Welcome to

Ins@fe Training Seminar

Secure browsing, plugins and privacy tools

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

Key words: multiple browsers, crypto, Torproject and how to protect yourself

Democracy now: Why do we bother?

Jacob Appelbaum @ioerror

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

In a democracy we need the citizens with freedom that can act without constant surveillance

Democracy requires that we can actively select which personal data to give up and to whom

Cryptography is peaceful protest against blanket surveillance

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

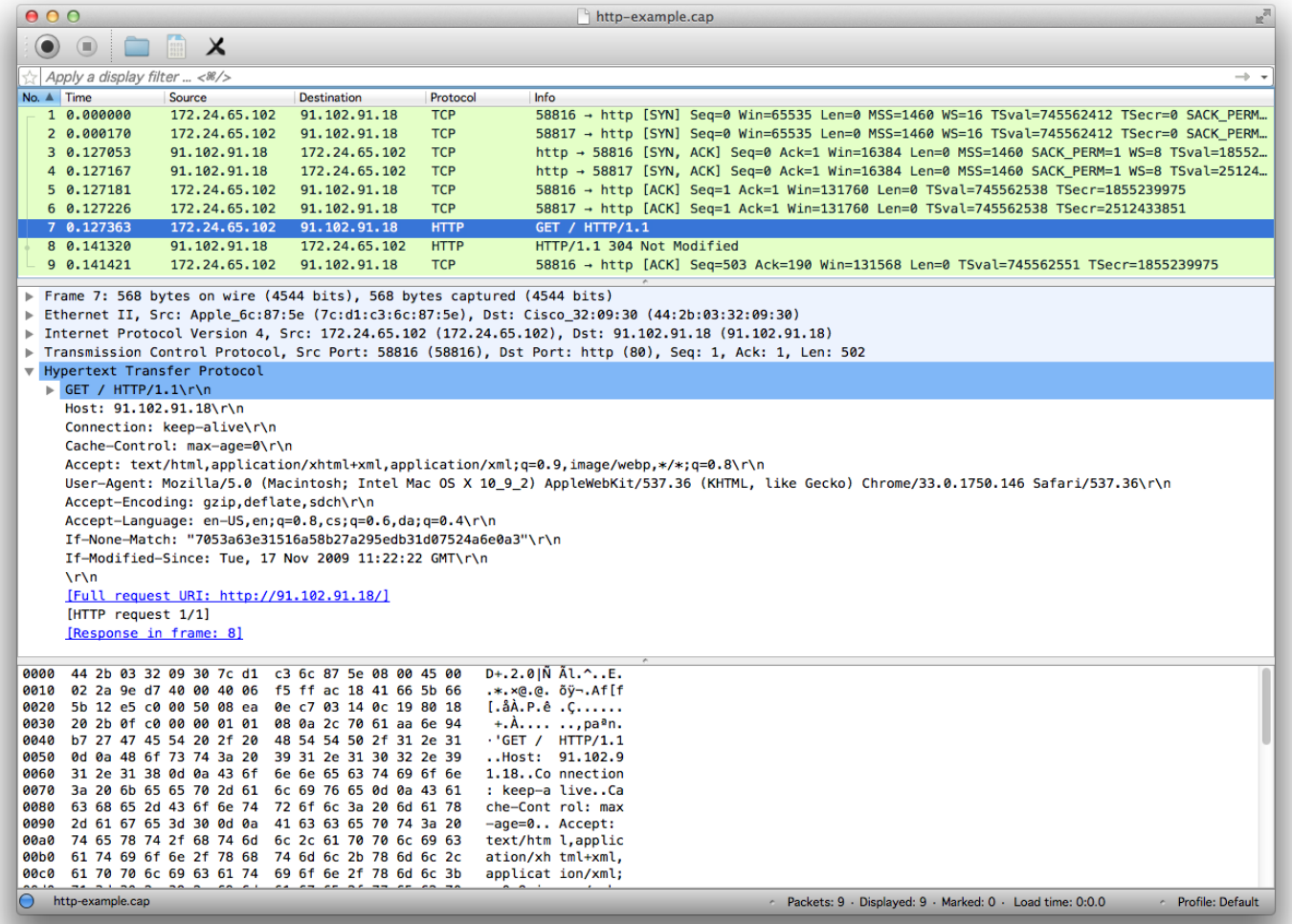
Follow news about security

Support communities, join and learn

Hacking is not magic

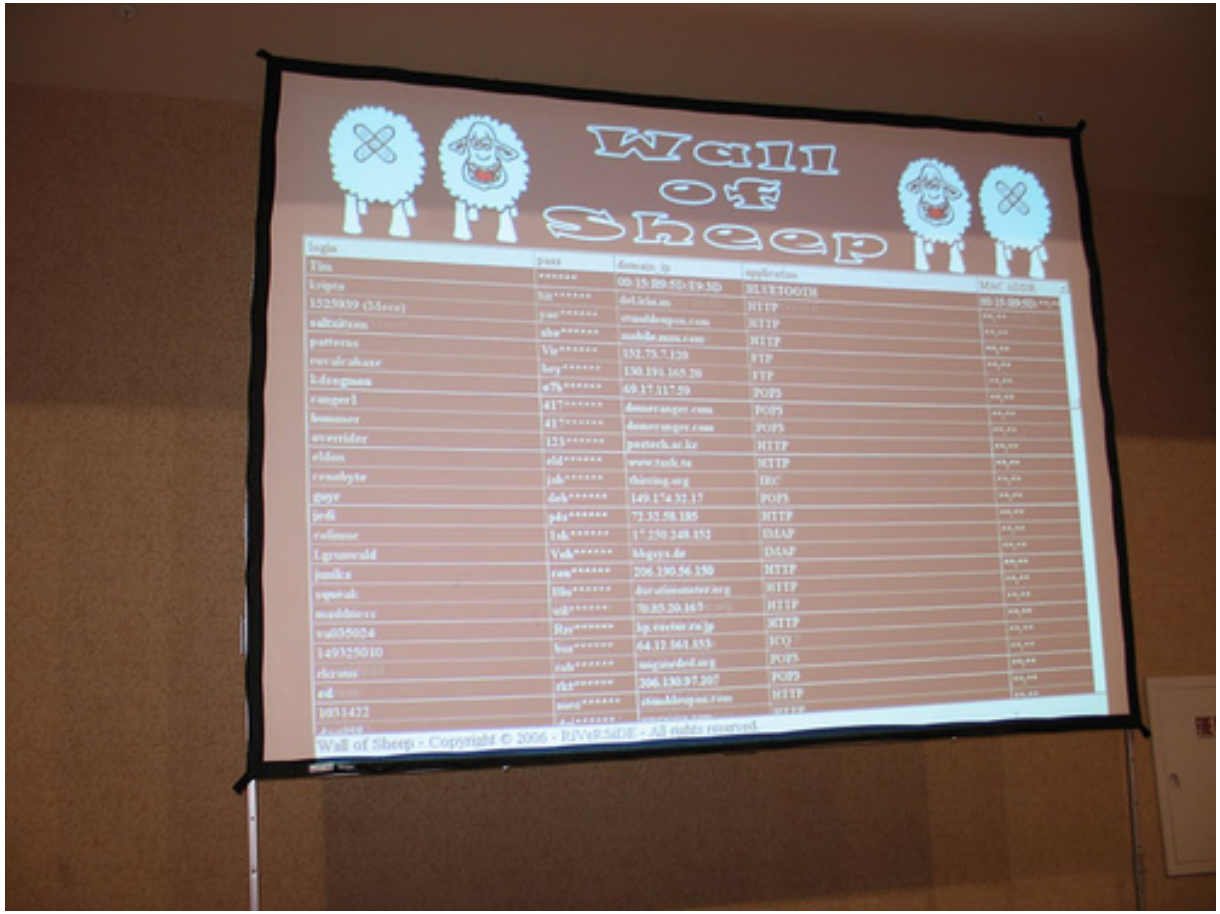
Hacking requires some ninja training

Dive into the bitstream



Anyone in the network path can sniff this!

Wall of sheep



Defcon Wall of Sheep - play nice!

What is YOUR password?

Hacker tools BackTrack and Kali

Hacking is fun and you can learn a lot

Remember to do it in a controlled environment lab setups

I recommend using Kali in a virtual environment, VMware Player, Virtualbox or similar

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

Then you can run other insecure virtual machines like Metasploitable for learning

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

Always try to make life worse and more costly for attackers

Multiple browsers

- Multiple browsers: one for facebook, one for net banking applications
- More strict secure settings and NoScripts for web surfing
- One browser with loose settings for: Netflix, and *trusted sites*
- Remember to install critical plugins like HTTPS Everywhere, NoScript, CertPatrol m.fl.

