Header Field Parameter for Media Plane Security
draft-dawes-dispatch-mediasec-parameter-00.txt

Abstract

Negotiating the security mechanisms used between a Session Initiation Protocol (SIP) user agent and its next-hop SIP entity is already described in an RFC. This document extends negotiation of a security mechanism to the media plane by defining a new Session Initiation Protocol (SIP) header field parameter to label security mechanisms that apply to the media plane.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [3].

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 21, 2010.

Copyright Notice
Copyright (c) 2010 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 BSD License.

Table of Contents

1. Introduction ................................. 3
   1.1. Motivations ............................. 3
   1.2. Design Goals ............................ 3
2. Solution .................................... 4
   2.1. Relationship to RFC3329 ............ 4
   2.2. Overview of Operation .............. 4
   2.3. Syntax ................................. 5
   2.4. Protocol Operation .................. 5
      2.4.1. The "mediasec" Header Field Parameter ..... 5
      2.4.2. Client Initiated ................. 6
      2.4.3. Server Initiated ............... 6
   2.5. Security Mechanism Initiation .... 6
   2.6. Duration of Security Associations .. 6
   2.7. Summary of Header Field Use ....... 6
3. Backwards Compatibility .................... 6
4. Examples .................................... 6
   4.1. Client Initiated ....................... 6
   4.2. Server Initiated ..................... 8
5. Formal Syntax ................................ 8
6. Acknowledgements ........................... 9
7. IANA Considerations ........................ 9
   7.1. Registration Information ............ 9
   7.2. Registration Template ............ 9
   7.3. Header Field Names .................. 9
   7.4. Response Codes ..................... 10
   7.5. Option Tags ......................... 10
8. Security Considerations .................... 10
9. References ................................ 10
   9.1. Normative References .............. 10
   9.2. Informative References ............ 10
Appendix A. Additional stuff ................ 10
Author’s Address ........................... 11
1.  Introduction

RFC 3329 [1] describes negotiation of a security mechanism for SIP signalling between a UAC and its first hop proxy. This document extends the concept of security negotiation by added exchange of security capability for the media plane. Similar to the signalling plane, the evolution of security mechanisms for media often introduces new algorithms, or uncovers problems in existing ones, making negotiation of mechanisms a necessity.

The purpose of this specification is to define negotiation functionality for the Session Initiation Protocol (SIP) [1]. This negotiation is intended to work only between a UA and its first-hop SIP entity.

1.1.  Motivations

RFC 3329 describes why security is needed to protect SIP signalling from man-in-the-middle attacks, and to accommodate the expected wide variation in security mechanism support by SIP entities. The media plane requires similar protection and capability, for example to prevent eavesdropping in environments such as public wireless access networks that have no inherent security.

1.2.  Design Goals

Security on the media plane differs from security for signalling, because it is applied per media stream and also because multiple media streams can be started and stopped within a single SIP session. For a single media stream, any one of the media plane security mechanisms supported by client and server may be applied, or no media plane security may be applied at all. Therefore, this specification defines secure capability exchange and use of security mechanisms for media, but with no obligation to use the indicated security mechanisms.

1.  The entities involved in the security agreement process need to find out exactly which security mechanisms to apply, preferably without excessive additional roundtrips.

2.  The selection of security mechanisms itself needs to be secure. Traditionally, all security protocols use a secure form of negotiation. For instance, after establishing mutual keys through Diffie-Hellman, IKE sends hashes of the previously sent data including the offered crypto mechanisms [8]. This allows the peers to detect if the initial, unprotected offers were tampered with.
3. The security agreement process should not introduce any additional state to be maintained by the involved entities.

2. Solution

This document defines the "mediasec" header field parameter that labels any of the Security-Client:, Security-Server:, or Security-Verify: header fields as applicable to the media plane and not the signalling plane. Any one of the mechanisms labelled with the "mediasec" header field parameter can be applied on-the-fly as a media stream is started, unlike mechanisms for signalling one of which is chosen and then applied throughout a session.

2.1. Relationship to RFC3329

As stated earlier, RFC 3329 [1] defines security mechanism agreement for signalling, including the "sec-agree" option tag that can appear in Supported:, Require:, and Proxy-Require: header fields. The "mediasec" header field parameter defined in this document places no requirements to support any function in RFC 3329 [1]. In other words, media plane security can be supported without implementing any of RFC 3329 [1], it is only the header field names that are re-used. A user agent or proxy that does not implement RFC 3329 [1] or this document and receives the Security-Client:, Security-Server; and Security-Verfiy; header fields containing only media plane security mechanisms, labelled with the "mediasec" header field parameter, will ignore them as unknown, and will not include these header fields in its response, thereby informing the entity that sent them that this document is not supported. This document adds 200 (OK) to the SIP responses that can contain the Security-Client, Security-Server, and Security-Verfiy header fields; RFC 3329 [1] allows Security-Server only in SIP responses 421 (Extension Required) and 494 (Security Agreement Required).

