Tor Update

Schneeflocken, Rost + mehr

Ben + Christoph

FraLUG Mai 2024

Übersicht

- Pluggable Transports
- Snowflake
- Changelog / Arti
- Roadmap
- Urbane Mythen

Pluggable Transports

Tor-Traffic wird manchmal von Internetprovidern, Regierungen oder anderen Zensoren erkannt und blockiert. Pluggable Transports:

- Transformieren des Tor-Traffic
- Datenfluss soll nicht mehr als Tor-Traffic erkennbar sein

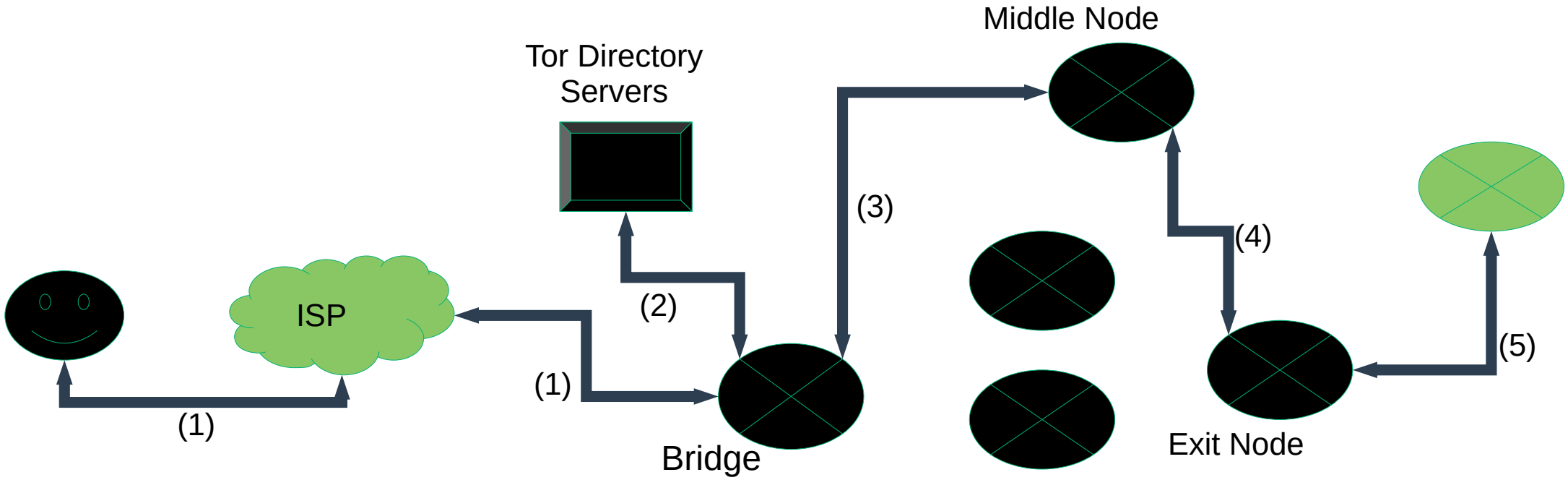
obfs4	obfs4 makes Tor traffic look random, and also prevents censors from finding bridges by Internet scanning. obfs4 bridges are less likely to be blocked than its predecessors, obfs3 bridges.
meek	meek transports make it look like you are browsing a major web site instead of using Tor. meek-azure makes it look like you are using a Microsoft web site.
Snowflake	Snowflake routes your connection through volunteer-operated proxies to make it look like you're placing a video call instead of using Tor.
WebTunnel	WebTunnel masks your Tor connection, making it appear as if you're accessing a website via HTTPS.

- https://blog.torproject.org/tor-heart-bridges-and-pluggable-transports/
- https://gitlab.torproject.org/tpo/anti-censorship/pluggable-transports
- https://tb-manual.torproject.org/circumvention/
- https://spec.torproject.org/pt-spec/

