3GPP TSG SA WG3 Security — SA3#35 **S3-040789**
5 - 8 October 2004
St. Paul's Bay, Malta

Source: **Ericsson, Qualcomm Europe, Vodafone**

Title: **Future of GERAN Security**

Document for: **Discussion and decision**

Agenda Item: **6.6 GERAN network access security**

1 Introduction

This document proposes a more in-depth study of appropriate measures to provide long-term GERAN security.

2 Background

While some short-term actions (removal of A5/2 from terminals, quick introduction of A5/3) are needed to remove the worst effects of the discovered A5/2 vulnerabilities [1], it is also agreed in SA3 that a long-term security enhancement is needed to secure GERAN in the future. Special RAND [2] and authenticated cipher command [6,12] (and other solutions, e.g. [3, 5, 10]) have been proposed as potential long-term solution.

While both special RAND and authenticated cipher command provide nice improvements, we feel that before deciding on the exact mechanism(s), it is appropriate to take a deeper look at what these countermeasures achieve, respectively what "holes" are left open. The purpose of this document is not to provide such an analysis, but rather to point to some potential issues and start a discussion on the need for a more careful analysis. Ultimately, the analysis should lead to the specification of an enhanced GERAN security solution that is more comprehensive and does not only concentrate on the effects of the A5/2 attack in GSM.

Based on current consensus and previous discussion in SA3, we make the assumption that at least one of Special RAND and/or Authenticated Cipher command is likely to be part of a long-term solution. We also assume A5/2 will be phased out.

3 Effects of Special RAND and Authenticated Cipher Command

Earlier contributions, e.g. [7,8] have analyzed the improvements (and possible problems) with these solutions, so we will not repeat the details here. Suffices to say that:

- A (properly implemented) authentication of the cipher command removes bidding down attacks from an active attacker. It does not provide any other protection, and negative side effects seem not to exist.
- Special RAND makes it impossible to run a non-allowed version of A5/GEA. Concerns as to the real effect have been raised, and some potential negative cryptographic side effects have been discussed [9]. (Also this does not protect user privacy if the attacker is willing to pay for the calls and the terminal supports A5/2 – a man-in-the-middle attacker can challenge with non-special RAND.)

Now, let us look at the root causes of the A5/2 (in)security implications.

3.1 Why A5/2 problems?

Looking closer, it is clear that the (various) problem arising from the A5/2 cryptanalysis is a combination of:

1. A weak algorithm (A5/2).

2. No replay protection (an old RAND will be accepted over and over again by the MS).
3. No network authentication (*any* RAND will be accepted by the mobile)
4. No key separation (same RAND, same Kc for any A5 algorithm).
5. No protection for algorithm selection (allowing bidding down attacks).

It is clear that each one of these is a potential opening for attacks to the network and/or subscriber, and UMTS security has been designed to counter these threats by combining network authentication, replay protection and security for algorithm selection. It is not clear that we should not strive for "UMTS level" security in GERAN, and there could even be reason to go beyond that for a future proof solution, see below.

3.2 What is NOT solved?

Clearly, authenticated cipher command and special RAND do not overcome all the vulnerabilities 1-5 above. Below, we briefly discuss potential impact of not taking care of these. It would seem prudent that a long-term enhancement of GERAN at least *considers* the risk of leaving one or more of 1-5 open for potential attack before deciding for which solution to choose. Moreover, there are some potential threats that not even countermeasures to 1-5 would take care of.

3.2.1 A5/1 (In)Security

A5/2 is not the only GSM cipher with questionable security. Recent attacks on A5/1 (e.g. [4]: about 20 seconds of known plaintext, and a ten minutes computational effort) raises the question how long we can trust A5/1. In a worst-case scenario A5/1 is as severely broken as A5/2 next year and needs to be phased out too. That leaves us with A5/3 and A5/4, and considering the high confidence/similarity of these, an authenticated cipher command will not do any good (they are most likely "equally" good/bad).

3.2.2 GPRS Security Problems

The authenticated cipher command is aimed at GSM. It is not unlikely (some may argue highly probable) that GEA1 (or even GEA2) could be broken. One can suspect that their security today relies largely on "security by obscurity". Looking at the authenticated cipher command in GSM, it is clear that it would not solve anything if GEA1 is broken, unless the same mechanism protecting algorithm choice is introduced in GPRS too. The possibility to apply the authenticated cipher command also in GPRS was discussed in [6].

3.2.3 Lack of Network Authentication

The fact that the network cannot be authenticated has well-known impacts and was considered a "real" threat when UMTS security a designed.

