

Welcome to

Overvågning og hacking

PROSA Stud Svendborg 2014

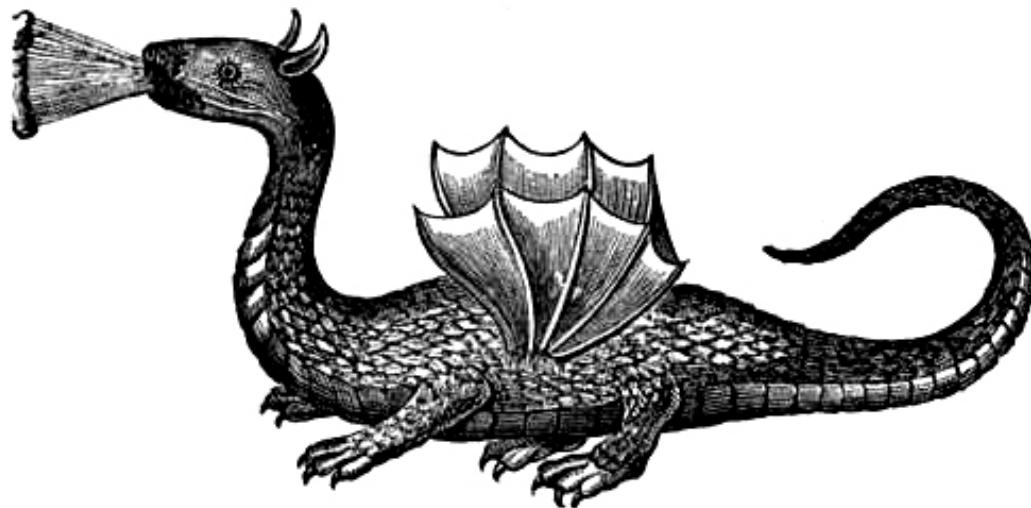
Henrik Lund Kramshøj, internet samurai
hlk@solidonetworks.com

<http://www.solidonetworks.com>

Parallelia

Airport til snif netværk

Internet - Here be dragons



KI 11:30-13:00

Paranoia defined

What are the risks, vulnerabilities and threats

Reduce risk and mitigate impact



Jacob Appelbaum @iocerror

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 færdens og kryptografi er en fredelig protest mod indsamling af data.



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



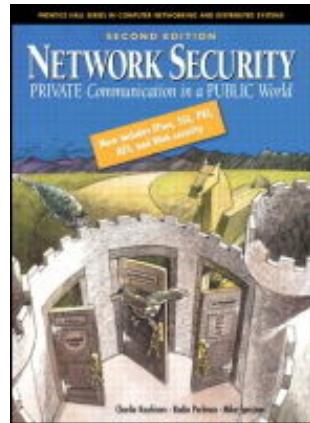
Think security, it may seem like magic - but it is not

Follow news about security

Support communities, join and learn



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

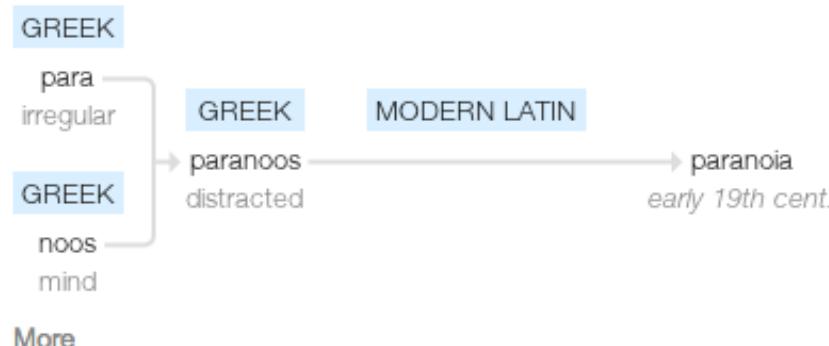
/parə'noiə/ ⓘ

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



Source: google paranoia definition

From the definition of paranoia:

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
- Governments 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!

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>

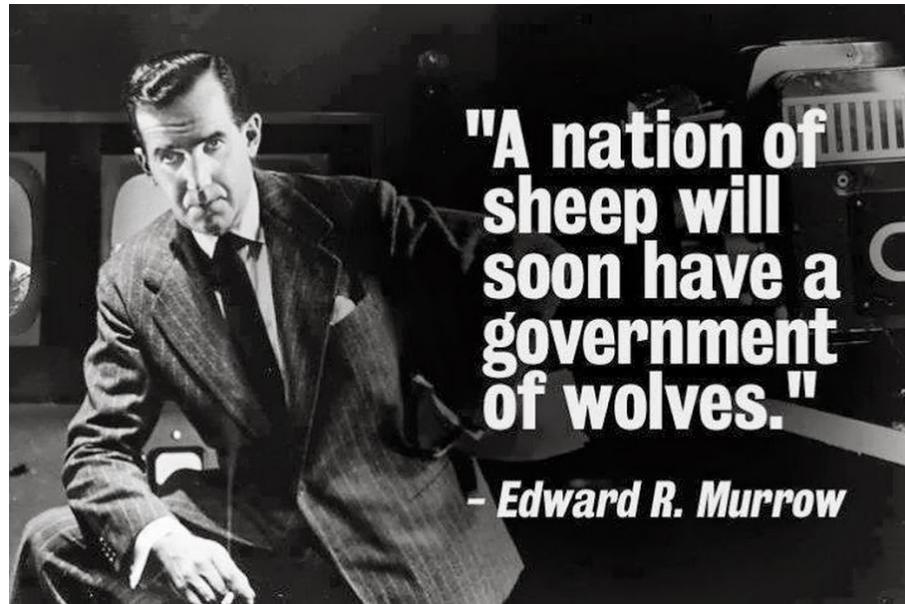
(Reuters) - British authorities came under pressure on Monday to explain why anti-terrorism powers were used to detain for nine hours the partner of a journalist who has written articles about **U.S. and British surveillance programs** based on **leaks from Edward Snowden**.

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_\(surveillance_program\)](http://en.wikipedia.org/wiki/PRISM_(surveillance_program))

Governments also implementing censorship, including danish gov.

Outlaw and/or discredit crypto, google: FBI director James Comey

Go after Tor exit nodes and their operators :-(



Investigative organizations, like europol, FBI and other want a "golden key" which they can get with a court order. This cant happen! This wont work. See below link, and Google: clipper chip and crypto wars

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.

Source: https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html



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 ☺



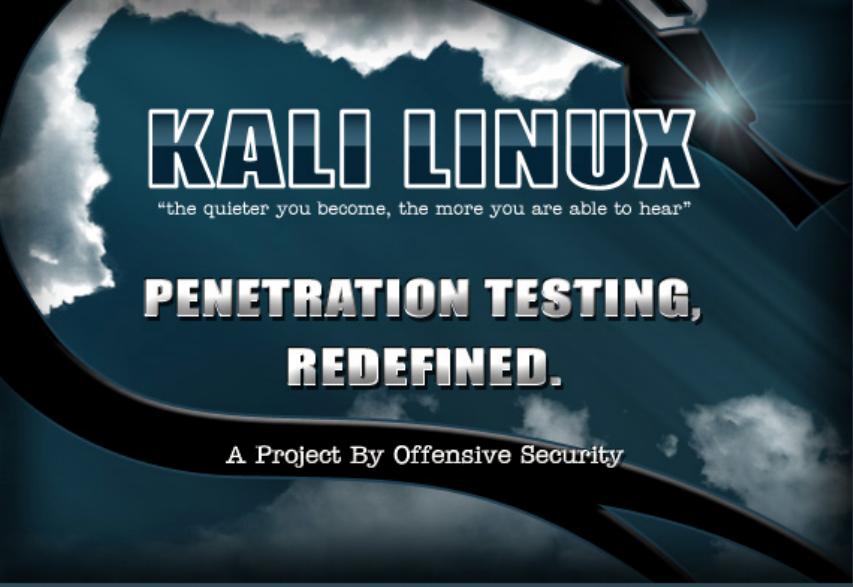
- Nmap, Nping - tester porte, godt til firewall admins <http://nmap.org>
- Metasploit Framework gratis på <http://www.metasploit.com/>
- Wireshark avanceret netværkssniffer - <http://www.wireshark.org/>
- Burpsuite <http://portswigger.net/burp/>
- Skipfish <http://code.google.com/p/skipfish/>
- OpenBSD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

Kilde: Angelina Jolie fra Hackers 1995

Kali Linux the new backtrack

The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - What's new ?



KALI LINUX
"the quieter you become, the more you are able to hear"

**PENETRATION TESTING,
REDEFINED.**

A Project By Offensive Security

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

Kali <http://www.kali.org/>

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

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.

<http://www.metasploit.com/>

Armitage GUI fast and easy hacking for Metasploit

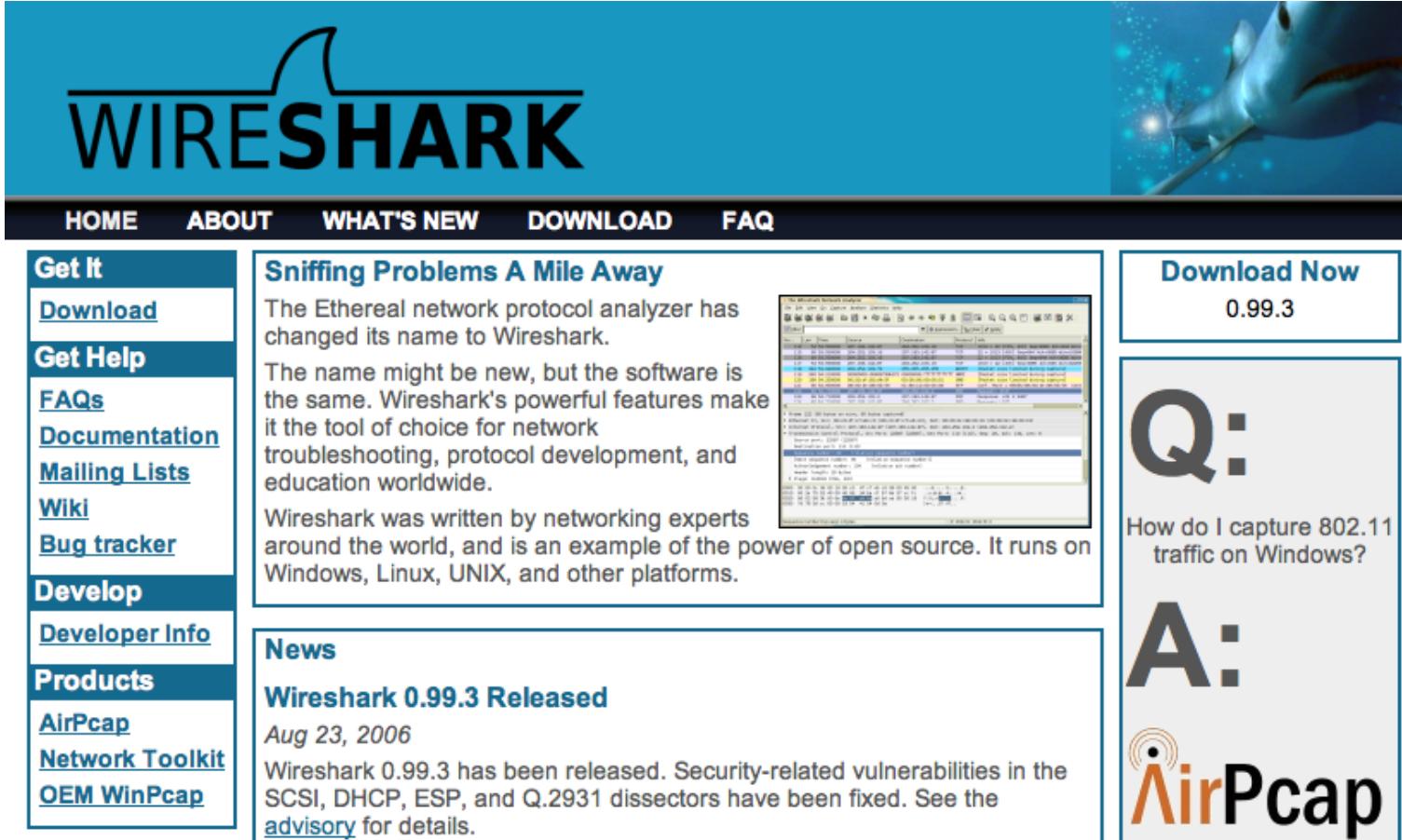
<http://www.fastandeasyhacking.com/>

Kursus Metasploit Unleashed

http://www.offensive-security.com/metasploit-unleashed/Main_Page

Bog: Metasploit: The Penetration Tester's Guide, No Starch Press

ISBN-10: 159327288X



The screenshot shows the official Wireshark website. At the top, there's a large blue header with the "WIRESHARK" logo. Below it is a black navigation bar with links for HOME, ABOUT, WHAT'S NEW, DOWNLOAD, and FAQ. To the right of the navigation is a background image of a shark swimming in water. On the left side, there's a sidebar with a dark blue background containing links under categories like "Get It", "Get Help", "Develop", and "Products". The main content area has several sections: one about name changes, news about the 0.99.3 release, and a Q&A section about capturing 802.11 traffic.

Sniffing Problems A Mile Away

The Ethereal network protocol analyzer has changed its name to Wireshark.

The name might be new, but the software is the same. Wireshark's powerful features make it the tool of choice for network troubleshooting, protocol development, and education worldwide.

Wireshark was written by networking experts around the world, and is an example of the power of open source. It runs on Windows, Linux, UNIX, and other platforms.

News

Wireshark 0.99.3 Released

Aug 23, 2006

Wireshark 0.99.3 has been released. Security-related vulnerabilities in the SCSI, DHCP, ESP, and Q.2931 dissectors have been fixed. See the [advisory](#) for details.

Download Now

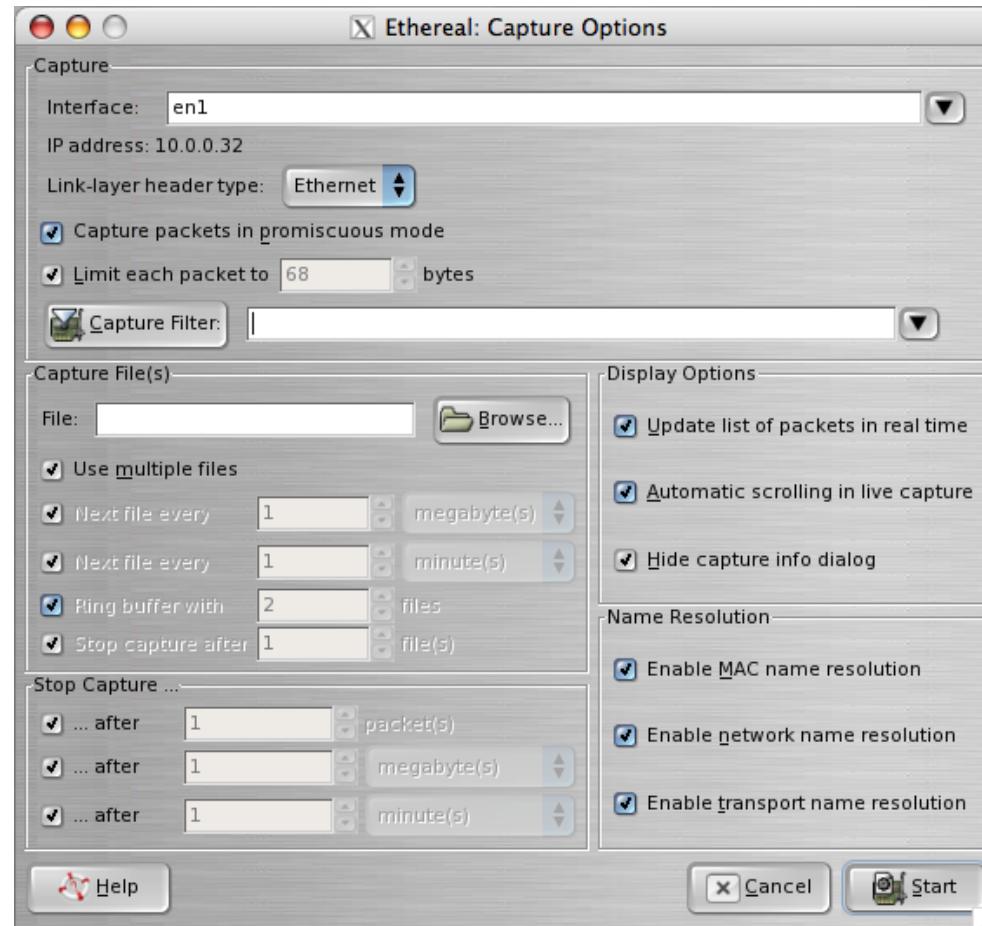
0.99.3

Q:
How do I capture 802.11 traffic on Windows?

