3GPP TSG SA WG3 Security#33 **S3-040372**
10 – 14 May, 2004
Beijing, China

Agenda Item: **6.10 WLAN**

Source: **Siemens**

Title: **Comments on S3-040275 (Ericsson, Nokia) and S3-040288 (Nokia) relating to PDG authentication using IKEv2 in scenario 3**

Document for: **Discussion and decision**

Abstract

The current version of TS 33.234 specifies in section 6.1.5 that "Public key signature based authentication with certificates, as specified in [ikev2], is used to authenticate the PDG." S3-040275 (EAP in IKEv2) by Ericsson and Nokia proposes a CR to replace this sentence by "Depending on the WLAN UE, either EAP-AKA or EAP-SIM within IKEv2, as specified in [32], is used to authenticate the PDG ". While it is correct to say that the use of certificates may be superfluous because EAP-SIM and EAP-AKA provide mutual authentication, there are several problems with this proposed CR which are addressed in this comment.

1 Man-in-the middle attacks when not using certificate-based authentication of responder (server) in IKEv2

1.1 Impersonation of a PDG (scenario 2) by a WLAN AP (scenario 2)

When EAP-AKA or EAP-SIM are used for authentication of the PDG in IKEv2, this gives only the assurance to the UE that the PDG is authorised by the EAP AAA server to receive the EAP session keys. On the other hand, draft-ietf-ipsec-ikev2-13 mandates the use of public key signature based authentication with certificates. This can give additional assurances to the UE, depending on the semantics of the certificate of the responder. In more detail:

For 3G-WLAN interworking, EAP-AKA and EAP-SIM are meant to be used for both, scenario 2 (IP connectivity over WLAN, EAP over IEEE 802.1X) and scenario 3 (IPsec tunnel between UE and Packet Data Gateway, set up using IKEv2+EAP). It is quite plausible that scenario 3 should come with higher security guarantees for the user than scenario 2 because the user is more likely to trust services provided by his home operator, reached through a PDG, than services provided by a WLAN access network.

But a rogue, or compromised, WLAN AP can impersonate a PDG, as follows: the EAP session key is the MSK from EAP-AKA and EAP-SIM, which is delivered from the EAP AAA server to the WLAN AP (in scenario 2) as well as to the PDG (in scenario 3). Hence the AUTH payload in IKEv2 is computed from MSK, and any attacker who can impersonate a WLAN AP, authorised to participate in scenario 2, towards the EAP AAA server, can obtain the MSK, and consequently compute the AUTH payload and impersonate the PDG towards the UE. But WLAN APs may be assumed to be much more vulnerable than PDGs in the 3GPP operator's home network, making an attack more likely.

1.2 Impersonation of a PDG in the home network by a PDG in a visited network

TS 23.234 allows PDGs to also reside in a visited network. Then a PDG in a visited network may also receive the EAP keys MSK from the EAP AAA server in the user's home network. In the same way as described in section 1.1, the PDG in the VN could impersonate a PDG in the home network without the user or the EAP AAA server in the home network knowing. However, it should be noted that UMTS does not allow the user to authenticate the PS or CS access network either, so, if the security objective is only to connect the user securely to any 3GPP network, then there is no problem, but if the security goal is to, in addition, assure the user that he is connected to the home network then the possibility of impersonation of a PDG by another PDG needs to be addressed. This is to be decided by operators.

2. Countermeasures against Mitm attacks

2.1 Use of public key signatures based authentication with certificates

This is the approach mandated in draft-ietf-ipsec-ikev2-13. The implicit semantics of the certificate could be as follows: the certificate may be verified with a root key which is only used to sign certificates of PDGs of the user's home operator. The UE is pre-configured to use only this root key in the context of scenario 3. In this way, the user knows that he is setting up an IPsec tunnel to the home operator, and not to somebody in control of a WLAN AP.

2.2 Secure context-information in EAP-SIM or EAP-AKA

EAP-SIM or EAP-AKA could be enhanced to securely carry context information between UE and EAP AAA server, which ensures that an AP or a PDG in a visited network cannot present two different contexts, one to UE and another to the EAP AAA server. E.g. in the attack in section 1.1, the AP pretends to the UE to be an authorised entity in the context of scenario 3, while the AP is (correctly) known to the EAP AAA server only as an authorised entity in the context of scenario 2.

An example of how to enhance EAP-SIM or EAP-AKA is contained in TS S3-040288 (Introducing the special RAND mechanism with GSM/GPRS and WLAN separation) by Nokia. This contribution proposes to change TS 43.020 to extend the special RAND mechanism to also separate WLAN scenario 2 from WLAN scenario 3 (cf. section C.4 of S3-040288), for the case of EAP-SIM. The proposal could be easily extended to also provide this separation for EAP-AKA, probably requiring a change to TS 33.102. The proposal does not necessitate any changes to the IETF specifications of EAP-SIM or EAP-AKA. Using the mechanism in S3-040288, one can prevent the attack described in section 1.1, but not the one in section 1.2. But it seems plausible, that, by introducing new EARV values, also PDGs in the home and the visited networks could be distinguished, if required.

Please also note that it is up to the operator to implement the special RAND mechanism, and a decision not to implement it would not cause any interoperability problems. Therefore, if PDG authentication is to be based on EAP-SIM or EAP-AKA rather than on certificates, a note should be added to TS 33.234 as a warning that measures against the Mitm attacks described in section 1 of this contribution need to be in place.

Another example, how to prevent the described Mitm attacks, is given in draft-arkko-eap-service-identity-auth-00 which is a generalised mechanism than those proposed in Section 11.4 of draft-tschofenig-eap-ikev2-03.txt. There, it is proposed that integrity-protected information about the authenticator (AP or PDG) is included in EAP messages.

3. Non-compliance with IKEv2 standard

The proposal in S3-040275 is in contradiction to draft-ietf-ipsec-ikev2-13, which is likely to evolve into the IKEv2 standard. It should be noted that draft-eronen-ipsec-ikev2-eap-auth-00.txt (reference [32] in S3-040275) addresses the issue of mutual authentication of initiator and responder in IKEv2 without using certificates, in situations when the EAP method already provides mutual authentication. But this draft is still work in progress.

Furthermore, it has to be clear from TS 33.234, exactly what has to be done by the PDG and the UE to perform authentication. The sentence *" Depending on the WLAN UE, either EAP-AKA or EAP-SIM within IKEv2, as specified in [32], is used to authenticate the PDG "* seems not sufficient, as the referenced draft [32] offers four alternative solutions, without making a decision for one. For interoperability reasons, no more than one of these alternatives shall be selected by 3GPP.

4. Proposal

It is proposed to only accept S3-040275 if

- the man-in-the-middle attacks described in section 1 are satisfactorily addressed, and a corresponding note is added to TS 33.234, how it is addressed;
- the issues arising from non-compliance with the IKEv2 standard are resolved.