Welcome to

Overvågning og IT-sikkerhed

Nyborg Strand 2014

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

Planen idag

Don’t Panic!

Kl 16:15-18:00 - med pause

Mindre enetale, mere foredrag 2.0 med sociale medier, informationsdeling og interaktion

Send gerne spørgsmål senere

PS er her nogle timer efter foredraget til spørgsmål og snak

The current situation

Internet security sucks

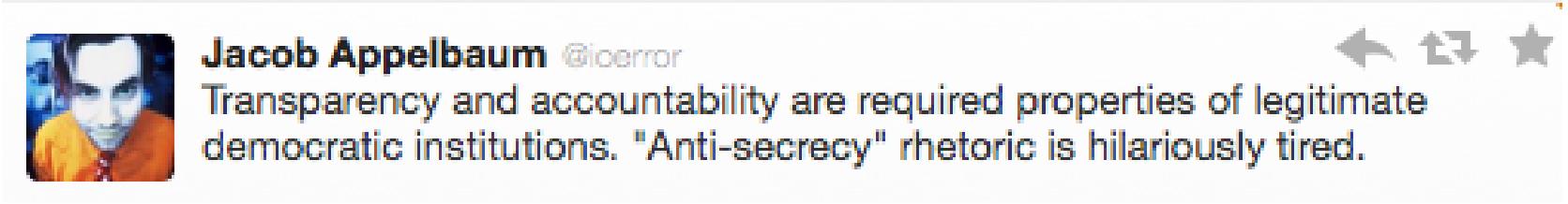
Personal computers like laptops suck at security

Mobile devices suck even more at security - less CPU/MEM/storage

We depend on cloud services and underfunded infrastructure - OpenSSL

We depend on others and the whole internet - DDoS

Goals: Why?

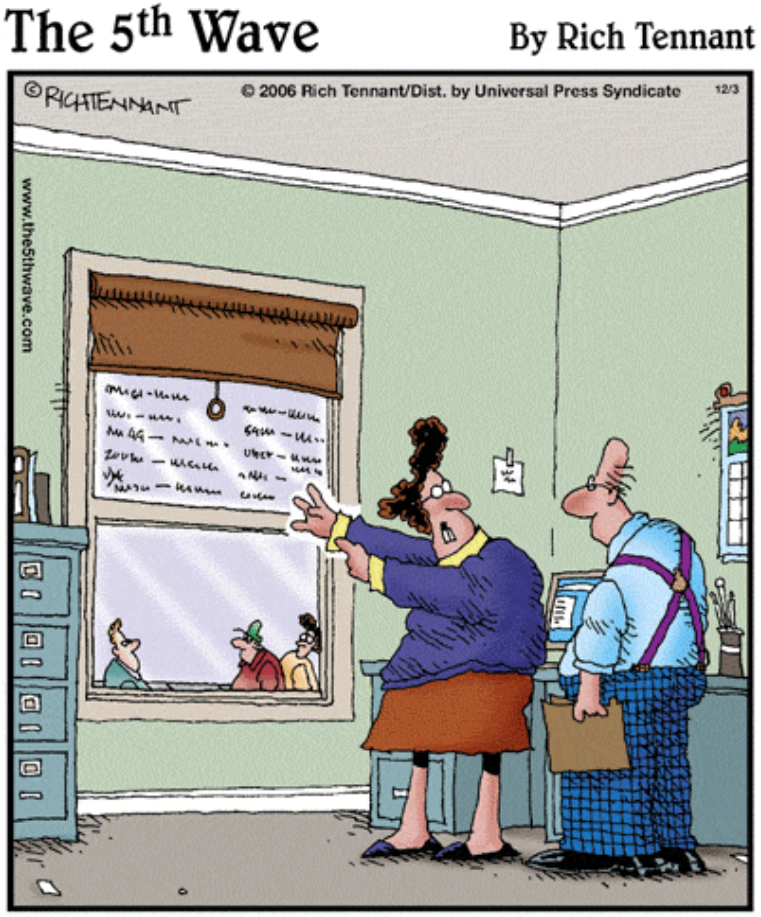


Jacob Appelbaum:
If Everything is Under Surveillance, How Can We Have a Democracy?

Democracy: A free democracy must allow citizens to take decisions without constant surveillance, which are free to use cryptography to control who we allow access to our data.

Crypto is a peaceful protest

Formål: sund paranoia



"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."

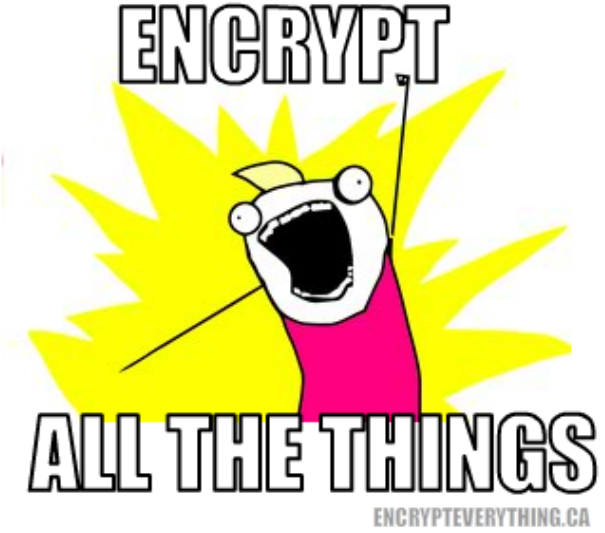
Opbevaring af passwords

Generic advice

SOLIDO NETWORKS

Recommendations

- Lock your devices, phones, tables and computers
- Update software and apps
- Do NOT use the same password everywhere
- Watch out when using open wifi-networks
- Multiple browsers: one for Facebook, and separate for home banking apps?
- Multiple laptops? One for private data, one for work?
- Think of the data you produce, why do people take naked pictures and SnapChat them?
- Use pseudonyms and aliases, do not use your real name everywhere
- Enable encryption: IMAP**S** POP3**S** HTTP**S** TOR OpenPGP VPN SSL/TLS



Security is magic

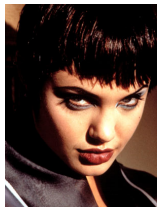
.

Think security always appropriate paranoia

Follow news about software security

Support communties, join and learn

Hackerværktøjer er også til dig!



- Hackers work all the time to break stuff, Use hackertools:
- Nmap, Nping `http://nmap.org`
- Wireshark - `http://http://www.wireshark.org/`
- Aircrack-ng `http://www.aircrack-ng.org/`
- Metasploit Framework `http://www.metasploit.com/`
- Burpsuite `http://portswigger.net/burp/`
- Skipfish `http://code.google.com/p/skipfish/`
- Kali Linux `http://www.kali.org`