2.2. Overview of Operation

The message flow is identical to the flow in RFC 3329 [1], with the exceptions that it is not mandatory for the user agent to apply media plane security immediately after it receives the list of supported media plane mechanisms from the server, or any timer after that, nor will the lack of a mutually supported media plane security mechanism prevent SIP session setup. In the message flow below, only Step 3 differs from RFC 3329 [1].
1. Client ---------------client list------------- Server
2. Client <-------------server list------------- Server
3. Client --(optional to turn on media security)-- Server
4. Client ---------------server list------------- Server
5. Client <-------------ok or error------------- Server

Figure 1: Security capability Exchange message flow

Step 1: Clients wishing to use this specification can send a list of their supported security mechanisms along the first request to the server.

Step 2: Servers wishing to use this specification can challenge the client to perform the security agreement procedure. The security mechanisms and parameters supported by the server are sent along in this challenge.

Step 3: The client may then proceed to select any media security mechanism they have in common and to turn on the selected security.

Step 4: The client contacts the server again, now using the selected security mechanism. The server’s list of supported security mechanisms is returned as a response to the challenge.

Step 5: The server verifies its own list of security mechanisms in order to ensure that the original list had not been modified.

2.3. Syntax

tbd.

2.4. Protocol Operation

2.4.1. The "mediasec" Header Field Parameter

The "mediasec" header field parameter may be used in the Security-Client; Security-Server; or Security-Verify; header fields defined in RFC 3329 [1] to indicate that a header field applies to the media plane. Any one of the media plane security mechanisms supported by both client and server, if any, may be applied when a media stream is started. Or, a media stream may be set up without security.

The value of the "mediasec" header field parameter will be specific to the security mechanism applied and the secure media transport protocol. This document defines the following value:
2.4.2. Client Initiated
tbd.

2.4.3. Server Initiated
tbd.

2.5. Security Mechanism Initiation
tbd.

2.6. Duration of Security Associations
tbd.

2.7. Summary of Header Field Use
tbd.

3. Backwards Compatibility

Security mechanisms that apply to the media plane only MUST NOT have the same name as any signalling plane mechanism. If a signalling plane security mechanism name is re-used for the media plane and distinguished only by the "mediasec" parameter, then implementations that do not understand the "mediasec" parameter may incorrectly use that security mechanism for the signalling plane.

4. Examples
tbd.

4.1. Client Initiated

As per RFC 3329 [1], a UA negotiates the security mechanism for signalling to be used with its outbound proxy without knowing beforehand which mechanisms the proxy supports as shown below.
Indication of media security mechanisms is added and identified by the "mediasec" header field parameter. Media security mechanisms are returned by the client to the server in the Security-Verify: header field in the same way as for signalling security mechanisms.
Figure 3: Use of mediasec parameter

4.2. Server Initiated

tbd.

5. Formal Syntax

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in RFC 5234 [RFC5234].

The "reg-type" URI parameter is a "header field parameter", as defined by [RFC3968].

Header Field Name in which the parameter can appear.
Security-Client
Security-Server
Security-Verify

<table>
<thead>
<tr>
<th>Header Fields</th>
<th>Parameter Name</th>
<th>Values</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security-Client</td>
<td>mediasec</td>
<td>No</td>
<td>[this document]</td>
</tr>
<tr>
<td>Security-Server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security-Verify</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Name of the Header Field Parameter being registered.
"mediasec"

6. Acknowledgements

Remember, it’s important to acknowledge people who have contributed to the work.

This template was extended from an initial version written by Pekka Savola and contributed by him to the xml2rfc project.

7. IANA Considerations

The "mediasec" parameter and any new security mechanisms for the media plane must be IANA registered.

7.1. Registration Information

tbd.

7.2. Registration Template

tbd.

7.3. Header Field Names

tbd.
7.4.  Response Codes

tbd.

7.5.  Option Tags

None?

8.  Security Considerations

Remember to consider security from the start. and all drafts are required to have a security considerations section before they will pass the IESG.

9.  References

9.1.  Normative References


9.2.  Informative References


Appendix A.  Additional stuff

You can add appendices just as regular sections, the only difference is that they go within the "back" element, and not within the "middle" element.  And they follow the "reference" elements.
Author’s Address

Peter Dawes
Vodafone Group Services Ltd.
Newbury
UK

Email: peter.dawes@vodafone.com