Privatsphäre und Anonymität

“Wie man im Internet seine Spuren verwischt”

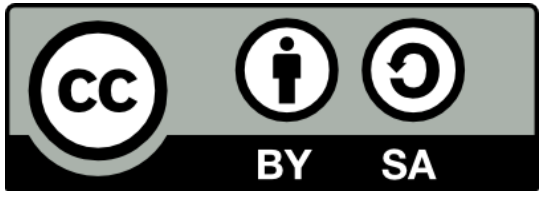
Severin Fürbringer

26.01.2018

Einleitung

Lizenz

- Dokumente stehen unter CC-BY-SA 4.0:



- URL `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

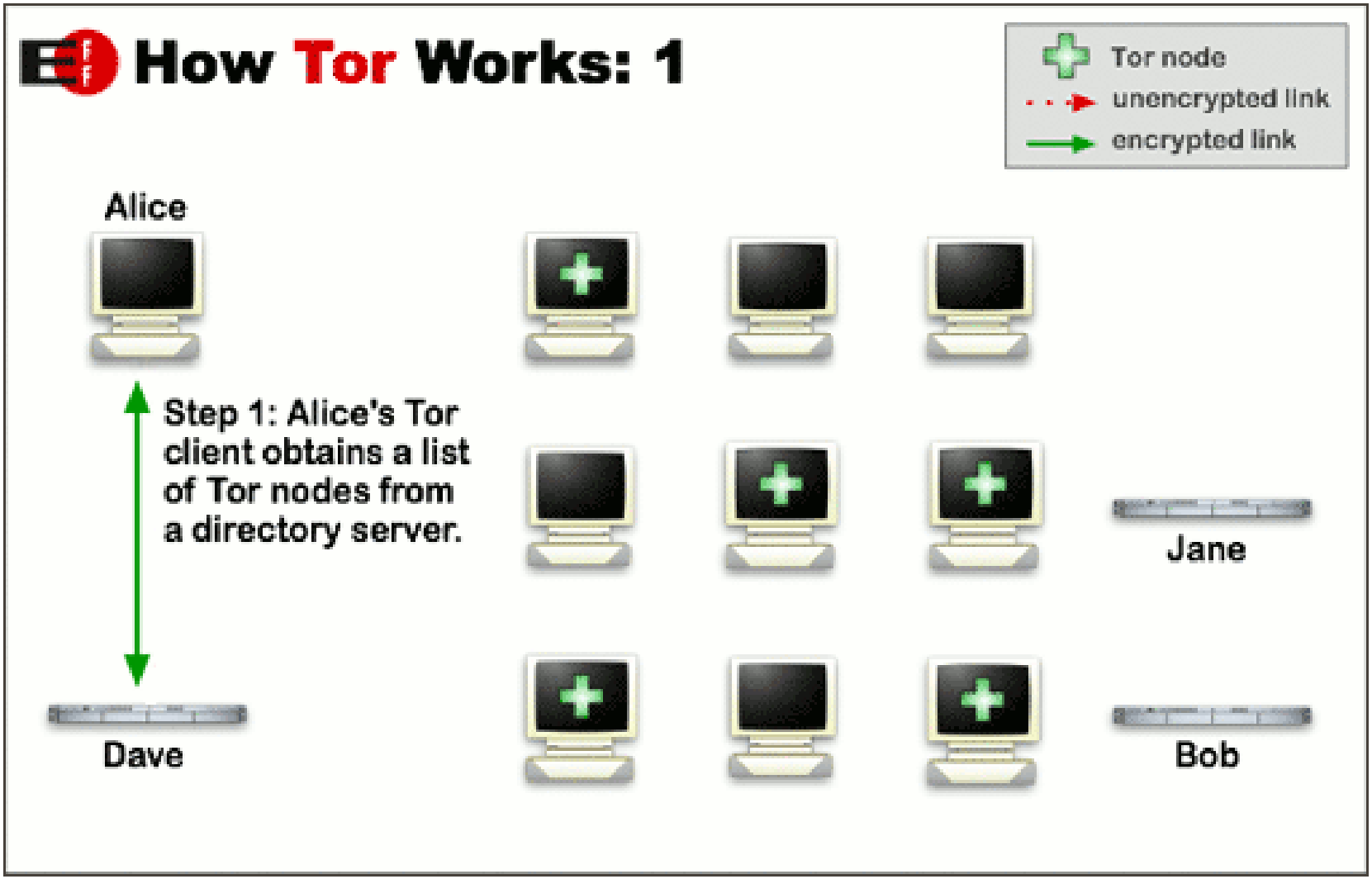
0. Funktionsweise von I2P
1. Vor- und Nachteile von I2P
2. Unterschied und Vergleich zum normalen Internet
3. Eignung und Use-Cases für I2P

