3GPP TSG SA WG3 Security — S3#34 **S3-040608**
July 6 - 9, 2004
Acapulco, Mexico

Title: LS on Binding Scenario Information to Mutual EAP Authentication
Release: Rel-6
Work Item: WLAN

Source: SA3
To: SA2
Cc: -

Contact Person:
Name: Dajiang Zhang
Tel. Number: +86 13901168924
E-mail Address: **Dajiang.zhang@nokia.com**

Attachments: -

---

1. Background:

In SA3#33 meeting, contribution S3-040372 was presented in order to show an attack against WLAN users. Basically, this attacks consists of that a compromised WLAN access point can simulate a PDG towards the user and act like an access point towards the AAA server. As the AAA server has no way to be aware of this attack, the user will be authenticated for scenario 3 while the AAA server believes the user is using scenario 2.
In order to solve this attack, there exist currently some solutions. The accepted solution in the IETF, which is mandatory in IKEv2, see draft-ietf-ipsec-ikev2-14.txt, and which has also been incorporated in TS 33.234 v610 is the use of a certificate to authenticate the network (the PDG) towards the user. This will make it impossible for an attacker to simulate a PDG by means of compromising an access point.

2. Discussion:

In SA3#34 meeting, the discussion paper S3-040562 was presented, in which it is proposed to use a modified version of the NAI in order to convey information of the scenario for which authentication is being performed. This solution will help to prevent man-in-the-middle attacks as the one described in S3-040372, and can be seen as an alternative to the use of certificates to authenticate the PDG.

The enhancement of the NAI works as follows:

The current format of NAI is specified in chapter 14.2 of 3GPP TS 23.003 and it is:
wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org
where:
mnc<MNC> and mcc<MCC> identify the home network.

For example: If MNC = 15 and MCC = 234 then realm part of NAI is "wlan.mnc015.mcc234.3gppnetwork.org".

The enhanced NAI shall contain WLAN scenario information and possible visited network information and it use the following format:
wlan<SCEN>.vmnc<VMNC>.vmcc<VMCC>.mnc<MNC>.mcc<MCC>.3gppnetwork.org
where:

- wlan<SCEN> identifies the WLAN scenario.
  The possible values could be wlan-scen2, wlan-scen3-hn, wlan-scen3-vn
- vmnc<VMNC> and vmcc<VMCC> identify the visited network.
  This part is omitted, when it is home network situation.
- mnc<MNC> and mcc<MCC> identify the home network.

For example: If visited network scenario 3 is used, the visited network is MNC =23 and MCC=123 and the home network is MNC =15 and MCC=234 then realm part of NAI is "wlan-scen3-vn.vmnc023.vmcc123.mnc015.mcc234.3gppnetwork.org"

It should be noted that the discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing in SA3 and SA3 has not yet agreed to replace the solution in TS 33.234 v610 with the solution proposed in S3-040562, even if SA2 confirms its feasibility. But SA2 is nevertheless contacted at this stage because the deadline for Release 6 is approaching fast, and a response to an LS sent from the next SA3 meeting would probably come too late to be considered for Release 6.

It should also be noted that there is ongoing work at the IETF to address the problems, which the modified NAI proposal in S3-040562 tries to solve, but by different means, cf. draft-eronen-ipsec-ikev2-eap-auth-01 and draft-arkko-eap-service-identity-auth-00.

3. Actions:

SA3 kindly asks SA2 to study the feasibility of using enhanced NAI and provide to response in order to take a decision on the mechanism to be used.

4. Date of Next TSG SA WG 3 Meetings:

TSG-SA3 Meeting #35	5-8 October 2004	Malta
TSG-SA3 Meeting #36	23-26 November 2004	Shenzhen, China