Velkommen til

Beskyt dine data, lær at kryptere

December 2005

Henrik Lund Kramshøj
hlk@security6.net

http://www.security6.net

Indbyrdes præsentation

Kort introduktion af deltagerne - 3 min.

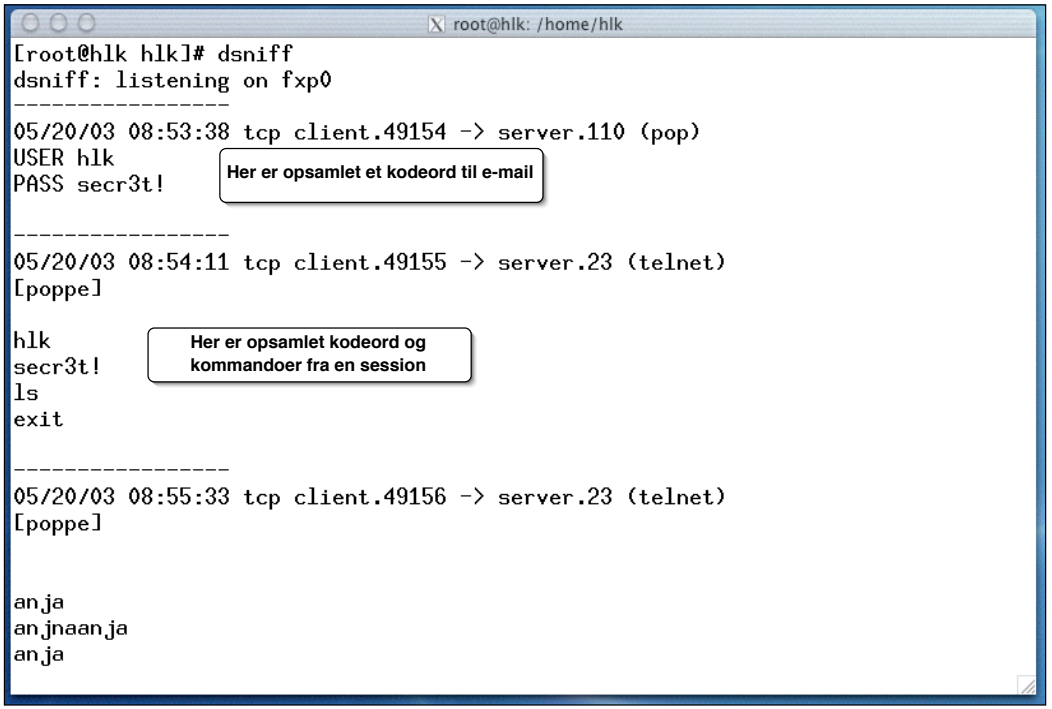
- Navn
- Forventninger til idag
- Hvad jeg skal bruge det her til
- Hvad kender I til kryptering?
- ...

Formål

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 lab nisi ut aliquip ex ea commodo consequa' Duis aute irure dolo nderit in voluptate velit esse cillum. Tia non ob ea soluad inco quae egen ium im end. Officia deserunt mollit a orum Et harumd dereud fac er expedit distinct. Gothica quam nunc putamus parum eposuerit litterarum formas humanitatis per seacula quarta; modo typ 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, sec t dolore magna aliquam is nostrud exercitatio lo conse e in voluptate velit esse cillum dolore eu fugiat nulla pariatur. At vver e am dignissum qui blandit est praesent.

- At introducere kryptering
- At forklare de sikkerhedsmæssige aspekter af aflytning
- Kendskab til eksempler på kendte krypteringsprogrammer
- Praktisk brug af programmer til hemmeligholdelse af data
- At inspirere jer til at bruge kryptering til blandt andet e-mail
- At udføre en keysigning - altså udveksle nøgler

Er kryptering interessant?



- Sikkerhedsproblemer i netværk er mange
- Trådløst udstyr er blevet meget billigt! - endnu flere kan sniffe traffik!
- Man vil gerne udveksle hemmeligheder som password m.v. over e-mail
- Terrorpakken giver anledning til stor bekymring!

Praktisk erfaring

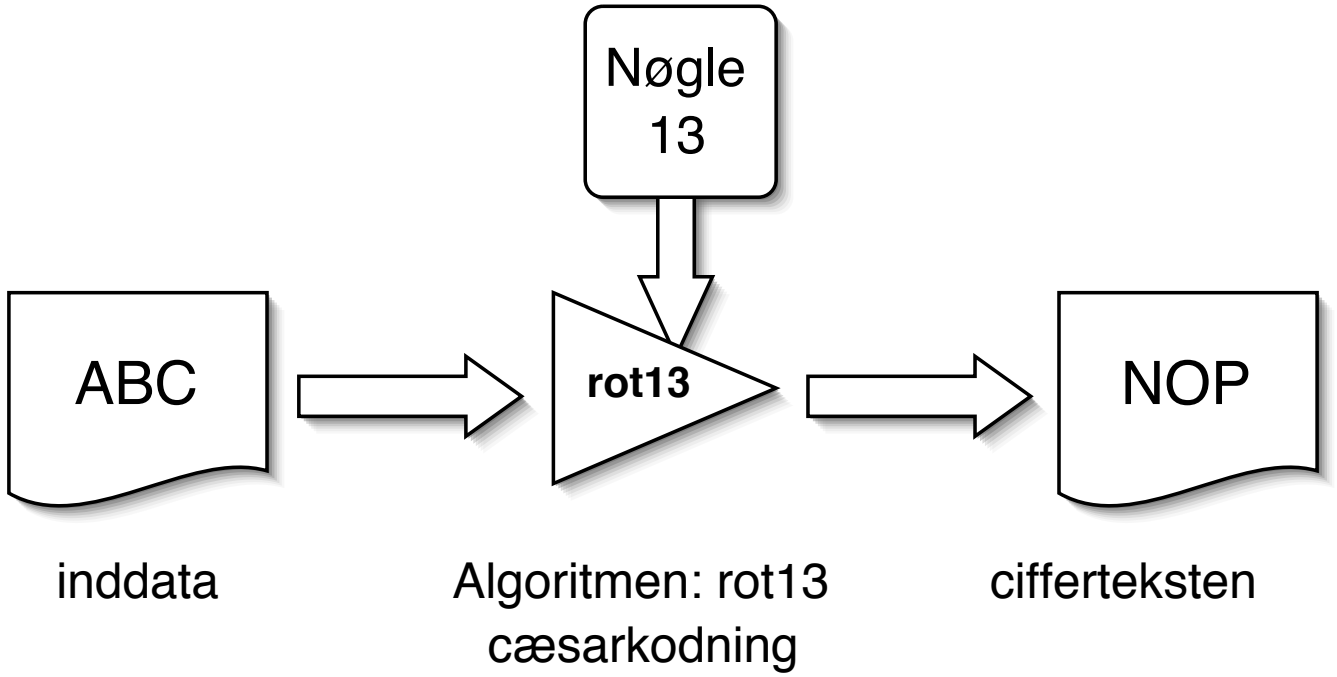
På kurset er der praktiske opgaver:

