3GPP TSG SA WG3 Security#31 **S3-030746**
18-21 November, 2003
Munich, Germany

Agenda Item: **6.9 (GAA) and 6.18 (Presence)**

Source: **Siemens**

Title: **Transfer of an asserted User Identity and Location of Access Control – Discussion and Pseudo-CRs to TSs on GAA/HTTPS 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 securely transfer an asserted user identity from AP to AS. If this feature was mandatory for implementation for all ASs it would prevent to use off-the-shelf web servers without this 3GPP-specific enhancements as ASs. This contribution shows that there are situations where the transfer of an asserted user identity to an AS is not required. We therefore propose to make the implementation of this feature in the AS optional and add corresponding requirements to the TSs on GAA/HTTPS and presence security. It is recommended to make the feature mandatory for implementation in the AP for interoperability reasons. We also have a few technical comments on the solution proposed in S3-030540 and propose a slight variant to overcome a possible technical problem.

1 Pseudo-CRs - motivation and proposal

1.1 Status for transfer of an asserted user identity and location of access control

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. This assumption makes sense in many applications, but it is too restrictive for all environments. There are situations were such a configuration is not wanted:

- The AS supports a service accessible for all legal MNO subscribers, i.e. all subscribers successfully passing the authentication, and without need for further authorization.
- The AS is build from an existing (e.g. general Internet) application not aware of this special protocol and perhaps has its own access control on user level.
- The MNO decides to do all authorization for AS access in the AP-NAF for internal organizational reasons, e.g. if only a coarse-grained authorization is necessary and the access control data does not reside on the AS.
- The MNO does not want authorization information in unsecured (plaintext) http headers within his network for some reason. This might happen, if the AS is situated outside the MNO security domain. RFC 2964 states in chapter 2.2.2 that use of cookies for authentication purposes is problematic for exactly this reason and discourages this application of cookies explicitly.
- Additionally there might be ASs not tolerant to the problems stated in the chapter 2 below.

Therefore this feature should be made optional. Ideally the use of this protocol should be manageable on a per server base, i.e. the operator of AP-NAF should be able to configure for each AS if this mechanism is used or not.

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

It is proposed to include the following requirements in TS ab.cde v011 (GAA/HTTPS, S3-030665), section 5.1, and in TS 33.141 v020 (Presence Security), section 5.1.4:

"

- Implementation of check of user identity in the AS is optional.
- Activation of transfer of asserted user identity shall be configurable in the AP on a per AS base."

It is proposed to include these requirements 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 ab.cde (GAA/HTTPS), and that TS 33.141 (Presence Security) only is to make reference to TS ab.cde (GAA/HTTPS).

2 Technical comments on solution proposed in S3-030540

2.1 Comments on existing proposal

We have two small technical comments on the solution proposed in S3-030540.

1. It must also be possible to support Cookie: $Version="1" or higher, as the client and server may send cookies according to their own choice of version and the AP-NAF may only inspect the field and add information, but not modify the version. I.e. AP-NAF must support all current versions of cookie mechanism (<= 1 at the time being according to RFC 2965).
2. As can be referred from chapter 7.2 of RFC 2965, unknown or unexpected cookies may be discarded by RFC 2965 conforming servers. Therefore an AS not capable of this protocol should not get in trouble, but silently discard this cookie value. Two problems still arise:
   a. This would not fulfil the "it shall deny the request" in clause 3 of 6.1.1.1 of the Pseudo-CR attached to S3-030540. The service will not be denied in case a cookie is not relatable to a user. The AS does not know of this mechanism.
   b. The AS (unaware of this mechanism) cannot use a cookie by itself with the same name as the AP uses, but a different content. This would be filtered by the AP as "false cookie" (clause 2 of 6.1.1.1 of Pseudo-CR attached to S3-030540) and disturb the function of the unaware AS.

Numbers 1 just needs a rewriting of the proposal. Number 2 is covered in the Pseudo-CR of chapter 1.

2.2 Variant of solution

With respect to remark number 1 and 2b, there exists an alternative mechanism to the "Cookie header field" enhancement of the proposal in S3-030540:

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.”

Why misuse the cookie field for the purpose of this proposal and not introduce an “extension header field” with new (mobile-specific) name, where all parties in the communication recognize this as a general header field? This would avoid any compatibility problems with session management executed between AS and client. And it would be dropped automatically and silently by all unaware servers.

2.3 Proposal

SA3 is asked to take the above comments (chapter 2.1 and 2.2) into account when developing a solution for the transfer of an asserted user identity.