Undgå aflytning med fri software

Databeskyttelsesdagen
2014-01-28

Ole Tange
Best.medl. IT-Politisk forening

Snowdens afsløringer: PRISM

TOP SECRET//SI//ORCON//NOFORN

Gmail facebook Hotmail YAHOO! Google skype paltalk.com YouTube AOL mail

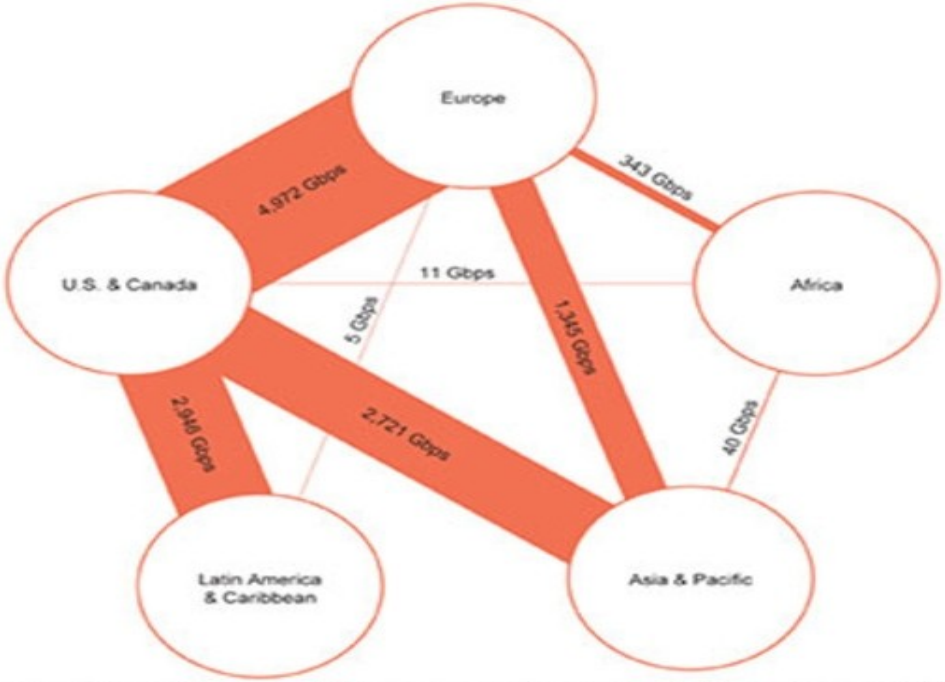
SPECIAL SOURCE OPERATIONS

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

PRISM

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

NSA SIGINT Enabling Project
(Bullrun)

Fra den lækkede projektbeskrivelse:

“The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs”

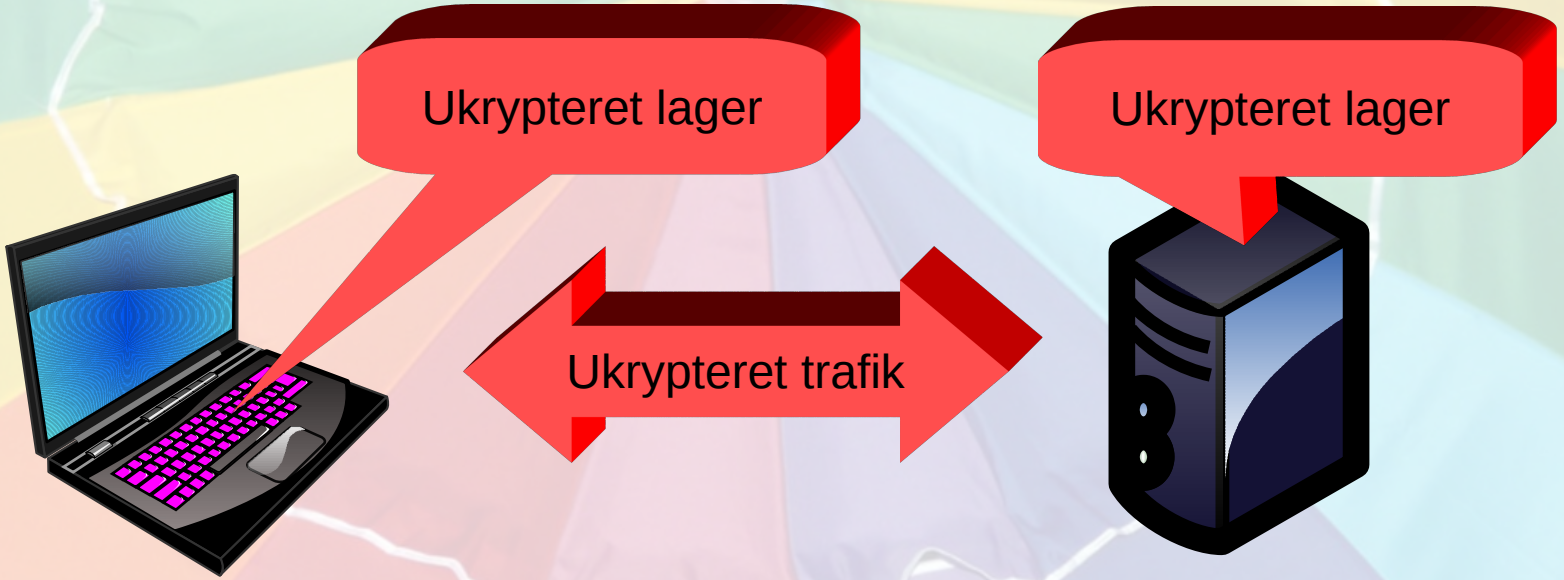
“Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.”

