

Network Working Group  
Request for Comments: 3554  
Category: Standards Track

S. Bellovin  
J. Ioannidis  
AT&T Labs - Research  
A. Keromytis  
Columbia University  
R. Stewart  
Cisco  
July 2003

## On the Use of Stream Control Transmission Protocol (SCTP) with IPsec

### Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

### Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

### Abstract

This document describes functional requirements for IPsec (RFC 2401) and Internet Key Exchange (IKE) (RFC 2409) to facilitate their use in securing SCTP (RFC 2960) traffic.

### 1. Introduction

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

When SCTP is used over IP networks, it may utilize the IP security protocol suite [RFC2402][RFC2406] for integrity and confidentiality. To dynamically establish IPsec Security Associations (SAs), a key negotiation protocol such as IKE [RFC2409] may be used.

This document describes functional requirements for IPsec and IKE to facilitate their use in securing SCTP traffic. In particular, we discuss additional support in the form of a new ID type in IKE [RFC2409] and implementation choices in the IPsec processing to accommodate for the multiplicity of source and destination addresses associated with a single SCTP association.

### 1.1. Terminology

In this document, the key words "MAY", "MUST", "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [RFC-2119].

## 2. SCTP over IPsec

When utilizing the Authentication Header [RFC2402] or Encapsulating Security Payload [RFC2406] protocols to provide security services for SCTP frames, the SCTP frame is treated as just another transport layer protocol on top of IP (same as TCP, UDP, etc.)

IPsec implementations should already be able to use the SCTP transport protocol number as assigned by IANA as a selector in their Security Policy Database (SPD). It should be straightforward to 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. This, however is not enough to fully support the use of SCTP in conjunction with IPsec.

Since SCTP can negotiate sets of source and destination addresses (not necessarily in the same subnet or address range) that may be used in the context of a single association, the SPD should be able to accommodate this. The straightforward, and expensive, 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 (in the case of non-SCTP traffic, these sets would contain only one element). While this is an implementation decision, implementors are encouraged to follow this or a similar approach when designing or modifying the SPD to accommodate SCTP-specific selectors.

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.

### 3. SCTP and IKE

There are two issues relevant to the use of IKE when negotiating protection for SCTP traffic:

a) Since SCTP allows for multiple source and destination network addresses associated with an SCTP association, it MUST be possible for IKE to efficiently negotiate these in the Phase 2 (Quick Mode) exchange. The straightforward approach is to negotiate one pair of IPsec SAs for each combination of source and destination addresses. This can result in an unnecessarily large number of SAs, thus wasting time (in negotiating these) and memory. All current implementations of IKE support this functionality. However, a method for specifying multiple selectors in Phase 2 is desirable for efficiency purposes. Conformance with this document requires that implementations adhere to the guidelines in the rest of this section.

Define a new type of ID, ID\_LIST, that allows for recursive inclusion of IDs. Thus, the IKE Phase 2 Initiator ID for an SCTP association MAY be of type ID\_LIST, which would in turn contain as many ID\_IPV4\_ADDR IDs as necessary to describe Initiator addresses; likewise for Responder IDs. Note that other selector types MAY be used when establishing SAs for use with SCTP, if there is no need to use negotiate multiple addresses for each SCTP endpoint (i.e., if only one address is used by each peer of an SCTP flow). Implementations MUST support this new ID type.

ID\_LIST IDs cannot appear inside ID\_LIST ID payloads. Any of the ID types defined in [RFC2407] can be included inside an ID\_LIST ID. Each of the IDs contained in the ID\_LIST ID must include a complete Identification Payload header.

