

reclaim your communication
and continue keeping it yours

Chaos Computer Club Salzburg

www.cccsbg.at

Sunday 3rd December, 2023



CC BY-NC-SA 4.0



- (almost) everyone wants to communicate private
- communication has always been intercepted and eavesdropped
- Would you send a love letter to your darling?
- Would you send a love letter to your darling in an open envelope?
- Would you like to receive your payslip openly besides your colleagues? Publish your bank account statement?
- content is only one aspect, metadata is the gold of the 21st century
- nothing new, but digitalization pushes it to a new level.

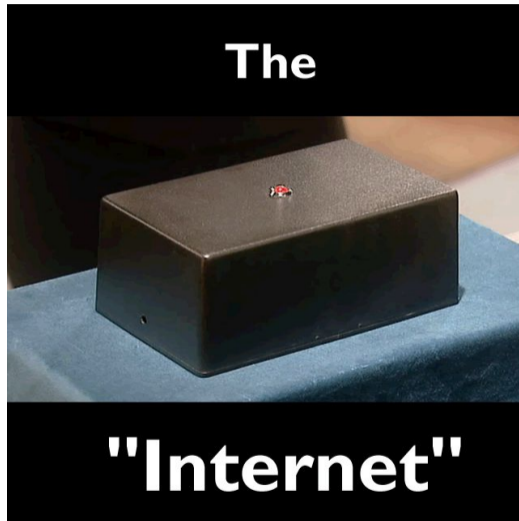
- 1 introduction, motivation and environment
- 2 basics of communication on the Internet
- 3 FOSS: An introduction
- 4 tools and alternatives
- 5 workshop - group work
- 6 summary and outlook
- 7 Q & A



- <https://www.cccsbg.at>
- quoted from the statutes[1]:
 - promoting the creative and critical use of technology
 - examination of technological developments and their effects on society and individuals with a focus on electronic data processing
 - commitment to open systems, freedom of information and net-neutrality
- associated to and under the auspices of <https://www.ccc.de>
- background of the speakers



- Who are you?
- What do you know already?
- Your expectations?
- How deep should we go?
- Do you already have questions or topics that you would like to have clarified or discussed?

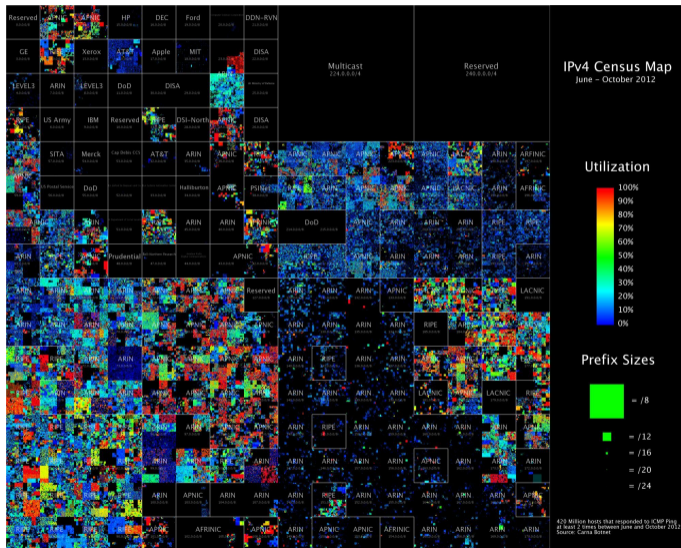


(A little bit of) History?

- 1965 - 1970: Military first, Science later (The ARPANET)
- 1974: First appearance of the Internet Protocol (IP)
- Organizations:
 - Internet Assigned Numbers Authority (IANA)
 - Subs: ARIN, LACNIC, RIPE NCC, AFRINIC, APNIC
 - The Internet Engineering Taskforce (IETF)

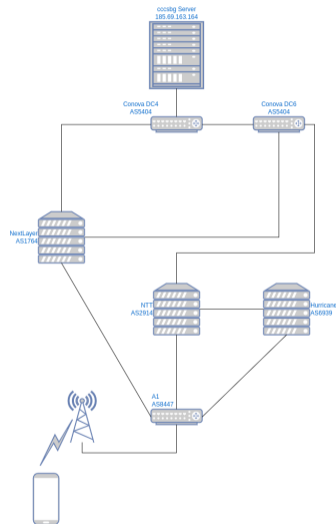
- Numbering system (like phone numbers)
- Two "versions": IPv4 and IPv6

- Length: 32bit
- Example: 185.69.163.164
- 3.702.258.432 public addresses
- BUT WE NEED MORE!



