Velkommen til

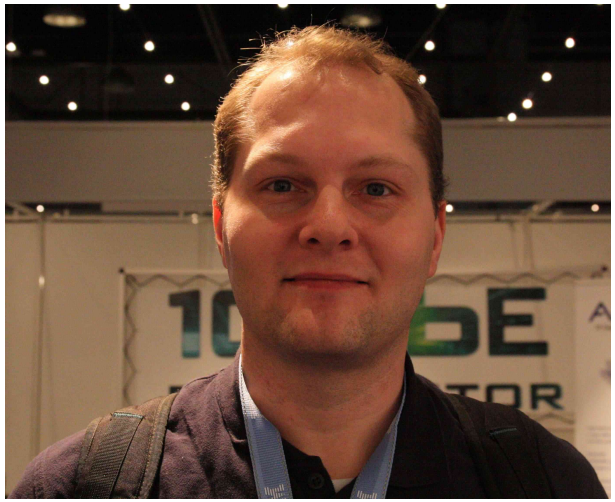
IT-sikkerhed 2012

PROSA Superhelteseminar

Henrik Lund Kramshøj
hlk@solido.net

http://www.solidonetworks.com

Kontaktinformation og profil



- 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

Planen idag

Don’t Panic!

Kl 17:00-19:00

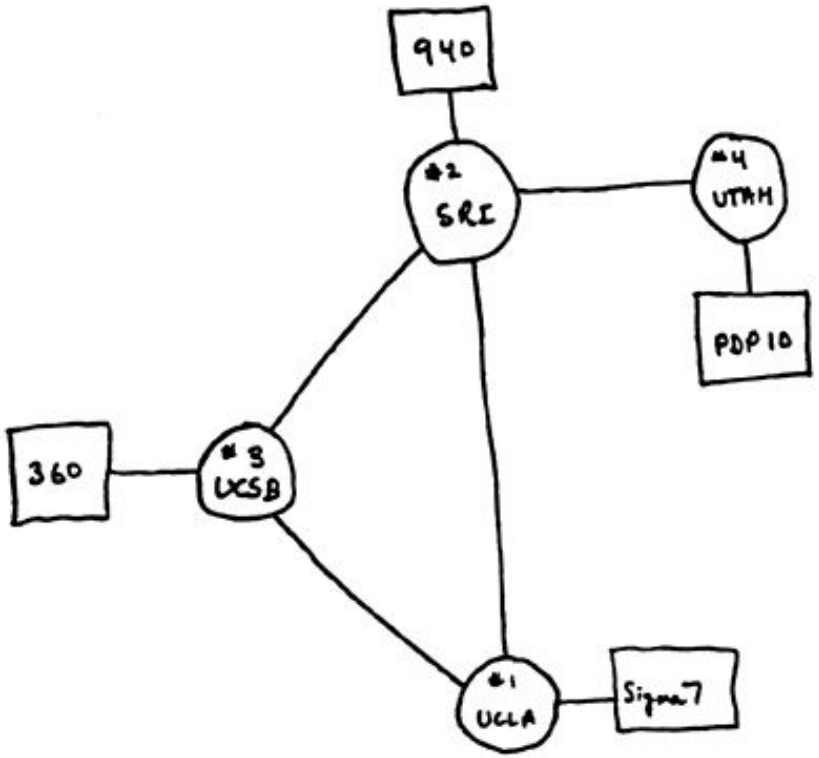
Mindre foredrag mere snak

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

Formål: mere specifikt

Vores data er overalt

Vi er afhængige af computere

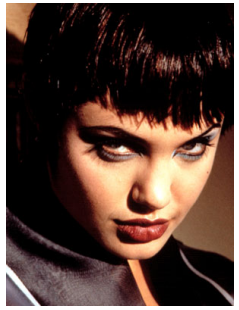
Vi er afhængige af netværk

Vi er afhængige af andres computere - servere og services

...

Formål: sund paranoia

Hackerværktøjer



- Nmap, Nping - tester porte, godt til firewall admins `http://nmap.org`
- Metasploit Framework gratis på `http://www.metasploit.com/`
- Wireshark avanceret netværkssniffer - `http://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

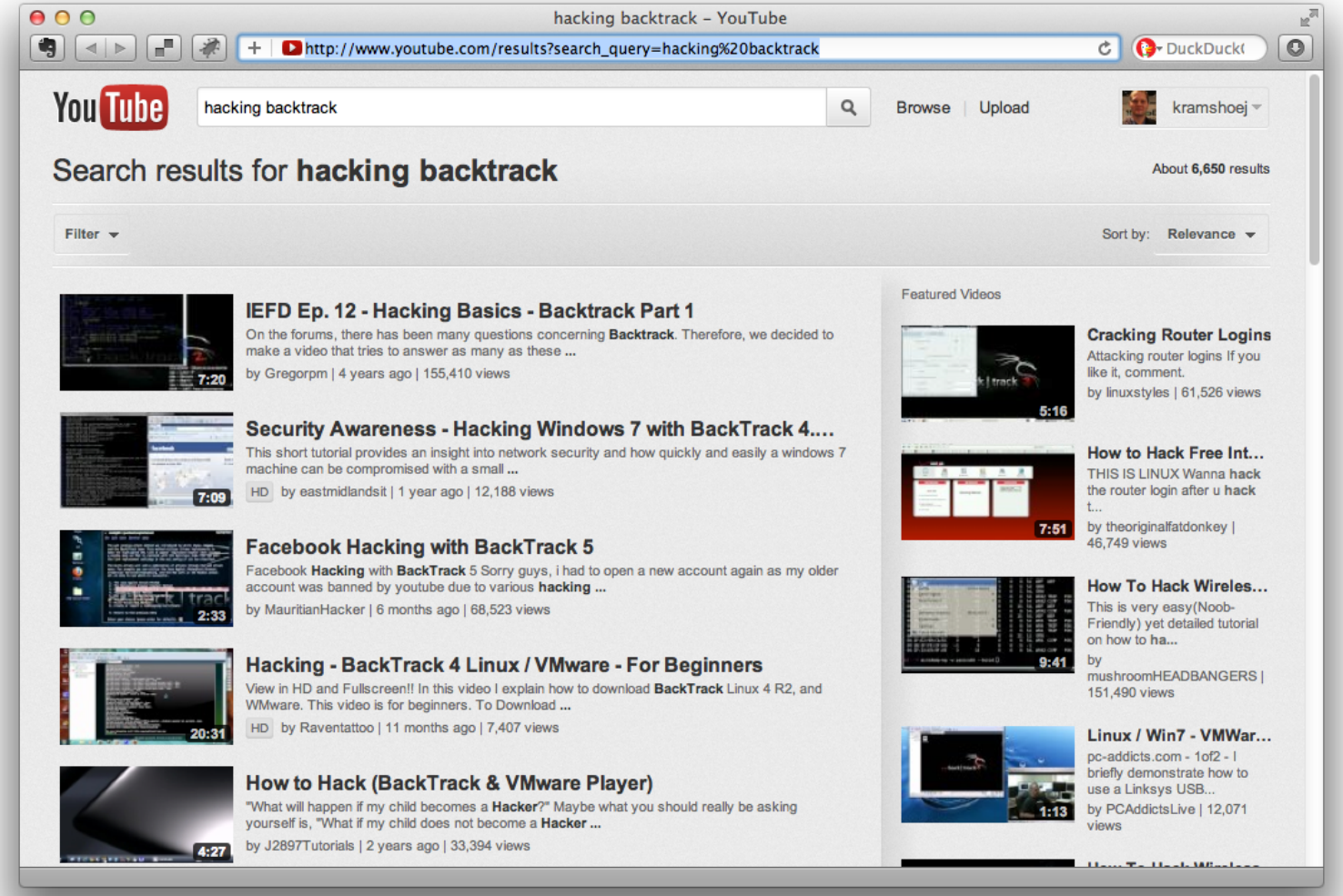
BackTrack 5 og sniffer programmer

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?

Status idag på internet



Worldwide Infrastructure Security Report 2011

SOLIDO NETWORKS

- 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`

Moderne botnets

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

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

Botnets og malware sælges med support

Dagens tilbud

trojanere

Køb 2 betal for 1

Friske botnets

Friske phish
inficeret indenfor den seneste uge

Supportaftale

trojanersupport
email, IRC, IM
Betal med kreditkort

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:

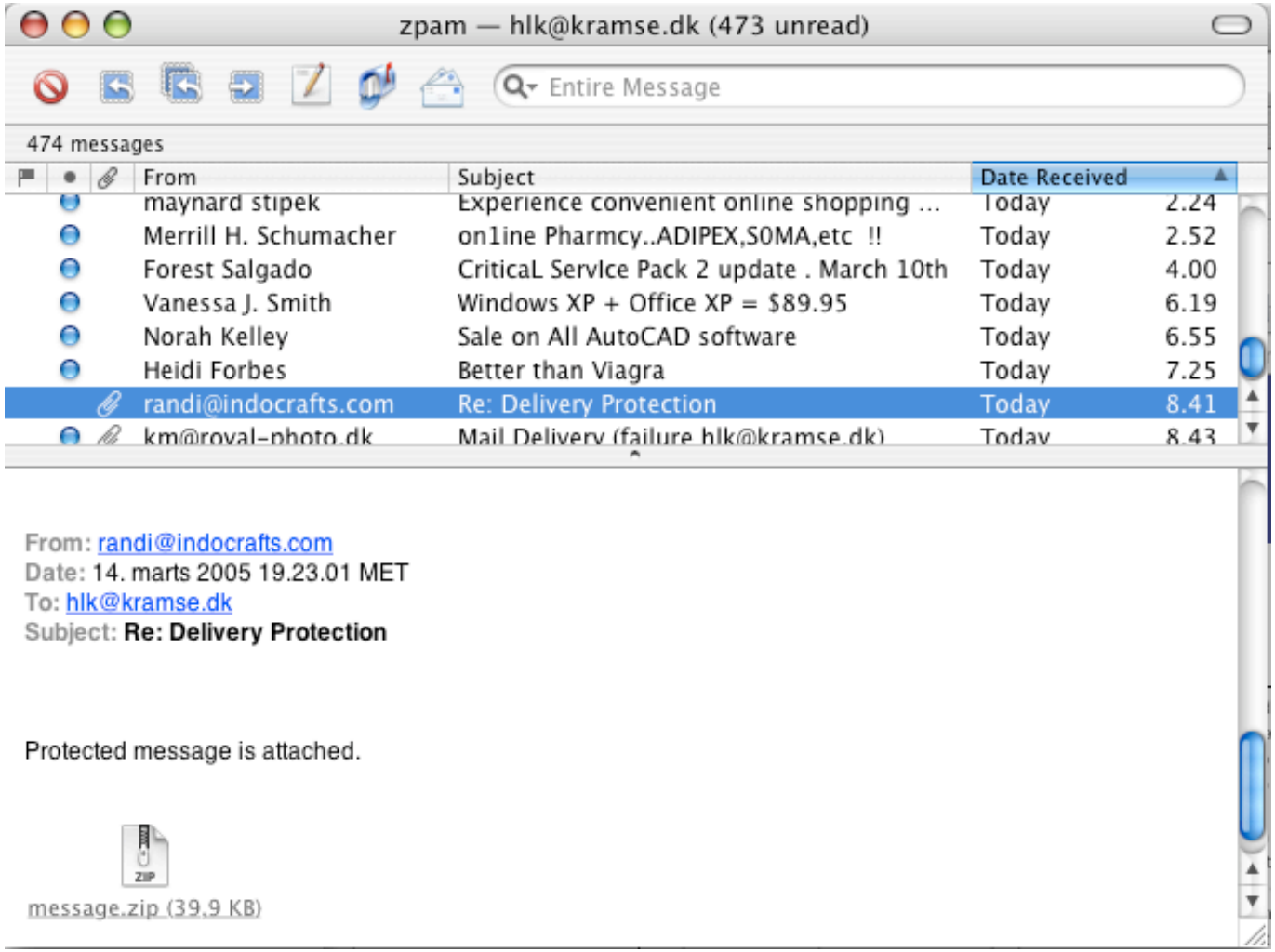
https://www.paypal.com/cgi-bin/webscr/cgi-bin/webscr?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