A:

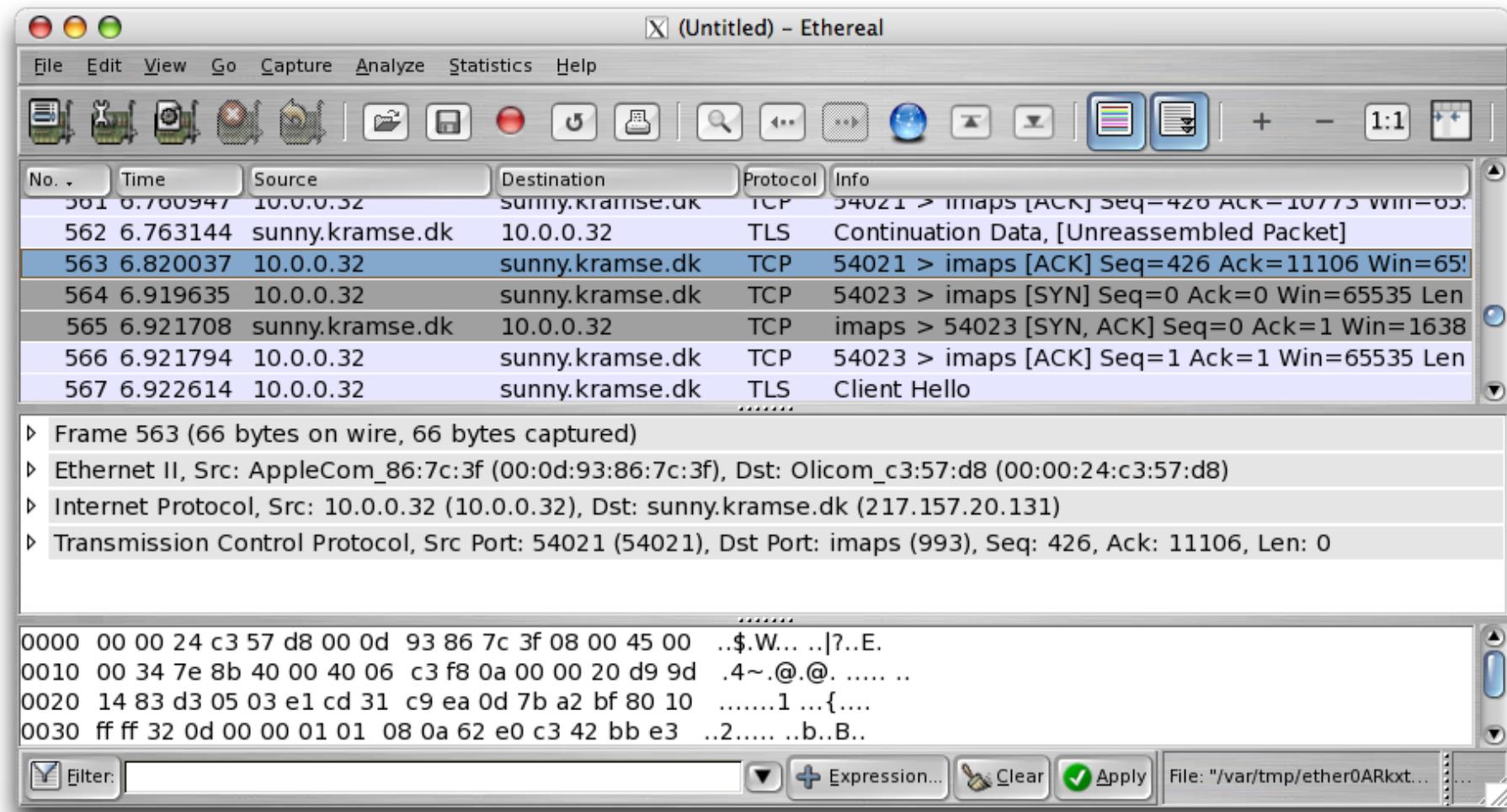

<http://www.wireshark.org>

både til Windows og UNIX, tidligere kendt som Ethereal



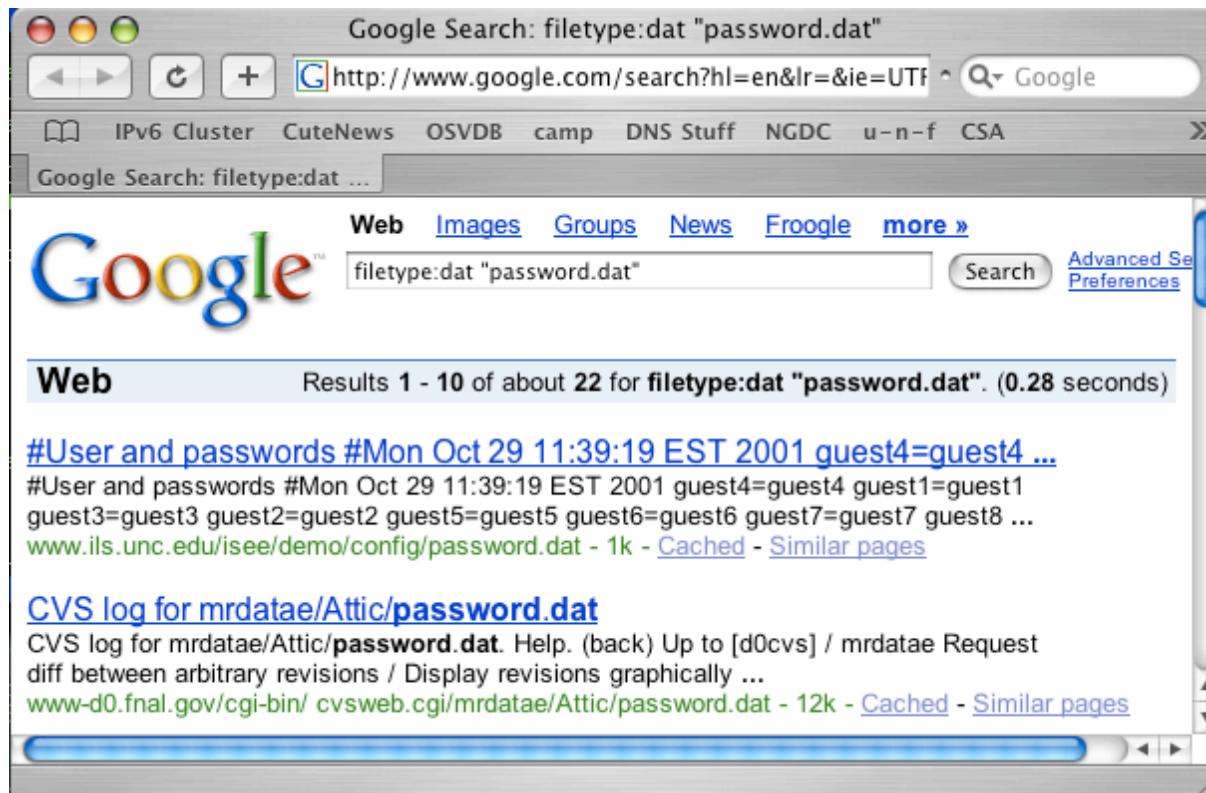
Man starter med Capture - Options

Brug af Wireshark



Læg mærke til filtermulighederne

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://www.exploit-db.com/google-dorks/> Originally from Johnny Long



Hacking ligner indimellem magi



Hacking kræver blot lidt ninja-træning

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

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



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

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

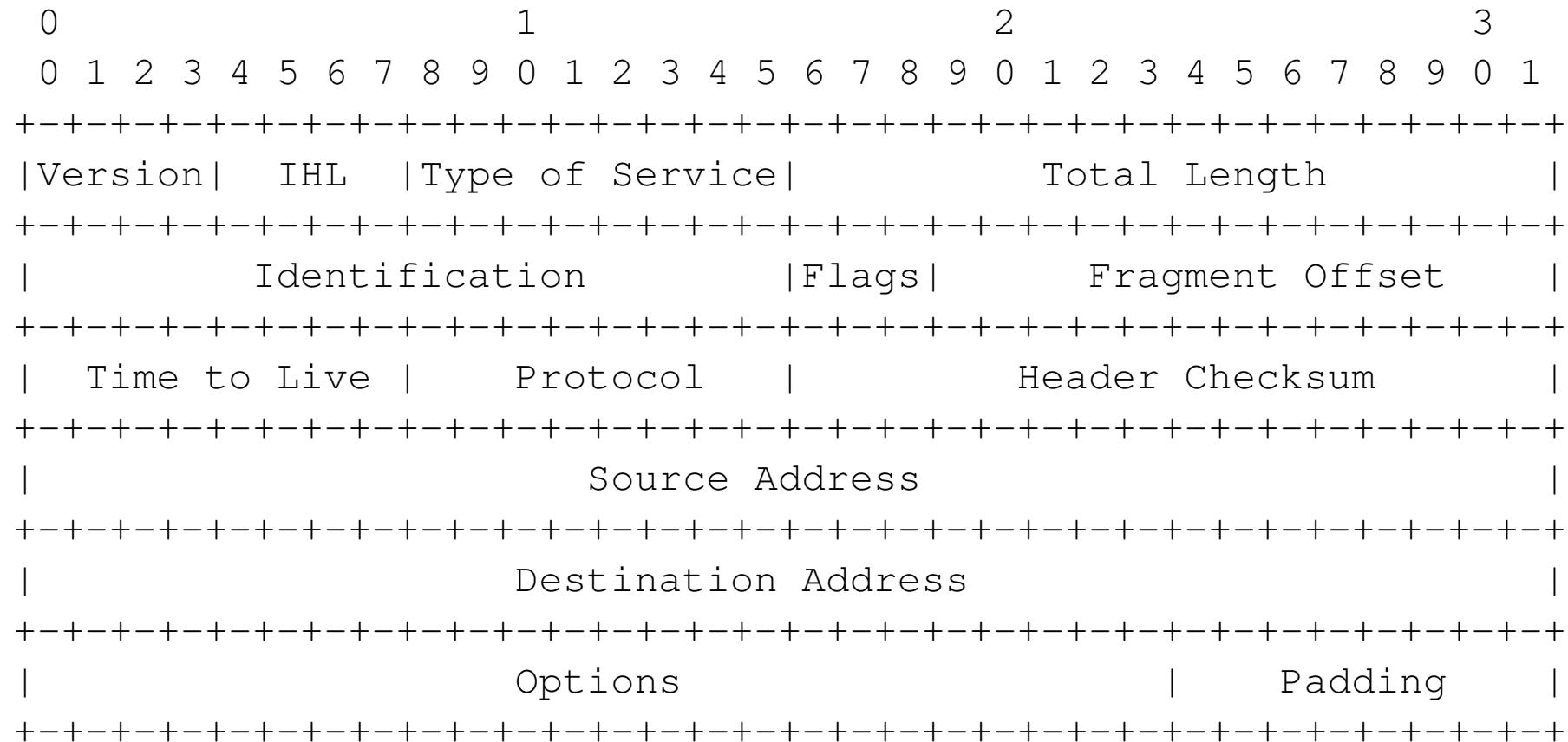
Typisk svarende til 48-bit MAC adresser som kendes fra Ethernet MAC-48/EUI-48

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 contains the following key components:

- ✓ An intercepting Proxy, which lets you inspect and modify traffic between your browser and the target application.
- ✓ An application-aware Spider, for crawling content and functionality.
- ✓ An advanced web application Scanner, for automating the detection of numerous types of vulnerability.
- ✓ An Intruder tool, for performing powerful customized attacks to find and exploit unusual vulnerabilities.
- ✓ A Repeater tool, for manipulating and resending individual requests.
- ✓ A Sequencer tool, for testing the randomness of session tokens.
- ✓ The ability to save your work and resume working later.
- ✓ Extensibility, allowing you to easily write your own plugins, to perform complex and highly customized tasks within Burp.

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

Twitter @PortSwigger

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/>

Demo investigating the current network

Old skool tools: dsniff

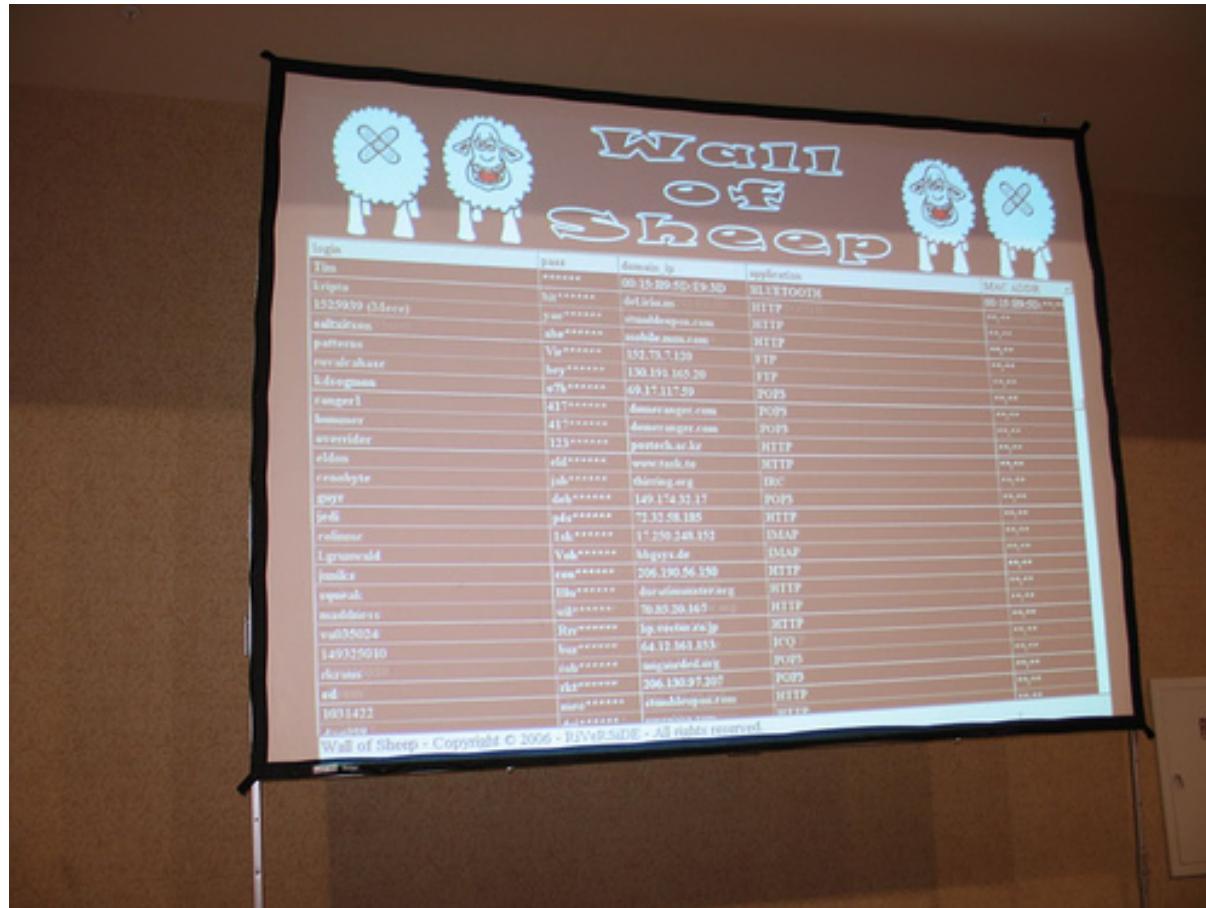
one sniffer for old protocols includes **arpspoof**

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



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

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 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/>

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

Accounting is important

Detecting DoS/DDoS and problems is essential

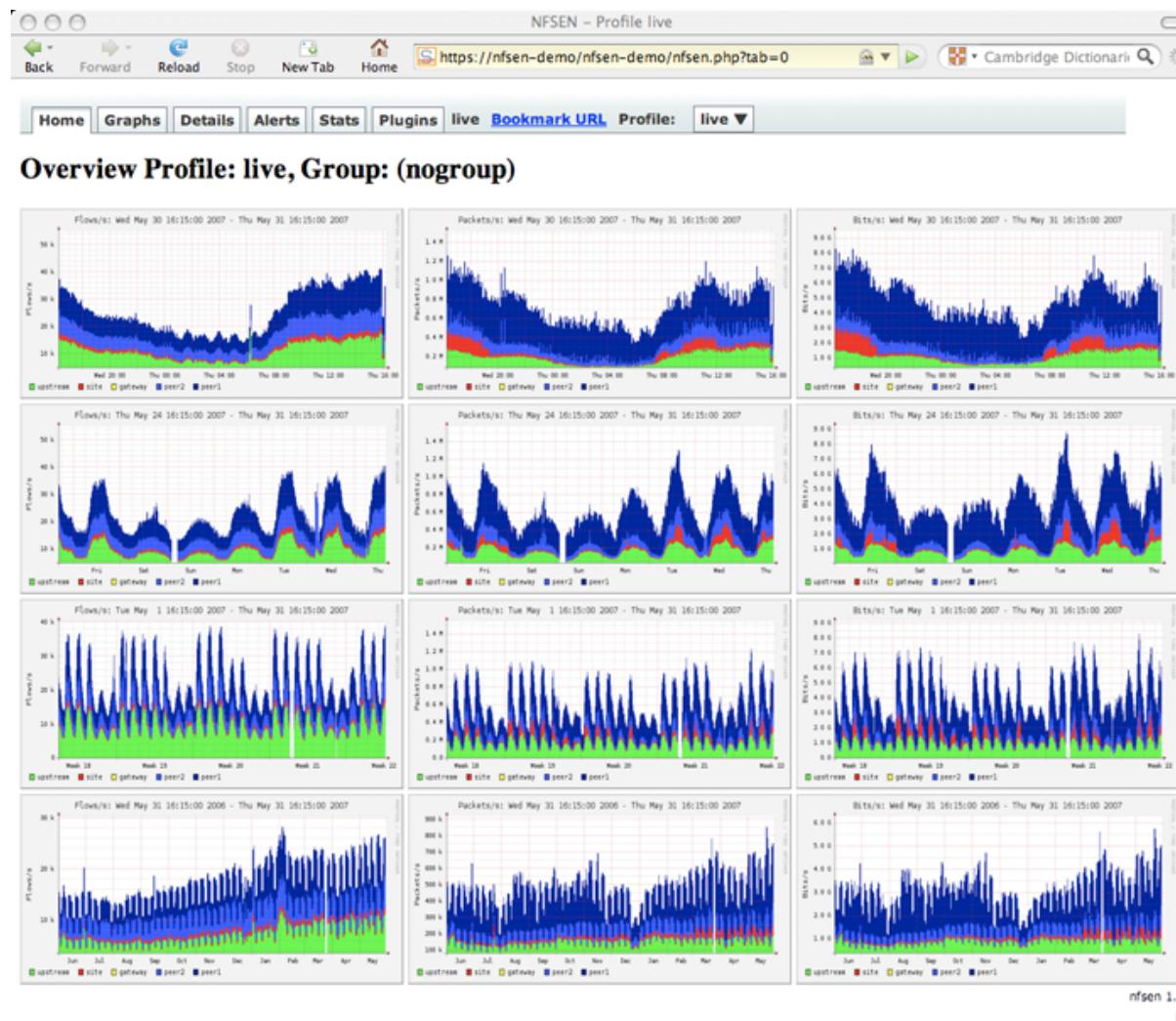
Netflow sampling is vital information - 123Mbit, but what kind of traffic

