Datorsäkerhet

2022-05-13, Origo, Umeå

Introduktion

Vem är jag?

- Tomas Härdin
- C06
- Aktiv i Umeå Hackerspace, ACC och Föreningen Umeå Radioamatörer (FURA)
- Mail: tomas at haerdin.se
- XMPP: tms at haerdin.se
- IRC: thardin at irc.acc.umu.se

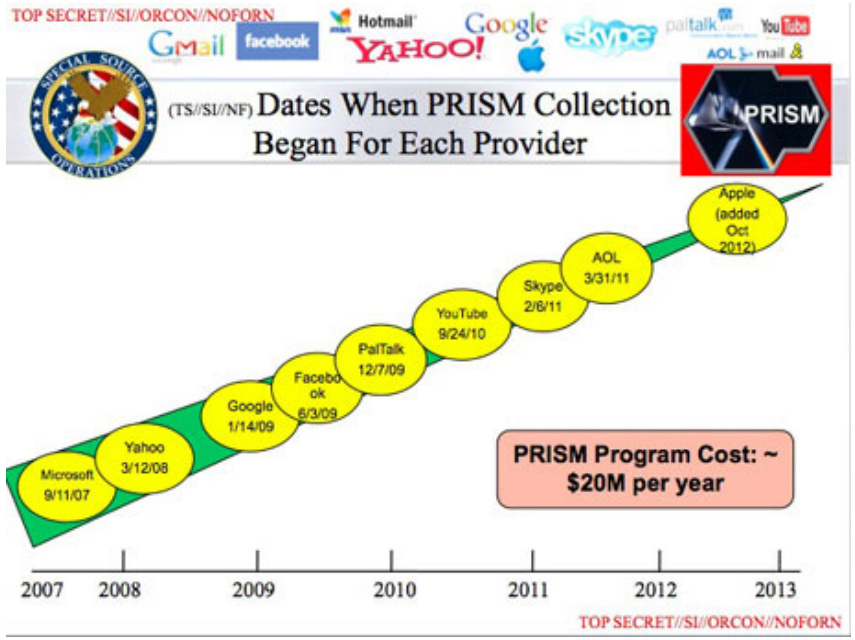
Umeå Hackerspace

- Fabriksgatan 8B (busshållplatsen)
  - Elektroniklabb
  - 3D-skrivare
  - Mekrum
  - Musikhack
  - Serverskrubb
- https://umeahackerspace.se/
  - Öppetstatus på hemsidan och IRC
  - MyHackerspace i Android/F-droid
- IRC: #uhck@irc.hethane.se

Generella saker

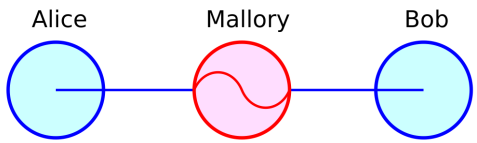
Hotmodell

- Vem vill åt dig?
- Vad vill de åt?
- Vad har de för resurser?
- Vad har *du* för resurser?
- Justera paranoia därefter



Problem

- Datorsäkerhet är *svårt*
- Buggar i allt
- Bakdörrar
  - Fri mjukvara viktigt, går att inspektera
- Fysisk tillgång? Evil maid attack
- Mikrofon kan höra knapptryckningar
- Datorer läcker radiosignaler
- Om möjligt, lämna dator och telefon hemma

