

Welcome to

Hacking - protect yourself

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

<http://www.solidonetworks.com>

Goal of this presentation

solido_networks_solid_RGE



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

solido_networks_solid_RGE

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 ☺

Introduktion til hacking

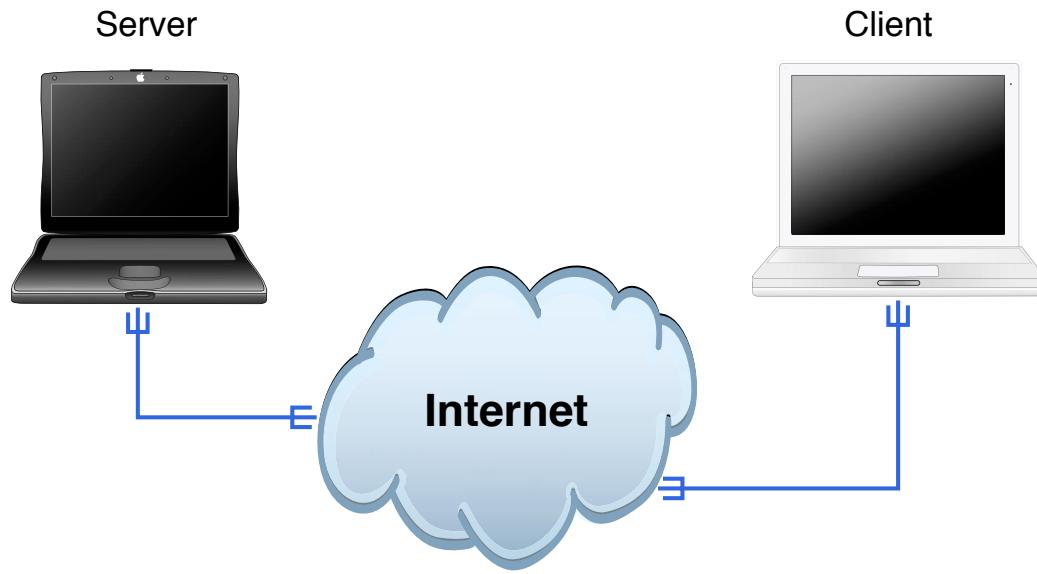
solido_networks_solid_RGE



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

Internet today

solido_networks_solid_RGE



Clients and servers

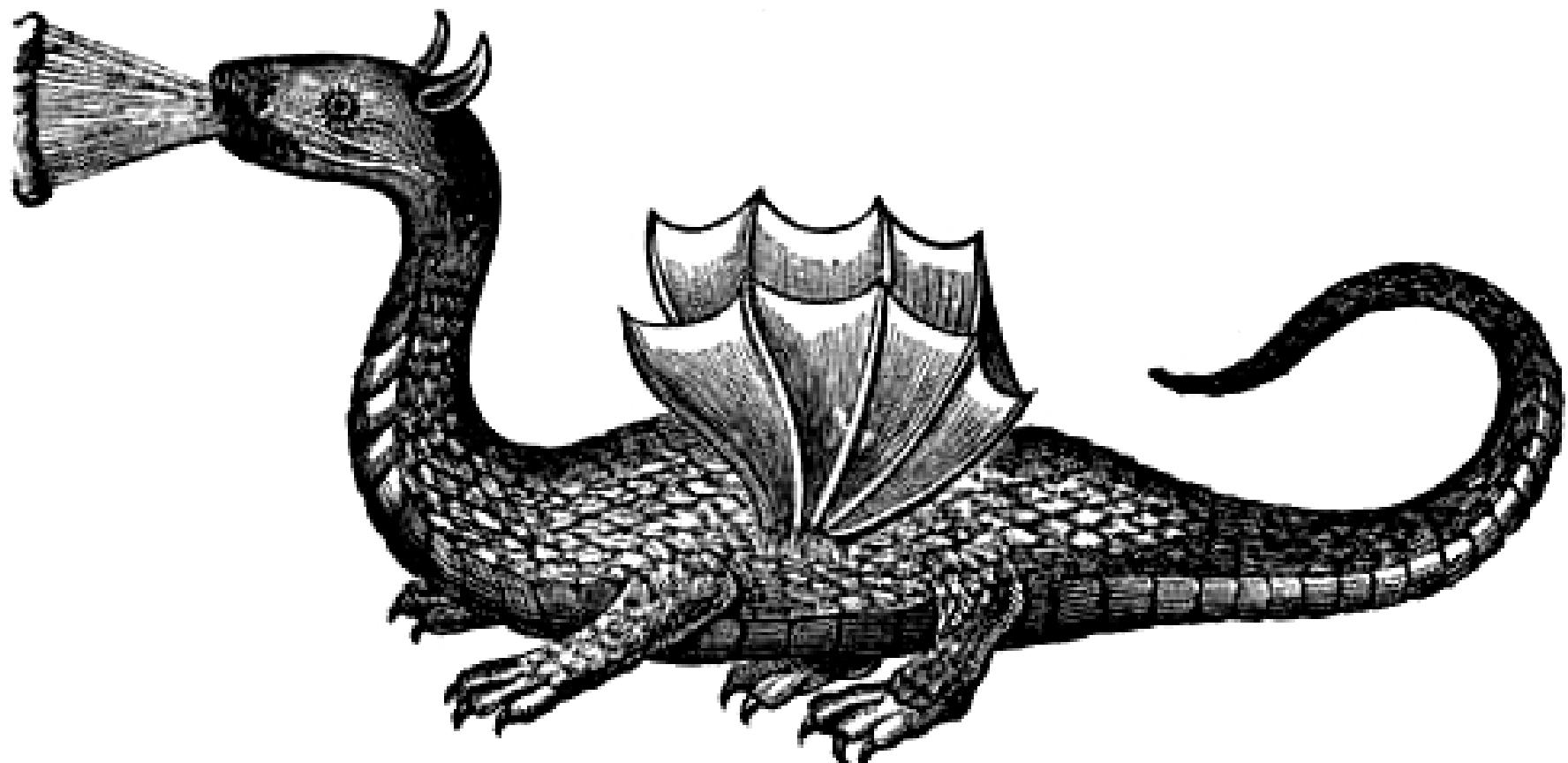
Rooted in academic networks

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_RGE



Matrix style hacking anno 2003

solido_networks_solid_RGE



Trinity breaking in

solido_networks_solid_RGE

```
80/tcp      open     http  
81/tcp      open     host<2>.nc  
10  [REDACTED] ( mobile)  
11  $ nmap -v -sS -O 10.2.2.2  
11  
13 Starting nmap 0. 2.54BETA25  
13 Insufficient responses for TCP sequencing (3). OS detection is  
13 inaccurate  
14 Interesting ports on 10.2.2.2:  
14 (The 1539 ports scanned but not shown below are in state: cle  
51 Port      State       Service  
51 22/tcp    open        ssh  
58  
68 No exact OS matches for host  
68  
24 Nmap run completed -- 1 IP address (1 host up) scanned  
50 $ sshnuke 10.2.2.2 -rootpw="Z10H0101"  
Connecting to 10.2.2.2:ssh ... successful.  
Re  
IP  
Attempting to exploit SSHv1 CRC32 ... successful.  
Resetting root password to "Z10H0101".  
System open: Access Level <9>  
$ ssh 10.2.2.2 -l root  
root@10.2.2.2's password: [REDACTED]  
[REDACTED] RIF CONTROL  
[REDACTED] ACCESS GRANTED
```

<http://nmap.org/movies.html>

Meget realistisk http://www.youtube.com/watch?v=51lGCTgqE_w

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

solido_networks_solid_RGE

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

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

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

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

Internet er e standard!

solido_networks_solid_RGE

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

solido_networks_solid_RGE

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_RGE



Hacking ligner indimellem magi

Hacking er ikke magi

solido_networks_solid_RGE



Hacking krr blot lidt ninja-trng

God sikkerhed

solido_networks_solid_RGE



Der benyttes en del vtr:

- nmap - <http://www.insecure.org> portscanner
- Wireshark - <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

solido_networks_solid_RGE

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 plættet 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_RGE

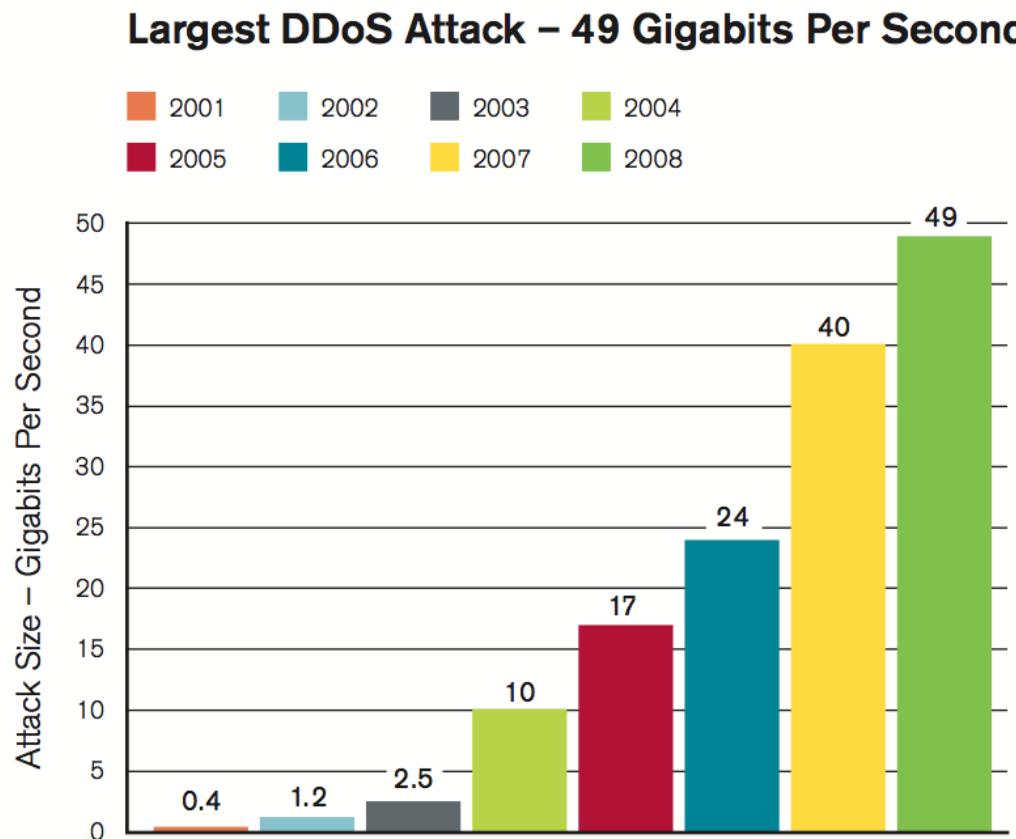


Figure 1: Largest DDoS Attack – 49 Gigabits Per Second

Source: Arbor Networks, Inc.

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

DDoS udviklingen, februar 2011

solido_networks_solid_RGE

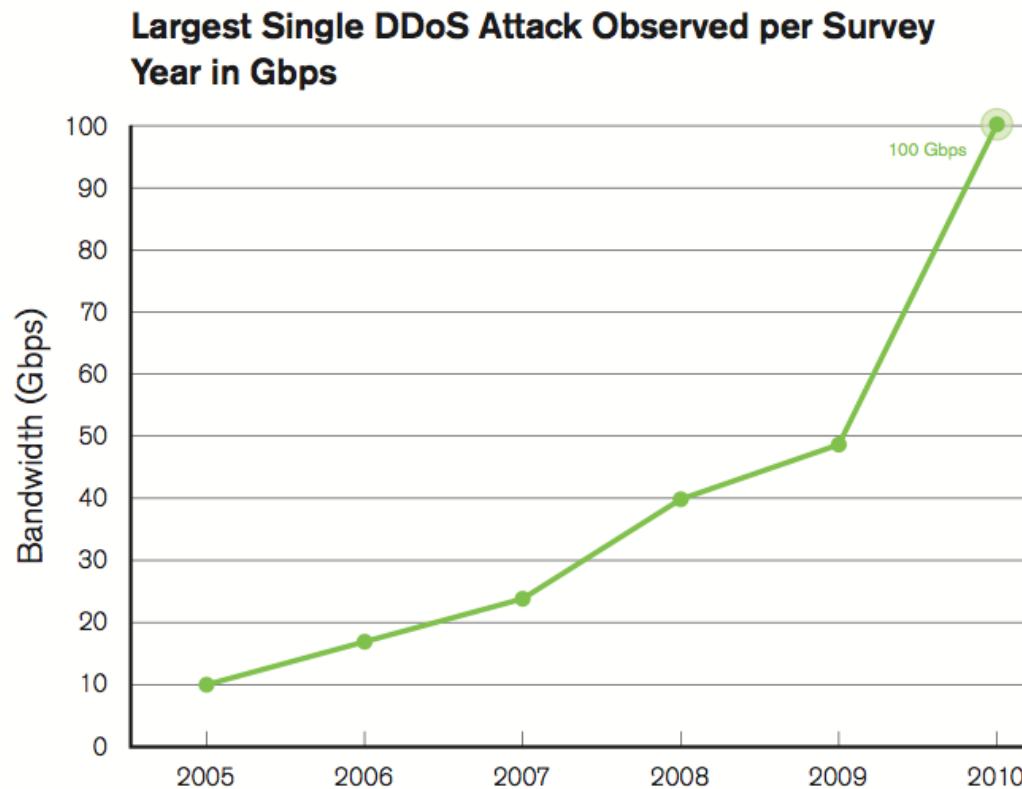


Figure 1
Source: Arbor Networks, Inc.

