

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

Manuel Schneider

Albert Ludwigs Universität - Institut für Informatik

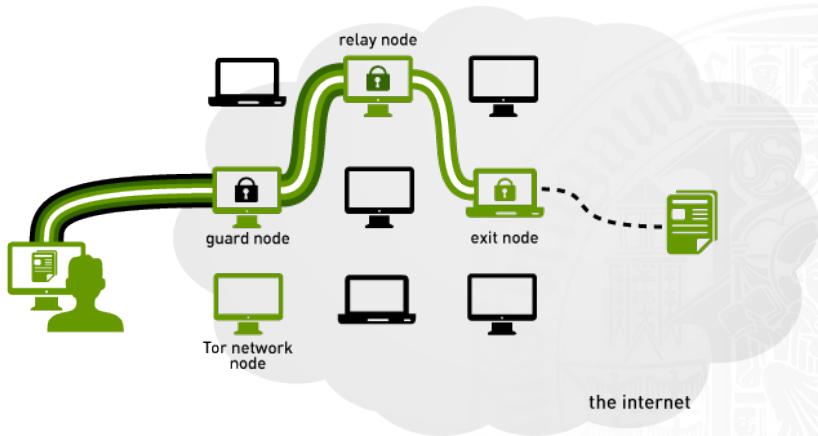
20. Januar 2015

Motivation

gfsdfs

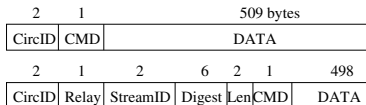


TOR - Architektur/Terminologie



Das Große und Ganze Onion Routing, Cell, Circuit, Stream, Onion Router,- Proxy

Cells - Das TOR Transportmittel



Quelle: [2]

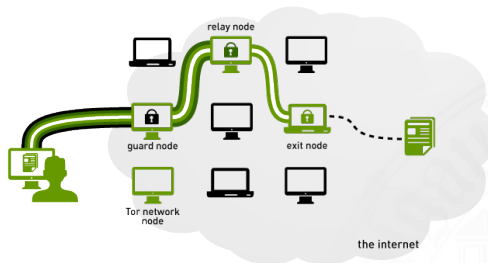
Control Cell

- Dienen dem Management der Circuits
 - Aufbau, Abbau, Keepalive
- Werden vom Onion Router interpretiert, der sie empfängt

Relay Cell

- Zur Weiterleitung der Daten auf dem Circuit
 - Zusätzlicher Relay Header
-
- Beide haben Circuit Identifier

Circuits - Die TOR Transportwege



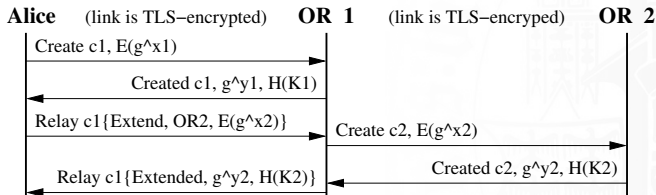
- Pfade im Netzwerk entlang welcher die Cells gesendet werden
- Werden Hop-by-hop aufgebaut
 - Mit jedem Knoten wird ein Schlüssel ausgehandelt
- Üblicherweise drei: Entry, Middle-, Exit Node
- Jeder Hop hat einen Circuit Identifier
- Werden nach einem Zeitintervall oder Fehler gewechselt
- Werden auf Vorrat angelegt (Performace)

Circuits - Inkrementeller Aufbau

- OP holt Informationen beim Directory Server
 - Router descriptor: Public Keys, Bandbreite, Adresse der OR
- Onion Proxy wählt anhand Exit Policies eine Exit Node
- Danach weitere Onion Router, sodass jeder nur einmal vorkommt

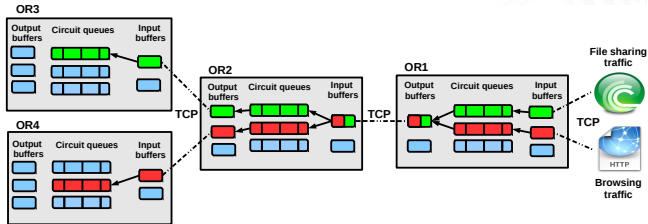
Circuits - Inkrementeller Aufbau

- **Create** Control Cell an OR 1
 - Enthält Diffie-Hellman Handshake
 - OR 1 kennt nun den Schlüssel
 - Circuit Identifier wurde von Alice festgelegt
- **Created** Control Cell zurück (OP kennt nun den Schlüssel)
 - Alice kennt nun den Schlüssel



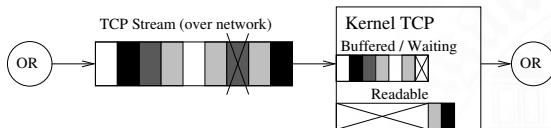
Quelle: [2]

Cross Circuit Interference Problem.