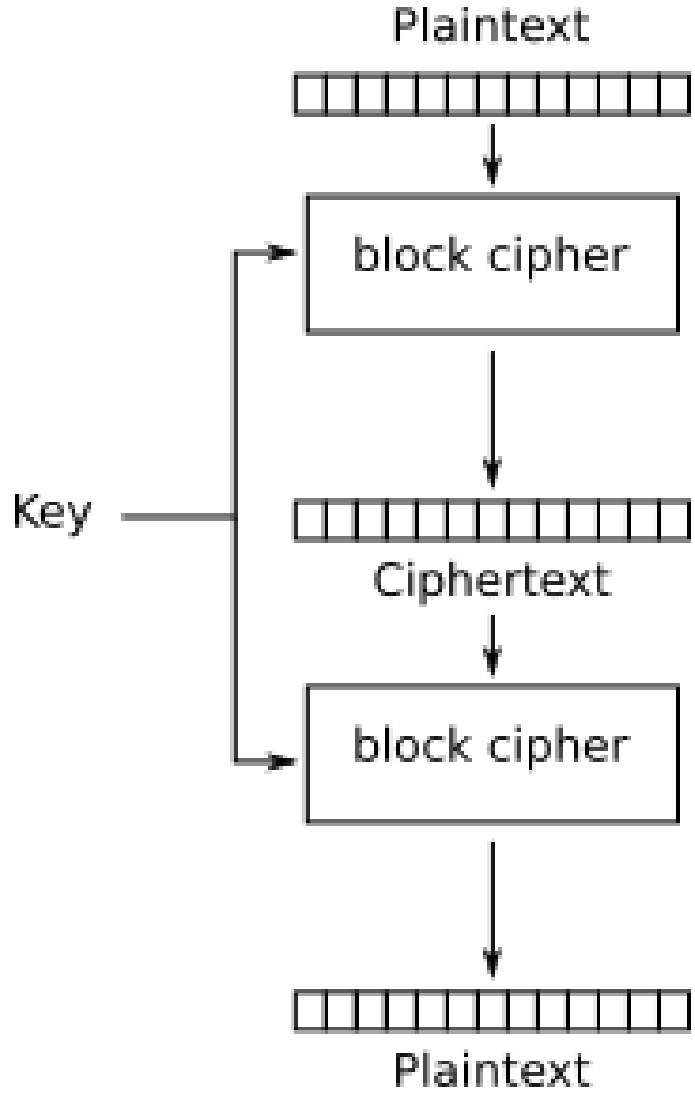



A.C.A.B.
ALL COMPUTERS ARE BROKEN

Detaljer

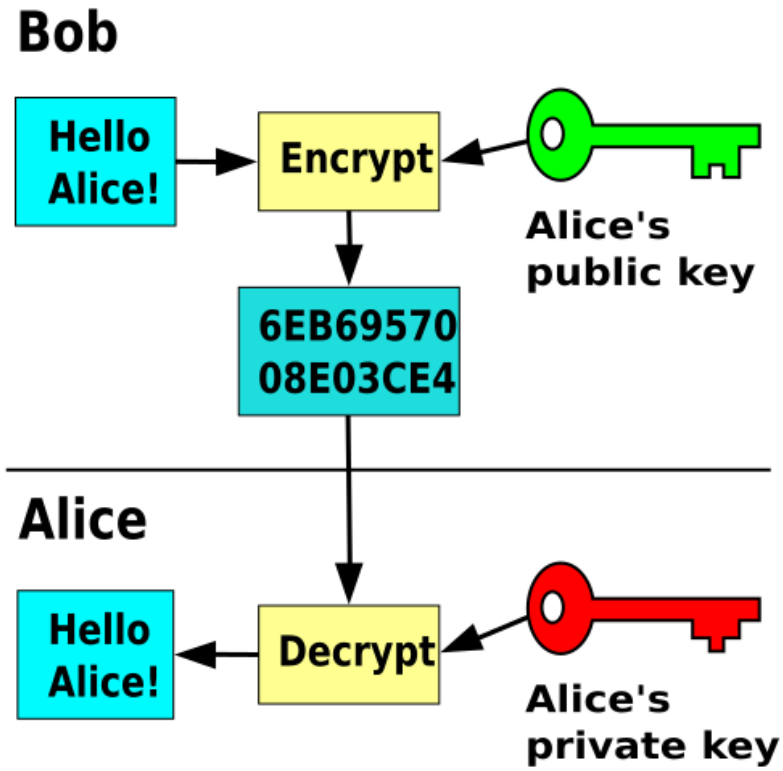
Symmetrisk kryptering

- Kom överens om en nyckel
- Använd nyckel för att kryptera och dekryptera meddelanden