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

Key findings

solido_networks_solid_RGE

- 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

solido_networks_solid_RGE

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

solido_networks_solid_RGE

Botnets spredes 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

solido_networks_solid_RGE

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

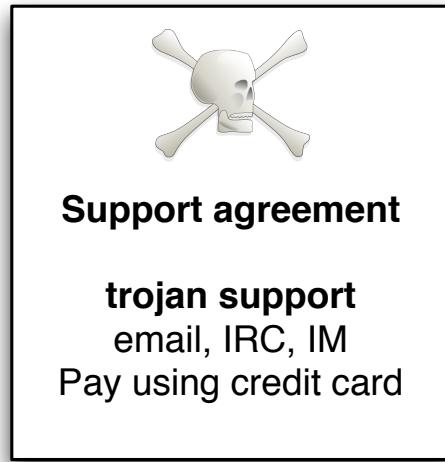
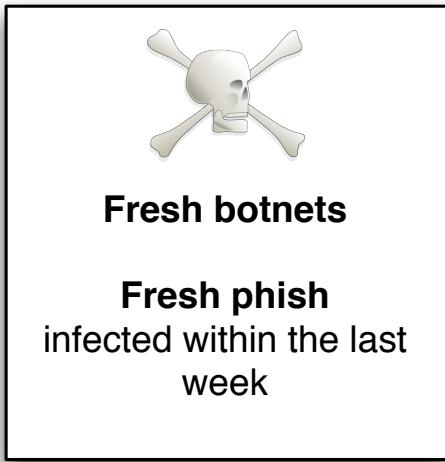
Benytter de seneste rootkit metoder til at holde sig skjult

Muterer efter alle kendte metoder for at undgå opdagelse

Larmer mindre end tidligere

Botnets og malware ses med support

solido_networks_solid_RGE



Malware programmr har 1 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

solido_networks_solid_RGE

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

Lejede 22.000 computere og afprøde skadenvirkninger

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_RGE

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_RGE

The screenshot shows a window titled "zpam — hlk@kramse.dk (473 unread)". The interface includes standard OS X-style window controls (red, yellow, green buttons) and a toolbar with icons for trash, search, and message actions. Below the toolbar, a message list displays 474 messages. The columns are "From", "Subject", and "Date Received". The "Date Received" column is sorted in descending order. Several messages from "Maynard Stipek" are listed, followed by a message from "randi@indocrafts.com" with the subject "Re: Delivery Protection", which is highlighted with a blue selection bar. Another message from "km@roval-photo.dk" is also visible. At the bottom of the message list, there is a note: "Protected message is attached." Below this note, a file icon for a ZIP archive is shown next to the filename "message.zip (39,9 KB)".

From	Subject	Date Received
maynard stipek	Experience convenient online shopping ...	Today 2.24
Merrill H. Schumacher	online Pharmcy..ADIPEX,SOMA,etc !!	Today 2.52
Forest Salgado	Critical Service Pack 2 update . March 10th	Today 4.00
Vanessa J. Smith	Windows XP + Office XP = \$89.95	Today 6.19
Norah Kelley	Sale on All AutoCAD software	Today 6.55
Heidi Forbes	Better than Viagra	Today 7.25
randi@indocrafts.com	Re: Delivery Protection	Today 8.41
km@roval-photo.dk	Mail Delivery (failure hlk@kramse.dk)	Today 8.43

Money!

solido_networks_solid_RGE

In (63 unread)

Entire Message

1353 messages

From	Subject	Date Received
Charlie Root	betty.kramse.dk daily output	14. marts 2005 1.37
Charlie Root	betty.kramse.dk daily insecurity output	14. marts 2005 1.37
Henrik Root	phoenix.devoteam.dk daily output	14. marts 2005 1.43
Charlie Root	betty.kramse.dk weekly output	12. marts 2005 3.37
Henrik Root	phoenix.devoteam.dk weekly output	12. marts 2005 3.43
Qualys, Inc.	@RISK: The Consensus Security Vulnerability Alert - Week 10 2005	12. marts 2005 3.15
Washington Mutual Online Banking	Confirm Your Washington Mutual Online Banking	12. marts 2005 2.21

From: Washington Mutual Online Banking <personalbanking@erms-02.wamu.com>
Subject: Confirm Your Washington Mutual Online Banking
Date: 12. marts 2005 2.19.18 MET
To: hlk@kramse.dk

wamu.com A Washington Mutual, Inc. Web site Customer Service Contact Us Locations

Dear Washington Mutual customer,

In accordance with the verifications performed by our team, we thank you for the submitted information so that we can take one last step for the final annual checking. Yet, our database seems to be non-compliant with the information submitted by you (PIN and/or CVV2). Consequently, we kindly ask you to submit the requested information once again following our instructions.



[Explanation](#)

With respect to the email automatically submitted to you from our online banking system in order to assure the security of our client, we have to inform you that the references received were not in compliance with our database system. Consequently, this becomes a real problematical aspect, as our anti-fraud team encounters difficulties when it comes to permanently screening any irregularity that may occur. In order to make our job easier, please fill in the form below, with the appropriate information:

<https://login.personal.wamu.com/registration/CreateLogonEntry.asp>

If you believe you have provided personal or account information in response to a fraudulent e-mail or Web site, please contact Washington Mutual at 800.788.7000 and contact the other financial institutions with which you have accounts

Thank you for trusting our services.

zspam — hlk@kramse.dk (464 unread)

Entire Message

474 messages

From	Subject	Date Received
hlk@kramse.dk	Mail Delivery (failure hlk@kramse.dk)	3/3-2005 10.50
viba@fa.dk	Mail Delivery (failure hlk@kramse.dk)	3/3-2005 21.23
Larry Martin	Institutions are buying Homeland Security,, ...	4/3-2005 5.37
info@opinionsland.co	Re: your data	4/3-2005 10.02
peter@bluesky.se	Mail Delivery (failure hlk@kramse.dk)	4/3-2005 10.02
everett wetterer	Quality meds without any hassel headquarter	4/3-2005 2.19
Jodie Harding	Protect your children	6/3-2005 16.10
Brandi Dutton	Re: susceptance baud where hines ideology	6/3-2005 6.50

From: info@opinionsland.co
Date: 4. marts 2005 10.02.43 MET
To: hlk@kramse.dk
Subject: Re: your data

Please read the important document.


[data.scr \(28,9 KB\)](#)

solido_networks_solid_RGE



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

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.

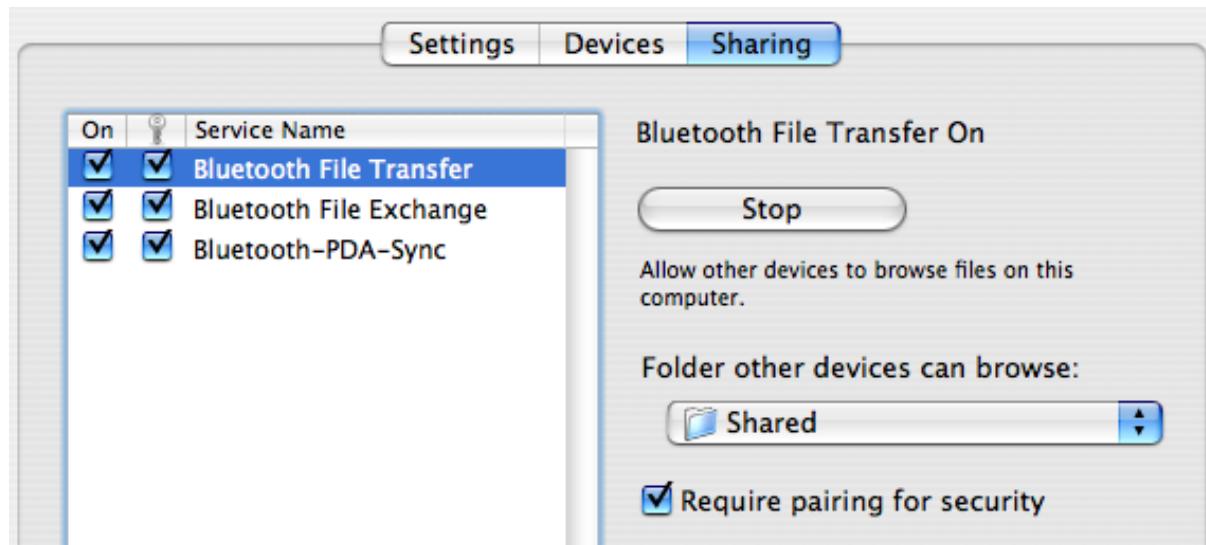
Kilde: Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010 - 2015

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 udoer GPRS/telefoni

Bluetooth sikkerhed

solido_networks_solid_RGE



- 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_RGE



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

- Man kan hente programmer pnet
- Man kan bruge en retningsbestemt antennne
- Man kan lytte med pamtaler i bilerne

Kilde:

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

Problemer med smart phones/PDA

solido_networks_solid_RGE

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?

Brug teknologien

Lteknologien at kende - lmanualen!

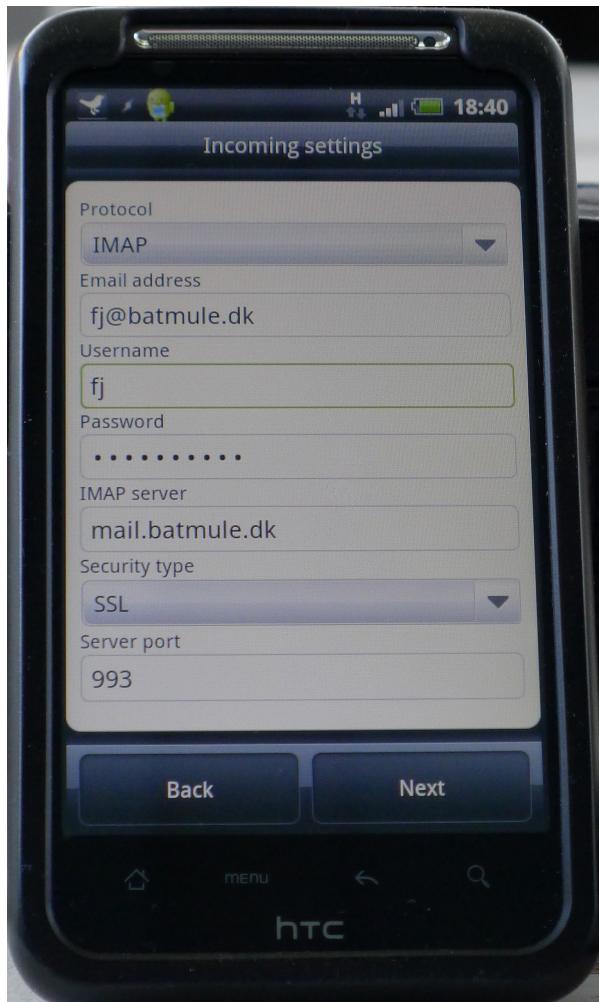
T pomheden af data I gemmer og overfr

- Sling fra som I ikke bruger
- Sluetooth 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 pingetryksafre

