I2P – (K)Eine Alternative zu Tor

17. Augsburger Linux-Infotag 2018

21.04.2018

I2P – wasn das?

- Low Latency Relay Netzwerk
- Anonymes Netzwerk
- „Black Box“ Tunnel zwischen Client und Server
- Internes Netzwerk, fast keine OutProxies
- Internationales Entwicklerteam mit ~10 Leuten
- Keine Firma, kein Verein, alles rein privat
- OpenSource
- Start 2003 als Freenet Project Transport

Grundsätze von I2P

- I2P versteckt nicht die Nutzung von I2P
- I2P versteckt die Nutzerspuren in I2P
- User soll sicher mit anderen anonym kommunizieren können
- Vertraue niemanden anderen, nur dir selber
- Selbst regulierendes Netz ohne zentrale Instanzen
- OpenSource
- Möglichst wenig eigene Crypto – Peer & Academic Review nötig

Funktionsweise, Teil 1

- Startup: Seeddatei von fixen Servern (oder alternative Quellen) holen
- Connect zu anderen I2P Peers aus der Seeddatei
- Aufbau lokaler netDB – Statistiken über bekannte I2P Peers
- Inbetriebnahme von lokalen Hidden Services
- Jeder Hidden Service erstellt per Default 2 Ein- & 2 Ausgangstunnel
- Jeder Tunnel hat per Default 3 Hops
- Tunnel werden aus bekannten, fähigen Peers der netDB erstellt
- Clients und Server bauen Hidden Services auf

Funktionsweise, Teil 2

- Nach Tunnelaufbau publizieren eines Leasesets an FloodFillDB
- FloodFillDB: verteilte Datenbank auf ~1000 Peers
- LeaseSet: Information welcher Eingangstunnel zu welchem Hidden Service weiterleitet
- Client fragt FF-DB nach LeaseSet zu einem Hidden Service
- Client sendet Daten an Server, Server antwortet, wenn erfolgreich
- Roundtrip mit 12 Hops:
  - Client => C-Ausgangstunnel => S-Eingangstunnel => Server
  - Client <= C-Eingangstunnel <= S-Ausgangstunnel <= Server

Was kann I2P?

- Basic: Tunnel von Client zum Server
- Tunnel per se TCP, aber auch UDP Transport ist machbar
- Datagrams möglich (einzelne Pakete an diverse Server)
- Da jeder I2P Router ein Relay ist, ausreichend Bandbreite
- Bei 12 Hops: Latenz 0,5-2 sec => Durchsatz im 50 kb/sec Bereich
- Keine Limitierungen seitens der Entwickler, Daten Agnostisch
- Tunnel supporten SOCKS, RAW, CONNECT, HTTP, IRC, STREAMR
- Diverse APIs: BOB,SAMv3,StreamingLib, Native Java

Services

- I2P dev Team stellt wenige Servics bereit, Community mehr
- Webseite, Trac Server, Monotone & Git Server, Forum vom Team
- Email Service mit Gateway in ClearNet
- IRC2p Netzwerk mit 3 linked IRC Servern
- Wiki
- Diverse Foren
- Torrent Tracker, OpenTracker, I2PSnark
- iMule,Gnutella Netzwerk,DHT Email Netzwerk I2PBote
- HTTP/HTTPS Outproxy

Java Router Built-In

- Susimail – Webmailer
- I2Psnark – Torrent Client (Auto-Update)
- Jetty – Webserver (Router Console)
- Addressbuch – I2P Petnames => b64 Adressen (wie DNS)
- Plugins für weitere Features

Weitere Implementationen

- I2P Team entwickelt Java I2P Router Suite
- Android I2P ist auch vom I2P Dev Team entwickelt & supported
- I2Pd ist eine C++ Version vom I2P Router, eigene Dev Gruppe, vor allem in Russland
- Kovri ist eine C++ Version vom I2P Router fürs Monero Projekt
- Eine Go Version ist auch in Entwicklung
- iMule, Aktie, Nightweb enthalten eigene I2P Router, meistens Java Router embedded
- Azureus/Vuze existiert ein I2P Plugin

(K)Ein Tor

- Internes Netz ohne zentrale Instanzen
- Auch für viel Traffic wie z.B. Torrent geeignet
- Gute Crypto
- Flexibel für den Nutzer
- UDP möglich
- -nur ein Outproxy
- -Nicht für den Kontakt zum ClearNet gedacht
- -noch kein Bridges, Obfuscation Transport

Recent activities

- Russland versucht Telegram zu blocken
- Telegram kann via HTTP(S) benutzt werden
- Viele I2P Nutzer in Russland nutzen den I2P Outproxy für Telegram
- Outproxy Cluster aus 4 Workstations für false.i2p
- Mehr Outproxy aus der Community
- => bessere Inkludierung von Outproxy in I2P

Danke!

- Danke für das Interesse
- Kontakt: echelon@i2pmail.org
- URL: https://geti2p.net
- Twitter: @i2p @echeloni2p
- IRC: #i2p #i2p-dev auf IRC2p und Freenode/Slack/OFTirc via Relay