Methodology for MAC-CE

vivo

Methodology

1. **Risk analysis in Annex**:
   A. Simplified risk-based methodology based on ISO 27005 and STRIDE with the below table
   B. Analysis the list of MAC CEs (On demand, contribution driven) in 5G as defined in TS 38.321 chapter 6.1.3 as mentioned in S3-254013

Risk ID	MAC CE-R1
Asset	(UL or DL) MAC CE IE1
Threat	STRIDE (i.e. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
Vulnerabilities	Lack of AAA (Authentication, Authorization, Audit) or CIA (Confidentiality, Integrity, Availability)
Assessment	Low, medium, High

2. **Once assessment of a Risk in Annex is identified as high, the related key Issue can be prioritized under security area:**
   - Key issue threat description can simply refer to the risk ID.
3. **Once we have key issue, we can have coordination with RAN2 on:**
   - Notify agreed risk analysis and key issue to answer Q1 and Q2 in LS S3-254013
   - Collect answer for questions to RAN2 for key issue assumptions

Pros-Cons

Pros:

1. The methodology follows security best practice, e.g. ISO 27005, and STRIDE methodology.
2. The methodology is simple and formative.
3. Duplicated work can be avoid (i.e. key issue threat refer to risk ID).
4. Focusing on “high” risk, SA3 work can be focused.
5. Clear coordination with RAN2

Cons:

1. Agreement on identified risk and key issue may take time.

Q to RAN2

- Whether the identified MAC CE IEs will be supported in 6GR day1.
- Any size limitation on additional security parameters (e.g. additional MAC-I and fresh parameter (e.g. COUNT))