Technical Objective Formats for the Autonomic Network Infrastructure
draft-carpenter-anima-ani-objectives-03

Abstract

This document defines the formats of several technical objectives for
the Generic Autonomic Signaling Protocol (GRASP) used by components
of the Autonomic Networking Infrastructure outlined in the ANIMA
reference model.

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 January 17, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.
1. Introduction

This document defines several technical objectives for use with for the Generic Autonomic Signaling Protocol (GRASP) [I-D.ietf-anima-grasp]. They are intended for use by corresponding Autonomic Service Agents (ASAs) that support infrastructure components of the Autonomic Network Infrastructure (ANI) outlined in the ANIMA reference model [I-D.ietf-anima-reference-model].

Note: This draft is posted to allow systematic discussion of the various objectives in a consistent way. It is possible that rather than this being published as an RFC, the various objective definitions will be incorporated directly in the relevant specifications.

The reference model identifies several infrastructure components that will fit together with GRASP to form the ANI:

Secure Bootstrap.

Autonomic Control Plane (ACP).

Stable Connectivity of Network OAM.

The following sections define GRASP objectives for each of these cases. They are described in an informal object notation and formally using CBOR data definition language (CDDL).
2. Objectives for Secure Bootstrap

Three ANI components are involved in the Bootstrapping Remote Secure Key Infrastructures (BRSKI) process described in [I-D.ietf-anima-bootstrapping-keyinfra]: the Join Registrar, the Join Proxy, and the Pledge (a node joining the domain). In the present document we only consider interactions between autonomic nodes involved in BRSKI; non-autonomic nodes are expected to use different methods not involving GRASP.

Note that since secure bootstrap takes place, by definition, on an incompletely secure network, the use of any protocol needs to be kept as simple and limited as possible. Between the proxy and the pledge, therefore, only one GRASP message type is used — flooding — to avoid giving away any unnecessary information. The proxy and pledge have a link-local connection between them. Mutual discovery and bootstrap can happen without any prior provisioning of helper information by an external mechanism. Instead, link-local multicast with GRASP is used. This will minimize exposure to eavesdroppers and malicious nodes. On the other hand, there may be multiple physical hops between the proxy and the registrar. Therefore, two different GRASP objectives are required: one that is used over an existing secure network (typically the ACP) between the registrar and the proxy, and another that is used over an insecure link-local hop between the proxy and the pledge. Further security aspects are discussed in [I-D.ietf-anima-bootstrapping-keyinfra] and [I-D.ietf-anima-grasp].

2.1. Additional value for GRASP message syntax

This document extends the syntax of the GRASP protocol [I-D.ietf-anima-grasp] by adding an additional value for the "transport-proto" element:

```
transport-proto /= IPPROTO_IPV6
IPPROTO_IPV6 = 41
```

This value indicates IP-in-IP encapsulation.

2.2. Discovered Synchronization Objective for the Join Registrar

The Join Proxy discovers a Join Registrar by using the "AN_join_registrar" GRASP objective. It must only be used when GRASP is running securely, typically because the Join Proxy is in a node that has already joined the ACP. The value of the objective will
indicate the BRSKI methods supported by the registrar and the corresponding locators for BRSKI traffic.

First, the pledge performs GRASP discovery. If multiple responses occur, it chooses one by an implementation-defined method. Then the pledge initiates GRASP synchronization to obtain the BRSKI methods supported by the discovered registrar. Alternatively, if implemented, GRASP rapid mode could be used to combine the two operations.

An example of the objective is informally:

"AN_join_registrar", 5, 6, [["BRSKI-TCP", [O_IPv6_LOCATOR, fd45:1345::6789, 6, 443]]]

The formal CDDL definition is:

```
registrar-objective = ["AN_join_registrar", objective-flags, loop-count, *[method, locator-option]]
```

```
objective-flags = ; as in the GRASP specification
loop-count = ; as in the GRASP specification
locator-option =  ; as in the GRASP specification
method = "BRSKI-TCP" / "BRSKI-UDP" / "BRSKI-IPIP"
          ; name of the BRSKI method supported
```

The objective-flags field is set to indicate synchronization.

The loop-count is set to a suitable value to limit the scope of discovery. A suggested default value is 6.

The Join Proxy, upon receiving this objective, will select one or more of the methods for announcement to Pledges. It will store the provided locator for each method for subsequent BRSKI operations. Note that this locator is distinct from the locator for the Join Registrar’s ASA, which is used only for GRASP operations.