SSL/TLS (1)

solido_networks_solid_RGE

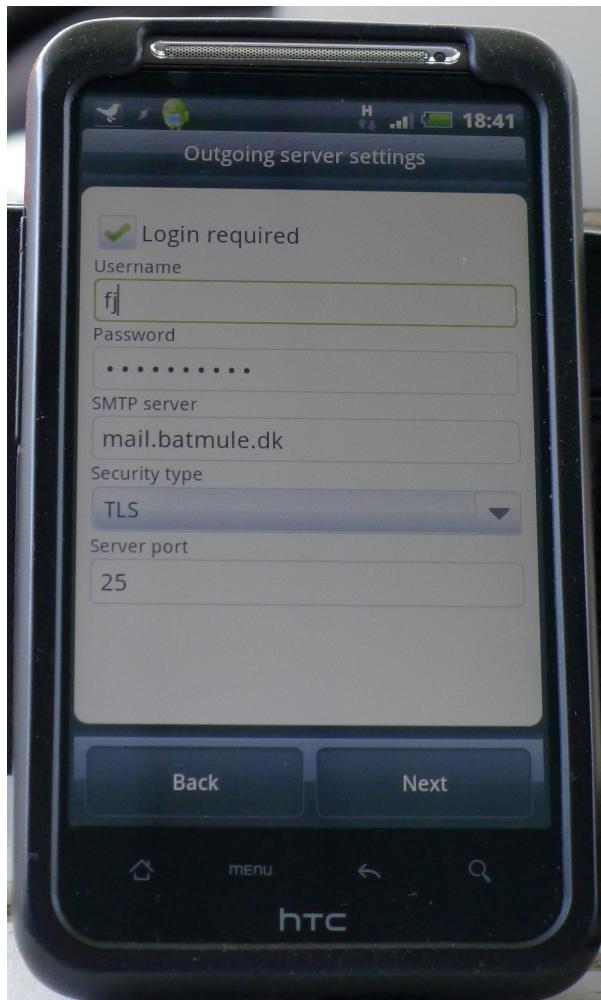
Istedet for POP3 brug POP3s, Istedet for IMAP brug IMAPs



SSL/TLS (2)

solido_networks_solid_RGE

SMTP kan erstattes med SMTP+TLS



Tyveri - behaven og lufthavnen

solido_networks_solid_RGE

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_RGE

Et ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. At vero eos et accusamus et iusto odio dignissim 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_RGE

Er det tid til en lille pause?



