Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 18, 2020

B. Carpenter
Univ. of Auckland

October 16, 2019

Quick and Dirty Security for GRASP
draft-carpenter-anima-quads-grasp-00

Abstract

A secure substrate is required by the Generic Autonomic Signaling Protocol (GRASP) used by Autonomic Service Agents. This document describes QUADS, a QUick And Dirty Security method using symmetric cryptography and preconfigured keys or passwords.

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 April 18, 2020.

Table of Contents

1. Introduction

As defined in [I-D.ietf-anima-reference-model], the Autonomic Service Agent (ASA) is the atomic entity of an autonomic function, and it is instantiated on autonomic nodes. When ASAs communicate with each other, they should use the Generic Autonomic Signaling Protocol (GRASP) [I-D.ietf-anima-grasp]. It is essential that such communication is strongly secured to avoid malicious interference with the Autonomic Network Infrastructure (ANI).

For this reason, GRASP must run over a secure substrate that is isolated from regular data plane traffic. This substrate is known as the Autonomic Control Plane (ACP). A method for constructing an ACP at the network layer is described in [I-D.ietf-anima-autonomic-control-plane]. Scenarios for link layer ACPs are discussed in [I-D.carpenter-anima-l2acp-scenarios]. The present document describes a simple method of emulating an ACP immediately above the transport layer, known as QUADS (QUick And Dirty Security) for GRASP.

2. Method

Every GRASP message, whether unicast or multicast, is encrypted immediately before transmission, and decrypted immediately after reception, using the same symmetric encryption algorithm and domain-wide shared keys. This applies to all unicast and multicast messages sent over either UDP or TCP. Typically encryption will take place immediately after a message is encoded as CBOR [RFC7049], and decryption will take place immediately before a message is decoded from CBOR.

There is no attempt to specify an automatic algorithm choice or key distribution mechanism. Every instance of GRASP in a given Autonomic

Network (AN) must be pre-configured with the choice of encryption algorithm and any necessary parameters, and with the same key(s).

An alternative to configuring the keys is that every instance of GRASP is pre-configured with a fixed salt value and the keys are created from a locally chosen domain password, using a pre-defined hash algorithm and that salt value. Note that the salt value cannot be secret as it must be the same in all QUADS for all GRASP implementations. In this model the secrecy depends on the password.

The choice of algorithms should follow best current practice, e.g. [RFC8221].

3. Implementation Status [RFC Editor: please remove]

QUADS for GRASP has been implemented as a small extension to the Python GRASP prototype, using the Python 'cryptography' module. The algorithm choices were:

Encryption: AES/CBC, key lengths 32/16, padding PKCS7(128).

Password hash: PBKDF2HMAC SHA256, length 32, 100000 iterations.

Salt used for password hash: 0xf474526a2e74accee189f1fbc1c34ceb.

The code will be posted to https://github.com/becarpenter/graspy when stable.

4. Security Considerations

QUADS provides effective secrecy for all GRASP messages, against any party not in possession of the relevant shared keys. However, before a GRASP message is encrypted or after it is decrypted, it is not protected within the host. Therefore, secrecy is only effective against nodes that do not contain a GRASP instance in possession of the keys. Those nodes cannot send valid GRASP messages, and they cannot interpret intercepted GRASP messages, including multicasts. However, they might attempt traffic analysis.

QUADS provides authentication of GRASP instances to the extent that they must be in possession of the relevant shared keys.

QUADS depends on manual configuration of keys, or on password entry, for each autonomic node.

QUADS offers no defence against denial of service attacks.

5. IANA Considerations

This document makes no request of the IANA.

6. Acknowledgements

Excellent suggestions were made by TBD

7. References

7.1. Normative References

[RFC8221] Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 8221, DOI 10.17487/RFC8221, October 2017, <https://www.rfc-editor.org/info/rfc8221>.

7.2. Informative References

[I-D.carpenter-anima-l2acp-scenarios]
Carpenter, B. and B. Liu, "Scenarios and Requirements for Layer 2 Autonomic Control Planes", draft-carpenter-anima-l2acp-scenarios-01 (work in progress), October 2019.

[I-D.ietf-anima-autonomic-control-plane]
Eckert, T., Behringer, M., and S. Bjarnason, "An Autonomic Control Plane (ACP)", draft-ietf-anima-autonomic-control-plane-20 (work in progress), July 2019.

[I-D.ietf-anima-grasp]
Bormann, C., Carpenter, B., and B. Liu, "A Generic Autonomic Signaling Protocol (GRASP)", draft-ietf-anima-grasp-15 (work in progress), July 2017.

[I-D.ietf-anima-reference-model]
Behringer, M., Carpenter, B., Eckert, T., Ciavaglia, L., and J. Nobre, "A Reference Model for Autonomic Networking", draft-ietf-anima-reference-model-10 (work in progress), November 2018.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

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

draft-carpenter-anima-quads-grasp-00, 2019-10-16:

Initial version

Author's Address

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

Email: brian.e.carpenter@gmail.com