Controlling Secure Network Enrollment in RPL networks
draft-ietf-roll-enrollment-priority-03

Abstract

   [I-D.ietf-6tisch-enrollment-enhanced-beacon] defines a method by
   which a potential [I-D.ietf-6tisch-minimal-security] enrollment proxy
   can announce itself as a available for new Pledges to enroll on a
   network. The announcement includes a priority for enrollment. This
   document provides a mechanism by which a RPL DODAG root can disable
   enrollment announcements, or adjust the base priority for enrollment
   operation.

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 https://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 March 29, 2021.

Copyright Notice

Table of Contents

1. Introduction

[RFC7554] describes the use of the time-slotted channel hopping
(TSCH) mode of [ieee802154]. [I-D.ietf-6tisch-minimal-security] and
[I-D.ietf-6tisch-dtsecurity-secure-join] describe mechanisms by which
a new node (the "pledge)" can use a friendly router as a Join Proxy.
[I-D.ietf-6tisch-enrollment-enhanced-beacon] describes an extension
to the 802.15.4 Enhanced Beacon that is used by a Join Proxy to
announce its existence such that Pledges can find them.

The term (1)"Join" has been used in documents like
[I-D.ietf-6tisch-minimal-security] to denote the activity of a new
node authenticating itself to the network in order to obtain
authorization to become a member of the network. This typically
involves a cryptographic authentication protocol in which a network
credential is provided.

In the context of the [RFC6550] RPL protocol, the term (2)"Join" has
an alternate meaning: that of a node (already authenticating to the
network, and already authorized to be a member of the network),
deciding which part of the RPL DODAG to attach to. This term "Join"
has to do with parent selection processes.

In order to avoid the ambiguity of this term, this document refers to
the process (1)"Join" as enrollment, leaving the term "Join" to mean
(2)"Join". The term "onboarding" (or IoT Onboarding) is sometimes
used to describe the enrollment process. However, the term _Join

Proxy_ is retained with it's meaning from
[I-D.ietf-6tisch-minimal-security].

It has become clear that not every routing member of the mesh ought
to announce itself as a _Join Proxy_. There are a variety of local
reasons by which a 6LR might not want to provide the _Join Proxy_
function. They include available battery power, already committed
network bandwidth, and also total available memory available for
Neighbor Cache Entry slots.

There are other situations where the operator of the network would
like to selective enable or disable the enrollment process in a
particular DODAG.

As the enrollment process involves permitting unencrypted traffic
into the best effort part of a (TSCH) network, it would be better to
have the enrollment process off when no new nodes are expected.

A network operator might also be able to recognize when certain parts
of the network are overloaded and can not accomodate additional
enrollment traffic, and it would like to adjust the enrollment
priority (the proxy priority field of
[I-D.ietf-6tisch-enrollment-enhanced-beacon]) among all nodes in the
subtree of a congested link.

This document describes an RPL DIO option that can be used to
announce a minimum enrollment priority. Each potential _Join Proxy_
would this value as a base on which to add values relating to local
conditions. As explained in
[I-D.ietf-6tisch-enrollment-enhanced-beacon], higher values decrease
the likelyhood of an unenrolled node sending enrollment traffic via
this path.

A network operator can set this value to the maximum value allowed,
effectively disable all new enrollment traffic.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in
BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

2. Protocol Definition

The following option is defined to transmission in the DIO issued by
the DODAG root. It may also be added by a router on part of the sub-
tree as a result of some (out of scope for this document) management
function.

6LRs that see this DIO Option SHOULD increment their minimum
enrollment priority if they observe congestion on the channel used
for enrollment traffic. The exact mechanism is a local decision, and
may be the subject for future work.

A 6LR which would otherwise be willing to act as a _Join Proxy_, will
examine the minimum priority field, and to that number, add any
additional local consideration (such as upstream congestion).

The Enrollment Priority can only be increased by each 6LR in value,
to the maximum value of 0x7f.

