



Welcome to

**Tor**

Paranoia and government hacking

Henrik Lund Kramshøj [hk@zencurity.dk](mailto:hk@zencurity.dk)

Slides are available as PDF, [kramshoej@Github](https://github.com/kramshoej)

Try searching for `tor-julecrypto.tex` in the repo

# Bjarne Jess Hansen - Vi voksne kan også være bange



<https://www.youtube.com/watch?v=ApRPz9FzkQM>

Source: Lyrics to the old-skool protest song about nuclear war

<http://www.fredsakademiet.dk/abase/sange/sang29.htm>

Fun fact: Søren Pind hates it 😊

# Syria: Protest singer Ibrahim Qashoush 2011



Four days later, his body was found dumped in the Assi River (also spelled: Isa River), with a big, open and bloody wound in his neck where his adam's apple and voice chord had been removed. A clear message to those who dare to raise their voice against the Syrian President Bashar al-Assad.

'Yalla Erhal Ya Bashar' (It's time to leave, Bashar), demanding an end to President Bashar al-Assads regime.

<https://www.youtube.com/watch?v=nox6sVyhBYk>

<http://freemuse.org/archives/5054>

# Data collected will be abused



Data collected will be **abused** either by criminals or for criminal purposes, commercial purposes no matter what the original intentions were. Today data is gathered to protect us from terrorists, extremism, nazis, pedophiles, abuse of children ... Le mal du jour.

but also enables stalking, employers doing abusive monitoring, spouses and parents abusing power, politicians abusing power, police investigations into legal protests

## You should take control of your data - that is democracy

# 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>

# Paranoia defined



par·a·noi·a

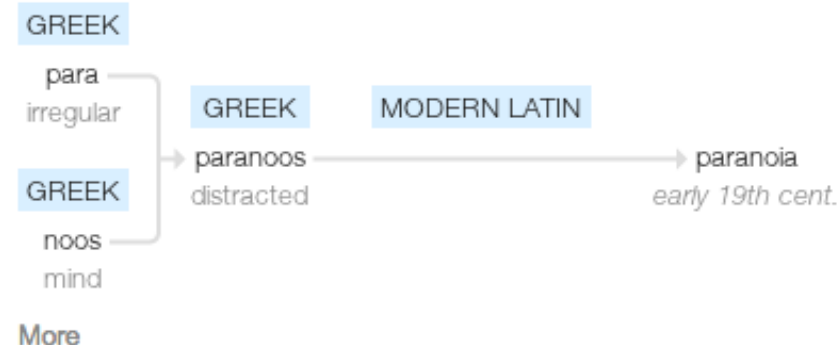
/ˌparəˈnoɪə/ 

*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 - Er du passende paranoid?

# Face reality



From the definition:

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

It is not paranoia when:

- Criminals sell your credit card information and identity theft
- 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

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*

Criminals have automated systems, trying to infect all!

Putting a sticker over your webcam is not paranoia, but common sense!





Using crypto is a peaceful protest  
and it is not magic



# Government back-doors



What if I told you:

## **Governments will introduce back-doors**

Intercepting encrypted communications with fake certificates - check

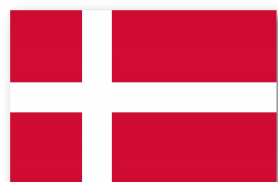
May 5, 2011 A Syrian Man-In-The-Middle Attack against Facebook

"Yesterday we learned of reports that the Syrian Telecom Ministry had launched a man-in-the-middle attack against the HTTPS version of the Facebook site."

Source:

<https://www.eff.org/deeplinks/2011/05/syrian-man-middle-against-facebook>

# Government back-doors in Denmark



Mapping out social media and finding connections - check Palantir

Danish police and TAX authorities have the legal means, even for small tax-avoidance cases, see *Rockerloven*

They did order Hacking Team software! Legal for DK Gov to do this, but have they used it?

Fun fact: Most danish gov institutions have a sniffer implemented controlled by GovCERT - which are now part of the danish department of defence. Actually part of the Danish Defence Intelligence Service, holy fuck!

