

Welcome to

Hacking and social media - controlling your data

Henrik Lund Kramshøj
hlk@solidonetworks.com

<http://www.solidonetworks.com>

Goal of this presentation



Don't Panic!

Talk about social media

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

Agenda

What are social media

Hacking protocols technical tools - various tools

Basic recommendations, encryption, add-ons for browsers etc.

The term Social Media refers to the use of web-based and mobile technologies to turn communication into an interactive dialogue. Andreas Kaplan and Michael Haenlein define social media as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content." [1]

Social media are media for social interaction, as a superset beyond social communication. Enabled by ubiquitously accessible and scalable communication techniques, social media substantially change the way of communication between organizations, communities, as well as individuals. [2]

Source: http://en.wikipedia.org/wiki/Social_media

Really what is social media

Kramses blog
Henrik Kramshøj personal blog

Search:

Switch to Elastic Layout

Kramses blog store

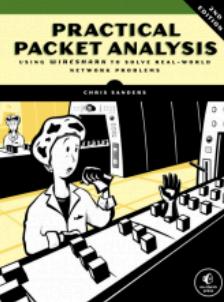
Classic Shell Scripting
Arnold Robbins, New £17.09 Best £9.64

The Book of Postfix
Ralf Hildebrandt, Best £72.27

THE BOOK OF PF
Peter N.M. Hansteen, New £22.79 Best £8.10

Thursday, 15 September 2011
[Practical Packet Analysis, 2nd Edition](#)

Practical Packet Analysis, 2nd Edition
Using Wireshark to Solve Real-World Network Problems by Chris Sanders
ISBN: 978-1-59327-266-1
Paperback: 280 pp
Publisher: No Starch Press July 2011



Review by Henrik Lund Kramshøj, hlk@kramse.org



ipvb

Are open source communities social media?

Uncontrolled data - for good and bad

Amateur websites, good ideas, bad implementation

Insecure protocols:

- SMTP Simple Mail Transfer Protocol
- HTTP Hyper Text Transfer Protocol
- Chat, instant messaging etc.

Friends - uploading that one *funny* picture or pranks

Ex-girlfriend, ex-boyfriend

Hackers

Also serious - governments - not discussed further right now.

Its just a prank



[Advanced search](#)

About 28,000,000 results (0.15 seconds)

[Slutty Ex Girlfriends - Ex Girlfriend Nude Pics!](#)

www.sluttyexgf.com/ 

Everybody loves girlfriends but more than that everybody loves **ex girlfriends** exposed.
Next Door GFs. I don't mind watching them naked and fucked as long as ...

[Watch Me Fuck My Teen Slut Ex Girlfriend - SlutLoad.com](#)

www.slutload.com/.../Watch-Me-Fuck-My-Teen-Slut-Ex-Girlfriend.h... 

Now you get to see me fuck my **ex girlfriend** in her tight sweet teen pussy.

[Ex Girlfriend slut gets fuckt and sucks Homemade - SlutLoad.com](#)

www.slutload.com/.../Ex-Girlfriend-slut-gets-fuckt-and-sucks-Home... 

This redhead with two pierced nipples doing a great job fucking her man ...

 Show more results from slutload.com



The Streisand effect is a primarily online phenomenon in which an attempt to hide or remove a piece of information has the unintended consequence of publicizing the information more widely. It is named after American entertainer Barbra Streisand, whose attempt in 2003 to suppress photographs of her residence inadvertently generated further publicity.

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

BBC Mobile News | Sport | Weather | Travel | TV |

NEWS EUROPE

Home | UK | Africa | Asia-Pac | Europe | Latin America | Mid-East | South Asia | US & Canada | Business | He

5 October 2011 Last updated at 21:22 GMT 552 Share 

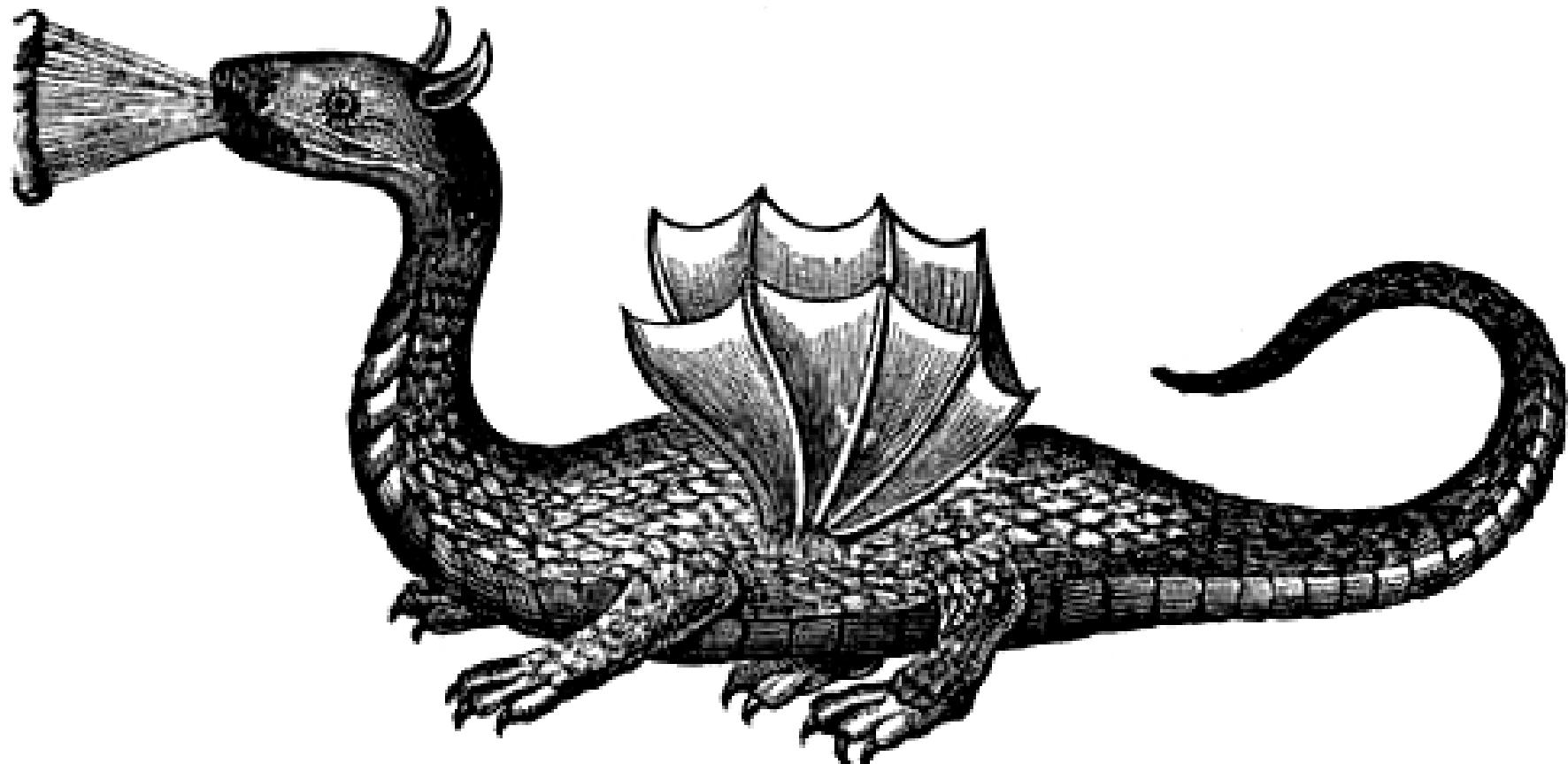
Italy wiretap law: Wikipedia hides pages in protest



Opponents of the draft law say Mr Berlusconi is seeking to gag his critics

<http://www.bbc.co.uk/news/world-europe-15192757>

Internet - Here be dragons



Matrix style hacking anno 2003



http://www.youtube.com/watch?v=511GCTgqE_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

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

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

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

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



Hacking ligner indimellem magi



Hacking kræver blot lidt ninja-træning



Der benyttes en del værktøjer:

- Nmap - <http://www.insecure.org> portscanner
- Wireshark - <http://www.wireshark.org/> avanceret netværkssniffer
- BackTrack <http://www.backtrack-linux.org> includes more than 300 hacker tools

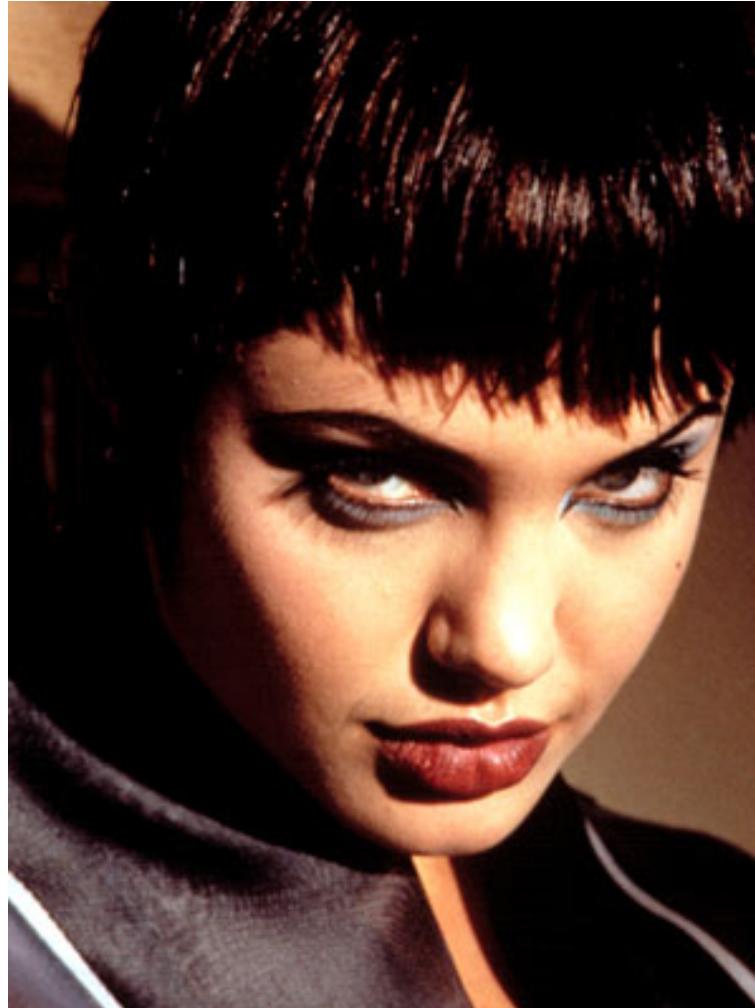
Why are we allowed to download these tools?

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

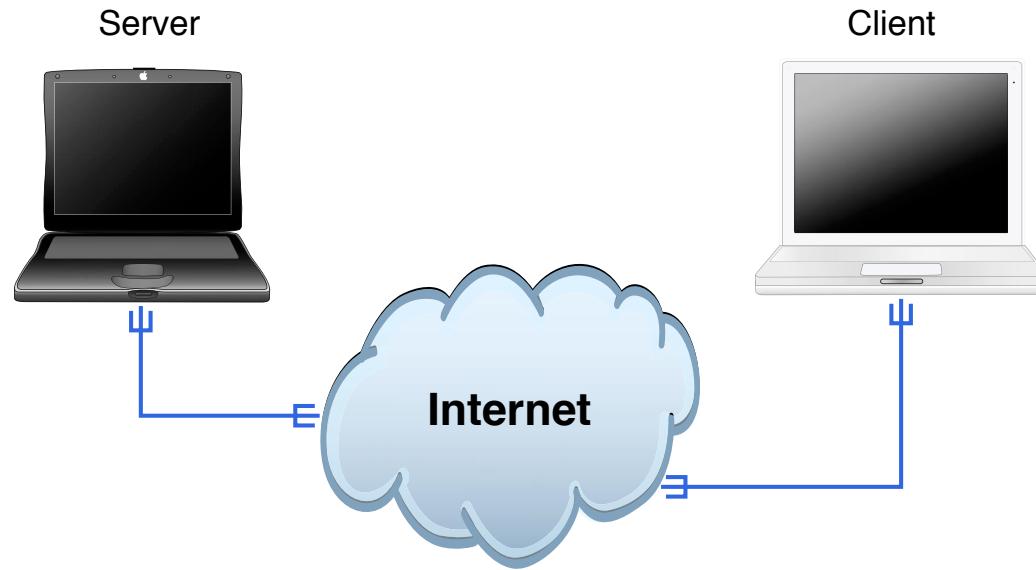
Hacking kan betyde:

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

Introduktion til hacking



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



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

We have seen lots of hacker stories, and we learn:

