Internet Engineering Task Force
Internet-Draft
Expires: May 24, 2005

P. Savola
CSC/FUNET

November 23, 2004

Last-hop Threats to Protocol Independent Multicast (PIM)
draft-savola-pim-lasthop-threats-00.txt

Status of this Memo

Copyright Notice

Abstract

Security threats analysis has been done on some parts of the multicast infrastructure, but the threats specific to the last-hop 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

There has been some analysis on the security threats to the multicast routing infrastructures [I-D.ietf-mboned-mroutesec], 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 of PIM at the last-hop links.

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

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.

2.1 Sending PIM Register Messages on Your Own

PIM Register messages are sent as unicast-encapsulated messages. Maliscious hosts could also send registers themselves for example to get around the rate-limiters, to interfere with foreign RPs, etc.

2.2 Becoming an Illegitimate PIM Neighbor

When PIM has been enabled on a router's "host" interface, any host can also become a PIM neighbor using PIM Hello messages unless special, rare precautions, such as protecting all the PIM traffic on the link using IPsec, have been taken.

Further PIM messaged should not be accepted except from valid PIM neighbors; if implementations are compliant to this recommendation in the PIM-SM specification, becoming a PIM Neighbor using Hello messages is the first step to be able to send other PIM messages.

2.3 Becoming an Illegitimate PIM DR

Designated Router is in "charge" of a particular LAN, for example, for registering new sources, generating PIM Join/Prune messages and forwarding multicast traffic.

A host which can became a PIM neighbor, can also, as part of becoming the neighbor, influence the DR election process: basically, if at least one neighbor did not have "DR Priority" field in the Hello message (a "bidding-down" attack), the neighbor with the numerically

highest IP address wins the election; if DR priority existed, the DR priority is first checked and only then the IP addresses are compared.

Further, it is not sufficient to secure DR election, because Assert messages can be used to obtain the responsibility for forwarding upstream traffic as described in the next section.

It seems that a DR can send PIM messages (like Prune/Join) to the non-DR to be forwarded upstream on behalf of directly connected (to both DR and non-DR) sources. In other words, a host on a stub LAN can be elected as a DR and act as a "man-in-the-middle" between the other hosts and the real PIM router. [XXX: Is this correct? Should non-DRs reject forwarding upstream messages from downstream LAN's DRs, because a real DR should have its own upstream connectivity?]

2.4 Becoming an Illegitimate PIM Asserted Forwarder

With a PIM Assert, a router can be elected to be in charge of handling all traffic from a particular (S,G) (where S might also be all of S? [XXX: true?]). This overrides DR behaviour.

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

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 on someone else's behalf to cause a temporary disruption on the LAN. However, it is not 100% clear what happens when the router which was spoofed receives "it's own assert" and CouldAssert(S,G,I) is False? [XXX: a PIM expert should say something? Is this an issue in the state machine?]

3. On-link Threats

The last section described some PIM vulnerabilities; this section gives an overview of the more concrete threats using these 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 from upstream on the link, or not registering or forwarding the multicast transmissions originated on the link upstream.

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 just not send any PIM Join/Prune messages based on the IGMP reports, not forward or Register any sourced packets, and maybe even send PIM Prune messages to cut off existings 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. This results in the same 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 the nodes beyond the link, especially in the environments where being 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 yourself 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 to PIM messaging requiring establishing a PIM adjacency, 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 integrity of an ASM group. This attack is also described in [I-D.ietf-mboned-mroutesec].

3.3 Confidentiality, Integrity or Authorization Violations

If a node can get to be a DR or craft an appropriate Assert, in addition to or instead of performing Denial-of-Service, it can also just operate as normal for some traffic, while violating confidentiality, integrity or authorization for some other traffic.

Some packets, whether sent by received, could be modified (possibly in a subtle, unnoticable ways) in transit resulting in an integrity violation. The packets can obviously be observed as well, so any data sent can be compromised.

A more elaborate attack is on authorization. There are some 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 of the others on the same link, etc.

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 messages on all PIM-enabled interfaces. Most implementations also require PIM to be enabled on the interface to send PIM registers from sourced data 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 for 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 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.

4.3 IP Filtering PIM Messages

To eliminate the PIM messages, and other PIM signalling, in the similar scenarios as with PIM Passive Mode, it might be possible to block IP protocol 103 (all PIM messages) as an input access-list.

This is also acceptable when IPsec is used with more than just one PIM router on the link.

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	Invalid DR	Y	Y	Y	*	Y	*
2.3	Adjacency not reqd	Y	Y	Y	*	Y	*
2.4	Invalid Forwarder	Y	Y	Y	*	Y	*

Figure 1

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

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.

6. IANA Considerations

This memo includes no request to IANA.

7. Security Considerations

This memo analyzes the threats at 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., Handley, M., Holbrook, H. and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode PIM-SM): Protocol Specification (Revised)", draft-ietf-pim-sm-v2-new-11 (work in progress), October 2004.

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.

[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.

Author's Address

Pekka Savola
CSC - Scientific Computing Ltd.
Espoo
Finland

EMail: psavola@funet.fi

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.