Network Working Group
Request for Comments: 3329
Category: Standards Track

J. Arkko
V. Torvinen
G. Camarillo
Ericsson
A. Niemi
T. Haukka
Nokia

January 2003

Security Mechanism Agreement for the Session Initiation Protocol (SIP)

Status of this Memo

Copyright Notice

Abstract

This document defines new functionality for negotiating the security mechanisms used between a Session Initiation Protocol (SIP) user agent and its next-hop SIP entity. This new functionality supplements the existing methods of choosing security mechanisms between SIP entities.

Table of Contents

1. Introduction 2
1.1 Motivations 2
1.2 Design Goals 3
1.3 Conventions 3
2. Solution 3
2.1 Overview of Operation 3
2.2 Syntax 4
2.3 Protocol Operation 6
2.3.1 Client Initiated 6
2.3.2 Server Initiated 8
2.4 Security Mechanism Initiation. 9
2.5 Duration of Security Associations. 10
2.6 Summary of Header Field Use. 10

3. Backwards Compatibility 11
4. Examples 12
4.1 Client Initiated 12
4.2 Server Initiated 14
5. Security Considerations 15
6. IANA Considerations. 17
6.1 Registration Information 17
6.2 Registration Template. 18
6.3 Header Field Names 18
6.4 Response Codes 18
6.5 Option Tags. 19
7. Contributors 19
8. Acknowledgements 19
9. Normative References 19
10. Informative References 20
A. Syntax of ipsec-3gpp 21
Authors' Addresses 23
Full Copyright Statement 24

1. Introduction

Traditionally, security protocols have included facilities to agree on the used mechanisms, algorithms, and other security parameters. This is to add flexibility, since different mechanisms are usually suitable to different scenarios. Also, the evolution of security mechanisms 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

Without a secured method to choose between security mechanisms and/or their parameters, SIP is vulnerable to certain attacks. Authentication and integrity protection using multiple alternative methods and algorithms is vulnerable to Man-in-the-Middle (MitM) attacks (e.g., see [4]).

It is also hard or sometimes even impossible to know whether a specific security mechanism is truly unavailable to a SIP peer entity, or if in fact a MitM attack is in action.

In certain small networks these issues are not very relevant, as the administrators of such networks can deploy appropriate software versions and set up policies for using exactly the right type of

security. However, SIP is also expected to be deployed to hundreds of millions of small devices with little or no possibilities for coordinated security policies, let alone software upgrades, which necessitates the need for the negotiation functionality to be available from the very beginning of deployment (e.g., see [11]).

1.2 Design Goals

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 entities involved in the security agreement process need to be able to indicate success or failure of the security agreement process.

4. The security agreement process should not introduce any additional state to be maintained by the involved entities.

1.3 Conventions

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 BCP 14, RFC 2119 [9].

2. Solution

2.1 Overview of Operation

The message flow below illustrates how the mechanism defined in this document works:

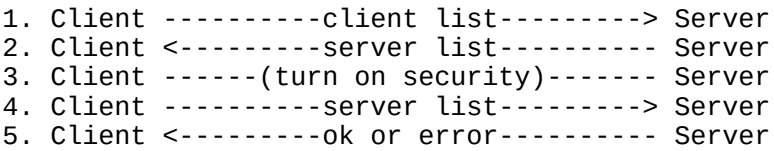

Figure 1: Security agreement message flow.

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 then proceeds to select the highest-preference 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.

This procedure is stateless for servers (unless the used security mechanisms require the server to keep some state).

The client and the server lists are both static (i.e., they do not and cannot change based on the input from the other side). Nodes may, however, maintain several static lists, one for each interface, for example.

Between Steps 1 and 2, the server may set up a non-self-describing security mechanism if necessary. Note that with this type of security mechanisms, the server is necessarily stateful. The client would set up the non-self-describing security mechanism between Steps 2 and 4.