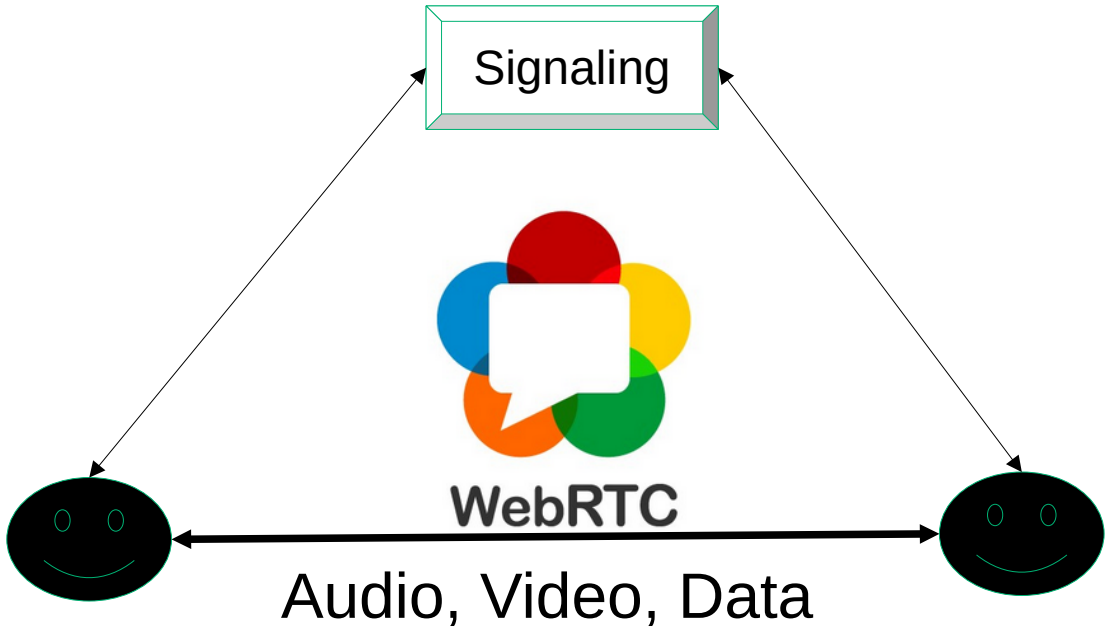
Bridge obfs4 - Beispiel

Zugang mittels Bridge ins Tor Netzwerk und raus zu Clearnet

(1) Verbindung zur Bridge
(2) Über Bridge zu Tor Directory Servers
(3) Zum nächsten Knoten
(4) Zum nächsten Knoten
(5) Tor Netzwerk verlassen



