Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: December 16, 2006

P. Savola
CSC/FUNET
J. Lingard

June 14, 2006

# Last-hop Threats to Protocol Independent Multicast (PIM)
## draft-savola-pim-lasthop-threats-02.txt



Abstract

An analysis of security threats has been done for some parts of the multicast infrastructure, but the threats specific to the last-hop ("Local Area Network") attacks by hosts on the PIM routing protocol have not been well described in the past. This memo aims to fill that gap.

Table of Contents

1. Introduction . . . . . 3
2. Last-hop PIM Vulnerabilities . . . . . 3
2.1. Nodes May Send Unauthorized PIM Register Messages . . . . 3
2.2. Nodes May Become Unauthorized PIM Neighbors . . . . . 4
2.3. Routers May Accept PIM Messages From Non-Neighbors . . . . 4
2.4. An Unauthorized Node May Be Elected as the PIM DR . . . . 4
2.5. A Node May Become an Unauthorized PIM Asserted Forwarder . . . . . 4
3. On-link Threats . . . . . 5
3.1. Denial-of-Service Attack on the Link . . . . . 5
3.2. Denial-of-Service Attack on the Outside . . . . . 5
3.3. Confidentiality, Integrity or Authorization Violations . . 6
4. Mitigation Methods . . . . . 6
4.1. Passive Mode for PIM . . . . . 7
4.2. Use of IPsec among PIM Routers . . . . . 7
4.3. IP Filtering PIM Messages . . . . . 7
4.4. Summary of Vulnerabilities and Mitigation Methods . . . . 8
5. Acknowledgements . . . . . 8
6. IANA Considerations . . . . . 9
7. Security Considerations . . . . . 9
8. References . . . . . 9
8.1. Normative References . . . . . 9
8.2. Informative References . . . . . 9
Authors' Addresses . . . . . 10
Intellectual Property and Copyright Statements . . . . . 11

## 1. Introduction

There has been some analysis of the security threats to the multicast routing infrastructures [I-D.ietf-mboned-mroutesec], some work on implementing confidentiality, integrity and authorization in the multicast payload [RFC3740], and also some analysis of security threats in IGMP/MLD [I-D.daley-magma-smld-prob], but no comprehensive analysis of security threats to PIM at the last-hop ("Local Area Network") links.

We define PIM last-hop threats to include:

- Nodes -- hosts or unauthorized routers -- using PIM to attack or deny service to hosts on the same link,
- Nodes using PIM to attack or deny service to valid multicast routers on the link, or
- Nodes using PIM (Register messages) to bypass the controls of multicast routers on the link.

A node originating multicast data can disturb existing receivers of the group on the same link, but this issue is not PIM-specific so it is out of scope. The impact on the outside of the link is described in [I-D.ietf-mboned-mroutesec].

This document analyzes the last-hop PIM vulnerabilities, formulates a few specific threats, proposes some potential ways to mitigate these problems and analyzes how well those methods accomplish fixing the issues.

It is assumed that the reader is familiar with the basic concepts of PIM.

## 2. Last-hop PIM Vulnerabilities

This section describes briefly the main attacks against last-hop PIM signalling, before we get to the actual threats and mitigation methods in the next sections.

The attacking node may be either a malicious host or an unauthorized router.

### 2.1. Nodes May Send Unauthorized PIM Register Messages

PIM Register messages are sent by unicast, and contain encapsulated multicast data packets. Malicious hosts or routers could also send

Register messages themselves, for example to get around rate-limits or to interfere with foreign Rendezvous Points (RPs) as described in [I-D.ietf-mboned-mroutesec].

The Register message can be targeted to any IP address, whether in or out of the local PIM domain. The source address may be spoofed unless spoofing has been prevented [RFC3704], to create arbitrary state at the RPs.

## 2.2. Nodes May Become Unauthorized PIM Neighbors

When PIM has been enabled on a router's "host" interface, any node can also become a PIM neighbor using PIM Hello messages. Having become a PIM neighbor in this way, the node is able to send other PIM messages to the router and may use those messages to attack the router.

## 2.3. Routers May Accept PIM Messages From Non-Neighbors

The PIM-SM specification recommends that PIM messages other than Hellos should not be accepted except from valid PIM neighbors. However, the specification does not mandate this, and so some implementations may be susceptible to attack from PIM messages sent by non-neighbors.

## 2.4. An Unauthorized Node May Be Elected as the PIM DR

The Designated Router (DR) on a LAN is responsible for Register-encapsulating data from new sources on the LAN, and for generating PIM Join/Prune messages on behalf of group members on the LAN.

