3GPP TSG SA WG3 Security#32 **S3-040043**
9-13 February 2004
Edinburgh, Scotland, UK

Agenda Item: **6.9.4 (GAA/HTTPS) and 6.18 (Presence)**

Source: **Siemens**

Title: **Transfer of an asserted User Identity – Discussion and Pseudo-CRs to TSs on GAA/HTTPS-based-services and Presence Security**

Document for: **Discussion and decision**

Abstract

TD S3-030540 "Protocol between authentication proxy (AP) and application server (AS)" suggests the use of the special "cookie protocol enhancement" in order to transfer an asserted user identity from AP to AS. TD S3-030731 "Proxy and various HTTP services" suggests the usage of a special, non-standard HTTP header "X-HTTP-Asserted-Identity" for the same purpose. In the discussion on the SA3 mailing list after SA3-31 use of the HTTP header "X-Forwarded-For" was proposed by NEC. This contribution discusses the proposals and recommends adopting the latter one as normative, as it most closely resembles current practice and implementations in the Internet.

Additionally it is proposed to correct a minor ambiguity in the text on transfer of asserted user identity to better reflect the intention of TD S3-030746 accepted at SA3-31.

We propose to add corresponding requirements to the TSs on GAA/HTTPS and presence security as the split between both is not yet decided.

1 Pseudo-CRs - proposals

1.1 Proposal for Pseudo-CR to TS on Presence Security

It is proposed to bring the structure of TS 33.141 v100 (Presence Security), section 5.1.4 (Authentication Proxy) in line with TS 33.222 v020 (GAA/HTTPS, S3-030xxx), section 5 (Use of authentication proxy).

This means:

Introduce subsections similar to TS (GAA/HTTPS):
- 5.1.4.1 Requirements and principles
- 5.1.4.2 Authentication proxy architecture
- 5.1.4.3 Interfaces
- 5.1.4.4 Management of UE identity

Shift existing text of section 5.1.4 to 5.1.4.1

This procedure allows handling both TSs on GAA/HTTPS and Presence Security in a similar manner for future work.

1.2 Proposal for Pseudo-CRs to TSs on GAA/HTTPS and Presence Security

It is proposed to add the following text in TS 33.222 v020 (GAA/HTTPS, S3-030xxx), section 5.3 (Interfaces), and in TS 33.141 v100 (Presence Security), section 5.1.4.3 (Interfaces):

> The authentication proxy provides the asserted user identity to the application server in a special http header field forwarded to the AS. The format of this special header field is

X-Forwarded-For = “X-Forwarded-For” “:” #(token|quoted-string)

where the field value represents a comma-separated list of identities (in notation of RFC 2616, HTTP/1.1).
The AP shall insert this header field in each request header forwarded to the AS. The field value consists in this case of one token or quoted-string representing the asserted user identity. To ensure conformance with current use of this header field the word “unknown” represents an unknown identity and IP addresses are represented by their standard notation.

If a X-Forwarded-For header field exists in the http request header sent from UE to AP, the AP may be configured to two cases on a per AS basis:

1. The existing X-Forwarded-For header field is dropped and replaced by the inserted X-Forwarded-For header field. This case shall be supported.
2. The asserted identity is appended to the (comma-separated) field value list or an additional X-Forwarded-For header field is inserted after all existing X-Forwarded-For header fields. This allows to transport the received information transparently through the AP to the AS in a way conformant to current use. To allow for an unambiguous interpretation of user identity by the AS, the AP may drop some elements of the existing X-Forwarded-For value list. This case may be supported.

If an asserted user identity is not to be revealed to the AS, the value “unknown” is sent.

It is proposed to adapt the second requirement in TS 33.222 v020 (GAA/HTTPS, S3-030xxx), section 5.1, and in TS 33.141 v100 (Presence Security), section 5.1.4.1 (old: 5.1.4) to the above requirement that each request carries the asserted user identity information:

– Authentication proxy shall send the authenticated identity of the UE to the application server belonging to the trust domain ~~at the beginning of new HTTP session~~in each HTTP request.

1.3 Proposal for Pseudo-CRs to TSs on GAA/HTTPS and Presence Security

It is proposed to enhance the second requirement in TS 33.222 v020 (GAA/HTTPS, S3-030xxx), section 5.1, and in TS 33.141 v100 (Presence Security), section 5.1.4.1 (old: 5.1.4):

– Authentication proxy shall be able to send the authenticated identity of the UE to the application server belonging to the trust domain at the beginning of new HTTP session.

Note: If Pseudo-CR of chapter 1.1 is accepted this requirement must read:

– Authentication proxy shall be able to send the authenticated identity of the UE to the application server belonging to the trust domain in each HTTP request~~at the beginning of new HTTP session~~.