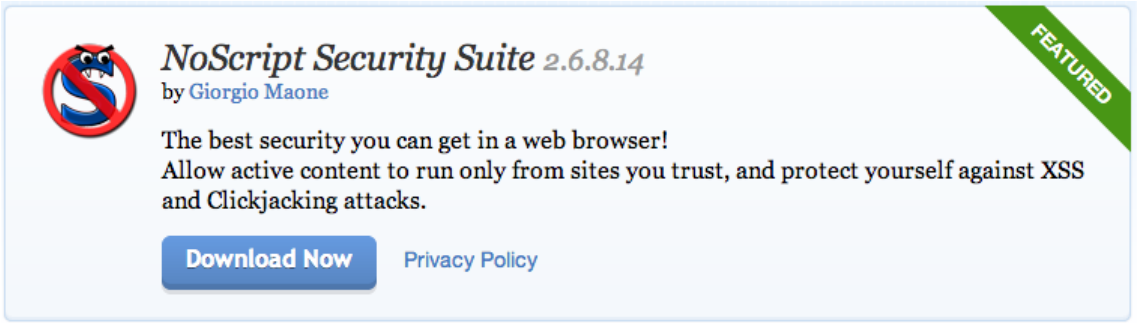
HTTPS Everywhere

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

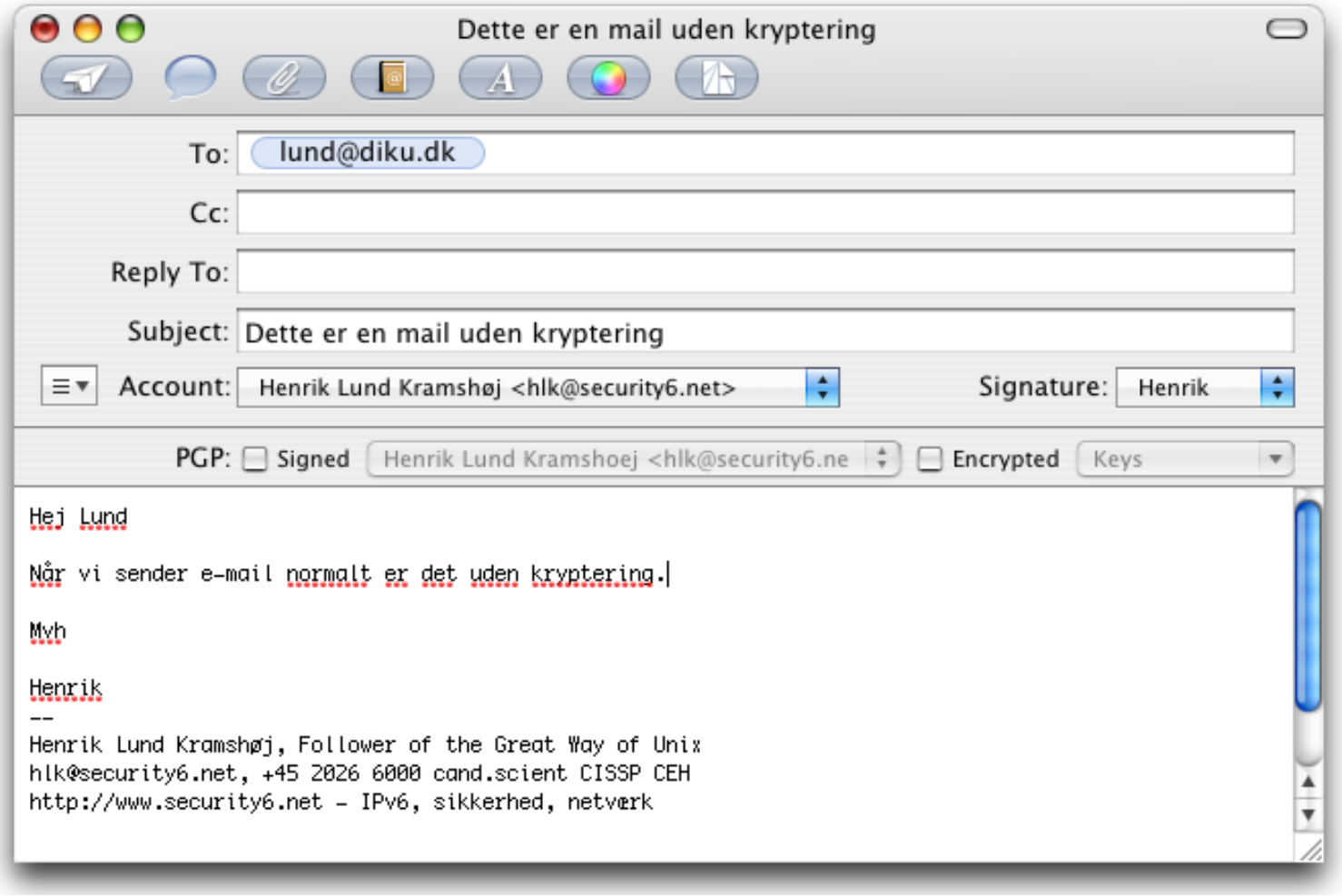
Pro tip: you can avoid lots of advertisements

CertPatrol - which site uses which certificate

An add-on formerly considered paranoid: CertPatrol implements ”pinning” for Firefox/Mozilla/SeaMonkey roughly as now recommended in the User Interface Guidelines of the World Wide Web Consortium (W3C).