Thus, locators for "BRSKI-TCP", "BRSKI-UDP" and "BRSKI-IPIP" could be:

```
[O_IPv6_LOCATOR, ipv6-address, IPPROTO_TCP, rport1]
[O_IPv6_LOCATOR, ipv6-address, IPPROTO_UDP, rport2]
[O_IPv6_LOCATOR, ipv6-address, IPPROTO_IPV6, null]
```
where 'ipv6-address' is the address of the registrar (typically an ACP address), and 'rport1' and 'rport2' are the appropriate TCP and UDP ports at the registrar.

2.3. Flooded Objective for Join Proxy

A Join Proxy announces itself to potential pledges by use of the "AN_join_proxy" objective. This is a synchronization objective intended only to be flooded on a single link using the GRASP Flood Synchronization (M_FLOOD) message. In accordance with the design of the Flood message, a locator consisting of a specific link-local IP address, IP protocol number and port number will be distributed with the flooded objective. An example of the objective is informally:

["AN_join_proxy", 5, 1, "BRSKI-TCP"]

The formal CDDL definition is:

proxy-objective = ["AN_join_proxy", objective-flags, loop-count, method]

objective-flags = ; as in the GRASP specification
loop-count = 1    ; limit to link-local operation
method = "BRSKI-TCP" / "BRSKI-UDP"

The objective-flags field is set to indicate synchronization.

The loop-count is fixed at 1 since this is a link-local operation.

A Join Proxy that supports more than one method will flood multiple versions of the "AN_join_proxy" objective. As specified for the GRASP M_FLOOD message, a locator may be attached to each version. The 'method' parameter indicates the specific BRSKI method available at the given locator.

Thus, locators for "BRSKI-TCP" and "BRSKI-UDP" would be:

[O_IPv6_LOCATOR, ipv6-address, IPPROTO_TCP, pport1]

[O_IPv6_LOCATOR, ipv6-address, IPPROTO_UDP, pport2]

where 'ipv6-address' is the link-local address of the proxy and 'pport1' and 'pport2' are the appropriate TCP and UDP ports at the proxy.

Note that the BRSKI-IPIP method is never announced to the Pledges, because it applies exclusively between the Proxy and the Join Registrar, being used to encapsulate one of the other methods.
By this mechanism, a proxy may announce one or more connection methods to all pledges, each with an associated link-local address, protocol number and port number.

This objective is only to be used in a Discovery Unsolicited Link-Local (DULL) instance of GRASP [I-D.ietf-anima-grasp].

3. Objective for Autonomic Control Plane

The Autonomic Control Plane (ACP) [I-D.ietf-anima-autonomic-control-plane] constructs itself without outside intervention. To achieve this, each node needs to identify its link-local neighbors on all interfaces, and agree on a secure connection method with each of them. As for the Join Proxy, a flooding mechanism, in which each node announces itself and its security methods to its neighbors, is used.

Thus each autonomic node runs an ASA that supports the corresponding objective. This ASA runs permanently, as long as the node is capable of being part of the ACP, in order to discover or detect new ACP neighbors or to remove failed neighbors.

A node announces itself to potential ACP peers by use of the "AN_ACP" objective. This is a synchronization objective intended to be flooded on a single link using the GRASP Flood Synchronization (M_FLOOD) message. In accordance with the design of the Flood message, a locator consisting of a specific link-local IP address, IP protocol number and port number will be distributed with the flooded objective. An example of the objective is informally:

["AN_ACP", 5, 1, ["IKEv2","dTLS"]]

The formal CDDL definition is:

```
acp-objective = ["AN_ACP", objective-flags, loop-count, method]

objective-flags = ; as in the GRASP specification
loop-count = 1    ; limit to link-local operation
method = "IKEv2" / "dTLS"     ; connection method supported
```

The objective-flags field is set to indicate synchronization.

The loop-count is fixed at 1 since this is a link-local operation.

A node that supports more than one method may flood multiple versions of the "AN_ACP" objective, each accompanied by its own locator, similar to "AN_join_proxy". The 'method' parameter indicates the
specific connection method available at the given locator. The initial possible values are "IKEv2" and "dTLS".

This objective is only to be used in a Discovery Unsolicited Link-Local (DULL) instance of GRASP [I-D.ietf-anima-grasp].

