

Welcome to

Surveillance and hacking, protect yourself

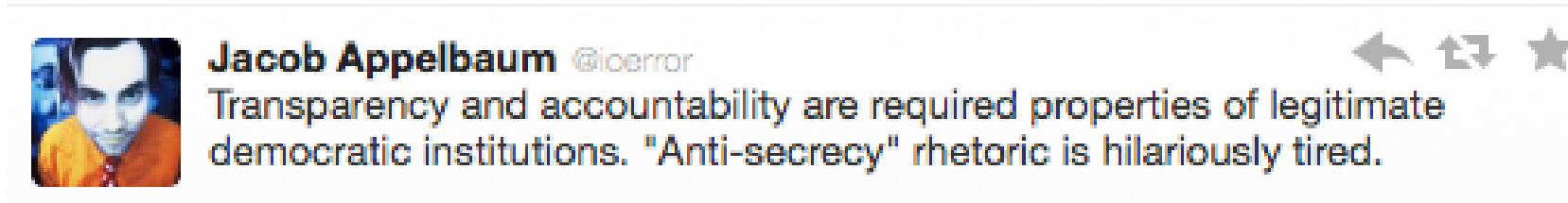
Driving IT 2014

Henrik Lund Kramshøj, internet samurai
hk@solido.net

<http://www.solidonetworks.com>

Go watch citizenfour <http://cphdox.dk/screening/citizenfour>

Slides on Github, open license: [kramshøj security-courses presentations/misc/surveillance-protect-yourself](#)



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

Beware the Four Horsemen of the Information Apocalypse: terrorists, drug dealers, kidnappers, and child pornographers. Seems like you can scare any public into allowing the government to do anything with those four.

Quote: Bruce Schneier 2005

https://www.schneier.com/blog/archives/2005/12/computer_crime_1.html

Data gathered **will be abused** either for criminal purposes, commercial purposes no matter what the original intended purpose was. The gathering of data itself becomes an easily abused target.

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.

Read more about Return of the Crypto Wars with Bruce Schneier

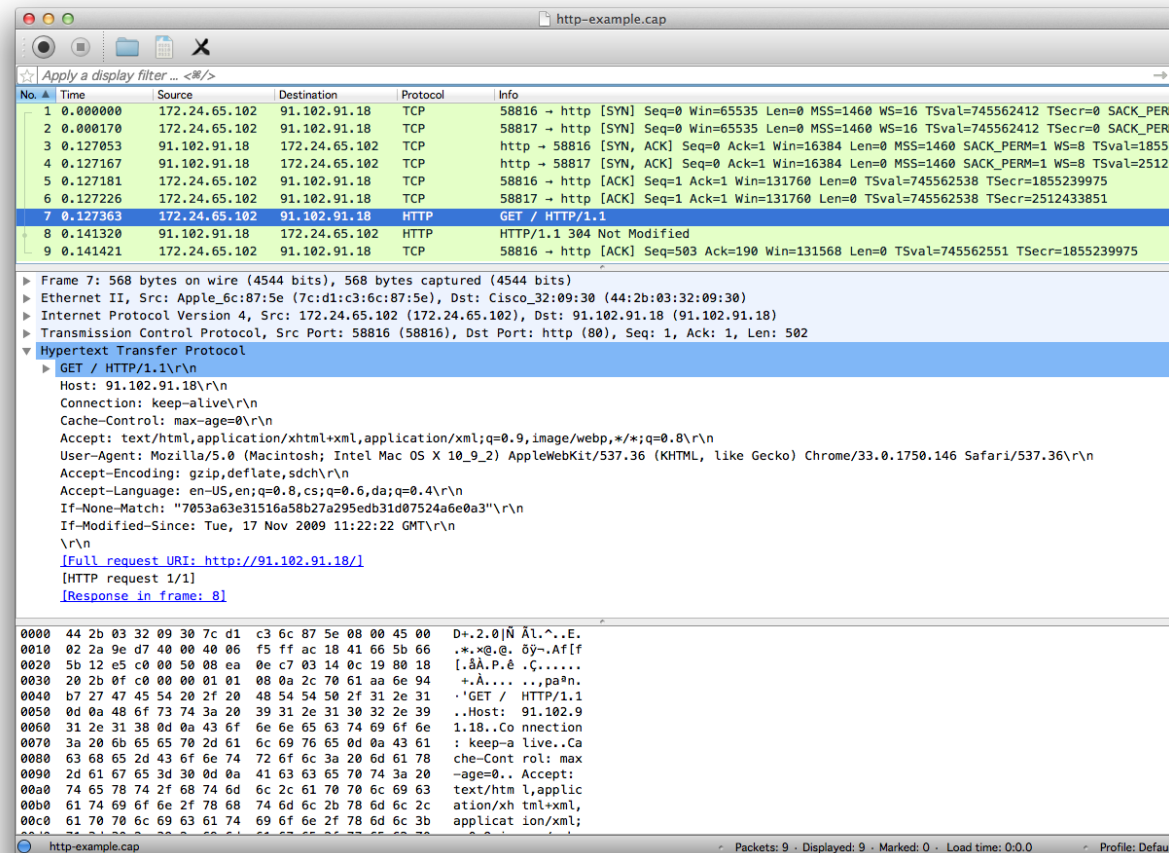
https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html