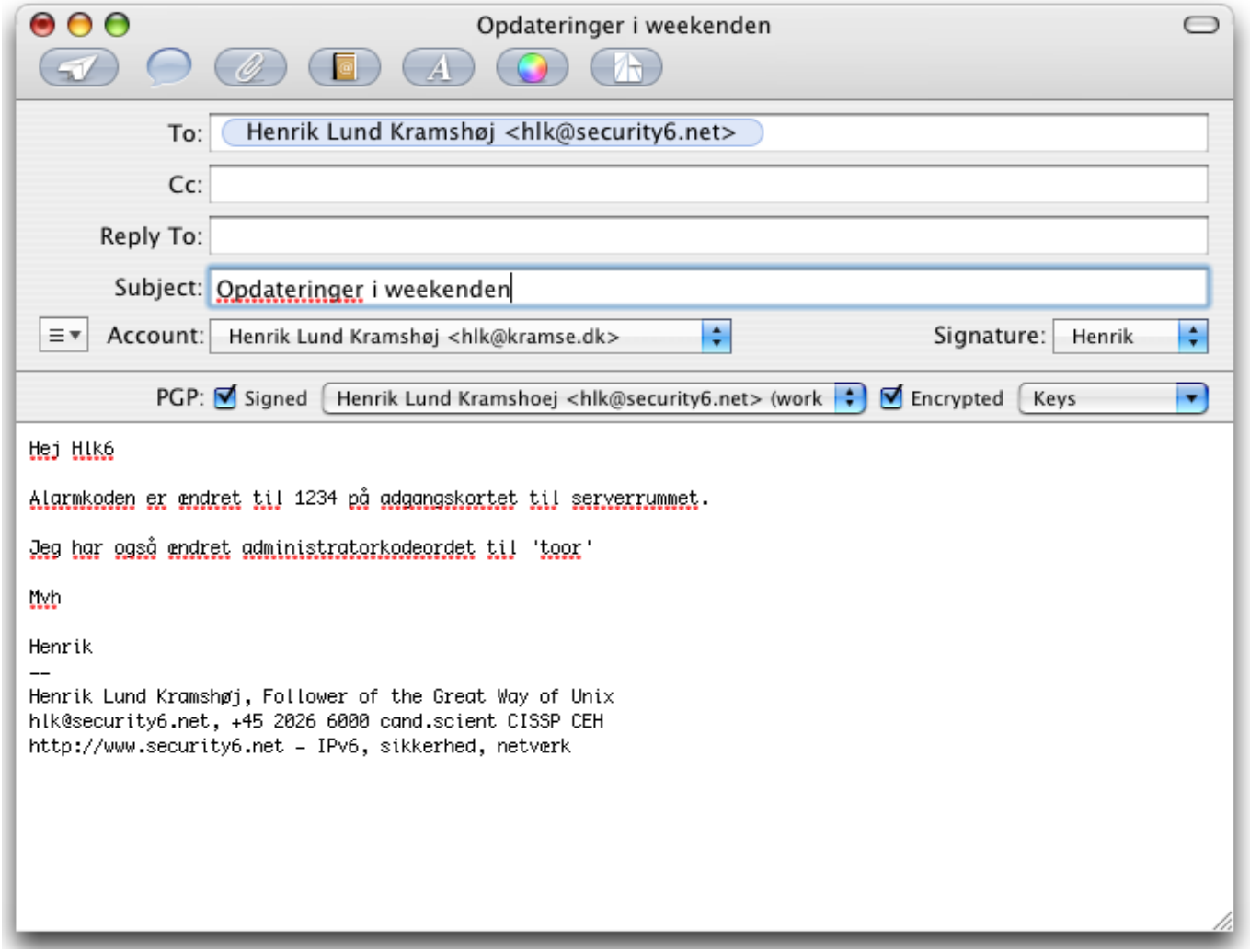
`http://patrol.psyced.org/`

Email is insecure



Email without encryption is like an open post card

Email with encryption - sending

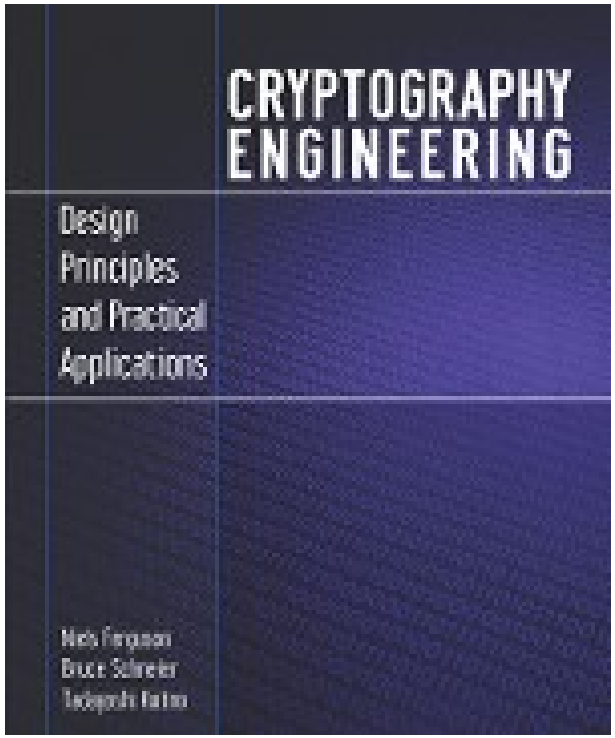


Sending a secure email is not hard

Encrypted in transit

A secure email is protected while being transported

Kryptering: Cryptography Engineering



Cryptography Engineering by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno
`https://www.schneier.com/book-ce.html`

Cryptography ensures confidentiality and integrity of messages

FileZilla - understøtter SFTP

SOLIDO NETWORKS

FileZilla Features

