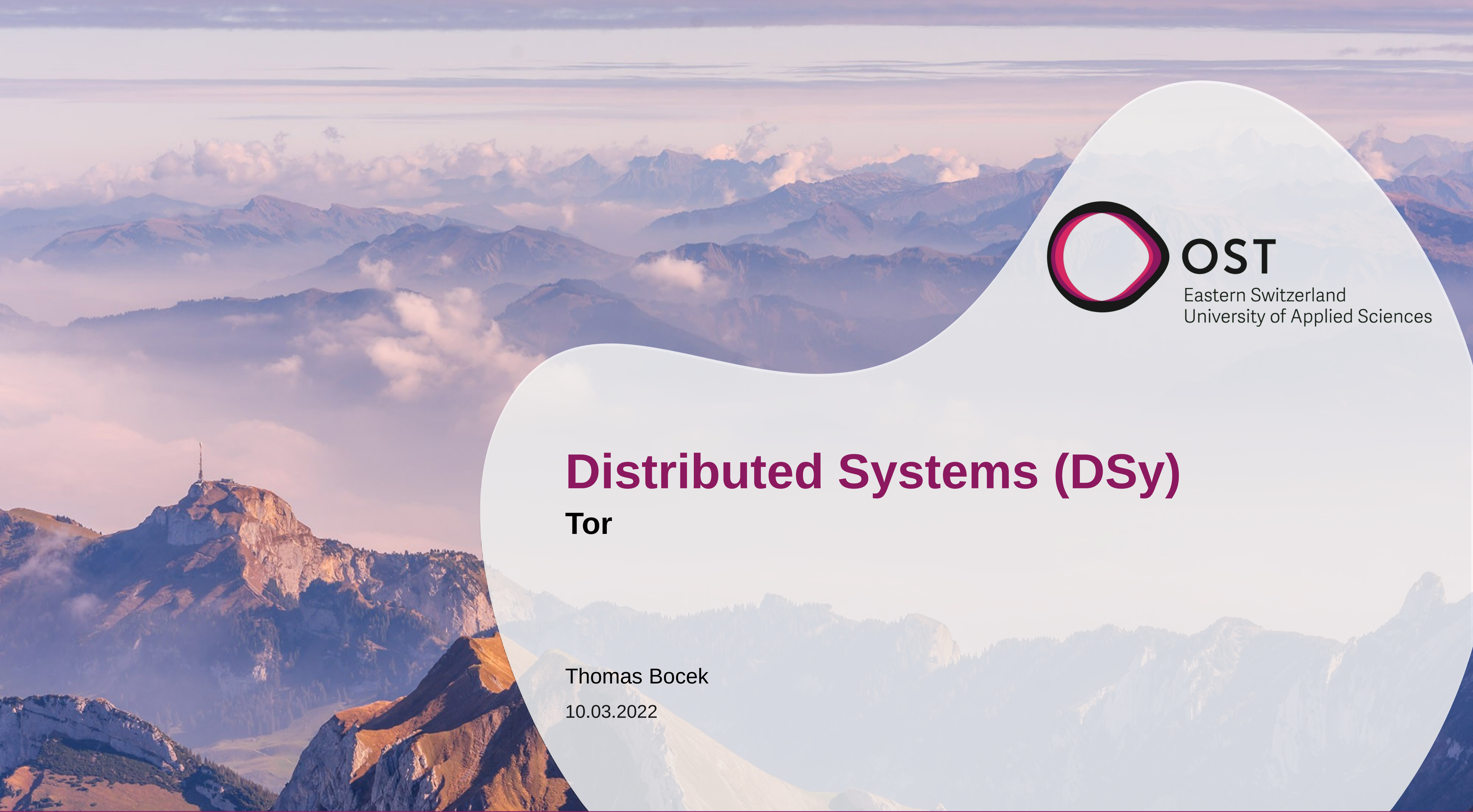


OST
Eastern Switzerland
University of Applied Sciences

Distributed Systems (DSy)

Tor

Thomas Bocek

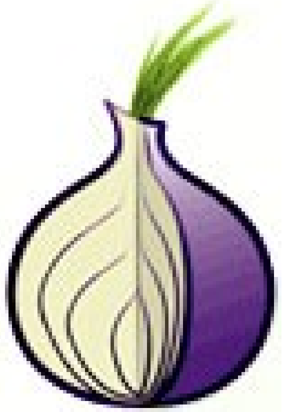
10.03.2022

Learning Goals

- Lecture 3
  - What is Tor?
  - How does it work?
  - Why do we need onion/hidden services?
  - How to setup an onion service?