Asymmetrisk kryptering

- Olika nycklar för kryptering och dekryptering
  - Publik nyckel
  - Privat nyckel
- Alla kan använda publik nyckel för att skicka meddelanden till dig
- Bara du kan dekryptera dem

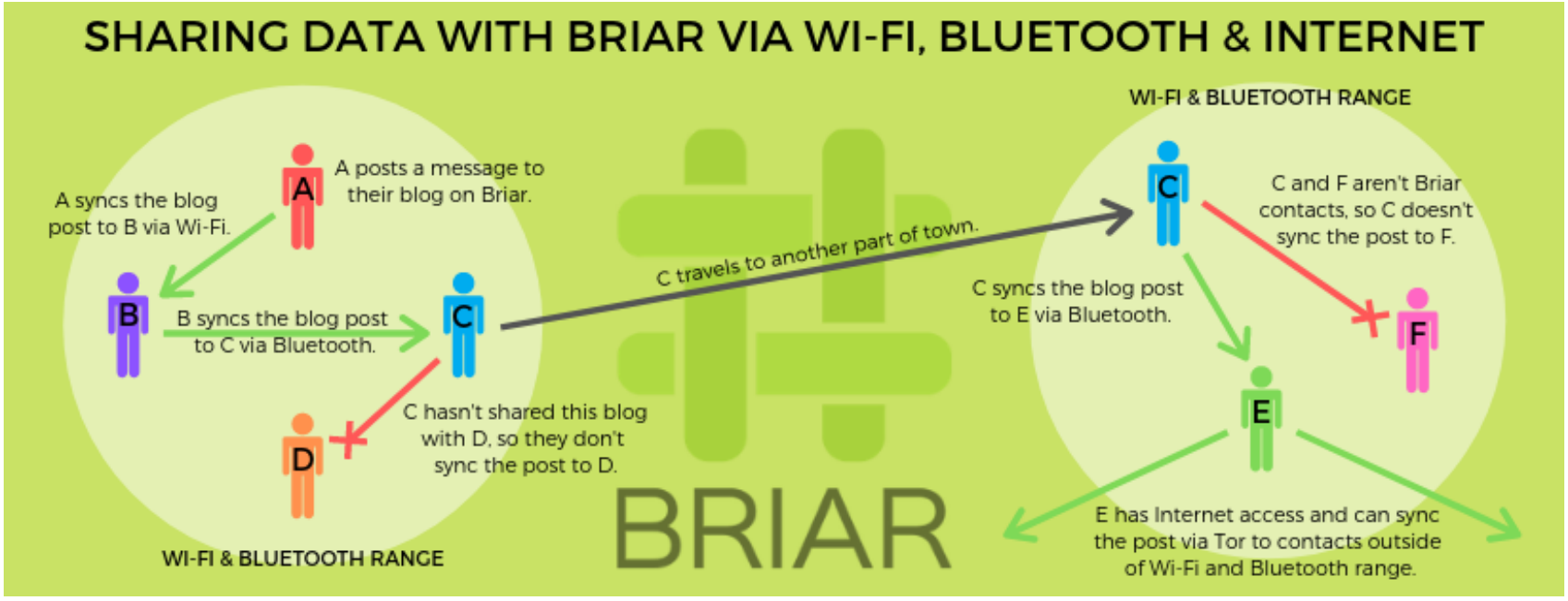


Chatt

Briar

- https://www.briarproject.org/
- Peer-to-peer över Tor, Bluetooth och Wifi
- End-to-end kryptering
- Store-and-forward
- Grupper och privatmeddelanden
- Metadataresistent
- Android/F-droid samt experimentell GTK-klient
  - Ej iOS pga Apple
- Måste vara online, slukar batteri