2.2 Syntax

We define three new SIP header fields, namely Security-Client, Security-Server and Security-Verify. The notation used in the Augmented BNF definitions for the syntax elements in this section is as used in SIP [1], and any elements not defined in this section are as defined in SIP and the documents to which it refers:

```
security-client  = "Security-Client" HCOLON
                   sec-mechanism *(COMMA sec-mechanism)
security-server  = "Security-Server" HCOLON
                   sec-mechanism *(COMMA sec-mechanism)
security-verify  = "Security-Verify" HCOLON
                   sec-mechanism *(COMMA sec-mechanism)
```

```
sec-mechanism    = mechanism-name *(SEMI mech-parameters)
mechanism-name   = ( "digest" / "tls" / "ipsec-ike" /
                     "ipsec-man" / token )
mech-parameters  = ( preference / digest-algorithm /
                      digest-qop / digest-verify / extension )
preference       = "q" EQUAL qvalue
qvalue           = ( "0" [ "." 0*3DIGIT ] )
                    / ( "1" [ "." 0*3("0") ] )
digest-algorithm = "d-alg" EQUAL token
digest-qop       = "d-qop" EQUAL token
digest-verify    = "d-ver" EQUAL LDQUOT 32LHEX RDQUOT
extension        = generic-param
```

Note that qvalue is already defined in the SIP BNF [1]. We have copied its definitions here for completeness.

The parameters described by the BNF above have the following semantics:

Mechanism-name
: This token identifies the security mechanism supported by the client, when it appears in a Security-Client header field; or by the server, when it appears in a Security-Server or in a Security-Verify header field. The mechanism-name tokens are registered with the IANA. This specification defines four values:

  * "tls" for TLS [3].

  * "digest" for HTTP Digest [4].

  * "ipsec-ike" for IPsec with IKE [2].

  * "ipsec-man" for manually keyed IPsec without IKE.

Preference
: The "q" value indicates a relative preference for the particular mechanism. The higher the value the more preferred the mechanism is. All the security mechanisms MUST have different "q" values. It is an error to provide two mechanisms with the same "q" value.

Digest-algorithm
: This optional parameter is defined here only for HTTP Digest [4] in order to prevent the bidding-down attack for the HTTP Digest algorithm parameter. The content of the field may have same values as defined in [4] for the "algorithm" field.

Digest-qop
This optional parameter is defined here only for HTTP Digest [4] in order to prevent the bidding-down attack for the HTTP Digest qop parameter. The content of the field may have same values as defined in [4] for the "qop" field.

Digest-verify
This optional parameter is defined here only for HTTP Digest [4] in order to prevent the bidding-down attack for the SIP security mechanism agreement (this document). The content of the field is counted exactly the same way as "request-digest" in [4] except that the Security-Server header field is included in the A2 parameter. If the "qop" directive's value is "auth" or is unspecified, then A2 is:

A2 = Method ":" digest-uri-value ":" security-server

If the "qop" value is "auth-int", then A2 is:

A2 = Method ":" digest-uri-value ":" H(entity-body) ":" security-server

All linear white spaces in the Security-Server header field MUST be replaced by a single SP before calculating or interpreting the digest-verify parameter. Method, digest-uri-value, entity-body, and any other HTTP Digest parameter are as specified in [4].

Note that this specification does not introduce any extension or change to HTTP Digest [4]. This specification only re-uses the existing HTTP Digest mechanisms to protect the negotiation of security mechanisms between SIP entities.

2.3 Protocol Operation

This section deals with the protocol details involved in the negotiation between a SIP UA and its next-hop SIP entity. Throughout the text the next-hop SIP entity is referred to as the first-hop proxy or outbound proxy. However, the reader should bear in mind that a user agent server can also be the next-hop for a user agent client.

2.3.1 Client Initiated

If a client ends up using TLS to contact the server because it has followed the rules specified in [5], the client MUST NOT use the security agreement procedure of this specification. If a client ends

up using non-TLS connections because of the rules in [5], the client MAY use the security agreement of this specification to detect DNS spoofing, or to negotiate some other security than TLS.