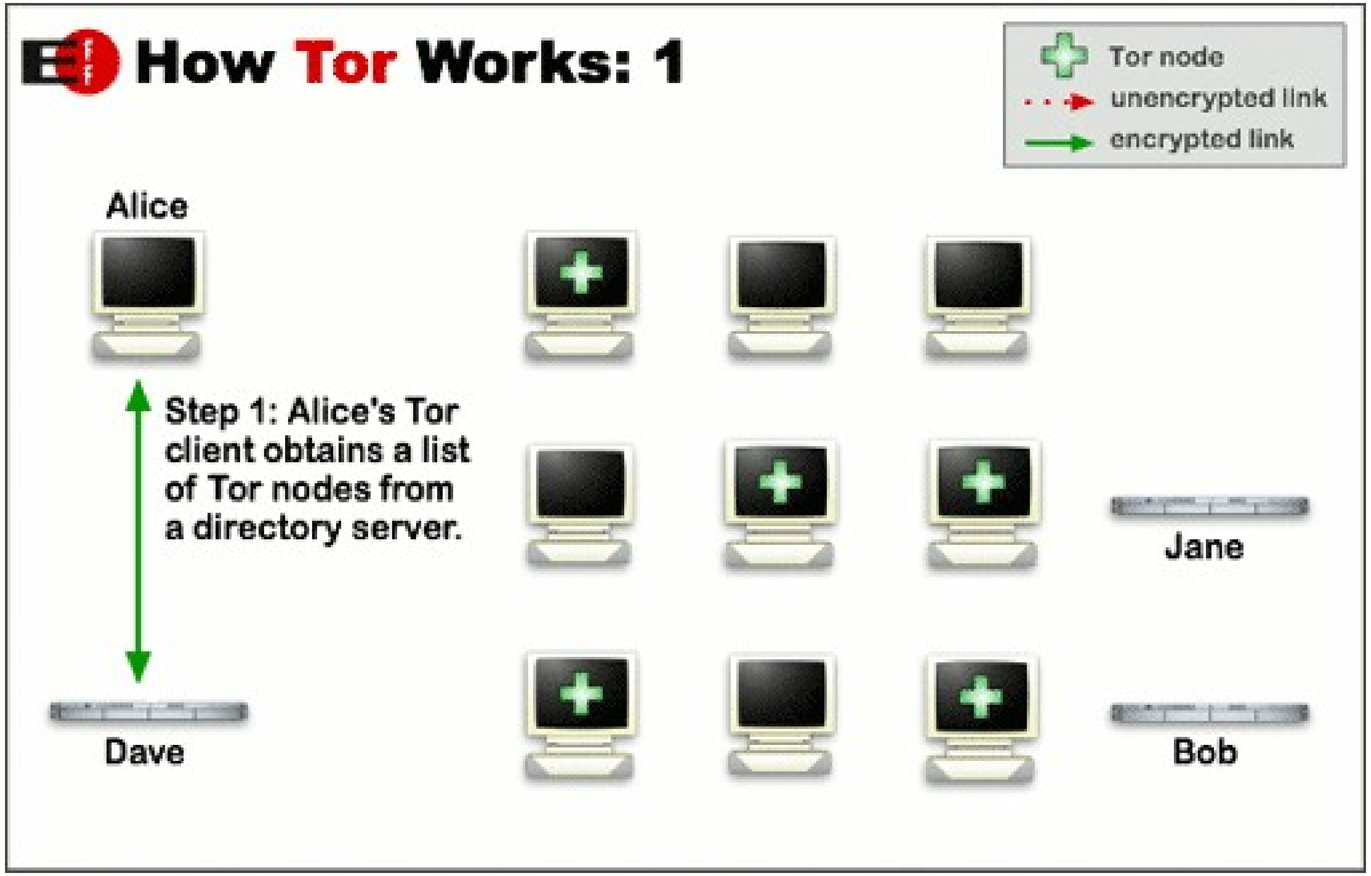
Tor - The Onion Router

- The Onion Router - overview
- Started ~1995 by U.S. Naval Research Laboratory
  - Protect US intelligence communication
  - Naval Research Laboratory released the code under free license in 2004
  - EFF began funding development
- Anonymous internet communication system
  - SSL / TLS is not enough
  - Protect privacy of users
- Encrypts all messages (also header, IP)
- Sends data through virtual circuit (3 random relays)
  - Guard/relay/exit relay (bridge)
  - Use SOCKS proxy to connect via Tor, TCP only
  - Example Tor Browser accessing https://dsl.i.ost.



