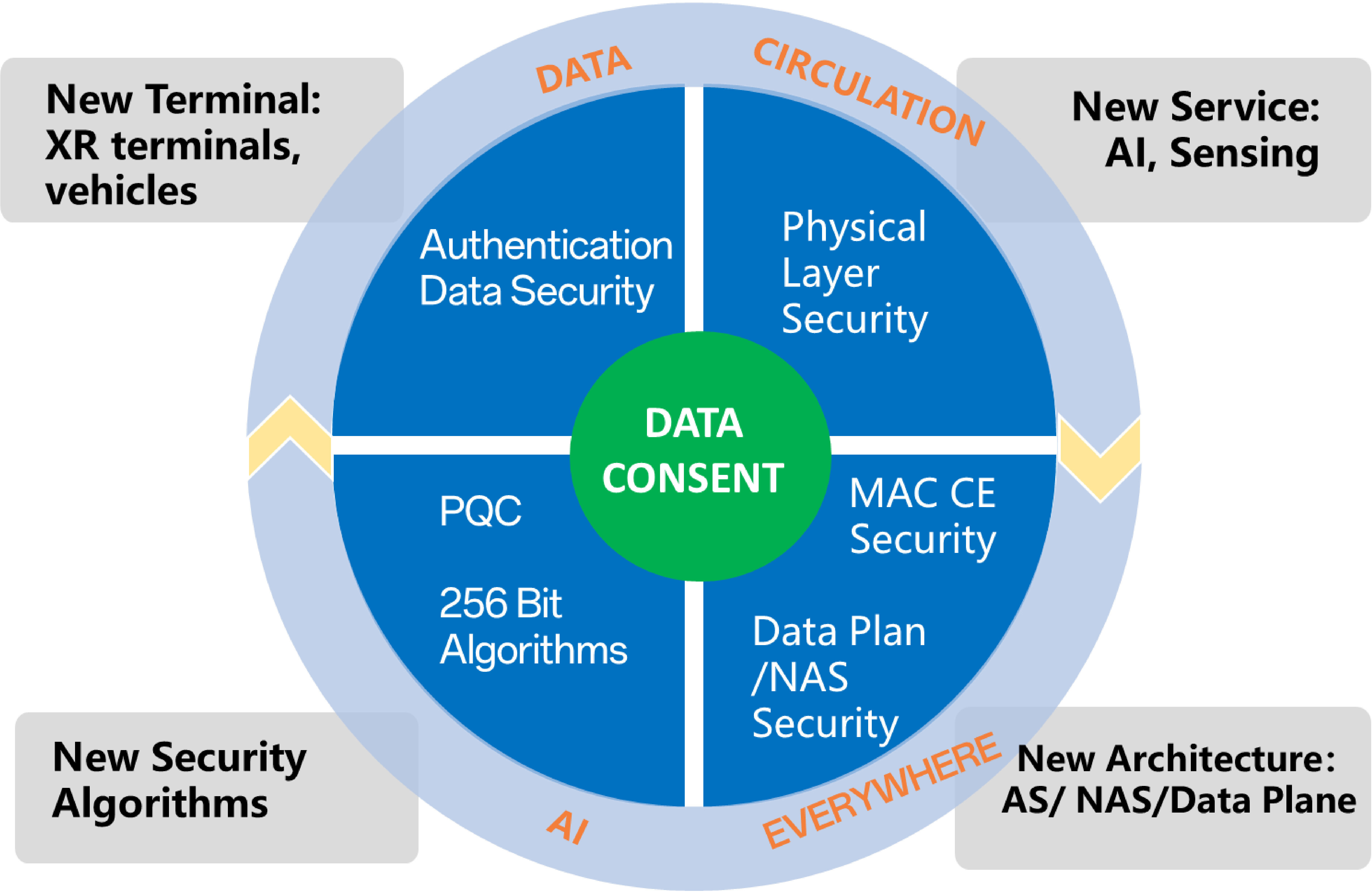
3GPP SA3 6G Security CC

Discussion on 6G Security

oppo

6G Security at a Glance – Security Paradigm shifts towards Data Protection

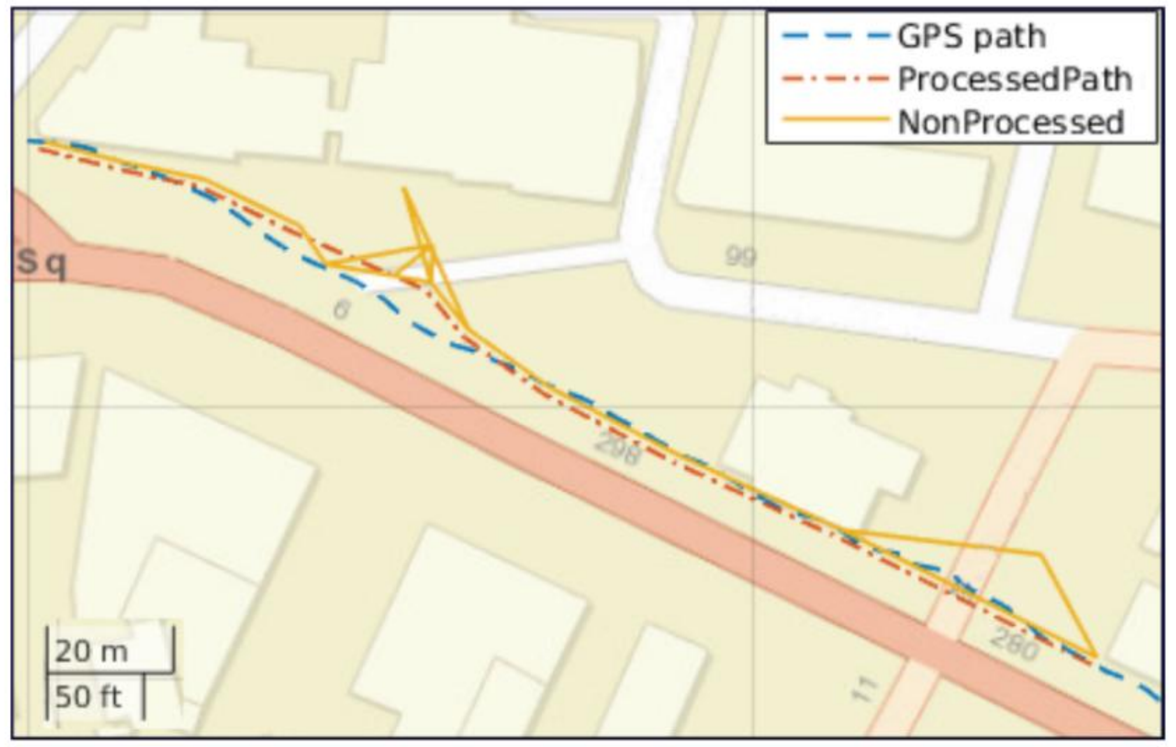
- The emergence of new terminal, new service and new architecture in 6G makes data more valuable, and pushes privacy & security towards protection of value of data.
- The lifecycle management of data/AI in 6G includes lower layer in the air interface, and extends security and privacy protection down to MAC and PHY layers.



- **Data consent for new terminal (XR terminals, Vehicles)**
  - Data security and authentication
- **Data consent for new service (Sensing Service)**
  - For physical layer sensing signal, PLS is needed for sensing signal protection and enable sensing data consent
- **Data consent for communication system architecture**
  - RAN Lower layer： PHY Layer Security，MAC CE Security
  - Core Network: Data consent for Data Framework, and NAS Security
- **New Security algorithm for data consent**
  - Post-Quantum Cryptography (PQC)
  - 256 bit algorithms

PHY and MAC CE Security Vulnerability Analysis

- Some unprotected PHY and MAC CE parameters would lead to potential privacy leakage for UE and procedure failure, especially with enhanced AI capabilities for attackers in 6G, some of the parameters that were once considered not privacy-sensitive may become exposed to privacy risks.
- The lack of PHY and MAC layer security may make L1/L2 vulnerable of spoofing and eavesdropping attacks, such as:
  - **Spoofing during LTM:** Attackers can tamper with sensitive information that may be transmitted in the LTM, such as PCI and NCC, leading to handover failure.
  - **Eavesdropping of C-RNTI, Serving Cell ID and TA Command :** Attackers can determine the distance from the UE to the base station based on the Serving Cell ID and TA information in the MAC CE, enabling precise UE (C-RNTI level) location tracking and privacy leakage.
  - **Eavesdropping of MIB/SIB:** Attackers can first listen to the broadcast information blocks, e.g., the MIB carried by the PBCH or the SIB transmitted in the PDSCH, to achieve the time-frequency synchronization with the gNB.
  - **Spoofing DCI:** The attackers can then analyze the DCI in CORESET to locate the time-frequency position of the PDSCH carrying SIB, perform a PO spoofing attack to trigger malicious RA procedure, and further estimate user location.
  - **Spoofing Air-interface AI inference:** Spoofing CSI/Beam measurement information may lead to AI inference failure for CSI/Beam prediction.



