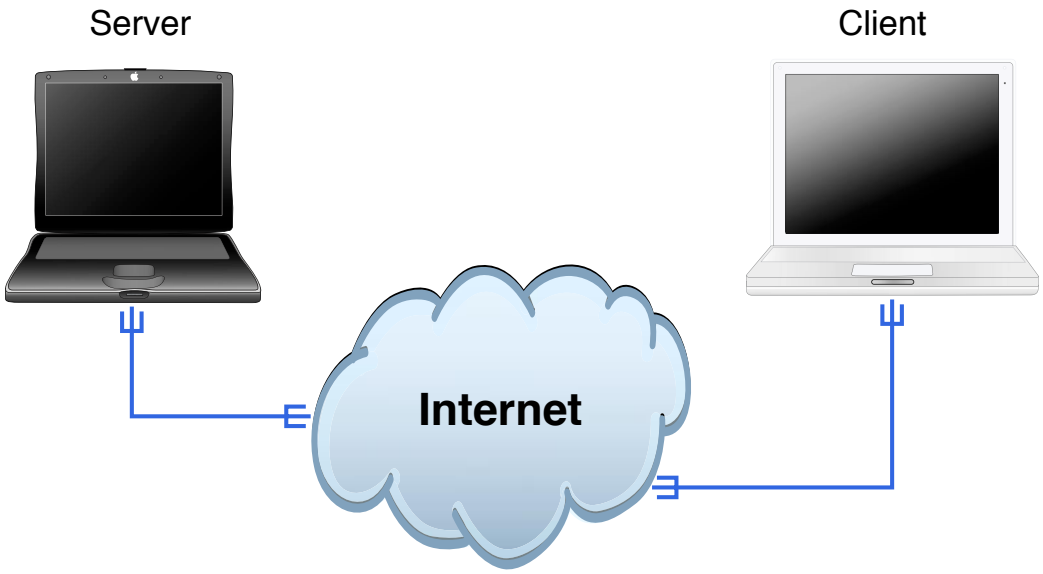
solido_networks_solid_RGB



http://www.imdb.com/title/tt0113243/ Hackers (1995)

# Internet today






Clients and servers

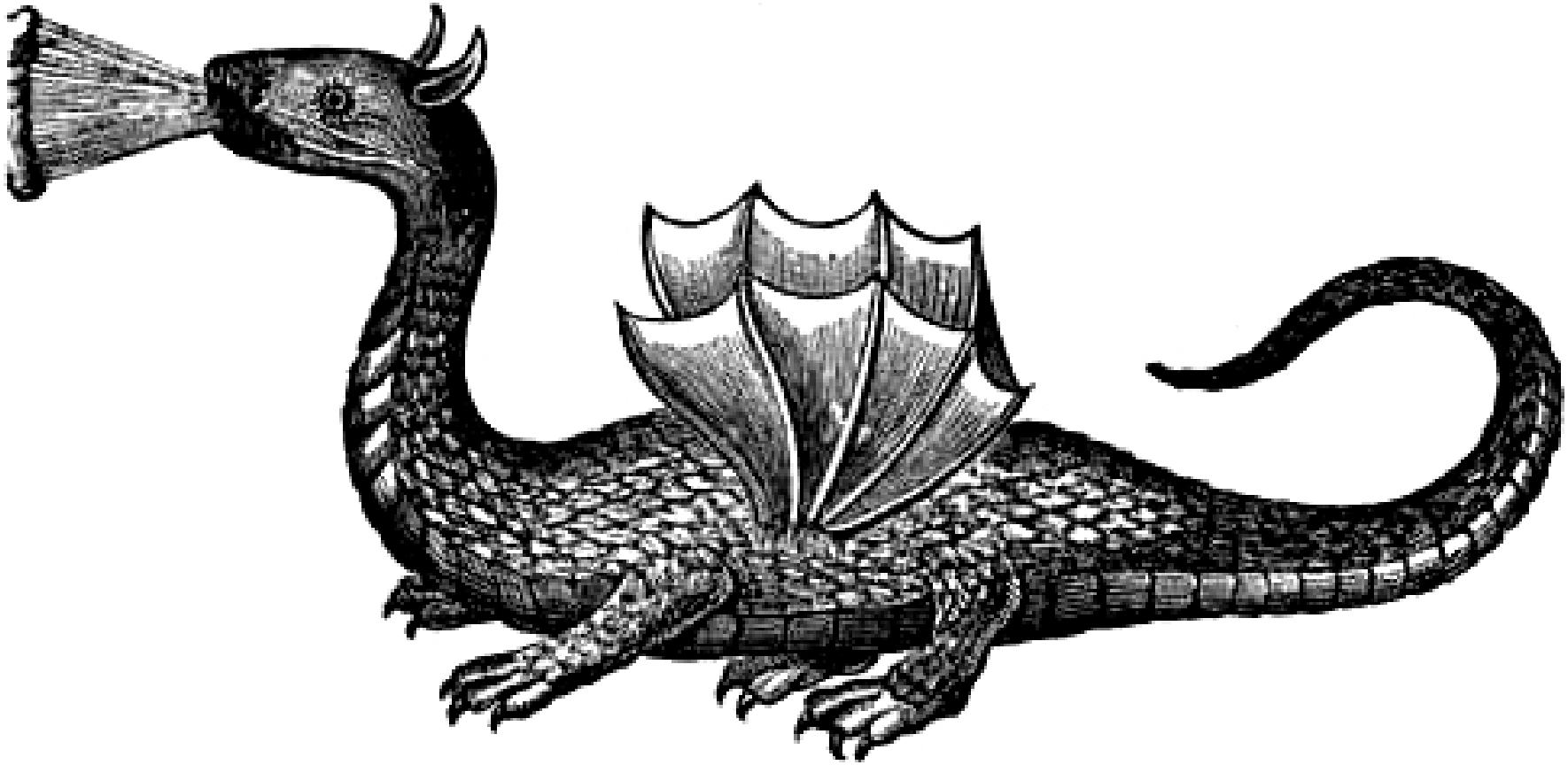
Rooted in academic networks

Protocols which are more than 20 years old, moved to TCP/IP in 1981

Trying to migrate to IPv6 - a lot of hacking opportunities here

# Internet - Here be dragons

solido_networks_solid_RGB

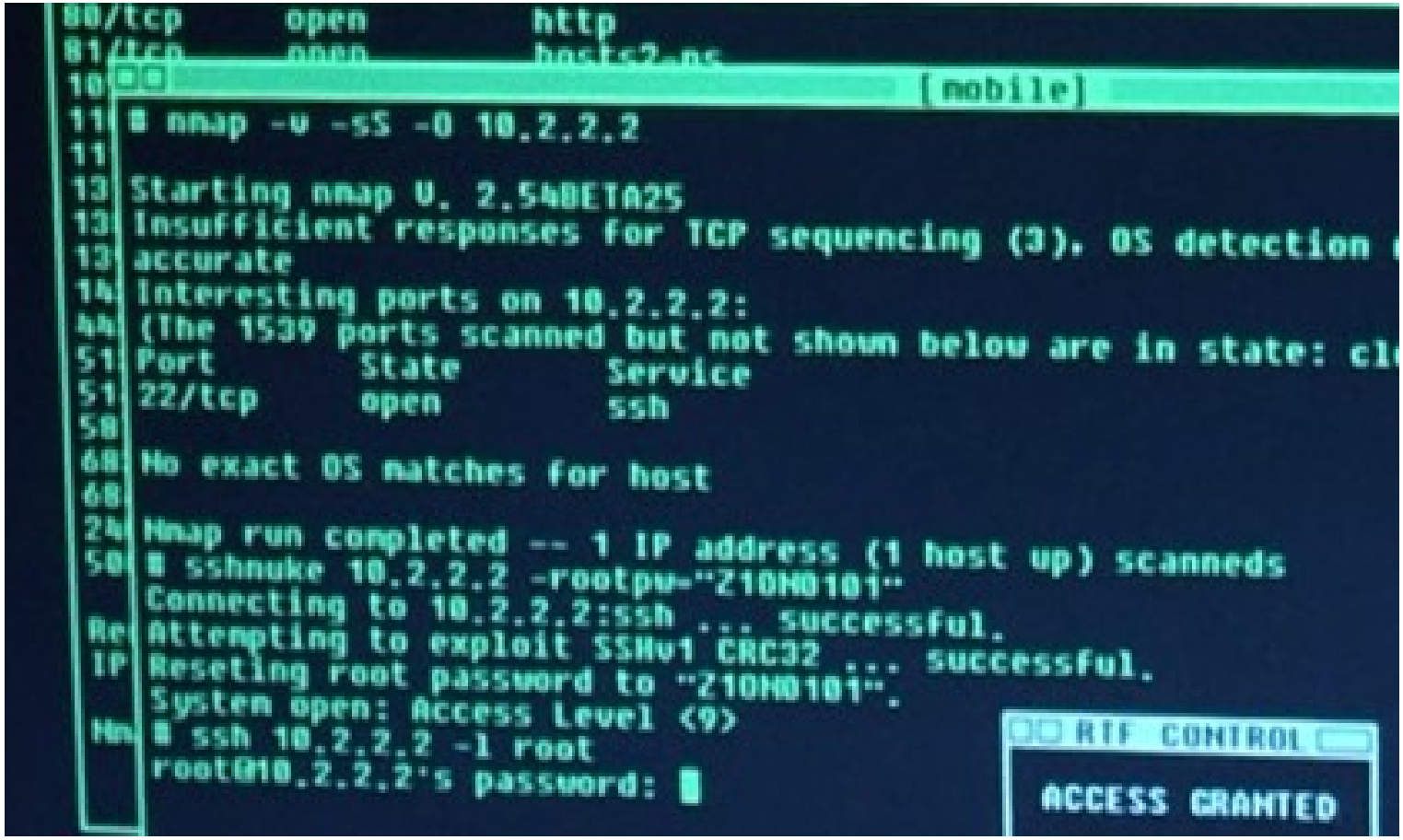


# Matrix style hacking anno 2003

solido_networks_solid_RGB

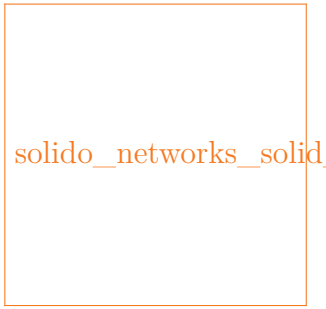
# Trinity breaking in






http://nmap.org/movies.html
Meget realistisk http://www.youtube.com/watch?v=51lGCTgqE_w

# Hacker - cracker




Det korte svar - drop diskussionen

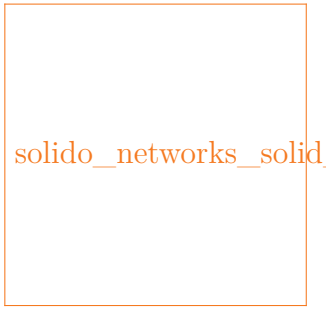
Det havde oprindeligt en anden betydning, men medierne har taget udtrykket til sig - og idag har det begge betydninger.

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

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

- 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

# Definition af hacking, oprindeligt




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

- En person, der nyder at unders detaljer i programmerbare systemer og hvordan man udvider deres anvendelsesmuligheder i modsing til de fleste brugere, der bare lr det mest nendige
- En som programmerer lidenskabligt (eller enddog fanatisk) eller en der foretrer at programmere frem-for at teoretiserer om det
- En ekspert i et bestemt program eller en der ofter arbejder med eller pet; som i "en Unixhacker".

Kilde: Peter Makholm, http://hacking.dk

Benyttes stadig i visse sammenhe se http://labitat.dk

# Internet er e standarder!

solido_networks_solid_RGB

We reject kings, presidents, and voting.
We believe in rough consensus and running code.
– The IETF credo Dave Clark, 1992.

Request for comments - RFC - er en serie af dokumenter

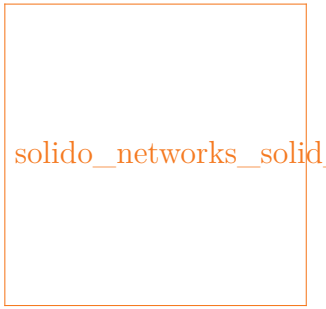
RFC, BCP, FYI, informational
de fte stammer tilbage fra 1969

res ikke, men fstatus Obsoleted nder udkommer en nyere version af en standard

Standards track:
Proposed Standard → Draft Standard → Standard

e standarder = nhed, ikke garanti for sikkerhed

# The Internet Worm 2. nov 1988




## Udnyttede fende sarheder

- buffer overflow i fingerd - VAX kode
- Sendmail - DEBUG
- Tillid mellem systemer: rsh, rexec, ...
- dige passwords

## Avanceret + camouflage!

- Programnavnet sat til 'sh'
- Brugte fork() til at skifte PID jligt
- password cracking med intern liste med 432 ord og /usr/dict/words
- Fandt systemer i /etc/hosts.equiv, .rhosts, .forward, netstat ...

## Lavet af Robert T. Morris, Jr.

## Medfe dannelsen af CERT, http://www.cert.org

# Hacking er magi

solido_networks_solid_RGB

Hacking ligner indimellem magi

# Hacking er ikke magi

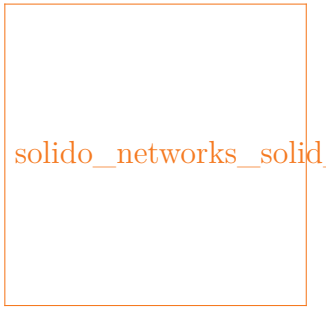
solido_networks_solid_RGB

Hacking krr blot lidt ninja-trng

# God sikkerhed

solido_networks_solid_RGB

# Hackervtr

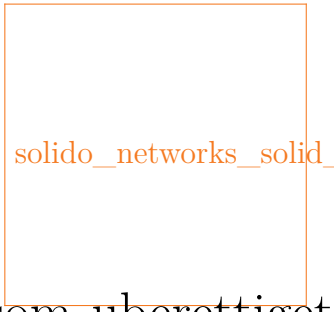



Der benyttes en del vtr:

- nmap - http://www.insecure.org portscanner
- Wireshark - http://http://www.wireshark.org/ avanceret netvssniffer
- OpenBSD - http://www.openbsd.org operativsystem med fokus pikkerhed
- BackTrack http://www.remote-exploit.org/backtrack.html
- Putty - http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html terminal emulator med indbygget SSH

Er det fornuftigt at man kan hente dem?

# Aftale om test af netv




Straffelovens paragraf 263 Stk. 2. Med b eller fsel indtil 6 mder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anltil elektronisk databehandling.

Hacking kan betyde:

- At man skal betale erstatning til personer eller virksomheder
- At man fkonfiskeret sit udstyr af politiet
- At man, hvis man er over 15 og bliver d for hacking, kan fn b - eller fselsstraf i alvorlige tilfe
- At man, hvis man er over 15 og bliver d for hacking, fen 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 Kriminalprntive R
- Frygten for terror har forstet ovenstde - sad v!

# DDoS udviklingen, januar 2010 rapporten

solido_networks_solid_RGB

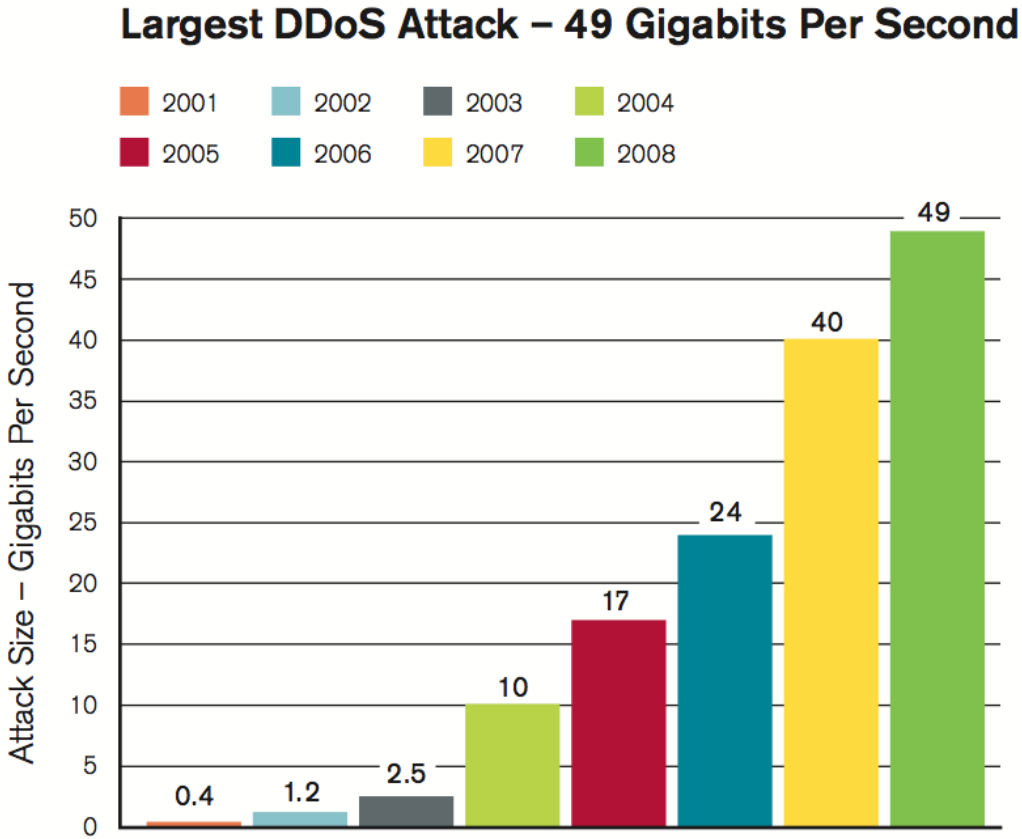



***Figure 1:*** *Largest DDoS Attack – 49 Gigabits Per Second*

Source: Arbor Networks, Inc.

