

# Privatsphäre und Anonymität

Severin Fürbringer

26.01.2018

## Einleitung

### Lizenz



- Dokumente stehen unter CC-BY-SA 4.0:
- URL [github.com/fuerbringer/efz-va](https://github.com/fuerbringer/efz-va) für mehr Infos.

### Kurzüberblick

**Die schriftliche Arbeit zusammengefasst:**

#### Fragen

- 0) Wie gut behandeln bekannte Internetdienste die Privatsphäre?
- 1) Bis zu welchem Grad ist die Anonymität möglich?
- 2) Sind Darknets besser für privates und anonymes surfen geeignet?

### Kurzüberblick

**Die schriftliche Arbeit zusammengefasst:**

#### Umfrage

- 1) Wie oft werden Anonymitätsnetzwerke eingesetzt?

## Kurzüberblick

Die schriftliche Arbeit zusammengefasst:

### Auswertung

- In der Auswertungen wurden ausserdem verschiedene alternative Applikationen angeschaut:
- 0) GNU Ring und Tox-chat (Alternativen zu *WhatsApp*)
  - 1) Searx und YaCy (Alternativen zu *Google*)
  - 2) Tor (Alternative zum normalen *TCP/IP-Routing*)

## Highlight

### Tor und weitere Anonymitätsnetzwerke

- **Was:** Im Rahmen dieser Präsentation wird **Tor** kurz erklärt und auf I2P näher eingegangen.
- **Wieso:** Aufgrund der begrenzten Seiten (im VA-Reglement) konnte ich I2P leider nicht behandeln.

## Persönlicher Bezug

Wieso ist mir das Thema weiterhin wichtig?

- Starker Bezug zur freien- und Open-Source-Software.
- Der Informationsfluss darf nicht einem Monopol unterstehen.



## I2P - The Invisible Internet Project

### Ziel

Ziel dieser Präsentation

0. Funktionsweise von I2P
1. Vor- und Nachteile von I2P
2. Unterschied und Vergleich zum normalen Internet
3. Eignung und Use-Cases für I2P

## Anonymisierungsnetzwerke

### Was ist ein Anonymisierungsnetzwerk

- Informationenbeschaffung durch alternative Wege basierend auf der Internet Infrastruktur.
- Zugriffe auf Informationen erfolgen meist über mehrere Knoten (Nodes).
- Bei Tor wird ein Zugriff über 3 “Schalen” nacheinander entschlüsselt.