Teknisk hvad er hacking

solido_networks_solid_RGE

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



buffer overflows et C problem

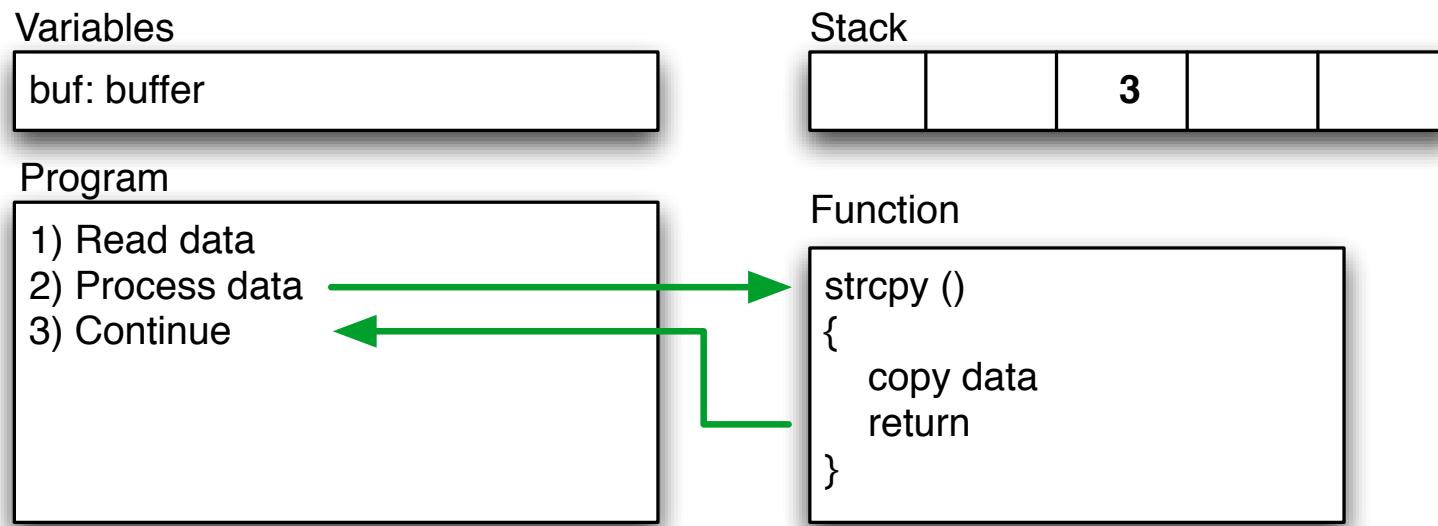
solido_networks_solid_RGE

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

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

Buffer og stacks

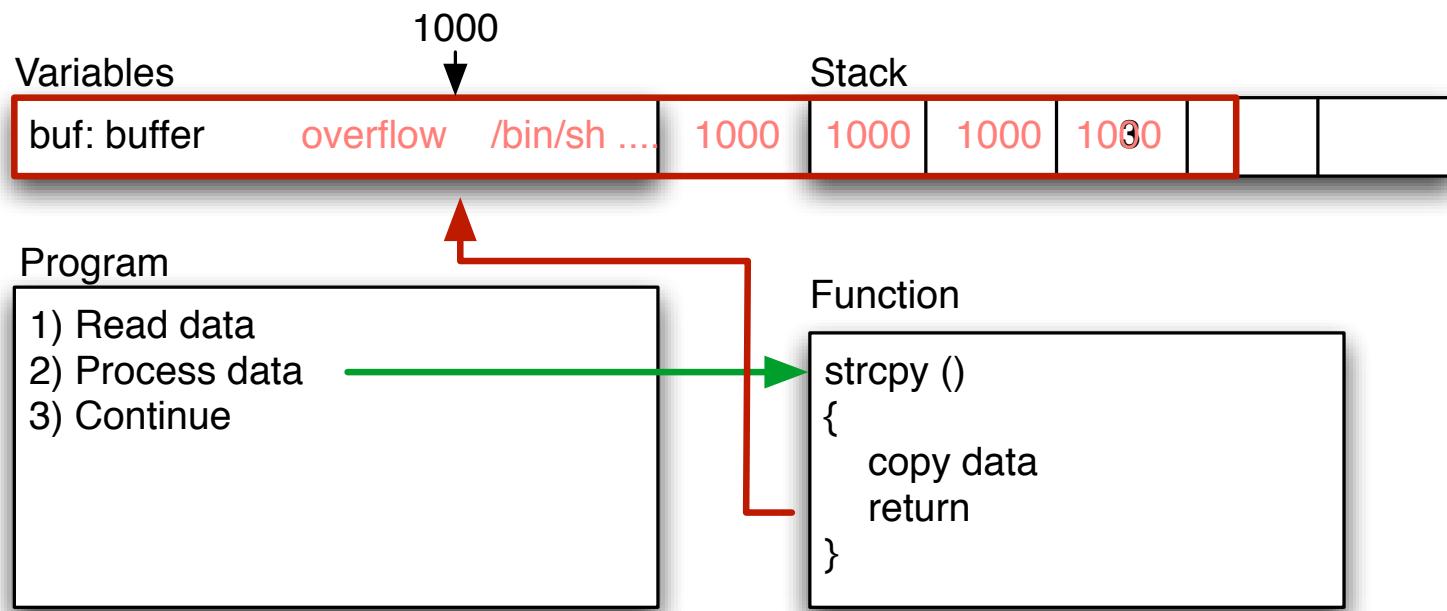
solido_networks_solid_RGE



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

Overflow - segmentation fault

solido_networks_solid_RGE



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

Exploits

solido_networks_solid_RGE

```
$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

solido_networks_solid_RGE

Black box testing

Closed source reverse engineering

White box testing

Open source betyder man kan log og analysere koden

Source code review - automatisk eller manuelt

Fejl kan findes ved at prøve sig frem - fuzzing

Exploits virker typisk mod specifikke versioner af software

The Exploit Database - dagens buffer overflow

solido_networks_solid_RGE

The screenshot shows the homepage of The Exploit Database. At the top, there's a navigation bar with links for home, news, remote, local, web, dos, shellcode, papers, search, D, submit, and rss. To the right, it says "Currently Archiving 10343 Exploits". The main content area features a banner with the text "The Exploit Database" and a subtext about being an archive for vulnerability researchers. Below this, a message about a general cleanup and submission policy is displayed, along with a note about DOS attacks. The page then transitions into a table titled "Remote Exploits" showing a list of vulnerabilities from January 2010.

Date	D	A	V	Description	Plat.	Author
2010-01-27	D	A	✓	CamShot v1.2 SEH Overwrite Exploit	windows	tecnik
2010-01-25	D	-	✓	AOL 9.5 Phobos.Playlist 'Import()' Buffer Overflow Exploit (Meta)	windows	Trancer
2010-01-22	D	A	✓	IntelliTamper 2.07/2.08 (SEH) Remote Buffer Overflow	windows	loneferret
2010-01-21	D	-	✓	EFS Easy Chat server Universal BOF-SEH (Meta)	windows	FB1H2S
2010-01-20	D	-	✓	AOL 9.5 ActiveX Oday Exploit (heap spray)	windows	Dz_attacker
2010-01-19	D	-	✓	Pidgin MSN <= 2.6.4 File Download Vulnerability	multiple	Mathieu GASPARD
2010-01-18	D	A	✓	Exploit EFS Software Easy Chat Server v2.2	windows	John Babio

<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

Udviklingsvitrne 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

solido_networks_solid_RGE

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 på udsinger

solido_networks_solid_RGE

Computeren skal vedtægts

Funktionen der misbruges skal vedtægts til

Executable stack

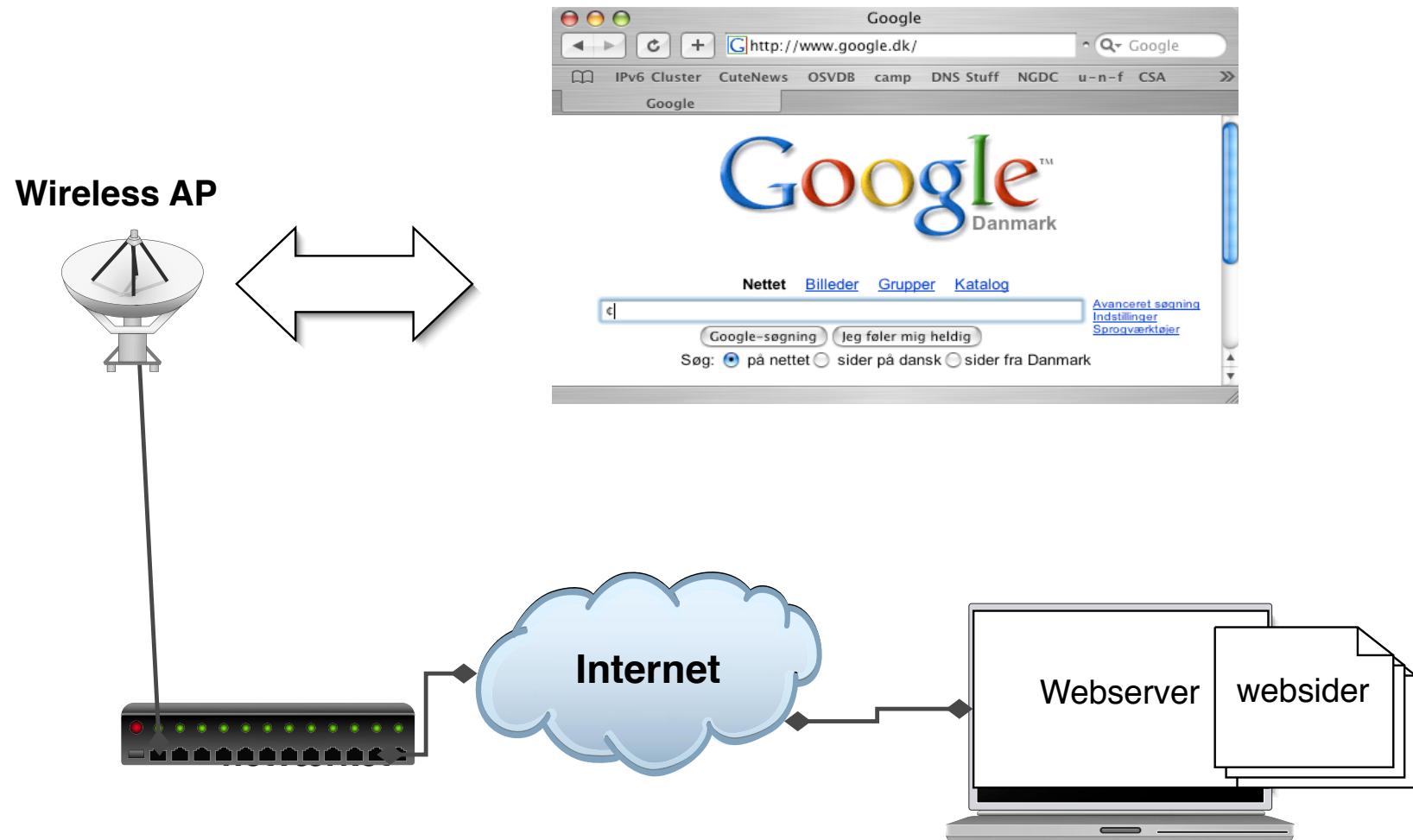
Executable heap

Fejl i programmet

alle programmer har fejl

Normal wireless brug

solido_networks_solid_RGE



BackTrack 5 og sniffer programmer

solido_networks_solid_RGE



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

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

Wireshark - grafisk pakkesniffer

solido_networks_solid_RGE

We're having a conference! You're invited!

Download Get Started Now

Learn Knowledge is Power

Enhance With Riverbed Technology

