Welcome to

Overvågning og hacking

PROSA Stud Svendborg 2014

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

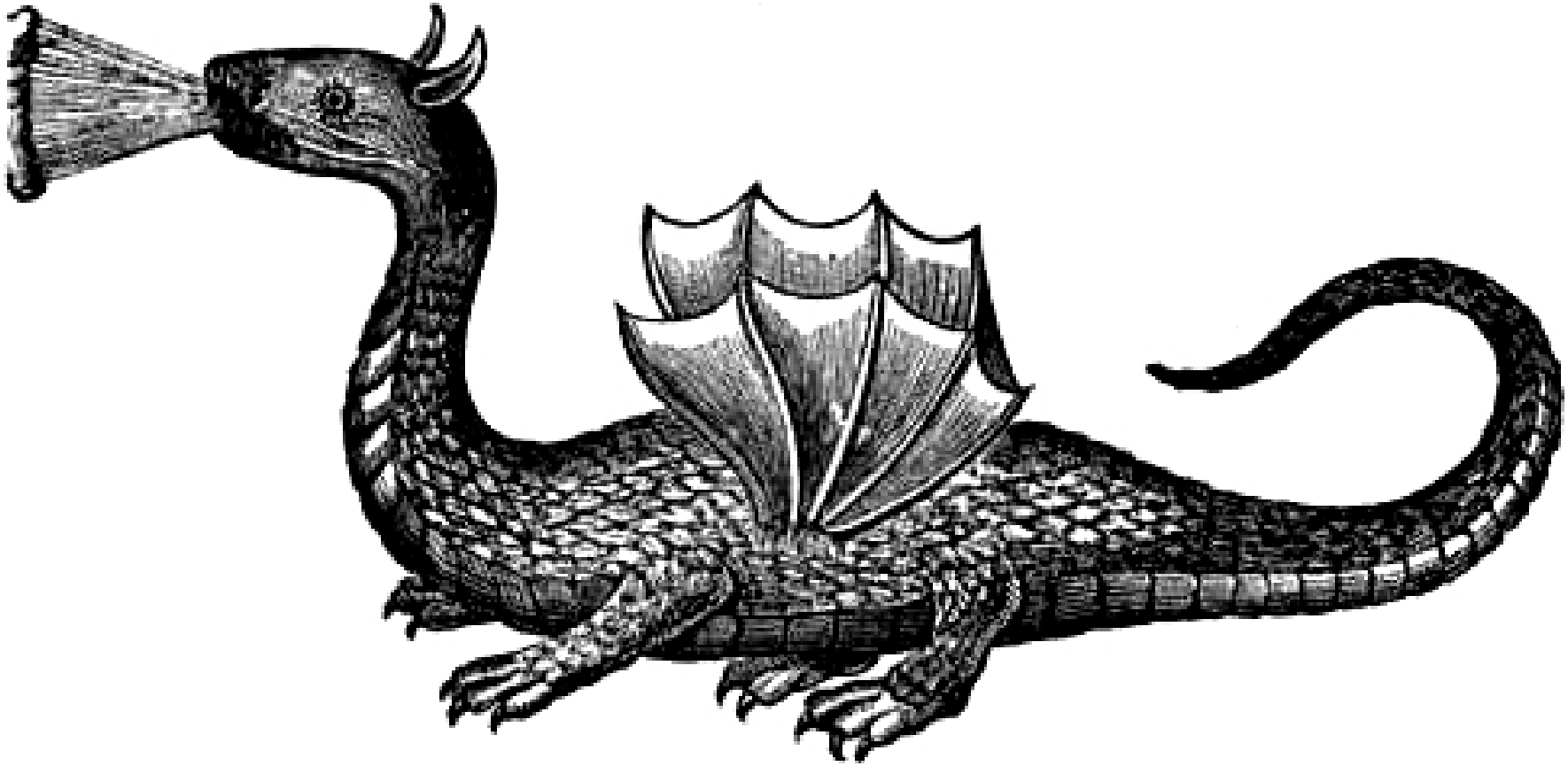
HUSK

Parallella

Airport til snif netværk

Agenda

Internet - Here be dragons



Kl 11:30-13:00

Paranoia defined

What are the risks, vulnerabilities and threats

Reduce risk and mitigate impact

Goals: Why?

Jacob Appelbaum @ioerror

Transparency and accountability are required properties of legitimate democratic institutions. "Anti-secrecy" rhetoric is hilariously tired.

Demokrati: Et frit demokrati fordrer borgere med frihed som har evnen til at tage beslutninger uden konstant at være overvåget.

Et demokrati fordrer borgere som aktivt vælger hvornår de afgiver personlige data om deres liv og færden og kryptografi er en fredelig protest mod indsamling at data.

Indsamlede data vil altid blive misbrugt

Data som indsamles **bliver misbrugt** enten til kriminelle formål, kommercielle formål uanset oprindelige formål med indsamlingen - under dække af beskyttelse mod terror, ekstremisme, nazisme, misbrug af børn, ... Le mal du jour / dagens onde.

Derudover stalking, ekskærester, arbejdsgivere, forældre, ...

Du bestemmer - det er privatliv og demokrati

Why think of security?

> Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world. A Cypherpunk's Manifesto by Eric Hughes, 1993

Copied from `https://cryptoparty.org/wiki/CryptoParty`

Security is not magic

.

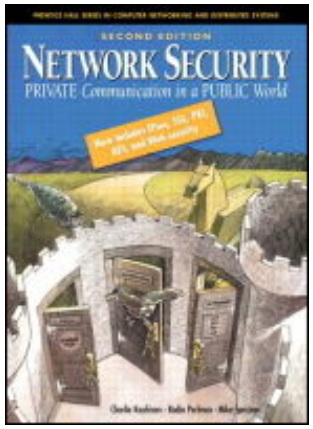
Think security, it may seem like magic - but it is not

Follow news about security

Support communities, join and learn

Rejsen starter

Hvor skal vi nu starte denne rejse?



Private Communications in an Public World

Anbefalelsesværdig bog som gennemgår grundlaget for kryptering, teknikker og protokollerne der bruges på internet idag, herunder: IPsec, SSL/TLS, PGP, PKI, AES m.fl.

Vi troede krypto kunne hjælpe os med næsten alle problemer ...

Part I: Paranoia defined

par·a·noi·a

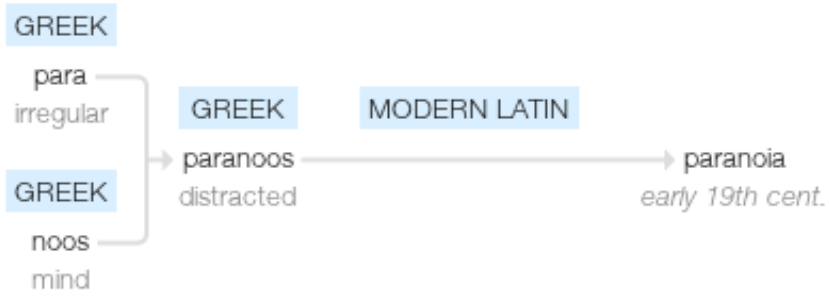
/ˌparəˈnoiə/

noun

noun: **paranoia**

1. a mental condition characterized by delusions of persecution, unwarranted jealousy, or exaggerated self-importance, typically elaborated into an organized system. It may be an aspect of chronic personality disorder, of drug abuse, or of a serious condition such as schizophrenia in which the person loses touch with reality.
   synonyms: persecution complex, delusions, obsession, psychosis More
- suspicion and mistrust of people or their actions without evidence or justification.
  "the global paranoia about hackers and viruses"

Origin



More

Source: google paranoia definition

Face reality

From the definition:

> suspicion and mistrust of people or their actions **without evidence or justification**. **”the global paranoia about hackers and viruses”**

It is not paranoia when:

- Criminals sell your credit card information and identity theft
- Hackers trade infected computers like a commodity
- Governments write laws that allows them to introduce back-doors - and use these
- Governments do blanket surveillance of their population
- Governments implement censorship, threaten citizens and journalist
- Governemnts monitor your sexting and naked chats over instant messaging apps
- Companies gather your personal data and sell access
- ... and the list goes on!

You are not paranoid when there are people actively attacking you!

Risk management defined

Information Risk Management

Life is full of risk.

Risk is the possibility of damage happening and the ramifications of such damage should it occur. ***Information risk management (IRM)*** is the *process* of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Source: Shon Harris *CISSP All-in-One Exam Guide*

Example UK: Seize smart phones and download data

Officers use counter-terrorism laws to remove a mobile phone from any passenger they wish coming through UK air, sea and international rail ports and then scour their data.

The blanket power is so broad they do not even have to show reasonable suspicion for seizing the device and can retain the information for ”as long as is necessary”.

Data can include call history, contact books, photos and who the person is texting or emailing, although not the contents of messages.

Source: http://www.telegraph.co.uk/technology/10177765/Travellers-mobile-phone-data-seized-by-police-at-border.html

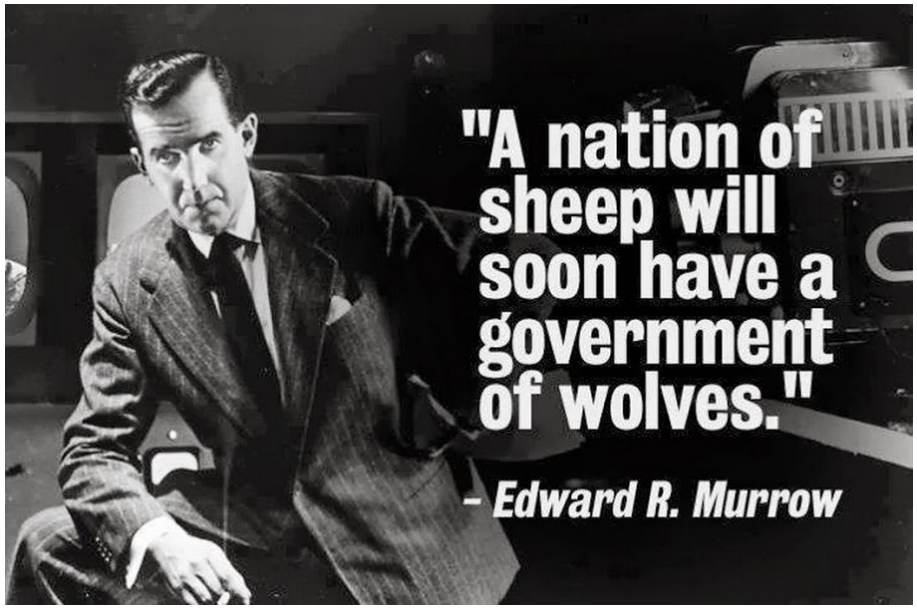
Example: UK wouldn't seize data like that, you are lying

SOLIDO NETWORKS

> (Reuters) - British authorities came under pressure on Monday to explain why anti-terrorism powers were used to detain for nine hours the partner of a journalist who has written articles about **U.S. and British surveillance programs** based on **leaks from Edward Snowden**.
>
> Brazilian David Miranda, the partner of American journalist Glenn Greenwald, was detained on Sunday at London's Heathrow Airport where he was in transit on his way from Berlin to Rio de Janeiro. **He was released without charge**.

Source:
http://www.reuters.com/article/2013/08/19/us-britain-snowden-detention-idUSBRE97I0J520130819

Government backdoors is not new information



Nothing new really, see for example D.I.R.T and Magic Lantern

D.I.R.T - Data Interception by Remote Transmission since the late 1990s
`http://cryptome.org/fbi-dirt.htm`
`http://cryptome.org/dirty-secrets2.htm`

They will always use *Le mal du jour* to increase monitoring

Governments blanket surveillance

NSA - need we say more?
`http://en.wikipedia.org/wiki/PRISM_(surveillance_program)`

Governments also implementing censorship

Outlaw and/or discredit crypto

Go after Tor exit nodes

Use protection - always

A vulnerability can and will be abused

SOLIDO NETWORKS

What if I told you:

Criminals will be happy to leverage backdoors created by government

It does not matter if the crypto product has a weakness to allow investigations or the software has a backdoor to help law enforcement. Data and vulnerabilities WILL be abused and exploited.

Ånden til at hacke

Don’t Panic!

Hacking betyder idag indbrud, kriminalitet, hærværk m.v.

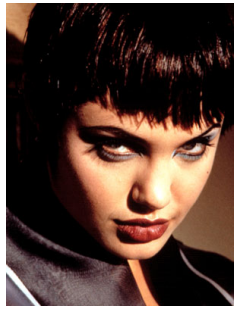
Oprindeligt betød hacking at man udforskede, undersøgte, involverede sig

Vi skal bruge ånden fra hacking til forskning, udvikling

Mange regler om at man ikke må noget er imod hacking.