- nøglegenerering
- signering af nøgler
- installation af applikationer
- kryptering af filer
- kryptering af e-mail med GPG

Emneområder

- Introduktion - begreber og teknologierne
- PGP historik Phil Zimmermann
- Basale værktøjer PGP og GPG
- Grafiske brugergrænseflader
- Keysigning - hvordan
- Keysigning - præsentation og identifikation

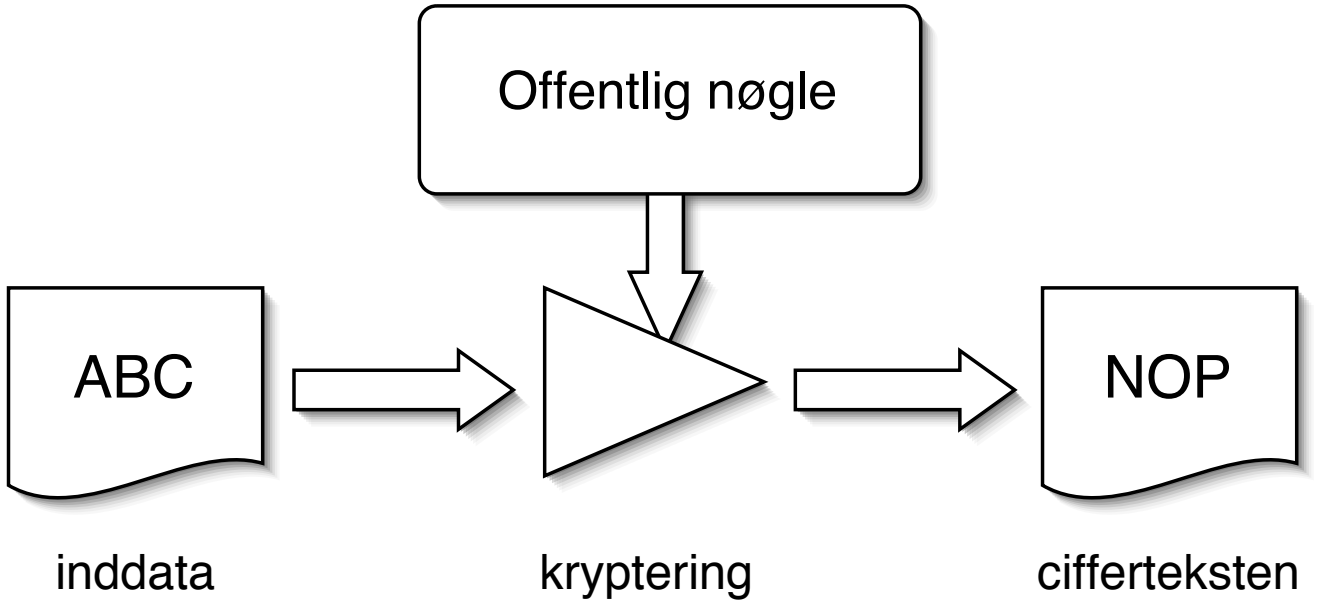
Kryptografi



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

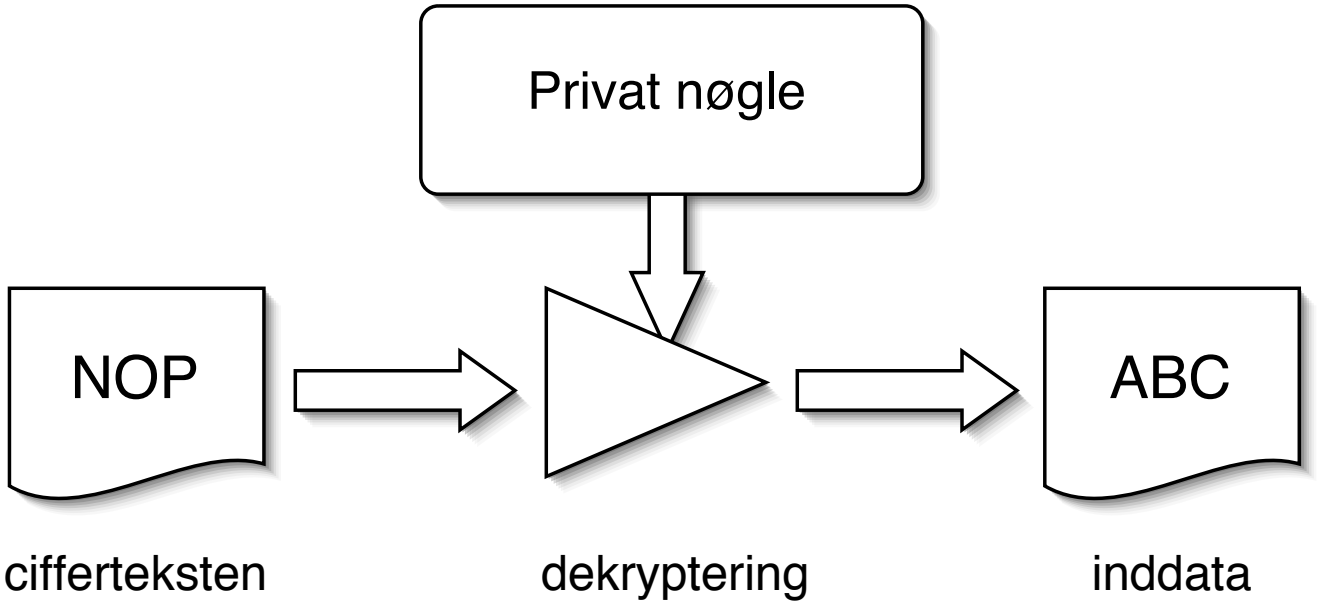
Public key kryptografi - 1



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`

DES, Triple DES og AES

Security .net

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/

Formålet med kryptering

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet

Kryptering i praksis

Kryptering af e-mail

- Pretty Good Privacy - Phil Zimmermann
- GNU Privacy Guard - Open Source implementation af OpenPGP
- OpenPGP = mail sikkerhed, OpenPGP RFC-2440, PGP/MIME RFC 3156)