News And Events

Join us at SHARKFEST '15!
SHARKFEST '15 will be held from June 22 – 25 at the Computer History Museum in Mountain View, CA.
[Learn More ▶](#)

Troubleshooting with Wireshark
By Laura Chappell
Foreword by Gerald Combs
Edited by Jim Aragon
This book focuses on the tips and techniques used to identify

Wireshark Blog

Cool New Stuff
Dec 17 | By Evan Huus

Wireshark 1.12 Officially Released!
Jul 31 | By Evan Huus

To Infinity and Beyond! Capturing Forever with Tshark
Jul 8 | By Evan Huus

[More Blog Entries ▶](#)

Enhance Wireshark

Riverbed is Wireshark's primary sponsor and provides our funding. They also make great products.

802.11 Packet Capture

- WLAN packet capture and transmission
- Full 802.11 a/b/g/n support
- View management, control and data frames
- Multi-channel aggregation (with multiple adapters)

[Learn More ▶](#)

[Buy Now ▶](#)

<http://www.wireshark.org>

b til Windows og UNIX, tidligere kendt som Ethereal

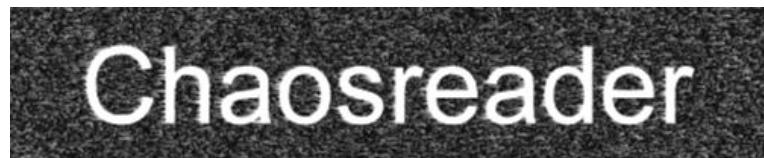
Programhygiejne!

solido_networks_solid_RGE

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.

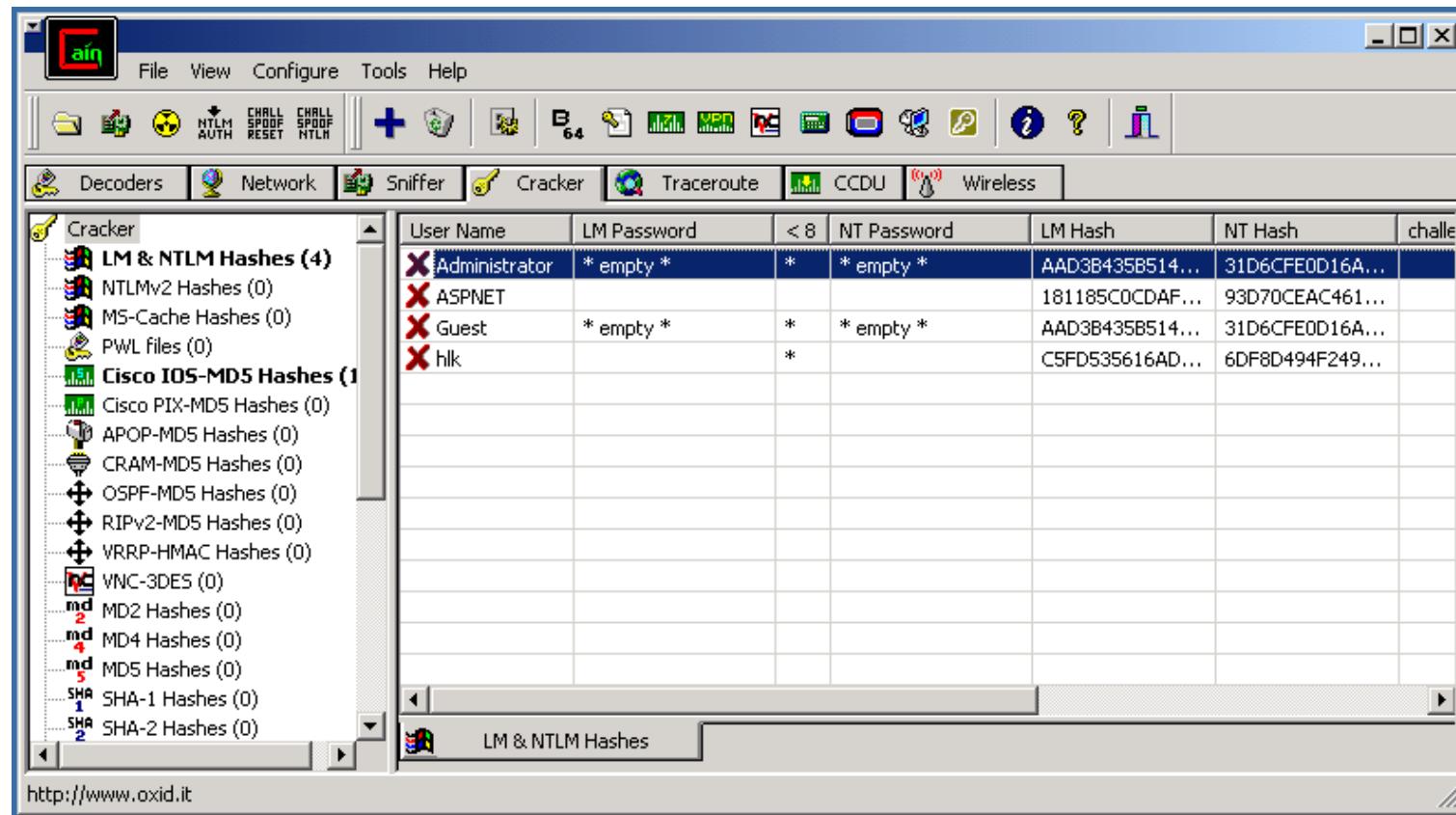
TCP/UDP/... Sessions

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 anbefales ofte istedet for 10phcrack <http://www.oxid.it>

Opbevaring af passwords

solido_networks_solid_RGE

The 5th Wave By Rich Tennant



"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_RGE

Er det tid til en lille pause?



What to do?

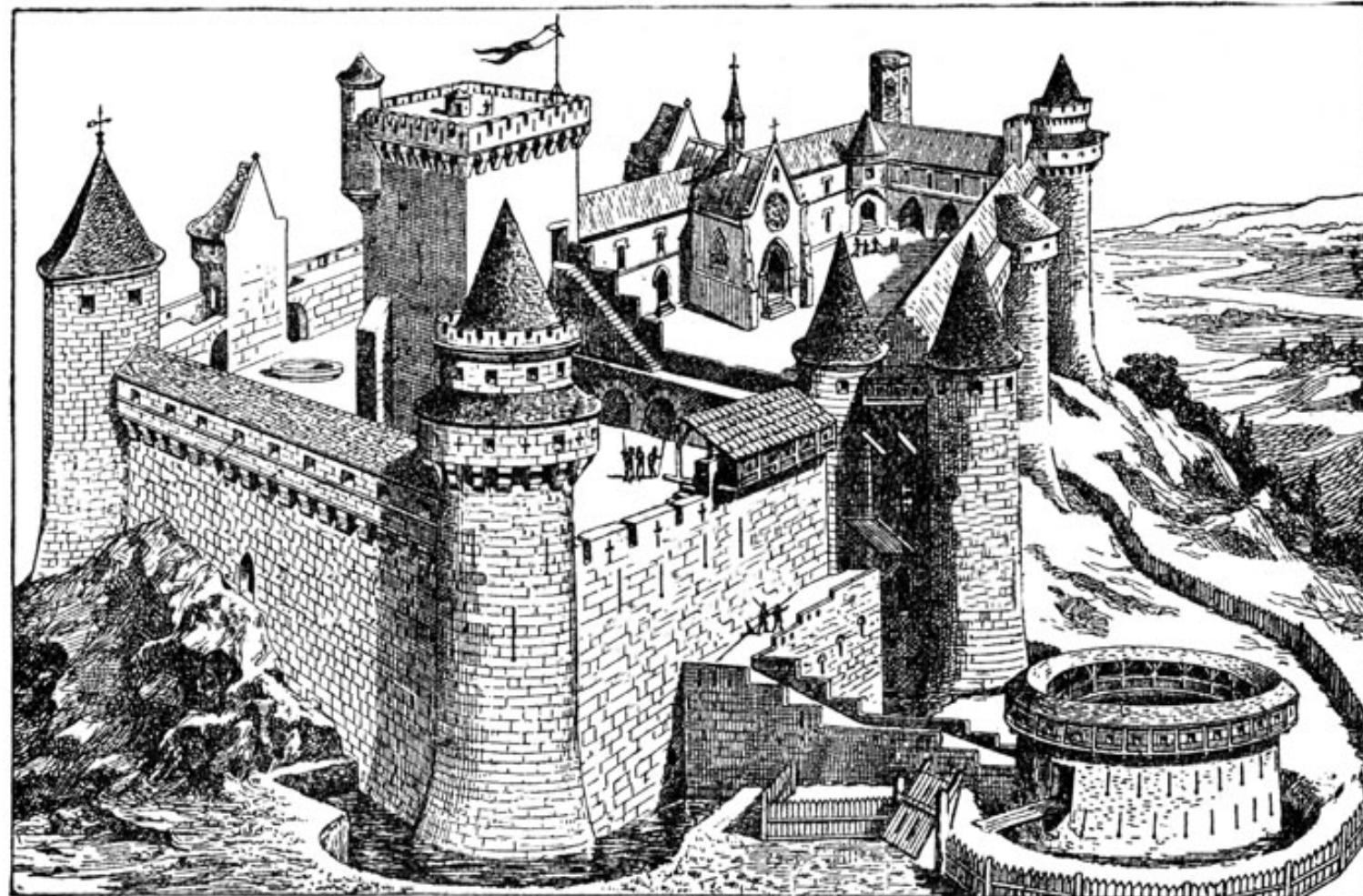
solido_networks_solid_RGE



What do we do?

Enhance and secure runtime environment

solido_networks_solid_RGE



Sidste chance er pfviklingstidspunktet

Gode operativsystemer

solido_networks_solid_RGE

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 fmedded systemer har beskyttelse!

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 compromised 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](#):

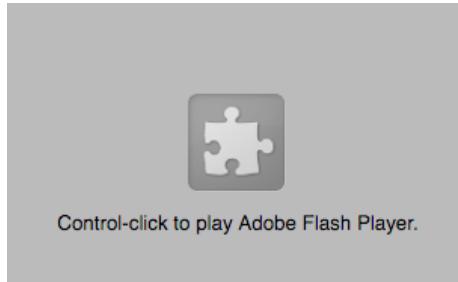
1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit [executable program](#), [ActiveX component](#), or [Java applet](#)). This is usually caused by poor security design [clarification needed]. The user should not be 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_RGE



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

solido_networks_solid_RGE

File Transfer Protocol - filoverfler

FTP bruges istil:

- FTP - drivere, dokumenter, rettelser - Windows Update? er enten HTTP eller FTP
- Opdatering af websites
- Overføl 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

solido_networks_solid_RGE

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

solido_networks_solid_RGE

POP3 sender brugernavn og kodeord i klartekst - ligesom FTP

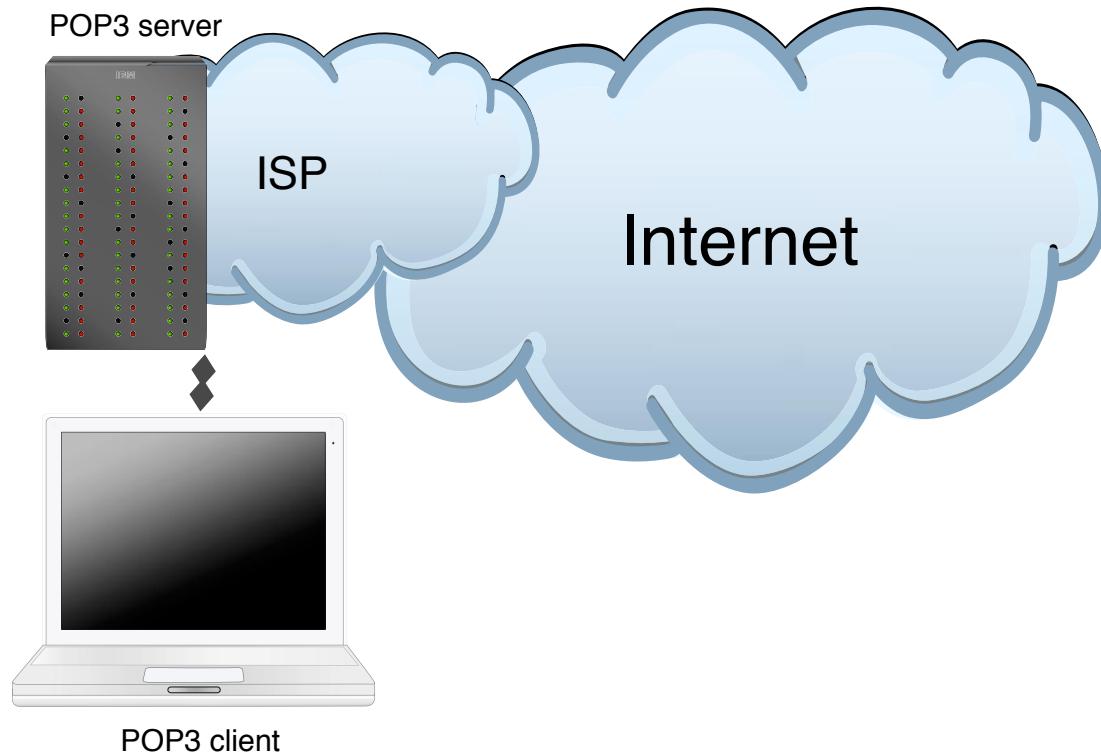
bruges dagligt af næn alle privatkunder

alle internetudbydere og postudbydere tilbyder POP3

der findes en variant, POP3 over SSL/TLS

POP3 i Danmark

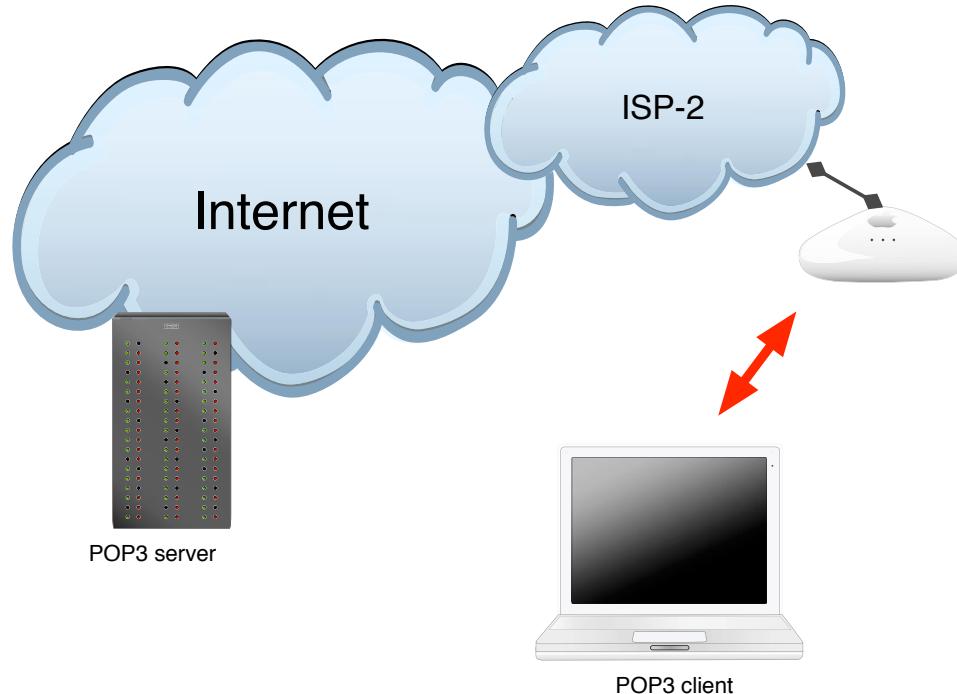
solido_networks_solid_RGE



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

POP3 i Danmark - tr

solido_networks_solid_RGE



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_RGE

