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

Manuel Schneider

Albert Ludwigs Universität - Institut für Informatik

18. Dezember 2014

Motivation

Übersicht

Tor
Grundlagen

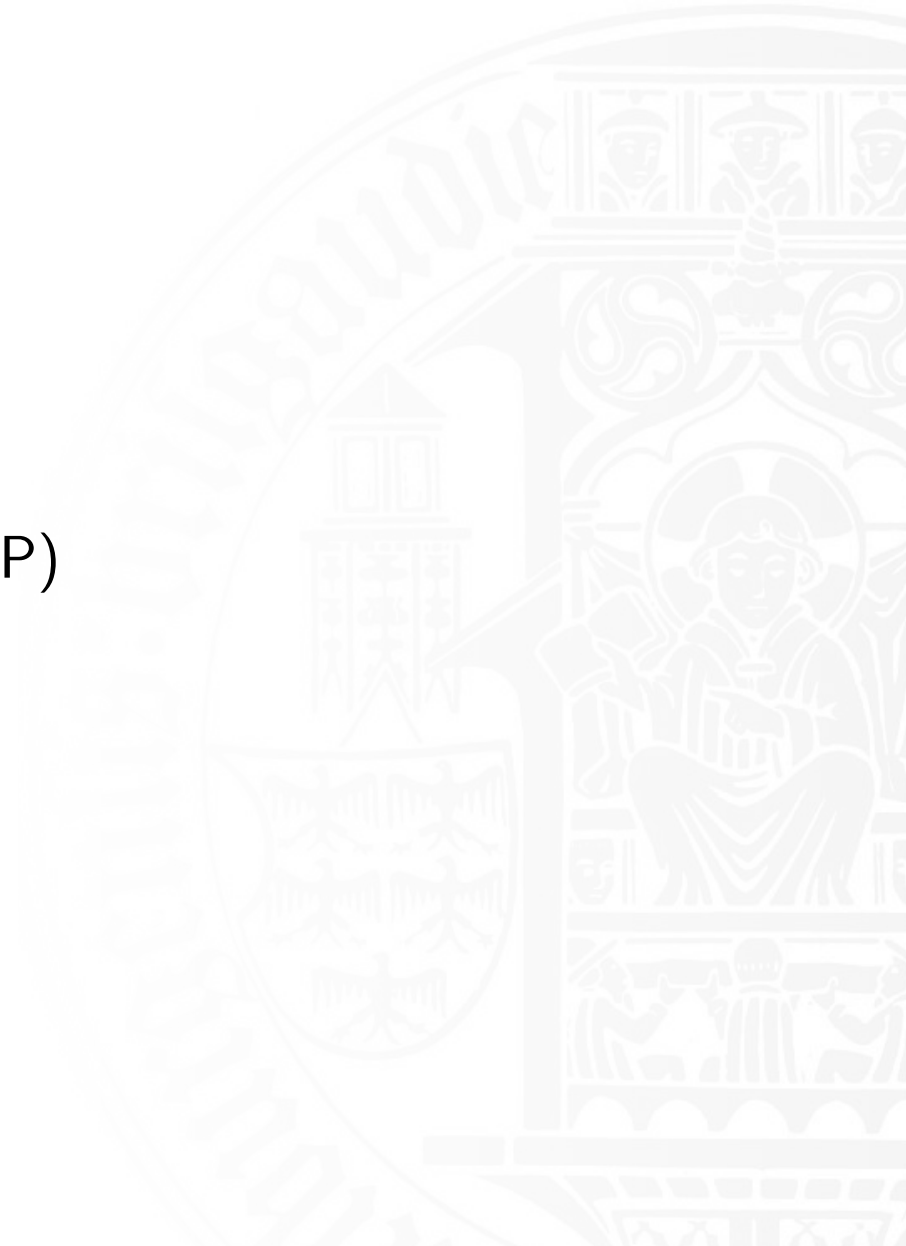
Basics zu Tor (Ausmaß in der Präsentation abhäangig von Dirk). Reduziert sich minimal auf die Performancemängel und die Transportlayergeschich- te, die für diese Arbeit besonders von Belang ist. Themen:

IPSec
Grundlagen

- Ipsec generell (Was warum wie wo)

Subprotokolle
Grundlagen/IPSec

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



Operationmodi
Grundlagen/IPSec

- transport mode
- tunnel mode

Übersicht

TCP-over-DTLS
Verwandte Arbeiten

-Einleitung in TCP-over-DTLS
-Wo wird es verwendet0

TCP-over-DTLS
Verwandte Arbeiten

-Funktionsweise

Probleme beim TCP-over-DTLS

Verwandte Arbeiten

-Aufzeigen der Probleme und der Punkte an denen die Verbesserungen ansetzen.
-Einleitung in das PCTCP

