TOR
The Onion Routing

Von Max Karl

Gliederung

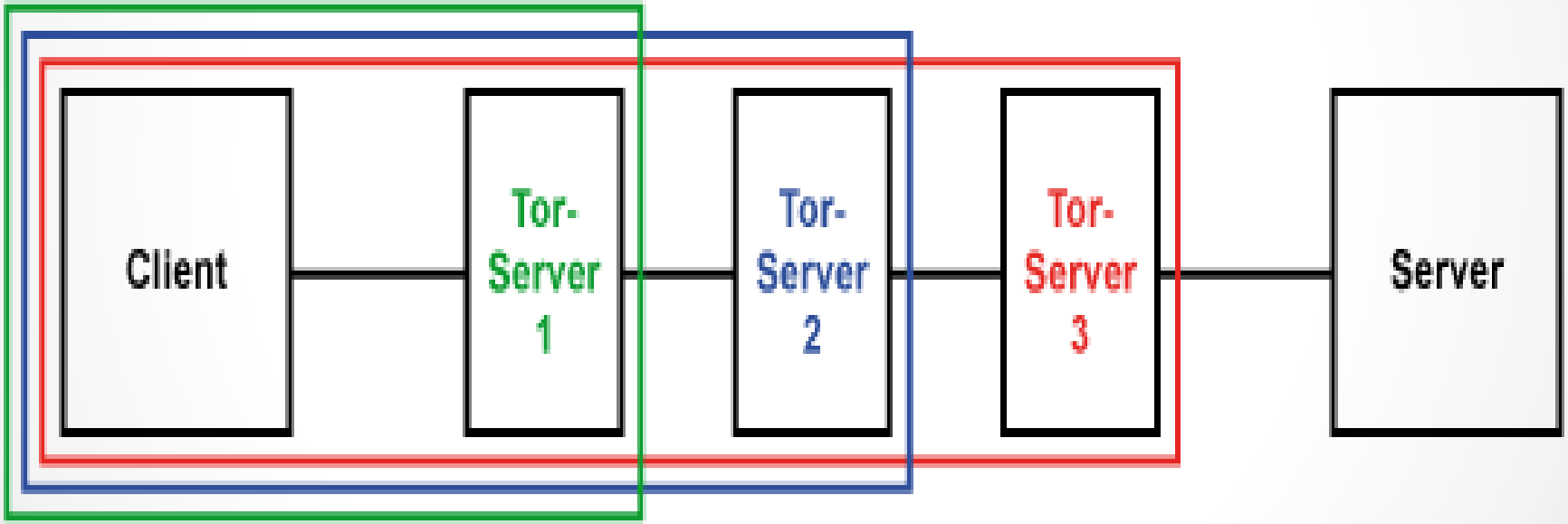
- Einleitung
- Kurze Historie
- Funktionsweise
- Entry Guards
- Tor-Bridges
- Sicherheit und Schwachpunkte
- Zahlen
- Fazit

Geschichte

- Erste Idee zu Tor schon 2000
- September 2002 Alpha Version
- März 2011 Preis für gesellschaftlichen Nutzen
- 2012 Zuwendungen zu etwa 60% von US-Regierung
- Juni 2014 NSA überwacht Betreiber eines Tor-Knotens