Most popular hacker tools `http://sectools.org/`

Kali Linux the new backtrack

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

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

100.000s of videos on youtube: ”kali hack” 60.000, ”backtrack hack” 125.000

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`

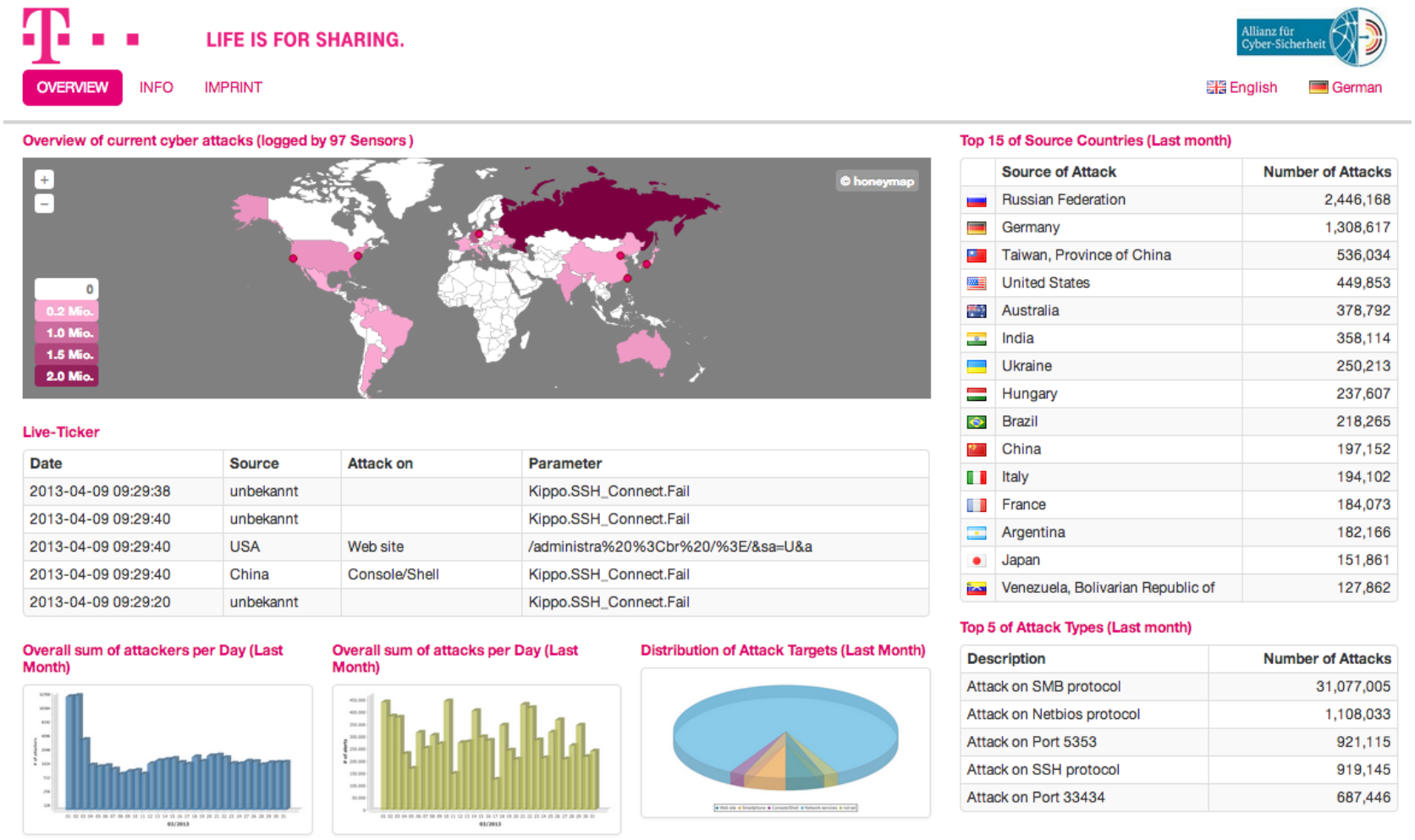
Heartbleed hacking

```
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_ins
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 XX XX XX XX XX XX XX XX XX XX XX XX XX XX 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.

Nothing more about HB in this presentation - we have better things to discuss

Attack overview



http://www.sicherheitstacho.eu/?lang=en

Protect yourself: 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`

Use protection - always

Indsamlede data vil altid blive misbrugt

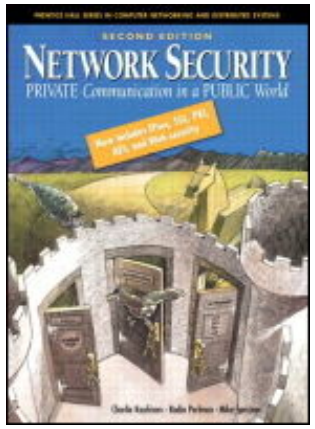
Data som indsamles **bliver misbrugt** enten til kriminelle formål, kommercielle formål uanset oprindelige formål med indsamlingen - under dække af beskyttelse mod terror, ekstremisme, nazisme, misbrug af børn, ... Le mal du jour / dagens onde.

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

Du bestemmer - det er privatliv og demokrati

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

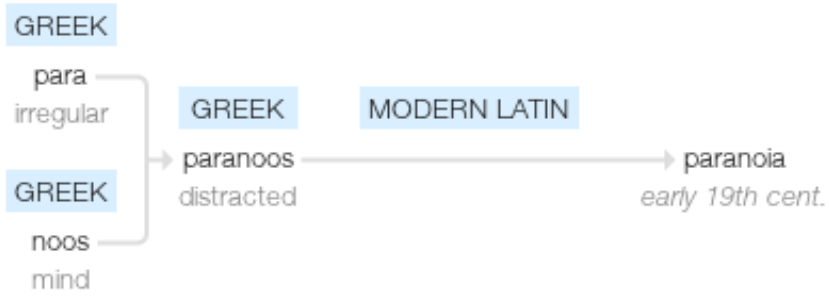
/ˌparəˈnoiə/

