3GPP TSG SA WG3 Security — S3#21b **S3z020042**

31st January - 1st February, 2002

Antwerp, Belgium

Source: **Nortel Networks**

Title: **Updates from IETF to SIP-Level Solution for IMS Integrity**

Document for: **Discussion**

Agenda Item: **IMS-6.1, SIP Signalling Protection: Integrity**

Abstract

This contribution shows updates to the description of the "SIP-level security solution" for IMS message integrity in draft TS 33.203. The updates reflect the agreements reached since IETF 52 among those parties that seek to enhance HTTP Digest such that it is a viable solution mechanism for SIP message integrity in the IMS.

1. Introduction

Discussion took place at IETF 52 regarding enhancing HTTP Digest to provide more complete integrity protection in one-hop situations and to enable last-hop (proxy to UAS) authentication to work properly. The SIP Working Group agreed that Digest authentication as is currently specified is inadequate and that enhanced Digest mechanisms may be required in SIP. Work on such enhancements proceeds within a focused Design Team.

To date, it has been agreed to propose a new 4xx error code to permit origin servers to challenge proxies from which they receive SIP requests, and new SIP headers to permit proxies to authenticate themselves to origin servers. New values of the Digest "qop-options" directive direct the client receiving a challenge to apply integrity protection with an extended scope to the response.

The next section proposes specific text adjustments to 33.203 section C.2 to reflect agreements reached to date among IETF membership that advocate enhancements to Digest that are pertinent to the "SIP-level security solution".

2. Proposed Text Adjustments for 33.203 Section C.2

[Editors note: There seems to be an unexpected shortcoming in the way SIP provides integrity protection on messages between UE and Proxies. In current SIP, HTTP Digest can be used to partially integrity protect the messages originated by an UE. However, SIP fails to provide integrity for Proxy to UE communication, i.e. for terminating INVITEs, for example. Proxies are not able to add Authorization headers on these messages, thus leaving the messages unprotected.

For the reason above, the headers and field names used in this section may not be final. However, the found inconsistency will probably make it easier for 3GPP to discuss about new SIP level integrity protection schemes with IETF.]

HTTP Digest shall provide integrity protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the SIP level.

The SA that is required for Digest integrity protection shall use the 128-bit integrity key IK generated through IMS AKA, as specified in section 6.1. The integrity algorithm and key are identical for integrity protection applied to messages travelling in either direction. Negotiation of the integrity algorithm to use occurs in the following way: The UE communicates the set of integrity algorithms that it supports to the P-CSCF through the Security-setup header field of the REGISTER message, as described in section 7.2. The P-CSCF selects an algorithm to use from the set of algorithm capabilities common to both the UE and the P-CSCF. The P-CSCF indicates the algorithm to use in the "algorithm" directive of the Digest challenge that is subsequently issued to the UE.

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". Digest supports integrity protection of the SIP message body plus a named list of headers when the "qop-options" directive is set to the value "auth-hdr-int". Digest supports integrity protection of the entire SIP message when the "qop-options" directive within the Digest challenge is set to the value "~~extended~~auth-extd-int". ~~(Use of either of these values of "qop-options" assumes that a context of client authentication has been previously established.)~~ To provide for protection of the entire SIP message, the P-CSCF shall issue a Digest challenge to the UE specifying the value "~~extended~~auth-extd-int" for the "qop-options" directive.

