(Ab?) Using IPsec for SEND

- Steven M. Bellovin
- smb@research.att.com
The Problem with IPsec

- Where do the keys come from?
- Use IKE? How can you negotiate without MAC addresses?
Reserved IPsec SPIs

- The ESP and AH RFCs (2406, section 2.1, and 2402, section 2.4) reserve SPIs 1-255 for special key management techniques.
- One original concept for this range was simple public key-protected packets.
- Let's go there.
I am *not* proposing a full protocol.
I am suggesting an approach that might work.
Packet Format

- ESP or AH header with special SPI
- Normal ND response packet
- Timestamp
- Digital signature of SHA1 of <ND,timestamp>
- "Certificate"
Recipient needs some way to securely associate a public key with the sender's IP address.

One answer is an address-based pki.

Not a PKI, a pki -- this one is small and local.

Could cryptographically generate IP address from public key.

63 bits isn't very many -- could an enemy precompute?

Use timestamp to nearest hour in the generation?
Challenges

- Replay protection -- will all nodes have clocks?
  - Add a "nonce" option to the ND solicit message? But that doesn't help the 63-bit problem.
- Certificates -- what about conference networks?
- What about RFC 3041-style addresses? Use the techniques suggested previously for address generation?