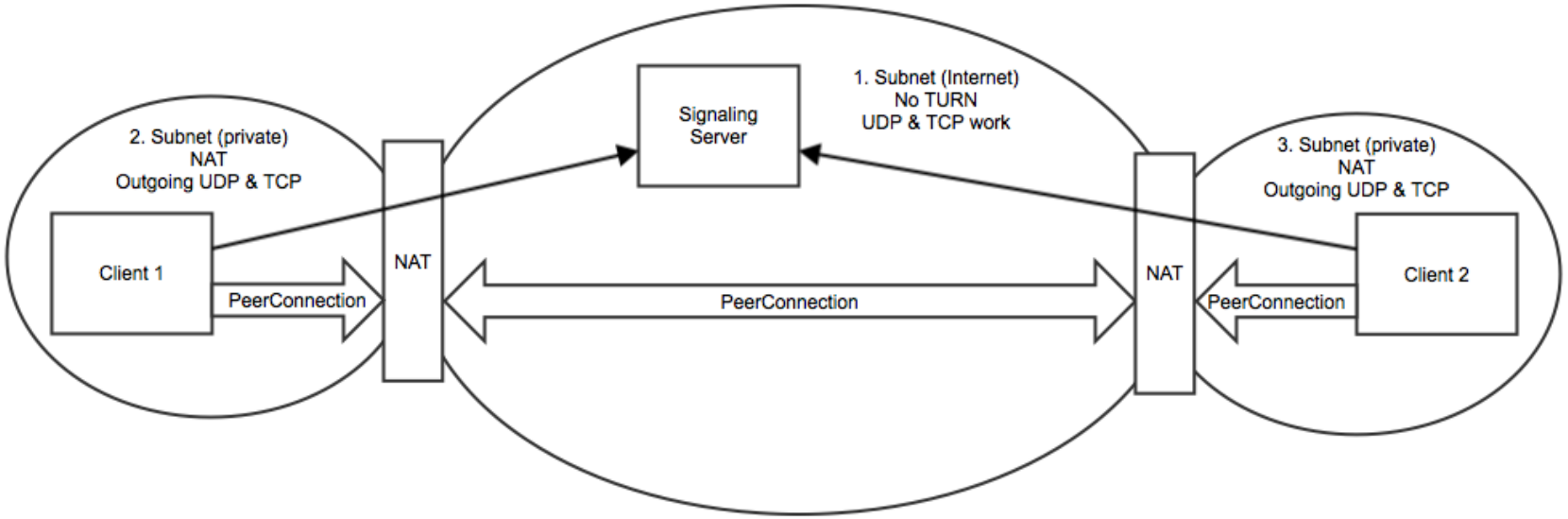
WebRTC



- Offener Standard
- Echtzeitkommunikation von Browser zu Browser
- Video, Chat, Dateitransfer, Desktopsharing, etc.
- Unterschiedliche technische Umsetzungen

- https://webrtc.org/getting-started/peer-connections
- https://de.wikipedia.org/wiki/WebRTC
- https://wiki.mozilla.org/Media/WebRTC

