

DIME
Internet-Draft
Intended status: Informational
Expires: December 10, 2016

H. Tschofenig
ARM Limited
J. Korhonen, Ed.
Broadcom Limited
G. Zorn
Network Zen
K. Pillay
Internet Solutions
June 8, 2016

**AVP Level Security for Non-neighboring Diameter Nodes: Scenarios and
Requirements
draft-ietf-dime-e2e-sec-req-05.txt**

Abstract

This specification specifies 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 December 10, 2016.

Copyright Notice

Copyright (c) 2016 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	2
2.	Terminology	3
3.	Security Threats	3
4.	Scenarios for Diameter AVP-Level Protection	5
5.	Requirements	7
6.	Security Considerations	8
7.	IANA Considerations	8
8.	Acknowledgments	8
9.	References	9
9.1.	Normative References	9
9.2.	Informative References	9
	Authors' Addresses	9

[1.](#) Introduction

The Diameter base protocol specification [2] defines security protection between neighboring Diameter peers. The Diameter mandates that peer connections must be protected by TLS (for TCP) [6], DTLS (for SCTP) [7] or using security mechanisms that are independent of Diameter such as IPsec [5]. 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. It should be understood that TLS/DTLS/IPsec in Diameter context does not provide end-to-end security unless the Diameter nodes are direct peers i.e., neighboring Diameter nodes. The current Diameter security is realized hop-by-hop.

The need to also offer additional security protection of Attribute Value Pairs (AVP) between non-neighboring Diameter nodes was recognized very early in the work on Diameter. This led 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) and new security building blocks were developed.

This document specifies requirements for developing a solution to protect Diameter AVPs between non-neighborng Diameter nodes.

2. Terminology

The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' in this documents are to be interpreted as described in [RFC 2119](#) [1].

This document re-uses terminology from the Diameter base specification [2].

In the figures below Attribute Value Pair (AVP) refers to an unprotected AVP and {AVP}k refers to an AVP that experiences security protection (using key "k") without further distinguishing between integrity and confidentiality protection.

The following terms are also used in this document:

AAA Broker

An entity that manages AAA traffic between roaming partner networks.

AAA Broker Network

A network operated by an AAA Broker, which consists of necessary AAA functions to provide AAA brokering services for its customer AAA networks.

Diameter Firewall

A Diameter firewall is a proxy (or a relay) agent that acts similarly to conventional IP traffic firewalls but only at the Diameter AVP and command level. A Diameter firewall may, for example, discard security policy offending AVPs from traversing through it. The Diameter firewall may even discard entire Diameter messages based on the security policy.

3. Security Threats

The following description aims to illustrate various security threats that raise the need for protecting Diameter Attribute-Value Pairs (AVPs). Figure 1 illustrates an example of Diameter based roaming

architecture in which Diameter clients within the visited networks need to interact with Diameter servers in the home domain. AAA domains are interconnected using a Diameter-based AAA interconnection network labeled as AAA Broker.

