Risk analysis methodology for MAC CE

Huawei, HiSilicon

Methodology

- It is proposed to go through all MAC CEs as they may have different usages, conditions, etc.
- For each MAC CE, it is proposed to analyze the following factors comprehensively to generate a matrix. The output is the risk severity respectively. This can be called factor analysis methodology.
- The factors description are shown in the table1.
- The risk severity shown in table2 for each MAC CE is based on the combined analysis of each factor.

Factors	Description	
Attack Type	e.g., Active or Passive attack in general e.g., eavesdropping, tampering, replay stating accurate means	
Attack Duration	How long the attack can last. e.g., seconds, minutes, hours, days, months	
Attack Scope	The exact impact scope or granularity of the attack. e.g., Per UE, Per cell, Per PLMN	
Attack Frequency	Explain how often the attack could happen	
Attack complexity	Reconnaissance phase	Explain how does the attacker prepare for the attack
	Attack phase	Explain how the attack is performed in detail
	Precondition summary	Summary of the preconditions
Attack Consequence	Consequence	Impact caused by the attack
	Reliability analysis	Analysis on what’s the reliability or possibility of the attack
	Other methods to achieve similar result	List other methods to achieve similar result if any

Table 1 - Risk analysis factors

Risk Severity of MAC-CEs
Very Low Risk
Low Risk
Medium Risk
High Risk
Critical Risk

Table 2 – Risk severity for MAC CEs

Pros/Cons

Pros

- Clearly illustrate all the aspects which should be used to determine whether there is a potential risk pertaining to a specific MAC CE.
- Using factor analysis approach, we can understand the MAC CE well.
- Questions to RAN2 could be generated during the analyzing course, e.g., what’s the usage and purpose of the MAC UE.

Cons

- Not identified.