SMG 10 meeting / 3GPP TSG SA WG3 Security — S3#13 **S3-000333**

23-26 May, 2000

Yokohama, Japan

Source : France Télécom

1 On the need for designing a new standard A5 algorithm for GSM

Encryption of the radio path plays a key role in the GSM security architecture. Not only because encryption provides confidentiality of the over the air transfer of signalling and user data, but also because encryption is an essential ingredient of fraud protection. In fact, systematic encryption of all communications is currently the main GSM mechanism to prevent :

- call selling by false base stations (capable to recover identification and authentication data from mobiles stations and to use these data to establish illicit calls) ;
- hijacking attacks (consisting of seizing the traffic channel of a mobile just after authentication has occurred in order to establish a call on his behalf).

The practical security offered by the A5/1 algorithm has been sufficient to offer these confidentiality and fraud protection services over the past years. However, this situation can be expected to gradually evolve in the next years until the A5/1 protection will eventually become inadequate[1].

As a consequence, we strongly support the SMG10 and GSMA proposals to develop a stronger A5 encryption algorithm A5/3. The new GSM encryption algorithm might be initially introduced as a mobile station and operator's option (and as a fallback algorithm in the event of any sudden deterioration of the practical protection offered by A5/1), and become a mandatory feature at a later stage.

2 Key sizes

- A 64-bit key size will of course represent an interesting initial value for operators (because with this length option – and taking into account the fact that algorithm

[1] As a matter of fact :

- Independently of whether A5/1 is used with a 54-bit key of a 64-bit key, the resistance of A5/1 against realistic attacks seems to stay somewhere between the resistance of full 56-bit DES and the resistance of 40-bit algorithms, e.g. 40-bit variants of DES. Whatever the exact position of A5/1 in this scale, it is obvious by year 2010, the strength of A5/1 will no longer be extremely dissuasive
- Improvements of the cryptanalysis of A5/1 are not precluded. The practical feasibility of using Shamir, Biryukov and Wagner's recent attacks (cf their FSE'2000 paper) to eavesdrop a GSM call is questionable because it requires the availability to the attacker of all the plaintext bits corresponding to 2 seconds of communication, i.e. approximately 400 entire 114 bit plaintext frames and the corresponding ciphertext frames. However their paper will stimulate research on how to mount optimised A5/1 attacks which really take the operational conditions of use of A5/1 into account. Even if this research does not result in the near future in low cost real time breaking machines, it is likely to at least result in experiments demonstrating that GSM eavesdropping is not totally infeasible.

negotiation mechanism is already present in GSM Rec. 04.08- the introduction of A5/3 will not require any modification of the GSM equipment outside from the BTS and MEs).

- However, if one wants the new A5/3 algorithm to be adequate for protecting mobile communications for the lifetime of the GSM system, one clearly cannot limit the key size to 64 bits (cf for instance Lenstra and Veheul's paper "selecting cryptographic key sizes" http://www.cryptosavvy.com). Moreover, there is no clear indication that such a restriction would much facilitate the exportability of the future A5/3 equipment, and the UMTS precedent indicates that most countries do no longer enforce limitations on the key sizes of encryption algorithms used to protect the radio path in public mobile systems. A 96 (or less, e.g. 80 bits) key size appears to offer some practical advantages for those operators using a block cipher with a 128-bit block size as their A3/A8 algorithm, because one single run of the block cipher will allow to output both a 32 bits SRES authentication response and a Kc key. But there is no obvious advantage in limiting the range of possible key sizes to 96 instead of 128 inside the algorithm external specification.

So in summary we believe that the key sizes range proposed in the current draft requirements specification (64-128 bits) is adequate.

3 Proposed actions

We believe that the A5/3 specification work and work on the protocol modifications required to enable future GSM systems to use A5/3 with key sizes of more than 64 bits should be undertaken as soon as possible (in parallel). Therefore we recommend the following actions to be taken by SMG10 during the Yokohama meeting.

- Submit the A5/3 requirements specification to the SMG plenary of June for approval.
- Request a new work item on the adaptation of the MAP and SIM-ME interface in the case of keys of more than 64 bits and mobile-network key length negotiation issues and A5/3 introduction scenarios.

As far as the algorithm design and specification work is concerned, the availability of the 3G algorithm KASUMI as the basic building block for A5/3 would of course be good news - since the work left for the task force would then only consist in specifying suitable modes of operations of KASUMI for A5/3. But in order to save time and not to make the entire A5/3 process dependent upon the outcome of the KASUMI IPR discussions, the set-up by ETSI and GSMA of an ETSI SAGE task force on the design and specification of the A5/3 algorithm should not be delayed until the IPR issues will have been settled – and alternatives (e.g. starting from another algorithm, or even entirely designing a new pseudo random generator) should not be precluded yet.