Kilde: http://www.arbornetworks.com/report 2009 rapporten

# DDoS udviklingen, februar 2011

solido_networks_solid_RGB

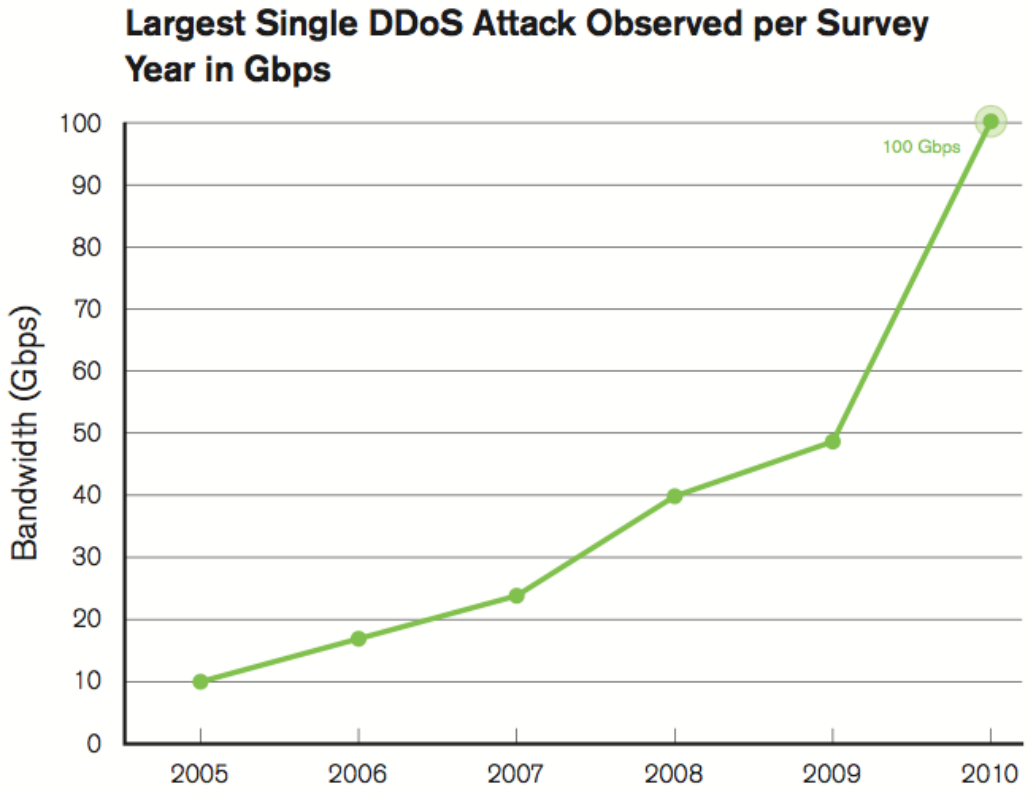



*Figure 1*
Source: Arbor Networks, Inc.

Kilde: http://www.arbornetworks.com/report 2010 rapporten

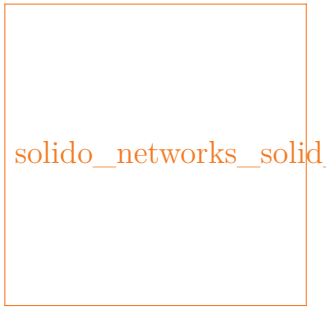
# Key findings

solido_networks_solid_RGB

- Application-Layer DDoS Attacks Are Increasing in Sophistication and Operational Impact
- Mobile/Fixed Wireless Operators Are Facing Serious Challenges to Maintaining Availability in the Face of Attacks
- Firewalls and IPS Devices Are Falling Short on DDoS Protection
- DNS Has Broadly Emerged as an Attack Target and Enabler
- Lack of Visibility into and Control over IPv6 Traffic Is a Significant Challenge
- Chronic Underfunding of Operational Security Teams
- Operators Continue to Express Low Confidence in the Efficacy of Law Enforcement
- Operators Have Little Confidence in Government Efforts to Protect Critical Infrastructure

Kilde: http://www.arbornetworks.com/report februar 2011

# Hacking rammer alle




Der er mange pointer at l fra de mange hacking historier

Social Engineering rockz! Uddannelse!

Alle er et m evt. som springbr ind til andre

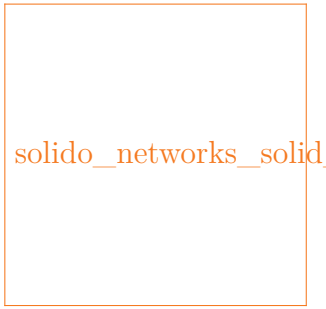
Anonymous er en flok forkde mnger? helte? egoer? l knyttet gruppe, tknyttet gruppe?

Hacktivism er okay, bare det rammer Scientology?

... flere pointer?

Hacking er ikke cool og koster mange resourcer!

# Moderne botnets




Botnets spreder sig ved at inficere sange systemer som muligt

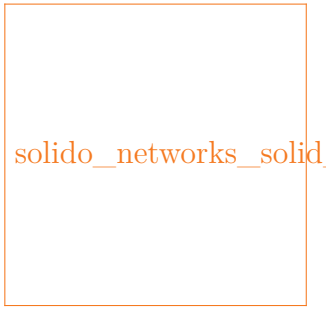
Botnets idag vokser gerne langsommere - ingen ny Code Red hastighedsrekord

Spreder sig via SMTP, HTTP, SMB, ... alle protokoller der kan overf data

Bannerkampagner og 3. parts kilder til elementer pin side?!

Nft der er kommet malware pystemet udvides med moduler

# Malware idag




Malware idag er sofistikeret

Modul opbygget

Benytter st kryptering til at sikre administrationen af inficerede computere

Benytter seneste sikkerhedshuller - 0 days til at sprede sig

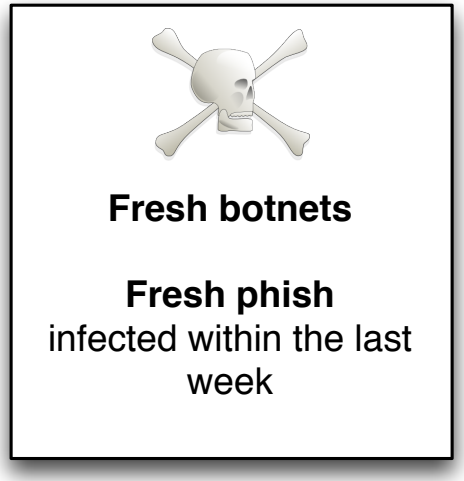
Benytter de seneste rootkit metoder til at holde sig skjult

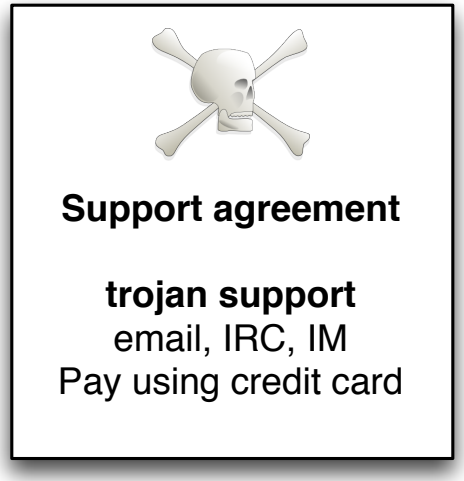
Muterer efter alle kendte metoder for at undgpdagelse

Larmer mindre end tidligere

# Botnets og malware ses med support



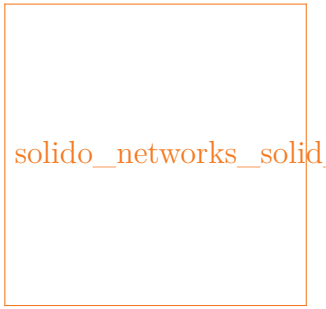

Malware programmr har l kundepleje

”Kdenne version og fratis opdateringer”

Lej vores botnet med 100.000 computere

http://www.version2.dk/artikel/breaking-nemid-hacket-31480

# Spamming as a service




BBC programmet Click underse mulighederne for at k sig adgang til et botnet

Lejede 22.000 computere og afprde skadevirkninger

Det virkede (desve) som forventet

Kilde: Marts 2009 BBC
http://news.bbc.co.uk/1/hi/programmes/click_online/7932816.stm

# Phishing - Receipt for Your Payment to mark561@bt....com

solido_networks_solid_RGB

Mark Willson
145 Church Lane East
Aldershot, Hampshire, GU11 3ST
United Kingdom

Important Note: Mark Willson has provided an Unconfirmed Address. If you are planning on shipping items to Mark Willson, please check the Transaction Details page of this payment to find out whether you will be covered by the PayPal Seller Protection Policy.

Note:

If you haven't authorized this charge ,click the link below to cancel transaction

Cancel Transaction:

https://www.paypal.com/cgi-bin/webscr/cgi-bin/webscr?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

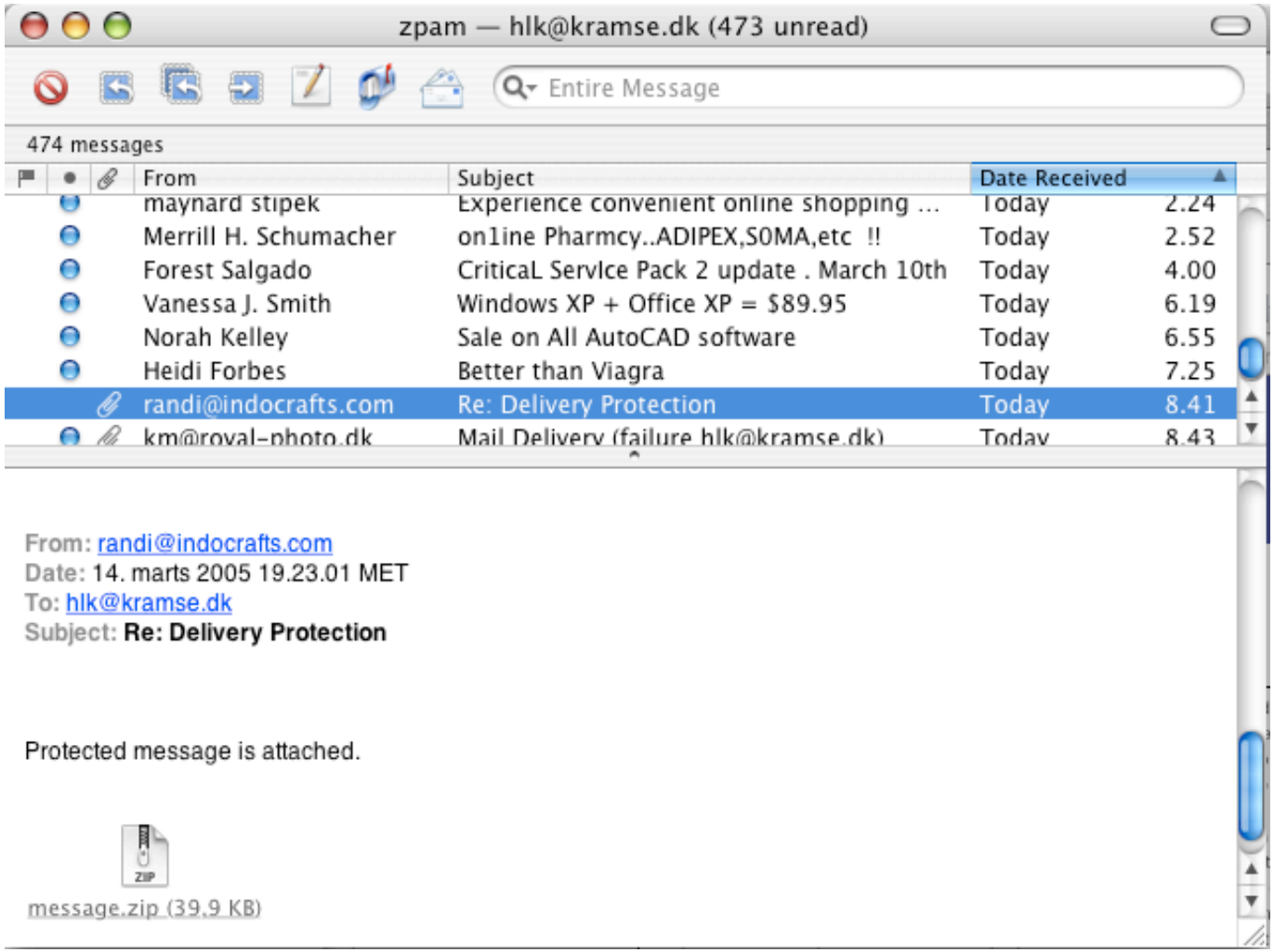
*SSL connection:
PayPal automatically encrypts your confidential information in transit from your computer to ours using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available)
---

http://paypal-co.uk.dt6.pl/?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

# Kan du selv genkende Phishing

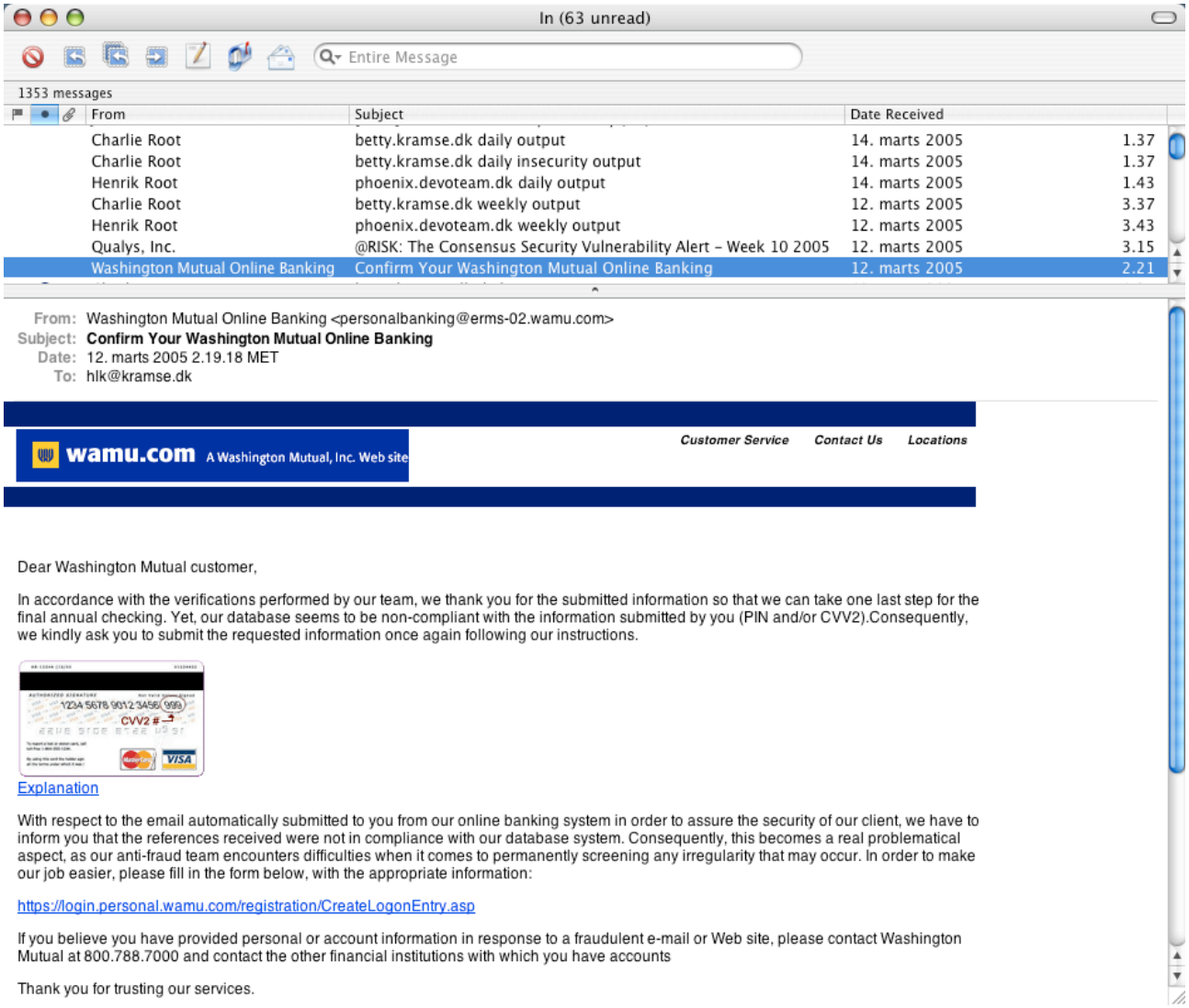
# Zip files?

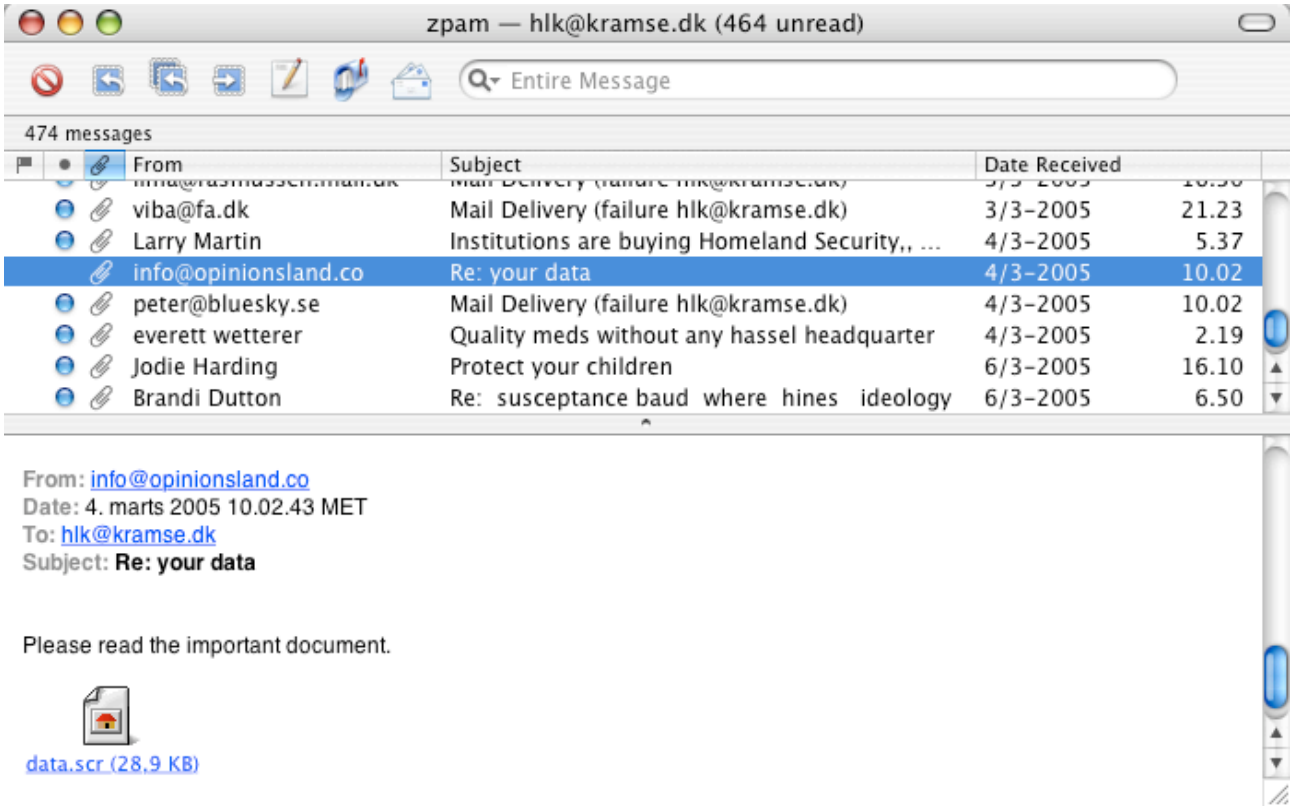
solido_networks_solid_RGB



# Money!

solido_networks_solid_RGB






SCR er screensaver files - programmer

# Sociale aspekter

solido_networks_solid_RGB


Fear, uncertainty and doubt http://en.wikipedia.org/wiki/Fear,_uncertainty_and_doubt

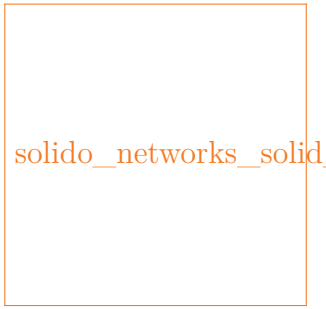
# Fremtiden - er success en risiko

solido_networks_solid_RGB

The Mobile Network in 2010 and 2011
Global mobile data traffic grew 2.6-fold in 2010, nearly tripling for the third year in a row. The 2010 mobile data traffic growth rate was higher than anticipated. Last year's forecast projected that the growth rate would be 149 percent. This year's estimate is that global mobile data traffic grew 159 percent in 2010.
...
Last year's mobile data traffic was three times the size of the entire global Internet in 2000. Global mobile data traffic in 2010 (237 petabytes per month) was over three times greater than the total global Internet traffic in 2000 (75 petabytes per month).
...
There will be 788 million mobile-only Internet users by 2015. The mobile-only Internet population will grow 56-fold from 14 million at the end of 2010 to 788 million by the end of 2015.

