



3GPP TSG RAN Rel-19 workshop
Taipei, June 15 - 16, 2023

RWS-230463

Source: Apple
Agenda Item: 5

Views on Rel-19 AS Security Enhancements

Apple

Background | Current status of the AS security protection

- Current AS security framework
 - Only unicast transmission after the AS security activation is protected
 - Ciphering and integrity protection is applicable for each PDCU SDU

Message types	Note	
Paging	PCCH	Unprotected
System Information	BCCH	Unprotected
Initial access procedure	RACH procedure, CCCH message	Unprotected
RRC unicast message before AS security activation	DCCH	Unprotected
Unicast messages after AS security activation	DCCH, DTCH.	Protected
L1 message	PDCCH, PUCCH, PRACH, SRS, SSB/CSI-RS...	Unprotected
L2 message	L2 Control PDUs, L2 header...	Unprotected

- More and more security risk cases are raised in GSMA

GSMA LS	The risky case
R2-2106454 (Stealth Pirating Attack by RACH Rebroadcast Overwriting (SPARROW))	The risk during the RACH procedure
R2-2102607 (User location identification from Carrier Aggregation secondary cell activation messages (FSAG Doc 88_009; contact: GSMA))	The risk on SCell activation/deactivation MAC CE



Background | Study in SA3

- The further AS security enhancement has been studied in SA3 under the Rel-17 SI of 5G security enhancement against false base station (5GFBS).
 - Following key issues have been captured in TR 33.809

Key Issues	Note
#1. Security of unprotected unicast messages	Focus on the security protection on DCCH message before AS security activation, CCCH, L2 message
#2. Security protection of system information	Focus on the security protection on system information
#3. Network detection of false base stations	Focus on NW detection based on UE measurement report and the cell ID report.
#4. Protection against SON poisoning attempts	Conclusion: no further study
#5. Mitigation against the authentication relay attack	Focus on NAS procedure protection
#6. Resistance to radio jamming	Conclusion: no further study
#7. Protection against Man-in-the-Middle false gNB attacks	Focus on the security protection on system information



Proposals | RAN proposals on AS security enhancement

- Study and specify the solutions that provide integrity protection of L1 and/or L2 messages in Rel-19
 - L2 message includes control PDUs of MAC/RLC/PDCP and L2 PDU headers
 - L1 message includes DCI and transport block



