Workgroup: CoRE
Internet-Draft:
draft-amsuess-core-edhoc-grease-01
Published: 22 October 2023
Intended Status: Informational
Expires: 24 April 2024
Authors: C. Amsüss

Applying Generate Random Extensions And Sustain Extensibility (GREASE) to EDHOC Extensibility

Abstract

This document applies the extensibility mechanism GREASE (Generate Random Extensions And Sustain Extensibility), which was pioneered for TLS, to the EDHOC ecosystem. It reserves a set of non-critical EAD labels and unusable cipher suites that may be included in messages to ensure peers correctly handle unknown values.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the Constrained RESTful Environments Working Group mailing list (core@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/core/.

Source for this draft and an issue tracker can be found at https://gitlab.com/chrysn/core-edhoc-grease.

Status of This Memo

Table of Contents

1. Introduction

[See abstract]

The introduction of [RFC8701] provides comprehensive motivation for adding such extensions.

The extension points of the EDHOC protocol ([I-D.ietf-lake-edhoc]) are cipher suites, methods, EADs (External Authorization Data items) and COSE headers. Of these, EADs and cipher suites can be used in such a way that even in the presence of an unknown value, a connection can still be established.

Unlike in TLS GREASE, EDHOC is operating on tight bandwidth and message size budget, with some messages just barely fitting within relevant networks' fragmentation limits. Thus, more than with TLS GREASE, it is up to implementations to decide whether in their particular use case they can afford to send addtional data.

2. The GREASE EAD labels

This document registers the following EAD labels as GREASE EADs:

160, 41120, 43690, 44975

These EADs are available in all EDHOC messages. The EADs are only used in their positive (non-critical) form.

2.1. Use of GREASE EADs by message senders

A sender of an EDHOC message MAY send a GREASE EAD using the non-critical (positive) form at any time, with any or no EAD value (that is, with or without a byte string of any usable length), in any message.

Senders SHOULD consider the properties of the network their messages are sent over, and refrain from adding GREASE when its use would be detrimental to the network (for example, when the added size causes fragmentation of the message).

On networks where the data added by the grease EADs does not significantly impact the network, senders SHOULD irregularly send arbitrary (possibly random) GREASE EADs with their messages to ensure that errors resulting from the use of GREASE are detected.

The GREASE EADs MAY be used as an alternative form of padding.

2.1.1. Pattern for limited fingerprinting

A method of deciding how to apply GREASE is suggested as follows:

* For every message, use GREASE with a random probability of 1 in 64.

* Pick a random GREASE label out of the uniform distribution of available options.

* Pick a random length from the uniformly distributed interval 9 to 40 (inclusive).

* Add the selected GREASE label with a value of the selected length, filled with random bytes.

2.2. Use of GREASE EADs by message recipients

A party receiving a GREASE EAD MUST NOT alter its behavior in any way that would allow random GREASE EADs to alter the security context that gets established.

It MAY alter its behavior in other ways; in particular, it SHOULD randomly insert GREASE EADs in later messages of an exchange in which any were received.

If it does not alter its behavior, it is RECOMMENDED that implementations make no attempt to recognize GREASE EADs, and apply the default processing -- that is, to ignoring any unknown non-critical EADs.

3. GREASE cipher suites

This document registers the following cipher suites:

160, 41120, -41121, 43690

An initiator may insert a GREASE cipher suite at any position in its sequence of preferred cipher suites.

A responder MUST NOT support any of these cipher suites, and MUST treat them like any other cipher suite it does not support.

Thus, these cipher suites never occur as the selected cipher suite. An initiator whose choice of a GREASE cipher suite is accepted needs to discontinue the protocol.

4. Privacy considerations

The way in which GREASE is applied can contribute to identifying which implementation of EDHOC is being used. Implementers of EDHOC are encouraged to use the algorithm described in Section 2.1.1, both to reduce the likelihood of their implementation to be identified through the use of GREASE and to increase the anonymity set of other users of the same algorithm.

5. Security Considerations

The use of the GREASE option has no impact on security in a correct EDHOC implementation.

6. IANA considerations

6.1. EDHOC EADs

IANA is requested to register four new entries into the EDHOC External Authorization Data Registry established in [I-D.ietf-lake-edhoc]:

160, 41120, 43690, 44975

All share the name "GREASE", the description "Arbitrary data to ensure extensibility", and this document as a reference.

6.2. EDHOC cipher suites

IANA is requested to register four new values into the EDHOC Cipher Suites Registry established in [I-D.ietf-lake-edhoc]:

160, 41120, -41121, 43690

All share the name "GREASE", the array N/A, the description "Unimplementable cipher suite to ensure extensibility", and this document as a reference.

7. References

7.1. Normative References

[I-D.ietf-lake-edhoc] Selander, G., Mattsson, J. P., and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)", Work in Progress, Internet-Draft, draft-ietf-lake-edhoc-22, 25 August 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-lake-edhoc-22>.

7.2. Informative References

[RFC8701] Benjamin, D., "Applying Generate Random Extensions And Sustain Extensibility (GREASE) to TLS Extensibility", RFC 8701, DOI 10.17487/RFC8701, January 2020, <https://www.rfc-editor.org/rfc/rfc8701>.

Appendix A. Open questions

Do the GREASE EADs add any value that padding does not already add?

Probably yes, because padding is "special enough" that it could be handled in a hard-coded fashion. (Then again, there's nothing but the effort stopping anyone else from doing the same with the GREASE EADs, right?)

Can anything be done about extra methods and COSE headers?

They would not result in successful operations, but maybe there is still some value in registering one or two -- using them would mean sacrificing the full connection, but it may still be possible to conclude that the extension points are in order from watching the EDHOC exchange fail in the predicted way.

Appendix B. Change log

Since -00:

* Fixed a mix-up between positivity and criticality of options.

* Adjusted numbers accordingly to once more fit in the 0xa. pattern (actually they're using 0x.a, but that doesn't work the same way with CBOR).

* Text improvements around recipient side processing.

Acknowledgements

Marco Tiloca pointed out a critical error in the numeric constructions. Göran Selander provided input to reduce mistakable text.

Author's Address

Christian Amsüss
Austria

Email: christian@amsuess.com