**3GPP TSG SA WG3 Security — S3#32** **S3-040036**
**09 - 13 February 2004**
**Edinburgh, Scotland, UK**

| | |
|---|---|
| **Title:** | **Authentication: A mechanism for preventing man-in-the-middle attacks** |
| **Work Items:** | |
| **Source:** | Charles Brookson DTI |
| **To:** | |
| **Cc:** | |

**Contact Person:**
**Name:** Charles Brookson
**Tel. Number:** +44 020 7215 3691
**E-mail Address:** cbrookson@iee.org

**Attachments:** **None**

## Introduction

Biham et al described a Man-In-The Middle attack against GSM, which forced a handset to use the weaker A5/2 algorithm, so that it could buffer traffic up, break out the Kc from the A5/2 traffic, then reencrypt using A5/1 for onward transmission to the network. From then on the MITM acts as a translator between A5/1 on the leg of the call to and from the basestation and A5/2 on the leg to and from the handset. The MITM is thus able to easily recover the session Kc (which he can use for fraud) and he can also listen to all the user's calls. The attack is generic in that it could be used to force any handset to use weaker algorithm than the one the basestation believed it to be using.

Other schemes have been proposed to protect against this attack, in particular the ' Special RAND' variation. In this paper, we describe a scheme which effectively blocks the attack, and which requires minimal changes to the GSM protocols. It also removes the need for the home network to know which version of A5 is in use in the visited network (which is sometimes difficult, and of course sometimes for engineering reasons the sue of encryption may be disabled in visted networks).

## Solution Outline

Biham's MITM begins his attack by interfering with the "cipher start" message. The cipher start message is transmitted by the basestation to the handset once authentication has been achieved. It tells the handset to begin ciphering using the Kc value it has just derived (as a byproduct of the A3/A8 authentication protocol) and it also tells the handset which A5 algorithm to use. The basestation decides on the A5 algorithm based on both network capability and handset capability (the latter of which it receives in the classmark message). Biham's MITM is successful in modifying this message because the message is not authenticated. The simple solution proposed here is to make sure this message cannot be interfered with by cryptographically authenticating it.

**Solution Detail**

The cipher start message contains details of the A5 algorithm to be used. We denote the choice of A5 by the flag, algflag. We propose filling the unused bits after the cipherstart message with the following value: hash(Kc, SRES, algflag). The basestation knows Kc because it the A5 algorithm needs it, and it knows SRES because the handset transmitted it in response to the authentication request. The handset knows each too as a result of the authentication process.  The hash function here can be any strong hash function, truncated so that the output fits into the spare bits following the cipher start message.

The handset, on receipt of the cipherstart message has all the ingredients necessary to recalculate the output of the hash function, and, once calculated, checks this against the value sent. If it doesn't match, it knows the message has been tampered with. A MITM cannot defeat this scheme without knowing the Kc value.
Changes Required to Implement the Scheme

Basestations (in both home and visited networks) will need to be upgraded so that the cryptographic hash is appended to the cipher start message. This is achievable through a simple software upgrade.

Handsets will need to be modified so that they know to check the cryptographic hash, and take appropriate action, should the check fail.

No change is necessary to any SIM functionality; neither are any changes required at the MSC or anywhere else further back into the network.

**Issues With Proposed Scheme**

All basestations have to have their software upgrade rolled out within a reasonable timeframe, otherwise the MITM could delete the appended cryptographic hash from the cipherstart,  and pretend to the handset that it was speaking to an old basestation which hadn't been fixed to prevent this MITM attack. Provided software upgrades are timely, this shouldn't be an issue.

Any handset that hasn't been upgraded, is still susceptible to the attack. This, however, is a problem with all the schemes proposed.