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 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!

Risk management defined

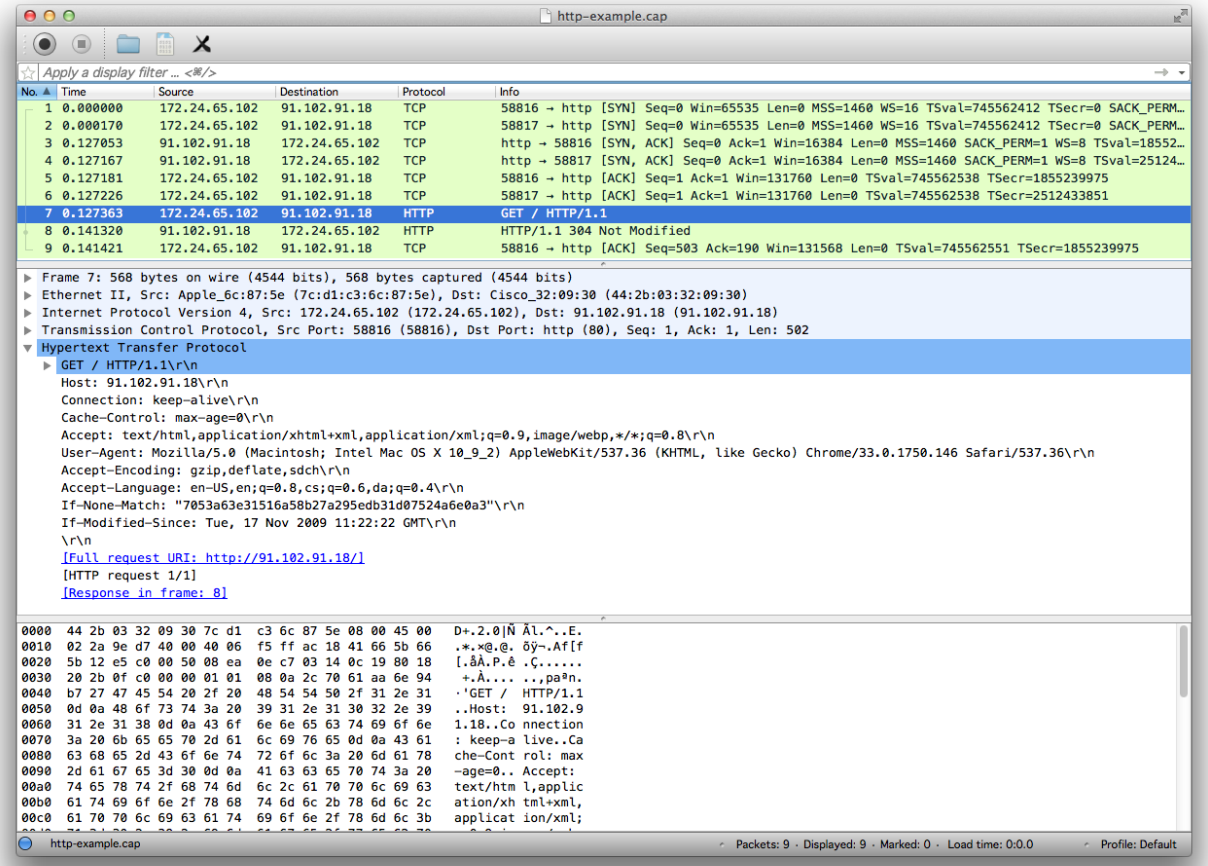
Information Risk Management

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*

Wireshark - grafisk pakkesniffer



http://www.wireshark.org

både til Windows og Unix

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 er magi

Hacking ligner indimellem magi

Hacking er ikke magi

Hacking kræver blot lidt ninja-træning

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`

Quick Wins: Opsec Light

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 ☺

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.

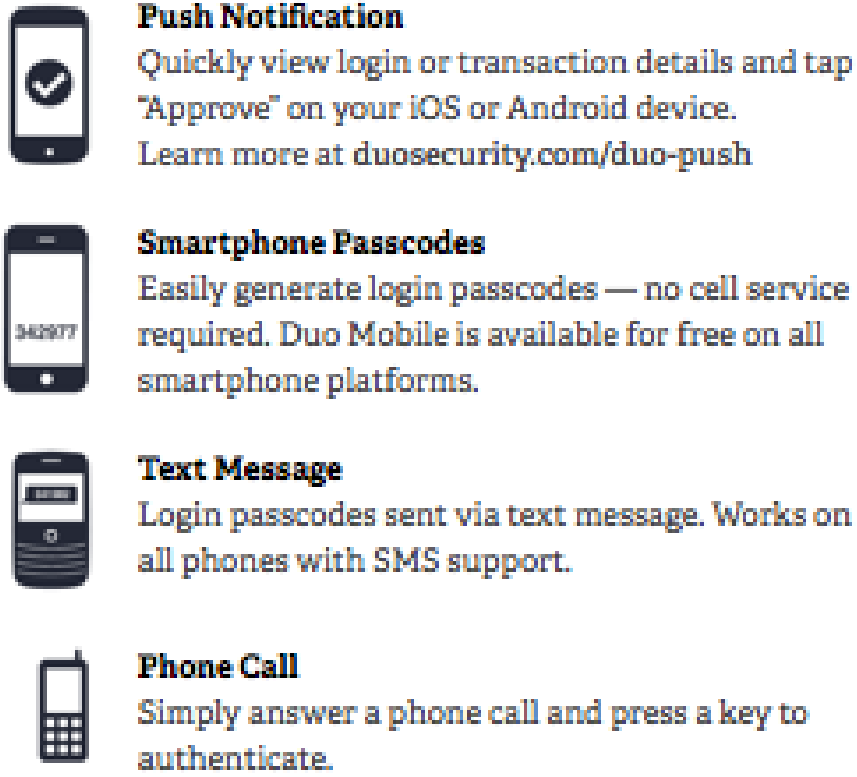
› Password Safe YubiKey

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.

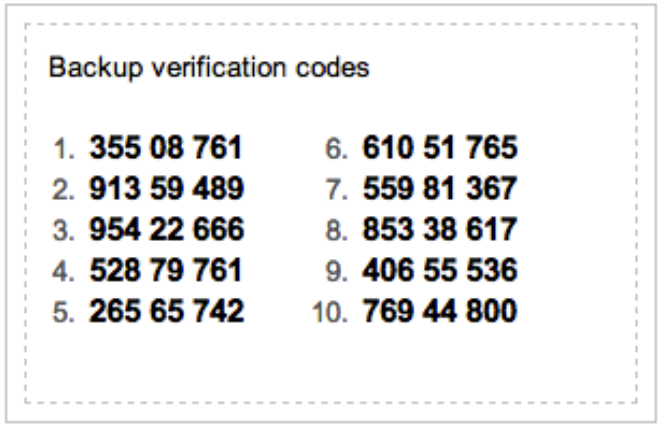
Video `https://www.duosecurity.com/duo-push`

`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?

SOLIDO NETWORKS

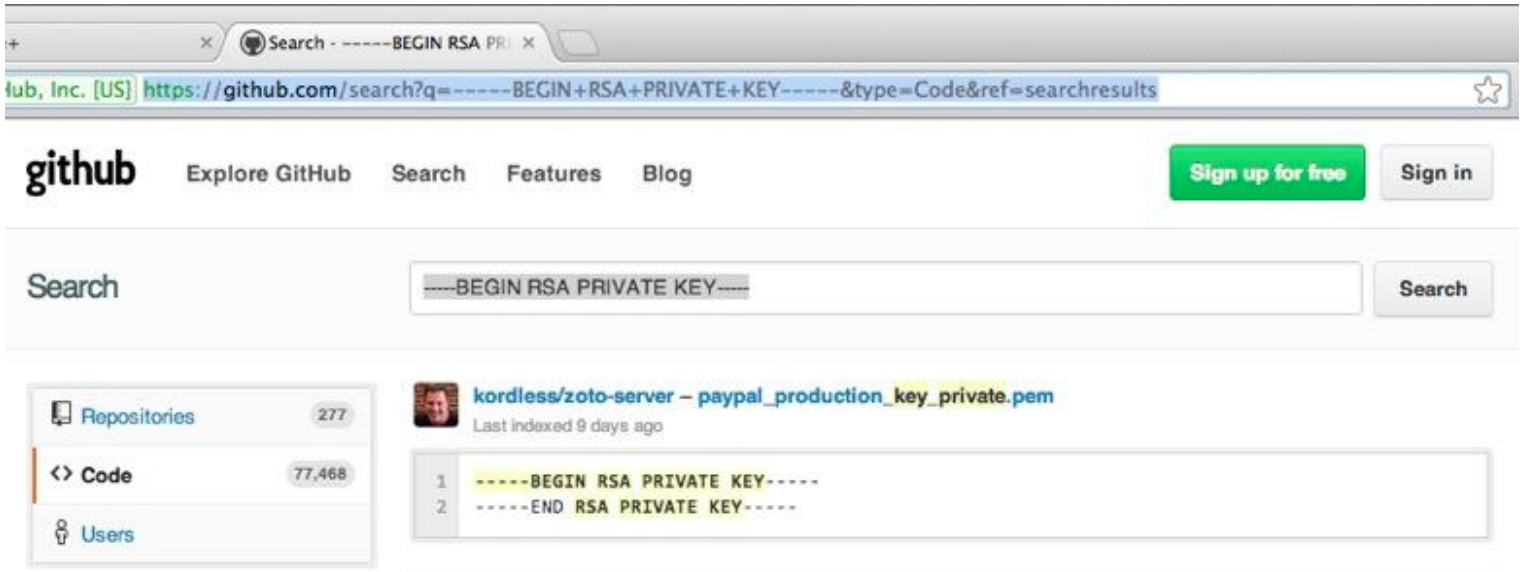
Dont:

- 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

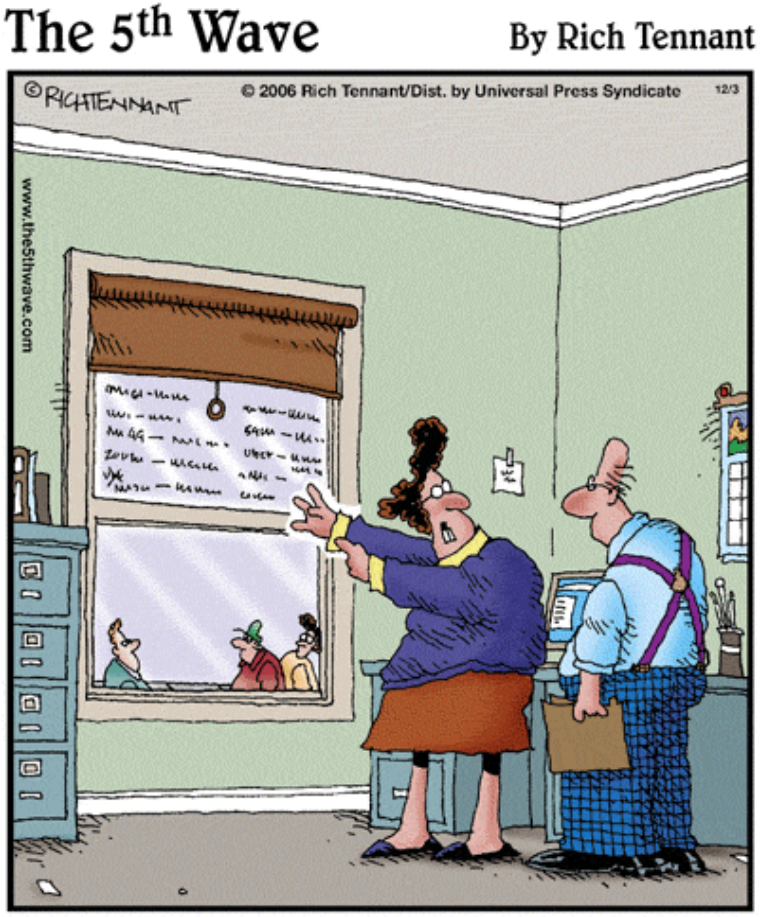
http://www.webmonkey.com/2013/01/users-scramble-as-github-search-exposes-passwords-security-de

http://www.leakedin.com/

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

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