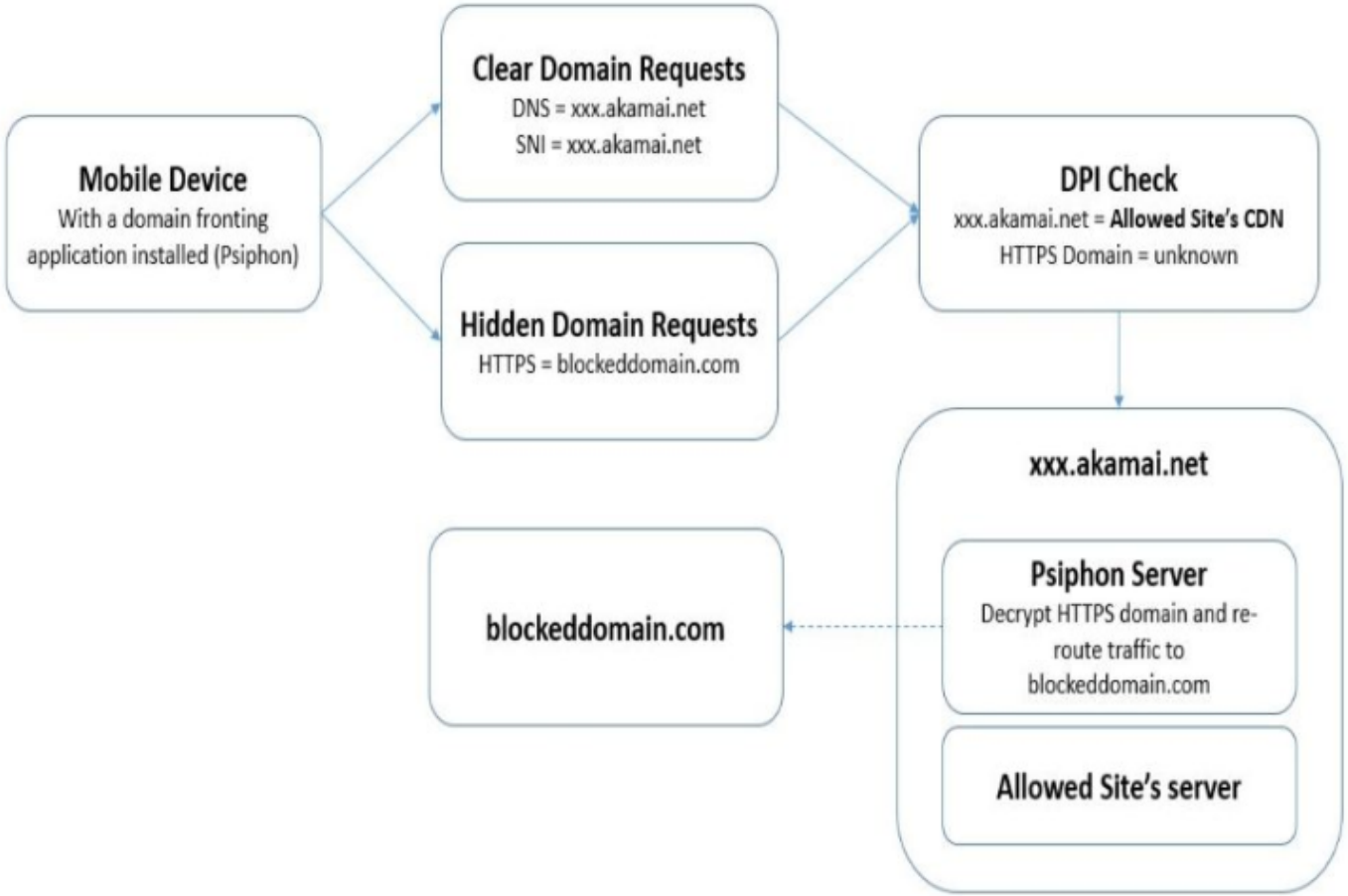
WebRTC



- Je nach Szenario werden unterschiedliche Verbindungsaufbautypen eingesetzt (ICE, STUN/TURN)
- Geeignet um Peers hinter NAT zu verbinden

- Picture above: https://wiki.mozilla.org/WebRTC/Test_Networks
- https://webrtc.org/getting-started/peer-connections
- https://de.wikipedia.org/wiki/WebRTC
- https://gitlab.torproject.org/tpo/anti-censorship/pluggable-transports/snowflake/-/wikis/NAT-matching