Tor

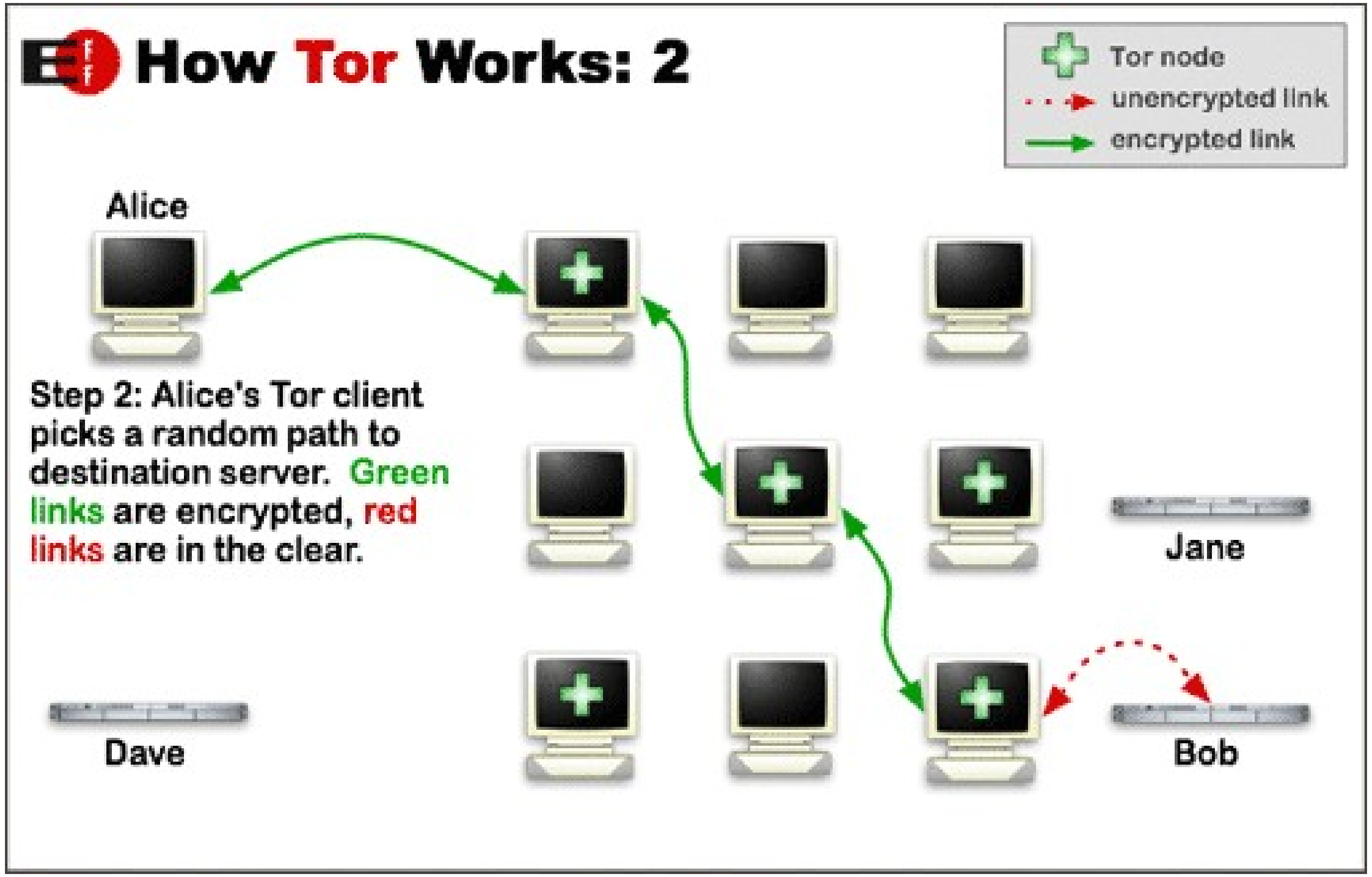
- How it works



Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.