The whiteboard features a title 'Wall of Sheep' flanked by cartoon sheep illustrations. Below the title is a table with the following columns: login, port, domain, ip, application, and MAC address. The table lists various user accounts with their corresponding details.

login	port	domain	ip	application	MAC address
Tin	*****		00:15:89:50:19:3D	BLUETOOTH	00:15:89:50:19:3D
kriget	80*****	defcon.us	HTTP		00:15:89:50:19:3D
1525939 (Mare)	80*****	crashsheep.com	HTTP		00:15:89:50:19:3D
calculator	80*****	sheep.com	HTTP		00:15:89:50:19:3D
patterns	80*****	Via	152.75.7.159	FTP	00:15:89:50:19:3D
recyclaholic	80*****	hey	130.199.165.26	FTP	00:15:89:50:19:3D
livesgreen	976*****	976*****	69.17.317.59	POP3	00:15:89:50:19:3D
ranger1	417*****	domeranger.com	POP3		00:15:89:50:19:3D
bomber	41*****	domeranger.com	POP3		00:15:89:50:19:3D
overrider	123*****	postech.ac.kr	HTTP		00:15:89:50:19:3D
eldam	80*****	www.rakn.no	HTTP		00:15:89:50:19:3D
rendytte	80*****	dharm.org	IRC		00:15:89:50:19:3D
gore	80*****	149.174.31.17	POP3		00:15:89:50:19:3D
jedi	80*****	71.32.58.185	HTTP		00:15:89:50:19:3D
colinair	17*****	17.250.248.152	IMAP		00:15:89:50:19:3D
Ljungqvist	80*****	Mugayz.de	IMAP		00:15:89:50:19:3D
junkka	80*****	206.190.56.350	HTTP		00:15:89:50:19:3D
equalek	80*****	deutschlandserver.de	HTTP		00:15:89:50:19:3D
maulder	80*****	70.85.30.16.9	HTTP		00:15:89:50:19:3D
vad35924	80*****	Ip.vad35924.jp	HTTP		00:15:89:50:19:3D
149329010	80*****	64.12.561.853	ICQ		00:15:89:50:19:3D
ekrasus	80*****	ekrasusfeld.org	POP3		00:15:89:50:19:3D
ed	80*****	206.130.97.207	POP3		00:15:89:50:19:3D
1001432	80*****	chimichangapizza.com	HTTP		00:15:89:50:19:3D

Defcon Wall of Sheep
Husk nu at vi er venner her! - idag er det kun teknikken

Twitter news

solido_networks_solid_RGE

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

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

solido_networks_solid_RGE

Egypten, Sudan, Tunesien, ...

Den der kontrollerer ISPerne kontrollerer trafikken

Facebook revolutionerne

Blokering er umulig, men det forss

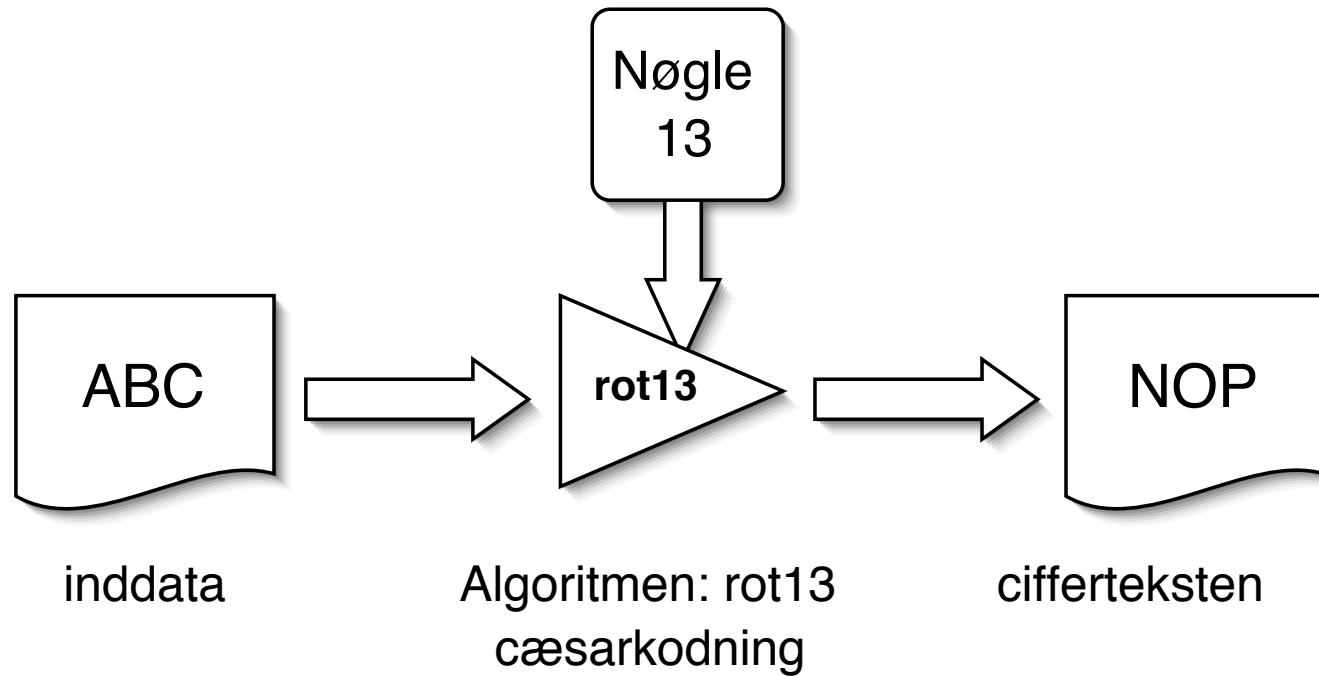
Spredning af falsk information

Diginotar Dutch Certificate Authority

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

Kryptografi

solido networks solid RGE

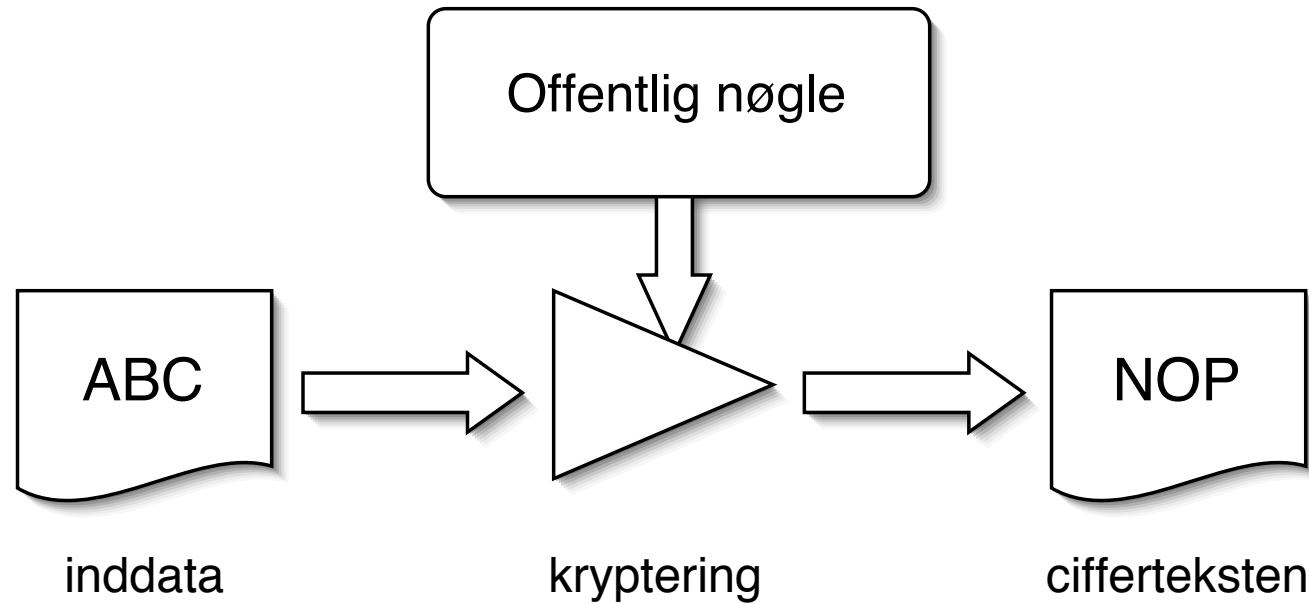


Kryptografi er ln om, hvordan man kan kryptere data

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

Public key kryptografi - 1

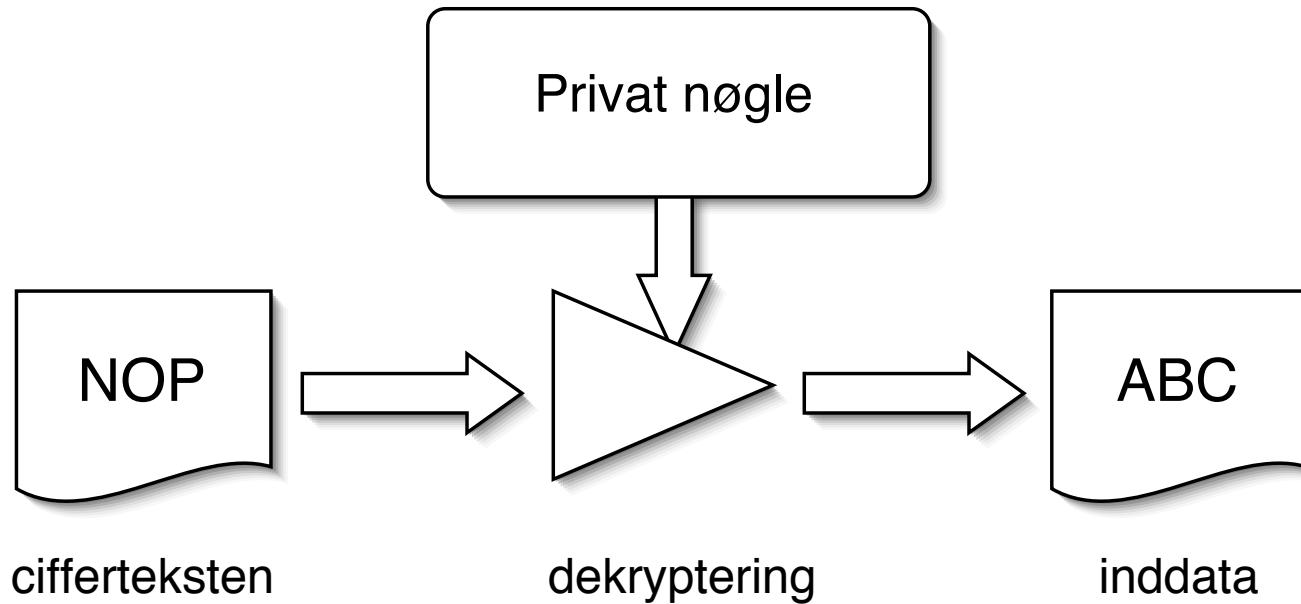
solido_networks_solid_RGE



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

solido_networks_solid_RGE



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

solido_networks_solid_RGE

Algoritmerne er kendte

Nerne er hemmelige

Ner har en vis levetid - de skal skiftes ofte

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

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

Se evt. Snake Oil Warning Signs: Encryption Software to Avoid <http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>

AES

Advanced Encryption Standard

DES kryptering baseret 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/>

Formt med kryptering

solido_networks_solid_RGE

kryptering er den eneste måt sikre:

fortrolighed

