3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010103**

14 September, 2001

Sophia Antipolis, France

Source:	**Nortel Networks**
Title:	**Digest-Based SIP Message Integrity Protection for IMS**
Document for:	**Discussion/Decision**
Agenda Item:	**6.1, SIP Signalling Protection - Integrity**

1. Introduction

It has been identified as a requirement in the 3GPP IM Subsystem that SIP messages travelling between the UE and the Proxy CSCF be integrity protected. Furthermore, it has been recognized that SIP does not currently define an adequate general mechanism for message integrity protection. The purpose of this contribution is to propose that an adaptation of the existing SIP authentication/integrity-protection framework called HTTP Digest be used to satisfy the requirement for UE-to-Proxy CSCF SIP integrity protection.

HTTP Digest [3] was standardized for use within SIP [1] to provide better user authentication than Basic. To date, HTTP Digest has become the predominantly used scheme for client to server authentication in SIP systems. The Digest scheme is used both to authenticate the client (user) and to protect the integrity of the message that contains the authentication response (as well as for certain other security functions such as anti-replay protection, plain-text attack protection, etc.). In the authentication response, Digest supports integrity protection of the SIP message body (not the headers) when the “qop-options” directive within the Digest challenge is set to the value “auth-int”. It is proposed that 3GPP IMS implementations adapt just the integrity protection component of Digest functionality to satisfy the requirement for a general-purpose integrity protection mechanism that operates within the context of a persistent Security Association. Since protection of the entire message has been identified as required in 3GPP IMS for the UE-to-Proxy CSCF hop, it is proposed that 3GPP IMS implementations apply Digest integrity protection to the entire SIP message (or at least to the invariant headers in the SIP request along with the message body). For 3GPP IMS, since there is a single “hop” between the UE and P-CSCF, protection of the entire message is feasible.

The next two sections discuss the proposed usage of the Digest directives by 3GPP IMS implementations. Per this proposal, the Proxy CSCF includes Digest challenge-related parameters in the Proxy-Authenticate header field of the 401 response message toward the UE. To protect the integrity of messages containing sensitive data, both the UE and the P-CSCF include Digest response-related parameters (in particular, the Message Authentication Code [MAC]) in such messages.

2. Digest Challenge Parameters

Per RFC 2617, the Digest challenge-related directives are carried in either the WWW-Authenticate or Proxy-Authenticate header fields. It is proposed that the 3GPP IMS Proxy CSCF add a Proxy-Authenticate header field to the 401 that is sent by the Serving CSCF (SIP registrar) toward the UE; the Proxy-Authenticate would contain the Digest challenge that has been constructed by the P-CSCF.

Following RFC 2617 [3], the Digest challenge in the SIP response is depicted in ABNF as:

```
challenge        =        Digest digest-challenge
digest-challenge  = 1#( realm | [ domain ] | nonce |
            [ opaque ] |[ stale ] | [ algorithm ] |
            [ qop-options ] | [auth-param] )
```

The following discusses usage of these directives relevant to 3GPP IMS implementations.

The “qop-options” directive is optional, but is made so only for backwards compatibility; it SHOULD be used by all implementations compliant with RFC 2617 and later. It is proposed that 3GPP IMS implementations use a new value “int” of the "qop-options" directive. The new value “int” shall communicate the following semantics to a user agent client: “use the indicated algorithm and nonce for subsequent bi-directional message integrity protection between the client and this server”.

Some other examples of IMS usage are:

```
realm = 3GPP-IMS
algorithm = HMAC-SHA-1  OR:  algorithm = SHA-1
```

The "realm" directive allows the protected resources associated with a server to be partitioned into a set of protection spaces and to apply authentication/integrity-check individually on each of these spaces.

The “algorithm” directive is a string that indicates the algorithm(s) used to produce the message digest and a hash function. The particular strings that may be associated with this directive are not standardized. This contribution illustrates the possible usage of HMAC [5] as the digest (MAC generation) algorithm, and of SHA-1 [6] serving as either the hash function alone or as both the digest algorithm and the hash function. The means by which the sender of a message to be integrity protected would generate the MAC in each of the two cases mentioned above is described in the next section.

Currently, Digest specifies a hash on user name and password to derive the secret key that is used by the MAC generation algorithm. However, it has been agreed by SA3 that the integrity key IK, produced by executing UMTS AKA [2], is to be used as the secret key. (The parameter RAND, which is required to derive IK, is separately carried in the WWW-Authenticate header of the 401 response.)

The nonce value, generated by the server and sent in the 40x response to the client, is used to prevent replay attacks and is implementation dependent. In 3GPP IP Multimedia, the Proxy CSCF can use the equivalent of the AKA [2] FRESH parameter as the nonce value. This value, along with the parameter nonce-count, is used for full anti-replay protection.

3. Digest Response Parameters

Per RFC 2617, the Digest response-related directives are carried in either the Authorization or Proxy-Authorization header fields, depending upon which header field carried the corresponding Digest challenge. These directives contain the credentials for the message integrity check. The 3GPP IMS UE should respond to the initial Digest challenge by adding a Proxy-Authorization header field to the REGISTER toward the S-CSCF (registrar). The UE should also preemptively add a Proxy-Authorization header field to all subsequent UE-initiated SIP messages in the context of the current authentication session.

Following RFC 2617, the credentials are depicted in ABNF as:

```
credentials = Digest digest-response
digest-response  = 1#( username | realm | nonce | digest-uri
          | response | [ algorithm ] | [cnonce] |
          [opaque] | [message-qop] |
          [nonce-count]  | [auth-param] )
```

The following discusses usage of these directives relevant to 3GPP IMS implementations.