We use mostly NFSen, but are looking at various software packages

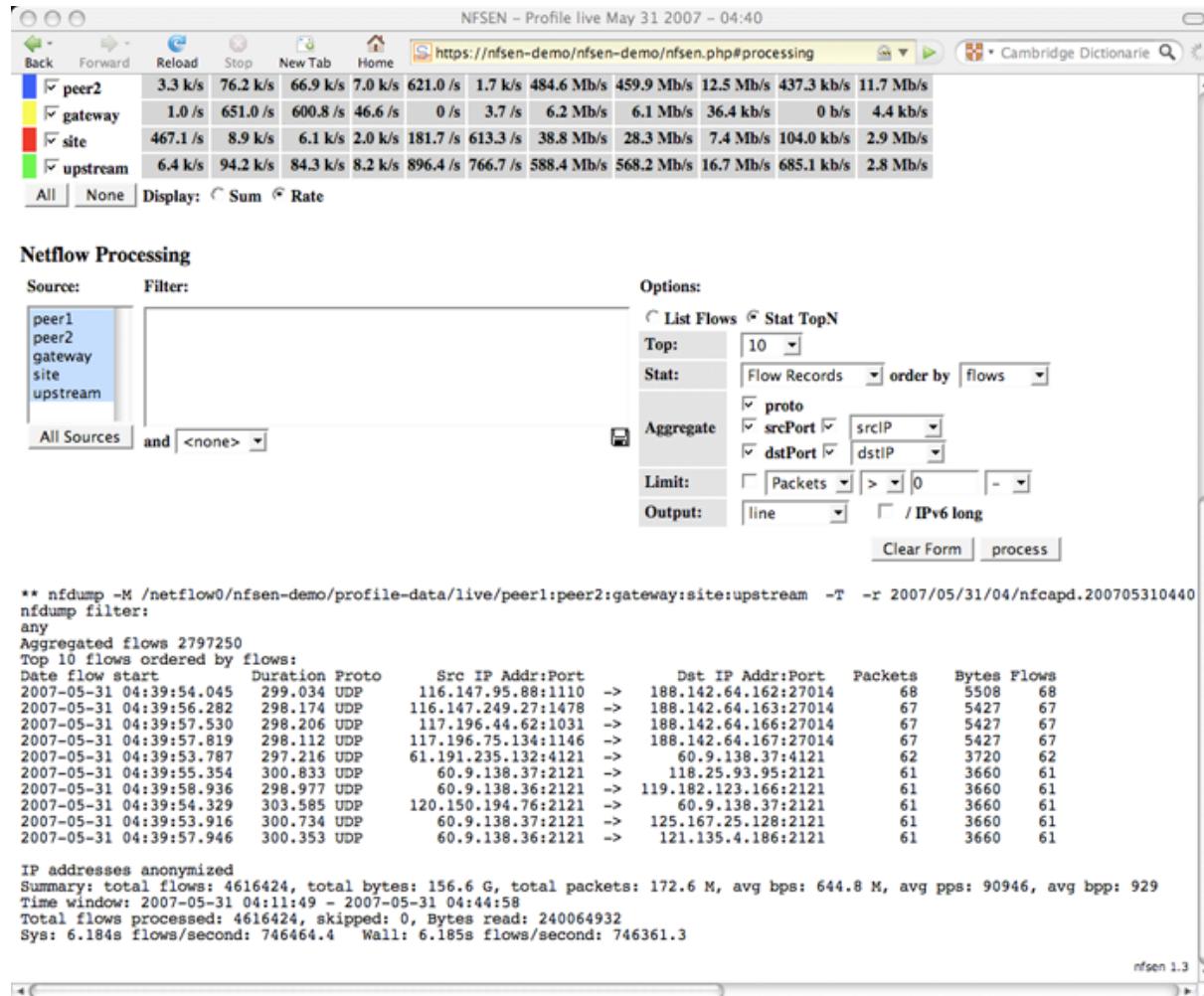
<http://nfsen.sourceforge.net/>

Currently also investigating sFlow - hopefully more fine grained

Netflow using NFSEN



Netflow processing from the web interface



The screenshot shows the NFSEN web interface with the following details:

- Header:** NFSEN - Profile live May 31 2007 - 04:40, URL: https://nfsen-demo/nfsen-demo/nfsen.php#processing.
- Legend:** peer2 (blue), gateway (yellow), site (red), upstream (green).
- Table:** Shows traffic statistics for four interfaces:

	peer2	gateway	site	upstream
3.3 k/s	76.2 k/s	66.9 k/s	7.0 k/s	621.0 /s
1.0 /s	651.0 /s	600.8 /s	46.6 /s	0 /s
467.1 /s	8.9 k/s	6.1 k/s	2.0 k/s	181.7 /s
6.4 k/s	94.2 k/s	84.3 k/s	8.2 k/s	896.4 /s
459.9 Mb/s	766.7 /s	613.3 /s	38.8 Mb/s	768.4 Mb/s
12.5 Mb/s	768.4 Mb/s	28.3 Mb/s	7.4 Mb/s	568.2 Mb/s
437.3 kb/s	104.0 kb/s	28.3 Mb/s	7.4 Mb/s	685.1 kb/s
11.7 Mb/s	2.9 Mb/s	2.8 Mb/s	2.8 Mb/s	16.7 Mb/s
- Display Options:** All, None, Sum, Rate.
- Netflow Processing Section:**
 - Source:** peer1, peer2, gateway, site, upstream (selected).
 - Filter:** All Sources, and <none>.
 - Options:**
 - Radio buttons: List Flows (selected), Stat TopN.
 - Top: 10.
 - Stat: Flow Records, order by flows.
 - Aggregate: proto, srcPort, dstPort, srcIP, dstIP.
 - Limit: Packets > 0.
 - Output: line, / IPv6 long.
 - Buttons: Clear Form, process.
- Command Line Output:**

```
** nfdump -M /netflow0/nfsen-demo/profile-data/live/peer1:peer2:gateway:site:upstream -T -r 2007/05/31/04/nfcapd.200705310440
nfdump filter:
any
Aggregated flows 2797250
Top 10 flows ordered by flows:
Date flow start Duration Proto      Src IP Addr:Port      Dst IP Addr:Port      Packets    Bytes Flows
2007-05-31 04:39:54.045 299.034 UDP      116.147.95.88:1110 -> 188.142.64.162:27014   68      5508   68
2007-05-31 04:39:56.282 298.174 UDP      116.147.249.27:1478 -> 188.142.64.163:27014   67      5427   67
2007-05-31 04:39:57.530 298.206 UDP      117.196.44.62:1031 -> 188.142.64.166:27014   67      5427   67
2007-05-31 04:39:57.819 298.112 UDP      117.196.75.134:1146 -> 188.142.64.167:27014   67      5427   67
2007-05-31 04:39:53.787 297.216 UDP      61.191.235.132:4121 -> 60.9.138.37:4121   62      3720   62
2007-05-31 04:39:55.354 300.833 UDP      60.9.138.37:4121 -> 118.25.93.95:2121   61      3660   61
2007-05-31 04:39:58.936 298.977 UDP      60.9.138.36:2121 -> 119.182.123.166:2121   61      3660   61
2007-05-31 04:39:54.329 303.585 UDP      120.150.194.76:2121 -> 60.9.138.37:2121   61      3660   61
2007-05-31 04:39:53.916 300.734 UDP      60.9.138.37:2121 -> 125.167.25.128:2121   61      3660   61
2007-05-31 04:39:57.946 300.353 UDP      60.9.138.36:2121 -> 121.135.4.186:2121   61      3660   61
```
- Summary:** IP addresses anonymized, total flows: 4616424, total bytes: 156.6 G, total packets: 172.6 M, avg bps: 644.8 M, avg pps: 90946, avg bpp: 929, Time window: 2007-05-31 04:11:49 - 2007-05-31 04:44:58, Total flows processed: 4616424, skipped: 0, Bytes read: 240064932, Sys: 6.184s flows/second: 746464.4 Wall: 6.185s flows/second: 746361.3.

Bringing the power of the command line forward



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>

Suricata with Dashboards



Picture from Twitter

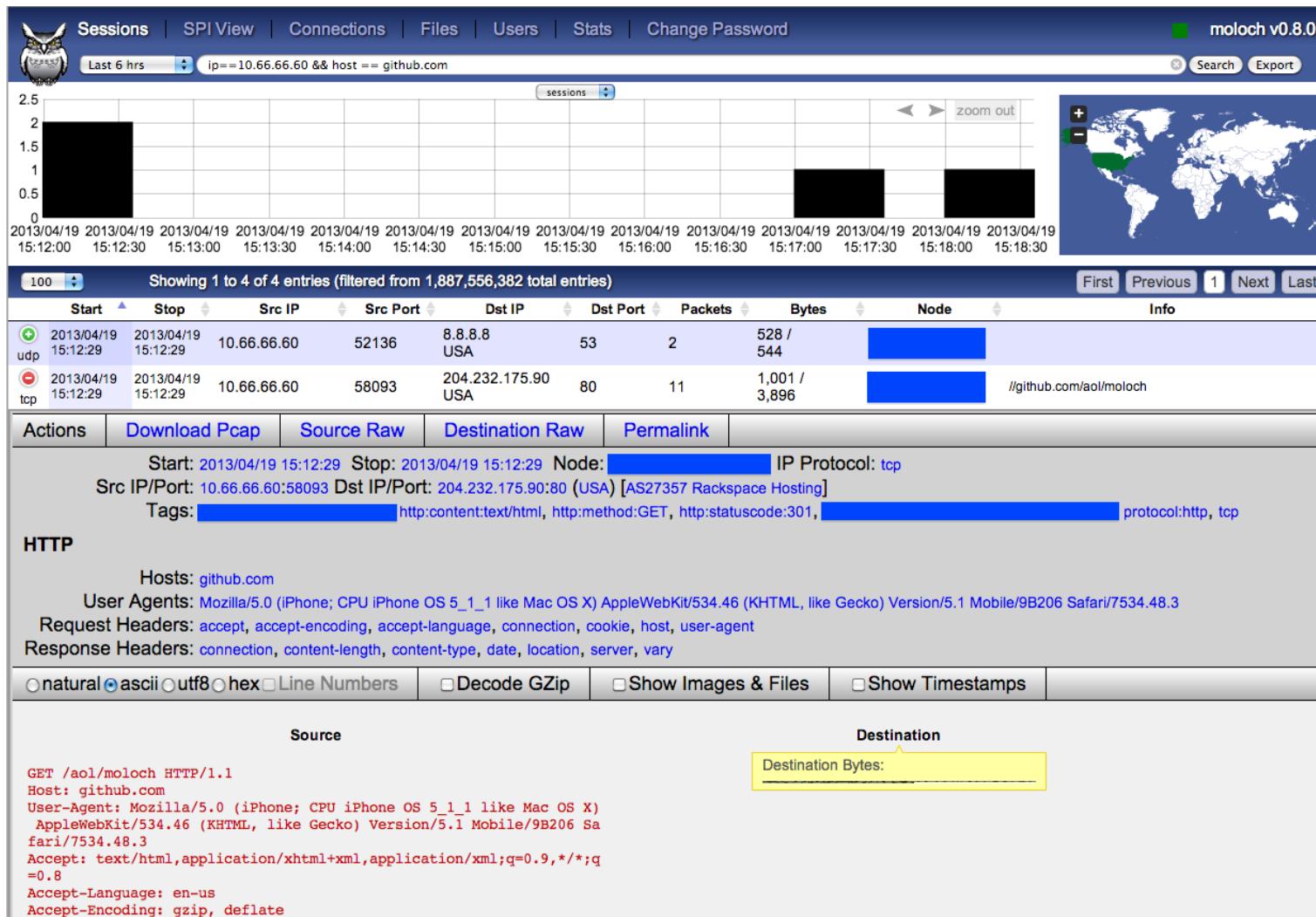
<https://twitter.com/nullthreat/status/445969209840128000>

New link March 2014: 10Gbits

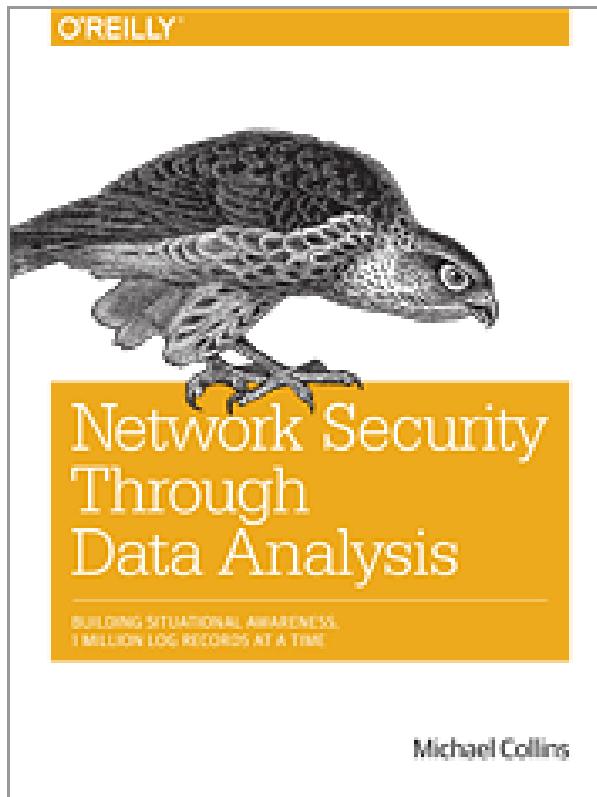
<http://pevma.blogspot.se/2014/03/suricata-preparing-10gbps-network.html>

<http://suricata-ids.org/2014/03/25/suricata-2-0-available/>

Administrators also checkout: D3js.org, Logstash, Elasticsearch, Kibana



Picture from <https://github.com/aol/moloch>

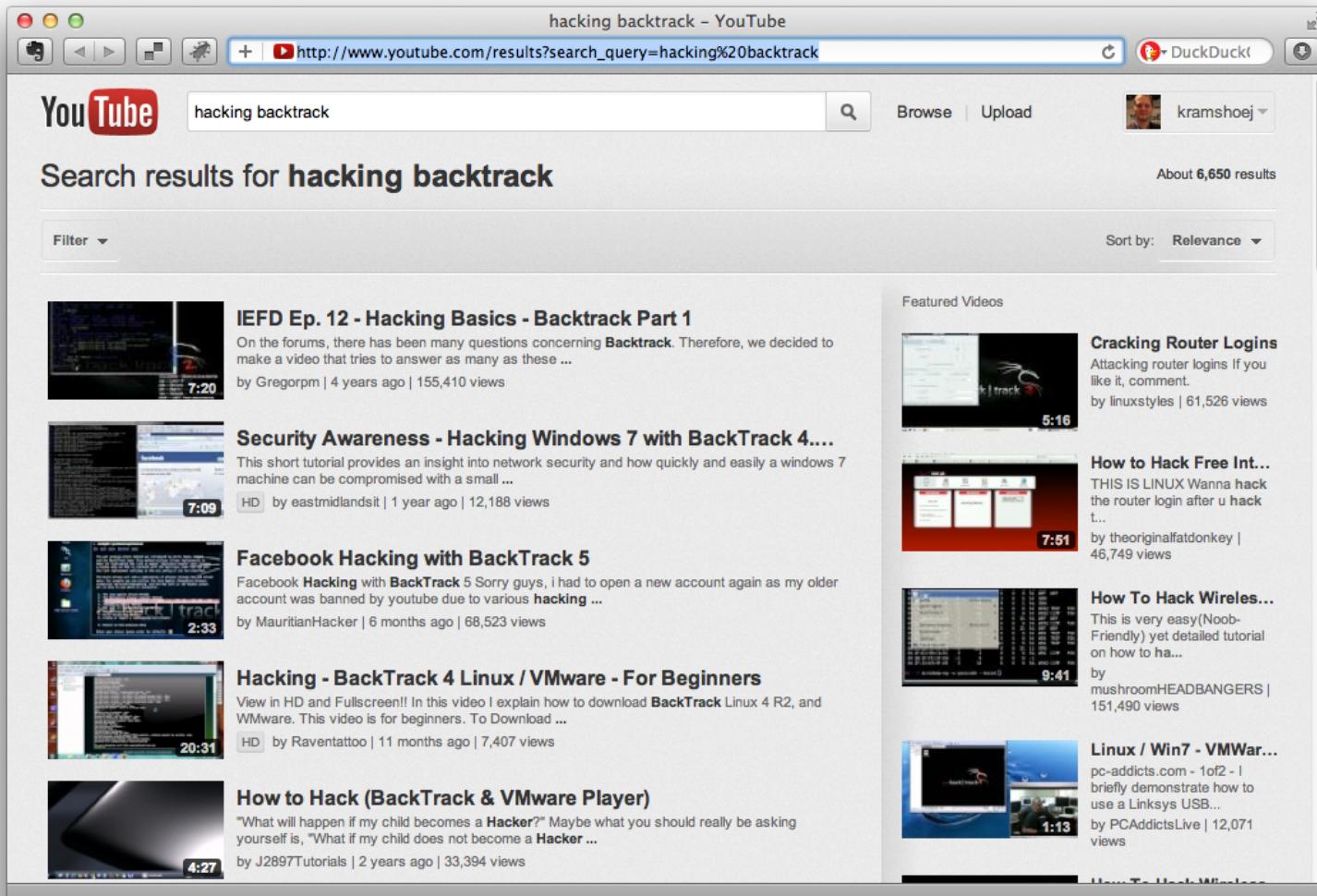


Low page count, but high value! Recommended.