Udokumenteret aflytning

- Merkels telefon
- Udenlandsk kontrollerede IT-leverandører
  - Snowdens advokat mener det er naivt at tro andet
- Netværksudstyr
  - USA, Kina, Korea, Taiwan
- Telefoniudstyr
  - USA, Kina, Sverige, Korea
- Operativsystemer
  - Windows, Mac OS

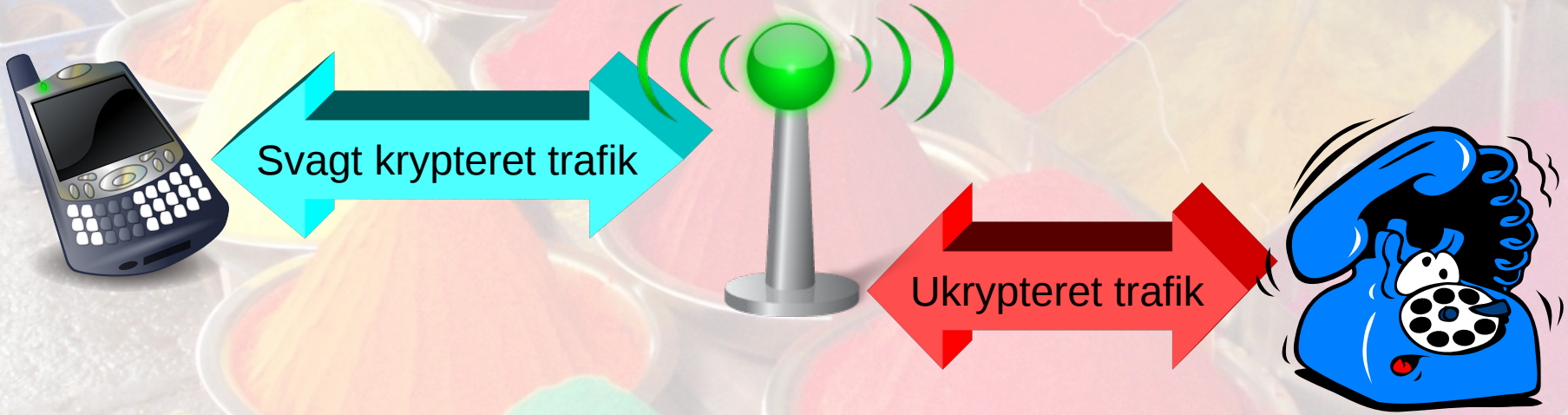
Email og web trafik (http)

- Ukrypteret hele vejen



Telefoni

- Svag kryptering mellem mobil og mast
- Ingen kryptering på fastnet



Den græske aflytningsskandale
2004-2005

- Telefoncentraler har fjernaflytningsfunktionalitet
  - Til politiet
- Benyttet af ukendte gerningsmænd