Lad være med at bryde love, men bøj gerne regler ☺

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

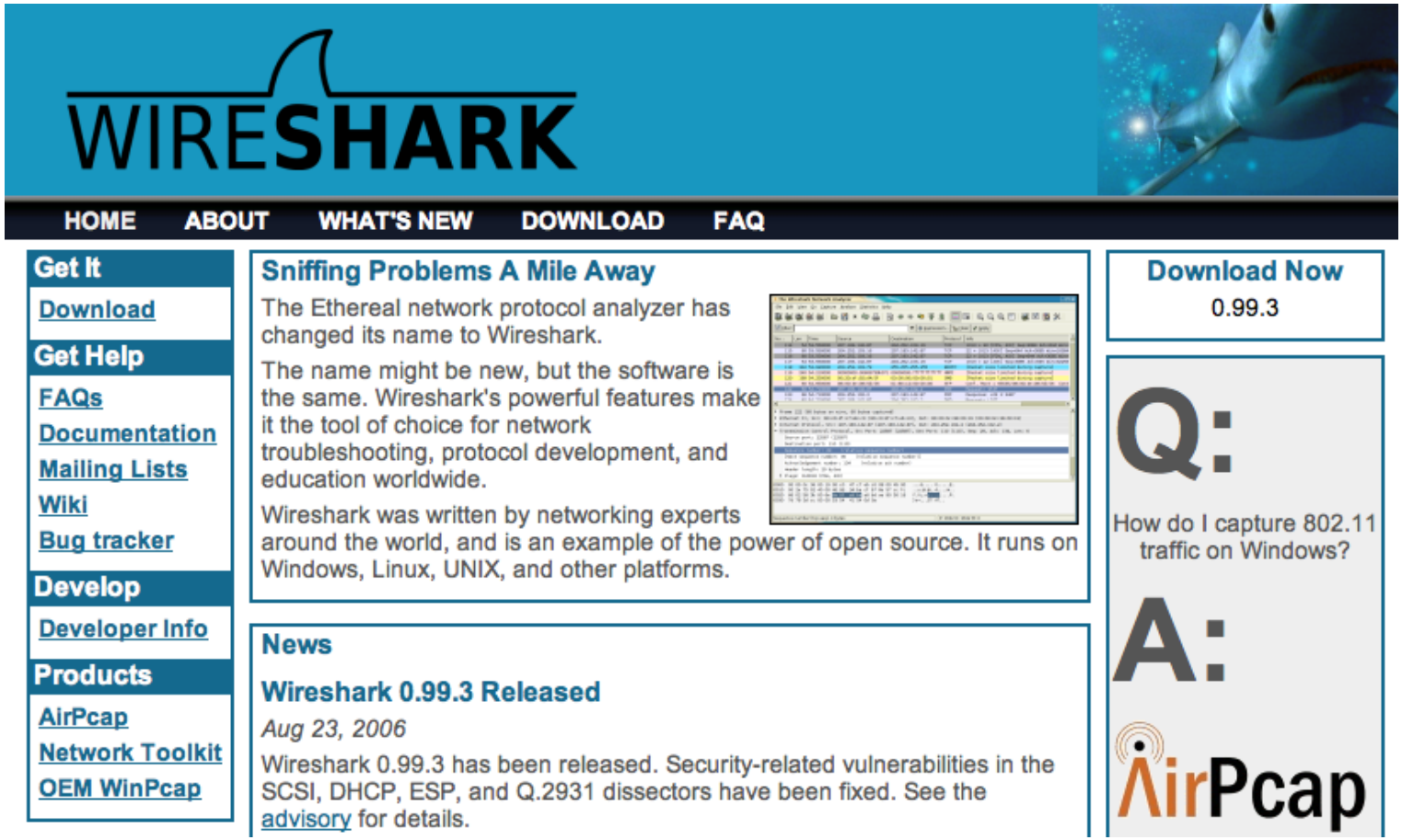
Kali Linux the new backtrack

BackTrack `http://www.backtrack-linux.org`

Kali `http://www.kali.org/`

Wireshark - `http://www.wireshark.org` avanceret netværkssniffer

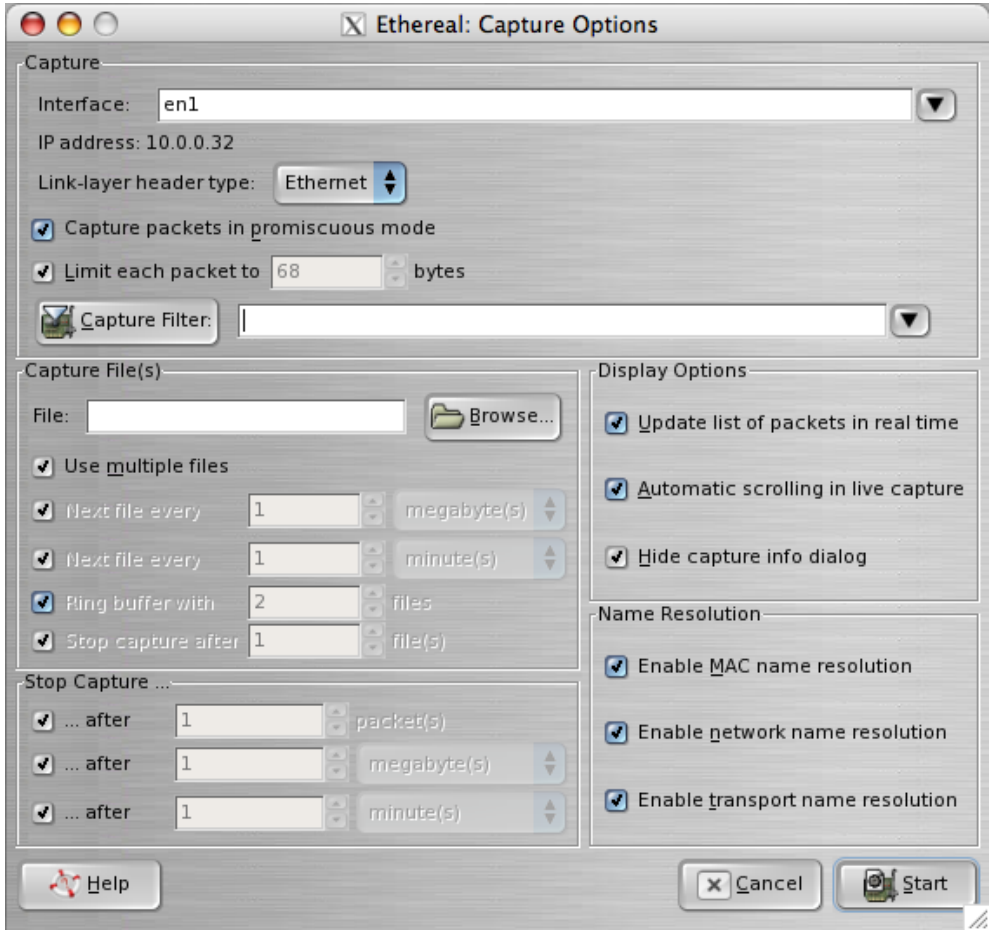
Wireshark - grafisk pakkesniffer



`http://www.wireshark.org`

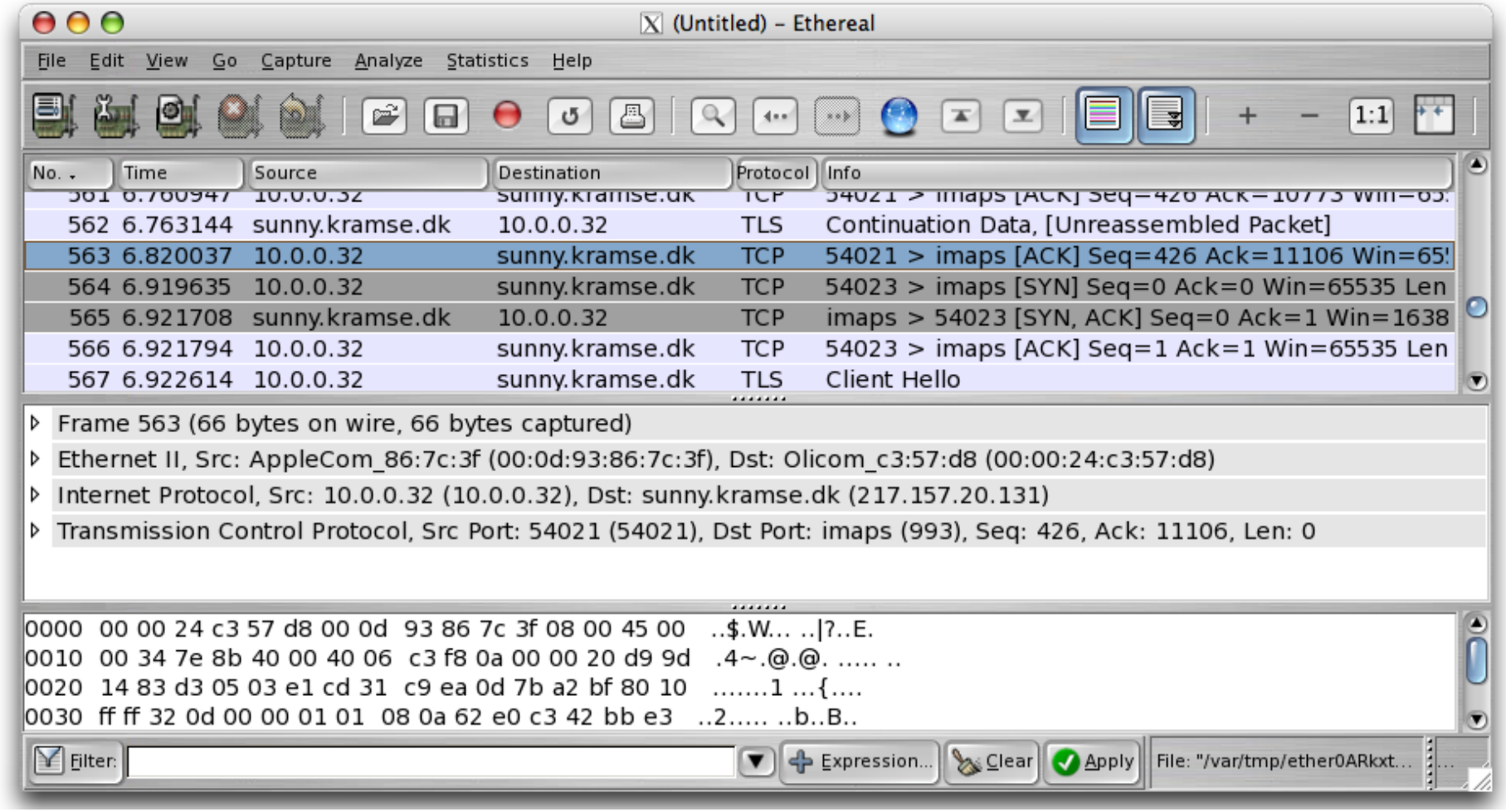
både til Windows og UNIX, tidligere kendt som Ethereal

Brug af Wireshark



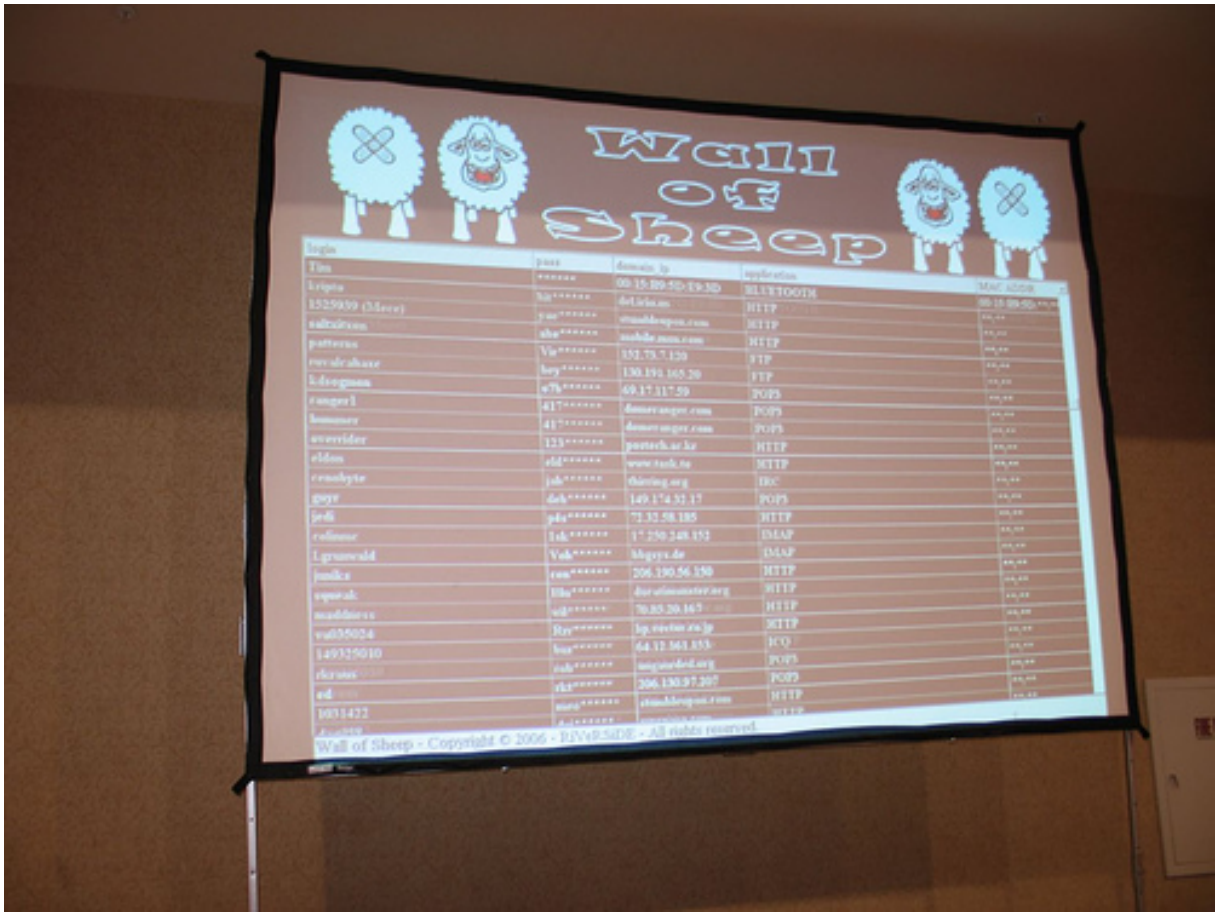
Man starter med Capture - Options

Brug af Wireshark



Læg mærke til filtermulighederne

Wall of sheep



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

Getting to your data: Google for it

Google as a hacker tools?

Concept named googledorks when google indexes information not supposed to be public `http://johnny.ihackstuff.com/`

Hacking er magi

Hacking ligner indimellem magi

Hacking er ikke magi

Hacking kræver blot lidt ninja-træning

Hacking eksempel - det er ikke magi

MAC filtrering på trådløse netværk

Alle netkort har en MAC adresse - BRÆNDT ind i kortet fra fabrikken

Mange trådløse Access Points kan filtrere MAC adresser

Kun kort som er på listen over godkendte adresser tillades adgang til netværket

Det virker dog ikke ☺

De fleste netkort tillader at man overskriver denne adresse midlertidigt

Myten om MAC filtrering

Eksemplet med MAC filtrering er en af de mange myter

Hvorfor sker det?

Marketing - producenterne sætter store mærkater på æskerne

Manglende indsigt - forbrugerne kender reelt ikke koncepterne

Hvad *er* en MAC adresse egentlig

Relativt få har forudsætningerne for at gennemskue dårlig sikkerhed

Løsninger?

Udbrede viden om usikre metoder til at sikre data og computere

Udbrede viden om sikre metoder til at sikre data og computere

MAC filtrering

Demo investigating the current network

SOLIDO NETWORKS

Old skool tools: dsniff

one sniffer for old protocols includes **arpspoof**

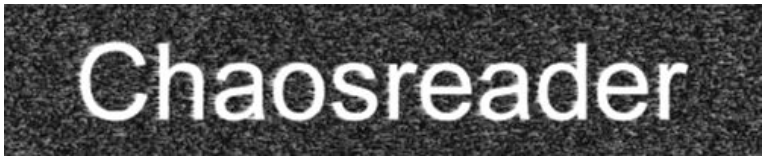
Lavet af Dug Song, dugsong@monkey.org

Want a gui, try Ettercap

```
dsniff is a password sniffer which handles FTP, Telnet,
SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin,
RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11,
CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker,
Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft
SMB, Oracle SQL*Net, Sybase and Microsoft SQL protocols.
```

Note: requires access to network traffic, like open wireless

Chaosreader



Chaosreader Report

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

Image Report - Click here for a report on captured images.
GET/POST Report (Empty) - Click here for a report on HTTP GETs and POSTs.
HTTP Proxy Log - Click here for a generated proxy style HTTP log.

TCP/UDP/... Sessions

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

Med adgang til et netværksdump kan man læse det med chaosreader

Output er HTML med oversigter over sessioner, billeder fra datastrømmen osv.

`http://chaosreader.sourceforge.net/`

Ettercap

Ettercap is a comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

Source: `https://ettercap.github.io/ettercap/`

Suricata IDS/IPS/NSM

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF and its supporting vendors.

- `http://suricata-ids.org/`
- `http://openinfosecfoundation.org`

Netflow

Netflow is getting more important, more data share the same links

Accounting is important

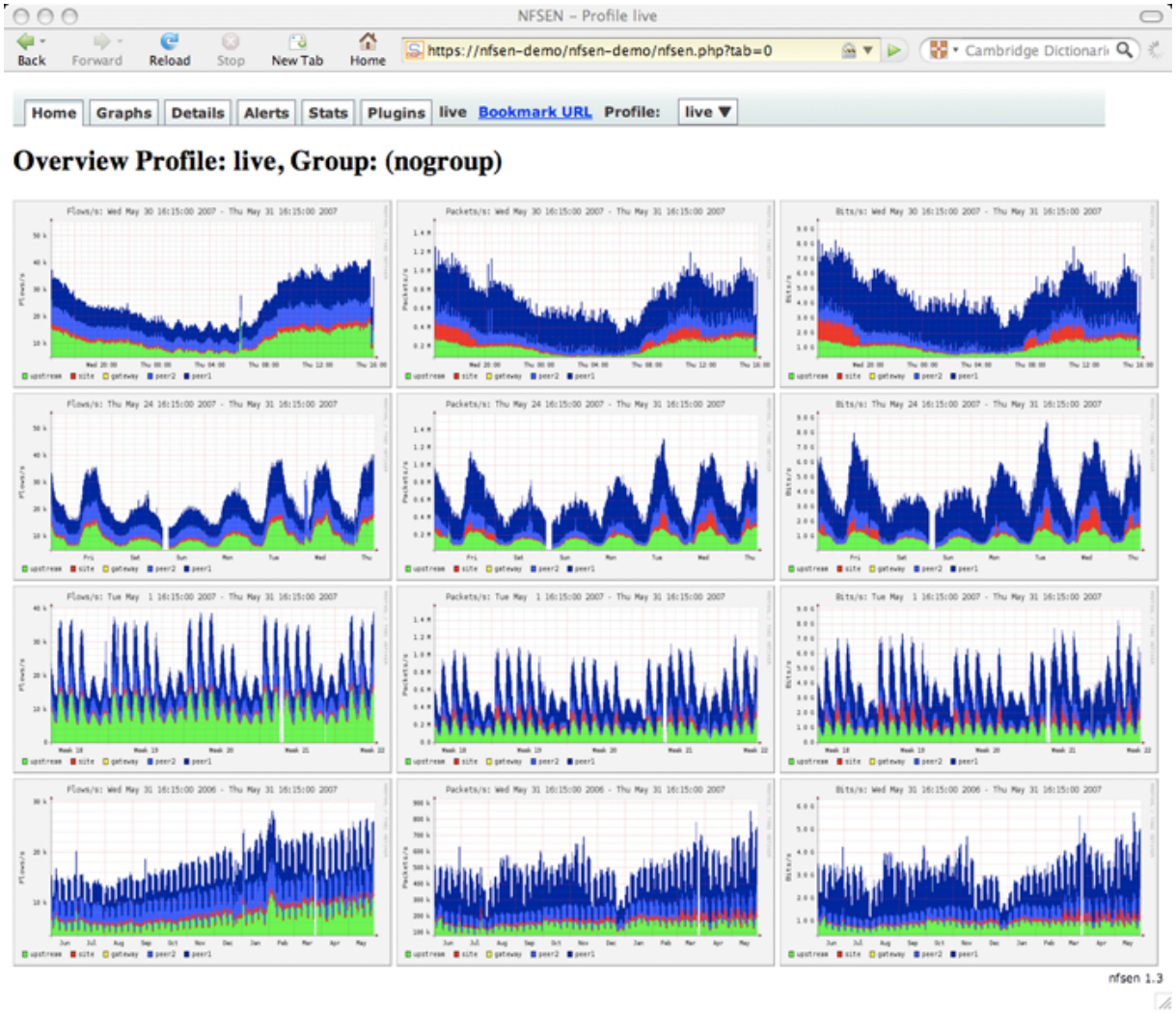
Detecting DoS/DDoS and problems is essential

