Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis M.Sc.

IDP

Performance Analysis of Transport Layer Security

Motivation

Transport layer protocols aim to implement application to application communication in either a stateful or stateless manner. Because of its properties, UDP and UDP-based protocols are simple to implement while achieving good performance results. Stateful protocols, especially when also offering cryptographic properties, remain a challenge for modern high-performance software packet processing frameworks.

In this thesis we want to have a closer look at the Datagram Transport Layer Security (DTLS) protocol [RFC 6347]. In short, it provides the properties of TLS – which is typically used for securing TCP connections for applications such as HTTPS or OpenVPN – for UDP. As TLS however requires additional guarantees that are not provided by UDP (packet order, guaranteed packet arrival), DTLS has small changes to overcome these problems. As a result, a minimal amount of shared state, primarily for the handshake, is introduced on both end hosts of a DTLS connection.

These properties – the simplicity and the minimal shared state – make DTLS an interesting candidate to be implemented as first stateful protocol with cryptographic properties in our libmoon packet processing framework. There are several frameworks available supporting DTLS, such as OpenSSL, OpenVPN, mbed TLS. Your job is to analyze, select, and port one of these frameworks to libmoon. Due to the enhanced packet processing capabilities of libmoon we expect near line rate performance (10 Gbit/s) for a reasonably priced server system.

The thesis will be part of the project ”Leistungszentrum Sichere Vernetzte Systeme” a collaboration between TUM and the Frauenhofer Institutes AISEC, EMFT and ESK.

Tasks

- Study existing DTLS implementations (e.g. OpenSSL, OpenVPN, mbed TLS)
- Analyze the requirements of the DTLS protocol
- Implement/port the protocol in/onto libmoon:
  - Protocol headers
  - Protocol specific state machines
  - Cryptographic algorithms
- Perform black/white box performance measurements

If you are interested or have questions, please feel free to contact us!

Contact

Dominik Scholz scholz@net.in.tum.de
Sebastian Gallenmüller gallenmu@net.in.tum.de