Software Requirement Specification for Implementation of IPsec support for SCTP over IPv4 and/or IPv6

R. Vamshi Krishna
vamshi@cse.iitb.ac.in
(04305015)

Kuldeep Gharat
kuldeep@cse.iitb.ac.in
(04305010)

Gautham Anil
gautham_anil@cse.iitb.ac.in
(04305013)

10^{th} September 2004

Contents

1 General Information

This document describes the specifications and requirements to implement IPsec support for SCTP over IPv4 and/or IPv6.

2 Introduction

Stream Control Transmission Protocol (SCTP) is a reliable transport protocol operating on top of a connection-less packet network such as IP. It provides a better alternative to existing transport layer protocols like TCP. SCTP supports multi-homing i.e allows maximum utilization of multiple ip-addresses available to host.

2.1 Advantages of SCTP over TCP

The advantage of SCTP over traditonal Transport Layer Protocols like RCP is that TCP suffers from head-of-the-line blocking. i.e one of the packets can block the entire queue.

SCTP overcomes this by defining what is called a stream. Data are logically grouped into streams and are assigned a stream identifier and a corresponding sequence number.

Only a packet that belongs to the same stream can block another packet of the same stream. Thus by defining multiple streams we are reducing the probability of the packet being blocked.

SCTP also is resitant to SYN flooding attack.

SCTP is more resistant to network line failures than TCP because it uses multiple lines(IP-IP path) between the same two nodes.

2.2 IPsec : IP Security

There exist many application-specific security mechanisms in many areas including electronic mail(S/MIME,PGP), client/server(Kerberos), Web access (Secure Sockets Layer), and others. However there are no mechanisms that cut across protocol layers. By implementing security at IP level, an organization can ensure secure networking not only for applications that have security mechanisms but also for those that do not have any. For this purpose IETF has introduced the IPsec protocol suite for authentication and confidentiality.

IPsec protocol suite is used to provide privacy and authentication services at the IP layer. IPsec is used to provide integrity and confidentiality. To dynamically establish IPsec Security Associations (SAs) , a key negotiation protocol such as IKE is used.

IPsec can be used to secure the SCTP traffic. This provides better security to data.

3 Motivation behind the Project

Traditional transport layer protocols like TCP supported only single ip address per host per connection. They never allowed multiple ip addresses of a machine(If a machine more than one NIC), to be part of the same connection.

SCTP allows multiple IP addresses from the same host to be aprt of the connection and in the process increasing the efficiency. Thus data could be sent concurrently over different IP addresses pairs between the same two hosts.

But this required a coreresponding change in the IPsec which so far only supported single IP address per association. Also the Security Policy Database (SPD), must be similarly modified.

Also to be considered is the fact that one of the hosts might not support address lists(multiple addresses) and hence care must be taken for this situation.

4 Implementation Issues

The Linux kernel already supports the new protocol. But currently the support is for IPv4. Gradually the focus will shift towards IPv6.

The Linux kernel also supports IPsec and has IPsec implementations for many of the existing protocols like TCP,UDP etc.. Thus as SCTP is much similar to the existing protocols, there will be lesser difficulty in the proposed IPsec support for SCTP in the Linux kernel.

To implement the above mentioned support, we must the extend the existing implementation to support a list of adresses. For this the IANA has assigned the ID 2 for Id type ID_LIST. Also we must allow for multiple quick mode connections in case the destination does not yet support list of addresses.

The linux kernel implementation is to be extended to support he following: 1. Corresponding entries for SCTP port numbers as SCTP selectors in SPD. 2. Support for list addresses. 3. Incase the destination does not list addresses then switch over to multiple quick modes.

The implementation is targeted as a linux kernel module so as to allow for developmental changes to easily be effected.

References

[1] Harkins D. and D. Carrel. The Internet Key Exchange (IKE). RFC 2409, November 1998.

[2] Maughan D., Schertler M., Schneider M., and J. Turner. Internet Security Association and Key Management Protocol. RFC 2408, November 1998.

[3] Piper D. The Internet IP Domain of Interpretation for ISAKMPD. RFC 2407, November 1998.

[4] Stewart R., Xie Q., Morneault K., Sharp C., Schwarzbauer H., Taylor T., Rytina I., Kalla M., Zhang L., and V. Paxson. Stream Control Transmission Protocol. RFC 2960, October 2000.

[5] Kent S. and R. Atkinson. IP Authentication Header. RFC 2402, November 1998.

[6] Kent S. and R. Atkinson. IP Encapsulating Payload (ESP). RFC 2406, November 1998.

[7] Kent S. and R. Atkinson. Security Architecture for the Internet Protocol. RFC 2401, November 1998.