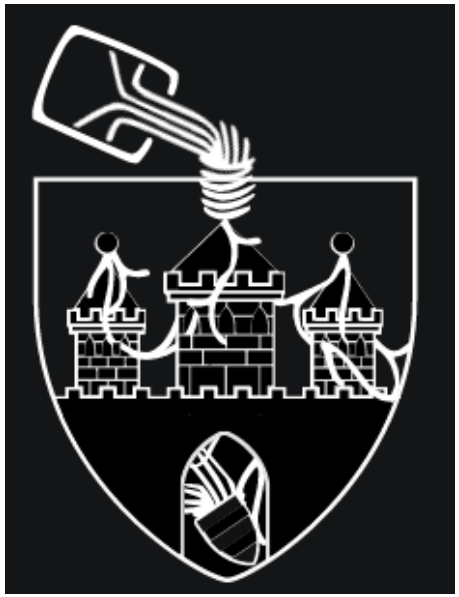
Sicheres surfen im Internet. Mit Tor!

Tobias Stöckmann und Peter Gewald

Chaostreff Oldenburg

14. November 2015



https://ccc-ol.de

https://mainframe.io

Gefahren im Netz

- Viren, Trojaner, Würmer
- Datendiebstahl
  - Kreditkartennummern, Zugangsdaten, ...
- Ransomware
  - Fremde Verschlüsselung eigener Daten
- Tracking
  - Erhebung persönlicher Daten
  - ... was ist daran schlimm?

Gesellschaft

- Verhaltensänderung durch Überwachung
- Beispiel: Privatgespräche in der Öffentlichkeit

Politik

"Daten werden der Rohstoff der Zukunft sein in der digitalen Welt."
- Angela Merkel, 9.6.2015

Wirtschaft

- Googles Jahreseinnahmen pro Person: 45 $
- Facebooks Jahreseinnahmen pro Person: 9 $
- Dafür sind die Dienste "gratis"
  - Und ich habe nichts zu verbergen

Snowden

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say. A free press benefits more than just those who read the paper."

" [...] they are misunderstanding the fundamental nature of human rights. Nobody needs to justify why they "need" a right."

Wirtschaft

- Dann benutze den Dienst nicht
  - Bild.de blockiert Adblock-Nutzer
- Viele Alternativen verfügbar
  - Duckduckgo statt Google als Suchmaschine
  - Zeitschriften/Zeitungen kaufen
  - ...
- Aber ich möchte den Dienst nutzen

Wirtschaft

- Stöbern auf Amazon
  - Ich möchte erst einmal gucken
  - Und später eines der Produkte bestellen
- Ich möchte nicht, dass Amazon weiß,
  - was ich alles gesucht habe
  - wann ich danach gesucht habe
  - wer ich bin
- Falls ich bestelle? Na gut.

Anonymität herstellen

- Cookies löschen
  - Tracking ist vielschichtiger
- Privaten Modus nutzen
  - Verschleiert nicht die Herkunft
- Tor verwenden

Was ist Tor?

- Tor ist **T**he **O**nion **R**outer Network
- Internationales Projekt von Freiwilligen
  - Ursprung in der US Navy
- Anonymisierungsnetzwerk
  - Ursprünglicher Sender ist dem Ziel unbekannt
  - Ziel des Datenpakets wird verschleiert
  - Nur der Sender kennt gesamte Route
    - Ausnahme sind die "Hidden Services"

Was ist Tor nicht?

- Keine Ende-zu-Ende-Verschlüsselung
  - Kein Ersatz für https, pop3s, smtps, imaps, ...
- Kein Schutz vor globaler Überwachung
  - Globaler Lauschangriff offenbart Route
  - Laut NSA-Dokumenten trotzdem recht gut

