RTGWG W. Atwood
Internet-Draft N. Prajapati
Intended status: Informational Concordia University/CSE
Expires: April 30, 2015 October 27, 2014

A Framework for Secure Routing Protocols
draft-atwood-rtgwg-secure-rtg-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 a way of organizing the security parameters and a method for conveniently controlling those parameters using YANG and NETCONF.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Much effort has been expended to ensure the security of end-to-end exchanges in the Internet. However, relatively little effort appears to be being expended to secure the router-to-router exchanges that define the forwarding path for the packets that make up the end-to-end exchanges.

Methods for ensuring router-to-router security have been written into the specifications of routing protocols for many years. However, the security parameters (keys, permitted neighbors, etc.) are typically installed manually on each router [RFC6862]. Because network management personnel are scarce, and updating security parameters is a labor-intensive task, if security is implemented at all, the keys are often left in place for five years or more [RFC6862], leaving ample opportunity for them to be compromised. This could lead to an intruder router pretending to be a legitimate one and capturing confidential data.

In March 2006, the Internet Architecture Board (IAB) held a workshop on the topic "Unwanted Internet Traffic". The report from that workshop is documented in [RFC4948]. Section 8.1 of that document states, "A simple risk analysis would suggest that an ideal attack target of minimal cost but maximal disruption is the core routing infrastructure". Section 8.2 calls for "[t]ightening the security of the core routing infrastructure".

One approach to achieving improved security is to automate the process of updating the security parameters. This will reduce the number of network management personnel needed and would potentially improve security for all users of the Internet. This leads us to the following requirements:

- o Ensuring the authenticity and integrity of the routing protocol messages;
- o Ensuring the legitimacy of the neighboring routers, by making sure that they are part of the "permitted adjacency" as explained below;
- o Automation of the entire process of key and adjacency management.

The notion of "permitted adjacency" can be re-stated as providing answers to the following questions:

- o Are you a legitimate member of my group? This is the question of authentication.
- o Are you permitted to connect to me for the purposes of this routing protocol? This is the question of authorization.

Figure 1 shows a potential framework for discussion of secure routing.

```
Routing Protocol            Layer 1

Keys and Security Protocol  Layer 2

Key and SA Management       Layer 3

Configuration Management    Layer 4
```

Figure 1: Secure Routing Framework

Layer 1 is the routing protocol layer. The routers run routing protocols among themselves to collect and distribute topological information for the network. The routing protocols distribute the network information by "exchanging messages" with their peer routers (neighbors). Each router processes all the information received from the routing protocol peers to create and maintain the forwarding table. This forwarding table is used to decide where to forward a particular packet when it arrives.

Layer 2 represents the security mechanisms available for a routing protocol. Each routing protocol will have a number of security mechanisms available to it (including no security at all). A routing protocol needs to be assured of two things about the messages that it receives from its peer routers:

- o that the peer is legitimate, and

- o that the message from that peer has not been altered in transit.

The most common approach today is for a routing protocol to use a pre-shared key for authorizing its neighbors as well as for validating the message integrity. In effect, all the neighbors (running the same routing protocol) that possess this key are authorized to communicate with each other.

The configuration of keys and security associations, the choice of keys and the security mechanism used for a routing protocol depend on the key management methods at Layer 3. As discussed in Section 1, the network operators use the manual management method, which is the only solution available at this time for routing protocols. As a result, keys are seldom changed.

Layer 4 focuses on the configuration and the distribution of keys and security associations for routing protocols. At this time, this is done manually, either by visiting the router itself, or accessing it remotely through some configuration procedure. Each router manufacturer has its own approach to faciltiate this.

Within the KARP Working Group, protocols and procedures for creating shared keys for specific environments have been proposed [I-D.hartman-karp-mrkmp][I-D.mahesh-karp-rkmp][I-D.tran-karp-mrmp], under the assumption that the end points of the exchanges (the routers) are entitled to enter into the conversation, i.e., that they can prove that they are who they say they are. However, this only addresses part of the problem at Layer 3, because these documents provide no mechanism to assess or ensure that the end points are entitled to be neighbors.

In addition, requirements for an operations and management model are specified in [RFC7210].

This document addresses two issues: providing a flexible method for managing the necessary keys and security associations, and providing a way to configure a set of routers while satisfying operational constraints.

2. Routing Protocol Security

To be able to effectively manage routing protocol security, it is necessary to have a representation of the choices open to a key negotiation protocol, and to have a convenient representation of the parameters to be used in a particular security association that is being used by the security features of a routing protocol.

The representation of parameters (keys and security associations, key derivation functions) is provided by the Crypto-Key-Table specified in [RFC7210].

The parameters for a specific peer router and protocol are provided in the Routing Security Parameter Database (RSPD). The Routing Peer Authorization Database (RPAD) provides information required for peer authentication and authorization and specifies a key management protocol to be used in establishing the peer relationship.

3. RPsec Configuration

To enable convenient configuration of the RPsec databases, YANG models of these databases can be used, in conjunction with a central controller to define updates to the security configurations.

