DIME
Internet-Draft
Intended status: Standards Track
Expires: March 30, 2014

H. Tschofenig, Ed.
Nokia Solutions and Networks
J. Korhonen
Renesas Mobile
G. Zorn
Network Zen
K. Pillay
Oracle Communications

September 26, 2013

Diameter AVP Level Security: Scenarios and Requirements
draft-ietf-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

Copyright Notice

Table of Contents

1. Introduction

The Diameter Base specification [2] 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 security building blocks were developed.

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 [1].

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

3. Use Case

Consider the following use case shown in Figure 1 where a a Diameter client wants to interact with its home Diameter server in the example.com realm. The visited domain the Diameter client is attached to makes use of a AAA interconnection provider, shown as AAA Broker in our example. While both the administrators of the visited as well as the home domain are likely to main a business relationship with the intermediate AAA broker network they may want to ensure that certain Diameter AVPs are not sent in the clear or are integrity protected. Note that the security services are likely offered between Diameter Proxy A and Diameter Proxy D for ease of deployment. Proxy A may act on behalf of the Diameter client and Diameter Proxy D acts on behalf of Diameter Server X and Y it serves.

```
      +oooooooooooooooooo+              +====================+
      |                  |              |                    |
      |                  |              |                    |
   +--------+      +--------+        +--------+        +--------+
   |Diameter|      |Diameter|        |Diameter|        |Diameter|
   |Client  +------+Proxy A +--------+Proxy B +--------+Proxy C |----+
   +--------+      +--------+        +--------+        +--------+    |
      |                  |              |                    |       |
      |  Visited Domain  |              |      AAA Broker    |       |
      +oooooooooooooooooo+              +====================+       |
                                                                     |
                                                                     |
                                                                     |
                                        +\\\\\\\\\\\\\\\\\\\\+       |
                                 +--------+  Example.com     |       |
                                 |Diameter|                  |       |
                                 |Server X+--+         +--------+    |
                                 +--------+  |         |Diameter|    |
                                 +--------+  +---------+Proxy D |----+
                                 |Diameter|  |         +--------+
                                 |Server Y+--+               |
                                 +--------+    Home Domain   |
                                        +////////////////////+
```

Figure 1: Example Diameter Deployment Setup.

Based on Figure 1 the following use cases can be differentiated. AVP refers to an unprotected AVP and {AVP}k refers to an AVP that experiences security protection without further distinguishing between integrity and confidentiality protection.

In the first scenario, shown in Figure 2, end-to-end security protection is provided between the Diameter client and the Diameter server. Diameter AVPs exchanged between these two Diameter nodes are protected.

```
   +--------+                                                +--------+
   |Diameter| AVP, {AVP}k                                    |Diameter|
   |Client  +-----------------........... -------------------+Server  |
   +--------+                                                +--------+
```

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.

```
   +--------+     +--------+                                 +--------+
   |Diameter| AVP |Diameter|   AVP, {AVP}k                   |Diameter|
   |Client  +-----+Proxy A +---------- .......... -----------+Server  |
   +--------+     +--------+                                 +--------+
```

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.

```
   +--------+                                 +--------+     +--------+
   |Diameter| AVP, {AVP}k                     |Diameter| AVP |Diameter|
   |Client  +-----------------........... ----+Proxy D +-----+Server  |
   +--------+                                 +--------+     +--------+
```

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

The forth and 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. Second, key management is also simplified since fewer number of key pairs need to be negotiated and provisioned.

```
+--------+     +--------+                  +--------+     +--------+
|Diameter| AVP |Diameter|   AVP, {AVP}k    |Diameter| AVP |Diameter|
|Client  +-----+Proxy A +-- .......... ----+Proxy D +-----+Server  |
+--------+     +--------+                  +--------+     +--------+
```

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

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 most benefits for existing deployments with minimal overhead and (potentially) operating in a full-backwards compatible manner.

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. Solutions for integrity protection MUST work in a backwards-compatible way with existing Diameter applications.

Requirement #3: Solutions MUST support replay protection. Any Diameter node has an access to network time and thus can synchronise their clocks.

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

Motivation: As described in Section 3 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: Solutions 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 may be necessary to apply security protection selectively.

Requirement #6: Solutions MUST recommend 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: Solutions 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 has to be provided. 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.

Requirement #9: The ability to statically provisioned keys (symmetric as well as asymmetric keys) has to be supported to simplify management for small-scale deployments that typically do not have a back-end network management infrastructure.

Requirement #10: Capability/Policy Discovery: This document talks about selectively protecting Diameter AVPs between different Diameter nodes. A Diameter node has to be configured such that it applies security protection to a certain number of AVPs. A number of policy related questions arise: What keying material should be used so that the intended recipient is also able to verify it? What AVPs shall be protected so that the result is not rejected by the recipient? In case of confidentiality protection the Diameter node encrypting AVPs needs to know ahead of time what other node is intended to decrypt them. Should the list of integrity protected AVP be indicated in the protected payload itself (or is it known based on out-of-band information)? Is this policy / capability information assumed to be established out-of-band (manually) or is there a protocol mechanism to distribute this information?

Requirement #11: Command-Line Support: Should solutions allow the provisioning of long-term shared symmetric credentials via a command-line interface / text file? This allows easier management for small-scale deployments.

5. Security Considerations

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

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

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

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 Solutions and 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

Kervin Pillay
Oracle Communications
100 Crosby Drive
Bedford, Massachusettes 01730
USA

Email: kervin.pillay@oracle.com