Selected Topics Regarding Protecting IP multicast data packets with IPsec

MSEC WG

Brian Weis

08/02/04

Topics

- IPsec Signatures draft

  draft-ietf-msec-ipsec-signatures-01.txt
- ESP Tunnel Mode vs. IP Multicast
- Anti-replay protection for multi-sender SAs

IPsec Signatures draft

- For a full presentation see the archived presentation:

  http://www.ietf.org/proceedings/03mar/slides/msec-4.pdf
- Summary of the draft: Alternative to an HMAC authentication tag.
  - Take a hash over the ESP or AH authenticated area
  - Encrypt the hash with an RSA private key
  - Put the ciphertext in the Integrity Check Value field
  - RSA public key is distributed by key management

What's the point?

- HMAC provides group authentication only.
- RSA signatures provide source origin authentication of the packet.

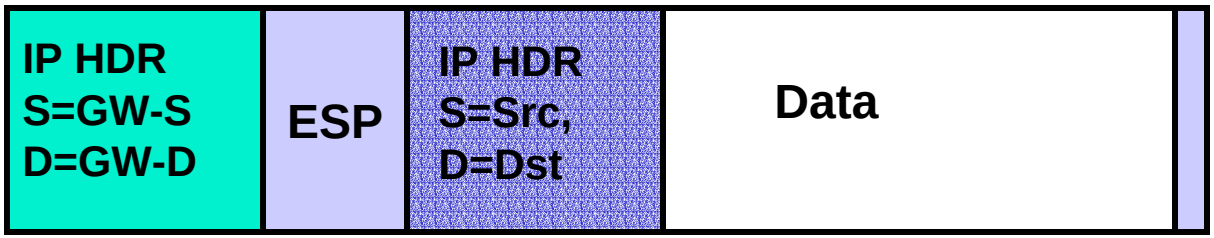
  "When you absolutely, positively, need to know who sent that packet"
- Useful for lower bandwidth data streams. E.g., signaling traffic.

Potential issues

- Invalid signatures can be a potential DoS issue.
  - If an application is at risk, then the recommendation is to encapsulate the SA in an AH or ESP SA with an HMAC
- Performance
  - Hardware cards are available, and supported by some kernels (e.g., OpenBSD)

ESP Tunnel Mode vs. IP Multicast

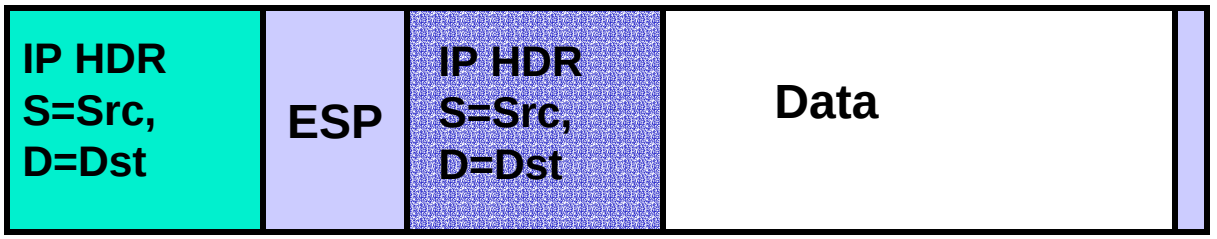
- An IPsec gateway “tunnels” an IP packet by placing gateway addresses on the IP packet.



- But if Dst is an IP multicast address, changing the address breaks multicast routing! You also lose the efficiencies of IP multicast.

Possible solutions

- Use transport mode
  - But IPsec gateways should not use transport mode: encapsulation of fragments is problematic.
- Use tunnel encapsulation, but preserve the original addresses
  - Multicast routing works as normal
  - Rfc2401bis rules are sufficiently broad so as to allow this behavior.



Best choice: Address Preservation

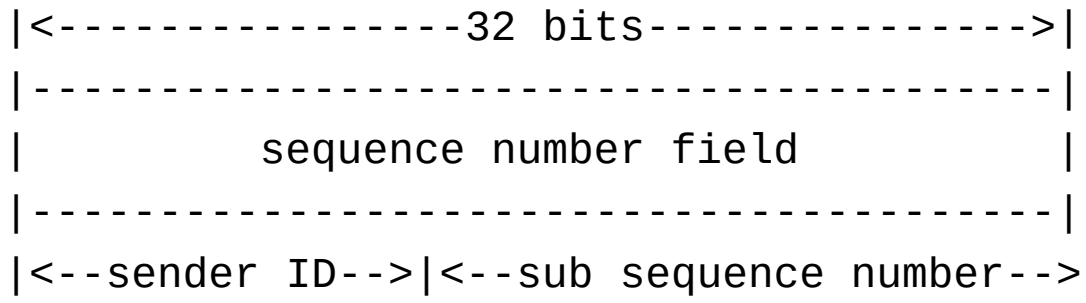
- We’ve long discussed the need for address preservation of IP multicast packets in MSEC, but never documented it.
- It needs to be documented for interoperability!

Anti-replay for multi-sender SAs

- Anti-replay for single-sender SAs follow normal IPsec semantics
  - Receivers maintain a replay window for the sender.
- A method of anti-replay for multi-sender SAs need to be standardized. Some options:
  - Partition the sequence number space
  - Multiple windows

Partition the sequence number space

- For example, as suggested by
  draft-zhao-ipsec-multi-sender-sa-00.txt



- But in practice, maintenance of the sender ID is tricky.

Multiple windows

- Receivers maintain a window per sender, indexed by source IP address.
- No sender ID namespace to maintain
- But there is a risk of using a lot of memory, if there are too many senders.

Proposed Steps

- Take IPsec signatures draft to WG last call
- Create a “son-of-MESP I-D describing these and other issues, but staying within the framework of rfc2401bis