PHY and MAC CE Vulnerability	
Parameters	**Impacts**
PCI, NCC	LTM failure
Serving Cell ID, TAC	Location information of UE
C-RNTI	UE identity information of certain range and certain time period
MIB, SIB	achieve the time-frequency synchronization with gNB
DCI	Spoofing DCI leads to malicious triggering RA procedure

[1] Ludant N, Vomvas M, Noubir G. Unprotected 4G/5G Control Procedures at Low Layers Considered Dangerous[J]. arXiv preprint arXiv:2403.06717, 2024.
[2] The Security Overview and Analysis of 3GPP 5G MAC CE   https://arxiv.org/html/2506.09502v2

The Security Requirements for MAC CE IEs

MAC CE protections serve as supplemental security protections when needed in addition to PDCP/RRC protection.

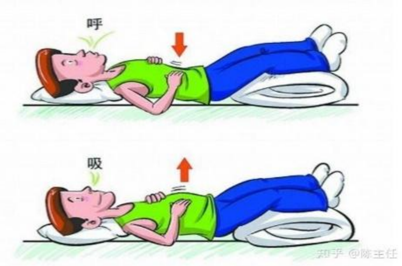
- □ **Potential RAN2 procedure related to MAC CE(s) security in 6G**
  - ➢ LTM, mobility in MAC layer
  - ➢ Random access- before AS security setup;
  - ➢ Mobility (AI mobility), introducing AI;
  - ➢ …
- □ **The security requirements for MAC CE(s) in 6G:**
  - ➢ The unprotected MAC CE(s) carries essential IEs (e.g., Beam index ID, SRS Resource's Cell ID, Serving Cell ID and etc.), potential tampering attacks may affect signal quality or further lead to unavailability of system services.
  - ➢ The attacker may estimate the approximate location of the UE based on some certain IEs (e.g., C-RNTI, Serving Cell ID, Beam index ID etc.) carried by MAC CE. Potential trackability and likability attacks of the UE may lead to the disclosure of privacy.
- □ **The identified security threats of the unprotected LTM MAC CE in 5G**
  - ➢ The attacker may manipulate the timing advance information, and cause the desynchronization between the UE and the BS. The Target Configuration ID may be tampered with, leading to connection failure between UE and the target cell.
  - ➢ Furthermore, the NCC, keySetChangeIndicator, or the chosen algorithms of the target gNB are carried by the LTM Cell Switch Command MAC CE, they could be tampered, this may result in out-of-sync, key mismatch or security negotiation failure between the UE and target gNB;
  - ➢ **SA3 has expected that security for the LTM MAC CE to be studied in 6G.**

Privacy-sensitive Use Cases of 3GPP Sensing

A. Smart Home：

- Use cases: **Intruder Detection**, **Health monitoring**
- Target User: Smart home consumers
- Products: **Cell phone, Smart IoT Devices.**
- Quality Requirements: Low/Normal

Intruder Detection



Health Monitoring

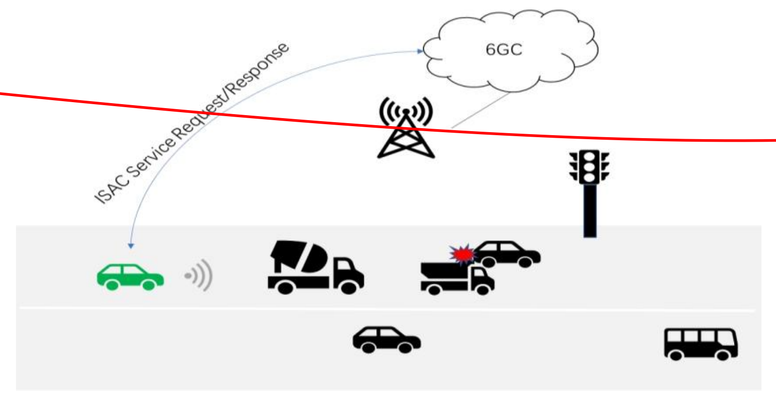
B. Interactive Entertainment：

- Use cases: Gestures/expressions/**movements capturing**
- Target User: AR/VR consumers, Gamers
- Products: **Cell phone, CPE, Smart IoT Devices.**
- Quality Requirements: High