[https://da.wikipedia.org/wiki/GovCERT\\_\(Danmark\)](https://da.wikipedia.org/wiki/GovCERT_(Danmark))

# Infecting activist machines



Infecting activist machines - check

Tibet activists are repeatedly being targeted with virus and malware, such as malicious apps for Android like KakaoTalk

Tor-users infected with malicious code to reveal their real IPs

<https://blog.torproject.org/blog/hidden-services-current-events-and-freedom-hosting>

Copying journalist data in airports - check

# 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

# Why use Tor?

Your public IP is **Red Information**, often lead directly to you

You like to browse things, without telling your ISP, the government, your teacher, ... everyone,

Avoid censorship

You want to avoid stalkers

You are an investigative journalist or high school student researching Al Qaeda, Daesh, ISIS for school

Consider getting the book *The Smart Girl's Guide to Privacy*

<http://smartprivacy.tumblr.com/>

## Who Uses Tor?



Internet.

### Family & Friends

People like you and your family use Tor to protect themselves, their children, and their dignity while using the



accountability.

### Businesses

Businesses use Tor to research competition, keep business strategies confidential, and facilitate internal



on corruption.

### Activists

Activists use Tor to anonymously report abuses from danger zones.

Whistleblowers use Tor to safely report



### Media

Journalists and the media use Tor to protect their research and sources online.



gathering online.

### Military & Law Enforcement

Militaries and law enforcement use Tor to protect their communications, investigations, and intelligence

# 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.

# Tor today



**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

- Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the U.S. Naval Research Laboratory.
- Today, it is used every day for a wide variety of purposes by **normal people, the military, journalists, law enforcement officers, activists, and many others.**
- Tor's **hidden services** let users publish web sites and other services

Source:

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



# Tor users 2007

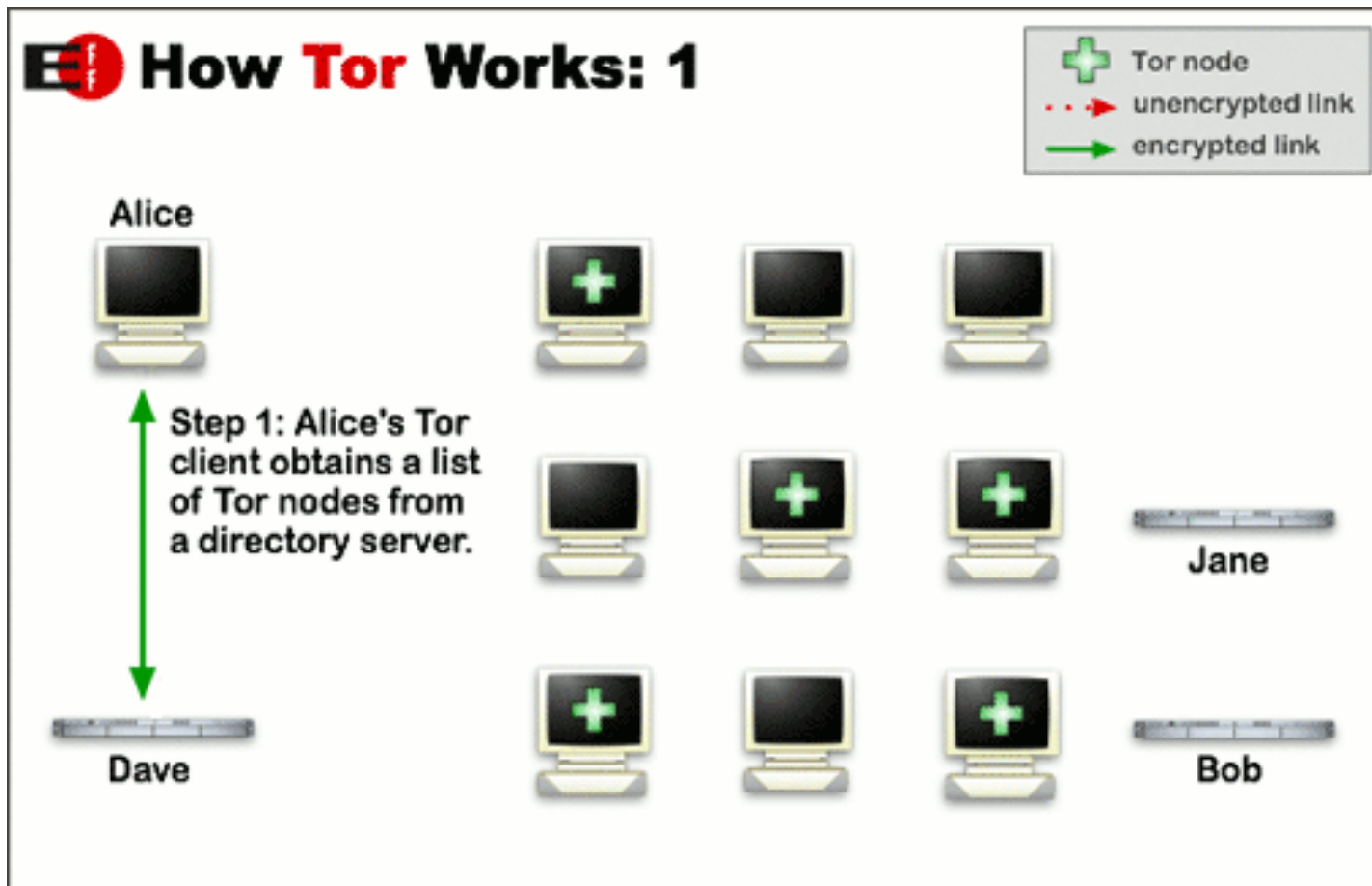


Dan Egerstad, Swedish computer security consultant obtained log-in and password information for 1,000 e-mail accounts belonging to foreign embassies, corporations and human rights organizations.

Use encryption and secure protocols AND Tor!

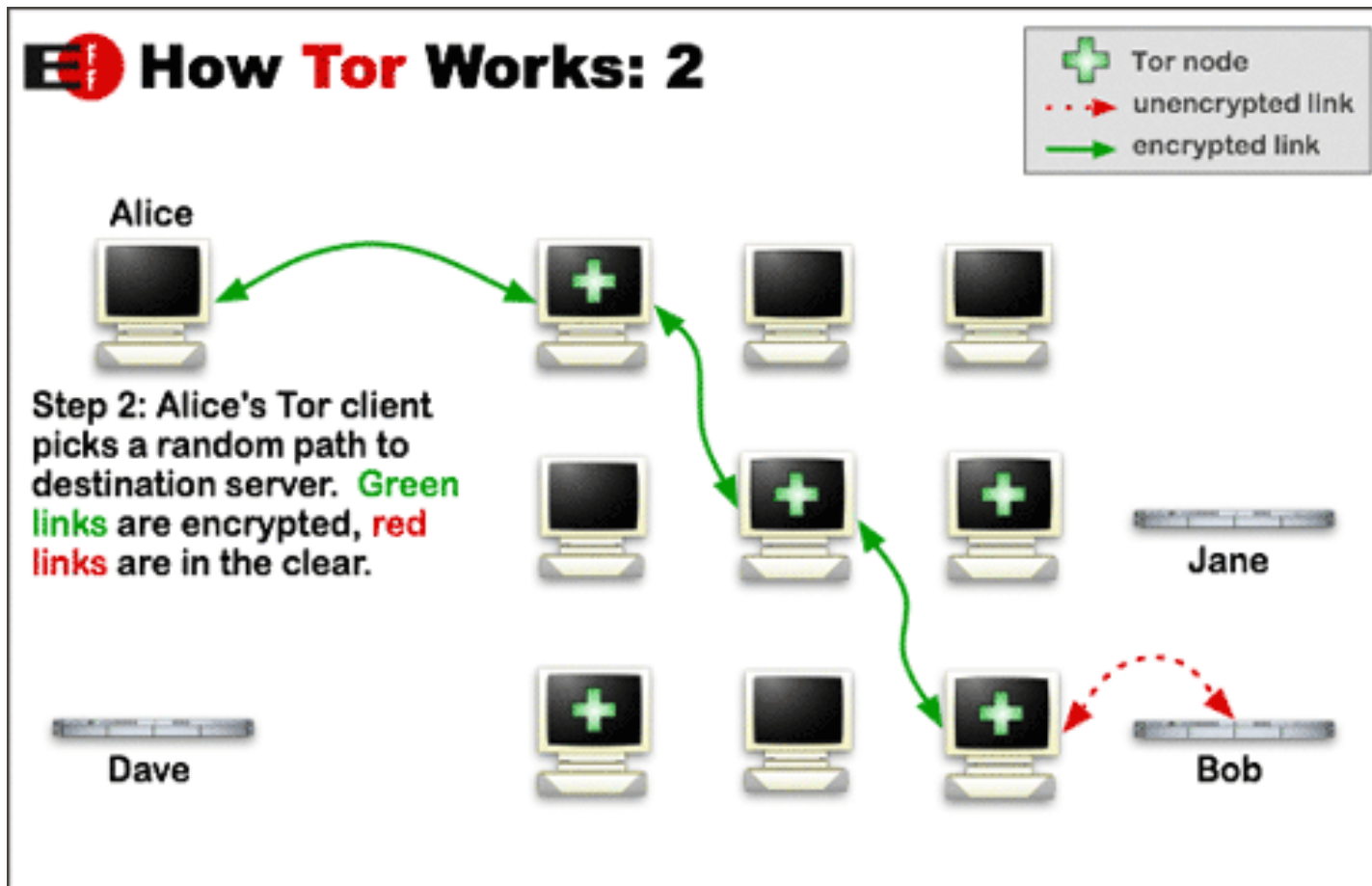
Note: I have no knowledge about the danish embassies using or not using Tor, but probably they do.