Overview

FileZilla Client is a fast and reliable cross-platform FTP, FTPS and SFTP client with lots of useful features

Features

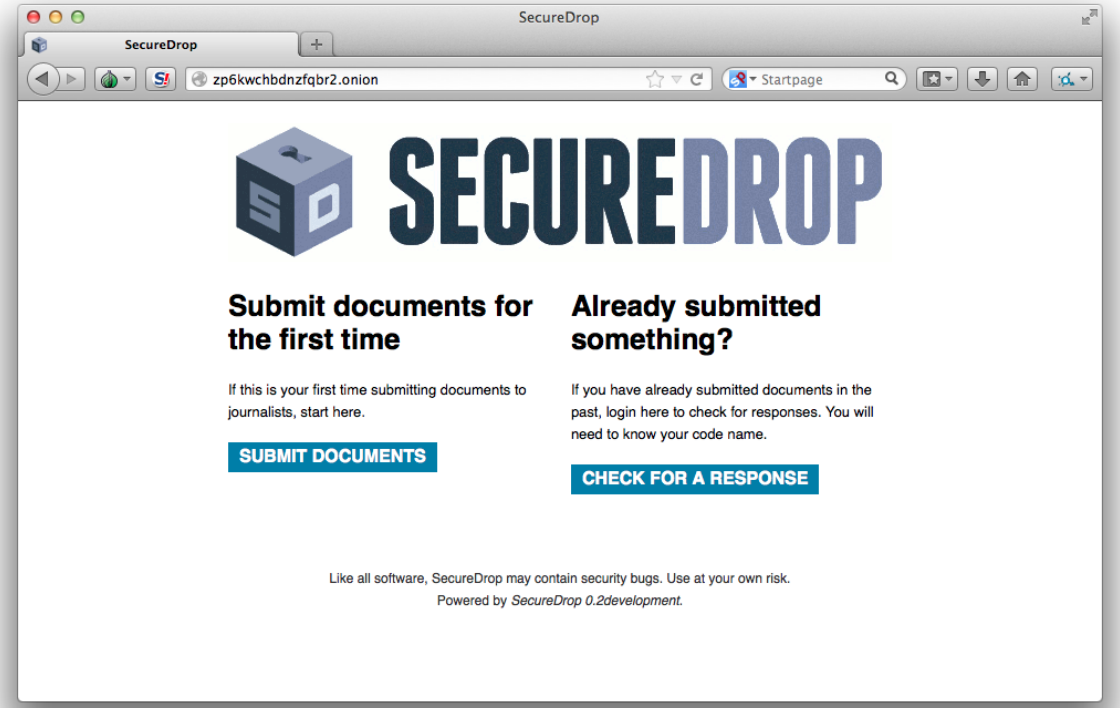
Among others, the features of FileZilla include the following:

- Easy to use
- Supports FTP, FTP over SSL/TLS (FTPS) and SSH File Transfer Protocol (SFTP)
- Cross-platform. Runs on Windows, Linux, *BSD, Mac OS X and more
- IPv6 support
- Available in many languages
- Supports resume and transfer of large files >4GB
- Tabbed user interface
- Powerful Site Manager and transfer queue
- Bookmarks
- Drag & drop support
- Configurable transfer speed limits