Übersicht

PCTCP
IPSec

-Einleitung in PCTCP. Wo wird es eingesetzt? Anlehnung an DTLS

Konzept
PCTCP/Kernel-mode per-circuit TCP

- Konzept der Verbindung innerhalb des netzwerks
- Schön mit Illustration

Notwendige Änderungen
PCTCP/Kernel-mode per-circuit TCP

- Änderung am Verbinungsaufbau

Deployment
PCTCP/Kernel-mode per-circuit TCP

- Vorteile des Deployments (Funktion des heterogenen Netzwerks (Plain tor + PCTCP)

Probleme
PCTCP/Kernel-mode per-circuit TCP

- Resultierende Probleme

- Lösung der Probleme mit IPSec

- Alternative Lösungen

Übersicht

Evaluation
IPSec in PCTCP

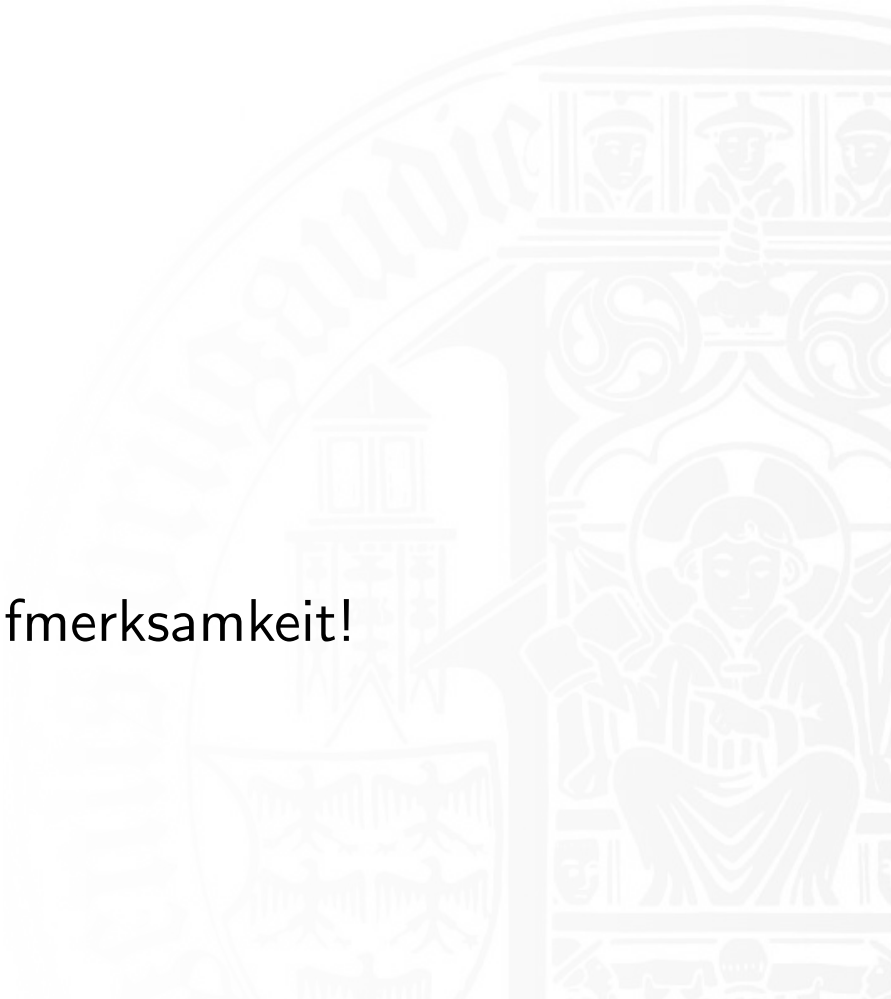
1 Grundlagen

2 Verwandte Arbeiten

3 PCTCP

4 Evaluation

Vielen Dank für die Aufmerksamkeit!



M. AlSabah and I. Goldberg.

PCTCP: Per-Circuit TCP-over-IPSec Transport for Anonymous Communication Overlay Networks.
Technical report, Centre for Applied Cryptographic Research (CACR) at the University of Waterloo, September 2013.

T. Dierks and E. Rescorla.

The Transport Layer Security (TLS) Protocol Version 1.2.
RFC 5246, Internet Engineering Task Force, August 2008.

S. Kent and R. Atkinson.

Security Architecture for the Internet Protocol.
RFC 2401, Internet Engineering Task Force, November 1998.

M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, and L. Jones.

SOCKS Protocol Version 5.
RFC 1928, Internet Engineering Task Force, März 1996.

J. Reardon and I. Goldberg.

Improving Tor Using a TCP-over-DTLS Tunnel.
Technical report, Centre for Applied Cryptographic Research (CACR) at the University of Waterloo, September 2009.