IREG Doc 48_016

Liason Statement: Request for Comments on Proposed Security Enhancements to GSM/GPRS Networks.

Meeting Name & Number:	IREG Plenary 48
Meeting Date:	2nd-3rd March 2005
Meeting Location:	Barcelona
Document Source:	IREG
Document Creation Date:	8th November 2004

Document Status:	**For Approval**	X
	For Information	
	For Discussion	

Associated Knowledge Base(s):	

Circulation Restricted *:	**GSM Association:**	
	Members	X
	Associate Members	X

Document History:	

N.B. All GSM Association meetings are conducted in full compliance with the GSM Associationís anti-trust compliance policy

High Level Document Summary:

This document provides as response from IREG to SA3 as requested in IREG47_067.

Liason Statement on Request for Comments on Proposed Security Enhancements to GSM/GPRS Networks. ì

To:- SA3

From:- IREG

Date:- 4th Novemer 2004

Contact person at IREG:-
Name: John Boggis, Vodafone UK
Email: john.boggis@vodafone.com
Telephone +44-1635-673712

Overview

The following text formed Document IREG 047_067 ìRequest for Comments on Proposed Security Enhancements to GSM/GPRS Networks. ì

In it IREG was asked to comment that if SA3 decided that that the authenticated cipher instruction mechanism should be mandated in networks globally, whether this would be feasible to achieve.

The response is contained at the foot of the document.

Introduction

In August 2003 an academic paper on GSM security was presented at a cryptography conference. The paper details how GSM communications encrypted using the weakest A5/2 algorithm can be efficiently attacked[1]. The paper also 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 algorithms. Although the attack is currently technically complex and expensive to undertake, it is feasible and equipment could emerge to exploit the weakness identified. A statement contained in SG Doc 105/03 on the implications of the attacks was issued to operators via Wireless Insider on 21st August 2003.

If attacks which make use of this technique emerge then GSM network operators, and their subscribers, are exposed to the following problems:

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

These difficulties are not only a concern for network operators that use A5/2, since the man-in-the-middle technique can target a network that uses a stronger A5 algorithm such as A5/1 or A5/3. All the man-in-the-middle requires is that the target terminal supports A5/2.

[1] E. Barkan, E. Biham, N. Keller: ìInstant Ciphertext-Only Cryptanalysis of GSM Encrypted Communicationî, In D. Boneh (Ed.): Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings. Lecture Notes In Computer Science Volume 2729, Springer 2003, pp600-616.

A joint ad hoc group between GSMA SG and 3GPP SA3 was convened to examine the implications of the attack and to identify possible countermeasures. The group concluded that the most effective short-term solution was to remove A5/2 from new terminals. In liaison statement SG Doc 51/10 to 3GPP SA3, GSMA SG reported that discussions to permit the export of A5/1 to current A5/2 networks have concluded, and that GSMA is now in a position to make A5/1 more widely available. Based on this statement, 3GPP have recently agreed to remove the requirement to support A5/2 in terminals from the 3GPP Release 6 specifications onwards.

Although A5/2 removal is a very effective short-term countermeasure, other complementary solutions are also being considered which will take longer to deploy. Some of these solutions provide more comprehensive protection against the new attacks as well as taking the opportunity to upgrade other aspects of GSM security at the same time. One such approach involves providing a mechanism to allow terminals to authenticate the commands from GSM networks that are used to instruct the terminal to enable the use of a particular encryption algorithm. Such a mechanism prevents the published man-in-the-middle attack because it prevents the attacker from spoofing an instruction to enable a weak encryption algorithm.

For circuit-switched services, the mechanism would require new cryptographic operations to be performed in the BSS to add a Message Authentication Code (MAC) to the GSM Cipher Mode Command. The MSC may also need a small upgrade. For PS services, the SGSN would also need to support similar cryptographic operations to add a MAC to certain GPRS signalling messages. In the terminal, new cryptographic operators would need to be implemented to verify the MAC on cipher instructions received from the network. Further details on the mechanism are contained in 3GPP SA3 Tdoc S3-040262[2].

For this mechanism to work effectively, upgraded terminals must reject cipher commands that are not authenticated. This means that all networks globally must be upgraded before the first upgraded terminals can be issued, otherwise roaming problems may occur. Note that terminals that do not support the mechanism will still be able to work with upgraded networks. This is because the old terminal will be able to ignore the new security fields that are added to the relevant signalling messages.

Actions

If 3GPP SA3 decide that that the authenticated cipher instruction mechanism should be mandated in networks globally, IREG are asked to comment on whether this would be feasible to achieve. Furthermore, if it were feasible to introduce such a mechanism, then IREG are asked to comment on the timescales for deployment.

Any comments should be sent to SA3 in a liaison statement..

IREG Response

IREG 047_067 ìRequest for Comments on Proposed Security Enhancements to GSM/GPRS Networks. ì was presented at IREG47 and there was some discussion generally to aid clarification. However because it was a very late submission to the document list, the meeting delegates felt that they needed more time assess the question. Accordingly the document was circulated on the mailing list for comment.

A range of comments were received:-
Most network operators recognised the need to enhance security.
Some actively supported the proposal.
Some were concerned about being ìheld to ransomî by network infrastructure vendors for a software upgrade which would be declared as manadatory by GSMA.
One network operator was concerned about the costs at a time when their licence is due to expire and

[2] 3GPP Tdoc S3-040262, ìAnalysis of the authenticated GSM cipher command mechanismî Vodafone. http://www/3gpp.org

would not support the proposal.
One network operator felt that there should be a better way to achieve the security enhancement.

On the issue of the timescale to deploy, a range of comments were made, which averaged at around 3 years .