*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)
---

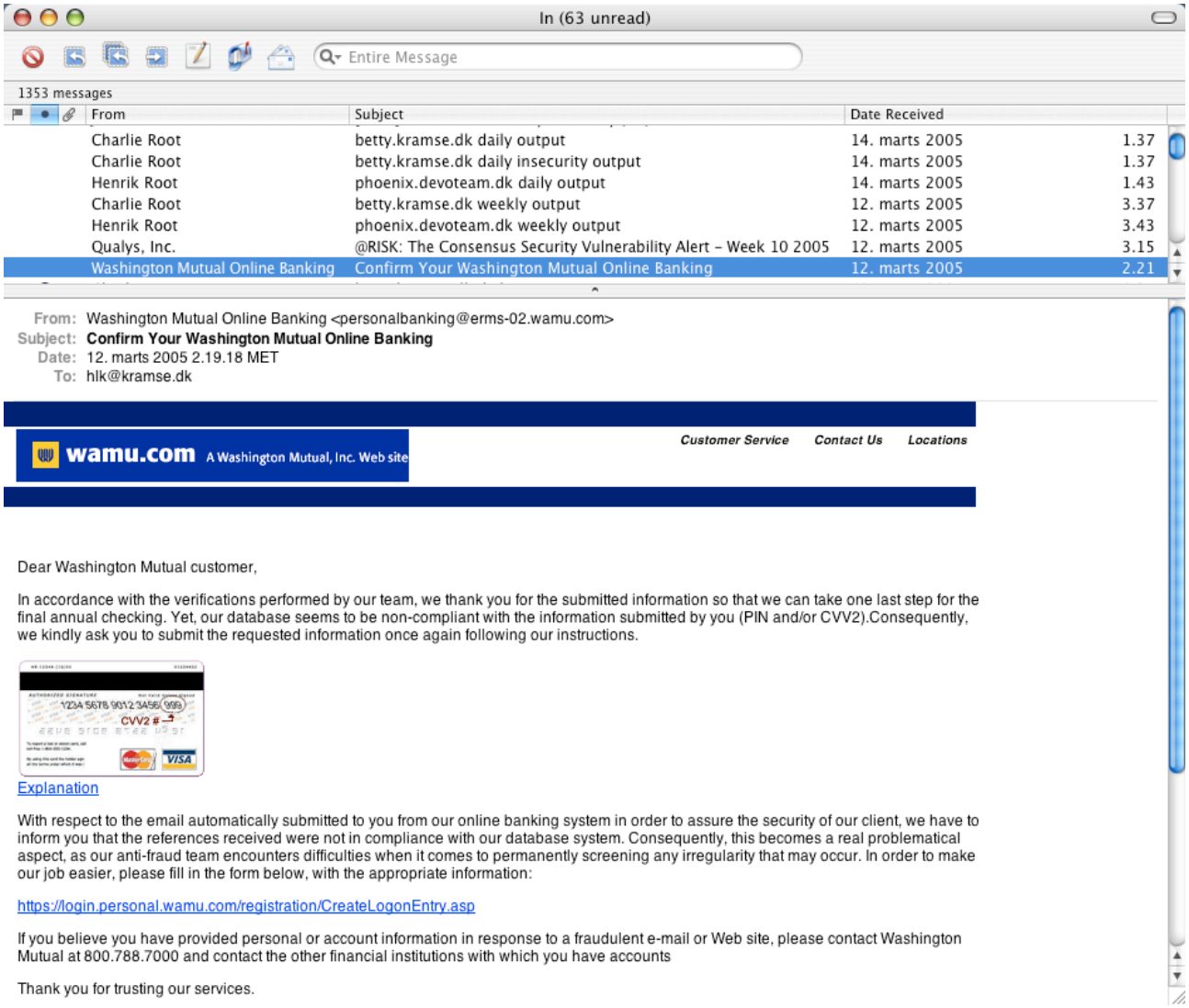
http://paypal-co.uk.dt6.pl/?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

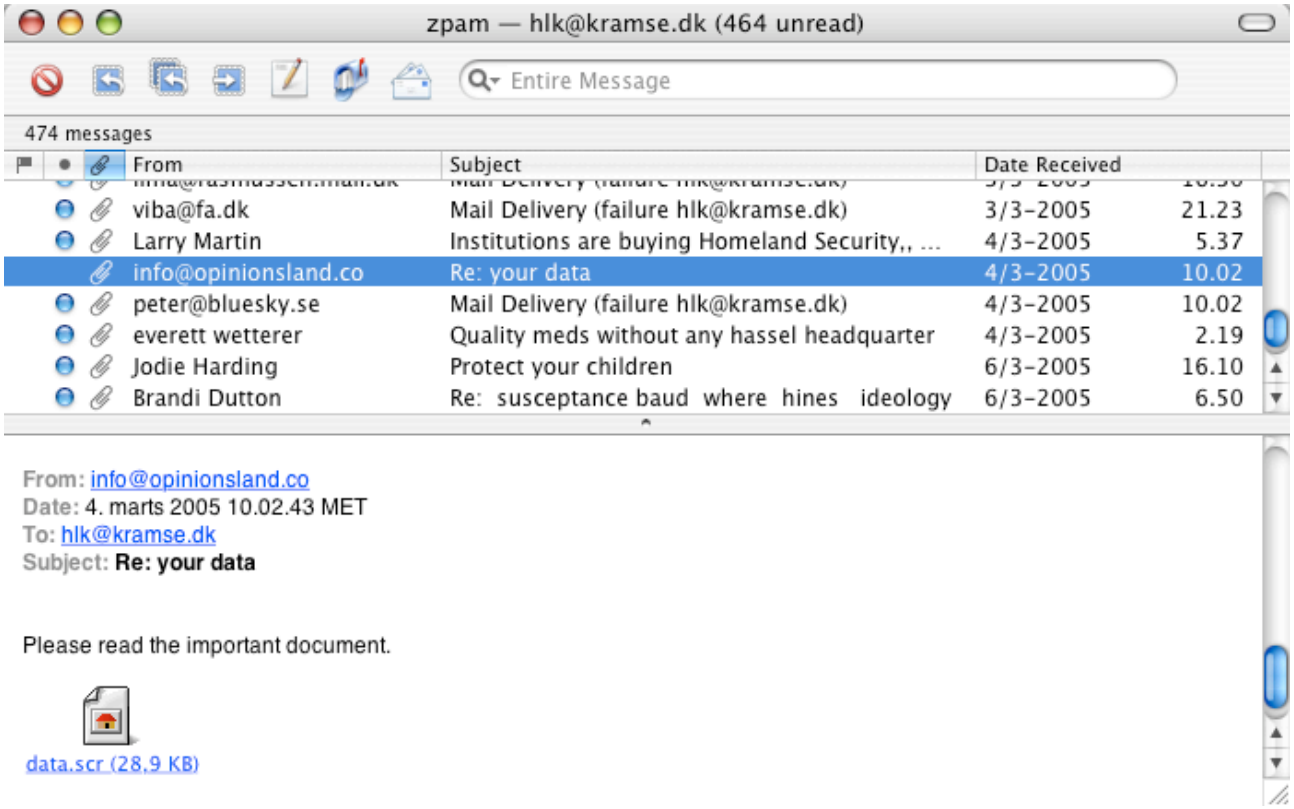
Kan du selv genkende Phishing

Zip files?



Money!





SCR er screensaver files - programmer

Fremtiden - er success en risiko

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*

Håndholdte enheder

SOLIDO NETWORKS

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 udover GPRS/telefoni

Problemer med smart phones/PDA

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?

Gode råd til jer

Brug teknologien

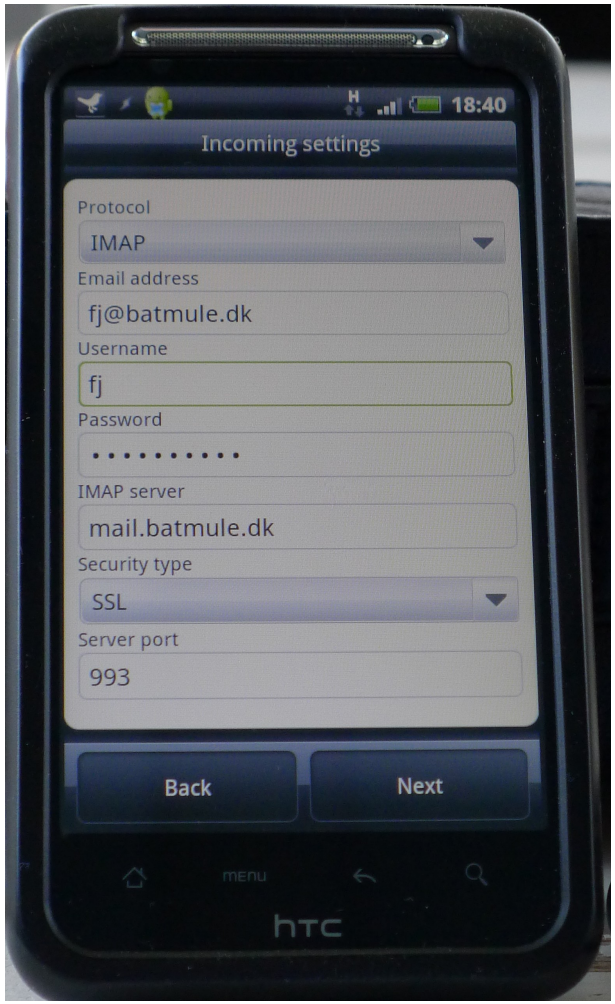
Lær teknologien at kende - læs manualen!

