3GPP TSG SA WG3 Security — SA3#35 **S3-040716**
October 5-8, 2004
St Paul's Bay, Malta

Title: **Using PDG certificate in scenario 3**

Source: **Nokia**

Document for: **Discussion and decision**

Agenda Item: **6.10**

Work Item: **WLAN-IW**

1 Introduction

In SA3#33 meeting, contribution S3-040372 showed 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 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.

An LS was sent to SA2 and asked SA2 to study the feasibility of using enhanced NAI. The reply from SA2 is in S2-042951(S3-040701).

This contribution discusses the use of server certificates scenario 3 in preventing a WLAN Access Point (AP) from masquerading a Packet Data Gateway (PDG) or vice versa.

2 Discussion

In S2-042951, it says:

EAP-AKA is used in two different situations; authentication for WLAN access (stated as scenario 2 in S3-040672) and authentication during tunnel setup (stated as scenario 3 in S3-040672). In the former case, EAP messages are routed via AAA servers, so NAI decoration is required. But in the latter case, EAP messages are transported directly between a WLAN UE and a PDG, so no NAI decoration is required.

SA2 acknowledges that the main purpose of the proposal in the LS is not EAP message routing but solving the security problem (i.e. Man-In-The-Middle attack). However, the enhanced NAI and the decorated NAI contains overlapping information about VPLMN identity when it is used for WLAN access authentication.

Decoration of the realm part of NAI is done according to the current version of EAP-AKA Internet-Draft and RFC 2486bis. SA2 thinks that the proposal from SA3 to decorate the realm part of the NAI needs to be checked against these documents.

To solve the problem, Server certificates can be used in IKEv2 tunnel setup in order to authenticate the PDG to the WLAN UE. When server certificates are used, a WLAN AP that does not have a suitable certificate will not be able to impersonate as a PDG, even if it was able to successfully run EAP authentication. However, since certificates are not used in WLAN scenario 2 authentication, this solution does not prevent a PDG from impersonating a WLAN AP. For example, a Visited PDG could pretend to be a WLAN AP of the home operator and successfully pass scenario 2 authentication.

3 Conclusions

The current TS does not contain enough information about the certificates and their processing to ensure interoperability between different UEs and PDGs. A certificate profile based on the OMA WAP certificate profile is proposed in a separate CR (S3-040717). It is proposed that server certificates are used in scenario 3 to authenticate the PDG. However, this solution will not protect against dishonest PDG impersonating as a WLAN AP. If this case is considered important, then support for enhanced NAI should still be included.

4 References