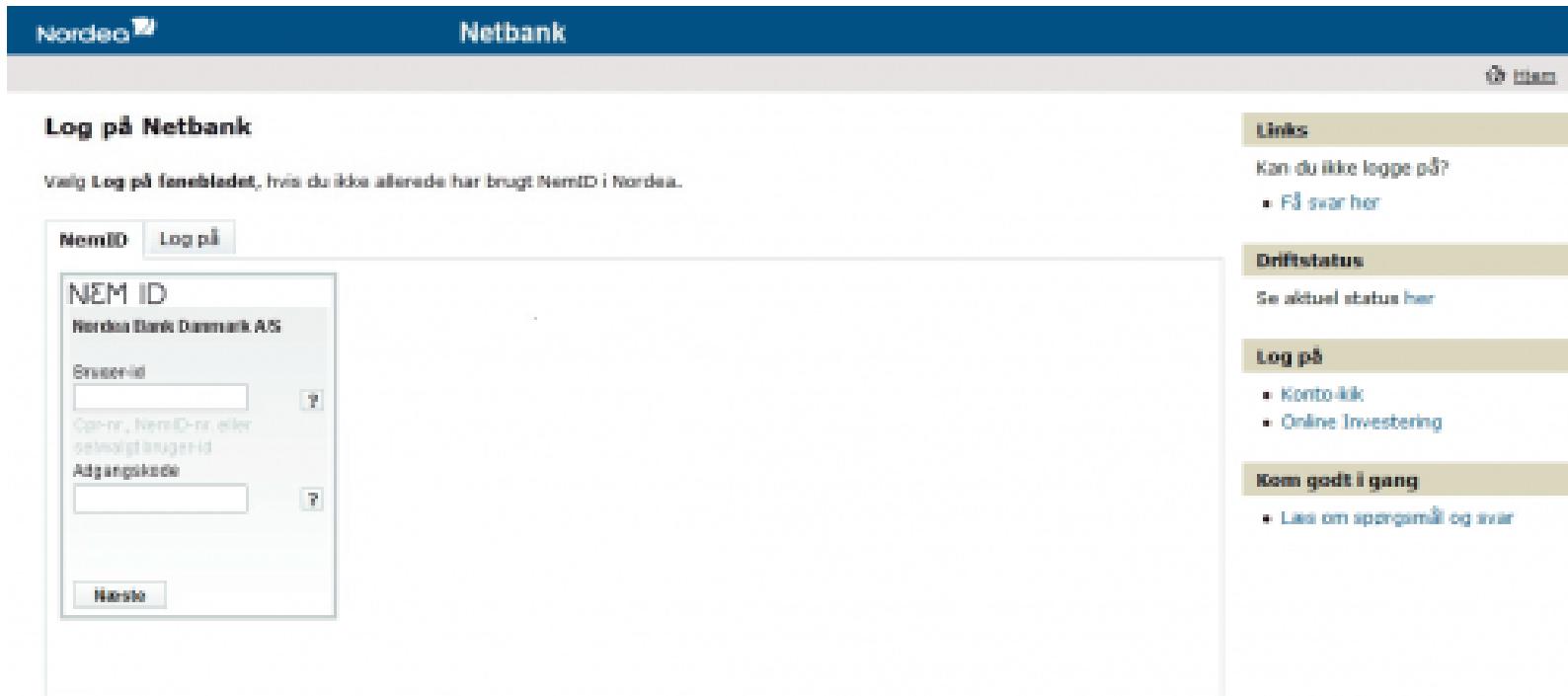
We are all targets of hacking

Social Engineering rockz! Phishing works.

Anyone can be hacked - resources used to protect vs attackers resources

Hacking is not cool

Secure web sites



The screenshot shows the Nordica Netbank login interface. At the top, there's a header with the Nordica logo and the word "Netbank". Below the header, a sub-header says "Log på Netbank". A message below it reads: "Vælg Log på fanebladet, hvis du ikke allerede har brugt NemID i Nordica.". A "NemID" button is highlighted in blue, while "Log på" is in grey. The main form is titled "NEM ID" and belongs to "Nordica Bank Danmark A/S". It contains fields for "Brugernavn" (User name) and "Adgangskode" (Access code), each with a question mark icon. A "Hængebil" (Handbag) button is at the bottom. To the right, there are several sections: "Links" with a link to "Få svar her"; "Driftstatus" with a link to "Se aktuel status her"; "Log på" with links to "Konto tilk" and "Online Investering"; and "Kom godt i gang" with a link to "Læs om spørgsmål og hvor". At the bottom left, there are two blue links: "Endre brugernavn og log på" and "Endre adgangskode og log på". A note at the bottom center states: "Denne forbindelse er sikret af SSL-kryptering. For at kontrollere at du har forbindelse til Nordica, kan du klikke på hængebil". The footer has a copyright notice: "© Nordica 2009".

[Endre brugernavn og log på](#)

[Endre adgangskode og log på](#)

 Denne forbindelse er sikret af SSL-kryptering. For at kontrollere at du har forbindelse til Nordica, kan du klikke på hængebil.

© Nordica 2009

Sources:

<http://www.computerworld.dk/art/198273?a=rss&i=0>

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

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



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.websrcmd=_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.websrcmd=_account-run.CaseIDNumberPP-046-631-789

Kan du selv genkende Phishing



Fear, uncertainty and doubt

http://en.wikipedia.org/wiki/Fear,_uncertainty_and_doubt



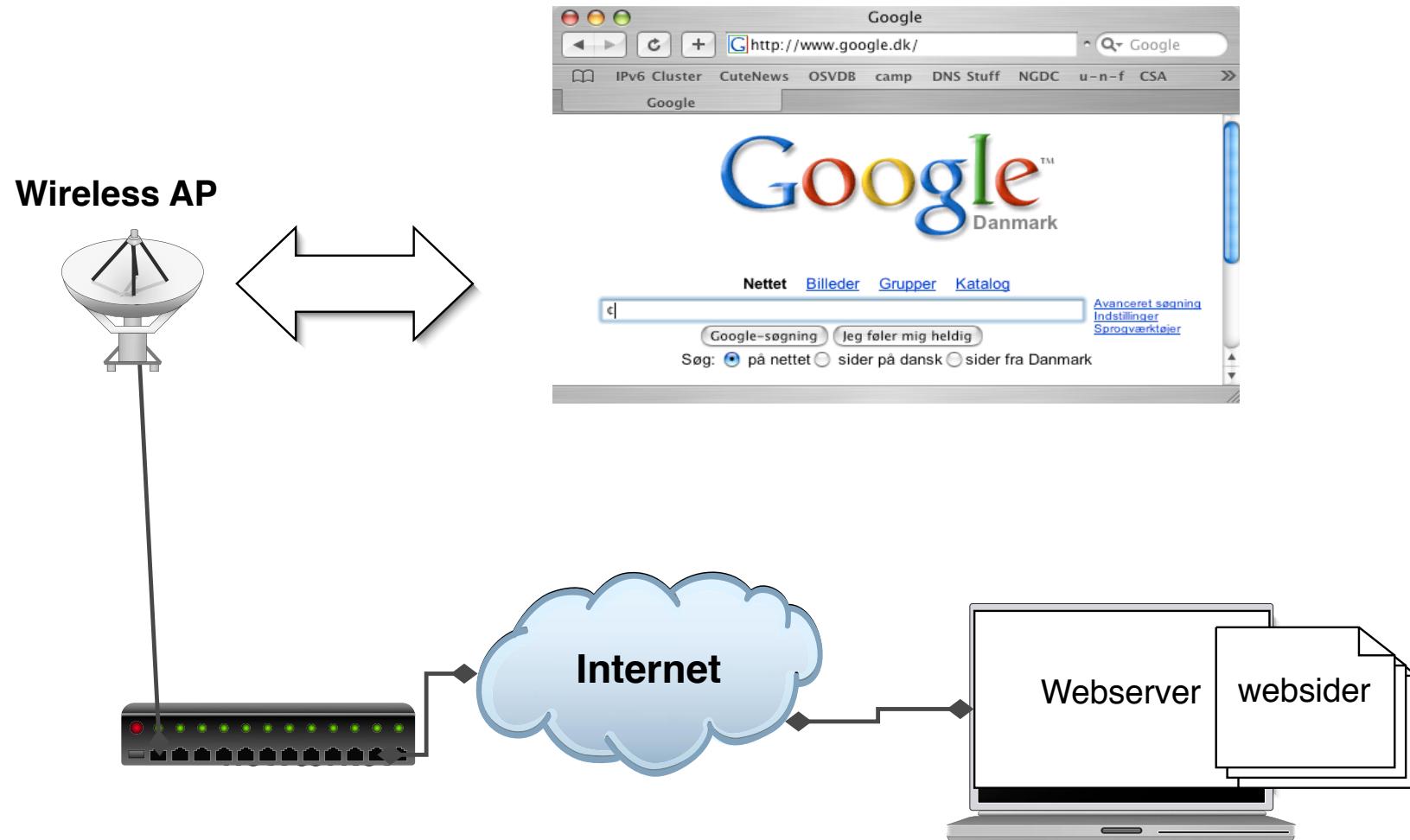
Wireshark - <http://www.wireshark.org> avanceret netværkssniffer
bruger vi til at sniffe, vi bruger Wireshark til primære demo, nævner Ettercap osv.

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

Wireshark - easy sniffing



<http://www.wireshark.org>
både til Windows og UNIX, tidligere kendt som Ethereal



Når vi 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

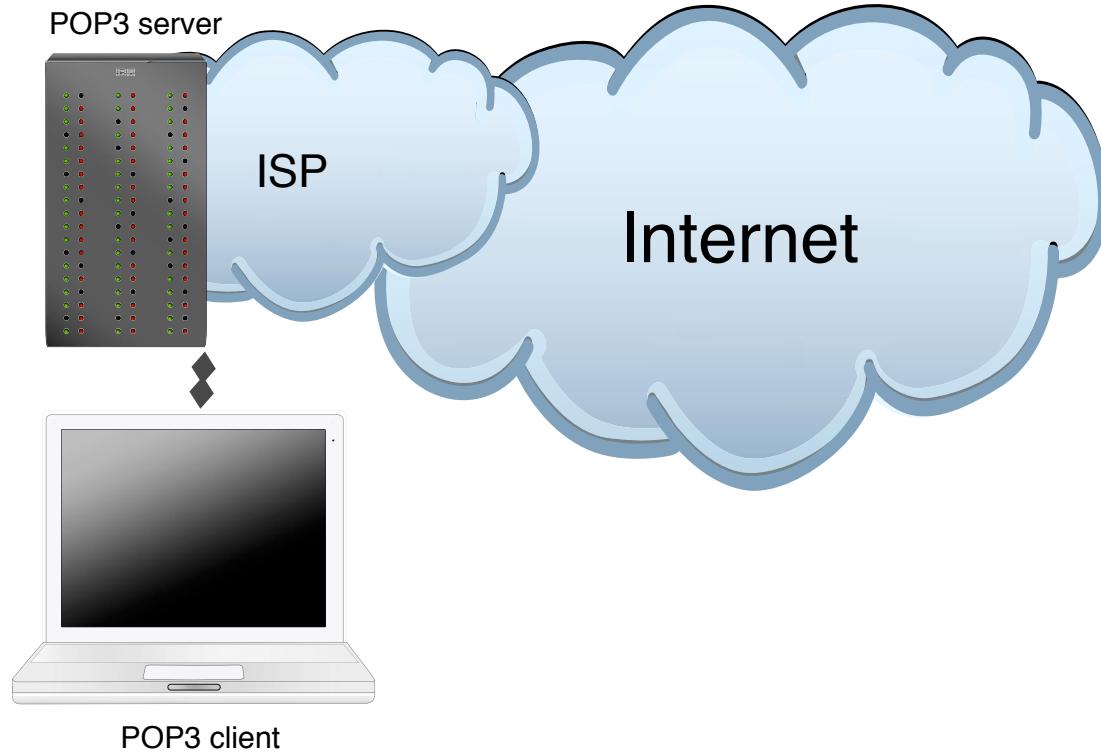
Forskellen mellem de to er at man typisk med POP3 henter posten, hvor man med IMAP lader den ligge på serveren

POP3 er bedst hvis kun en klient skal hente

IMAP er bedst hvis du vil tilgå din post fra flere systemer

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

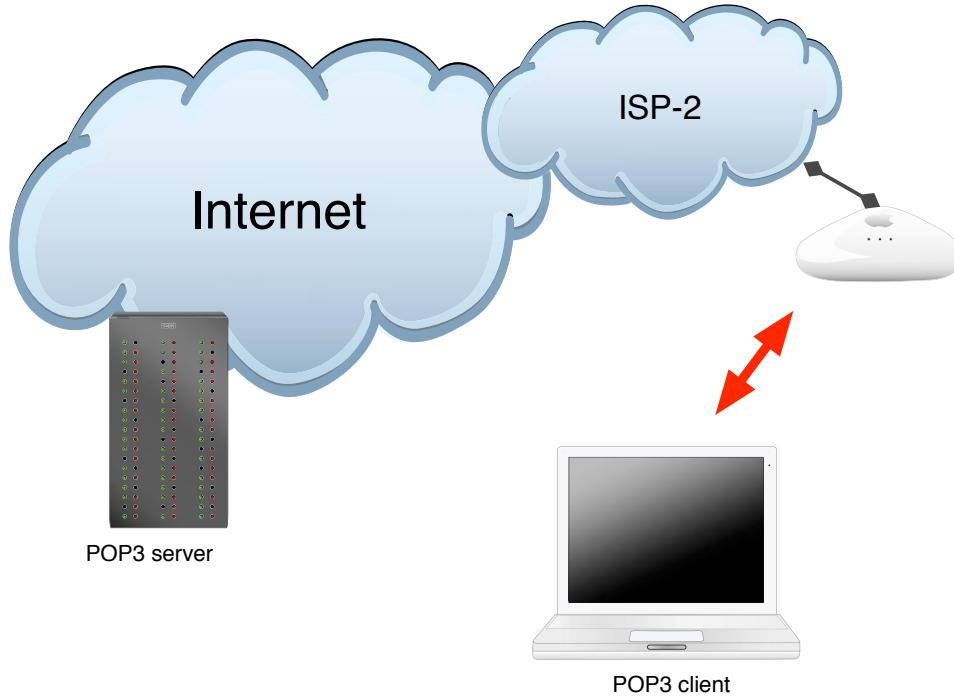
SMTP bruges til at sende mail mellem servere