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: IMAP**S**, POP3**S**, HTTP**S** og over bluetooth
- Brug låsekode fremfor tastaturlås uden kode på mobiltelefonen
- Stol ikke for meget på fingertryksaflæsere

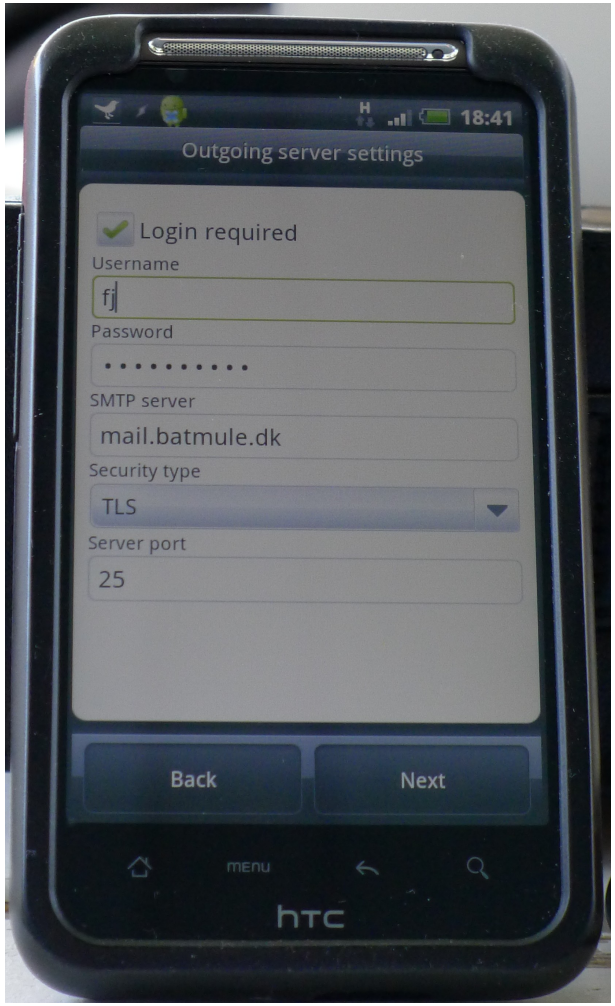
SSL/TLS (1)

Istedet for POP3 brug POP3s, Istedet for IMAP brug IMAPs



SSL/TLS (2)

SMTP kan erstattes med SMTP+TLS



Tyveri - børnehaven og lufthavnen

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?

Er dine data sikre

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

Stjålet laptop

Slettede eller ødelagte data

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

Superhelt

Hvad betyder det at være superhelt?

Beskytte andre - og sig selv

Have ekspertviden

Hacking er ikke magi

Hacking kræver blot lidt ninja-træning

God sikkerhed

Teknisk hvad er hacking

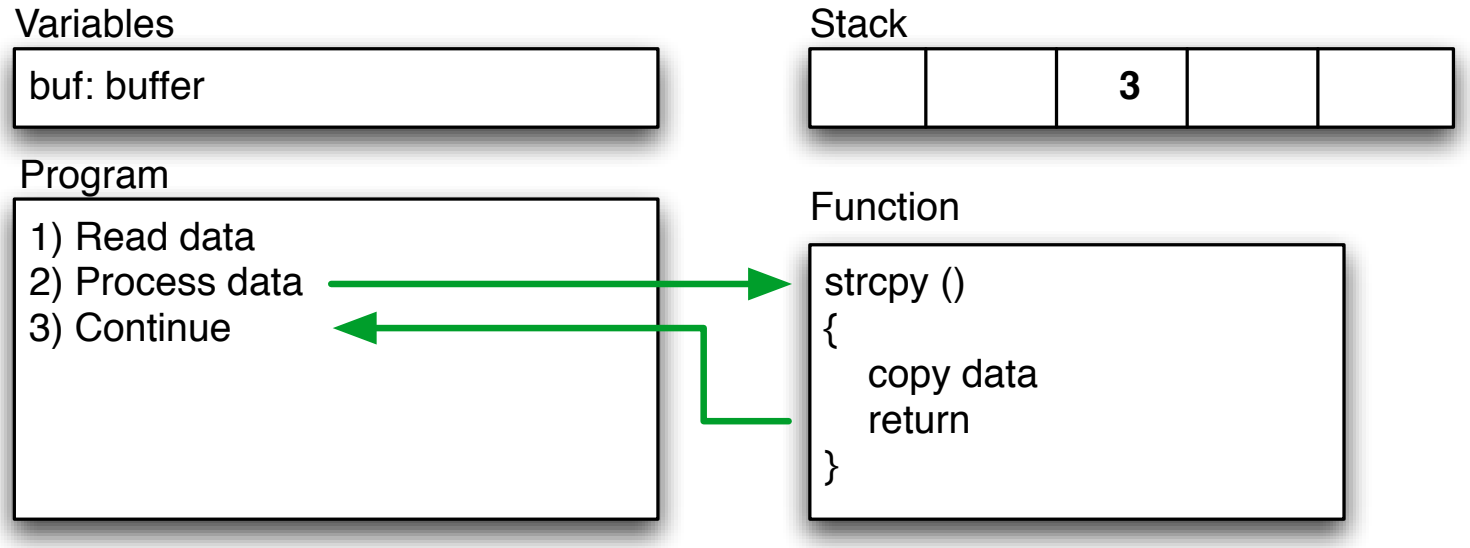
buffer overflows et C problem

SOLIDO NETWORKS

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.

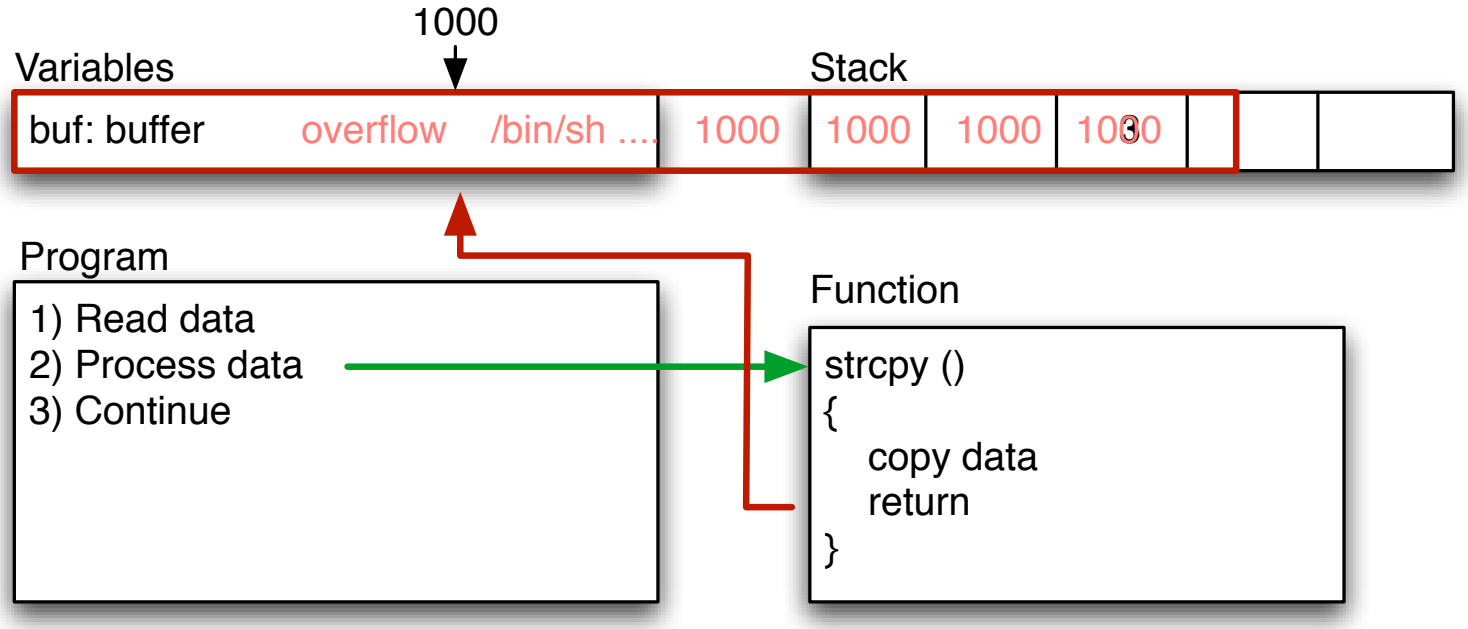
Stack protection er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.

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

Exploits

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

Demo exploit in Perl

Hvordan finder man buffer overflow, og andre fejl

SOLIDO NETWORKS

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

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

Metasploit

SOLIDO NETWORKS

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 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/`

Forudsætninger

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!

