3GPP TSG SA WG3 Security — S3#34 **S3-040522**

6 - 9 July 2004

Acapulco, Mexico

Title: **Security threats in Wa interface**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **WLAN-IW**

1 Introduction

This paper analyzes the possible threats in the Wa interface. In particular, the risks associated to the sending of the Pairwise Master Key (PMK) from the 3GPP AAA server to the WLAN access network.

2 Discussion

2.1 Wa i/f with Diameter

If the AAA server/proxy communicates with the WLAN AN using Diameter, according to ref [1], the use of IPsec is mandatory and TLS is optional for Diameter clients (in this case, the WLAN access network). Both methods (IPsec and TLS) are mandatory for Diameter servers (the AAA server/proxy).

IPsec includes in the headers (AH and ESP) a sequence number, so replay attacks are not possible.

2.2 Wa i/f with RADIUS

When the Wa interface is implemented using RADIUS, the RADIUS message where the PMK is sent (Access-Accept) is authenticated with the Response Authenticator field. Furthermore, the attribute in which the PMK is carried, MS-MPPE-Recv-Key, is encrypted. The encryption of this attribute (fully described in ref. [2]) is performed calculating an MD5 digest of the string formed by shared secret (the one shared by the RADIUS client and the server), the Request-Authenticator (random generated by the client) and the Salt (random generated by the server). Then the MD5 digest is XORed with the key to be sent (the PMK in our case). This encryption method prevents replay attacks as both the client and the server give a random number used to generate the encrypted key.

This protection is performed hop-by-hop, that is, in a roaming situation, the home network has to trust the visited network (i.e. the AAA proxy) to perform these security measures.

3 Conclusions

As no attack has been identified to IPsec implementations, the use of Diameter for Wa interface is considered secure.

In the other hand, the encryption of the AVP that contains the PMK, together with integrity protection in the Access-Accept message, make the interface secure enough when working with RADIUS.

It is proposed to remove the following editor's note in chapter 4.2.2 of TS 33.234:

"Threats on the Wa interface are not clear yet, so protection on this interface is for further study."

4 References

[1] RFC 3588, September 2003, "Diameter Base Protocol"

[2] RFC 2548, March 1999, "Microsoft Vendor-specific RADIUS Attributes"