Connection ID

Hannes Tschofenig, Eric Rescorla, Thomas Fossati
Overview

CID specified for DTLS 1.2
draft-ietf-tls-dtls-connection-id-06

CID specified for DTLS 1.3
draft-ietf-tls-dtls13-32

New: Return Routability Check
draft-tschofenig-tls-dtls-rrc-00
Problem Description (1/4)
Amplification attack problem if single request triggers large response
Adversary

Client

Server

Key & algorithm parameters

Rewrite

Security Parameter Database

Void
Problem Description (4/4)

Adversary

Key & algorithm parameters

Security Parameter Database

Client

Server
Proposed Resolution

• Enhanced security consideration section to discuss DoS risk and suggests to only update IP address if no replay has happened.
  • Extra text in PR #70
• For asymmetric traffic patterns we suggest to perform a return routability check. This check can happen at the application layer or be done at the DTLS layer.
  • New draft with RRC to add return routability check message to DTLS 1.2 and DTLS 1.3