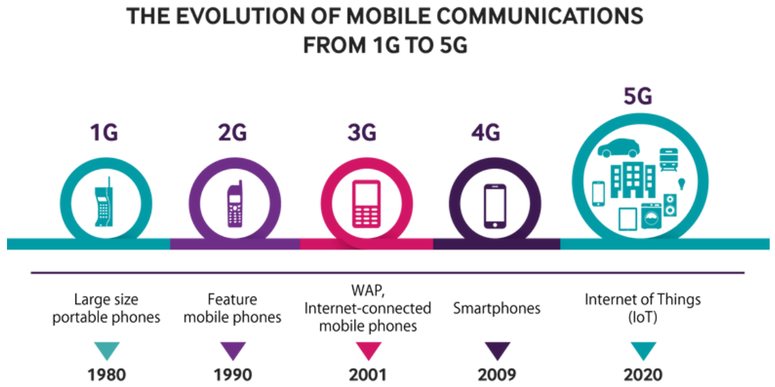
Alessandro Castelli

ID: 147073

5G SECURITY

The Evolution Towards 5G



1G

Characterized by low service quality and non-existent security, but it allowed mobile connectivity for the first time.

2G

Communication becomes digital. Better performance in terms of bandwidth, efficiency, and security.

3G

It introduces the concept of mobile broadband, thus enabling internet browsing.

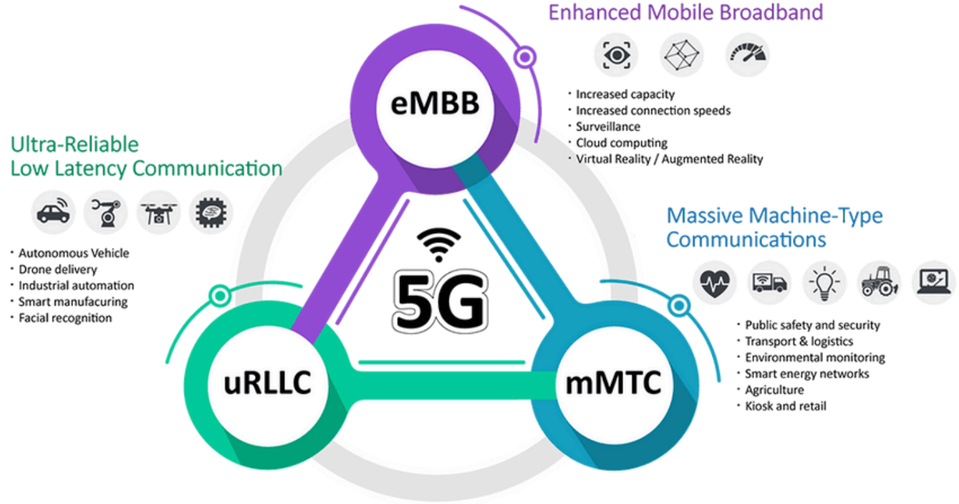
4G

It significantly increases performance, allowing for video streaming, online gaming, etc., in high definition with theoretical speeds of up to 100 Mbps.

5G

The new era of mobile communication

5G Technology: main categories of services



eMBB

Enhanced Mobile Broadband

Objective:
To provide enhanced mobile broadband connectivity.

Features:

- High data transmission speeds.
- Supports applications that require high bandwidth.
- Optimal for HD video streaming, online gaming, and augmented/virtual reality.

mMTC

Massive Machine Type Communications

Objective:
Enable communication between a large number of IoT devices.

Features:

- Supports millions of connected devices simultaneously.
- Optimization for low bandwidth operations.
- High energy efficiency for long battery life devices.