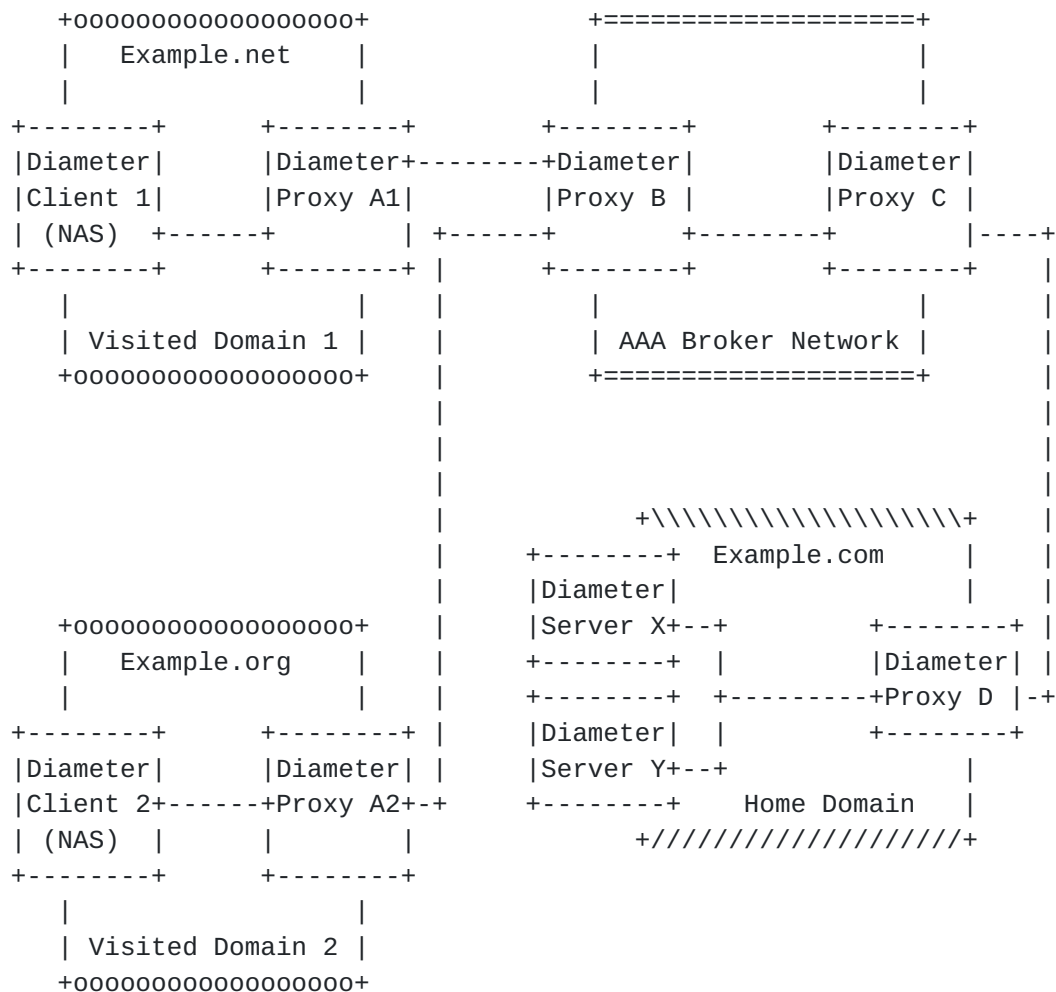


Figure 1: Example Diameter Deployment.

Eavesdropping: Some Diameter applications carry information that is only intended for consumption by end points, either by the Diameter client or by the Diameter server but not by intermediaries. As an example, consider the Diameter EAP application [4] that allows the transport of keying material between the Diameter server to the Diameter client (using the EAP-Master-Session-Key AVP) for the protection of the air interface (i.e., the wireless link) between the end device (such as a mobile phone; not shown in the figure) and the Network Access Server (NAS). The content of the EAP-Master-Session-Key AVP should

benefit from protection against eavesdropping by intermediaries. Other AVPs, for example those listed in Section 13.3 of [2], might also carry sensitive personal data that, when collected by intermediaries, allow for traffic analysis.

In context of the deployment shown in Figure 1 the adversary could, for example, be in the AAA broker network.

Injection and Manipulation: The Diameter base protocol specification mandates security protection between neighboring nodes but Diameter agents may be compromised or misconfigured and inject or manipulate AVPs. To detect such actions additional security protection needs to be applied at the Diameter layer.

Nodes that could launch such an attack are any Diameter agents along the end-to-end communication path.

Impersonation: Imagine a case where a Diameter message from Example.net contains information claiming to be from Example.org. This would either require strict verification at the edge of the AAA broker network or cryptographic assurance at the Diameter layer to prevent a successful impersonation attack.

Any Diameter realm could launch such an attack aiming for financial benefits or to disrupt service availability.

4. Scenarios for Diameter AVP-Level Protection

This scenario outlines a number of cases for deploying security protection of individual Diameter AVPs.

In the first scenario, shown in Figure 2, end-to-end security protection is provided between the Diameter client and the Diameter server with any number of intermediate Diameter agents. Diameter AVPs exchanged between these two Diameter nodes may be protected end-to-end (notation '{AVP}k') or unprotected (notation 'AVP').



Figure 2: End-to-End Diameter AVP Security Protection.

In the second scenario, shown in Figure 3, a Diameter proxy acts on behalf of the Diameter client with regard to security protection. It

applies security protection to outgoing Diameter AVPs and verifies incoming AVPs. Typically, the proxy enforcing the security protection belongs to the same domain as the Diameter client/server without end-to-end security features.

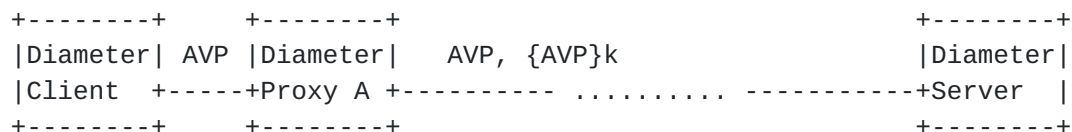


Figure 3: Middle-to-End Diameter AVP Security Protection.

In the third scenario shown in Figure 4 a Diameter proxy acts on behalf of the Diameter server.



Figure 4: End-to-Middle Diameter AVP Security Protection.