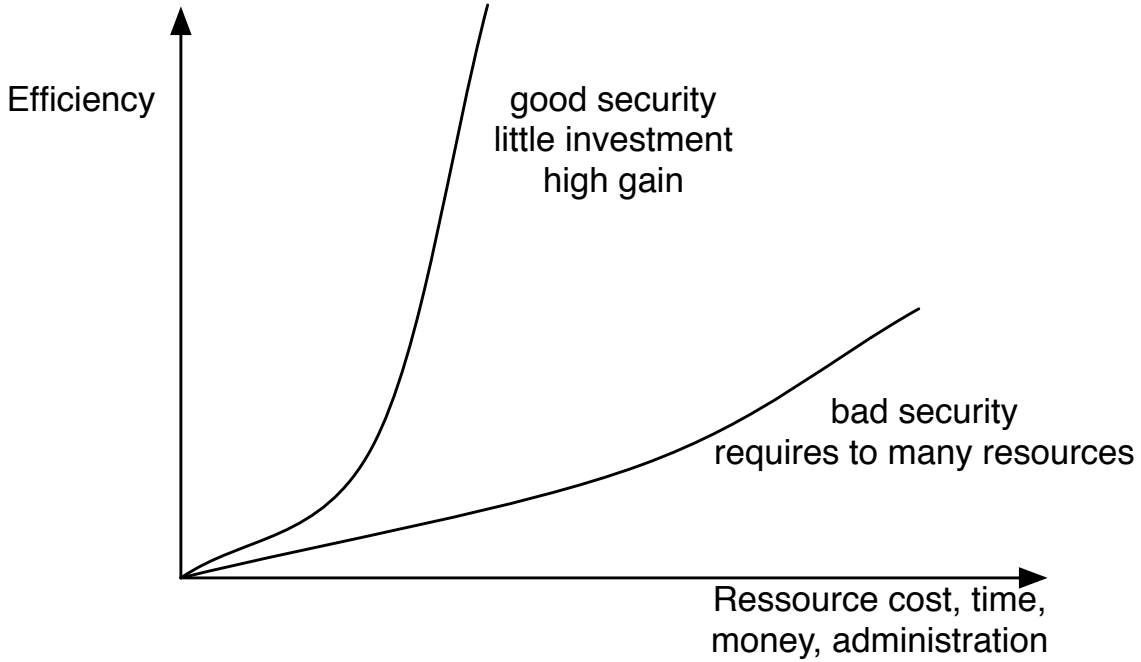
Opbevaring af passwords



"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

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

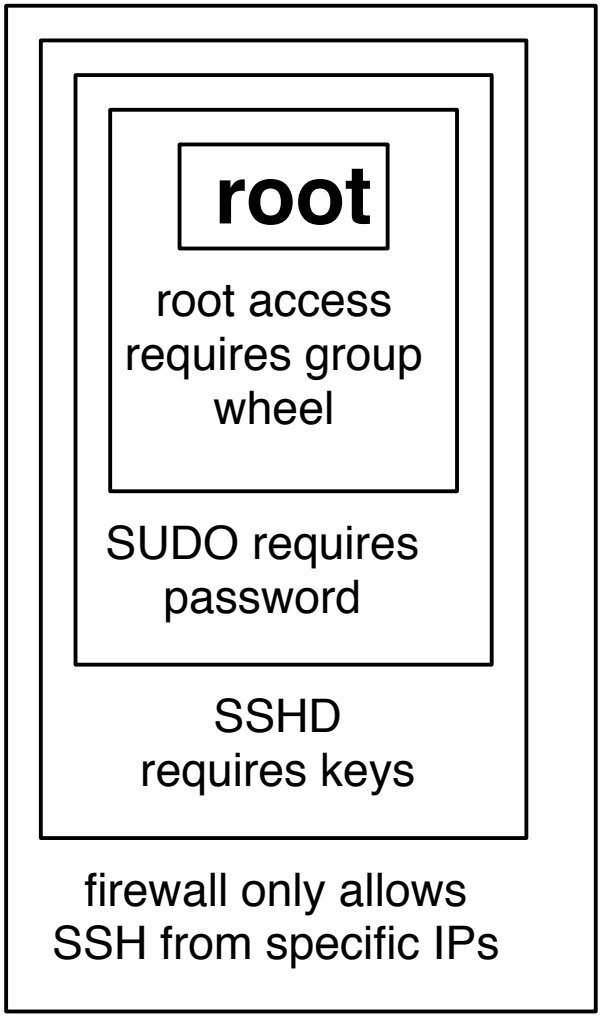
- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

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!

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`

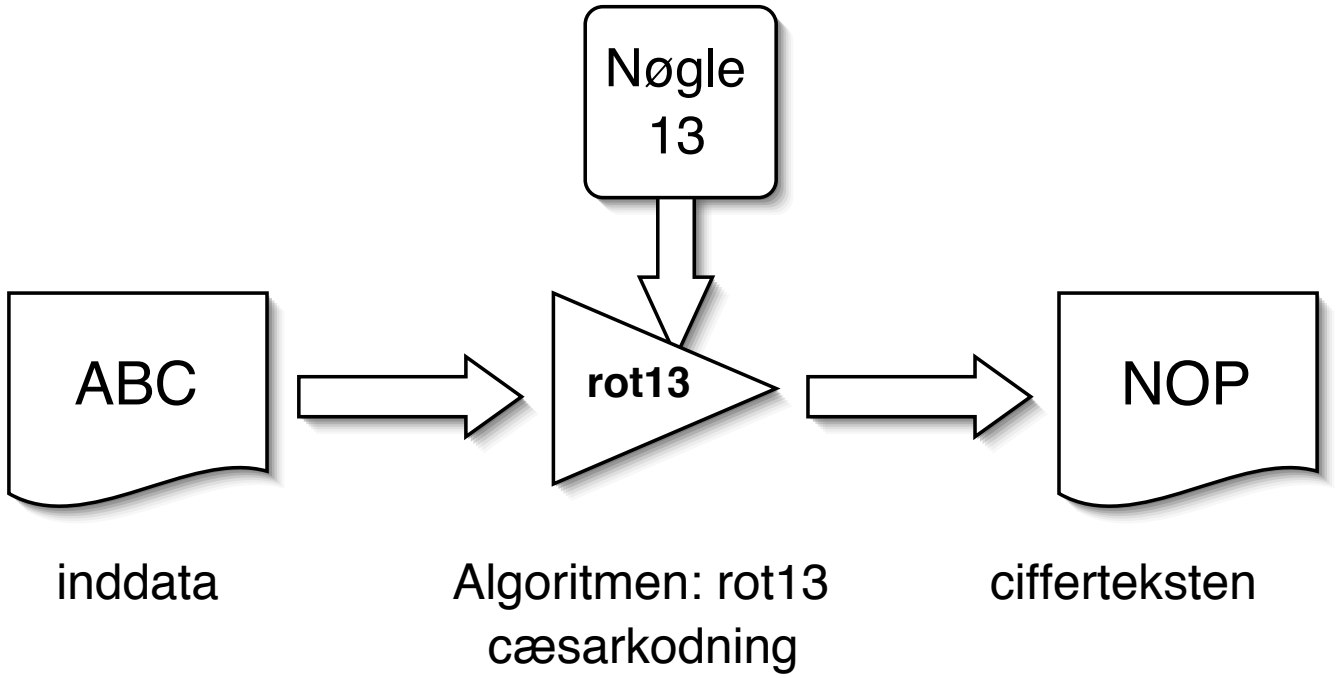
Formålet med kryptering

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet

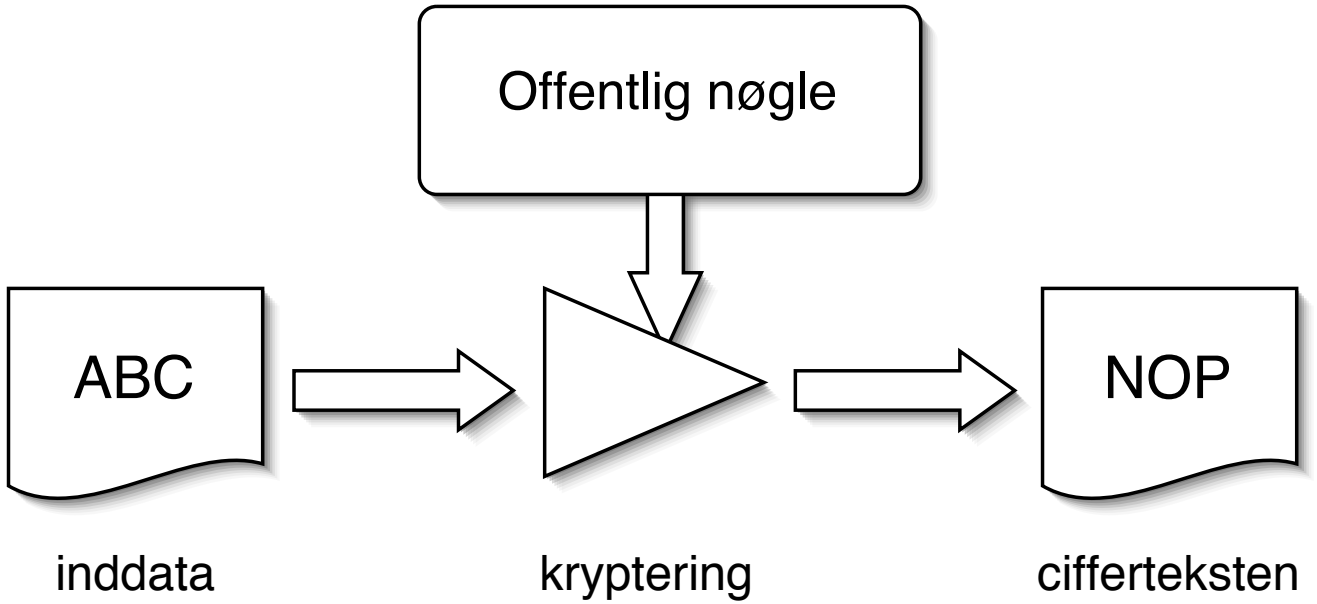
Kryptografi



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

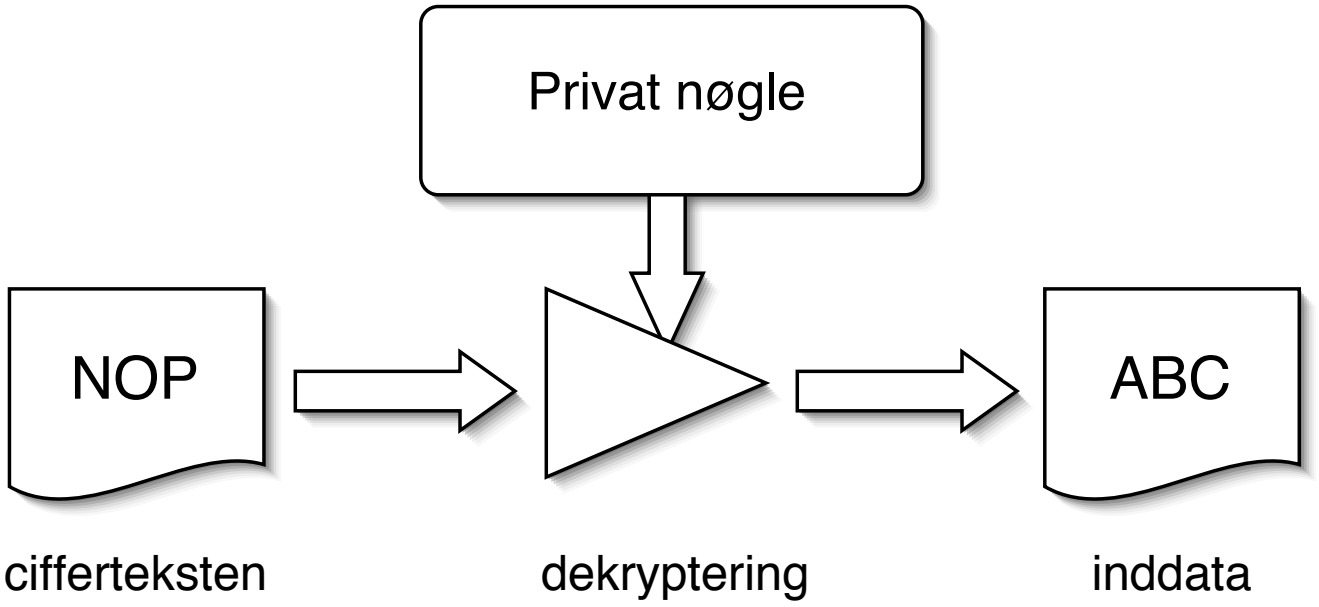
Public key kryptografi - 1



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

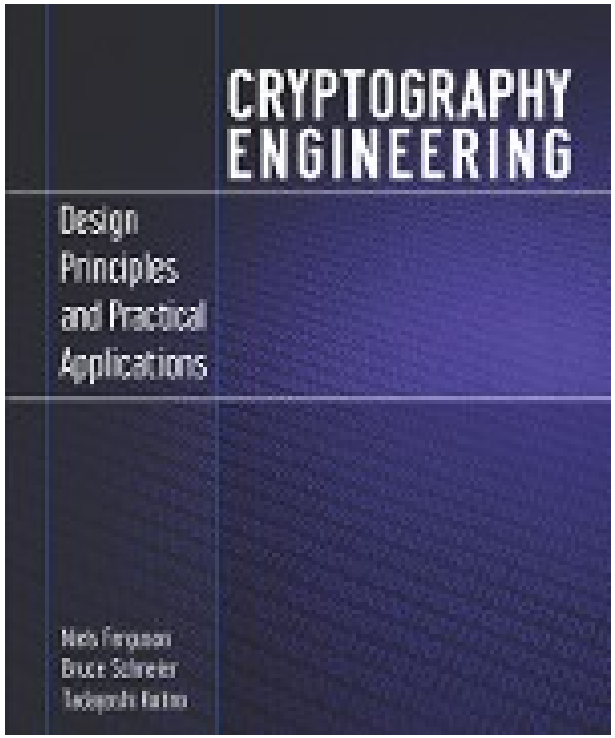
Public key kryptografi - 2



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

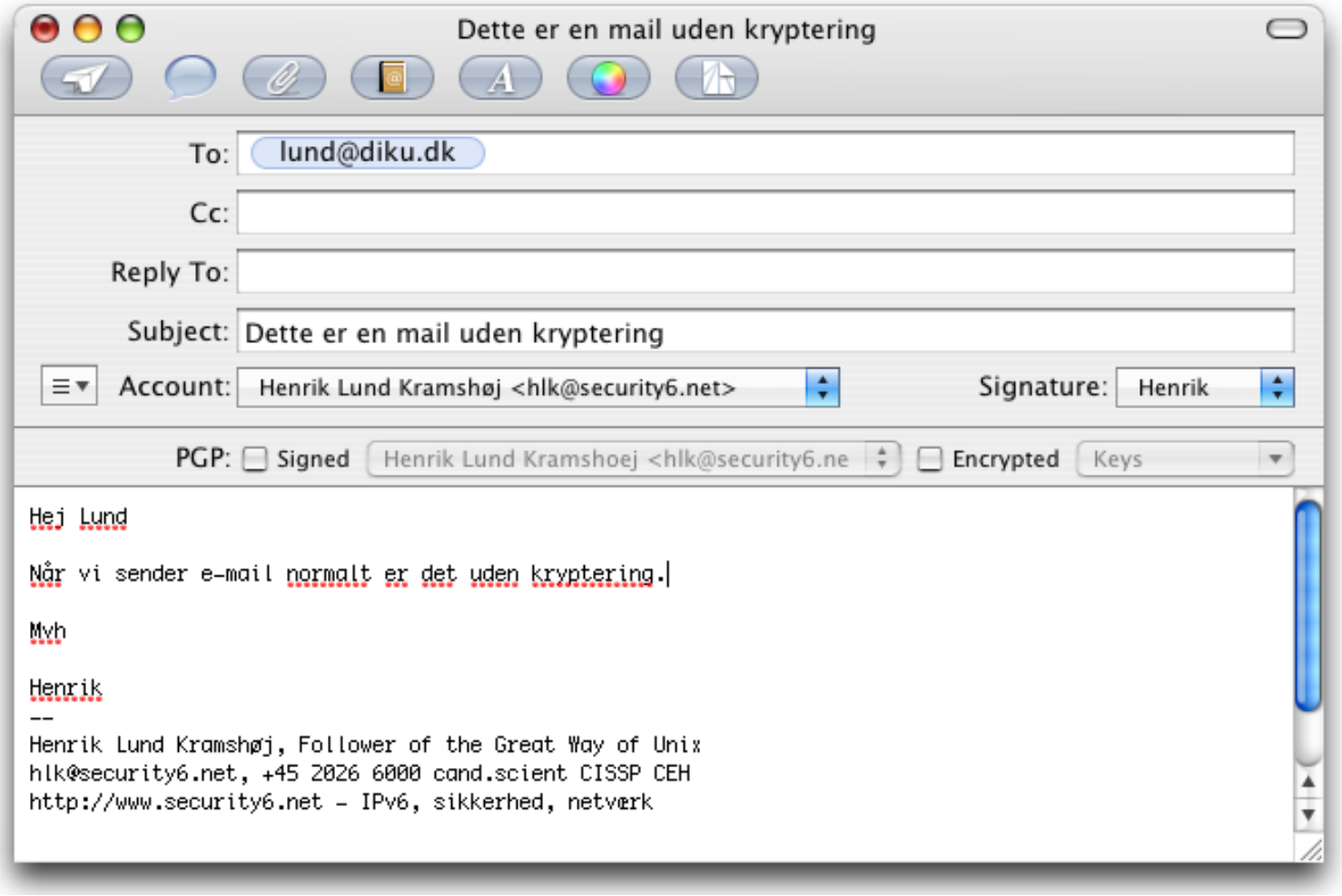
Cryptography Engineering



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

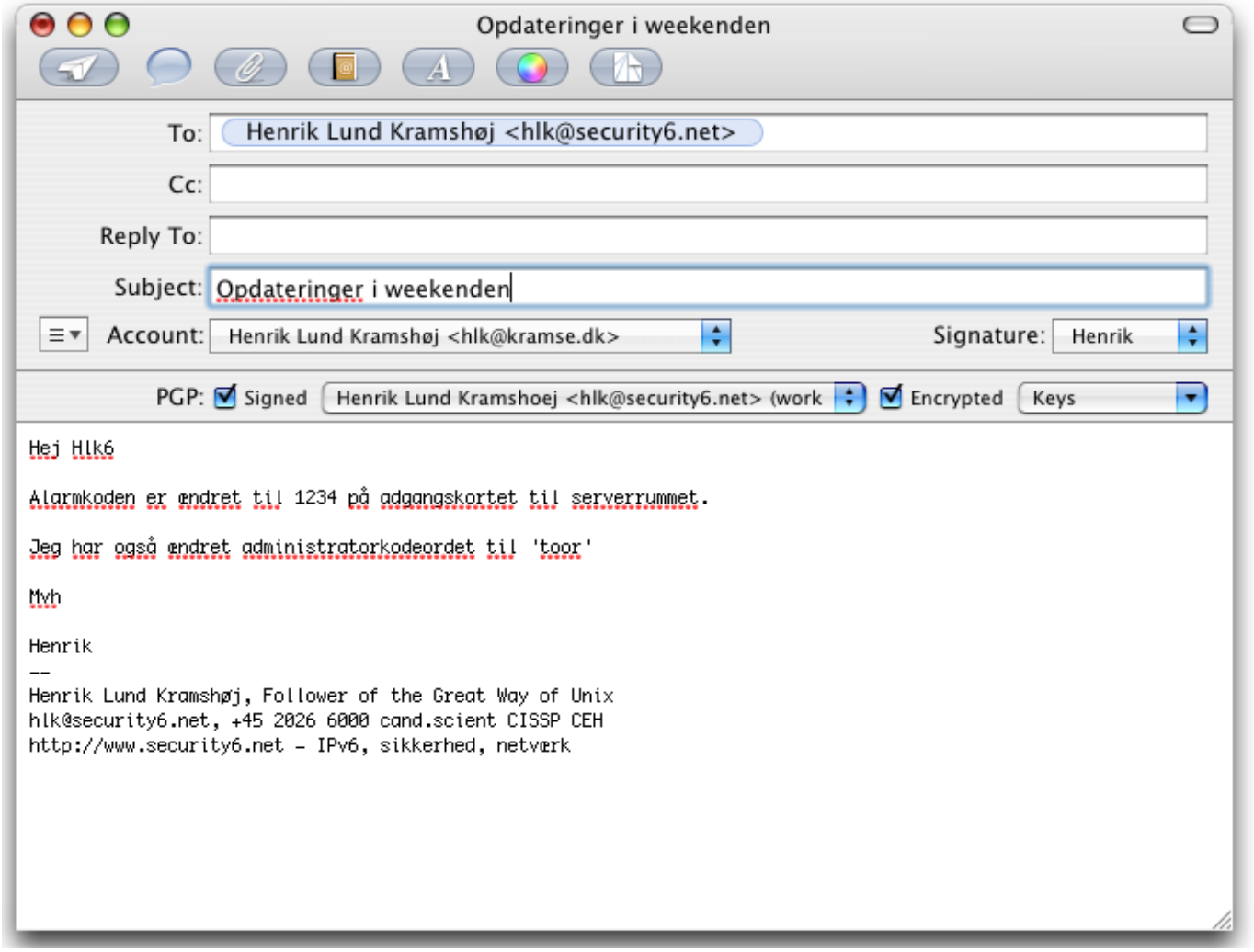
`https://www.schneier.com/book-ce.html`

Email is insecure



Email without encryption is like an open post card

Email with encryption - sending



Sending a secure email is not hard

Encrypted in transit

A secure email is protected while being transported

SOLIDO NETWORKS

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`

SOLIDO NETWORKS