Funktion

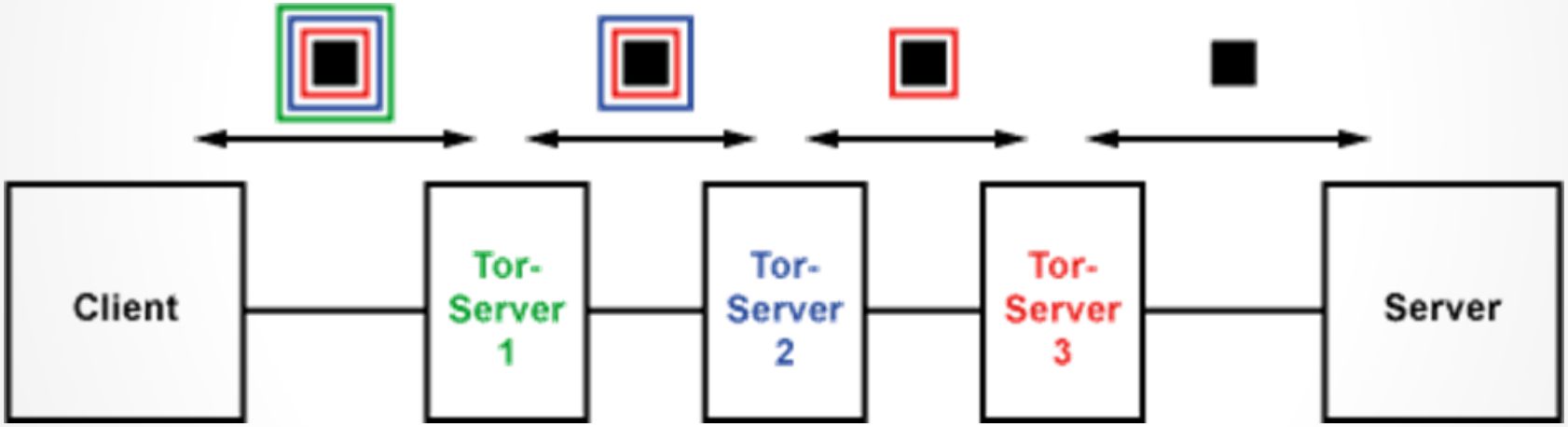
- Basiert auf Prinzip des Onion-Routings



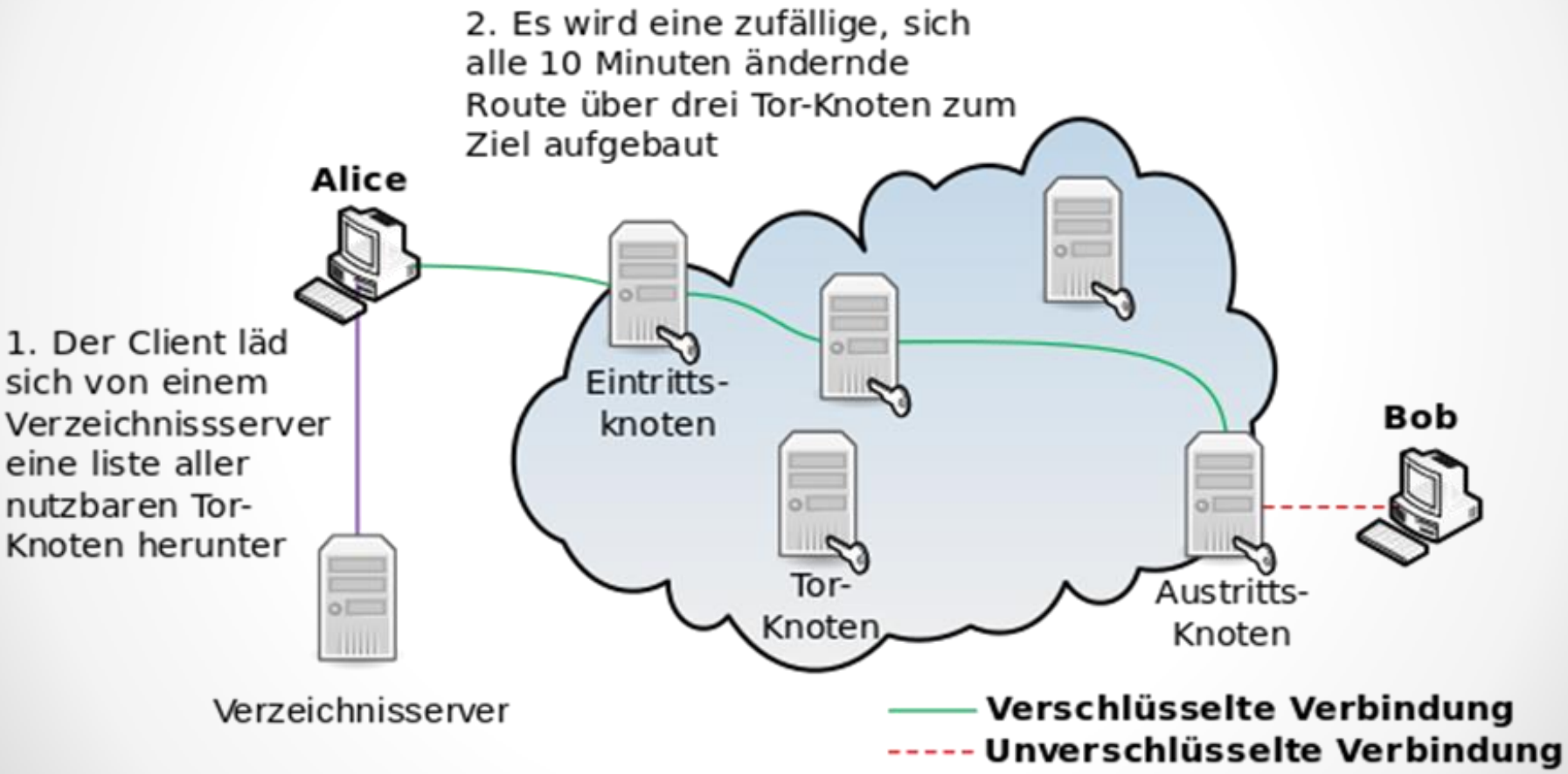
Verschlüsselung nach dem Zwiebel-Prinzip