Briar

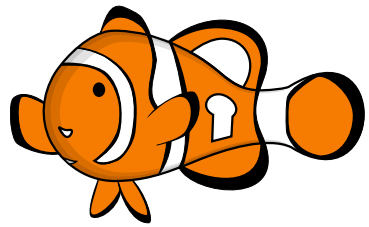

SHARING DATA WITH BRIAR VIA WI-FI, BLUETOOTH & INTERNET
A
A posts a message to their blog on Briar.
A syncs the blog post to B via Wi-Fi.
B
B syncs the blog post to C via Bluetooth.
C
C travels to another part of town.
D
C hasn't shared this blog with D, so they don't sync the post to D.
WI-FI & BLUETOOTH RANGE
BRIAR
WI-FI & BLUETOOTH RANGE
C
C and F aren't Briar contacts, so C doesn't sync the post to F.
C syncs the blog post to E via Bluetooth.
F
E
E has Internet access and can sync the post via Tor to contacts outside of Wi-Fi and Bluetooth range.

XMPP

- Federerat (servrar och klienter)
- TLS-kryptering
- Gruppchattar och privatmeddelanden
- Audio, video och fildelning
- Finns till alla plattformar
- Admins kan läsa meddelanden
- Kan lägga end-to-end ovanpå (OMEMO)

OMEMO

- End-to-end kryptering för XMPP
- Publika nycklar
- Gruppchattar och privatmeddelanden
- Ej audio och video (än)
- Måste ej vara online
- Ej metadataresistent
  - Admin ser vem du pratar med och när, men inte om vad



Signal

- End-to-end kryptering
- Centraliserad
- Kräver telefonnummer
  - Föreslår kontakter mha din telefonbok
- Grupper och privatmeddelanden
- Audio och video
- Kryptovaluta
- Android och iOS
- Ej metadataresistent

E-post

OpenPGP

- OpenPGP (Pretty Good Privacy)
  - GnuPG (aka GPG) = fri implementation
- Asymmetrisk kryptering
- Publika nycklar publiceras via keyservers
- Kan signera andra personers nycklar
- Indikerar att personen är den den säger den är
- Publik social graf