The resulting priority, if less than 0x7f should enable the _Join
Proxy_ function.

```
   0                   1                   2
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |   Type = TBD01|Opt Length = 1|R| min. priority  |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

min.priority a 7 bit field which provides a base value for the
   Enhanced Beacon Join priority. A value of 0x7f (127) disables the
   Join Proxy function entirely.

R a reserved bit that SHOULD be set to 0 by senders, and MUST be
   ignored by receivers. This reserved bit SHOULD be copied to
   options created.

This document uses the extensions mechanism designed into [RFC6550].
It does not need any mechanism to enable it.

Future work like [I-D.ietf-roll-capabilities] will enable collection
of capabilities such as this one in reports to the DODAG root.

2.1. Upwards compatibility

A 6LR which did not support this option would not act on it, or copy
it into it's DIO messages. Children and grandchildren nodes would
therefore not receive any telemetry via that path, and need to assume
a default value.

6LRs that support this option, but whose parent does not send it
SHOULD assume a value of 0x40 as their base value. The nodes then
adjust this base value based upon their observed congestion, emitting
their adjusted DIO value to their children.

A 6LR downstream of a 6LR where there was an interruption in the
telemetry could err in two directions: * if the value implied by the
base value of 0x40 was too low, then a 6LR might continue to attract
enrollment traffic when none should have been collected. This is a
stressor for the network, but this would also be what would occur
without this option at all. * if the value implied by the base value
of 0x40 was too high, then a 6LR might deflect enrollment traffic to
other parts of the DODAG tree, possibly refusing any enrollment
traffic at all. In order for this to happen, some significant
congestion must be seen in the sub-tree where the implied 0x40 was
introduced. The 0x40 is only the half-way point, so if such an
amount of congestion was present, then this sub-tree of the DODAG
simply winds up being more cautious than it needed to be.

It is possible that the temporal alternation of the above two
situations might introduce cycles of accepting and then rejecting
enrollment traffic. This is something an operator should consider if
when they incrementally deploy this option to an existing LLN. In
addition, an operator would be unable to turn off enrollment traffic
by sending a maximum value enrollment priority to the sub-tree. This
situation is unfortunate, but without this option, the the situation
would occur all over the DODAG, rather than just in the sub-tree
where the option was omitted.

3. Security Considerations

As per [RFC7416], RPL control frames either run over a secured layer
2, or use the [RFC6550] Secure DIO methods. This option can be
placed into either a "clear" (layer-2 secured) DIO, or a layer-3
Secure DIO. As such this option will have both integrity and
confidentiality mechanisms applied to it.

A malicious node (that was part of the RPL control plane) could see
these options and could, based upon the observed minimal enrollment
priority signal a confederate that it was a good time to send
malicious join traffic.

Such as a malicious node, being already part of the RPL control
plane, could also send DIOs with a different minimal enrollment
priority which would cause downstream mesh routers to change their
Join Proxy behaviour.

Lower minimal priorities would cause downstream nodes to accept more pledges than the network was expecting, and higher minimal priorities cause the enrollment process to stall.

The use of layer-2 or layer-3 security for RPL control messages prevents the above two attacks, by preventing malicious nodes from becoming part of the control plane. A node that is attacked and has malware placed on it creates vulnerabilities in the same way such an attack on any node involved in Internet routing protocol does. The rekeying provisions of [I-D.ietf-6tisch-minimal-security] exist to permit an operator to remove such nodes from the network easily.

4. Privacy Considerations

