Flemham Park, NJ 07932
AT&T Labs Research
973-360-8656
sm@research.att.com

Steven M. Bellovin

Protecting SCTP with IPsec

IPsec/SCTP
Either or both ends of connection can be multihomed.

- Resists SYN flooding-style attacks via cookies.
- Resist a single connection.
- Originally intended to carry PSTN signaling messages, but much broader. (For example, it permits multiple streams to be multiplexed in a single connection.)

Product of SIGTRAWS working group.

**SCTP — Simple Control Transmission Protocol**
How can IPsec support multihoming?

- Must extend this to have a "list" type.
- Must add that type to certificate, too, or be able to send multiple certificates in the negotiation.
- Current DOI supports single addresses and address ranges.
- It also supports FQDNS, but is silent on handling multi-homed hosts.
Can we set up multiple SAS?

- Must negotiate m x n SAS upfront. Expensive...
- Switch-over must be rapid.
- These endpoints will be multihomed.
In principle, we don’t need multiple keys.

Each of the m x n SAs will require three messages. If PFS is desired, it becomes very expensive.

Besides, this is a single connection, so we don’t need multiple keys. In principle, we can, but it’s still expensive.

What About Multiple Quick Modes?
IPsec/SCTP

Minor Issue

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

Recommendation