uRLLC

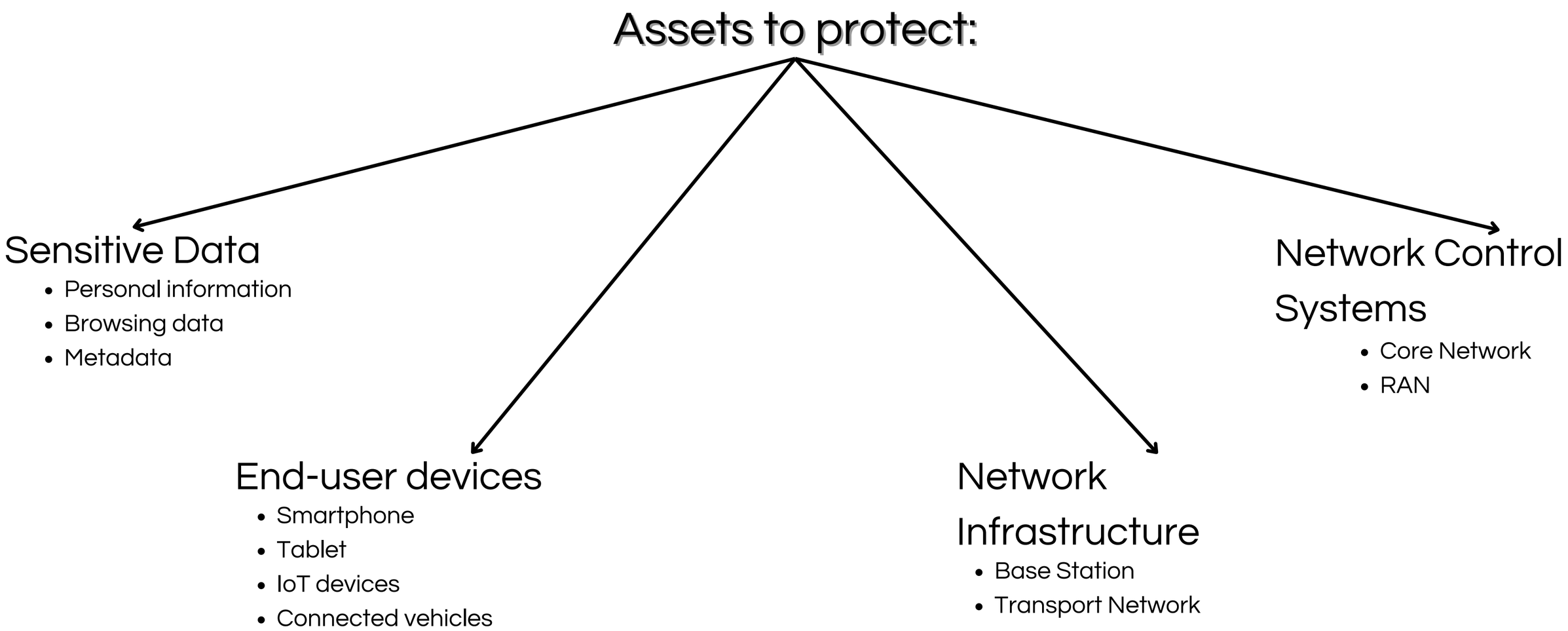
Ultra-Reliable Low Latency Communications

Objective:
Provide ultra-reliable communications with low latency.

Features:

- Latency of less than 1 millisecond.
- High reliability in transmissions.
- Necessary for real-time critical applications.

Threat model



Threat model – Attackers

The potential attackers within such a widely used technology could be very diverse:

- Individual hackers seeking to intercept and manipulate data for illicit purposes
- Groups of organized cybercriminals
- Malicious insiders, meaning personnel with legitimate access to the network

Threat model – Attack vectors

Attack Vector	Description
Insecure radio interfaces	Communication protocols that can be compromised if not implemented correctly.
Inadequate roaming parameter management	Failure to update security measures when switching between different networks, exposing vulnerabilities.
Misconfigured network settings	Errors in configuring network devices that can be exploited by attackers.
Unencrypted control channels	Unprotected communications that can be easily intercepted.
Vulnerable user devices	Smartphones and IoT devices with weak security measures, subject to compromise.
Outdated software	Applications and operating systems that are not updated and may have known vulnerabilities.
Poor credential management	Use of weak or poorly managed credentials that can be easily guessed or stolen.
Vulnerabilities in SDN and NFV protocols	Innovative technologies like software-defined networking and network function virtualization may have security flaws.
Non-robust authentication systems	Authentication methods that do not provide adequate security, allowing unauthorized access.
Direct phishing attacks on end users	Attempts to deceive individuals into revealing sensitive information directly.