Funktion

- Jeder Knoten bildet eine Verschlüsselungsschicht



Funktion


2. Es wird eine zufällige, sich alle 10 Minuten ändernde Route über drei Tor-Knoten zum Ziel aufgebaut
Alice
1. Der Client läd sich von einem Verzeichnisserver eine liste aller nutzbaren Tor-Knoten herunter
Eintritts-knoten
Tor-Knoten
Austritts-Knoten
Bob
Verzeichnisserver
Verschlüsselte Verbindung
Unverschlüsselte Verbindung

Entry Guards

- Tor bietet keinen Schutz falls Angreifer den ersten und letzten Knoten kontrolliert
- Durch Kurzlebigkeit der Routen und Routenboykott zwangsläufig auf unsichere Route gedrängt
- Deshalb werden Entry Guards gewählt
- 3 zufällige Knoten die mehrere Wochen und über mehrere Sitzungen hinweg genutzt werden

Tor-Bridges

- Tor kann auch genutzt werden um Zugriffssperren zu umgehen ➡ nicht erwünscht !
- Wird z.B. durch chinesischer Internetkontrolle gesperrt
- Deswegen Erweiterung um Bridge
- Vermittelt zwischen geblockten Nutzern und Tor-Netzwerk
- Internetadressen können in einen von drei Adresspools hinterlegt werden