Before you would trust your ISP, had access to both network and server

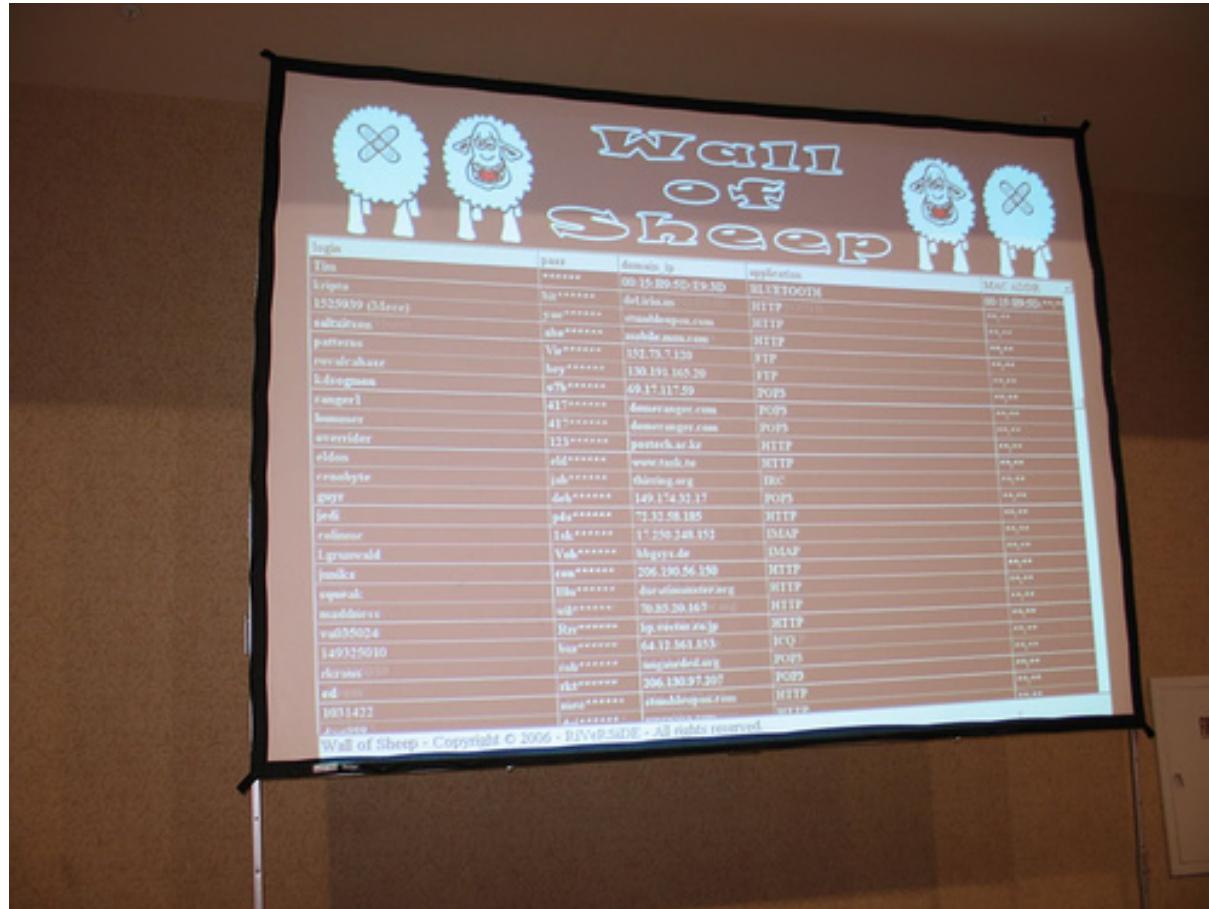
POP3 was OK, and you did not send anything *really important*

POP3 today on wireless networks



Do you trust other ISPs - All ISPs?

Shared network medium - anyone can read data



Defcon Wall of Sheep

Chaosreader

Chaosreader Report

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

[Image Report](#) - Click here for a report on captured images.

[GET/POST Report](#) (Empty) - Click here for a report on HTTP GETs and POSTs.

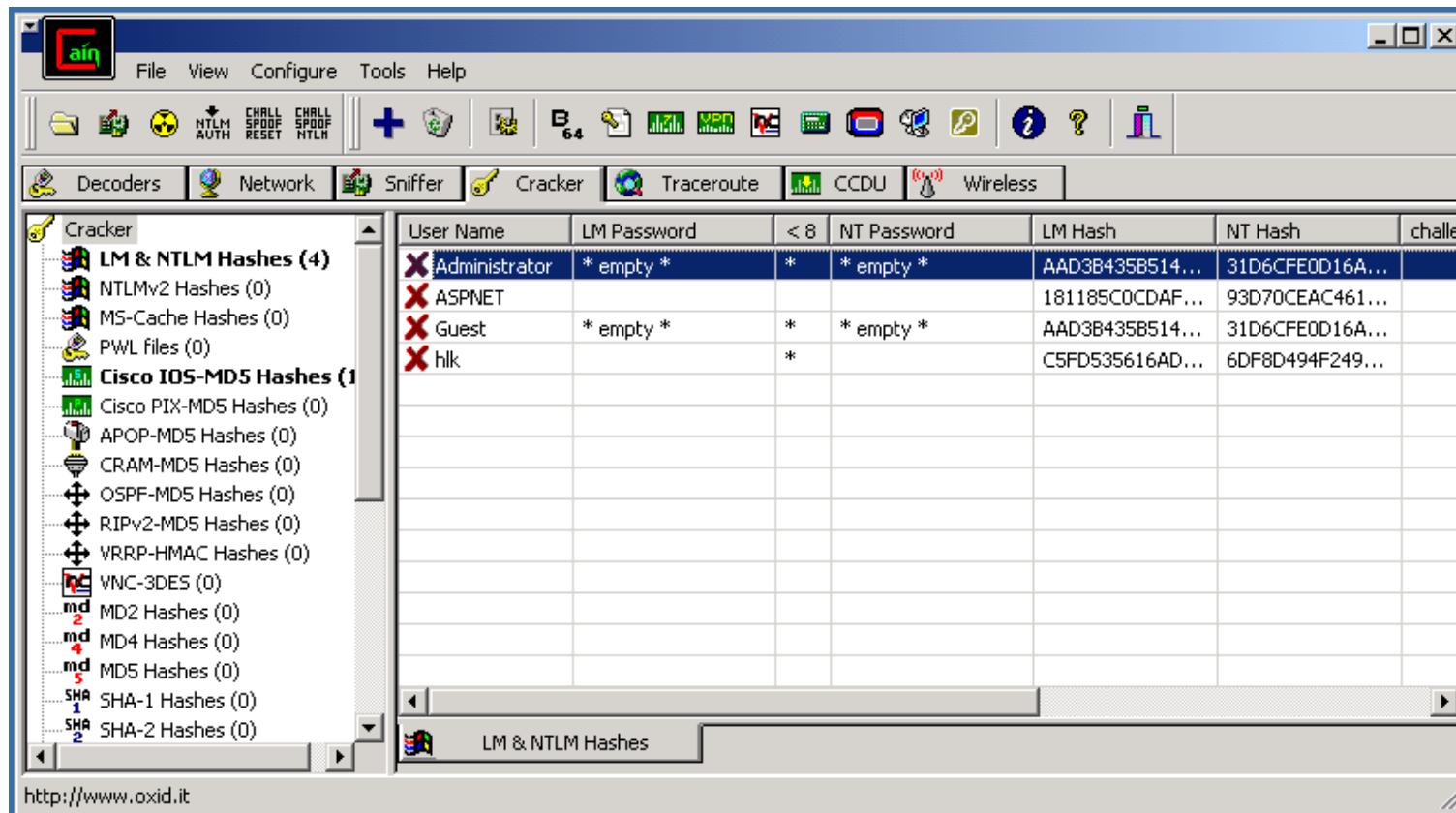
[HTTP Proxy Log](#) - Click here for a generated proxy style HTTP log.

TCP/UDP/... Sessions

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

Process capture files automatically, output HTML and pictures

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



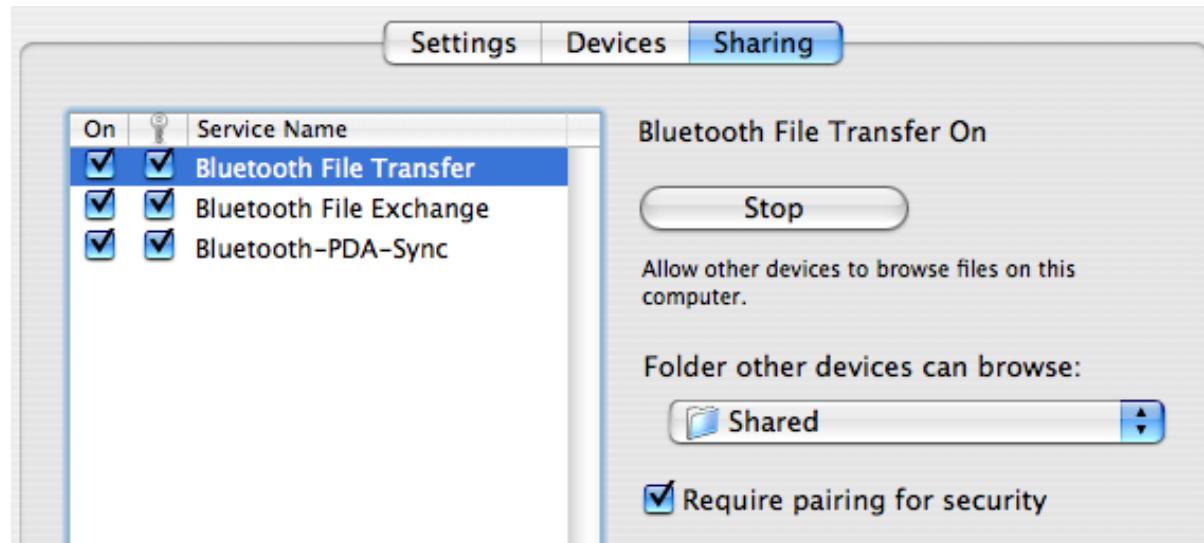
sniff, crack and hack <http://www.oxid.it>

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."



- Bluetooth - turn it off when not in use
- In your car - built-in bluetooth, GPS has bluetooth?
- Turn on security features for bluetooth allow access on to *paired* devices

Car Whisperer using bluetooth



Bluetooth kits for cars use passkey like '0000' or '1234'

Sources:

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

Er det tid til en lille pause?



What to do?



What do we do?

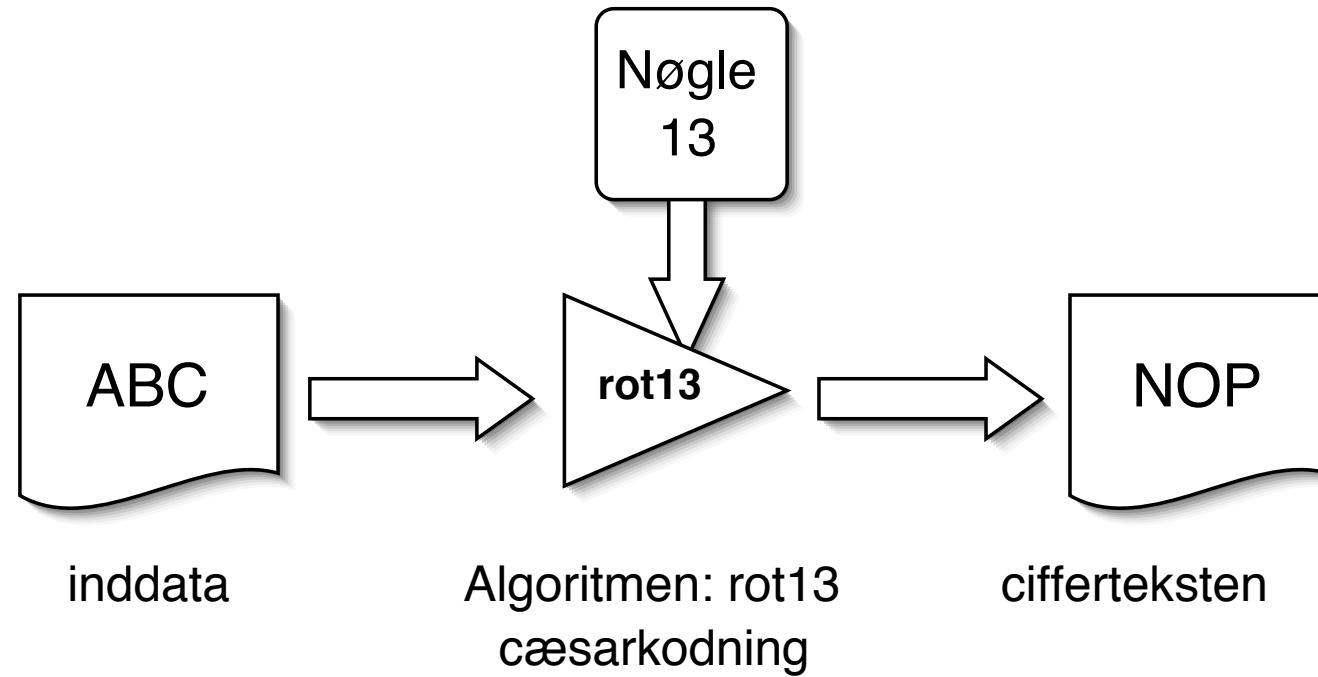
Use technology

Learn the technology - read the freaking manual

Think about the data you have, upload, facebook license?! WTF!