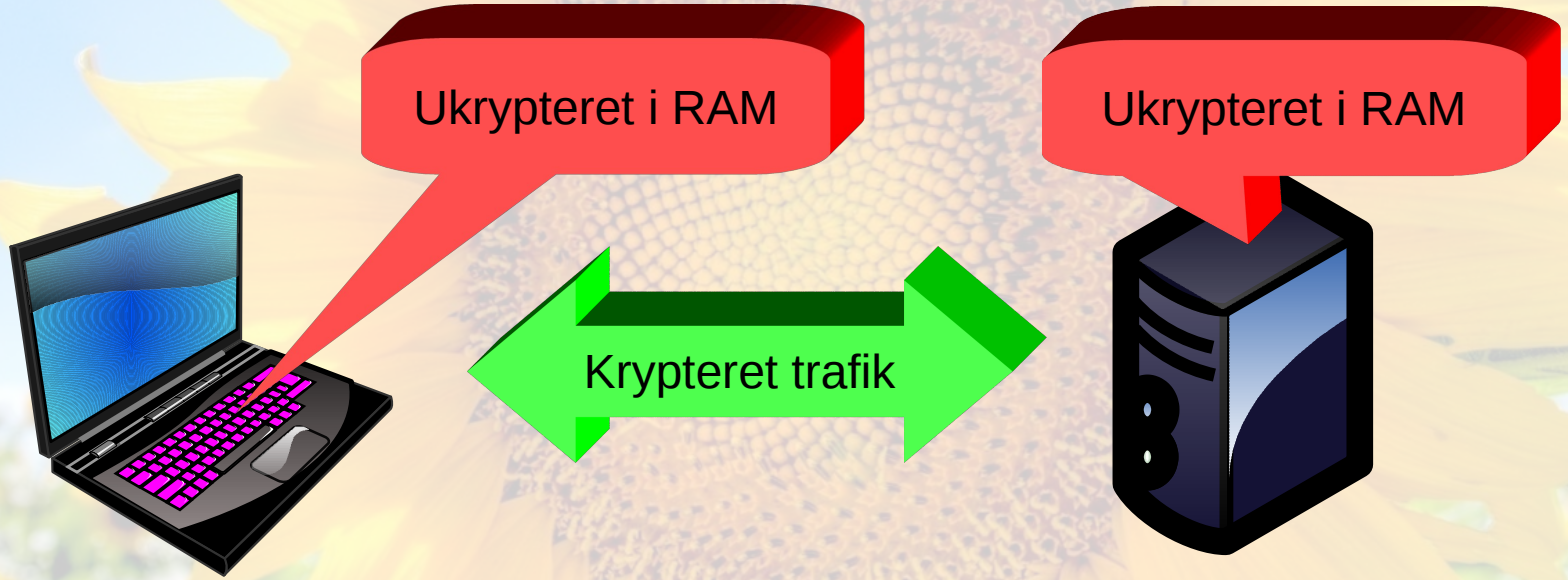
- Konklusion: Regn ikke med at bagdøre kun vil blive brugt af de, der indsætter dem

Kryptering

- Moderne krypteringsalgoritmer kan ikke brydes inden for få år
  - Men der kan være indbygget bagdøre i softwaren
- Performance
  - 1 GByte/s på moderne CPU: Ikke en begrænsning

VPN, cloud, server park, https

- Aflytning kan kun ske hvor data er ukrypterede
  - F.eks. i enderne af VPN eller https



Cloud, server park

- PATRIOT act/FISA Amendment Act
  - Mulighed for CIA/FBI at få adgang til data
  - Administrator må ikke fortælle dig det
  - Administrator må ikke tale med egen advokat
- USA-baserede virksomheder er underlagt
- Er virksomheder med afdelinger i USA underlagt?
  - Det bør I undersøge

Tillid og cloud/server park

- Teknisk vil en leverandør altid kunne aflytte RAMmen
  - Virtuelle maskiner: nemt
  - Fysiske maskiner: mere bøvlet
- Et spørgsmål om tillid
- Den eneste sikre løsning: Eget serverrum
- Brug kun cloud/server park til ikke-fortrolige data

Krypteret backup/filsystem i skyen

- Krypteres det af klienten: OK
- Krypteres det af serveren: Kan aflyttes af serveradministrator
  - F.eks. Dropbox, Google Drive, Skydrive

Software-bagdøre

- Dokumenterede bagdøre i:
  - Windows (NSA-key, automatisk opdatering)
  - Amazons Kindle e-bogslæser (“1984”)
  - iPhone NSA indbrud
- Det er nemt at for leverandøren at putte bagdøre i. Det kan camoufleres som programmeringsfejl.
- Snowden har bekræftet NSA arbejder med at give leverandører incitament til at sætte bagdøre i.

