Mein Tor zum Internet

oder

wie ich mich vor neugierigen Blicken schützen kann

Jens Kubieziel

Chemnitzer Linux-Tage, 2006-03-05

Ich dachte immer ...

„On the internet nobody knows you’re a dog.“

Heutzutage:

Heute gilt leider: „On the internet *everybody* knows you're a dog."

Datenschnüffler sind überall

- Privatpersonen
- Firmen und
- der Staat

wollen an unsere Daten!

Firmen

- Überwachung der Arbeitsplätze
- Auswertung des Internettraffic
  - Accesslogs
  - Webbugs
  - uvm.
- Verlust von Daten

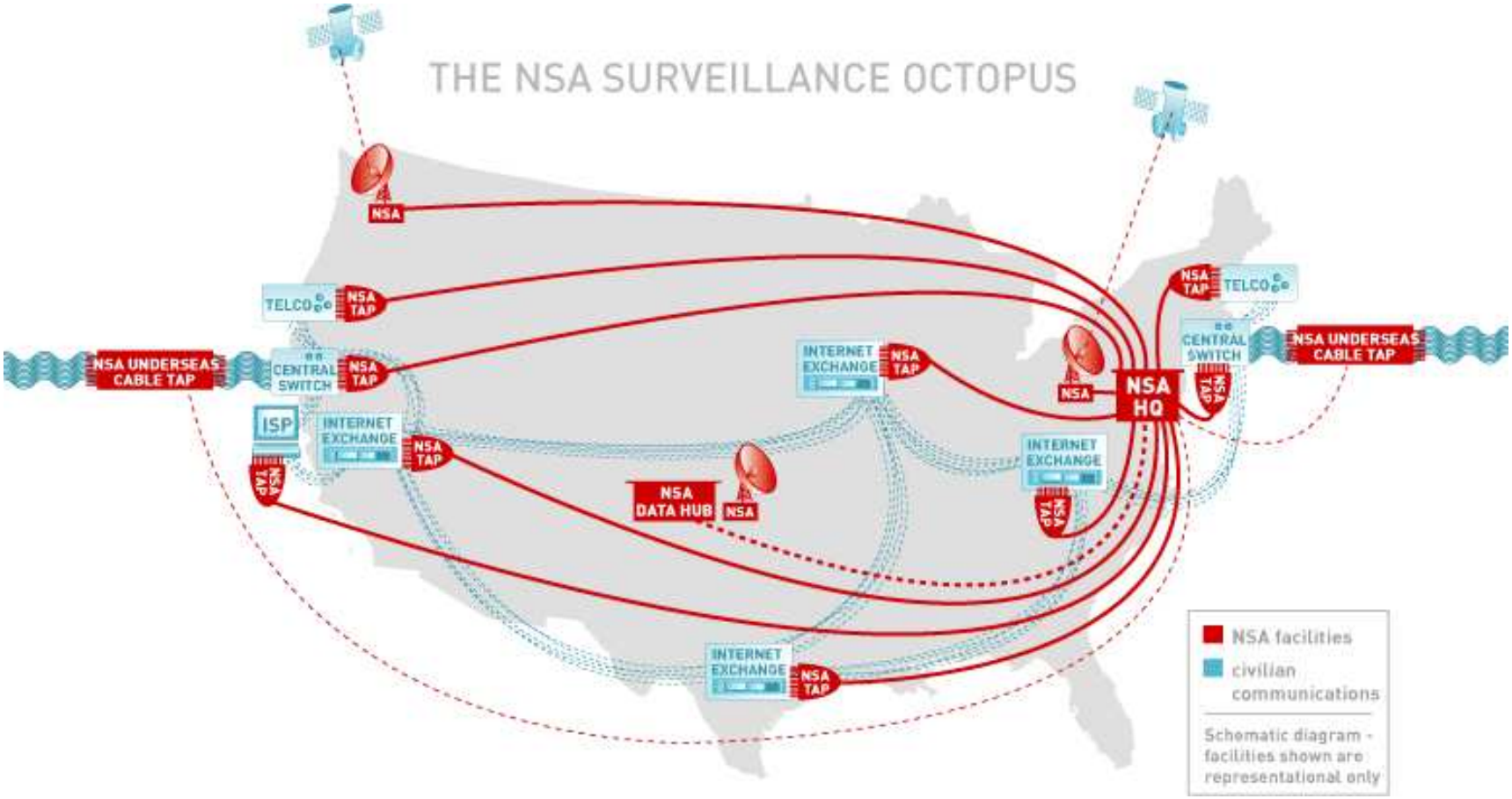
Staat

Vater Staat bietet spätestens seit 9/11 die gesamte Palette diverser Überwachungsmassnahmen.