Netflow sampling is vital information - 123Mbit, but what kind of traffic

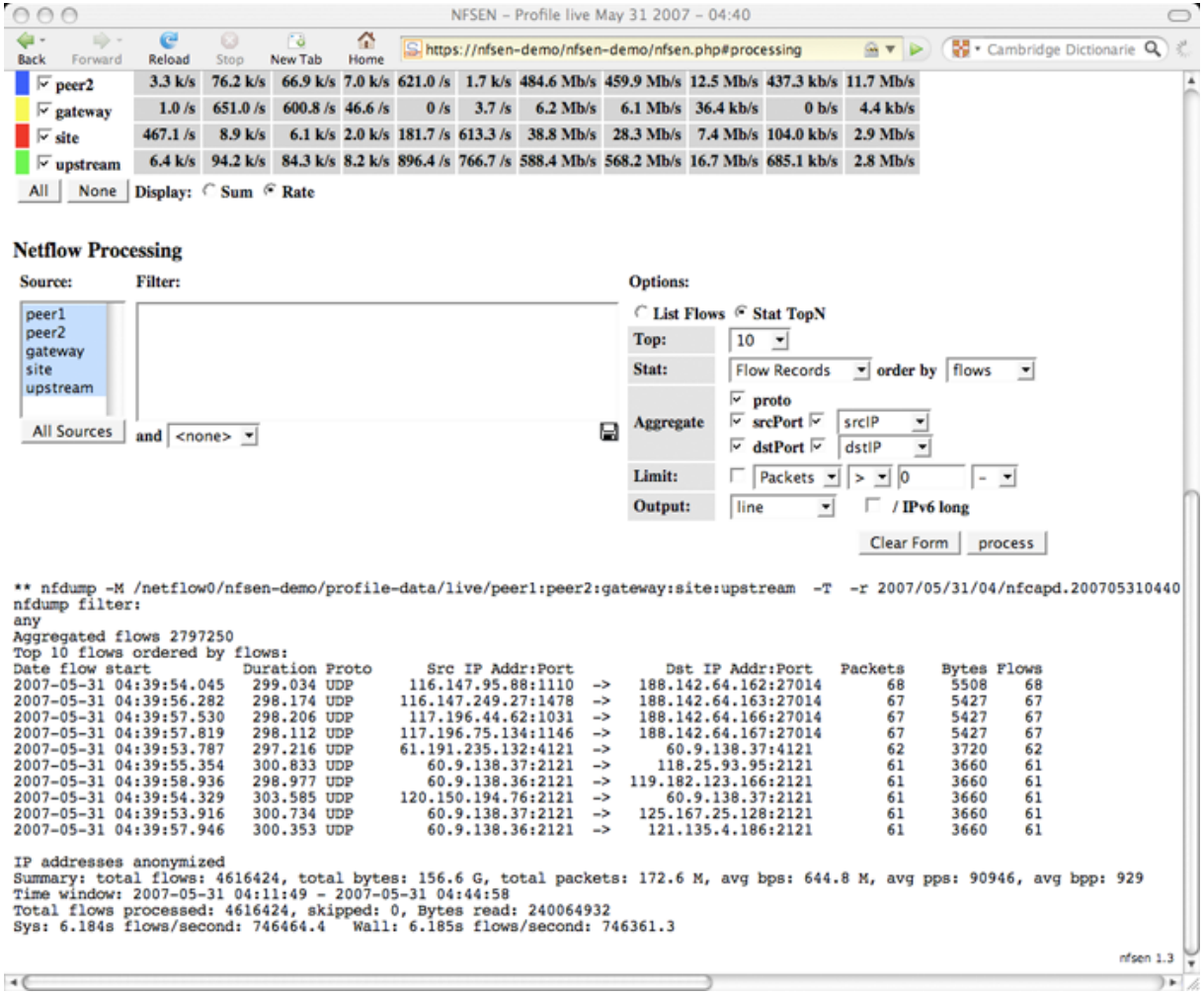
We use mostly NFSen, but are looking at various software packages
`http://nfsen.sourceforge.net/`

Currently also investigating sFlow - hopefully more fine grained

Netflow using NFSen

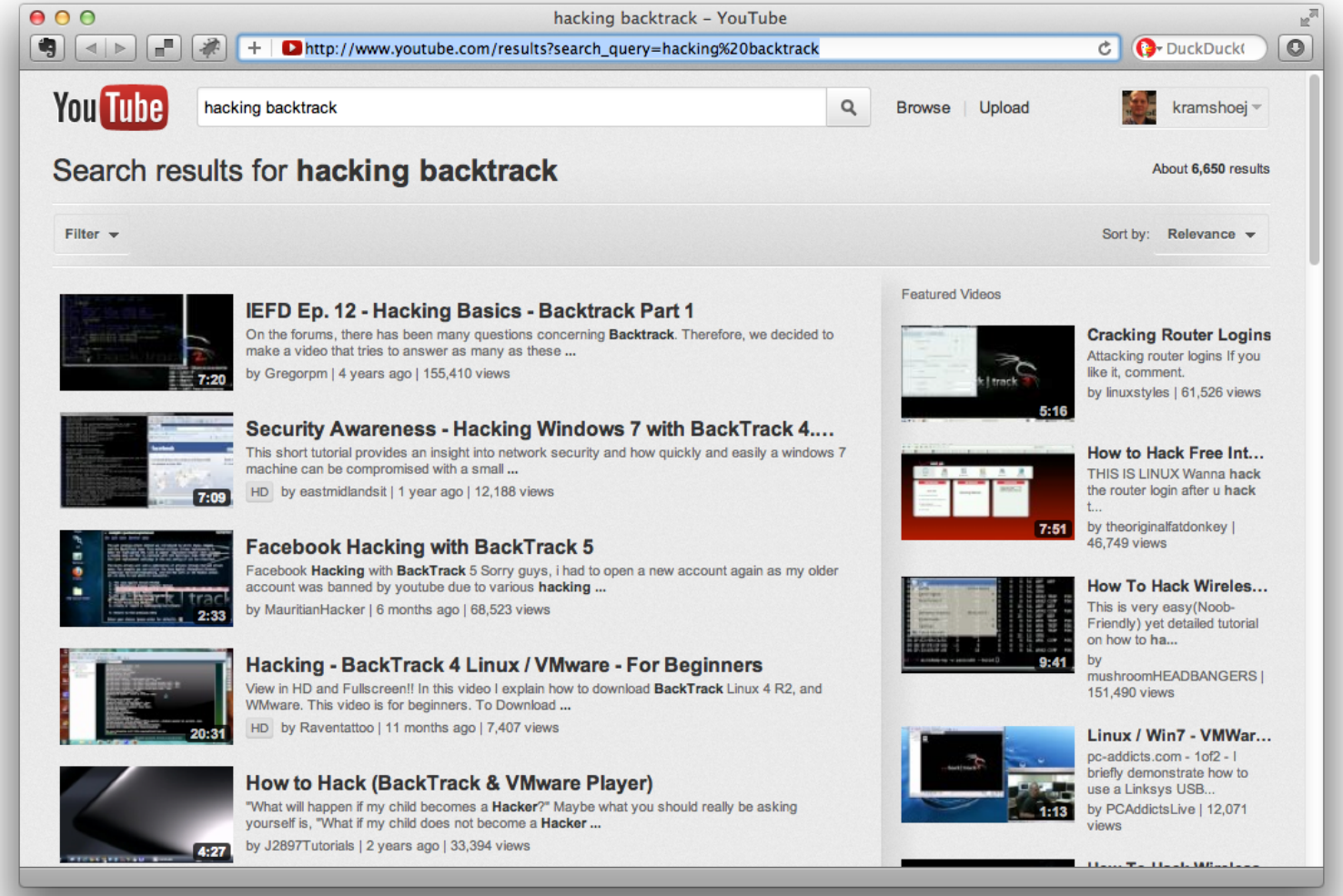


Netflow processing from the web interface



Bringing the power of the command line forward

Status idag på internet



Quick Wins

Using different password for each service, unpossible!

OTP One Time Password, sniff one and you can use it, if you have a time machine ☺

Yubico Yubikey

› YubiKey Standard

Our flagship product, making strong two-factor authentication, easy and affordable for everyone.

› YubiKey NEO

Our premium YubiKey, combining USB, NFC, one-time password and PKI technology.

› YubiKey Nano

The world's smallest one-time password token, designed to stay inside the USB-slot.

› YubiKey VIP

A YubiKey Standard pre-configured with a Symantec VIP credential, enabling two-factor authentication against Symantec VIP enabled services, such as PayPal.

› LastPass YubiKey

LastPass Premium is the leading cross platform password manager supporting the YubiKey. We offer a number of discounted bundles of YubiKey + LastPass Premium Subscriptions.

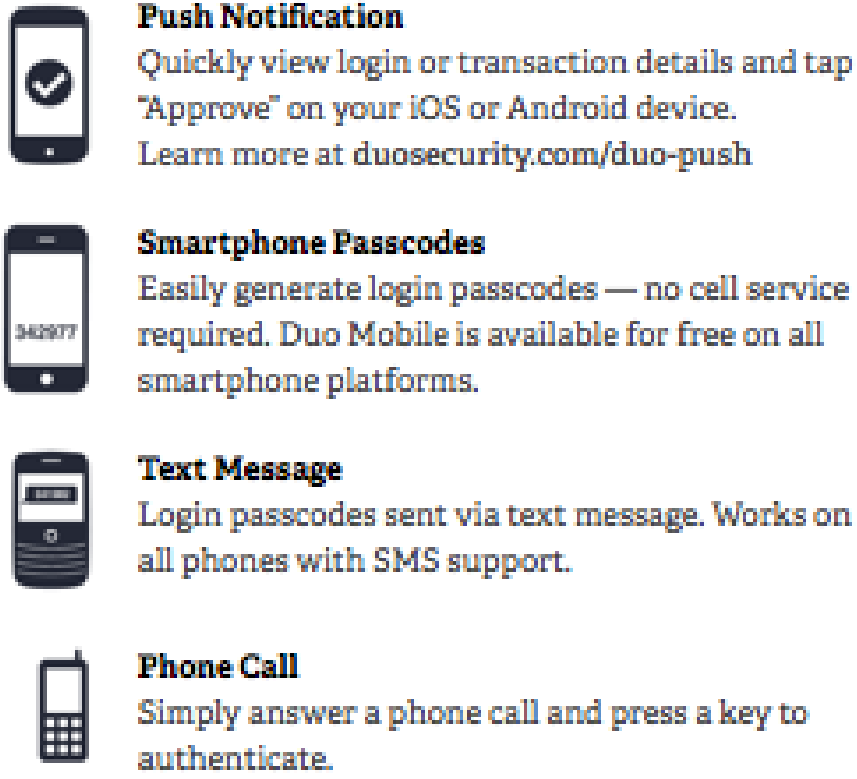
› Password Safe YubiKey

Pasword Safe is an open source password manager initiated by Bruce Schneier. The YubiKey is used in Challenge-response mode to for 2 factor encryption of the database.

A Yubico OTP is unique sequence of characters generated every time the YubiKey button is touched. The Yubico OTP is comprised of a sequence of 32 Modhex characters representing information encrypted with a 128 bit AES-128 key

`http://www.yubico.com/products/yubikey-hardware/`

TwoFactor authentication: Example Duosecurity



Push Notification
Quickly view login or transaction details and tap "Approve" on your iOS or Android device.
Learn more at duosecurity.com/duo-push

Smartphone Passcodes
Easily generate login passcodes — no cell service required. Duo Mobile is available for free on all smartphone platforms.

Text Message
Login passcodes sent via text message. Works on all phones with SMS support.

Phone Call
Simply answer a phone call and press a key to authenticate.

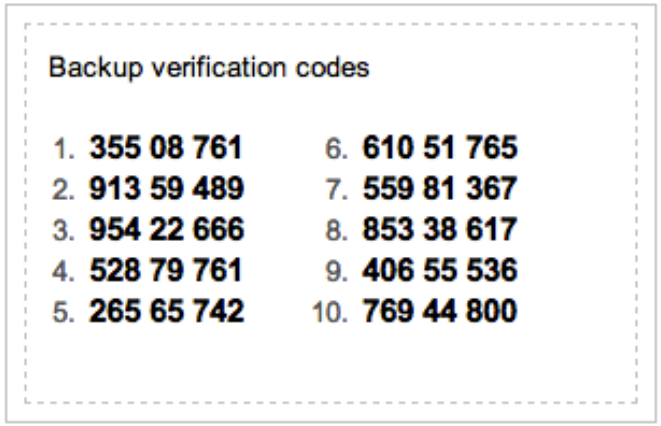
Video `https://www.duosecurity.com/duo-push`

`https://www.duosecurity.com/`

Low tech 2-step verification

SOLIDO NETWORKS

Printing code on paper, low level pragmatic



Login from new devices today often requires two-factor - email sent to user

Google 2-factor auth. SMS with backup codes

Also read about S/KEY developed at Bellcore **in the late 1980s**
`http://en.wikipedia.org/wiki/S/KEY`

Conclusion passwords: integrate with authentication, not reinvent

Integrate or develop?

From previous slide:

Conclusion passwords: integrate with authentication, not reinvent

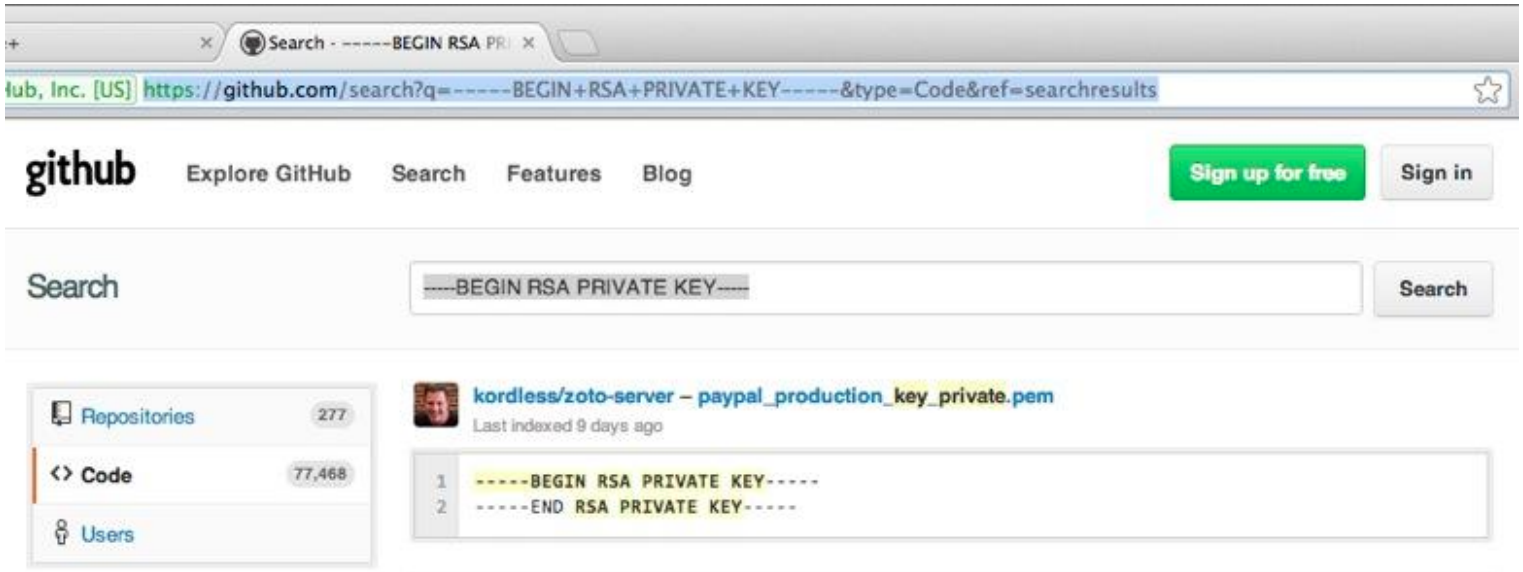
Dont:

- Reinvent the wheel - too many times, unless you can maintain it afterwards
- Never invent cryptography yourself
- No copy paste of functionality, harder to maintain in the future

Do:

- Integrate with existing solutions
- Use existing well-tested code: cryptography, authentication, hashing
- Centralize security in your code
- Fine to hide which authentication framework is being used, easy to replace later

January 2013: Github Public passwords?



Sources:

https://twitter.com/brianaker/status/294228373377515522

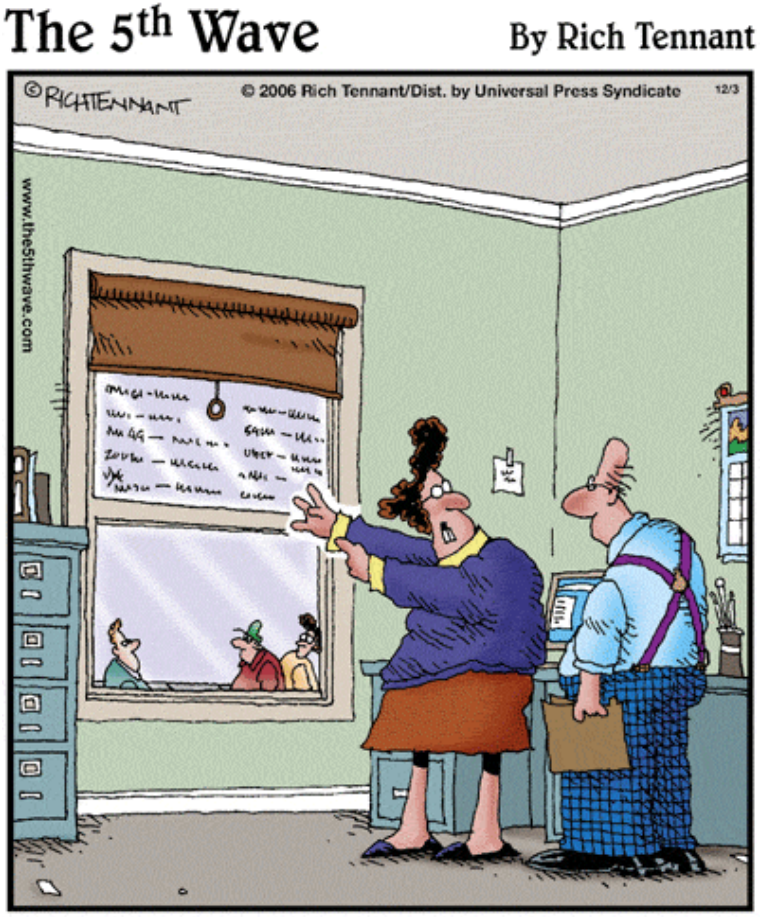
http://www.webmonkey.com/2013/01/users-scramble-as-github-search-exposes-passwords-security-de

http://www.leakedin.com/

http://www.offensive-security.com/community-projects/google-hacking-database/

Use different passwords for different sites, yes - every site!