Eksempler på forudsætninger

Computeren skal være tændt

Funktionen der misbruges skal være slået til

Executable stack

Executable heap

Fejl i programmet

alle programmer har fejl

Gode operativsystemer

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

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

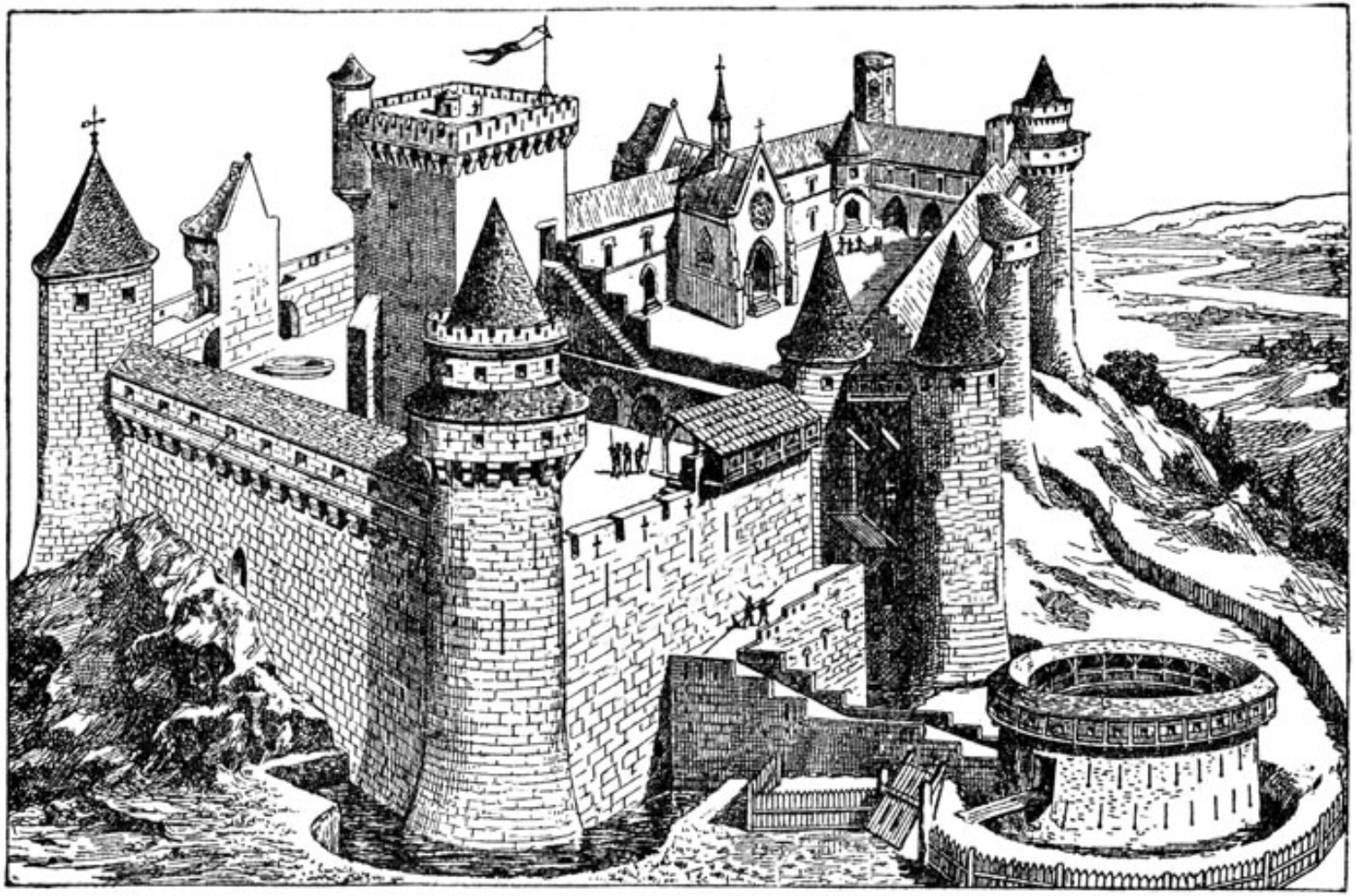
Vælg derfor hellere:

- 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

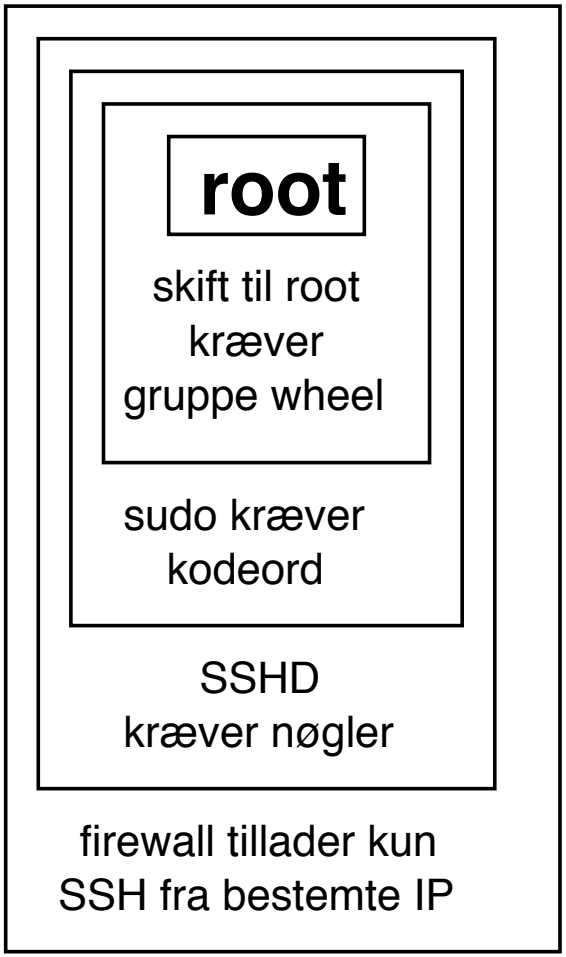
NB: meget få embedded systemer har beskyttelse!

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!

Chroot, Jails and

SOLIDO NETWORKS

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

OpenBSD systrace

SOLIDO NETWORKS

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)
```

Apache 6.0.18 catalina.policy (uddrag) - Java JVM

```
// ========== 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

Flashback

SOLIDO NETWORKS

Adobe Flash problems, player security issues & exploits - 2011

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

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

Flash security vulnerabilities affects Microsoft Excel - March 2011

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

USB flash security compromized by major design flaw - February 2011

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

Adobe flash security sandbox bypassed - January 2011

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

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

Client side: Flash, PDF, Facebook

SOLIDO NETWORKS

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`

Flash blockers

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?

Superheltegerninger

.

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

SOLIDO NETWORKS

Kom igang!

