

Welcome to

# IT-sikkerhed 2012

## PROSA Superhelteseminar

Henrik Lund Kramshøj, internet samurai  
[hlk@solido.net](mailto:hlk@solido.net)

<http://www.solidonetworks.com>

# Kontaktinformation og profil



- Henrik Lund Kramshøj, IT-sikkerhed og internet samurai
- Email: [hlk@solido.net](mailto: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



## Don't Panic!

KI 17:00-19:00

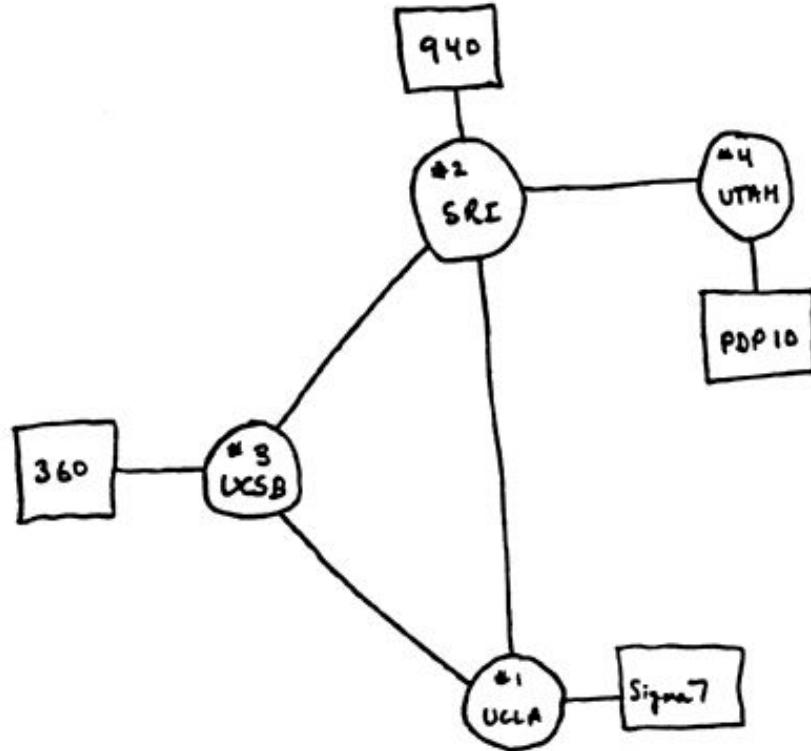
Mindre foredrag mere snak

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

Send gerne spørgsmål senere

PS er her hele weekenden

# Formål: IT-sikkerhed generelt



TCP/IP-baserede netværk - internet er overalt



Vores data er overalt

Vi er afhængige af computere

Vi er afhængige af netværk

Vi er afhængige af andres computere - servere og services

...





- Nmap, Nping - tester porte, godt til firewall admins <http://nmap.org>
- Metasploit Framework gratis på <http://www.metasploit.com/>
- Wireshark avanceret netværkssniffer - <http://www.wireshark.org/>
- Burpsuite <http://portswigger.net/burp/>
- Skipfish <http://code.google.com/p/skipfish/>
- OpenBSD operativsystem med fokus på sikkerhed <http://www.openbsd.org>

Kilde: Angelina Jolie fra Hackers 1995



BackTrack er baseret på Linux og må kopieres frit :-)

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

Wireshark - <http://www.wireshark.org>

Er det fornuftigt at man kan hente dem?

hacking backtrack – YouTube  
[http://www.youtube.com/results?search\\_query=hacking%20backtrack](http://www.youtube.com/results?search_query=hacking%20backtrack) DuckDuckGo

YouTube hacking backtrack Search results for **hacking backtrack** About 6,650 results

Filter ▾ Sort by: Relevance ▾

**IEFD Ep. 12 - Hacking Basics - Backtrack Part 1**  
On the forums, there has been many questions concerning **Backtrack**. Therefore, we decided to make a video that tries to answer as many as these ...  
by Gregorpm | 4 years ago | 155,410 views

**Security Awareness - Hacking Windows 7 with BackTrack 4....**  
This short tutorial provides an insight into network security and how quickly and easily a windows 7 machine can be compromised with a small ...  
HD by eastmidlandsit | 1 year ago | 12,188 views

**Facebook Hacking with BackTrack 5**  
Facebook **Hacking** with **BackTrack** 5 Sorry guys, i had to open a new account again as my older account was banned by youtube due to various **hacking** ...  
by MauritianHacker | 6 months ago | 68,523 views

**Hacking - BackTrack 4 Linux / VMware - For Beginners**  
View in HD and Fullscreen!! In this video I explain how to download **BackTrack** Linux 4 R2, and VMware. This video is for beginners. To Download ...  
HD by Raventattoo | 11 months ago | 7,407 views

**How to Hack (BackTrack & VMware Player)**  
"What will happen if my child becomes a **Hacker**?" Maybe what you should really be asking yourself is, "What if my child does not become a **Hacker** ...  
by J2897Tutorials | 2 years ago | 33,394 views

Featured Videos

**Cracking Router Logins**  
Attacking router logins If you like it, comment.  
by linuxstyles | 61,526 views

**How to Hack Free Int...**  
THIS IS LINUX Wanna hack the router login after u hack t...  
by theorignalfatdonkey | 46,749 views

**How To Hack Wireles...**  
This is very easy(Noob-Friendly) yet detailed tutorial on how to ha...  
by mushroomHEADBANGERS | 151,490 views

**Linux / Win7 - VMWar...**  
pc-addicts.com - 1of2 - I briefly demonstrate how to use a Linksys USB...  
by PCAddictsLive | 12,071 views

# Worldwide Infrastructure Security Report 2011

- Ideologically-Motivated "Hactivism" and Vandalism Are the Most Readily-Identified DDoS Attack Motivations
- 10 Gbps and Larger Flood-Based DDoS Attacks Are the "New Normal"
- Increased Sophistication and Complexity of Application-Layer (Layer 7) DDoS Attacks and Multi-Vector DDoS Attacks Are Becoming More Common
- Visibility and Security of Mobile and Fixed Wireless Networks Are an Ongoing Concern
- **First-Ever Reports of IPv6 DDoS Attacks "in the Wild" on Production Networks**
- **Rarity of IPv6-Enabled Attacks Indicates Low IPv6 Market Penetration and Lack of Critical Mass**
- Stateful Firewalls, IPS and Load-Balancer Devices Continue to Fall Short on DDoS Protection Capabilities
- The Overwhelming Majority of Network Operators Do Not Engage Law Enforcement

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

Botnets spreder sig ved at inficere så mange systemer som muligt

Botnets idag vokser gerne langsommere - ingen ny Code Red hastighedsrekord

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

Bannerkampagner og 3. parts kilder til elementer på din side?!

Når først der er kommet malware på systemet udvides med moduler

Malware idag er sofistikeret

Modulært opbygget

Benytter stærk 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



**Todays offer  
trojans**

Buy 2 pay for one



**Fresh botnets**

**Fresh phish**  
infected within the last  
week



**Support agreement**

**trojan support**  
email, IRC, IM  
Pay using credit card

Malware programmører har lært kundepleje

"Køb denne version og få gratis opdateringer"

Lej vores botnet med 100.000 computere

# 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](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](http://paypal-co.uk.dt6.pl/?login-run.websrcmd=_account-run.CaseIDNumberPP-046-631-789)

## Kan du selv genkende Phishing

# Zip files?

zspam — hlk@kramse.dk (473 unread)

Entire Message

474 messages

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

From: [randi@indocrafts.com](mailto:randi@indocrafts.com)  
Date: 14. marts 2005 19.23.01 MET  
To: [hlk@kramse.dk](mailto:hlk@kramse.dk)  
Subject: Re: Delivery Protection

Protected message is attached.

 message.zip (39.9 KB)

In (63 unread)

Entire Message

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](mailto:info@opinionsland.co)  
Date: 4. marts 2005 10.02.43 MET  
To: [hlk@kramse.dk](mailto:hlk@kramse.dk)  
Subject: Re: your data

Please read the important document.

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

## SCR er screensaver files - programmer

## 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 håndholdte enheder

- små - kan typisk ligge i en lomme
- meget lille lager til rådighed
- begrænset funktionalitet
- kan synkroniseres med en stationær computer ■
- meget stor lagerkapacitet i moderne udgaver!
- udvidet funktionalitet
- *viewer programmer* til Word, Excel, PDF m.fl.
- alt er forbundet idag, typisk netværk udeover GPRS/telefoni

Kan gemme mange data - hvor følsomme er data

- Kalender
- Kontakter
- Opgaver - To Do listen

Nem backup af data - nemt at stjæle alle oplysninger!

- flyt data applikationen på Nokia - data flytning **uden SIM kort**
- sikkerhedskopi til MMC kort - næsten alle data kan overføres < 1 minut

Adgang ind til virksomheden - via wireless?

