MAC CE security risk analysis methodology

ZTE Corporation

Methodology proposal

- **Mapping MAC CEs to security risk & impact range**

  Examples of the mapping table:

	Security Risk				Impact Range
	Privacy Leakage	Link interruption/ service disruption	Service degradation	Resource waste	Impact to multiple users/more than one cell
DL MAC CE					
LTM cell switch command MAC CE		x	x	x	x
.....					
UL MAC CE					
.....					

- **Determine risk criticality level**

  High criticality: Successful attack could directly cause link interruption, service disruption, or impact multiple users/cells

  Medium criticality: Successful attack could cause service degradation or resource inefficiency

  Low Criticality: Successful attack would cause minor performance reduction or leakage of non-sensitive information

- **Identify MAC CEs with high risk criticality**

pros/cons

Pros:

- **Future proof & reusable**: can be applied to MAC CEs in future 6G releases
- **Clear output**: clearly distinguish high-risk/medium-risk/low-risk MAC CEs

Cons:

- Need RAN2 further check from overhead and latency prespective

Queries for RAN2

- Identify overhead-critical and/or time critical MAC CEs
- If integrity protection for MAC CE is need, what is the accpetable length of MAC-I considering overhead criticality?
- Whether the exact MAC CEs to be protected are up to configuration?