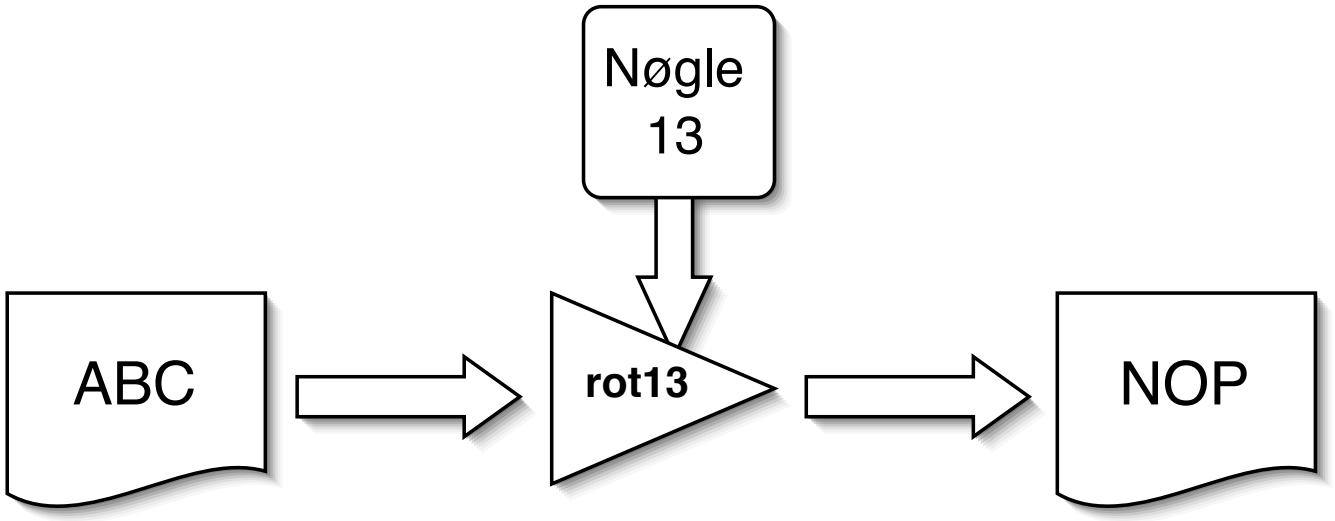
Formålet med kryptering

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet

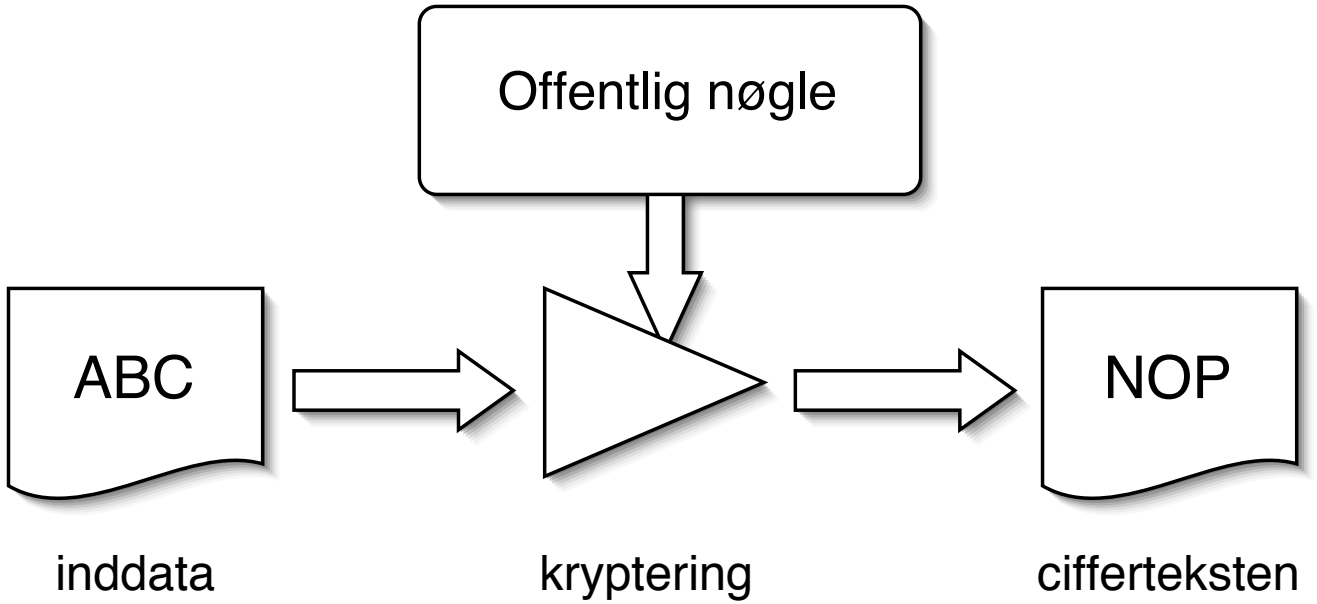
Kryptografi



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

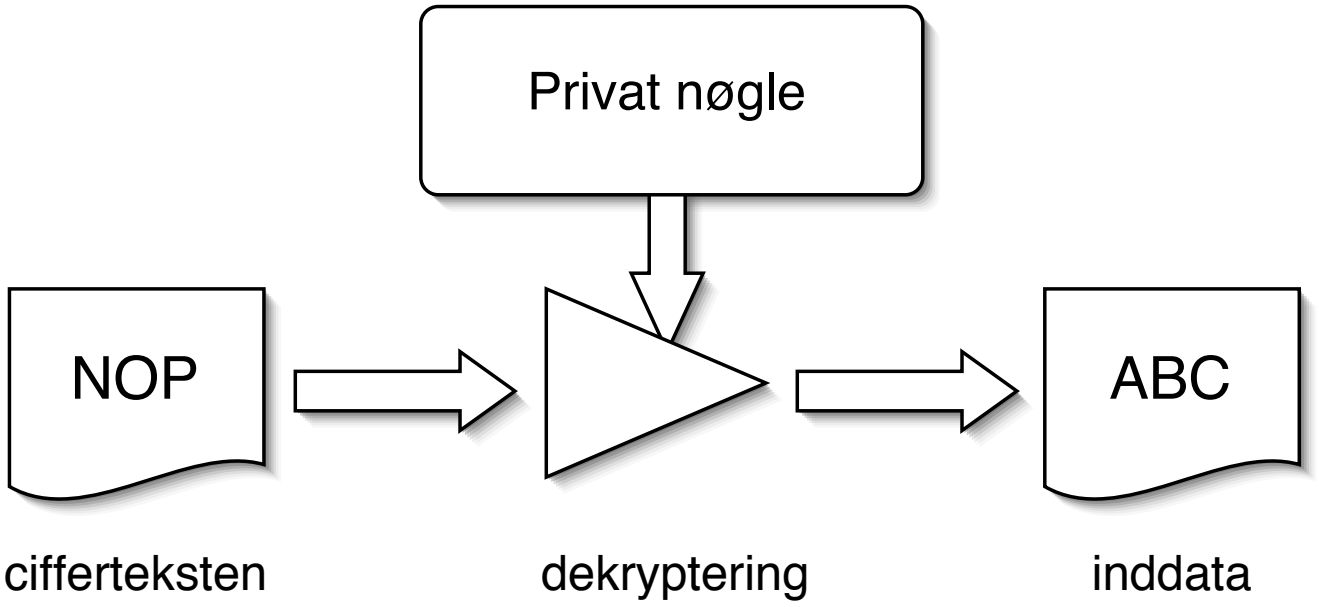
Public key kryptografi - 1



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

Public key kryptografi - 2



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

Kryptografiske principper

Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

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

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

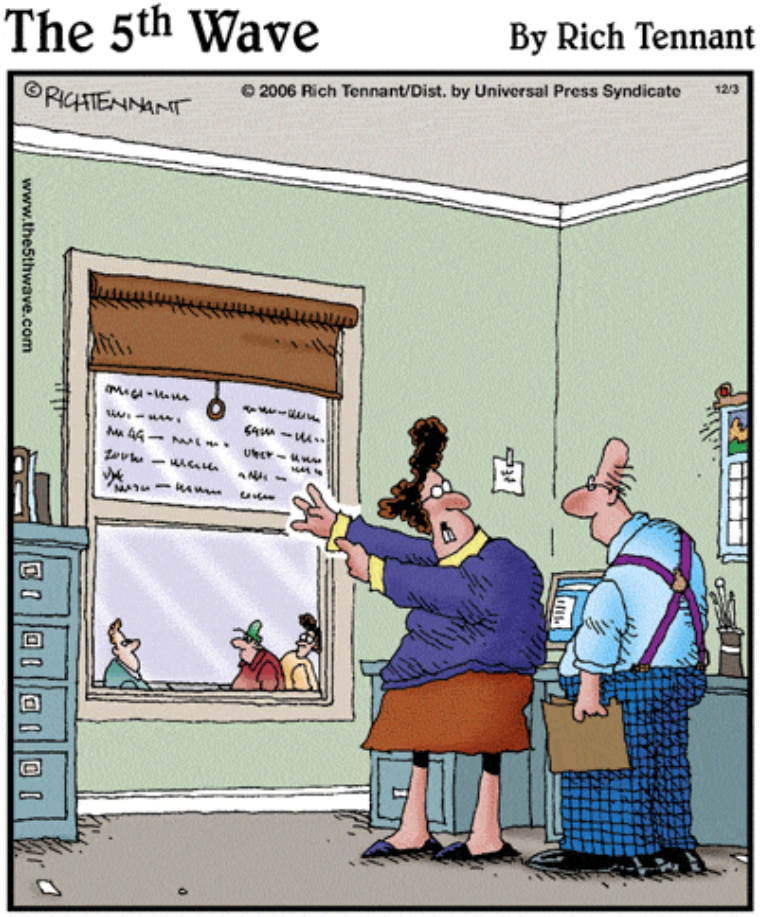
Se evt. Snake Oil Warning Signs: Encryption Software to Avoid `http://www.interhack.net/people/cmcurtin/snake-oil-faq.html`

harddisk beskyttelse og data kryptering

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

Opbevaring af passwords



"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."

Sikre protokoller som bruger krypto

Kryptering af e-mail

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

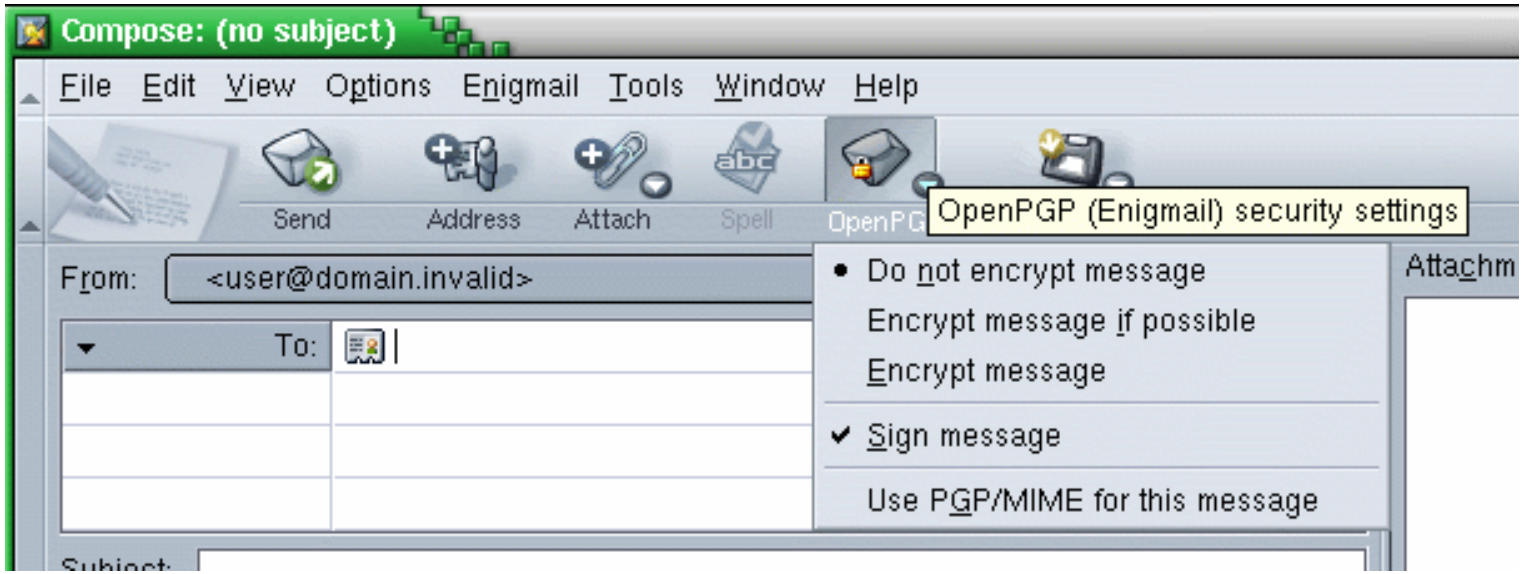
Kryptering af sessioner SSL/TLS

- 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

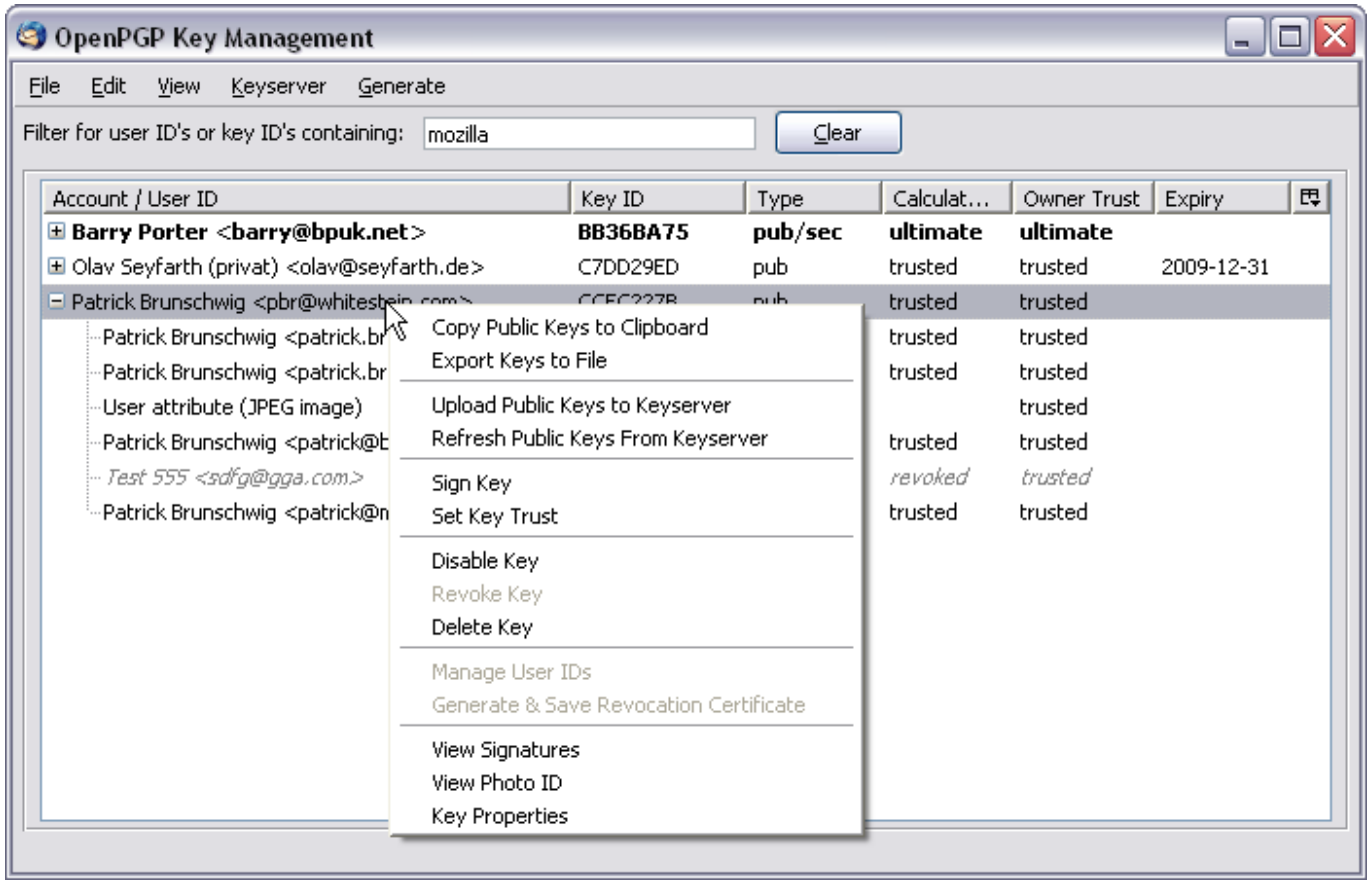
- IPsec IP Security Framework, se også L2TP
- PPTP Point to Point Tunneling Protocol - dårlig og usikker, brug den ikke mere!
- OpenVPN m.fl.