Szenario: Nachricht austauschen

1. Ohne Tor
2. Mit Tor

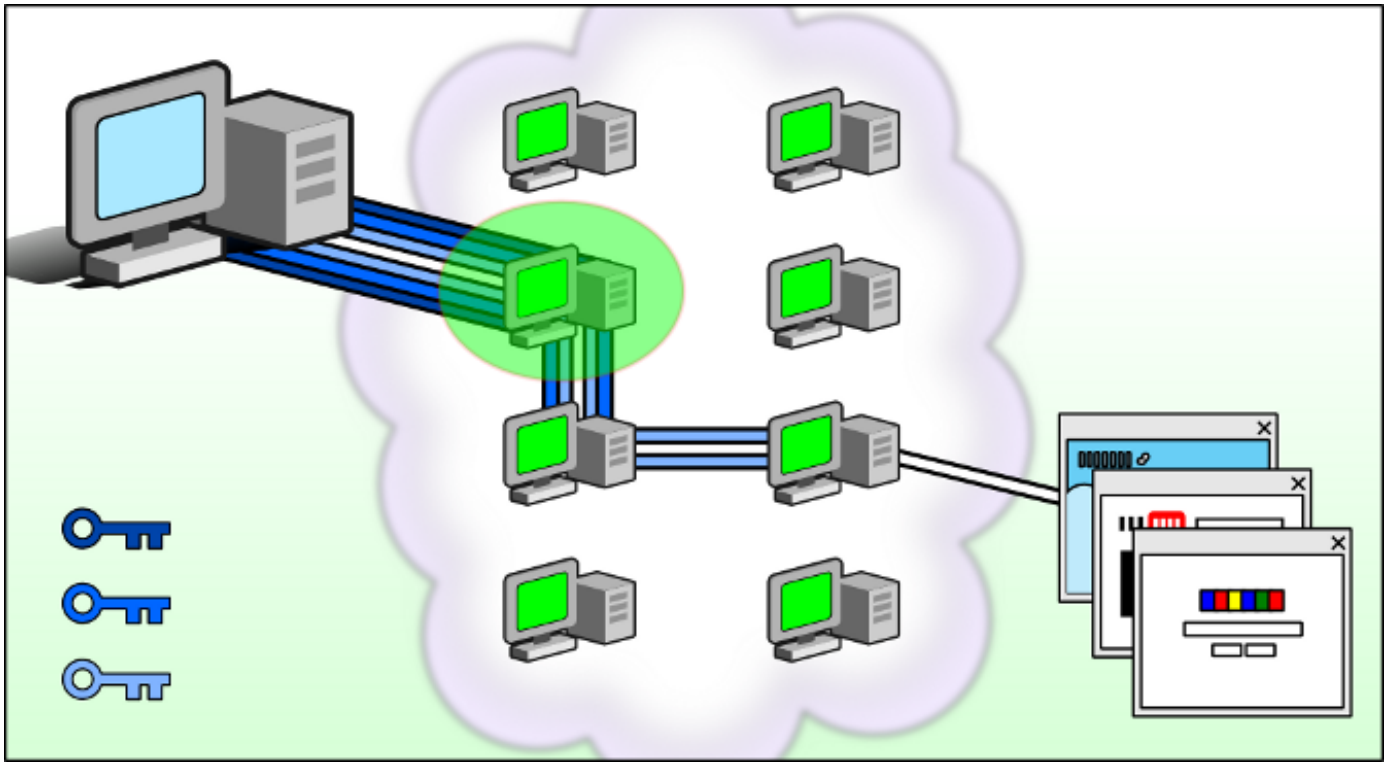
Directory Service

- Verzeichnisserver
- Signierte Liste von Tor-Nodes
- Prüfbar anhand des Tor-Clients (public key)
- Node = Server des Tor-Netzwerks

