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 ~Cypherpunk Manifesto

Velkommen til Kryptoparty!

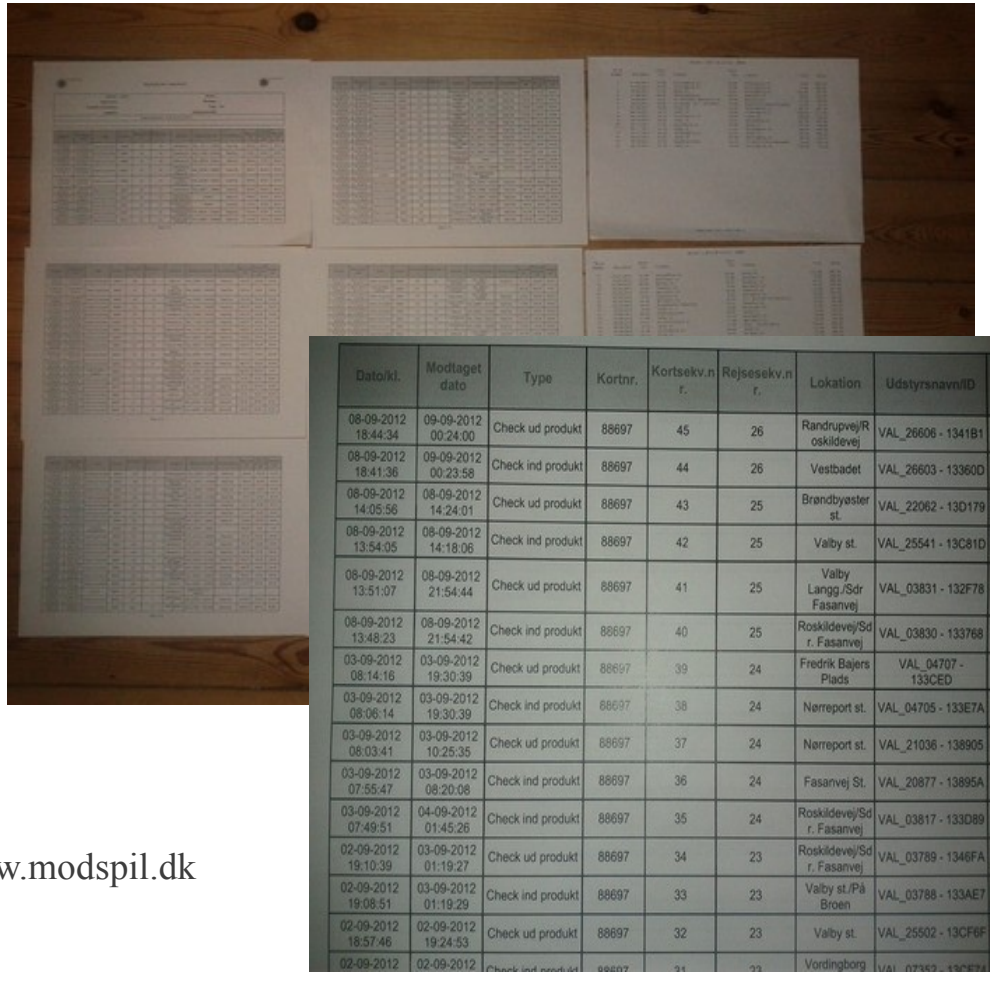
- Det handler om at beskytte vores privatliv mod uønsket overvågning
- ”Privacy is not secrecy” - det handler om *selv* at bestemme, hvor meget af vores private færden er til rådighed for andre
- Vi bliver i dag logget, registreret og overvåget som aldrig før
- Private oplysninger flyder rundt på nettet og samles i store centrale databaser, der kan hackes eller misbruges

Hvad registreres?