A client wishing to use the security agreement of this specification MUST add a Security-Client header field to a request addressed to its first-hop proxy (i.e., the destination of the request is the first-hop proxy). This header field contains a list of all the security mechanisms that the client supports. The client SHOULD NOT add preference parameters to this list. The client MUST add both a Require and Proxy-Require header field with the value "sec-agree" to its request.

The contents of the Security-Client header field may be used by the server to include any necessary information in its response.

A server receiving an unprotected request that contains a Require or Proxy-Require header field with the value "sec-agree" MUST respond to the client with a 494 (Security Agreement Required) response. The server MUST add a Security-Server header field to this response listing the security mechanisms that the server supports. The server MUST add its list to the response even if there are no common security mechanisms in the client's and server's lists. The server's list MUST NOT depend on the contents of the client's list.

The server MUST compare the list received in the Security-Client header field with the list to be sent in the Security-Server header field. When the client receives this response, it will choose the common security mechanism with the highest "q" value. Therefore, the server MUST add the necessary information so that the client can initiate that mechanism (e.g., a Proxy-Authenticate header field for HTTP Digest).

When the client receives a response with a Security-Server header field, it MUST choose the security mechanism in the server's list with the highest "q" value among all the mechanisms that are known to the client. Then, it MUST initiate that particular security mechanism as described in Section 3.5. This initiation may be carried out without involving any SIP message exchange (e.g., establishing a TLS connection).

If an attacker modified the Security-Client header field in the request, the server may not include in its response the information needed to establish the common security mechanism with the highest preference value (e.g., the Proxy-Authenticate header field is missing). A client detecting such a lack of information in the

response MUST consider the current security agreement process aborted, and MAY try to start it again by sending a new request with a Security-Client header field as described above.

All the subsequent SIP requests sent by the client to that server SHOULD make use of the security mechanism initiated in the previous step. These requests MUST contain a Security-Verify header field that mirrors the server's list received previously in the Security-Server header field. These requests MUST also have both a Require and Proxy-Require header fields with the value "sec-agree".

The server MUST check that the security mechanisms listed in the Security-Verify header field of incoming requests correspond to its static list of supported security mechanisms.

> Note that, following the standard SIP header field comparison rules defined in [1], both lists have to contain the same security mechanisms in the same order to be considered equivalent. In addition, for each particular security mechanism, its parameters in both lists need to have the same values.

The server can proceed processing a particular request if, and only if, the list was not modified. If modification of the list is detected, the server MUST respond to the client with a 494 (Security Agreement Required) response. This response MUST include the server's unmodified list of supported security mechanisms. If the list was not modified, and the server is a proxy, it MUST remove the "sec-agree" value from both the Require and Proxy-Require header fields, and then remove the header fields if no values remain.

Once the security has been negotiated between two SIP entities, the same SIP entities MAY use the same security when communicating with each other in different SIP roles. For example, if a UAC and its outbound proxy negotiate some security, they may try to use the same security for incoming requests (i.e., the UA will be acting as a UAS).

The user of a UA SHOULD be informed about the results of the security mechanism agreement. The user MAY decline to accept a particular security mechanism, and abort further SIP communications with the peer.

2.3.2 Server Initiated

A server decides to use the security agreement described in this document based on local policy. If a server receives a request from the network interface that is configured to use this mechanism, it must check that the request has only one Via entry. If there are

several Via entries, the server is not the first-hop SIP entity, and it MUST NOT use this mechanism. For such a request, the server must return a 502 (Bad Gateway) response.

A server that decides to use this agreement mechanism MUST challenge unprotected requests with one Via entry regardless of the presence or the absence of any Require, Proxy-Require or Supported header fields in incoming requests.

A server that by policy requires the use of this specification and receives a request that does not have the sec-agree option tag in a Require, Proxy-Require or Supported header field MUST return a 421 (Extension Required) response. If the request had the sec-agree option tag in a Supported header field, it MUST return a 494 (Security Agreement Required) response. In both situation the server MUST also include in the response a Security-Server header field listing its capabilities and a Require header field with an option-tag "sec-agree" in it. The server MUST also add necessary information so that the client can initiate the preferred security mechanism (e.g., a Proxy-Authenticate header field for HTTP Digest).