Network Security Through Data Analysis: Building Situational Awareness
By Michael Collins
Publisher: O'Reilly Media Released: February 2014 Pages: 348



- Security Onion is a Linux distro for IDS, NSM, and log management
- securityonion.blogspot.dk
- <http://blog.securityonion.net/p/securityonion.html>



The screenshot shows a web browser window with the title bar "hacking backtrack - YouTube". The address bar contains the URL "http://www.youtube.com/results?search_query=hacking%20backtrack". The main content area displays search results for "hacking backtrack". The results include several video thumbnails, titles, descriptions, and view counts. On the right side, there is a sidebar titled "Featured Videos" with more video thumbnails and titles.

Search results for hacking backtrack

Sort by: Relevance

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

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

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

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

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

Featured Videos

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

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

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

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

Operations security (OpSec, OPSEC), what do you need?

https://en.wikipedia.org/wiki/Operations_security

Great description

"OpSec is about attracting the right amount of attention and not to raise any suspicion."

<https://www.cryptoparty.at/opsec>

Use multiple devices, isolate data

less critical on phone, most critical on laptop with full disk encryption

Using different password for each service, unpossible!

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



› 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

Password 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.



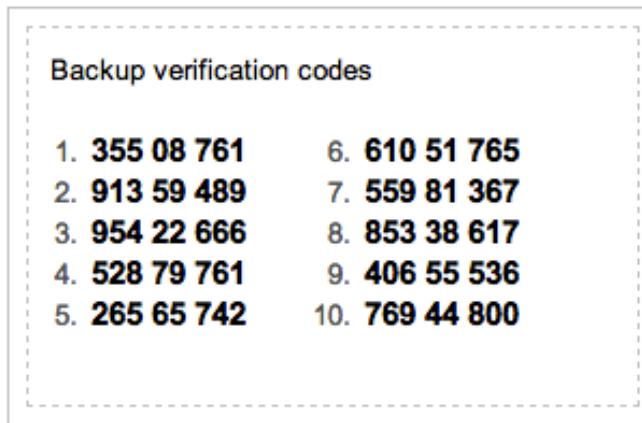
Phone Call

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

Video <https://www.duosecurity.com/duo-push>

<https://www.duosecurity.com/>

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

From previous slide:

Conclusion passwords: integrate with authentication, not reinvent

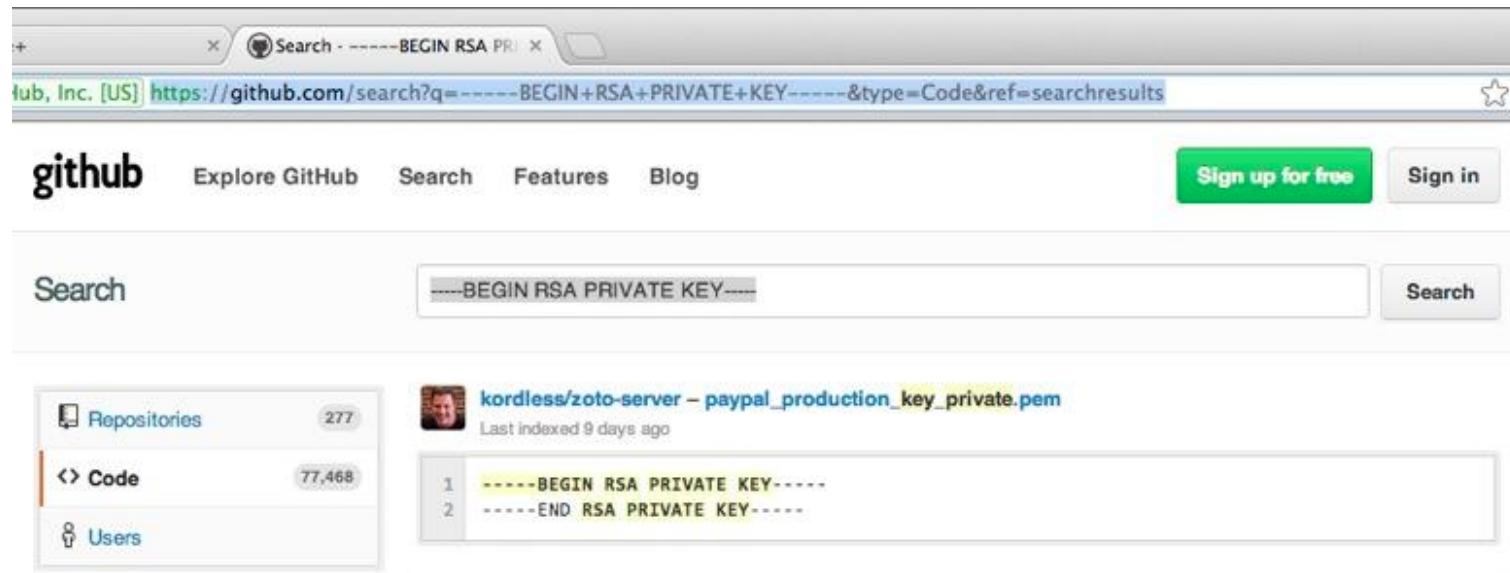
Dont:

- 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!

The 5th Wave

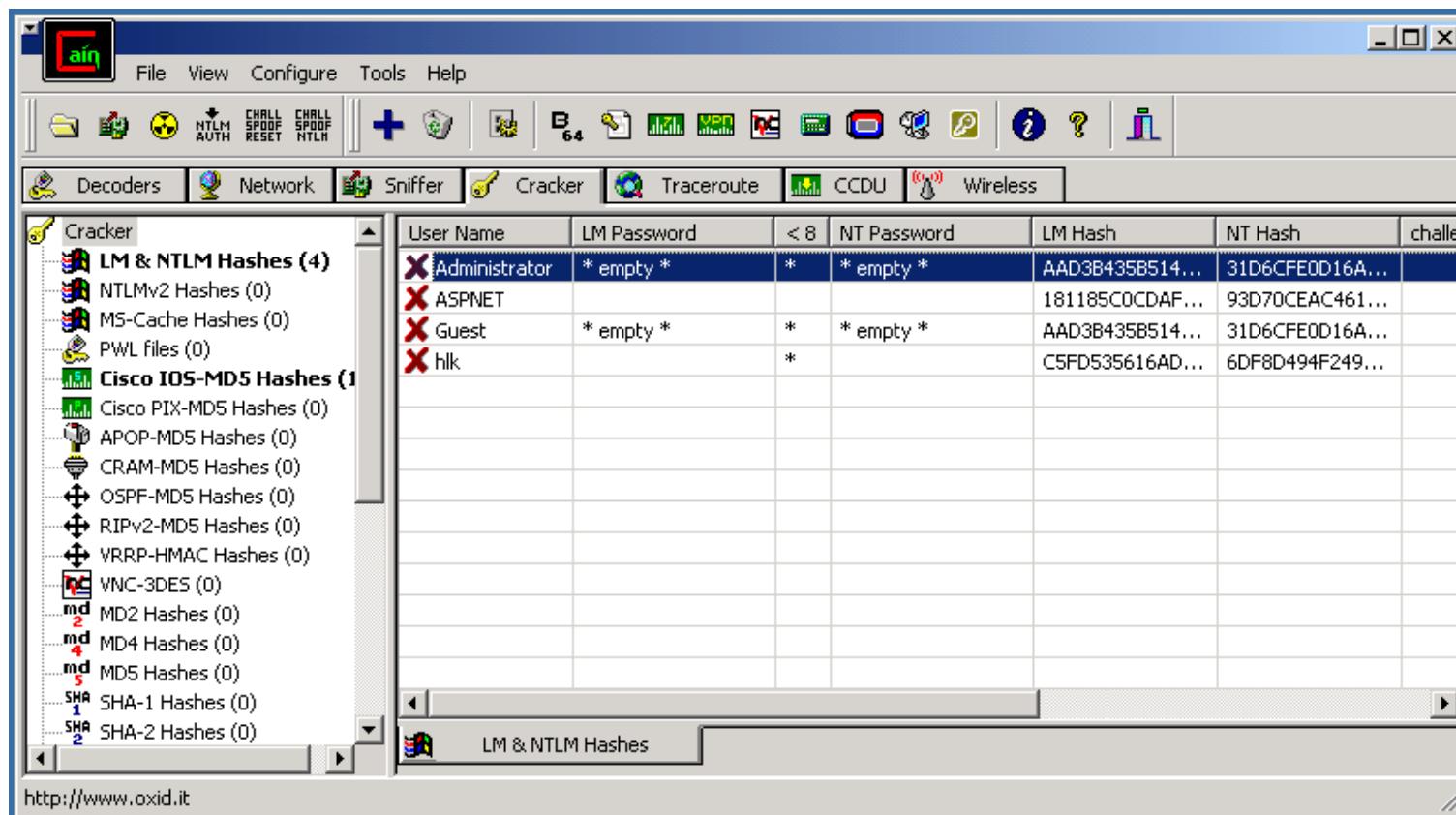
By Rich Tennant



"Don't be silly — of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."

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

Dont forget that hashes can often be cracked



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

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

- Hashcat is the world's fastest CPU-based password recovery tool.
- oclHashcat-plus is a GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.
- oclHashcat-lite is a GPGPU cracker that is optimized for cracking performance. Therefore, it is limited to only doing single-hash cracking using Markov attack, Brute-Force attack and Mask attack.
- John the Ripper password cracker old skool men stadig nyttig

Source:

<http://hashcat.net/wiki/>

<http://www.openwall.com/john/>

 [Henrik Kramshoej](#) retweeted

 **Solar Designer** @solardiz    

Similarly expensive Xeon E5-2670 is 2.4x to 3.3x slower than Zynq 7045 #FPGA on this test, yet consumes ~20x more power; GPUs are way behind

 [Henrik Kramshoej](#) retweeted

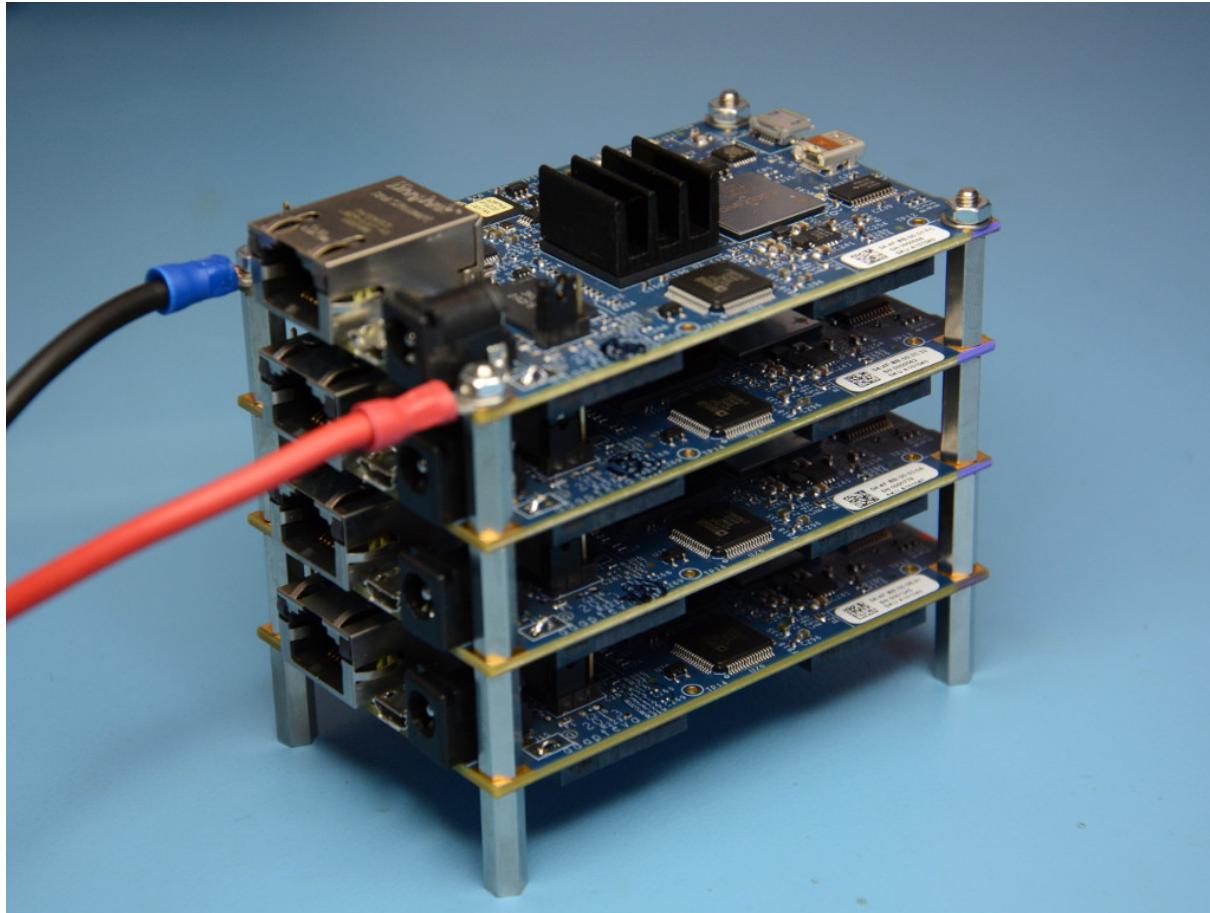
 **Solar Designer** @solardiz   

On last night to submit WOOT final paper, @kmalvoni got bcrypt \$2a\$05 to 20538 c/s, \$2a\$12 to 226 c/s on Zynq 7045 #FPGA. Not the limit yet.

<https://twitter.com/solardiz/status/492037995080712192>

Warning: FPGA hacking - not finished part of presentation ☺

Stacking Parallella boards



<http://www.parallella.org/power-supply/>

hvad betyder bruteforcing? afprøvning af alle mulighederne

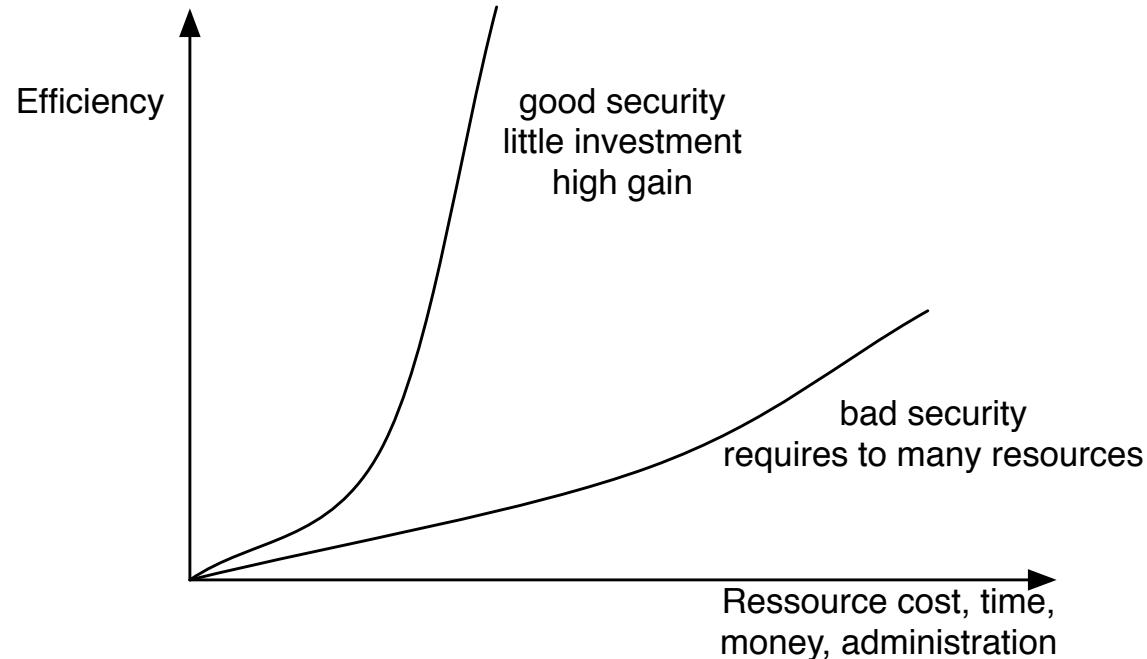
Hydra v2.5 (c) 2003 by van Hauser / THC <vh@thc.org>

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

...