Kilde: Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010 - 2015

# Hholdte enheder

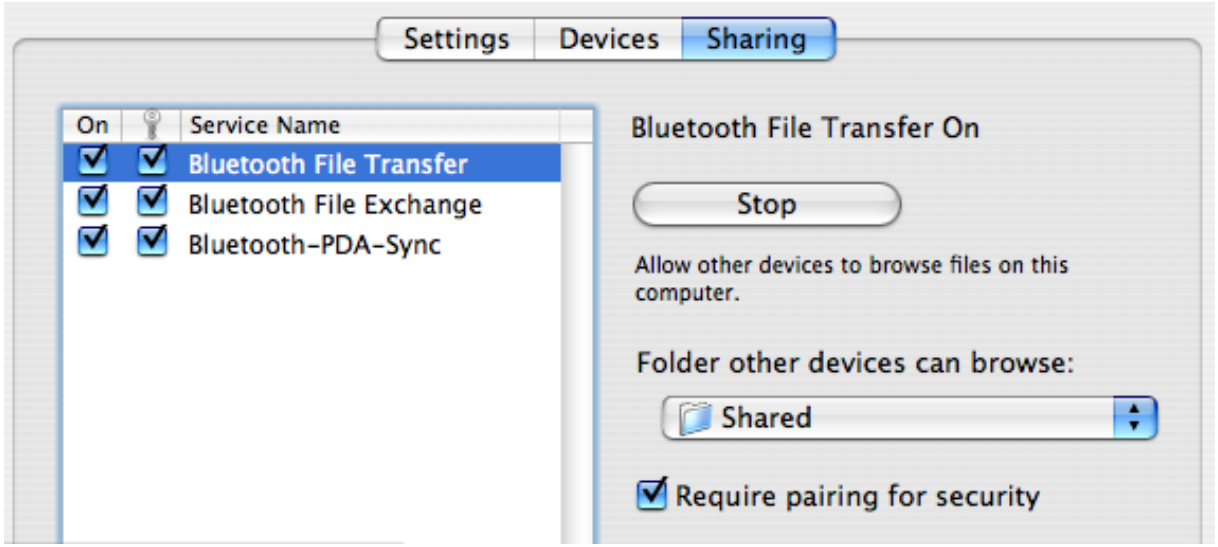



## Hvad kendetegner hholdte enheder

- sm kan typisk ligge i en lomme
- meget lille lager til rghed
- begret funktionalitet
- kan synkroniseres med en stationcomputer
- meget stor lagerkapacitet i moderne udgaver!
- udvidet funktionalitet
- viewer programmer til Word, Excel, PDF m.fl.
- alt er forbundet idag, typisk netv udover GPRS/telefoni

# Bluetooth sikkerhed

solido_networks_solid_RGB




- Bluetooth - slet fra nI ikke bruger det
- Slet fra i jeres bil, hvis I ikke har planer om at bruge det!
- Gjeres bedste for at slryptering til
- Tillad kun adgang med pairing
- S for kun at tilbyde et minimum af services over bluetooth

# Aflytning af biler - Car Whisperer

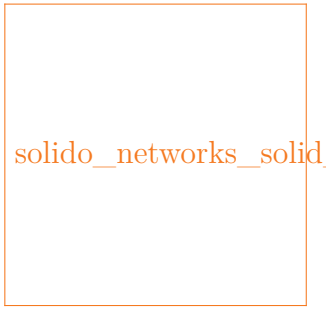
solido_networks_solid_RGB


Bluetooth kits til biler bruger passkey som '0000' or '1234'

- Man kan hente programmer pnternet
- Man kan bruge en retningsbestemt antenne
- Man kan lytte med pamtaler i bilerne

Kilde:
http://trifinite.org/blog/archives/2005/07/introducing_the.html

# Problemer med smart phones/PDA




Kan gemme mange data - hvor fomme er data

- Kalender
- Kontakter
- Opgaver - To Do listen

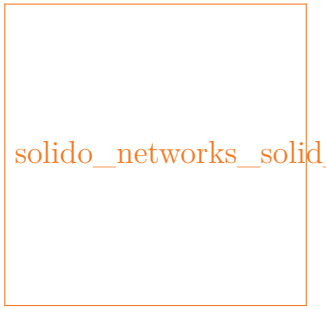
Nem backup af data - nemt at stj alle oplysninger!

- flyt data applikationen pokia - data flytning uden SIM kort
- sikkerhedskopi til MMC kort - nen alle data kan overfs $<$ 1 minut

Adgang ind til virksomheden - via wireless?

- Genbruge loginoplysninger fra PDA og koble en laptop petvet?

# Gode rtil jer




Brug teknologien

Lteknologien at kende - lmanualen!

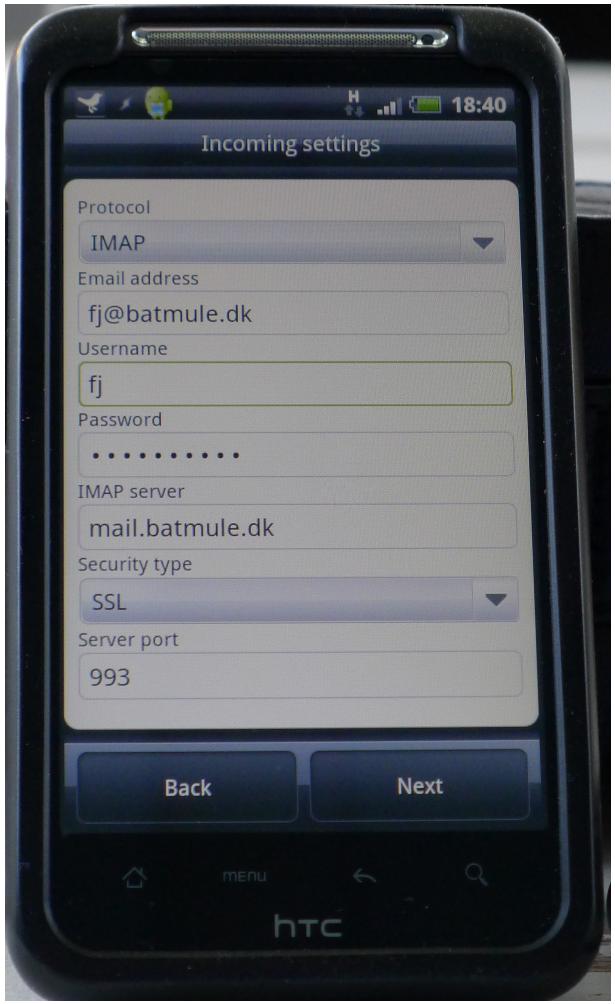
T pomheden af data I gemmer og overfr

- Sling fra som I ikke bruger
- Slluetooth fra nI ikke bruger den
- Opdater softwaren pnheden
- Slryptering til hvor I kan: IMAPS, POP3S, HTTPS og over bluetooth
- Brug lkode fremfor tastaturluden kode pobiltelefonen
- Stol ikke for meget pingertryksaflre

# SSL/TLS (1)

solido_networks_solid_RGB

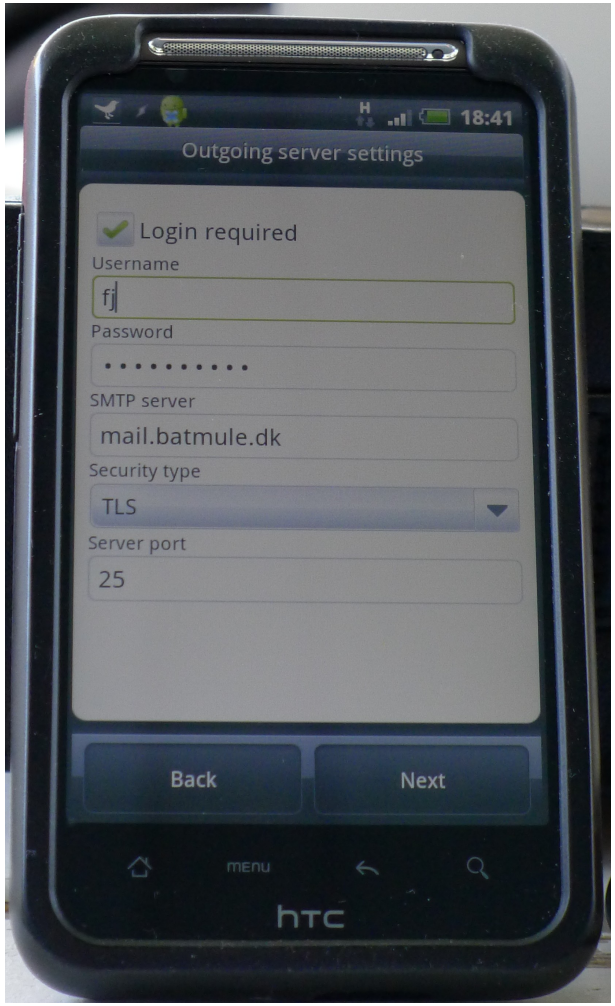
Istedet for POP3 brug POP3s, Istedet for IMAP brug IMAPs



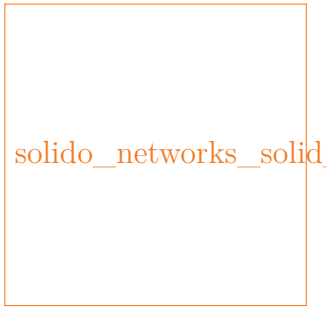
# SSL/TLS (2)

solido_networks_solid_RGB

SMTP kan erstattes med SMTP+TLS



# Tyveri - behaven og lufthavnen




Mange glemmer at l bilen nde skal hente b - travlhed

Mange lader deres baggage v ubevogtet i lufthavnen - sult tt

Mange lader deres bare stontoret - frit fremme

Mange forlader deres bare pt bord under konferencer

... simpelt tyveri er ofte muligt

eller er det industrispionage?

# Er dine data sikre

solido_networks_solid_RGB

Lorem ipsum dolor sit amet, consectetur adipiscing elit, set eiusmod tempor incidunt et labore et dolore magna aliquam. Ut enim ad minim veniam, qu nostrud exerc. Irure dolor in reprehend incididunt ut labore et dolore magna aliqua. Ut enim ad minim v ostrud exercitation ullamco la si 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 pa 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 nonor et imper r et, conse ing 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.

Stjt laptop

Slettede eller lagte data

- og hvordan sletter man data? Huskede du mini SD kortet med dine private billeder?

# Pause

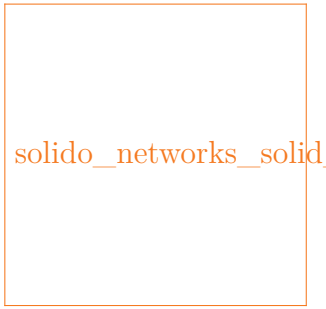
solido_networks_solid_RGB

Er det tid til en lille pause?

# Teknisk hvad er hacking

solido_networks_solid_RGB

# buffer overflows et C problem

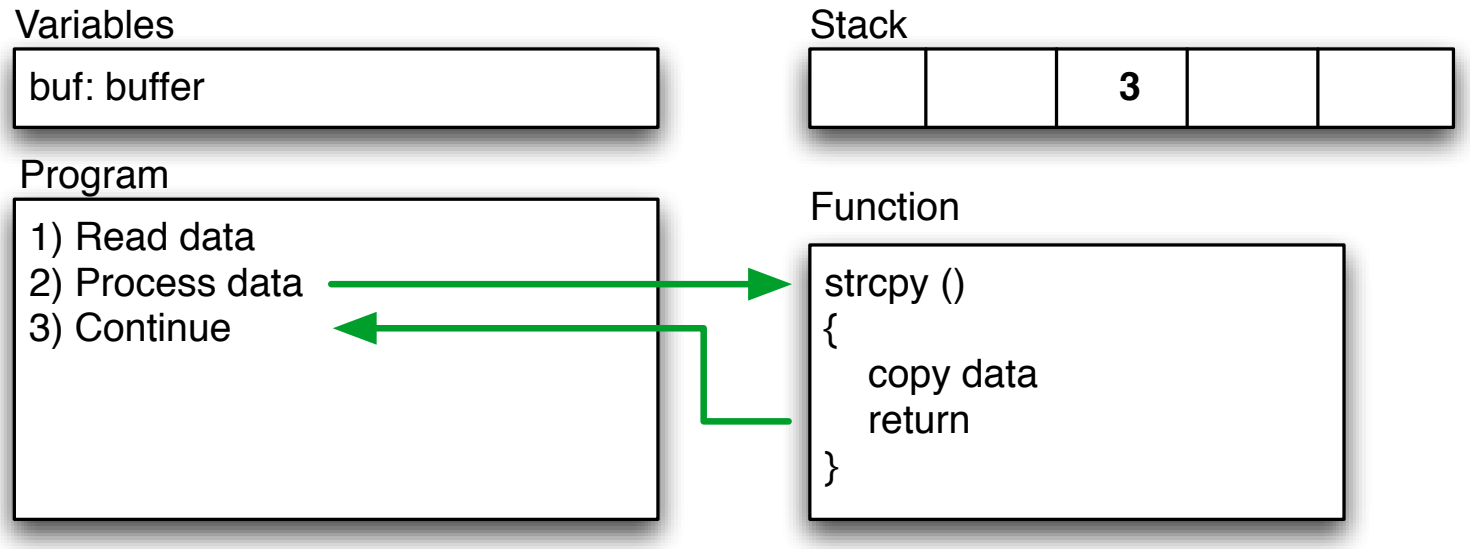



Et buffer overflow er det der sker nman skriver flere data end der er afsat plads til i en buffer, et dataomr. Typisk vil programmet ged, men i visse tilfe kan en angriber overskrive returadresser for funktionskald og overtage kontrollen.

Stack protection er et udtryk for de systemer der ved hj 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.

# Buffer og stacks

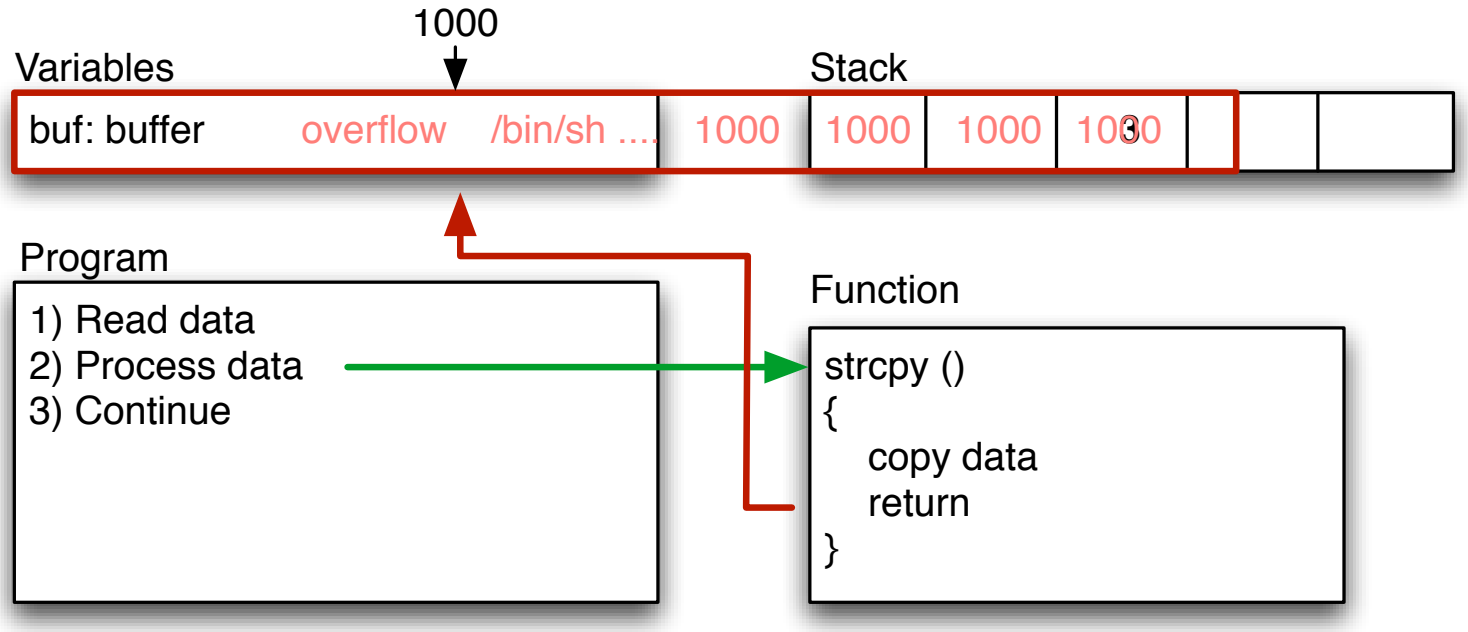





```
main(int argc, char **argv)
{       char buf[200];
        strcpy(buf, argv[1]);
        printf("%s\n",buf);
}
```

# Overflow - segmentation fault



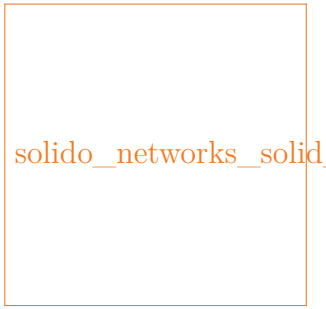



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

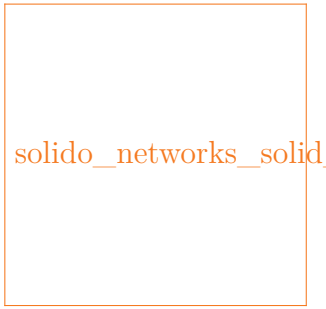
# Exploits




```
$buffer = "";
$null = "\x00";
$nop = "\x90";
$nopsize = 1;
$len = 201; // what is needed to overflow, maybe 201, maybe more!
$the_shell_pointer = 0xdeadbeef; // address where shellcode is
# Fill buffer
for ($i = 1; $i < $len;$i += $nopsize) {
    $buffer .= $nop;
}
$address = pack('l', $the_shell_pointer);
$buffer .= $address;
exec "$program", "$buffer";
```

Demo exploit in Perl

# Hvordan finder man buffer overflow, og andre fejl




Black box testing

Closed source reverse engineering

White box testing

Open source betyder man kan l og analysere koden

Source code review - automatisk eller manuelt

Fejl kan findes ved at pr sig frem - fuzzing

Exploits virker typisk mod specifikke versioner af software

# The Exploit Database - dagens buffer overflow




http://www.exploit-db.com/

## What is it?

The Metasploit Framework is a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers world-wide. The framework is written in the Ruby programming language and includes components written in C and assembler.