- Length: 128bit
- Example: 2a02:16a8:dc4:10ff:1337:dead:cafe:beef
- More addresses than grains of sand in the desert (340 trillion, trillion, trillion addresses)
- They think hope that is enough....for now

- Hero of the Internet: BGP (border gateway protocol)
- was sketched out in 1989 by engineers on the back of "three ketchup-stained napkins", and is still known as the three-napkin protocol
- there are other protocols, but BGP has the broadest support
- Question: How can we censor/block on this layer?



DNS - The Domain Name System

- Like a Phonebook: cccsbg.at has IPv4 -> 185.69.163.164
- We don't want to remember IP addresses, not even IPv4.
- Many different records (MX=mailserver, A=IPv4, AAAA=IPv6, TXT=can be used for anything, ...)
- Resolver, Authoritative Nameservers, Root Nameserver
- censoring/blocking happens mostly here
- Use better DNS providers or build your own
- Provider suggestion: Quad9 - 9.9.9.9
- Selfhosting suggestion: pihole (censor DNS for your own good)

Lets play a game...

What is **FOSS**?
Why should we support it?
And why does it matter?

Free and Open Source Software

Who/What is the GNU Project?

- GNU is not Unix
- Announced and started in 1983 by Richard Matthew Stallman (RMS).
- GNU grants rights with licenses (A)GPL.
- Copyleft

Who/What is FSF?

- Free Software Foundation
- Founded 1985 by RMS.
- FSF approved licenses.
- FSFE (Free Software Foundation Europe) founded in 2001.

- The freedom to run the program as you wish, for any purpose (freedom 0).
- The freedom to study how the program works, and change it so it does your computing as you wish (freedom 1). Access to the source code is a precondition for this.
- The freedom to redistribute copies so you can help others (freedom 2).
- The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

- Started through 1970 as a product of the 1970s.
- RMS formally founded the movement in 1983 by launching the GNU Project.
- To understand the concept, you should think of “free” as in “free speech,” not as in “free beer.”

- The term Open-Source was coined in the late 1990s.
- Software is just software. There are no ethics associated directly with it.

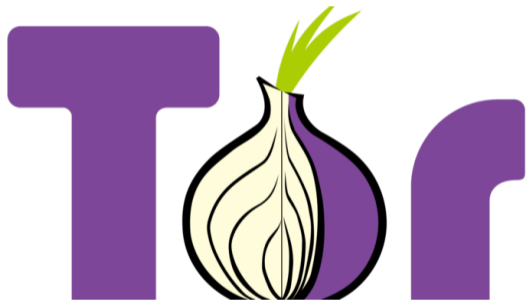
are there alternatives (FOSS)

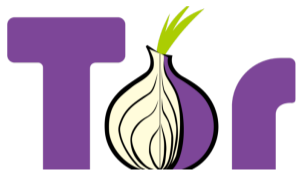
- tl;dr: yes
- within the Internet:
 - companies that do not sell my data, and promise not to analyze the content, that's a matter of trust!
 - encryption
- outside of the Internet:
 - increasingly complicated, POTS, Fax use the Internet as a bottom layer
 - WalkieTalkie, amateur radio,
 - software like briar with lowering one's sights
 - carrier pigeons and other analogous alternatives
 - what else ...

- applications used everyday, alternatives and so on ...

Android, Apache web server, Audacity, Blender, Firefox, GIMP, GNU/Linux, GNU Compiler Collection, Inkspace, Krita, LibreOffice, Python, VLC

surfing (almost) anonymously through the internet





- surf anonymously, conceals the location of your device against the webserver
- anonymizing overlay network, all network traffic is encrypted and sent via the tor network,
- classical accessmethod for the “dark web” with the tor-browser
- offers hidden services



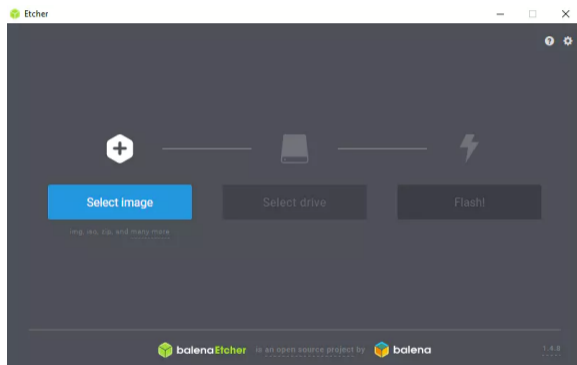
- complete OS, with office suite, webbrowser, connects only through tor to the internet,
- runs from a stick, no installation on the device, after shutdown: everything is forgotten (you can configure a persistent encrypted area on the stick, restricted apps)
- ideal for investigative journalists, dissidents, people in countries with repression, circumvents censorship
- read the manual, read opsec handbooks, nothing is 100% bulletproof/waterproof if not used in a proper way