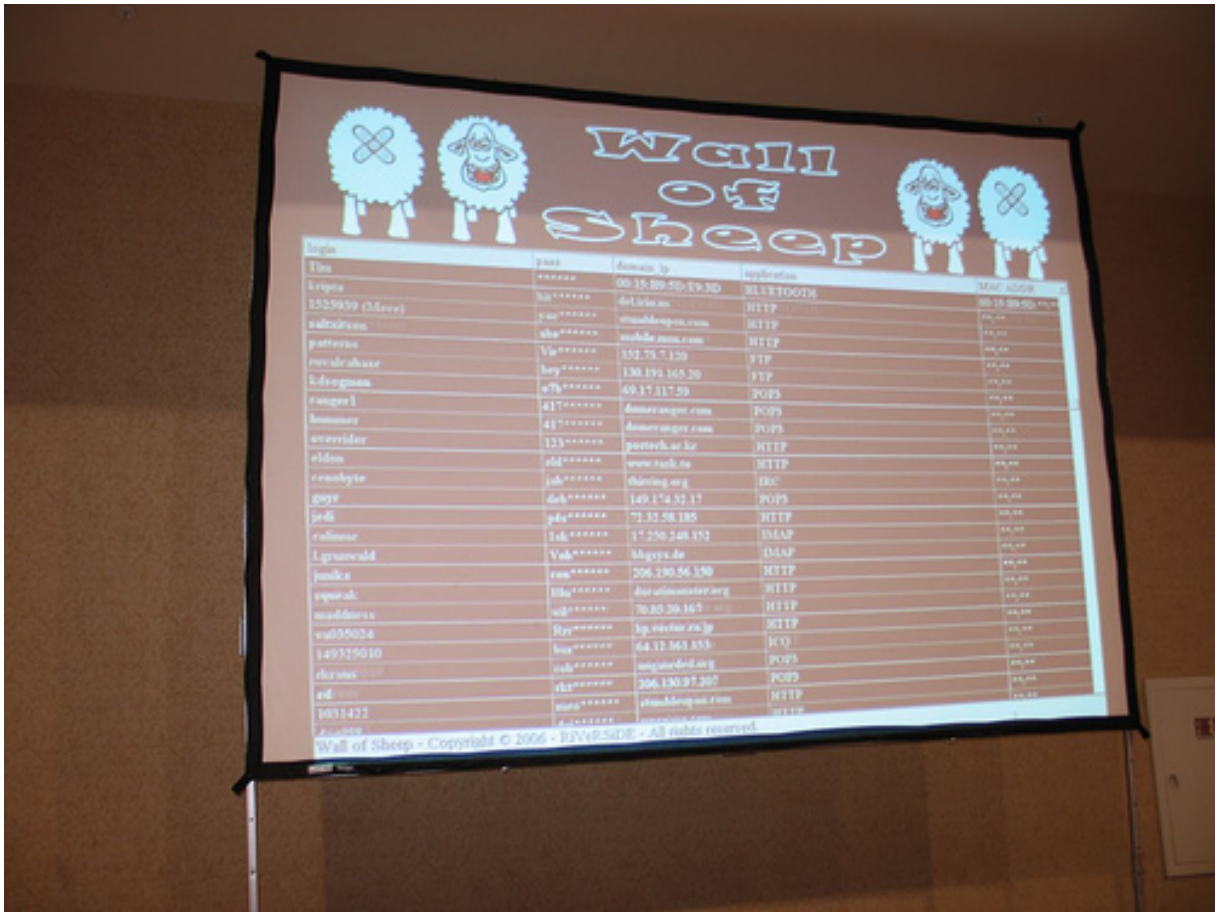
Opbevaring af passwords



"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."

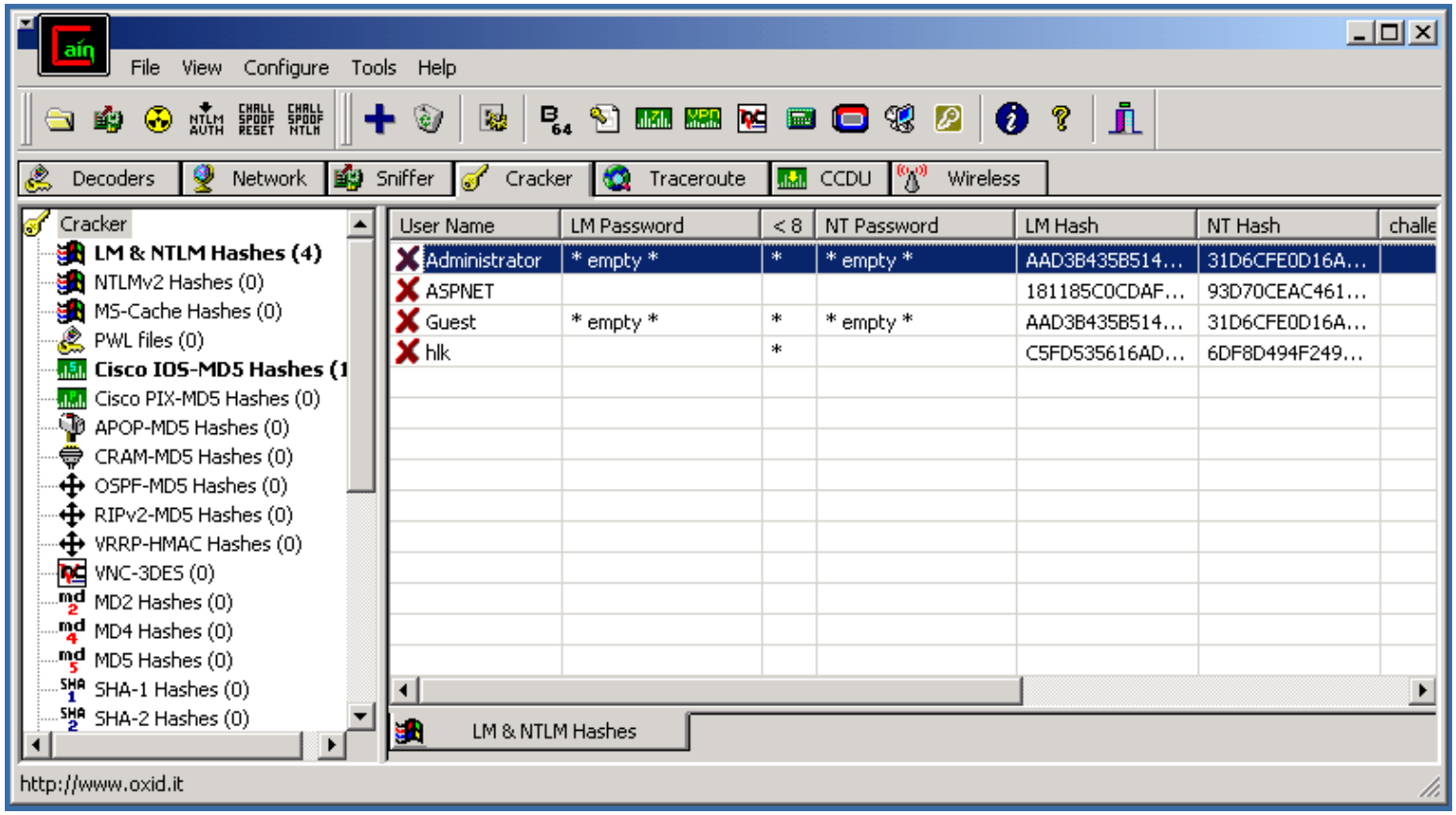
Use some kind of Password Safe program which encrypts your password database

Wall of sheep



Defcon Wall of Sheep

Cain & Abel



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

John the ripper

> John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches.

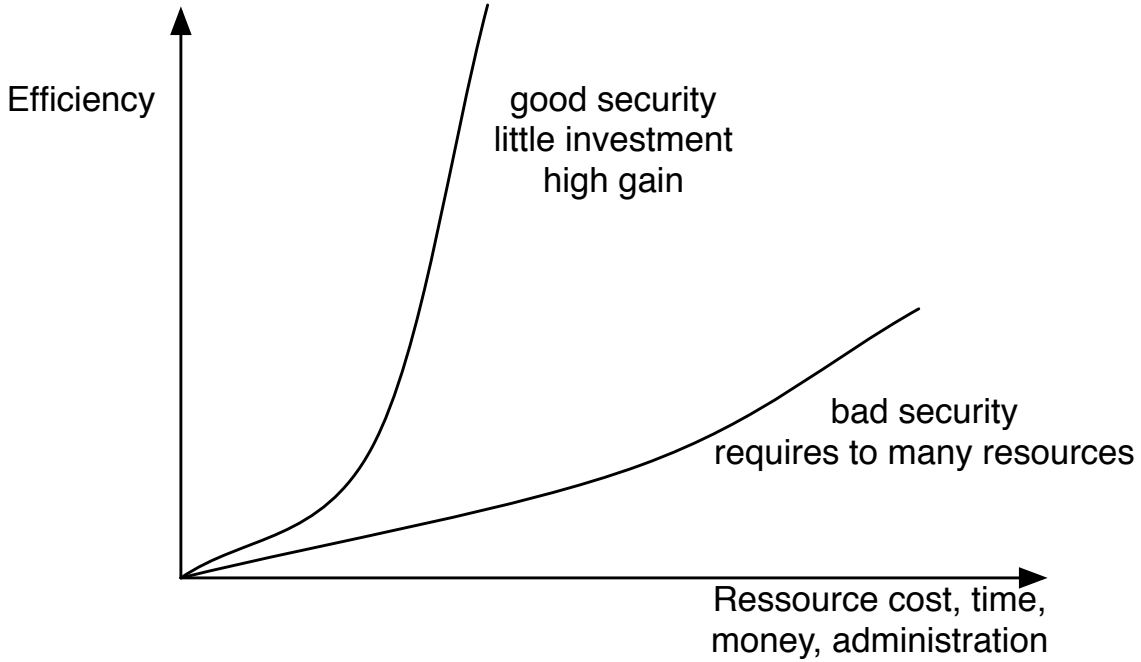
UNIX passwords kan knækkes med alec Muffets kendte Crack program eller eksempelvis John The Ripper `http://www.openwall.com/john/`

Jeg bruger selv John The Ripper

Pause

Er det tid til en lille pause?

Good security



You always have limited resources for protection - use them as best as possible

First advice

Use technology

Learn the technology - read the freaking manual

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

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

- Turn off features you don't use
- Turn off network connections when not in use
- Update software and applications
- Turn on encryption: IMAP**S**, POP3**S**, HTTP**S** also for data at rest, full disk encryption, tablet encryption
- Lock devices automatically when not used for 10 minutes
- Dont trust fancy logins like fingerprint scanner or face recognition on cheap devices

First advice use the modern operating systems

Newer versions of Microsoft Windows, Mac OS X and Linux

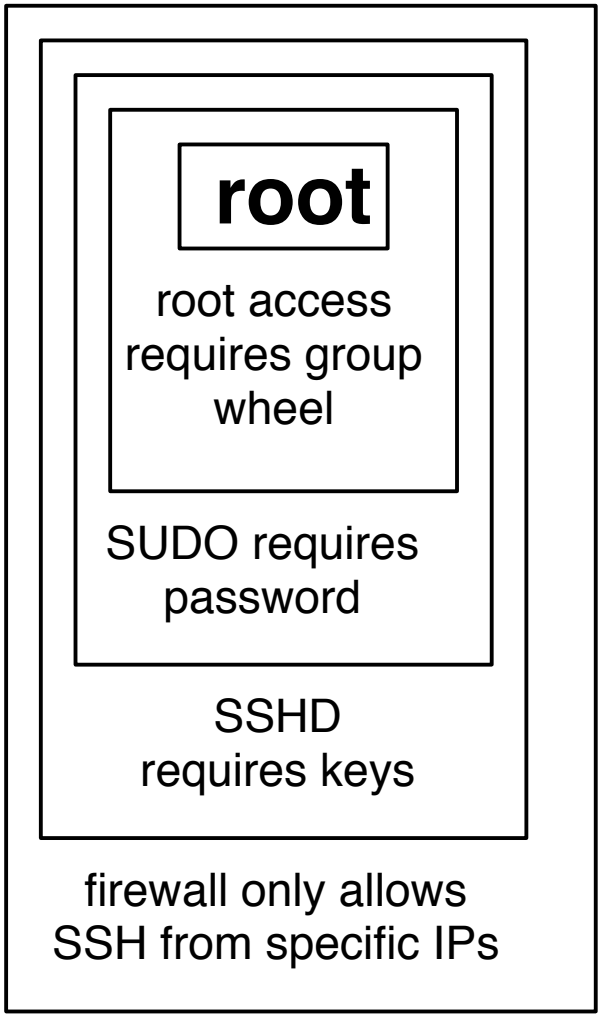
- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

Note: these still have errors and bugs, but are better than older versions

OpenBSD has shown the way in many cases
`http://www.openbsd.org/papers/`

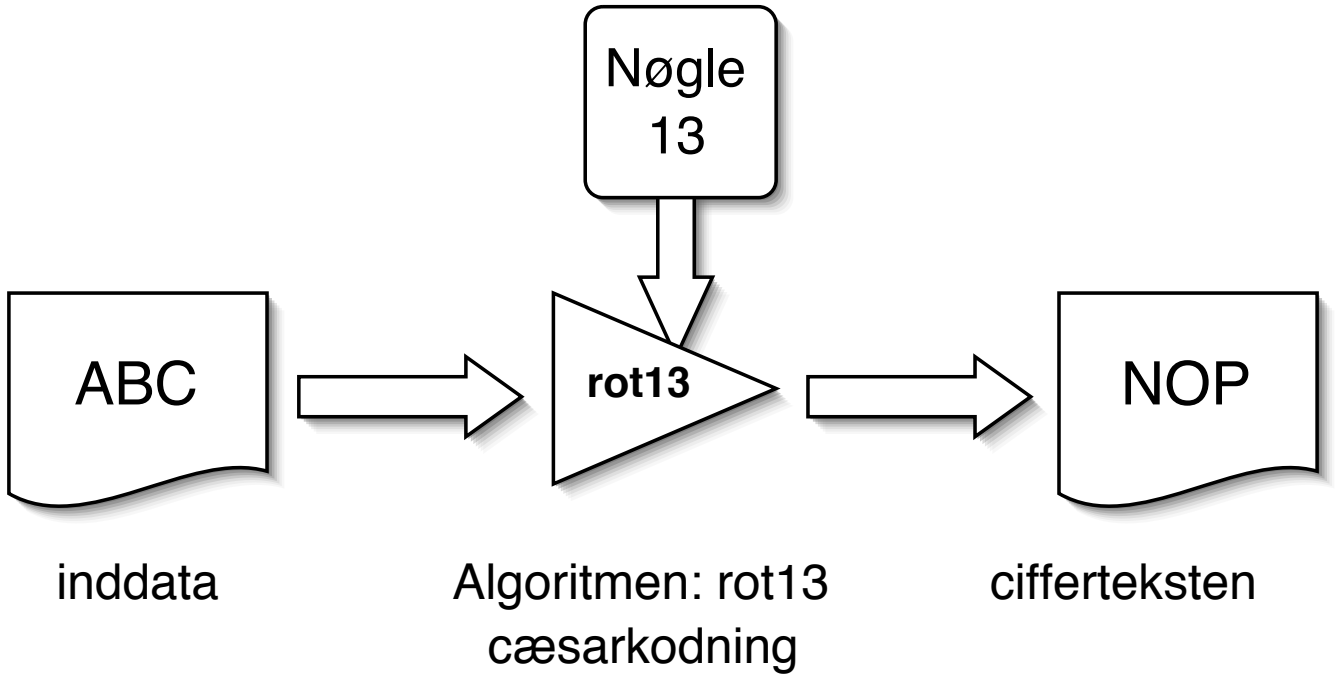
Always try to make life worse and more costly for attackers

Defense in depth



Defense using multiple layers is stronger!