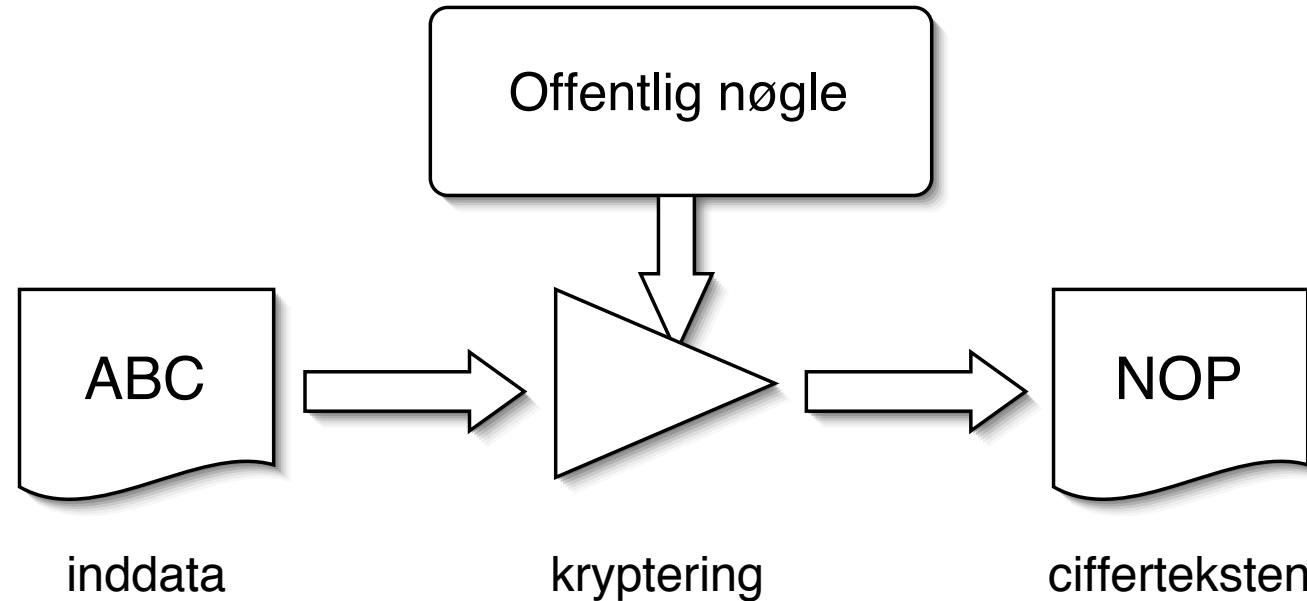
Think about the data you create - nude pictures taken, where will they show up?

- Turn off features you don't use
- Update software and applications
- Turn on encryption: **IMAPS, POP3S, HTTPS**
- Lock devices when not used for 10 minutes



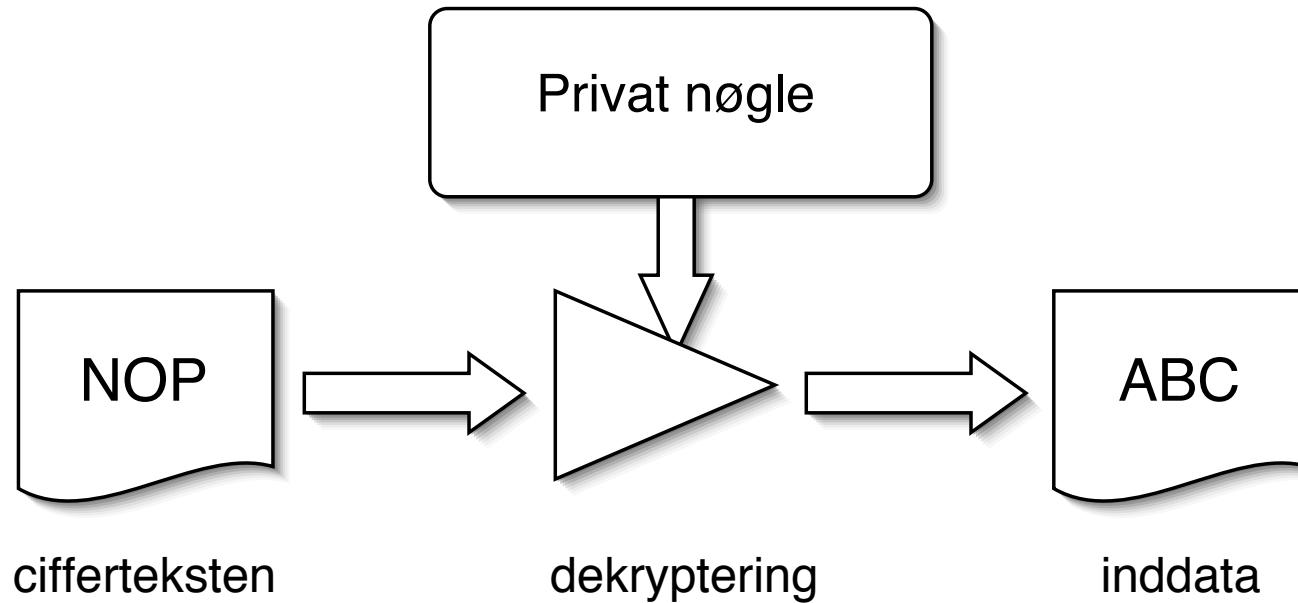
Kryptografi er læren om, hvordan man kan kryptere data

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



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

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



offentlig-nøgle kryptografi (eksempelvis RSA) bruger den private nøgle til at dekryptere man kan ligeledes bruge offentlig-nøgle kryptografi til at signere dokumenter - som så verificeres med den offentlige nøgle

Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

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

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

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

AES

Advanced Encryption Standard

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

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

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

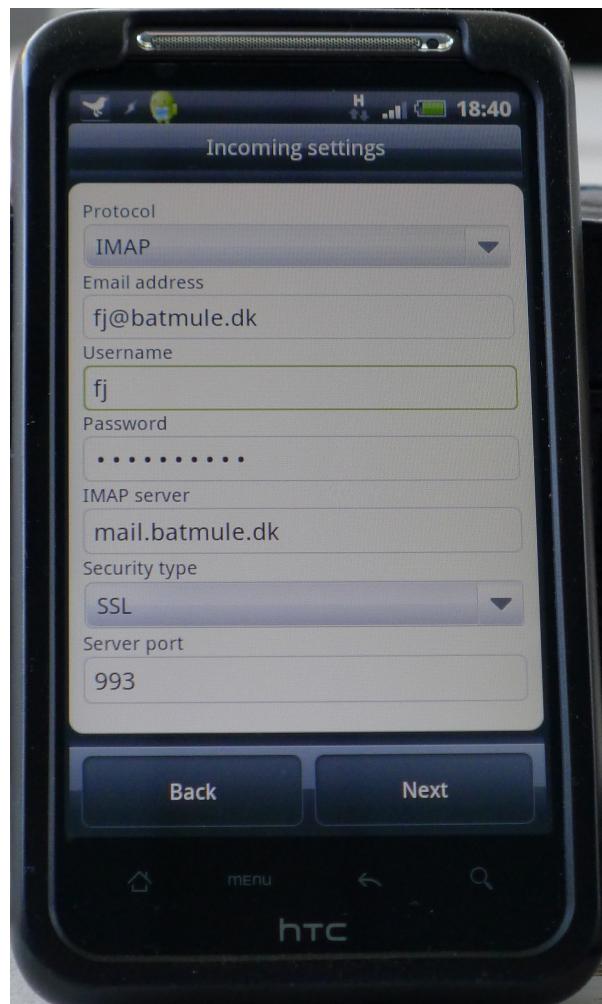
Kilde: <http://csrc.nist.gov/encryption/aes/>
<http://www.esat.kuleuven.ac.be/~rijmen/rijndael/>

kryptering er den eneste måde at sikre:

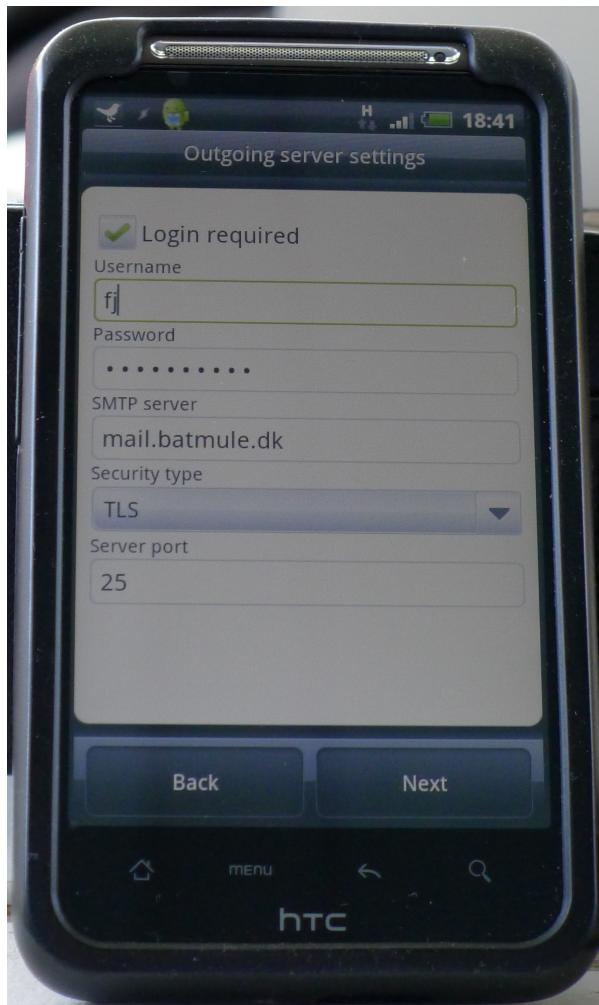
fortrolighed

autenticitet / integritet

Use POP3S, use IMAPS



Try to use SMTP with encryption SMTP+TLS



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

Nu vi snakker om kryptering - SSL overalt?

Kan vi klare det på vores servere? ■

Google kan:

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

Men alt for få gør det

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

Ægypten, Sudan, Tunesien, ...

Den der kontrollerer ISPerne kontrollerer trafikken

Facebook revolutionerne

Blokering er umulig, men det forsøges

Spredning af falsk information

Diginotar Dutch Certificate Authority

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



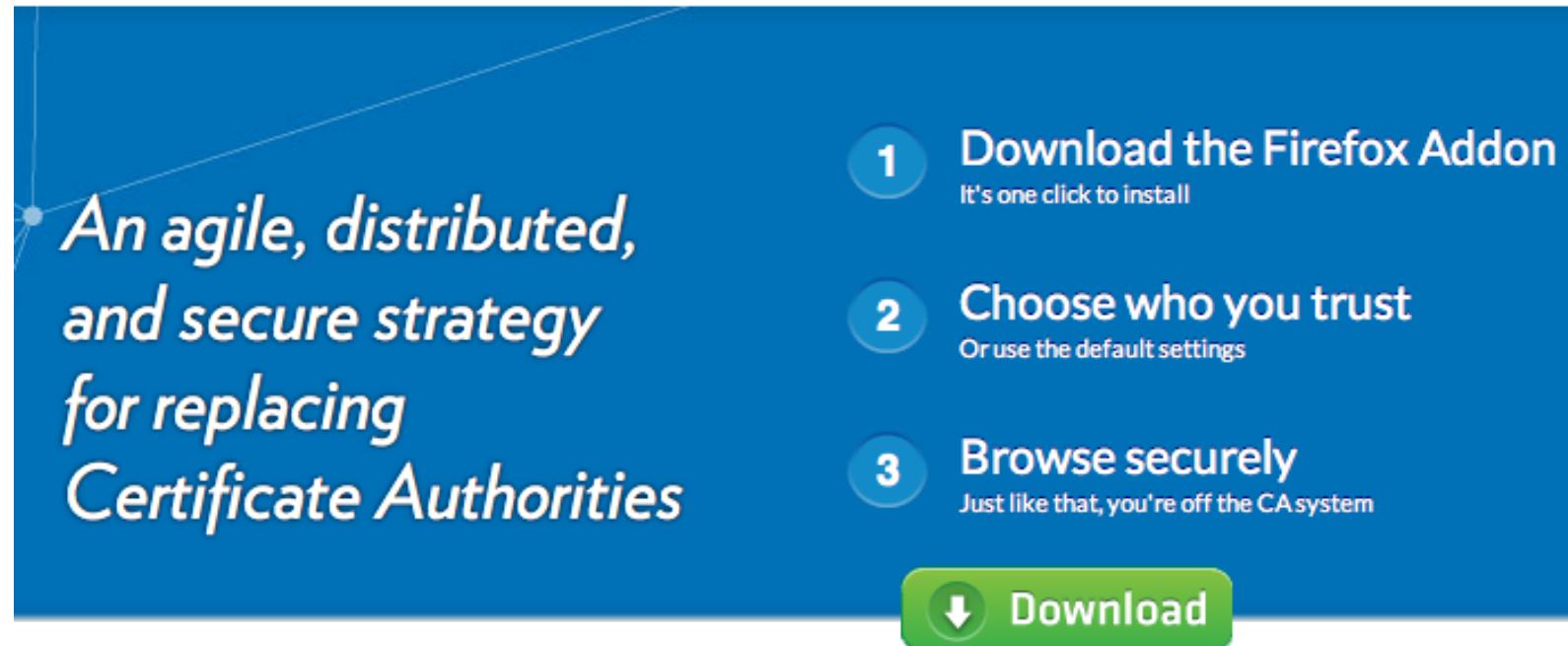
HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

<http://www.eff.org/https-everywhere>



An add-on formerly considered paranoid: CertPatrol implements "pinning" for Firefox/Mozilla/SeaMonkey roughly as now recommended in the User Interface Guidelines of the World Wide Web Consortium (W3C).

