3GPP TSG SA WG3 Security — S3#11 **S3-000109**
22-24 February, 2000
Mainz, Germany

System behaviour on receipt of an invalid Message Authentication Code (MAC)

Duncan Mills, Vodafone AirTouch
3GPP TSG CN WG1

4th February 2000

Introduction

In TS24.008, in sections 4.3.2.5.1 and 4.7.7.5.1 the MS procedure following the receipt of an invalid MAC is described as being 'for further study' (ffs). This document provides that study, discussing the best way to progress this issue.

Background

For a UMTS authentication challenge, the network sends either an AUTHENTICATION REQUEST message (for Circuit Switched (CS) services) or an AUTHENTICATION & CIPHERING REQUEST message (for Packet Switched (PS) services) to the MS.

Both of these messages contain an authentication challenge (RAND) and an authentication token (AUTN). The first thing the MS does is derive some information from the AUTN. This information includes the Message Authentication Code (MAC) and the sequence number (SQN).

The MS checks the validity of the MAC before it does anything else. This enables the MS to ascertain whether or not the authentication challenge has come from a genuine source.

To do this, the MS uses the RAND and the AUTN and an internal algorithm to generate an expected MAC (XMAC). If the MAC received in the AUTN does not match the generated XMAC, then the MS shall send an AUTHENTICATION FAILURE message (CS services) or an AUTHENTICATION & CIPHERING FAILURE message (PS services) to the network, with the cause code 'MAC failure.'

This document proposes how this procedure should continue.

TMSI mapping problem in a genuine network

The first scenario to be considered upon receipt of an invalid MAC is that some kind of error has occurred and the network from which the authentication challenge originated is a genuine one.

The most likely cause of this is that the look-up tables used to resolve the TMSI from the IMSI contained a mistake.

In this situation, it makes sense for the network to be given a second chance. Therefore, upon receipt of an AUTHENTICATION FAILURE message or an AUTHENTICATION & CIPHERING FAILURE message

with the reject cause ‘MAC failure,’ the network should send an IDENTITY REQUEST message to the MS to request the (encrypted) IMSI.

The MS should then respond with an IDENTITY RESPONSE message, containing the (encrypted) IMSI. This would enable a genuine network to detect that the wrong TMSI was originally used and re-order authentication quintuplets from the HLR/AuC. The network would then send a new AUTHENTICATION REQUEST message or AUTHENTICATION & CIPHERING REQUEST message.

If the new challenge also contains an invalid MAC, then it is reasonable to assume that the network is not genuine.

MS behaviour towards a ‘false’ network

If the source of the authentication challenge does not respond to the failure message sent by the MS, or if the MS still cannot resolve the MAC after the identification procedure has been performed, then the source network can be deemed as being ‘false.’

In such a scenario, the behaviour of the MS needs to satisfy the following conditions:

- The MS should not signal in any way to the ‘false’ network. (This prevents fraudulent activity).
- After leaving the ‘false’ cell, the MS should not return to it. (Otherwise an MS could become ‘stuck’ on the false cell).
- As a result of leaving the ‘false’ cell, the MS (or potentially several MSs) should not immediately perform a Location Area/Routing Area update procedure in a genuine cell. (An MSC or SGSN could become overloaded as a result).
- As a result of leaving the ‘false’ cell, the MS (or potentially several MSs) should not immediately perform a PLMN search procedure. (A genuine network could become overloaded as a result).
- No LA/RA, PLMN or CELL should be stored permanently as forbidden in the MS. (The likelihood is that the false cell is using the LAI or network number of a genuine network element).

It is difficult to satisfy these conditions. For example, if the MS was to treat the false cell as from a forbidden LA, then overload could occur when several mobiles try to perform a LA/RA update. Also, if the false cell copied the LAI from a genuine location area, then the MS will have ‘barred’ itself from this too.

The same can be said of storing the network on the forbidden PLMN list. An attacker could, for example, set up a duplicate cell at an airport terminal, and prevent all roamers entering a country from ever accessing a genuine network.

Proposed solution

The problem is not a straight forward one, and satisfying the conditions mentioned above is not easy. We propose the following solution:

The first issue is the detection of a false network. The network should be treated as false, when either:

- The first authentication challenge contains an invalid MAC and after an amount of time (at the expiry of a timer, started after sending the failure message to the network), no IDENTITY REQUEST message is received, or
- The authentication challenge received immediately after an IMSI identification procedure has been performed contains an invalid MAC, or

- An amount of time after sending an IDENTITY RESPONSE message, the MS has received no new authentication challenge. (Another timer should be used to realise this).

Next, the consideration must be as to how the MS reacts to the false network. We propose that the MS treats the cell as barred and does not try to access it again. In addition, when/if the MS reads the false BTS's System Information (SI) 3 or 4, its cell bar status must not be changed (unless the time synch of the cell has changed). It must not go back and periodically check for barring on that cell. (If it did, it would discover that the false cell is not really barred!)

The understanding of the author is that (in GSM) the MS reads System Information (SI) 3 or 4 of the strongest 6 cells. If SI 3 or SI 4 indicates that the cell is barred, then the MS will update its records to reflect this. Periodically the MS will return to the cell and check the barring status again.

As previously discussed, the cell identity information element (CELL ID IE) may be copied from a genuine cell. So when treating a false cell as barred, the MS shall identify the cell by the Base Station Identity Code (BSIC), the Absolute Radio Frequency Carrier Number (ARFCN) and the cell's timing (SCH info) rather than by the CELL IDENTITY IE.

Within the MS a primitive must be sent to the correct entity- after a false network is detected- to mark the cell (as identified by the BSIC, ARFCN and timing) as barred. Such a primitive would be unique, and could also indicate that no future checking of this cell is required. As soon as the MS moves away from the false cell, it will be removed from the MS list of the 6 best cells.

Note 1: The aim of this process is to reuse the existing GSM lower layer functionality.

Note 2: An assumption is made that (for UMTS) the RAN specifications include a similar method for cell barring.

Summary of the proposal

1. Upon sending the AUTHENTICATION FAILURE or the AUTHENTICATION & CIPHERING FAILURE message the MS starts a timer.

2. Upon expiry of the timer the MS deems the network to be false.

3. Upon receipt of a failure message with reject cause 'MAC failure' the network may send an IDENTITY REQUEST message. Upon receipt of the IDENTITY REQUEST message, the MS shall stop the timer and send its (encrypted) IMSI to the network in the IDENTITY RESPONSE message. A second timer shall be started.

4. Having sent the IDENTITY RESPONSE message, the MS may then receive a new authentication challenge. If it does then it shall stop the second timer. If the new challenge contains an invalid MAC then the MS shall deem the network as being false. If no new authentication challenge is received, the second timer will expire and the MS shall deem the network as being false.

5. Once the MS has deemed the network to be false, an internal mechanism shall treat the cell (as identified by the BSIC, ARFCN and timing) as barred and shall prevent the MS from camping on that cell.

Anticipated areas of Impact to the Specifications

The main description of the new procedures should be in TS24.008, for Release 99. This document assumes that RAN specifications include a similar method for cell barring as SMG2 specifications. Both SMG2 and RAN experts will need to be contacted, although impact on their specifications should be minimal.