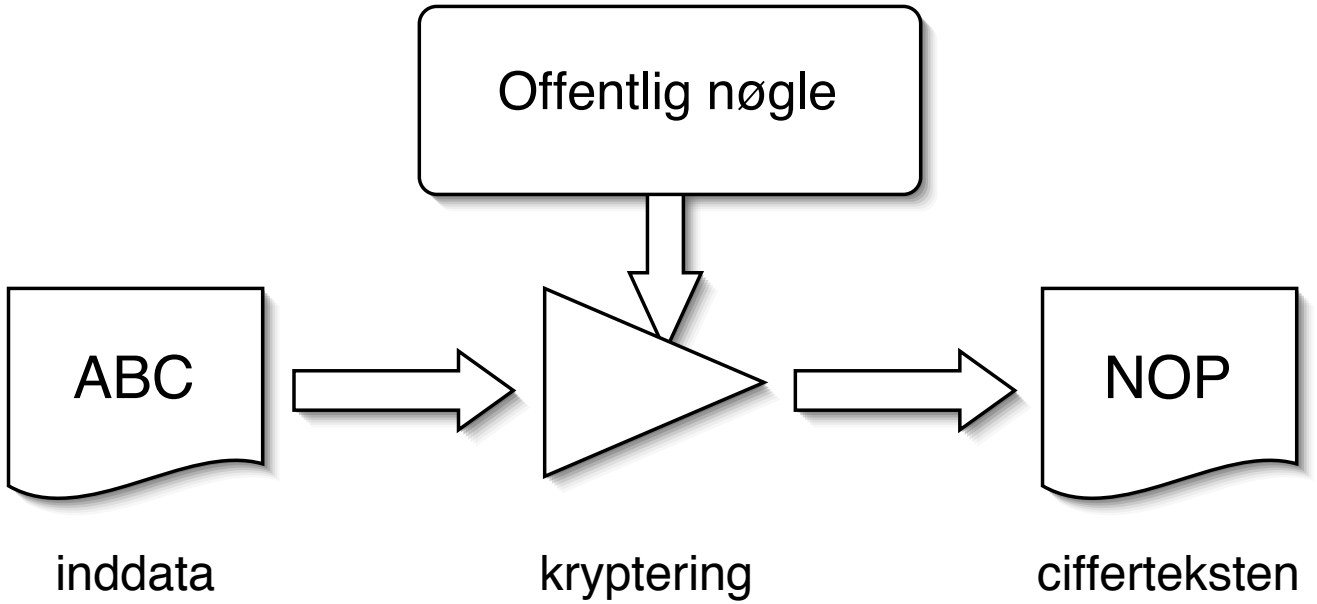
Kryptografi



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

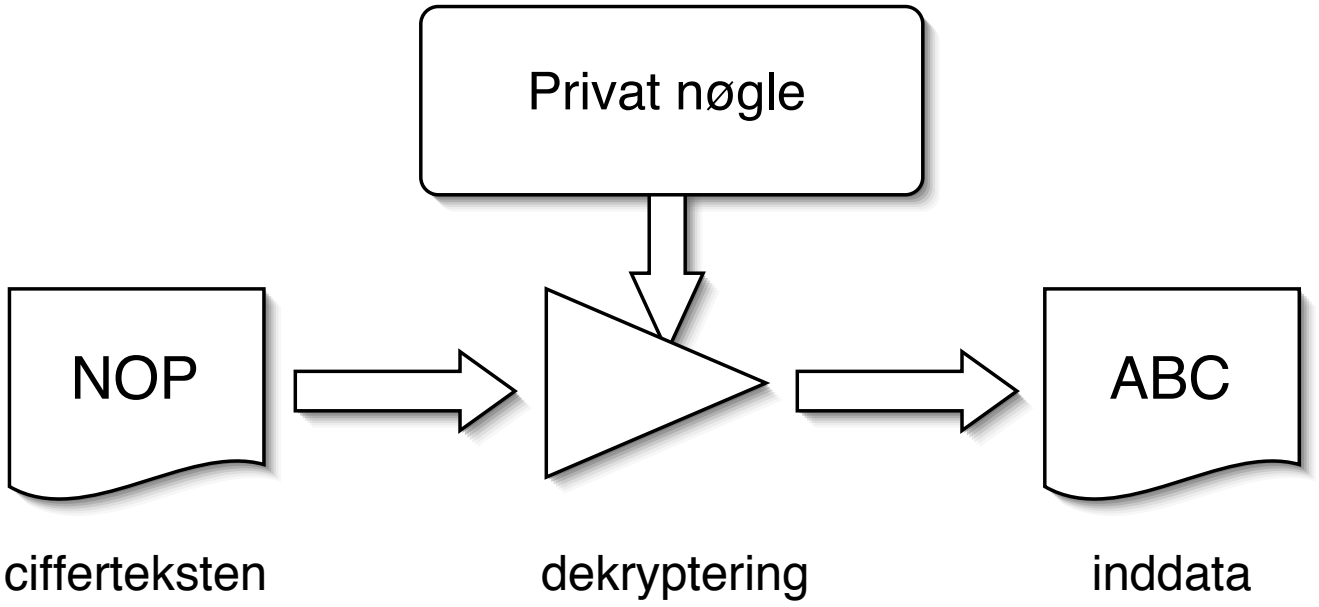
Public key kryptografi - 1



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`

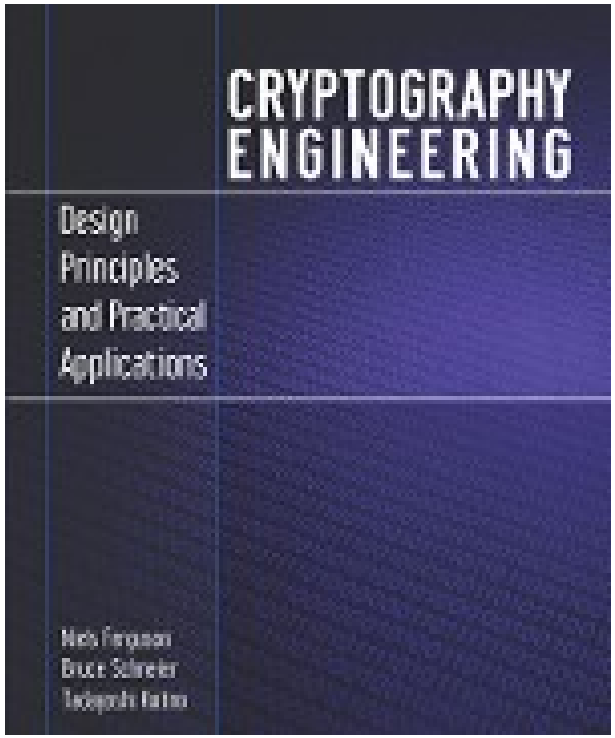
Formålet med kryptering

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet

Cryptography Engineering



Cryptography Engineering by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno

`https://www.schneier.com/book-ce.html`

SOLIDO NETWORKS

Sorry, none

SSL

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

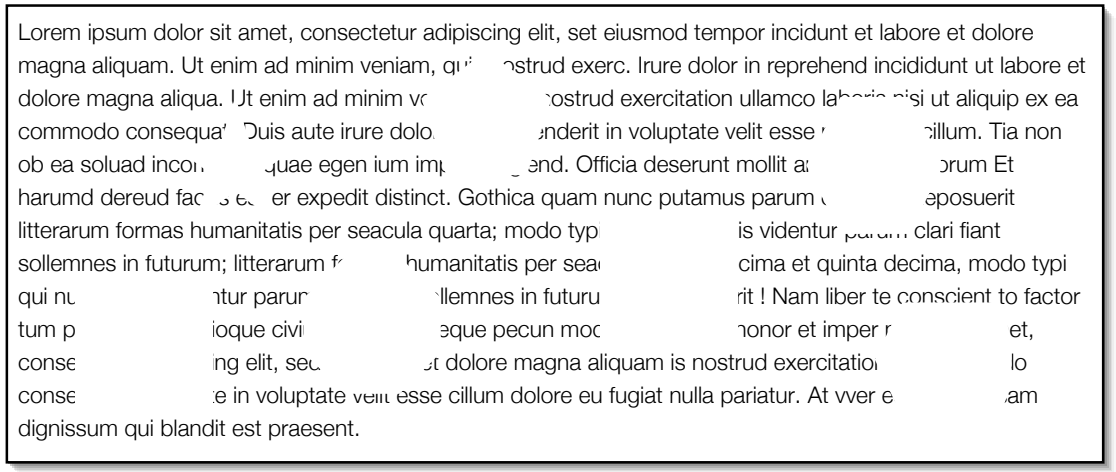
OpenSSL, LibreSSL, Apple SSL flaw exit exit exit!, Android SSL, certs certs cert!!!111, SSLv2, Heartbleed

Sorry, brain overflow from SSL/TLS vulnerabilities

Heartbleed

insert here from /userdata/projects/security-courses/presentations/misc/heartbleed-bug

Are your data secure



Stolen laptop, tablet, phone - can anybody read your data?

Do you trust ”remote wipe”

How do you in fact wipe data securely off devices, and SSDs?

Encrypt disk and storage devices before using them in the first place!

Circumvent security - single user mode boot

Unix systems often allows boot into singleuser mode
press command-s when booting Mac OS X

Laptops can often be booted using PXE network or CD boot

Mac computers can become a Firewire disk
hold t when booting - firewire target mode

Unrestricted access to un-encrypted data

Moving hard drive to another computer is also easy

Physical access is often - **game over**

Mac OS X

Firewire target mode: Macbook disken kan tilgås fra en anden Mac

Press t to enter firewire target mode ☺

`http://support.apple.com/kb/ht1661`

Theft - kindergarten and airports

Many parents are in a hurry when they are picking up their kids

Many people can easily be distracted around crowds

Many people let their laptops stay out in the open - even at conferences

... making theft likely/easy

Stolen for the value of the hardware - or for the data?

Industrial espionage, economic espionage or corporate espionage is real

SOLIDO NETWORKS

Kom igang!

- Skriv på DVD - DVD brændere i mange laptops idag
- Gem på netværket - Dropbox, husk en yderligere backup!
- Brug Duplicity på egen server, eller tilsvarende services

Mat Honan epic hacking :-(

`http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/`

SOLIDO NETWORKS

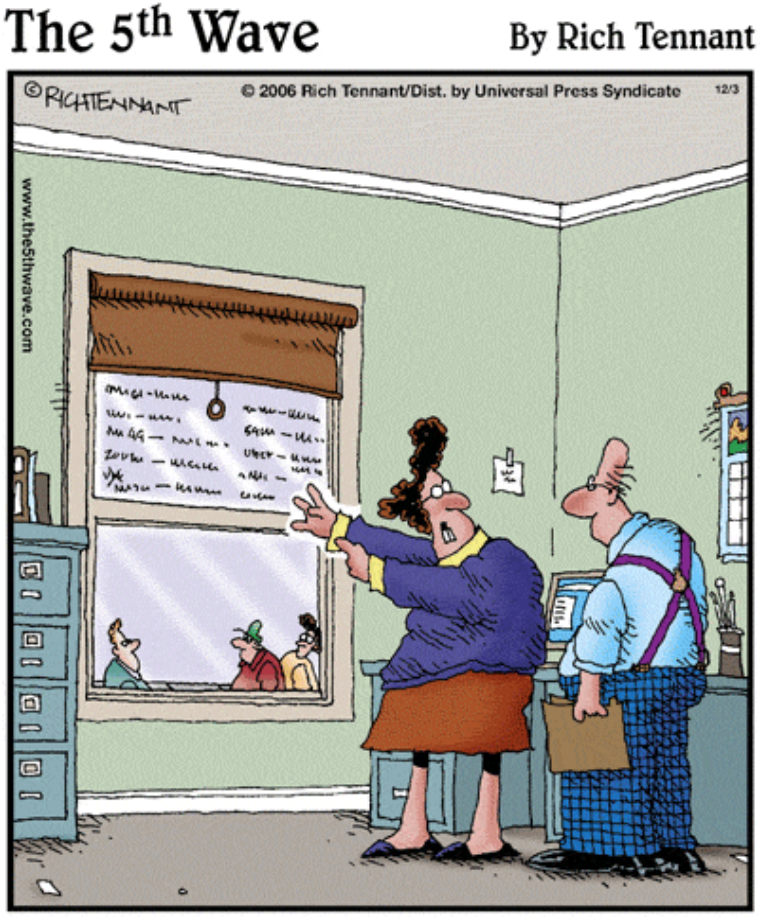
What is it?

Duplicity backs directories by producing encrypted tar-format volumes and uploading them to a remote or local file server. Because duplicity uses librsync, the incremental archives are space efficient and only record the parts of files that have changed since the last backup. Because duplicity uses **GnuPG** to encrypt and/or sign these archives, they will be safe from spying and/or modification by the server.

`http://duplicity.nongnu.org/` duplicity home page

`http://www.gnupg.org/` The GNU Privacy Guard

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."

Encrypting hard disk

Becoming available in the most popular client operating systems

- Microsoft Windows Bitlocker - requires Ultimate or Enterprise
- Apple Mac OS X - FileVault og FileVault2
- FreeBSD GEOM og GBDE - encryption framework
- Linux distributions like Ubuntu ask to encrypt home dir during installation
- PGP disk - Pretty Good Privacy - makes a virtuel krypteret disk
- TrueCrypt - similar to PGP disk, a virtual drive with data, cross platform
- Some vendors have BIOS passwords, or disk passwords

http://blog.cryptographyengineering.com/2013/10/lets-audit-truecrypt.html

Note: truecrypt halted and insecure? who knows?

Email security - PGP pretty good privacy

- Pretty Good Privacy - PGP
- Oprindeligt udviklet af Phil Zimmermann
- nu kommercielt, men der findes altid en freeware version `http://www.pgp.com`
- 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

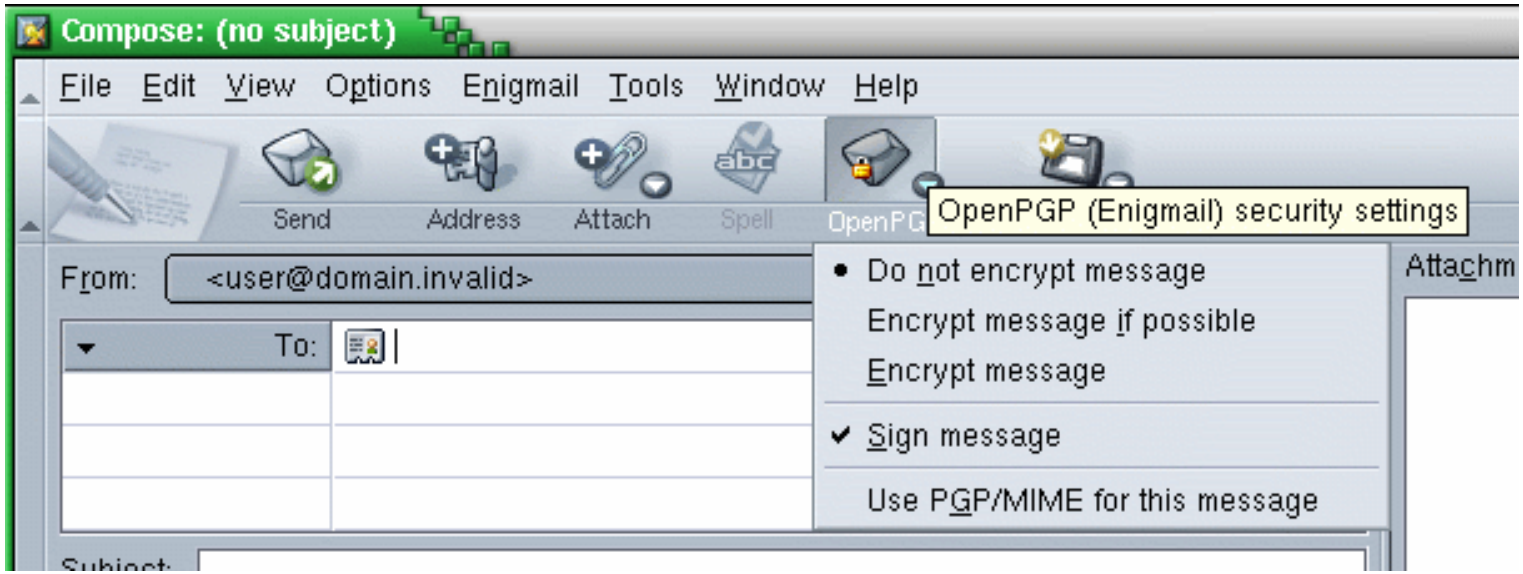
Gnu Privacy Guard, forkortes GnuPG eller GPG

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

Open Source med GPL licens.