OpenPGP

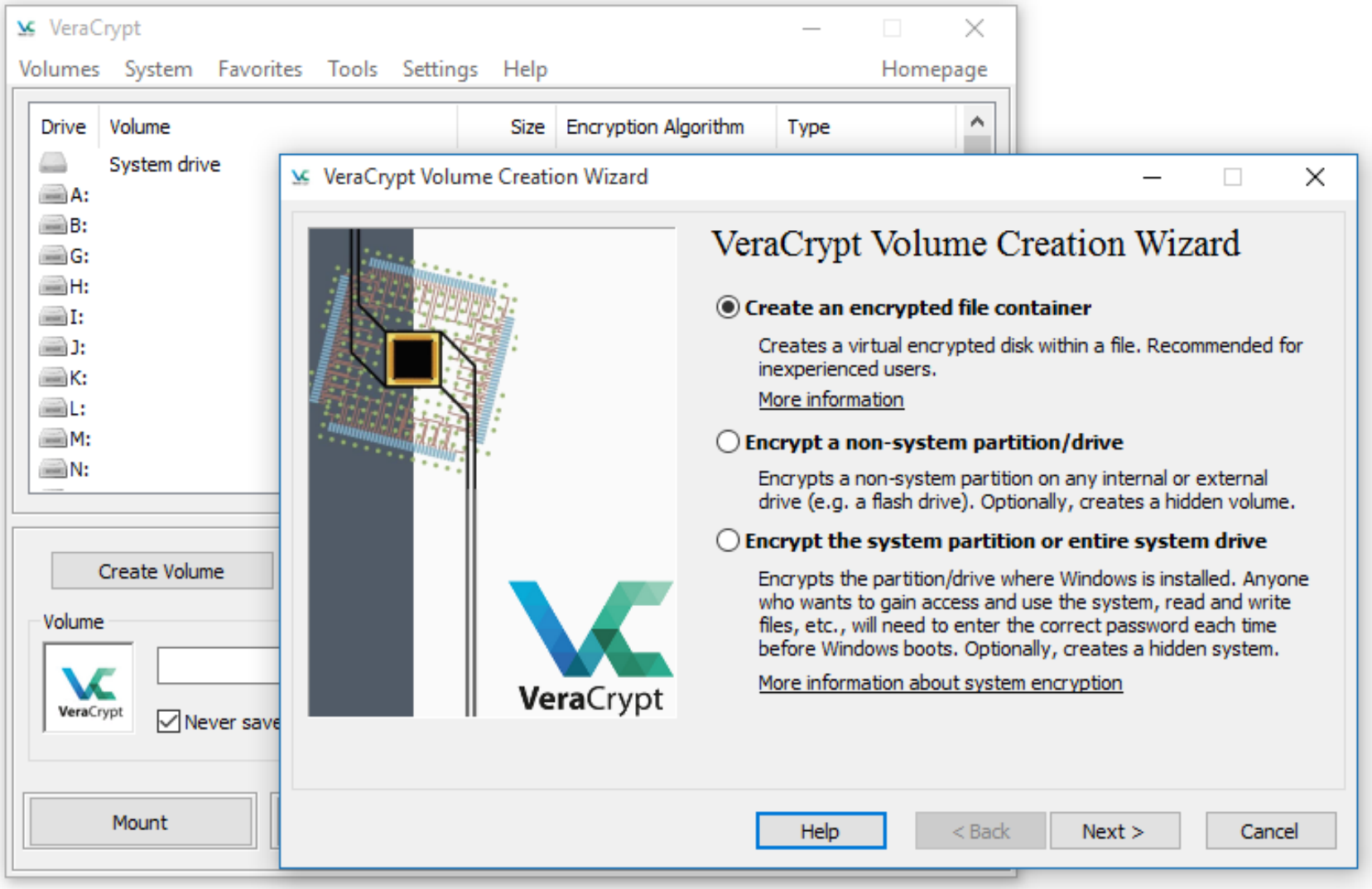
—BEGIN PGP MESSAGE—
hQIMA9rtEKLtqzXZAQ/8DogC0KrGG2W0IpCcZsDM
3zbZFw74qRI6by5tsFrvyj62yT2f2rlGqllQKg6Z
buZztJBxmadFwzCgSXD2kG5ptvNrlJd7j+Qyh3Uq
77sogsfSOM2VENyrH81sO+JvlIFX6j02UL6TlBPF
/cFQv7FxohwPcfpcszHTJKTRu6Ja/Q/uz5t6kelJ
UB1b9BOTl04aBn/iP+68si6DOuHeZmzsojsq8ql4
SAG8SMCJOpg2cAyyclJrircuYs3jhoGLXXfiiRP0
Xr3KAGU+0cJCZOD6Syz2JB6rj0iTVGHMOw==
=YAVT
—END PGP MESSAGE—

Diskkryptering

Veracrypt

- Krypterad partition eller ”disk-på-fil”
- Lösenord för att låsa upp
- Windows, macOS, Linux
- Fri mjukvara, många ögon

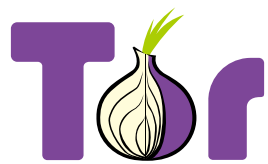
Veracrypt


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
System drive
A:
B:
G:
H:
I:
J:
K:
L:
M:
N:
Create Volume
Volume
VeraCrypt
Never save
Mount
VeraCrypt Volume Creation Wizard
VeraCrypt Volume Creation Wizard
Create an encrypted file container
Creates a virtual encrypted disk within a file. Recommended for inexperienced users.
More information
Encrypt a non-system partition/drive
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.
Encrypt the system partition or entire system drive
Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.
More information about system encryption
VeraCrypt
Help
< Back
Next >
Cancel