- Hvor vi opholder os (logning af IP og masteinformation)
- Hvilke hjemmesider, vi besøger
- Hvem vi ringer til, sender SMS, sender email til
- Hvor vi handler (brug af kreditkort, bankinformation)

Case: Panton og Rejsekortet

- Rejsekort med rabat kræver CPR-nummer
- Christian Panton fra Bitbureauet søgte aktindsigt hos Rejsekortet A/S
- Tid og sted angives på sekundet for samtlige rejser
- Gemmes efter bogføringsloven i 5 år
- Kan udleveres mod dommerkendelse



Dato/kl.	Modtaget dato	Type	Kortnr.	Kortsekv.nr.	Rejsesekv.nr.	Lokation	Udstyrsnavn/ID
08-09-2012 18:44:34	09-09-2012 00:24:00	Check ud produkt	88697	45	26	Randrupvej/Roskildevej	VAL_26606 - 1341B1
08-09-2012 18:41:36	09-09-2012 00:23:58	Check ind produkt	88697	44	26	Vestbadet	VAL_26603 - 13360D
08-09-2012 14:05:56	08-09-2012 14:24:01	Check ud produkt	88697	43	25	Brøndbyøster st.	VAL_22062 - 13D179
08-09-2012 13:54:05	08-09-2012 14:18:06	Check ind produkt	88697	42	25	Valby st.	VAL_25541 - 13C81D
08-09-2012 13:51:07	08-09-2012 21:54:44	Check ud produkt	88697	41	25	Valby Langg./Sdr Fasanvej	VAL_03831 - 132F78
08-09-2012 13:48:23	08-09-2012 21:54:42	Check ind produkt	88697	40	25	Roskildevej/Sdr. Fasanvej	VAL_03830 - 133768
03-09-2012 08:14:16	03-09-2012 19:30:39	Check ud produkt	88697	39	24	Fredrik Bajers Plads	VAL_04707 - 133CED
03-09-2012 08:06:14	03-09-2012 19:30:39	Check ind produkt	88697	38	24	Nørreport st.	VAL_04705 - 133E7A
03-09-2012 08:03:41	03-09-2012 10:25:35	Check ud produkt	88697	37	24	Nørreport st.	VAL_21036 - 138905
03-09-2012 07:55:47	03-09-2012 08:20:08	Check ind produkt	88697	36	24	Fasanvej St.	VAL_20877 - 13895A
03-09-2012 07:49:51	04-09-2012 01:45:26	Check ind produkt	88697	35	24	Roskildevej/Sdr. Fasanvej	VAL_03817 - 133D89
02-09-2012 19:10:39	03-09-2012 01:19:27	Check ud produkt	88697	34	23	Roskildevej/Sdr. Fasanvej	VAL_03789 - 1346FA
02-09-2012 19:08:51	03-09-2012 01:19:29	Check ind produkt	88697	33	23	Valby st./På Broen	VAL_03788 - 133AE7
02-09-2012 18:57:46	02-09-2012 19:24:53	Check ud produkt	88697	32	23	Valby st.	VAL_25502 - 13CF6F
02-09-2012	02-09-2012					Vordingborg	

Internet: Logningsbekendtgørelsen

- Implementerer EUs logningsdirektiv af 2005
- Internetudbyder skal logge
  - samtlige besøg på hjemmesider
  - afsender, modtager, tidspunkt for samtlige emails
  - afsender, modtager, masteoplysninger for telefonsamtaler og SMS
- ”Terrorlogning” - værdi i praksis meget tvivlsom

Logningsdirektivet: Problemer

- Retssikkerhed: Tillader retrospektiv efterforskning op til et år efter (måske i helt andre ting)
- Krænker princip om uskyldig til det modsatte er bevist
- Tillader endevending af lovlydige borgeres private kommunikation
- Bedre med målrettet logning efter dommerkendelse
- Kan let omgås (og er ubrugelig)

Sociale medier

- Eksempel: Facebook
- FB gemmer alle billeder, opslag, emails, chat, nuværende venner, tidligere venner, kommentarer, alt
- Hvis du bruger det flittigt = hvor du er, hvem du taler med, år tilbage
- Oplysninger mines og sælges til annoncører – du er ikke kunden, du er produktet
- Der registreres mere, end du selv lægger op