Enigmail - GPG plugin til Mail



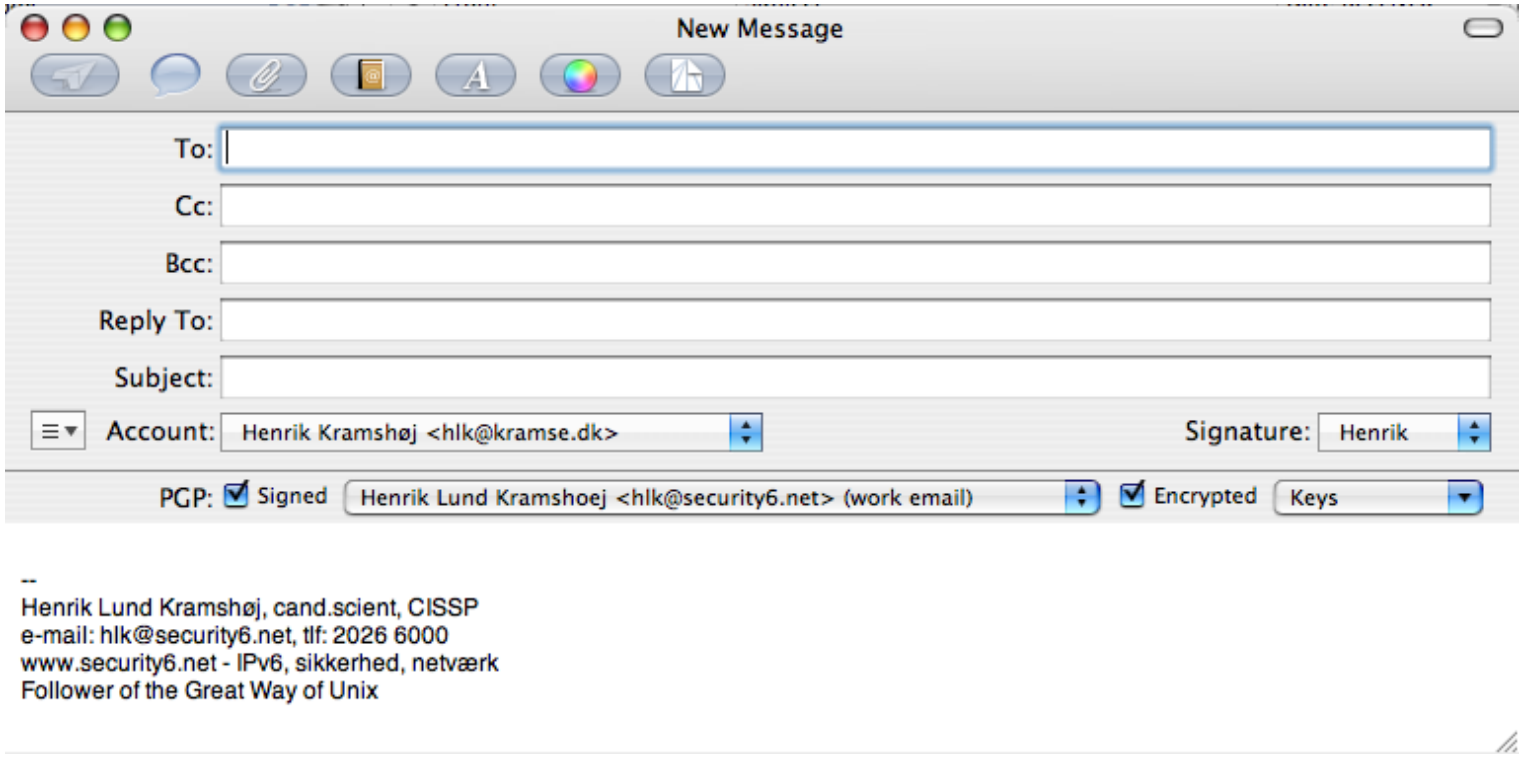
- Enigmail er en udvidelse til
- mailklienten i Mozilla/Netscape
- standalone mailklienten Thunderbird
- Billede fra `http://enigmail.mozdev.org`

Enigmail - OpenGPG Key Manager



Key Manager funktionaliteten i Enigmail kan anbefales

GPGMail plugin til Mac OS X Mail.app



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

VPN

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

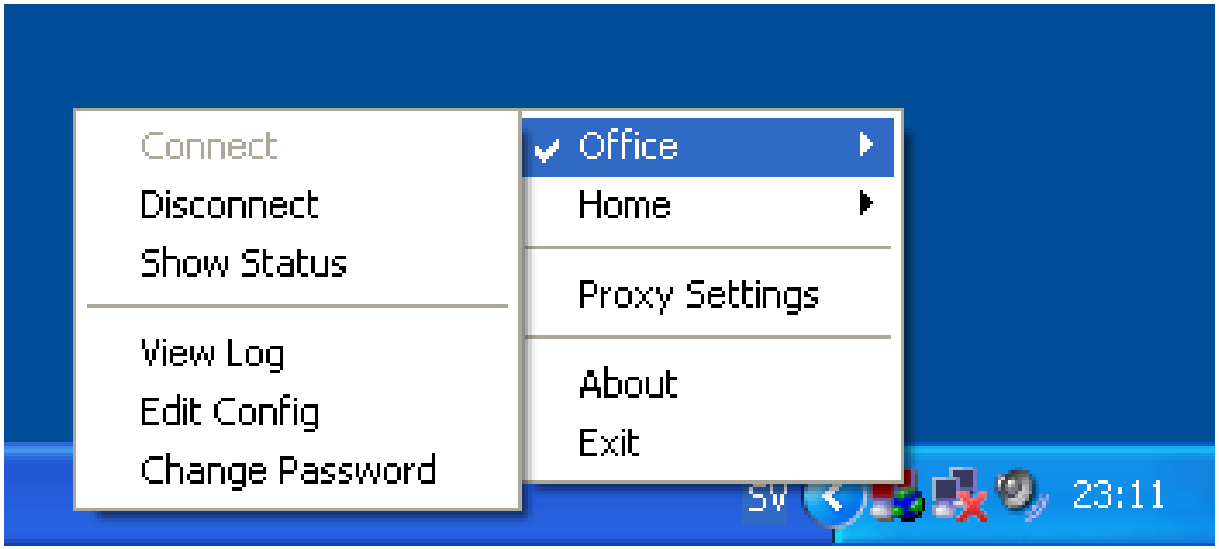
SSL/TLS VPN - Generelt koncept. Adskillige leverandører: Cisco, Juniper, F5 Big IP

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 client



OpenVPN GUI - easy to use

Internet sniffing by government

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

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.