Clients that support the extension defined in this document SHOULD add a Supported header field with a value of "sec-agree".

2.4 Security Mechanism Initiation

Once the client chooses a security mechanism from the list received in the Security-Server header field from the server, it initiates that mechanism. Different mechanisms require different initiation procedures.

If "tls" is chosen, the client uses the procedures of Section 8.1.2 of [1] to determine the URI to be used as an input to the DNS procedures of [5]. However, if the URI is a SIP URI, it MUST treat the scheme as if it were sips, not sip. If the URI scheme is not sip, the request MUST be sent using TLS.

If "digest" is chosen, the 494 (Security Agreement Required) response will contain an HTTP Digest authentication challenge. The client MUST use the algorithm and qop parameters in the Security-Server header field to replace the same parameters in the HTTP Digest challenge. The client MUST also use the digest-verify parameter in the Security-Verify header field to protect the Security-Server header field as specified in 2.2.

To use "ipsec-ike", the client attempts to establish an IKE connection to the host part of the Request-URI in the first request to the server. If the IKE connection attempt fails, the agreement procedure MUST be considered to have failed, and MUST be terminated.

Note that "ipsec-man" will only work if the communicating SIP entities know which keys and other parameters to use. It is outside the scope of this specification to describe how this information can be made known to the peers. All rules for minimum implementations, such as mandatory-to-implement algorithms, apply as defined in [2], [6], and [7].

In both IPsec-based mechanisms, it is expected that appropriate policy entries for protecting SIP have been configured or will be created before attempting to use the security agreement procedure, and that SIP communications use port numbers and addresses according to these policy entries. It is outside the scope of this specification to describe how this information can be made known to the peers, but it would typically be configured at the same time as the IKE credentials or manual SAs have been entered.

2.5 Duration of Security Associations

Once a security mechanism has been negotiated, both the server and the client need to know until when it can be used. All the mechanisms described in this document have a different way of signaling the end of a security association. When TLS is used, the termination of the connection indicates that a new negotiation is needed. IKE negotiates the duration of a security association. If the credentials provided by a client using digest are no longer valid, the server will re-challenge the client. It is assumed that when IPsec-man is used, the same out-of-band mechanism used to distribute keys is used to define the duration of the security association.

2.6 Summary of Header Field Use

The header fields defined in this document may be used to negotiate the security mechanisms between a UAC and other SIP entities including UAS, proxy, and registrar. Information about the use of headers in relation to SIP methods and proxy processing is summarized in Table 1.

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
Security-Client	R	ard	-	o	-	o	o	o
Security-Server	421,494		-	o	-	o	o	o
Security-Verify	R	ard	-	o	-	o	o	o

Header field	where	proxy	SUB	NOT	PRK	IFO	UPD	MSG
Security-Client	R	ard	o	o	-	o	o	o
Security-Server	421,494		o	o	-	o	o	o
Security-Verify	R	ard	o	o	-	o	o	o

Table 1: Summary of Header Usage.

The "where" column describes the request and response types in which the header field may be used. The header may not appear in other types of SIP messages. Values in the where column are:

* R: Header field may appear in requests.

* 421, 494: A numerical value indicates response codes with which the header field can be used.

The "proxy" column describes the operations a proxy may perform on a header field:

* a: A proxy can add or concatenate the header field if not present.

* r: A proxy must be able to read the header field, and thus this header field cannot be encrypted.

* d: A proxy can delete a header field value.

The next six columns relate to the presence of a header field in a method:

* o: The header field is optional.

3. Backwards Compatibility

The use of this extension in a network interface is a matter of local policy. Different network interfaces may follow different policies, and consequently the use of this extension may be situational by nature. UA and server implementations MUST be configurable to operate with or without this extension.