Tor

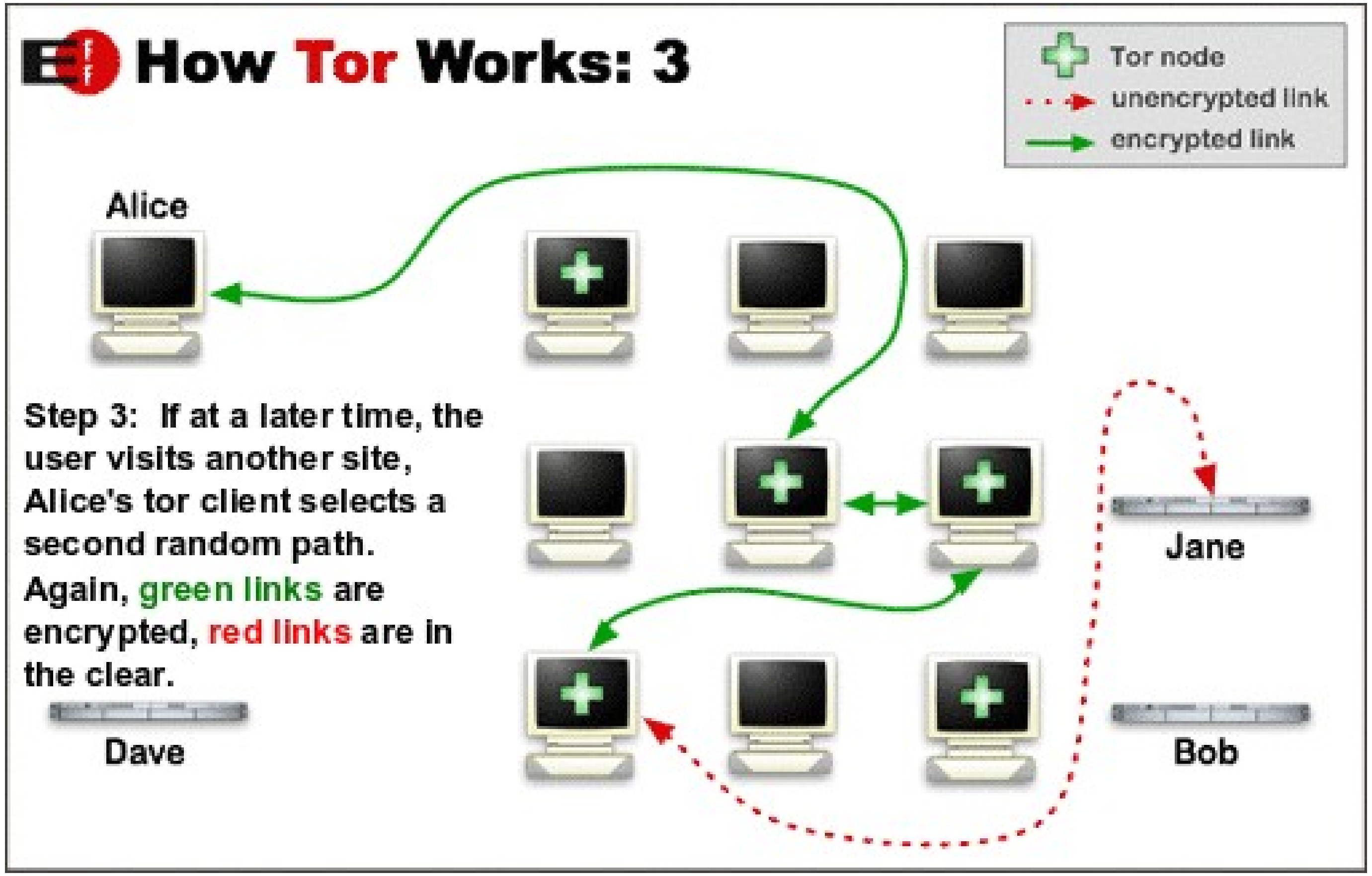
- Alice to Bob



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

Tor

- Alice to Jane



Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Tor

- Tor in Russia
  - 8.12.2021: Russia Blocks Privacy Service Tor, Ratcheting up Internet Control [link]
  - “300,000 users in Russia, or 14% of all daily users, second only to the United States”
  - But: 6.3.2022: Ukraine latest: BBC World Service pulled off air in Russia amid Putin media crackdown [link]
    - “Both its Ukrainian and Russian language services are available on the dark web through the Tor network”

- Onion (Hidden) services:
  - Servers configured to receive connections only through Tor
  - Why hidden services at all? 08.03.2022 [link]
- Main use-case: journalists, whistleblowers, and dissidents
  - Can be used against price discrimination

- Tor exit node can see traffic if not using hidden services! – Use SSL/TLS
  - Services block Tor exit nodes, e.g., example: Wikipedia
  - Tor exit node operator facing copyright claims - template