Additionally it is proposed to shift the 7th requirement “Activation of transfer of asserted user identity shall be configurable in the AP on a per AS base” to 3rd position, as it gives the reason for the enhancement of the second requirement.

1.4 Remark on affected TSs

It is proposed to include requirements 1.2 and 1.3 in both draft TSs, as it is currently unclear whether both TSs will be completed within the Release 6 timeframe. If both TSs will be completed in time, SA3 may decide later that all material on authentication proxies is to be contained in TS 33.222 (GAA/HTTPS), and that TS 33.141 (Presence Security) only is to make reference to TS 33.222 (GAA/HTTPS).

2 Pseudo-CRs - motivation

2.1 Status for transfer of an asserted user identity

It is clear that the transfer of an asserted user identity is required if the AS is to take access control decisions based on the user identity. As there is no standard way to achieve this, different proposals arose:

1. TD S3-030540 “Protocol between authentication proxy (AP) and application server (AS)” suggests the use of the special “cookie protocol enhancement” in order to transfer an asserted user identity from AP to AS.
2. TD S3-030731 “Proxy and various HTTP services” suggests the usage of a special, non-standard HTTP header “X-HTTP-Asserted-Identity” for the same purpose.
3. In the discussion on the SA3 mailing list after SA3-31 the inclusion of user identity into the request by UE and successive check of this identity by AP was proposed by Tao Haukka from Nokia.
4. In the discussion on the SA3 mailing list after SA3-31 use of the non standard but existing HTTP header ”X-Forwarded-For” was proposed by Bernd Lamparter from NEC.

The following gives an overview of these proposals and an evaluation as rationale for the proposed Pseudo-CR in chapter 1.2.

2.2 Cookie protocol enhancement

This solution was proposed in S3-030540 for SA3-31 and was discussed in more detail in S3-030746.

While this solution can in principle solve the task it has some shortcomings. To summarize:

- It may interfere with common usage of cookies for transfer of information between UE and AS.
- It has to support all versions of the cookie mechanism (adaptation on future versions necessary).
- Parsing of a cookie list sent from the UE is necessary in the AP.
- Removal of existing cookie fields by a proxy is not allowed in RFC 2965 (even if it would be necessary here because of interference with the transport of asserted identities).

Taking this into account, the solutions described further down are more attractive.

2.3 Inclusion of user identity into the request by UE

This proposal requires the inclusion of user identity in the request header sent from UE to AP. As this identity is not authenticated, the AP has to check the authenticity and to remove any incorrect one. It was stated, that this was more in conformance with the communication of UE to AS without AP in between, as such a header would be necessary there anyway (cf. proposal in S3-030555). The reference (in the email) to S3-030555 could not be verified, as S3-030555 proposes such an information element for the communication UE to BSF only, but not for UE to NAF or AS.

The following statements apply to this solution:

- The identity is unasserted and therefore a hint only. The AP has to determine the authentic identity anyhow. Therefore the load on the AP will not be reduced.
- It was claimed in the email cited above that, in case no AP is used (direct connection of UE to AS), the UE would have to include a identity in a request header anyhow. But this is not necessarily true, as can be seen from the example of shared-key TLS. The mere transmission of an unasserted identity does not give any advantage in this case either.

It seems that the transmission of user identity in request header from UE to AP does not present significant advantages.

2.4 Introduction of “special header fields”

The introduction of special HTTP header fields to carry the asserted identity information was introduced in S3-030731 and S3-030746. The following two paragraphs (in italic) cite S3-030746 for general remarks about special header fields.

RFC 2616 states in chapter “4.5 General Header Fields” the following:

> *“There are a few header fields which have general applicability for both request and response messages, but which do not apply to the entity being transferred. These header fields apply only to the message being transmitted. … General-header field names can be extended reliably only in combination with a change in the protocol version. However, new or experimental header fields may be given the semantics of general header fields if all parties in the communication recognize them to be general-header fields. Unrecognized header fields are treated as entity-header fields.”*

Further on in “5.3 Request Header Fields” it states that entity-header fields may also be extension-headers which are characterized as follows:

"The extension-header mechanism allows additional entity-header fields to be defined without changing the protocol, but these fields cannot be assumed to be recognizable by the recipient. Unrecognized header fields SHOULD be ignored by the recipient and MUST be forwarded by transparent proxies."

This gives an ideal background for the use of the extension-header mechanism.

- As the recipient SHOULD ignore any unrecognized header field, any AS not aware of this mechanism just drops this header field silently.
- An additional proxy who might be situated between AP and AS MUST forward this header field if it does not recognize it.
- An additional proxy who is aware of this header field might even do a filtering of this information in case e.g. an external AS should be blocked from receiving asserted identities (and~~f~~ this is not configured in the AP itself). As the connection between AP and AS is in a domain controlled by the MNO, no misconfigured header-aware proxy is to be expected.