- Genbruge loginoplysninger fra PDA og koble en laptop på netværket?

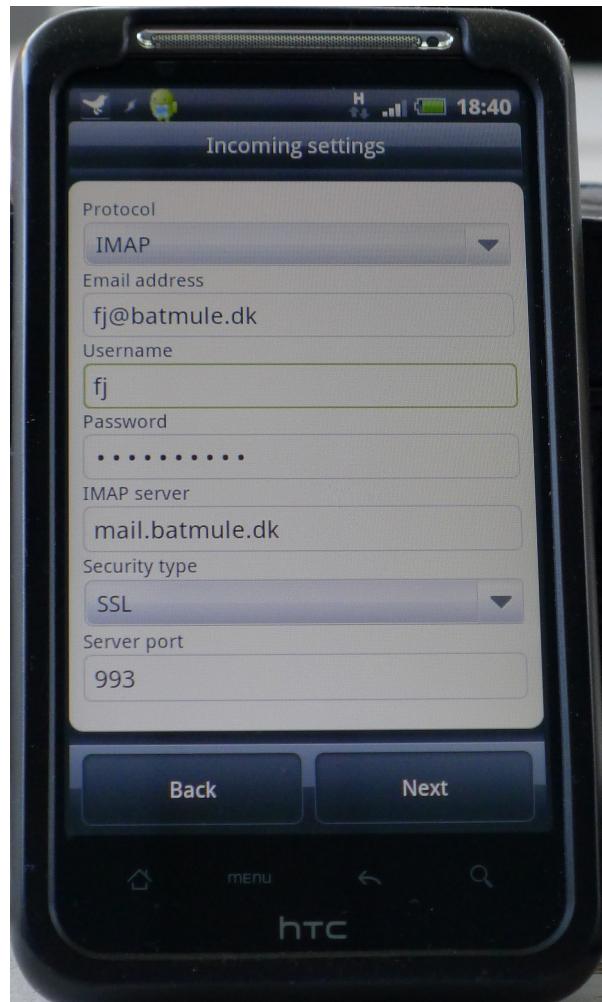
Brug teknologien

Lær teknologien at kende - læs manualen!

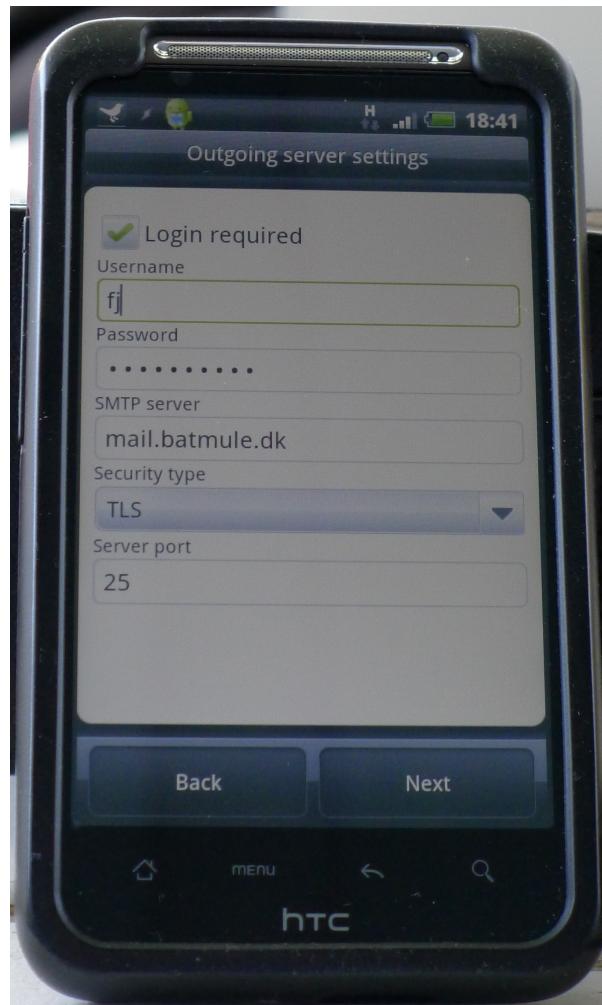
Tænk på følsomheden af data I gemmer og overfører

- Slå ting fra som I ikke bruger
- Slå bluetooth fra når I ikke bruger den
- Opdater softwaren på enheden
- Slå kryptering til hvor I kan: IMAPS, POP3S, HTTPS og over bluetooth
- Brug låsekode fremfor tastaturlås uden kode på mobiltelefonen
- Stol ikke for meget på fingertryksaflæsere

Istedet for POP3 brug POP3s, Istedet for IMAP brug IMAPs



SMTP kan erstattes med SMTP+TLS



Mange glemmer at låse bilen når de skal hente børn - travlhed

Mange lader deres baggage være ubevogtet i lufthavnen - sult tørst

Mange lader deres bærbare stå på kontoret - frit fremme

Mange forlader deres bærbare på et bord under konferencer

... simpelt tyveri er ofte muligt

eller er det industrispionage?

Lore ipsum dolor sit amet, consectetur adipisciing elit, set eiusmod tempor incididunt et labore et dolore magna aliquam. Ut enim ad minim veniam, qui nostrud exerc. Irure dolor in reprehend incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, qui nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse, cillum. Tia non ob ea soluad inco, quae egen ium impend. Officia deserunt mollit animorum. Et harumd dereud fac se er expedit distinct. Gothicā quam nunc putamus parum, aposuerit litterarum formas humanitatis per seacula quarta; modo typi is videntur parum clari flant sollemnes in futurum; litterarum formas humanitatis per seacula quinta et quinta decima, modo typi qui nūntur parur sollemnes in futuru rit ! Nam liber te conscient to factor tum pioque civi eque pecun moc honor et imper r et, conse ing elit, se ut dolore magna aliquam is nostrud exercitatio lo conse te in voluptate ve esse cillum dolore eu fugiat nulla pariatur. At vver e dignissum qui blandit est praesent.

# Stjålet laptop

## Slittede eller ødelagte data

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



Hvad betyder det at være superhelt?

Beskytte andre - og sig selv

Have ekspertviden



Hacking kræver blot lidt ninja-træning



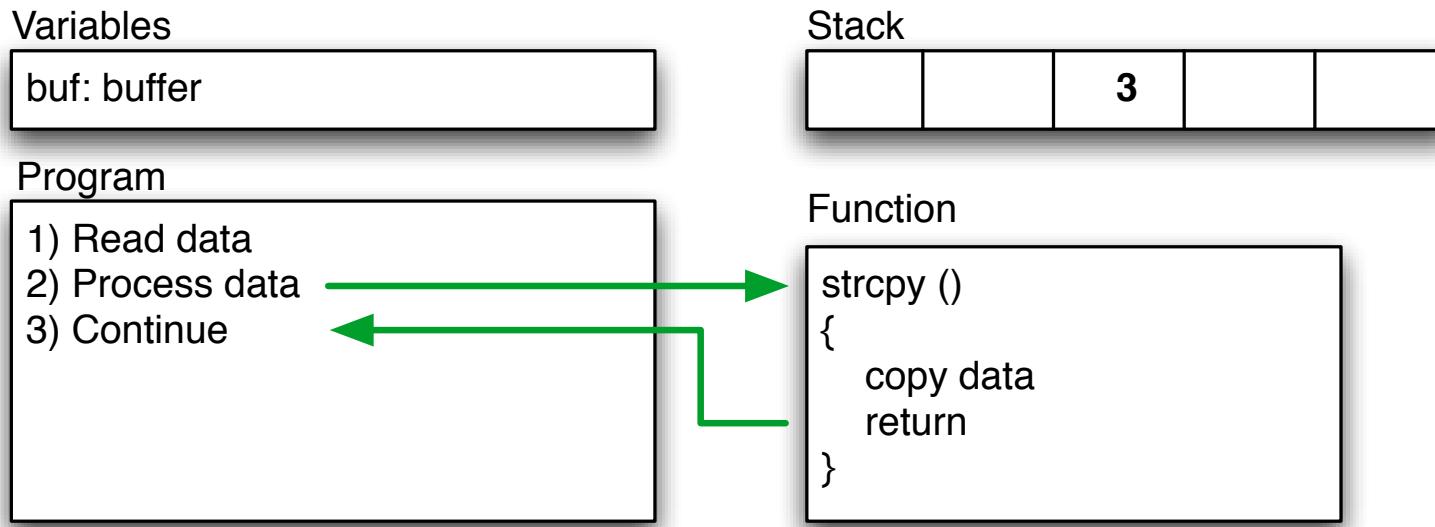
```
main(int argc, char **argv)
{
    char buf[200];
    strcpy(buf, argv[1]);
    printf("%s\n", buf);
}
```