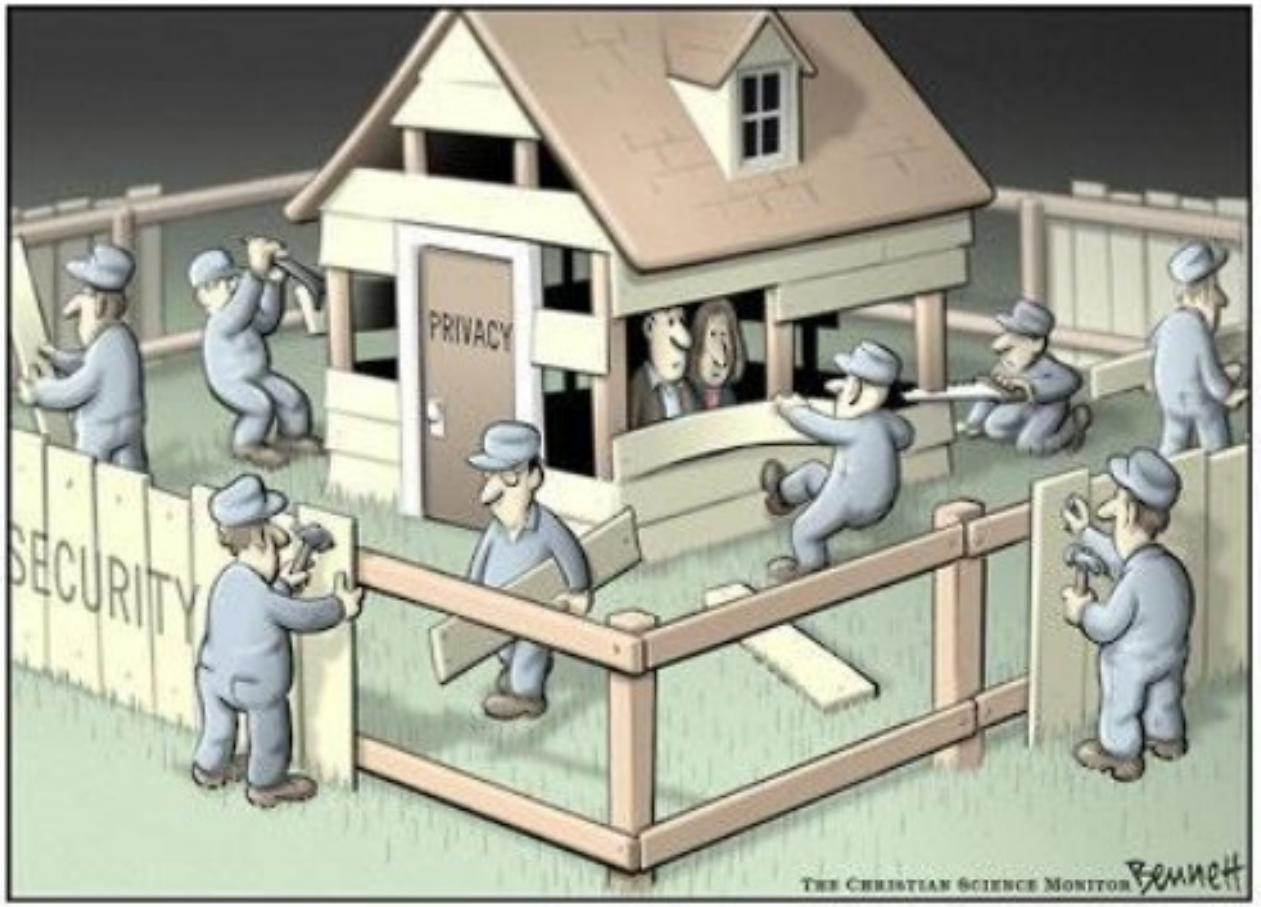
Facebook, fortsat

- Mange hjemmesider har ”Like on Facebook-knap
- Kan f.eks. vise dig, hvad dine venner har læst
  - FB ser og registrerer, at *du* går derind
  - FB ser alle sider med ”Like”-knap, du besøger
- FB ser alle IP-adresser, du logger ind fra (GPS-koordinater for smartphone)
- Total kortlægning af dit liv og din færden
- Google og FB er *busted* for at registrere visning af ”Like-sider” selv om du er logget ud
- Hvem kan få de oplysninger?

Det bliver værre

- CISPA
  - foreslået overvågningslov i USA
  - tillader firmaer at overvåge kommunikation og give til myndigheder
  - ”sikkerhed” er begrundelse nok
  - stort set alle data til ikke specificerede myndigheder
  - besejret i kongressen 2012, nu på vej tilbage
- UK ”snooper's law”
  - Politiet skal have adgang til emails, SMS, telefonsamtaler osv. i ”real time”
  - ”on demand” - %dommerkendelse
  - ”private data” fra Facebook, Google+ mv
  - besejret/afvist, men regeringen har ikke givet op
- Canadisk overvågningslov C-30 – vidtgående overvågning, ingen dommerkendelse, fremsat og besejret 2012, fremsat igen, besejret februar 2013
- Begynder det at ligne et mønster?