Övrigt

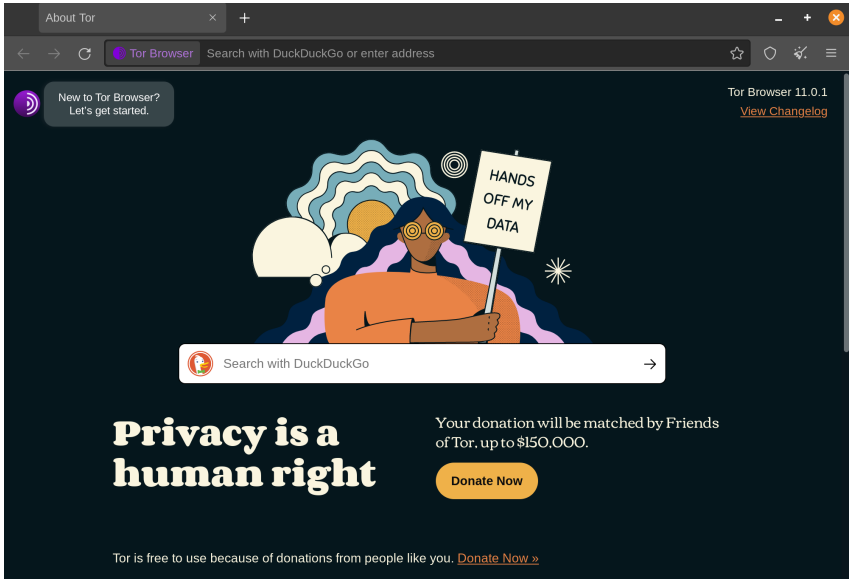
Tor

- The Onion Router
- Krypterat, nästlat nätverk ovanpå internet
- Möjliggör anonymt* webbsurf
- Går även använda för andra protokoll
  - XMPP och mail
- Hidden services
  - Helt ”inuti” Tor-nätverket
  - http://pfcgmo5hwfffwhis3zty2u2ufryrnzypue34h74va6ykw5iazgcvvtqd.onion/ = min webb
- Riktad övervakning möjligt i specifika fall
- Massövervakning ej möjligt (så vitt vi vet)



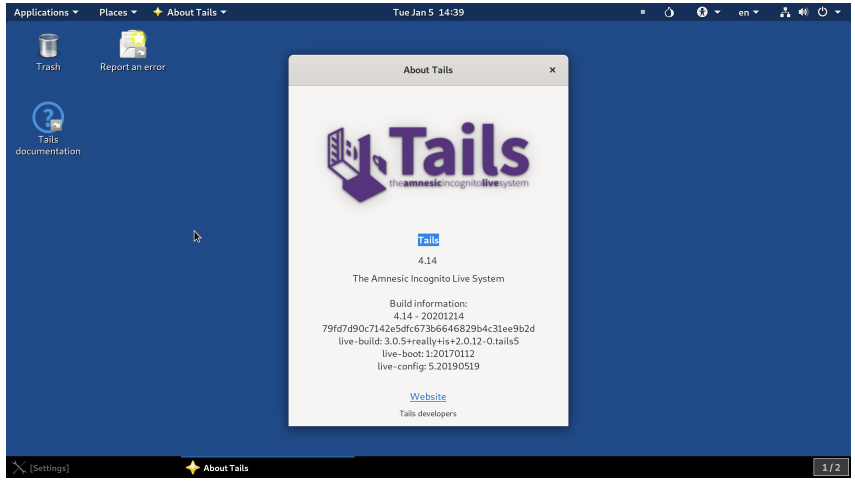
Tor Browser

- Firefox bundlad med Tor
- Diverse anonymitets-förbättringar
- Lätt att använda
- Kan få ny ”identitet” genom att trycka ctrl+shift+U



Tails

- The Amnesic Incognito Live System
- Operativsystem på USB-sticka
- Ansluter till internet via Tor
- Sparar inget
- Rensar RAM och stänger av om stickan rycks ur



Sammanfattning

Sammanfattning

- Datasäkerhet svårt
- Använd fri mjukvara
- Chatt: Briar, XMPP+OMEMO, Signal
- Mail: GPG
- Disk: Veracrypt
- Webb: Tor
- OS: Tails

Frågor?

Kontaktinfo igen

- Mail: tomas at haerdin.se
- XMPP: tms at haerdin.se
- IRC: thardin at irc.acc.umu.se