**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.

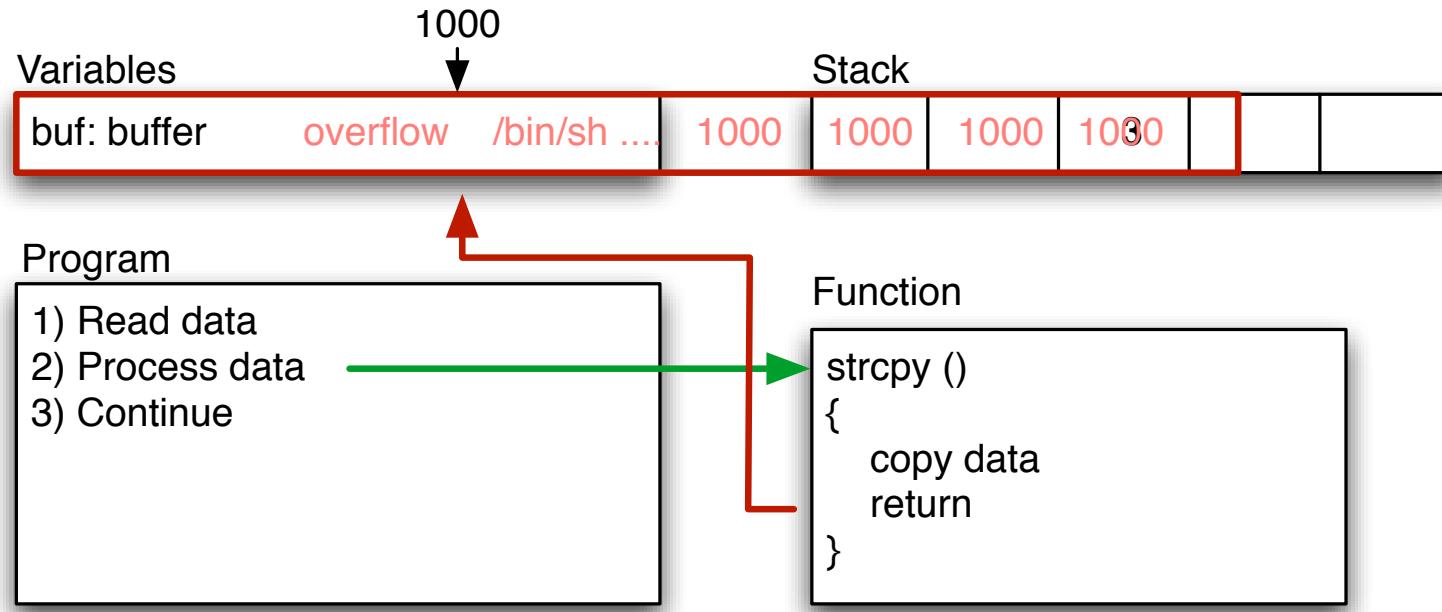
**Stack protection** er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.

# 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 Exploit Database - dagens buffer overflow



The screenshot shows the homepage of The Exploit Database. At the top, there is a navigation bar with links: [ home ], [ news ], [ remote ], [ local ], [ web ], [ dos ], [ shellcode ], [ papers ], [ search ], [ D ], [ submit ], and [ rss ]. To the right of the navigation bar, 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 of exploits and vulnerable software. It also mentions a cleanup and submission policy. Below this, there is a section titled "Remote Exploits" with a table listing various exploits. The table has columns for Date, D, A, V, Description, Plat., and Author. The exploits listed are:

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 exploit-db eller exploit packs

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**

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.

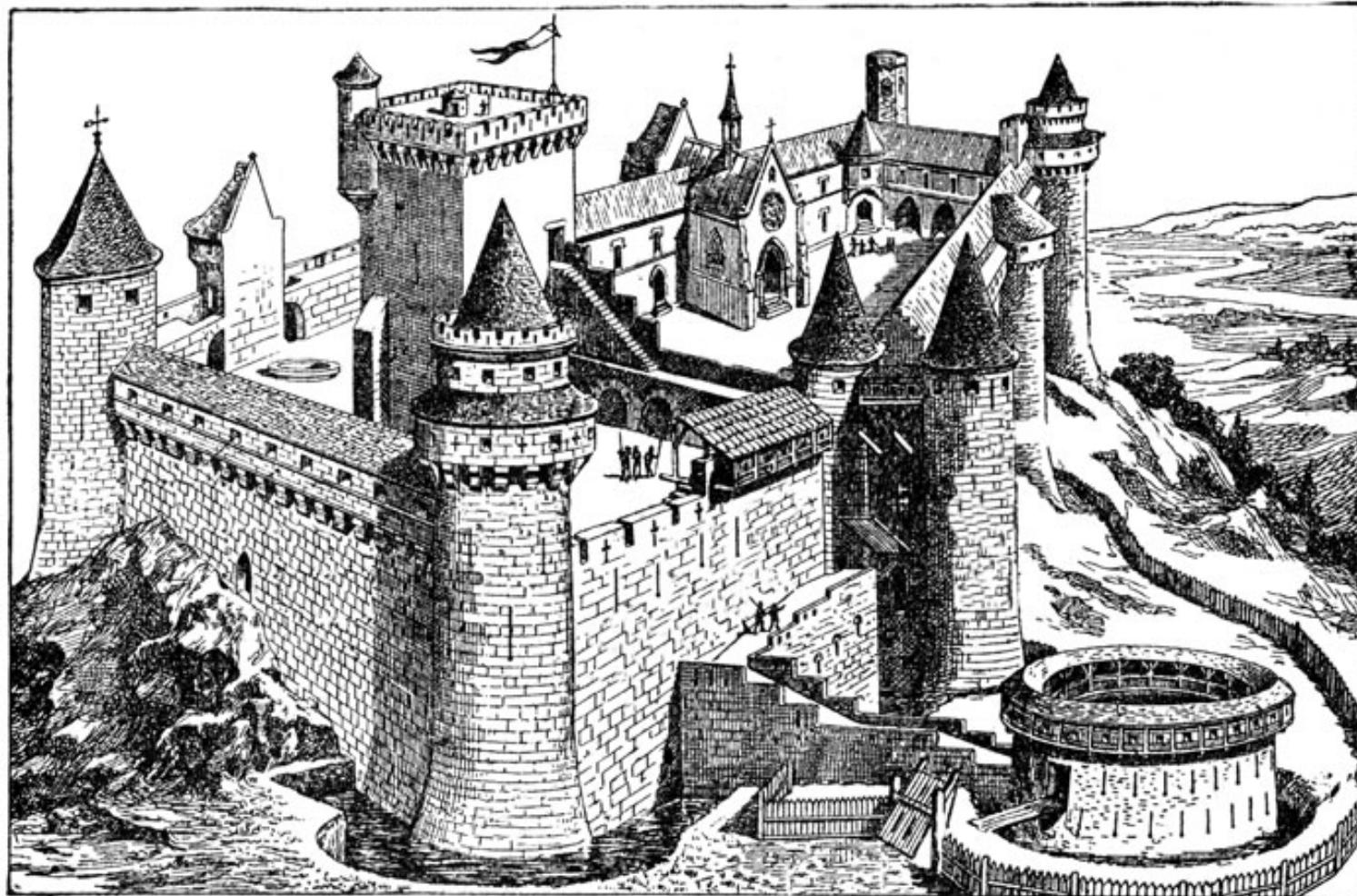
Vælg derfor hellere:

- 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

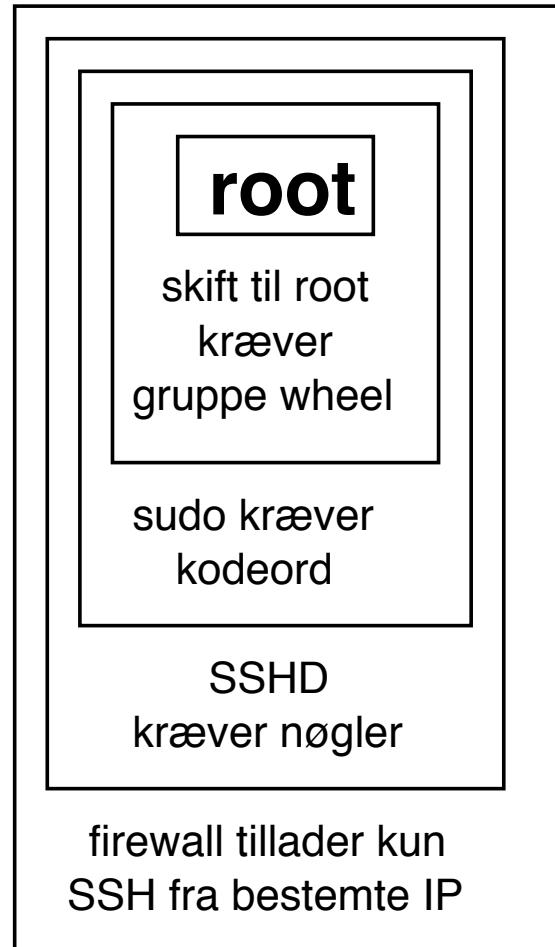
NB: meget få embedded systemer har beskyttelse!