In IMS implementations, the UAC need not be concerned with the particular values associated with the following two mandatory directives in RFC 2617:

(1) "username"

> In RFC 2617, the username value is used to compute the request-digest value to authenticate the user at the server. Digest is not used to perform user authentication in 3GPP.

(2) "digest-uri"

> In RFC 2617, digest-uri value (Request URI) is used to compute the request-digest value at the server. The purpose of duplicating this value in this directive from the Request URI field is to deal with the possibility that an intermediate proxy can alter the Request URI. In 3GPP, since the integrity protection terminates at the first proxy (CSCF), the UAC need not be concerned with this parameter.

However, to enable a 3GPP UAC interact with any SIP server, the above two directives are syntactically required.

The value of the “response” directive is the output of the integrity protection algorithm. According to RFC 2617 [3], the response value is computed as follows, where KD is the MAC generation algorithm and H is the hash function:

```
KD [H(A1), unq(nonce) ":" nc ":" unq(cnonce) ":" unq(qop) ":" H(A2)]
A2 = Method ":" request-uri ":" H(entity-body)
```

If the “algorithm” directive in the Digest challenge has the value "HMAC-SHA-1", then HMAC serves the role of KD and SHA-1 serves the role of H (see below). H(A1) is replaced by the AKA-produced integrity key IK. (The original length of the HMAC output is 160 bits. To reduce overhead, a truncated 96-bit MAC can be generated using HMAC-SHA-1-96 [4].)

```
HMAC [IK, unq(nonce) ":" nc ":" unq(cnonce) ":" unq(qop) ":" SHA-1(A2)]
A2 = Method ":" SIP request-uri ":" SHA-1 (entire SIP message)
```

If the “algorithm” directive in the Digest challenge has the value "SHA-1", then SHA-1 serves not only as the hash function H, but as the MAC generation algorithm KD as well. Thus, the response is computed as follows:

SHA-1 [Base64(IK) ":" unq(nonce) ":" nc ":" unq(cnonce) ":" unq(qop) ":" SHA-1(A2)]

A2 = Method ":" SIP request-uri ":" SHA-1 (entire SIP message)

Here, Base64(IK) is the ASCII-converted binary IK parameter. Thus, the response directive is the SHA-1 of the ASCII-converted IK string, concatenated with a colon, concatenated with the rest of the data.

In both of these cases, there are differences with the traditional way of computing the Digest response: 1) IK is used as the secret key instead of a hash on user-name, password and realm; and 2) A2 is defined such that a hash of the entire SIP message is performed instead of just the message body.

4. Illustrative Message Flow

The message flow shown below illustrates the use of the Proxy-Authenticate and Proxy-Authorization header fields for the proposed adaptation of Digest as the integrity protection mechanism for 3GPP IMS. The protocol associated with message #1 features “algorithm=HMAC-SHA-1” as an example. The enhancements to SIP are shown in bold print.

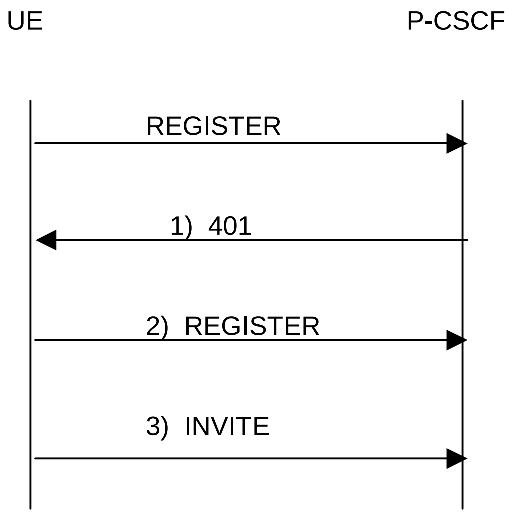

Figure 1. Simplified IMS User Registration and Session Initiation

1) 40x response:

SIP/2.0 401 Unauthorized

WWW-Authenticate: EAP <RAND AUTN>

Proxy-Authenticate: Digest realm=3GPP-IMS nonce=<FRESH> algorithm=HMAC-SHA-1 qop=int

...

2) The integrity protection is turned on with the next REGISTER:

REGISTER sip: ... SIP/2.0

Authorization: EAP <RES>

Proxy-Authorization: Digest username=ABC realm=3GPP-IMS nonce=<FRESH> uri=<SIP-URI> response=<MAC> cnonce=<value> nc=1 qop=int

3) A subsequent INVITE request carries the Proxy-Authorization header

INVITE sip: … SIP/2.0

Proxy-Authorization: Digest username=ABC realm=3GPP-IMS nonce=<FRESH> uri=SIP-URI response=<MAC> cnonce=<value> nc=2 qop=int

5. Pro’s and Con’s of using the Digest framework

Some of the advantages of using the Digest adaptation are:

1. Digest is by far the most commonly implemented authentication /integrity-protection framework in today’s SIP systems.
2. Allows various hash functions and MAC generation algorithms to be used.
3. Results in low message overhead.
4. Provides anti-replay protection without the need for synchronized counters in both client and server.
5. Unlike IPsec, there is no requirement that transport layer port allocation remain unchanged during the lifetime of the security association.

Disadvantages:

1. Does not provide encryption support.

6. Recommendation

It is recommended that SA3 adopt as a working assumption the described adaptation of HTTP Digest as the SIP integrity protection mechanism for 3GPP IMS. This working assumption will lay the groundwork for presenting extension proposals to Digest within IETF.

REFERENCES

[1] Internet draft ietf-sip-rfc2543bis-04.txt

[2] 3GPP TS 33.102, “3G Security; Security Architecture”

[3] "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617

[4] "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404

[5] "HMAC: Keyed hashing for message authentication", RFC 2104

[6] "Secure Hash Algorithm", NIST publication FIPS PUB 180