The following chapter gives a comparison of the two remaining proposals.

2.5 Use of "special header fields"

TD S3-030731 proposed the use of the (new) special HTTP request header field "X-HTTP-Asserted-Identity". In the following email discussion the use of the existing (but still non standard) special HTTP request header field "X-Forwarded-For" was proposed.

2.5.1 X-HTTP-Asserted-Identity

This header field is "newly invented" and as such has the properties:

- No compatibility issues
- Support has to be implemented for 3GPP use only (and in addition to existing implementations)
- Accidental use of an equally-named header by other parties is not probable, but it cannot be excluded.

2.5.2 X-Forwarded-For

This header field is used by some proxies to include the origin IP address in forwarded requests also. The following citations give an impression of the current use of this header field.

SQUID Frequently Asked Questions
(C) 2001 Duane Wessels, wessels@squid-cache.org
http://www.squid-cache.org/Doc/FAQ/FAQ.txt

4.17. What is ``HTTP_X_FORWARDED_FOR''? Why does squid provide it to WWW servers, and how can I stop it?

When a proxy-cache is used, a server does not see the connection coming from the originating client. Many people like to implement access controls based on the client address. To accommodate these people, Squid adds its own request header called "X-Forwarded-For" which looks like this:

X-Forwarded-For: 128.138.243.150, unknown, 192.52.106.30

Entries are always IP addresses, or the word unknown if the address could not be determined or if it has been disabled with the for-warded_for configuration option.

We must note that access controls based on this header are extremely weak and simple to fake. Anyone may hand-enter a request with any IP address whatsoever. This is perhaps the reason why client IP addresses have been omitted from the HTTP/1.1 specification.

Because of the weakness of this header support for access controls based on X-Forwarder-For is not yet available in any officially released version of squid. However, unofficial patches are available from the follow_xff <http://devel.squid-cache.org/follow_xff/index.html> Squid development project and may be integrated into later versions of Squid once a suitable trust model have been developed.

SQUID mail archive
http://www.squid-cache.org/mail-archive/squid-users/200312/0480.html

Here is how X-Forwarded-For works:

Each proxy in the hierarchy is going to append something to the X-Forwarded-For header. If 'forwarded_for' is on, then Squid appends the client's IP address. If it is off, then Squid appends the string 'unknown'.

In other words, Squid does not remove or replace X-Forwarded-For entries, it only adds to them. If you want to remove the header completely, use the 'header_access' and 'header_replace' directives.

Duane W.

With respect to our task it has the following properties:

- Use should be compatible with the above use. As this use is exactly for the same purpose as with 3GPP, this should not be difficult.
- Support in some proxies and ASs exists. Thus 3GPP may use an existing SW base with only 3GPP specific extensions, if necessary. The concept of X-Forwarded-For is familiar to AS and proxy administrators and thus eases integration into existing infrastructures.
- This header may be used by others and it may appear in requests coming from the UE. If needed, the AP can strip any unwanted existing header field before inserting its own header field.
- To avoid confusion with existing use of this header, the (minor) requirement is that the keyword “unknown” and the standard notation of IP addresses in the header field value have the common meaning also within 3GPP use.

2.5.3 Comparison

Evaluating the properties given in chapters 2.5.1 and 2.5.2, we propose to select the “X-Forwarded-For” special header field for transfer of asserted identity:

- The “X-HTTP-Asserted-Identity “ header field has no advantage over the “X-Forwarded-For” header field, as even the former must be blocked (or at least be checked) by the AP, as malicious users might introduce such fields in their requests.
- The “X-Forwarded-For” header field has some support (and experience) in existing implementations, while support for the “X-HTTP-Asserted-Identity “ header field has to be invested for 3GPP use only.
- The notion of the “X-Forwarded-For” header field is familiar within web-based infrastructure.

With respect to the security concerns raised e.g. in the citations from squid, these are common to all solutions discussed here and are not particular to e.g. one header field. They arise always when the communication between AP and AS is not secured, and are therefore by definition a non-problem in this environment.

2.6 Why to send asserted identity header with each request

The Pseudo-CR also proposes to send the asserted identity in each request inside a session from AP to AS. (The old text states that it is sent only at the beginning of a session).

This is to align the behaviour with common HTTP behaviour. As HTTP does not keep state between successive requests, all authentication methods used with HTTP supply their credentials on every request. To alleviate this task for the user, commonly the browser asks for the credentials only once and keeps state for subsequent requests to resources within the same security realm. As the AP knows the security realm and has the user credentials (tied to the AP sided end point of the TLS tunnel), the best place to keep track of the state is AP. Thus the AS has no longer a need to keep state of the session (except, naturally, if state is kept on higher protocol levels, outside the scope of this protocol).