IPSec Implementation for SCTP.
System Requirement Specifications.

Srivatsa R
Dept. CSE.
IIT Bombay. Mumbai
vatsa@cse.iitb.ac.in

Alok Sontakke
Dept. CSE.
IIT Bombay. Mumbai
aloksontakke@cse.iitb.ac.in

Aditya Kelkar
Dept. CSE.
IIT Bombay. Mumbai
adityak@cse.iitb.ac.in

September 10, 2004

Contents

1 Executive Overview

Traditionally in IP networks security was being provided by implementing encryption and authentication at the application layer. Examples of such applications include SSL (web access) SSH (terminal) etc. By implementing security at the IP layer an enterprise can ensure security not only for the applications that have security mechanisms but also for other security ignorant applications. This has been incorporated into IPv4/v6 protocols and is now broadly known as IPSec.

SCTP (Stream Control Transmission Protocol) is the latest addition to the TCP/IP protocol suite. SCTP is a transport layer protocol and works in the same level as UDP/TCP in the TCP/IP protocol suite. IPSec implementation requires a few changes in implementation to exploit the additional functionality provided by SCTP compared to TCP/UDP. This document describes the functional requirements for IPSec and IKE to facilitate their use in securing SCTP traffic.

2 Introduction

2.1 Introduction to IPSec

IPSec [2] is an IP level security mechanism that facilitates Authentication, Confidentiality and Key management between the endpoints of communication. Authentication mechanism ensures that the IP packet was indeed transmitted by the party identified as the source in the packet header. Confidentiality mechanism ensures that the packet has neither been altered no been read by a third party in transit and key management mechanism facilitates secure exchange of keys between the two parties trying to communicate.

2.1.1 IPSec Architecture

IPSec architecture includes standards for defining Authentication Header (AH) which corresponds to the authentication mechanism, Encapsulation of Security Payload (ESP) which corresponds to confidentiality and IKE (Internet Key Exchange) for key management.

2.1.2 Security Associations and Policies

A key concept that appears both in AH and ESP mechanisms in IPSec is the security association. A security association is a one-way relationship between a sender and a receiver that describes which mechanisms of the IPSec should be applied to the traffic being transmitted and how these mechanisms are to be applied. In practice two such associations are required to ensure security of traffic between sender and receiver in both directions. SAs are uniquely identified by Security Parameter Index (SPI), an IP Destination Address, and a security protocol (AH or ESP) identifier. The set of all SAs in an IPSec implementation is called Security Association Database (SAD). Apart for SAs, there is some additional information maintained in IPSec implementation to apply SAs to outgoing IP traffic, called Security Policy (SP). In its simplest form SP defines a subset of IP traffic and the corresponding SA to use for that subset. The set of all SPs in an IPSec implementation is called Security Policy Database (SPD).

2.2 Introduction to SCTP

The Stream Control Transmission Protocol (SCTP) [4] is a reliable transport protocol operating on top of a connectionless packet network such as IP. SCTP is designed to transport PSTN signaling messages over IP networks, but is capable of broader applications.

The main difference between TCP and SCTP relevant to this context is the delivery of user messages within multiple streams. SCTP provides the means for each SCTP endpoint to provide the other endpoint with a list of transport addresses through which that endpoint can be reached and from which it will originate SCTP packets. An SCTP connection (referred to as association) spans transfers over all of the possible source/destination combinations which may be generated from each endpoint's lists. Hence an SCTP connection is identified by a set of source and a set of destination IP addresses.

3 Scope of the document

This document describes the possible extensions/modifications required in an implementation of IPSec so that the security associations can be defined for multiple source or destination addresses. It also describes about possible extensions/modifications required for IKE for efficient key exchange between the source and destination.

4 Functional requirements for IPSec over SCTP

The following changes are required in an IPSec implementation [1] to be able to support SCTP.

- Extend existing implementations to use the SCTP source and destination port numbers as selectors in the SPD. Since the concept of a port, and its location in the transport header is protocol-specific, the IPsec code responsible for identifying the transport protocol ports has to be suitably modified.

- SCTP can negotiate sets of source and destination addresses that may be used in the context of a single association, the SPD implementation should be changed to accommodate this. The straightforward way is to create one SPD entry for each pair of source/destination addresses negotiated.

A better approach is to associate sets of addresses with the source and destination selectors in each SPD entry.

- Similarly, SAs may have multiple associated source and destination addresses. Thus an SA is identified by the extended triplet ({set of destination addresses}, SPI, Security Protocol). A lookup in the Security Association Database (SADB) using the triplet (Destination Address, SPI, Security Protocol), where Destination Address is any of the negotiated peer addresses, must return the same SA.

- SCTP allows for multiple source and destination network addresses associated with an SA. Therefore IKE [3] should efficiently negotiate these SAs. One approach is to negotiate one pair of IPSec SAs for each combination of source and destination addresses. This results in a large number of SAs, which is not efficient. Current IKE implementations support only this functionality. Such implementations should be modified appropriately for specifying multiple SAs for efficiency purposes.

5 Conclusion

This document explores methods by which current implementations for IPSec and IKE can be enhanced for use with SCTP and enumerates the ways to optimize some of those approaches as enumerated in the functional requirements.

References

[1] S. Bellovin et. al. Rfc-3554: On the use of stream control transmission protocol (sctp) with ipsec, 2003.

[2] S. Kent et. al. Rfc-2401: Security architecture for the internet protocol, 1998.

[3] D. Harkins. Rfc-2409: The internet key exchange (ike), 1998.

[4] R. Stewart. Rfc-2960: Stream control transmission protocol, 2000.