Network Working Group
INTERNET DRAFT
Expire in six months

PIM Working Group
Editor,
Liming Wei
Redback Networks Inc.
July 14, 2000

Authenticating PIM version 2 messages
<draft-ietf-pim-v2-auth-01.txt>

Status of this Memo

Abstract

This draft specifies the use of IPSEC authentication header [KA98] to provide protocol message integrity protection and groupwise message origin authentication.

The text in this draft will be either incorporated into or referenced by the PIM version 2 protocol specifications.

1. Factors in authenticating PIM messages

Using authentication for PIM messages can protect routers from unwanted behaviors due to unauthorized or altered PIM messages. The extent of possible damage depends on the type of counterfeit messages accepted. When there is a breach in security, those messages that travel only one hop may affect a small number of routers or multicast groups,

while other multi-hop messages, such as the bootstrap messages, may affect a larger number of routers. For this reason, sometimes, fine grained controls uncommon in unicast protocols may be desired for different PIM message types. The following explains the impact by these multi-hop messages in more detail.

There are three main cases where a PIM router interacts with other routers on different subnets. The PIM messages involved are not changed or processed by routers in between the message originator and receiver:

1) The bootstrap router sends authoritative group-to-RP mappings to all other routers in the same PIM domain. If PIM routers accept bootstrap messages from non-authorized candidate BSRs, it can potentially disrupt multicast routing for the entire PIM domain.

2) Candidate RPs sending candidate RP advertisement messages to the BSR. The BSR needs to avoid advertising bogus group-to-RP mappings, which can lead to unpredictable routing state.

3) DRs sending Register messages to the RPs. The RPs need to ignore register messages from unauthorized PIM sources.

In some networks, it is sufficient to trust all routers equally, and let them all share the same secret for authentication. While other networks may be more sensitive to to the potential impact of a security breach in the first two cases above, and would want different mechanisms to restrict the set of routers capable of being a BSR or RP.

There is a fair number of security machineries from the IETF security working groups, and we try to adhere to the most stable and widely used solution. It is expected that the mechanism described in this note will be able to accommodate newer algorithms and solutions without redesigning the packet format.

2. Authentication Methods

When security is enabled, all PIM version 2 messages will carry an IPSEC authentication header (AH) [KA98]. This section specifies two message authentication methods based on manual key distributions. More general key management issues are outside of the scope of this specification. The authentication mechanism MUST support HMAC-MD5-96 [MG98][RFC1321] and HMAC-SHA-1-96 [SHA] security transformations. In the subsequent text, a key is assumed to be associated with the two standard transformations, unless explicitly declared otherwise.

2.1 "Equal Opportunity" Method

All routers within the domain use the same key for all PIM messages. As its name suggests, once a router gained the shared

secret, it gains the ability to conduct any PIM actions. This key is called the "equal opportunity" key.

This method is simple and effective in preventing unauthorized routers from participating in protocol actions.

2.2 "Differentiated Capabilities" Method

The most likely PIM routers requiring additional securities are the candidate bootstrap routers, and the candidate RPs. Such requirements may be due to administrative needs, e.g. by network design that covers pseudo-autonomous subdomains, or one that takes advantage of the security features to manage the evolution.

As in the previous method, all PIM routers in the same domain still share a single secret (the "equal opportunity" key) that is used to compute digests for PIM messages. Except, the candidate BSRs and RPs use two more keys to protect bootstrap and the candidate RP advertisement messages:

- All BSRs own an identical RSA [PKCS1] key pair, and uses the private key to sign an entire bootstrap message. The other routers only have the public key to verify the signature, and be assured that the bootstrap message was indeed originated from one of the candidate BSRs, and intact. These keys are called the "BSR private key" and "BSR public key" respectively.

- All RPs and BSRs share another symmetric key. No other routers have this key. This key is called "the RP key". For candidate RP advertisement the digest is only calculated with the RP key, instead of the equal opportunity key.

Clearly, this method is more flexible than the previous one, with the following advantages:

- Only authorized candidate BSRs can become a bootstrap router;

- Only the authorized candidate RPs can advertise their candidacy to the BSR;

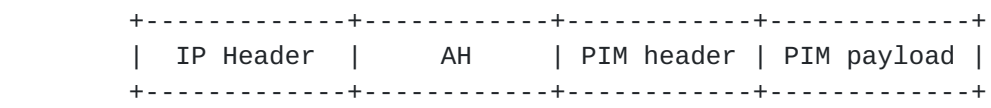
This makes it easier to support very large PIM domains where some PIM routers may be managed by multiple operators.