LARGE Start hacking your devices, watch them and learn

- Nmap, Nping - tester porte, godt til firewall admins <http://nmap.org>
- Metasploit Framework <http://www.metasploit.com/>
- Wireshark advanced network analyzer - <http://http://www.wireshark.org/>
- Burpsuite <http://portswigger.net/burp/>
- Skipfish <http://code.google.com/p/skipfish/>
- OpenBSD operating system extreme focus on security <http://www.openbsd.org>

Picture: Angelina Jolie, Acid Burn Hackers 1995



<http://www.wireshark.org>
Windows and Unix

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, impossible!

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.



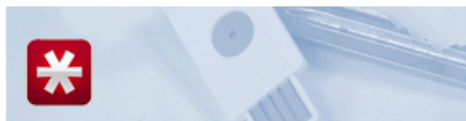
> YubiKey Nano

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



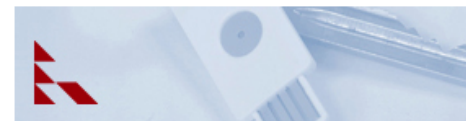
> YubiKey VIP

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.



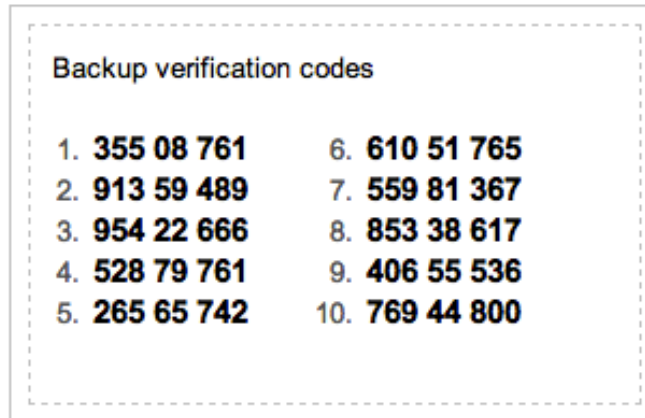
> Password Safe YubiKey

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/>

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>

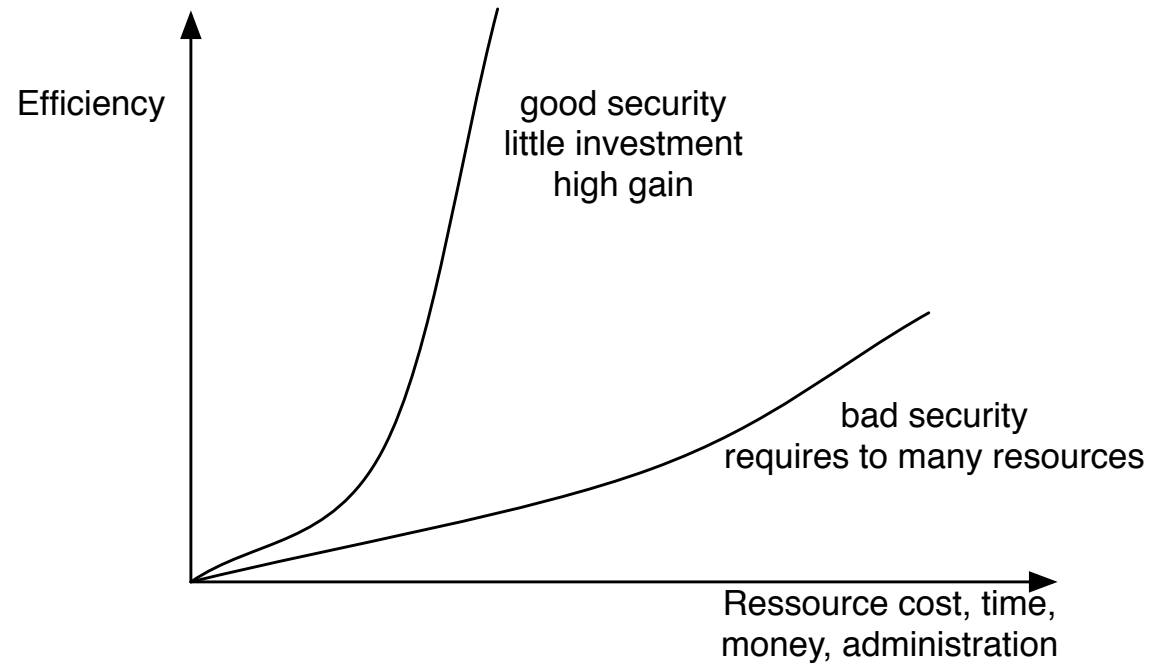
Conclusion passwords: integrate with authentication, not reinvent

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



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

Second 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

I dont think we will see good security in the mobile platforms for years to come, sorry!

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>

```
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 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.

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

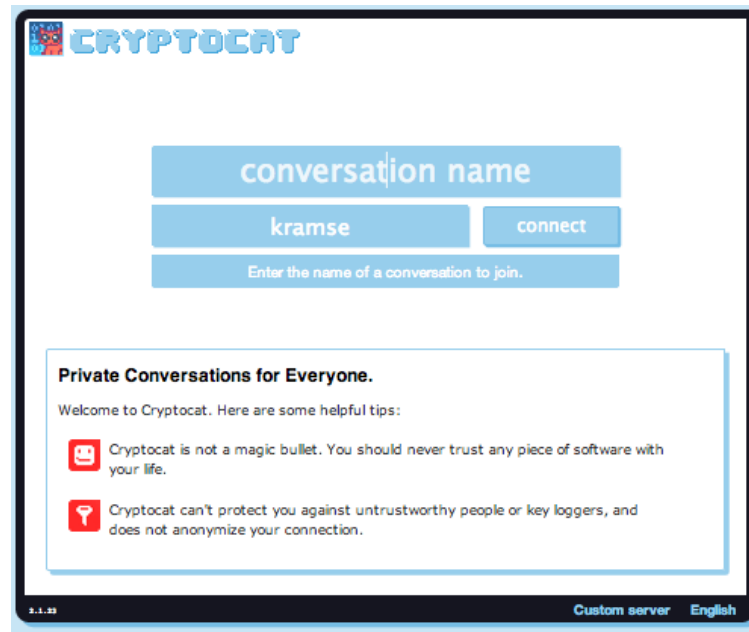
```
ssl_prefer_server_ciphers on;  
ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # not possible to do exclusive  
ssl_ciphers 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+\  
    \aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!\  
    \eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256\  
    \-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 up-dated, 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/>



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

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 LUKS and dm-crypt <https://en.wikipedia.org/wiki/Dm-crypt>
- PGP disk - Pretty Good Privacy - makes a virtuel krypteret disk
- TrueCrypt? *Let's audit Truecrypt!* Note: truecrypt halted and insecure? who knows?
<http://blog.cryptographyengineering.com/2013/10/lets-audit-truecrypt.html>

Note: in closed source product you ofc trust the developer/company producing the software

