

Protecting SCTP with IPsec

Steven M. Bellovin

`smb@research.att.com`

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

SCTP — Simple Control Transmission Protocol

- Product of SIGTRANS working group.
 - Originally intended to carry PSTN signaling messages, but much broader. (For example, it permits multiple streams to be multiplexed in a single connection.)
 - Resists SYN flooding-style attacks via cookies.
- ⇒ Either or both ends of *connection* can be multihomed.

How Can IPsec Support Multihoming?

- Current DOI supports single addresses and address ranges.
- It also supports FQDNs, but is silent on handling multi-homed hosts.
- Must extend this to have a “list” type.
- Must add that type to certificates, too, or be able to send multiple certificates in the negotiation.

Can We Set Up Multiple SAs?

- These endpoints *will* be multihomed.
- Switch-over *must* be rapid.
- Must negotiate $m \times n$ SAs up front. Expensive...

What About Multiple Quick Modes?

- In principle, we can, but it's still expensive.
- Each of the $m \times n$ SAs will require three messages.
- If PFS is desired, it becomes very expensive.
- Besides, this is a single connection; we don't need multiple keys.

Minor Issue

- Must have SPD entries for SCTP protocol.
- Fortunately, port number syntax/semantics match TCP and UDP's.

Recommendation

- A new RFC should add address lists to the DOI, and clarify behavior for FQDNs.
- In the interim, IKE implementations should provide a convenient UI and API to permit multiple Quick Modes for each address pair.
- Implementations that support address lists should automatically fall back to multiple Quick Modes if the other side doesn't support lists.