The fourth and the final scenario (see Figure 5) is a combination of the end-to-middle and the middle-to-end scenario shown in Figure 4 and in Figure 3. From a deployment point of view this scenario is easier to accomplish for two reasons: First, Diameter clients and Diameter servers remain unmodified. This ensures that no modifications are needed to the installed Diameter infrastructure, except for the security enabled proxies obviously. Second, the key management is also simplified since fewer number of keys need to be negotiated and provisioned. The assumption here is that the number of security enabled proxies would be significantly less than unprotected Diameter nodes in the installed base.



Figure 5: Middle-to-Middle Diameter AVP Security Protection.

5. Requirements

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

Motivation: Solutions MUST be able to evolve 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: The solution MUST support confidentiality, integrity, and data-origin authentication. Solutions for integrity protection MUST work in a backwards-compatible way with existing Diameter applications and therefore be able to traverse legacy proxy and relay agents.

Requirement #3: The solution MUST support replay protection.

Requirement #4: The solution MUST support the ability to delegate security functionality to another entity

Motivation: As described in [Section 4](#) the ability to let a Diameter proxy to perform security services on behalf of all clients within the same administrative domain is important for incremental deployability. The same applies to the other communication side where a load balancer terminates security services for the servers it interfaces.

Requirement #5: The solution MUST be able to selectively apply their cryptographic protection to certain Diameter AVPs.

Motivation: Some Diameter applications assume that certain AVPs are added, removed, or modified by intermediaries. As such, it must be possible to apply security protection selectively. Furthermore, there are AVPs that must not be confidentiality protected but may still be integrity protected such as those required for Diameter message routing.

Requirement #6: The solution MUST define a mandatory-to-implement cryptographic algorithm.

Motivation: For interoperability purposes it is beneficial to have a mandatory-to-implement cryptographic algorithm specified (unless profiles for specific usage environments specify otherwise).

Requirement #7: The solution MUST support symmetric keys and asymmetric keys.

Motivation: Symmetric and asymmetric cryptographic algorithms provide different security services. Asymmetric algorithms, for example, allow non-repudiation services to be offered.

Requirement #8: A solution for dynamic key management MUST be included in the overall solution framework.

However, it is assumed that no "new" key management protocol needs to be developed; instead existing ones are re-used, if at all possible. Rekeying could be triggered by (a) management actions and (b) expiring keying material.

6. Security Considerations

This entire document focused on the discussion of new functionality for securing Diameter AVPs selectively between non-neighbor nodes.

Various security threats are mitigated by selectively applying security protection for individual Diameter AVPs. Without protection there is the possibility for password sniffing, confidentiality violation, AVP insertion, deletion or modification. Additionally, applying digital signature offers non-repudiation capabilities; a feature not yet available in today's Diameter deployment. Modification of certain Diameter AVPs may not necessarily be the act of malicious behavior but could also be the result of misconfiguration. An over-aggressively configured firewalling Diameter proxy may also remove certain AVPs. In most cases data origin authentication and integrity protection of AVPs will provide the most benefits for existing deployments with minimal overhead and (potentially) operating in a full-backwards compatible manner.

7. IANA Considerations

This document does not require actions by IANA.

8. Acknowledgments

We would like to thank Guenther Horn, Martin Dolly, Steve Donovan, Lionel Morand and Tom Taylor (rest in peace Tom) for their review comments.

The authors also thank Qin Wu, Christer Holmberg, Ben Campbell and Radia Perlman who provided additional reviews during the Last Call.

9. References

9.1. Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [2] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", [RFC 6733](#), DOI 10.17487/RFC6733, October 2012, <<http://www.rfc-editor.org/info/rfc6733>>.

9.2. 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.
- [4] Eronen, P., Ed., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", [RFC 4072](#), DOI 10.17487/RFC4072, August 2005, <<http://www.rfc-editor.org/info/rfc4072>>.
- [5] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), DOI 10.17487/RFC4301, December 2005, <<http://www.rfc-editor.org/info/rfc4301>>.
- [6] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), DOI 10.17487/RFC5246, August 2008, <<http://www.rfc-editor.org/info/rfc5246>>.
- [7] Tuexen, M., Seggelmann, R., and E. Rescorla, "Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)", [RFC 6083](#), DOI 10.17487/RFC6083, January 2011, <<http://www.rfc-editor.org/info/rfc6083>>.

Authors' Addresses

Hannes Tschofenig
ARM Limited
Austria

Email: Hannes.tschofenig@gmx.net
URI: <http://www.tschofenig.priv.at>

Jouni Korhonen (editor)
Broadcom Limited
3151 Zanker Rd.
San Jose, CA 95134
USA

Email: jouni.nospam@gmail.com

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

Email: glenzorn@gmail.com

Kervin Pillay
Internet Solutions
South Africa

Email: kervin.pillay@gmail.com