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

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: **IMAPS**, **POP3S**, **HTTPS** 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

Newer versions of Microsoft Windows, Mac OS X and Linux

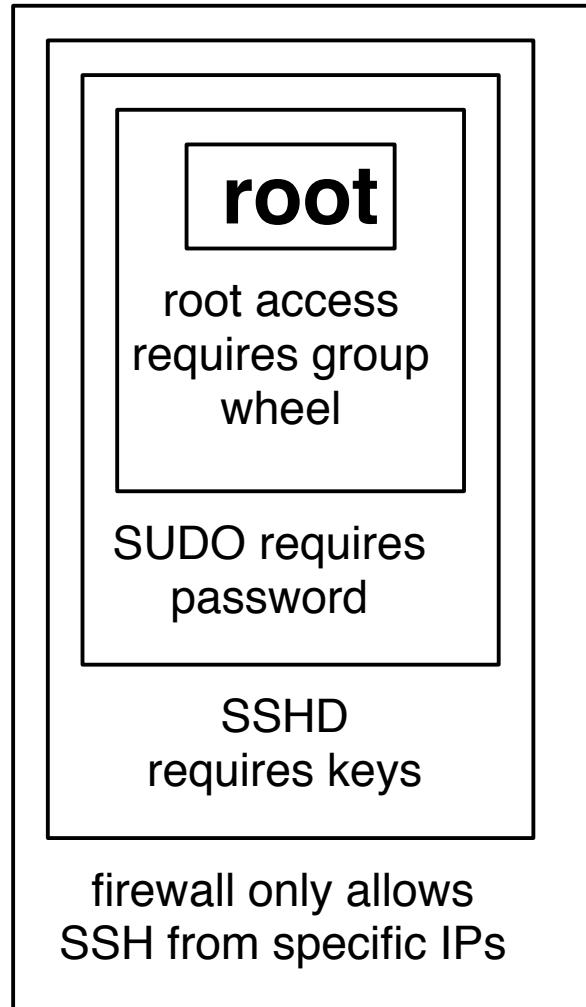
- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

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

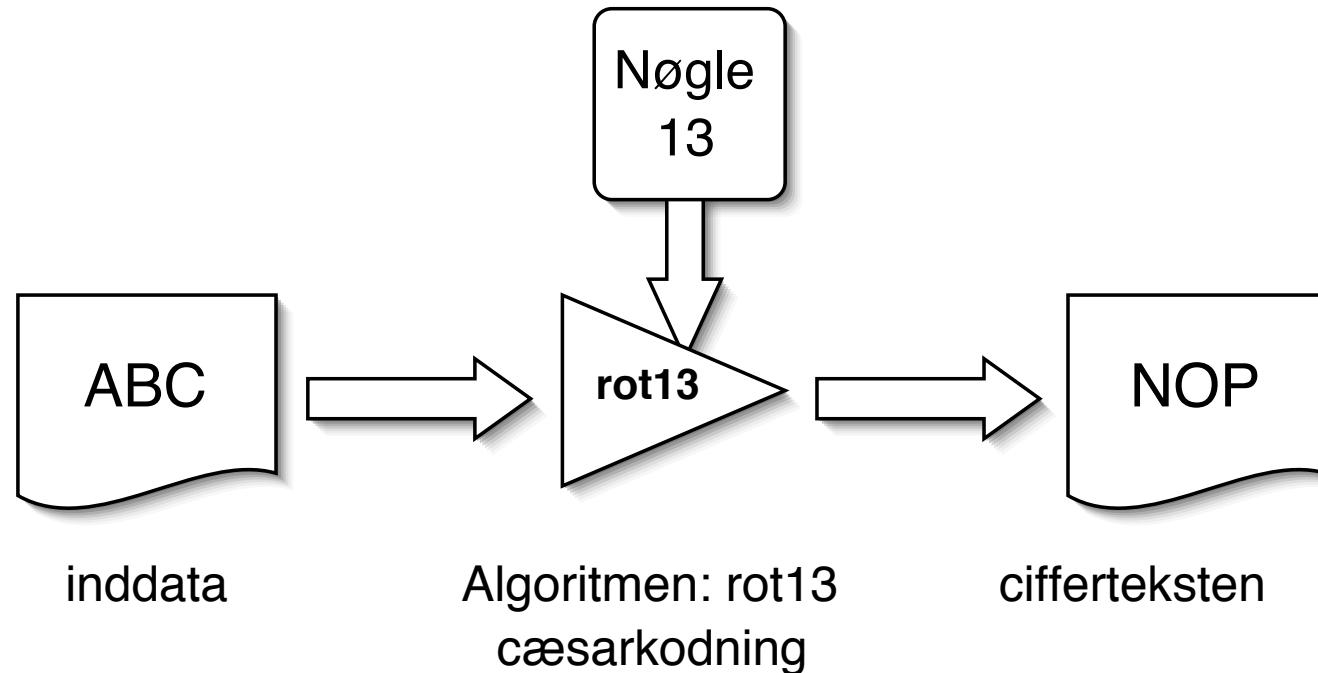
OpenBSD has shown the way in many cases

<http://www.openbsd.org/papers/>

Always try to make life worse and more costly for attackers

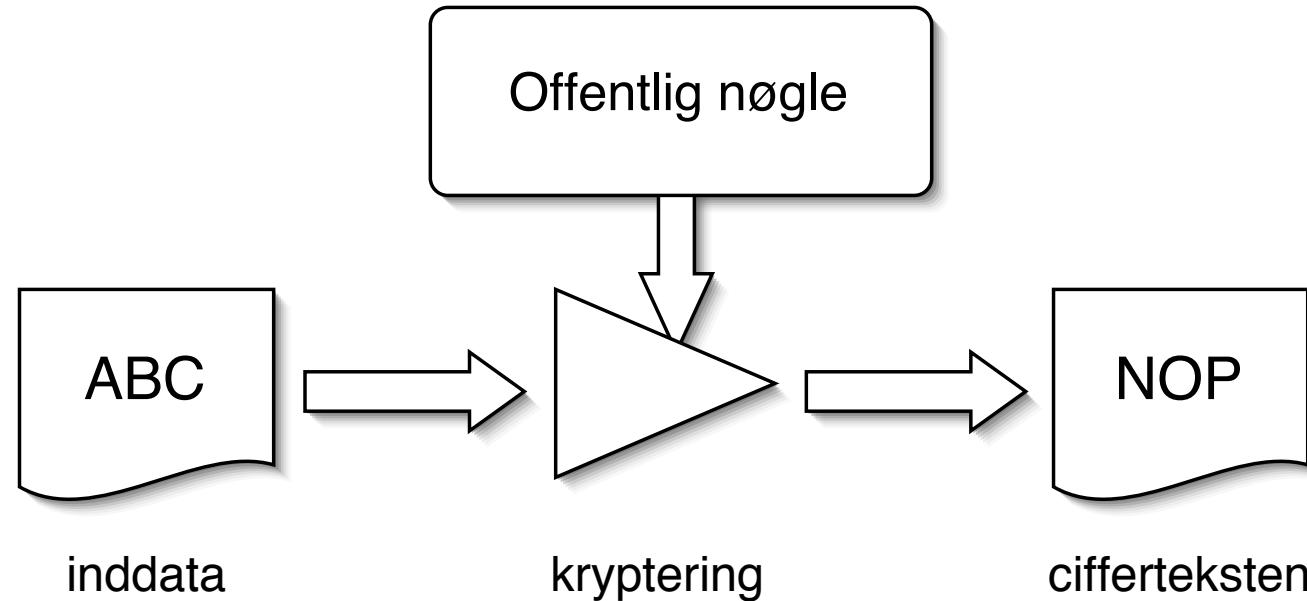


Defense using multiple layers is stronger!



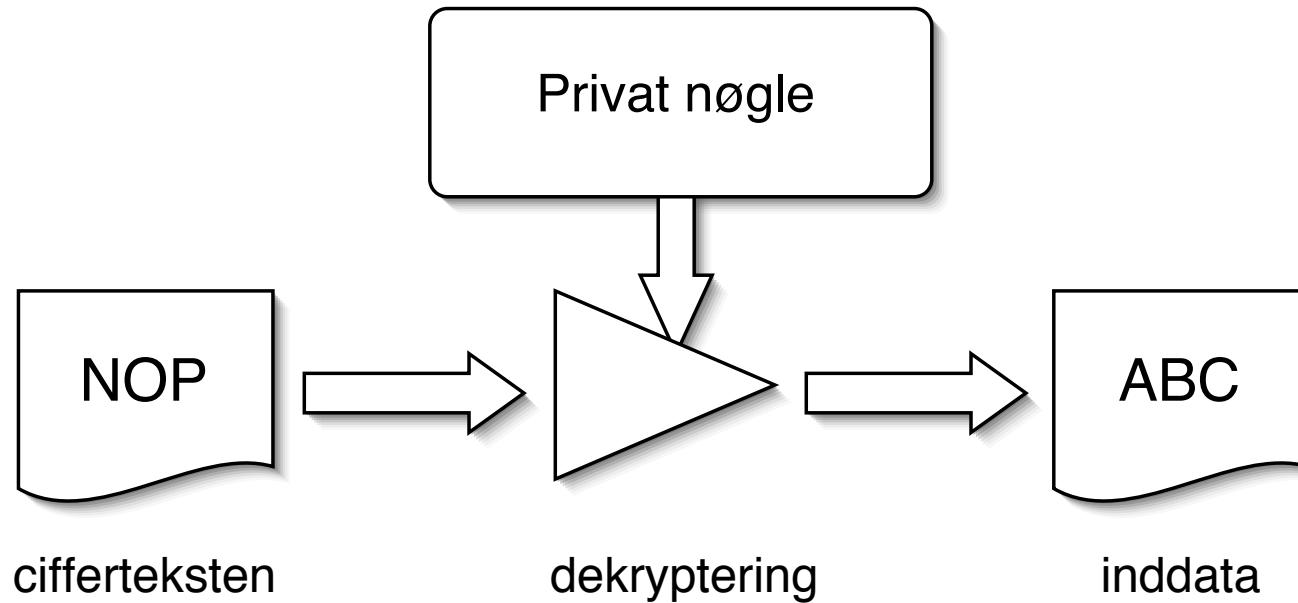
Kryptografi er læren om, hvordan man kan kryptere data

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



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

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



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

Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

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

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

Se evt. Snake Oil Warning Signs: Encryption Software to Avoid

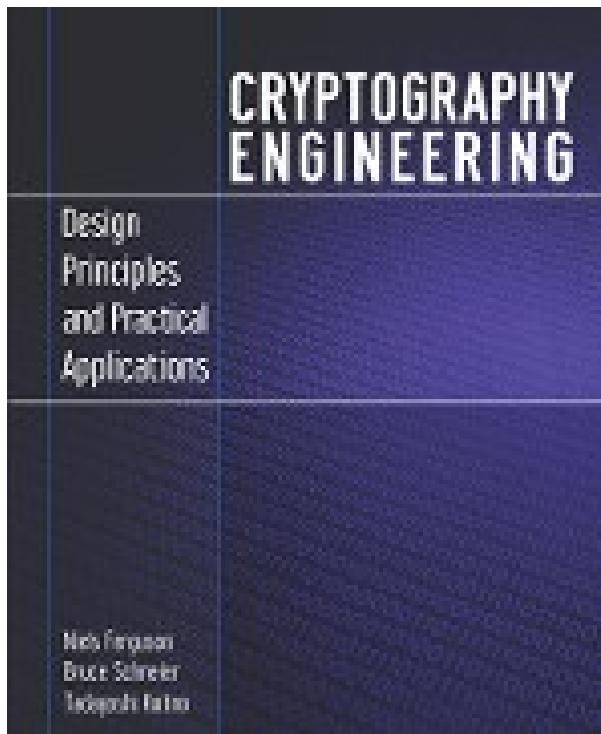
<http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>

Formålet med kryptering

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet



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

<https://www.schneier.com/book-ce.html>

Sorry, none

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, SSLv3, Heartbleed

Sorry, brain overflow from SSL/TLS vulnerabilities

Sources: see my blog posts about heartbleed for more links and tools

<http://www.version2.dk/blog/openssl-er-doed-laenge-leve-libressl-57640>

<http://www.version2.dk/blog/opdater-openssl-og-dit-os-nu-57202>

The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.



Source: <http://heartbleed.com/>

Heartbleed is yet another bug in SSL products



What versions of the OpenSSL are affected?

Status of different versions:

- * OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
- * OpenSSL 1.0.1g is NOT vulnerable
- * OpenSSL 1.0.0 branch is NOT vulnerable
- * OpenSSL 0.9.8 branch is NOT vulnerable

Bug was introduced to OpenSSL in December 2011 and has been out in the wild since OpenSSL release 1.0.1 on 14th of March 2012. OpenSSL 1.0.1g released on 7th of April 2014 fixes the bug.

Why is heartbleed different?



Great PR, name, web site, logo

OpenSSL is very widespread

OpenSSL has been criticized before

The spotlight is now on a lot of products, infrastructure

BOTH Open Source products and Proprietary products hurt by this

TL;DR

OpenSSL is everywhere and an example of our dependency on weak components

Key points after heartbleed



Source: picture source

<https://www.duosecurity.com/blog/heartbleed-defense-in-depth-part-2>

- Writing SSL software and other secure crypto software is hard
- Configuring SSL is hard
check your own site <https://www.ssllabs.com/ssltest/>
- SSL is hard, finding bugs "all the time" <http://armoredbarista.blogspot.dk/2013/01/a-brief-chronology-of-ssltls-attacks.html>
- Rekeying is hard - slow, error prone, manual process - Automate!
- Proof of concept programs exist - good or bad?

Some of the tools released shortly after Heartbleed announcement

- <https://github.com/FiloSottile/Heartbleed> tool i Go
site <http://filippo.io/Heartbleed/>
- <https://github.com/titanous/heartbleeder> tool i Go
- <http://s3.jspenguin.org/ssltest.py> PoC
- <https://gist.github.com/takeshixx/10107280> test tool med STARTTLS support
- <http://possible.lv/tools/hb/> **test site**
- <https://twitter.com/richinseattle/status/453717235379355649> Practical Heartbleed attack against session keys links til, <https://www.mattslifebytes.com/?p=533> og "Fully automated here"
<https://www.michael-p-davis.com/using-heartbleed-for-hijacking-user-session>
- Metasploit er også opdateret på master repo
<https://twitter.com/firefart/status/453758091658792960>
https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/ssl/openssl_heartbleed.rb

Heartbleed hacking

```
06b0: 2D 63 61 63 68 65 0D 0A 43 61 63 68 65 2D 43 6F -cache..Cache-Co
06c0: 6E 74 72 6F 6C 3A 20 6E 6F 2D 63 61 63 68 65 0D ntrol: no-cache.
06d0: 0A 0D 0A 61 63 74 69 6F 6E 3D 67 63 5F 69 6E 73 ...action=gc_in
06e0: 65 72 74 5F 6F 72 64 65 72 26 62 69 6C 6C 6E 6F ert_order&billno
06f0: 3D 50 5A 4B 31 31 30 31 26 70 61 79 6D 65 6E 74 =PZK1101&payment
0700: 5F 69 64 3D 31 26 63 61 72 64 5F 6E 75 6D 62 65 _id=1& card'numbe
0710: XX r=4060xxxx413xxx
0720: 39 36 26 63 61 72 64 5F 65 78 70 5F 6D 6F 6E 74 96&card'exp'mont
0730: 68 3D 30 32 26 63 61 72 64 5F 65 78 70 5F 79 65 h=02&card'exp'ye
0740: 61 72 3D 31 37 26 63 61 72 64 5F 63 76 6E 3D 31 ar=17&card'cvn=1
0750: 30 39 F8 6C 1B E5 72 CA 61 4D 06 4E B3 54 BC DA 09.l...r.aM.N.T..
```

- Obtained using Heartbleed proof of concepts - Gave full credit card details
- "can XXX be exploited" - yes, clearly! PoCs ARE needed without PoCs even Akamai wouldn't have repaired completely!
- The internet was ALMOST fooled into thinking getting private keys from Heartbleed was not possible - scary indeed.

Analysis of the heartbleed bug

- analyse af problemet i koden

<http://blog.existentialize.com/diagnosis-of-the-openssl-heartbleed-bug.html>

- IDS regler Detecting OpenSSL Heartbleed with Suricata

<http://blog.inliniac.net/2014/04/08/detecting-openssl-heartbleed-with-suricata/>

- god beskrivelse af hvordan man kan fixe hurtigere hvis man har automatiseret infrastruktur

<https://www.getpantheon.com/heartbleed-fix>

- Mange blogindlæg om emnet - eksempelvis

<http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/>

- "nse script ssl-heartbleed.nse committed to nmap as rev 32798. "

- You can now use Masscan to scan the whole internet for the Heartbleed vulnerability in under 6 minutes <https://twitter.com/jedisct1/status/453679529710460928>

og <https://github.com/robertdavidgraham/masscan/commit/23497c448b0a1c7058e84>

```
ssl_prefer_server_ciphers on;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # not possible to do exclusive
ssl_ciphers 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+\n
  \aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!\\
  \eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256\\
  \-SHA:CAMELLIA128-SHA:AES128-SHA';
add_header Strict-Transport-Security max-age=15768000; # six months
# use this only if all subdomains support HTTPS!
# add_header Strict-Transport-Security "max-age=15768000; includeSubDomains";
```

*Listing 2.6: SSL settings for nginx
[configuration/Webservers/nginx/default]*

Overview

This whitepaper arose out of the need for system administrators to have an updated, solid, well researched and thought-through guide for configuring SSL, PGP, SSH and other cryptographic tools in the post-Snowden age. ... This guide is specifically written for these system administrators.

