3GPP TSG SA WG3 Security — SA3#35 **S3-040728**

October 5-8, 2004

St Paul's Bay, Malta

Agenda Item: 6.6

Source: QUALCOMM Europe, Ericsson

Title: An observation about Special RAND in GSM

Document for: Discussion and Decision

1. Background and introduction

This contribution raises a potential problem with the proposed Special RAND mechanisms when used in conjunction with GSM A3/8 example algorithm COMP128, or other A3/8 algorithms which exhibit collisions. Alas, despite well-known weaknesses with COMP128 it is believed that this algorithm remains in use by a significant number of operators. Enhancements supporting COMP128, such as adding counters to disable the SIM after a certain number of challenges, do not guard against the attack described.

2. Discussion

Several contributions (eg [1]) propose the introduction of a Special RAND mechanism as a means to overcome problems arising from a lack of key separation in GSM/GPRS. One of the aims is to allow operators to improve GSM security for customers replacing their terminals, without requiring a change in subscribers' SIM cards.

However, we raise some concerns about whether this approach is necessarily as effective as it would first appear. One concern is that a significant number of operators support SIMs using the example A3/8 algorithm COMP128. While significant weaknesses have been known for some time, it has been perceived that COMP128 is not susceptible to over-the-air attacks and that cloning risks are limited.

However, the concern raised here is that operators using COMP128 will be vulnerable to active Barkan-Biham-Keller attacks [2] even if Special RAND mechanisms are employed.

The issue is that even if an operator challenges with Special RAND, an attacker may tweak two bytes of this RAND to make it non-special, yet expect the same output from COMP128 with probability approximately about 2^(-14) according to the analysis by Briceno, Goldberg and Wagner [3].

Thus suppose an operator is using COMP128 and deploys a special RAND mechanism to establish a call and force the use of A5/3. An attacker may later challenge the mobile with tweaked non-special RAND. If the resulting RES matches the original then a collision may be assumed and the attacker can force the new call into A5/2, launch the BBK attack, and derive the keys used in the original 'secure' call.

Alternatively during the authentication procedure a man-in-the-middle may tweak a Special RAND to become non-special, and forward it to the terminal. The attacker next relays the resulting SRES to the network, while forcing the call into A5/2 and deriving Kc using BBK. Thus a man-in-the-middle attempting to attack approximately 2^14 authentication attempts may expect to hijack a call, while the network will believe authentication and key separation to have been successful and the call to have been encrypted using a stronger algorithm. Note that these 2^14 authentication attempts may be spread across any number of subscribers; it is not necessary to conduct repeated challenges of the same SIM in order to conduct the attack.

3. Conclusion

Those operators who have deployed COMP128 will remain susceptible to man-in-the-middle attacks even if they employ special RAND mechanisms, because weaknesses in COMP128 may be used to break the purported key separation in special RAND. The simplest and most effective approach to improving GERAN security across the board will be to promote the ubiquitous adoption of A5/1 and A5/3, and remove support of A5/2 from terminals immediately. Approaches to add a MAC the cipher mode command should then be phased in as soon as practical.

4. References

[1] Nokia and Orange, Analyse of the countermeasures to Barkan-Biham-Keller attack, S3-040528.

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

[3]. See for example David Wagner’s site http://www.isaac.cs.berkeley.edu/isaac/gsm.html