KARP
Internet-Draft
Intended status: Standards Track
Expires: January 10, 2013

W. Atwood
R. Bangalore Somanatha
Concordia University/CSE

July 09, 2012

Automatic Key and Adjacency Management for Routing Protocols
draft-atwood-karp-akam-rp-00

Abstract

When tightening the security of the core routing infrastructure, two steps are necessary. The first is to secure the routing protocols' packets on the wire. The second is to ensure that the keying material for the routing protocol exchanges is distributed only to the appropriate routers. This document specifies requirements on that distribution and proposes the use of a set of protocols to achieve those requirements.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 10, 2013.

Table of Contents

1. Introduction

Within the Keying and Authentication for Routing Protocols working group, there are several goals:

- o Determining how to update the security of existing routing protocols, and guiding this work;
- o Development of automated mechanisms for management of the keying material.

Within the second goal, there is at this time considerable activity on protocols and procedures for creating shared keys, under the assumption that the end points of the exchanges (the routers) are entitled to enter into the conversation. However, there appears to be no work on ensuring that the end points are legitimate.

This document addresses this issue. In particular, it addresses the need to ensure that keying material is distributed only to routers that legitimately form part of the "neighbor set" of a particular speaking router.

1.1. Terminology

Autonomous System ...

Administrative Domain ...

2. Keying Groups (Key Scopes)

2.1. Keying Groups

In an AD, all routers having the same TEK can be referred to as forming a `keying group'. We can have routers forming a `keying group' as follows:

- o A group per AD -
- o This is the most coarsely grained category of keying group where all routers in an AD share the same traffic key. Hence the incoming and outgoing keys for protecting control traffic on all routers are the same. This is the case typically in usage today with manual keying.
- o A group per link -
- o Here, all routers sharing a link share the key for that link. The routers could have different keys on their different interfaces, and share them with the other routers connected to those respective links.

- A group per sending router -
- This category is more finely grained compared to the previous two cases; each router uses a different key to secure its outgoing control traffic.
- A group per sending router per interface -
- This is the most finely grained category wherein each router has a different key for each of its interfaces, which in turn is different from the keys used by other routers to secure their outgoing traffic.
- A group per peer router -
- This category is strictly for unicast communication wherein peer routers share keys for their interaction. There is one outgoing key corresponding to each router in every pair of routers. These keys can be established through a unicast key management protocol such as IKE RFC 2409 [RFC2409].

2.2. Key Scopes

Alternatively, keying groups can be viewed from another perspective. Instead of looking at the granularity of keying from the point of view of the members, we can look at it from the point of view of the keys. This can be referred to as `key scope'. This viewpoint helps us to show the number of different keys required in an AD with an arbitrary number of routers `n'. During this calculation, we consider that every router in the AD is a sending router and hence uses keys to secure its control traffic. In fact, it is true that every router is a potential sender as far as control traffic is concerned.

The key scopes corresponding to the above categories of keying groups in the same order could be defined as follows:

- Same key for the entire AD -
- all routers in the domain share the same key.
- Key per link -
- all routers on a link share the same key.
- Key per sending router -
- each router has a different key to secure its outgoing control traffic.
- Key per sending router per interface -
- each router uses different keys for each of its interfaces, which in turn are different from the keys used by the other routers for securing their outgoing traffic.
- Key per peer router -
- THere, there exist two keys corresponding to every pair of routers.

3. Problem Statement

We have 11 security goals and 5 non-security goals. They will be listed in the next version of the draft.

4. High Level Design

In this section, we propose an architecture for an automated key management and adjacency management system. In order to build this framework, we have reused parts of the existing proposals and fit them into their correct places in the overall architecture. We have then extended/ modified them so as to handle the key management isues overlooked by them.

Our design deals with securing the control traffic of routers within an AD.

4.1. Global View

The main entities in our system are the following:

- Administrator
- Policy Server
- GCKS
- Standby GCKS
- GMs

These entities and their functions are explained in the next section.

4.2. Entities in the system

The entities are based on those in GSAKMP. The difference is that the Group Owner in GSAKMP has been replaced by a Policy Server, and the Subordinate GC/KS has been replaced by a Standby GCKS in our design. We have chosen the term `Policy Server' in order to be consistent with RFC 6407 [RFC6407], and the term `Standby GCKS' since it is not a subordinate in our design and is a standby that is capable of performing all operations performed by the active GCKS. Our design conforms to the Multicast Group Security Architecture RFC 3740 [RFC3740]

The network administrator makes configurations for the Policy Server and the GCKS. Security policies go to the policy server, and configs related to the AD go to the GCKS.

Policy Server is the entity that manages security policies for the AD. The behavior of the policy server we describe here draws

contents from and is very similar to the `Group Owner' in GSAKMP. The security policies include general policies such as authorization details for the GCKS, access control for the GMs, rekey intervals, as well as other specific policies that may be necessary for the group. These policies are put together into a `Policy Token' (term taken from GSAKMP) and sent to the GCKS.