Security Goals

It is necessary that the system refers to the principles of:

Confidentiality

This principle ensures that sensitive information is accessible only to those authorized to view it. Techniques to maintain confidentiality include encryption, access controls, and data masking.

Integrity

Integrity involves maintaining the accuracy and completeness of data. This means that information cannot be altered in an unauthorized way. Mechanisms to ensure integrity include checksums, hashing, and digital signatures, which help detect unauthorized changes to data.

Availability

This principle ensures that authorized users have access to information and resources when needed. It involves maintaining hardware, performing regular maintenance, and implementing failover strategies to protect against outages or Denial of Service (DoS) attacks.

Authentication

Authentication verifies the identity of users or systems before granting access to resources. Common methods of authentication include passwords, biometrics, tokens, and multi-factor authentication (MFA).

Accountability

Accountability ensures that actions taken on a system can be traced back to the individual or entity responsible for them. This is typically achieved through logging and auditing, which provide a record of user activity and system changes.

Security Goals

Confidentiality

- Personal and corporate user data
- Sensitive IoT application data
- Network traffic
- Location data
- Payment and billing information

Integrity

- Network control data
- Network configurations and updates
- Signaling traffic
- Firmware integrity in devices
- Data integrity in IoT sensor networks
- Packet integrity in data transmission
- Secure software updates

Availability

- 5G base stations
- Cloud and virtual infrastructure
- Network core infrastructure
- Edge computing nodes
- Service continuity for critical applications

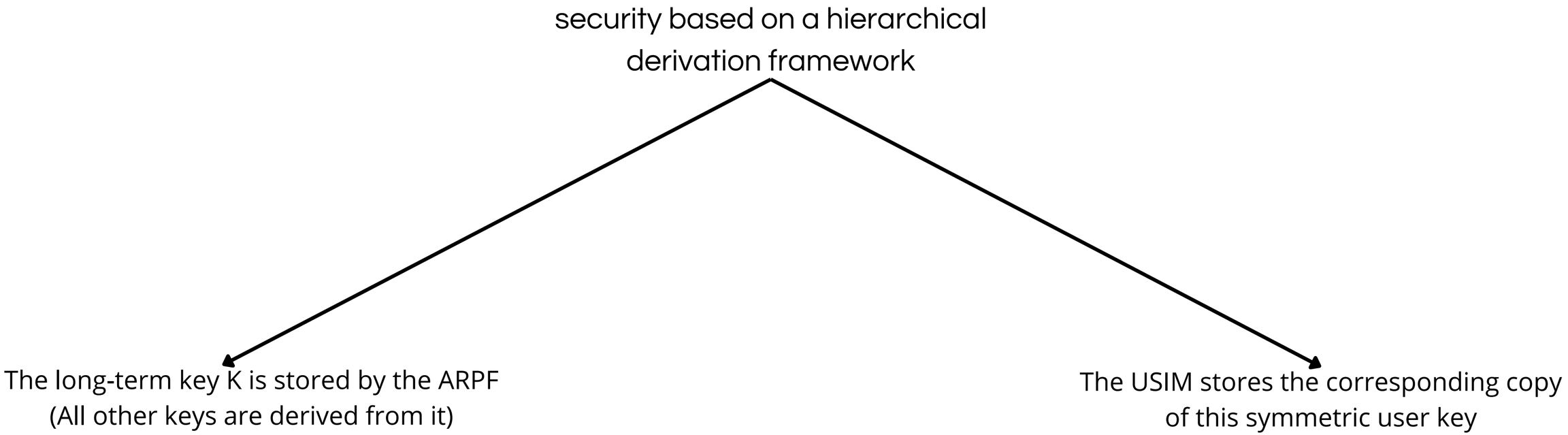
Authentication

- IoT devices
- User identities
- Network components (edge, core, etc.)
- SIM card authentication
- Device and network equipment identities
- Multi-factor authentication systems

Accountability

- Network logs
- User transactions and activities
- Tracking of network access and usage
- Incident and event logs
- Legal and compliance records
- Monitoring of unauthorized access attempts
- Detailed usage history

Security Service



Security Service

Authentication Protocol

- Introduction of the Extensible Authentication Protocol (EAP) by 3GPP.
- Mandatory methods: EAP-AKA and 5G AKA for device and network authentication.
- Ensures mutual authentication and service protection.
- During registration, the device sends the SUCI to initiate the authentication process.