Idag findes der samlinger af exploits som milw0rm

Udviklingsvtrne til exploits er idag meget raffinerede!

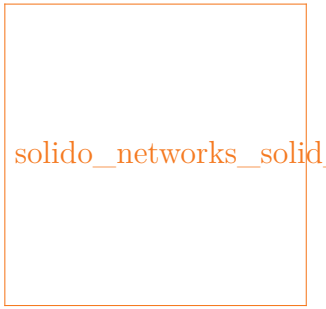
http://www.metasploit.com/

http://www.fastandeasyhacking.com/ Armitage GUI til Metasploit

http://www.offensive-security.com/metasploit-unleashed/

# Forudsinger



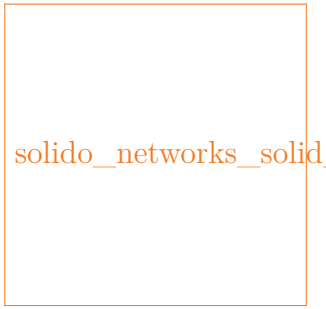

Bem: alle angreb har forudsinger for at virke

Et angreb mod Telnet virker kun hvis du bruger Telnet

Et angreb mod Apache HTTPD virker ikke mod Microsoft IIS

Kan du bryde kn af forudsinger har du vundet!

# Eksempler porudsinger




Computeren skal v tt

Funktionen der misbruges skal v sl til

Executable stack

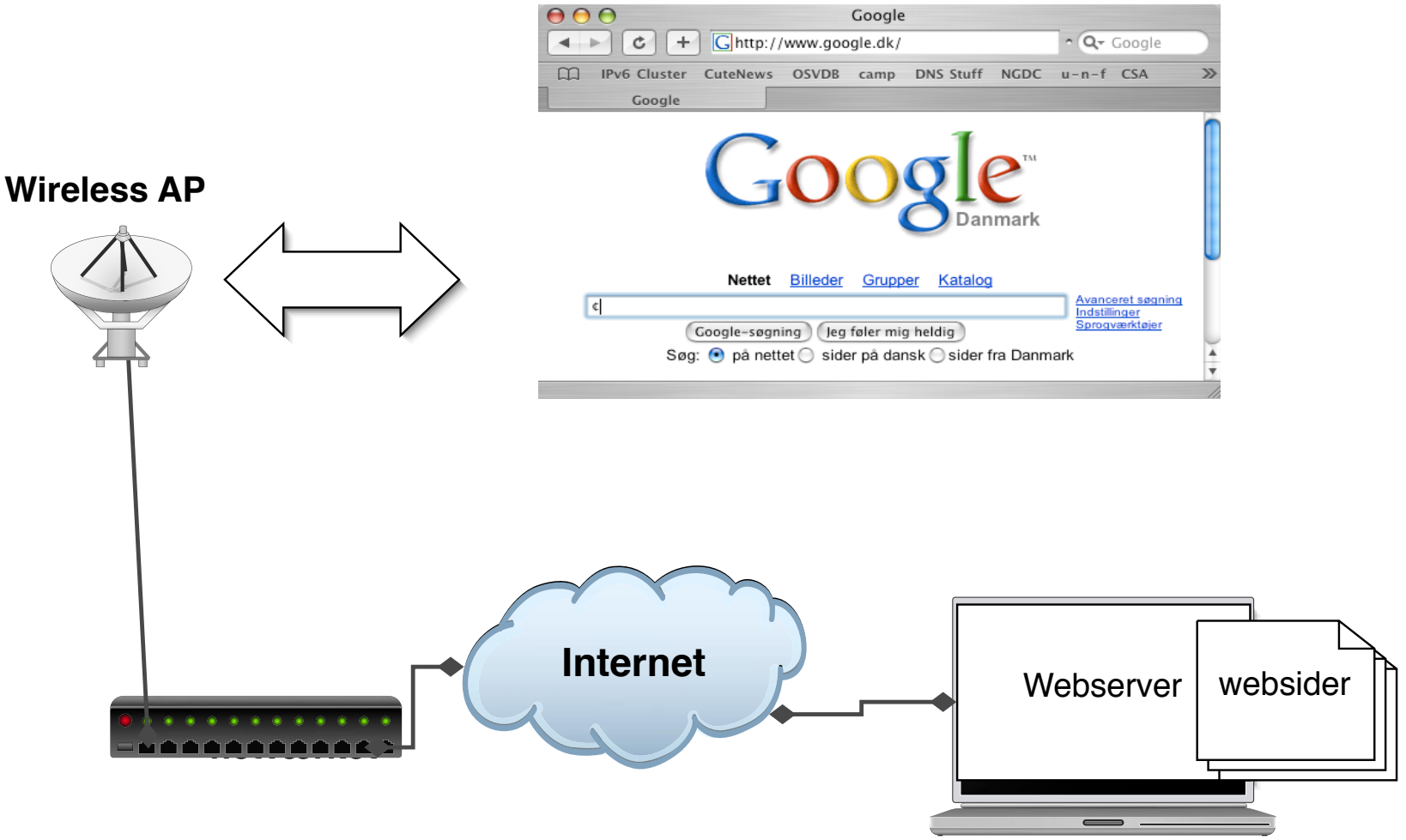
Executable heap

Fejl i programmet

alle programmer har fejl

# Normal wireless brug





# BackTrack 5 og sniffer programmer

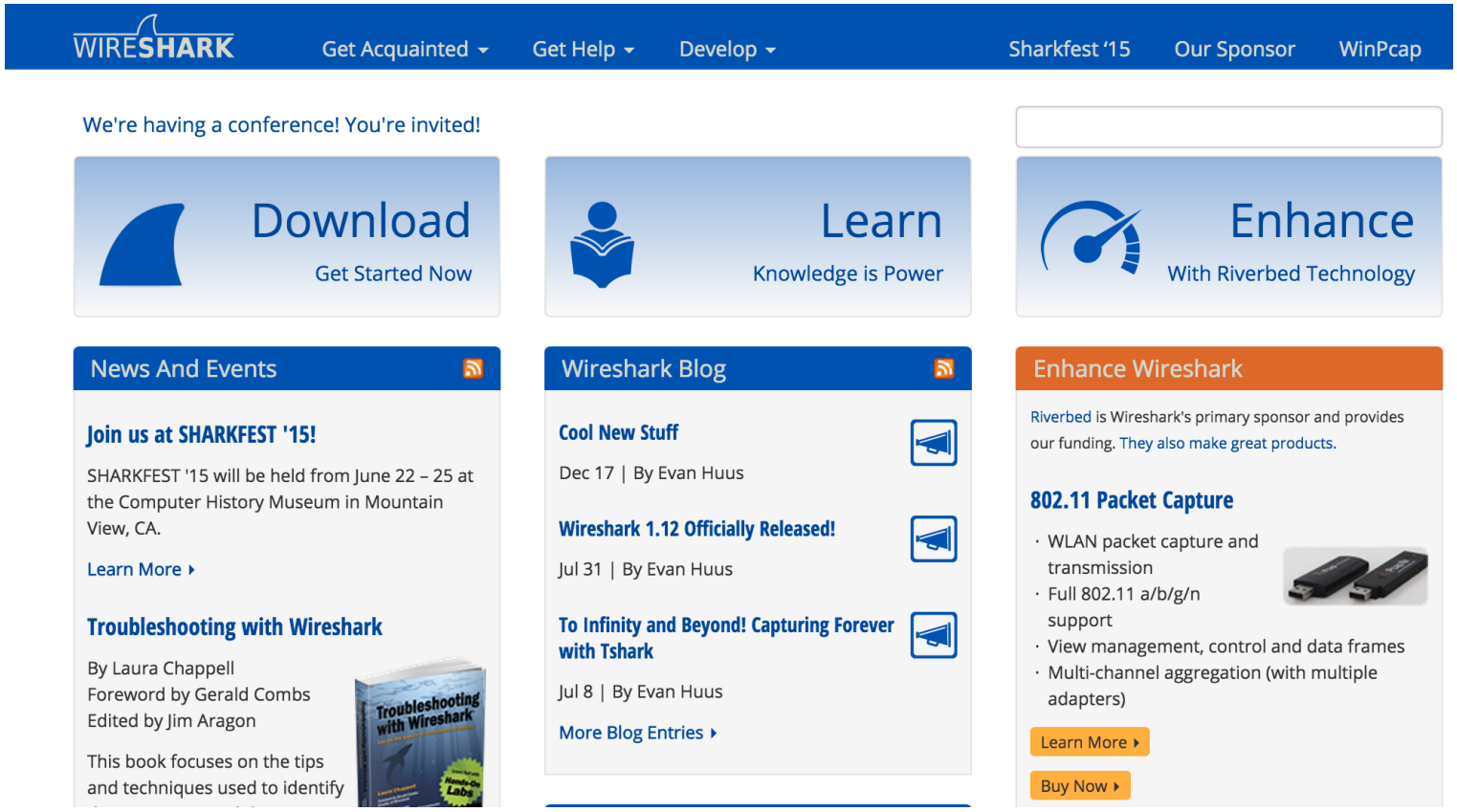
solido_networks_solid_RGB


Wireshark - http://www.wireshark.org avanceret netvssniffer
bruger vi til at sniffe, vi bruger Wireshark til prim demo, ner Ettercap osv.

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

# Wireshark - grafisk pakkesniffer

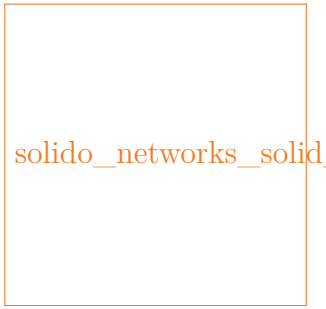
solido_networks_solid_RGB




http://www.wireshark.org

b til Windows og UNIX, tidligere kendt som Ethereal

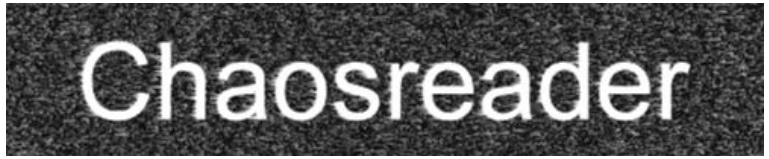
# Programhygiejne!




Download, installer - k - farligt!

Sn gs det:

- download program OG signaturfil/MD5
- verificer signatur eller MD5
- installer
- brug programmet
- hold programmet opdateret!




## 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 |

Med adgang til et netvsdump kan man l det med chaosreader

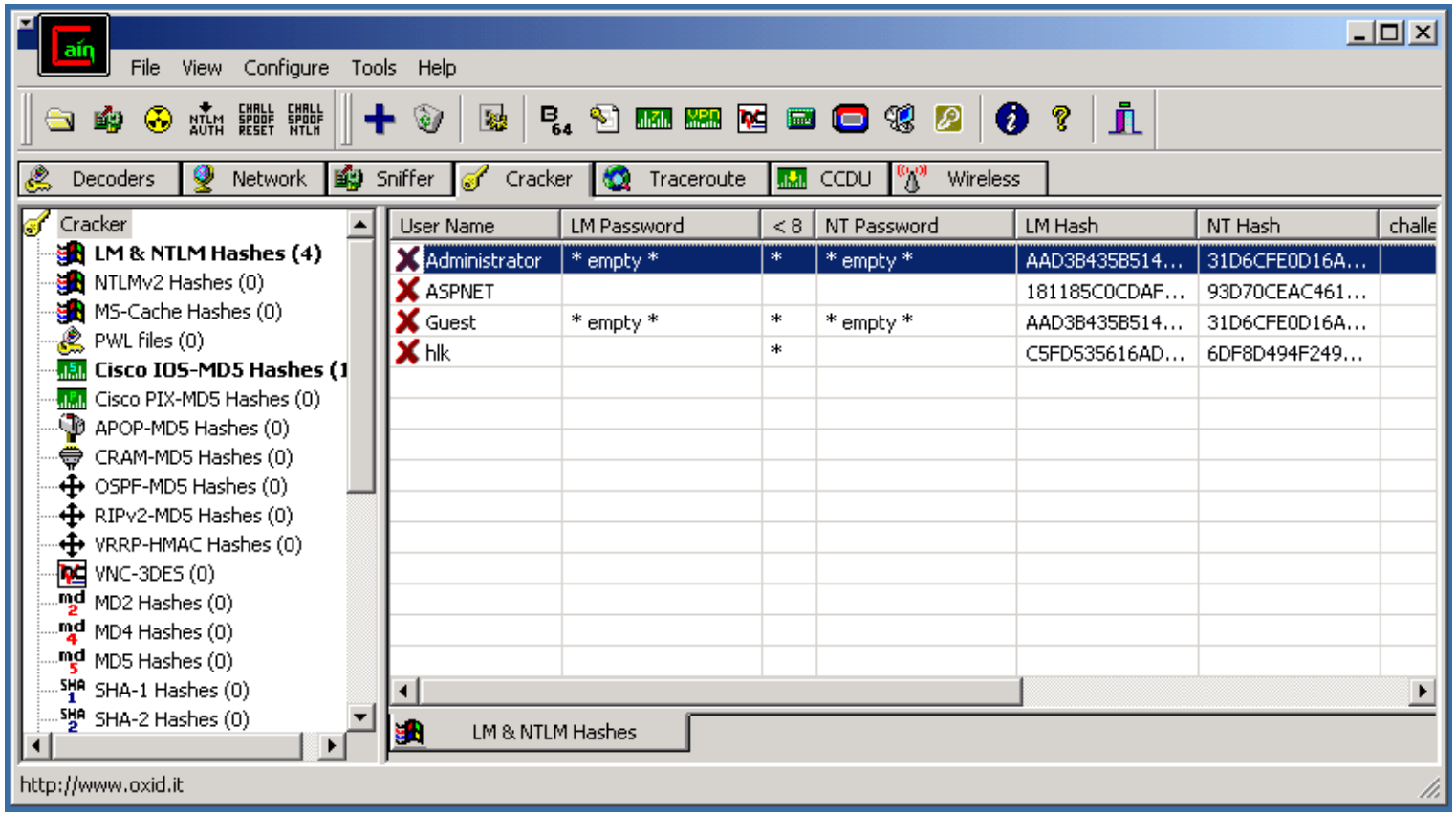
Output er HTML med oversigter over sessioner, billeder fra datastren osv.

http://chaosreader.sourceforge.net/

# Cain og Abel

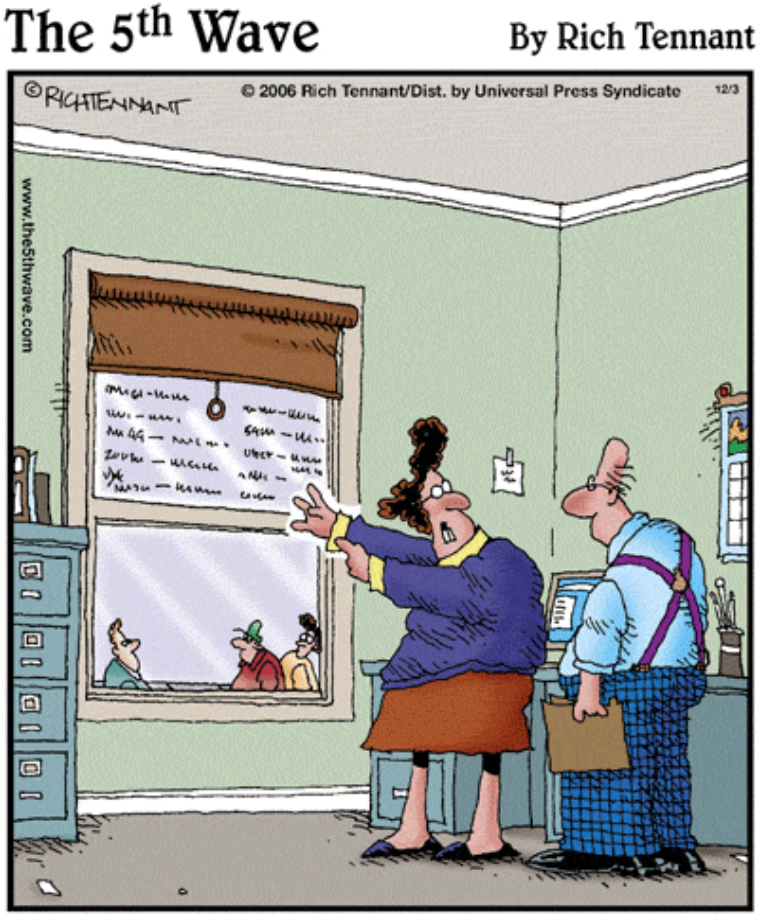





Cain og Abel anbefales ofte istedet for l0phtcrack http://www.oxid.it

# Opbevaring af passwords

solido_networks_solid_RGB




"Don't be silly — of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."

