

Ausarbeitung zum Seminar

Per-Circuit TCP-over-IPsec Transport for Anonymous Communication Overlay Networks

Manuel Schneider

Albert-Ludwigs-Universität Freiburg
Lehrstuhl für Kommunikationssysteme

11. April 2013

Zusammenfassung

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

1 Motivation

Eventuell grobe Basics zu Tor was es ist, wozu man es braucht.

Performancemeasurement

Problemeingrenzung

Was kann dagegen gemacht werden, was wird gemacht? (Name „TCP-over-DTLS“ fällt)

Was ist das Ziel dieser Publikation vom PCTCP?

2 Grundlagen

2.1 TOR

Basics zu Tor (Ausmaß in der Präsentation abhängig von Dirk).

Reduziert sich minimal auf die Performancemängel und die Transportlayergeschichte, die für diese Arbeit besonders von Belang ist.

Themen:

- Circuit construction
- Diffie Hellman
- SOCKS Proxy
- Source Routing
- Cross Circuit Interference Problem (Unfair TCP Congestion Control)

2.2 IPSEC

Basics zu IPSec

Erklärungen zu den Subprotokollen:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

Erklärungen zu Operationmodes:

- transport mode
- tunnel mode

3 Verwandte Arbeiten

- Einleitung in TCP-over-DTLS, der Ansatz den die Autoren versuchen zu verbessern.
- Aufzeigen der Probleme und der Punkte an denen die Verbesserungen ansetzen.

4 PCTCP

4.1 Kernel-mode per-circuit TCP

- Konzept der Verbindung innerhalb des netzwerks
- Illustrationen
- Vorteile des Deployments (Funktion des heterogenen Netzwerks (Plain tor + PCTCP))
- Änderung am Verbindungsaufbau
- Resultierende Probleme

4.2 IPSec in PCTCP

- Lösung der Probleme mit IPSec
- Alternative Lösungen

5 Fazit