- Videokameras
- RFID in Ausweis(en) und vielleicht bald in Geldscheinen
- Biometrie
- Überwachung der Telekommunikation (E-Mail, HTTP, Telefon, etc.)

NSA

Telekommunikationsüberwachung am Beispiel der NSA



Quelle:

`http://www.aclu.org/safefree/nsaspying/nsamap013006.html`

Vorratsdatenspeicherung

Was ist das?

- als EU-Richtlinie Ende 2005 beschlossen
- Speicherung *aller* Telekommunikationsdaten auf Vorrat $\Rightarrow$ Jeder Bürger steht somit unter Generalverdacht.
- umstritten wegen Eingriff in Fernmeldegeheimnis und Einschränkung des Informantenschutzes

Vorratsdatenspeicherung

Wo ist das Problem?

- Umkehrung der Unschuldsvermutung
- evtl. nicht konform mit Verfassung
- Steigerung der Kosten für Internetanschlüsse

Was kann ich tun?

Was kann ich tun?

- „Ich habe nichts zu verbergen“
- Rechner ausschalten und auf einsame Insel absetzen
- Immer darauf achten, was man schreibt, surft, etc. $\Rightarrow$ Wo bleibt die Demokratie und Pluralismus?
- Benutzung von Kryptographie *aber* Routinginformationen bleiben erhalten
- Benutzung von Anonymisierungssoftware

Was kann ich tun?

Anonym?

Machen das nicht nur Kriminelle, Hacker, Terroristen oder, noch viel schlimmer, Raubkopierer?

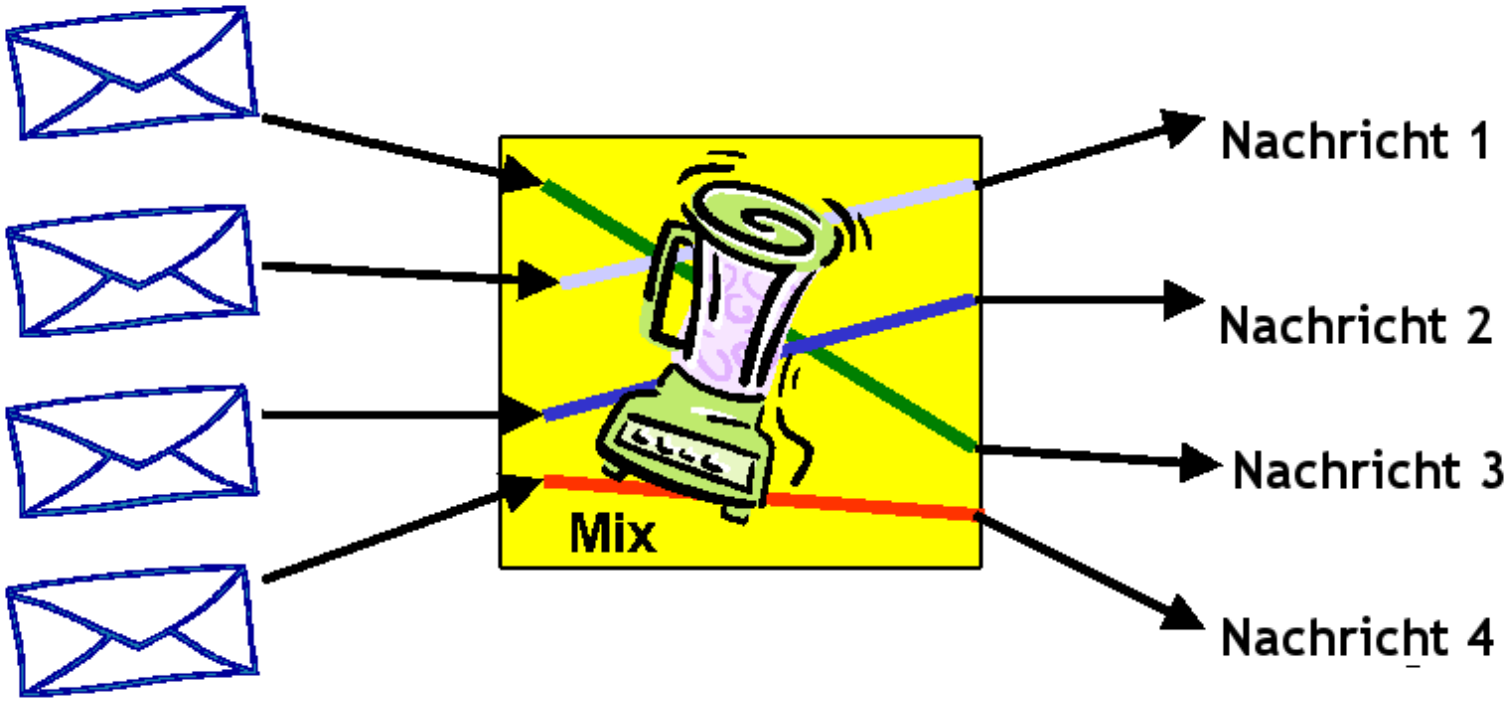
Nein!