4. RPsec Databases

4.1. RSPD

The objective of the RSPD is to provide security options (choice of security protocol) for a routing protocol’s security. Each entry (a choice) specifies the security parameters required to establish a security association between the peers. An authorized device may communicate with many routing protocol peers. To do so, it must agree on the security requirements of the routing protocol peer for successful communication. The peers must agree on security protocols, transforms, mode of communication along with the key required to integrity protect messages exchanged between them. This database aims to provide such information. The RSPD contains the traffic descriptors for identifying each routing protocol traffic that needs to be protected, bypassed or discarded. The RSPD, thus, is a database to specify the traffic descriptors for the routing protocol traffic, security protocols, lifetime and related parameters for securing the communication between the two devices or among a group in case of the multicast communication. This database provides partial information towards security requirements of the routing protocols. The rest of the information is provided by the CKT.

4.2. CKT

The CKT is an important database that provisions key material and associated cryptographic algorithms to protect the routing protocol messages. In RPsec, the CKT performs the role similar to the SAD in IPsec. It stores the negotiated (or manually configured) SAs for the routing protocols. In that, each RSPD entry points to an appropriate entry in the CKT. Each RSPD entry that protects the routing protocol traffic, provides a (security) protocol id and a peer id (traffic descriptor) that identify an entry in this database. The form of the protocol id and the peer id is specified in [RFC7210]. The RSPD together with CKT ensure that the key is provided to a security protocol that is used for securing the routing protocol.

4.3. RPAD

The RPAD’s objective is to provide authentication information and a KMP for the routing peers. It provides authentication information necessary to assert a local device’s identity and to validate the identity asserted by the peer devices. A KMP uses the information in the RPAD and the RSPD for authentication and SA negotiation, respectively. Authentication is required to ensure that the devices participating in the network infrastructure are legitimate. A legitimate device should present its identity, identity of remote peer(s) or group it wishes to communicate with, and an organization-wide acceptable credential. If the device successfully passes the peer device’s scrutiny, it is authenticated to communicate with the requested peer(s) or a group in the network. The communication between the two devices must stop if the KMP fails to authenticate the peers using the information available in the RPAD database. A KMP negotiates a security association only after the authentication is successful.

5. RPsec in Detail

Detailed design of the RPsec databases. To be included in the next version of the draft.

6. Representation and Distribution of RPsec Policies

This section explains the YANG models for each RPsec database. It describes a possible way of configuring RPsec databases in the network in compiance with the IETF’s policy-based network managment (PBMN) and distributed management architecture.

For management of the contents of the RPsec databases, the data fields of the RPsec databases are organized and defined in four modules:

- RPsec common types module
- RPAD module
- RSPD module
- CKT module

The material on YANG models will be included in the next version of the draft.

7. IANA Considerations

This document has no actions for IANA.

8. Acknowledgements

The original idea for the RAPD database was presented in [I-D.atwood-karp-aapm-rp].

9. 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-rtgwg-secure-routing-00 (original submission, based on Nitin's thesis)

- copied in some sections of the thesis that are relevant to the specification.

10. 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

- Flesh out sections on RPsec databases and YANG models.
-
-
-
-

11. References

11.1. Normative References

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

11.2. Informative References

[I-D.atwood-karp-aapm-rp]
william.atwood@concordia.ca, w., Somanatha, R., Hartman, S., and D. Zhang, "Authentication, Authorization and Policy Management for Routing Protocols", draft-atwood-karp-aapm-rp-00 (work in progress), July 2013.

[I-D.hartman-karp-mrkmp]
Hartman, S., Zhang, D., and G. Lebovitz, "Multicast Router Key Management Protocol (MaRK)", draft-hartman-karp-mrkmp-05 (work in progress), September 2012.

[I-D.mahesh-karp-rkmp]
Jethanandani, M., Weis, B., Patel, K., Zhang, D., Hartman, S., Chunduri, U., Tian, A., and J. Touch, "Negotiation for Keying Pairwise Routing Protocols in IKEv2", draft-mahesh-karp-rkmp-05 (work in progress), November 2013.

[I-D.tran-karp-mrmp]
Tran, P. and B. Weis, "The Use of G-IKEv2 for Multicast Router Key Management", draft-tran-karp-mrmp-02 (work in progress), October 2012.

[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.

[RFC4535] Harney, H., Meth, U., Colegrove, A., and G. Gross, "GSAKMP: Group Secure Association Key Management Protocol", RFC 4535, June 2006.

[RFC4948] Andersson, L., Davies, E., and L. Zhang, "Report from the IAB workshop on Unwanted Traffic March 9-10, 2006", RFC 4948, August 2007.

[RFC5374] Weis, B., Gross, G., and D. Ignjatic, "Multicast Extensions to the Security Architecture for the Internet Protocol", RFC 5374, November 2008.

[RFC5796] Atwood, W., Islam, S., and M. Siami, "Authentication and Confidentiality in Protocol Independent Multicast Sparse Mode (PIM-SM) Link-Local Messages", RFC 5796, March 2010.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

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

[RFC6518] Lebovitz, G. and M. Bhatia, "Keying and Authentication for Routing Protocols (KARP) Design Guidelines", RFC 6518, February 2012.

[RFC6862] Lebovitz, G., Bhatia, M., and B. Weis, "Keying and Authentication for Routing Protocols (KARP) Overview, Threats, and Requirements", RFC 6862, March 2013.

[RFC7210] Housley, R., Polk, T., Hartman, S., and D. Zhang, "Database of Long-Lived Symmetric Cryptographic Keys", RFC 7210, April 2014.

[RFC7211] Hartman, S. and D. Zhang, "Operations Model for Router Keying", RFC 7211, June 2014.

Authors' Addresses

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

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

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

Email: prajapatinitin@hotmail.com