<http://patrol.psyced.org/>



*An agile, distributed,
and secure strategy
for replacing
Certificate Authorities*

- 1 Download the Firefox Addon**
It's one click to install
- 2 Choose who you trust**
Or use the default settings
- 3 Browse securely**
Just like that, you're off the CA system

 Download

<http://convergence.io/>

Warning: radical change to how certificates work

Anonymity Online

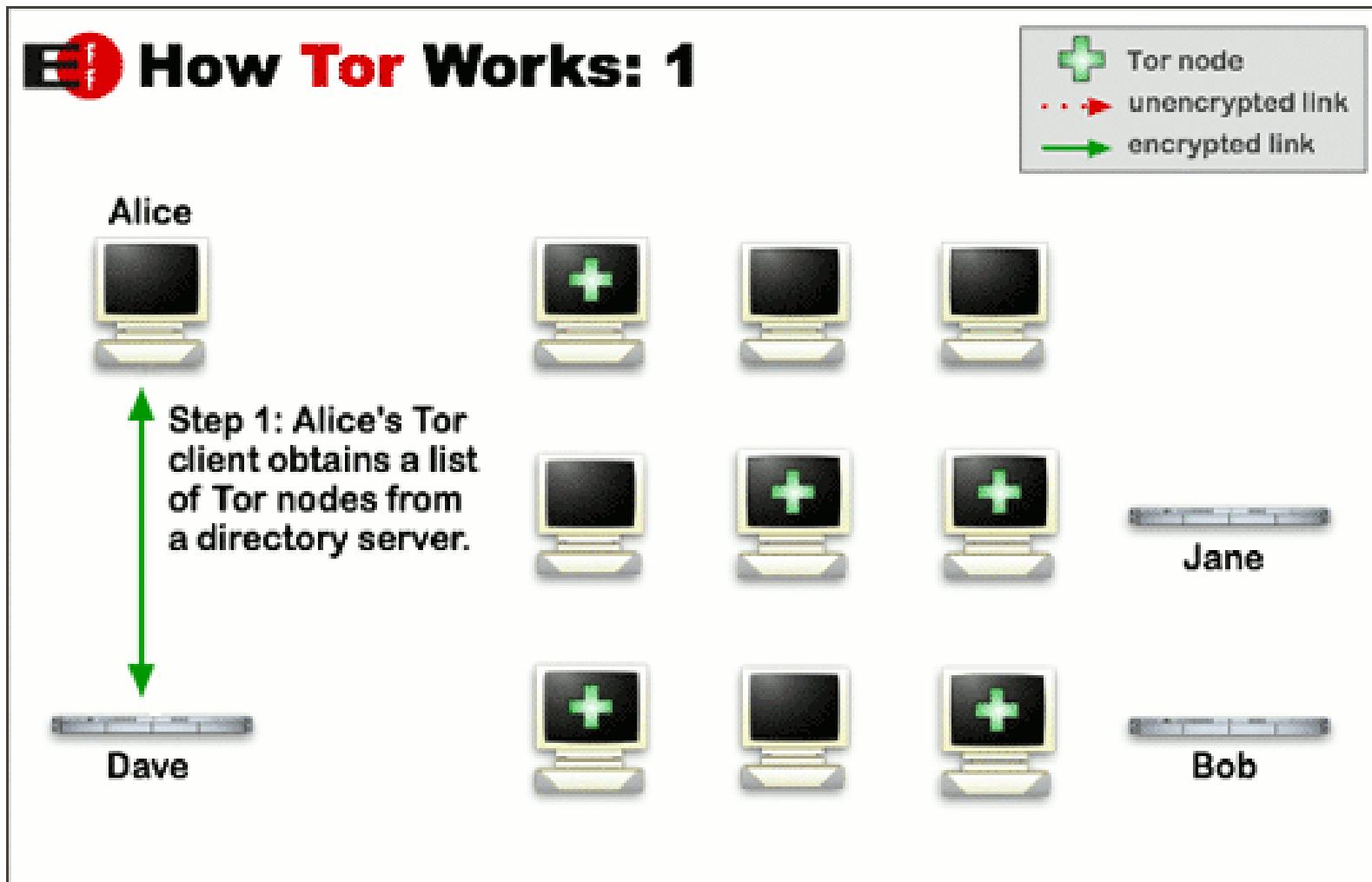
Protect your privacy. Defend yourself against network surveillance and traffic analysis.



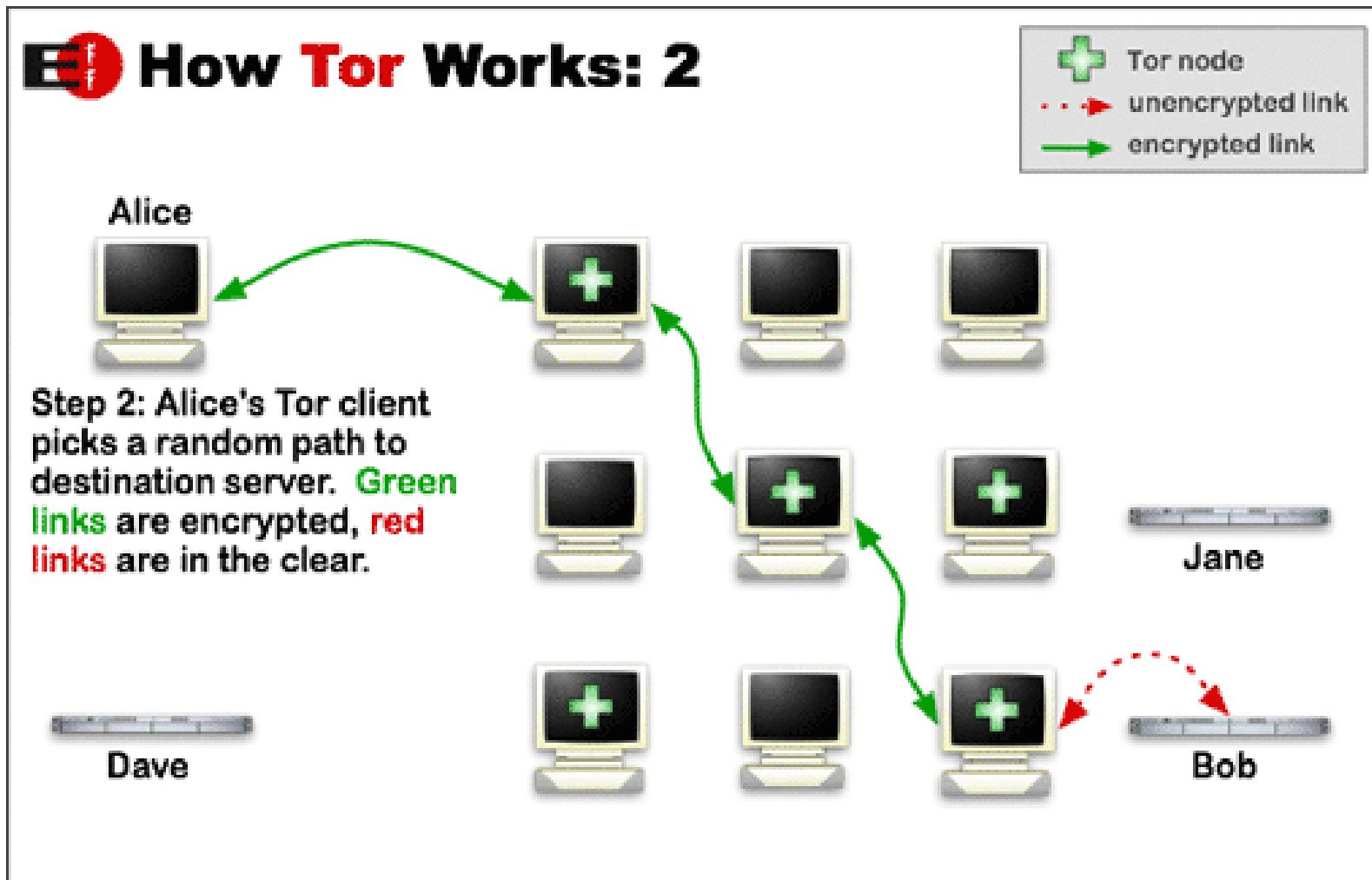
Download Tor 

- ➔ Tor prevents anyone from learning your location or browsing habits.
- ➔ Tor is for web browsers, instant messaging clients, remote logins, and more.
- ➔ Tor is free and open source for Windows, Mac, Linux/Unix, and Android

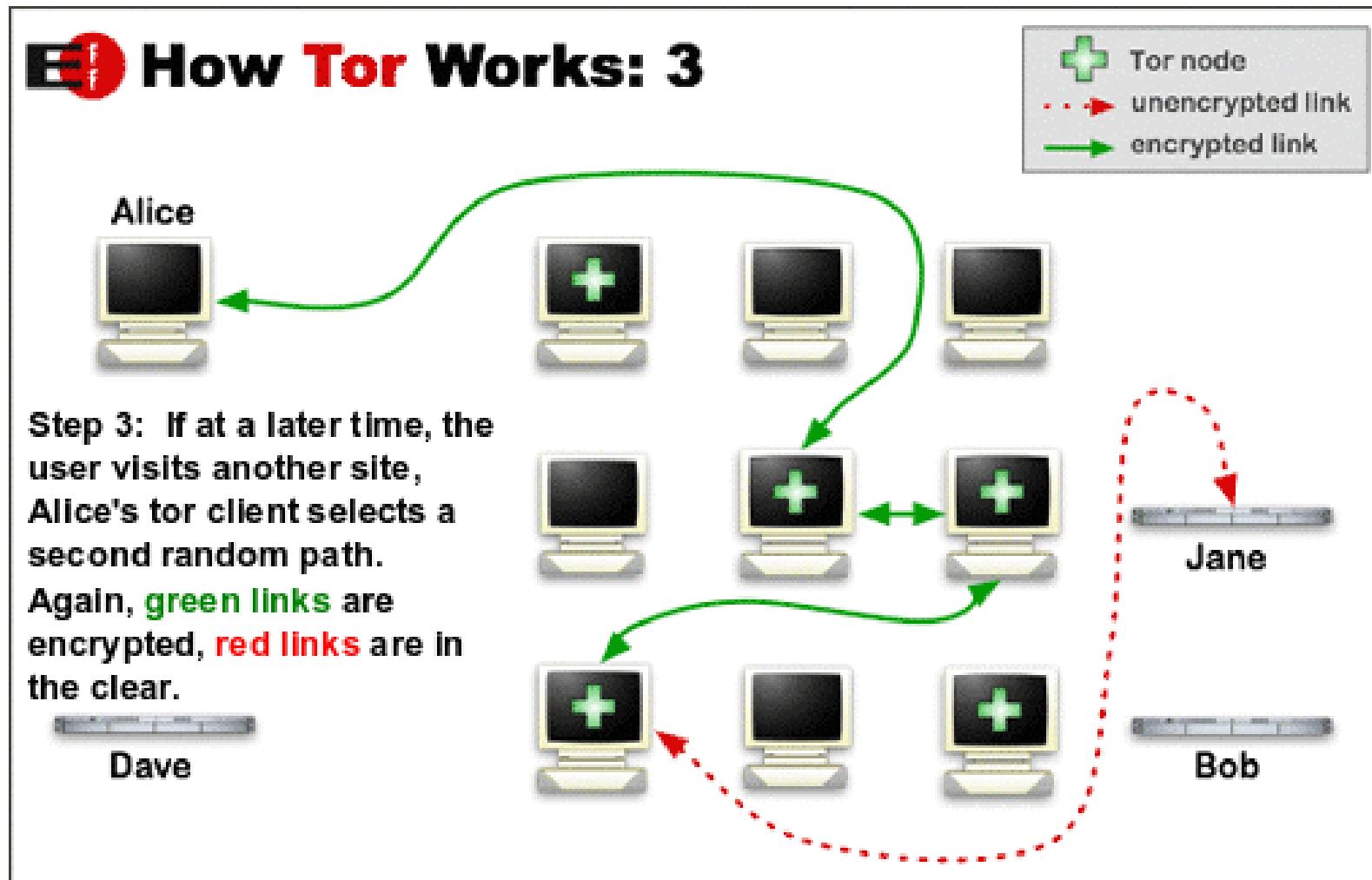
<https://www.torproject.org/>



pictures from <https://www.torproject.org/about/overview.html.en>



pictures from <https://www.torproject.org/about/overview.html.en>



pictures from <https://www.torproject.org/about/overview.html.en>

Kryptering af e-mail

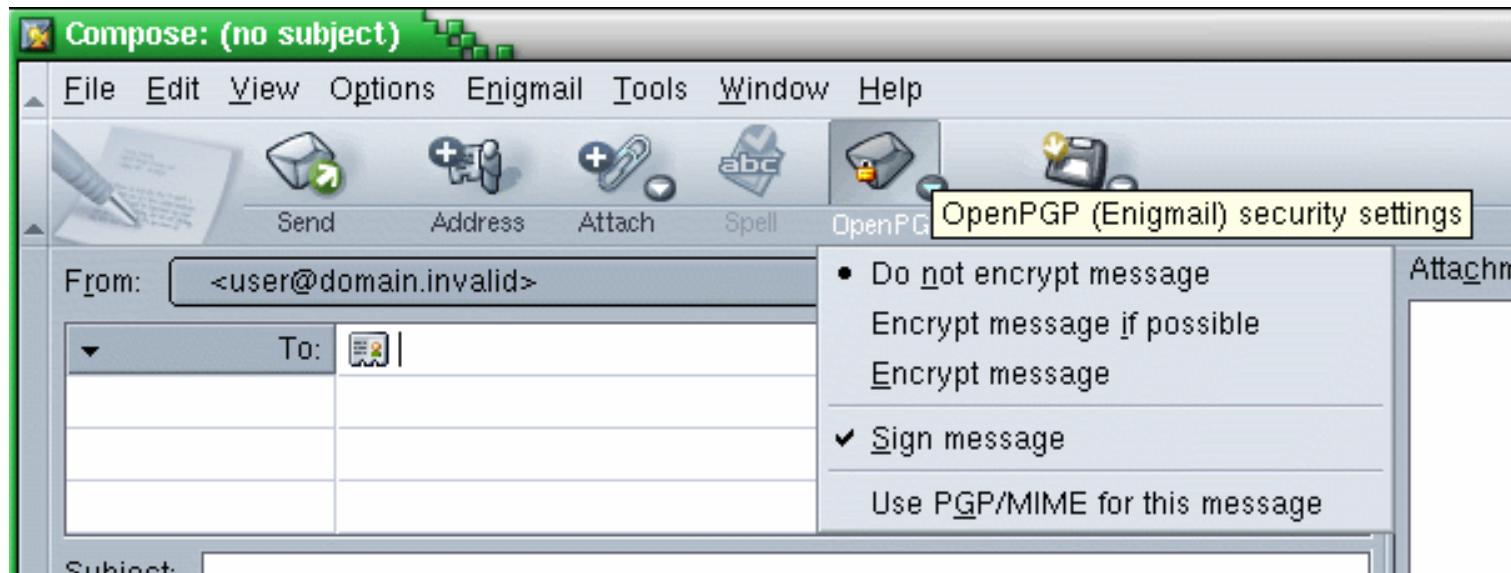
- Pretty Good Privacy - Phil Zimmermann
- PGP = mail sikkerhed

