3GPP TSG SA WG3 Security — S3#14 **S3-000466**

1-4 August, 2000

Oslo, Norway

Source: **Vodafone**

Title: **Evolution of GSM circuit switched encryption**

Document for: **Decision**

Agenda Item: **7.11**

Summary

It is proposed that S3 concentrate its efforts on the development of a solution for adding a new encryption layer in GSM circuit switched systems which extends to the Release 2000 BSC rather than focusing on the development of an A5/3 algorithm. It is believed that deployment of new encryption functions in the BSC for GSM circuit switched systems is more cost effective and easier to deploy, particularly for existing GSM installations. This solution also provides opportunities for adding integrity protection for GSM circuit switched systems.

Background

Work has started in S3 to specify the requirements for new GSM encryption algorithms. The primary motivation has been to develop a new A5 algorithm for GSM circuit switched encryption, known as A5/3. However, the work has also investigated the possibility of acquiring a new GEA algorithm for GPRS encryption and the development of any new algorithms that may be required in the R00 GERAN security architecture. One possibility that has been proposed is to use a common “building block” for all these different algorithms.

In parallel with this work, the GERAN concept has been elaborated upon, in particular for user plane PS services. What is now clear is that the R00 BSC must support an Iu-ps interface as well as the existing Gb interface. A consequence of this is that the encryption terminating point moves from the SGSN into the GSM BSS when the Iu-ps interface is used to connect to the core network. In a reply LS to the GERAN group, S3 have stated that the GERAN should offer the same level of security as UTRAN and that the security architectures should be aligned to allow the core network and the mobile equipment to deal with both as uniformly as possible. In particular, regarding the level of security that is provided, it is envisaged that for PS services encryption terminates in the BSC rather than the BTS and that integrity protection of signaling traffic is applied alongside encryption. Note that the GERAN CS architecture is at a much less developed stage than the PS architecture.

A5/3 deployment issues

Although it is possible to design A5/3 for new BTS equipment and mobile equipment, it is likely to be prohibitively expensive to upgrade existing BTS equipment to support the new algorithm. A cost effective solution must be found to allow existing networks to be upgraded to support A5/3 otherwise the benefits of introducing the new algorithm will be severely reduced.

Even if A5/3 can be deployed cost effectively in BTS equipment, it will be some time before virtually all mobile equipment supports the new algorithm thereby removing the requirement for networks to support A5/1 or A5/2 alongside A5/3 in new BTS hardware. Until this point has been reached there is also the risk that an active attacker may mount an active “roll-back” attack by modifying the mobile station classmark to force the network to instruct the target mobile to use A5/1 or A5/2 even when A5/3 is available (i.e. “rolling back” to a potentially weaker algorithm). Although this risk exists, the deployment of A5/3 still offers significant benefits, since the rollback attack is quite sophisticated and may be of limited practical use to the attacker.[1]

Proposal

It is proposed that a new security architecture for GSM circuit switched services is standardised as part of the Release 2000 GERAN standards development. The security architecture should include a new encryption mechanism which terminates in the BSC rather than the BTS. The architecture should also include a new integrity mechanism which allows the GERAN security mode to be securely established. Integrity protection is introduced primarily to prevent the suppression of the instruction from the network to turn on GERAN encryption and to guard against “roll back” attacks if multiple GERAN encryption algorithms are deployed in the future. Integrity protection across the GSM radio access network enables dual mode GSM-UMTS terminals to benefit from UMTS integrity protection.

It is further proposed that efforts are concentrated on the development of new encryption and integrity algorithms for GERAN. The requirements for a new BTS-based A5 algorithm or a new SGSN-based GEA algorithm are for further study.

[1] Note that a roll-back attack to force the use of A5/2 when A5/1 is available is not applicable since all mobile equipment must support A5/1 as a mandatory requirement so the network will not accept a mobile that claims only to support A5/2. A further consequence of this is that ”A5/1 networks“ do not need to support A5/2 in their BTS equipment whereas “upgraded A5/3 networks” would have to support both A5/1 and A5/3 during the transition period.