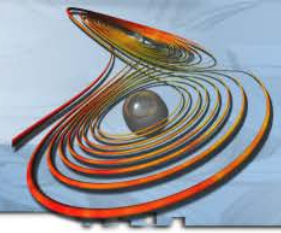


I2P,Tor,Freenet,VPN – Techniken der Anonymisierung

Lars Schimmer

CLT 2013

17.März , 2013

TU Graz

Internet – Basics

- Internet nutzt TCP/IP
- Immer eine IP als Absender
- Verbindung mit 2 IPs – beide kenne die 2 IP Adressen, sonst kein Datenaustausch!
- Die meisten IP Adressen sind registriert auf Personen/Kunden

Pseudo Anonyme Software

- Software bietet Verschlüsselung und Steganografie (z.B. torrent, eMule, skype)
- Meistens direkte IP-IP Verbidung
- Nur Daten sind verschlüsselt oder in harmlos scheinenden Daten versteckt
- Sender/Empfänger einfach identifizierbar
- Daten abgreifbar und speicherbar
- Oft keine Kontrolle über die Methodik

VPN Dienste

- Meistens kommerziell => User ID
- Verschlüsselte Verbindung zum VPN Server
- User bekommt IP vom VPN Anbieter
- Gesamter Internetverkehrt geht über die Server des VPN Anbieters
- Webserver sehen nur die IP vom VPN Anbieter
- VPN Anbieter kann anders handeln als auf der Webseite erklärt
- VPN Dienst muß dem Gesetz folgen (auf Anordnung loggen, Daten herausgeben)

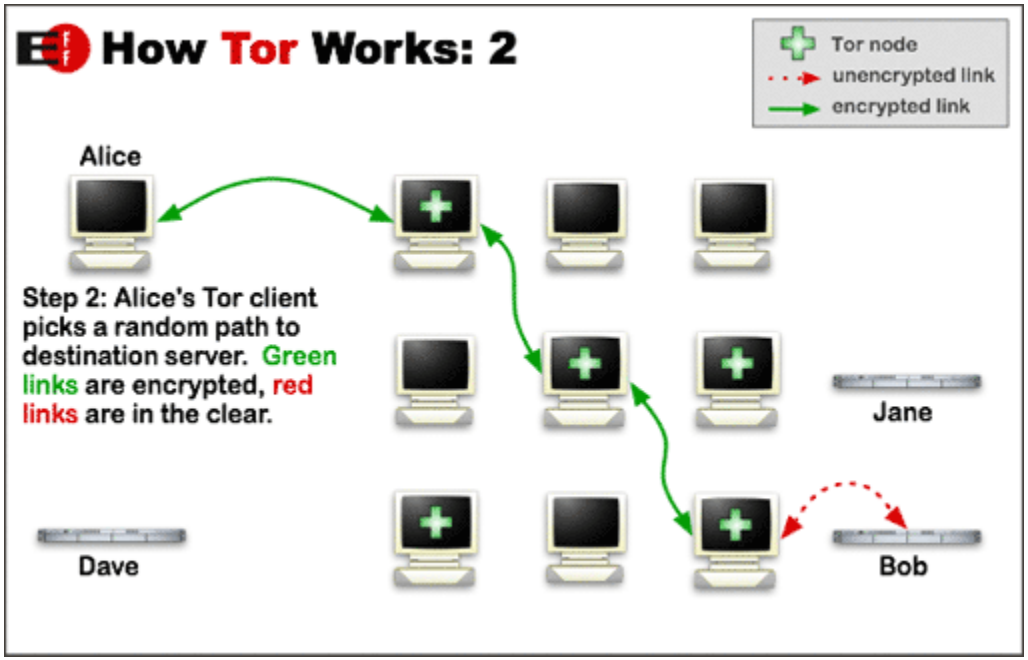
Proxy Dienste

- Meistens kommerziell => User ID
- Client verbindet sich zum Proxy Server, der reicht die Anfragen weiter zum Webserver und dann die Daten wieder zurück zum Client
- Meistens nur limitierte Protokolle (http), ungefiltert!
- Webserver sieht die IP des Proxy Servers
- Proxy Server ohne Kontrolle durch User!
- Proxy Server kann Client IP weiterreichen
- Proxy Dienst muß dem Gesetz folgen (auf Anordnung loggen, Daten herausgeben)

Multi-Hop Services

- Mehrere Proxy hintereinander
- Kommerzielle wie JonDo/JAP aus Dresden
- Tor aus der EFF Gruppe
- I2P
- Filter auf gewissen Diensten (http/IRC)
- Limitierte Protokolle (http/irc/...)
- Webserver sieht nur IP des letzten Hops
- Risiko beim letzten Hop!
- Jeder Hop kann Logfiles erstellen, aber man braucht Logfiles aller beteiligten Server

Beispiel Tor



Freenet

- Datencontainer mit verteilter Speicherung
- Dateien werden in kleine Pakete aufgeteilt und mehrfach auf verschiedenen Freenet Clients verschlüsselt gespeichert
- Daten werden von Client zu Client weitergereicht, bis das Ziel erreicht ist
- Client oder Server kennen den Weg vorher nicht, jeder Client entscheidet selber, wie die Daten weiter gesendet werden
- Sehr spezielle Nutzungsform, hohe Latenzen, Daten mit „Haltbarkeitsdatum“

GNUnet

- Mix aus Multi-Proxy und Freenet
- Direkte Verbindungen und Hop zu Hop zu Hop
- Daten können auf Nodes gespeichert werden
- Dateien werden in kleinere Pakete geteilt
- Selbst organisierend, Kademlia Algo