`http://filezilla-project.org/`

Stop using unencrypted FTP, use SSL/TLS or SFTP

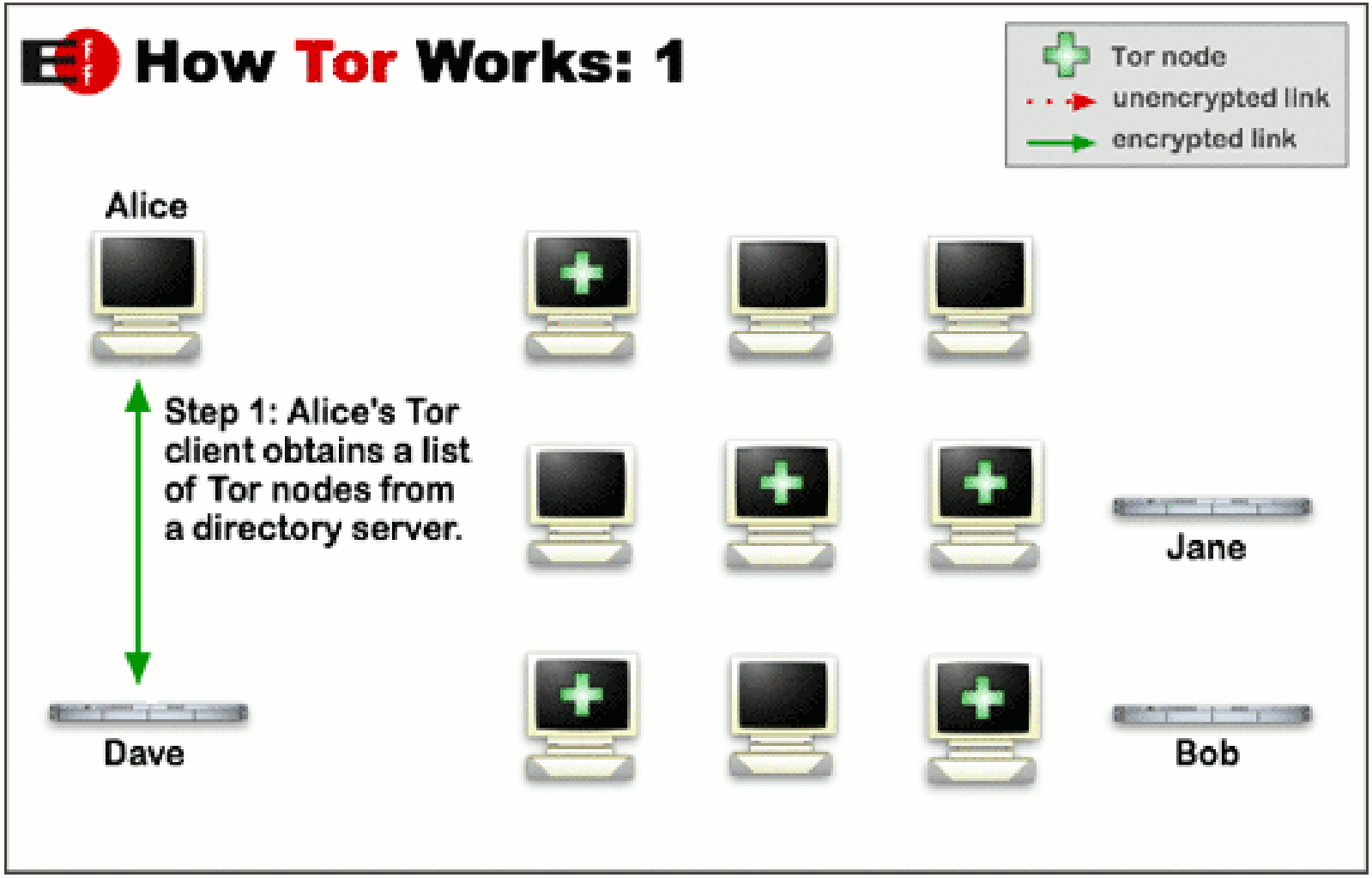
Tor project anonymized web browsing and services



Sample site Secure Drop whistleblower site
There are alternatives, but Tor is well-known