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 netværkstraffik - Virtual Private Networks VPN

- IPsec IP Security Framework, se også L2TP
- PPTP Point to Point Tunneling Protocol
- OpenVPN m.fl.

harddisk beskyttelse og data kryptering

Vi kan altså begynde at beskytte os ved hjælp af kryptering

Konceptet kendes fra alle de gængse klient operativsystemer

- Microsoft Windows 2000 EFS Encrypting Filesystem - kryptering af filer
- Apple Mac OS X - krypterer nemt hjemmekataloget for en bruger med FileVault
- 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

Safeguard Easy

Hvad man vælger afhænger af operativsystemet og pengepungen

Tvind brugte Safeguard Easy fra det tyske firma Utimaco

Politiet *knækkede* harddiskene ved brug af kodeord som de enten gættede eller fik - ikke selve krypteringen

http://www.utimaco.de/content_products/sg_easy.html

En god algoritme i et godt produkt med en god nøgle kan ikke brydes

Basale tools - PGP

- Pretty Good Privacy - PGP
- Oprindeligt udviklet af Phil Zimmermann
- nu kommercielt, men der findes en freeware version
- Vist nok eksporteret fra USA på papir og scannet igen - det var lovligt
- I dag kan en masse information om PGP findes gennem:
  `http://www.pgpi.org`

Basale tools - GPG

Gnu Privacy Guard, forkortes GnuPG eller GPG

brug linket: `http://www.gnupg.org/`

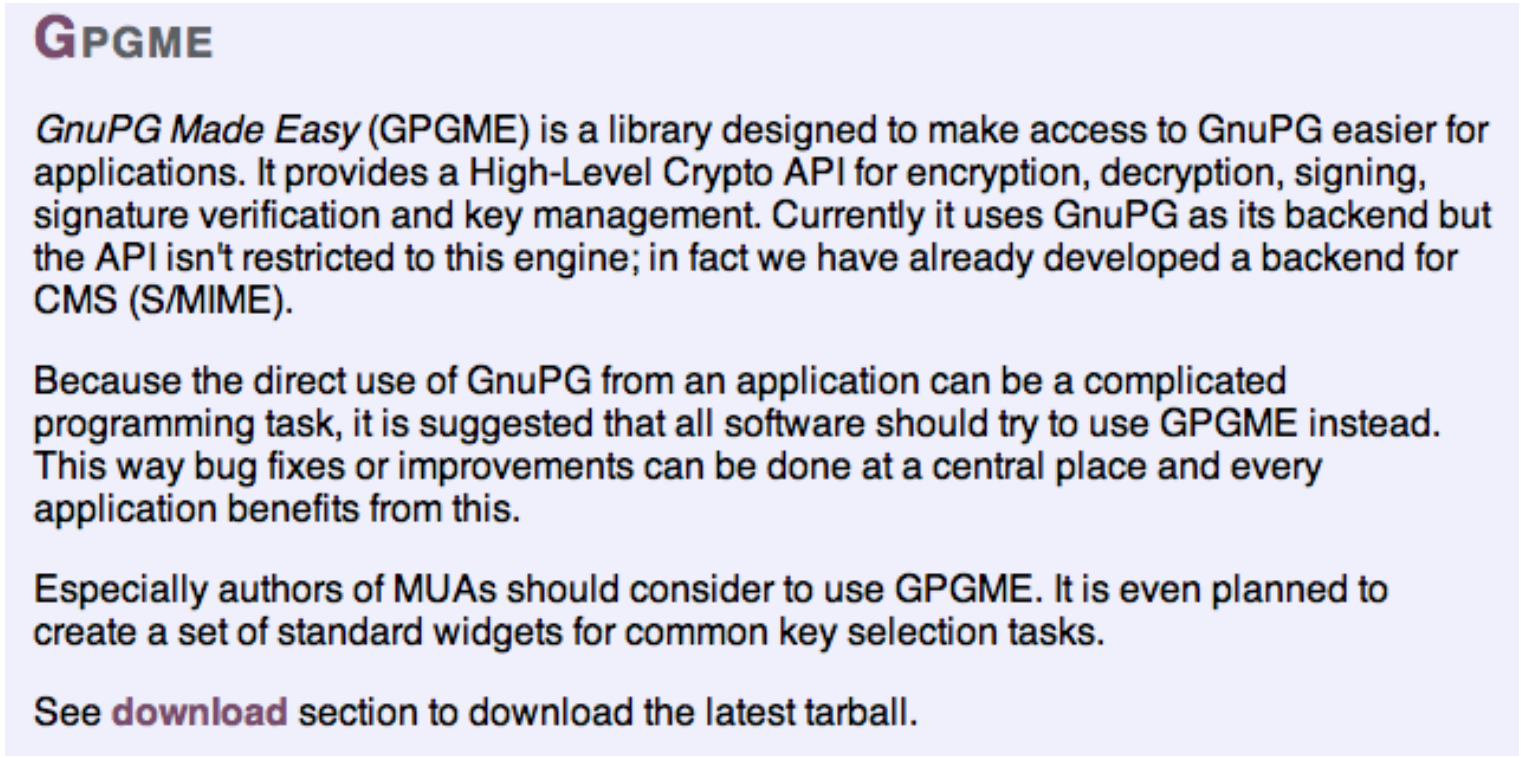
Open Source med GPL licens. Findes også til Windows

GnuPG

```
hlk@bigfoot:hlk$ gpg --version
gpg (GnuPG) 1.4.2
Copyright (C) 2005 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Home: ~/.gnupg
Supported algorithms:
Pubkey: RSA, RSA-E, RSA-S, ELG-E, DSA
Cipher: 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH
Hash: MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512
Compression: Uncompressed, ZIP, ZLIB, BZIP2
$
```

GPGME



GPGME

GnuPG Made Easy (GPGME) is a library designed to make access to GnuPG easier for applications. It provides a High-Level Crypto API for encryption, decryption, signing, signature verification and key management. Currently it uses GnuPG as its backend but the API isn't restricted to this engine; in fact we have already developed a backend for CMS (S/MIME).