# Tor project - how it works 1



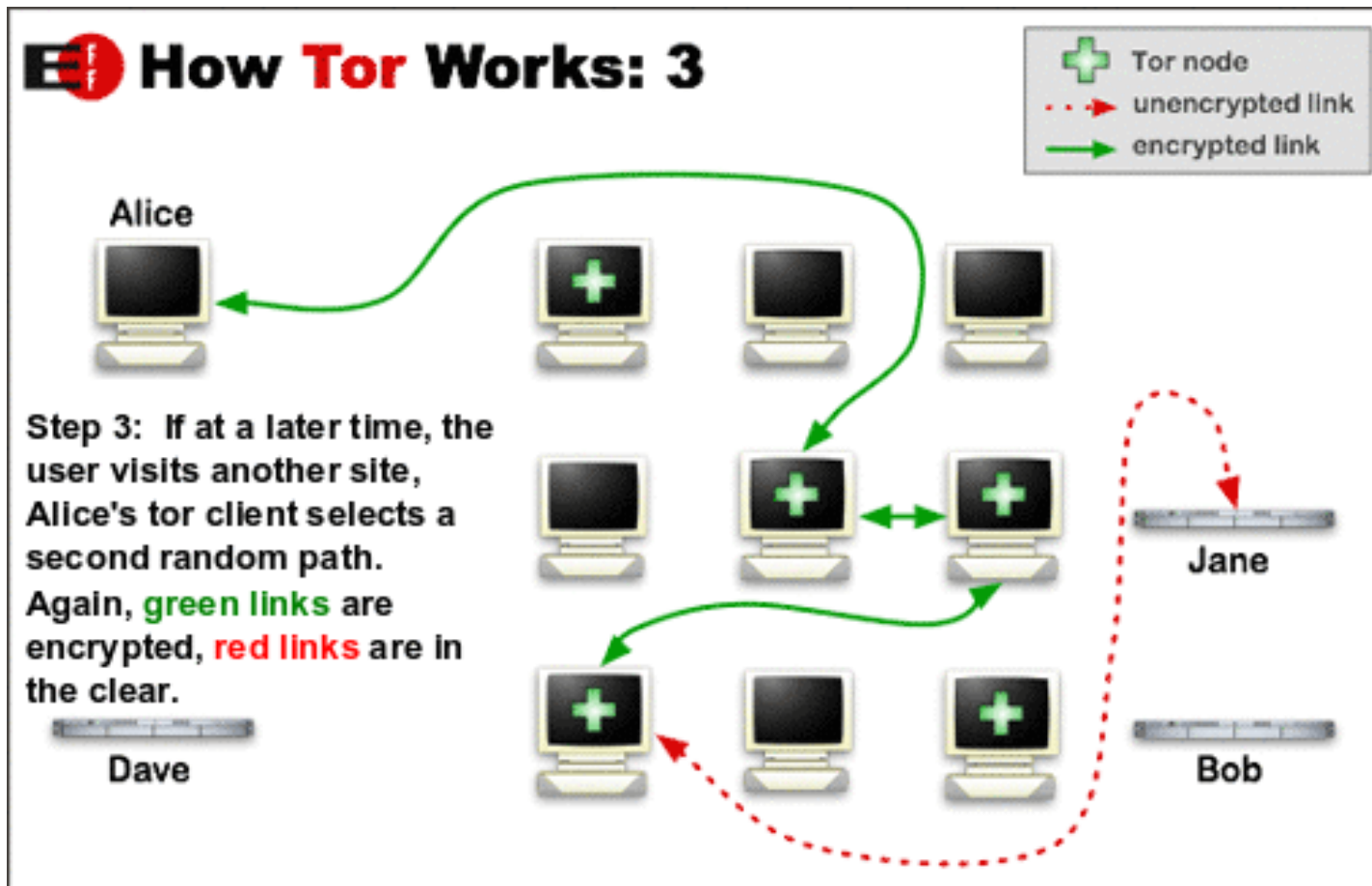
pictures from <https://www.torproject.org/about/overview.html.en>

