        Analysis of RSVP-TE Security According to KARP Design Guide
                draft-mahesh-karp-rsvp-te-analysis-01.txt

Abstract

   This document analyzes Resource reSerVation Protocol-Traffic
   Engineering (RSVP-TE) according to guidelines set forth in section
   4.2 of KARP Design Guidelines (RFC 6518).

Status of This Memo

   This Internet-Draft is submitted 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 May 20, 2014.

Table of Contents

1. Introduction

In March 2006, the Internet Architecture Board (IAB) described an
attack on core routing infrastructure as an ideal attack that would
inflict the greatest amount of damage, in their Report from the IAB
workshop on Unwanted Traffic March 9-10, 2006 [RFC4948], and
suggested steps to tighten the infrastructure against the attack.
Four main steps were identified for that tightening:

1. Create secure mechanisms and practices for operating routers.

2. Clean up the Internet Routing Registry (IRR) repository, and
    securing both the database and the access, so that it can be used
    for routing verifications.

3. Create specifications for cryptographic validation of routing
    message content.

4. Secure the routing protocols' packets on the wire.

In order to secure the routing protocols this document performs an
initial analysis of the current state of RSVP-TE according to the
requirements of KARP Design Guidelines [RFC6518]. This draft builds
on several previous analysis efforts into routing security:

o Issues with existing Cryptographic Protection Methods for Routing
   Protocols [RFC6039] an analysis of cryptographic issues with
   routing protocols.

o Analysis of OSPF Security According to KARP Design Guide
   [RFC6863].

o Analysis of BGP, LDP, PCEP, and MSDP Issues According to KARP
   Design Guide [RFC6952] which is a analysis of the four routing
   protocols.

Resource reSerVation Protocol (RSVP) [RFC2205] is a resource
reservation setup protocol designed for an integrated services. RSVP
Security Properties [RFC4230] indicates the unfeasibility of using
IPSec to secure RSVP signaling messages. RSVP Cryptographic
Authentication [RFC2747] describes the format and use of RSVP's
INTEGRITY objects to provide hop-by-hop integrity and authentication
of RSVP messages. RSVP-TE: Extensions to RSVP for LSP Tunnels
[RFC3209] is an extension of the RSVP protocol to establish Multi-
Protocol Label Switching (MPLS) Label Switch Paths (LSPs). RSVP-TE
signaling messages are used to establish both intra- and inter-domain
TE LSPs. The security mechanisms for RSVP, RSVP Cryptographic
Authentication [RFC2747] can be used by RSVP-TE to provide the
security protection for the RSVP-TE message transportation.
Therefore, the rest of the document will focus on the current state
of security efforts for RSVP and assume that will apply to RSVP-TE
also.

Section 2 looks at the current security state of RSVP-TE. Section 3
does an analysis of the gap between the existing and the optimal
security state of the protocol and suggest some areas where we need
to improve.

1.1. Abbreviations

BGP - Border Gateway Protocol

DoS - Denial of Service

KARP - Key and Authentication for Routing Protocols

KDF - Key Derivation Function

KEK - Key Encrypting Key

KMP - Key Management Protocol

LDP - Label Distribution Protocol

LSP - Label Switch Path

MAC - Message Authentication Code

MKT - Master Key Tuple

MPLS - Multi Protocol Label Switching

MSDP - Multicast Source Distribution Protocol

MD5 - Message Digest algorithm 5

PCEP - Path Computation Element Protocol

RSVP - Resource reSerVation Protocol

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

[2](#). Current Assessment of RSVP-TE

This section looks at RSVP-TE and the underlying transport protocol
and key mechanisms built for the protocol.

[2.1](#). Transport Layer

RSVP operates on top of IPv4 or IPv6, occupying the place of a
transport protocol in the protocol stack. However, RSVP does not
transport application data but is rather an Internet control
protocol, like ICMP, IGMP, or routing protocols.

[2.1.1](#). UDP Encapsulation

An RSVP implementation generally requires the ability to perform
"raw" network I/O. However, some systems may not support raw network
I/O. To use RSVP, such hosts must encapsulate RSVP messages in UDP.

[2.2](#). Keying Mechanism

[Section 7](#) of RSVP Cryptographic Authentication discusses the
possibility of using Kerberos to generate and distribute RSVP
authentication keys. However, the design of Automated Key Management
(AKM) mechanism for RSVP is still incomplete. There is no other AKM
solution proposed at this time. If anything, manual key management
is used.

The protocol states that manual keying should be supported and states
the need for a key management protocol to distribute keys. It even
states that the Key Identifier be the hook between RSVP and the key
management protocol. But it deliberately excludes defining a
integrated key management protocol technique in the document. It
does define a key lifetime that should be recorded for all systems
although how they are presented e.g. using the start time and the end
time of the key life period, is not specified. It even advises that
the keys should be changed on a regular basis and that multiple keys
should be used to transition from one key to another.

2.3. Message Integrity and Node Authentication

RSVP-TE makes use of RSVP Cryptographic Authentication [RFC2747].
Note that there is currently no RSVP-TE specific security mechanism.
It is required that RSVP-TE headers and payload be authenticated, but
there is no requirement that RSVP-TE headers be encrypted.

RSVP Cryptographic Authentication [RFC2747] defines the use HMAC-MD5
for both message integrity and node authentication. The length of
the keyed digests is 128 bits. In these cases RSVP checksum can be
disabled in lieu of message digest. In addition, no algorithm
agility is supported.