# Pause

solido_networks_solid_RGB

Er det tid til en lille pause?

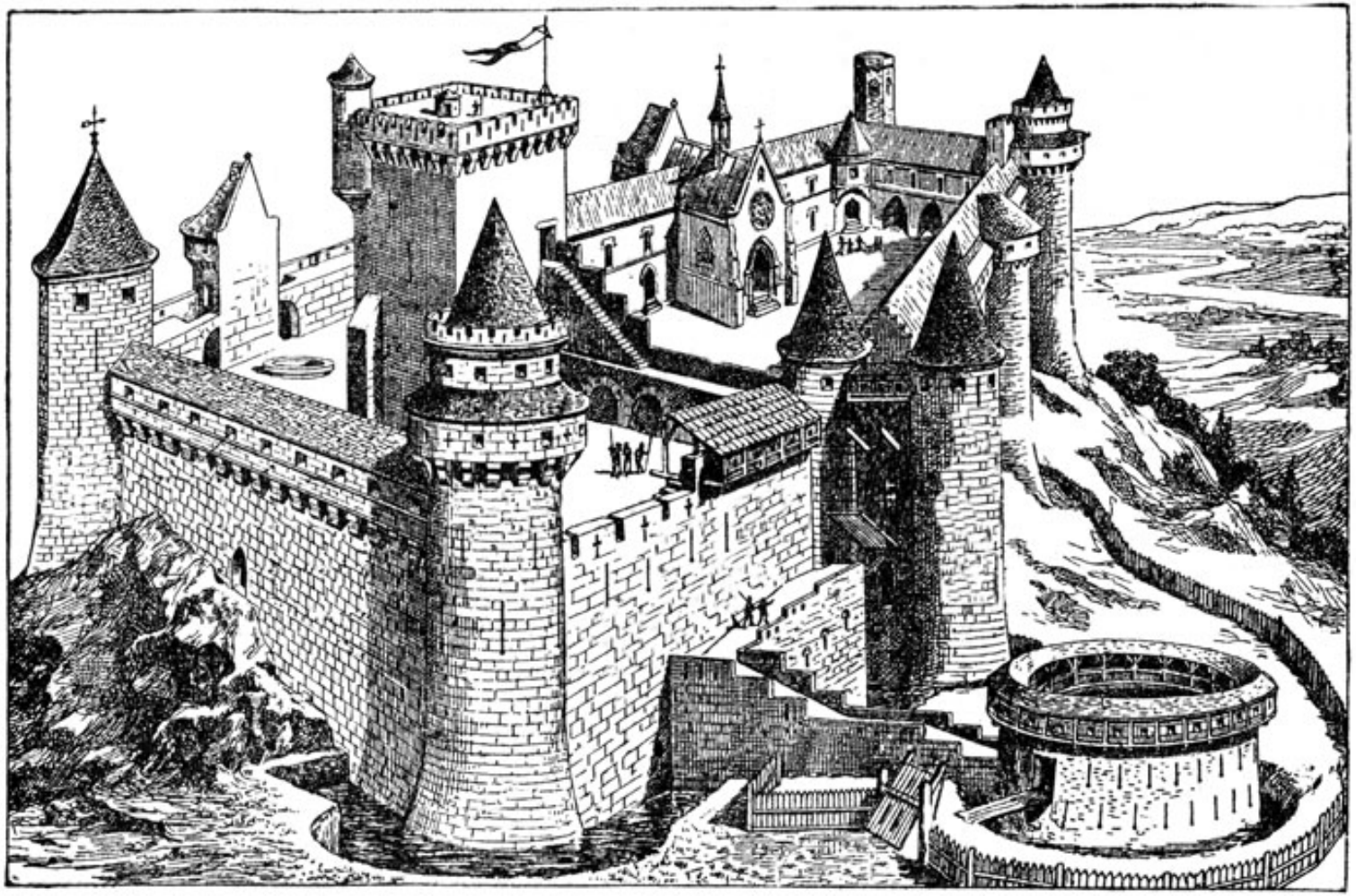
# What to do?

solido_networks_solid_RGB


What do we do?

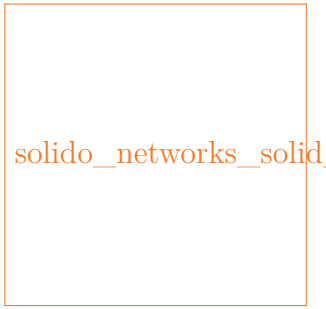
# Enhance and secure runtime environment

solido_networks_solid_RGB



Sidste chance er pfviklingstidspunktet

# Gode operativsystemer




Nyere versioner af Microsoft Windows, Mac OS X og Linux distributionerne inkluderer:

- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- Randomization of parameters stack gap m.v.

V derfor hellere:

- Windows 7, end Windows Xp
- Mac OS X 10.7 fremfor 10.6
- Linux sikkerhedsopdateringer, sig ja nde kommer

Det samme ger for serveroperativsystemer

NB: meget fmbedded systemer har beskyttelse!

# Flashback

solido_networks_solid_RGB

## Adobe Flash problems, player security issues & exploits - 2011

**Google Chrome offers to help stop Flash security problems** - March 2011

Google have extended their flash security sandbox to allow Adobe flash to take advantage of it. Google have also enhanced plug-in security by notifying the user of out-of-date plug-ins that may cause vulnerabilities.

**Flash security vulnerabilities affects Microsoft Excel** - March 2011

A flash security issue is currently being exploited by hackers by embedding malicious SWF files into Microsoft Excel spreadsheets. These are then emailed to unsuspecting users. All major OS's are affected by this flash security flaw.

**USB flash security compromized by major design flaw** - February 2011

Secure flash drives manufactured by some of the big brand flash memory-makers can be sent an 'unlock' flag to the devices which makes them unlock without requiring the password. The system is inherently insecure because when the secure flash drive software authenticates the supplied password it sends an 'unlock' flag to the drive (a common 'conditional jump'), which can be patched to unlock the device.

**Adobe flash security sandbox bypassed** - January 2011

Adobe flash player security has been bypassed by a security researcher who used a file request to a network machine. Adobe flash problems were meant to be minimized by use of the sandbox but the security researcher detailed how this could be easily bypassed by a malicious person.

Kilde: http://www.locklizard.com/adobe-flash-security.htm

# Drive-by download

From Wikipedia, the free encyclopedia

**Drive-by download** means three things, each concerning the unintended download of computer software from the Internet:

1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet). This is usually caused by poor security design[*clarification needed*]. The user should not be frequently asked to accept security-critical decisions, often with very limited knowledge and within limited time.
2. Any download that happens without a person's knowledge.
3. Download of spyware, a computer virus or any kind of malware that happens without a person's knowledge.

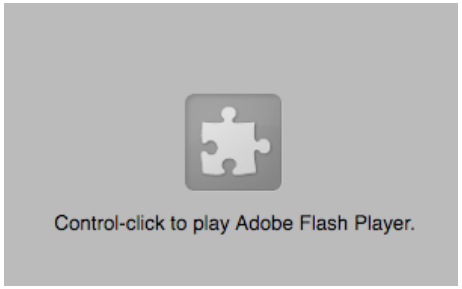
Kan vi undv Flash og PDF?

Kilde: http://en.wikipedia.org/wiki/Drive-by_download

# Flash blockers

solido_networks_solid_RGB




Safari http://clicktoflash.com/

Firefox Extension Flashblock

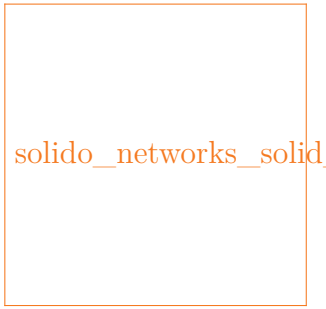
Chrome extension called FlashBlock

Internet Explorer 8: IE has the Flash block functionality built-in so you don't need to install any additional plugins to be able to block flash on IE 8.

FlashBlock for Opera 9 - bruger nogen Opera mere?

FlashBlockere til iPad? iPhone? Android? - hvorfor er det ikke default?

# Do NOT USE FTP




File Transfer Protocol - filoverfler

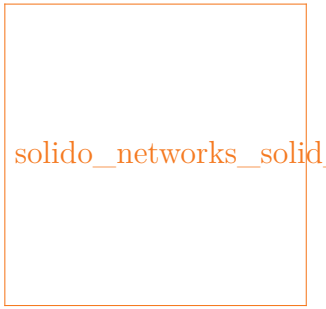
FTP bruges istil:

- FTP - drivere, dokumenter, rettelser - Windows Update? er enten HTTP eller FTP
- Opdatering af websites
- Overfel af data mellem virksomheder
- Serveren er indbygget i de fleste serveroperativsystemer

FTP sender i klartekst
USER brugernavn og
PASS hemmeligt-kodeord

Gode protokoller - men hvad er en protokol overhovedet

# Postservere til klienter




Nvi skal hente post sker det typisk med POP3 eller IMAP

- POP3 Post Office Protocol version 3 RFC-1939
- Internet Message Access Protocol (typisk IMAPv4) RFC-3501

Forskellen mellem de to er at man typisk med POP3 henter posten, hvor man med IMAP lader den ligge perveren

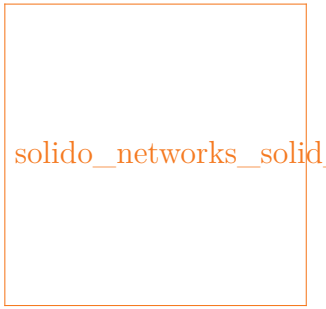
POP3 er bedst hvis kun en klient skal hente

IMAP er bedst hvis du vil tilgin post fra flere systemer

Jeg bruger selv IMAPS, IMAP over SSL kryptering - idet kodeord ellers sendes i klartekst

SMTP bruges til at sende mail mellem servere

# POP3 - e-mail i Danmark




POP3 sender brugernavn og kodeord i klartekst - ligesom FTP

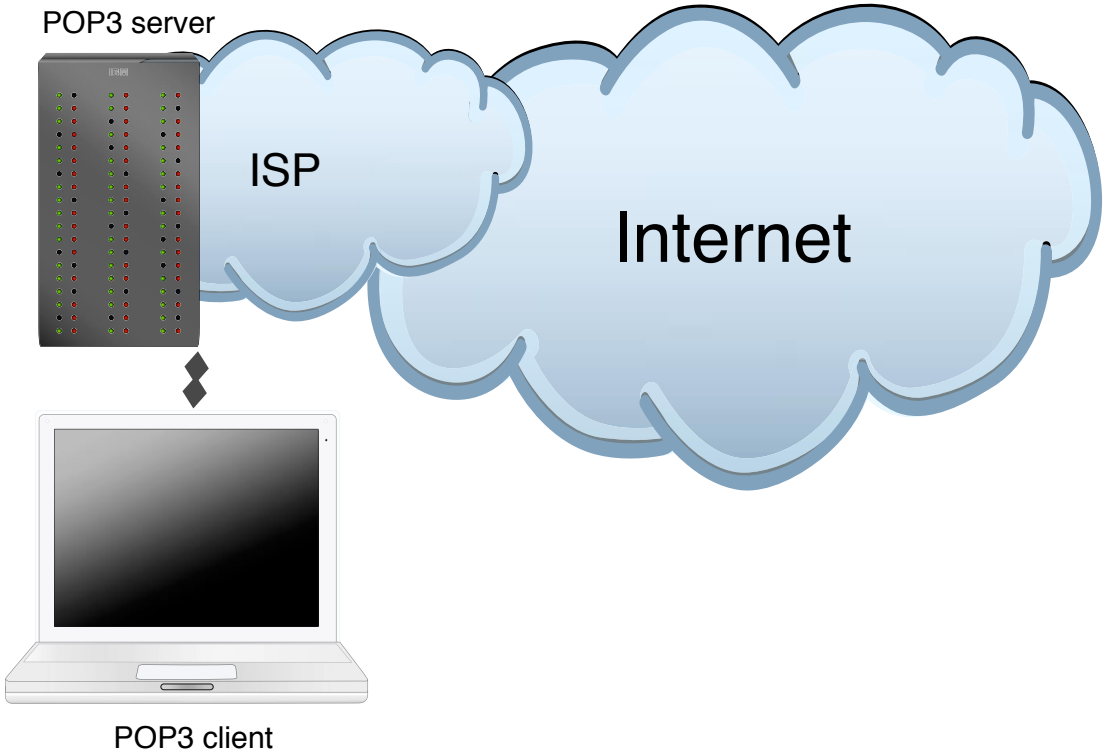
bruges dagligt af nen alle privatkunder

alle internetudbydere og postudbydere tilbyder POP3

der findes en variant, POP3 over SSL/TLS

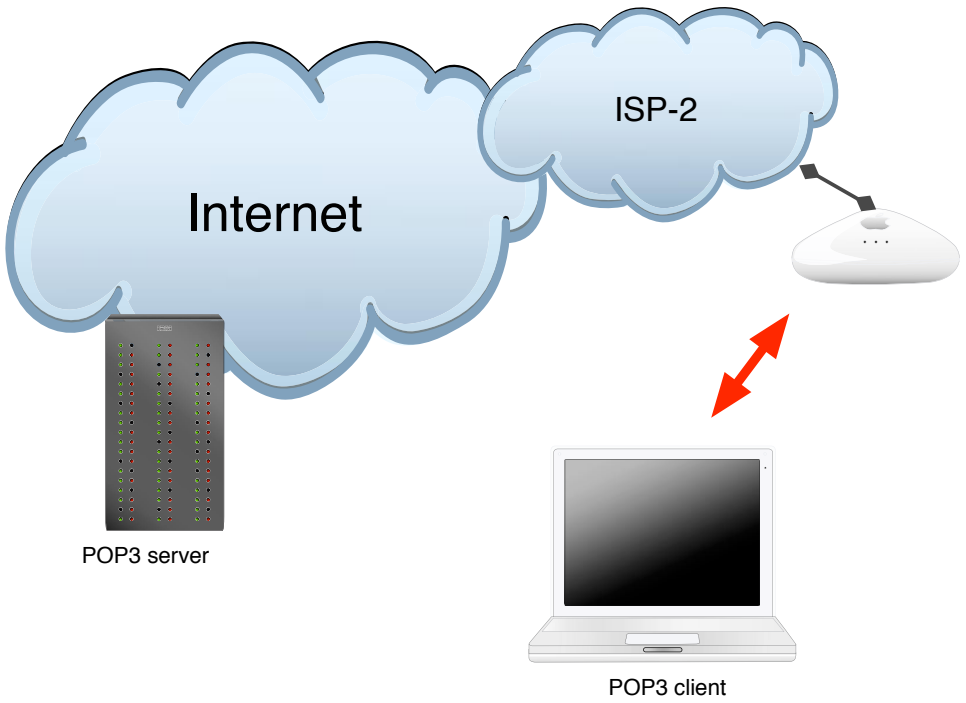
# POP3 i Danmark






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

# POP3 i Danmark - tr



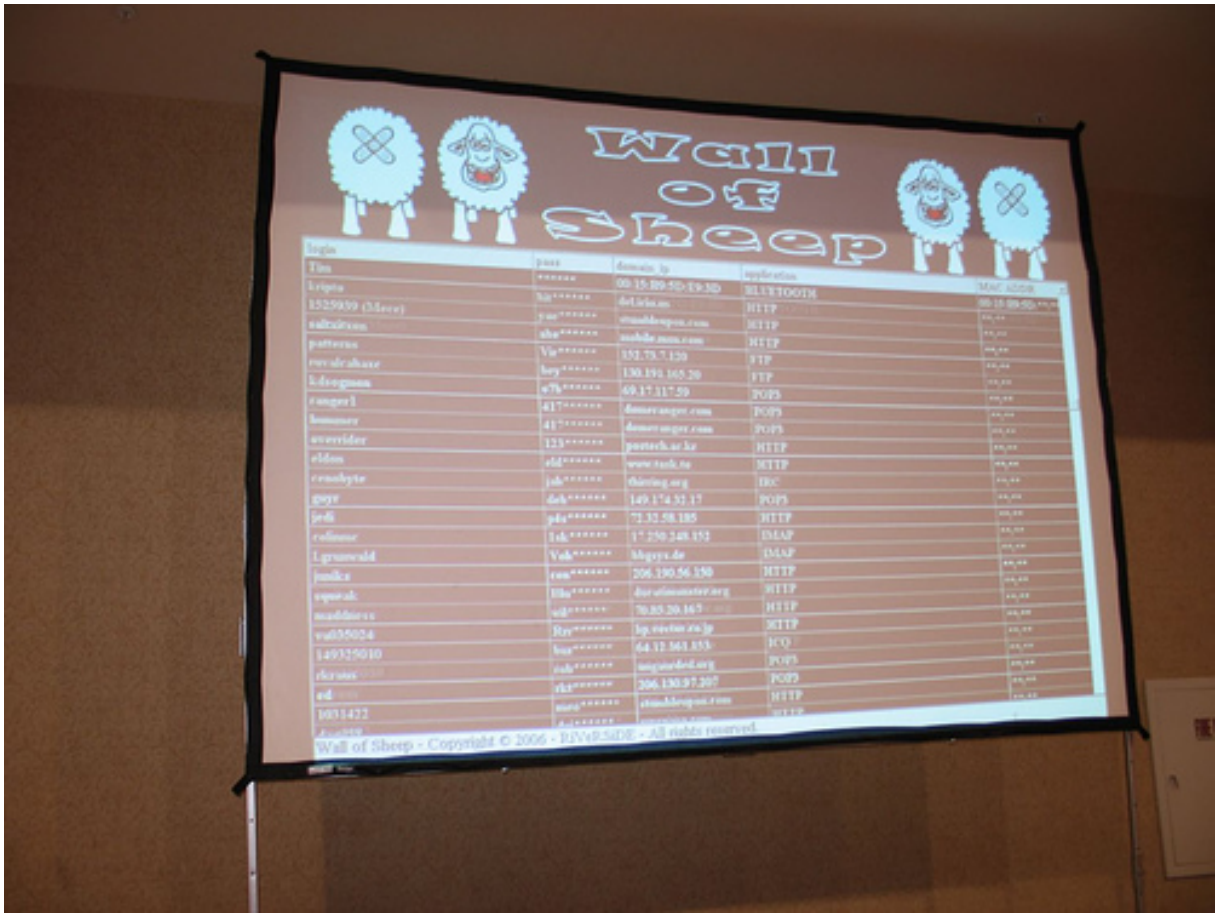

Har man tillid til andre ISP'er? Alle ISP'er?