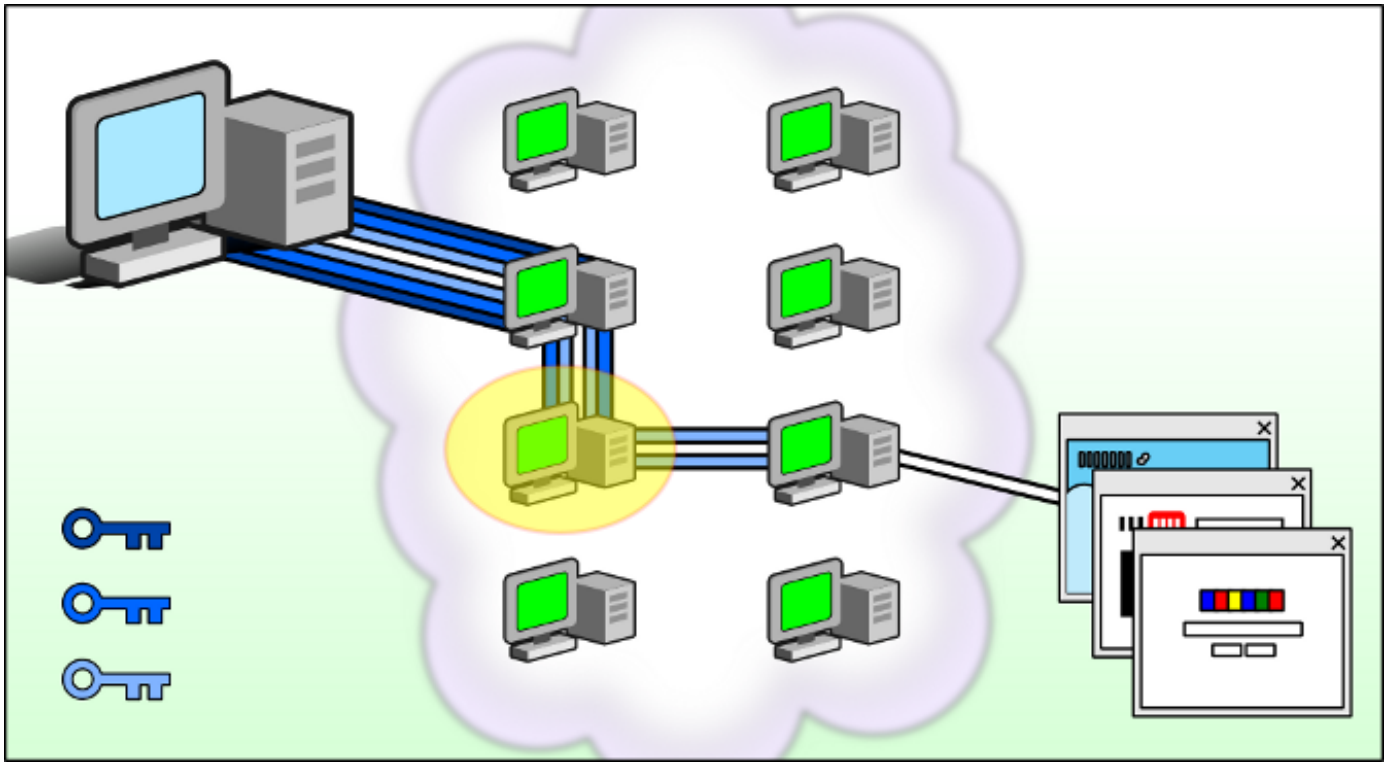
Paketvorbereitung Verschlüsselung

- Sender verschlüsselt Datenpaket für jeden Node
- Verwendung von Sitzungsschlüsseln (vorher ausgehandelt)

