**3GPP TSG-SA3 Meeting #102-e *S3-210036***

**meeting, 18 -22 January 2021**

**Source: MITRE**

**Title: New Key Issue: MBS Location Privacy**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***This pCR proposes a new key issue: MBS Location Privacy.***

# 2 Rationale

With Multicast-Broadcast Services (MBS) protocol it is important to consider any weaknesses that may jeopardize the privacy of the UE(s) participating in the MBS session. The location of active MBS sessions, in some applications, could give adversaries information that would affect the MBS recipient’s privacy. Such applications can include public safety and military where UE privacy is important.

The issue is there may still be opportunities for adversaries to determine the locations where there are active MBS sessions. If a common Identifier (e.g., TMGI) across multiple cells is used to identify an MBS session, then attackers could use this to determine which cells have the active MBS session. The attacker can correlate the identifier to an organization by inferring the properties of the MBS, such as if the MBS identifier is broadcasted in areas from where the MBS service is known to be operational. When the attacker discovers active MBS sessions, they can use this information to further exploit the privacy of victim UE(s).

This proposal aims to add a Key Issue (KI) that will address any concerns with discovering the active MBS session location (e.g., 5G cell).

# 3 Detailed proposal

SA3 is kindly requested to agree to the below pCR to TR 33.850.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* First Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 5.X Key issue #X: MBS Location Privacy

### 5.X.1 Key issue details

MBS session management procedures are studied in TR 23.757 [2].

With Multicast-Broadcast Services (MBS) protocol it is important to consider any weaknesses that may jeopardize the privacy of the UE(s) participating in the MBS session. The location of active MBS sessions, in some applications, could give adversaries information that would affect the MBS recipient’s privacy. Such applications can include public safety and military where UE privacy is important.

The issue is there may still be opportunities for adversaries to determine the locations where there are active MBS sessions. If a common Identifier (e.g., TMGI) across multiple cells is used to identify an MBS session, then attackers could use this to determine which cells have the active MBS session. The attacker can correlate the identifier to an organization by inferring the properties of the MBS. For example, if the MBS identifier is broadcasted in areas from where the MBS service is known to be operational. When the attacker discovers active MBS sessions, they can use this information to further exploit the privacy of victim UE(s).

### 5.X.2 Threats

If an attacker can determine whether there are other UEs present in the MBS session, they can assume the UE(s) are present within the service area of that cell. The attacker can use this information to further exploit the privacy of victim UE(s). Consider the following attack scenarios:

* ***Public Safety:*** In large public events such as parades, sports events, etc. law enforcement agents are strategically deployed to assist people and respond to emergencies. The agents often communicate via an MBS session to synchronize their tasks. Within a dense city environment where small cells are needed for coverage, criminals can use law enforcement MBS sessions to determine if law enforcement agents are within a coverage area before committing a crime.
* ***Mission Critical:***The attacker can infer the properties (e.g., size, shape, location etc.) of a mission critical deployment via the described vulnerability. This attack is particularly relevant if the MBS session is established via non-terrestrial network (NTN), e.g., satellite network or UAVs.

### 5.X.3 Potential security requirements

The solution must prevent attacks that would suggest the MBS Session is active within a certain area, to protect the privacy of MBS recipients.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of pCR\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*