3.2 PIM message formats

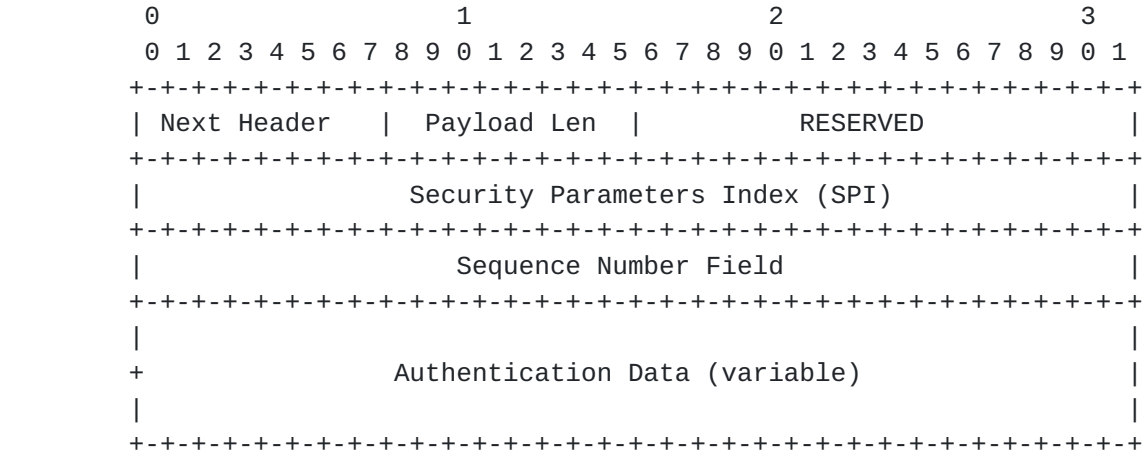
When security is enabled, all PIM message headers are appended an authentication header that is identical to the IPSEC Authentication Header (AH) defined in [KA98]. The IP header contains 51 in its Protocol

field.

The following illustrates how the AH is inserted in a PIM packet:



The following AH format is extracted from [KA98]. When generating a packet, for the purpose of calculating a digest or RSA signature, the authentication data field is zeroed. When verifying a received packet, the value in the authentication data field is saved before zeroing.



Next Header: 103, the value for PIM protocol.

Payload len: 4, when HMAC-MD5-96 or HMAC-SHA-1-96 is used (AH total length is 6 32-bit words).
Variable, depending on the RSA key length for bootstrap messages.

RESERVED: 0 when sent, ignored when received.

SPI: Security parameter index.
When the differentiated capability method is in use, separate SPIs are needed for the different security associations.

Sequence Number: Initialized to zero, incremented by one on each subsequent PIM message from the same originator.

Authentication Data: message digest

The sequence number field in the AH header MUST be filled in with a non-decreasing 32-bit number, the receivers SHOULD check the

sequence number and reject duplicate or old messages.

When the sequence number wraps around, newer messages may be rejected because the sequence numbers are smaller. Although it takes extremely long time to wrap around the sequence number (e.g. if on average 1 PIM message is sent in every second, it will take 136 years for the sequence number to wrap around.), to guard against sequence number wrap-around in abnormal conditions, each staticly configured SPI SHOULD have one or more rollover SPIs, to be used upon sequence number wrap around.

4. Security Considerations

The strength of message integrity protection and groupwise message origin authentication depends on the strength of the underlying security transformations used. According to [MG98][SHA][PKCS1], to date, there are no known attacks against these algorithms.

5. Acknowledgements

The ideas in this draft were contributed or instigated by Dino Farinacci, David Meyer, Dan Harkins, Tony Speakman, Cheryl Madson, Brian Weis, Achutha Rao and Tom Pusateri. Other members of the PIM working group also contributed to the discussions and ideas in this draft.

6. References

[KA98] Kent Stephen, Randall Atkinson, "IP Authentication Header", "draft-ietf-ipsec-auth-header-07.txt", July 1998

[RFC1321] R. Rivest, "MD5 Digest Algorithm", RFC1321, April 1992

[MG98] C. Madson, R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", "draft-ietf-ipsec-auth-hmac-md5-96-03.txt", Feb 1998

[PKCS1] RSA Laboratories, "PKCS#1: RSA Encryption Standard", Volume1.5, No. 1993

[SHA] C. Madson, R Glenn "The Use of HMAC-SHA-1-96 within ESP and AH", "draft-ietf-ipsec-auth-hmac-sha1-96-03.txt", Feb, 1998

6. Editor's address

Liming Wei

Redback Networks, Inc.
350 **Holger Way,**
San Jose, CA 95134
lwei@redback.com