Konklusion

- Regn med at al teletrafik uden for organisationen bliver aflyttet
- Forvent jeres cloud/server camp leverandør kan blive presset
- Regn med at ufri software har bagdøre
  - Så får du ikke en ubehagelig overraskelse senere

Fri software

- Kendte eksempler
  - Android, LibreOffice, Firefox, Chromium, Drupal, Apache, VLC, GNU/Linux
- Definition: Friheden til at:
  - K øre programmet.
  - K ikke i programmets source-kode.
  - K opiere programmet.
  - K ode programmets source-kode om.

Fri software

- Sourcekoden er tilgængelig, så der er færre muligheder for at skjule bagdøre.
- Programmører bliver offentligt holdt ansvarlige.
- Andre kan kikke med over skulderen og finde fejl
- Den bedste garanti mod bagdøre med vilje.
  - Men ingen 100% garanti
- Hvis I alligevel betaler hele regningen for udvikling, så få softwaren under en fri licens.

Læses sourcekode?
GNU Parallel case

- Ikke sikkerhedssoftware (Data processing)
- 2011-01-25 indsættes følgende test:

  # Guvf vf n grfg gb frr vs bguref ner ernqvat zl pbqr. Cyrnfr rznvy
  # pbbxvr@gnatr.qx jura lbh ernq guvf

  - Indsættes i et “mørkt hjørne i pulterkammeret”
  - Svagt krypteret, så det ikke dukker op i en søgning

  A→N B→O C→P … Z→M. Altså:

  # This is a test to see if others are reading my code. Please email
  # cookie@tange.dk when you read this

- 2011-04-09: Email om “Jeg har læst din kode”

Fri software til kontorbrug

- Tekstbehandling, regneark, præsentation: LibreOffice
  - Samtidig redigering i samme dokument: Etherpad
- Browser: Firefox
- Bogholderi: Saldi.dk
- Webserver med kryptering: Apache
- Filserver med kryptering: Tahoe-LAFS

Krypteret telefoni

- Kræver begge ender kan kryptere (ligesom telefax)
- Skype
  - Krypteret, men har PRISM-bagdør: Ikke en acceptabel løsning.
- Åben standard: ZRTP
  - F.eks. Fri software Lumicall App til Android
  - Blackphone.ch (ikke ~~Blackberry~~)

Anbefalinger

- Skift mindset: Argumenter ikke for kryptering, men imod.
- Tilbyd krypteret telefoni
  - eDag-2 gav borgerne mulighed for at send krypteret email. Giv på samme måde borgerne/kunderne mulighed for at ringe krypteret til jer. F.eks. med en Android telefon med Lumicall eller en Blackphone (ikke ~~Blackberry~~).
- Krypteret webadgang som standard
  - Installer server-kryptering (SSL-certifikater og https)
- Benyt fri software til fortrolige data
  - Benyt kun ufri software til at behandle data, der gerne må kompromiteres.
- Benytte kun cloud til ikke-fortrolige data (incl. bl.a. krypteret backup og krypteret filsystem).

Referencer

- PRISM/Bullrun: https://www.youtube.com/watch?v=BMwPe2KqYn4
- NSA bagdøre: https://www.youtube.com/watch?v=vILAlhwUgIU
- Lumicall: lumicall.org
- Blackphone: blackphone.ch
- Fotos (Creative commons): Benedict_Adam@flickr, SteveD@flickr, AdamSelwood@flickr, Alaskan_Dude@flickr, Highway_Patrol_Images@flickr, Jesse@flickr, Katia@flickr, Mark_Fischer@flickr, Matthew_Straubmuller@flickr, NeilsPhotography@flickr, Randy_Pertiet@flickr, Robert_McDon@flickr, Wonderlane@flickr, anieto2k@flickr, brian.gratwicke@flickr, fontplaydotcom@flickr, harinaivoteza@flickr, hyku@flickr, liber@flickr, magnetismus@flickr, momentcaptured1@flickr, mrhayata@flickr, radiant_guy@flickr, www.freestock.ca, magnetismus@flickr, paul_bica@flickr, y_Matthieu_Aubry@flickr, D_H_Parks, Matt_Erasmus@flickr, SteveD@flickr, www.freestock.ca, Dragon781O@flickr, Jakob_Montrasio, NaJina_McEnany, Dale_Chihuly@flickr, Chris_Willis@flickr, kaybee07@flickr, NeilsPhotography@flickr, Lloyd_Smith@google+, Cristian_bercaru