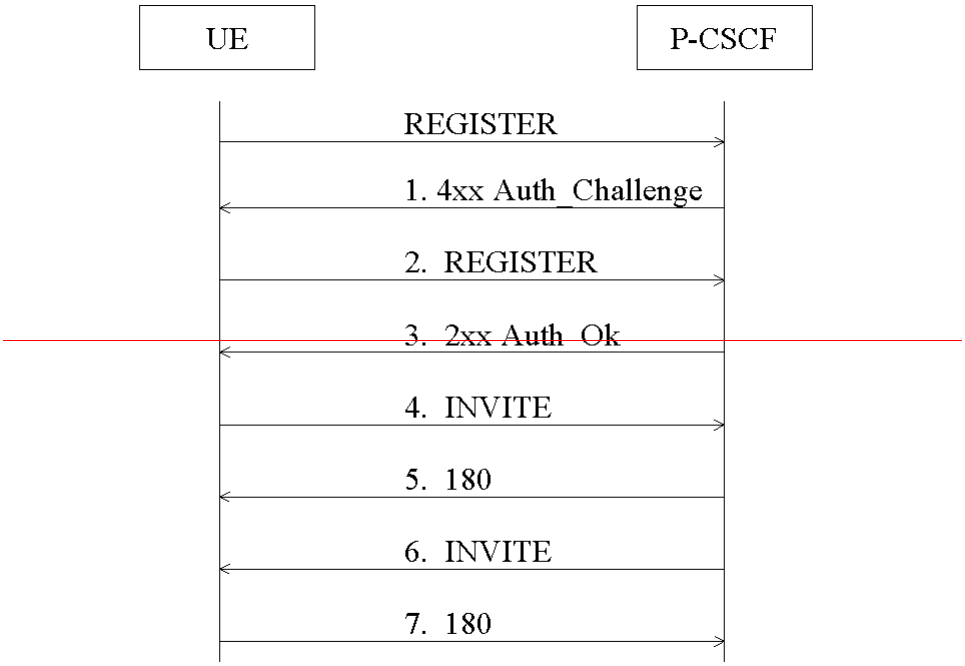
The message 'digest', or message authentication code, is conveyed in the "response" directive of the Digest response. The rules for computing "response" are as described in [1] with the following consideration: if the UE receives a Digest challenge with the "qop-options" directive set to either "int" or "~~extended-int~~auth-extd-int", and the associated authentication challenge was an IMS AKA challenge, then the UE substitutes IK for the "password" component of A1 when computing "response=" in the Digest response. The UE sets the "username" component of A1 to a fixed value (e.g., "ims-user"). When sending messages to the UE that are to be integrity protected, the P-CSCF applies the same rules when computing "response". In this manner, the whole SIP message is always protected.

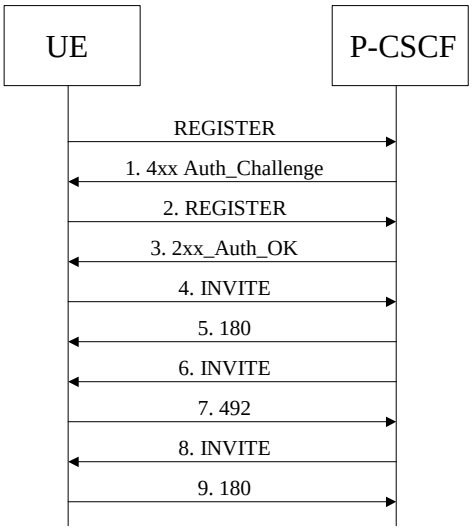
The Digest framework specifies that a server-initiated nonce is to be used by the client as a random number input to the production of the message digest. This nonce, along with a counter that is incremented by either endpoint when sending a message that is to be protected, facilitate anti-replay protection.

In the 3GPP IMS, then, normal operation of the Digest challenge-response mechanism for integrity protection is as follows:

~~Per RFC 2617, t~~The Digest challenge-related directives are carried in ~~either~~ the WWW-Authenticate, ~~or~~ Proxy-Authenticate or UAS-Authenticate header fields. The P-CSCF adds a Proxy-Authenticate header field to the 4xx Auth_Challenge that is sent by the S-CSCF (SIP registrar) toward the UE; the Proxy-Authenticate contains the Digest challenge that has been constructed by the P-CSCF.

~~Per RFC 2617, T~~the Digest response-related directives are carried in ~~either~~ the Authorization, ~~or~~ Proxy-Authorization or UAS-Authorization header fields, depending upon which header field carried the corresponding Digest challenge. These directives contain the credentials for the message integrity check. In the IMS context, the UE responds to the initial Digest challenge by adding a Proxy-Authorization header field to the REGISTER toward the S-CSCF (registrar). The UE pre-emptively adds a Proxy-Authorization header field to all subsequent UE-initiated SIP requests. The ~~UE and the~~ P-CSCF adds the Proxy-Authentication-Info header to all SIP responses. **~~Finally, t~~The P-CSCF adds an ~~Integrity~~ UAS-Authorization header field to all SIP requests sent toward the UE. Finally, the UE adds the UAS-Authentication-Info header to all SIP responses.** The simplified message flow shown below illustrates the relevant header fields and contents for the SIP-level integrity protection mechanism. Please note that the message flow contains three cases: a registration (1-3), and two SIP sessions: one UE initiated (4-5) and one UE terminated (6-7).