### Anonymisierungsnetzwerk Visualisiert: Schritt 1

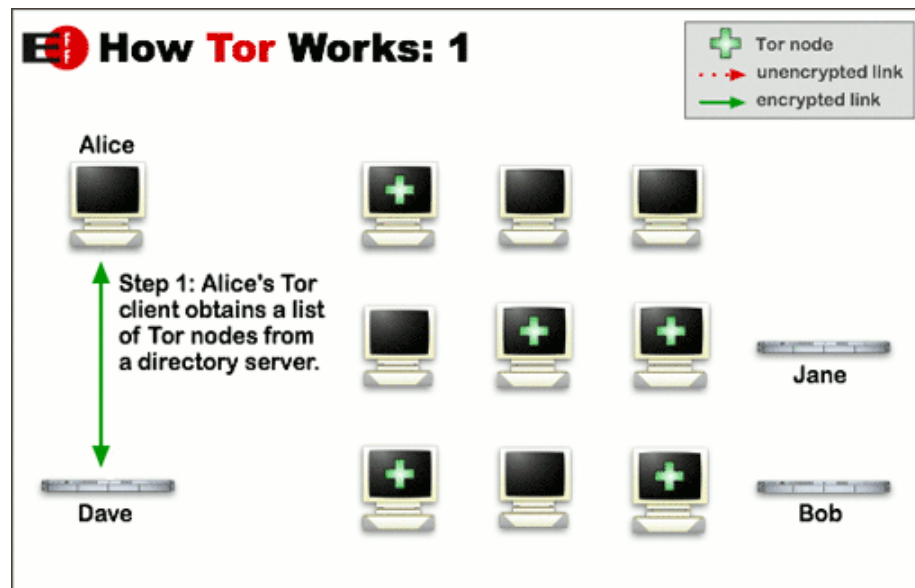


Figure 1: tor1

### Anonymisierungsnetzwerk Visualisiert: Schritt 2

### Anonymisierungsnetzwerk Visualisiert: Schritt 3

## I2P

### Wie unterscheidet sich I2P zu Tor?

0. Garlic Routing anstatt Tor's Onion Routing.
1. Das Netzwerk ist weitaus dezentralisierter.

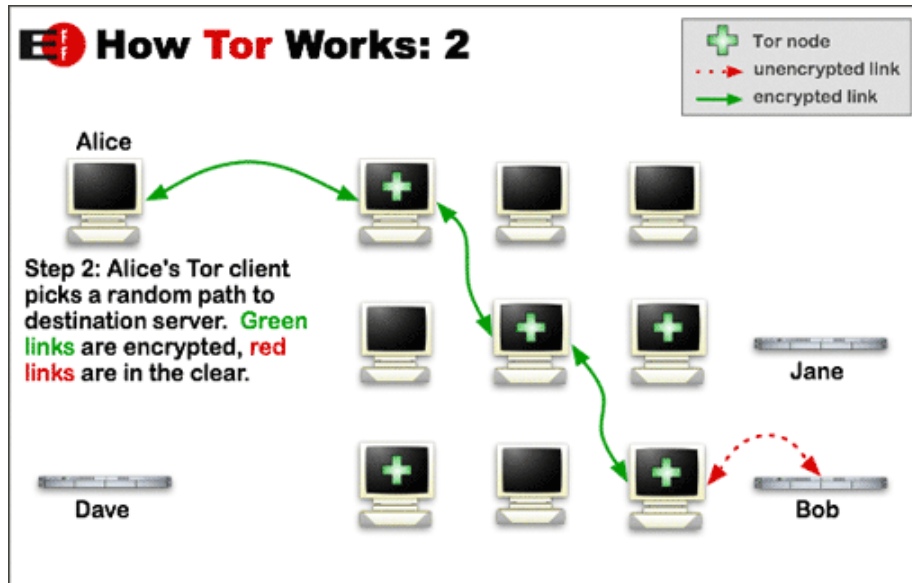


Figure 2: tor2

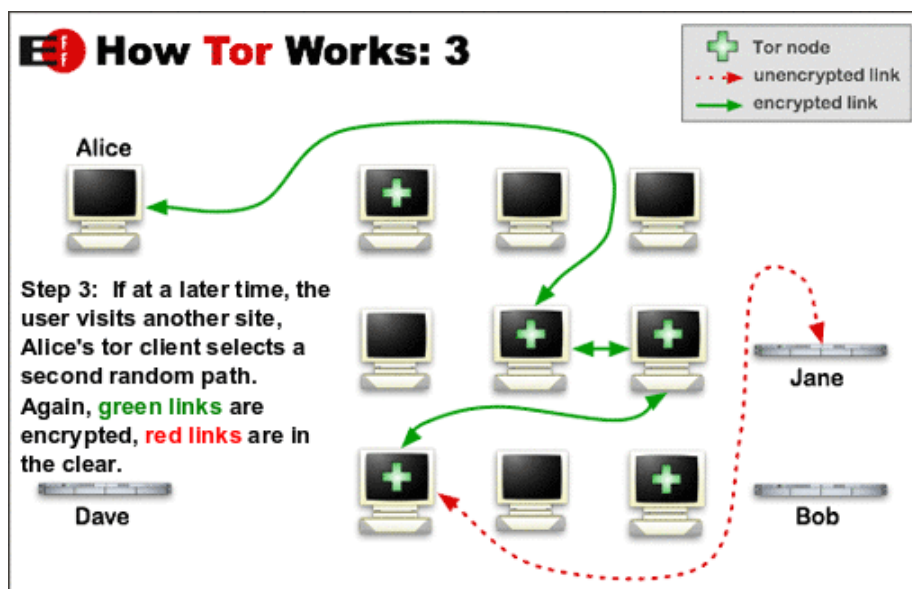


Figure 3: tor2

## I2P Visualisiert

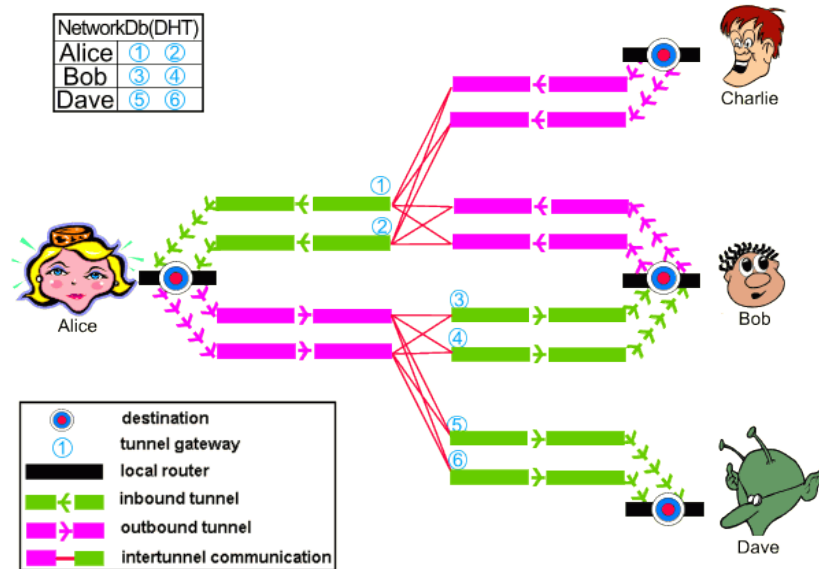


Figure 4: i2p

## I2P Demo

- I2P Router Console

## Wrapup

### Zusammenfassung I2P

#### (+) Pro

1. Hohe dezentralisierung führt zu Anonymität
2. Anonymer als Tor
3. Alle wichtigen Services bereits integriert (Mail, Torrent, IRC)

### **(-) Kontra**

1. Konzipiert für langlebige Tunnel
2. Kaum kompatibel mit dem Surfaceweb (+1 für Tor)
3. Java ;\_;

### **Zusammenfassung I2P**

- Eignet sich für Communities, deren erste Priorität die Anonymität ist.

### **Rückblick VA**

asd