3GPP TSG SA WG3 Security — SA3#35 **S3-040747**

October 5-8, 2004

St Paul's Bay, Malta

Title: **Control of simultaneous session in scenario 3**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item: **6.10 WLAN interworking**

Work Item: **WLAN-IW**

1 Introduction

Currently in TS 33.234 it is defined that control of simultaneous sessions in scenario 2 makes use of three parameters sent by the WLAN access network to the home AAA server: MAC address, WLAN AN identification and VPLMN identification. This discussion paper will analyze the suitability of the two latter parameters for the control of simultaneous sessions in scenario 3, now named "WLAN 3GPP IP Access"

A recent LS from SA1 has strong influence on this analysis. This LS (S3-040597) states that:

"… SA1 does require that it shall be possible for an explicit check for I-WLAN access authorization to be performed before accessing 3GPP PS based services. "

and

"…there is no requirement to preclude access to PS based services from access networks other than I-WLAN."

These two sentences can be interpreted in the way that the authorization to access WLAN 3GPP IP Access services can be preceded by a checking of WLAN access authorization, but not necessarily. Furthermore, the last sentence points out that other accesses different to WLAN networks are allowed for 3GPP IP Access, which in practice means that the device accessing the PDG does not have necessarily to be connected to a WLAN access network, and even not authorized to.

2 Discussion

The need of the VPLMN id and the WLAN AN id is discussed separately:

VPLMN id

This parameter may be known by the WLAN UE but this is not guaranteed. In scenario 2 (WLAN access) the 3GPP AAA proxy is in charge of sending this parameter to the 3GPP AAA server, but in scenario 3 there is no 3GPP AAA proxy because the authentication flows from the WLAN UE to the PDG in the 3GPP network. These authentication messages traverse some nodes in the WLAN AN and in the VPLMN but they cannot insert or even read any contents of the authentication messages as they are run over IKEv2 which establishes an encrypted and integrity protected channel.

The protected channel IKEv2 sets up makes the WLAN UE the only element able to send the VPLMN id. However, as pointed out before, this is not always known to the WLAN UE. Furthermore, the parameter could be spoofed by an attacker that wants to access through different visited networks. Nevertheless, when the access WLAN 3GPP IP access (scenario 3) is with a PDG in the VPLMN, it is possible to know the VPLMN id as the PDG will send that information to the AAA server via the Wm interface.

WLAN AN id

TS 29.234 specifies that the WLAN AN id is a parameter which in scenario 3 the WLAN AN sends to the AAA server/proxy within an attribute called "Operator name", defined in ref. [1]. The description is:

> This attribute contains an operator name which uniquely identifies the ownership of an access network. The Attribute value is a non-NULL terminated string whose Length MUST NOT exceed 253 bytes. The attribute value is comprised of the prefix and the identity, separated by a colon. The prefix identifies the operator type; example: GSM, CDMA, and REALM. The identity uniquely identifies the operator name within the scope of the operator type.
>
> As an example consider the string 'GSM:TADIG' where GSM is a prefix indicating an operator type and TADIC is a unique globally known GSM operator ID.
>
> This document defines three operator type prefixes which are: GSM, CDMA, and REALM. The GSM prefix can be used to indicate operator names based on GSMA TADIG codes. REALM can be used by any domain name acquired from IANA. Possible forthcoming operator types MUST be associated with an organization responsible for assigning/managing operator names.

The "Operator name" value is sent by the WLAN AN to the PLMN through the Wa interface, and according to its description it does not correspond with the SSID, so the WLAN UE does not have knowledge of the WLAN AN id.

Then the WLAN UE cannot send the WLAN AN id to the AAA server in scenario 3. And as in the case of the VPLMN id, this parameter cannot be inserted by any intermediate node because of the IKEv2 protected channel.

3 Conclusions

The control of simultaneous sessions in scenario 3 has to be made without the help of VPLMN id and WLAN AN id parameters, as it has been proven that these ones would have to be sent from the WLAN UE. The major drawback is that these parameters are not always available in the WLAN UE and, if they are, there is no mechanism to authenticate them so they could be spoofed by an attacker.

The only exception is when the PDG is in the VPLMN. This situation can be detected by the AAA server and use the VPLMN id received by the PDG.

4 References

[1] IETF Draft, "Attributes for Access Network Location and Ownership Information", http://www.ietf.org/internet-drafts/draft-tschofenig-geopriv-radius-lo-00.txt, work in progress