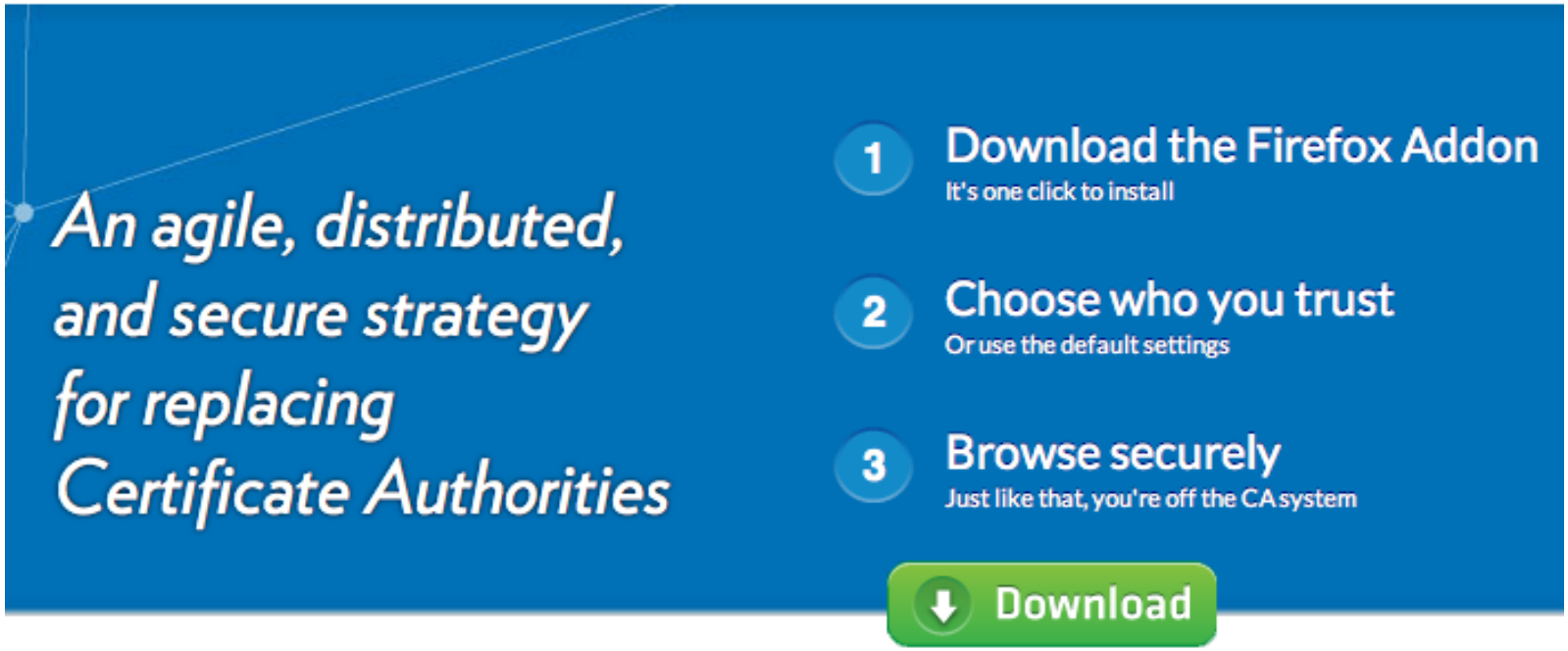
`http://www.eff.org/https-everywhere`

CertPatrol - which site uses which certificate

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/`

Convergence - who do you trust



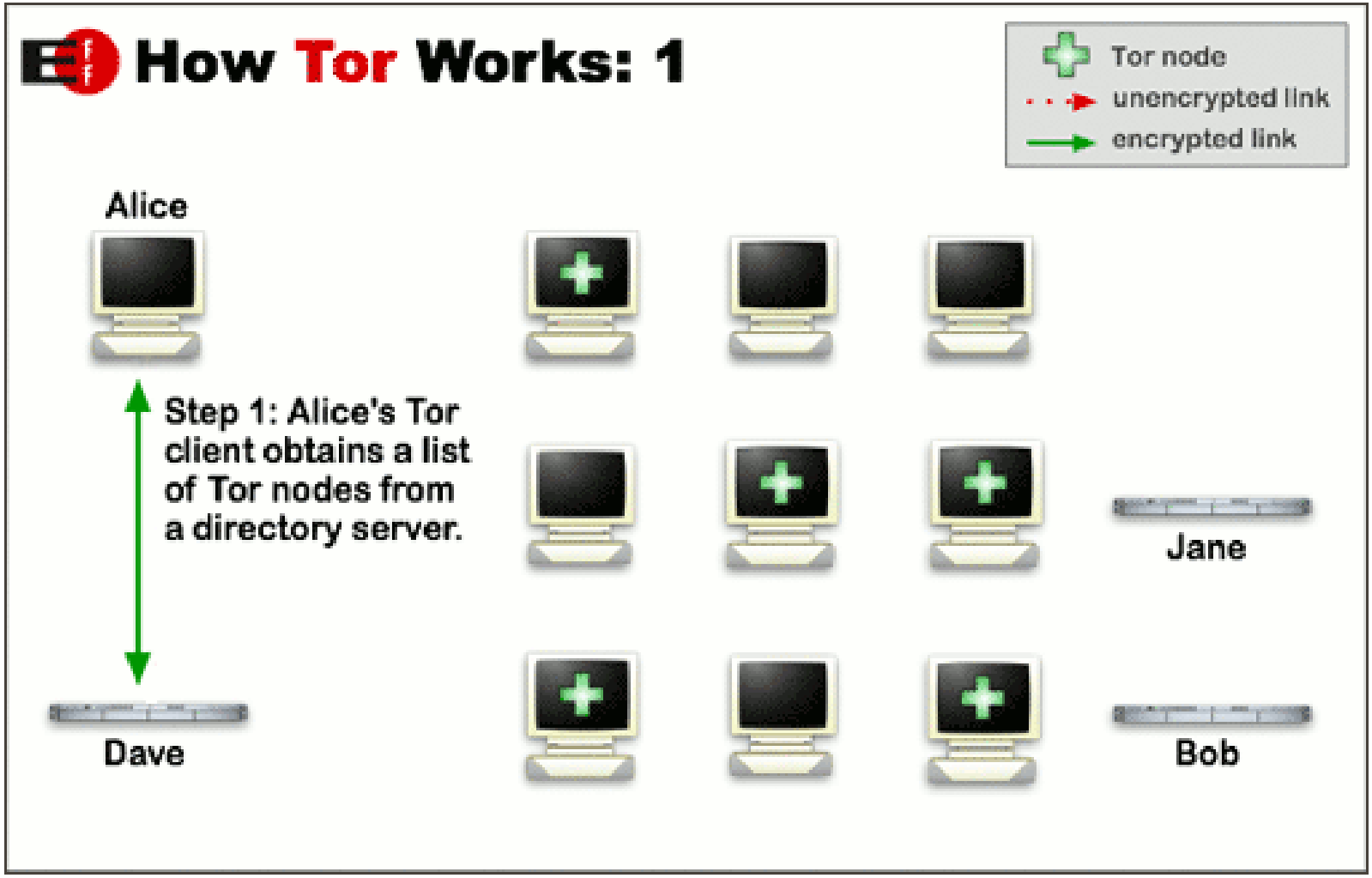
http://convergence.io/

Warning: radical change to how certificates work

Tor project

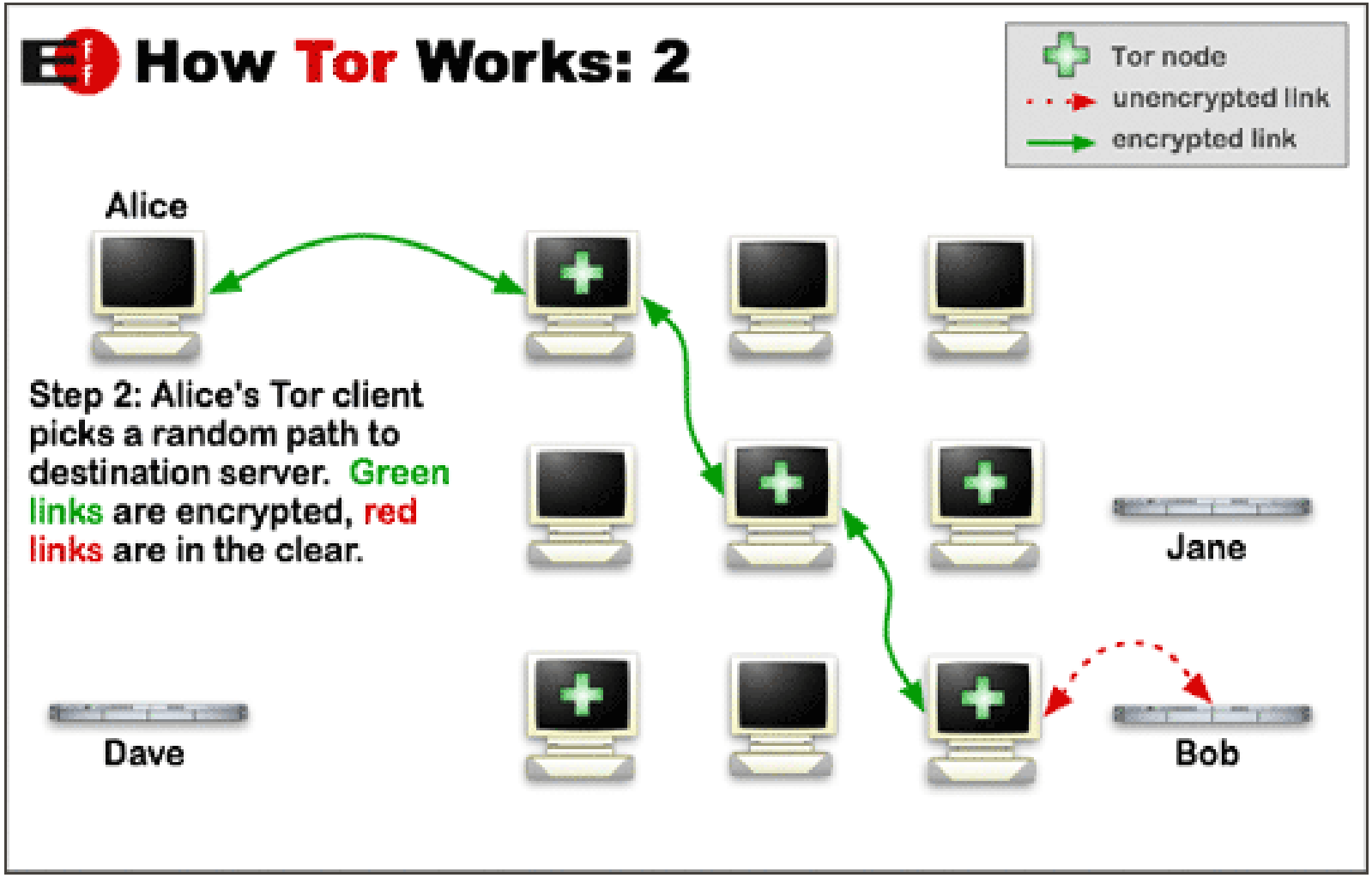
https://www.torproject.org/

Tor project - how it works 1



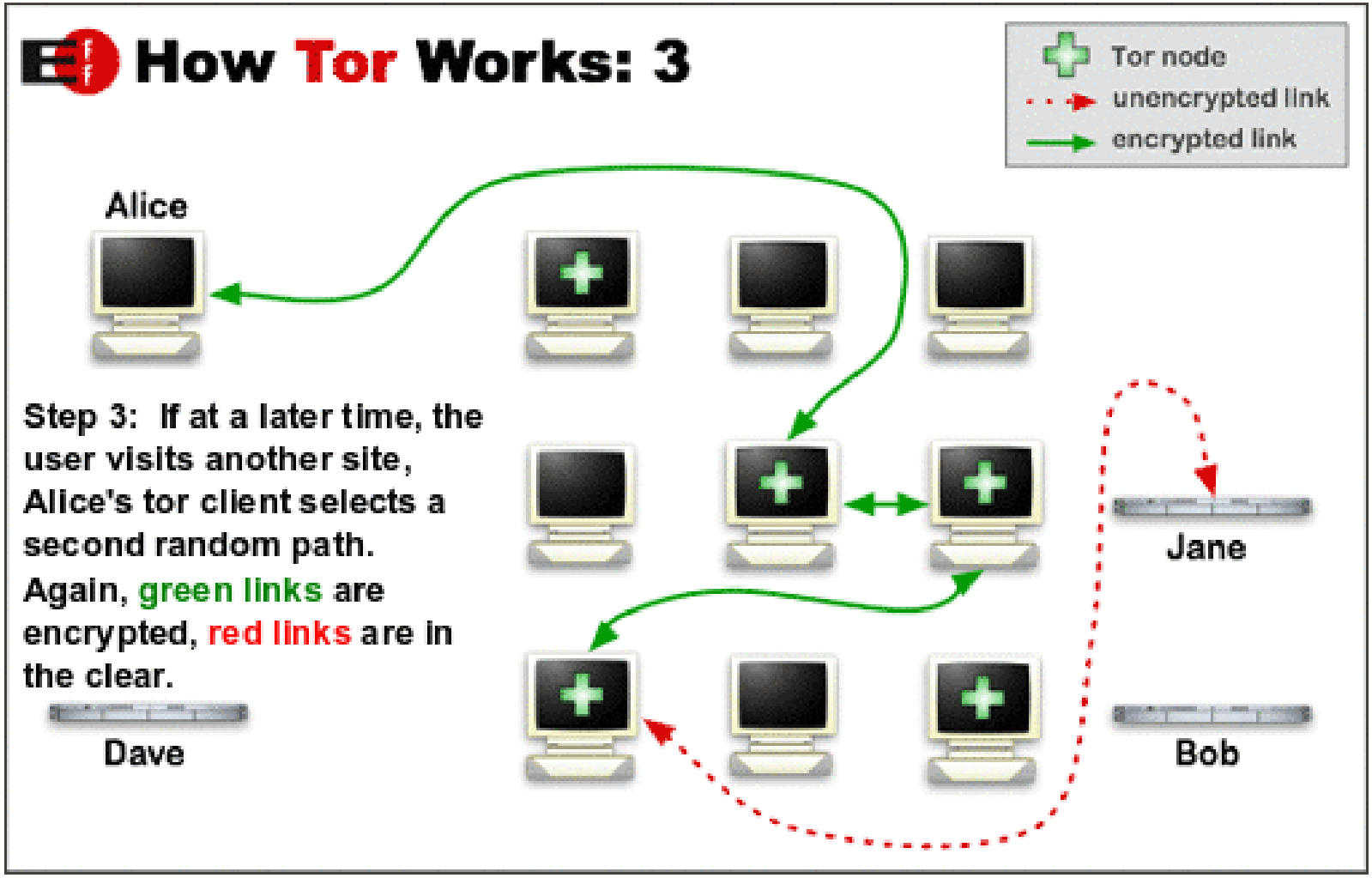
pictures from `https://www.torproject.org/about/overview.html.en`

Tor project - how it works 2



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

Tor project - how it works 3



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

Bonus: brug Bitcoins?

Er du passende paranoid?

Vær på vagt

Hvordan bliver du sikker

Lad være med at bruge computere :-)

Lad være med at bruge een 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

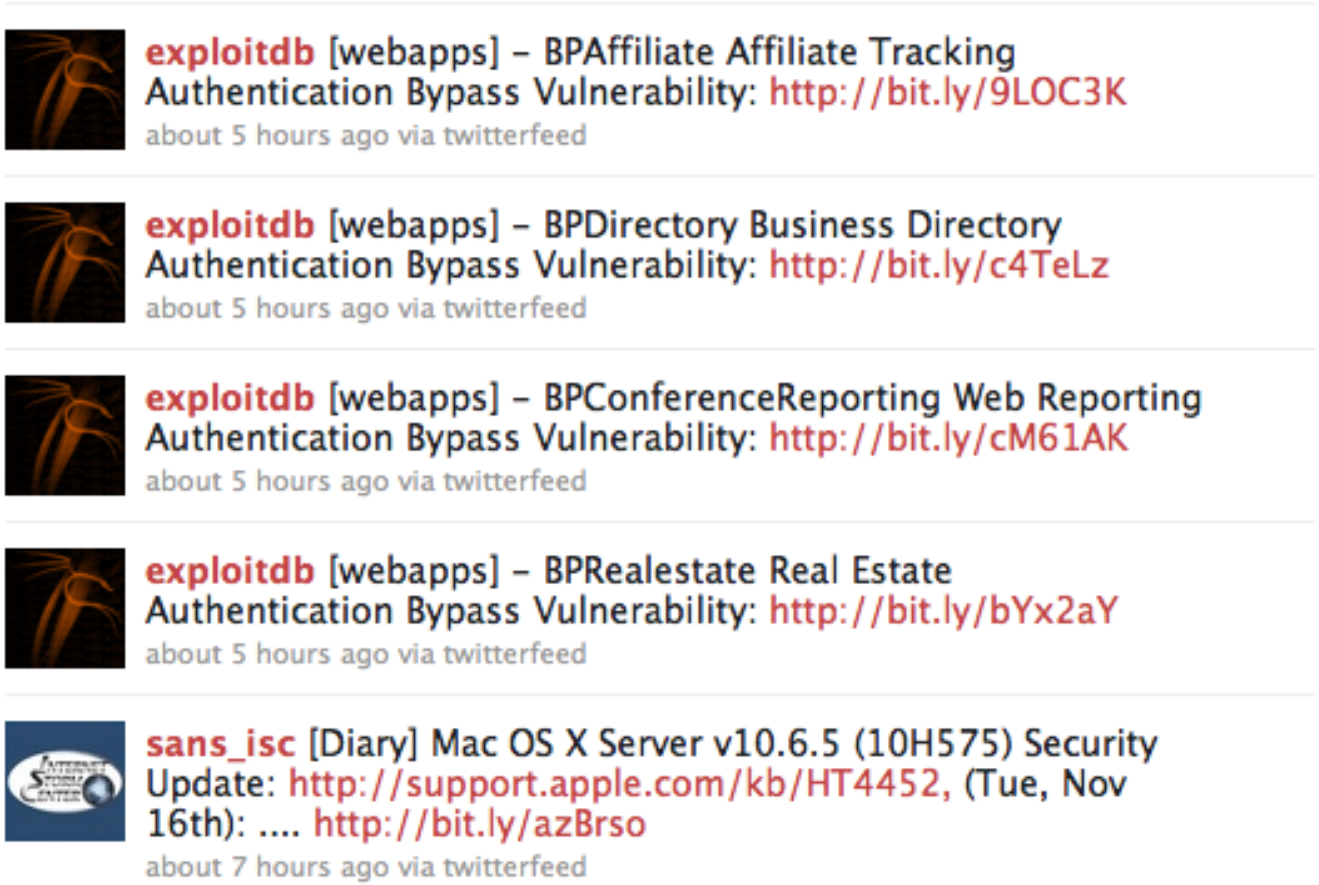
- `http://csrc.nist.gov/publications/PubsSPs.html`
- `http://www.nsa.gov/research/publications/index.shtml`