Security Service

Security contexts

- Various contexts are defined for: individual 5G service networks (SN), between multiple SNs, and between 5G and 4G
- Autonomous management of security contexts when a device is connected to two SNs
- Separate NAS connections but with a common NAS security context when registered on two SNs within the same PLMN

Security Service

Security management during the transition

- Configuration of the handover type is at the discretion of the operator
- Security during handover is an optional feature and may potentially be insecure

Security Service

Encryption and Data Protection

- Cryptographic separation and protection against replay attacks are ensured through a shared NAS security context
- 128-bit encryption algorithms are used in NAS
- Possibility of null encryption and integrity protection
- The initial NAS message is transmitted in plain text if a NAS security context is not present

Security Service

Radio Resource Control

- Integration and confidentiality are ensured by the PDCP layer between the device and the gNB.
- RRC integrity checks are performed on the device and the gNB.

Security Service

User Plane: Session Management Function (SMF) Responsibilities

- Role of SMF: Provides security policies for PDU (Protocol Data Unit) sessions to the gNB during session establishment.
- Integrity Protection: If integrity protection is not activated for Data Radio Bearers (DRB), neither the gNB nor the device can ensure the integrity of traffic for those DRBs.
- User Plane Encryption: Without encryption activated for DRBs, the traffic remains unencrypted.
- Local SMF Authority: The local SMF can override the privacy option specified in the user plane security policy received from the Home Network (HN) SMF

Security Service

Privacy

- SUCI as a hidden version of SUPI to prevent identity exposure.
- SUCI generation using the operator's public key and asymmetric encryption.
- Null protection system used during unauthenticated emergency sessions.
- Introduction of 5G-GUTI to reduce exposure of SUPI and SUCI, reassigned based on device triggers.

Attacks and Vulnerabilities

5G NSA

5G is being implemented using the existing 4G infrastructure. LTE manages the control plane and signaling, while 5G New Radio primarily handles data transmission.

5G SA

5G operates completely independently without relying on LTE infrastructure. The 5G NR network handles both signaling (control plane) and data (user plane).

Attacks and Vulnerabilities – 5G NSA

The main threats in 5G NSA networks are:

- Information leakage
- DoS attacks
- Interception
- Unauthorized use of data

Attacks and Vulnerabilities – 5G NSA

Radio Access Network Threats

Attack	Description
Information Leakage	Includes paging sniffing and IMSI decoding. Attackers intercept paging messages broadcasted by base stations to obtain the user's IMSI, using devices like Software Defined Radio (SDR).
Denial of Service (DoS) for the User	Comprises attacks such as RRC connection DoS, RRC rejection DoS, and RRC release DoS, exploiting the victim's S-TMSI. The attacker sends RRC connection requests using the victim's S-TMSI, causing disconnection and preventing legitimate access.
Base Station DoS	Aims to exhaust the resources of the base station by increasing the number of active RRC connections through unauthorized requests, causing delays or interruptions in services for legitimate users.
Eavesdropping	Interception of voice communications, where an attacker can record encrypted voice communications and then use the same bearer ID to extract the keystream needed to decode previous communications.
Unauthorized Data Use	Attackers exploit predefined and dedicated bearers to access data unauthorizedly, such as establishing cost-free communications. It also includes caller masquerading, where the attacker falsifies the caller's identity to deceive the victim.