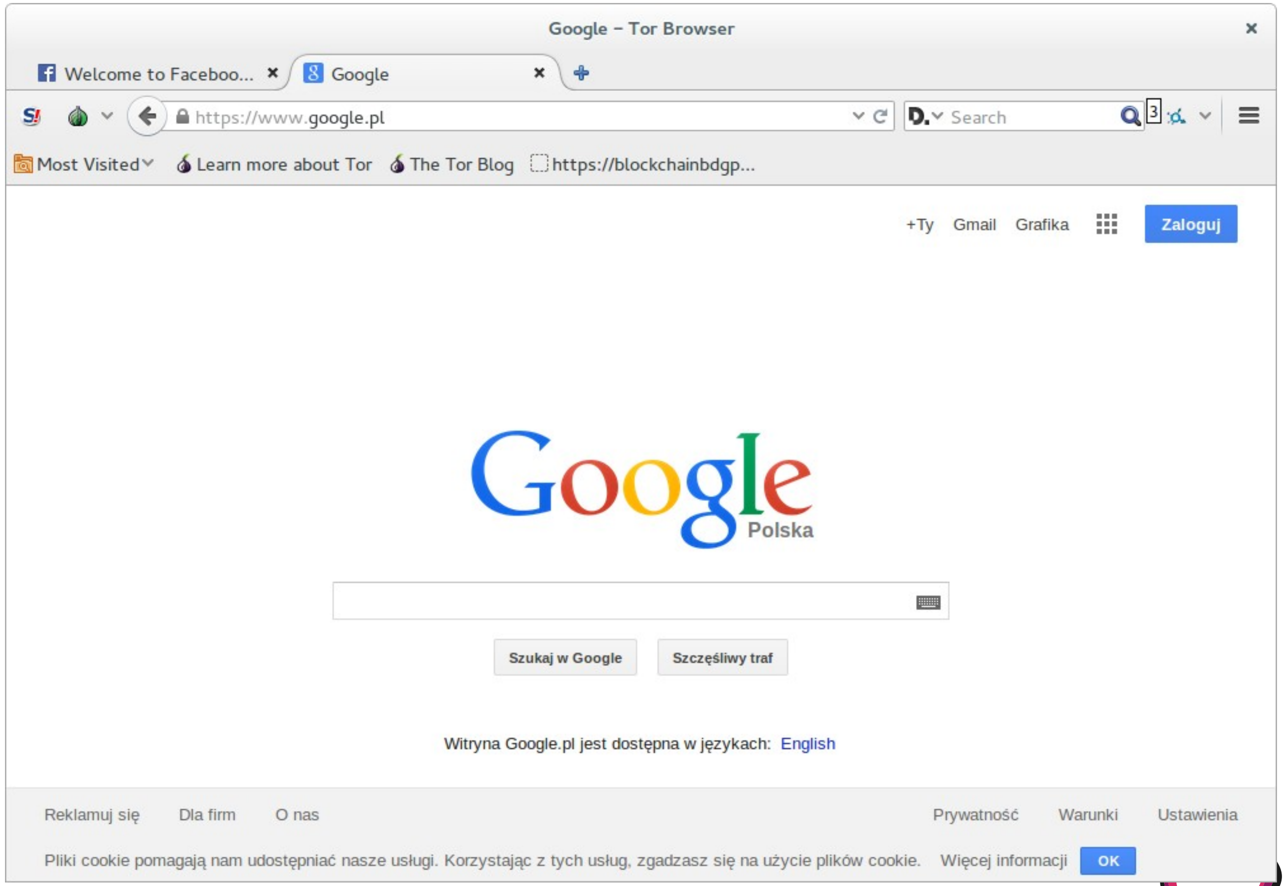
Tor – Onion (Hidden) Services

- Onion Services - mechanisms
- End-to-end authentication
  - content can only come from that particular onion
- End-to-end encryption
  - Onion traffic is encrypted from the client to the onion host. HTTPS for free

- Running your server via Tor hidden services [howto]
  - http://qszjvkizpbwfo7lsw23awbm5atzndglixjcv3ozk3zdbgg3p57dayjqd.onion:8080/

Tor

- Don't provide your name or other revealing information in web forms
- Data is only encrypted within Tor – if no HTTPS is used, it still can be read
- Language may be different



Witryna Google.pl jest dostępna w językach: English

Pliki cookie pomagają nam udostępniać nasze usługi. Korzystając z tych usług, zgadzasz się na użycie plików cookie.

- Bomb threats at Harvard
  - FBI found that Tor was used – check who was using Tor in the Harvard network → 2 days later student was caught