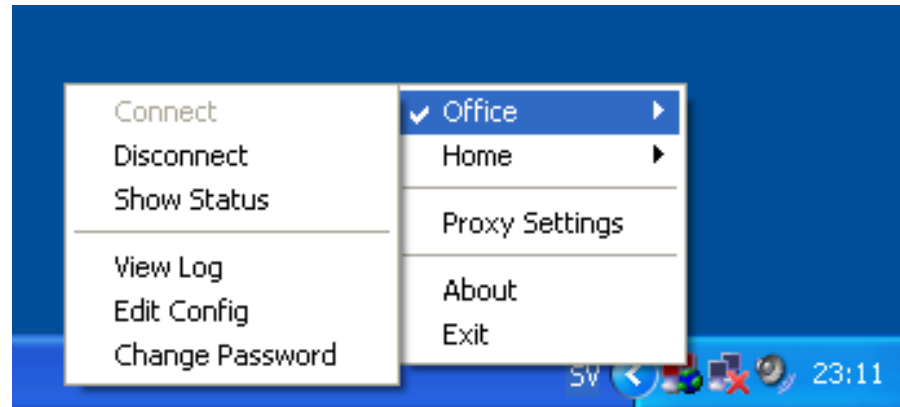
What is it?

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



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

L2TP IPsec - easy with OpenBSD as the VPN server

<http://undeadly.org/cgi?action=article&sid=20120427125048>

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



- 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

`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.

It is unacceptable to mess with DNS!

Keep the DNS, change the government!