A server that is configured to use this mechanism, may also accept requests from clients that use TLS based on the rules defined in [5]. Requests from clients that do not support this extension, and do not support TLS, can not be accepted. This obviously breaks interoperability with some SIP clients. Therefore, this extension should be used in environments where it is somehow ensured that every client implements this extension or is able to use TLS. This extension may also be used in environments where insecure communication is not acceptable if the option of not being able to communicate is also accepted.

4. Examples

The following examples illustrate the use of the mechanism defined above.

4.1 Client Initiated

A UA negotiates the security mechanism to be used with its outbound proxy without knowing beforehand which mechanisms the proxy supports. The OPTIONS method can be used here to request the security capabilities of the proxy. In this way, the security can be initiated even before the first INVITE is sent via the proxy.

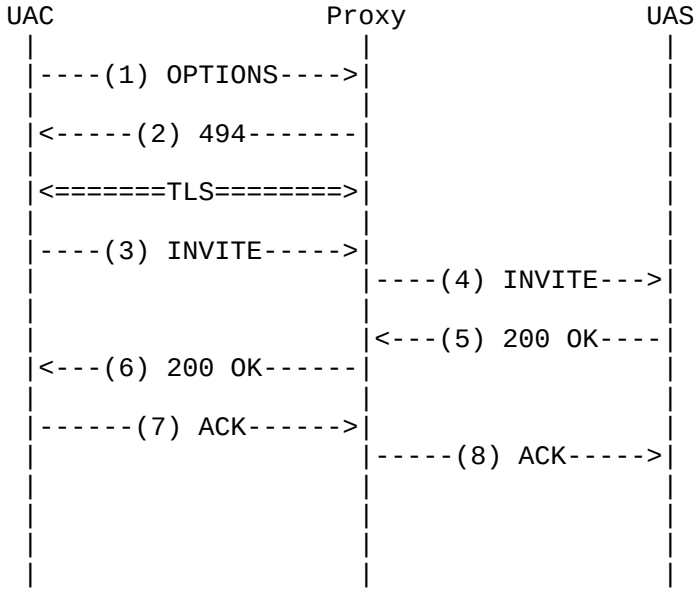

Figure 2: Negotiation Initiated by the Client.

The UAC sends an OPTIONS request to its outbound proxy, indicating at the same time that it is able to negotiate security mechanisms and that it supports TLS and HTTP Digest (1).

The outbound proxy responds to the UAC with its own list of security mechanisms - IPsec and TLS (2). The only common security mechanism is TLS, so they establish a TLS connection between them. When the connection is successfully established, the UAC sends an INVITE request over the TLS connection just established (3). This INVITE contains the server's security list. The server verifies it, and since it matches its static list, it processes the INVITE and forwards it to the next hop.

If this example was run without Security-Server header in Step 2, the UAC would not know what kind of security the other one supports, and would be forced to error-prone trials.

More seriously, if the Security-Verify was omitted in Step 3, the whole process would be prone for MitM attacks. An attacker could spoof "ICMP Port Unreachable" message on the trials, or remove the stronger security option from the header in Step 1, therefore substantially reducing the security.

```
(1) OPTIONS sip:proxy.example.com SIP/2.0
    Security-Client: tls
    Security-Client: digest
    Require: sec-agree
    Proxy-Require: sec-agree

(2) SIP/2.0 494 Security Agreement Required
    Security-Server: ipsec-ike;q=0.1
    Security-Server: tls;q=0.2

(3) INVITE sip:proxy.example.com SIP/2.0
    Security-Verify: ipsec-ike;q=0.1
    Security-Verify: tls;q=0.2
    Route: sip:callee@domain.com
    Require: sec-agree
    Proxy-Require: sec-agree
```

The 200 OK response (6) for the INVITE and the ACK (7) are also sent over the TLS connection. The ACK will contain the same Security-Verify header field as the INVITE (3).