<https://bettercrypto.org/>

Heartbleed Conclusions



Nothing new, but more focus on problems?

Really is there something new in this?

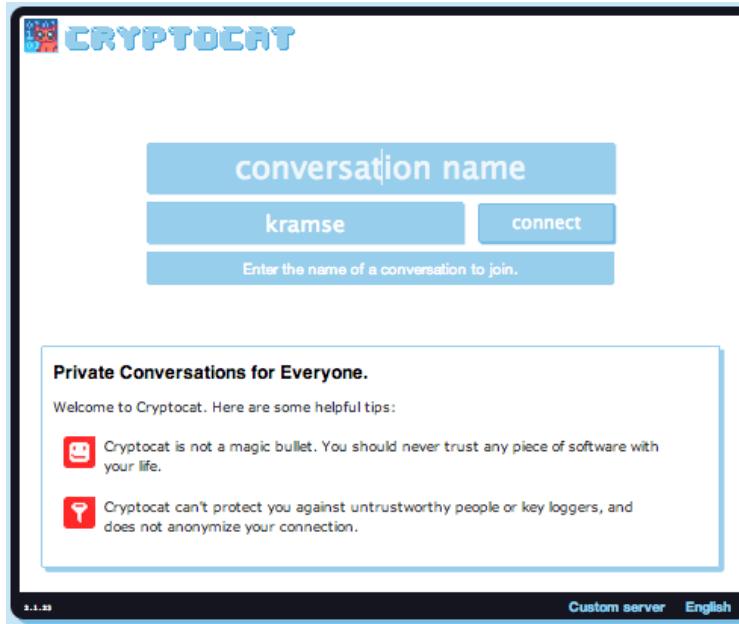
Software has bugs - stay vigilant, implement defense in depth

Software need funding - especially software used in our critical systems

Security needs proof of concepts and open communication

Akamai fix that wasn't good enough!

TL;DR Fund more security audits, stop using untested/unaudited software



Truecrypt audit

<https://isecpartners.github.io/news/2014/04/14/iSEC-Completes-Truecrypt-Audit.html>

Cryptocat audit

<https://blog.crypto.cat/2013/02/cryptocat-passes-security-audit-with-flying-colors/>

Secure products need funding! Donate to multiple including OpenBSD

```
/* Read type and payload length first */
if (1 + 2 + 16 > s->s3->rrec.length)
    return 0; /* silently discard */
hbtype = *p++;
n2s(p, payload);
if (1 + 2 + payload + 16 > s->s3->rrec.length)
    return 0; /* silently discard per RFC 6520 sec. 4 */
pl = p;
```

Ditch OpenSSL - write our own?

SSL implementations compared - above code from OpenSSL copied from this:

<http://tstarling.com/blog/2014/04/ssl-implementations-compared/>

LibreSSL announced, OpenBSD people

<http://www.libressl.org/> and <http://opensslrampage.org/>

Are your data secure

...lo
am

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**



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

Press t to enter firewire target mode ☺

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

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/GELI - 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 *Let's audit Truecrypt!* Note: truecrypt halted and insecure? who knows?

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

Firewire, DMA & Windows, Winlockpwn via FireWire
Hit by a Bus: Physical Access Attacks with Firewire Ruxcon 2006

Removing memory from live system - data is not immediately lost, and can be read under some circumstances

Lest We Remember: Cold Boot Attacks on Encryption Keys

<http://citp.princeton.edu/memory/>

This is very CSI or Hollywoord like - but a real threat

VileFault decrypts encrypted Mac OS X disk image files

<https://code.google.com/p/vilefault/>

FileVault Drive Encryption (FVDE) (or FileVault2) encrypted volumes

<https://code.google.com/p/libfvde/>

So perhaps use both hard drive encryption AND turn off computer after use?

Crypto Projects that Might not Suck



Steve Weis
PrivateCore
! <http://bit.ly/CryptoMightNotSuck>

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

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/>

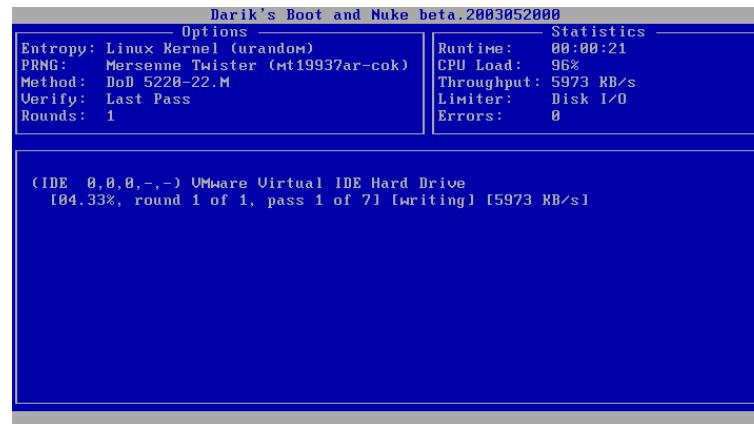
What is it?

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

- 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



- 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



- Pretty Good Privacy - PGP
- Oprindeligt udviklet af Phil Zimmermann
- nu kommersielt, 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>



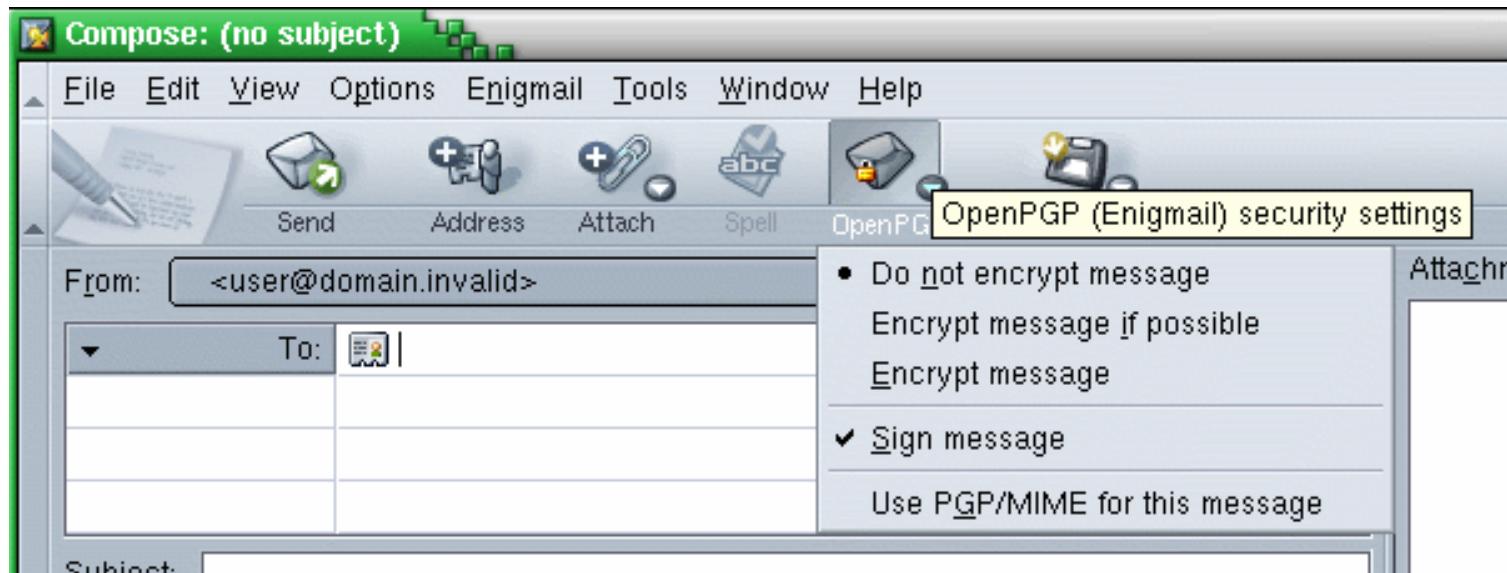
Gnu Privacy Guard, forkortes GnuPG eller GPG

brug linket: <http://www.gnupg.org/>

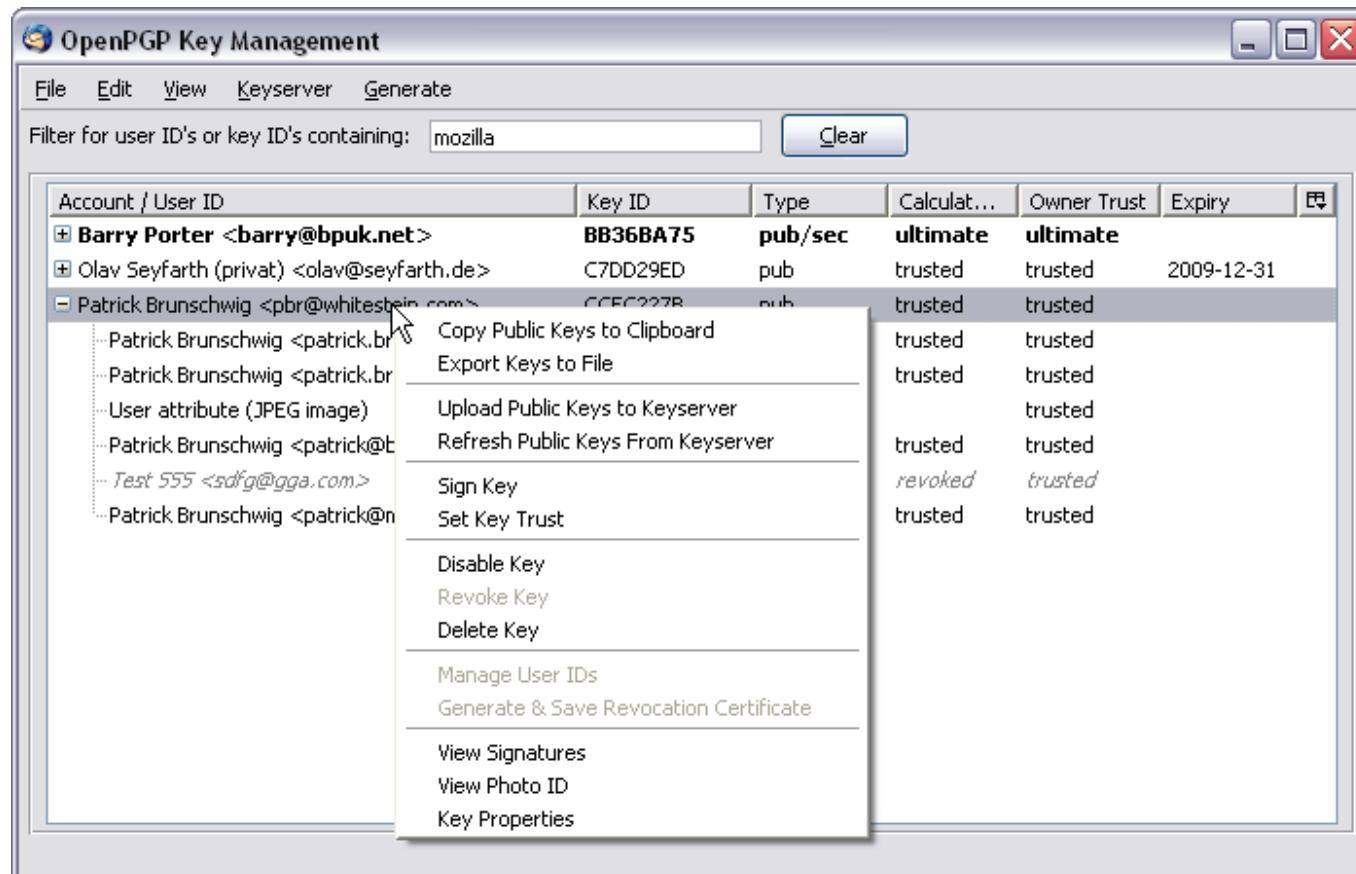
Open Source med GPL licens.

Kan bruges på alle de gængse operativsystemer

Enigmail - GPG plugin til Mail

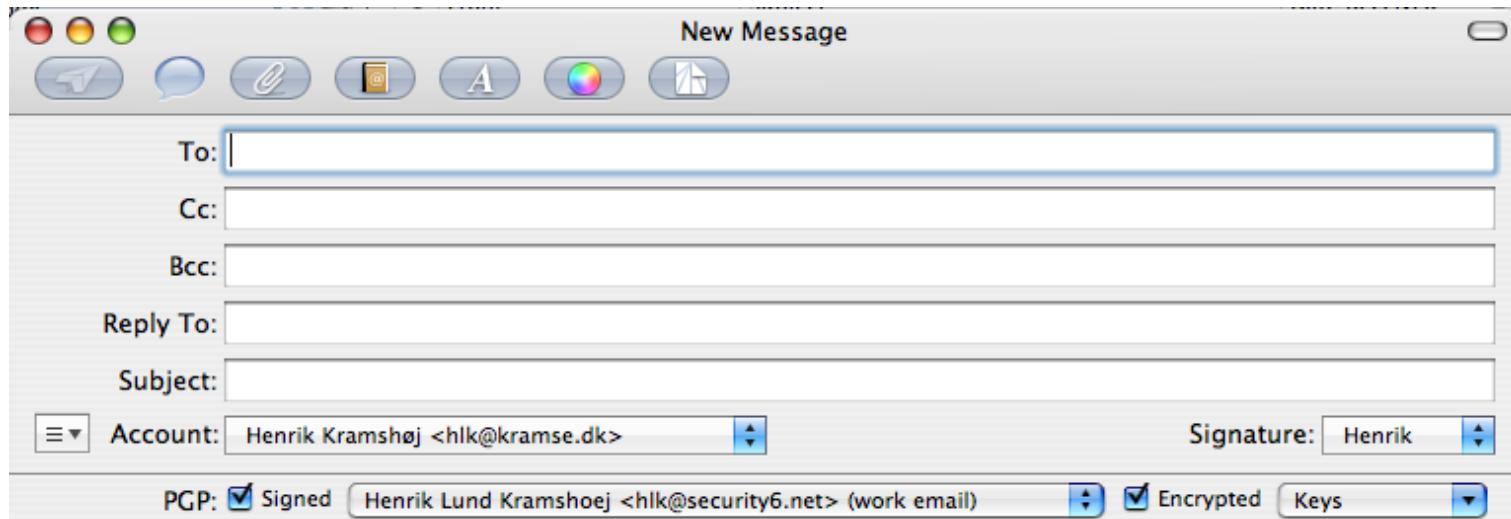


- Enigmail er en udvidelse til
- mailklienten i Mozilla/Netscape
- standalone mailklienten Thunderbird
- Billede fra <http://enigmail.mozdev.org>



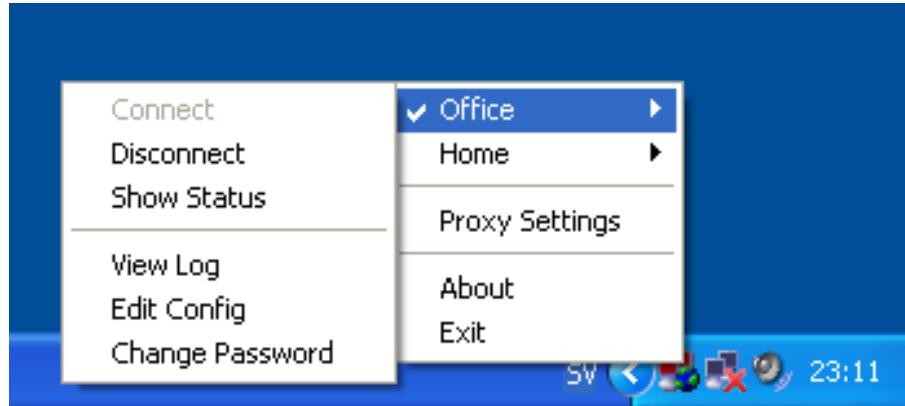
Key Manager funktionaliteten i Enigmail kan anbefales

GPGMail plugin til Mac OS X Mail.app



--
Henrik Lund Kramshøj, cand.scient, CISSP
e-mail: hlk@security6.net, tlf: 2026 6000
www.security6.net - IPv6, sikkerhed, netværk
Follower of the Great Way of Unix

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



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!

Multiple browsers



Firefox



Allow active content to run
only from sites you trust



chrome



noscripts

Take control of the javascript, iframes, and plugins



TorProject.org



- Strict Security settings in the general browser, Firefox or Chrome?
- More lax security settings for "trusted sites" - like home banking
- Security plugins like HTTPS Everywhere and NoScripts for generic browsing



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>

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)

<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!



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/>

Anonymity Online

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



Download Tor 

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

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

Der findes alternativer, men Tor er mest kendt

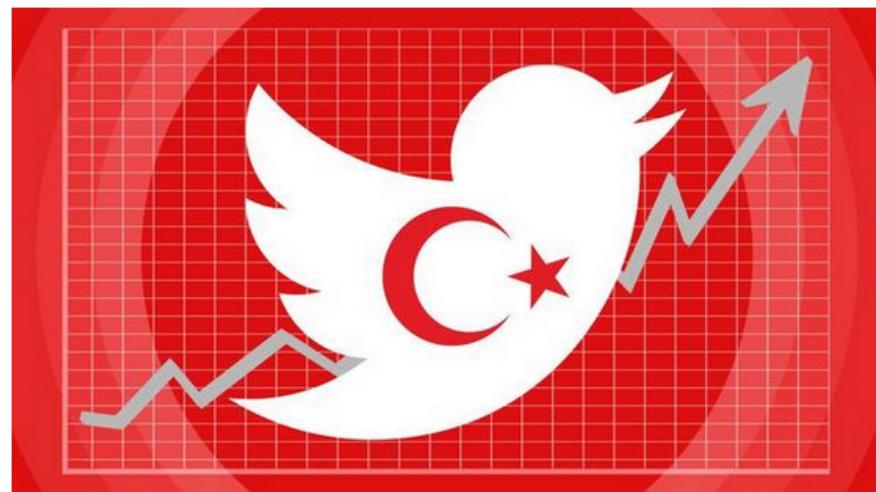
Turkey: Erdogan bans Twitter

 **Mashable** 
@mashable

Whoa: 1.2 million tweets sent in Turkey,
despite ban on.mash.to/1kQ7ijw
#OccupyTwitter #direntwitter
pic.twitter.com/opvuEeEh7f

 View translation

 Reply  Retweet  Favorite  More



RETWEETS 1,311 FAVORITES 379



The Net interprets censorship as damage and routes around it.