Quelle: [1]

Head On Line Blocking



Quelle: [4]

Internet Protocol Security (IPSec)

- Arbeitet auf Vermittlungsschicht
- Stellt Schutzziele sicher
 - Vertraulichkeit
 - Authentizität
 - Integrität
- Umfasst Protokolle für eine gesicherte Kommunikation
 - Authentication Header (AH)
 - Encapsulating Security Payload (ESP)
- Je zwei Betriebsmodi
 - Transport Modus
 - Tunnel Modus

IPSec - Protokolle

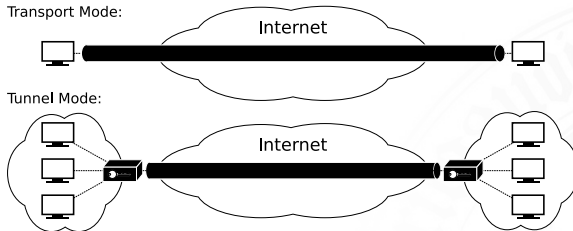
IP Authentication Header (AH)

- Stellt Authentizität und Integrität der Daten sicher
- Authentifiziert Sender
- Schützt gegen Replay-Angriffe
- Inkompatibel mit Network Address Translation!

IP Encapsulating Security Payload (ESP)

- Selbes Featureset wie AH
- Stellt zusätzlich Vertraulichkeit der Daten sicher

IPSec - Betriebsmodi

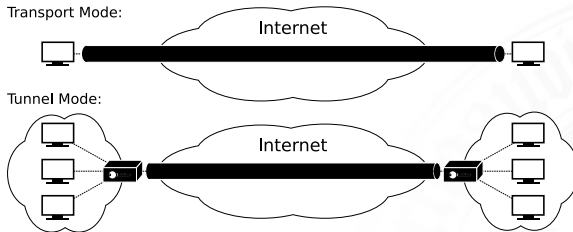


Quelle: www.wikimedia.com

Transport Modus

- IP Header bleibt unberührt, auch bei ESP

IPSec - Betriebsmodi

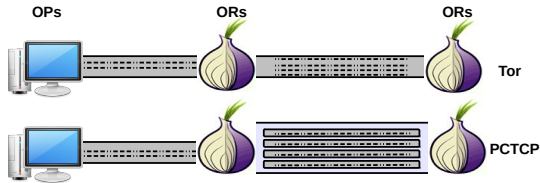


Quelle: www.wikimedia.com

Tunnel Modus

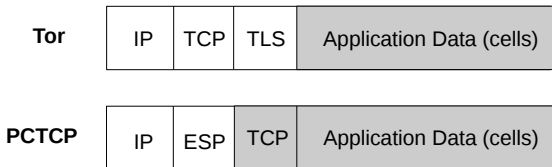
- Zusätzlicher IP Header

PCTCP Design



Vergleich des Designs zwischen Standard-Tor und PCTCP.

IPSec in PCTCP



Vergleich der Inter Onion Router Pakete zwischen Standard-TOR und PCTCP. Grau schattierte Teile sind verschlüsselt.

Quelle:[1]

PCTCP - Circuit construction



Ease of deployment

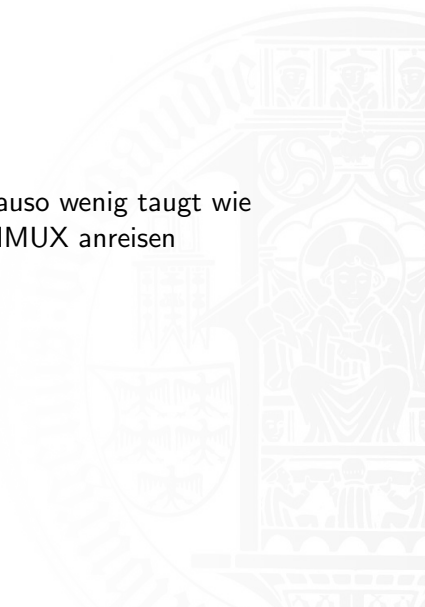


Socket Exhaustion Attacks



Ausblick

Kurz sagen, dass PCTCP beinahe genauso wenig taugt wie TCPoverDTLS und warum. Vielleicht IMUX anreisen



Reference

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.



Roger Dingledine, Nick Mathewson, and Paul Syverson.

Tor: The second-generation onion router.

In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13, SSYM'04*. USENIX
Association, 2004.



John Geddes, Rob Jansen, and Nicholas Hopper.

IMUX: Managing Tor Connections from Two to Infinity, and Beyond.

Technical report, Centre for Applied Cryptographic Research (CACR) at the University of Waterloo,
November 2014.



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.



R. Ringledine and S. Murdoch.

Performance Improvements on Tor or, Why Tor is slow and what we're going to do about it.
März 2009.