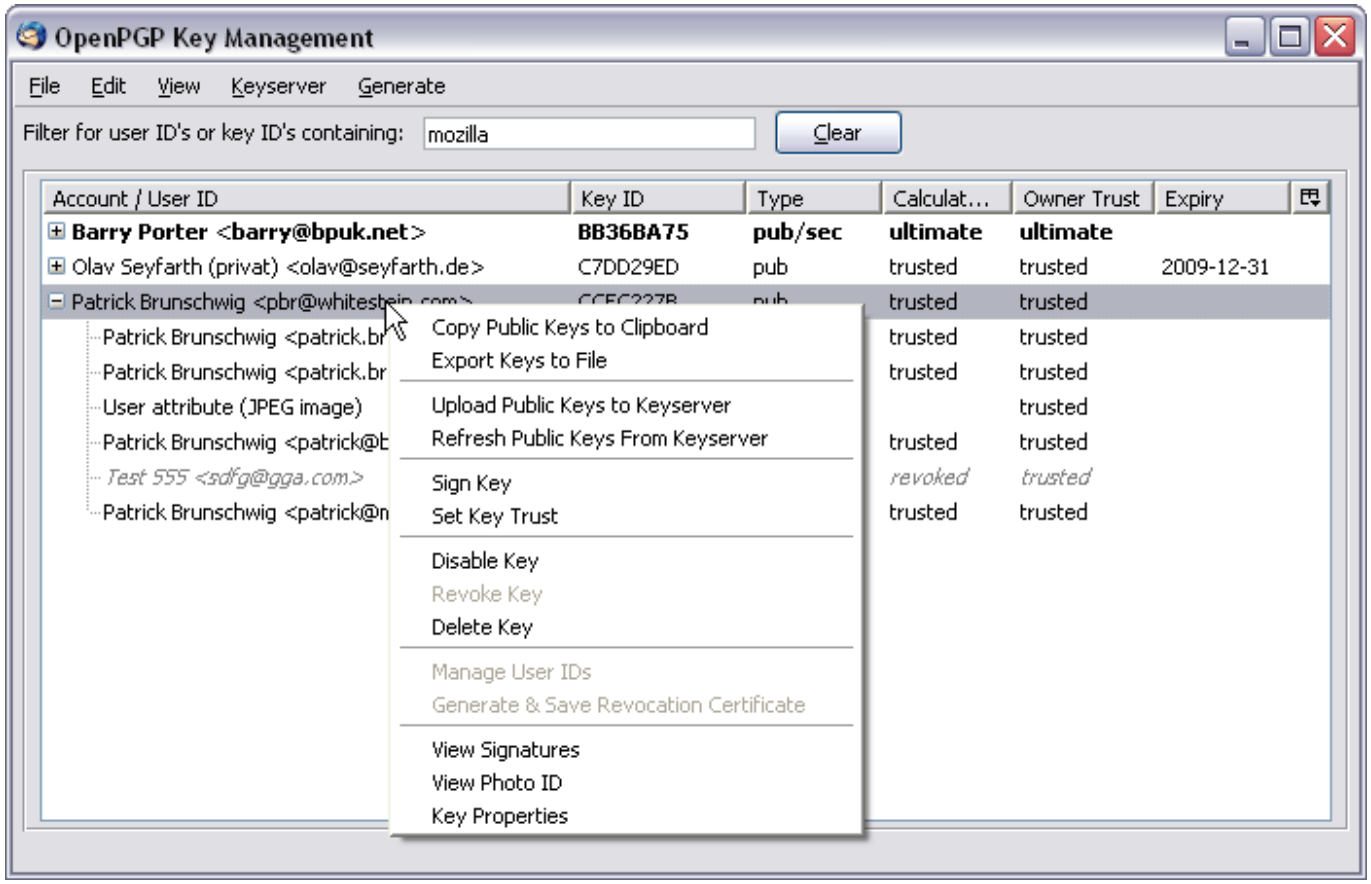
Kan bruges på alle de gængse operativsystemer

Enigmail - GPG plugin til Mail



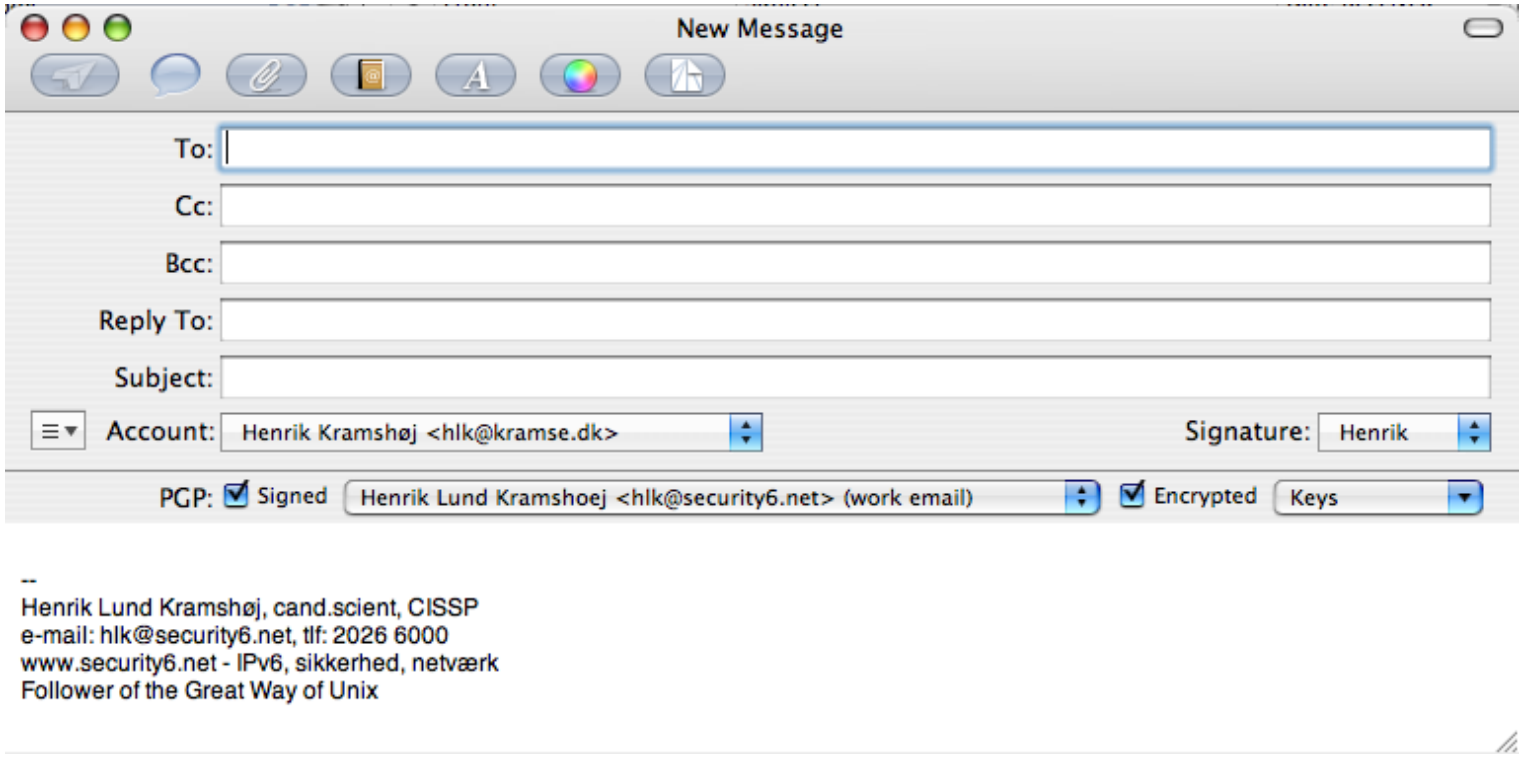
- Enigmail er en udvidelse til
- mailklienten i Mozilla/Netscape
- standalone mailklienten Thunderbird
- Billede fra `http://enigmail.mozdev.org`

Enigmail - OpenGPG Key Manager



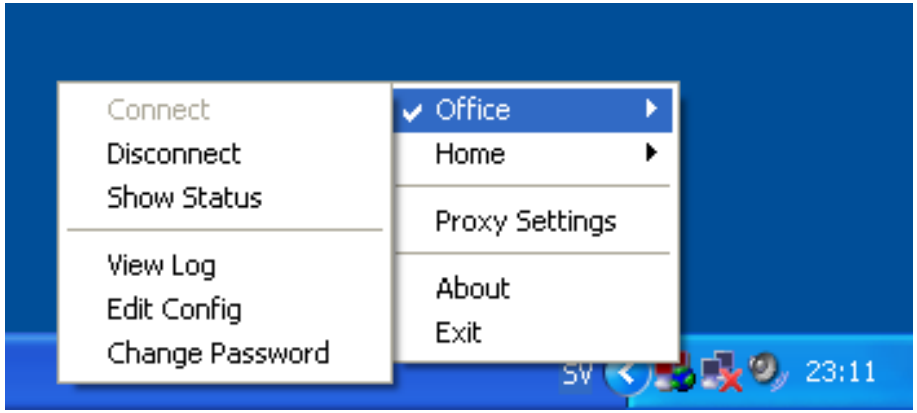
Key Manager funktionaliteten i Enigmail kan anbefales

GPGMail plugin til Mac OS X Mail.app



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

Use VPN!



Virtual Private Networks are **useful** - or even **required when traveling**

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

SSL/TLS VPN - Multiple incompatible vendors: OpenVPN, Cisco, Juniper, F5 Big IP

IETF IPsec does work cross-vendors - sometimes, and is also increasingly becoming blocked or unusable due to NAT :-(

Note: your VPN provider may be forced to give up your identity and traffic, beware!

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`

SOLIDO NETWORKS

Objective:

Specify mechanisms and techniques that allow Internet applications to establish cryptographically secured communications by using information distributed through DNSSEC for discovering and authenticating public keys which are associated with a service located at a domain name.

DNS-based Authentication of Named Entities (dane)

`https://datatracker.ietf.org/wg/dane/charter/`

`http://googleonlinesecurity.blogspot.dk/2011/04/improving-ssl-certificate-security.html`

DNSSEC er ved at være godt udbredt - undtagen i DK

(findes på .dk zonen, men næsten ingen resolvere)

Censurfridns.dk uncensoredDNS

```
http://www.censurfridns.dk

www.censurfridns.dk

Welcome to www.censurfridns.dk. You are welcome to use:

anycast.censurfridns.dk / 91.239.100.100 / 2001:67c:28a4::
ns1.censurfridns.dk / 89.233.43.71 / 2002:d596:2a92:1:71:53::
as a resolver to avoid DNS censorship.
Please see blog.censurfridns.dk/en for more information.
```

Det er uacceptabelt at pille ved DNS - punktum!

DNSSEC trigger

Der findes mange DNSSEC programmer, blandt andet DNSSEC-trigger som er en navneserver til din lokale PC

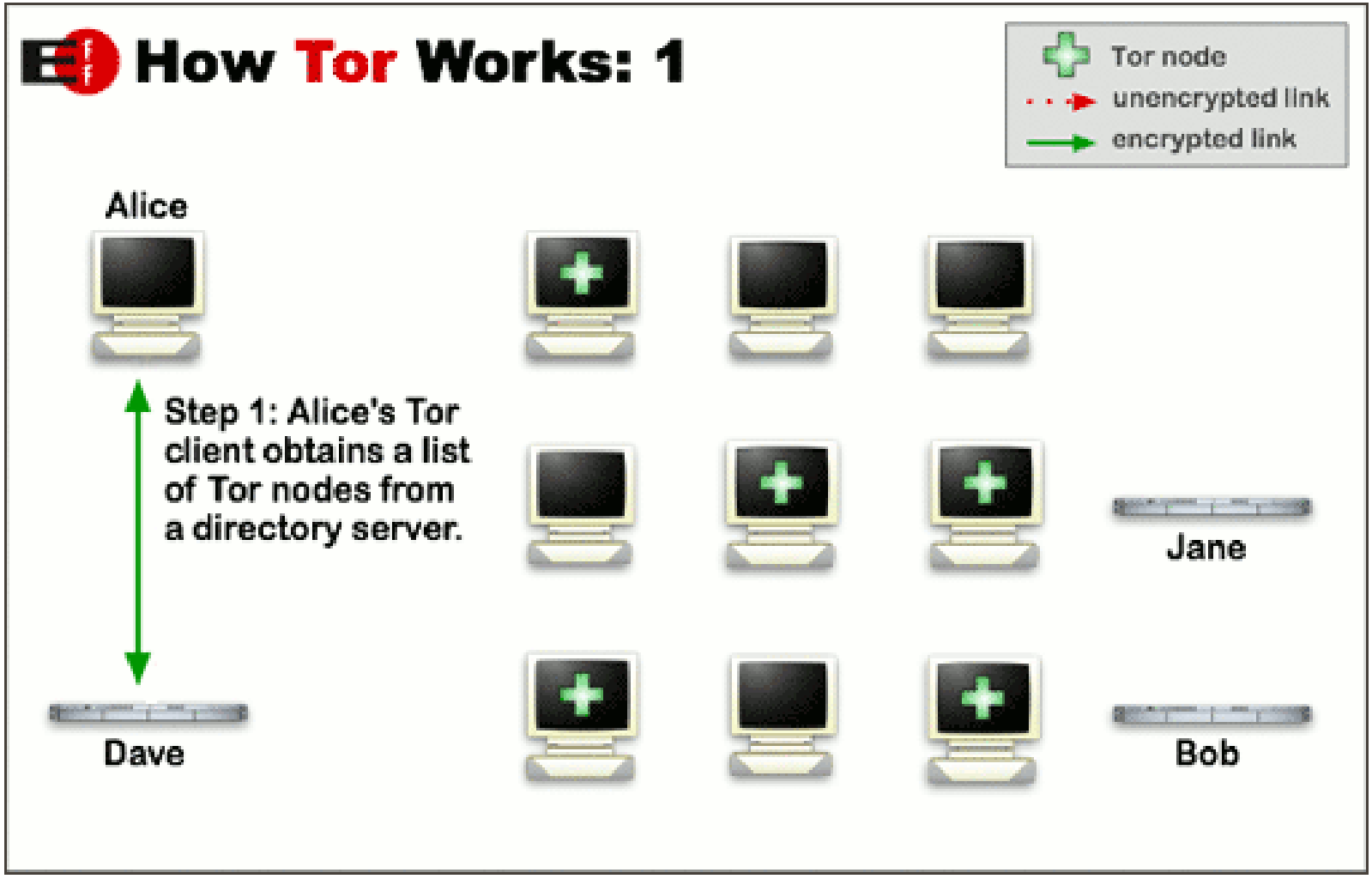
- DNSSEC Validator for firefox
  `https://addons.mozilla.org/en-us/firefox/addon/dnssec-validator/`
- OARC tools `https://www.dns-oarc.net/oarc/services/odvr`
- `http://www.nlnetlabs.nl/projects/dnssec-trigger/`

Tor project

`https://www.torproject.org/`

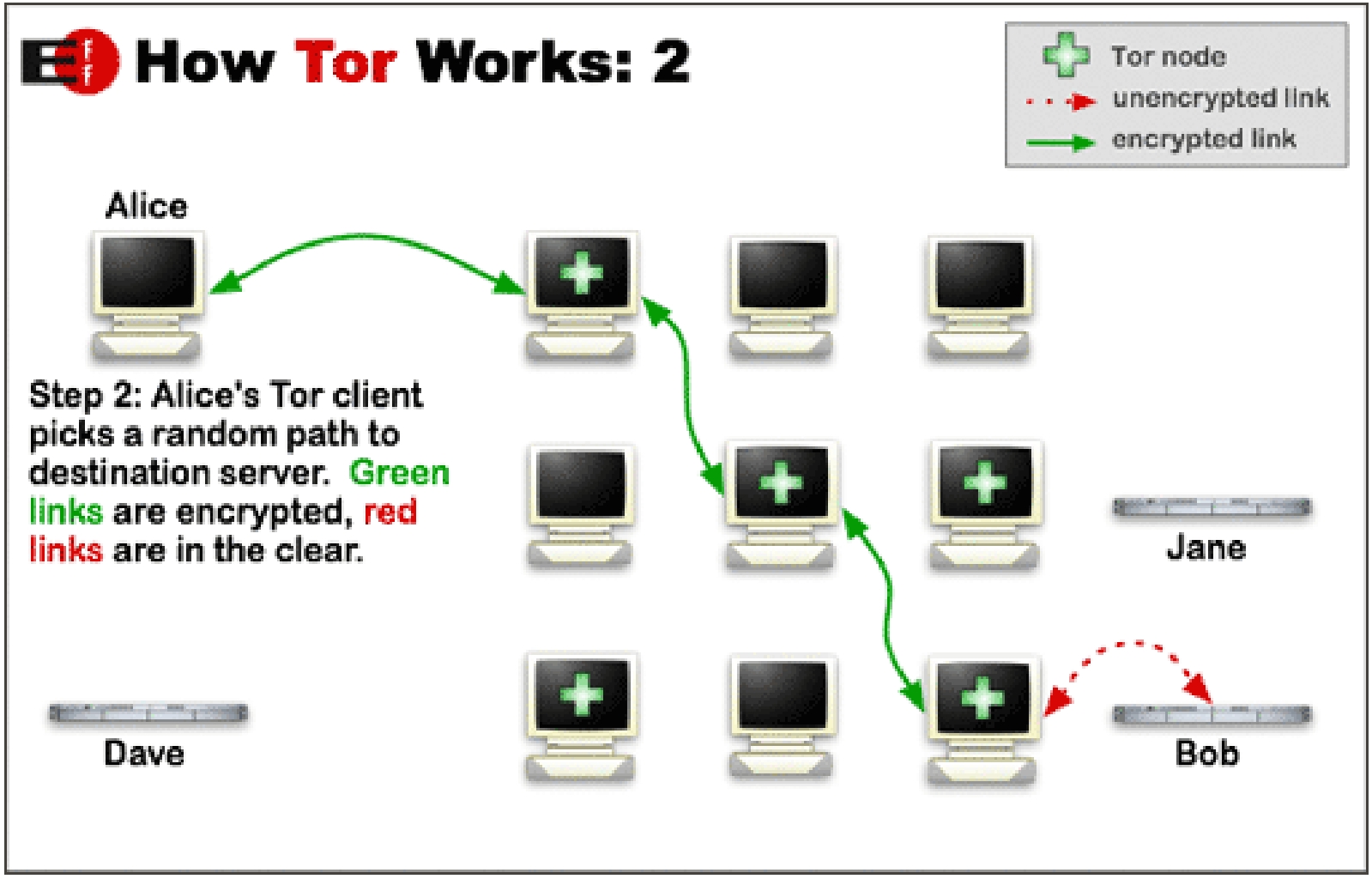
Der findes alternativer, men Tor er mest kendt