Because the direct use of GnuPG from an application can be a complicated programming task, it is suggested that all software should try to use GPGME instead. This way bug fixes or improvements can be done at a central place and every application benefits from this.

Especially authors of MUAs should consider to use GPGME. It is even planned to create a set of standard widgets for common key selection tasks.

See **download** section to download the latest tarball.

Et bibliotek til nem adgang til GPG fra applikationsprogrammer

Kilde: `http://www.gnupg.org/(en)/related_software/gpgme/index.html`

GPG GUI frontends

GUI Frontends

GPA
Aims to be the standard GnuPG graphical frontend. GPA is hosted on this site.

GPGee
GPGee (GNU Privacy Guard Explorer Extension) is a shell extension that adds Windows explorer right-click menu support for GnuPGIs a MS-Windows program to integrate GnuPG into the Desktop.

KGpg
Is a KDE frontend for GnuPG.

Seahorse
Is a GNOME frontend for GnuPG.

TkPGP
Is another graphical tool to control GnuPG.

WinPT
Is a MS-Windows program to integrate GnuPG into the Desktop.

XAP
Is the X application panel and filemanager.

Kilde: `http://www.gnupg.org/(en)/related_software/frontends.html`

GnuPG - send en mail fra kommandolinien

```
#! /bin/sh
#
# encrypt a message and send to hlk and CEM

PROGRAM=`basename $0`

if [ $# -ne 1 ]; then
   echo " to encrypt a message I need a filename!"
   echo "Usage: $0 filename"
   echo "example $0 pentest-report"
   exit 0
fi

filename=$1
#hlk is D1EFBAA6
gpg -e -a -r D1EFBAA6 <$filename > $filename.pgp
$
```

.pgp filen kan nu vedhæftes en mail og sendes sikkert.

GnuPG - verifikation af downloads


```
$ cd /userdata/download/src/postfix/
$ ls -l *.sig
-rw-r--r--  1 hlk  admin  152 13 Sep  2003 postfix-2.0.16.tar.gz.sig
-rw-r--r--  1 hlk  admin  152  3 May 13:34 postfix-2.1.1.tar.gz.sig
$  gpg --verify postfix-2.1.1.tar.gz.sig
gpg: Signature made Mon May  3 19:34:08 2004 CEST using RSA key ID D5327CB9
gpg:  Good signature from "wietse venema <wietse@porcupine.org>"
gpg:                 aka "wietse venema <wietse@wzv.win.tue.nl>"
$
```

Generering af keys 1

Generering af key

```
$ gpg --gen-key
```

- Vælg ”DSA and Elgamal”
- Vælg passende keysize - 4096 skader næppe
- Vælg passende udløbsdato - ”no expire” vil virke for de fleste
- Brug din officielle mailaddresse i forbindelse med dit navn, så Email klienter kan finde din key aytomatisk
- Brug en god passphrase.
  En lang sætning som du kan huske, og som ikke kan gættes udfra kendskab til dig.
- Når nøglen genereres, så hjælp med at generere ”randomness” i systemet. Det får genereringen til at gå hurtigere, og det giver en bedre key.

Generering af keys 2

Du har nu en GnuPG key klar til at blive signeret

Er du **sikker** på at du kan huske din passphrase?

- Når nøglen er genereret bliver der printet et kort sammendrag af indholdet
  Dette kan også fås frem med:

```
$ gpg --fingerprint addr@domain.dk
pub   1024D/10019953 2005-05-07
      Key fingerprint = F643 81E1 0D8A 68A0 1024  C503 40B6 7A22 1001 9953
uid                  Test Bruger <addr@domain.dk>
sub   4096g/47A33D01 2005-05-07
```

Opsætning af defaults

Vi sætter defaults der sikrer:

- Ingen brok over ulåste sider (at låse sider kræver root, dvs. SUID)
- Valg af default keyserver
- Valg af default key (hvis du har flere)
- Valg af karaktersæt

```
$ tail ~/.gnupg/gpg.conf
no-secmem-warning
keyserver hkp://pgp.mit.edu/
default-key 47A33D01
charset ISO-8859-1
```

Det gør livet lidt lettere

Upload af keys

For at andre kan signere din key skal de have en kopi af din publickey.

Dette kan enten gøres ved at du eksporterer den til en fil og sender filen via Email, diskette, scp, USBkey, etc.:

```
gpg -a --export addr@domain.dk
```

Eller det kan gøres ved at den uploades til keyserverne, hvorfra alle kan hente den:

```
gpg --send-keys 47A33D01
```

Download af keys

Download kan enten foretages via en webside med søgemuligheder
http://pgp.mit.edu/
Herfra kan en publickey gemmes i en fil, og importeres med:
gpg –import FILE

Download kan også foretages direkte hvis keyid kendes:

```
gpg --recv-keys DCC399C7
```