# Enhance and secure runtime environment



Sidste chance er på afviklingstidspunktet

# Defense in depth - flere lag af sikkerhed



Forsvar dig selv med flere lag af sikkerhed!

Der findes mange typer *jails* på Unix

Ideer fra Unix chroot som ikke er en egentlig sikkerhedsfeature

- Unix chroot - bruges stadig, ofte i daemoner som OpenSSH
- FreeBSD Jails
- SELinux
- Solaris Containers og Zones - *jails på steroider*
- VMware virtuelle maskiner, er det et jail?

Hertil kommer et antal andre måder at adskille processer - sandkasser

Husk også de simple, database som `postgresql`, Tomcat som `tomcat`, Postfix postsystem som `postfix`, SSHD som `sshd` osv. - simple brugere, få rettigheder

## systrace - generate and enforce system call policies

### EXAMPLES

An excerpt from a sample `ls(1)` policy might look as follows:

```
Policy: /bin/ls, Emulation: native
[...]
    native-fsread: filename eq "$HOME" then permit
    native-fchdir: permit
[...]
    native-fsread: filename eq "/tmp" then permit
    native-stat: permit
    native-fsread: filename match "$HOME/*" then permit
    native-fsread: filename eq "/etc/pwd.db" then permit
[...]
    native-fsread: filename eq "/etc" then deny[eperm], if group != wheel
```

### SEE ALSO

`systrace(4)`

```
// ===== WEB APPLICATION PERMISSIONS =====
// These permissions are granted by default to all web applications
// In addition, a web application will be given a read FilePermission
// and JndiPermission for all files and directories in its document root.
grant {
    // Required for JNDI lookup of named JDBC DataSource's and
    // javamail named MimePart DataSource used to send mail
    permission java.util.PropertyPermission "java.home", "read";
    permission java.util.PropertyPermission "java.naming.*", "read";
    permission java.util.PropertyPermission "javax.sql.*", "read";
...
};
// The permission granted to your JDBC driver
// grant codeBase "jar:file:$catalina.home/webapps/examples/WEB-INF/lib	driver.jar!/-" {
//     permission java.net.SocketPermission "dbhost.mycompany.com:5432", "connect";
// };
```

Eksempel fra apache-tomcat-6.0.18/conf/catalina.policy

# Apple sandbox named generic rules

```
; ; named - sandbox profile
; ; Copyright (c) 2006-2007 Apple Inc. All Rights reserved.
; ;
; ; WARNING: The sandbox rules in this file currently constitute
; ; Apple System Private Interface and are subject to change at any time and
; ; without notice. The contents of this file are also auto-generated and not
; ; user editable; it may be overwritten at any time.
; ;
(version 1)
(debug deny)

(import "bsd.sb")

(deny default)
(allow process*)
(deny signal)
(allow sysctl-read)
(allow network*)
```

# Apple sandbox named specific rules

```
;; Allow named-specific files
(allow file-write* file-read-data file-read-metadata
  (regex "^(/private)?/var/run/named\\\.pid$"
         "^(/Library/Logs/named\\\.log$"))

(allow file-read-data file-read-metadata
  (regex "^(/private)?/etc/rndc\\\.key$"
         "^(/private)?/etc/resolv\\\.conf$"
         "^(/private)?/etc/named\\\.conf$"
         "^(/private)?/var/named/"))
```

Eksempel fra /usr/share/sandbox på Mac OS X

## **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 Java, Flash og PDF?

Kilde: [http://en.wikipedia.org/wiki/Drive-by\\_download](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?

Backup - jævnligt

Kryptografi - brug så vidt muligt kryptering og kryptoværktøjer

Sikre protokoller - som ofte bruger kryptering

Tal frit

Lær og lær fra dig

Følg med i nyhederne



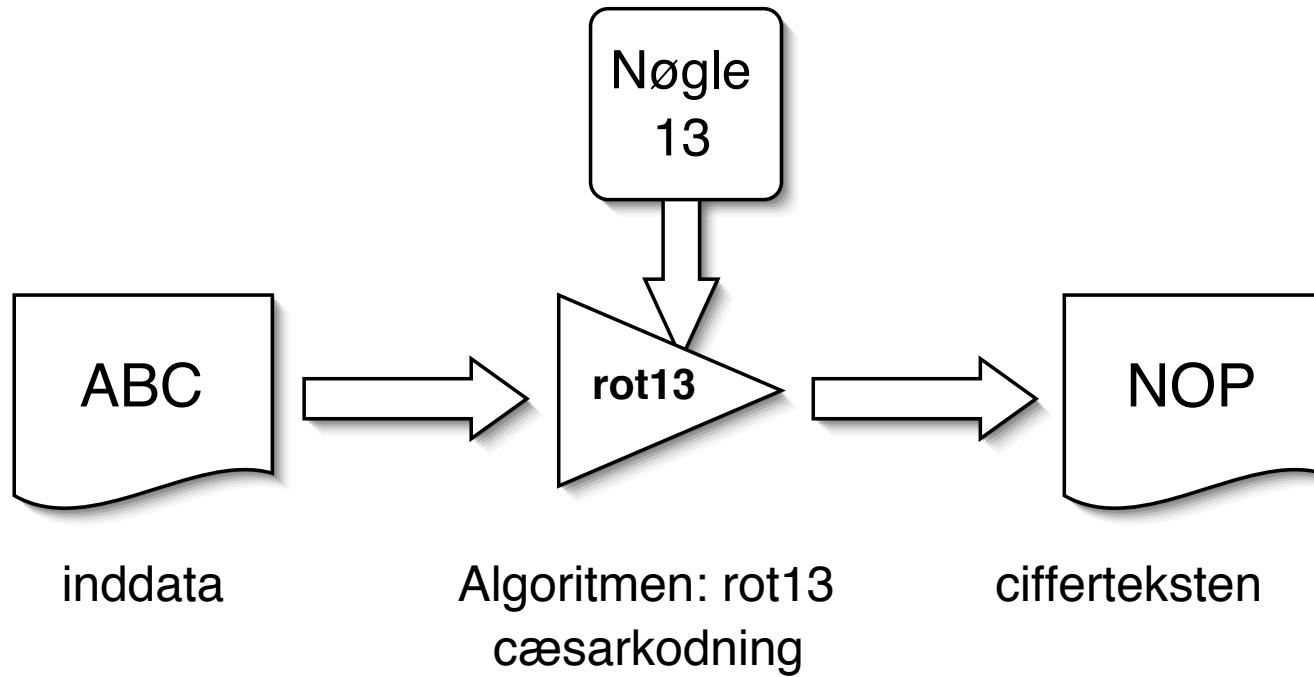
# Kom igang!

Formålet med kryptering

kryptering er den eneste måde at sikre:

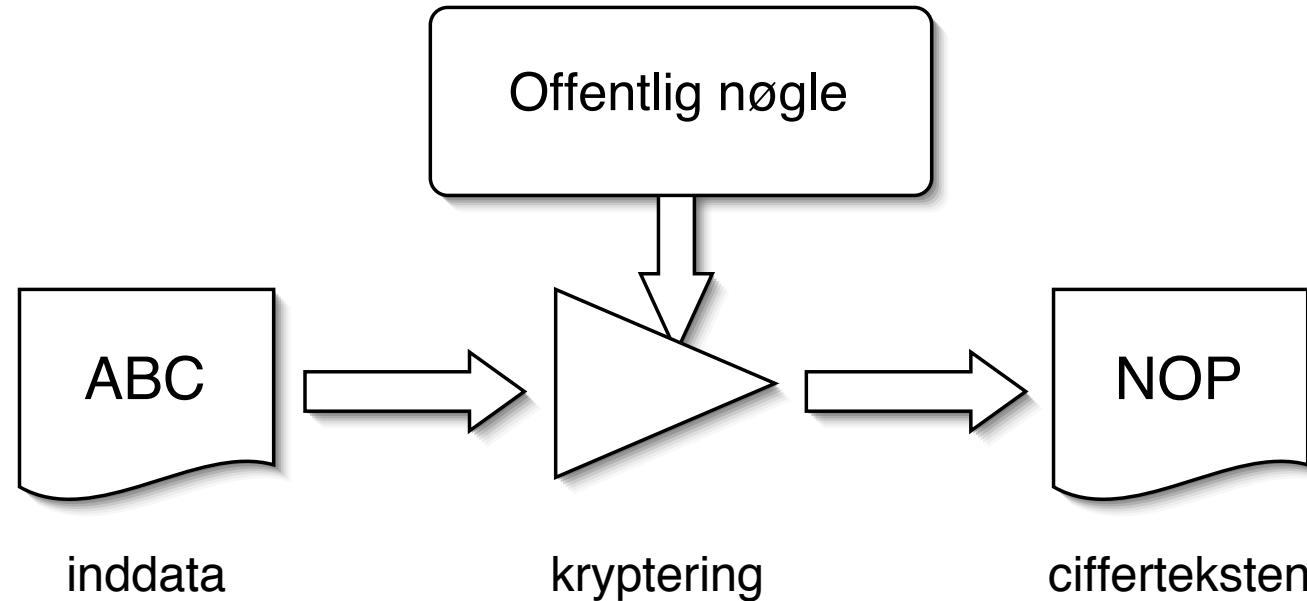
fortrolighed

autenticitet / integritet



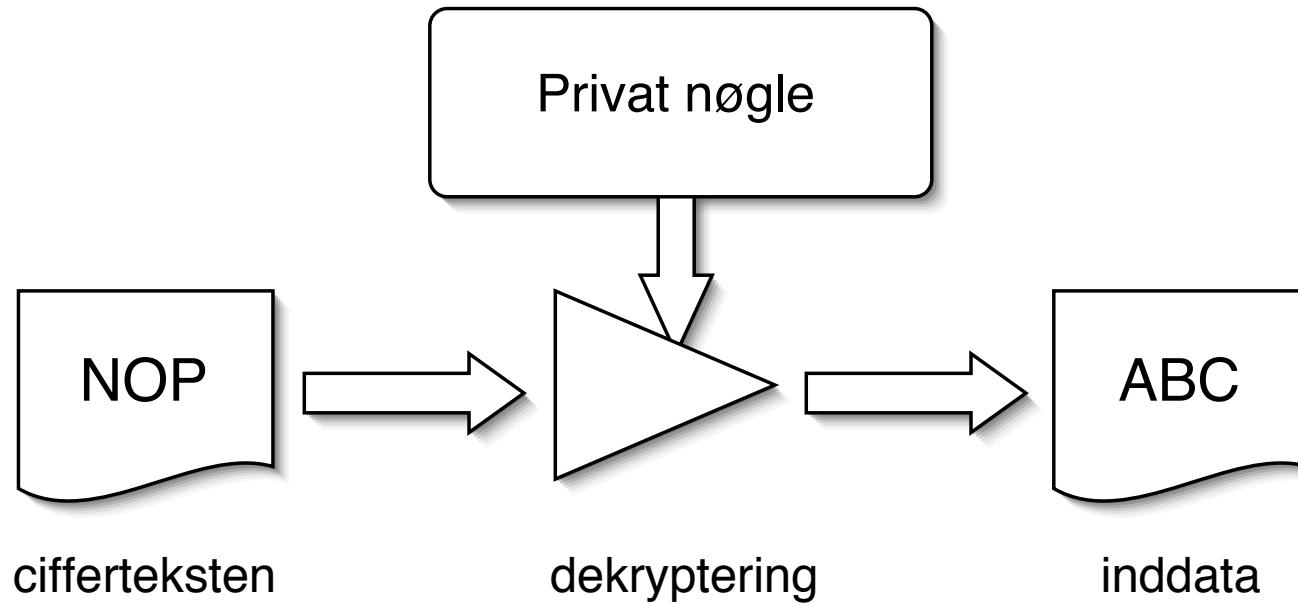
Kryptografi er læren om, hvordan man kan kryptere data

Kryptografi benytter algoritmer som sammen med nøgler giver en cifertekst - 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>



## 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

## The 5<sup>th</sup> 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."**

## Kryptering af e-mail

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

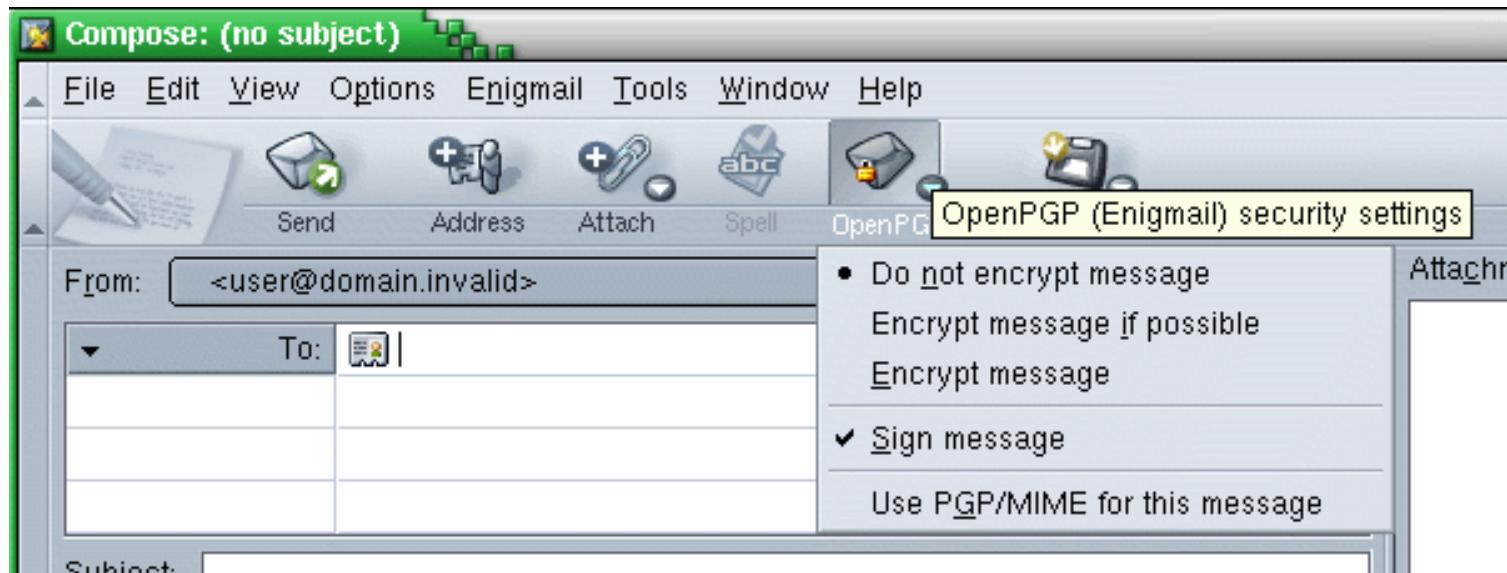
## Kryptering af sessioner SSL/TLS

- 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.

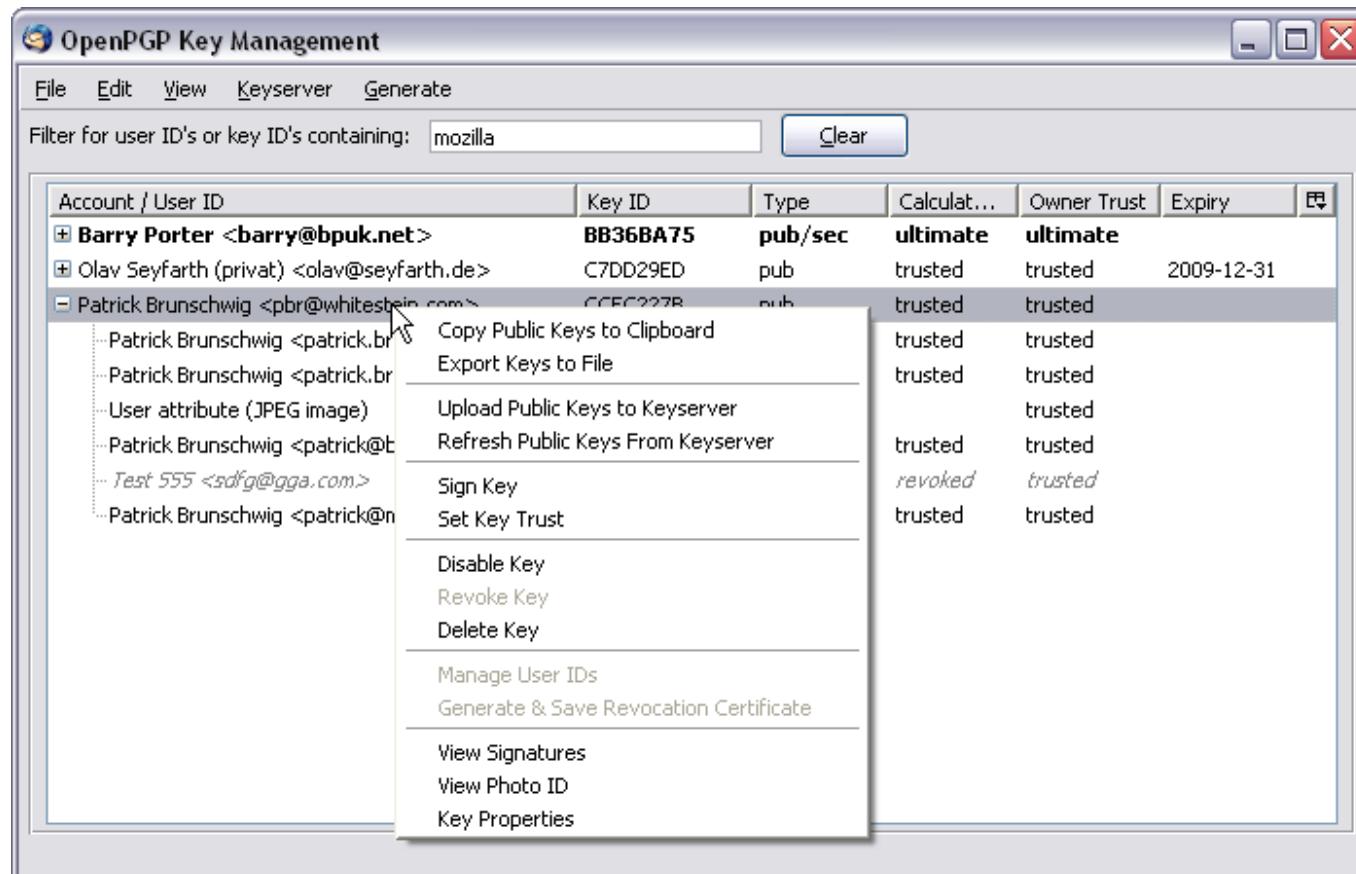
## Kryptering af netværkstrafik - Virtual Private Networks VPN