Kryptering af sessioner SSL/TLS

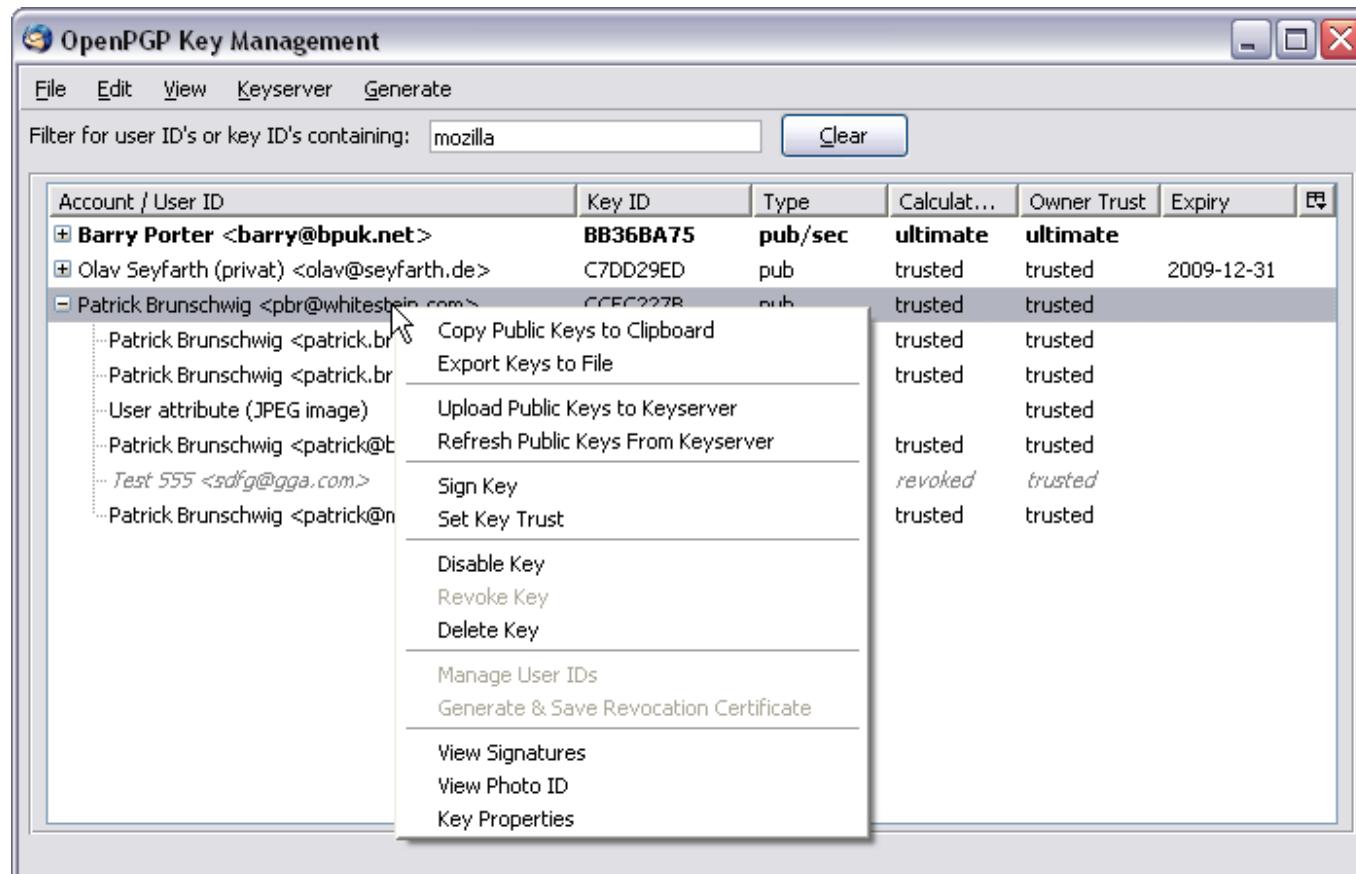
- Secure Sockets Layer SSL / Transport Layer Services TLS
- krypterer data der sendes mellem webservere og klienter
- SSL kan bruges generelt til mange typer sessioner, eksempelvis POP3S, IMAPS, SSH m.fl.

Sender I kreditkortnummeret til en webserver der kører uden https?

Enigmail - GPG plugin til Mail

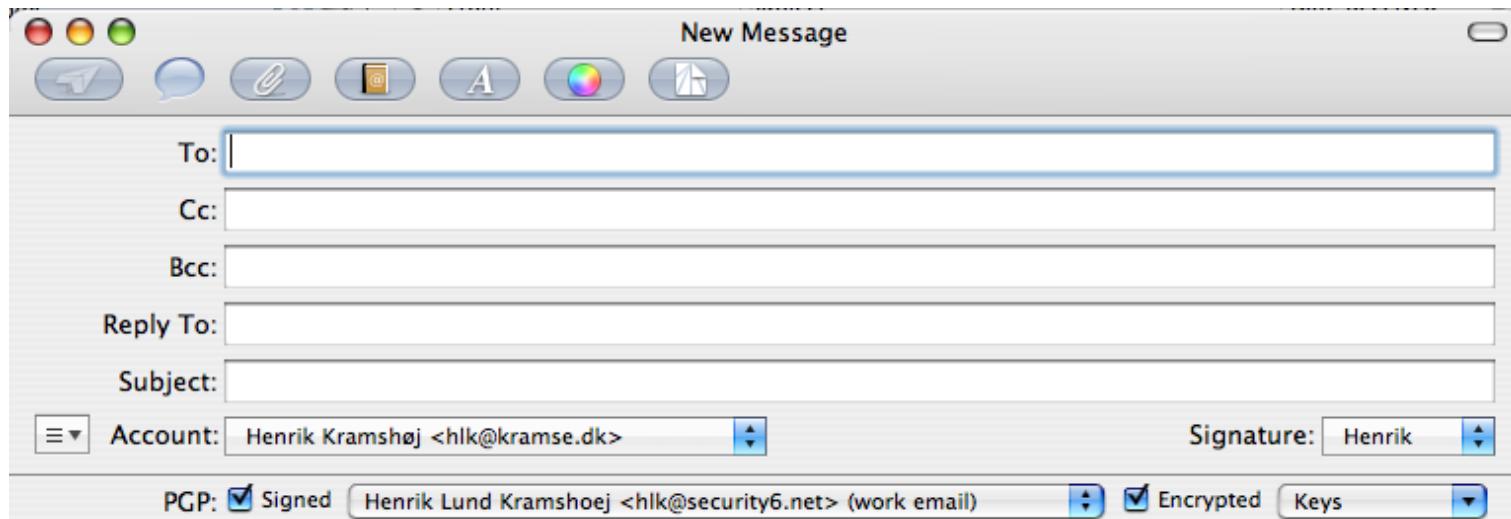


- Enigmail er en udvidelse til
- mailklienten i Mozilla/Netscape
- standalone mailklienten Thunderbird
- Billede fra <http://enigmail.mozdev.org>



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>

File Transfer Protocol - filoverførsler

FTP bruges især til:

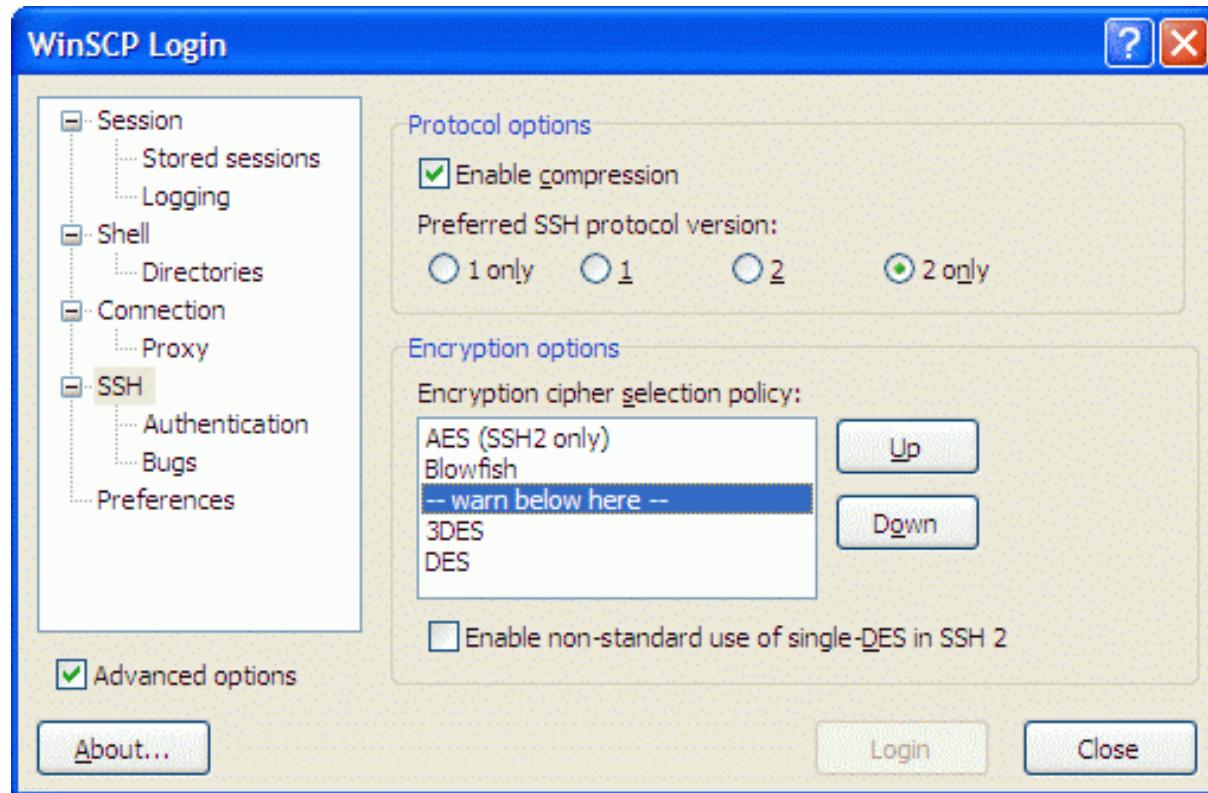
- FTP - drivere, dokumenter, rettelser - Windows Update? er enten HTTP eller FTP
- Opdatering af websites
- Overførsel af data mellem virksomheder
- Serveren er indbygget i de fleste serveroperativsystemer

FTP sender i klartekst

USER brugernavn og

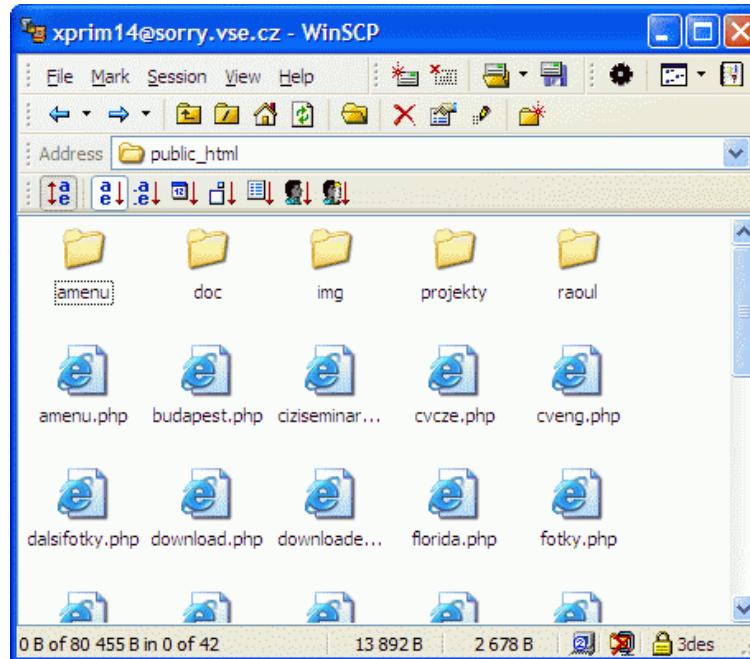
PASS hemmeligt-kodeord

Gode protokoller - men hvad er en protokol overhovedet



screenshot fra

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



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/>

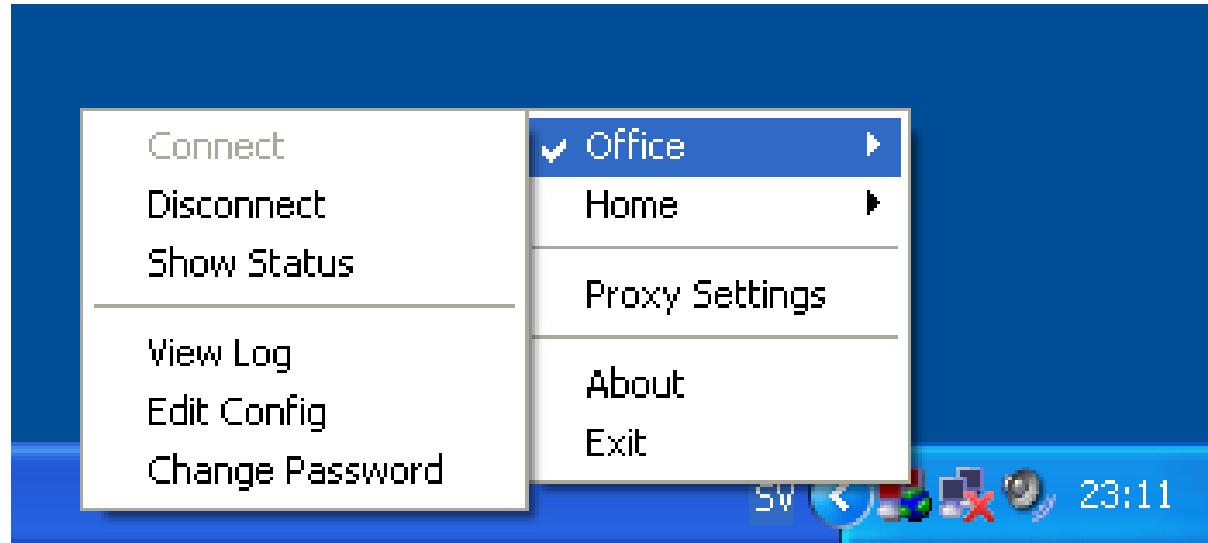
VPN http://en.wikipedia.org/wiki/Virtual_private_network

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

De snakker ikke ret godt sammen på tværs. Brug IPSec for dette.