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/>

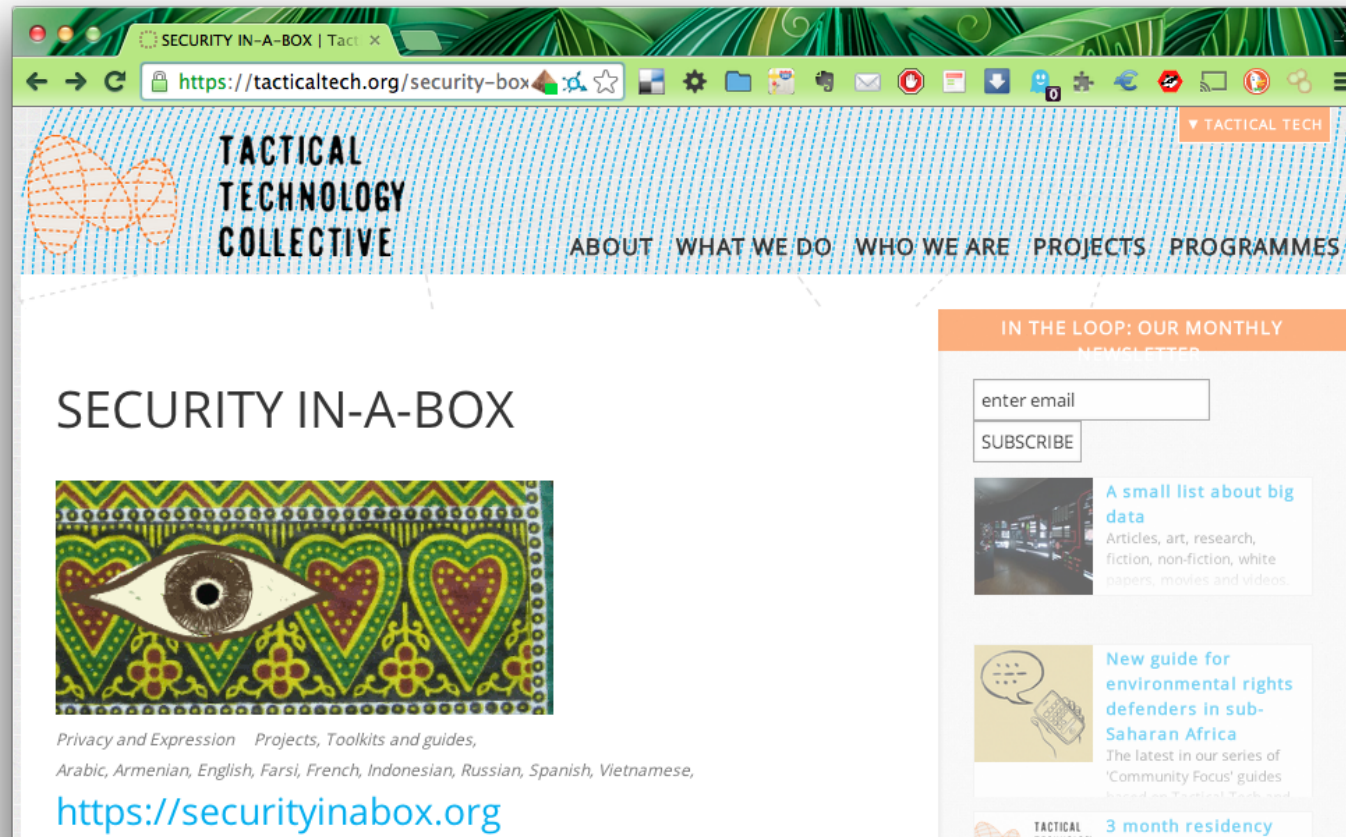


Tips, Tools and How-tos For Safer Online Communications

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/>

Be careful - questions?



Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

Source: Michael Conrad <http://www.hillstreetblues.tv/>

Slides on Github, open license: kramshøj security-courses presentations/misc/surveillance-protect-yourself

Sorry, didnt have room for them in 20 minutes



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



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

Get the Tor browser bundle from <https://www.torproject.org/>

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) [\[link\]](#)
 - 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* [\[link\]](#) 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* [\[link\]](#)