A node which can become a PIM neighbor can also cause itself to be elected DR, whether or not the DR Priority option is being used in PIM Hello messages on the LAN.

## 2.5. A Node May Become an Unauthorized PIM Asserted Forwarder

With a PIM Assert message, a router can be elected to be in charge of forwarding all traffic for a particular (S,G) or (*,G) onto the LAN. This overrides DR behaviour.

The specification says that Assert messages should only be accepted from known PIM neighbors, and "SHOULD" be discarded otherwise. So, either the node must be able to spoof an IP address of a current neighbor, form a PIM adjacency first, or count on these checks being disabled.

The Assert Timer, by default, is 3 minutes; the state must be

refreshed or it will be removed automatically.

As noted before, it is also possible to spoof an Assert (e.g., using a legitimate router's IP address) to cause a temporary disruption on the LAN.

## 3. On-link Threats

The previous section described some PIM vulnerabilities; this section gives an overview of the more concrete threats exploiting those vulnerabilities.

### 3.1. Denial-of-Service Attack on the Link

The easiest attack is to deny the multicast service on the link. This could mean either not forwarding all (or parts of) multicast traffic from upstream onto the link, or not registering or forwarding upstream the multicast transmissions originated on the link.

These attacks can be done multiple ways: the most typical one would be becoming the DR through becoming a neighbor with Hello messages and winning the DR election. After that, one could for example:

- Not send any PIM Join/Prune messages based on the IGMP reports,
- Not forward or register any sourced packets, or
- Send PIM Prune messages to cut off existing transmissions because Prune messages are accepted from downstream interfaces even if the router is not a DR.

An alternative mechanism is to send a PIM Assert message, spoofed to come from a valid PIM neighbor or non-spoofed if a PIM adjacency has already been formed. For the particular (S,G) or (*,G) from the Assert message, this creates the same result as getting elected as a DR.

### 3.2. Denial-of-Service Attack on the Outside

It is also possible to perform Denial-of-Service attacks on nodes beyond the link, especially in environments where a multicast router and/or a DR is considered to be a trusted node.

In particular, if DRs perform some form of rate-limiting, for example on new Join/Prune messages, becoming a DR and sending those messages oneself allows one to subvert these restrictions: therefore rate-limiting functions need to be deployed at multiple layers as

described in [I-D.ietf-mboned-mroutesec].

In addition, any host can send PIM Register messages on their own, to whichever RP it wants; further, if unicast RPF mechanisms [RFC3704] have not been applied, the packet may be spoofed. This can be done to get around rate-limits, and/or to attack remote RPs and/or to interfere with the integrity of an ASM group. This attack is also described in [I-D.ietf-mboned-mroutesec].

### 3.3. Confidentiality, Integrity or Authorization Violations

Contrary to unicast, any node is able to legitimately receive all multicast transmission on the link by just adjusting the appropriate link-layer multicast filters. Confidentiality (if needed) must be obtained by cryptography.

If a node can get to be a DR, it is able to violate the integrity of any data streams sent by sources on the LAN, by modifying (possibly in subtle, unnoticeable ways) the packets sent by the sources before Register-encapsulating them.

If a node can form a PIM neighbor adjacency or spoof the IP address of a current neighbor, then if it has external connectivity by some other means other than the LAN, the node is able to violate the integrity of any data streams sent by external sources onto the LAN. It would do this by sending an appropriate Assert message onto the LAN to prevent the genuine PIM routers forwarding the valid data, obtaining the multicast traffic via its other connection, and modifying those data packets before forwarding them onto the LAN.

In either of the above two cases, the node could operate as normal for some traffic, while violating integrity for some other traffic.

A more elaborate attack is on authorization. There are some very questionable models [I-D.hayashi-igap] where the current multicast architecture is used to provide paid multicast service, and where the authorization/authentication is added to the group management protocols such as IGMP. Needless to say, if a host would be able to act as a router, it might be possible to perform all kinds of attacks: subscribe to multicast service without using IGMP (i.e., without having to pay for it), deny the service for the others on the same link, etc. In short, to be able to ensure authorization, a better architecture should be used instead (e.g., [RFC3740]).

## 4. Mitigation Methods

This section lists some ways to mitigate the vulnerabilities and

threats listed in previous sections.

## 4.1. Passive Mode for PIM

The current PIM specification seems to mandate running the PIM Hello protocol on all PIM-enabled interfaces. Most implementations require PIM to be enabled on an interface in order to send PIM Register messages for data sent by sources on that interface or to do any other PIM processing.