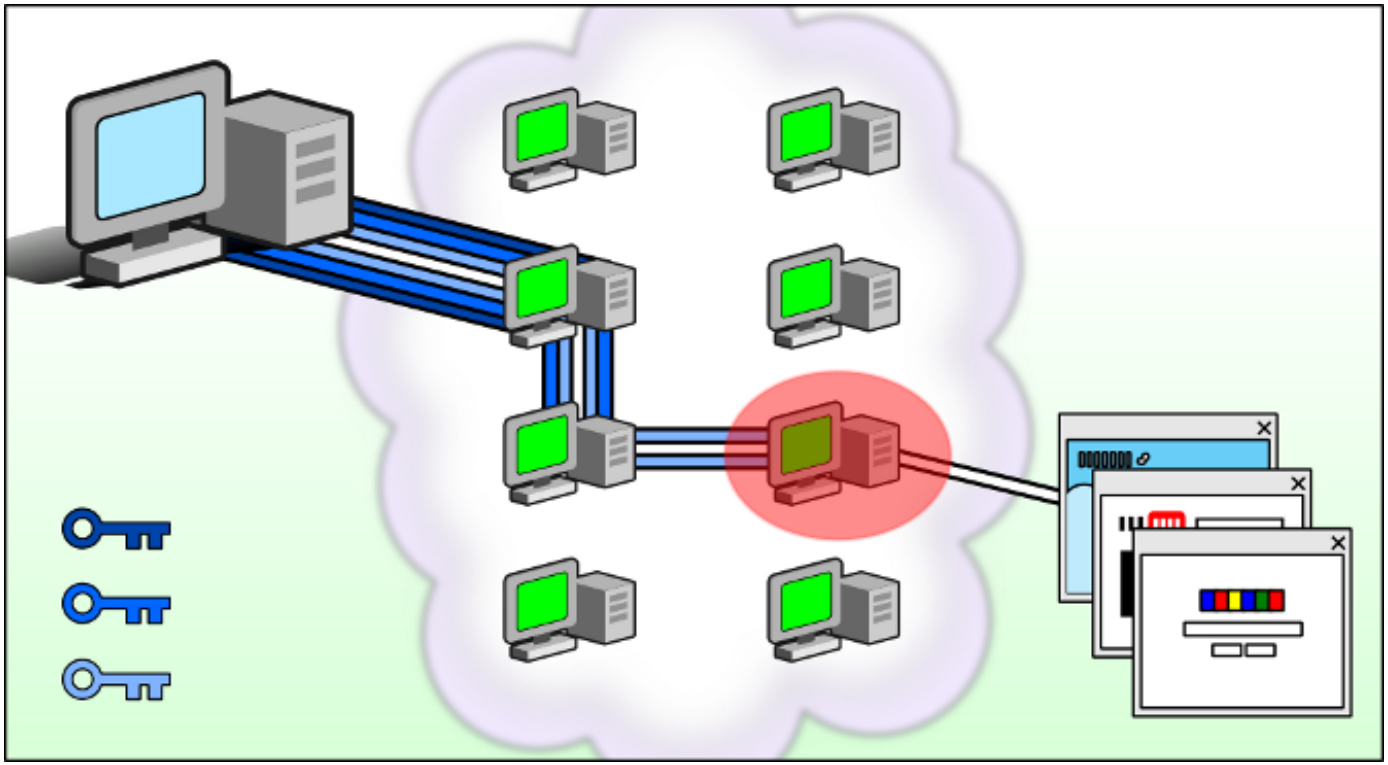
Entry-Node



Middle-Node



Exit-Node



- Verbindung zu Zielserver Tor-seitig unverschlüsselt!