Sikkerhed kontra privatliv



Så hvad gør vi?

- Mere registrering → større risiko for misbrug, også af kriminelle
- August 2012 → Ny ”snooping law” i Australien
- Asher Wolf foreslår ”cryptoparty” på Twitter
- Oktober 2012 var afholdt 30 cryptoparties verden over
- Februar 2013 har der været cryptoparty i mindst 70 byer verden over
- https://cryptoparty.org

Kryptoparty – fordi:

- Vi har ret til at beskytte vores privatliv
- Kryptering er lovlig
- Overvågning truer den enkeltes sikkerhed (indbrud, misbrug, botnets)
- Hvad en lovlydig borger laver og taler med kommer kun vedkommende selv ved
- Retten til privatliv er en grundlæggende menneskerettighed – artikel 12 i FNs Menneskeretserklæring
- So let's do it!

Pause og spørgsmål

Kryptering og privatliv i praksis

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 ~Cypherpunk Manifesto

Advarsel

- Kryptografiske værktøjer kan kun beskytte dit privatliv – er ikke skudsikre
- **Læs advarsler i manualerne!**
- Skal bruges rigtigt
- Folk, der bruger stærk kryptering, kan afsløres med: keyloggers, indbrud, almindeligt politiarbejde (f.eks. regimekritiske bloggere i Iran)
- Kryptering kan hjælpe meget, hvis det bruges rigtigt
- Bruges overalt på nettet

Case: General Petraeus

- CIAs direktør Petraeus havde affære m. Paula Broadwell, kommunikerede via ”Kladder” i anonym GMail-konto (dumt!)
- FBI blev involveret, da ny elskerinde modtog chikanemails fra Broadwell – fra anden GMail-konto
- Broadwell brugte kun disse konti fra caféer, hoteller mv.
- FBI gennemgik gæstelister – fællesmængde gav dem Broadwell og som bonus hende og Petraeus' Gmail
- FBI kan tilgå usendte emails i GMail uden ”warrant”
- Skandale
- Vi kan senere tale om, hvordan de skulle have gjort!

Plan

- Først vil vi gennemgå ”tunge”, effektive værktøjer, du let kan bruge: Tor, VPN, torchat, OTR chat, TAILS
- Generelle råd om anonym kommunikation
- Herefter mindre specifik tale om disk-kryptering og BitCoin
- Herefter anvisninger på små ting, der kan gøre en stor forskel

VPN

- Virtual Private Network
- Bruges bl.a. af firmaer til at give sikker adgang til kontornetværk
- For forbrugere – skjuler al din netværkstrafik (browser, email) for det lokale netværk
- Krypteret linje til udbyderen (proxy), herefter normal trafik ud til internettet