Gestures/expressions/movements capturing

C. Autonomous Driving：

- Use cases: **Environment detection**
- Target User: Autonomous Driving Users
- Products: **vehicles, UE on board of the vehicle**
- Quality Requirements: High



- User privacy protection
- Data security

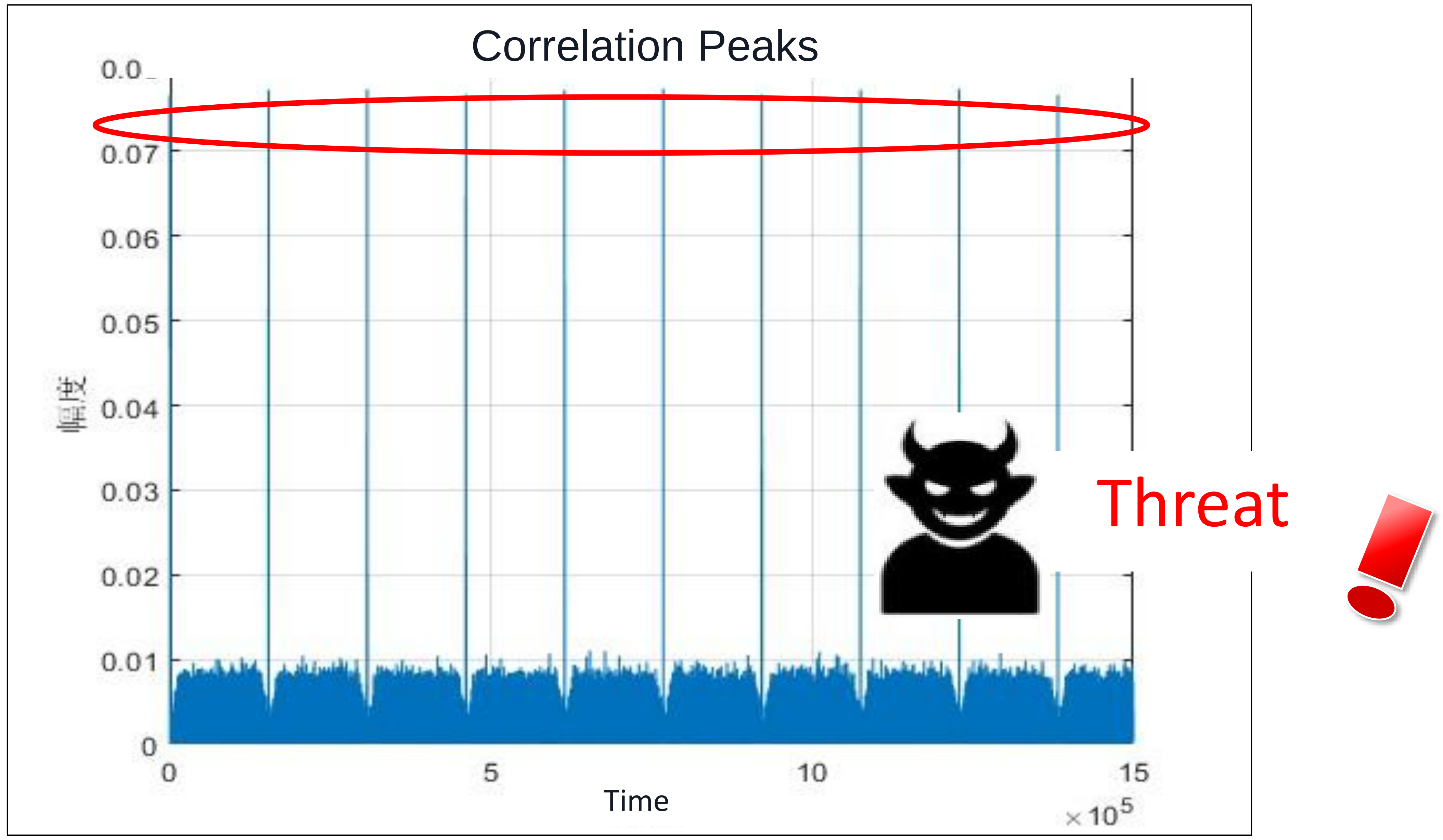
TS 22137 R19 ISAC service request

4.3 Sensing security and privacy aspects

- 5G wireless sensing service also brings challenges related to confidentiality and privacy. There is a need to protect the sensing data from unauthorized access, interception and eavesdropping, but also to make sure the 5G wireless sensing service is in compliance with regulatory requirements.
- The introduction of sensing capabilities can enable tracking of people and objects in the environment, including people not carrying UEs. Thus, additional considerations are needed to protect their rights to privacy.