```
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+\
  \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";
```

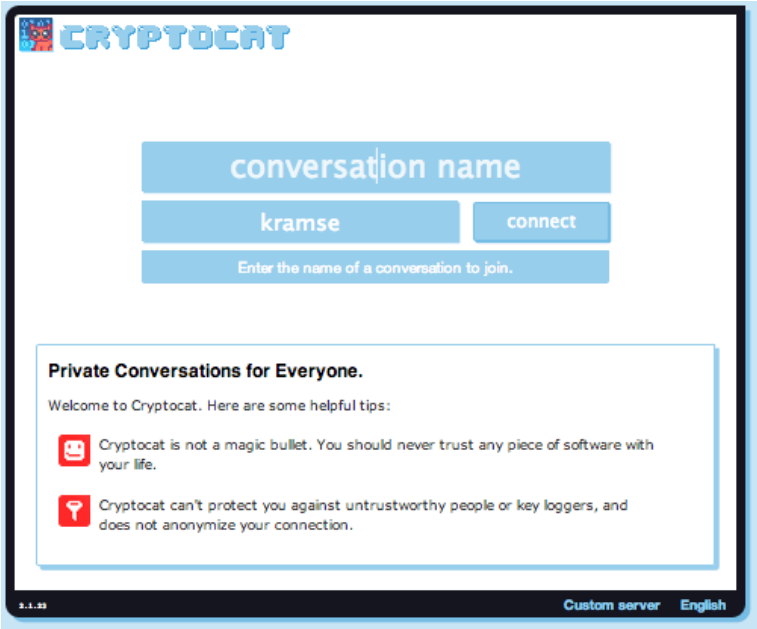
Listing 2.6: *SSL settings for nginx*
[configuration/Webservers/nginx/default]

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/`

Audits



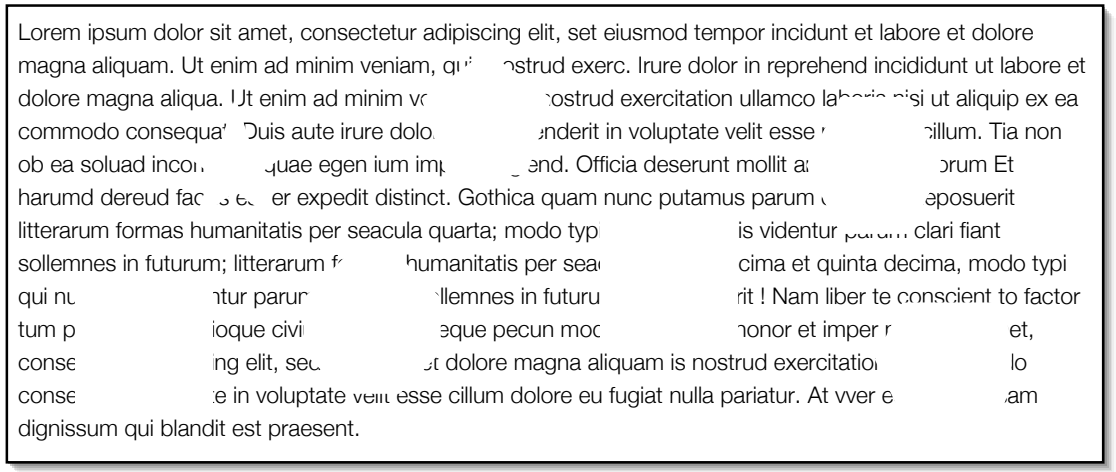
Truecrypt audit

`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/`

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`

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`

Attacks on disk encryption

SOLIDO NETWORKS

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?

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

Security breaches happens any day of the week

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?

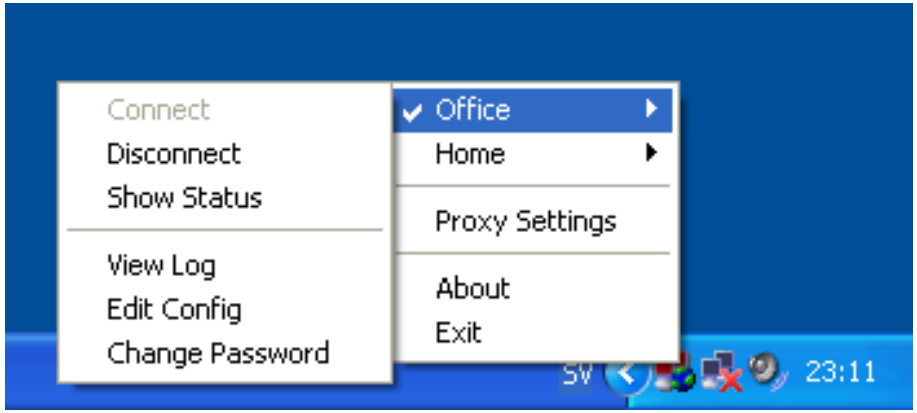
Duplicity backs directories by producing encrypted tar-format volumes and uploading them to a remote or local file server. Because duplicity uses librsync, the incremental archives are space efficient and only record the parts of files that have changed since the last backup. Because duplicity uses **GnuPG**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

Dont forget to DELETE data also, write over or physically destroy

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!

Multiple browsers

- 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

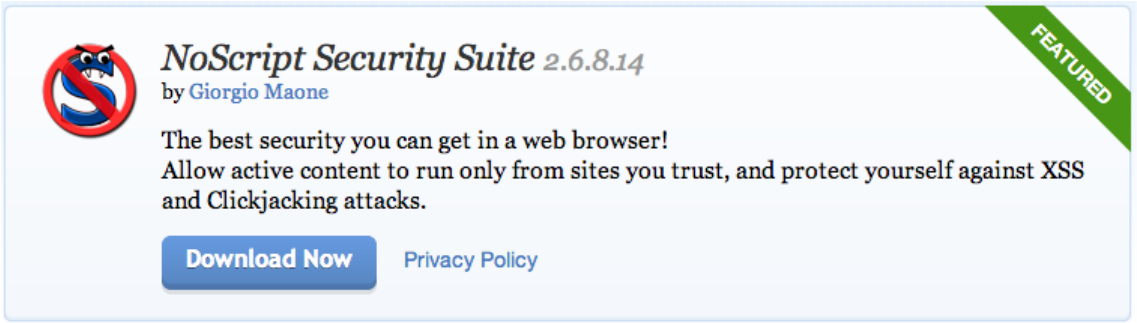
HTTPS Everywhere

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`

Also in Chrome web store!

NoScript and NotScripts



NotScripts
A clever extension that provides a high degree of 'NoScript' like control of javascript, iframes, and plugins on Google Chrome.

NoScripts for Firefox or NotScripts for Chrome
Only allow scripting and active content on pages where it is required

Pro tip: you can avoid lots of advertisements

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/`