4.2 Server Initiated

In this example of Figure 3 the client sends an INVITE towards the callee using an outbound proxy. This INVITE does not contain any Require header field.

```
          UAC                 Proxy               UAS
           |                    |                   |
           |-----(1) INVITE---->|                   |
           |                    |                   |
           |<-----(2) 421-------|                   |
           |                    |                   |
           |------(3) ACK------>|                   |
           |                    |                   |
           |<=======IKE========>|                   |
           |                    |                   |
           |-----(4) INVITE---->|                   |
           |                    |----(5) INVITE--->|
           |                    |                   |
           |                    |<---(6) 200 OK----|
           |<----(7) 200 OK-----|                   |
           |                    |                   |
           |------(8) ACK------>|                   |
           |                    |-----(9) ACK----->|
           |                    |                   |
           |                    |                   |
```

Figure 3: Server Initiated Security Negotiation.

The proxy, following its local policy, does not accept the INVITE. It returns a 421 (Extension Required) with a Security-Server header field that lists IPsec-IKE and TLS. Since the UAC supports IPsec-IKE it performs the key exchange and establishes a security association with the proxy.

The second INVITE (4) and the ACK (8) contain a Security-Verify header field that mirrors the Security-Server header field received in the 421. The INVITE (4), the 200 OK (7) and the ACK (8) are sent using the security association that has been established.

```
(1) INVITE sip:uas.example.com SIP/2.0

(2) SIP/2.0 421 Extension Required
    Security-Server: ipsec-ike;q=0.1
    Security-Server: tls;q=0.2
```

```
   (4) INVITE sip:uas.example.com SIP/2.0
       Security-Verify: ipsec-ike;q=0.1
       Security-Verify: tls;q=0.2
```

5. Security Considerations

This specification is about making it possible to select between various SIP security mechanisms in a secure manner. In particular, the method presented herein allow current networks using, for instance, HTTP Digest, to be securely upgraded to, for instance, IPsec without requiring a simultaneous modification in all equipment. The method presented in this specification is secure only if the weakest proposed mechanism offers at least integrity and replay protection for the Security-Verify header field.

The security implications of this are subtle, but do have a fundamental importance in building large networks that change over time. Given that the hashes are produced also using algorithms agreed in the first unprotected messages, one could ask what the difference in security really is. Assuming integrity protection is mandatory and only secure algorithms are used, we still need to prevent MitM attackers from modifying other parameters, such as whether encryption is provided or not. Let us first assume two peers capable of using both strong and weak security. If the initial offers are not protected in any way, any attacker can easily "downgrade" the offers by removing the strong options. This would force the two peers to use weak security between them. But if the offers are protected in some way -- such as by hashing, or repeating them later when the selected security is really on -- the situation is different. It would not be sufficient for the attacker to modify a single message. Instead, the attacker would have to modify both the offer message, as well as the message that contains the hash/ repetition. More importantly, the attacker would have to forge the weak security that is present in the second message, and would have to do so in real time between the sent offers and the later messages. Otherwise, the peers would notice that the hash is incorrect. If the attacker is able to break the weak security, the security method and/or the algorithm should not be used.

In conclusion, the security difference is making a trivial attack possible versus demanding the attacker to break algorithms. An example of where this has a serious consequence is when a network is first deployed with integrity protection (such as HTTP Digest [4]), and then later new devices are added that support also encryption (such as TLS [3]). In this situation, an insecure negotiation procedure allows attackers to trivially force even new devices to use only integrity protection.

Possible attacks against the security agreement include:

1. Attackers could try to modify the server's list of security mechanisms in the first response. This would be revealed to the server when the client returns the received list using the security.

2. Attackers could also try to modify the repeated list in the second request from the client. However, if the selected security mechanism uses encryption this may not be possible, and if it uses integrity protection any modifications will be detected by the server.

3. Attackers could try to modify the client's list of security mechanisms in the first message. The client selects the security mechanism based on its own knowledge of its own capabilities and the server's list, hence the client's choice would be unaffected by any such modification. However, the server's choice could still be affected as described below:

   * If the modification affected the server's choice, the server and client would end up choosing different security mechanisms in Step 3 or 4 of Figure 1. Since they would be unable to communicate to each other, this would be detected as a potential attack. The client would either retry or give up in this situation.