2.4. Replay Protection

RSVP uses 64 bit monotonically increasing sequence numbers to prevent
against replay attacks. The sequence number space is large enough to
guarantee that a sequence number will never reach its maximum and
roll back within a reasonable long period.

The solution provides three approaches to generate unique
monotonically increasing sequence numbers across a failure or a
restart. The solutions include:

1. Maintaining sequence numbers in stable memory

2. Introducing the data from a local time clock into the generation
    of sequence numbers after a restart

3. Introducing the timing information from a Network Recovered Clock
    into the generation of sequence numbers after a restart.

In addition, a handshake is defined for a receiver to get the latest
value of a sequence number. Therefore, this solution is effective in
addressing the issues caused by the rollback of sequence numbers
across a system restart or failure. However, when a router uses the
approach to generating sequence numbers with the time information

from NTP, an attacker may try to deceive the router to generate a
sequence number which is less than the sequence numbers it used to
have, by sending replayed or foiled NTP information.

2.5. Out of Order Protection

To address the issue of out-of-order message delivery, the solution
proposed in RSVP Cryptographic Authentication [RFC2747] allows
administrators to specify a sequence number window corresponding to
the worst case reordering behavior. Instead of requiring the
sequence number of an incoming packet to be strictly larger than the
ones previously received, a packet will be accepted if its sequence
number is within the window.

2.6. Denial of Service Attack Protection

RSVP does not explicitly mention Denial of Service (DoS) attacks and
how to prevent against it. However, a RSVP-TE node does know the
peers that it should be communicating with and can therefore accept
packets from known hosts only. This feature can largely mitigate the
security risks caused by DoS attacks.

3. Gap Analysis for RSVP-TE

This section outlines the differences between the current state of
RSVP-TE and the desired state as outlined in sections 4.1 and 4.2 of
KARP Design Guidelines [RFC6518].

In RSVP Cryptographic Authentication [RFC2747], only the usage of MD5
to generate digests for RSVP-TE messages is defined. In order to
fulfill the requirement of supporting strong algorithms and
cryptographic algorithm agility, at least the support of SHA-2 and
the ability to indicate additional algorithms needs to be provided..

In addition, in RSVP Cryptographic Authentication [RFC2747], three
approaches to generating unique monotonically increasing sequence
numbers across a failure and restart are introduced, but no approach
is mandated. However, as mentioned above, when using Network
Recovered Clocks into the generation of sequence numbers, the
capability of RSVP-TE in tolerating inter-connection replay attacks
will largely rely on the security of network timing protocols.
Therefore, in future this approach should not be recommended.

4. IANA Requirements

   This document makes no IANA requests, and the RFC Editor may consider
   deleting this section on publication of this document as a RFC.

5. Security Consideration

   This document is all about security considerations for RSVP-TE.

6. Acknowledgements

   The authors would like to thank Sean Turner for his review and
   comments on the draft.

7. References

7.1. Normative References

   [RFC2205] Braden, B., Zhang, L., Berson, S., Herzog, S., and S.
              Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1
              Functional Specification", RFC 2205, September 1997.

   [RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5
              Signature Option", RFC 2385, August 1998.

   [RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V.,
              and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP
              Tunnels", RFC 3209, December 2001.

   [RFC5926] Lebovitz, G. and E. Rescorla, "Cryptographic Algorithms
              for the TCP Authentication Option (TCP-AO)", RFC 5926,
              June 2010.

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

7.2. Informative References

   [RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-
              Hashing for Message Authentication", RFC 2104, February
              1997.

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

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

   [RFC2747] Baker, F., Lindell, B., and M. Talwar, "RSVP Cryptographic
              Authentication", RFC 2747, January 2000.

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

   [RFC4230] Tschofenig, H. and R. Graveman, "RSVP Security
              Properties", RFC 4230, December 2005.

   [RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway
              Protocol 4 (BGP-4)", RFC 4271, January 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.

   [RFC5036] Andersson, L., Minei, I., and B. Thomas, "LDP
              Specification", RFC 5036, October 2007.

   [RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., and C.
              Pignataro, "The Generalized TTL Security Mechanism
              (GTSM)", RFC 5082, October 2007.

   [RFC5440] Vasseur, JP. and JL. Le Roux, "Path Computation Element
              (PCE) Communication Protocol (PCEP)", RFC 5440, March
              2009.

   [RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP
              Authentication Option", RFC 5925, June 2010.

   [RFC5961] Ramaiah, A., Stewart, R., and M. Dalal, "Improving TCP's
              Robustness to Blind In-Window Attacks", RFC 5961, August
              2010.

   [RFC6039] Manral, V., Bhatia, M., Jaeggli, J., and R. White, "Issues
              with Existing Cryptographic Protection Methods for Routing
              Protocols", RFC 6039, October 2010.

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

   [RFC6863] Hartman, S. and D. Zhang, "Analysis of OSPF Security
              According to the Keying and Authentication for Routing
              Protocols (KARP) Design Guide", RFC 6863, March 2013.

   [RFC6952] Jethanandani, M., Patel, K., and L. Zheng, "Analysis of
              BGP, LDP, PCEP, and MSDP Issues According to the Keying

                  and Authentication for Routing Protocols (KARP) Design
                  Guide", [RFC 6952](), May 2013.

Authors' Addresses

   Mahesh Jethanandani
   Ciena Corporation
   3939 North First Street
   San Jose, CA 95134
   USA

   Phone: +1 (408) 904-2160
   Email: mjethanandani@gmail.com

   Dacheng Zhang
   Huawei Technologies co., LTD.
   Beijing
   China

   Email: zhangdacheng@huawei.com