PHY Security and Privacy Analysis: PRS Signal of Respiratory Rate

- Based on the existing PRS threats analysis[1][2], human respiration rate is even more vulnerable.
- With PRS periodicity, and the respiratory rate can be analyzed from the correlation peaks.



◆Attackers can leverage the periodicity of PRS to analyze respiratory rate through correlation detection.

- The PRS signal format, sequence type, sequence mapping method, etc., are all publicly known and follow specific distribution patterns in time, frequency, and space. Based on these patterns and the correlation characteristics of PRS signals, attackers can measure and analyze some core PRS parameters.

- The total combination of PRS configuration parameter types and candidate values is limited. The combinatorial space is approximately on the order of magnitude of 2^{58} or even 2^{31}, far below the search space corresponding to 128-bit or 256-bit keys, may become vulnerable to brute-force attack.

[1]Gao K, Wang H, Lv H, et al. Your Locations May Be Lies: Selective-PRS-Spoofing Attacks and Defence on 5G NR Positioning Systems[C]//IEEE INFOCOM 2023
[2]Singh M, Roeschlin M, Ranganathan A, et al. V-range: Enabling secure ranging in 5g wireless networks[C]//NDSS. 2022.

The Security Aspects of Core Network Enhancements-1

- The section introduces security aspects of architectural enhancements, including the following:
  - Security for NAS System enhancement
  - Security for Data Framework
  - Security for Migration and interworking

- Security for System enhancement
  - Description: In the 5G network, some NAS messages (e.g., SM, LM, UE policy) relies on the piggybacking on NAS MM messages. For 6G network, a design of decoupling NAS transport and Access and Mobility Management may be necessary to avoid extra processing or delay.
  - Security requirements:
    - NAS security should extend 5G NAS security while adapting to 6G NAS System enhancement, such as the potential shift of the NAS security endpoint away from the AMF.
    - The design of 6G NAS system shall incorporate mechanisms to mitigate potential cyber-attacks targeting core network elements. (e.g., Fundamental security principles shall continue to apply, including the prohibition of exposing network topology information to UEs)

The Security Aspects of Core Network Enhancements-2

- The section introduces security aspects of architectural enhancements, including the following:
  - Security for NAS System enhancement
  - Security for Data Framework
  - Security for Migration and interworking

- Security for Data Framework
  - Description: It is an unified data management framework (i.e., the process of ingesting, storing, organizing and maintaining the data collected and pre-processed by the 6G system) to provide the data services (e.g., data collection, data refinement, data pre-processing, data storage etc.) in order to support the data-driven operations (e.g., AI/ML training/inference/data analytics, Sensor filtering/analysis etc.).
  - Security requirements
    - Authentication between entities in Data Framework;
    - Authorization of data resources in various data services (e.g., data storage and data consumption) to prevent data resources from being abused;
    - Fairness and traceability of data transactions in Data Framework;
    - To support any-to-any security data transmission with possible one or more intermediate hops for data processing.

The Security Aspects of Core Network Enhancements-3

- The section introduces security aspects of architectural enhancements, including the following:
  - Security for NAS System enhancement
  - Security for Data Framework
  - Security for Migration and interworking

Security for Migration and interworking

- Description: Deployments based on different 3GPP architecture options (i.e. 5GC based or 6GC based) and UEs with different capabilities (5GC NAS and 6GC NAS) may coexist at the same time within one PLMN.
- Security requirements:
  - Security handling during mobility from 5GS to 6GS;
  - Security mechanism for handover between 5GS to 6GS;
  - Mapping of security context between 5GS and 6GS.

Potential Security WTs

WT1: Core Network Security

- Security enhancement for Connectivity (e.g., NAS System enhancement, System Migration and Interworking)
- Security enhancement for Beyond Connectivity (e.g., Data Framework)

WT2: MAC Layer Security

- To avoid failure of RAN procedures such as LTM and RA procedure, integrity protection could prevent tempering some critical MAC CE parameters.
- To protect sensitive information such as location information during MAC CE transmission, encryption could prevent attacker from eavesdropping MAC CE information.

WT3: PHY Layer Security

- Taking security into consideration at the beginning of 6G reference signal or channel design can effectively prevent potential PHY layer security and privacy threats.

Thanks for listening!