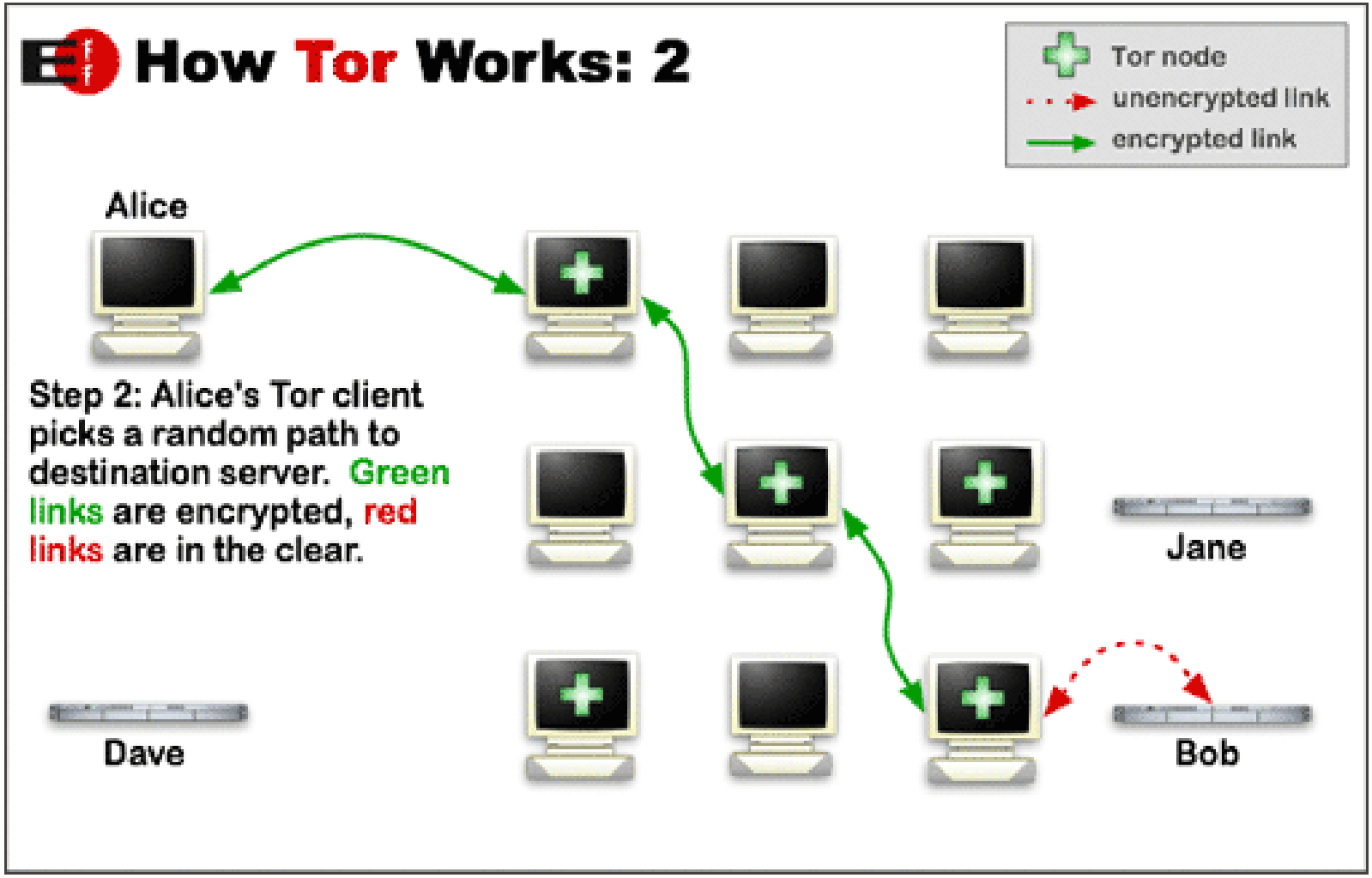
`https://www.torproject.org/`

Tor project - how it works 1



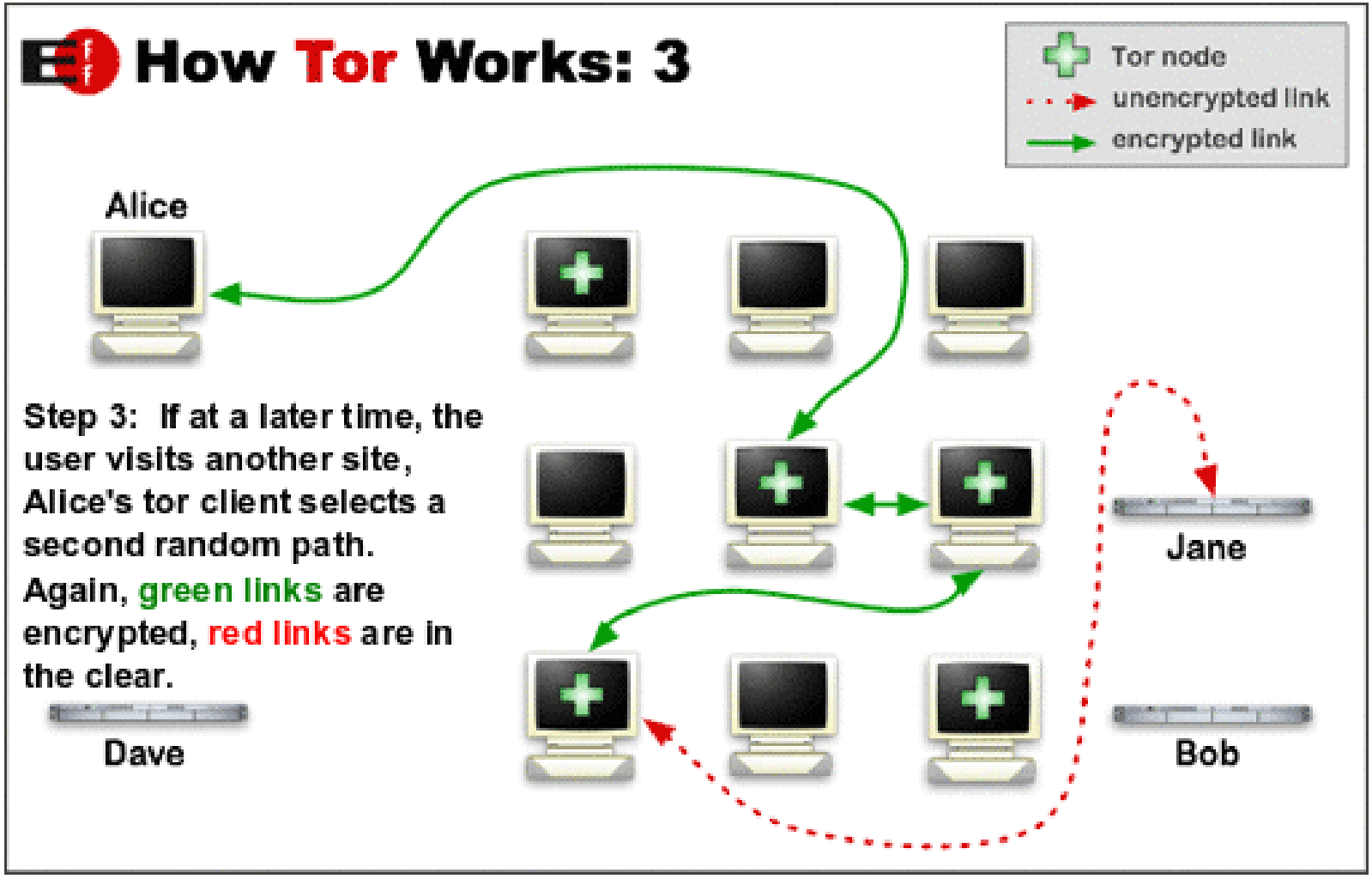
pictures from `https://www.torproject.org/about/overview.html.en`