Signering af keys

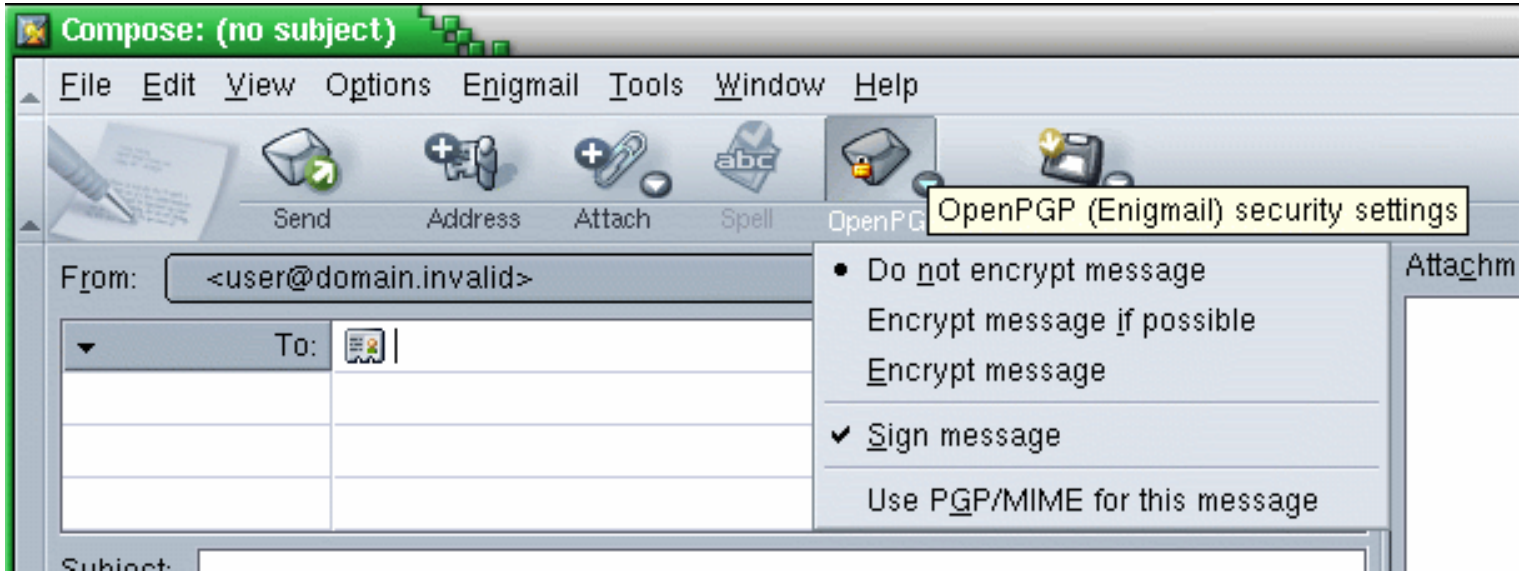
Keys signeres med:

```
gpg --sign-key addr@domain.dk  # Eller keyid
```

Husk at sikre at det nu også er den korrekte key i signerer
Kontroller med:

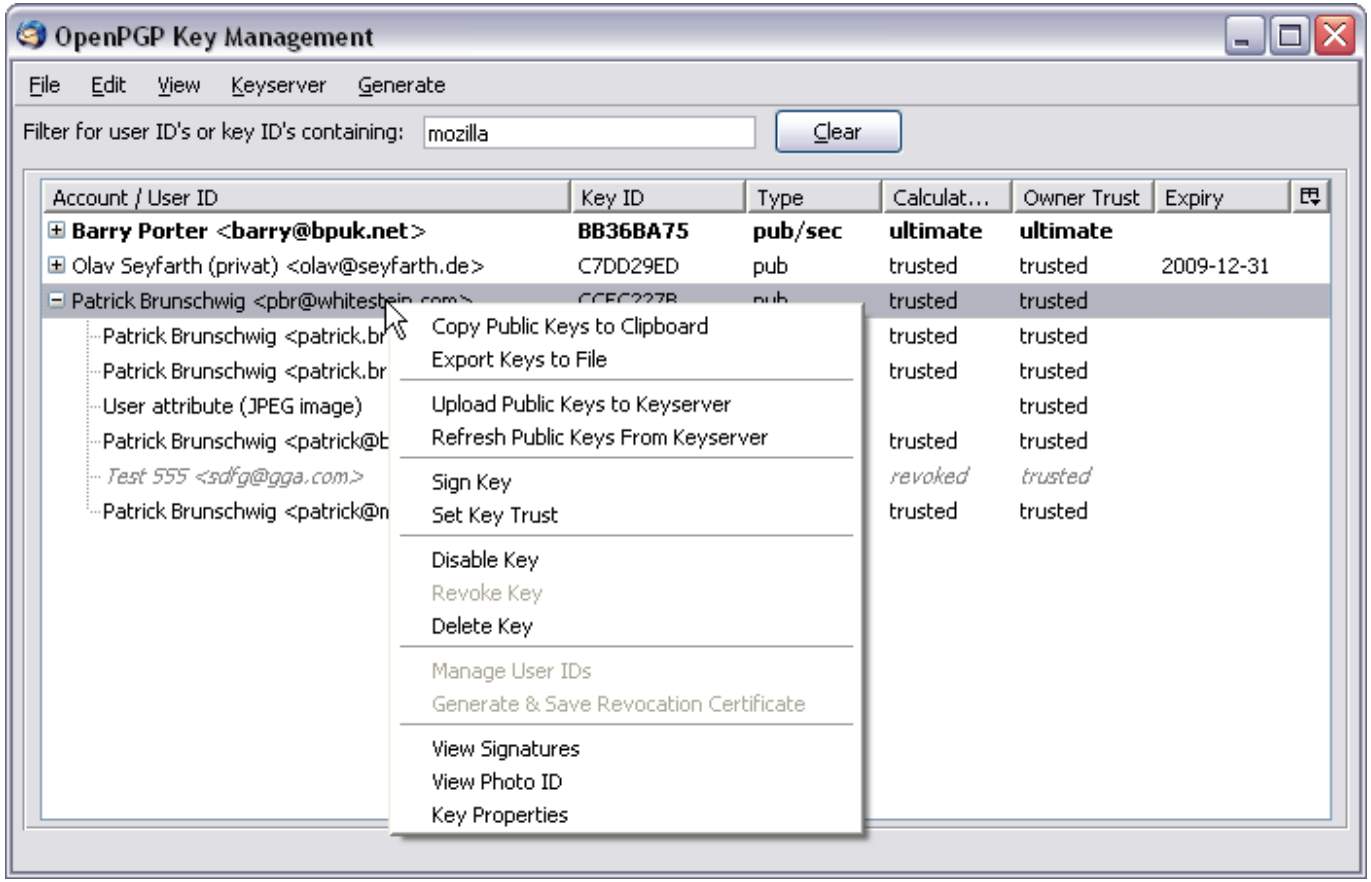
```
gpg --fingerprint addr@domain.dk
```