Wahrscheinlich nutzt auch du Anonymität jeden Tag (nur nicht im Internet).

Anonymität im Internet

MIXe

basiert auf dem Prinzip so genannter MIXe:



Anonymität im Internet

Prinzip der MIXe

- entwickelt von David Chaum
- mischen Nachrichten durcheinander
- Angreifer kann nicht erkennen, welche Nachrichten aus welcher Quelle stammen

Anonymität im Internet

Software

- Mixmaster bzw. Mixminion für E-Mails
- anonymizer.com, anonymouse.org als alleinstehende Proxies
- JAP und Tor
- viele andere

Was ist Tor?

- steht für The Onion Router oder Tor's Onion Routing oder ...
- entwickelt von DARPA, ONR und später EFF
- läuft seit Oktober 2003 ohne Unterbrechung
- Infrastruktur auf freiwilliger Basis

Was ist Tor?

Details

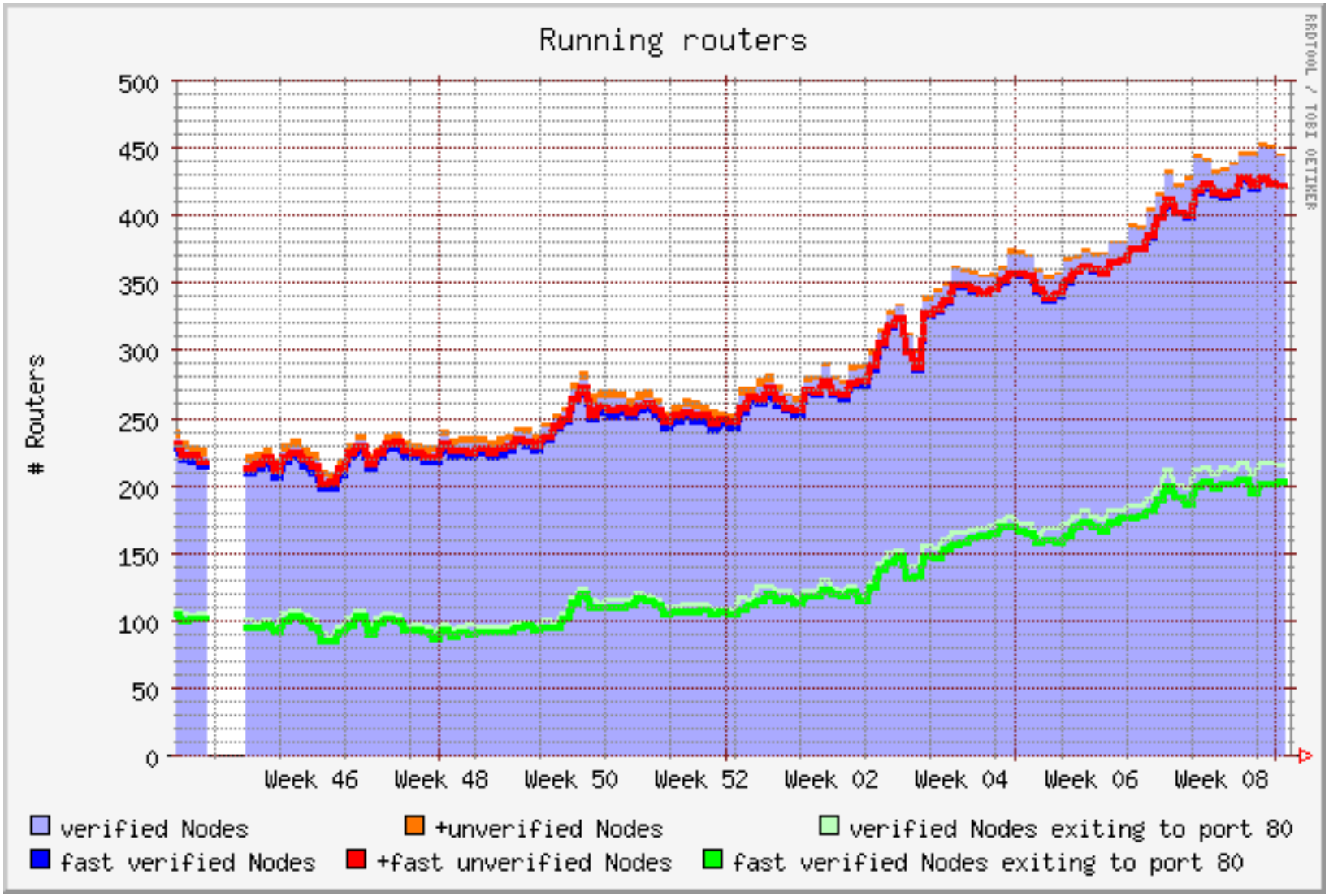
- Programm im Userspace (=keine Rootrechte)
- SOCKS-Proxy
- *wichtig:* Verbindung wird anonymisiert, keine Beeinflussung der Kommunikationsinhalte, wie JavaScript, Cookies, etc.