Tor project - how it works 1



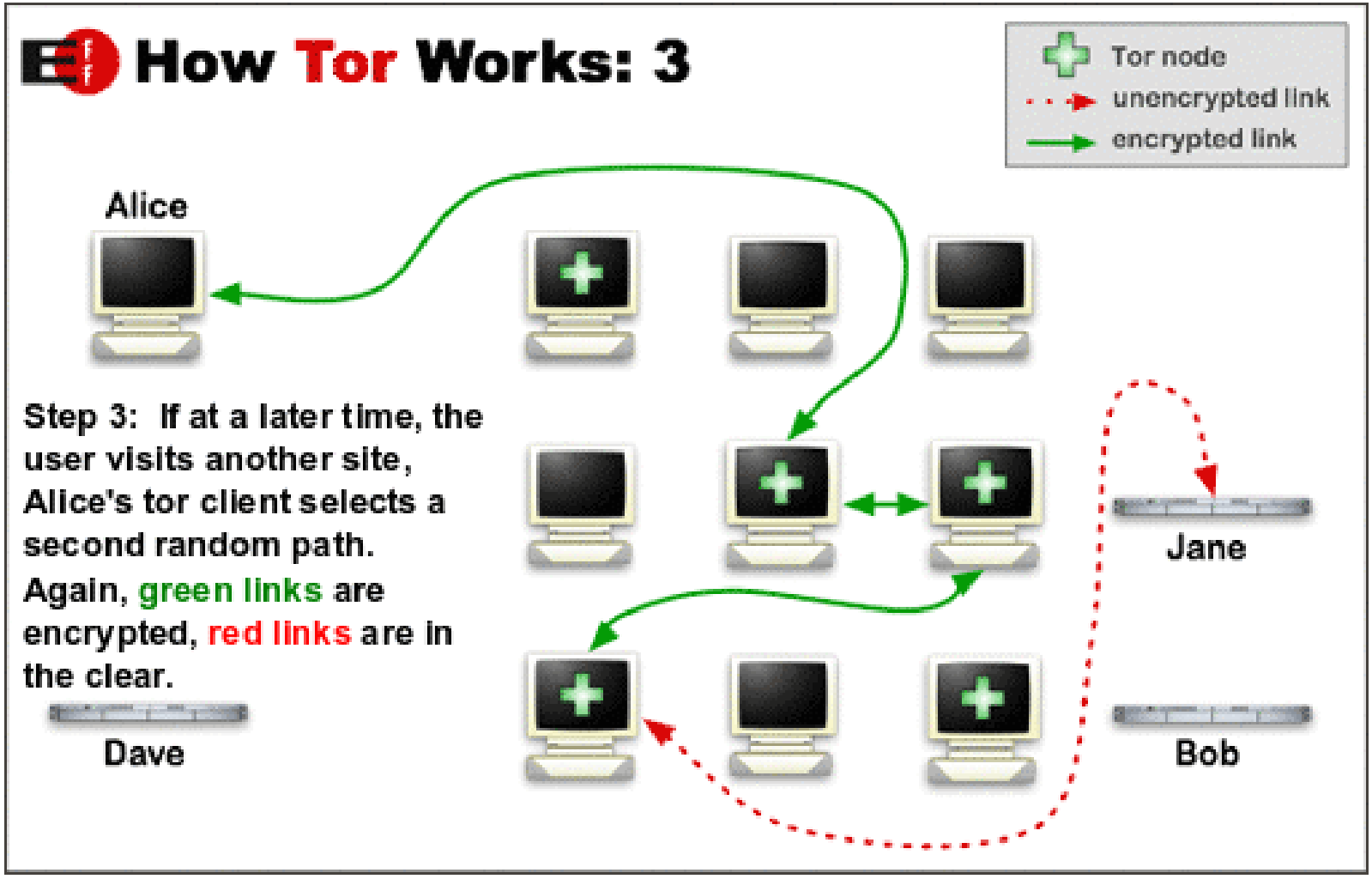
pictures from `https://www.torproject.org/about/overview.html.en`

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`

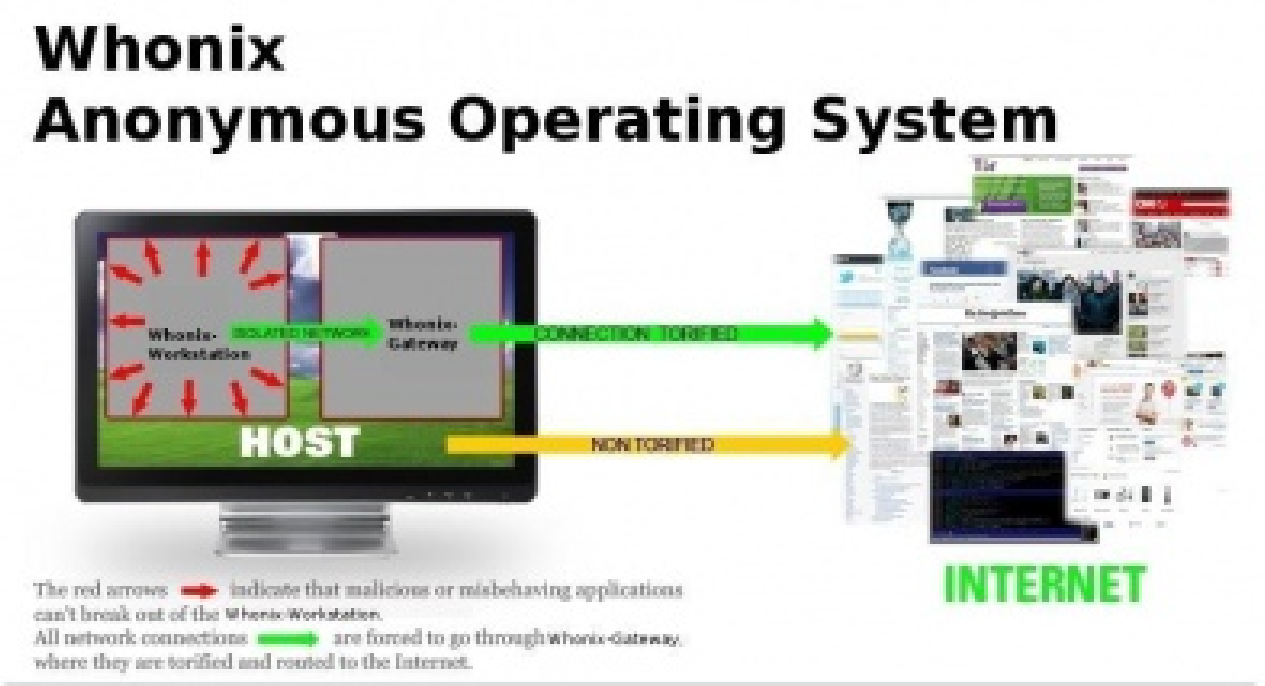
Tor project install

Der findes diverse tools til Tor, Torbutton on/off knap til Firefox osv.

Det anbefales at bruge bundles fra `https://www.torproject.org/`

Pause mens dem som vil installere gør det

Whonix



Whonix is an operating system focused on anonymity, privacy and security. It's based on the Tor anonymity network[5], Debian GNU/Linux[6] and security by isolation. DNS leaks are impossible, and not even malware with root privileges can find out the user's real IP.

`https://www.whonix.org/`

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`

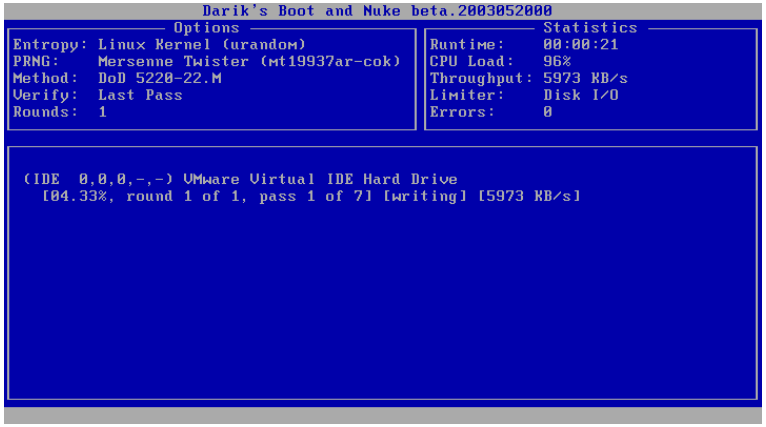
TASK kan betragtes som en erstatning for TCT the coroners toolkit lavet af Dan Farmer og Wietse Venema

Autopsy er en Forensic Browser - et interface til TASK

Hvordan slettes data

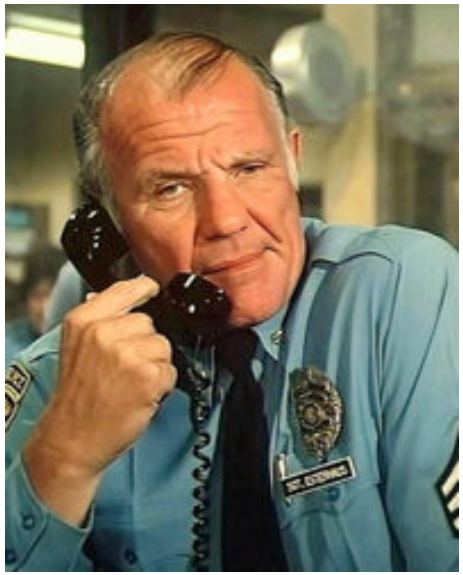
- Filsystemer skal være hurtige - skal ikke lave unødvendige operationer
- En harddisk er en fysisk disk med en arm der skal bevæges og et læse/skrivehoved som skal tændes og slukkes
- Hvis man kan undgå at skulle skrive over hele filen ved sletning er det hurtigere
- De fleste operativsystemer sletter 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

Darik's Boot and Nuke



- ad-hoc oprydning, formatering og sletning af filer giver ingen sikkerhed!
- 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/`
- NB: Brug `http://unetbootin.sourceforge.net/` til at skrive CD-image til

Be careful



Hey, Lets be careful out there!

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

Nødvendigt eller er det ekstreme teknikker vi har diskuteret?

Pause

Er det tid til en lille pause?

Informationsindsamling

Det vi har udført er informationsindsamling

Indsamlingen kan være aktiv eller passiv indsamling i forhold til målet for angrebet

passiv kunne være at lytte med på trafik eller søge i databaser på Internet

aktiv indsamling er eksempelvis at sende ICMP pakker og registrere hvad man får af svar

MAC adresser

```
00-03-93    (hex)          Apple Computer, Inc.
000393      (base 16)      Apple Computer, Inc.
                           20650 Valley Green Dr.
                           Cupertino CA 95014
                           UNITED STATES
```

Netværksteknologierne benytter adresser på lag 2

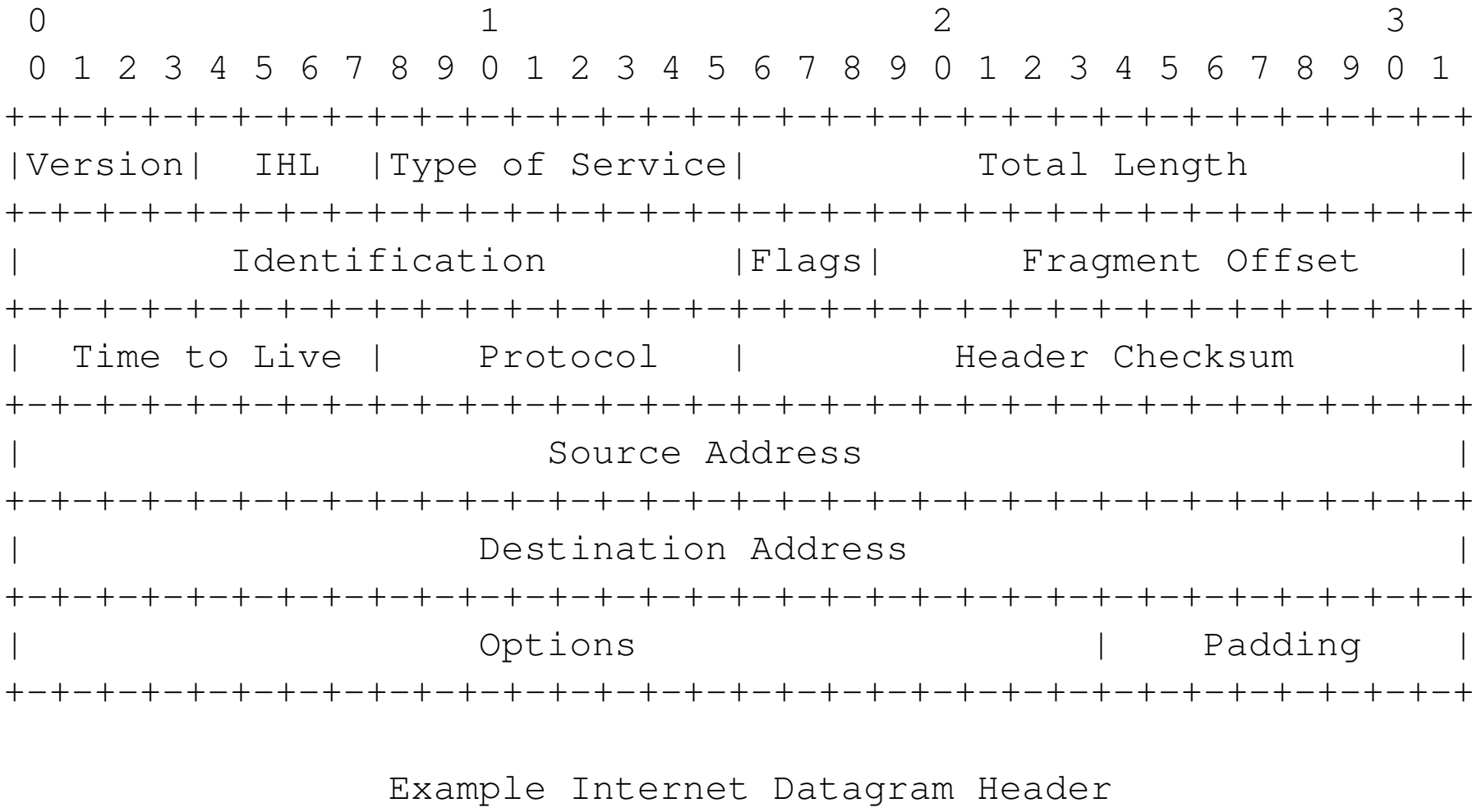
Typisk svarende til 48-bit MAC adresser som kendes fra Ethernet MAC-48/EUI-48

Første halvdel af adresserne er Organizationally Unique Identifier (OUI)

Ved hjælp af OUI kan man udlede hvilken producent der har produceret netkortet

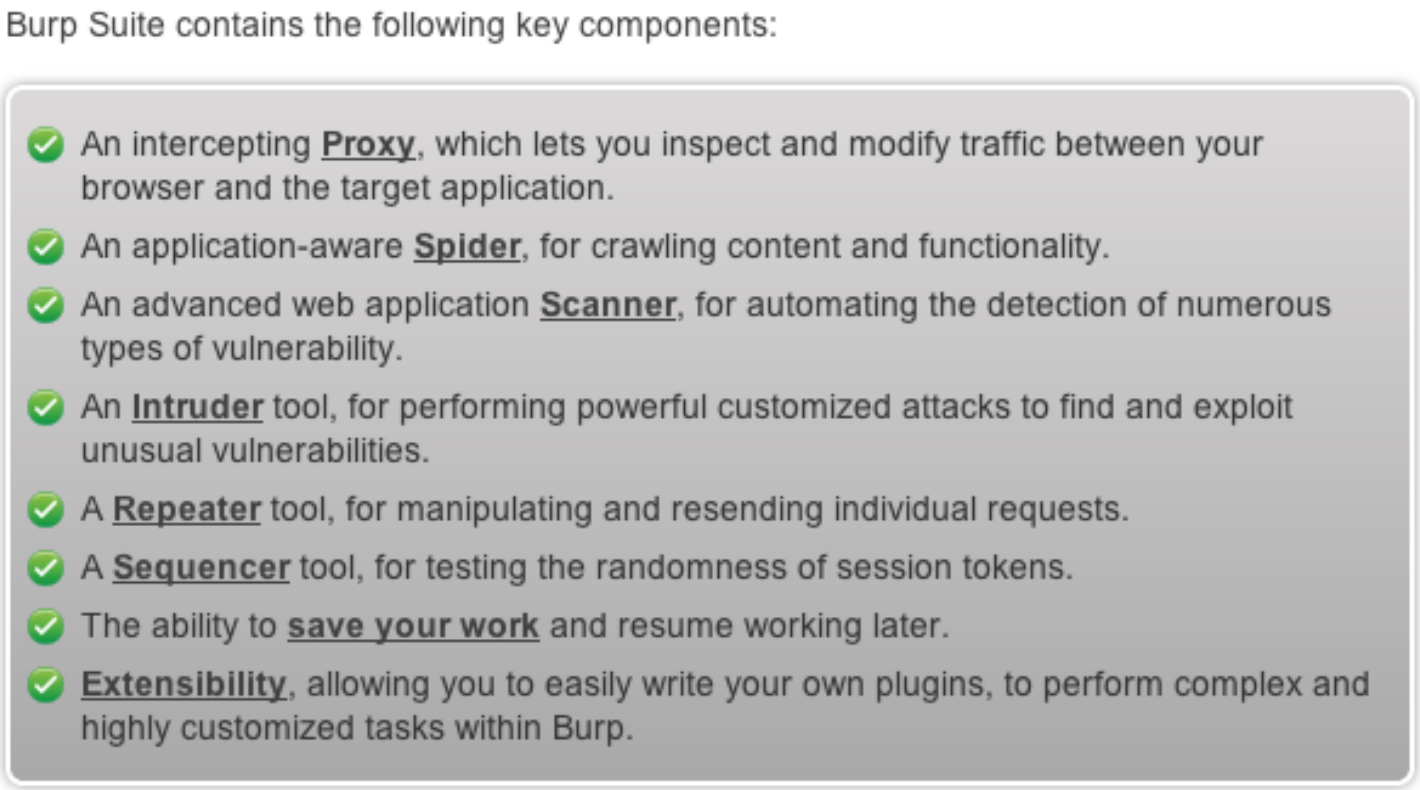
`http://standards.ieee.org/regauth/oui/index.shtml`

IPv4 pakken - header - RFC-791



Example Internet Datagram Header

Burp Suite



Burp Suite af Dafydd Stuttard `http://portswigger.net/burp/`

Twitter @PortSwigger

Burpsuite

SOLIDO NETWORKS

> Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.
>
> Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Burp suite indeholder både proxy, spider, scanner og andre værktøjer i samme pakke - NB: EUR 249 per user per year.