Deler man et netvsmedium med andre?

Brug de rigtige protokoller!

# Wall of sheep

solido_networks_solid_RGB




Defcon Wall of Sheep

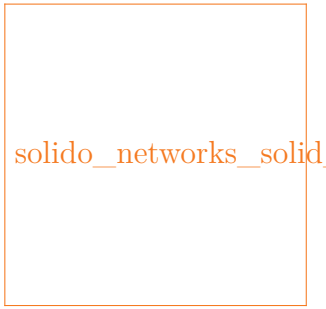
Husk nu at vi er venner her! - idag er det kun teknikken

# Twitter news


Twitter has become an important new ressource for lots of stuff

Twitter has replaced RSS for me

# 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?

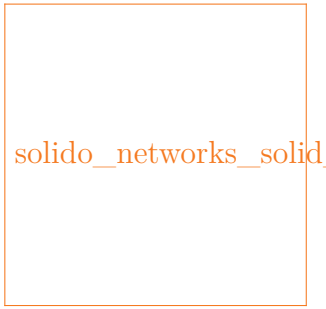
Kan vi klare det pores servere?

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

Men alt for fdet

Ne spsmer svilke rod-certifikater man stoler p..

# Internet sniffing by government




pten, Sudan, Tunesien, ...

Den der kontrollerer ISPerne kontrollerer trafikken

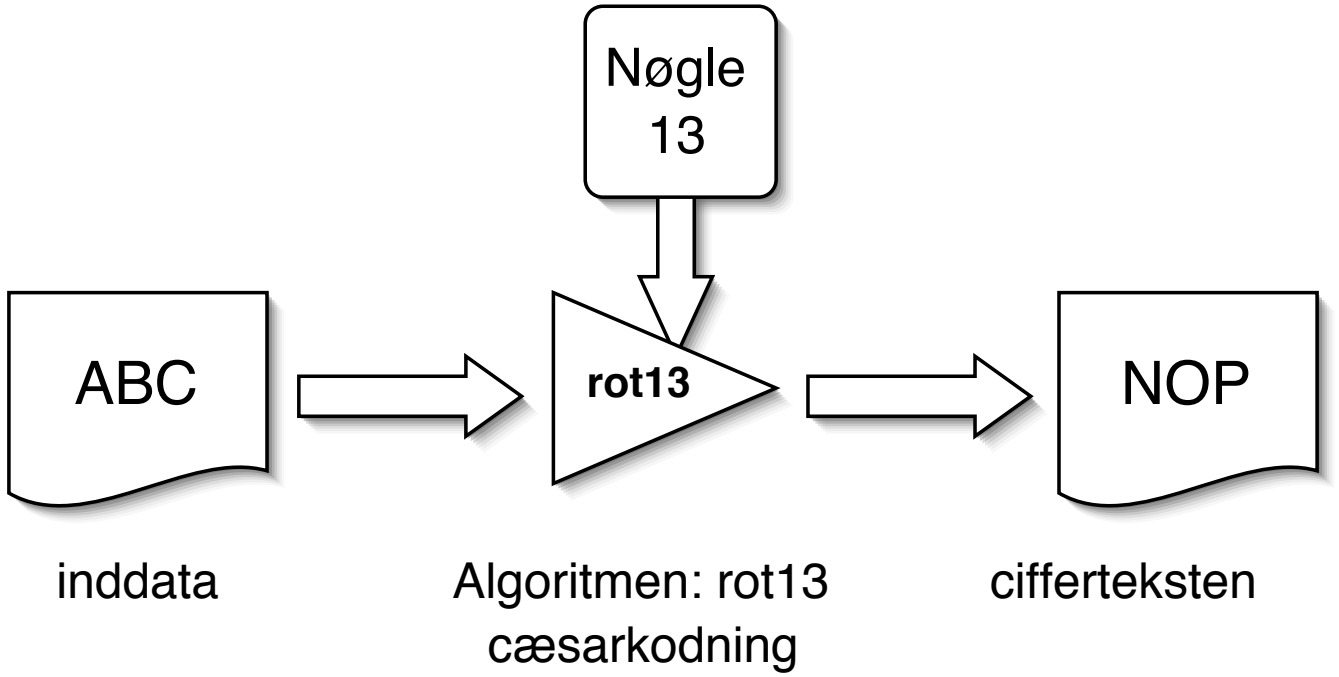
Facebook revolutionerne

Blokering er umulig, men det forss

Spredning af falsk information

Diginotar Dutch Certificate Authority

Kilde: http://irevolution.net/2011/02/10/facebook-for-repressive-regimes/



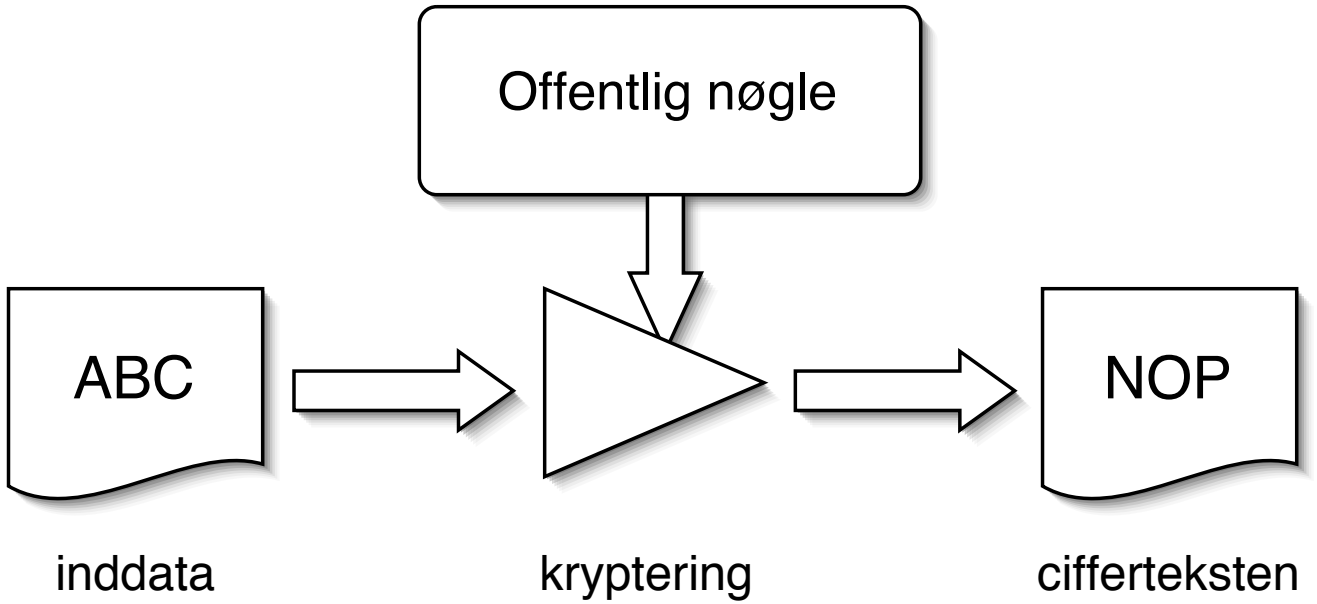

Kryptografi er ln om, hvordan man kan kryptere data

Kryptografi benytter algoritmer som sammen med ner giver en ciffertekst - der kun kan ls ved hj af den tilhnde ne

# Public key kryptografi - 1

solido_networks_solid_RGB

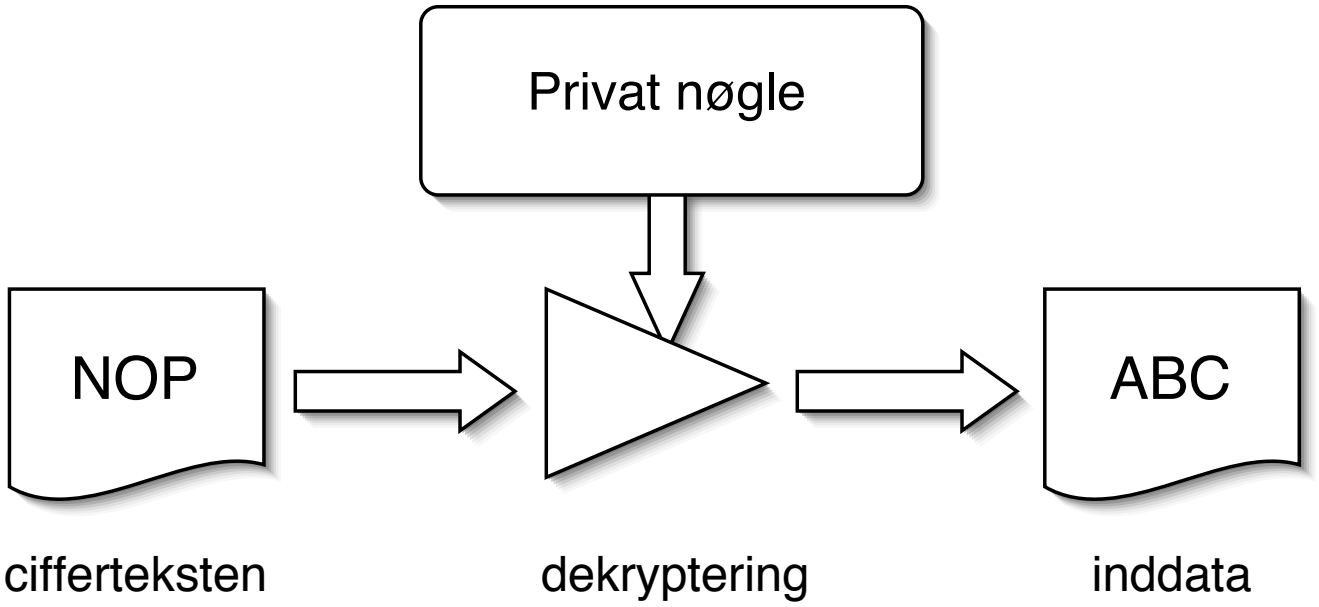



privat-ne kryptografi (eksempelvis AES) benyttes den samme ne til kryptering og dekryptering

offentlig-ne kryptografi (eksempelvis RSA) benytter to separate ner til kryptering og dekryptering

# Public key kryptografi - 2

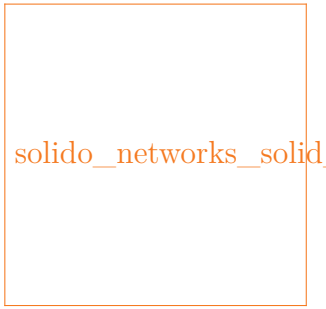





offentlig-ne kryptografi (eksempelvis RSA) bruger den private ne til at dekryptere

man kan ligeledes bruge offentlig-ne kryptografi til at signere dokumenter - som serificeres med den offentlige ne

# Kryptografiske principper




Algoritmerne er kendte

Nerne er hemmelige

Ner har en vis levetid - de skal skiftes ofte

Et successfuldt angreb pn krypto-algoritme er enhver genvej som krr mindre arbejde end en gennemgang af alle nerne

Nye algoritmer, programmer, protokoller m.v. skal gennemgn!

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

solido_networks_solid_RGB


DES kryptering baseret pen IBM udviklede Lucifer algoritme har vt benyttet gennem mange

Der er vedtaget en ny standard algoritme Advanced Encryption Standard (AES) som aflr 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/

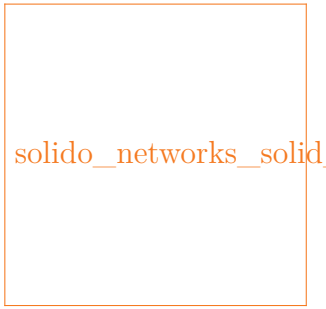
solido_networks_solid_RGB

kryptering er den eneste m at sikre:

fortrolighed

autenticitet / integritet

# Single user mode boot




Unix systemer tillader ofte boot i singleuser mode
hold command-s nede under boot af Mac OS X

Bare tillader typisk boot fra CD-ROM
hold c nede pn Mac

Mac computere kan i nogle tilfe v firewire diske
hold t nede under boot

Harddisken kan typisk nemt fjernes fra en bar

Fysisk adgang til systemet - game over

# Tid til en demo

solido_networks_solid_RGB

Target: Macbook disken

Press t to enter ☺
http://support.apple.com/kb/ht1661

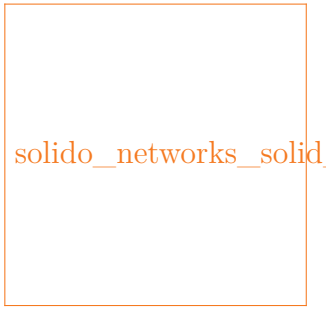
# harddisk beskyttelse og data kryptering




Kryptering findes i alle de gse klient operativsystemer

- Microsoft Windows Bitlocker - kryptering af disken Ultimate eller Enterprise
- Apple Mac OS X - krypterer nemt med FileVault og FileVault2
- FreeBSD GEOM og GBDE - giver mulighed for at kryptere enheder generelt
- PGP disk - Pretty Good Privacy - laver en virtuel krypteret disk
- Nogle producenter har kodeord pisken - IBM harddisk BIOS kodeord

# e-mail og forbindelser




## Kryptering af e-mail

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

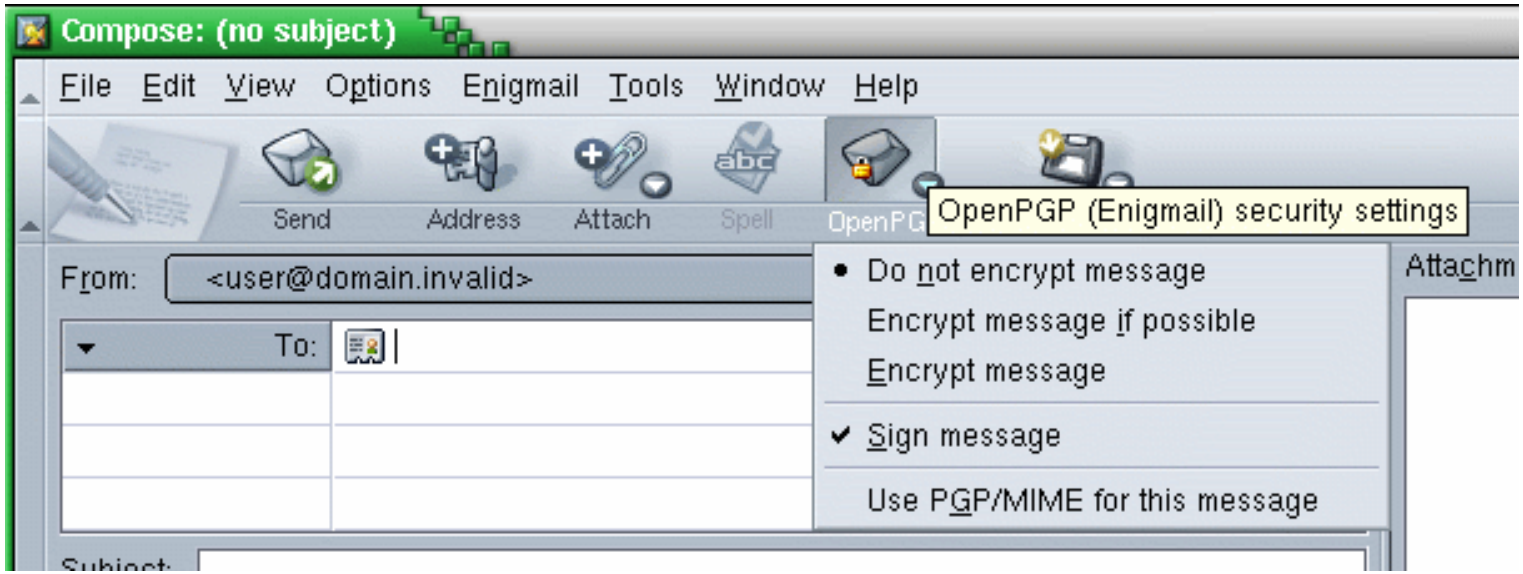
## Kryptering af sessioner SSL/TLS

- 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 kr uden https?