Größe des Netzwerks

- Verkehr pro Tag zwischen einem und 100 GB
- geschätzte 50-100000 Nutzer
- rund 400 Server

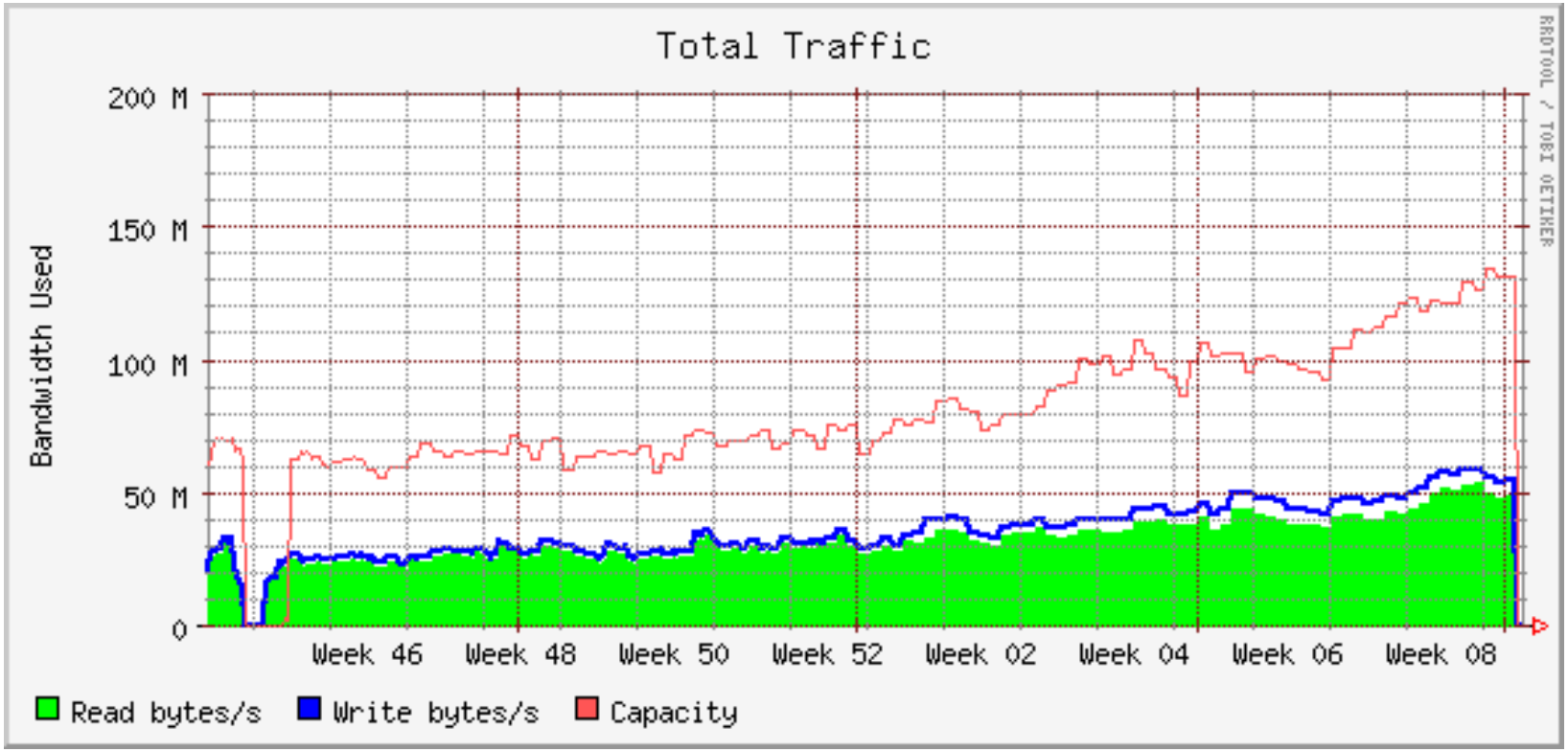
Größe des Netzes

Anzahl der Server



Größe des Netzes

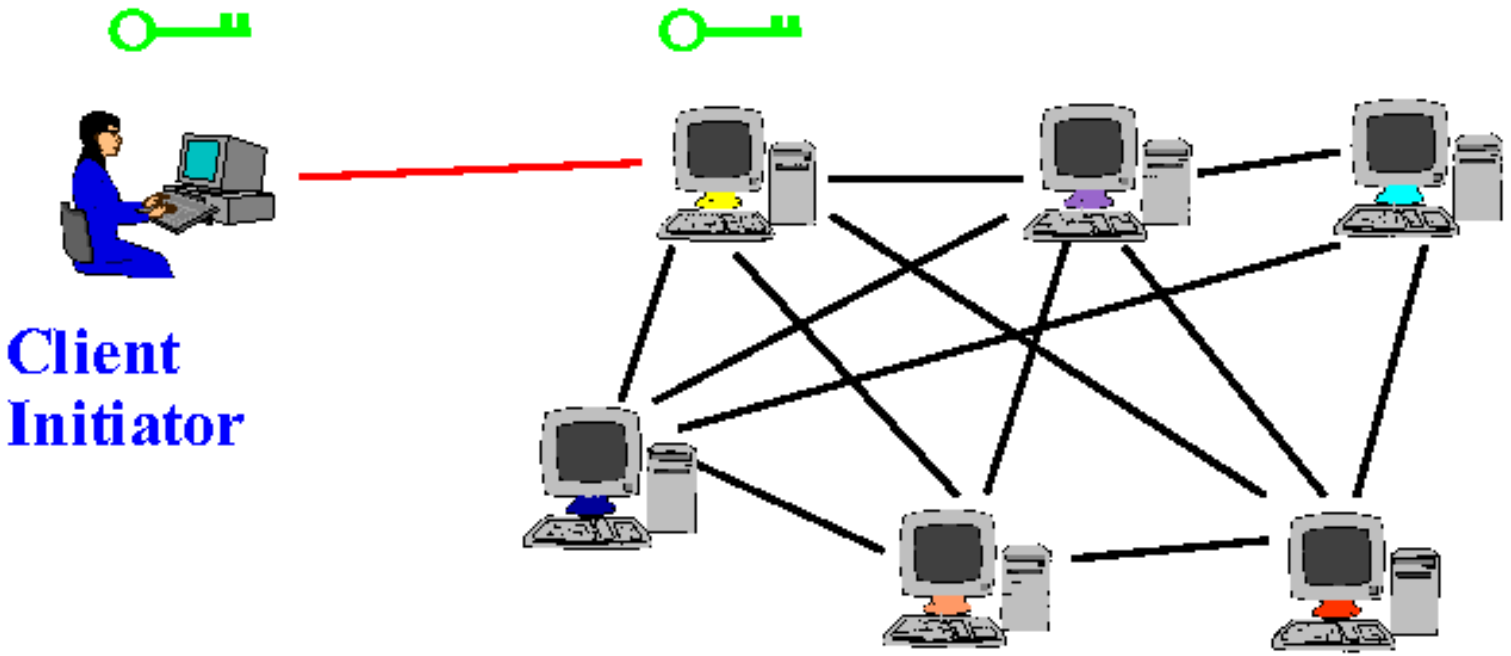
Netzverkehr