   * If the modification did not affect the server's choice, there's no effect.

4. Finally, attackers may also try to reply old security agreement messages. Each security mechanism must provide replay protection. In particular, HTTP Digest implementations should carefully utilize existing reply protection options such as including a time-stamp to the nonce parameter, and using nonce counters [4].

All clients that implement this specification MUST select HTTP Digest, TLS, IPsec, or any stronger method for the protection of the second request.

6. IANA Considerations

This specification defines a new mechanism-name namespace in Section 2.2 which requires a central coordinating body. The body responsible for this coordination is the Internet Assigned Numbers Authority (IANA).

This document defines four mechanism-names to be initially registered, namely "digest", "tls", "ipsec-ike", and "ipsec-man". In addition to these mechanism-names, "ipsec-3gpp" mechanism-name is also registered (see Appendix A). Following the policies outlined in [10], further mechanism-names are allocated based on IETF Consensus.

Registrations with the IANA MUST include the mechanism-name token being registered, and a pointer to a published RFC describing the details of the corresponding security mechanism.

6.1 Registration Information

IANA registers new mechanism-names at http://www.iana.org/assignments/sip-parameters under "Security Mechanism Names". As this document specifies five mechanism-names, the initial IANA registration for mechanism-names will contain the information shown in Table 2. It also demonstrates the type of information maintained by the IANA.

Mechanism Name	Reference
digest	[RFC3329]
tls	[RFC3329]
ipsec-ike	[RFC3329]
ipsec-man	[RFC3329]
ipsec-3gpp	[RFC3329]

Table 2: Initial IANA registration.

6.2 Registration Template

To: ietf-sip-sec-agree-mechanism-name@iana.org
Subject: Registration of a new SIP Security Agreement mechanism

Mechanism Name:

(Token value conforming to the syntax described in Section 2.2.)

Published Specification(s):

(Descriptions of new SIP Security Agreement mechanisms require a published RFC.)

6.3 Header Field Names

This specification registers three new header fields, namely Security-Client, Security-Server and Security-Verify. These headers are defined by the following information, which has been included in the sub-registry for SIP headers under http://www.iana.org/assignments/sip-parameters.

Header Name: Security-Client
Compact Form: (none)

Header Name: Security-Server
Compact Form: (none)

Header Name: Security-Verify
Compact Form: (none)

6.4 Response Codes

This specification registers a new response code, namely 494 (Security Agreement Required). The response code is defined by the following information, which has been included to the sub-registry for SIP methods and response-codes under http://www.iana.org/assignments/sip-parameters.

Response Code Number: 494
Default Reason Phrase: Security Agreement Required

6.5 Option Tags

This specification defines a new option tag, namely sec-agree. The option tag is defined by the following information, which has been included in the sub-registry for option tags under http://www.iana.org/assignments/sip-parameters.

Name: sec-agree
Description: This option tag indicates support for the Security Agreement mechanism. When used in the Require, or Proxy-Require headers, it indicates that proxy servers are required to use the Security Agreement mechanism. When used in the Supported header, it indicates that the User Agent Client supports the Security Agreement mechanism. When used in the Require header in the 494 (Security Agreement Required) or 421 (Extension Required) responses, it indicates that the User Agent Client must use the Security Agreement Mechanism.

7. Contributors

Sanjoy Sen and Lee Valerius from Nortel Networks have contributed to the document.

8. Acknowledgements

In addition to the contributors, the authors wish to thank Allison Mankin, Rolf Blom, James Undery, Jonathan Rosenberg, Hugh Shieh, Gunther Horn, Krister Boman, David Castellanos-Zamora, Miguel Garcia, Valtteri Niemi, Martin Euchner, Eric Rescorla and members of the 3GPP SA3 group for interesting discussions in this problem space.