- IPsec IP Security Framework, se også L2TP
- PPTP Point to Point Tunneling Protocol - dårlig og usikker, brug den ikke mere!
- OpenVPN m.fl.

# Enigmail - GPG plugin til Mail

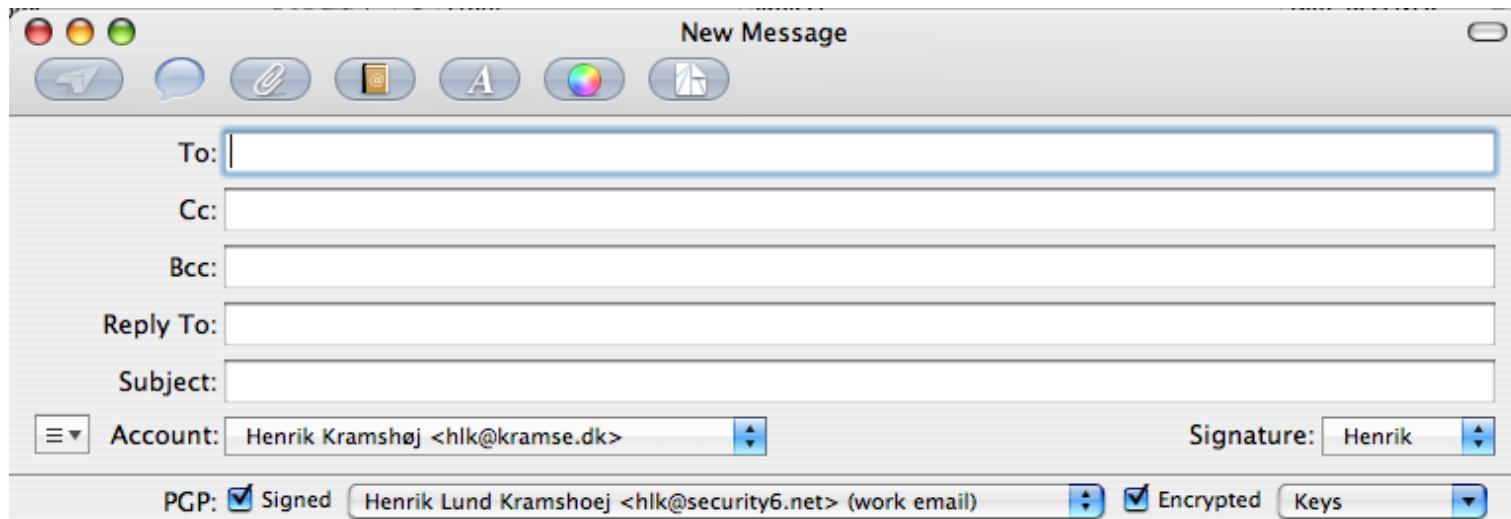


- Enigmail er en udvidelse til
- mailklienten i Mozilla/Netscape
- standalone mailklienten Thunderbird
- Billede fra <http://enigmail.mozdev.org>



Key Manager funktionaliteten i Enigmail kan anbefales

# GPGMail plugin til Mac OS X Mail.app



--  
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>

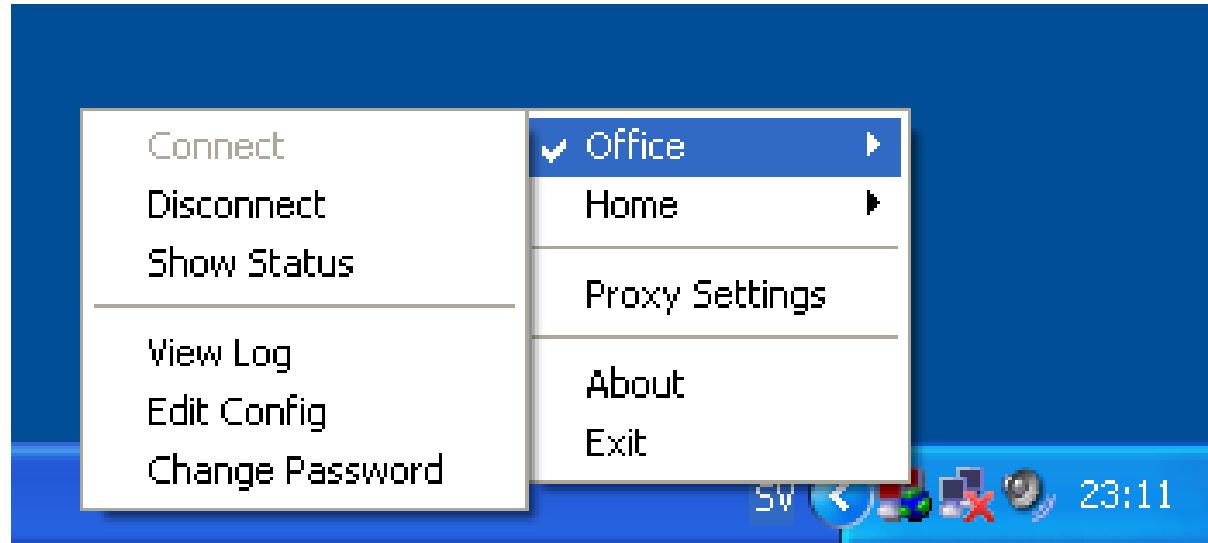
VPN [http://en.wikipedia.org/wiki/Virtual\\_private\\_network](http://en.wikipedia.org/wiki/Virtual_private_network)

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

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/>



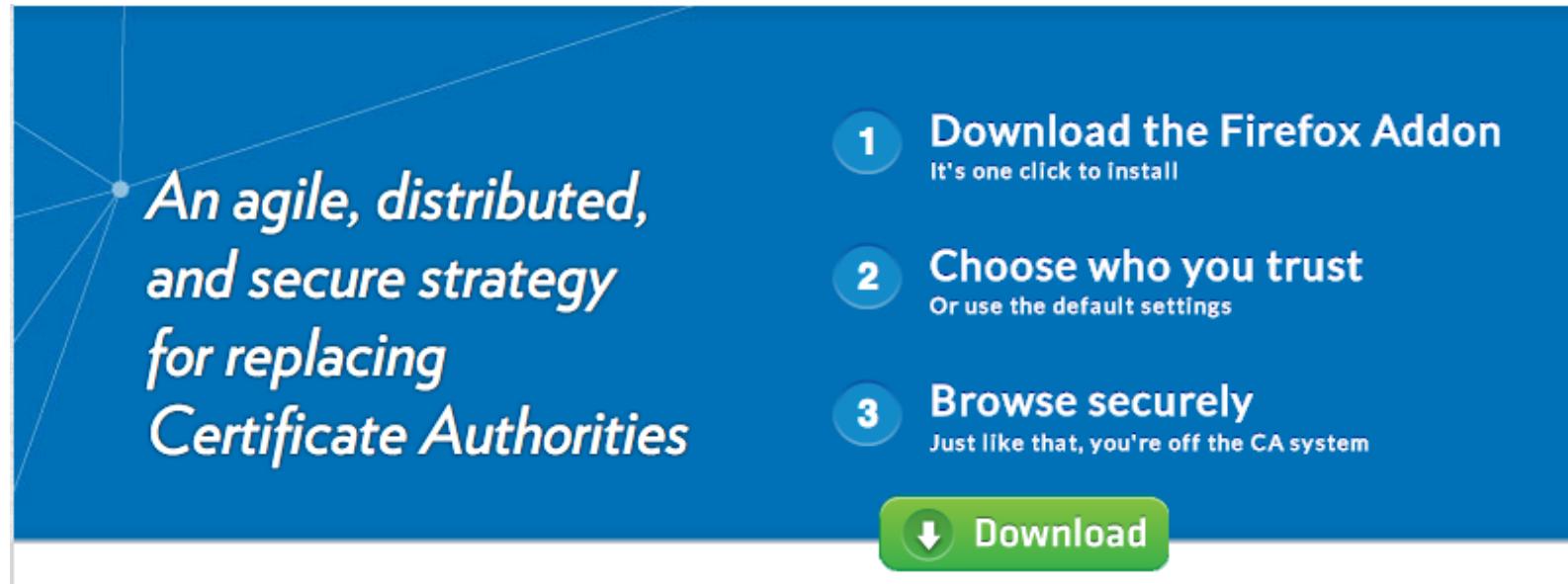
HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