# Tor project - how it works 2



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

# Tor project - how it works 3

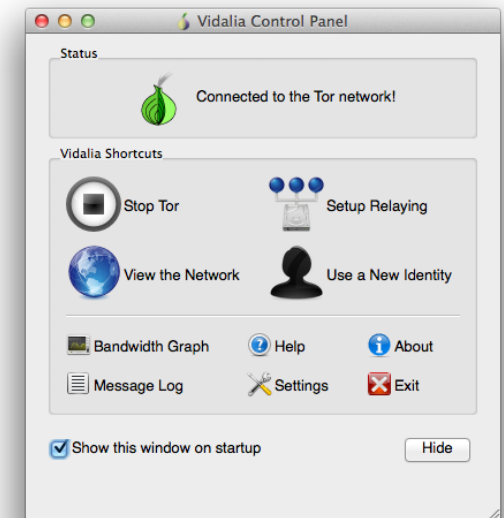
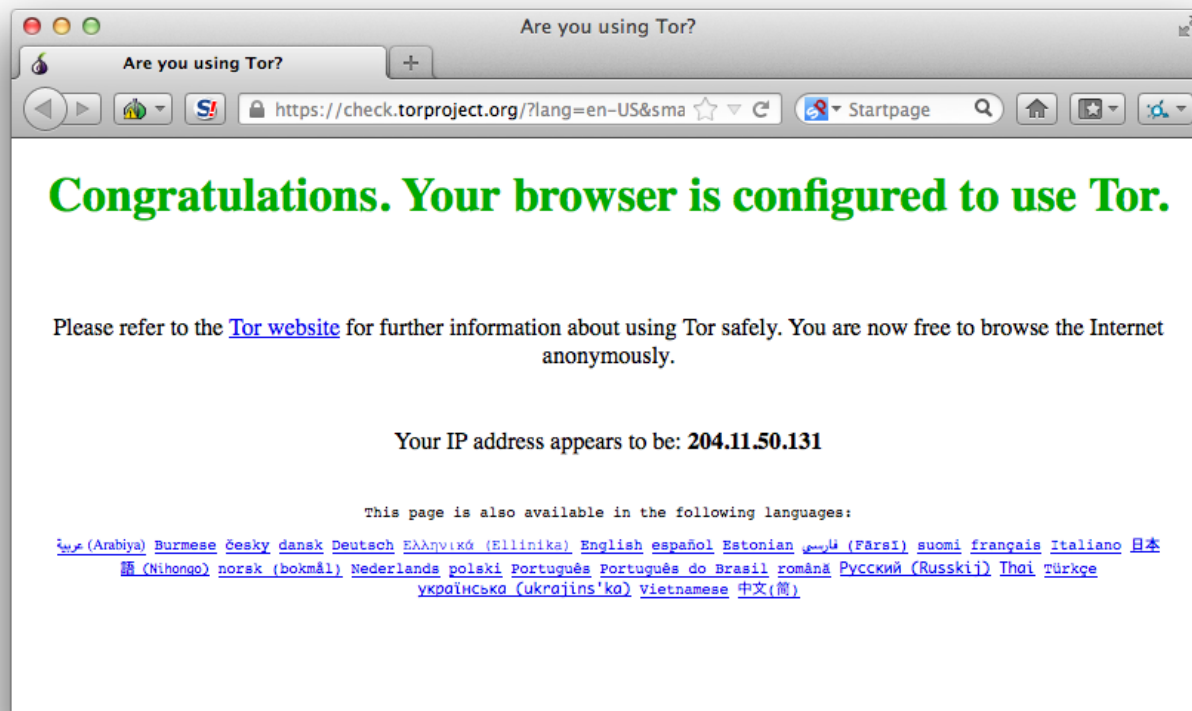