autenticitet / integritet

Single user mode boot

solido_networks_solid_RGE

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 tilfælde 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_RGE



Target: Macbook disk'en

Press t to enter ☺

<http://support.apple.com/kb/ht1661>

harddisk beskyttelse og data kryptering

solido_networks_solid_RGE



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

Kryptering af e-mail

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

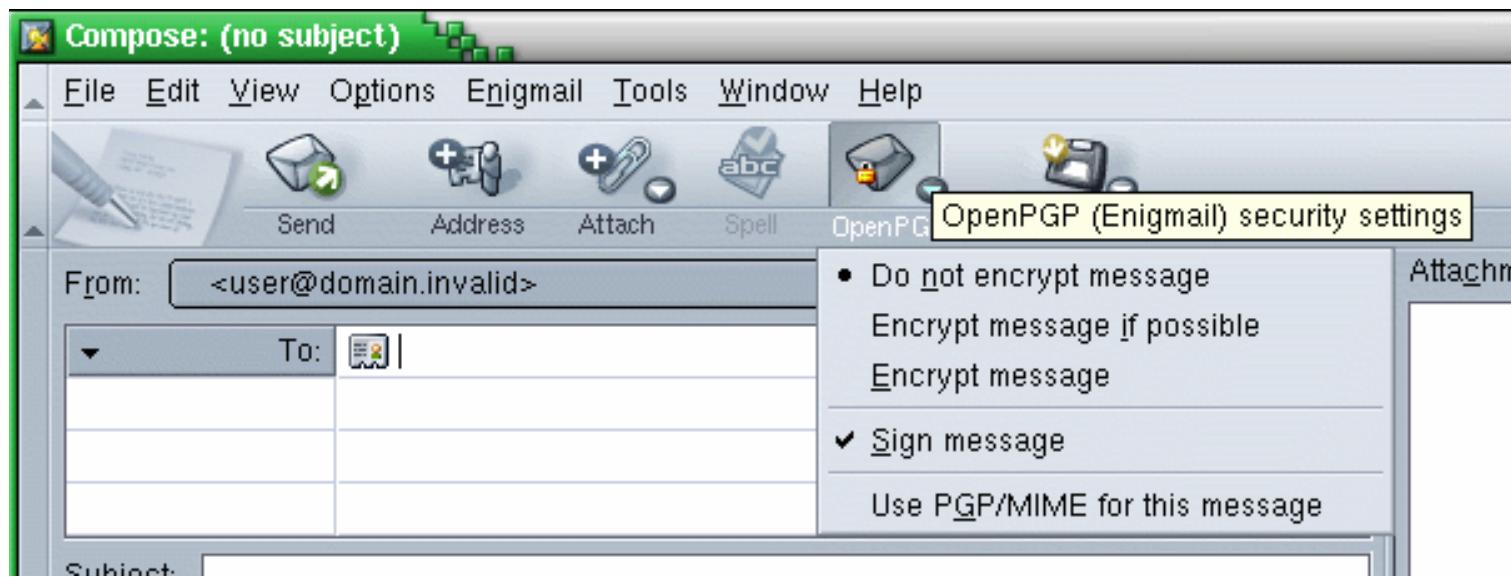
Kryptering af sessioner SSL/TLS

- 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

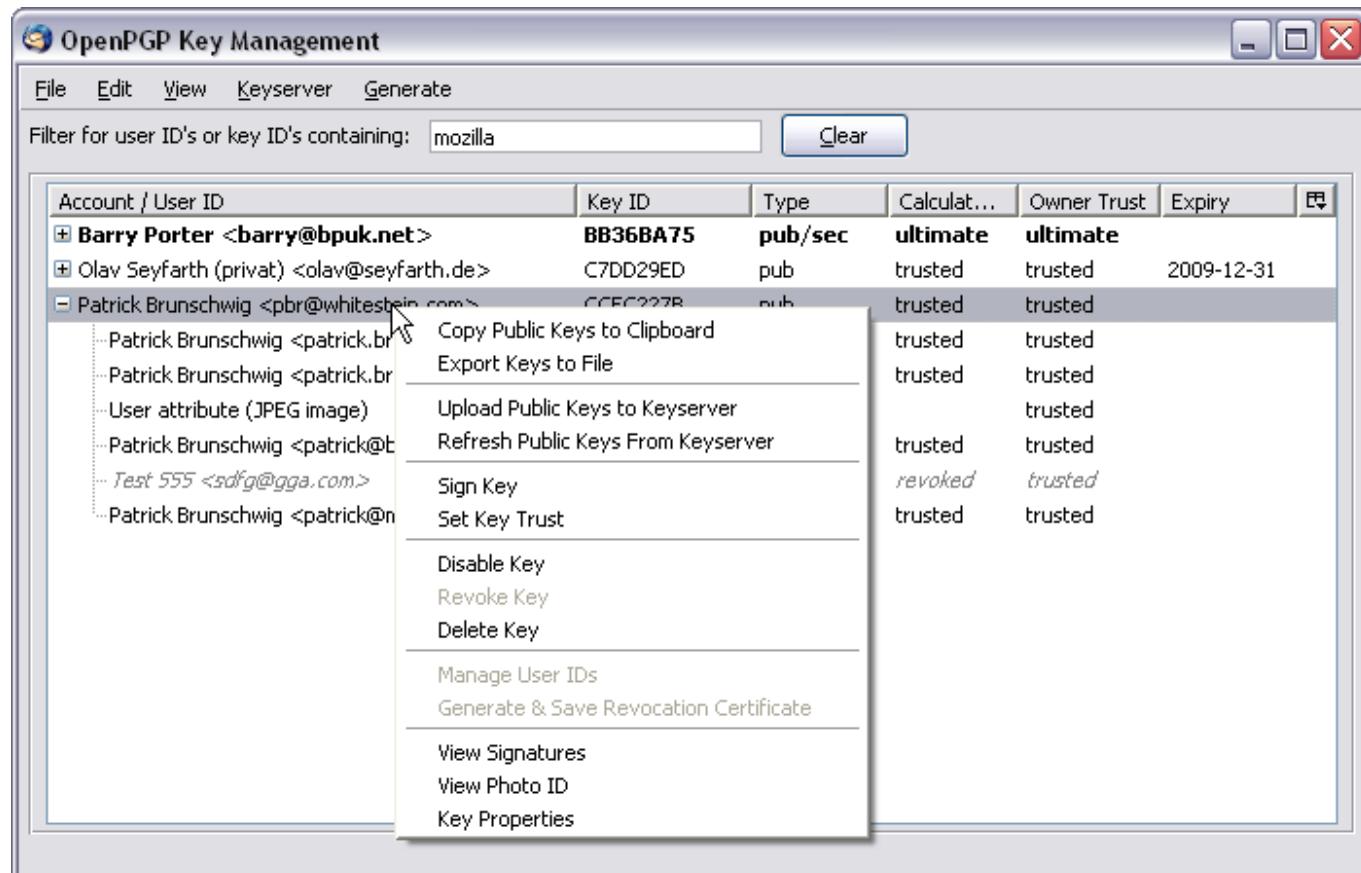
solido_networks_solid_RGE



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

Enigmail - OpenGPG Key Manager

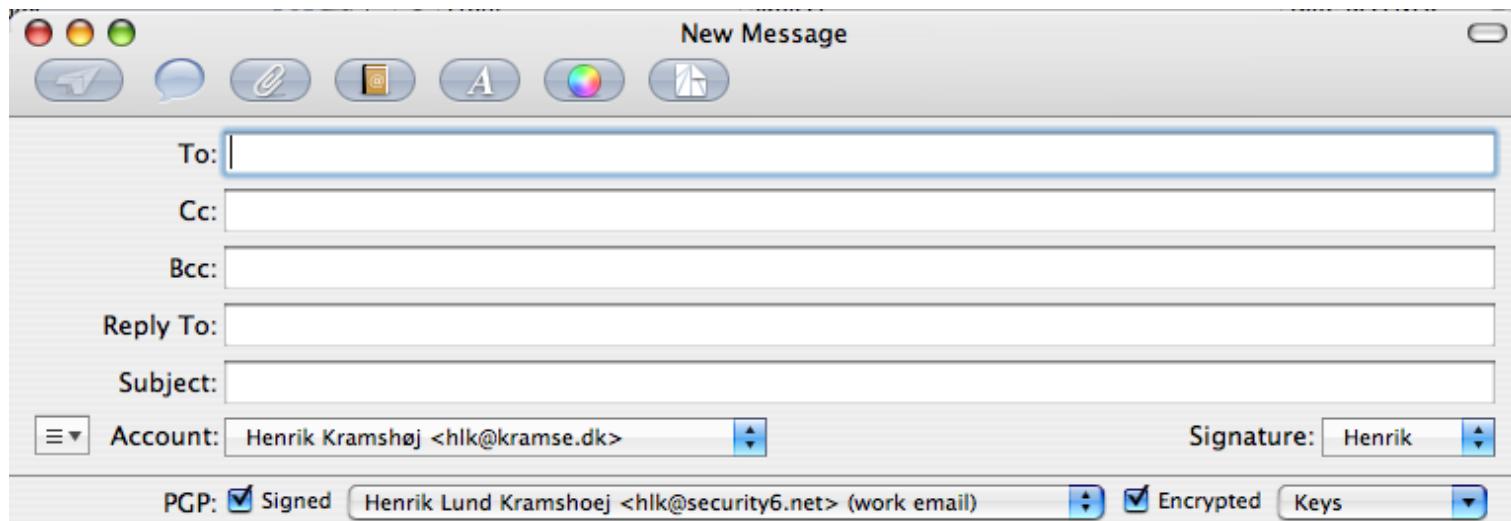
solido_networks_solid_RGE



Key Manager funktionaliteten i Enigmail kan anbefales

GPGMail plugin til Mac OS X Mail.app

solido_networks_solid_RGE

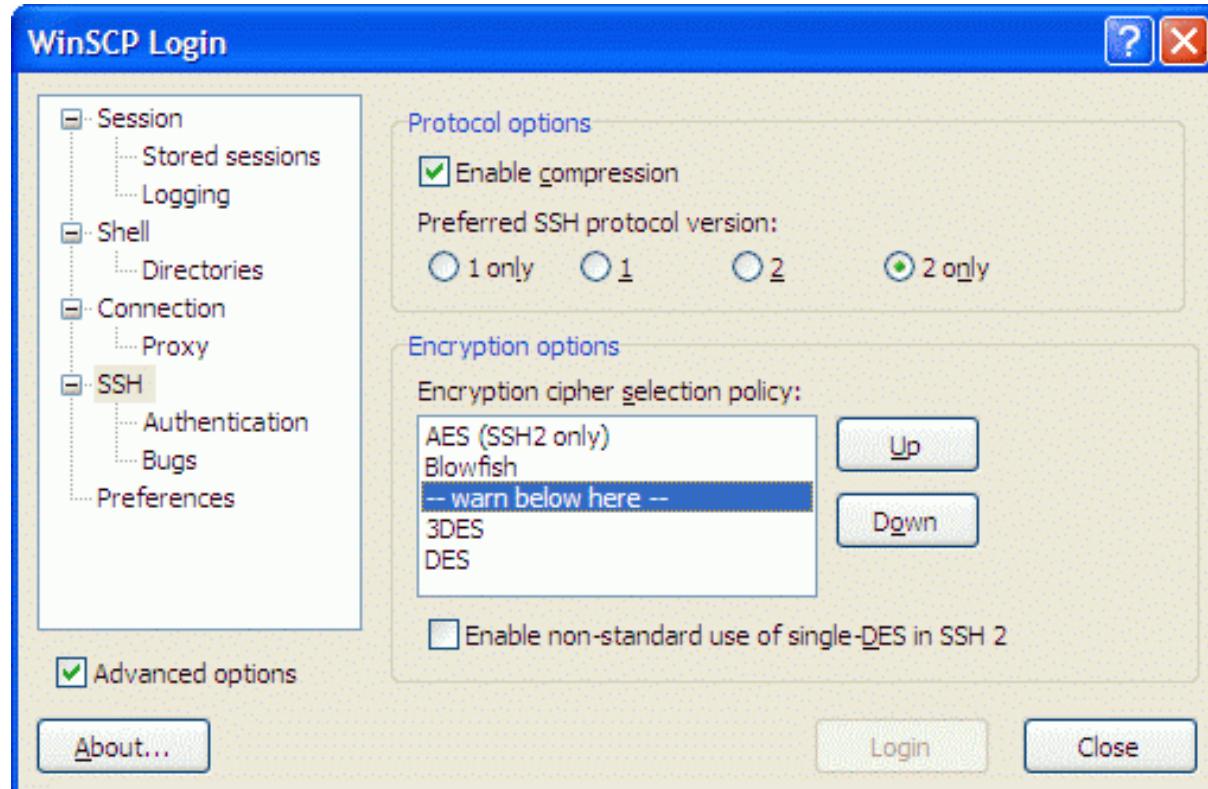


--
Henrik Lund Kramshøj, cand.scient, CISSP
e-mail: hlk@security6.net, tlf: 2026 6000
www.security6.net - IPv6, sikkerhed, netværk
Follower of the Great Way of Unix

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

Grafisk Secure Copy - WinSCP

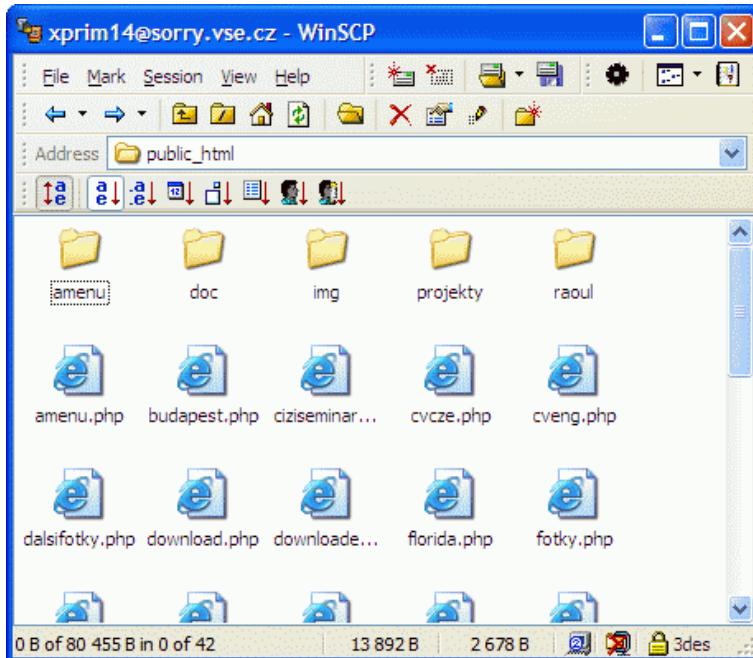
solido_networks_solid_RGE



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

Grafisk Secure Copy - WinSCP

solido_networks_solid_RGE



benytter Secure Shell protkollen (SSH)

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

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

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

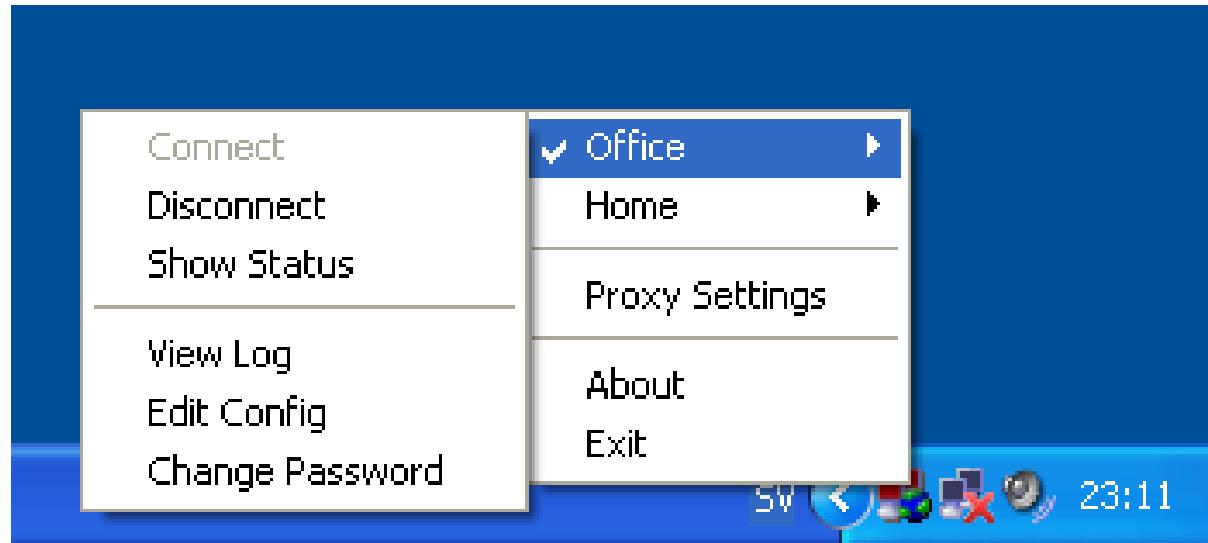
De snakker ikke ret godt sammen pv. Brug IPsec for dette.

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

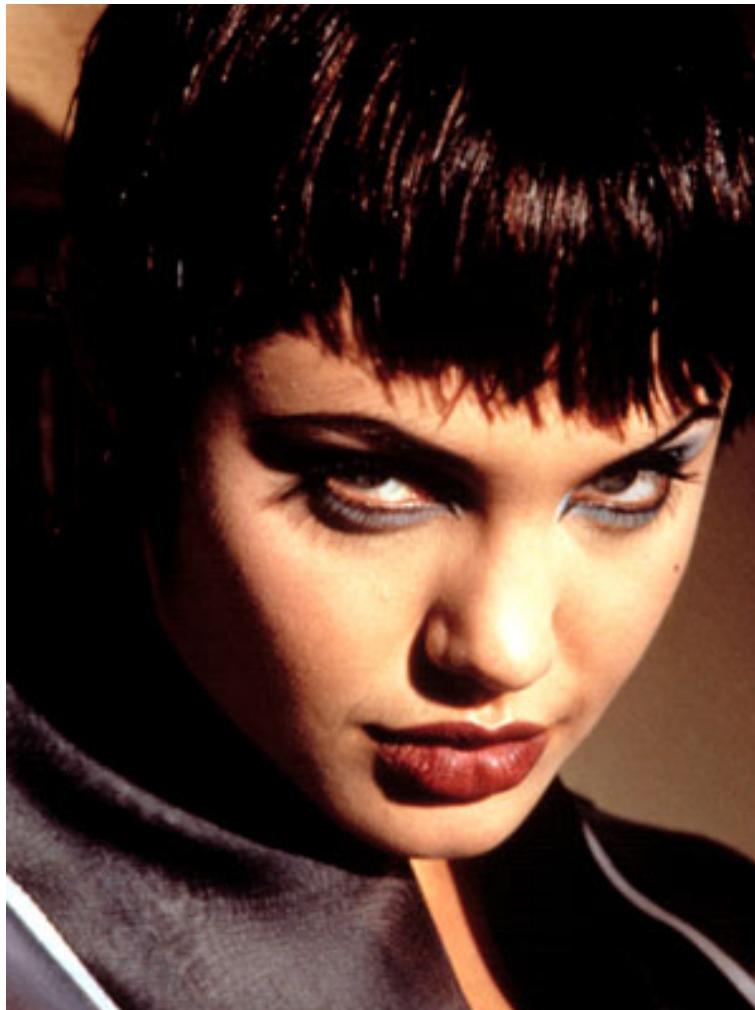
solido_networks_solid_RGE



OpenVPN GUI - easy to use

Hackertyper anno 1995

solido_networks_solid_RGE



Lad os lige gilbage til hackerne

Hackertyper anno 2008

solido_networks_solid_RGE



Lisbeth laver PU, personunderslser ved hj af hacking

Hvordan finder man information om andre

Fra mtre til person

solido_networks_solid_RGE

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

solido_networks_solid_RGE

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

solido_networks_solid_RGE

Email

DNS

Ger

Google

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

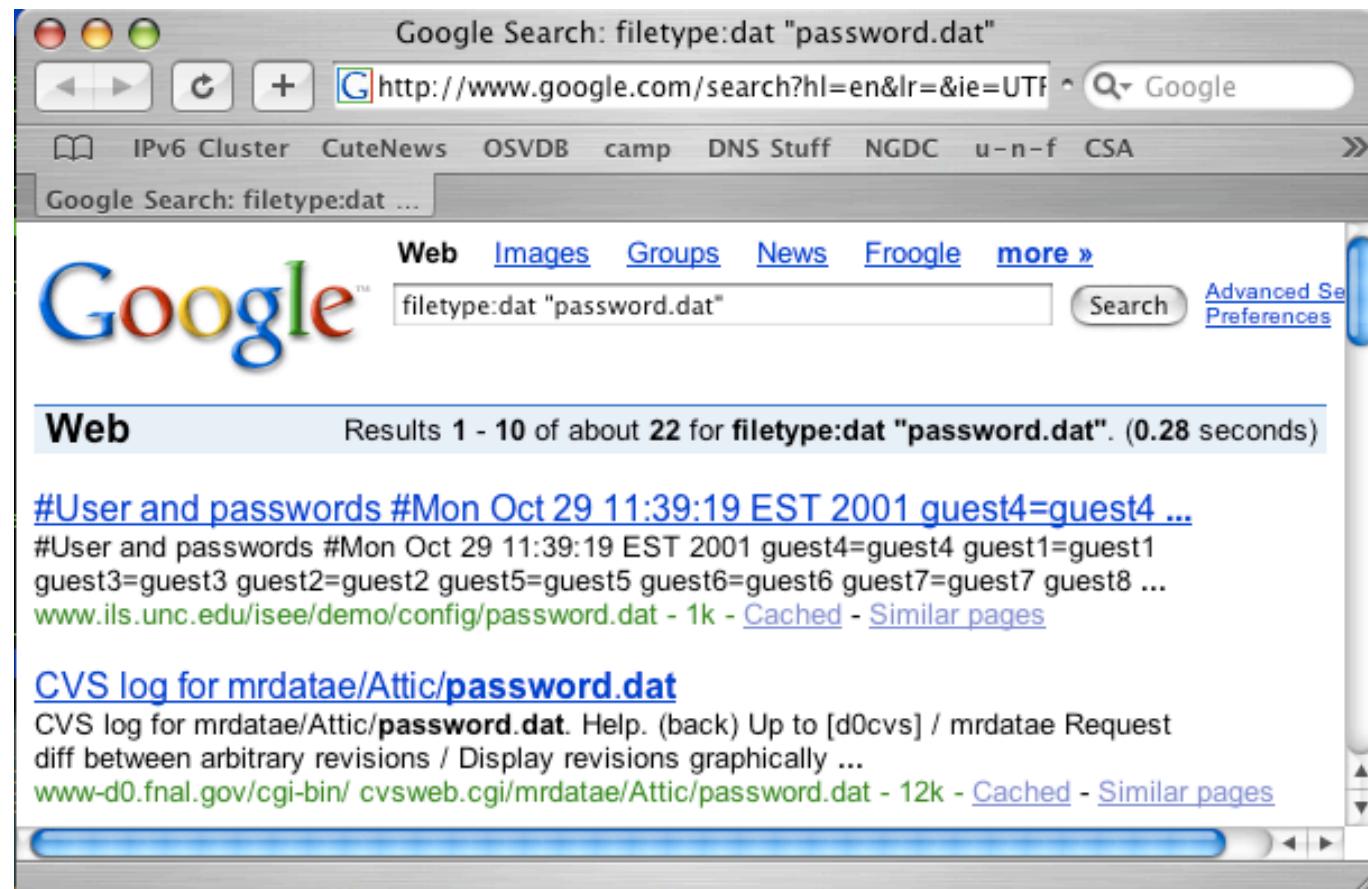
IP adresserne administreres i dagligdagen af et antal Internet registries, hvor de står er:

- 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 modsætning til Local Internet Registries (LIRs) og National Internet Registry (NIR)

Google for it

solido_networks_solid_RGE

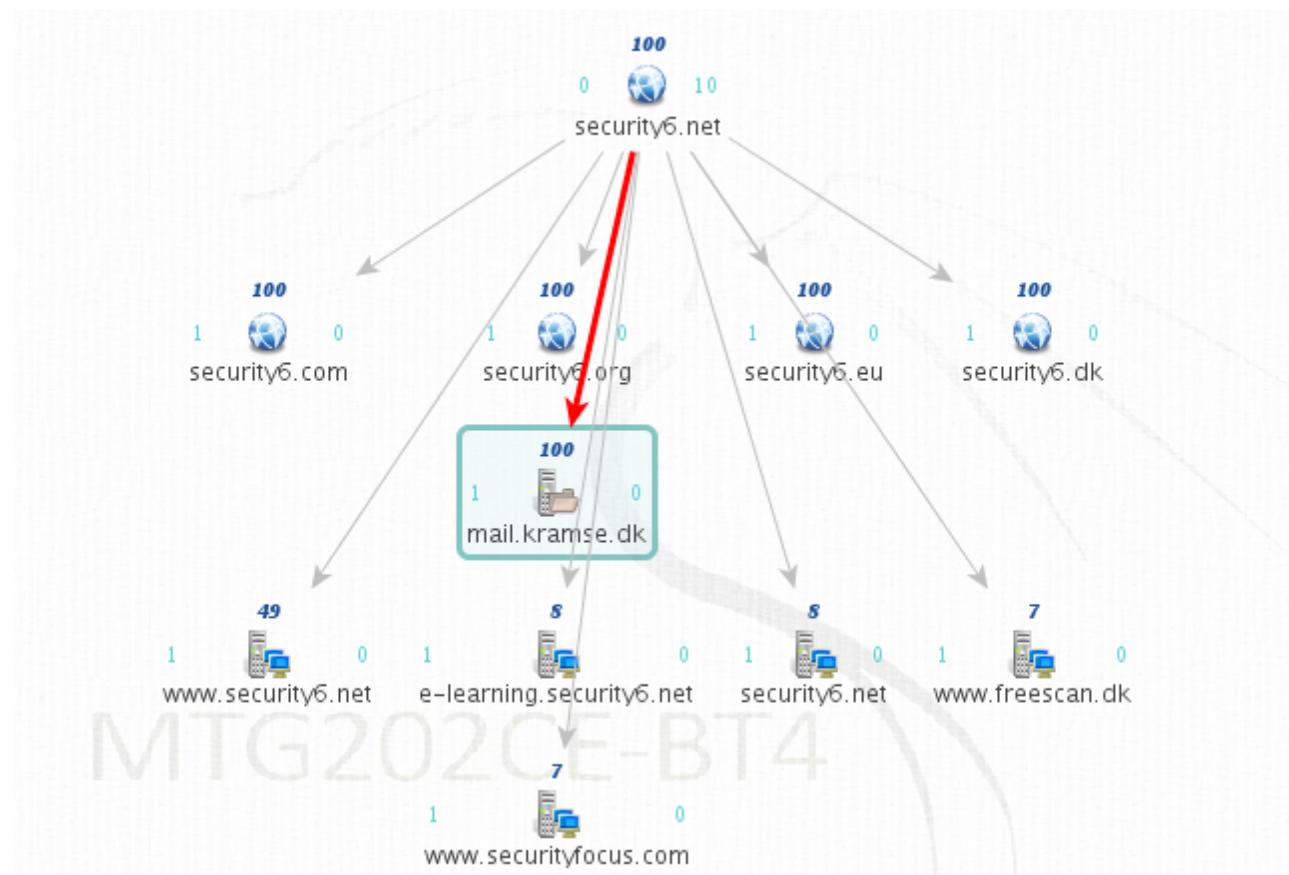


Google som hacker vt

Googledorks <http://johnny.ihackstuff.com/>

Listbeth in a box?

solido_networks_solid_RGE



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

Er du passende paranoid?

solido_networks_solid_RGE



Vpagt

Hvordan bliver du sikker

solido_networks_solid_RGE

Lad v med at bruge computere

Lad v med at bruge en 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