<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

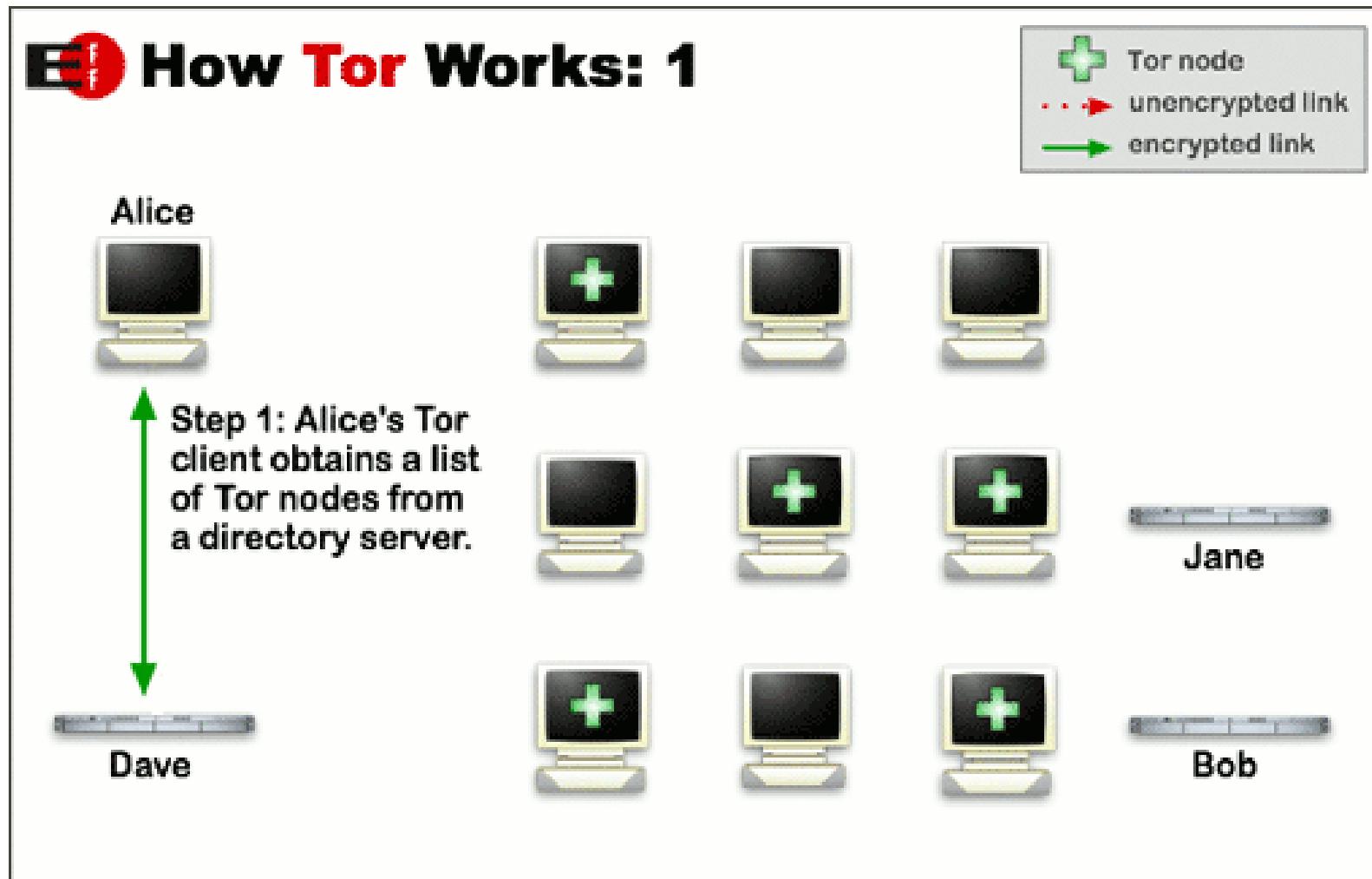
Protect your privacy. Defend yourself against network surveillance and traffic analysis.