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

Turkey: Erdogan bans Twitter

Censorship on the internet - lol

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)

Directly connection Tor Users from Turkey

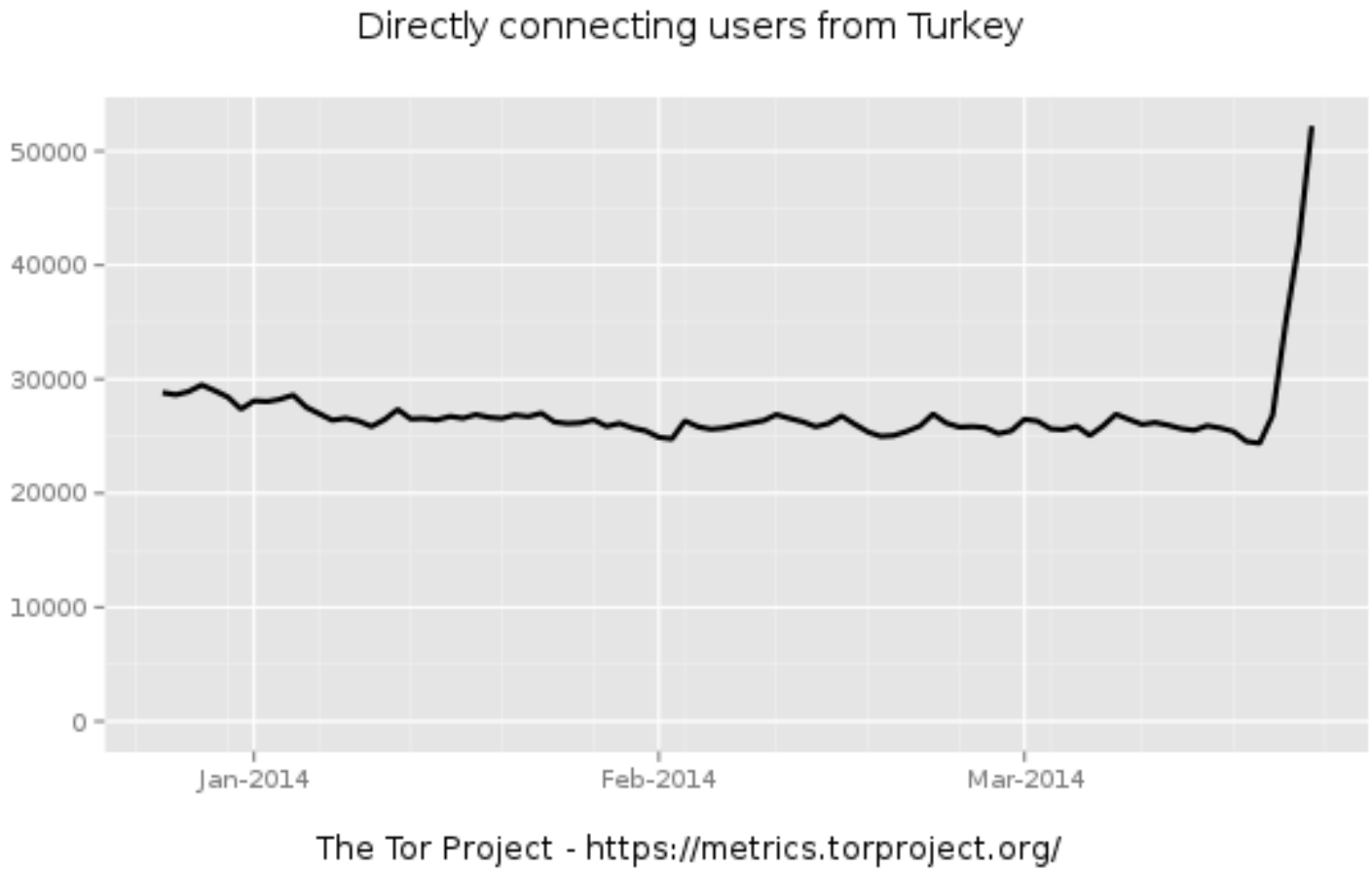


Image from `https://metrics.torproject.org`
via `https://twitter.com/runasand`

Directly connection Tor Users from Turkey +10.000

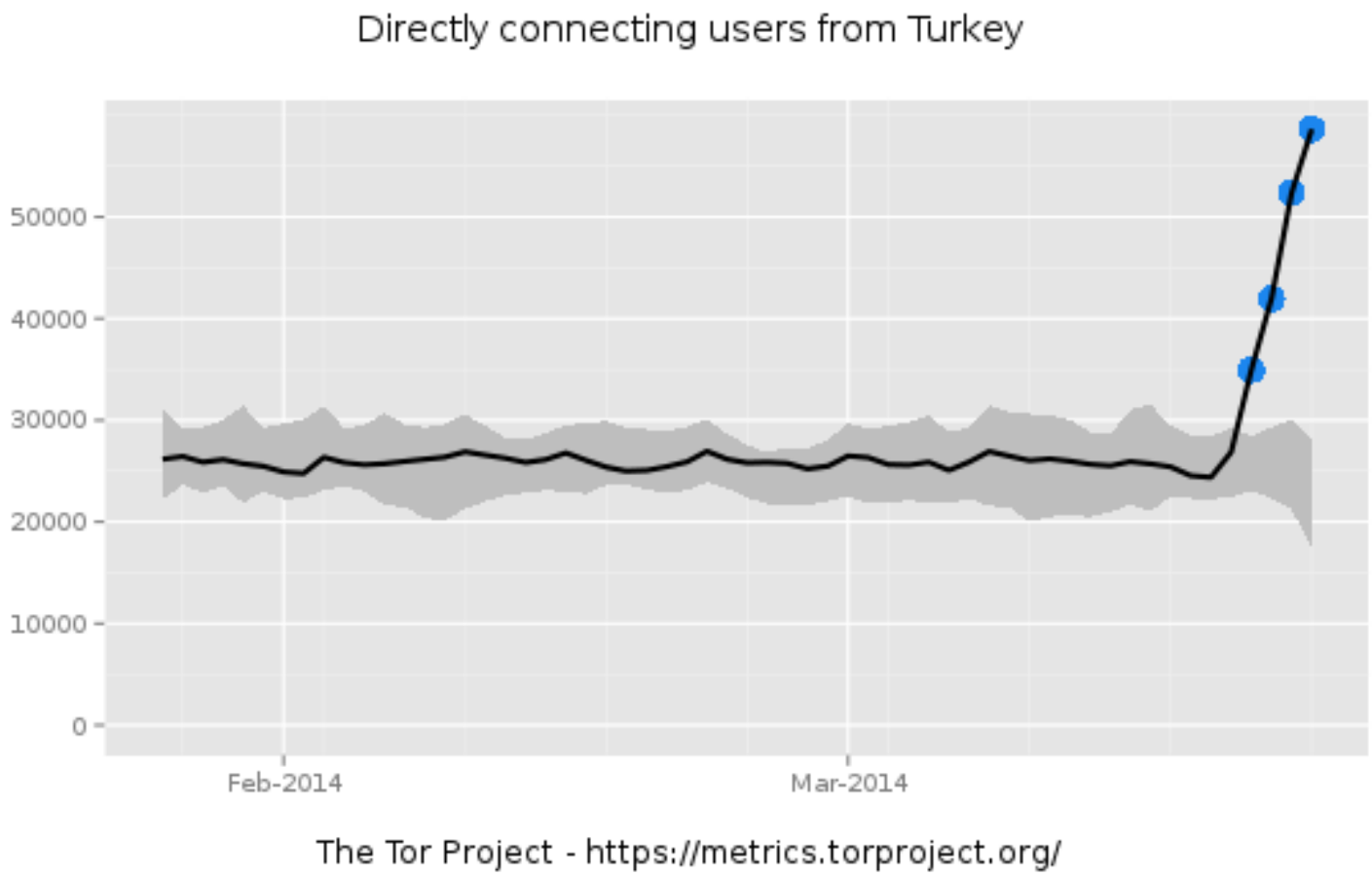
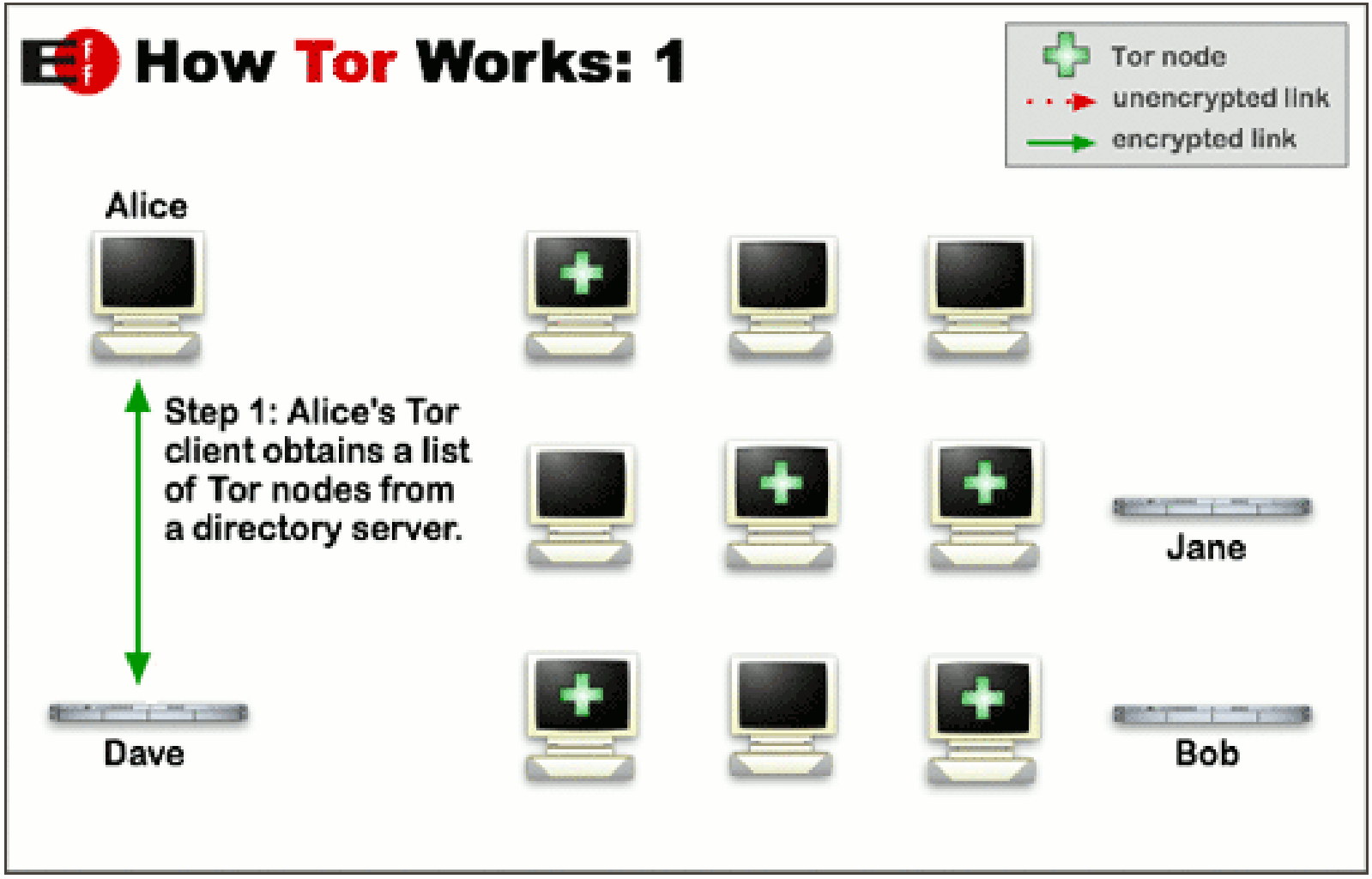


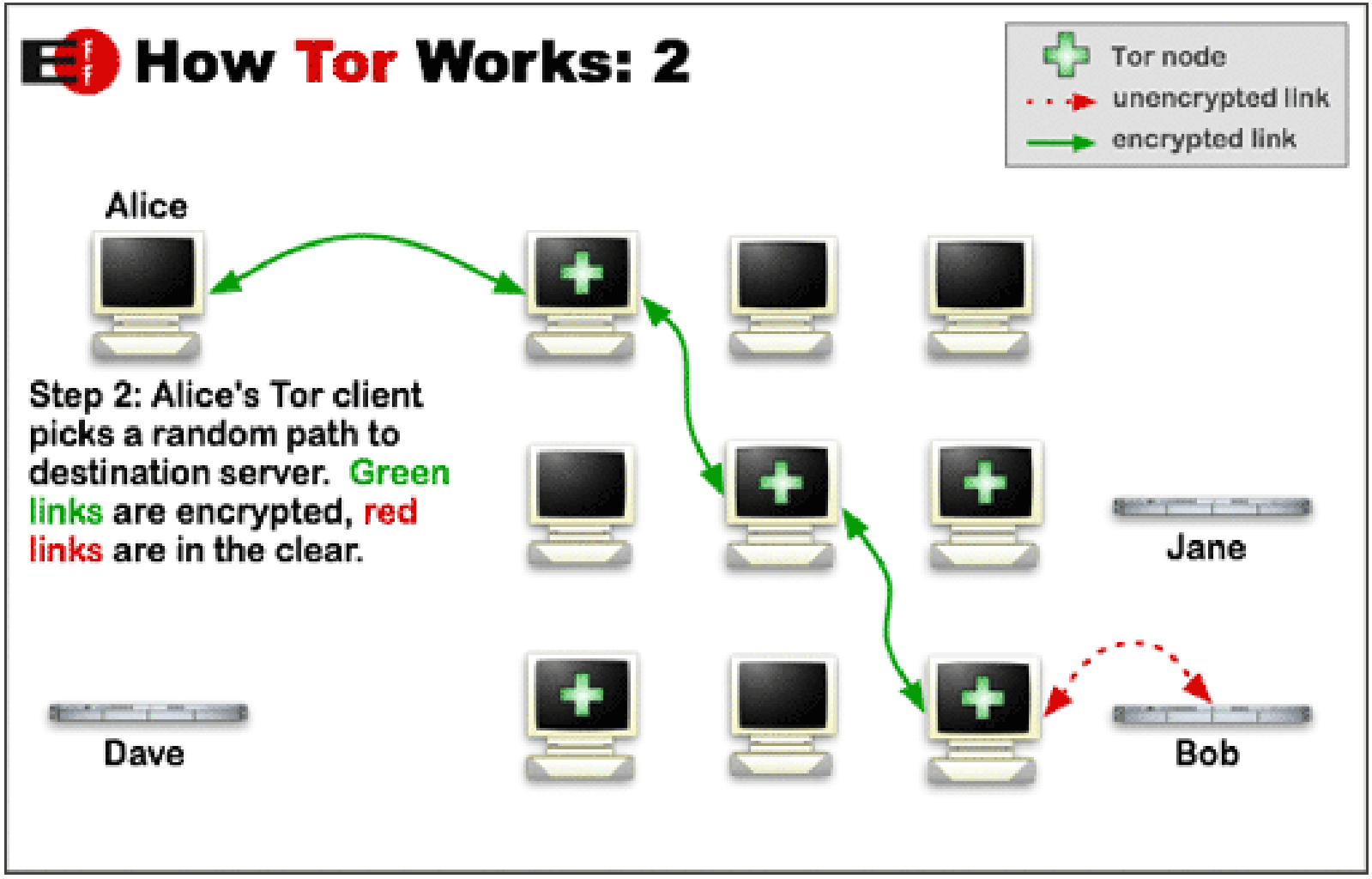
Image from `https://metrics.torproject.org` via `https://twitter.com/ioc32/status/448791582423408640`

Tor project - how it works 1



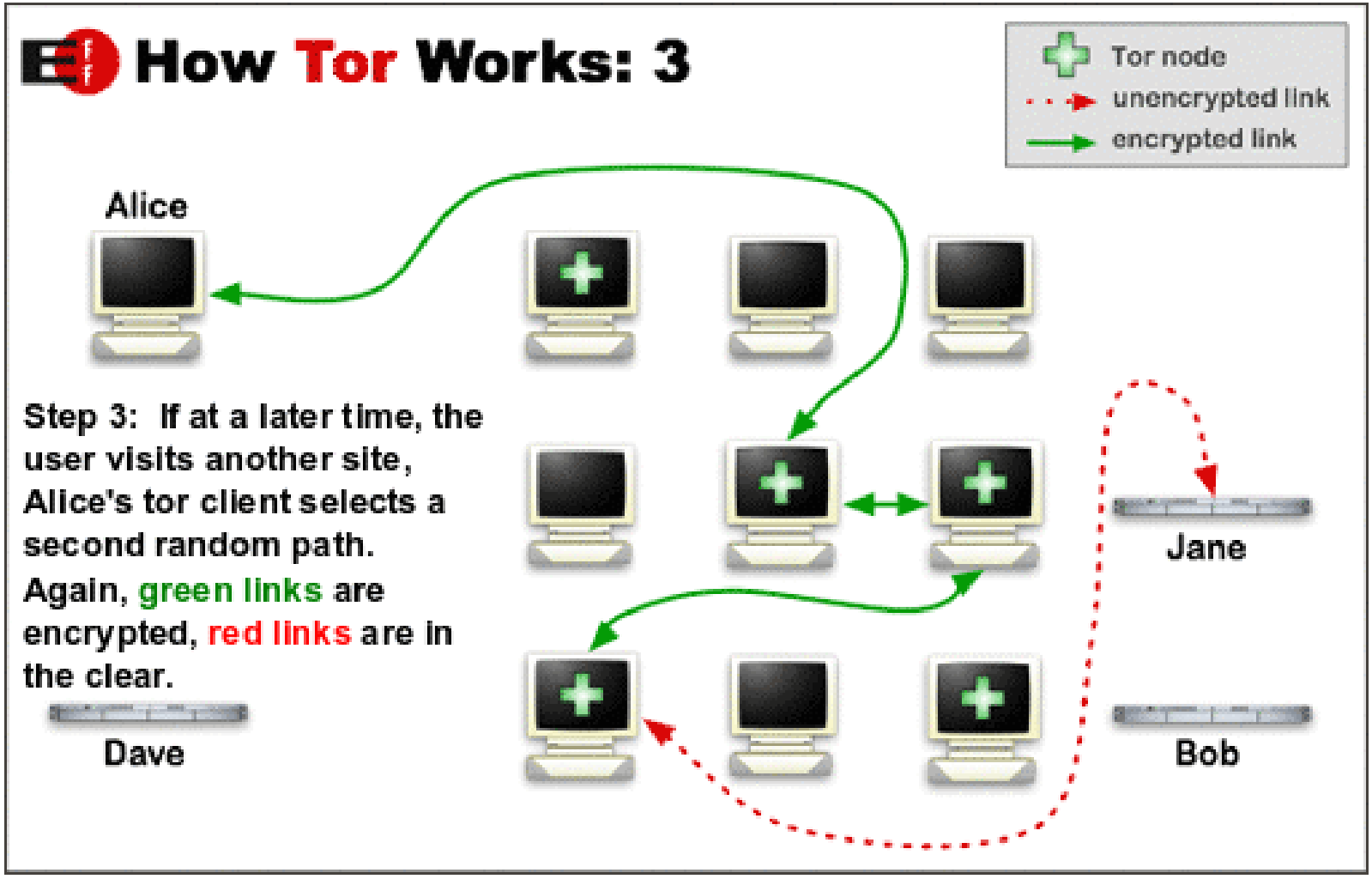
pictures from `https://www.torproject.org/about/overview.html.en`

Tor project - how it works 2



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

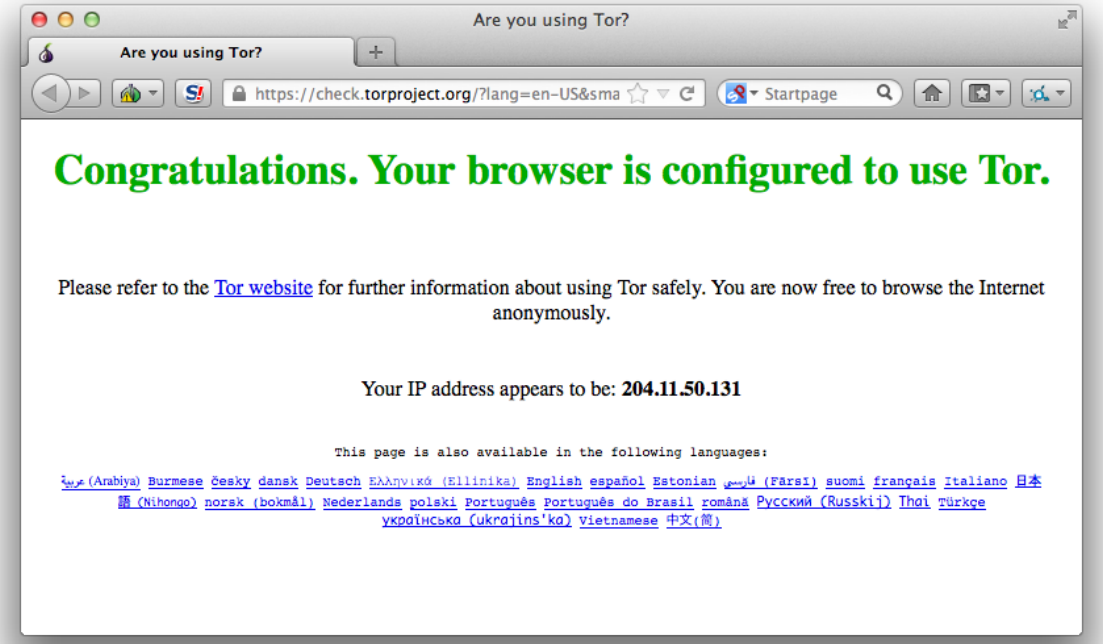
Tor project - how it works 3

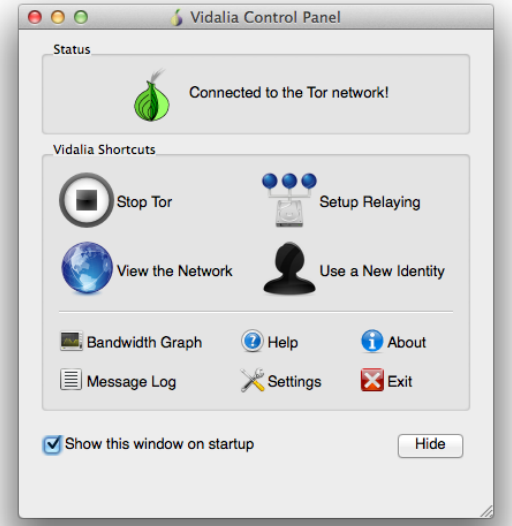


pictures from `https://www.torproject.org/about/overview.html.en`

Using Tor

Recommendation is to run Tor browser





Also plugins to Firefox etc. beware of browser fingerprint and DNS leaks!

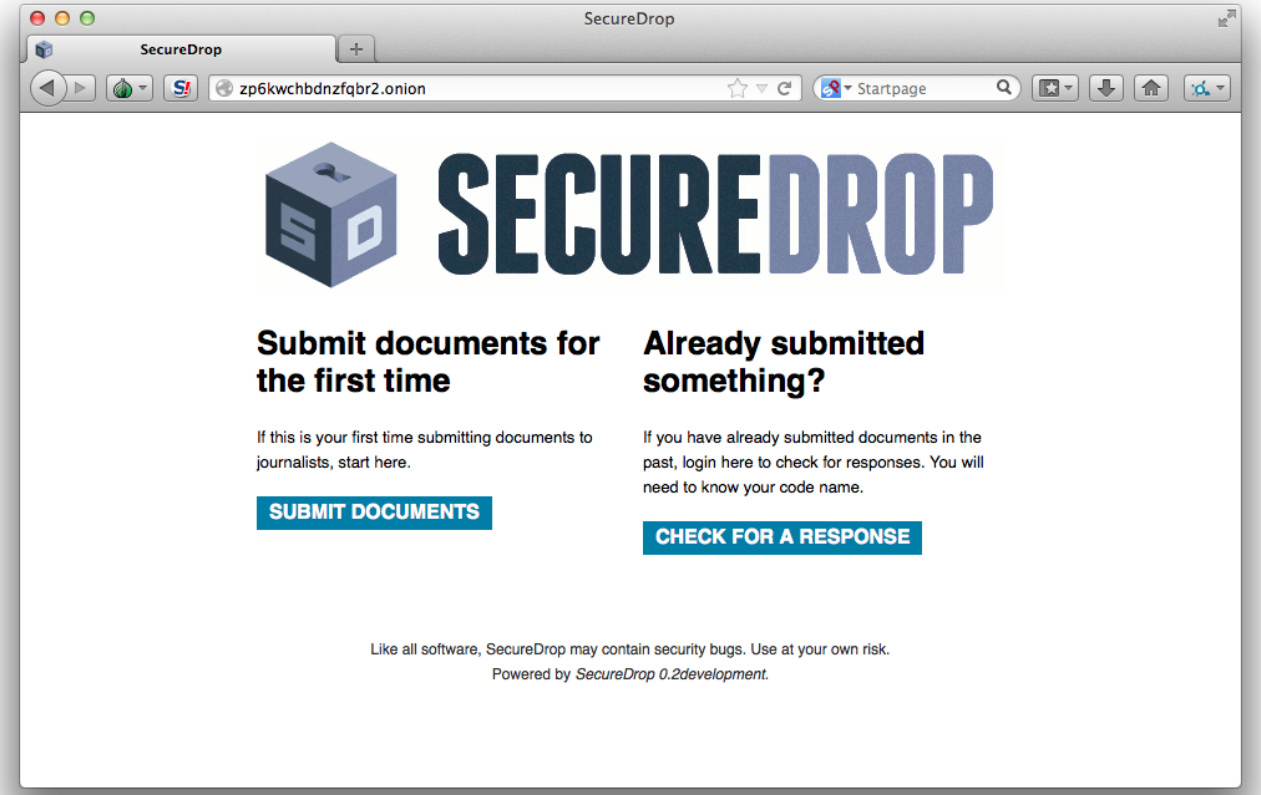
Torbrowser - outdated

Hov den mangler opdatering!

Torbrowser - anonym browser

Mere anonym browser - Firefox i forklædning

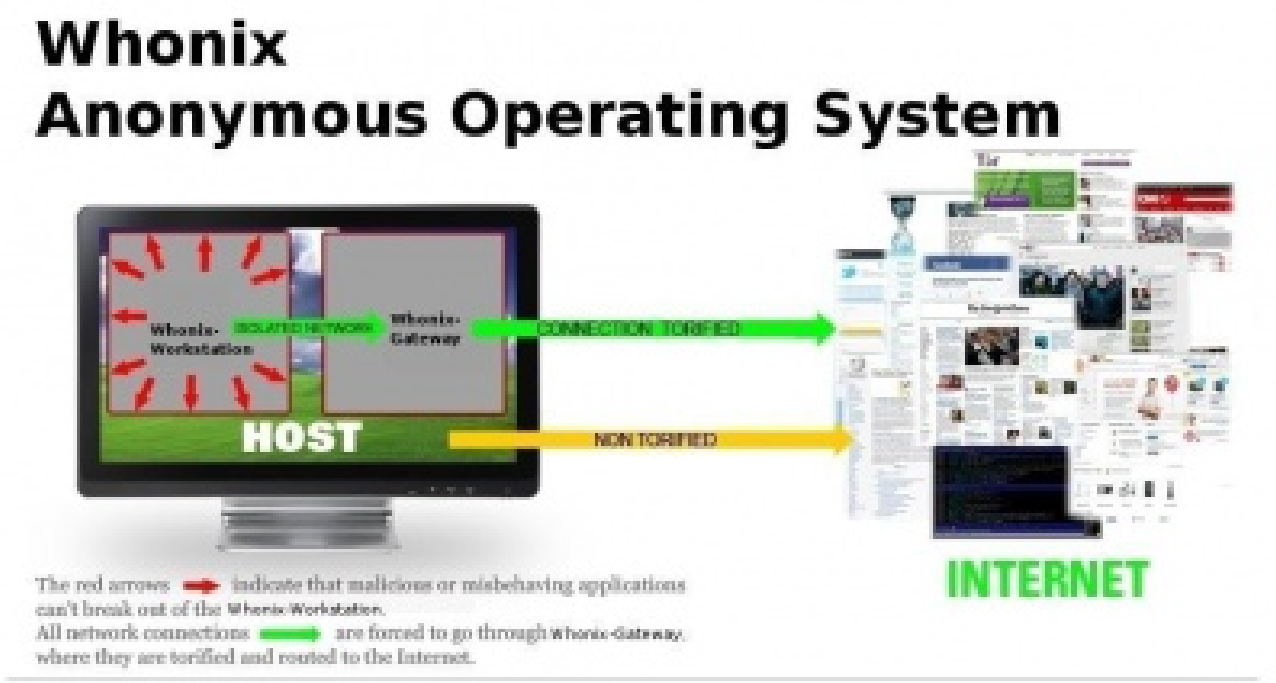
Torbrowser - sample site



.onion er Tor adresser - hidden sites

Den viste side er SecureDrop hos Radio24syv `http://www.radio24syv.dk/dig-og-radio24syv/securedrop/`

Whonix



Whonix is an operating system focused on anonymity, privacy and security. It's based on network[5], Debian GNU/Linux[6] and security by isolation. DNS leaks are impossible, ware with root privileges can find out the user's real IP.

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

Tor is BAD

The only users of Tor are bad people, BAD people I tell you!

Criminals

Drugs - lots of drugs