pictures from <https://www.torproject.org/about/overview.html.en>

# Using Tor



Recommendation is to run Tor browser

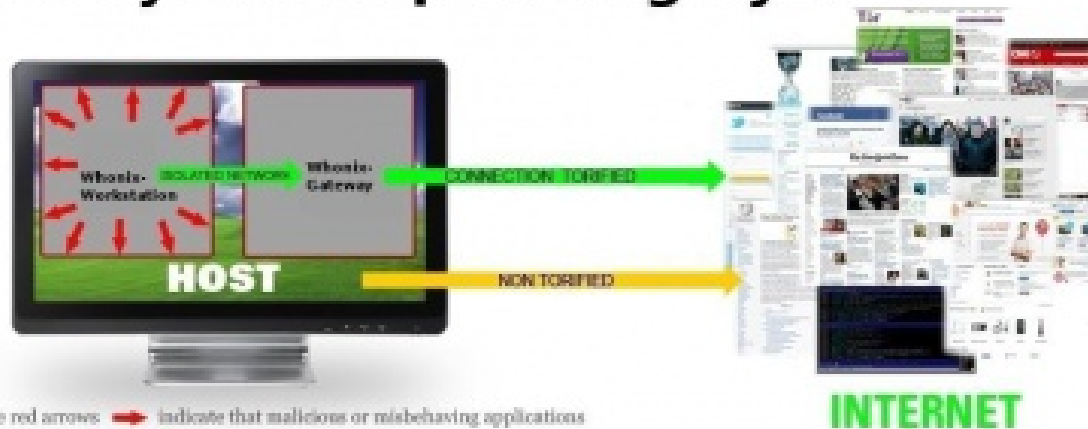


Also plugins to Firefox etc. beware of browser fingerprint and DNS leaks!

# Whonix - a better idea



## Whonix Anonymous Operating System



The red arrows → indicate that malicious or misbehaving applications can't break out of the Whonix-Workstation. All network connections → are forced to go through Whonix-Gateway, where they are torified and routed to the Internet.

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/>

# Tor news



- **Tor blog** Great news stories about Tor  
<https://blog.torproject.org/blog/>
- **Electronic Frontier Foundation (EFF)**  
<https://www.eff.org/>
- **Tor users are also Access users**  
<https://www.accessnow.org/>
- **cryptoparty.org and Asher Wolf**  
<https://en.wikipedia.org/wiki/CryptoParty> [https://twitter.com/Asher\\_Wolf](https://twitter.com/Asher_Wolf)
- **Schneier on Security**  
<https://www.schneier.com/>  
**Sample analysis How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID**  
[https://www.schneier.com/blog/archives/2013/10/how\\_the\\_nsa\\_att.html](https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html)
- **Cryptome welcomes documents for publication that are prohibited by governments worldwide**  
[cryptome.org/](http://cryptome.org/)