There are no new privacy issues caused by this extension.

5. IANA Considerations

Allocate a new number TBD01 from Registry RPL Control Message Options. This entry should be called Minimum Enrollment Priority.

6. Acknowledgements

This has been reviewed by Pascal Thubert and Thomas Wattenye.

7. References

7.1. Normative References

[I-D.ietf-6tisch-enrollment-enhanced-beacon]
          Dujovne, D. and M. Richardson, "IEEE 802.15.4 Information
          Element encapsulation of 6TiSCH Join and Enrollment
          Information", draft-ietf-6tisch-enrollment-enhanced-
          beacon-14 (work in progress), February 2020.

[I-D.ietf-6tisch-minimal-security]
          Vucinic, M., Simon, J., Pister, K., and M. Richardson,
          "Constrained Join Protocol (CoJP) for 6TiSCH", draft-ietf-
          6tisch-minimal-security-15 (work in progress), December
          2019.

[ieee802154]
          IEEE standard for Information Technology, ., "IEEE Std.
          802.15.4, Part. 15.4: Wireless Medium Access Control (MAC)
          and Physical Layer (PHY) Specifications for Low-Rate
          Wireless Personal Area Networks", n.d.,
          <http://standards.ieee.org/findstds/
          standard/802.15.4-2015.html>.

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
            Requirement Levels", BCP 14, RFC 2119,
            DOI 10.17487/RFC2119, March 1997,
            <https://www.rfc-editor.org/info/rfc2119>.

[RFC6550]   Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J.,
            Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur,
            JP., and R. Alexander, "RPL: IPv6 Routing Protocol for
            Low-Power and Lossy Networks", RFC 6550,
            DOI 10.17487/RFC6550, March 2012,
            <https://www.rfc-editor.org/info/rfc6550>.

[RFC7416]   Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A.,
            and M. Richardson, Ed., "A Security Threat Analysis for
            the Routing Protocol for Low-Power and Lossy Networks
            (RPLs)", RFC 7416, DOI 10.17487/RFC7416, January 2015,
            <https://www.rfc-editor.org/info/rfc7416>.

[RFC7554]   Watteyne, T., Ed., Palattella, M., and L. Grieco, "Using
            IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the
            Internet of Things (IoT): Problem Statement", RFC 7554,
            DOI 10.17487/RFC7554, May 2015,
            <https://www.rfc-editor.org/info/rfc7554>.

[RFC8174]   Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
            2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
            May 2017, <https://www.rfc-editor.org/info/rfc8174>.

7.2. Informative References

[I-D.ietf-6tisch-architecture]
            Thubert, P., "An Architecture for IPv6 over the TSCH mode
            of IEEE 802.15.4", draft-ietf-6tisch-architecture-29 (work
            in progress), August 2020.

[I-D.ietf-6tisch-dtsecurity-secure-join]
            Richardson, M., "6tisch Secure Join protocol", draft-ietf-
            6tisch-dtsecurity-secure-join-01 (work in progress),
            February 2017.

[I-D.ietf-6tisch-terminology]
            Palattella, M., Thubert, P., Watteyne, T., and Q. Wang,
            "Terms Used in IPv6 over the TSCH mode of IEEE 802.15.4e",
            draft-ietf-6tisch-terminology-10 (work in progress), March
            2018.

   [I-D.ietf-roll-capabilities]
              Jadhav, R., Thubert, P., Richardson, M., and R. Sahoo,
              "RPL Capabilities", draft-ietf-roll-capabilities-07 (work
              in progress), September 2020.

   [RFC8137] Kivinen, T. and P. Kinney, "IEEE 802.15.4 Information
              Element for the IETF", RFC 8137, DOI 10.17487/RFC8137, May
              2017, <https://www.rfc-editor.org/info/rfc8137>.

   [RFC8366] Watsen, K., Richardson, M., Pritikin, M., and T. Eckert,
              "A Voucher Artifact for Bootstrapping Protocols",
              RFC 8366, DOI 10.17487/RFC8366, May 2018,
              <https://www.rfc-editor.org/info/rfc8366>.

Appendix A. Change history

   version 00.

Authors' Addresses

   Michael Richardson
   Sandelman Software Works

   Email: mcr+ietf@sandelman.ca

   Rahul Arvind Jadhav
   Huawei Tech

   Email: rahul.ietf@gmail.com