Anonymisierungsnetzwerke

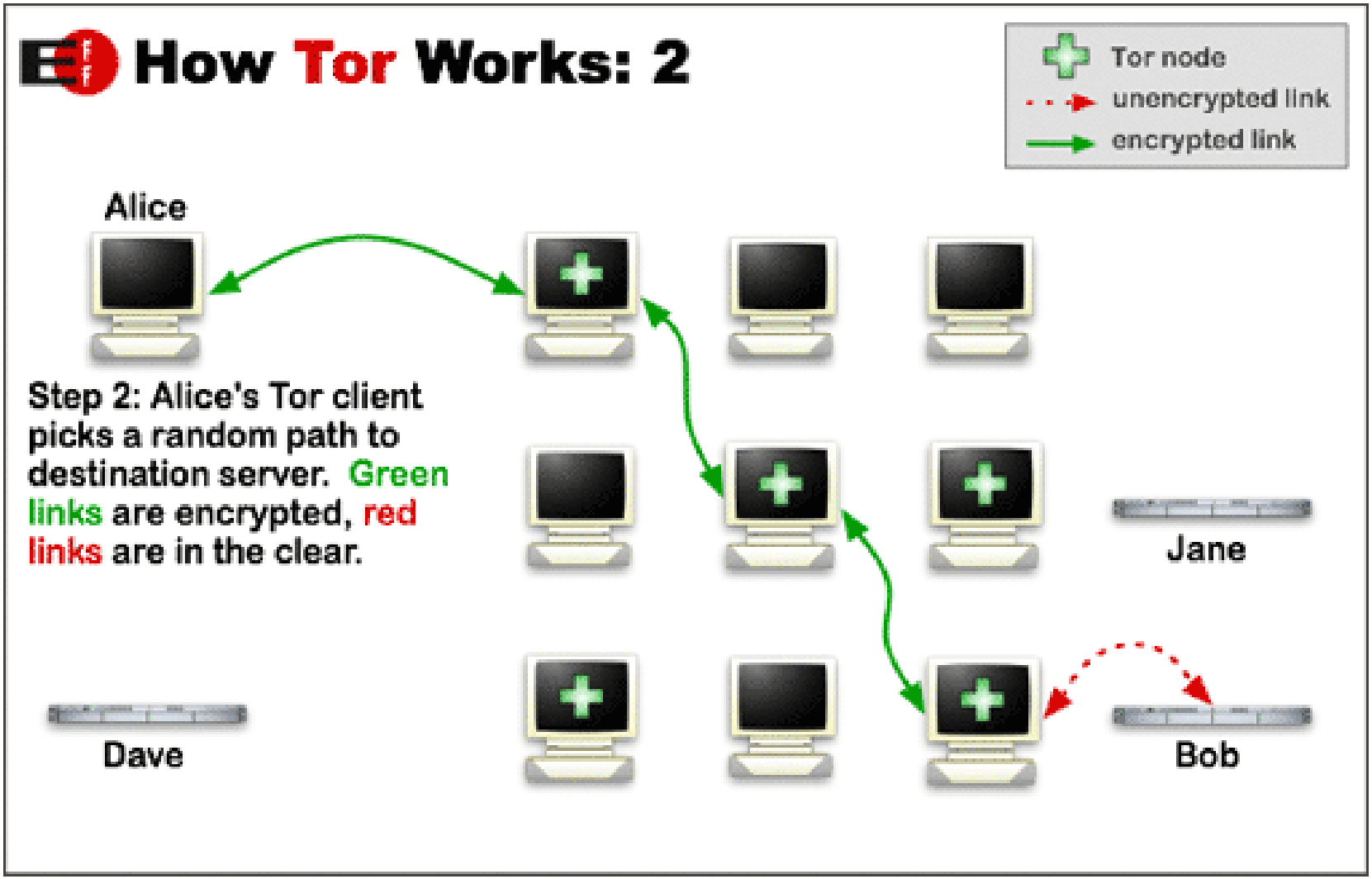
Was ist ein Anonymisierungsnetzwerk

- 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.