Note that a node serving both as an ACP node and BRSKI Join Proxy may choose to distribute the "AN_ACP" objective and "AN_join_proxy" objective in the same flood message, since GRASP allows multiple objectives in one flood message.

4. Objective for Stable Connectivity of Network OAM

For OAM purposes [I-D.ietf-anima-stable-connectivity], a special-purpose ASA, which we will call the NOC ASA, mediates connectivity between NOC systems performing OAM operations and autonomic nodes that can be reached securely via the ACP. This requires a discovery operation, which could be handled in two ways: the NOC ASA discovers all nodes, or each node discovers the NOC ASA. The latter seems much more practical since nodes might join or leave the network at any time. However, the NOC might need to know something about each target node, so the corresponding objective is defined as a negotiation objective to allow for this: each node can pass data to the NOC in an M_REQ_NEG message, and receive data from the NOC in an M_NEGOTIATE message.

An example of the objective is informally:

["AN_NOC", 3, 6, [TBD]]

The formal CDDL definition is:

noc-objective = ["AN_NOC", objective-flags, loop-count, [TBD]]

objective-flags = ; as in the GRASP specification
TBD = any ; node information to be defined

The objective-flags field is set to indicate negotiation.

Dry run mode must not be used.

The loop-count is set to a suitable value to limit the scope of discovery. A suggested default value is 6.

When a node joins the ACP, one of its initial actions must be to perform GRASP discovery for "AN_NOC" and then to send a Request Negotiate message to the NOC ASA supplying the value TBD. If successfully received, the NOC ASA should reply with a Negotiate message.
message, providing a value TBD in return. This value will inform the requesting node of various NOC parameters. The requesting node must then send an End Negotiate message. From then on, any OAM communication between NOC services and the node in question will proceed over the ACP using the information TBD.

5. Flood Frequency

Any ASA that floods one of the above objectives should do so at a carefully chosen frequency. Recipient nodes may be starting up, reconnecting, or waking up from sleep, so floods need to be refreshed periodically. On the other hand, excessive flooding will consume bandwidth, CPU and battery capacity throughout the network, and might even resemble a DoS attack. A general guideline is to flood an objective once immediately after its value is initialised or changed, and then repeat the flood at intervals of at least 30 seconds. Additionally, the flooding interval should be slightly jittered to avoid synchronicity with other floods. Finally, the value of a flooded objective should change as rarely as possible (on a timescale of at least minutes, not seconds).

6. Security Considerations

General security issues for GRASP are covered in [I-D.ietf-anima-grasp]. The objectives "AN_join_proxy" and "AN_ACP" must be implemented using a DULL instance of GRASP. Specific issues not mentioned above are discussed in the referenced drafts for each use case.

7. IANA Considerations

IANA is requested to add the following entries to the GRASP Objective Names Table registry created by [I-D.ietf-anima-grasp]:

   AN_join_registrar
   AN_join_proxy
   AN_ACP
   AN_NOC

8. Acknowledgements

Valuable comments were made by Toerless Eckert, Max Pritikin, and Michael Richardson.
9. References

9.1. Normative References

[I-D.greevenbosch-appsawg-cbor-cddl]

[I-D.ietf-anima-grasp]

9.2. Informative References

[I-D.ietf-anima-autonomic-control-plane]

[I-D.ietf-anima-bootstrapping-keyinfra]

[I-D.ietf-anima-reference-model]

[I-D.ietf-anima-stable-connectivity]

Appendix A. Change log [RFC Editor: Please remove]

draft-carpenter-anima-ani-objectives-03, 2017-07-16:
Align with latest BRSKI and ACP drafts and discussions, various details corrected.

draft-carpenter-anima-ani-objectives-02, 2017-06-30:
Limited scope to initial ANI components

Updated details and removed alternatives

draft-carpenter-anima-ani-objectives-01, 2017-02-13:

Added prefix management case

Updated objectives for BRSKI

Editorial corrections

draft-carpenter-anima-ani-objectives-00, 2016-11-15:

Initial version

Authors’ Addresses

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland 1142
New Zealand

Email: brian.e.carpenter@gmail.com

Bing Liu
Huawei Technologies Co., Ltd
Q22, Huawei Campus
No.156 Beiqing Road
Hai-Dian District, Beijing 100095
P.R. China

Email: leo.liubing@huawei.com