3GPP TSG SA WG3 Security — SA3#33 **S3-040376**
10-14 May 2004
Beijing, China

Source: **GSM Association Security Group, SG Chairman**

Title: **A5/2 withdrawal from handsets**

Document for: **Discussion and decision**

AGENDA ITEM: GSMA SG REPORT

Contact details:
Charles Brookson, SG Chairman

This input document proposes the withdrawal of A5/2 from handsets to reduce the threat of easily deriving the key Kc, and using this knowledge to exploit GSM.

SG Doc 51/10

Position Statement to Phase out A5/2

Meeting Name & Number:	SG #51	
Meeting Date:	21st to 22nd June 2004	
Meeting Location:	Amsterdam, Netherlands	
Document Source:	SG Chairman	
Document Creation Date:	5th May 2004	
Document Status:	**For Approval**	X
(please mark with an x)	**For Information**	
Associated Knowledge Base(s):		
(enter if applicable)		
Circulation Restricted:	UNRESTRICTED	
(please complete)		

All GSM Association meetings are conducted in full compliance with the GSM Association's anti-trust compliance policy

High Level Document Summary:

This document contains a proposed position statement relating to the phasing out of A5/2. Specifically, 3GPP TSG SA3 is requested to approve the proposed deadline of end 2005 for the phasing out of A5/2.

INTRODUCTION

In August 2003 an academic paper attacking GSM encryption was published which detailed how GSM communication encrypted using the weakest A5/2 algorithm can be efficiently attacked. Since the original GSM A5 algorithm was developed in 1987 it is inevitable that attacks such as this are now possible.

The paper describes how, by using a man in the middle technique, this attack may be used to gain knowledge of the encryption key used for one of the stronger A5 privacy algorithms. Although the attack is currently technically complex and expensive to undertake it is feasible and equipment could emerge to exploit the weakness identified.

The majority of GSM operators around the world, for export control reasons, currently use A5/2 and are exposed to the published attack. To do nothing would expose GSM network operators, and their subscribers, to the following difficulties;

- Fraud exposure is greatly increased
- Billing integrity is compromised
- Calls on GSM networks can be eavesdropped
- Degradation of network quality experienced by users

The consequences of this latest attack are most serious for the industry with the result that a joint ad hoc group between GSMA SG and 3GPP SA3 (GSM Security Working Group) was convened to examine the implications of the attack and to identify possible countermeasures.

PROPOSED WITHDRAWAL OF A5/2

The GSM Security Working Group (GSWG) in the course of its discussions has considered a number of possible countermeasures to mitigate the threat posed by the published attack. Some of the options considered included adjustment of network timers, additional authentication, use of spare bits of RAND to select algorithms, etc. However, GSWG has agreed that the removal of A5/2 from handsets and networks is a solution that must be pursued. It is likely that technical solutions, which will require modifications of handsets and infrastructure, will take considerably longer than simple withdrawal of A5/2.

The phase out of A5/2 will impact the industry and the successful withdrawal is dependent on three factors;

- Availability of an alternative algorithm to A5/2 in the event that it is to be dropped
- Willingness of GSM network operators to upgrade their BSS software to support an alternative algorithm within agreed timescales
- Availability of handsets that do not support A5/2 within agreed timescales

Discussions to permit the export of A5/1 to current A5/2 users have concluded and GSMA is now in a position to make the algorithm more widely available.

In order to phase out A5/2, operators are required to remove the algorithm from their BSS and replace it with A5/1. This is assumed to be a minor software upgrade which could be incorporated into routine upgrades already scheduled by operators.

It is also necessary to ensure A5/2 is removed from handsets and, as this is a software modification, it should be possible to phase out A5/2 from GSM terminals by end 2005.

CRITICALITY FOR ACTION

The implications of the published attack are significant for network operators and GSMA and 3GPP TSG SA3 should take leadership on this issue by agreeing and co-ordinating industry

action, communicating the identified measures to all stakeholders, and monitoring compliance with agreed collective action.

The effect of phasing out A5/2 will be to dramatically reduce the risk of fraud to network operators and the risk of eavesdropping to their subscribers. The proposed action will help counter the threats posed by the published attack against A5/2. It will also allow operators worldwide to deploy A5/1, for which no published attacks exit. This will increase the perceived security of the GSM standard.

IMPACT ANALYSIS

It is assumed that handset manufacturers will not have any difficulties withdrawing A5/2 and that BSS suppliers will have no objections as they already supply equipment containing A5/1 so the proposed changes should not pose difficulties for GSM equipment suppliers. It is hoped that the changes can be delivered in a timely manner to ensure that A5/2 can be phased out in all BSS and handset equipment by end 2005.

BSS and handset suppliers have already been invited to provide feedback to help assess the impact of phasing out A5/2 and the supplier feedback is critical to progressing this work.

TIMESCALES

It is critical that A5/2 is phased out as one of a package of measures to combat the threat posed by the publication of the A5/2 attack. For the withdrawal to be effective it needs to start immediately and be completed by end 2005, as there is a considerable risk that equipment may emerge to exploit the published weakness.

Deliverable	**Estimated Time-line**
Obtain export permission for A5/1 to replace A5/2	Completed
Table proposals and time lines to withdraw A5/2 at 3GPP SA3	Mid May
Obtain GSMA EMC approval for withdrawal of A5/2	End May
Communicate phase out of A5/2 to handset manufacturers and operators	Mid June

DESICSIONS

3GPP TSG SA3 is requested to approve the proposed deadline of end 2005 for the phasing out of A5/2. Comments are invited on the impact of these proposals to the SG Chairman.