- Ende-zu-Ende Verschlüsselung!

Rückantwort

- Gleiche Schlüssel
- Nodes halten Verbindung offen

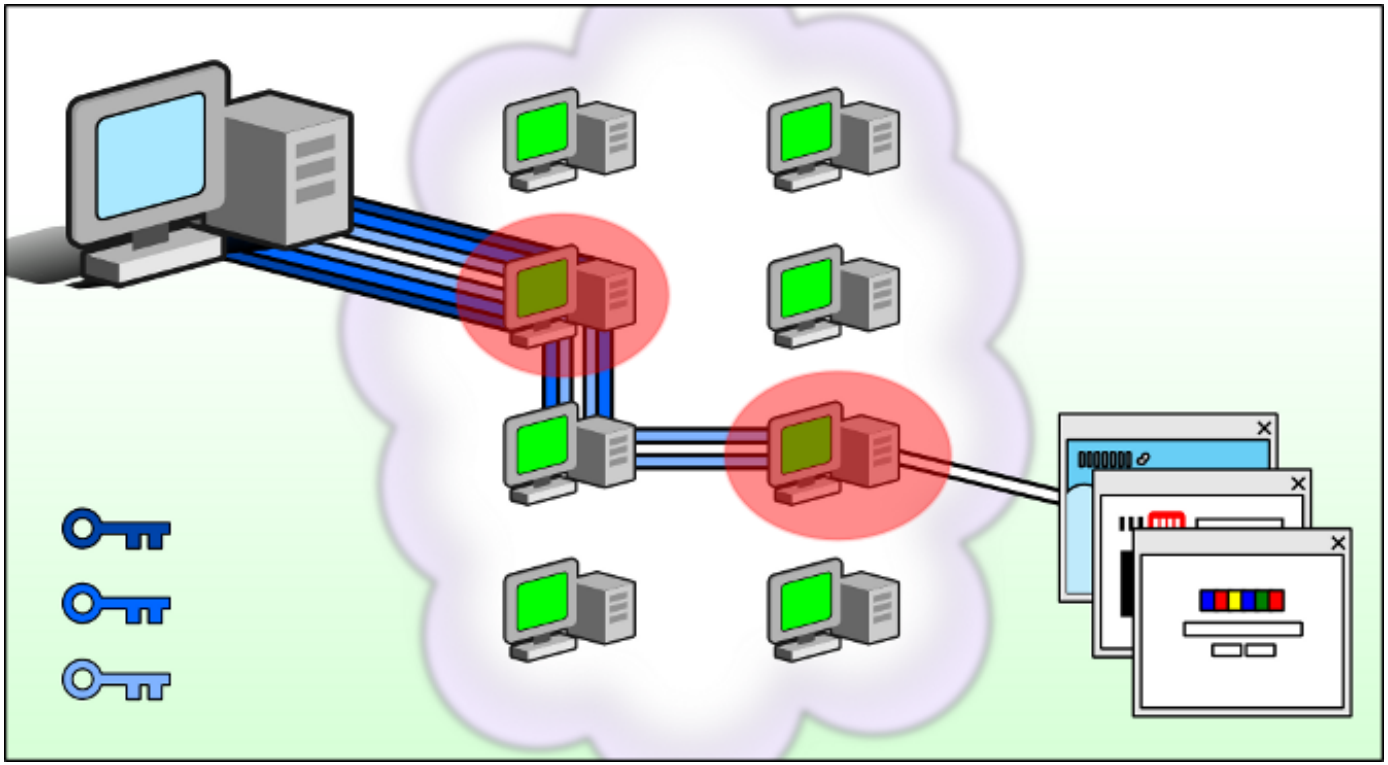
Neue URL? Neue Route!

