Abstract

In 2000, the Signaling Transport (SIGTRAN) working group of the IETF defined the Stream Control Transmission Protocol (SCTP) as a new transport protocol. SCTP is a new multi-purpose reliable transport protocol. Due to its various features and easy extensibility it is a valid option not only for already standardised applications but also in many new application scenarios. SCTP has several advantages over TCP and UDP.

The analysis of already standardised as well as potential SCTP application scenarios clearly indicates that secure end-to-end transport is one of the crucial requirements for SCTP in the future. Up to now there exist two standardised SCTP security solutions which are called TLS over SCTP [37] and SCTP over IPSec [12].

The goal of this thesis was to evaluate existing SCTP security solutions and find an optimised and efficient security solution. Several drawbacks of the standardised SCTP security solutions identified during the analysis are mainly related to features distinguishing SCTP from TCP and UDP. To avoid these drawbacks a new security solution for SCTP, called Secure SCTP (S-SCTP), is proposed which integrates the cryptographic functions into SCTP.

One main requirement was that S-SCTP should be fully compatible with standard SCTP while additionally providing strong security i.e. data confidentiality, integrity and authentication. This also means that all features, options and extensions available for standard SCTP have to be supported. Furthermore, S-SCTP should have advantages with respect to performance over all parameter ranges of SCTP and be user-friendly.

To specify the S-SCTP protocol extension several new control messages and new message parameters have been defined. Furthermore, procedures for initialisation, rekeying, and termination of secure sessions have been specified and modelled in SDL.

Based on an SCTP implementation available in our group and an open source implementation of TLS, TLS over SCTP and S-SCTP have been implemented. These implementations as well as an SCTP over IPSec configuration were used to do comparative performance studies in a lab testbed.

These experiments show that the S-SCTP concept achieves its design goals. It supports all features and current extensions of SCTP. Furthermore, it avoids the inefficiencies of the other solutions over a wide range of application scenarios and protocol parameter settings.

Keywords: SCTP, Transport Protocol, Security, TLS, IPSec, Performance Evaluation
Schlagworte: SCTP, Transportprotokoll, Sicherheit, TLS, IPSec, Leistungsbewertung