Attacks and Vulnerabilities – 5G NSA

Core Network Security Threats

Attack	Description
Information Leakage	5G core networks can be divided into EPC devices for data processing and IMS devices for services. Attackers can target the GTP protocol between EPC devices or the SIP protocol in IMS devices to extract desired information. A common technique is GTP-C packet injection to extract IP information from EPC devices.
IP Exhaustion	Using the GTP-in-GTP technique, an attacker can exhaust the pool of IP addresses by sending session requests with incremented terminal numbers, preventing legitimate terminals from connecting.
Denial of Service (DoS)	A DoS attack can be executed by repeatedly sending connection request messages to the 5G NSA network, overloading the core network and causing service interruption.
NAS Manipulation	NAS protocol messages, used for signaling between terminals and the core network, are not always protected by encryption. An attacker can exploit this vulnerability by installing a malicious base station to manipulate messages and alter critical parameters for encryption and data integrity.
Eavesdropping	Voice communications in 5G networks use the IMS network and the SIP protocol. If an attacker can disable IPSec encryption in the victim's terminal, they can intercept unencrypted voice traffic through man-in-the-middle (MitM) attacks.
Spoofing	IP spoofing is a common attack where the attacker sends packets with falsified IP addresses, causing billing issues and potential DoS attacks. Additionally, spoofing the "from" field in SIP or MMS packets can be used for voice phishing, presenting fake numbers on the receiving terminal.

Attacks and Vulnerabilities – GUTI attack

- GUTI is a temporary identifier assigned to users to ensure their privacy
- Ensures user privacy through random and unpredictable reassignment.

Key Issue:

- Vulnerability arises when the GUTI reallocation command is sent without encryption or integrity protection, exposing users to potential attacks.

Attacks and Vulnerabilities – GUTI attack

Attack Scenarios

1. Man-in-the-Middle (MiTM) Attack:
   - Attacker intercepts and modifies the GUTI value in the configuration update message.
   - If the device reconnects with this altered GUTI, the network fails to recognize it, causing a Denial of Service (DoS).
2. GUTI Refreshment Neutralization:
   - No ACK required: Attacker blocks or alters commands without acknowledgment, preventing completion notifications from the UE.
3. Victim Tracking:
   - Without encryption, attackers can track user location by sending silent messages and monitoring network responses to infer UE's presence.

Attacks and Vulnerabilities – GUTI attack

Attack Complexity in Large Networks

- Challenge in Large-Scale Networks:
  - High device density complicates isolating individual devices due to message volume.

Attacks and Vulnerabilities – GUTI attack

Operator Responsibilities and Countermeasures

Role of Network Operators:

- Vulnerabilities are often due to implementation flaws in 5G networks.
- Operators are advised to avoid sending NAS messages without integrity verification.

Countermeasures:

- Encrypt NAS Messages: Operators should enforce encryption as specified by 3GPP guidelines.
- Ensure Integrity Checks: Avoid transmitting sensitive commands without integrity protection to safeguard user privacy.

Attacks and Vulnerabilities – Security Capabilities Bidding-Down Attack

What is the Bidding-Down Attack?

- It’s a vulnerability in 5G networks that affects both NSA (Non-Standalone) and SA (Standalone) configurations.
- Results from implementations where operators do not fully adhere to 3GPP security specifications.
- Potential impact: compromise of confidentiality and integrity of transmitted data.

Attacks and Vulnerabilities – Security Capabilities Bidding-Down Attack

Attack Procedure

- Device Registration (UE): The user device communicates its security capabilities, including encryption and integrity algorithms.
- Data Interception and Modification: An attacker in man-in-the-middle mode intercepts the registration message, altering the security capabilities to enforce weaker algorithms.
- NAS SMC Command: The core network sends a NAS Security Mode Command (SMC) without a MAC (Message Authentication Code), leaving the message vulnerable to undetectable modifications.

Attacks and Vulnerabilities – Security Capabilities Bidding-Down Attack

Consequences

- Complete Compromise of Security: the device may use vulnerable algorithms.
- Loss of Confidentiality and Integrity: transmitted data may be intercepted or altered.
- Persistent Threat to the Network: every connection may be at risk if the network does not properly implement 3GPP specifications.

Attacks and Vulnerabilities – Security Capabilities Bidding-Down Attack

Prevention Measures

- Always Include a MAC: ensures the integrity of SMC messages.
- Robust Verification of Capabilities: the network should compare the security capabilities communicated by the device with its own.
- Use Advanced Algorithms: avoid obsolete algorithms; prefer modern, robust algorithms to maximize security.

Thank you!