IPsec er desværre 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 GUI - easy to use

Er det tid til en lille pause?



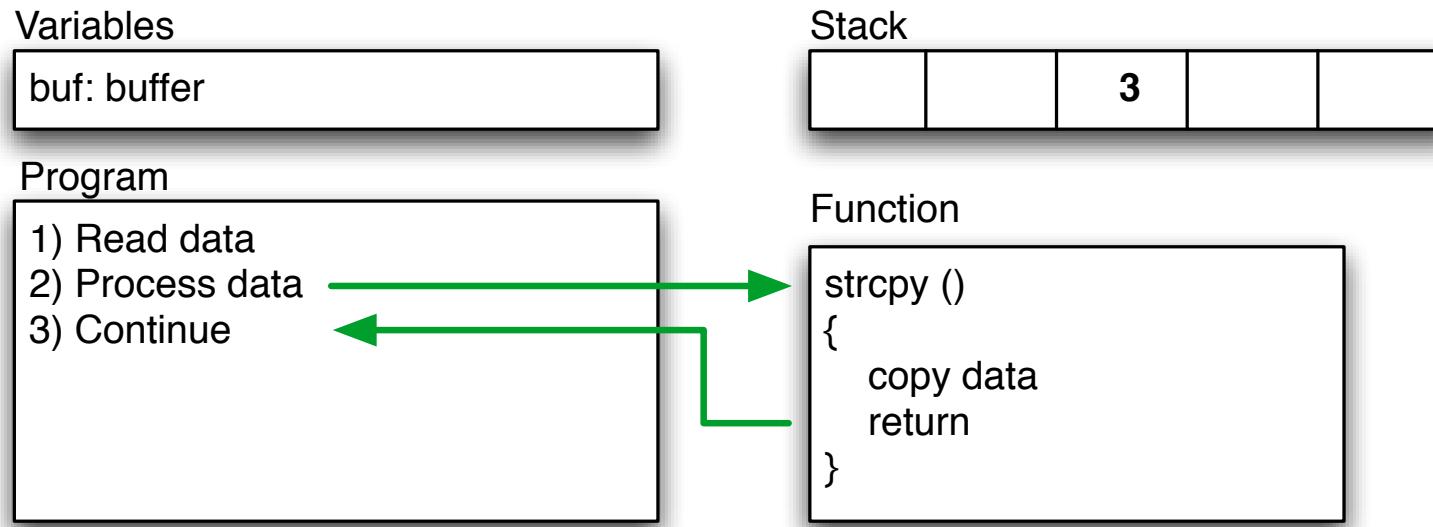
```
main(int argc, char **argv)
{
    char buf[200];
    strcpy(buf, argv[1]);
    printf("%s\n", buf);
}
```



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

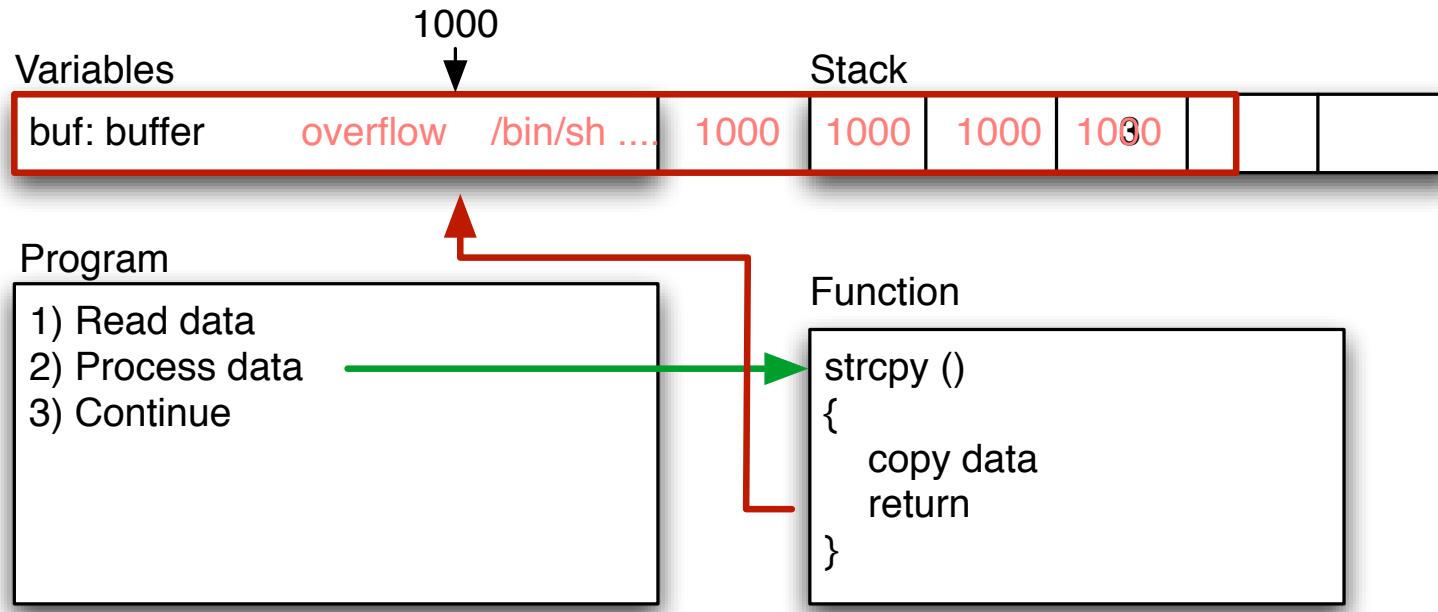
Stack protection er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.