Enigmail - GPG plugin til Mail



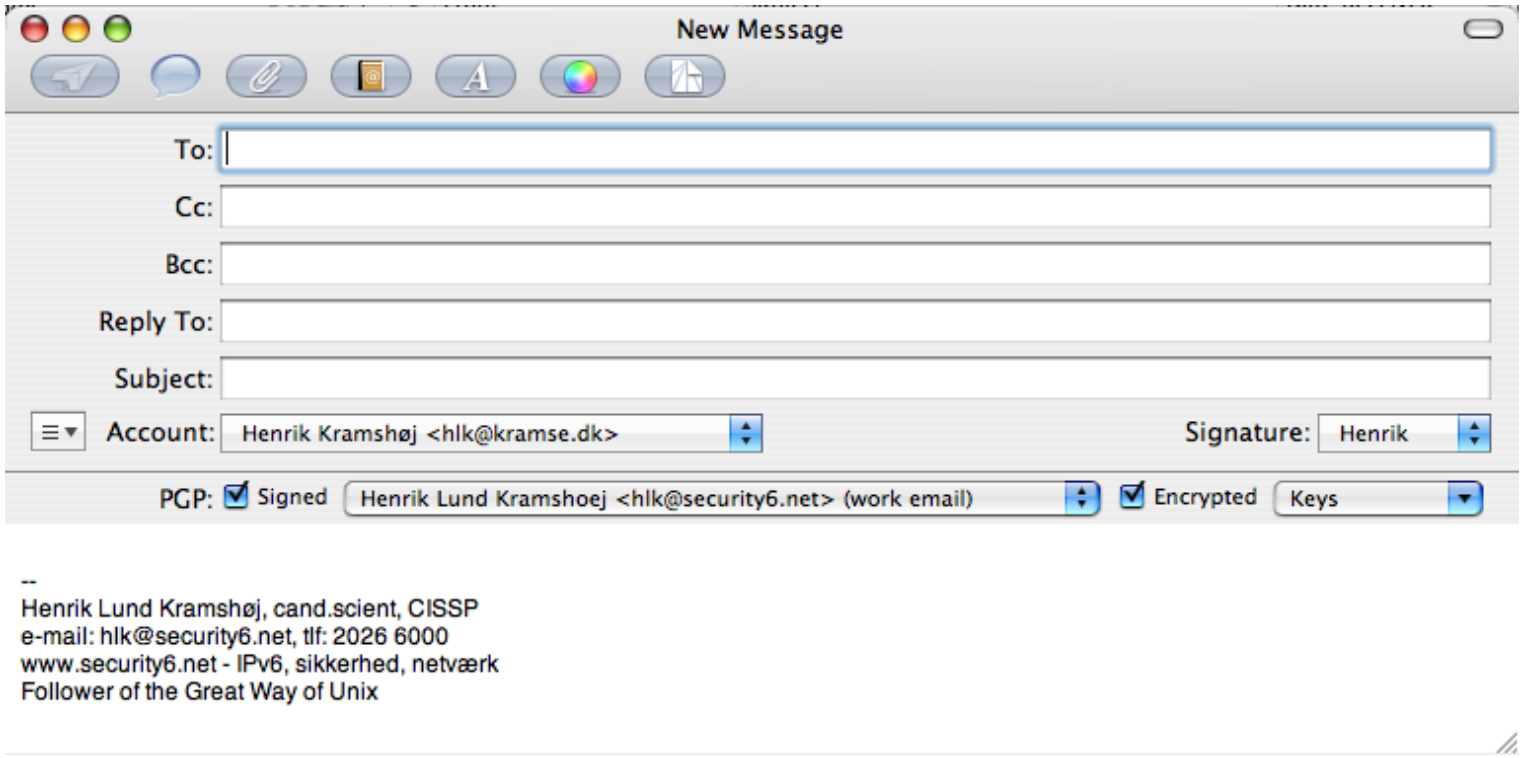
- Enigmail er en udvidelse til
- mailklienten i Mozilla/Netscape
- standalone mailklienten Thunderbird
- Billede fra `http://enigmail.mozdev.org`

Enigmail - OpenGPG Key Manager



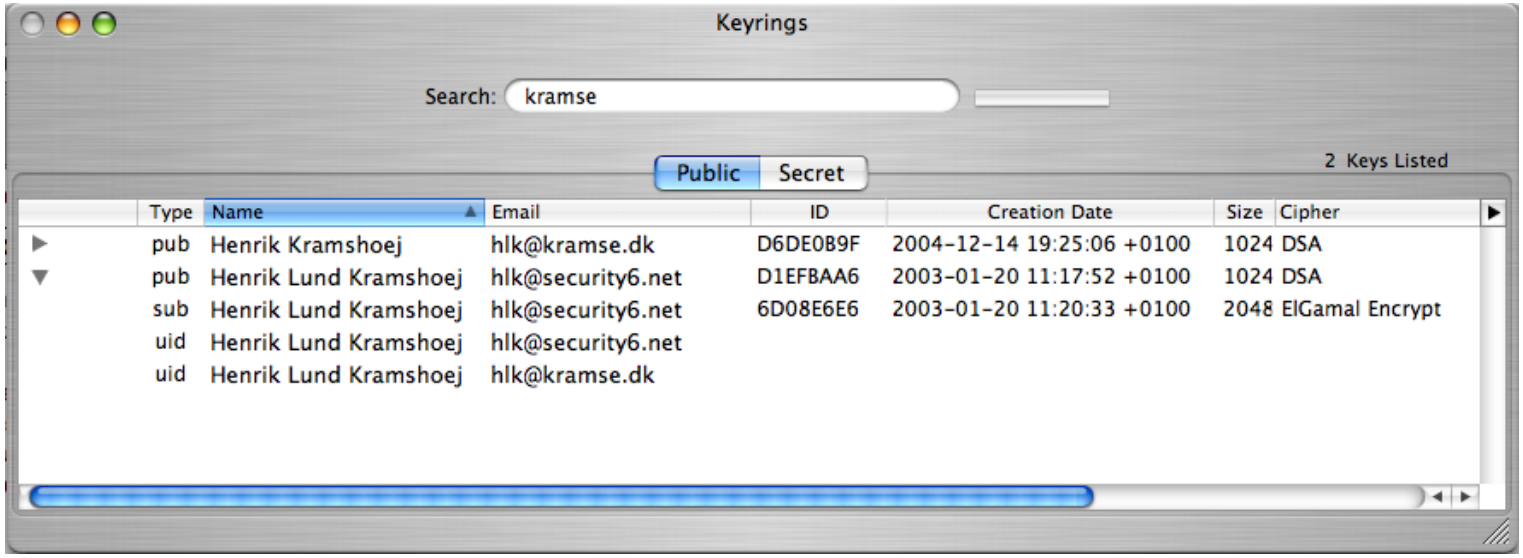
Key Manager funktionaliteten i Enigmail kan anbefales