- **When the X500 revolution comes, your name will be lined against the wall and shot.**
 - As quoted in Peter Gutmann's *X509 style guide* [\[link\]](#)



The Net interprets censorship as damage and routes around it. [\[link\]](#)

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

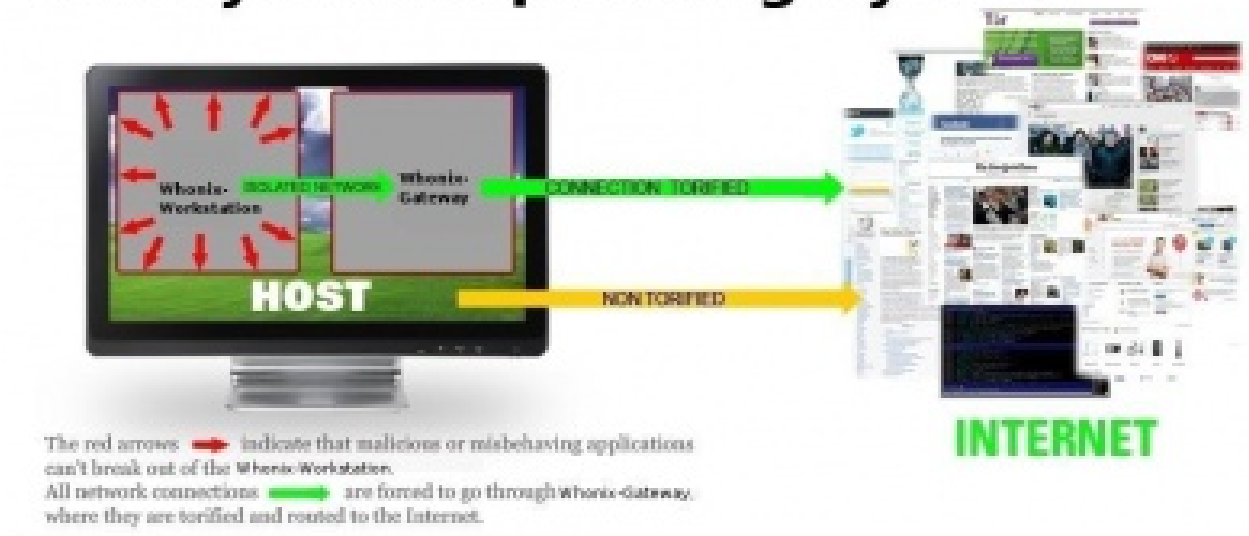
[http://en.wikipedia.org/wiki/John_Gilmore_\(activist\)](http://en.wikipedia.org/wiki/John_Gilmore_(activist))

Directly connection Tor Users from DK 8.000



Image from <https://metrics.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/>

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 lidenskabeligt (eller enddog fanatisk) eller en der foretrækker at programmere fremfor at teoretiserer om det
- En ekspert i et bestemt program eller en der ofte arbejder med eller på det; som i "en Unixhacker".

Kilde: Peter Makhholm, <http://hacking.dk>

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