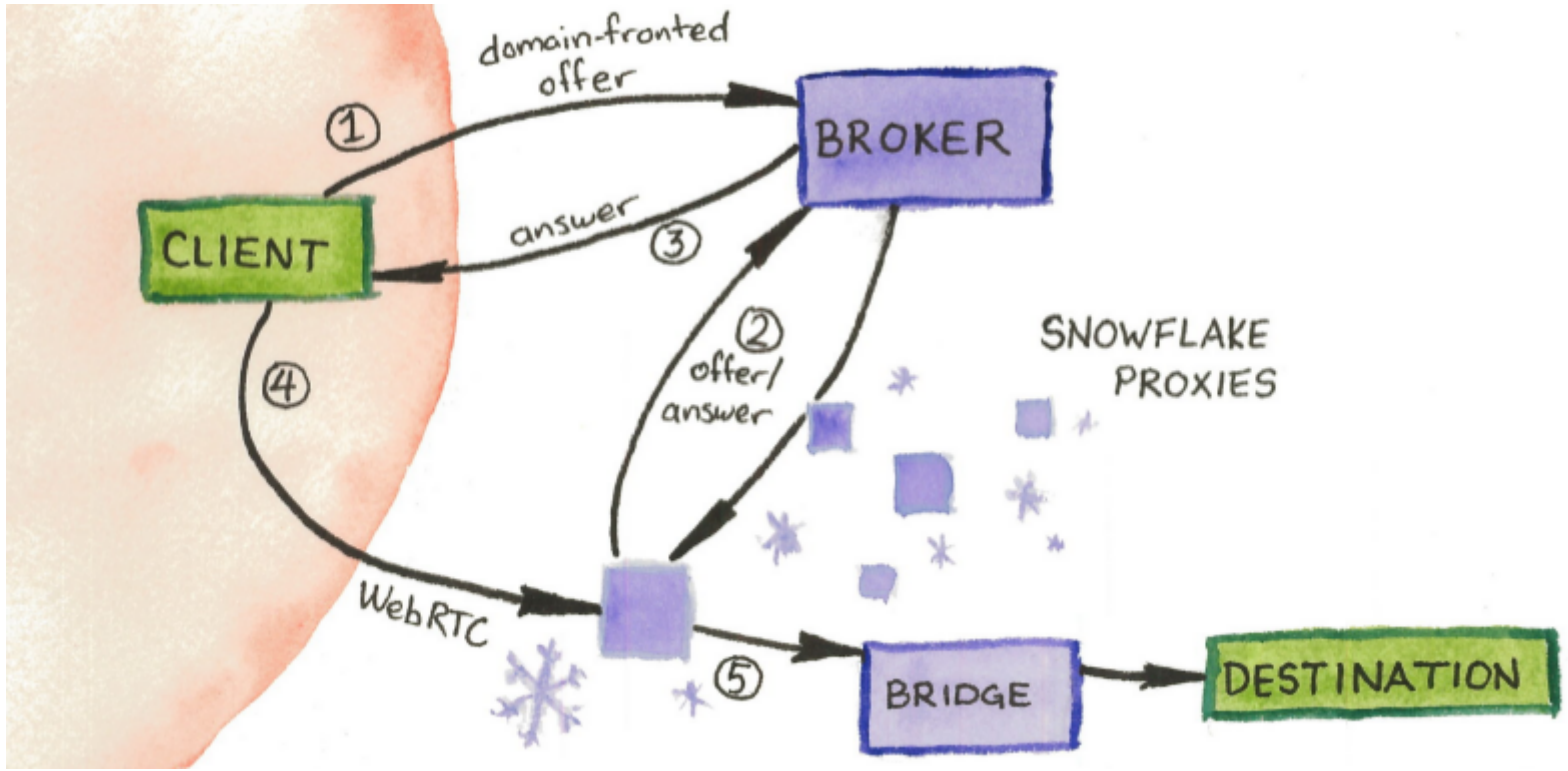
Domain Fronting



- Wird nicht nur für/von Tor genutzt
- Kann Zuordnung von tatsächlicher Verbindung hinter erlaubter Domain verhindern
- Unterschiedliche use-cases

- Picture above: https://andreafortuna.org/2018/05/07/domain-fronting-in-a-nutshell/
- https://blog.torproject.org/domain-fronting-critical-open-web/
- https://de.wikipedia.org/wiki/Domain_Fronting

Snowflake - Konzept



- Picture above: https://snowflake.torproject.org/
- https://gitlab.torproject.org/tpo/anti-censorship/pluggable-transports/snowflake
- https://gitlab.torproject.org/tpo/anti-censorship/pluggable-transports/snowflake/-/wikis/home
- https://support.torproject.org/glossary/domain-fronting/
- https://gitlab.torproject.org/tpo/anti-censorship/pluggable-transports/snowflake/-/wikis/NAT-matching

- Sehr einfach ein Snowflake Proxy zu sein(z.B. mit Browser Plugin)
- Nutzt Domain Fronting
- Domain Fronting nur als Rendevouz
- Snowflake ist Peer-to-Peer Proxy als Durchgang zu Tor (Datentransfer)

Snowflake - Verwendung

- Snowflake kann helfen mehr Menschen einzubinden
- Snowflake ist eine zusätzliche, starke Methode

  → Snowflake WebRTC Addon im Browser (Für alle umsetzbar)

  → Snowflake auch als Serverbetrieb (Host oder Docker)

- Ersetzt obfs4/WebTunnel Bridges nicht
- Je nach NAT Typ können Verbindungen nicht zustande kommen
  (kein Peer-to-Peer möglich)

Wie auch immer: Nutzen und mitmachen!

Changelog

- Proof of Work für Onion Services:
  - Motivation: Schutz vor (D)DoS-Angriffen
  - Proof of Work: Crypto-Mining, etc.
  - Dynamische Aktivierung basierend auf Traffic-Analyse
  - Ab 0.4.8.10
- Andere Neuerungen:
  - TB => FF ESR
  - Mobile (Orbot, TB)
- Exkurs: The Guardian Project

Arti

- Re-Implementierung der gesamten CB in Rust
- Motivation: technische Schuld der 20 Jahre alten C-CB
- Aktives Projekt seit 2017
- Funding: Zcash / ZOMG
- Feature Parity => Ende 2024
- Status: 1.0 Bootstrapping, SOCKS-Proxy

Urbane Mythen

- Angriffsszenarien:
  - Traffic Analysis (aktiv/passiv)
  - Browser Fingerprinting
  - Theoretische Ansätze

➢ Quintessenz: Tor ist immer noch mit einer sichersten Wege, anonym zu bleiben

F & A

Vielen Dank

Ben + Christoph
benlason at <ignore>space</ignore>disroot<dot></dot>org
monochromec at <ignore>space</ignore>gmail<dot></dot>com

const void* ptr = (void *) 1

FraLUG Tor Vorträge aus den Jahren 2020, 2017

Anonymous & Friends: `https://programm.openrheinruhr.de/current/events/549.de.html`

Tor Projekt: `https://www.torproject.org`

Tor Browser Bundle: `https://www.torproject.org/download`

Snowflake: `https://snowflake.torproject.org`

PoW für Onion Sites: `https://blog.torproject.org/introducing-proof-of-work-defense-for-onion-services`

- Arti: `https://github.com/dgoulet-tor/arti`
- The Guardian Project: `https://guardianproject.info`