- Tor Route zeitlich begrenzt
- URL bedingte Routenänderung
- Angriffsprevention

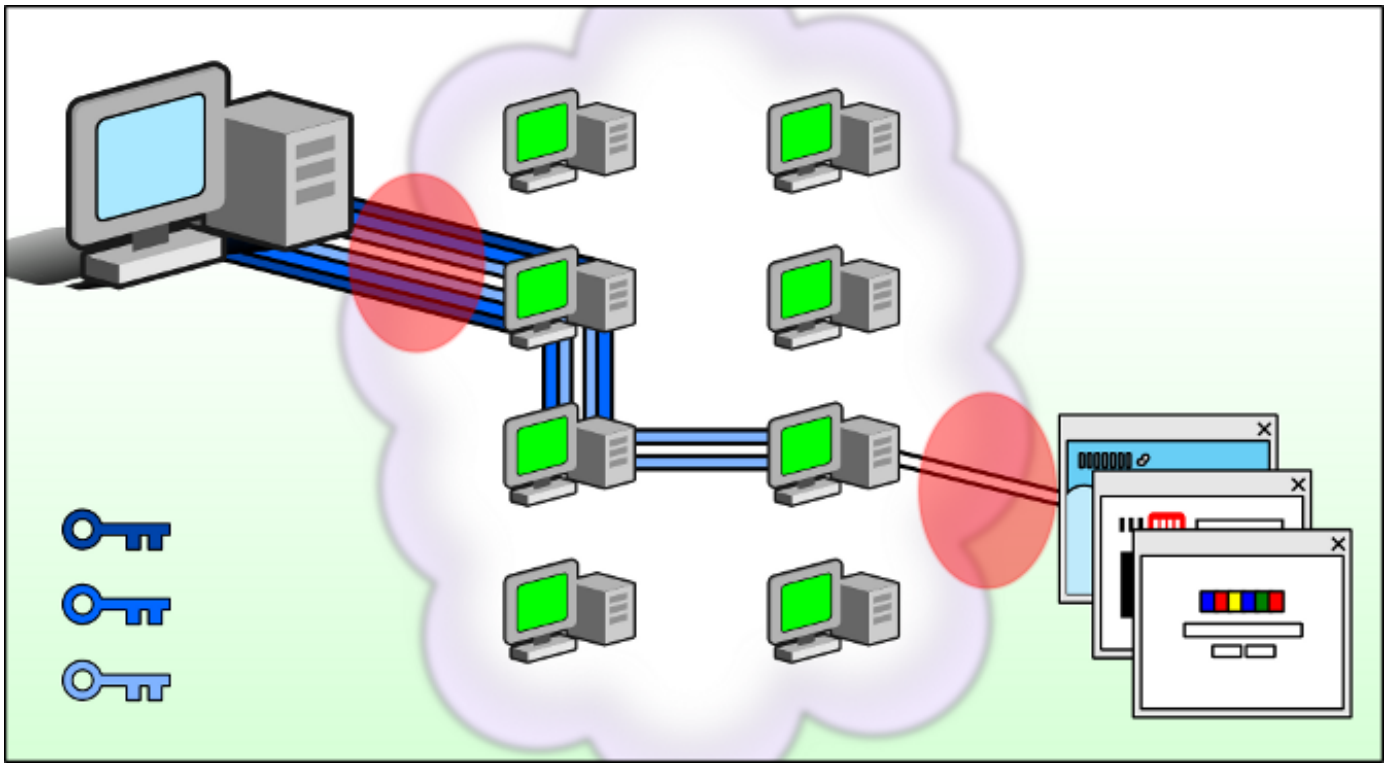
Statistische Verteilung der Nodes

- Kontrolle von Entry und Exit Node
- Aufgrund häufiger Routenwechsel möglich
- Zeitliche Abfolge und Datenaufkommen analysieren
- Traffic Entry- und Exit-Node vergleichen
- Identitätsaufdeckung möglich
- Je mehr Nodes in verschiedener Hand, desto besser

Kontrolle der Nodes



Kontrolle der Verbindungen (komplexer)