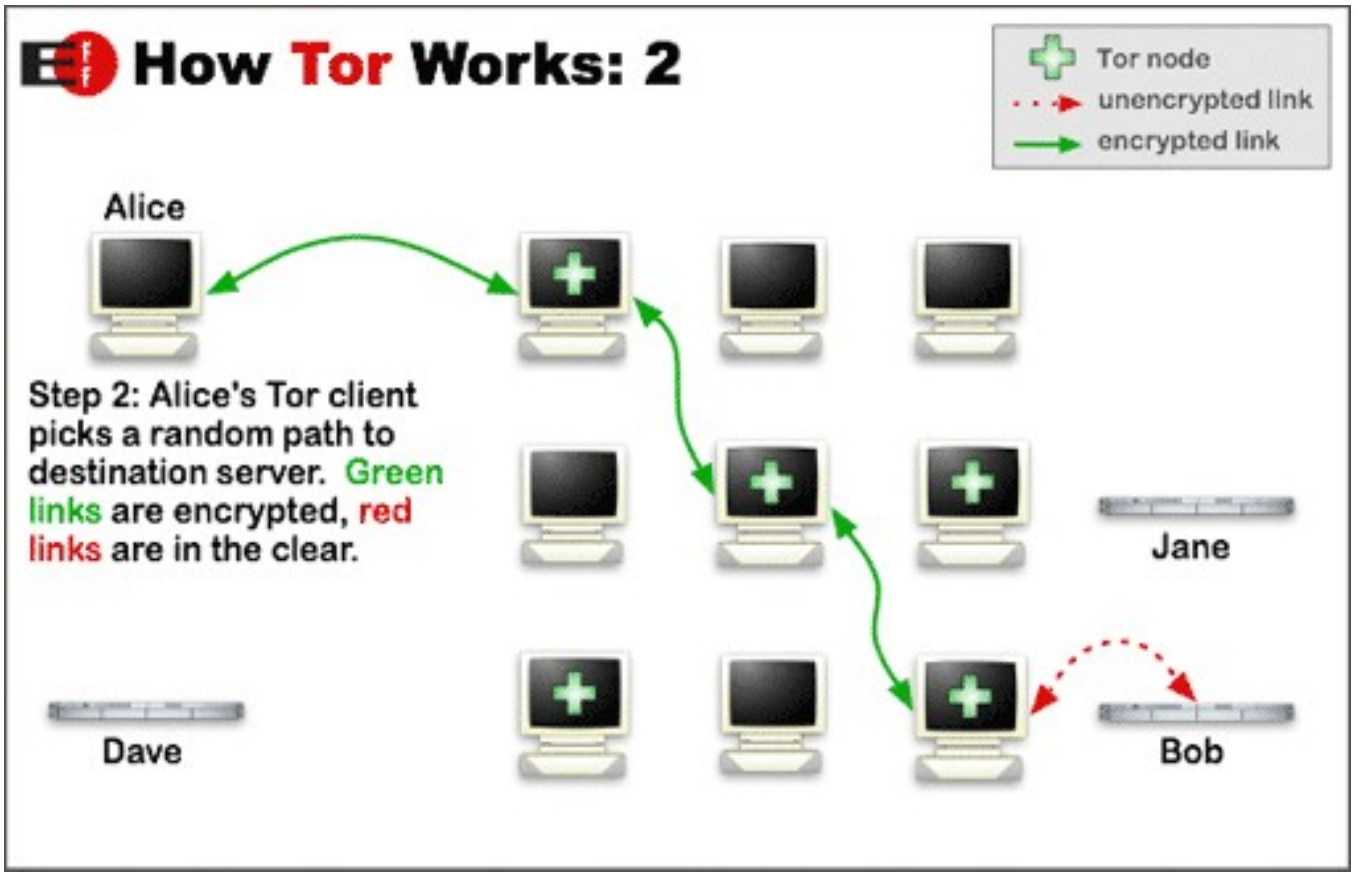
VPN, fortsat

- + Omgår logning, undgår overvågning
- + Er let at sætte op
- - Kræver, at du stoler på VPN-udbyderen
- Koster penge
- Eks:
  - AirVPN (EU)
  - BeeVPN (DK)
  - RiseUp (USA)
- Download her:
  http://openvpn.net/index.php/download.html
- Ubuntu:
  sudo apt-get install network-manager-openvpn-gnome

Tor, The Onion Router

- Bedste og sikreste måde at færdes anonymt
- Al trafik går gennem tre relæer i Tor-netværket
- Al trafik pakkes ind i tre lag kryptering
- Kun sidste lag kan se, hvor trafikken skal hen
- Kun første lag kan se, hvor den kommer fra
- Ingen måde at ”regne tilbage”

Tor, The Onion Router



- Den valgte rute skifter hele tiden

Tor, The Onion Router

- Skabt af US Naval Research Labatory
- Adopteret af EFF
- Download Tor fra www.torproject.org
- Giver *anonymitet*, ikke (altid) kryptering
- Beskytter mod lokal overvågning
- Som VPN, men ikke én udbyder at stole på

