3GPP TSG SA WG3 Security — S3#32 **S3-040100**
09 - 13 February 2004
Edinburgh, Scotland, UK

Title: **Using Special RANDs to separate WLAN and GSM/GPRS**

Source: **Nokia**

Document for: **Discussion and decision**

Agenda Item: **6.10 WLAN interworking**

1 Introduction

Ericsson and TeliaSonera proposed in [1] that Special RANDs sent to the WLAN AAA server should prohibit the use of all A5 and GEA algorithms. A terminal implementing Special RANDs would then reject these RANDs on the GSM/GPRS interface. This would mean that an attacker cannot use the Barkan et al. real-time A5/2 attack [2] to impersonate a WLAN client towards the WLAN network.

2 Discussion

We agree with the basic proposal in [1], but suggest some improvements. Unlike GSM/GPRS, EAP-SIM [3] provides a (somewhat weak) form of network authentication. An attacker cannot impersonate the WLAN access network towards the WLAN client unless he knows 2-3 triplets acceptable to the WLAN client.

GSM encryption algorithms have a number of known weaknesses that allow an attacker to obtain valid triplets. The most serious attacks are probably the real-time A5/2 attack and the passive A5/1 attack, both by Barkan et al. [2].

If there are RAND values that are accepted by both GSM/GPRS and WLAN side of the terminal, an attacker can use these GSM/GPRS attacks to get two triplets, and then impersonate the WLAN network towards the terminal. This is probably a less serious concern than impersonating the WLAN client towards the network, but a concern nevertheless.

3 Proposal

We propose that the special RAND mechanism should be implemented in a way that would allow the terminals to use disjoint RAND spaces for GSM/GPRS and EAP-SIM. This would mean that any vulnerabilities in GSM/GPRS could not be used to attack EAP-SIM, and vice versa.

The Special RAND mechanism in [4] adds two fields inside the RAND. The "flag" field is 32 bits all set to 1, and is used to distinguish special RANDs from non-special RANDs. The "Encryption Algorithms Restriction Vector (EARV)" specifies which encryption algorithms are allowed. As currently proposed, it contains 16 bits for the A5/0...A5/7 and GEA0...GEA7 algorithms.

If the RAND is not a special RAND, all algorithms are allowed. This is required to handle the situation where the terminal supports special RANDs but HLR/AuC does not. That means that the RAND spaces used in GSM/GPRS and EAP-SIM are not disjoint, since non-special RANDs are accepted in both contexts.

However, if the terminal knows (by manual configuration or other mechanism) that the HLR/AuC supports special RANDs, it could implement "strict" special RAND processing. By "strict" processing, we mean that:

1. The terminal rejects all non-special RANDs, at least when accessing a WLAN network.

2. When accessing a WLAN network, the terminal rejects all special RANDs that allow any A5/GEA algorithms.

3. When accessing a GSM/GPRS network, the terminal rejects all special RANDs that allow WLAN access (EAP-SIM)

This would mean that the RANDs accepted by GSM/GPRS and those accepted in EAP-SIM are disjoint sets. Some possibilities how strict special RAND processing could be implemented include the following.

1. Specify that all-zero EARV (prohibiting all A5 and GEA algorithms) means "WLAN access".

2. Add one more bit to EARV (indicating EAP-SIM), and specify that this bit MUST NOT be set to 1 unless all the other bits are set to 0.

3. Add a "context" field before the EARV. It is TBD how many different values this field should have (e.g. "GSM", "GPRS", "WLAN scenario 2 (EAP-SIM for 802.11)", "WLAN scenario 3 (EAP-SIM for IKEv2)").

If implemented, this strict special RAND processing would prevent an attacker from using GSM/GPRS weaknesses to impersonate WLAN network towards the terminal. Separating these contexts also means that a compromise of some component in one context (e.g. AAA server) does not allow the attacker to impersonate the network towards the client in some other context.

4 References

[1] S3-030733; Ericsson, TeliaSonera: Implications of the A5/2 Attack for 3GPP WLAN Access

[2] Barkan, Biham, Keller: Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication; CRYPTO 2003

[3] Haverinen, Salowey: EAP SIM Authentication; draft-haverinen-pppext-eap-sim-12.txt

[4] S3-030698; Orange, Vodafone: Introducing the special RAND mechanism