Funktionsweise

erster Schritt

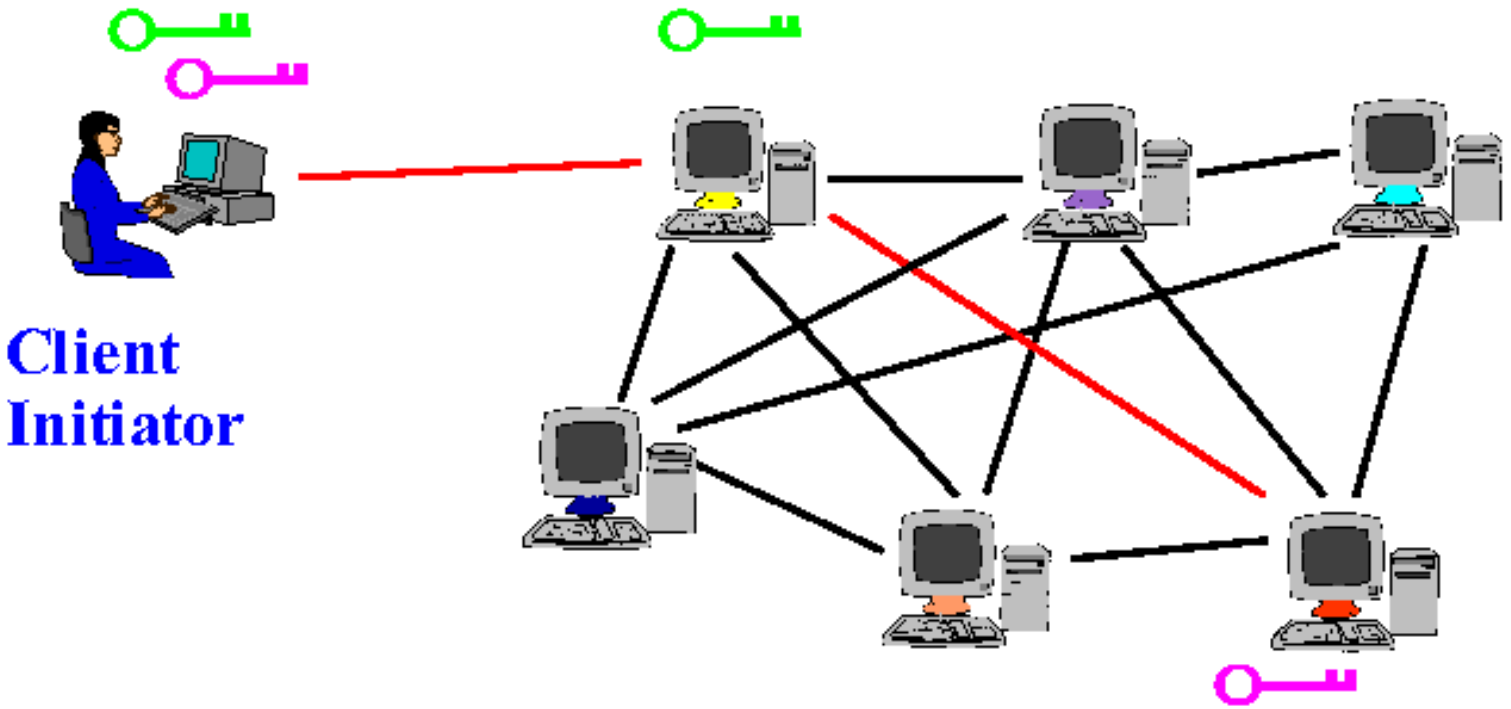
Client nimmt Verbindung zum ersten Onionrouter auf:



Funktionsweise

zweiter Schritt

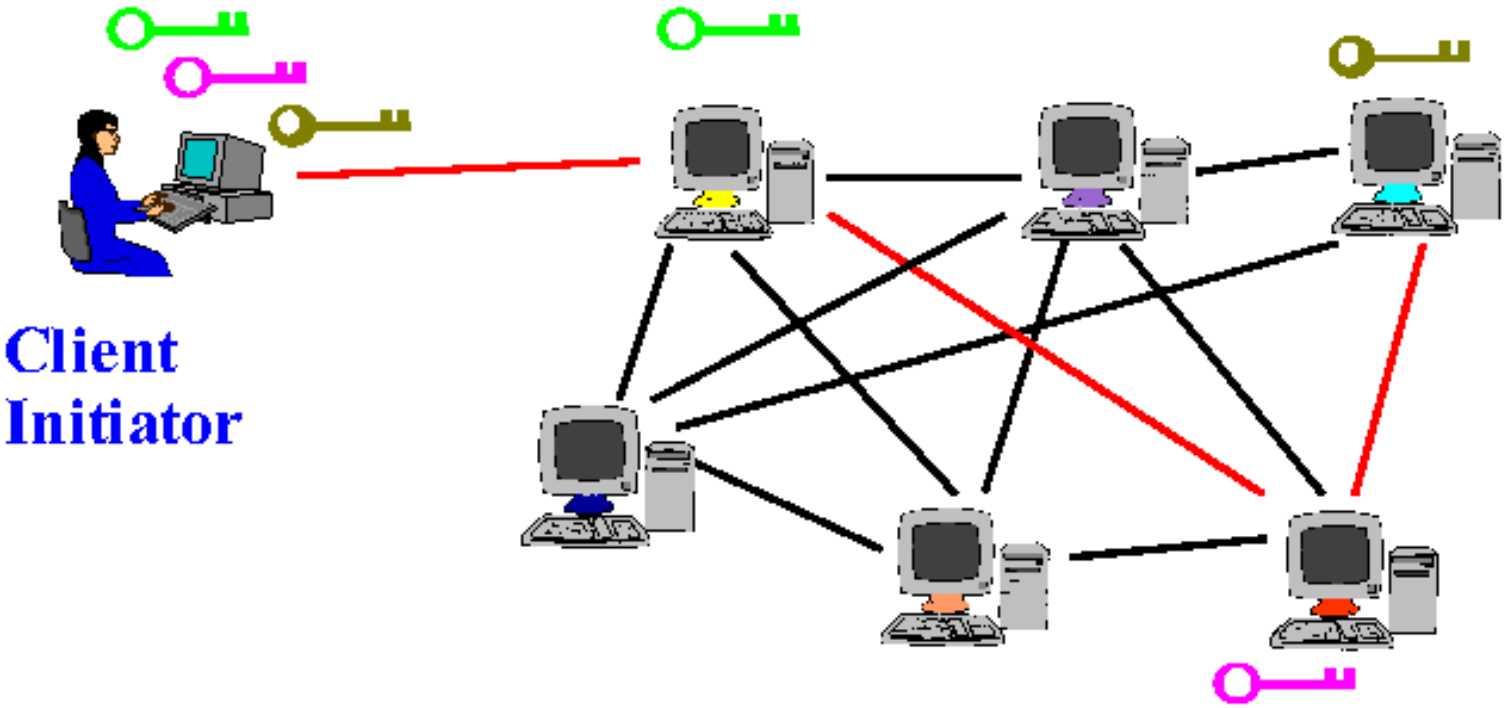
Neue Verbindung wird über die bereits bestehende initiiert:



Funktionsweise

dritter Schritt

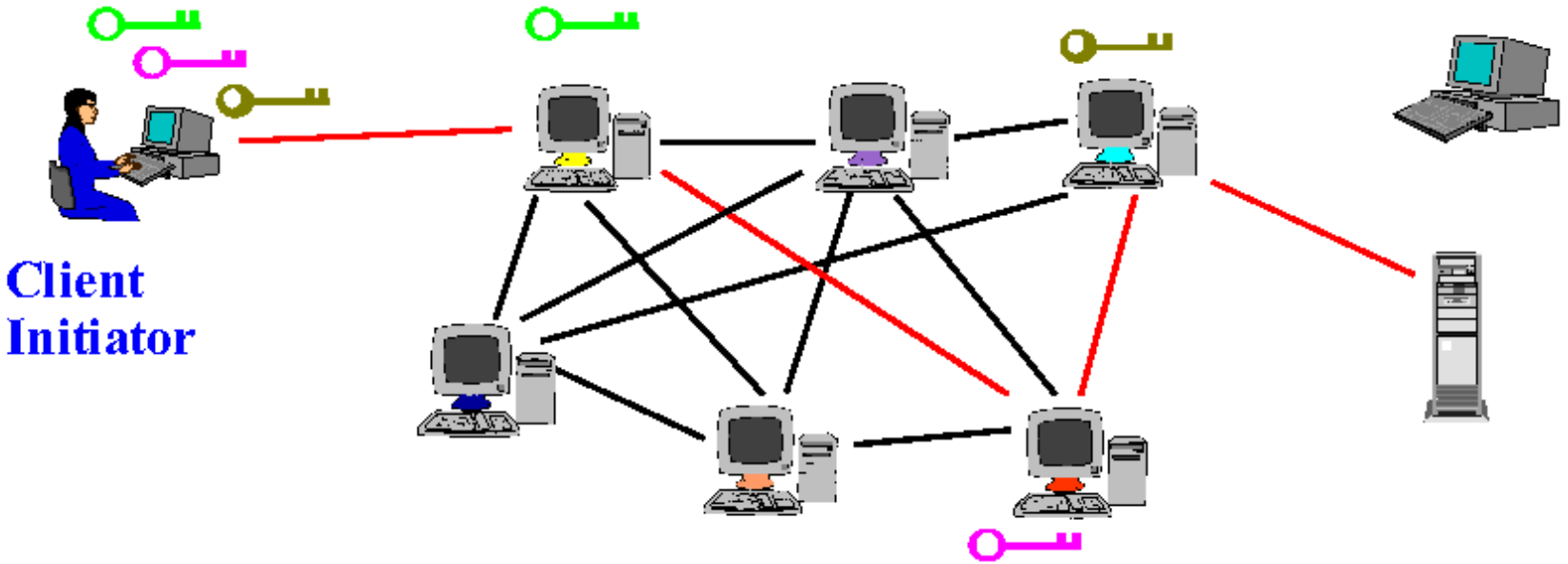
Eine weitere Verbindung wird aufgebaut.



Funktionsweise

vierter Schritt

Der letzte Torserver (Exitknoten) nimmt Verbindung zur eigentlichen Anwendung auf.



Installation und Einrichtung

Installation Tor und Privoxy über Distribution oder UNIX-Dreisatz

Einrichtung

- Konfiguration in /etc/{tor/}torrc
- in Privoxy: forward-socks4a / localhost:9050 .
- im Browser Proxy einstellen

Tor kann

- HTTP
- SMTP
- SSH
- IRC
- und vieles mehr

anonymisieren.

Was bleibt für euch?

Installieren, Testen und eigenen Server aufsetzen.

Schlusswort

Ich wünsche euch viel Spass mit Tor. Gibt es Fragen?

Literatur

Allgemeine Informationen

Informationen zur Vorratsdatenspeicherung
`http://www.vorratsdatenspeicherung.net/`

Informationen des Unabhängigen Landeszentrum für Datenschutz
`http://www.datenschutzzentrum.de/rotekarte/`

Anfertigung von Fingerabdrücken `http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml`

Advisory des RUS-CERT zu ivwbox `http://cert.uni-stuttgart.de/ticker/article.php?mid=641`

Literatur

Tor

David Chaum: Untraceable electronic mail, return addresses, ... http://world.std.com/~franl/crypto/chaum-acm-1981.html

Homepage des Projektes http://tor.eff.org

FAQ zu Tor http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ

Installationsanleitung http://kai.iks-jena.de/bigb/asurf.html
sowie http://kubieziel.de/blog/archives/199-Kurzanleitung-zur-Installation-von-Tor.html