Terrorists planning World War IIIII

Pedophiles

More drugs - and high quality!

Copyright infringement

Did you know the roads are being used by criminals in the physical world

Tor History Inception

`http://www.onion-router.net/`

> This website comprises the onion-router.net site formerly hosted at the Center for High Assurance Computer Systems of the U.S. Naval Research Laboratory. It primarily covers the work done at NRL during the first decade of onion routing and reflects the onion-router.net site roughly as it existed circa 2005. As a historical site it may contain dead external links and other signs of age.

Accessnow.org

Access defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

Helping out - run a relay

Tor Network Status -- Router Detail

General Information	
Router Name:	kramse
Fingerprint:	3C5D F71E 0358 B535 4FC3 9847 4CED BC27 88DE E62F
Contact:	Henrik Lund Kramshoej <hlk AT solido dot net>
IP Address:	94.126.178.1
Hostname:	tor-exit01.solidonetworks.com
Onion Router Port:	9001
Directory Server Port:	9030
Country Code:	DK
Platform / Version:	Tor 0.2.4.17-rc on FreeBSD
Last Descriptor Published (GMT):	2013-11-04 01:49:54
Current Uptime:	14 Day(s), 10 Hour(s), 56 Minute(s), 3 Second(s)
Bandwidth (Max/Burst/Observed - In Bps):	524288000 / 524288000 / 7262872
Family:	No Info Given

solidaritetskryptering

more expensive to do *blanket surveillance* and focus will switch to targeted monitoring!

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/`

How to become secure

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

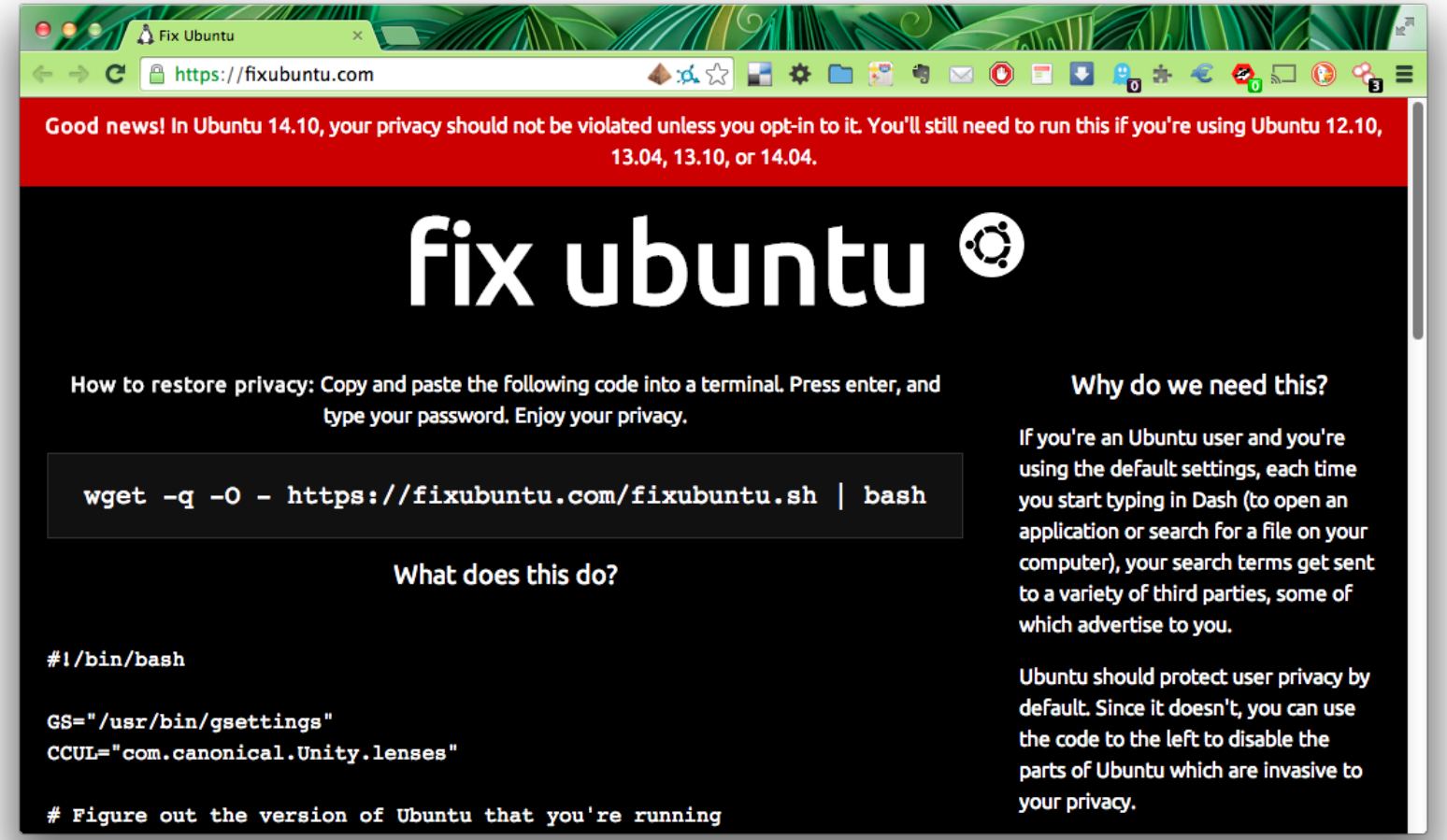
Dont use a single device for all types of data

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

Configure systems to be secure by default, or change defaults

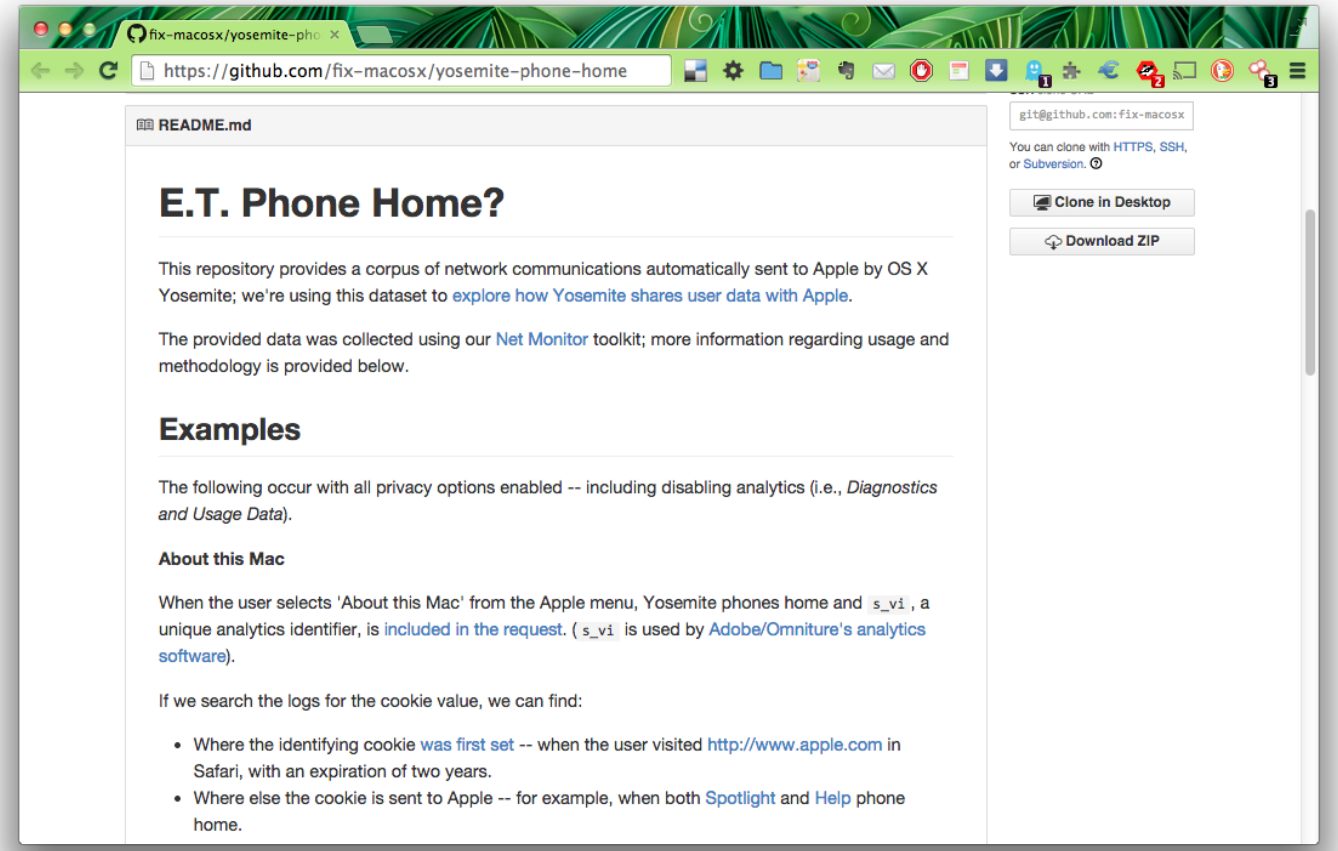
Use secure protocols and VPN solutions

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

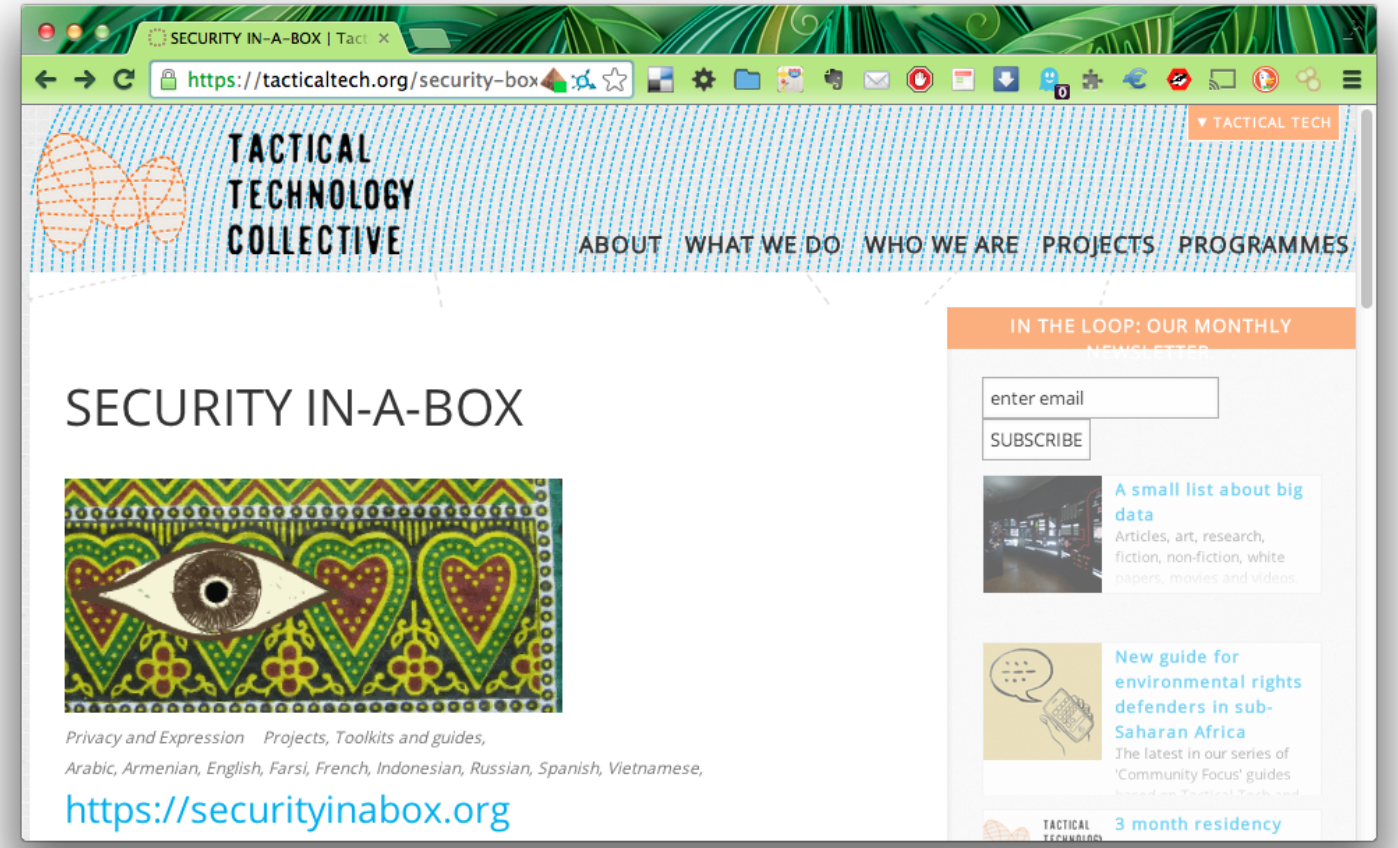