3.2.4 Lack of Replay Protection

GSM (for good reasons) relies on stream ciphers. These are vulnerable to replay attacks, causing so-called two-time-pads. On could imagine an attack as follows. An A5/1 (say) session is recorded. Later, the victim is (somehow) fooled into sending a known message (e.g. email) using the same replayed RAND. This enables the attacker (using a false base station) to decrypt the recorded traffic. Even if *this* attack is not considered realistic, it shows an "unsoundness" in allowing replay that could potentially be exploited also in other ways.

Network authentication (3.2.3) is typically a pre-requisite to obtain replay protection.

3.2.5 Lack of Key Separation

The scenario above (3.2.4) can also serve as a demonstrator of the issues involved with (non)key-separation. In fact, Special RAND combined with A5/2 removal would not counter the above attack since it can be performed with totally secure and allowed stream ciphers.

3.2.6 General Ciphering Practice

The above-mentioned lack of key separation is *one* example of a sub-optimal ciphering practice. Are there other examples? In [13,14] issues were raised concerning potential loss of security in connection to PS handover. The security of the GPRS ciphering depends on the uniqueness of a 32-bit IOV value; in case of collision (which may occur in such hand over situations) a two-time-pad is generated, revealing *at least* the XOR of the corresponding plaintexts. With the coming 128-bit GEA4 algorithm, the overall security will potentially depend on accidental collisions between 32-bit values, and may not reach the expected 128-bit level.

3.2.7 New Threats

It is very hard to predict new threats, but there are some that we see lurking at the horizon that would be suitable to at least take into account before deciding on "the" protection mechanism. A potential threat scenario is discussed in [11]. Another example is given next.

There is a trend towards decreased trust in the visited network. E.g. in IMS, authentication is done in the home. Consider the following "repudiation" scenario, which might be a WLAN access scenario. A somewhat dishonest visited network, X, claims that that home network Y's subscriber, S, is roaming in X. Y will happily (?) provide authentication vectors but will really not have any chance to determine if S is really in X's network. Later S might claim he never was. It is impossible to (robustly) decide if S was in X's network or if X is lying in an attempt to get compensation with current AKA mechanisms. However, it would be very easy to solve this cryptographically by introducing non-repudiation mechanisms. Note that non-repudiation can in this case be achieved with lightweight symmetric (SIM based) techniques without the need for PKI.

This serves merely as an example to stimulate discussion on what the future threats might be. Nevertheless, we feel the scenario is not completely unrealistic.

4 Conclusions and Proposal

We propose that a study item is established to investigate foreseeable threats in GERAN security. The study should include, not only solving "obvious" side effects of the A5/2 attack in GSM, but also possible GPRS issues and consideration of future attack scenarios that (perhaps) not even UMTS security will take care of. Only after that do we feel that decision on a long-term enhancement of GERAN security can be taken.

5 References

[1] Elad Barkan, Eli Biham and Nathan Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Proceedings of Crypto 2003, Springer LNCS 2729.

[2] Vodafone, "Cipher key separation for A/Gb security enhancements", S3-030463, S3#29, 15 – 18 July 2003, San Francisco, USA.

[3] Ericsson, "Enhanced Security for A/Gb", S3-030361, S3#29, 15 – 18 July 2003, San Francisco, USA.

[4] A. Maximov, T. Johansson and S. Babbage, "An improved correlation attack on A5/1", Proceeding of SAC 2004.

[5] Ericsson, "On the introduction and use of UMTS AKA in GSM", S3-040534, S3#34, 6 - 9 July 2004, Acapulco, Mexico.

[6] Vodafone, "Analysis of the authenticated GSM cipher command mechanism", S3-040262, S3#33, 10-14 May 2004, Beijing, China.

[7] Vodafone, "Evaluations of mechanisms to protect against Barkan-Biham-Keller attack", S3-040263, S3#33, 10-14 May 2004, Beijing, China.

[8] Ericsson, "Comparison of Suggested A5/2 Attack Countermeasures", S3-040341, S3#33, 10-14 May 2004, Beijing, China.

[9] Qualcomm Europe, "An observation about Special RAND in GSM", S3-040572, S3#34, 6 - 9 July 2004, Acapulco, Mexico.

[10] Ericsson, “Enhancements to GSM/UMTS AKA”, S3-030542, S3#30, 6 – 10 October 2003, Povoa de Varzim, Portugal.

[11] Lucent, “Eavesdropping without breaking the GSM encryption algorithm”, S3-040360, S3#33, 10-14 May 2004, Beijing, China.

[12] C. Brookson, “Authentication: A mechanism for preventing man-in-the-middle attacks”, S3-040036, S3#32, 9 - 13 Feb 2004, Edinburgh, Scotland, UK.

[13] Ericsson, “Generation of IOV-UI/IOV-I values during PS Handover”, GP-041987, GERAN#21, 23 – 27 Aug 2004, Montreal, Canada.

[14] Nokia, “Handling of ciphering during PS Handover”, GP-042046, GERAN#21, 23 – 27 Aug 2004, Montreal, Canada.