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

```
$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

Black box testing

Closed source reverse engineering

White box testing

Open source betyder man kan læse og analysere koden

Source code review - automatisk eller manuelt

Fejl kan findes ved at prøve sig frem - fuzzing

Exploits virker typisk mod specifikke versioner af software



The screenshot shows the homepage of The Exploit Database. At the top, there's a banner with the word "EXPLOIT" in large letters, where each letter has a different background color. Below the banner, it says "D a t a b a s e". To the right, it displays "Currently Archiving 10343 Exploits". A navigation bar below the banner includes links for home, news, remote, local, web, dos, shellcode, papers, search, D, submit, and rss.

The Exploit Database

The ultimate archive of exploits and vulnerable software - A great resource for vulnerability researchers and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.

We are running a general cleanup on the DB and have changed our submission policy - please [check it out](#) before submitting exploits to us.

Due to recent DOS attacks, our application downloads are now captcha protected.

Remote Exploits

Date	D	A	V	Description	Plat.	Author
2010-01-27	D	A	✓	CamShot v1.2 SEH Overwrite Exploit	windows	technik
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 0day 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 assemblers.

Idag findes der samlinger af exploits som milw0rm

Udviklingsværktøjerne 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/>

Bemærk: alle angreb har forudsætninger for at virke

Et angreb mod Telnet virker kun hvis du bruger Telnet

Et angreb mod Apache HTTPD virker ikke mod Microsoft IIS

Kan du bryde kæden af forudsætninger har du vundet!

Computeren skal være tændt

Funktionen der misbruges skal være slået til

Executable stack

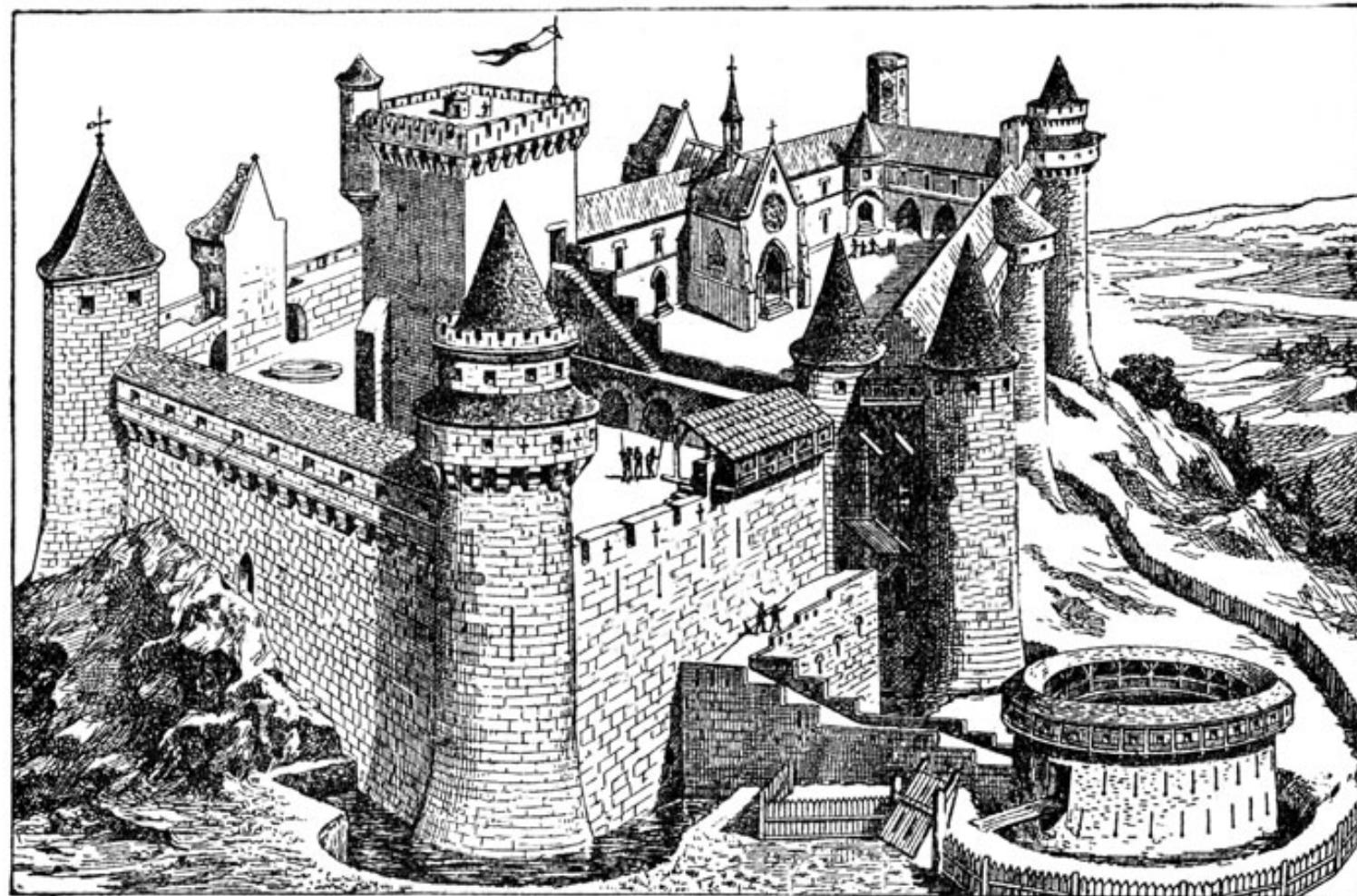
Executable heap

Fejl i programmet

|

alle programmer har fejl

Enhance and secure runtime environment



Sidste chance er på afviklingstidspunktet

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.

Vælg derfor hellere:

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

Det samme gælder for serveroperativsystemer

NB: meget få embedded 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 undvære Flash og PDF?

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



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?



The screenshot shows the Twitter profile for the account @safety. The profile picture is the Twitter bird icon. The name is "Safety" with a blue verified checkmark. Below the name is the handle "@safety" and the text "Twitter HQ". A description reads "Twitter's Trust and Safety Updates!" followed by a link: "http://help.twitter.com/forums/10711/entries/76036". Below the profile information is a green "Following" button, a reply icon, and a direct message icon. A text input field says "Tweet to @safety". Below this is a navigation bar with tabs: "Tweets" (selected), "Favorites", "Following", "Followers", and "Lists". Three tweets are listed:

- safety Safety**
Also, we will never send you an email saying that you've been suspended for "tweeting too much." Those emails are fake & not from us.
26 Sep
- safety Safety**
We will never send you emails requiring you to "complete offers" in order to unsuspend your account. That's spam, not us.
26 Sep
- safety Safety**
Warn your friends if they sent you a DM saying "When I found this about you" with a link - they've been phished. bit.ly/accountamiss
21 Sep

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

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

Bærbare tillader typisk boot fra CD-ROM
hold c nede på en Mac

Mac computere kan i nogle tilfælde være firewire diske
hold t nede under boot

Harddisken kan typisk nemt fjernes fra en bærbar



Fysisk adgang til systemet - **game over**



Target: Macbook disket

Press t to enter ☺

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



Kryptering findes i alle de gængse 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 på disken - IBM harddisk BIOS kodeord

Hackertyper anno 1995



Lad os lige gå tilbage til hackerne



Lisbeth laver PU, personundersøgelser ved hjælp af hacking

Hvordan finder man information om andre

Først vil vi finde nogle mønstre

Derefter vil vi søge med de mønstre

Nogle giver direkte information

Andre giver baggrundsinformation

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

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

Diverse idnumre, som CPR - tør du søge på dit CPR nr?

Computerrelaterede informationer: IP, Whois, Handles

Øgenavne, kendenavne

Skrivestil, ordbrug mv.

Tiden på din computer?

Tænk kreativt ☺

Email

DNS

Gætter

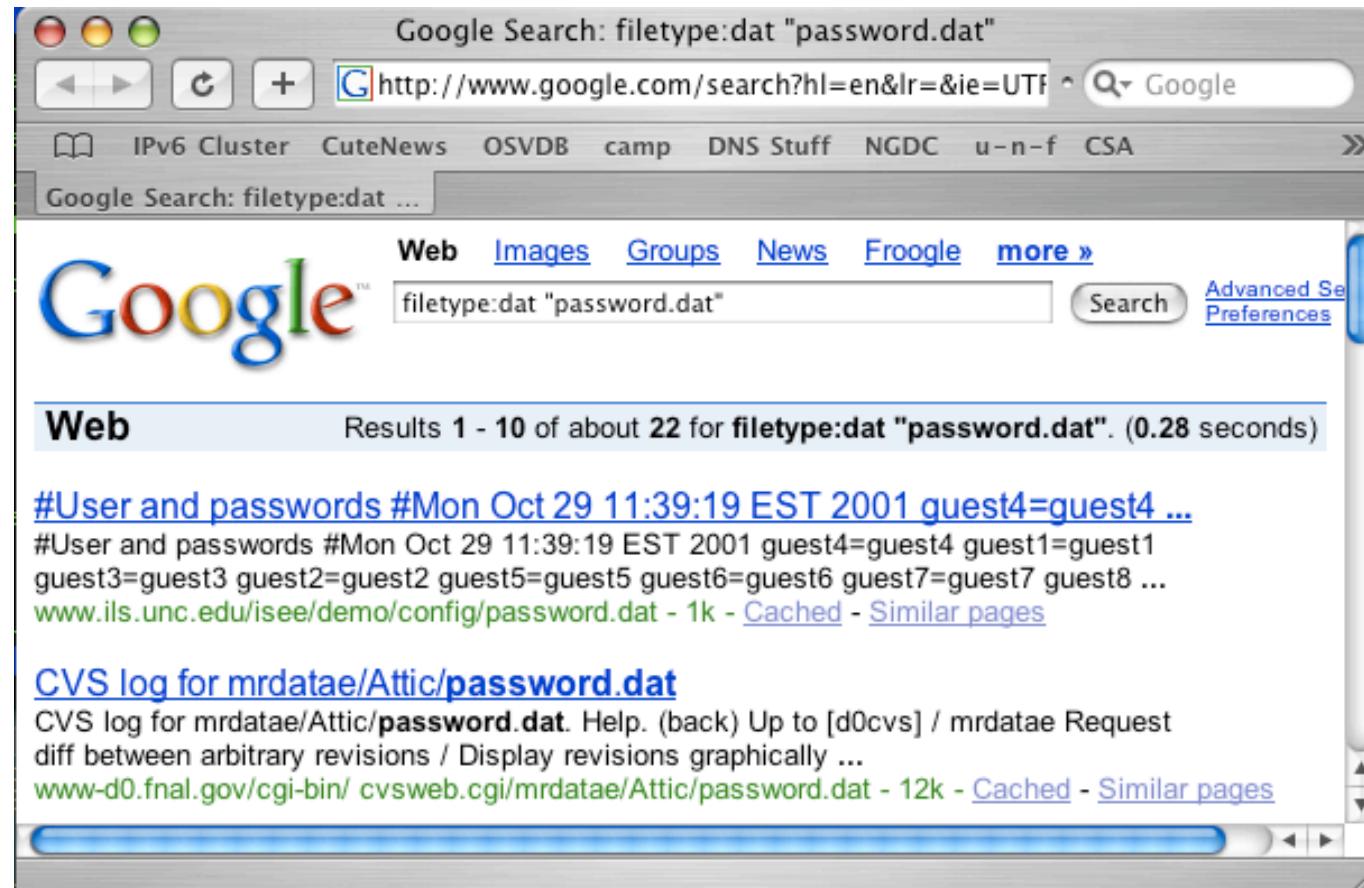
Google

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 største er:

- RIPE (Réseaux IP Européens) <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

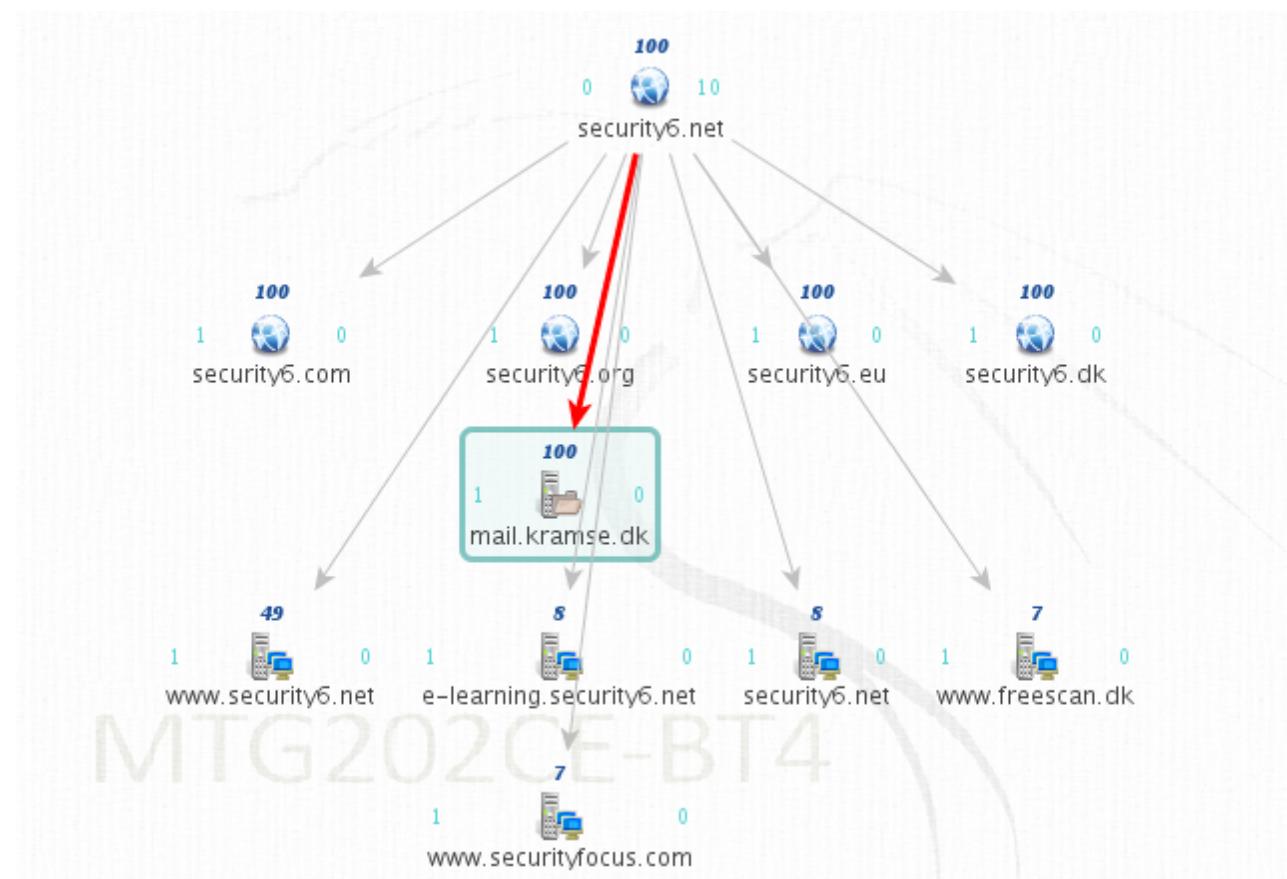
disse fire kaldes for Regional Internet Registries (RIRs) i modsætning til Local Internet Registries (LIRs) og National Internet Registry (NIR)



Google som hacker værktøj?

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

Listbeth in a box?



BT4 udgaven, kommercial udgave på <http://www.paterva.com/maltego/>

Er du passende paranoid?



Vær på vagt

Lad være med at bruge computere

Lad være med at bruge en computer til alt - en privat bærbar ER mere privat end en firmacomputer

Forskellige computere til forskellige formål, en server er mail-server en anden er web-server

Brug en sikker konfiguration, minimumskonfiguration

Brug sikre protokoller, kryptering, evt. TOR

Opsætning af netværk, hvordan? Security Configuration Guides + paranoia

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

- BIOS kodeord, pin-kode til telefon
- Firewall - specielt på laptops
- Installer anti-virus og anti-spyware hvis det er på Windows
- 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 jævnligt
- **Backup af vigtige data - harddiske i bærbare kan også dø**
- Husk: sikker sletning af harddiske, medier osv.



PROSA afholdt fredag 17. september - til lørdag 18. september 2010 Capture the Flag
Distribueret CTF med 6 hold og arrangørerne i Aalborg
Sjovt og lærerigt - gentages helt sikkert

Kilde: <http://prosa-ctf.the-playground.dk/>
Get ready! Lær debuggere, perl, java at kende, start på at hacke

prosa capture the flag 2011 *hacking for fun*

Søgning:

Hjem Tips og Hints Udfordringer Teknik Hold Regler CTF hold server

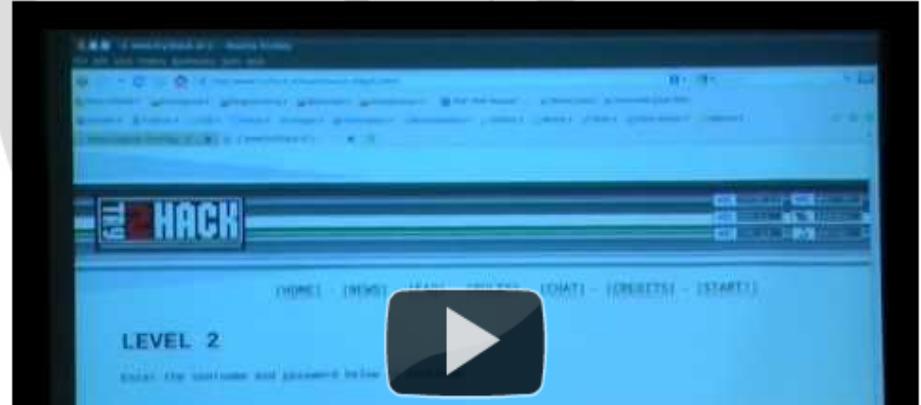
Menu

- Hjem
- Tips og Hints
- Udfordringer
- Teknik
- Hold
- Regler
- CTF hold server

Hjem

Velkommen til Proosas Capture The Flag konkurrence anno 2011.

For en forklaring af, hvad dette CTF handler om kan du se en videopræsentation fra sidste år.



One month! October 4. - 5. 2011

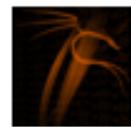
Questions?



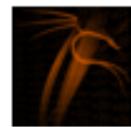
Henrik Lund Kramshøj
hlk@solidonetworks.com

<http://www.solidonetworks.com>

You are always welcome to send me questions later via email



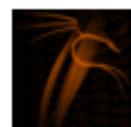
exploitdb [webapps] – BPAffiliate Affiliate Tracking
Authentication Bypass Vulnerability: <http://bit.ly/9LOC3K>
about 5 hours ago via twitterfeed



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] – BPRealestate 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 afløst RSS? NB: favoritsite <http://isc.sans.edu/index.html>

Welcome to VikingScan – miniscan

http://miniscan6.vikingscan.org/ Google

VikingScan.org - free portscanning

Home Miniscan List

On this page you can configure and start a portscan of your IP-address from this server.
Your IP-address is: 2001:16d8:dd0f:cf0f:223:6cff:fe9a:f52c

Configure and start a scan of the IP-address

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.

Do you need more? What about a basic webtest for DKK 8.000 ex VAT?

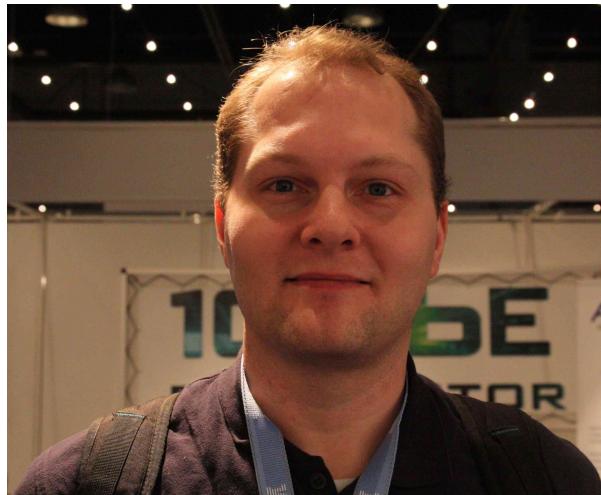
© 2009 VikingScan.org: Free portscanning
<http://www.vikingscan.org>

WEB SCANNING WIRELESS SCANNING
PENETRATION TESTING SECURITY TRAINING
SECURE WEBSERVERS
IMPLEMENTING IPV6
FIREWALLS & VPN

Security is a process, not a tool, not a single portscan


Security .net

VikingScan.org is a service of Security6.net
Security6.net provides this service for the community for free. If you need firewalls, penetration testing, security consulting please visit [Security6.net](http://www.security6.net).



- 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 og CEH certificeret
- 2003 - 2010 Selvstændig sikkerhedskonsulent
- 2010 Stifter og partner i Solido Networks ApS

Følgende kurser afholdes med mig som underviser

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

Se mere på <http://www.solidonetworks.com>