solido_networks_solid_RGE

- 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

solido_networks_solid_RGE



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

Distribueret CTF med 6 hold og arrangeret 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?

solido_networks_solid_RGE

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

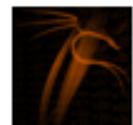
<http://www.solidonetworks.com>

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

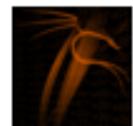
informationskilder

solido_networks_solid_RGE



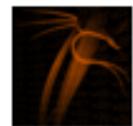
exploitdb [webapps] – BPAffiliate Affiliate Tracking
Authentication Bypass Vulnerability: <http://bit.ly/9LOC3K>

about 5 hours ago via twitterfeed



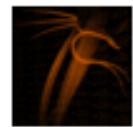
exploitdb [webapps] – BPDirectory Business Directory
Authentication Bypass Vulnerability: <http://bit.ly/c4TeLz>

about 5 hours ago via twitterfeed



exploitdb [webapps] – BPConferenceReporting Web Reporting
Authentication Bypass Vulnerability: <http://bit.ly/cM61AK>

about 5 hours ago via twitterfeed



exploitdb [webapps] – BPRalestate Real Estate
Authentication Bypass Vulnerability: <http://bit.ly/bYx2aY>

about 5 hours ago via twitterfeed



sans_isc [Diary] Mac OS X Server v10.6.5 (10H575) Security
Update: <http://support.apple.com/kb/HT4452>, (Tue, Nov
16th): <http://bit.ly/azBrso>

about 7 hours ago via twitterfeed

Nye kilder til information:

har twitter af! RSS? NB: favoritsite <http://isc.sans.edu/index.html>

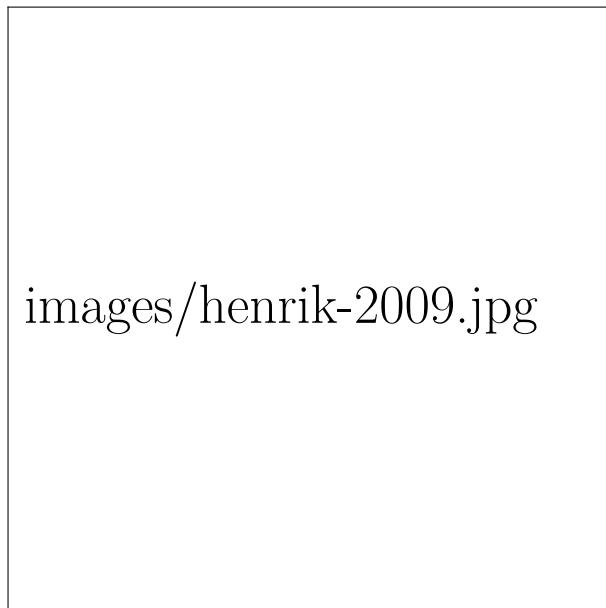
VikingScan.org - free portscanning

solido_networks_solid_RGE

The screenshot shows a web browser window titled "Welcome to VikingScan". The address bar displays "miniscan.vikingscan.org". The main content area is titled "VikingScan.org - free port scanning for IPv4 and IPv6". It includes a navigation bar with "Home" and "Miniscan List" links. A message states: "On this page you can configure and start a portscan of your IP-address from this server. Your IP-address is: 79.142.233.18". Below this is a large button labeled "Configure and start a scan of the IP-address". A note below the button says: "Note that this service is currently software in development and you also need to make sure that you are allowed to scan the IP-address specified.". At the bottom, copyright information reads: "© 2011 VikingScan.org: Free portscanning <http://www.vikingscan.org>". To the right of the main content, there is a logo for "SOLIDO NETWORKS" featuring a stylized orange bird icon. Text next to the logo says: "VikingScan.org is a service of Solido Networks ApS". Another paragraph explains: "Solido Networks provides this service for the community for free. If you need firewalls, penetration testing, security consulting please visit [Solido Networks ApS](#)".

Kontaktinformation og profil

solido_networks_solid_RGE



- 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

solido_networks_solid_RGE

Reklamer: kursusafholdelse

solido_networks_solid_RGE

Fønde 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 virksomhedsnetv.
- 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