Tor – ting at passe på

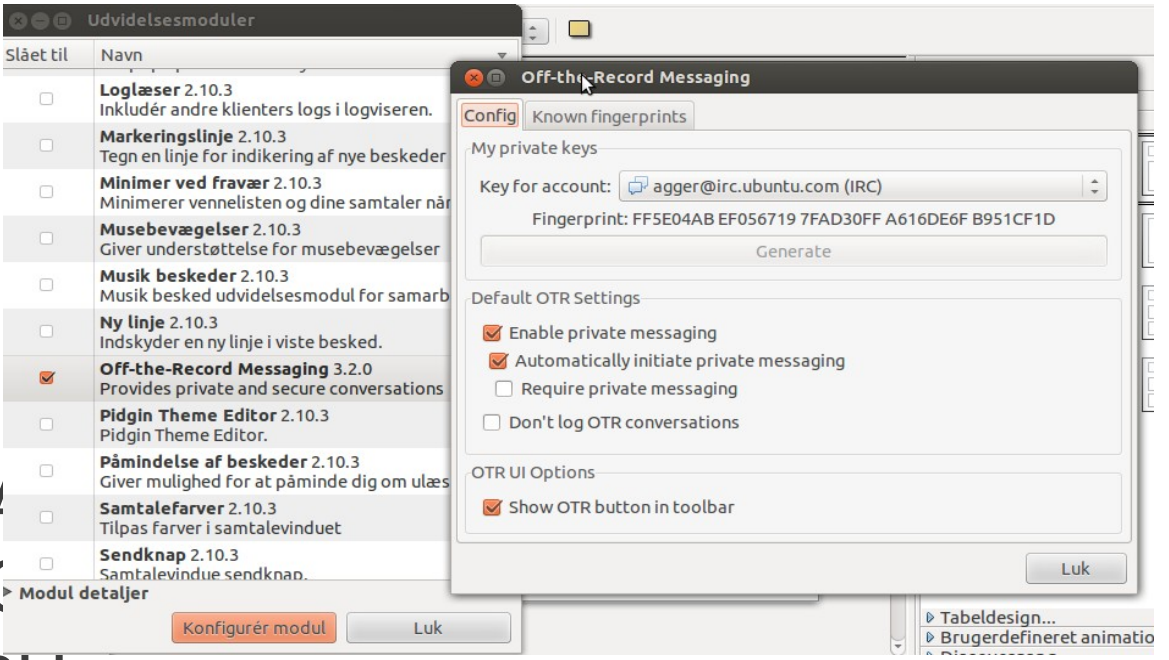
- Åbn ikke PDF- eller Word-filer e.l. fra sites du browser anonymt (kan hente ting fra nettet udenom Tor)
- Exit nodes kan overvåge dig. Brug altid SSL/HTTPS når muligt
- Din udbyder/lokale overvågende myndigheder kan se, du bruger Tor – *timing attack*
- Ellers p.t. bedst mulige anonymisering
- Download fra www.torproject.org

OTRChat

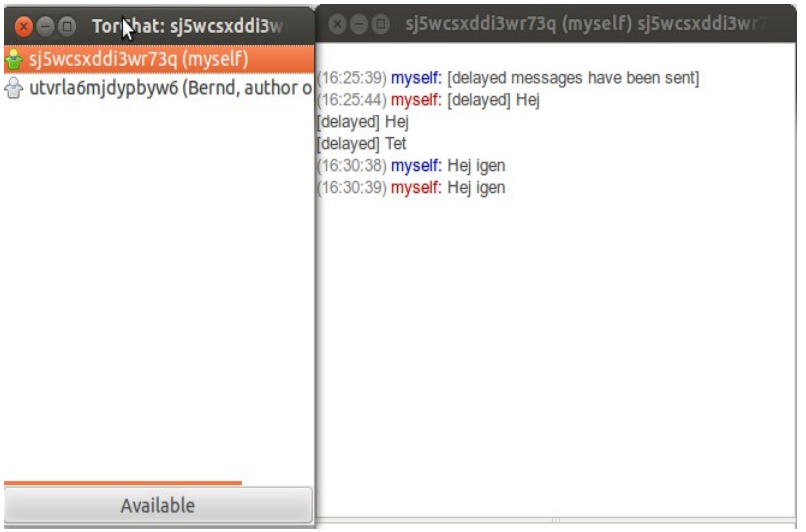
- Er et krypteringsplugin til Pidgin (IM-klient)
- Download fra http://www.cypherpunks.ca/otr/
- Download Pidgin fra www.pidgin.im/download
- Virker med XMPP, f.eks. Google Talk
- Du autentikerer din partner ved at angive en fælles hemmelighed eller et hemmeligt svar, I kan aftale i telefonen
- Dette garanterer din partners identitet så længe samtalen varer

