Attacks against 5G UEs over radio interfaces
Active Attacks (1)
Passive Attacks (2)
Radio Jamming (1.1)
Signal Shadowing (1.2)
Message attacks (1.3)
Uplink sniffing (2.1)
Downlink sniffing (2.2)
PCI (1.2.1)
MIB/SIB1-9 (1.2.2)
CP/UP (1.2.3)
MIB/SIB1 spoofing (1.3.1)
MIB/SIB1 replaying (1.3.2)
MIB/SIB modification (1.3.3)
SUPI stealing (2.1.1)
User tracking (2.2.1)
Other data (2.2.2)
DoS (Type1) (1.1.1)
Downgrade-3 (1.2.2.1)
DoS (Type2) (1.2.3.1)
Unicast message spoofing (1.3.1.1)
SIB2-9 spoofing (1.3.1.2)
MITM (1.3.2.1)
DoS (Type 1) (1.3.3.1)
Downgrade-3 (1.3.3.2)
REVOLTE (2.2.2.1)
DoS of all gNBs (1.1.1.1)
Identity Request (1.3.1.1.1)
Service Rejects (1.3.1.1.2)
Fake PWS (1.3.1.2.1)
Tampering (1.3.2.1.1)
Relaying (1.3.2.1.2)
DoS (Type3) (1.1.1.1.1)
Downgrade-1 (1.1.1.1.2)
SUPI stealing (1.3.1.1.1.1)
Downgrade-1 (1.3.1.1.2.1)
Downgrade-2 (1.3.1.1.2.2)
DoS (Type4) (1.3.1.1.2.3)
CP/UP (1.3.2.1.1.2)
Auth Relay (1.3.2.1.2.1)
Service hijacking (1.3.1.1.2.1.1)
Fake SMSs (1.3.1.1.2.1.2)
Other attacks (1.3.1.1.2.1.2)
Linkability (1.3.2.1.1.2.1)
DoS (Type2) (1.3.2.1.1.2.2)
aLTEr/IMP4GT (1.3.2.1.1.2.3)
Other attacks (1.3.2.1.1.2.4)
Location poisoning (1.3.2.1.2.1.1)
Threat identified in the TR
Threat already mitigated or studied in 5G or being addressed in another TR