Mobile (in)Security - Bug #1480

A5/3 is not deployed in GSM networks

02/19/2016 10:51 PM - laforge

Status:	New	**Start date:**	
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:	MS (Mobile Station)		
Target version:			
Resolution:		**Spec Reference:**	

Description

The 3GPP has specified the Kasumi-derived A5/3 cipher for use in GSM networks. This would significantly increase the confidentiality and security of the GSM network, since it avoids the known-weak and known-broken A5/1 cipher. The passive A5/1 key-cracking attacks would no longer work.

In order to use A5/3, both the MS and the BTS will have to implement the A5/3 cipher, and the BSC will have to configure the BTSs to actually use it.

Many modern phones (whether 3G or not) support A5/3 operation on GSM and indicate this capability in their CLASSMARK.

However, none of the networks we have seen are using A5/3 on GSM.

Thus, the operators and/or equipment manufacturers are actively preventing a higher level of security and confidentiality.

History

#1 - 02/21/2016 04:34 PM - laforge

- Assignee deleted (laforge)