As described in [I-D.ietf-mboned-mroutesec], running full PIM, with Hello messages and all, is unnecessary for those stub networks for which only one router is providing multicast service. Therefore such implementations should provide an option to specify that the interface is "passive" with regard to PIM: no PIM packets are sent or processed (if received), but hosts can still send and receive multicast on that interface.

## 4.2. Use of IPsec among PIM Routers

Instead of passive mode, or when multiple PIM routers exist on a single link, one could also use IPsec to secure the PIM messaging, to prevent anyone from subverting it. The actual procedures have been described in [I-D.ietf-pim-sm-v2-new] and [I-D.atwood-pim-sm-linklocal].

However, it is worth noting that setting up IPsec Security Associations (SAs) manually can be a very tedious process, and the routers might not even support IPsec; further automatic key negotiation may not be feasible in these scenarios either. A Group Domain of Interpretation (GDOI) [RFC3547] server might be able to mitigate this negotiation.

## 4.3. IP Filtering PIM Messages

To eliminate both the unicast and multicast PIM messages, in similar scenarios to those for which PIM passive mode is applicable, it might be possible to block IP protocol 103 (all PIM messages) in an input access-list. This is more effective than PIM passive mode, as this also blocks Register messages.

This is also acceptable when there is more than one PIM router on the link if IPsec is used (because the access-list processing sees the valid PIM messages as IPsec AH/ESP packets). However, this presumes that the link is not used to transit unicast packets between the PIM routers, or that the Register messages are also being sent with IPsec.

### 4.4. Summary of Vulnerabilities and Mitigation Methods

This section summarizes the vulnerabilities, and how well the mitigation methods are able to cope with them.

Summary of vulnerabilities and mitigations:

| Sec | Vulnerability | One stub router | | | >1 stub routers | | |
|---|---|---|---|---|---|---|---|
| | | PASV | IPsec | Filt | PASV | IPsec | Filt |
| 2.1 | Hosts Registering | N | N+ | Y | N | N+ | * |
| 2.2 | Invalid Neighbor | Y | Y | Y | * | Y | * |
| 2.3 | Adjacency Not Reqd | Y | Y | Y | * | Y | * |
| 2.4 | Invalid DR | Y | Y | Y | * | Y | * |
| 2.5 | Invalid Forwarder | Y | Y | Y | * | Y | * |

Figure 1

"*" means Yes if IPsec is used in addition; No otherwise.

"N+" means that the use of IPsec between the on-link routers does not protect from this; IPsec would have to be used at RPs.

To summarize, IP protocol filtering for all PIM messages appears to be the most complete solution when coupled with the use of IPsec between the real stub routers when there are more than one of them. If hosts performing registering is not considered a serious problem, IP protocol filtering and passive-mode PIM seem to be equivalent approaches.

## 5. Acknowledgements

Greg Daley and Gopi Durup wrote an excellent analysis of MLD security issues [I-D.daley-magma-smld-prob], which gave inspiration in exploring the on-link PIM threats problem space.

Ayan Roy-Chowdhury, Beau Williamson, and Bharat Joshi provided good feedback for this memo.

## 6. IANA Considerations

This memo includes no request to IANA.

## 7. Security Considerations

This memo analyzes the threats to the PIM multicast routing protocol at the last-hop, and proposes some possible mitigation techniques.

## 8. References

### 8.1. Normative References

[I-D.ietf-mboned-mroutesec]
Savola, P., Lehtonen, R., and D. Meyer, "PIM-SM Multicast Routing Security Issues and Enhancements", draft-ietf-mboned-mroutesec-04 (work in progress), October 2004.

[I-D.ietf-pim-sm-v2-new]
Fenner, B., "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", draft-ietf-pim-sm-v2-new-12 (work in progress), March 2006.

### 8.2. Informative References

[I-D.atwood-pim-sm-linklocal]
Atwood, J., "Security Issues in PIM-SM Link-local Messages", draft-atwood-pim-sm-linklocal-00 (work in progress), October 2004.

[I-D.daley-magma-smld-prob]
Daley, G. and G. Kurup, "Trust Models and Security in Multicast Listener Discovery", draft-daley-magma-smld-prob-00 (work in progress), July 2004.

[I-D.hayashi-igap]
Hayashi, T., "Internet Group membership Authentication Protocol (IGAP)", draft-hayashi-igap-03 (work in progress), August 2003.

[RFC3547] Baugher, M., Weis, B., Hardjono, T., and H. Harney, "The Group Domain of Interpretation", RFC 3547, July 2003.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC3740] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.

## Authors' Addresses

Pekka Savola
CSC - Scientific Computing Ltd.
Espoo
Finland

Email: psavola@funet.fi

James Lingard

Email: james@lingard.com

## Full Copyright Statement



## Intellectual Property



## Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).