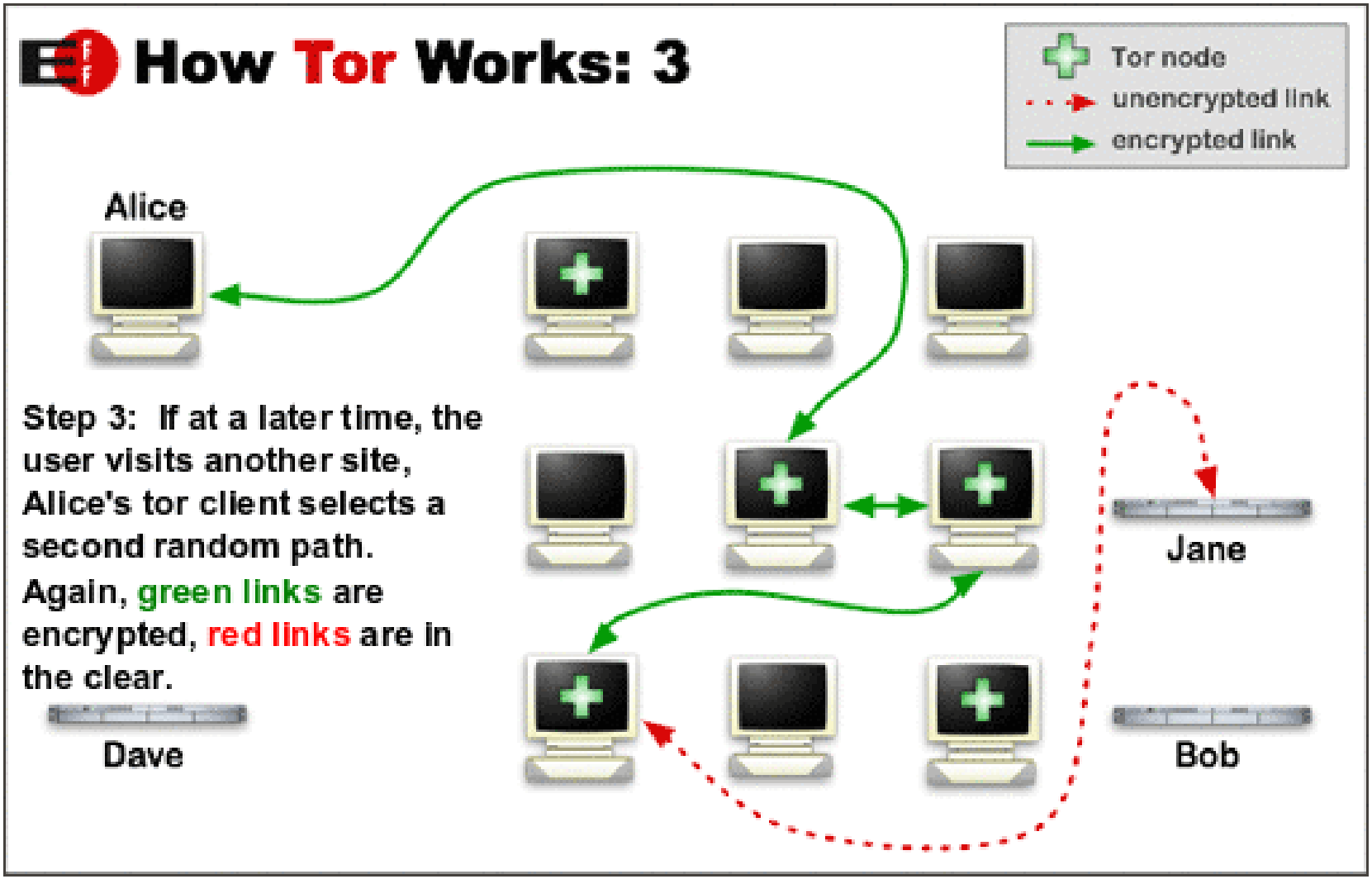
Anonymisierungsnetzwerk Visualisiert: Shritt 1