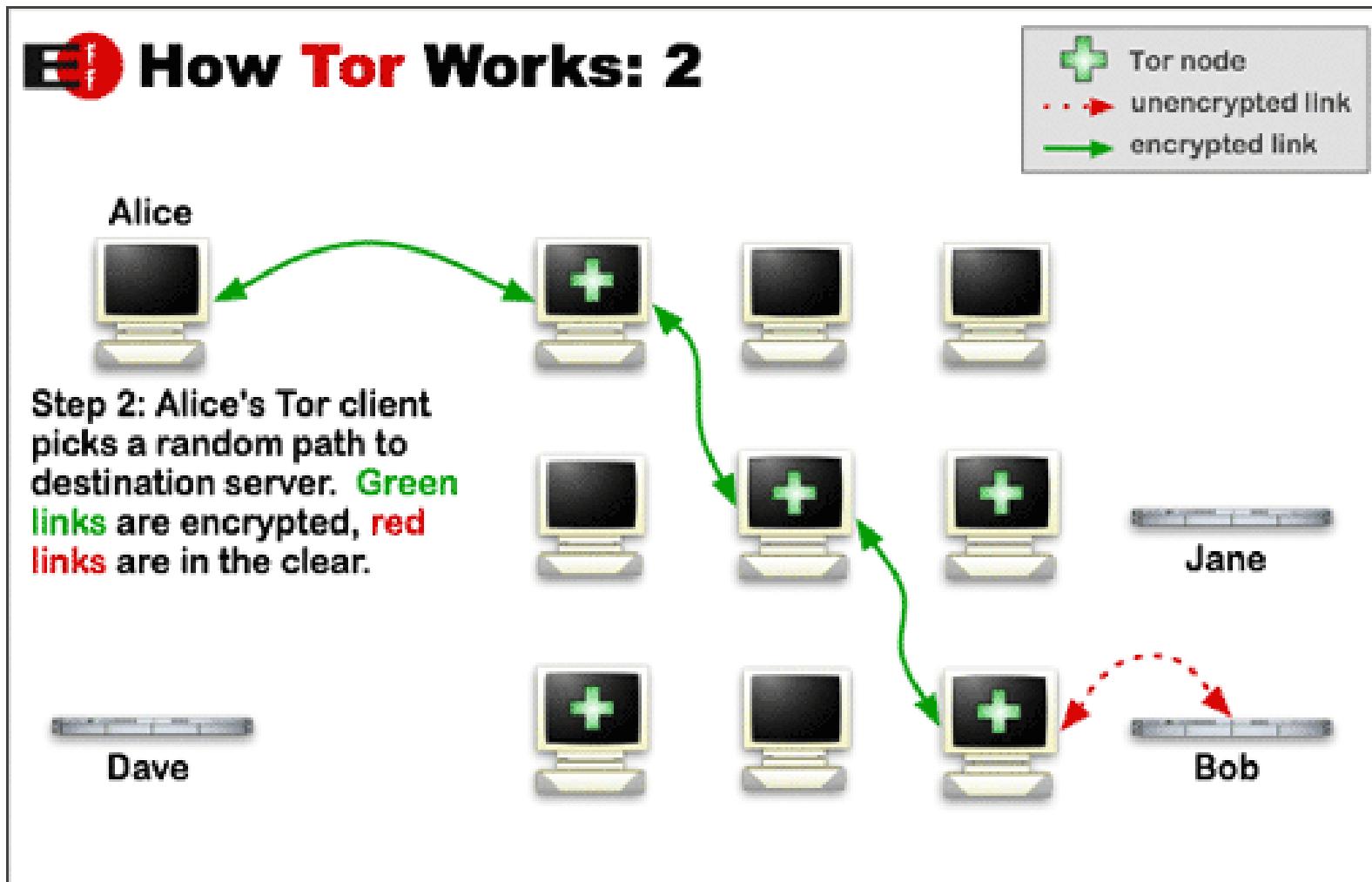
Download Tor 

- ➔ 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

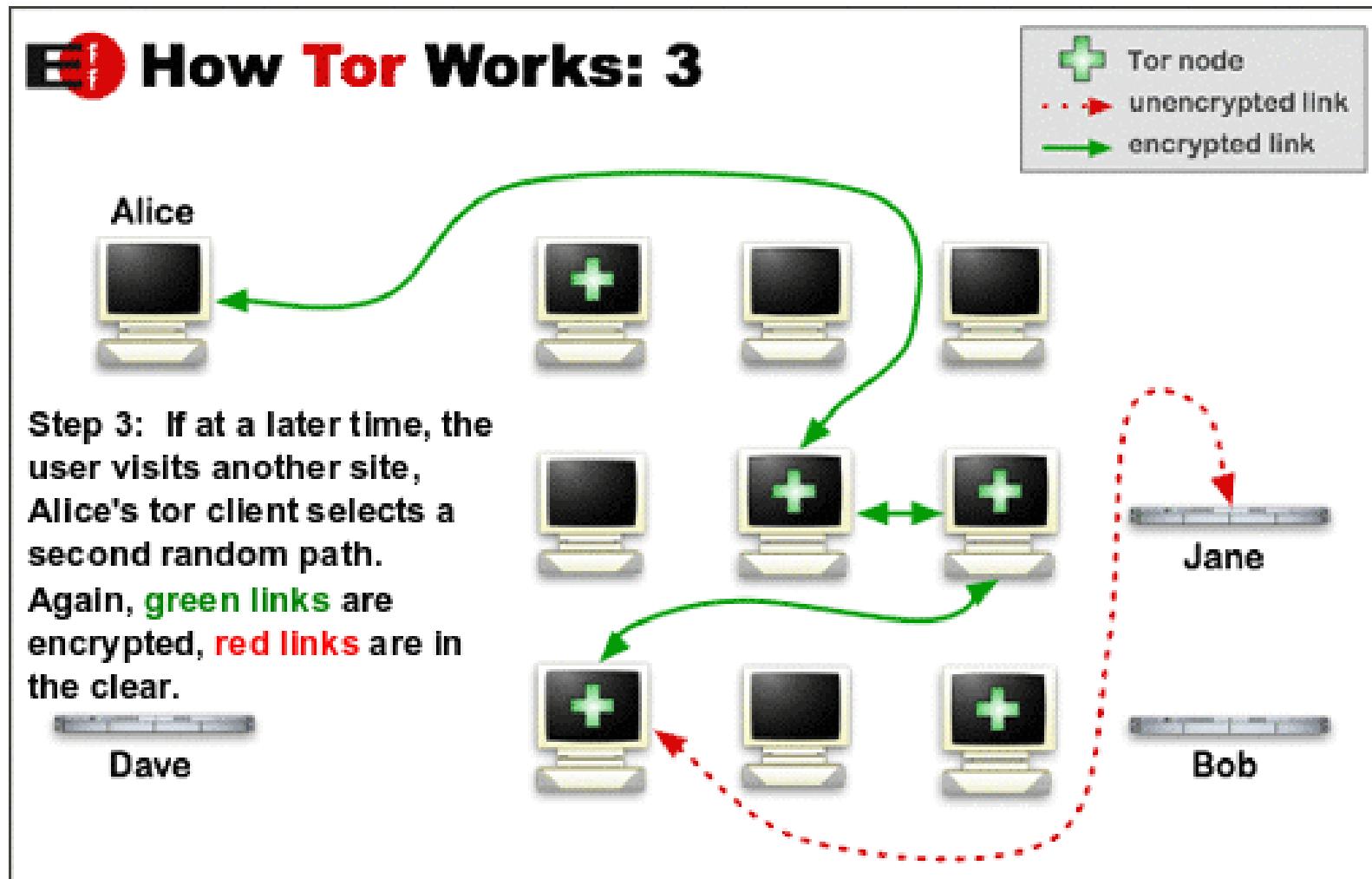
<https://www.torproject.org/>



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>

# Bonus: brug Bitcoins?

## BITCOIN NORDIC

Instant Bitcoins

[Buy Bitcoins](#) [Sell Bitcoins](#) [News](#) [About us](#)



Credit card



Pay through eWire which accepts VISA, VISA Electron, MasterCard, Maestro, and DanKort issued in Scandinavian countries.  
Delivery time: 1 minute.

Bank transfer



Domestic, SEPA (European Union) or international wire transfers to our Danish bank account.  
Delivery time: 0-48 hours.

Cash or check



Cash or check by mail or in-person deposit at various locations.  
Delivery time: 5 minutes.

# 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](http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml)

# Følg med Twitter news



The screenshot shows the Twitter profile for the account @safety, which is associated with Twitter HQ. The profile picture is the blue Twitter bird. The account has a verified checkmark and is followed by the user who took the screenshot. The bio reads: "Twitter's Trust and Safety Updates! http://help.twitter.com/forums/10711/entries/76036". Below the bio is a green "Following" button. A text input field says "Tweet to @safety". The navigation bar includes "Tweets" (which is selected), "Favorites", "Following", "Followers", and "Lists". Three tweets are listed:

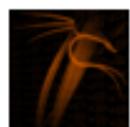
- safety Safety**  
Also, we will never send you an email saying that you've been suspended for "tweeting too much." Those emails are fake & not from us.  
26 Sep
- safety Safety**  
We will never send you emails requiring you to "complete offers" in order to unsuspend your account. That's spam, not 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](http://bit.ly/accountamiss)  
21 Sep

Twitter has become an important new resource for lots of stuff

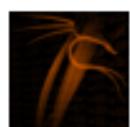
Twitter has replaced RSS for me



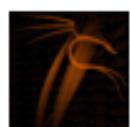
**exploitdb** [webapps] – BPAffiliate Affiliate Tracking  
Authentication Bypass Vulnerability: <http://bit.ly/9LOC3K>  
about 5 hours ago via twitterfeed



**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



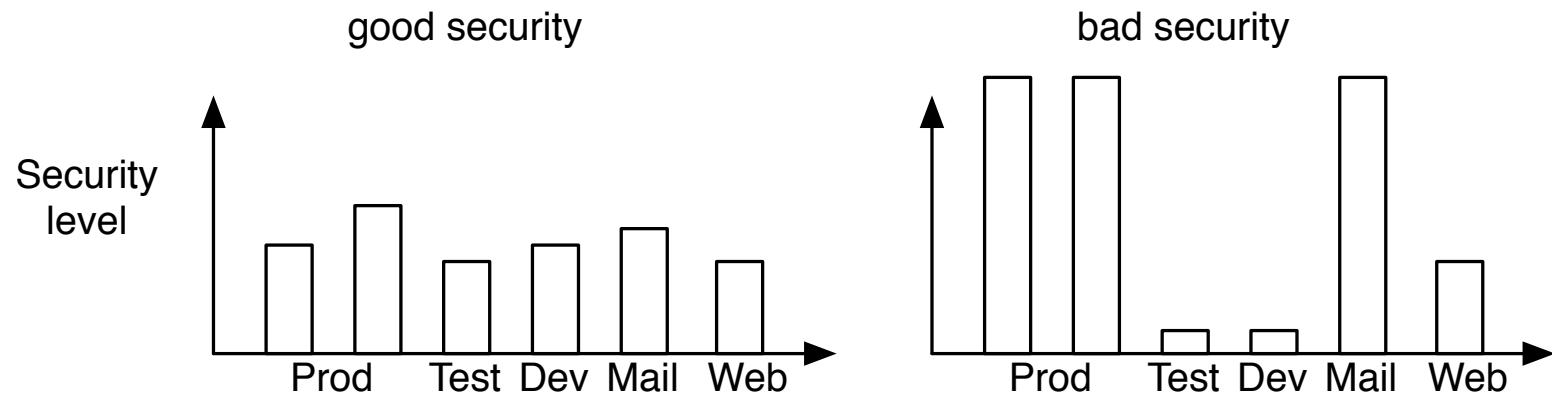
**exploitdb** [webapps] – BPRalestate Real Estate  
Authentication Bypass Vulnerability: <http://bit.ly/bYx2aY>  
about 5 hours ago via twitterfeed



**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

## Exploits og nye sårbarheder

- 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.



Det er bedre at have et ensartet niveau

Hvor rammer angreb hvis du har Fort Knox et sted og kaos andre steder

Hackere vælger ikke med vilje den sværreste vej ind



Team up!

Snak med din sidemand/dame - I har sikkert mange af de samme udfordringer.



PROSA afholdt fredag 17. september - til lørdag 18. september 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

I 1993 skrev Dan Farmer og Wietse Venema artiklen  
*Improving the Security of Your Site by Breaking Into it*

I 1995 udgav de softwarepakken SATAN  
*Security Administrator Tool for Analyzing Networks*

We realize that SATAN is a two-edged sword - like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

Se <http://sectools.org> og <http://www.packetstormsecurity.org/>

Kilde: <http://www.fish2.com/security/admin-guide-to-cracking.html>



Hey, Lets be careful out there!

Kilde: Michael Conrad <http://www.hillstreetblues.tv/>

Henrik Lund Kramshøj, internet samurai  
[hlk@solido.net](mailto:hlk@solido.net)

<http://www.solidonetworks.com>

I er altid velkomne til at sende spørgsmål på e-mail

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).