DIME
Internet-Draft
Intended status: Standards Track
Expires: August 22, 2013

H. Tschofenig, Ed.
Nokia Siemens Networks
J. Korhonen
Renesas Mobile
G. Zorn
Network Zen

February 18, 2013

Diameter AVP Level Security: Requirements and Scenarios
draft-tschofenig-dime-e2e-sec-req-00.txt

Abstract

This specification discusses requirements for providing Diameter security at the level of individual Attribute Value Pairs.

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 August 22, 2013.

Copyright Notice

Copyright (c) 2013 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.

Table of Contents

1. Introduction

The Diameter Base specification [1] offers security protection between neighboring Diameter peers and mandates that either TLS (for TCP), DTLS (for SCTP), or IPsec is used. These security protocols offer a wide range of security properties, including entity authentication, data-origin authentication, integrity, confidentiality protection and replay protection. They also support a large number of cryptographic algorithms, algorithm negotiation, and different types of credentials.

The need to also offer additional security protection of AVPs between non-neighboring Diameter nodes was recognized very early in the work on Diameter. This lead to work on Diameter security using the Cryptographic Message Syntax (CMS) [3]. Due to lack of deployment interest at that time (and the complexity of the developed solution) the specification was, however, never completed.

In the meanwhile Diameter had received a lot of deployment interest from the cellular operator community and because of the sophistication of those deployments the need for protecting Diameter AVPs between non-neighboring nodes re-surfaced. Since early 2000 (when the work on [3] was discontinued) the Internet community had seen advances in cryptographic algorithms (for example, authenticated encryption algorithms were developed) and new requirements emerged.

This document collects requirements for developing a solution to protect Diameter AVPs.

2. Terminology

The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' in this specification are to be interpreted as described in [2].

This document re-uses terminology from the Diameter base specification [1].

3. Use Case

Consider the following use case shown in Figure 1. A Diameter client interacts with a Diameter server through two Diameter proxies. The Diameter client and the Diameter Proxy A belong to the same realm, example.com.

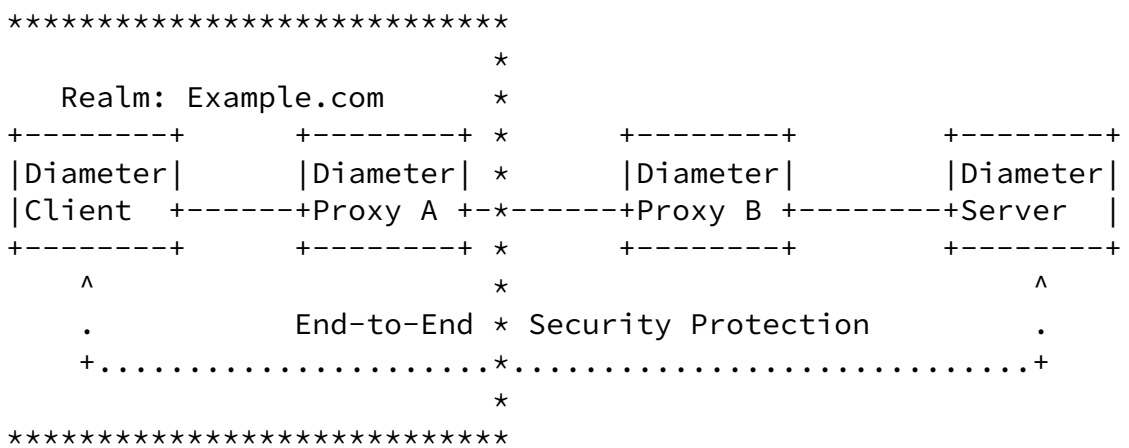

Figure 1: Example Diameter Deployment Setup.

The Diameter AVPs are protected end-to-end, from the Diameter client to the Diameter server, as shown in Figure 1 with the dotted line.

Other use cases are possible as well. For example, Diameter Proxy A could act on behalf of the Diameter clients in the example.com realm. In a general case, however, encryption of AVPs between arbitrary Diameter nodes can be challenging since it is upfront not know what Diameter nodes a message will traverse.

QUESTION: Which scenarios should be supported? Should the focus be on the protection of selected Diameter AVPs between the Diameter client to the Diameter server only?

4. Requirements

Requirement #1: Solutions MUST support an extensible set of cryptographic algorithms.

Motivation: Crypto-agility is the ability of a protocol to adapt to evolving cryptographic algorithms and security requirements. This may include the provision of a modular mechanism to allow cryptographic algorithms to be updated without substantial disruption to deployed implementations.

Requirement #2: Solutions MUST support confidentiality, integrity, and data-origin authentication.

QUESTION: Should solutions for integrity protection work in a

backwards-compatible way with existing Diameter applications? Should the list of integrity protected AVP be indicated in the protected payload itself?

Requirement #3: Solutions MUST support replay protection.

QUESTION: Should replay protection be based on timestamps (i.e., assume synchronized clocks in Diameter networks)?

Requirement #4: Solutions MUST be able to selectively apply their cryptographic protection to certain Diameter AVPs.

Requirement #5: Solutions MUST recommend a mandatory-to-implement cryptographic algorithm.

Requirement #6: QUESTION: Should we support symmetric keys and / or also asymmetric keys?

Requirement #7: QUESTION: Should requirements for dynamic key management be included in this document as well?

Requirement #8: QUESTION: Should statically provisioned keys be supported?

Requirement #9: QUESTION: Should solutions allow the provisioning of long-term shared symmetric credentials via a command-line interface / text file?

5. Security Considerations

This entire document focused on the discussion of new functionality for securing Diameter AVPs end-to-end.

6. IANA Considerations

This document does not require actions by IANA.

7. Acknowledgments

We would like to thank Guenther Horn for his review comments.

8. References

8.1. Normative References

[1] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", RFC 6733, October 2012.

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

8.2. Informative References

[3] Calhoun, P., Farrell, S., and W. Bulley, "Diameter CMS Security Application", draft-ietf-aaa-diameter-cms-sec-04 (work in progress), March 2002.

Authors' Addresses

Hannes Tschofenig (editor)
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at

Jouni Korhonen
Renesas Mobile
Porkkalankatu 24
Helsinki 00180
Finland

Email: jouni.nospam@gmail.com

Glen Zorn
Network Zen
227/358 Thanon Sanphawut
Bang Na Bangkok 10260
Thailand

Email: glenzorn@gmail.com