surfing (almost) anonymously through the internet



<https://tails.net/install/windows/index.en.html>

surfing (almost) anonymously through the internet

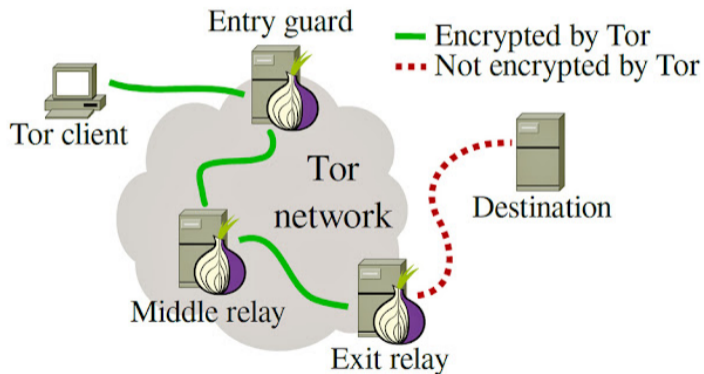


<https://etcher.balena.io/>

a system that doesn't rely on the internet



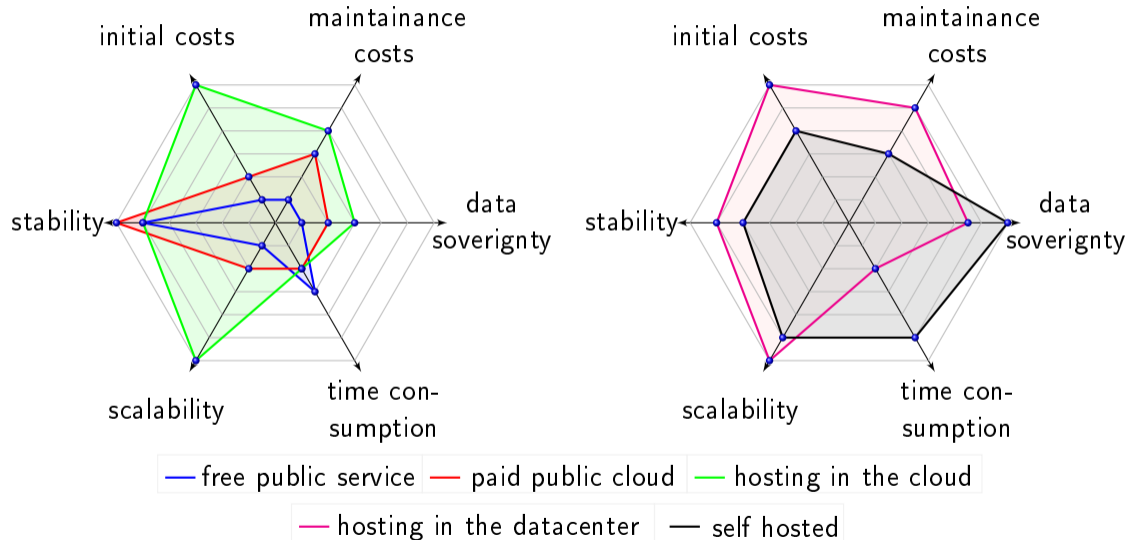
enough time for the achitecture of the tor network?



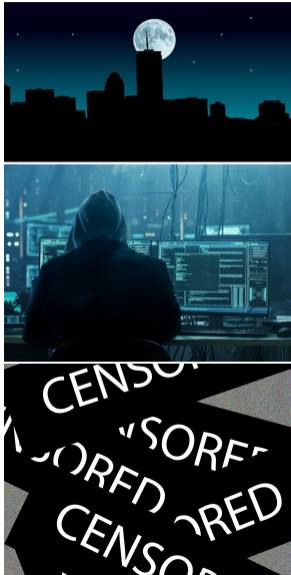


- download `https://tails.net/`
- burn to stick
- start and configure the persistent storage

comparison: cloud, datacenter, self hosted



[click here for the timer ...](#)



- blackout/power outage
- censorship/false information
- failure/service disruption
- targeted hacker attack

Create a 5 minute presentation about your topic ...

summary and the core thoughts you could take home with you

- you need time, read articles, talk with others
- fuel awareness, join groups like ours
- depends on your needs, depends on your situation
- it doesn't work without preparation, know your tools
- compare it to fill the pantry, compare it to K-tests, bluelightorganizations
- the less infrastrucure you can rely on, the more complicated it will end up
- it's not a once in a lifetime event, it's a process
- it's more complicated than filling the pantry

thanks for the attention



still questions?

- ✉ 42@cccsbg.at
- ✉ Ulrike-Gschwandtner-Straße 5, 5020 Salzburg



every Friday evening, from approximately 6:00 p.m.



- [1] V. des CCC Salzburg, “Vereinsstatuten”, (Oct. 2010), [Online]. Available: <https://cccsbg.at/about/statuten.pdf>.