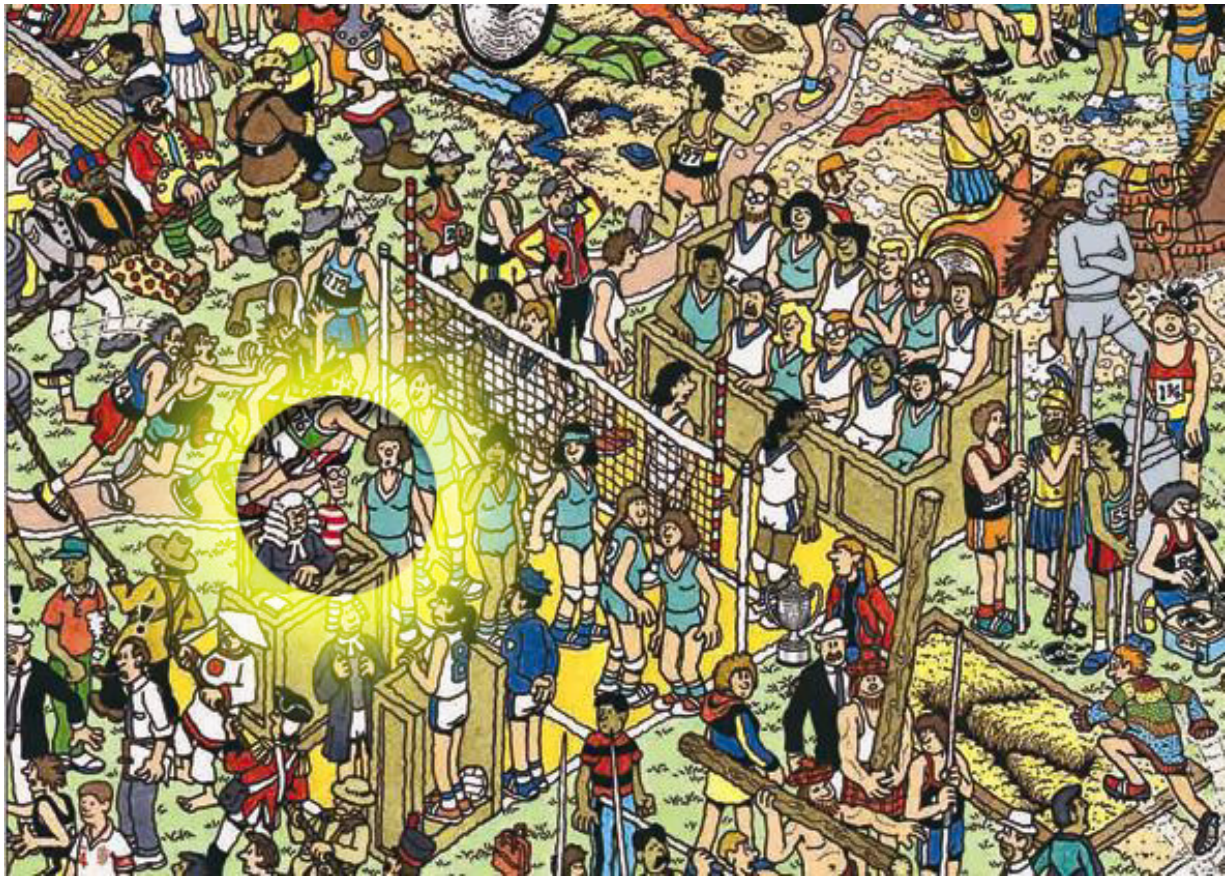


Alle Verbindungen kontrollieren = Publikum

Fazit

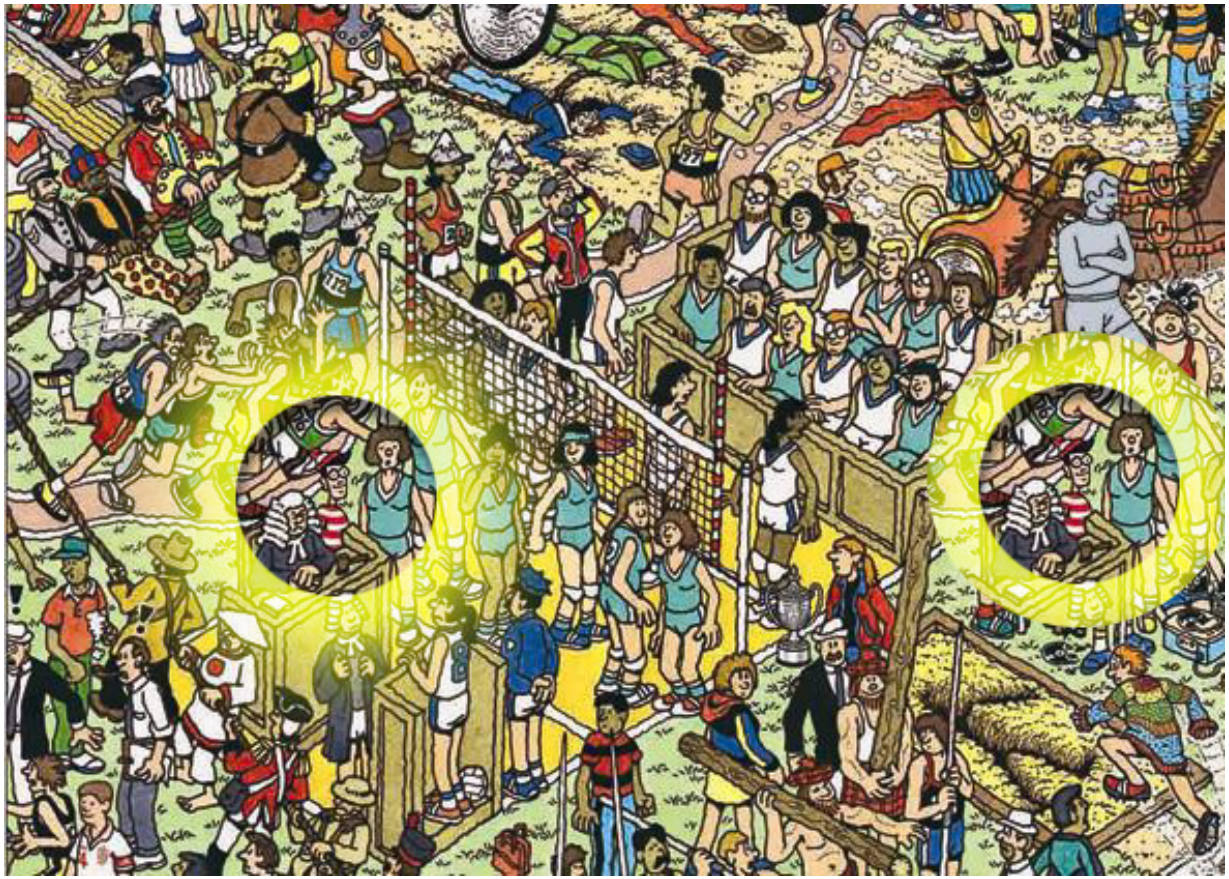
- Exit-Node → Server unverschlüsselt (https benutzen)
- Anonymität ist ein Gesellschaftsthema
- Mehr Clients ⇒ Mehr Anonymität