Tor project - how it works 2



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

Tor project - how it works 3



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

Tor project install

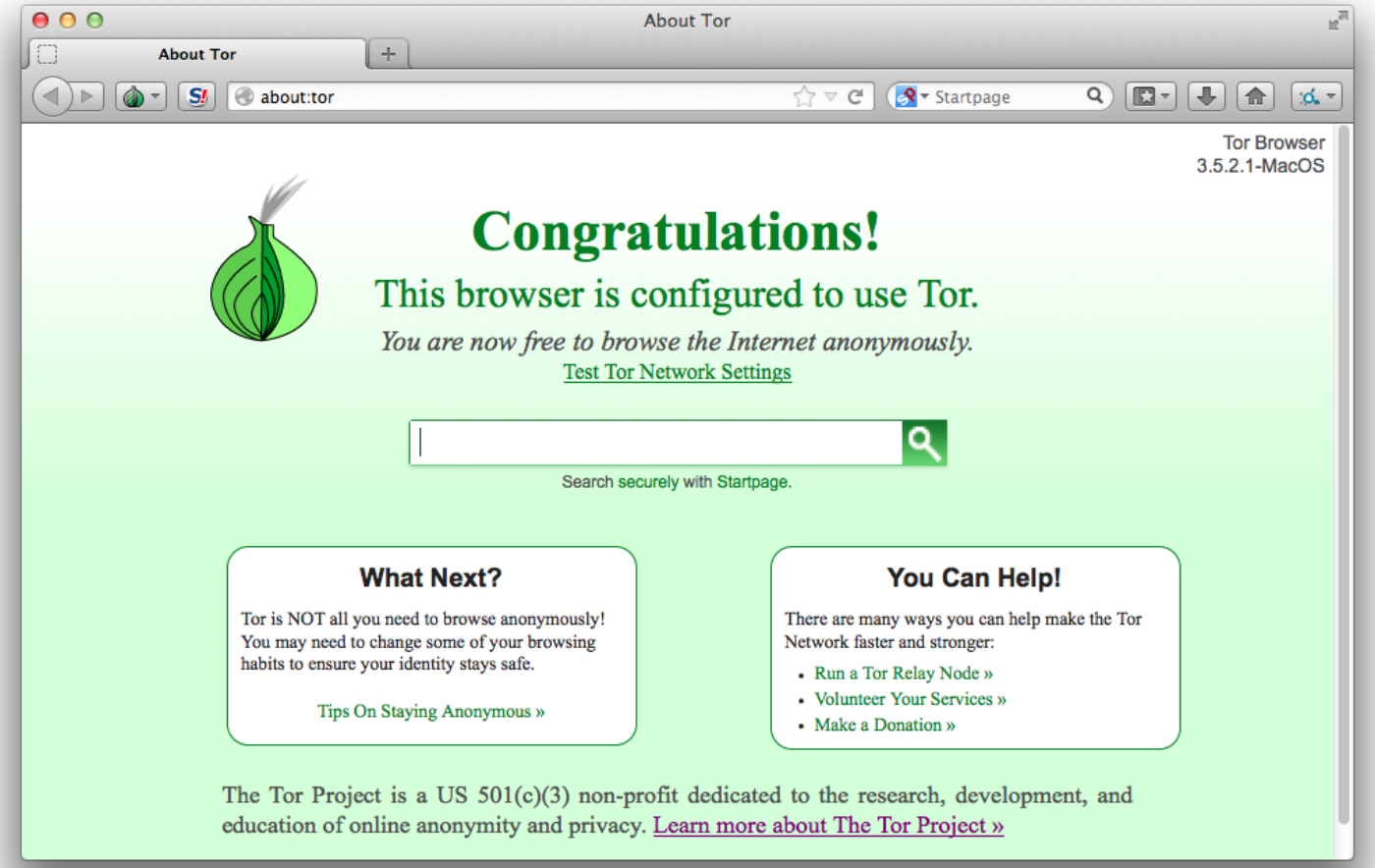
Multiple Tor tools, like Torbutton on/off for Firefox

We recommend starting out with the Torbrowser bundles from
`https://www.torproject.org/`