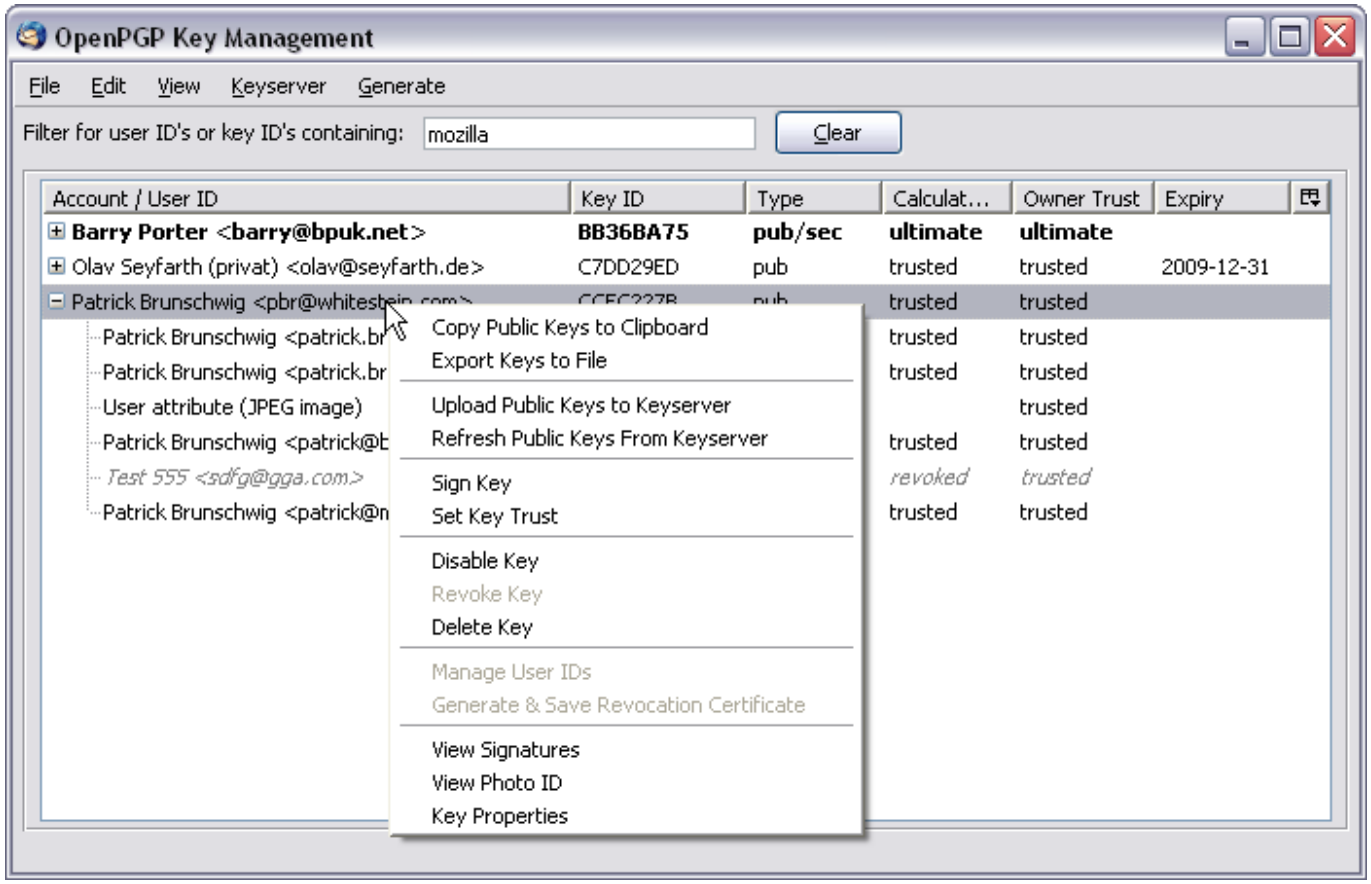
# Enigmail - GPG plugin til Mail






- Enigmail er en udvidelse til
- mailklienten i Mozilla/Netscape
- standalone mailklienten Thunderbird
- Billede fra http://enigmail.mozdev.org

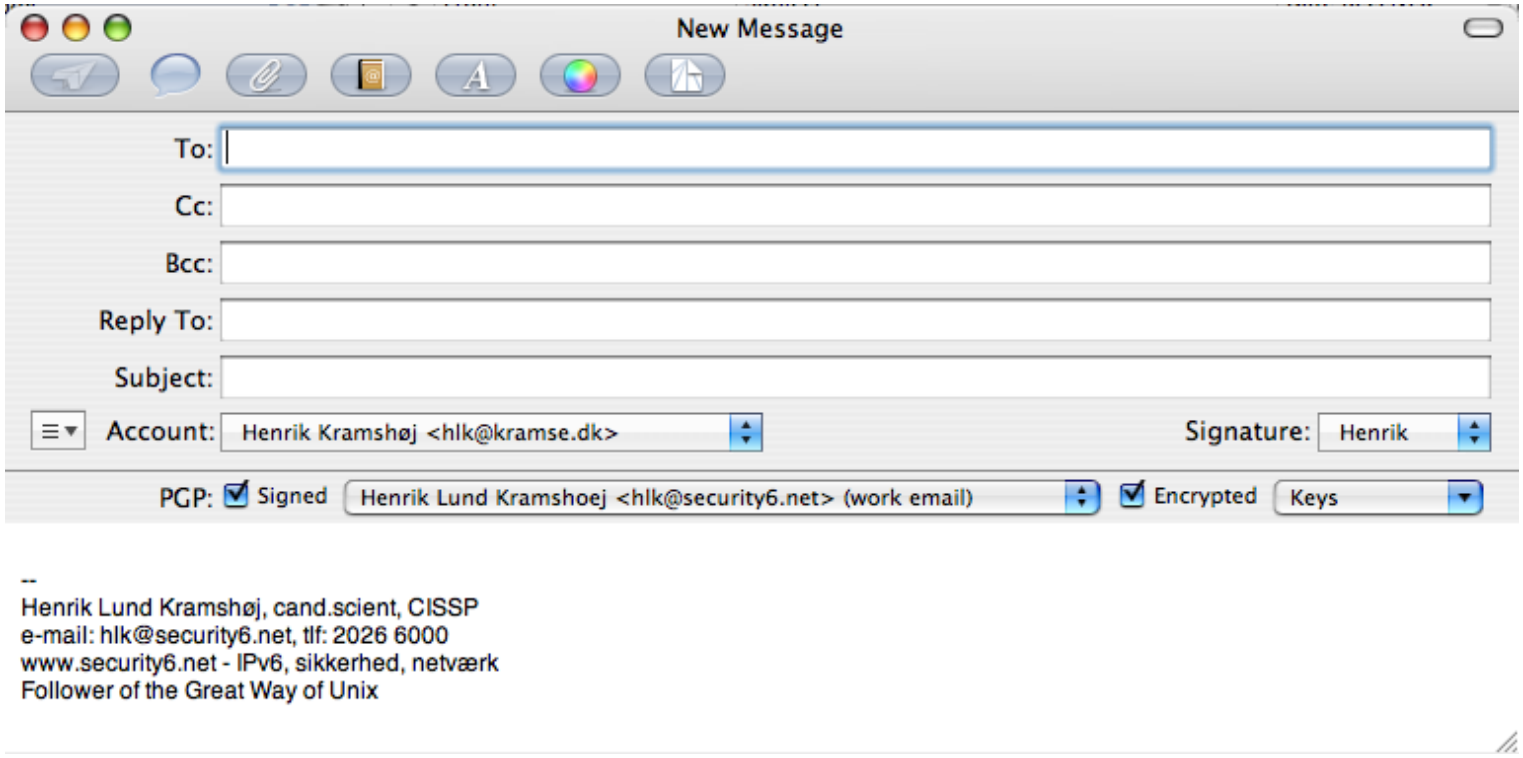
# Enigmail - OpenGPG Key Manager




Key Manager funktionaliteten i Enigmail kan anbefales

# GPGMail plugin til Mac OS X Mail.app

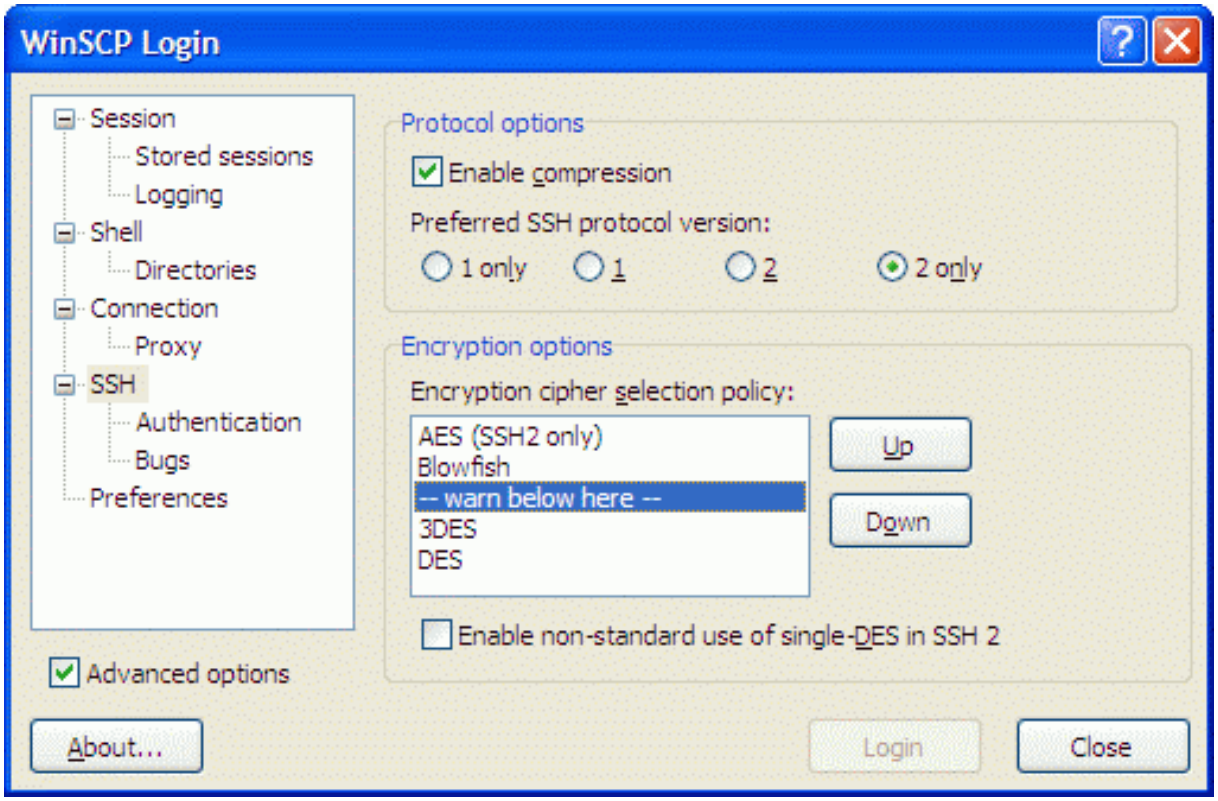





- Bruger GPG
- kilde: http://www.sente.ch/software/GPGMail/English.lproj/GPGMail.html

# Grafisk Secure Copy - WinSCP

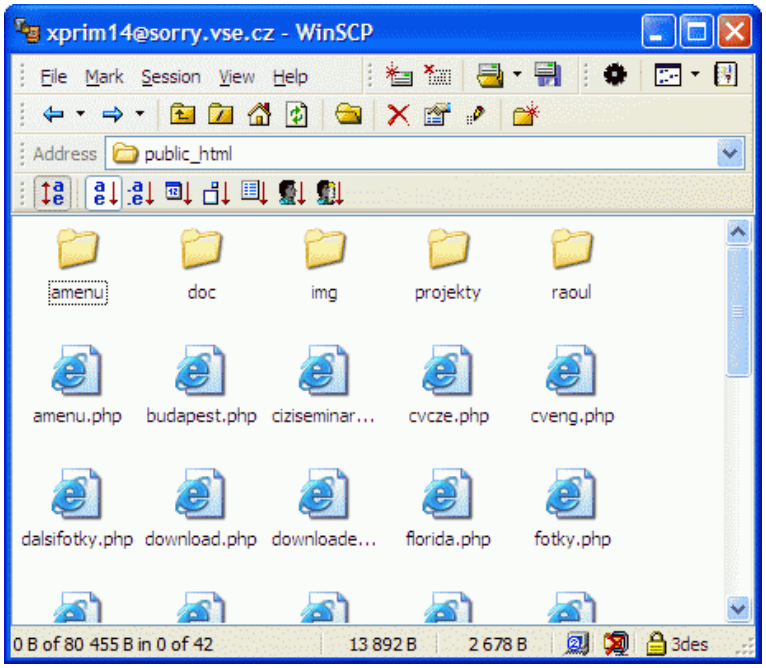
solido_networks_solid_RGB




screenshot fra http://winscp.vse.cz/eng/screenshots/large/advanced.gif

# Grafisk Secure Copy - WinSCP

solido_networks_solid_RGB




benytter Secure Shell protkollen (SSH)

screenshot fra http://winscp.vse.cz/eng/screenshots/large/explorer.gif

# FileZilla - underster SFTP



## FileZilla Features

### Overview

FileZilla Client is a fast and reliable cross-platform FTP, FTPS and SFTP client with lots of useful features

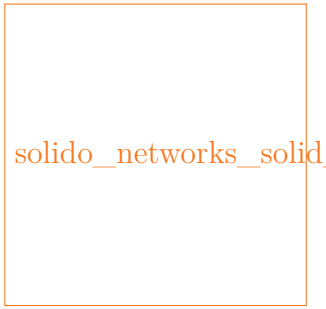
### Features

Among others, the features of FileZilla include the following:

- Easy to use
- Supports FTP, FTP over SSL/TLS (FTPS) and SSH File Transfer Protocol (SFTP)
- Cross-platform. Runs on Windows, Linux, *BSD, Mac OS X and more
- IPv6 support
- Available in many languages
- Supports resume and transfer of large files >4GB
- Tabbed user interface
- Powerful Site Manager and transfer queue
- Bookmarks
- Drag & drop support
- Configurable transfer speed limits

http://filezilla-project.org/

# VPN




VPN http://en.wikipedia.org/wiki/Virtual_private_network

SSL/TLS VPN - Generelt koncept. Adskillige leverandr: Cisco, Juniper, F5 Big IP

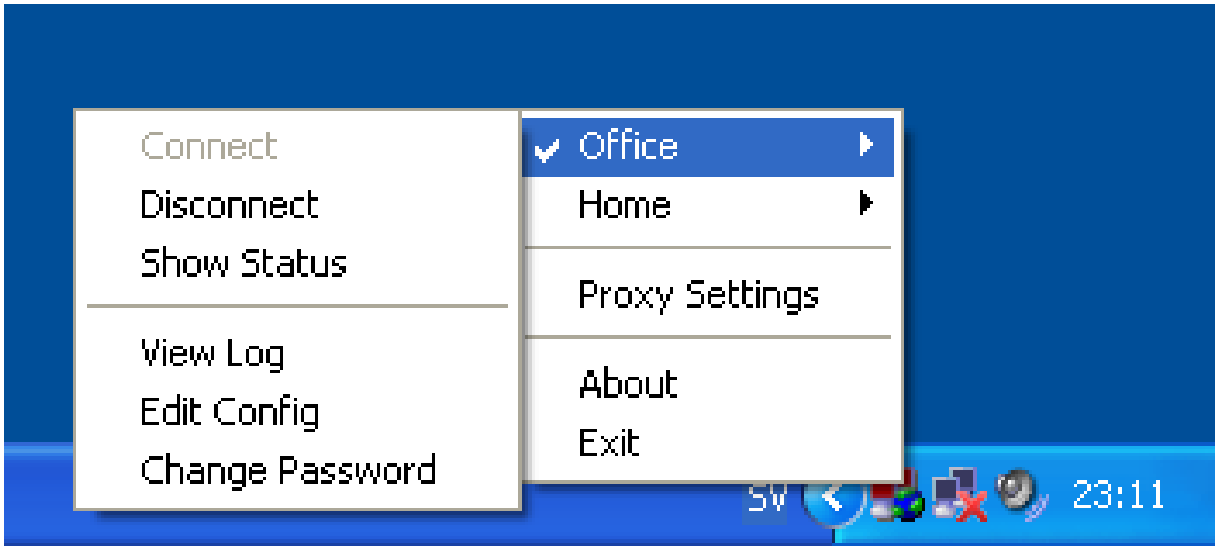
De snakker ikke ret godt sammen pv. Brug IPSec for dette.

IPsec er desve blokeret mange steder og man skal bruge en klient
(I praksis bruger SSL VPN ofte en klient, men den downloades fra web)

Open source variant: OpenVPN

# OpenVPN client

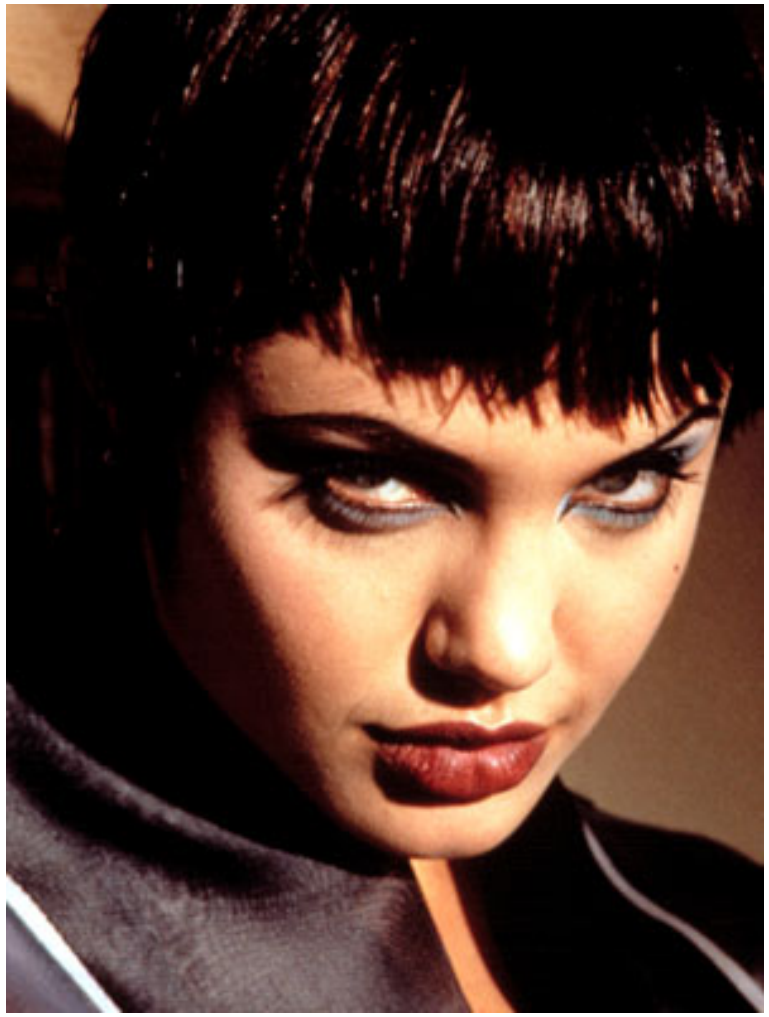





OpenVPN GUI - easy to use

# Hackertyper anno 1995

solido_networks_solid_RGB



Lad os lige gilbage til hackerne

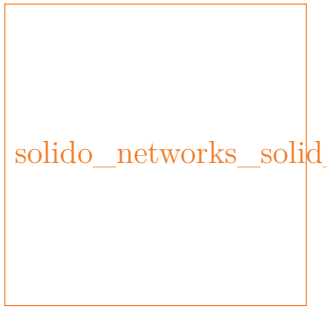
# Hackertyper anno 2008

solido_networks_solid_RGB

Lisbeth laver PU, personunderslser ved hj af hacking

Hvordan finder man information om andre

# Fra mtre til person




Ft vil vi finde nogle mtre

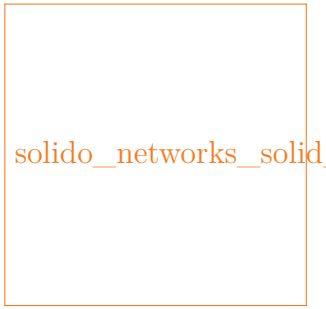
Derefter vil vi s med de mtre

Nogle giver direkte information

Andre giver baggrundsinformation

Hvad er offentligt og hvad er privat? (googledorks!)