John Gilmore

John Gilmore is an American computer science innovator, Libertarian, Internet activist, and one of the founders of [Electronic Frontier Foundation](#). He created the alt.* hierarchy in [Usenet](#) and is a major contributor to the [GNU](#) project.



This [scientist](#) article is a [stub](#). You can help Wikiquote by [expanding it](#).

Sourced [\[edit\]](#)

- **The Net interprets censorship as damage and routes around it.**
 - As quoted in [TIME magazine \(6 December 1993\)](#)
 - Unsourced variant:
The Net treats censorship as a defect and routes around it.
 - How many of you have broken no laws this month?
 - As quoted in a [speech](#) to the First Conference on Computers, Freedom, and Privacy in 1991
 - If you're watching everybody, you're watching nobody.
 - As quoted in [Subject: \[IP\] John Gilmore on government trustworthiness and spy gear](#)
- **When the X500 revolution comes, your name will be lined against the wall and shot.**
 - As quoted in Peter Gutmann's [X509 style guide](#)



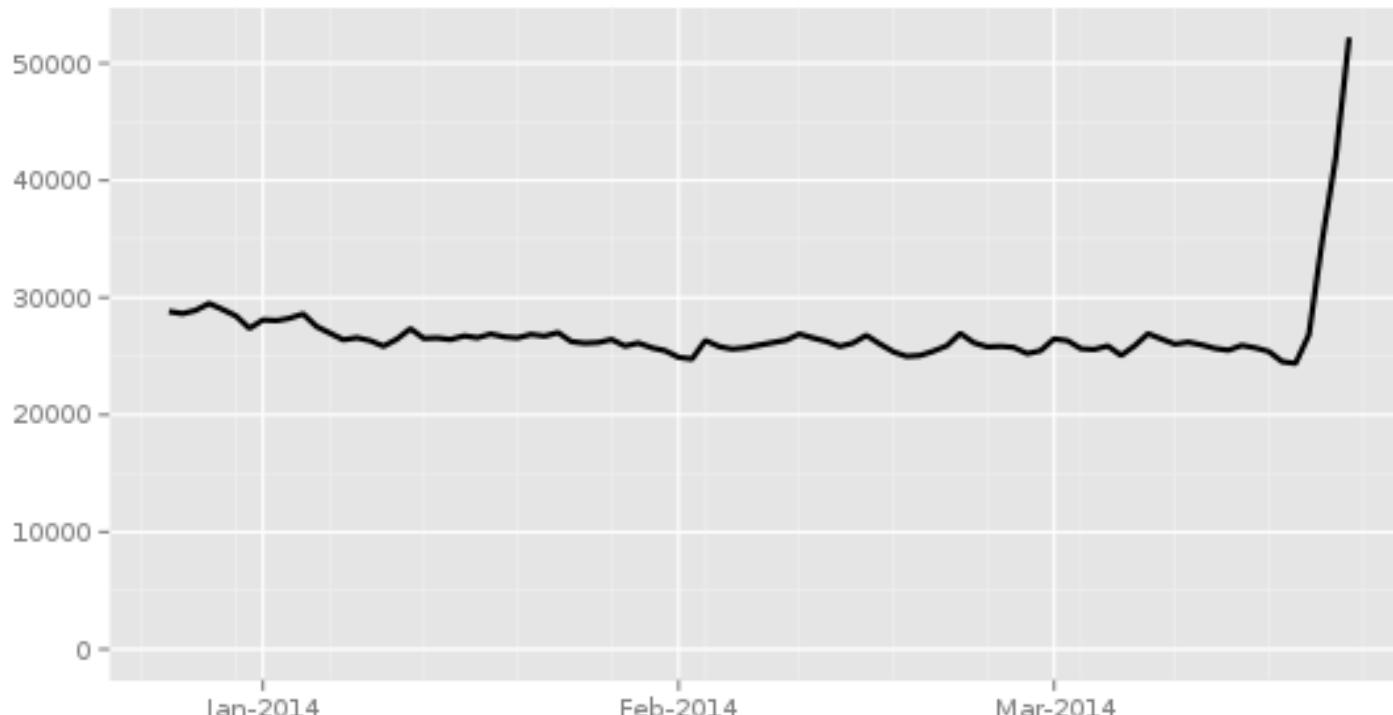
The Net interprets censorship as
damage and routes around it.

http://en.wikiquote.org/wiki/John_Gilmore

[http://en.wikipedia.org/wiki/John_Gilmore_\(activist\)](http://en.wikipedia.org/wiki/John_Gilmore_(activist))

Directly connection Tor Users from Turkey

Directly connecting users from Turkey

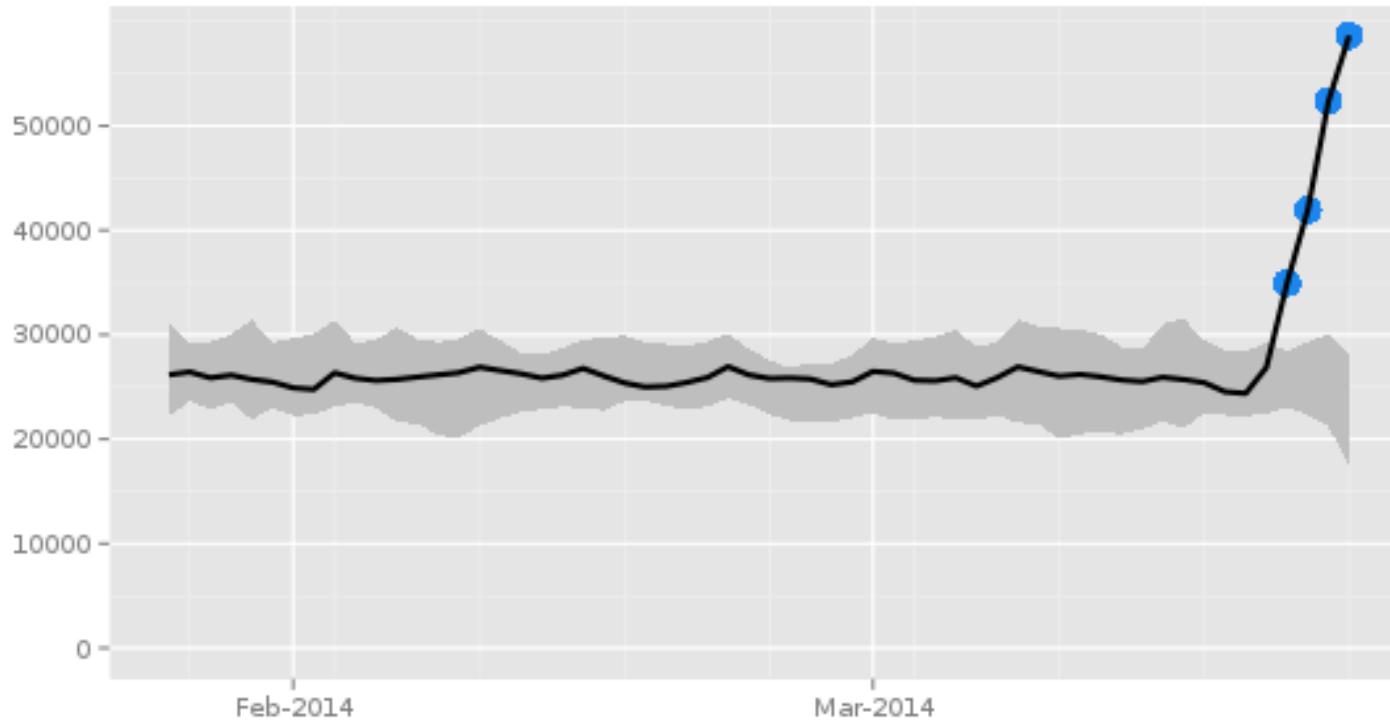


The Tor Project - <https://metrics.torproject.org/>

Image from https://metrics.torproject.org
via <https://twitter.com/runasand>

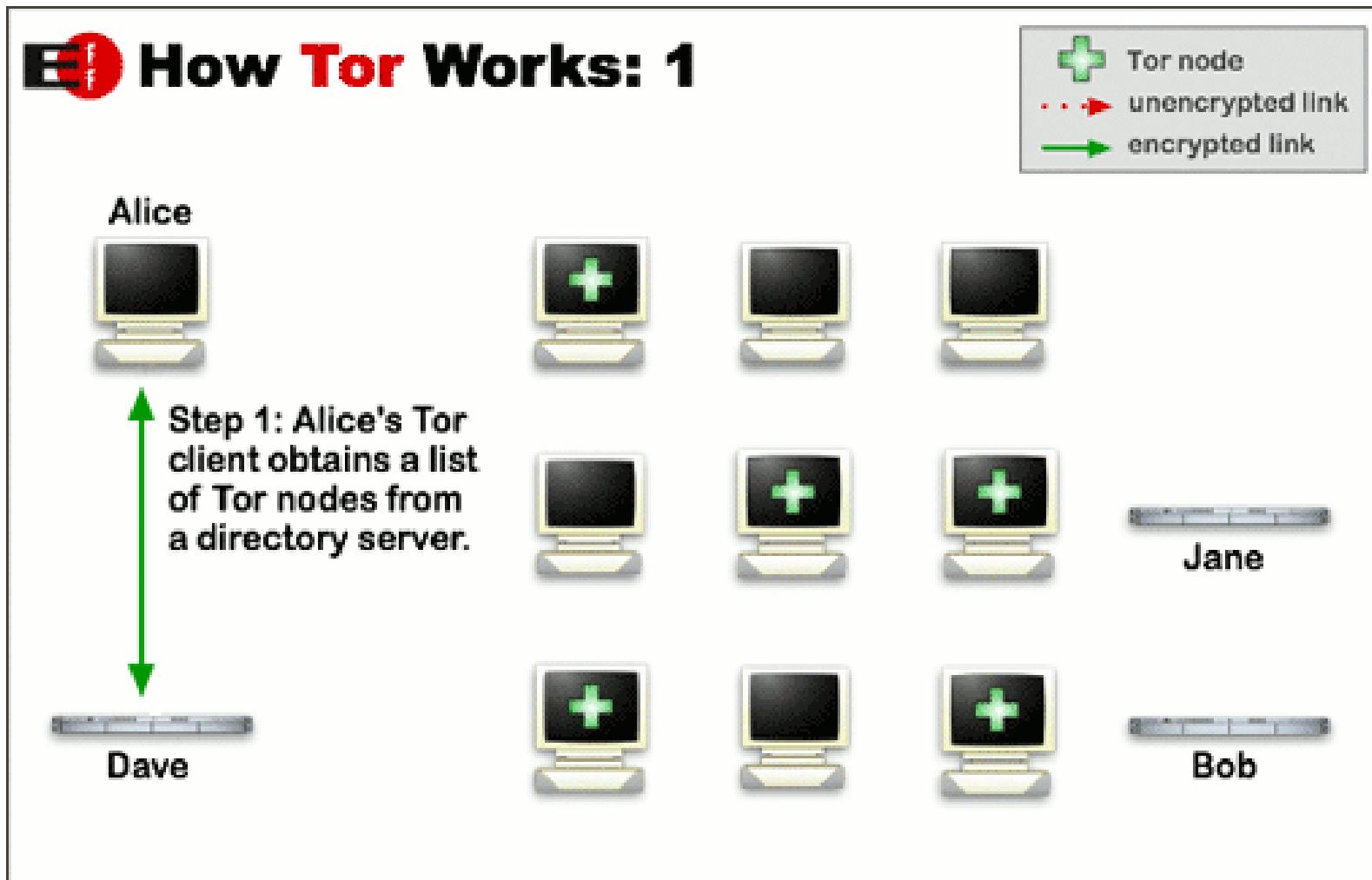
Directly connection Tor Users from Turkey +10.000