GPGMail plugin til Mac OS X Mail.app



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

GPGKeys Key Manager for Mac OS X



- Bruger GPG
- Der er flere Mac GPG programmer tilgængeligt
- kilde: `http://macgpg.sourceforge.net`
- Der findes tilsvarende programmer til både KDE og GNOME

Definition

Computer Forensics involves the preservation, identification, extraction, documentation and interpretation of computer data.

Computer Forensics: Incident Response Essentials, Warren G. Kruse II og Jay G. Heiser, Addison-Wesley, 2002

TASK og Autopsy

Inspireret af TCT har Brian Carrier fra Atstake lavet flere værktøjer til forensics analyse

Det officielle hjem for TASK og autopsy er nu: `www.sleuthkit.org`

TASK kan betragtes som en erstatning for TCT the coroners toolkit lavet af Dan Farmer og Wietse Venema

Autopsy er en Forensic Browser - et interface til TASK

Hvordan slettes data

- Filsystemer skal være hurtige - skal ikke lave unødvendige operationer
- En harddisk er en fysisk disk med en arm der skal bevæges og et læse/skrivehoved som skal tændes og slukkes
- Hvis man kan undgå at skulle skrive over hele filen ved sletning er det hurtigere
- De fleste operativsystemer sletter derfor kun metadata og overskriver derfor ikke alle datablokke for filer
- Eksempel DOS FAT
  Når man slettede en fil på MS-DOS fjernede man reelt kun det første bogstav i filnavnet undelete bestod i at skrive det første bogstav i filnavnet - og håbe på at alle datablokke der hørte til filen stadig var at finde på disken

Guttman paper - analyse af diske

Secure Deletion of Data from Magnetic and Solid-State Memory Peter Gutmann, 1996

Det er et klassisk paper om sletning af data som man bør læse
http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

Der findes mange kommercielle værktøjer til sletning og en del Open Source - baseret på Guttman's dokument

Autoclave er efter min mening et af de bedste
http://staff.washington.edu/jdlarios/autoclave/

Autoclave - disk eraser

Sletning af diske kan foretages med eksempelvis autoclave

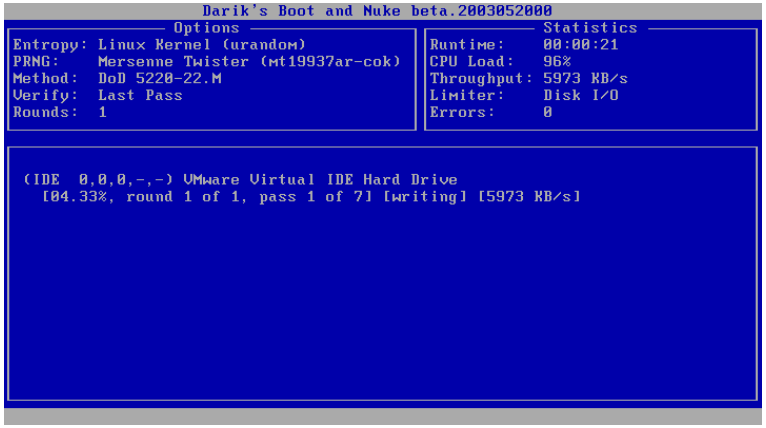
Den findes på følgende link:

`http://staff.washington.edu/jdlarios/autoclave/install.html`

Man kan nemt labe et CD image der kan skrives på en CD-R og bootes på nyere laptops - der sjældent har floppy drev

ad-hoc oprydning, formatering og sletning af filer giver ingen sikkerhed!

Darik's Boot and Nuke



- Autoclave forfatteren henviser selv til DBAN
- følgende 4 punkter beskriver DBAN på hjemmesiden:
- Free.
- Fast. Rapid deployment in emergency situations.
- Easy. Start the computer with DBAN and press the ENTER key.
- Safe. Irrecoverable data destruction. Prevents most forensic data recovery techniques.

http://dban.sourceforge.net/

Informationssikkerhed

Husk følgende:

Sikkerhed kommer fra langsigtede intiativer

Hvad er informationssikkerhed?

Data på elektronisk form

Data på fysisk form

Social engineering - *The Art of Deception: Controlling the Human Element of Security* af Kevin D. Mitnick, William L. Simon, Steve Wozniak

Informationssikkerhed er en proces

Free software - free som i gratis software

AVG antivirus- www.grisoft.com

ZoneAlarm http://www.zonelabs.com

Utimaco SafeGuard PrivateCrypto http://www.utimaco.com

Spybot-Search and Destroy
http://www.safer-networking.org

Password Safe http://passwordsafe.sourceforge.net

Mozilla Firefox http://www.mozilla.org

PGP Freeware - begrænset version
http://www.pgp.com/downloads/freeware/index.html

Spørgsmål?

Henrik Lund Kramshøj
hlk@security6.net

http://www.security6.net

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

Oversigt over anbefalinger

Følg med! - læs websites, bøger, artikler, mailinglister, ...

