3GPP TSG SA WG3 Security — S3#32 **S3-040109**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda Item: **6.10 (WLAN)**

Source: **Siemens**

Title: **Comments on S3-040048 and S3-040083 - comparison of alternatives for UE functionality split**

Document for: **Discussion and decision**

Three alternatives were presented by Siemens in S3-030747. Alternatives 2 and 3 are discussed further in the contributions S3-040048 and S3-040083.

To recap:

In alternative 2, the EAP client resides entirely on the MT, only the MSK is sent to the TE.

In alternative 3, the EAP client resides almost entirely on the TE, only the MK is derived on the MT and sent to the TE.

Comments on statements in S3-040048:

Alternative 2

(-) Potential difficulties with WLAN UE –initiated re-authentication as the MT is not aware of the state of the radio link (cf. S3-040048, section 3.2.1)

comment: agree

Alternative 3

"*when a fast re-authentication takes place, then there is no need for the TE to contact the (U)SIM in the 3GPP UE via a Bluetooth link in alternative 3. This would save signaling on the Bluetooth link between the TE and MT and also power consumption in the MT*." (cf. S3-040048, section 3.1.1)
comment: agree

Additional comment: Also full authentication would be faster as there is only one roundtrip over Bluetooth and not two (as in EAP-AKA) or three (as in EAP-SIM), and messages over Bluetooth are shorter.

Additional comment: impact on MT implementation (e.g. mobile phone) is minimised, the functionality split in alternative 3 is more likely to reflect the balance of capabilities of MT (small) and TE (powerful). This, in our view, is a major argument.

Note on success of attack for EAP-SIM: S3-040048 says: " In Alternative 3, replay attacks will not be prevented by the NONCE_MT parameter in EAP-SIM, as the TE allocates the NONCE_MT value but the MT calculates the MK, using the NONCE_MT has input. " This seems not correct. It appears that it was overlooked that the MAC in the EAP request is computed also over NONCE_MT, hence the MAC cannot be replayed, cf. the Siemens contribution S3-040091.

Comments on statements in S3-040083:

Alternative 3

" *(-) On the other hand, the re-authentication procecure no longer ensures that the laptop is in possession of the smart card. Sharing of subscription until re-authentication state exprises [expires?] may be possible*."

Comment: the smart card is not involved in re-authentication, for either alternative. It is acknowledged, though, that the MT may be a more secure environment in general. However, one should remember the threats which were meant to be addressed by the functionality split. These are the separation of the WLAN domain from other domains, and the prevention of network impersonation.

" *(-) this solution is specific to certain versions of EAP-SIM and EAP-AKA. Other EAP methods are not supported at all. If EAP-SIM or EAP-AKA is updated, then the BT profile also needs to be updated*."

Comment: first of all, 3GPP should concentrate on the measures required for 3G-WLAN interworking. From a 3GPP point of view, there seems to be no need to support other EAP methods. The 3GPP decision should not be driven by speculations about what could be useful for non-3GPP purposes. If the need for a BT profile for general EAP transport arises in the future, driven by an application, then it should be possible to add such a profile. Remember that there are currently over two dozen different BT profiles already. Secondly, the statement seems not correct as, with a Bluetooth profile supporting EAP-AKA and EAP-SIM, all EAP methods would be supported where the MT computes the MK from keys available to the MT and key derivation parameters sent from the TE. As far as the BT profile is concerned only the transport of such parameters is required, their content does not matter.

" *(-) EAP-SIM network authentication is performed by the laptop, so a malicious piece of software running on the laptop can make the card holding device calculate EAP-SIM master keys for chosen triplets and nonce values that are easier to break the SIM. This may enable the malicious piece of software to mount attacks against the SIM*"

Comment: this does not seem correct, at least as long as it may be assumed that the one-way property of SHA-1, which is used to derive MK, cannot be broken. Therefore it is not clear how an attacker should infer any information about the content of the SIM from the MK he receives.

Conclusion

Both alternatives provide good security and seem feasible. Some arguments against alternative 3 in S3-040083 seem not valid, while the advantage regarding implementation was overlooked. So, Siemens prefers alternative 3 for performance and implementation reasons, in contrast to the conclusion in S3-040083.

References

S3-040048 Ericsson, " Split WLAN UE: Termination of EAP-AKA/SIM protocol"

S3-040083 Nokia, " WLAN BT alternatives"