A Comparison of End-to-End Security Solutions for SCTP

Anna Brunstrom
Department of Computer Science
Karlstad University, Karlstad, Sweden
anna.brunstrom@kau.se

Stefan Lindskog
Centre for Quantifiable Quality of Service in Communication Systems
Norwegian University of Science and Technology, Trondheim, Norway
stefan.lindskog@q2s.ntnu.no

Introduction

- A comparison of three different end-to-end (E2E) security solutions for the stream control transmission protocol (SCTP) is presented
- The studied services are
  - SCTP over IPsec
  - TLS over SCTP
  - Secure socket SCTP (SS-SCTP)
- The comparison focuses on three main issues
  - packet protection
  - security differentiation
  - message complexity

Overview of SCTP

- SCTP is a general purpose transport protocol
  - provides a reliable and connection-oriented transport service
  - supports multiple concurrent data streams
  - supports the concept of multihoming
  - is message-oriented
- E2E security is, however, not provided by SCTP

SCTP over IPsec

- Packet protection is provided by either the authentication header (AH) protocol or the encapsulating payload protocol (ESP)
- The Internet key exchange (IKE) is used to dynamically establish security associations
- Security differentiation is applied on a per-association basis (an all-or-nothing approach)

TLS over SCTP

- TLS provides
  - key exchange and authentication
  - integrity protection
  - confidentiality protection
- Only data chunks are protected
- Security differentiation is applied on a per-connection basis (a (TLS) connection consists of two SCTP streams—one in each direction)
- Packet protection is provided by either the authentication header (AH) protocol or the encapsulating payload protocol (ESP)
- The Internet key exchange (IKE) is used to dynamically establish security associations
- Security differentiation is applied on a per-association basis (an all-or-nothing approach)

SS-SCTP

- AUTH provides integrity protection
- TLS is used for key exchange and authentication
- The socket extension provides confidentiality protection of data chunks
- Integrity protection is applied on a per-connection basis, and confidentiality protection on a per-message basis

Message Complexity

Unbundled data transfers

SCTP over IPsec
TLS over SCTP
SS-SCTP

Bundled data transfers (message size = 256 bytes)

SS-SCTP
SCTP over IPsec
TLS over SCTP

Conclusions and Future Work

- SCTP over IPsec offers the lowest degree of security differentiation, but the highest level of security
- TLS over SCTP produces the least communication overhead for large messages
- SS-SCTP provides the finest degree of security differentiation and produces the least communication overhead when messages are bundled
- The next step in the development of SS-SCTP is to finalize the prototype implementation, and then perform an experimental evaluation