IPsec Issues for SCTP

Steven M. Bellovin

AT&T Labs Research
973-360-8656
smb@research.att.com

Florham Park, NJ 07932

Steven M. Bellovin — March 29, 2000
IPsec Issues

Protecting SCTP with IPsec

- Minor issue — must have policy rules for SCTP.
- Major issue — multihomed connections not properly supported.
- IPsec proper can do handle it, but IKE cannot.
Each IPsec-protected packet contains an SA identifier (the security parameter index (SPI)).

SAs are also linked to a security policy database (SPD) that specifies what packets to encrypt.

Note carefully: SAs are unidirectional.

Each security association (SA) has an associated key, cryptographic algorithms, etc.
IKE (Internet Key Exchange) negotiates pairs of SAs.

Endpoint identifiers in IKE are host addresses, subnets, or ranges.

We could do multiple IKE exchanges, but:
(a) it would be expensive;
(b) we'd get $m \times n$ SAs; and (c) we don't really need or want different keys for the different host addresses.
Proposed Solution

- Modify IKE to permit lists of addresses as endpoint identifiers.
- Must also modify certificates to handle that.
- Until that is common, IKE implementations should fall back to setting up multiple SAs when talking to older versions that don't support address lists.