Anonymisierungsnetzwerk Visualisiert: Shritt 2



Anonymisierungsnetzwerk Visualisiert: Shritt 3

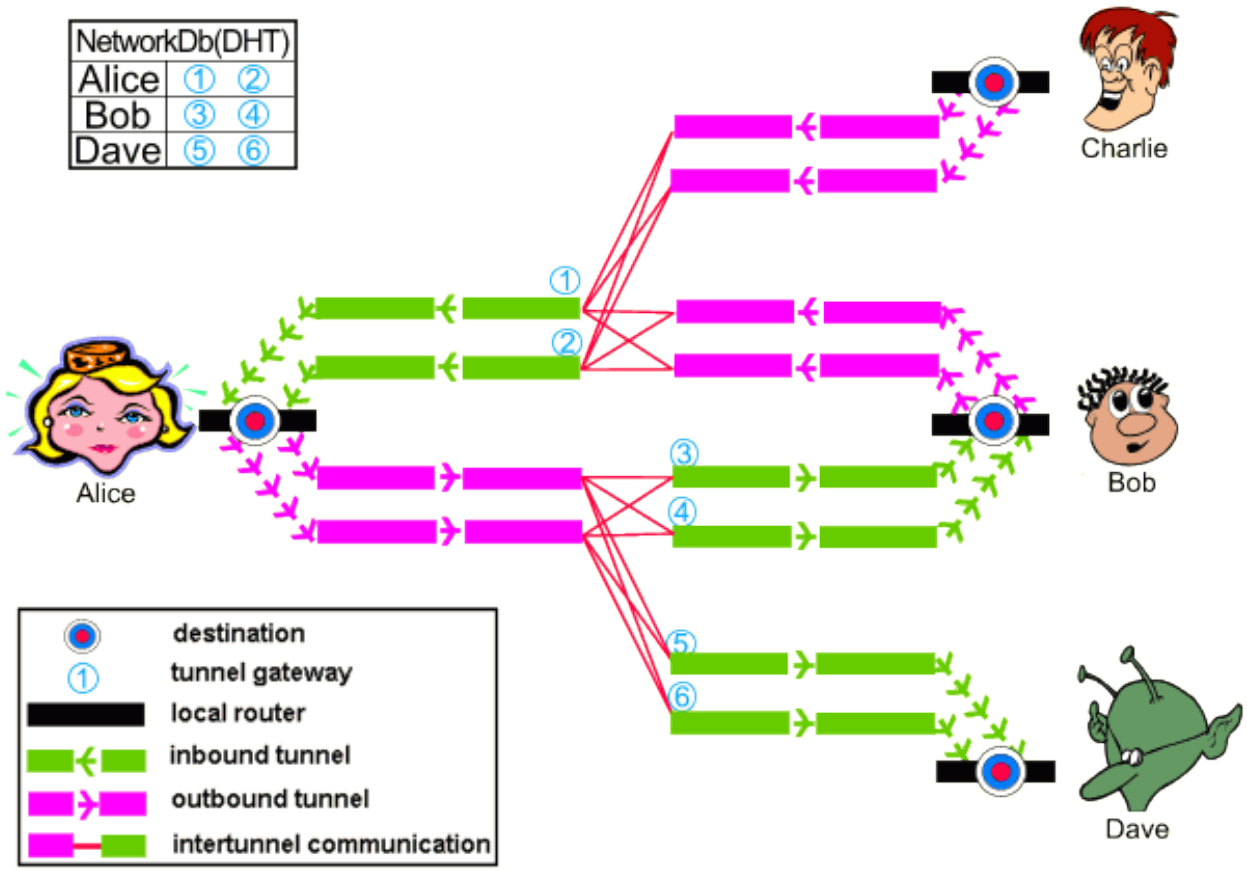


I2P

Wie unterscheidet sich I2P zu Tor?

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

I2P Visualisiert



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

Vorgehen

- “Fahrplan” mit Themen bei der VA und PP.
- Zeitplan gemacht und sogar zu 50% eingehalten.

Rückblick VA

Was ging gut?

- Durch Vorwissen entstand viel Inhalt
- Neue Technologien gefunden

Rückblick VA

Was machte mir Mühe?

- Limits einhalten
- Zeitplan einhalten
- Roten Faden nicht verlieren

Rückblick VA

Selbstbeurteilung

- Guter Überblick über die digitalen Anonymisierungsmöglichkeiten
- Teilweise unnötige Informationen

Rückblick VA

Was ich in Zukunft besser machen werde

- Arbeit klar abgrenzen. Und somit die Vorgabe nicht ums 4-fache zu überschreiten.