1. **4xx response – this carries both the IMS AKA challenge (from the registrar) and the Digest challenge for integrity protection (from the P-CSCF):**

   SIP/2.0 4xx Auth_Challenge

   WWW-Authenticate: EAP <RAND AUTN>

   Proxy-Authenticate: Digest realm=3GPP-IMS nonce=<~~random-number~~P-nonce1> algorithm=MD5 qop=~~extended~~auth-extd-int

2. **Integrity protection is turned on with the next REGISTER – the integrity credentials are placed in the Digest response:**

   REGISTER sip: ... SIP/2.0

   Authorization: EAP <RES>

Proxy-Authorization: Digest username=ims-user, realm=3GPP-IMS, nonce=<~~echo-random-number~~P-nonce1>, uri=<SIP-URI>, response=<message-digest>, cnonce=<value>, nc=1, qop=~~extended-int~~auth-extd-int

3. **The 2xx response is also integrity protected – the P-CSCF adds the Proxy-Authentication-Info header to carry the message digest:**

   SIP/2.0 2xx Auth_Ok

   Proxy-Authentication-Info: nextnonce=<P-nonce2>, qop=~~extended-int~~auth-extd-int, rspauth=<message-digest>, nc=~~2~~1, cnonce=<value>

4. **A subsequent INVITE request must also be integrity protected – the UE pre-emptively adds the Proxy-Authorization header:**

   INVITE sip: … SIP/2.0

   Proxy-Authorization: Digest username=ims-user, realm=3GPP-IMS, nonce=<~~echo-random-number~~P-nonce2>, uri=<SIP-URI>, response=<message-digest>, cnonce=<value>, nc=~~3~~1, qop=~~extended-int~~auth-extd-int

   Note: The client (UE) may re-use the previously issued nonce (i.e. set "nonce" to <P-nonce1> and "nc" to 1), but Digest recommends against this.

5. **The 180 is integrity protected in the same fashion was the 2xx response (message #3):**

   SIP/2.0 180 Ringing

   Proxy-Authentication-Info: nextnonce=<P-nonce3>, qop=~~extended-int~~auth-extd-int, rspauth=<message-digest>, nc=~~4~~1, cnonce=<value>

6. **An incoming INVITE must also be integrity protected – the first terminating SIP request, however, must be sent without the integrity credential (this permits the UE to issue a Digest challenge containing its own server-provided nonce).**

7. **The UE issues a 492 response containing a Digest challenge:**

   SIP/2.0 492 Proxies Unauthorized

   UAS-Authenticate: Digest realm=3GPP-IMS, nonce=<UE-nonce1>, algorithm=MD5, qop=auth-extd-int, target=<address>

8. **The P-CSCF adds the UAS-Authorization header, which has similar syntax to Proxy-Authorization:**

   INVITE sip: … SIP/2.0

   ~~Integrity~~UAS-Authorization: Digest username=ims-user, realm=3GPP-IMS, nonce=<~~echo-random-number~~UE-nonce1>, uri=<SIP-URI>, response=<message-digest>, cnonce=<value>, nc=~~5~~1, qop=~~extended-int~~auth-extd-int, responder=<address>

~~7.~~9. **The UE protects the 180 response by adding UAS-Authentication-Info:**

   SIP/2.0 180 Ringing

   UAS-Authentication-Info: nextnonce=<UE-nonce2>, qop=~~extended-int~~auth-extd-int, rspauth=<message-digest>, nc=~~6~~1, cnonce=<value>

[Editors Note: Further details will be provided on how replay protection is accomplished. It has been identified that the scheme above needs to be enhanced since otherwise unnecessary loss of calls can occur. The reason for that is that both originating and terminating calls can occur and the counters in the P-CSCF and in the UE are not independent.]

[Editors Note: A description of the security mode setup headers shall be included in this Annex. Furthermore the message flows need to be enhanced.]

REFERENCES

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