9. Normative References

[1] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[2] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[3] Dierks, T. and C. Allen, P. Kocher, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[4] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A. and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[5] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[6] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[7] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[8] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

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

[10] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

10. Informative References

[11] Garcia-Martin, M., "3rd-Generation Partnership Project (3GPP) Release 5 requirements on the Session Initiation Protocol (SIP)", Work in Progress.

[12] 3rd Generation Partnership Project, "Access security for IP-based services, Release 5", TS 33.203 v5.3.0, September 2002.

[13] Madson, C. and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", RFC 2403, November 1998.

[14] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[15] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

Appendix A. Syntax of ipsec-3gpp

This appendix extends the security agreement framework described in this document with a new security mechanism: "ipsec-3gpp". This security mechanism and its associated parameters are used in the 3GPP IP Multimedia Subsystem [12]. The Augmented BNF definitions below follow the syntax of SIP [1].

```
mechanism-name   = ( "ipsec-3gpp" )
mech-parameters    = ( algorithm / protocol /mode /
                       encrypt-algorithm / spi /
                       port1 / port2 )
algorithm          = "alg" EQUAL ( "hmac-md5-96" /
                                   "hmac-sha-1-96" )
protocol           = "prot" EQUAL ( "ah" / "esp" )
mode               = "mod" EQUAL ( "trans" / "tun" )
encrypt-algorithm  = "ealg" EQUAL ( "des-ede3-cbc" / "null" )
spi                = "spi" EQUAL spivalue
spivalue           = 10DIGIT; 0 to 4294967295
port1              = "port1" EQUAL port
port2              = "port2" EQUAL port
port               = 1*DIGIT
```

The parameters described by the BNF above have the following semantics:

Algorithm
: This parameter defines the used authentication algorithm. It may have a value of "hmac-md5-96" for HMAC-MD5-96 [13], or "hmac-sha-1-96" for HMAC-SHA-1-96 [14]. The algorithm parameter is mandatory.

Protocol
: This parameter defines the IPsec protocol. It may have a value of "ah" for AH [6], or "esp" for ESP [7]. If no Protocol parameter is present, the protocol will be ESP by default.

Mode
: This parameter defines the mode in which the IPsec protocol is used. It may have a value of "trans" for transport mode, or a value of "tun" for tunneling mode. If no Mode parameter is present the IPsec protocol is used in transport mode.

Encrypt-algorithm
: This parameter defines the used encryption algorithm. It may have a value of "des-ede3-cbc" for 3DES [15], or "null" for no encryption. If no Encrypt-algorithm parameter is present, encryption is not used.

Spi
Defines the SPI number used for inbound messages.

Port1
Defines the destination port number for inbound messages that are protected.

Port2
Defines the source port number for outbound messages that are protected. Port 2 is optional.

The communicating SIP entities need to know beforehand which keys to use. It is also assumed that the underlying IPsec implementation supports selectors that allow all transport protocols supported by SIP to be protected with a single SA. The duration of security association is the same as in the expiration interval of the corresponding registration binding.

Authors' Addresses

Jari Arkko
Ericsson
Jorvas, FIN 02420
Finland

Phone: +358 40 507 9256
EMail: jari.arkko@ericsson.com

Vesa Torvinen
Ericsson
Joukahaisenkatu 1
Turku, FIN 20520
Finland

Phone: +358 40 723 0822
EMail: vesa.torvinen@ericsson.fi

Gonzalo Camarillo
Advanced Signalling Research Lab.
Ericsson
FIN-02420 Jorvas
Finland

Phone: +358 40 702 3535
EMail: Gonzalo.Camarillo@ericsson.com

Aki Niemi
NOKIA Corporation
P.O.Box 321, FIN 00380
Finland

Phone: +358 50 389 1644
EMail: aki.niemi@nokia.com

Tao Haukka
Nokia Corporation
P.O. Box 50
FIN - 90570 Oulu
Finland

Phone: +358 40 517 0079
EMail: tao.haukka@nokia.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.