- `http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml`

Følg med Twitter news

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

Følg med Twitter news

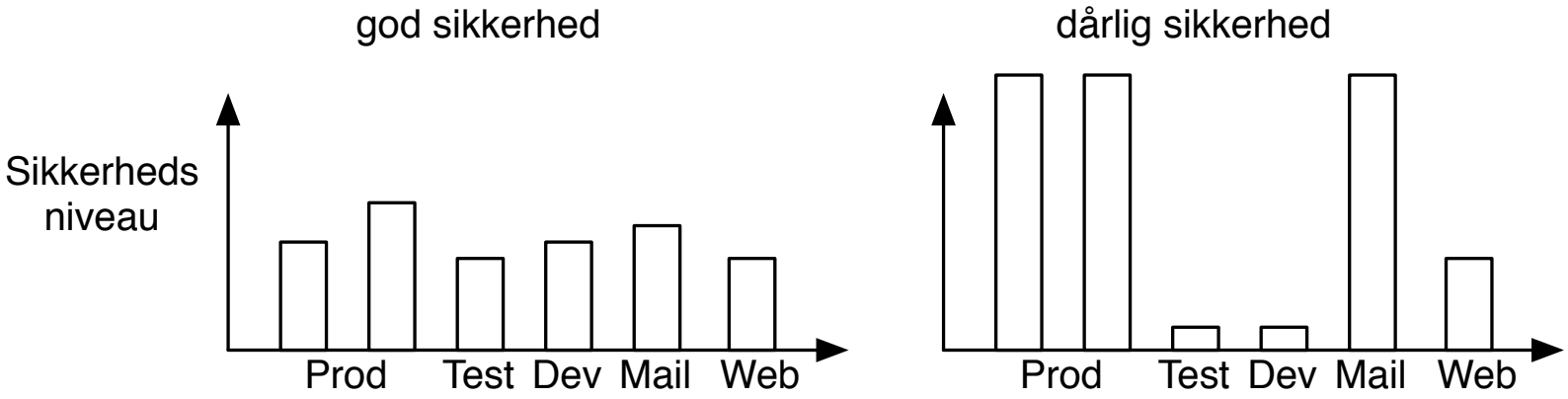


Exploits og nye sårbarheder

Checklisten

- 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.

Afbalanceret sikkerhed



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 sværeste vej ind

For lidt samarbejde

Team up!

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

PROSA CTF

SOLIDO NETWORKS

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

Fri adgang til hackerværktøjer

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

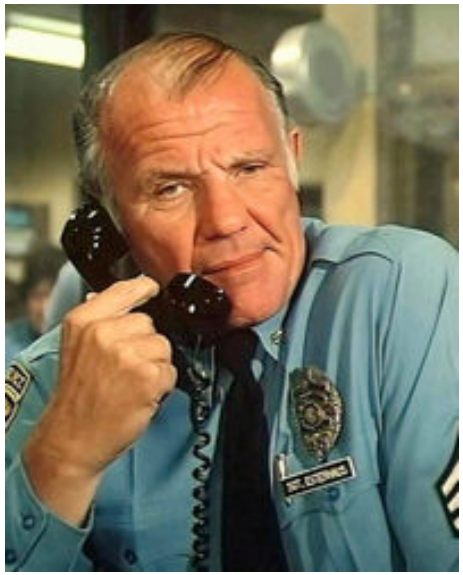
I 1995 udgav de softwarepakken SATAN
Security Administrator Tool for Analyzing Networks

> 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`

Be careful



Hey, Lets be careful out there!

Kilde: Michael Conrad `http://www.hillstreetblues.tv/`

Spørgsmål?

SOLIDO NETWORKS

Henrik Lund Kramshøj
hlk@solido.net

http://www.solidonetworks.com

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

VikingScan.org - free portscanning