Vurder altid sikkerhed - skal integreres i processer

Hændelseshåndtering - du vil komme ud for sikkerhedshændelser

Lav en sikkerhedspolitik - herunder software og e-mail politik

CISSP fra ISC2

Approved marks of the International Information Systems Security Certification Consortium, Inc.

Primære website: `http://www.isc2.org`

Vigtigt link `http://www.cccure.org/`

Den kræver mindst 3 års erfaring indenfor et relevant fagområde

Multiple choice 6 timer 250 spørgsmål - kan tages i Danmark

GIAC GSEC krav

Security Essentials - basal sikkerhed

Krav om en *Practical assignment* - mindst 8 sider, 15 sider i gennemsnit

multiple choice eksamen

Primære website: `http://www.giac.org`

Reading room: `http://www.sans.org/rr/`

Der findes en god oversigt i filen *GIAC Certification: Objectives and Curriculum*
`http://www.giac.org/GIAC_Cert_Brief.pdf`

Referencer

Papers - der findes MANGE dokumenter på Internet

- CERT/CC `http://www.cert.org`
- AusCERT Computer Emergency Response Team for Australia `http://www.auscert.org.au/`
- `http://www.securityfocus.com`
- CERIAS hotlist `http://www.cerias.purdue.edu/tools_and_resources/hotlist/`

Honeypots og sårbare systemer

- `http://www.project.honeynet.org` - diverse honeynet projekter information om pakker og IP netværk

Husk også at mange forlag tillader at man henter et kapitel som PDF!

Referencer: bøger

- *Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, Ed Skoudis, Prentice Hall PTR, 1st edition July 2001
- *CISSP All-in-One Exam Guide*, Shon Harris, McGraw-Hill Osborne Media, 2nd edition, June 17 2003
- *Practical UNIX and Internet Security*, Simson Garfinkel, Gene Spafford, Alan Schwartz, 3rd Edition, O'Reilly February 2003
- *Network Security Assessment: Know Your Network*, Chris McNab, O'Reilly March 2004
- *Secure Coding: Principles & Practices*, Mark G. Graff, Kenneth R. van Wyk, O'Reilly June 2003
- *Firewalls and Internet Security*, William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, Addison-Wesley, 2nd edition, 2003
- *Building Firewalls with OpenBSD and PF*, Jacek Artymiak, 2nd edition 2003
- bøger om TCP/IP - Alle bøger af Richard W Steven kan anbefales!
- Reference books for the CISSP CBK domains - en liste der vedligeholdes af Rob Slade `http://victoria.tc.ca/int-grps/books/techrev/mnbksccd.htm`

Hackerværktøjer

- nmap - http://www.insecure.org portscanner
- Nessus - http://www.nessus.org automatiseret testværktøj
- l0phtcrack - http://www.atstake.com/research/lc/ - The Password Auditing and Recovery Application, kig også på Cain og Abel fra http://oxid.it hvis det skal være gratis
- Ethereal - http://www.ethereal.com avanceret netværkssniffer
- OpenBSD - http://www.openbsd.org operativsystem med fokus på sikkerhed
- http://www.isecom.org/ - Open Source Security Testing Methodology Manual - gennemgang af elementer der bør indgå i en struktureret test
- Putty - http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html terminal emulator med indbygget SSH
-  http://www.remote-exploit.org/?page=auditor - Auditor security collection - en boot CD med hackerværktøjer

Hvordan bruges hackerværktøjerne

Tænk som en hacker

Rekognoscering

- ping sweep
- portscan
- OS detection - TCP/IP eller banner grab
- Servicescan - rpcinfo, netbios, ...
- telnet/netcat interaktion med services

Udnyttelse/afprøvning: Nessus, whisker, exploit programs

Oprydning

- Lav en rapport
- Gennemgå rapporten, registrer ændringer
- Opdater programmer, konfigurationer, arkitektur, osv.

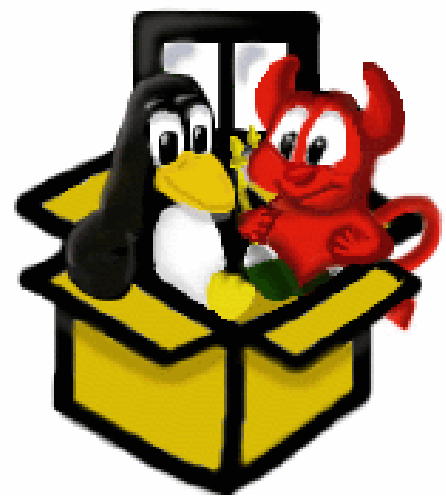
I skal jo også VISE andre at I gør noget ved sikkerheden.

Reklamer: kursusafholdelse

Security6.net afholder følgende kurser med mig som underviser

- IPv6 workshop - 1 dag
  Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk. Internetprotokollerne har eksisteret i omkring 20 år, og der er kommet en ny version kaldet version 6 af disse - IPv6.
- Wireless teknologier og sikkerhed workshop - 2 dage
  En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk og integration med eksempelvis hjemmepc og wirksomhedens netværk
- Hacker workshop 2 dage
  Workshop med detaljeret gennemgang af hackermetoderne angreb over netværk, exploitprogrammer, portscanning, Nessus 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.

Foreninger



BSD-DK - dansk forening for BSD'erne,
http://www.bsd-dk.dk

SSLUG, Skåne Sjælland Linux User Group
http://www.sslug.dk

DKUUG, Dansk UNIX User Group
http://www.dkuug.dk
medlemsskab giver god rabat på bøger gennem
http://www.polyteknisk.dk, typisk 15-20%

Soekris bestilling i Danmark

Et lille embedded system

- Soekris 4501-30 + case 1300,-
- Soekris 4801-50 + case 1750,-
- Strømforsyning 1.5A (lille) 130,-
- Strømforsyning 3A (stor) 170,-
- vpn1411 miniPCI 550,-
- 4801 Harddisk mount kit 2.5” 70,-
- Alle priser er cirkapriser og ekskl. moms. kontakt Catpipe for nøjagtige oplysninger! `http://www.catpipe.net`
- Andre leverandører `http://www.kd85.com` og `http://www.cortexsystems.dk`