`http://portswigger.net/burp/`

brute force

SOLIDO NETWORKS

hvad betyder bruteforcing?
afprøvning af alle mulighederne

```
Hydra v2.5 (c) 2003 by van Hauser / THC <vh@thc.org>
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]]
[-o FILE] [-t TASKS] [-g TASKS] [-T SERVERS] [-M FILE] [-w TIME]
[-f] [-e ns] [-s PORT] [-S] [-vV] server service [OPT]

Options:
  -S         connect via SSL
  -s PORT    if the service is on a different default port, define it here
  -l LOGIN   or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS    or -P FILE try password PASS, or load several passwords from FILE
  -e ns      additional checks, "n" for null password, "s" try login as pass
  -C FILE    colon seperated "login:pass" format, instead of -L/-P option
  -M FILE    file containing server list (parallizes attacks, see -T)
  -o FILE    write found login/password pairs to FILE instead of stdout
...
```

Følg med Twitter news

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

Work together

Team up!

We need to share security information freely

We often face the same threats, so we can work on solving these together

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`

How to become secure

Dont use computers at all, data about you is still processed by computers :-(

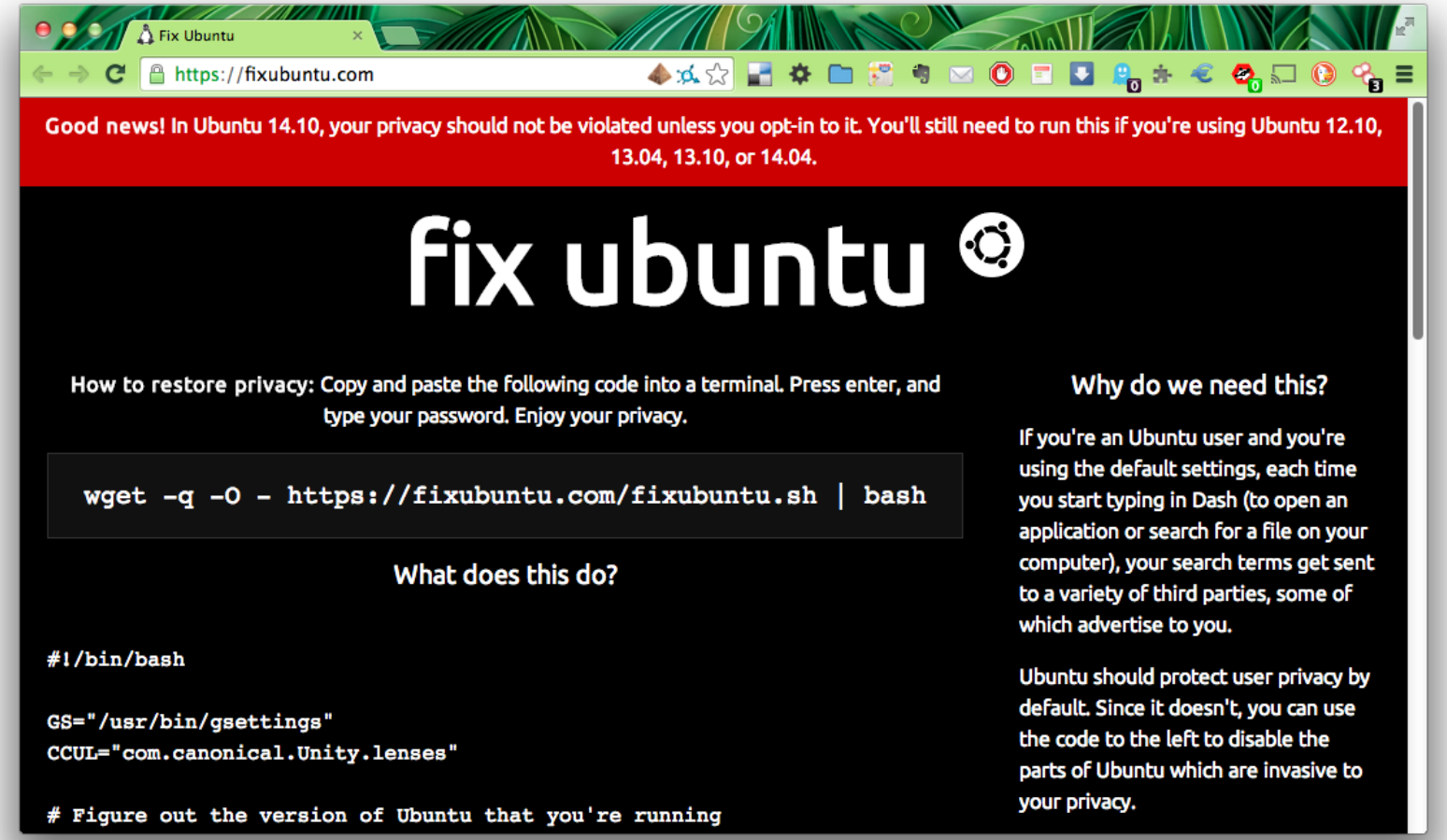
Dont use a single device for all types of data

Dont use a single server for all types of data, mail server != web server

Configure systems to be secure by default, or change defaults

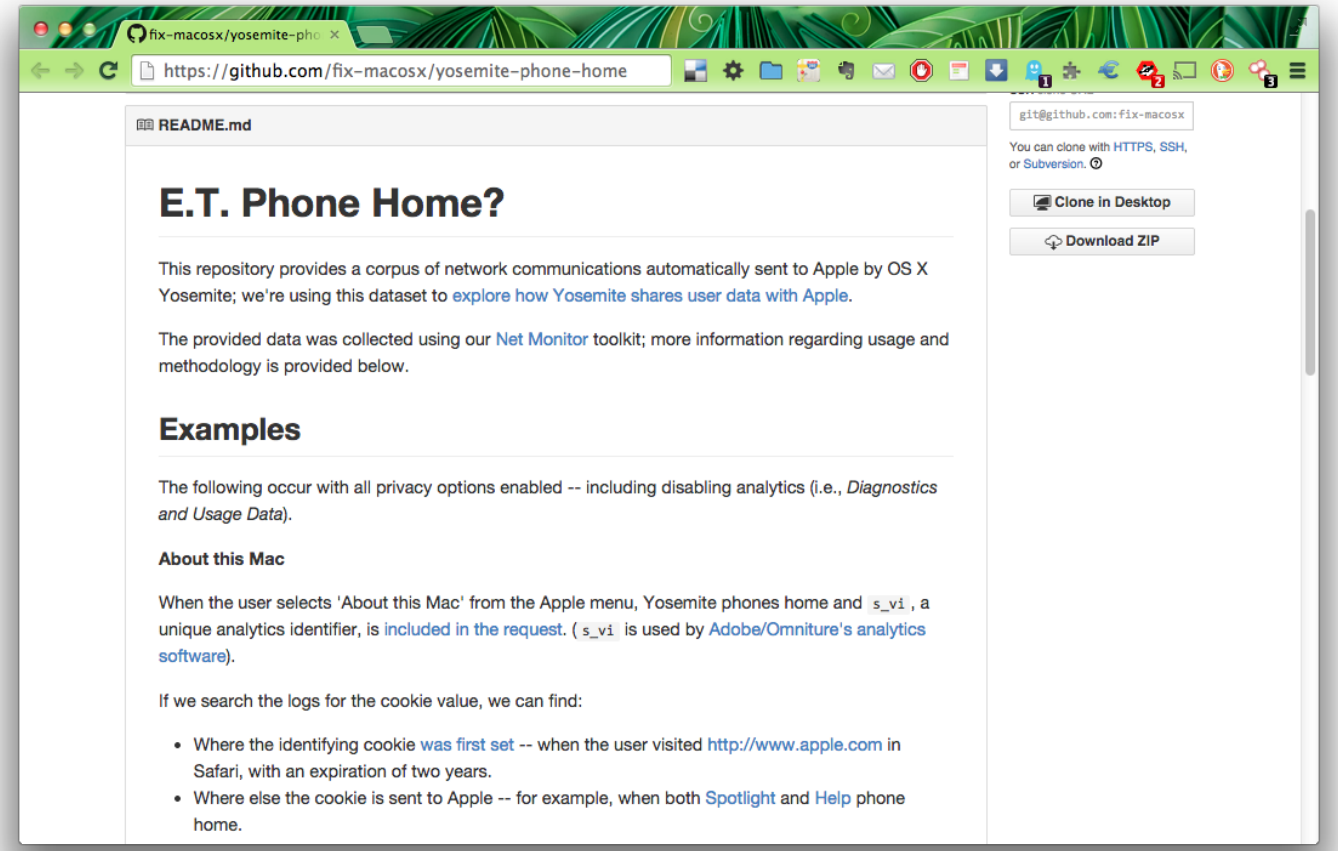
Use secure protocols and VPN solutions

Ubuntu Unity Privacy problems



Source: `https://fixubuntu.com/`

Mac OS X Yosemite - E.T. Phone Home



Source: https://github.com/fix-macosx/yosemite-phone-home

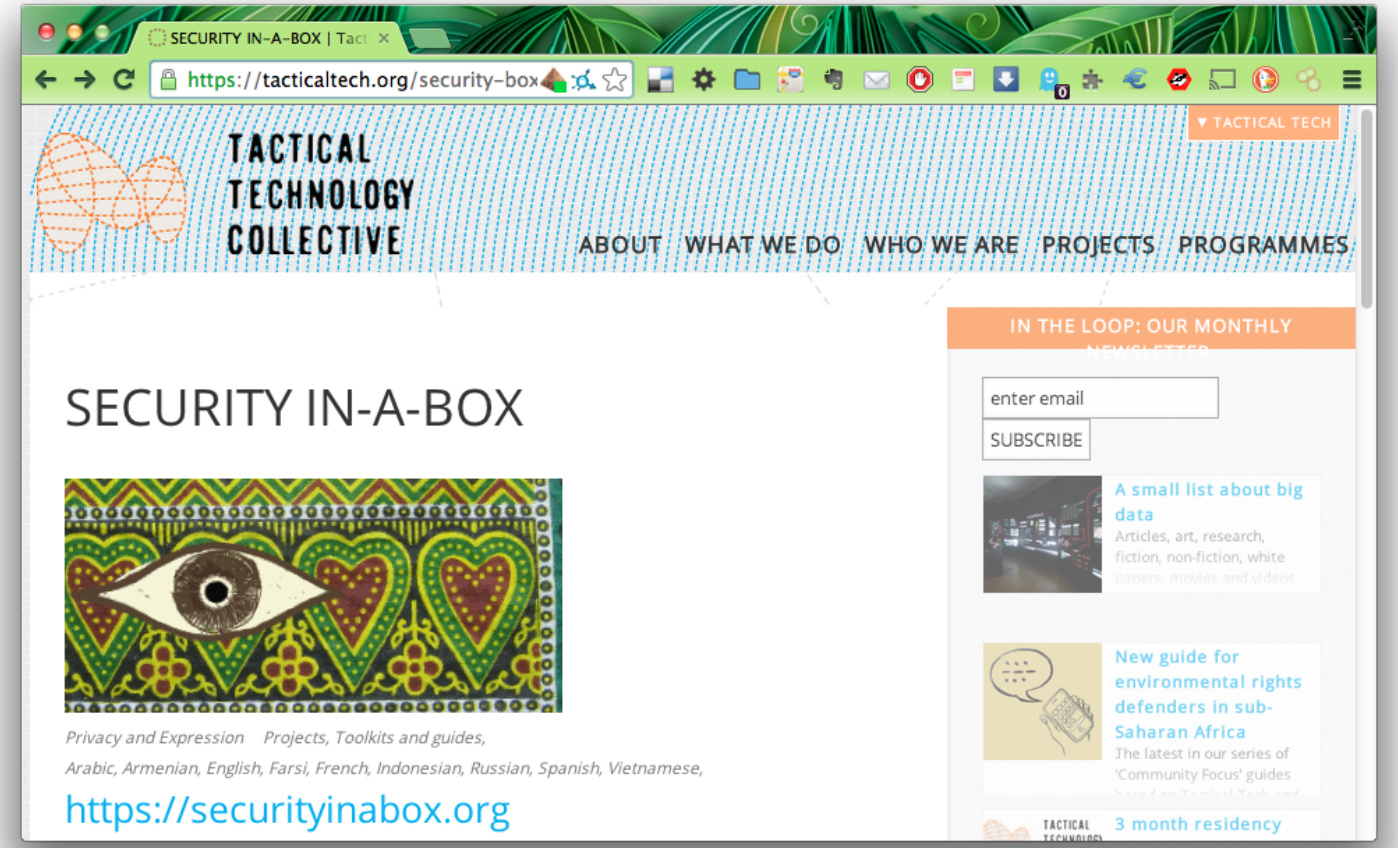
Surveillance Self-Defense EFF

Tips, Tools and How-tos For Safer Online Communications

Modern technology has given the powerful new abilities to eavesdrop and collect data on innocent people. Surveillance Self-Defense is EFF's guide to defending yourself and your friends from surveillance by using secure technology and developing careful practices.

Source: `https://ssd.eff.org/`

Ononymous robot, formerly ONO robot

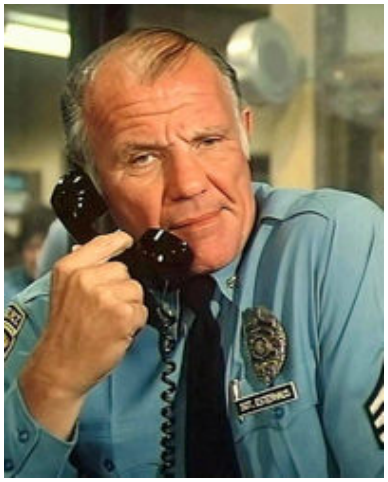


Source: `https://tacticaltech.org/`

Checklisten

- BIOS kodeord, lock-codes for mobile devices
- Firewall - specifically for laptops
- Two browser strategy, one with paranoid settings
- Use OpenPGP for email
- Use a password safe for storing passwords
- Use hard drive encryption
- Keep systems updated
- Backup your data
- Dispose of data securely

Be careful - questions?



Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

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

PROSA CTF

PROSA afholder CTF konkurrence fredag den 29. november 13 til lørdag

Capture the Flag er en mulighed for at afprøve sine hackerskillz

Distribueret CTF med hold Sjovt og lærerigt

Kilde: `http://prosa-ctf.the-playground.dk/`

Get ready! Lær debuggere, perl, java at kende, start på at hacke

Det korte svar - drop diskussionen

Det havde oprindeligt en anden betydning, men medierne har taget udtrykket til sig - og idag har det begge betydninger.

Idag er en hacker stadig en der bryder ind i systemer!

ref. Spafford, Cheswick, Garfinkel, Stoll, ... - alle kendte navne indenfor sikkerhed

- *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Clifford Stoll
- *Hackers: Heroes of the Computer Revolution*, Steven Levy
- *Practical Unix and Internet Security*, Simson Garfinkel, Gene Spafford, Alan Schwartz

Definition af hacking, oprindeligt

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

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

Kilde: Peter Makholm, `http://hacking.dk`

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