# Eksempler ptre




Navn, fulde navn, fornavne, efternavne, alias'es

Diverse idnumre, som CPR - tdu s pit CPR nr?

Computerrelaterede informationer: IP, Whois, Handles

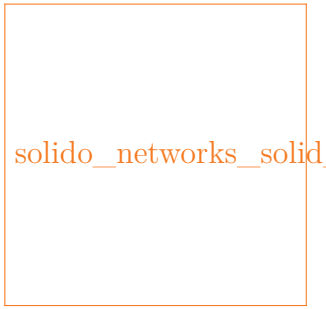
navne, kendenavne

Skrivestil, ordbrug mv.

Tiden pin computer?

T kreativt ☺

# Hvor finder du informationerne




Email

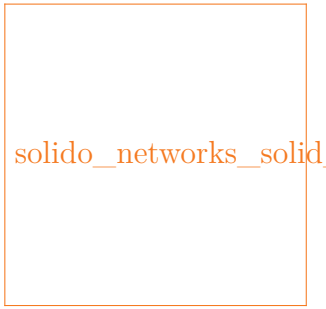
DNS

Ger

Google

Alt hvad du ellers har adgang til - eller som Lisbeth tilraner sig adgang til

# whois systemet




IP adresserne administreres i dagligdagen af et antal Internet registries, hvor de stte er:

- RIPE (Raux IP Europs) http://ripe.net
- ARIN American Registry for Internet Numbers http://www.arin.net
- Asia Pacific Network Information Center http://www.apnic.net
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) - Latin America and some Caribbean Islands

disse fire kaldes for Regional Internet Registries (RIRs) i modsing til Local Internet Registries (LIRs) og National Internet Registry (NIR)

# Google for it

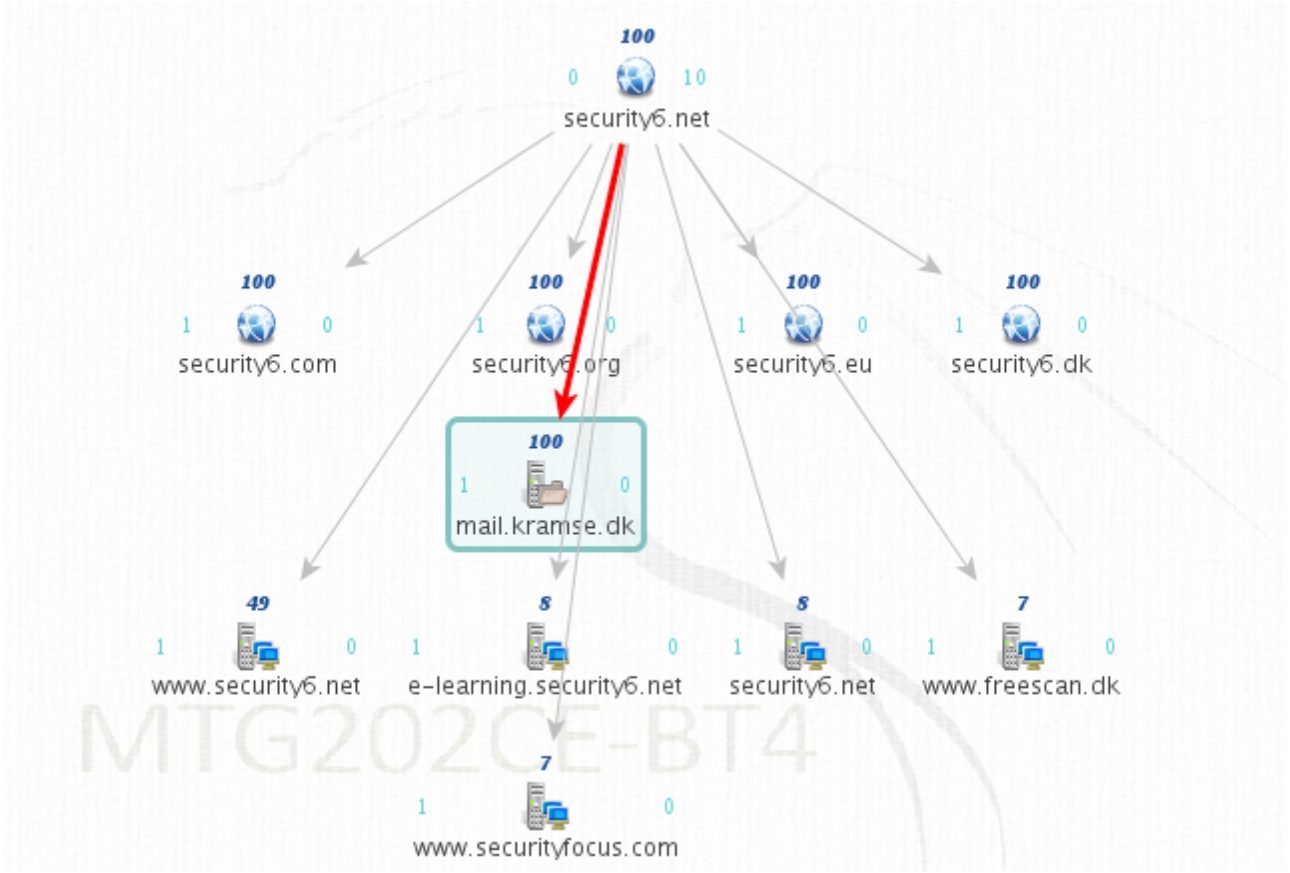



Google som hacker vt

Googledorks http://johnny.ihackstuff.com/

# Listbeth in a box?

solido_networks_solid_RGB



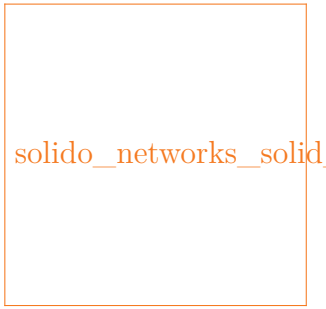

BT4 udgaven, kommerciel udgave plinkhttp://www.paterva.com/maltego/

# Er du passende paranoid?

solido_networks_solid_RGB

Vpagt

# Hvordan bliver du sikker




Lad v med at bruge computere

Lad v med at bruge een computer til alt - en privat bar ER mere privat end en firmacomputer

Forskellige computere til forskellige form en server er mail-server en anden er web-server

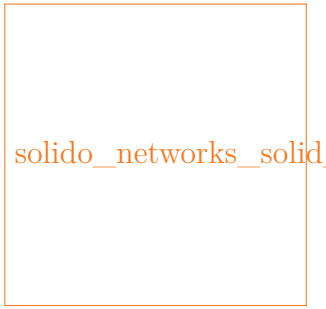
Brug en sikker konfiguration, minimumskonfiguration

Brug sikre protokoller, kryptering, evt. TOR

Opsing af netv, hvordan? Security Configuration Guides + paranoia

- http://csrc.nist.gov/publications/PubsSPs.html
- http://www.nsa.gov/research/publications/index.shtml
- http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml

# Checklisten




- BIOS kodeord, pin-kode til telefon
- Firewall - specielt paptops
- Installer anti-virus og anti-spyware hvis det er pindows
- Brug to browsere med forskellige indstillinger
- Brug evt. PGP til mailkryptering
- Brug Password Safe, Keychain Access (OSX) eller tilsvarende
- Overvej at bruge harddisk eller filkryptering
- Opdatere alle programmer jligt
- Backup af vigtige data - harddiske i bare kan ogs
- Husk: sikker sletning af harddiske, medier osv.

# PROSA CTF



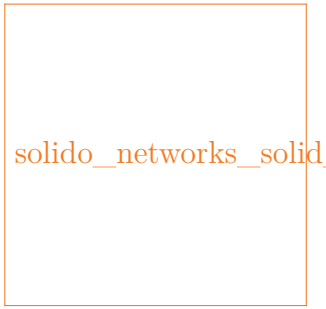
PROSA afholdt fredag 17. september - til lag 18. september Capture the Flag

Distribueret CTF med 6 hold og arrangrne i Aalborg

Sjovt og lrigt - gentages helt sikkert

Kilde: http://prosa-ctf.the-playground.dk/
Get ready! Ldebuggere, perl, java at kende, start pt hacke

# Questions?




Henrik Lund Kramshøj, internet samurai
hlk@solido.net

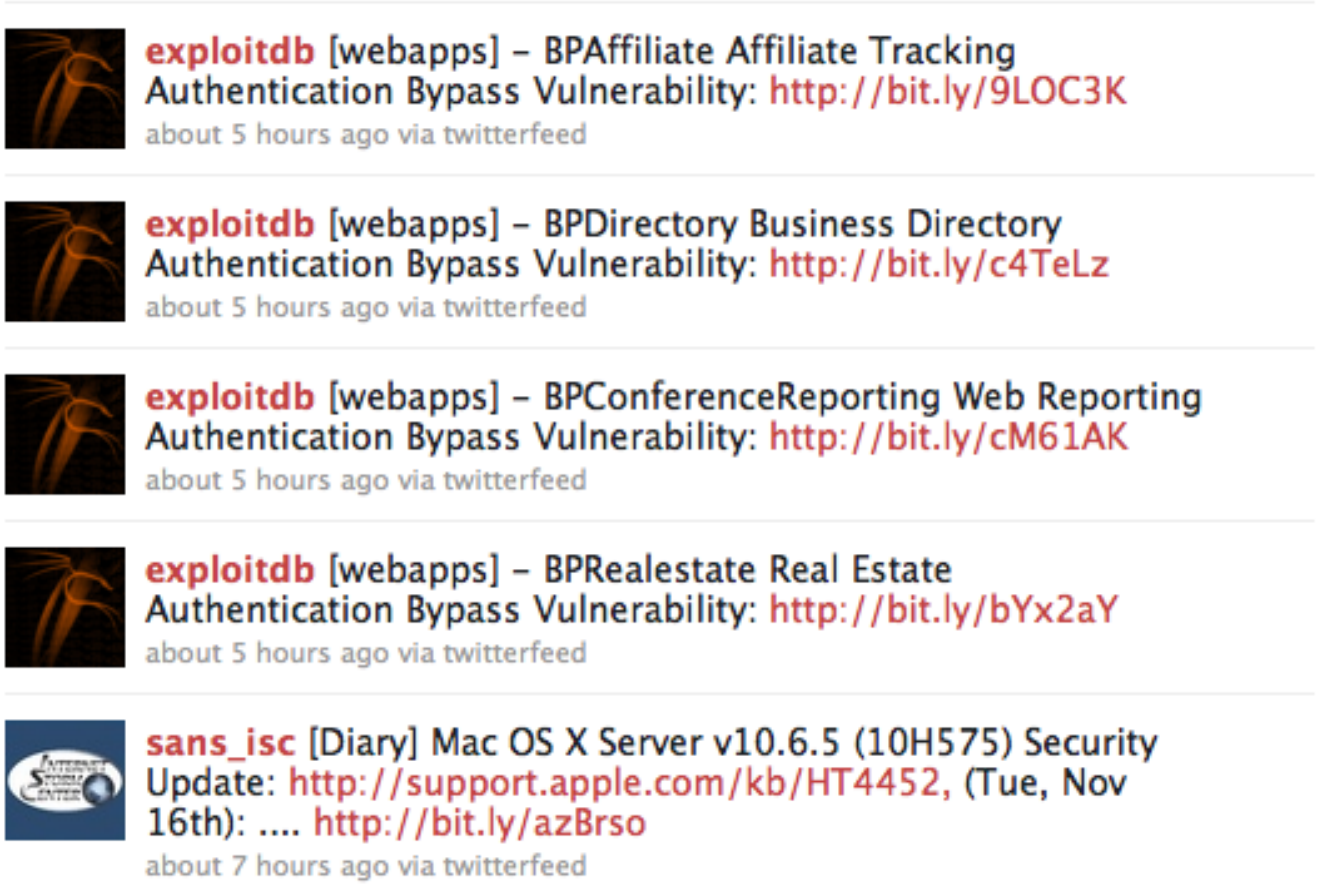
http://www.solidonetworks.com

You are always welcome to send me questions later via email

Did you notice how a lot of the links in this presentation use HTTPS - encrypted

# informationskilder



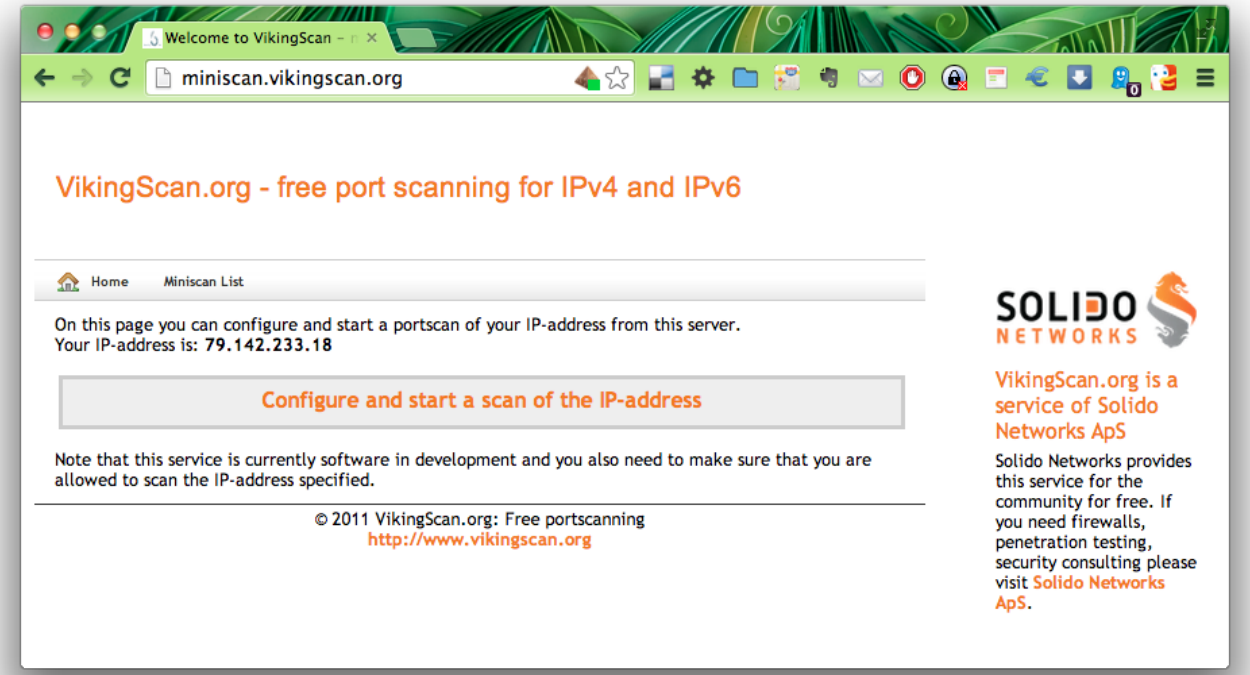



Nye kilder til information:

har twitter afl RSS? NB: favoritsite http://isc.sans.edu/index.html

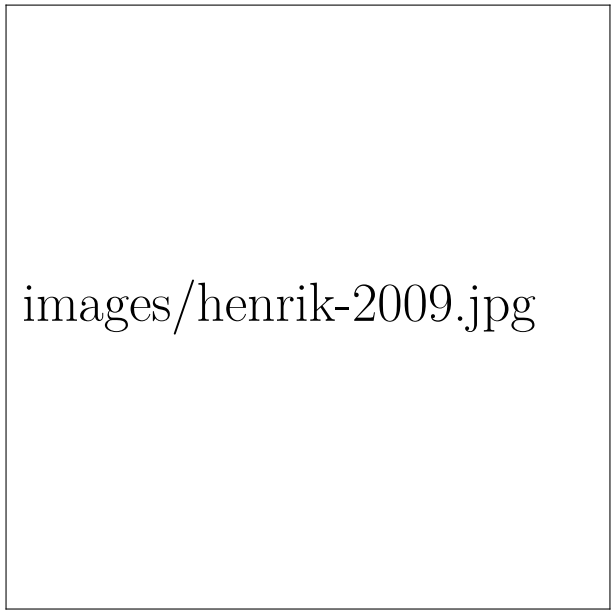
# VikingScan.org - free portscanning

solido_networks_solid_RGB



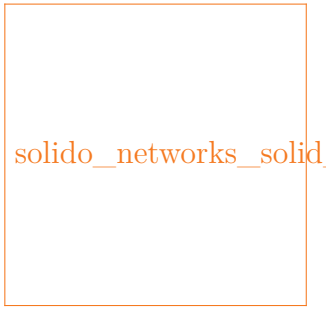
# Kontaktinformation og profil

solido_networks_solid_RGB



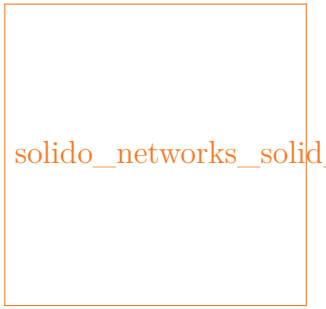

- Henrik Lund Kramshøj, IT-sikkerhed og internet samurai
- Email: hlk@solido.net Mobil: +45 2026 6000
- Cand.scient fra Datalogisk Institut ved Københavns Universitet, DIKU
- CISSP certificeret
- 2003 - 2010 Selvstændig sikkerhedskonsulent

- 2010 Stifter og partner i Solido Networks ApS



# Reklamer: kursusafholdelse




Fende kurser afholdes med mig som underviser

- IPv6 workshop - 2 dage
  Introduktion til Internetprotokollerne og forberedelse til implementering i egne netv.
- Wireless teknologier og sikkerhed workshop - 1-2 dage
  En dag med fokus petvsdesign og fornuftig implementation af tr netv, samt integration med hjemmepc og wirksomhedsnetv.
- Hacker workshop 2 dage
  Workshop med detaljeret gennemgang af hackermetoderne angreb over netv, exploitprogrammer, portscanning, OpenVAS m.fl.
- Forensics workshop 2 dage
  Med fokus pilgelige open source vtr gennemgmetoder og praksis af underslse af diskimages og spor pomputer systemer
- Moderne Firewalls og Internetsikkerhed 2 dage
  Informere om trusler og aktivitet pnternet, samt give et bud pvorledes en avanceret moderne firewall idag kunne konfigureres.

Se mere plinkhttp://www.solidonetworks.com