Directly connecting users from Turkey

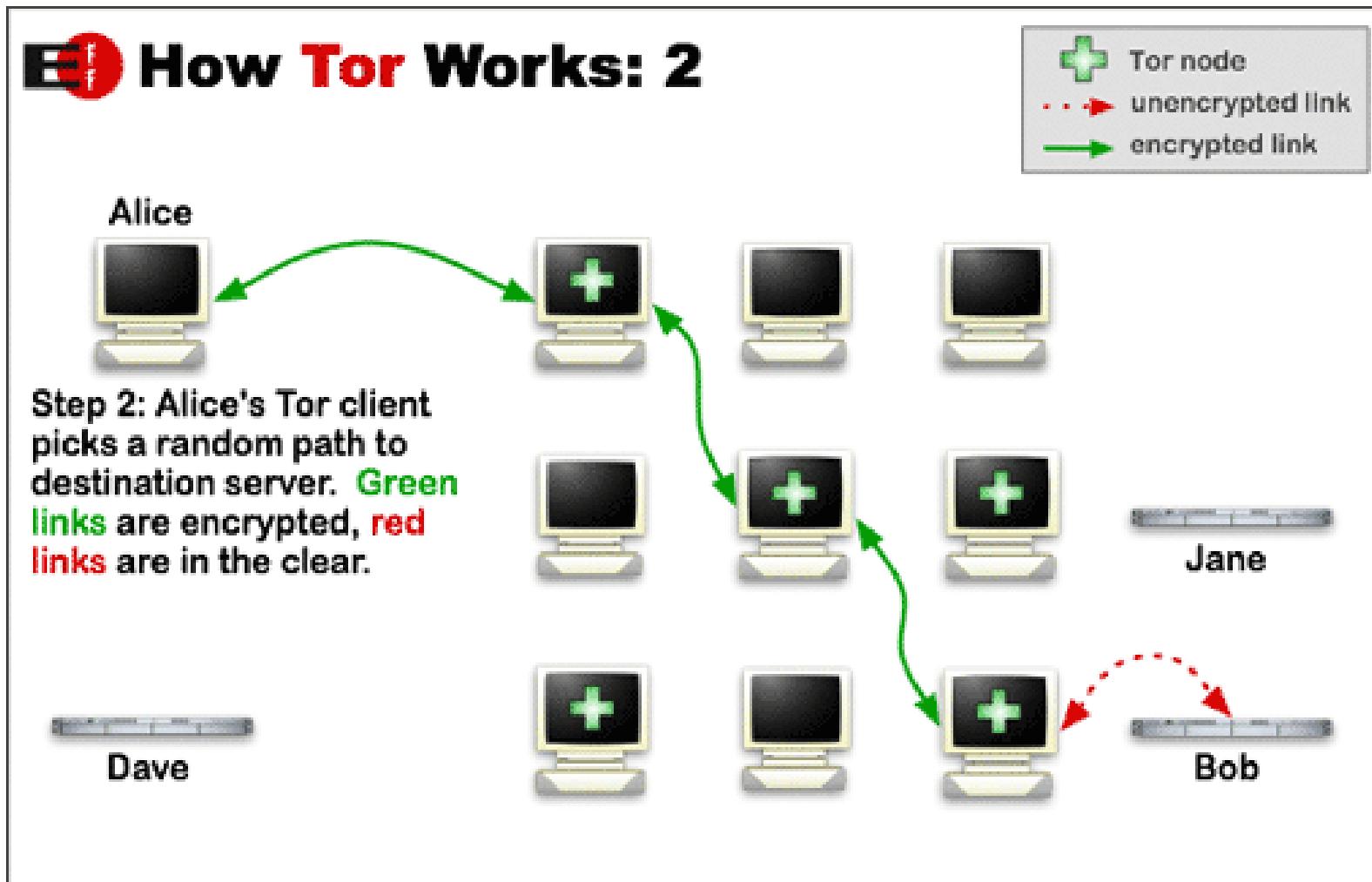


The Tor Project - <https://metrics.torproject.org/>

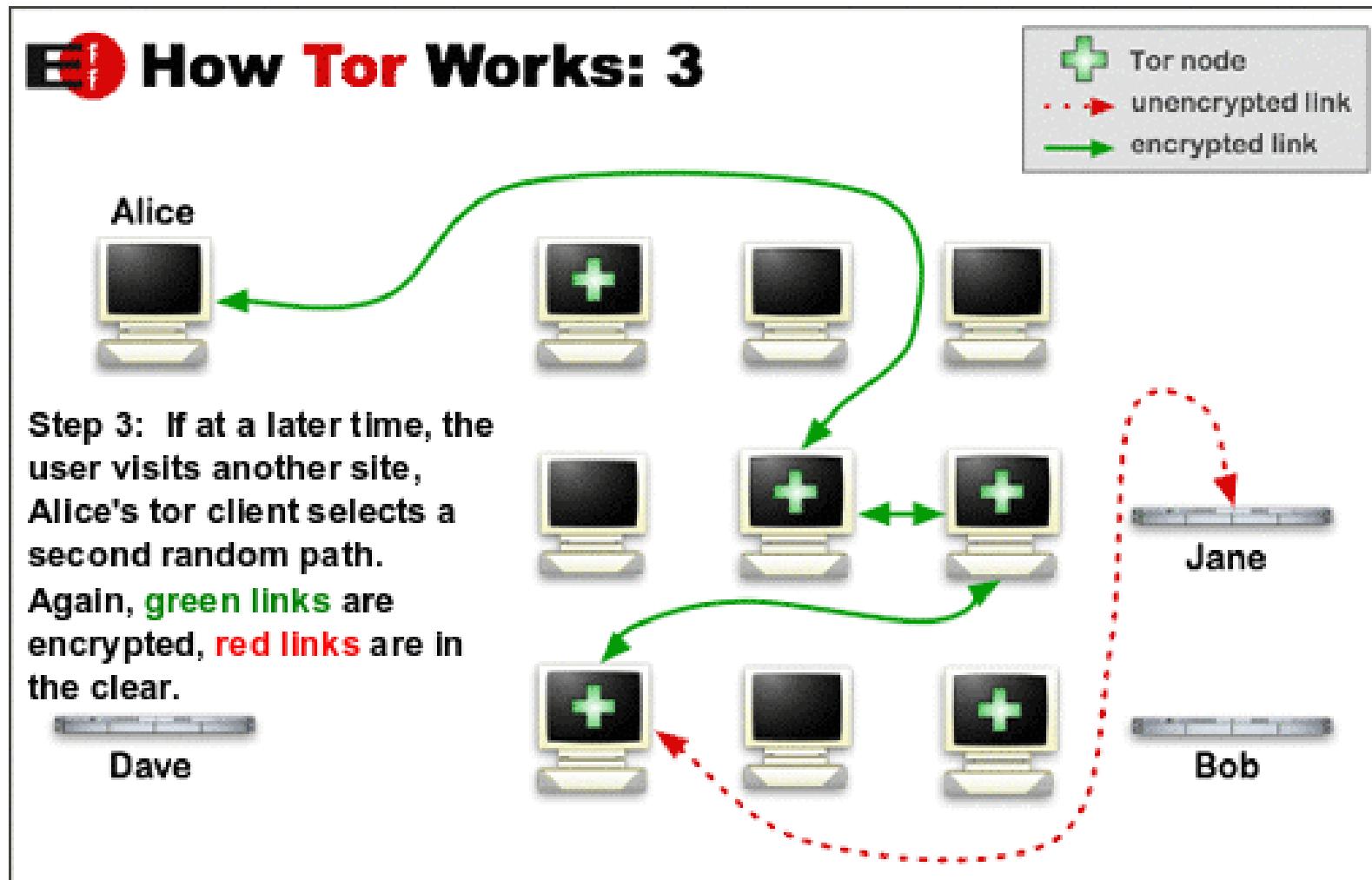
Image from <https://metrics.torproject.org> via <https://twitter.com/ioc32/status/448791582423408640>



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



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



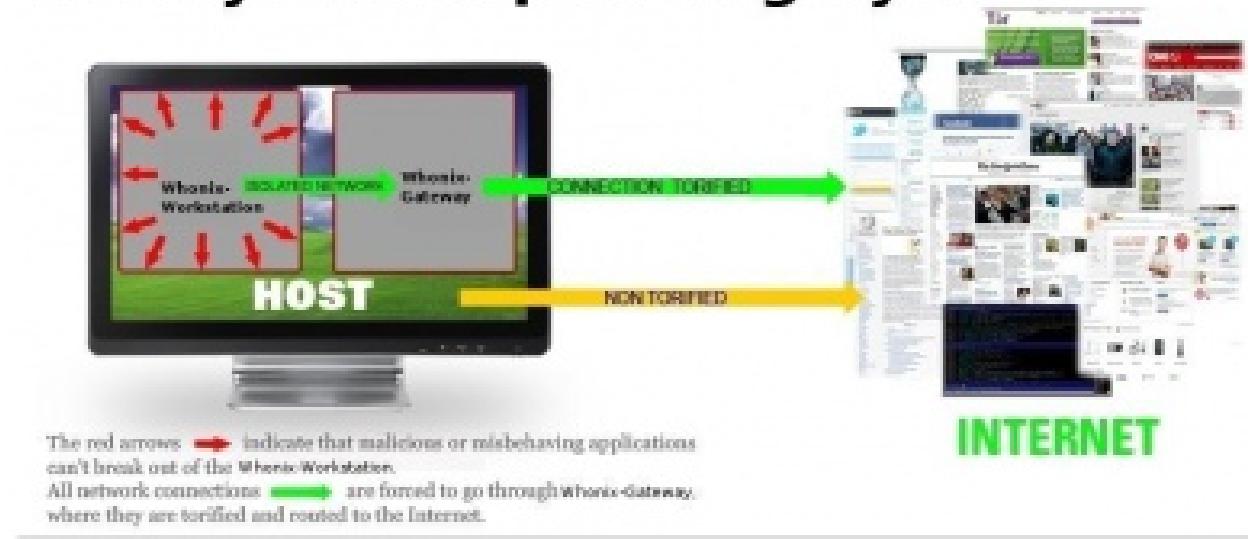
pictures from <https://www.torproject.org/about/overview.html.en>



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

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

Whonix Anonymous Operating System



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/>

Secure your mobile



Orbot:
Proxy With Tor



Orweb:
Private Web Browser



ChatSecure:
Private and Secure Messaging



ObscuraCam:
The Privacy Camera



Ostel:
Encrypted Phone Calls



CSipSimple:
Encrypted Voice Over IP (VOIP)



K-9 and APG:
Encrypted E-mail



KeySync:
Syncing Trusted Identities



TextSecure:
Short Messaging Service (SMS)



Pixelknot:
Hidden Messages

Dont forget your mobile platforms <https://guardianproject.info/>



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

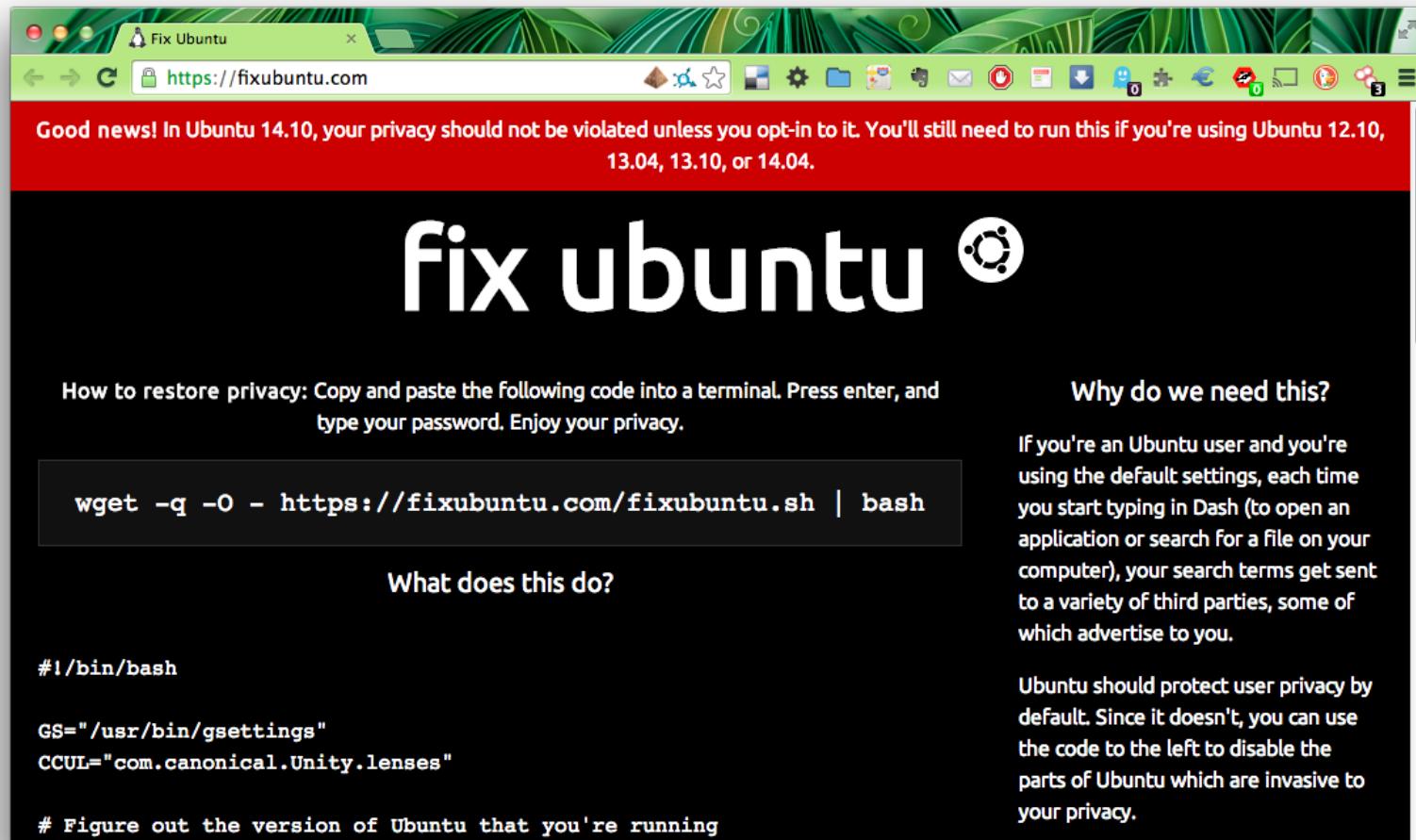
Dont use a single device for all types of data

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

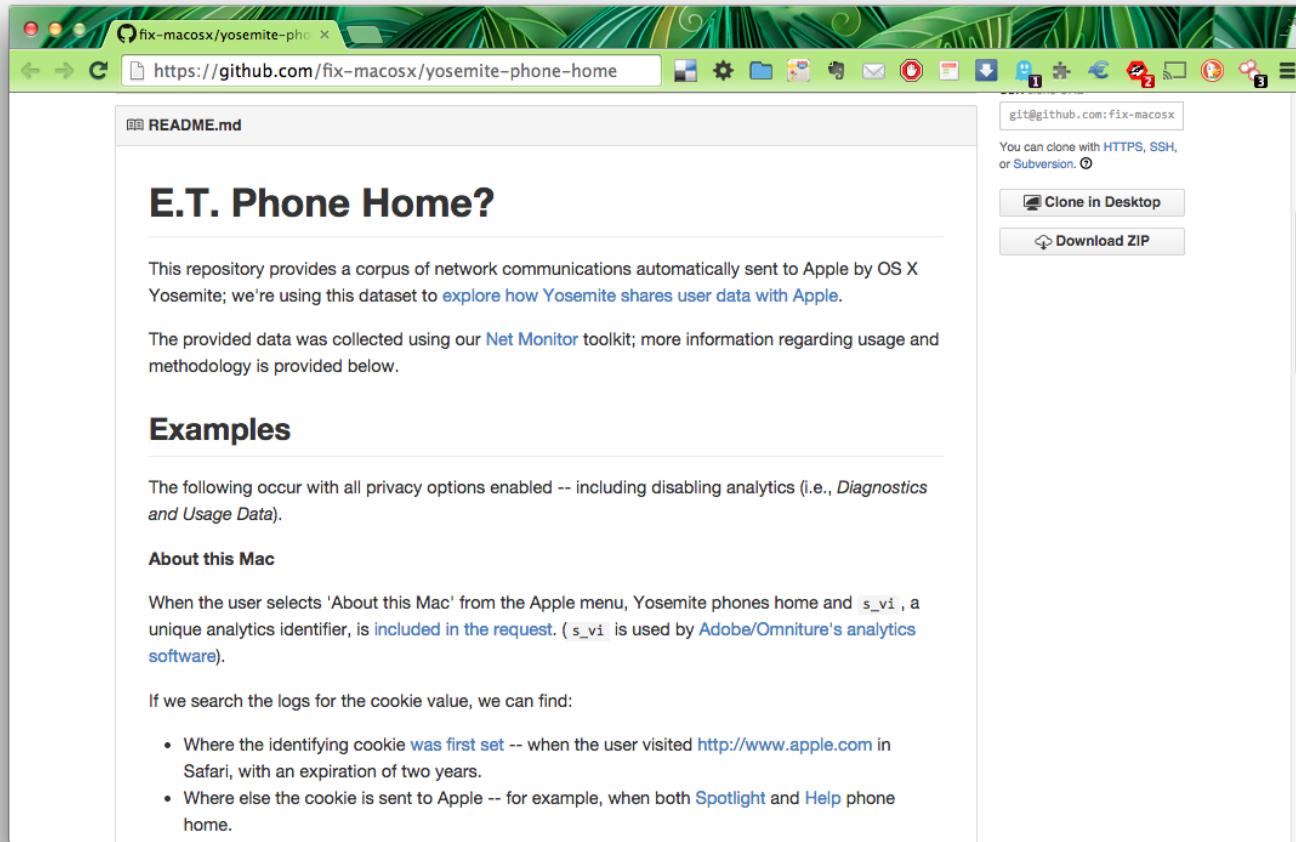
Configure systems to be secure by default, or change defaults

Use secure protocols and VPN solutions

Ubuntu Unity Privacy problems



Source: <https://fixubuntu.com/>



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

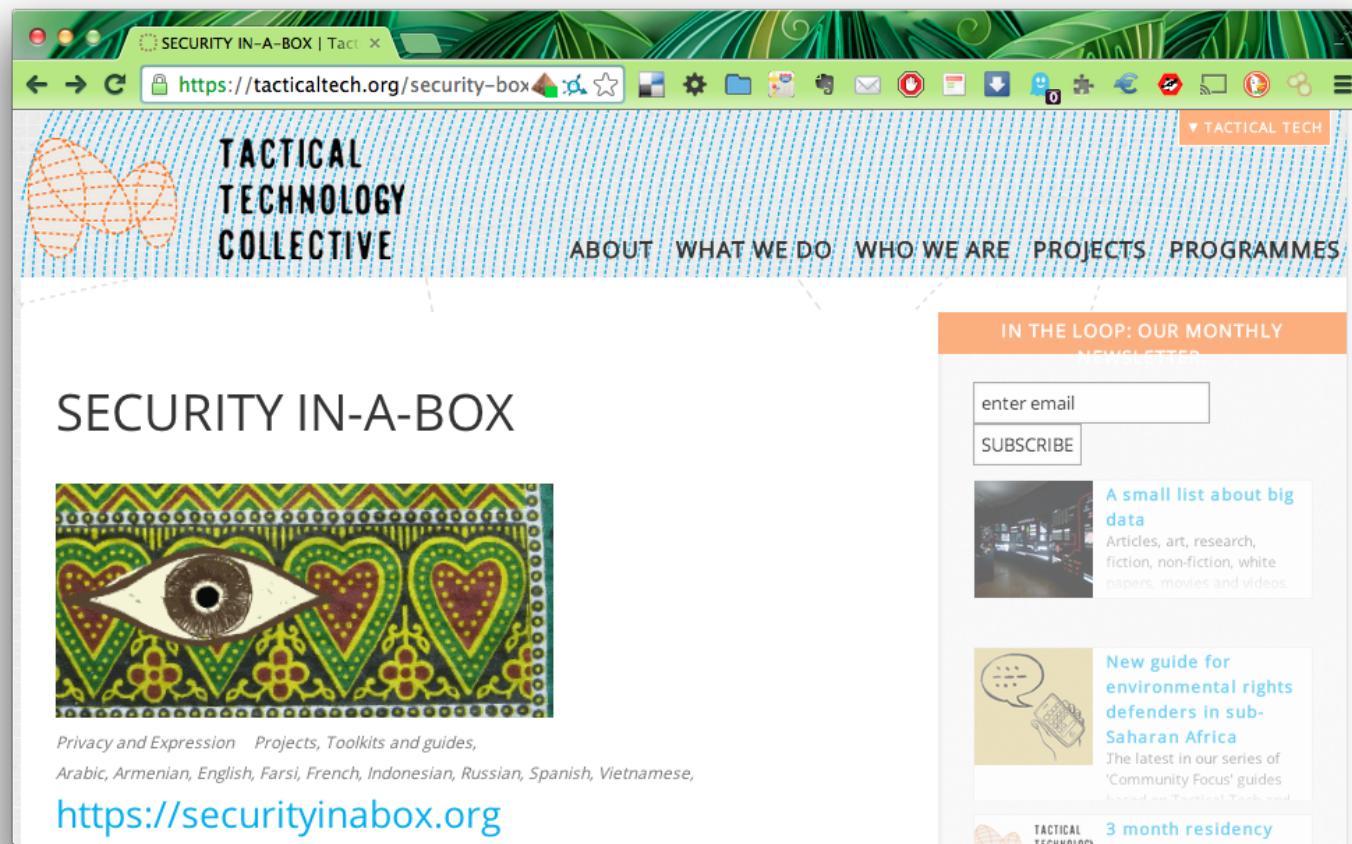


Tips, Tools and How-tos For Safer Online Communications

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/>

Følg med Twitter news



The screenshot shows the Twitter profile for the account @safety, which is verified. The profile bio reads: "Twitter's Trust and Safety Updates! http://help.twitter.com/forums/10711/entries/76036". Below the bio, there is a green "Following" button, a reply icon, and a direct message icon. A text input field says "Tweet to @safety". The navigation bar includes "Tweets" (which is selected), "Favorites", "Following", "Followers", and "Lists". Three tweets from the account are listed:

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

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me



Team up!

We need to share security information freely

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

- 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 afholder CTF konkurrence fredag den 28. november 2014 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

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>