Surveillance Self-Defense EFF

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/`

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!

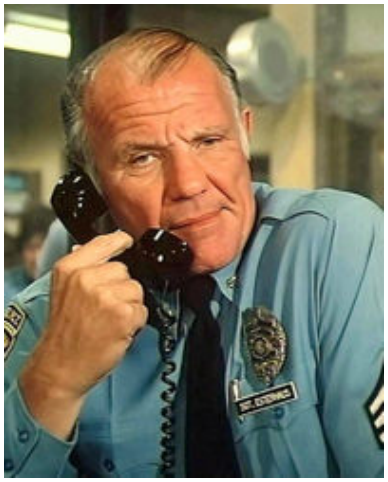
We need to share security information freely

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

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 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

Hacker - cracker

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`

Turkey: Erdogan bans Twitter

Censorship on the internet - lol

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)

Directly connection Tor Users from Turkey

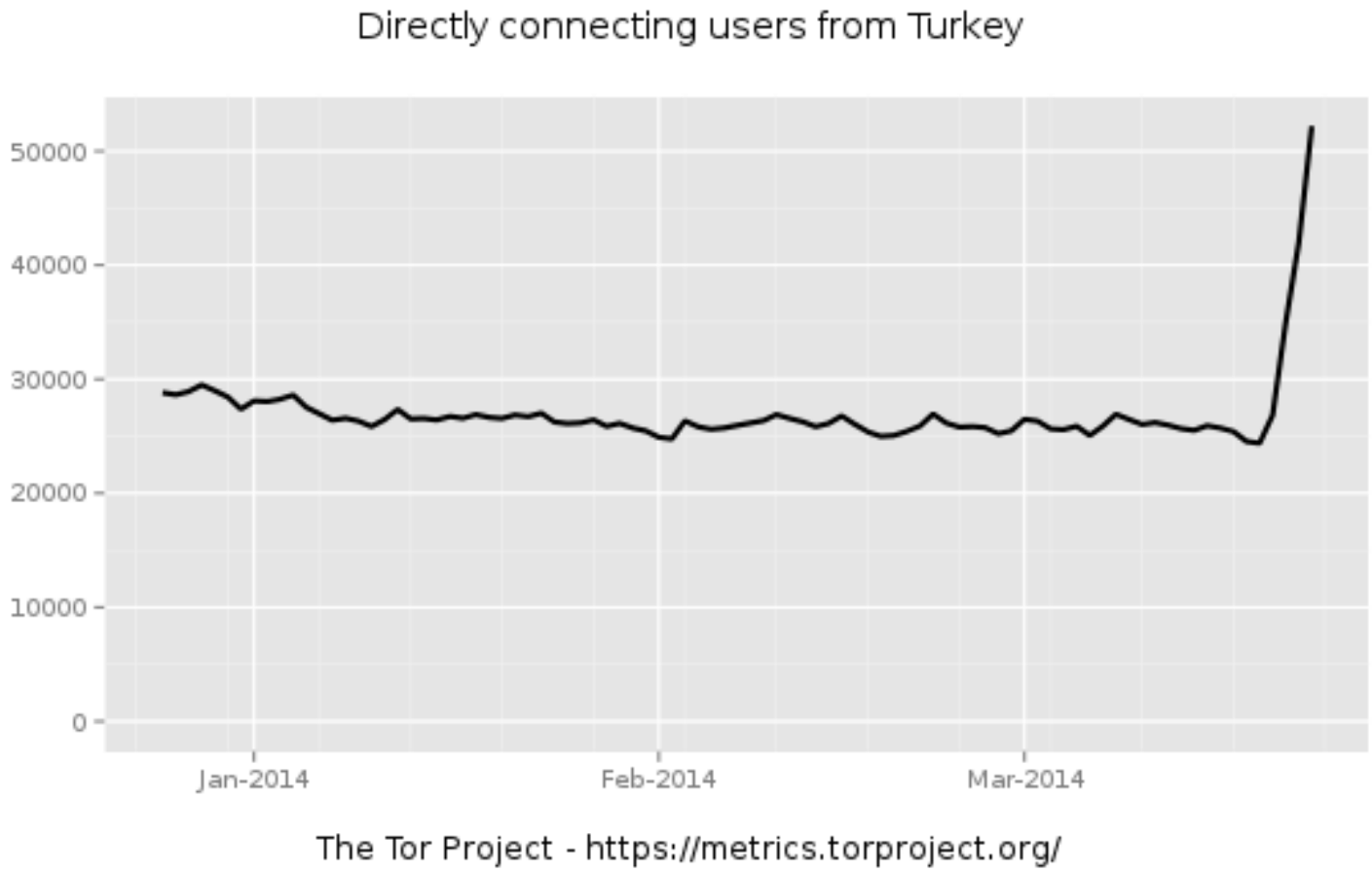


Image from `https://metrics.torproject.org`
via `https://twitter.com/runasand`

Directly connection Tor Users from Turkey +10.000

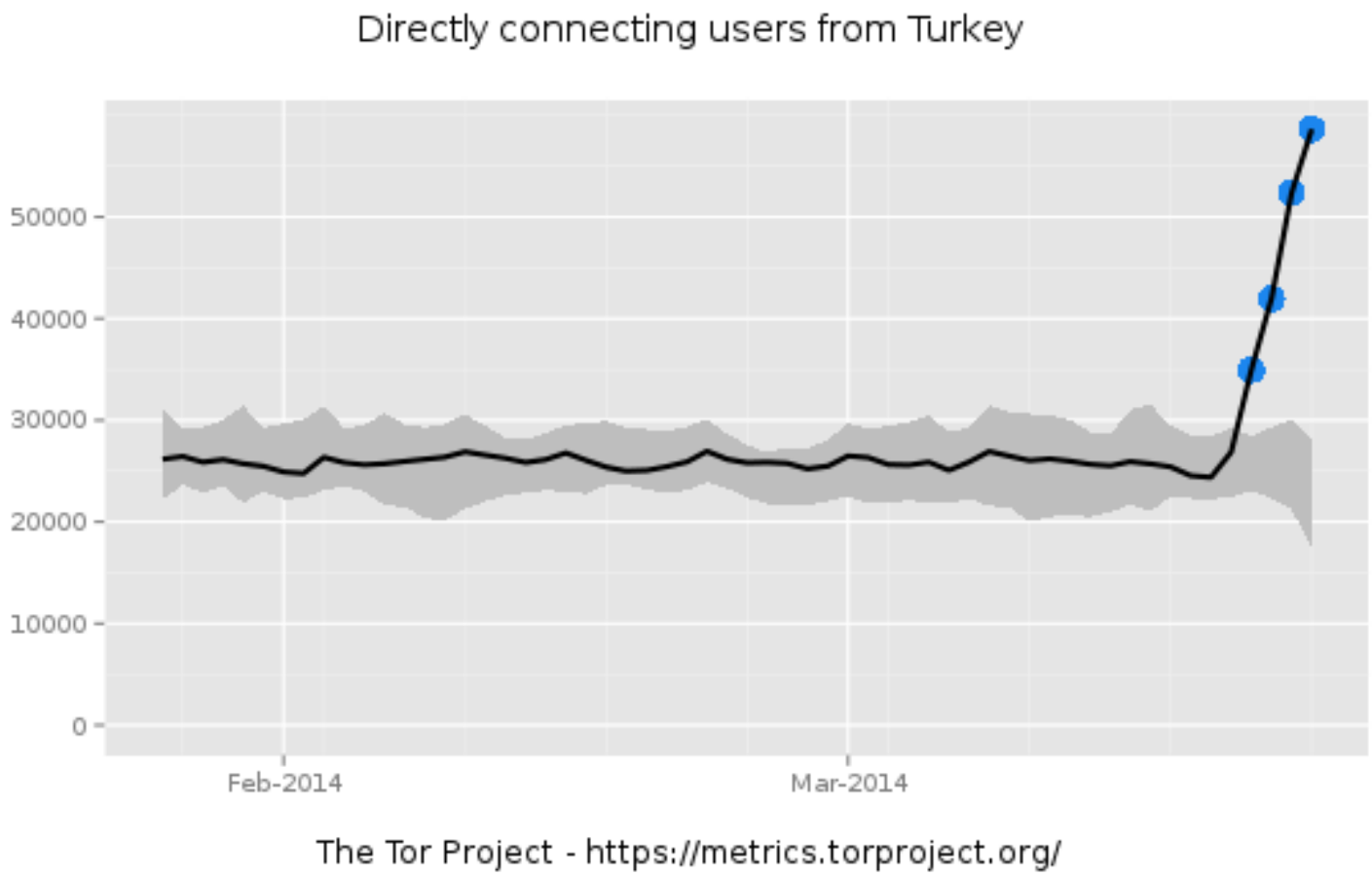


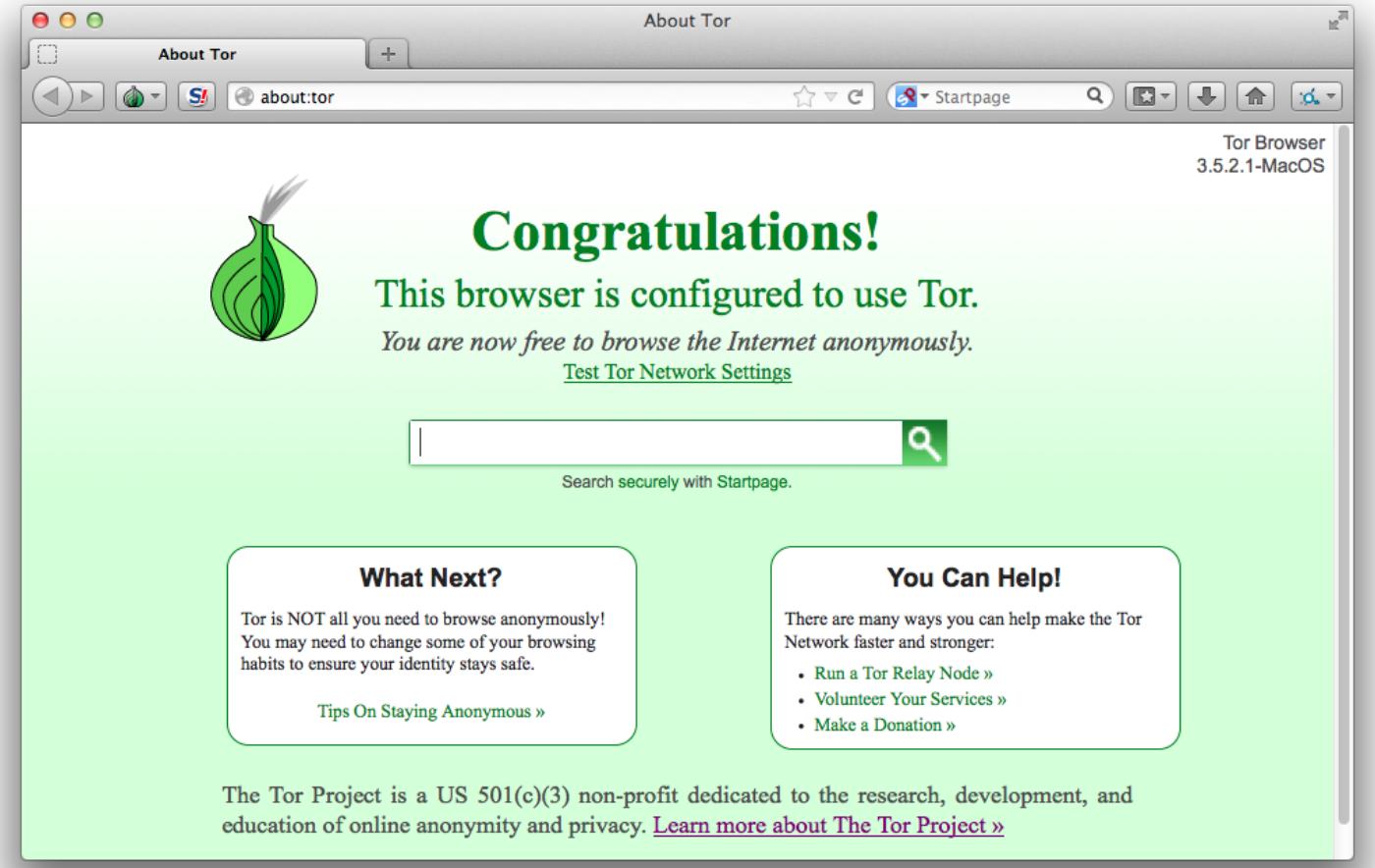
Image from `https://metrics.torproject.org` via `https://twitter.com/ioc32/status/448791582423408640`

Tor project install

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

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

Torbrowser - anonym browser



Mere anonym browser - Firefox in disguise

Whonix - Tor to the max!

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/`

Torbrowser er godt, Whonix giver lidt ekstra sikkerhed

DNSSEC trigger

Lots of DNSSEC tools, I recommend DNSSEC-trigger a local name server for your laptop

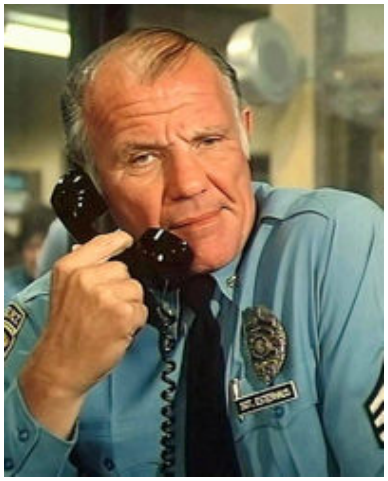
- DNSSEC Validator for firefox
  `https://addons.mozilla.org/en-us/firefox/addon/dnssec-validator/`
- OARC tools `https://www.dns-oarc.net/oarc/services/odvr`
- `http://www.nlnetlabs.nl/projects/dnssec-trigger/`

Følg med Twitter news

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

Be careful - spørgsmål?



Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

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

VikingScan.org - free portscanning