3GPP TSG SA WG3 Security — S3#13 **S3-000322**

23-26 May, 2000

Yokohama, Japan

Source: Lucent Technologies Inc., Motorola

Title: Improved conversion functions for GSM-UMTS interoperation

Document for: Consideration

Agenda Item: ___

Introduction

This contribution proposes improved conversion functions for GSM-UMTS interoperation to replace the functions (c4 and c5) currently described in TSG 33.102 Rev 3.4.0 section 6.8.2.3. The upgraded conversion functions include the 32 bits (least significant bits) of the International Mobile Subscriber Identity (IMSI).

Short History

GSM AKA results in the establishment of a 64-bit "GSM" ciphering key Kc. When the user is attached to a serving system capable of supporting a 3GPP 128-bit ciphering key (CK) and a 128-bit integrity key (IK), a translation function has to be developed capable of converting the Kc (GSM) into a CK and an IK (UMTS).

A number of proposals have been put forward, each attempting to improve the key robustness and cryptographic strength. The current proposal in discussion at the S3 meeting #12 is shown here:

C4: $CK_{[UMTS]} = K_C \,||\, K_C$

C5: $IK_{[UMTS]}$ = Kc1 xor Kc2 || K_C || Kc1 xor Kc2

(Where Kc1 and Kc2 are both 32 bits long and Kc = KC1 || Kc2)

Although this approach is relatively robust, we are putting forth an improved proposal that will significantly add to the CK and IK protection against a brute force attack.

Proposal:

The proposal put forth is to implement the following translation functions:

C4: $CK_{[UMTS]}$ = KC || $IMSI_{64}$
C5: $IK_{[UMTS]}$ = KC xor $IMSI_{64}$ || KC

Whereby:

$IMSI_{64}$ = $IMSI_{32}$ || $IMSI_{32}$ while the $IMSI_{32}$ is the least significant 32 bits (the most unique part of the subscription identity) of the International Mobile Subscriber Identity (IMSI) stored in the USIM and the VLR/SGSN.

This proposal significantly adds to the practical difficulty of decrypting the CK and IK keys; especially increases the complexity of a brute force attack. Although, cryptographically speaking, one cannot have more than 64 bits of strength, if we began with a 64 bit secret, including the IMSI as an input to the C4/C5 functions adds a practical difficulty to the attacker who does not know the IMSI.

Suppose an attacker has built a 64-bit hardware cracker, which can recover a 64-bit key in few seconds. Repeating Kc||Kc would not significantly increase the complexity of a brute force attack. However, adding IMSI into the mix means that a brute force searching requires approximately 2^{96} (64_{KC} bits + 32_{IMSI} bits) tries which is not feasible with current hardware.

The other attacker's alternative would be to apply a false basestation attack to get the IMSI, but this alternative has its own practical difficulties and it may become even more difficult in future UMTS releases. But even if the IMSI is captured, there is no security degradation compared with the current C4/C5 functions that use only the K_C as input.

Conclusion

Including the KC and the IMSI as inputs to the C4/C5 translation functions increases the complexity of a potential brute force attack targeted at capturing the mobile's CK and/or IK. We are recommending that TSG SA 3 adopts the functions described above and 3G TS 33.102 document be changed to reflect the new function definitions.