Torbrowser - outdated

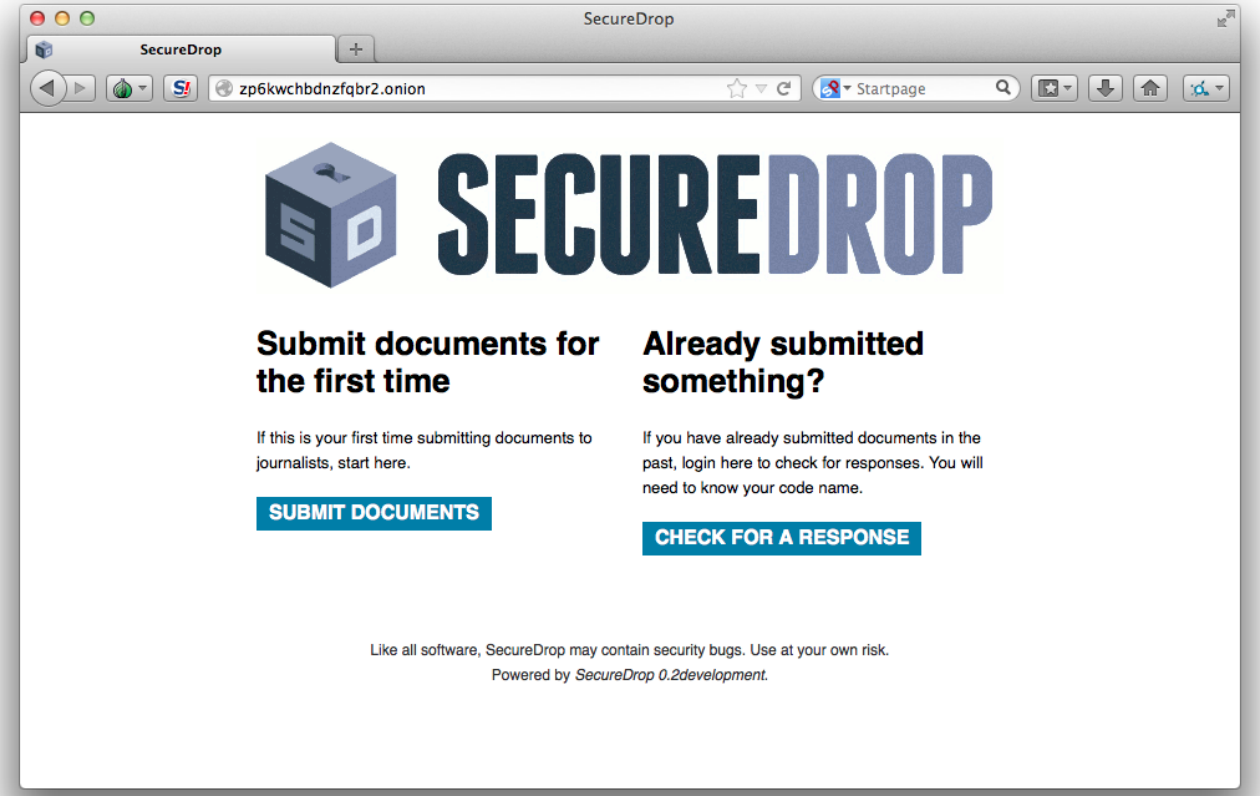
Missing an update!

Torbrowser - anonym browser



More anonymized browsing - uses Firefox in disguise

Torbrowser - sample site



.onion er Tor adresser - hidden sites

Example SecureDrop from Radio24syv, danish media

`http://www.radio24syv.dk/dig-og-radio24syv/securedrop/`

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 is nice, but limited, Whonix Tor-encrypts all traffic

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

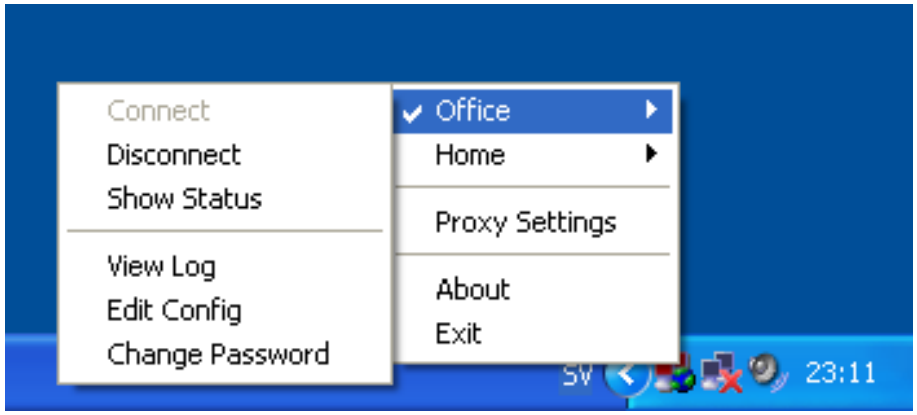
KeySync:
Syncing Trusted Identities

TextSecure:
Short Messaging Service (SMS)

Pixelknot:
Hidden Messages

Don’t forget your mobile platforms `https://guardianproject.info/`

VPN a tunnel for all your traffic



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

DNS censorship in Denmark

There is a lot of DNS tampering today, you can change to: Censurfridns.dk UncensoredDNS

- ns1.censurfridns.dk / 89.233.43.71 / 2002:d596:2a92:1:71:53::
- ns2.censurfridns.dk / 89.104.194.142 / 2002:5968:c28e::53

also see the web site and blog for more information:
`http://www.censurfridns.dk` and `blog.censurfridns.dk`

DNS tampering is unacceptable

DNSSEC trigger

Using DNSSEC and DANE will help

I use DNSSEC-trigger secure local DNS server for your Windows or Mac 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/`

Follow Twitter Safety news

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

The Twitter team actively promotes good security practives

Checklist

- BIOS kodeord, pin for your phone
- Firewall - especially on laptops
- Install anti virus and anti-spyware if using Windows
- Use multiple browsers with different security settings
- Use OpenPGP and email encryption
- Use Password Safe, Keychain Access (OSX) or other password saving programs
- Consider using hard disk or file encryption like Truecrypt `http://www.truecrypt.org/`
- Keep systems and applications updated with security fixes
- **Backup your data** - perhaps the single most important point
- Secure wipe your devices when you stop using them

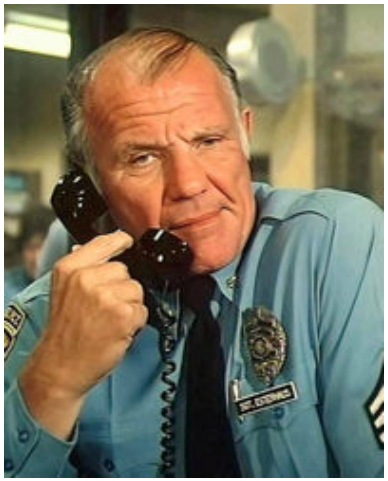
Work together

Team up!

We need to share security information freely

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

Be careful - questions?



Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

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