# 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 Kramshøj <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!



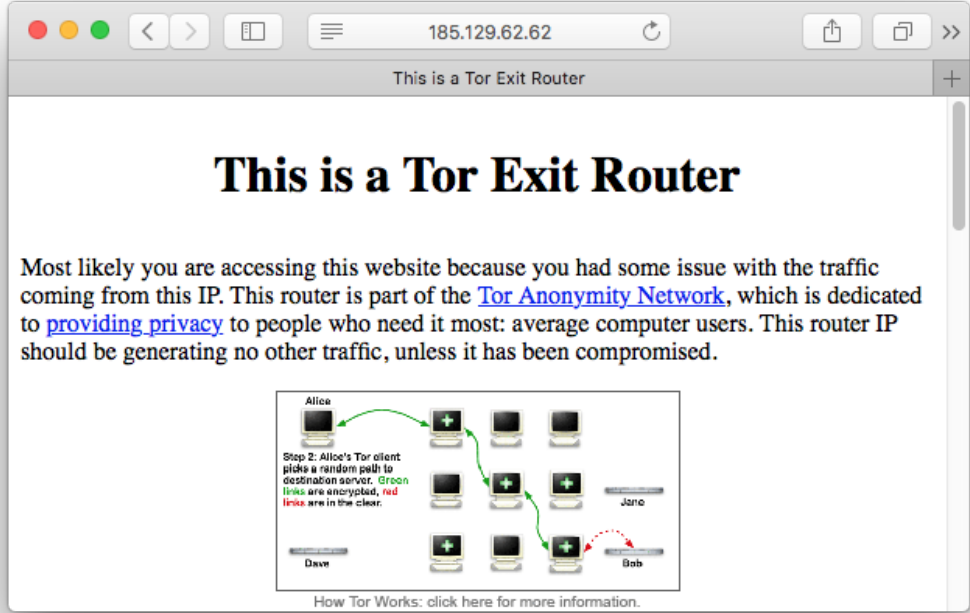
# Tor relay config - exit node



RTFM! Read them again, and decide if you really want to run exit-node

```
h1k@kunoichi $ grep -v "^#" torrc.txt
Log notice file /var/log/tor/notices.log
ORPort 9001
ORPort [2a06:d380:0:3700::63]:9001
Address tor02.zencurity.dk
Nickname kramse2
ContactInfo Henrik Kramshøj <h1k AT zencurity dot dk>
DirPort 9030 # what port to advertise for directory connections
DirPort [2a06:d380:0:3700::63]:9030 NoAdvertise
DirPortFrontPage /usr/local/etc/tor/tor-exit-notice.html
MyFamily ACDD9E85A0...47212E8A38F,A44AE029...1E22B,F94A7BAC5D...625B8B533
ExitPolicy reject 31.28.24.114:* # you can still configure rejects
ExitRelay 1
IPv6Exit 1
```

FreeBSD has `tor_enable="YES"` in `/etc/rc.conf`



It is recommended to show a tor-exit-notice.html on exit nodes `/etc/pf.conf`:

```
rdr pass on $ext_if proto tcp from any to any port 80 -> 127.0.0.1 port 9030
```

# Tor relay config - non-exit node



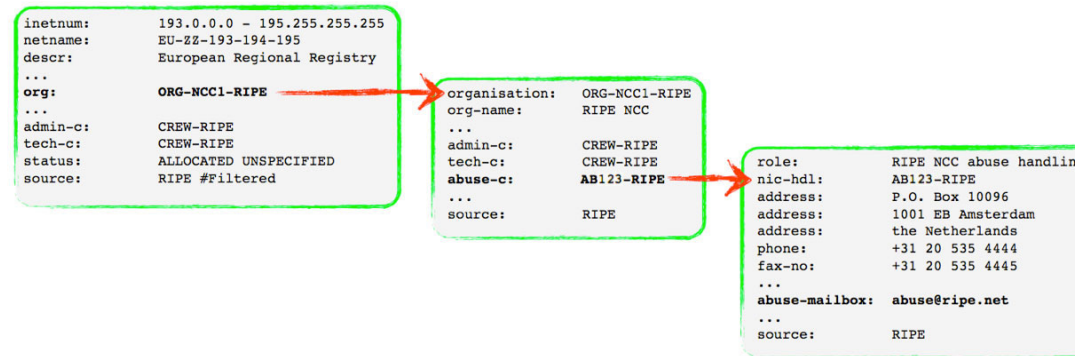
Running a non-exit should be trouble free in Denmark

```
root@turris:~# grep -v "^#" /etc/tor/torrc
Log notice file /var/log/tor/notices.log
RunAsDaemon 1
DataDirectory /var/lib/tor
ORPort 9001
Nickname kramseturris
ContactInfo Henrik Kramshøj <hlk AT zencurity dot dk>
DirPort 9030 # what port to advertise for directory connections
MyFamily ACDD9E...12E8A38F,A44AE029015BA6F...D1E22B,F94A7BAC5D1E3...5B8B533
ExitPolicy reject *: * # no exits allowed
User tor
```

BandwidthRate and BandwidthBurst are in Bytes, not Bits, and you can limit the total amount of bandwidth used

<https://www.torproject.org/docs/faq.html.en#BandwidthShaping>

# What to expect - abuse mails



Make it easy for people to see it is a Tor relay

<https://blog.torproject.org/blog/tips-running-exit-node>

If possible get yourself listed as the abuse contact

Respond with polite emails

I have a little less than 300 emails in 2016 regarding abuse from my nodes

# Sample reponse email



Re: 185.129.62.62 blocked at XXX

Very sorry,

This IP is in use for Tor exit router. The IP is a Tor node relay, and we have no further data regarding sessions. The Tor network by design limits data and you can read more about Tor at: <https://www.torproject.org/>

Unfortunately the software is hardened against de-masking users and we cannot help. We are of course sorry when the network is abused, but Tor is helping a lot of people around the world to communicate more securely. We consider the benefits from Tor greater than occasional abuse and hope you understand.

If problem persists we can filter out selected ranges from our server.