Ein Tor-Nutzer



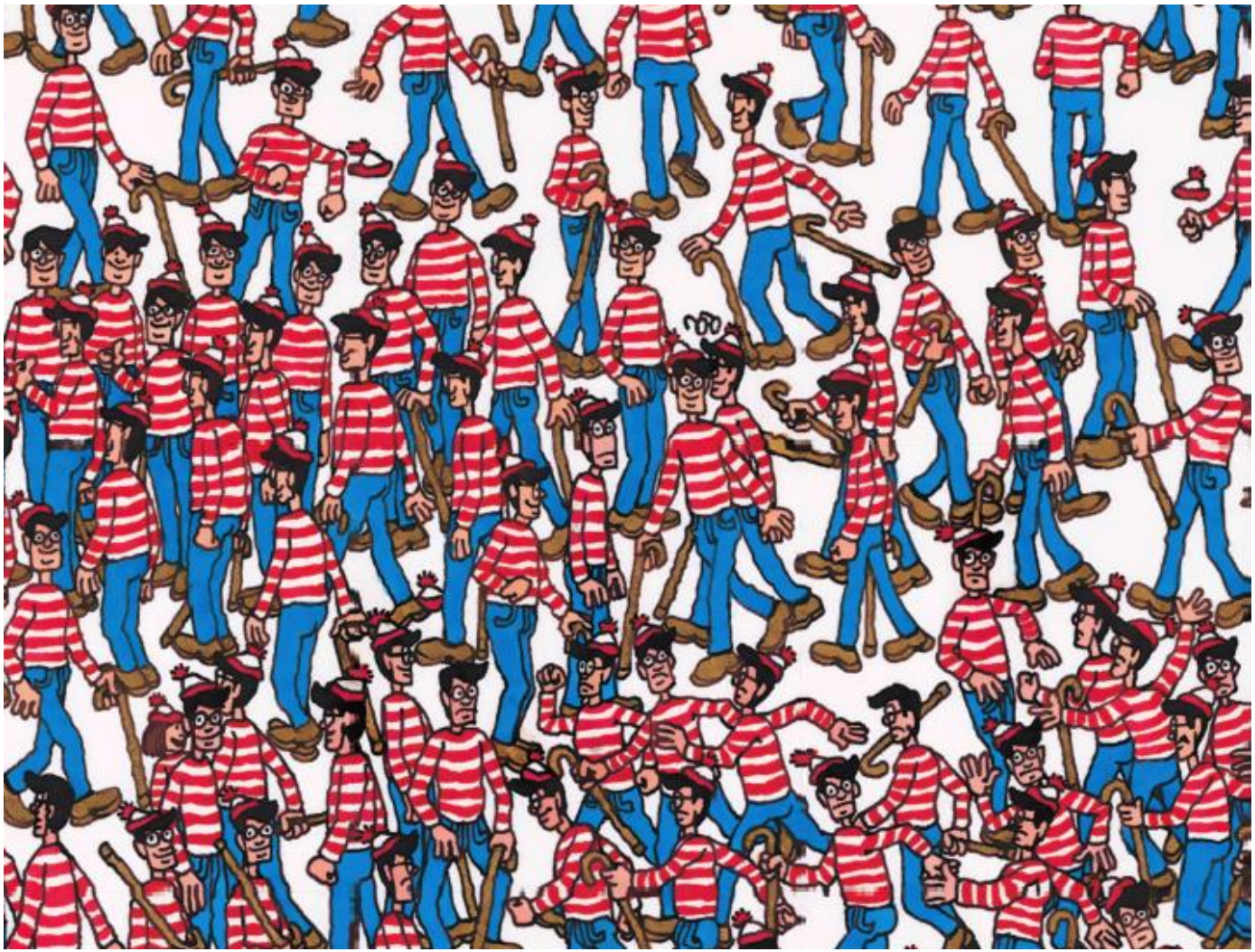
http://www.weltenschummler.com/wp-content/uploads/2013/11/wheres-waldo.jpg

Zwei Tor-Nutzer



http://www.weltenschummler.com/wp-content/uploads/2013/11/wheres-waldo.jpg

Gruppe von TOR-Nutzern



http://www.maclife.de/media/maclife/styles/tec_frontend_fullscreen/public/data/editors/2010_23/image-11706--15809.PNG

Wie verwende ich Tor?

- Tor Browser Bundle
  - Für Windows/Linux/OS X verfügbar
  - Enthält angepassten Firefox
  - https://tor-project.org
- Tails
  - Auf Anonymität/Tor spezialisierte Linux-Distribution
  - In virtueller Maschine oder direkt starten
  - https://tails.boum.org
- Orbot
  - Über Android Playstore erhältlich
  - Tor für Browser, Mail, Instant Messaging, ...
  - Playstore