Sicherheit

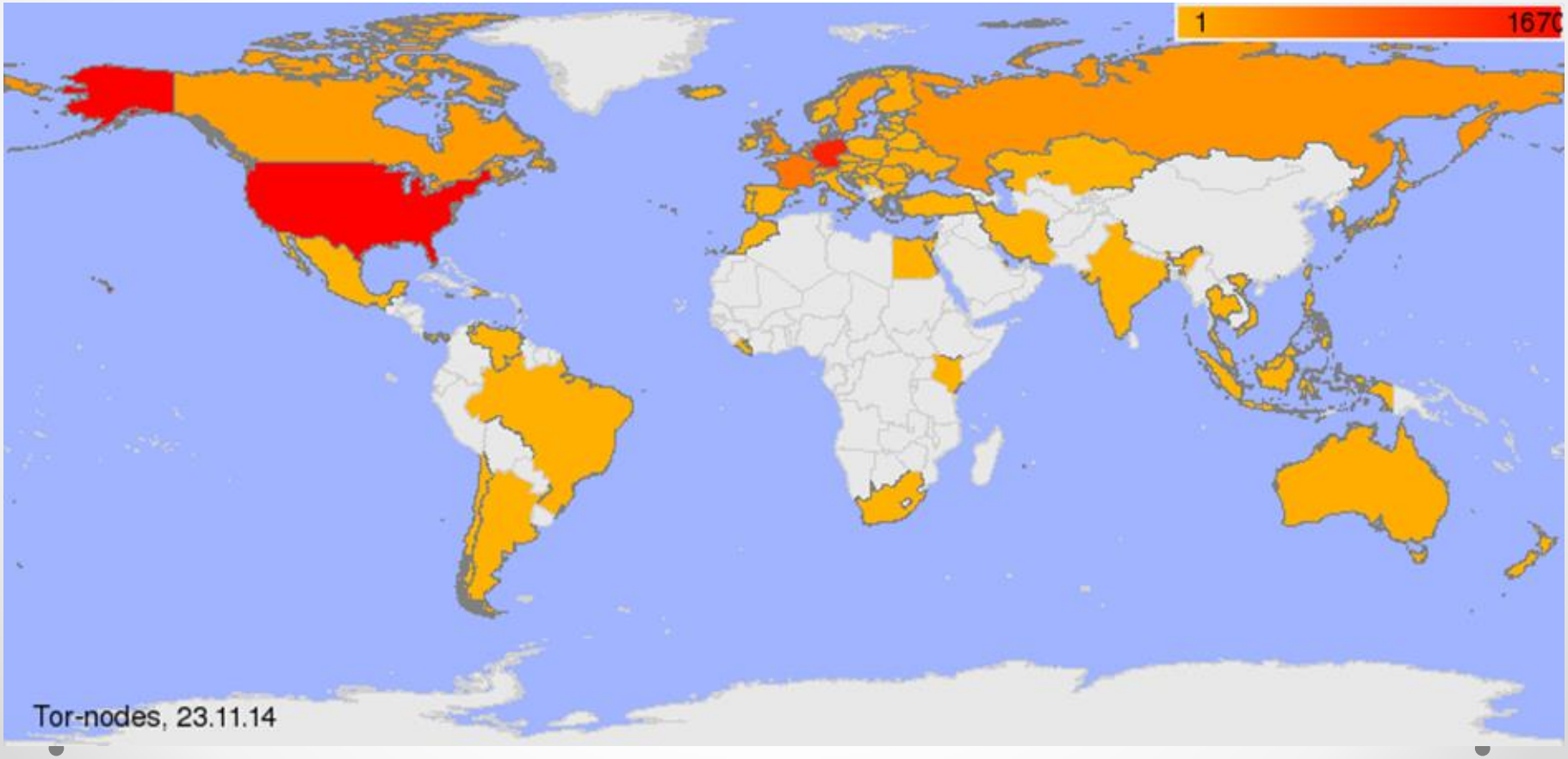
- Suche nach Traffic-Mustern zur Deanonymisierung des Datenverkehrs
- Muster von HTTP-Anfragen kann erkannt und zugeordnet werden
- Erkennung individueller Einstellungen möglich
- Zeitliche Analyse von Ende-zu-Ende Verbindung lässt Verbindung auffliegen
- Markieren von Paketen - dadurch Ankunftszeit berechnen
- Directory Server übernehmen – Beeinflussung der Aufnahme von Routern

Schwachpunkte

- Die selbe Route für Datenübertragung mehrerer Anwendungen
- Falls IP aufgedeckt wird können alle Anwendungen des Clients zugeordnet werden
- Sicherheitslücke im Webbrowser Firefox
- Dadurch Protokollierung des gesamten Datenverkehrs möglich

Zahlen

- Oktober 2011 standen rund 2350 Tor-Nodes
- Mittlerweile über 6000 Tor-Nodes
- Verteilung heute:



Fazit

- Nie den Betreibern der Tor-Server trauen
- Daten sollten immer zusätzlich verschlüsselt werden
- Als Nutzer muss man immer davon ausgehen das die Verbindung überwacht wird

Quellen

- wiki.ubuntuusers.de/Tor/Gefahren
- http://www.heise.de/netze/meldung/Tor-Nutzer-ueber-Firefox-Luecke-verfolgt-1930154.html
- http://www.dianacht.de/torstat/
- http://www.golem.de/news/anonymisierung-tor-nutzer-surfen-nicht-anonym-1309-101417.html
- http://www.elektronik-kompendium.de/sites/net/1809171.htm
- http://www.zeit.de/digital/datenschutz/2013-08/angriff-tor-netzwerk-nsa/komplettansicht
- http://de.wikipedia.org/wiki/Tor_(Netzwerk)
- http://privacyknowledge.org/blog/das-tor-netzwek-wie-es-funktioniert-und-was-sie-darüber-wissen-sollten