The GCKS is either a router or a server chosen by the administrator as the group controller. It is the entity whose major function is key management and adjacency management. The GCKS should also ensure that the security policies in the policy token are enforced. This implies that whenever a GM requests keys from the GCKS, the GCKS should enforce access control for the GM according to the terms specified in the policy token. The administrator configures the GCKS with information such as the type of keying group to be enforced for the AD and the adjacencies for each router in the AD corresponding to a particular routing protocol (or a set of similar routing protocols). This last point is due to our proposal that there could be one instance of a GCKS per routing protocol or a set of similar routing protocols. This is in fact necessary because GCKS is the entity that should ensure adjacency management, and adjacencies may be defined differently for different routing protocols. Also, according to [I-D.ietf-karp-ops-model] , ``KARP must not permit configuration of an inappropriate key scope''. This means that each routing protocol could have a different requirement of key scope and that needs to be satisfied. The GCKS also generates, distributes and updates keys, depending on the type of keying group to be enforced in the AD.

The standby GCKS is an entity that is always kept in sync with the active GCKS, ready to take over at any time should the active fail. This design eliminates the possibility of a single point of failure in a centralized system.

GMs are the group member routers that communicate with each other as well as with the GCKS. When they request keys from the GCKS, they are given the keys along with the policy token. GMs are required to check the rules specified in the policy token to determine if the GCKS is authorized to act in that role. Each GM has a Local Key Server (LKS). The term `LKS' has been taken from Citation{automated-key-mgmt-dks-lks}. It is a key generation and storage entity within the GM. A GM may sometimes be required to generate keys itself depending on the category of keying group being enforced. This kind of design ensures that the architecture is distributed in the sense that key management responsibility is divided between the GCKS and the LKSes.

From the description above, it can be seen that the architecture we

propose is a balance between a completely centralized model and a completely distributed one, developed by picking the plus points of both types. It defines the concept of a GCKS, which is a centralized entity, as well as the concept of a LKS, which is distributed as being one entity per router. The design tries to bring in the advantages of both models. A centralized entity is considered necessary mainly to make adjacency management possible. In the absence of a central controller that has information about the adjacencies of each router in the AD, individual routers will not be able to establish the legitimacy of their neighbors. Adjacency management is especially important since we are dealing with control packets, which are usually exchanged with immediate neighbors. At the same time, loading the centralized entity with multiple responsibilities may lead to its failure. Hence we have a localized entity that can take up some of the functions of the central controller as and when the need arises. This enhances scalability, which is so important in a key management system. Another factor leading to scalability is the presence of the standby GCKS. A centralized system could have the disadvantage of having a single point of failure. Our design tries to eliminate this by defining a standby for the central controller that is always kept in sync with it, ready to take over at any time.

5. Detailed Design

To be copied into the draft in version -01

6. Other Aspects of the Key Management Problem

To be copied into the draft in version -01

7. Detailed Packet Formats

TBD

8. IANA Considerations

This document has no actions for IANA.

9. Acknowledgements

10. Change History (RFC Editor: Delete Before Publishing)

[NOTE TO RFC EDITOR: this section for use during I-D stage only. Please remove before publishing as RFC.]

atwood-kmart-kam-rp-00 (original submission, based on Revathi's thesis)

- removed sections of the thesis that are not part of the specification.

11. Needs Work in Next Draft (RFC Editor: Delete Before Publishing)

[NOTE TO RFC EDITOR: this section for use during I-D stage only. Please remove before publishing as RFC.]

List of stuff that still needs work
- Copy in section on Detailed Design
- Copy in section on Other Aspects
- Create the section on packet formats
- List the security goals.
-

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

12.2. Informative References

[I-D.ietf-karp-ops-model]
Hartman, S. and D. Zhang, "Operations Model for Router Keying", draft-ietf-karp-ops-model-02 (work in progress), April 2012.

[I-D.ietf-pim-sm-linklocal]
Atwood, W., Islam, S., and M. Siami, "Authentication and Confidentiality in PIM-SM Link-local Messages", draft-ietf-pim-sm-linklocal-10 (work in progress), December 2009.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

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

[RFC6407] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, October 2011.

Authors' Addresses

J. William Atwood
Concordia University/CSE
1455 de Maisonneuve Blvd, West
Montreal, QC H3G 1M8
Canada

Phone: +1(514)848-2424 ext3046
Email: bill@cse.concordia.ca
URI: http://users.encs.concordia.ca/~bill

Revathi BS
Concordia University/CSE
1455 de Maisonneuve Blvd, West
Montreal, QC H3G 1M8
Canada

Phone: +1(514)848-2424 ext3046
Email: r_bangal@cse.concordia.ca