OTRChat – opsætning i Pidgin

- Demo
- Hvad der kommer ud i GT-loggen er: ? OTR:AAIDAAAAAAMA… Efhj0G/DHpDMwBGZq… gU1un3qKnyRLLgCrUlsH …
- Chat-server kan se, man snakker sammen, men ikke spor af hvad om.
- IP kan stadig beskyttes med VPN eller Tor



torchat



- Download fra
- https://github.com/prof7bit/TorChat/downloads
  `(Ubuntu: sudo apt-get install torchat)`
- Standalone chat-klient med Tor indbygget
- Kører *internt* i Tot-netværket
- 100% skjult – ingen kan vide, hvad din torchat-bruger er, hvis du ikke fortæller dem det
- 100% anonym - ingen kan finde dig ud fra en torchat-bruger hvis du ikke selv røber dig
- 100% krypteret, umulig at detektere (uden en keylogger e.l.).
- Velegnet til absolut privat kommunikation, helplines e.l.
- Let at bruge – download, start, tilføj venner

Anonym adfærd – what should Petraeus have done?

- Vi vil gerne være klogere, end CIAs direktør var
- Opret anonym mailkonto et sted, hvor du ikke skal give personlige oplysninger (Hushmail, f.eks.)
- Brug Tor til dette
- Læs *aldrig* denne email uden at bruge Tor
- Hvis du har flere anonyme mailkonti, læs dem ikke i samme session
- Hav intet i adresse mv, der kan identificere dig (disse punkter ville have reddet Petraeus)
- Hvis du skriver med nogen, undgå navne o.l. eller krypter alt
- Du kan oprette en blog f.eks. på smartlog.dk med din anonyme mail – læs eller skriv *aldrig* på den uden at bruge Tor

Kort om kryptering af harddisk

- Hvad hvis din computer eller bærbare bliver stjålet?
- Hvis harddisken er krypteret, kan ingen læse noget uden dit password
- I Ubuntu kan man vælge ”krypteret hjemmemappe”, når man opretter ny bruger (eCryptfs) - ANBEFALES
- Alt krypteres, når brugeren logger ud
- I Windows kan man f.eks. bruge TrueCrypt (kan også oprette krypteret partition, alle OS)
- **Advarsel:** Mistet password for kryptering → dine data er tabt.

Kort om BitCoin

- Kryptografisk valuta, læs mere på www.weusecoins.com
- Muliggør ”kontant”, anonym betaling på nettet
- Bruges til handel med mange tvivlsomme ting – pas på!
- Man kan betale VPN med BitCoin → VPN-udbyderen ved ikke hvem du er. Ekstra anonymitet.
- Download klient (bitcoin-qt) på bitcoin.org, synkroniser og køb bitcoins på nettet
- Mange tvivlsomme aspekter, men effektivt til anonym og hurtig overførsel af små beløb

Kort om kryptering af email

- Pragmatisk kryptering – sæt dit mailprogram op til SSL/TLS
- Emails krypteres rigtigt med PGP
- Download fra http://www.gnupg.org
- Er et public key system – send folk din offentlige nøgle, dekrypter med din private
- Kan bruges med EnigMail plugin til Mozilla Thunderbird
- Virker også fint i Evolution og Claws

Små ting gør en stor forskel

- Drop Internet Explorer – brug Firefox (IE har endeløse sikkerhedsproblemer)
- Drop om muligt Windows – virus er alvorlig trussel (Ubuntu er godt alternativ)
- Brug sikkerhedsplugins – HTTPS Everywhere, AdBlock Plus mm.
- *Log ud* af sociale medier som Facebook, når du ikke bruger dem
- Slet jævnligt alle cookies
- Meld dig ud af logningen – brug Tor eller VPN
- Kør NemID med Java i virtuel maskine eller som separat bruger
- Flere forslag?

Savner vi noget

- Input og kritik modtages
- Skriv til agger@modspil.dk med kommentarer
- Hvis folk vil vide mere → arranger selv flere cryptoparties
- Spørgsmål?

Nu er det jeres tur

- Download Tor: www.torproject.org
- Download torchat:
  github.com/prof7bit/TorChat/downloads
- Download Pidgin og OTRChat:
  http://www.pidgin.im
  http://www.cypherpunks.ca/otr
- Check VPN:
  airvpn.org, beevpn.com, riseup.net99
- Prøv TAILS:
  tails.boum.org
- Download TrueCrypt: www.truecrypt.prg
- Download GnuPG, krypter emails: www.gnupg.org
- Installer Firefox-plugins – HTTPS Everywhere, AdBlock Plus, DoNotTrackMe, Ghostery
- Tor-browser m.m. til Android: https://guardianproject.info/