Mvh/Best regards

Henrik

**Also checkout** <https://www.torservers.net/wiki/abuse/templates>

# Be careful - questions?

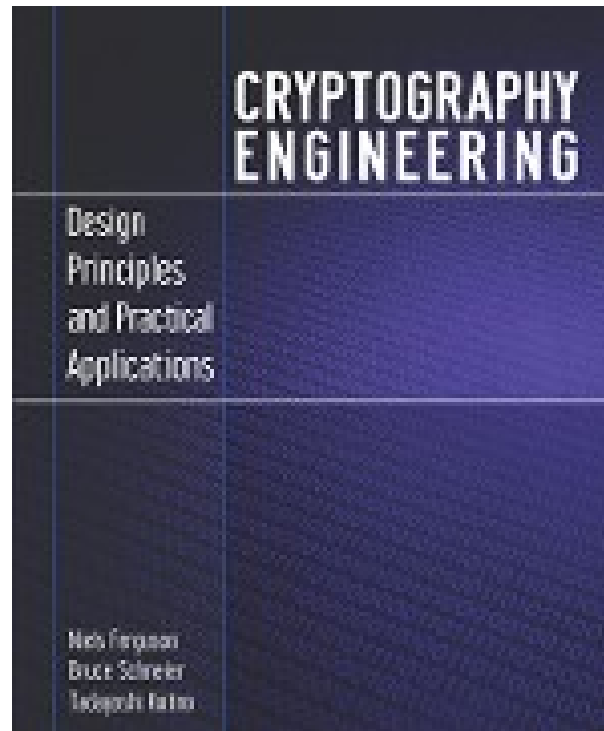


Hey, Lets be careful out there!

Henrik Lund Kramshøj [hik@zencurity.dk](mailto:hik@zencurity.dk)

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

# Cryptography Engineering



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

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

# 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`

And configure your browser to not activate content like Flash before you click

Plugins like NoScript for Firefox and NotScripts for Chrome is highly recommended



## 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>

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



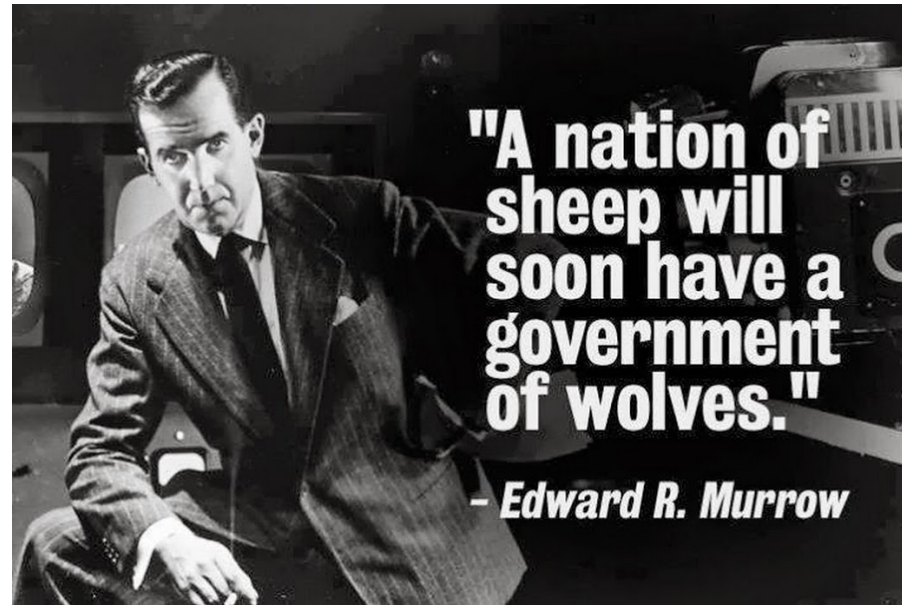
(Reuters) - British authorities came under pressure on Monday to explain why anti-terrorism powers were used to detain for nine hours the partner of a journalist who has written articles about **U.S. and British surveillance programs** based on **leaks from Edward Snowden**.

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 news



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

# Government monitoring is not news



## FBI Carnivore

"... that was designed to monitor email and electronic communications. It used a customizable packet sniffer that can monitor all of a target user's Internet traffic." [http://en.wikipedia.org/wiki/Carnivore\\_\(software\)](http://en.wikipedia.org/wiki/Carnivore_(software))

NarusInsight "Narus provided Egypt Telecom with Deep Packet Inspection equipment, a content-filtering technology that allows network managers to inspect, track and target content from users of the Internet and mobile phones, as it passes through routers on the information superhighway. Other Narus global customers include the national telecommunications authorities in Pakistan and Saudi Arabia, ..."

<http://en.wikipedia.org/wiki/NarusInsight>