The following diagram illustrates the content of an ID\_LIST ID payload that contains two ID\_FQDN payloads.

```

 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
! Next Payload !   RESERVED   !           Payload Length           !
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
!   ID Type    ! Protocol ID !           Port                      !
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
! Next Payload !   RESERVED   !           Payload Length           !
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
!   ID Type    ! Protocol ID !           Port                      !
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
~                               FQDN 1 Identification Data                               ~
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
! Next Payload !   RESERVED   !           Payload Length           !
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
!   ID Type    ! Protocol ID !           Port                      !
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
~                               FQDN 2 Identification Data                               ~
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

The Next Payload field in any of the included IDs (for FQDN 1 and FQDN 2) MUST be ignored by the Responder. The Payload Length, ID Type, Protocol ID, and Port fields of the included Payloads should be set to the appropriate values. The Protocol ID and Port fields of the ID\_LIST Payload should be set to zero by the Initiator and MUST be ignored by the Responder.

Different types of IDs (e.g., an ID\_FQDN and an ID\_IPV4\_ADDR) can be included inside the same ID\_LIST ID. If an ID type included in an ID\_LIST ID payload is invalid in the context the ID\_LIST ID is used, the whole ID\_LIST should be considered to be at fault, e.g., if an ID\_LIST ID payload that contains an ID\_FQDN and an ID\_IPV4\_ADDR is received during an IKE Quick Mode exchange, the Responder should signal a fault to the Initiator and stop processing of the message (the same behavior it would exhibit if simply an ID\_FQDN was received instead).

The IANA-assigned number for the ID\_LIST ID is 12.

b) For IKE to be able to validate the Phase 2 selectors, it must be possible to exchange sufficient information during Phase 1. Currently, IKE can directly accommodate the simple case of two peers talking to each other, by using Phase 1 IDs corresponding to their IP addresses, and encoding those same addresses in the SubjAltName of the certificates used to authenticate the Phase 1 exchange. For more complicated scenarios, external policy (or some other mechanism) needs to be consulted, to validate the Phase 2 selectors and SA parameters. All addresses presented in Phase 2 selectors MUST be validated. That is, enough evidence must be presented to the

Responder that the Initiator is authorized to receive traffic for all addresses that appear in the Phase 2 selectors. This evidence can be derived from the certificates exchanged during Phase 1 (if possible); otherwise it must be acquired through out-of-band means (e.g., policy mechanism, configured by the administrator, etc.).

In order to accommodate the same simple scenario in the context of multiple source/destination addresses in an SCTP association, it **MUST** be possible to:

- 1) Specify multiple Phase 1 IDs, which are used to validate Phase 2 parameters (in particular, the Phase 2 selectors). Following the discussion on an ID\_LIST ID type, it is possible to use the same method for specifying multiple Phase 1 IDs.
- 2) Authenticate the various Phase 1 IDs. Using pre-shared key authentication, this is possible by associating the same shared key with all acceptable peer Phase 1 IDs. In the case of certificates, we have two alternatives:
  - a) The same certificate can contain multiple IDs encoded in the SubjAltName field, as an ASN.1 sequence. Since this is already possible, it is the preferred solution and any conformant implementations **MUST** support this.
  - b) Multiple certificates **MAY** be passed during the Phase 1 exchange, in multiple CERT payloads. This feature is also supported by the current specification. Since only one signature may be issued per IKE Phase 1 exchange, it is necessary for all certificates to contain the same key as their Subject. However, this approach does not offer any significant advantage over (a), thus implementations **MAY** support it.

In either case, an IKE implementation needs to verify the validity of a peer's claimed Phase 1 ID, for all such IDs received over an exchange.

Although SCTP does not currently support modification of the addresses associated with an SCTP association (while the latter is in use), it is a feature that may be supported in the future. Unless the set of addresses changes extremely often, it is sufficient to do a full Phase 1 and Phase 2 exchange to establish the appropriate selectors and SAs.

The last issue with respect to SCTP and IKE pertains to the initial offer of Phase 2 selectors (IDs) by the Initiator. Per the current IKE specification, the Responder must send in the second message of the Quick Mode the IDs received in the first message. Thus, it is assumed that the Initiator already knows all the Selectors relevant to this SCTP association. In most cases however, the Responder has more accurate knowledge of its various addresses. Thus, the IPsec Selectors established can be potentially insufficient or inaccurate.

If the proposed set of Selectors is not accurate from the Responder's point of view, the latter can start a new Quick Mode exchange. In this new Quick Mode exchange, the roles of Initiator and Responder have been reversed; the new Initiator MUST copy the SA and Selectors from the old Quick Mode message, and modify its set of Selectors to match reality. All SCTP-supporting IKE implementations MUST be able to do this.

#### 4. Security Considerations

This document discusses the use of a security protocol (IPsec) in the context of a new transport protocol (SCTP). SCTP, with its provision for mobility, opens up the possibility for traffic-redirection attacks whereby an attacker X claims that his address should be added to an SCTP session between peers A and B, and be used for further communications. In this manner, traffic between A and B can be seen by X. If X is not in the communication path between A and B, SCTP offers him new attack capabilities. Thus, all such address updates of SCTP sessions should be authenticated. Since IKE negotiates IPsec SAs for use by these sessions, IKE MUST validate all addresses attached to an SCTP endpoint either through validating the certificates presented to it during the Phase 1 exchange, or through some out-of-band method.

The Responder in a Phase 2 exchange MUST verify the Initiator's authority to receive traffic for all addresses that appear in the Initiator's Phase 2 selectors. Not doing so would allow for any valid peer of the Responder (i.e., anyone who can successfully establish a Phase 1 SA with the Responder) to see any other valid peer's traffic by claiming their address.

#### 5. IANA Considerations

IANA has assigned number 12 for ID\_LIST (defined in Section 3) in the "IPSEC Identification Type" registry from the Internet Security Association and Key Management Protocol (ISAKMP) Identifiers table.

## 6. Intellectual Property Rights Notice

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

## Normative References

- [RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
- [RFC2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.
- [RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.
- [RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMPD", RFC 2407, November 1998.
- [RFC2408] Maughan, D., Schertler, M., Schneider, M. and J. Turner, "Internet Security Association and Key Management Protocol", RFC 2408, November 1998.
- [RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.
- [RFC2960] 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.

## Authors' Addresses

Steven M. Bellovin  
AT&T Labs - Research  
180 Park Avenue  
Florham Park, New Jersey 07932-0971

Phone: +1 973 360 8656  
EMail: [smb@research.att.com](mailto:smb@research.att.com)

John Ioannidis  
AT&T Labs - Research  
180 Park Avenue  
Florham Park, New Jersey 07932-0971

EMail: [ji@research.att.com](mailto:ji@research.att.com)

Angelos D. Keromytis  
Columbia University, CS Department  
515 CS Building  
1214 Amsterdam Avenue, Mailstop 0401  
New York, New York 10027-7003

Phone: +1 212 939 7095  
EMail: [angelos@cs.columbia.edu](mailto:angelos@cs.columbia.edu)

Randall R. Stewart  
24 Burning Bush Trail.  
Crystal Lake, IL 60012

Phone: +1-815-477-2127  
EMail: [rrs@cisco.com](mailto:rrs@cisco.com)



## Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

