Mobile (in)Security - Bug #1481

Random LAPDm MAC-block padding is not deployed yet

02/19/2016 10:51 PM - laforge

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

Description

Recent versions of TS 44.006 (Version >= 6.7.0 from October 2008) specify that the BTS shall use randomized padding (fill bits) in its Layer2 frames.

This will help to combat the known passive A5/1 cracking attacks that rely on a small portion of known plaintext.

By using randomized padding, the amount of known plaintext can be reduced.

However, as of 07/2010, no network has been found to use this randomized padding.

History

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

- Assignee deleted (laforge)