Mobile Network Protocols, from 2G to 5G. Evolution and Lessons Learned

***Abstract*— Mobile network protocols are the foundation of wireless communication, providing customers with a variety of services and seamless connectivity. They dictate how mobile devices connect, transmit data, and communicate with network infrastructure while ensuring the secure operation of mobile connection systems. These protocols control voice and data transmissions and range from the original GSM to the state-of-the-art 5G NR technology.**

***Index Terms*— Signaling System 7 (SS7), Location Tracking, SMS Interception, GSM, LTE, MAP, SCTP, Sigploit**

I. Introduction

Mobile network protocols are essential to facilitate services and communication in wireless networks. In the evolution from 2G GSM to 5G NR, various protocols play crucial roles. Voice and data are established using GSM through protocols like GSM-MAP and SS7. For higher data speeds, WCDMA and RANAP were introduced by the 3G standard UMTS. LTE, a 4G technology, introduced S1AP and X2AP for effective signaling between base stations and the core network. It uses LTE-Uu for high-speed data. NGAP is used for signaling in the advanced core network and NR-U for unlicensed spectrum operation in the 5G NR standard. IMS integrates SIP and RTP to enable multimedia services. VoLTE, or voice-over LTE, uses RTP for real-time audio transmission and IMS and SIP for call setup. All these protocols operate together to facilitate smooth communication, rapid data transfer, and the provision of various services across mobile networks.

II. Evolution Of Cellular Networks

The evolution of cellular networks has significantly improved communication, transitioning from early wired telephony using copper wires to the current wireless cellular networks. Initially, Mobile Radio Telephone systems, considered 0G, relied on a centralized operator and required heavy equipment. Advancements led to better connectivity, progressing through generations (1G to 5G), enhancing features, and addressing various issues. Modern cellular networks now enable long-distance connectivity, data transmission, and seamless communication between wireless and wired devices.

1G (First Generation)

Japan's NTT launched the first commercial cellular network in 1979, marking the advent of 1G technology. Utilizing analog signal technology, 1G faced limitations such as distorted voice signals, vulnerability to interference, and the inability to support text messages or internet services. Nascent technology often collapsed during peak demand, resembling the early challenges in the evolution of computers (Gawas, 2015).

2G (Second Generation)

In the 1980s, 2G introduced digital signals for voice communication, employing GSM technology for continuous connectivity and improvements in encryption, radio spectrum utilization, and the advent of internet services and SMS (Zontou, 2023).

GSM Architecture:

- *Mobile Station (MS)*: Components include SIM (Subscriber Identity Module), IMEI (International Mobile Equipment Identity), IMSI (International Mobile Subscriber Identity), and MSISDN (Mobile Subscriber ISDN Number). SIM serves as a subscriber identifier, and MSISDN is the actual mobile number.
- *Base Station Subsystem (BSS):* Acts as a link between MS and the network, comprising Base Transceiver Station (BTS) and Base Station Controller (BSC).
- *Network Switching Subsystem (NSS):*
  - MSC (Mobile Switching Center): Primary node managing call routing, SMS routing, call set-up, and interactions with other networks (Kheddar, 2022). Multiple MSCs facilitate continuous connectivity during subscriber movement.
  - HLR (Home Location Register): Database storing subscriber data, using MSISDN as a unique key. Manages subscriber mobility and interacts with VLR.
  - VLR (Visitor Location Register): Database in each MSC for roamed-in MS. Updates data from HLR, ensuring a single VLR for each MSC.
  - AuC (Authentication Center): Authenticates new SIM cards, using a secret key linked to IMSI. Generates a session key for secure communication.
  - OSS (Operations Support Subsystem): Manages network maintenance, configuration, and service delivery.

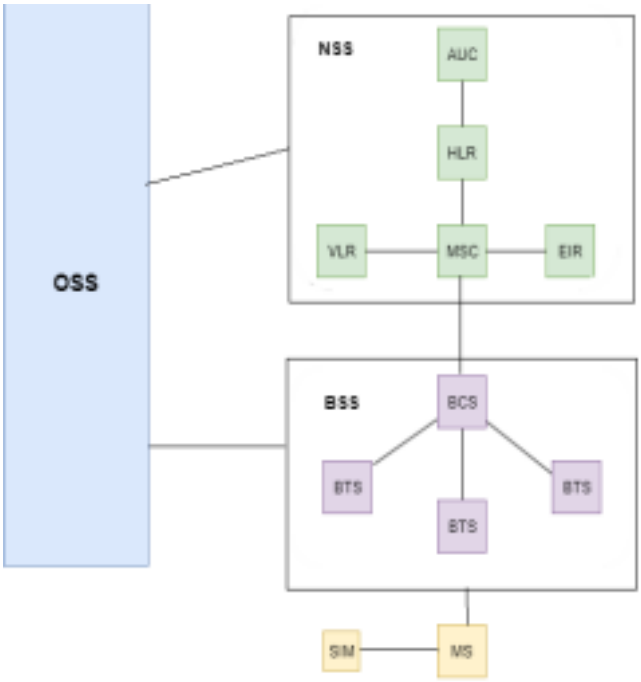


Fig 1. The 2G architecture (Zontou, 2023)

The 2G technology provides two digital modulation schemes – TDMA (Time Division Multiple Access) and CDMA (Code Division Multiple Access). The TDMA breaks down calls on a signal by time and divides them into time slots while CDMA breaks them down by codes. This allows for a boost in network capacity and reduced interference (Gawas, 2015).

Now, 2G networks have some limited capabilities such as low data rate (up to 9.6 kbps) which means no web browsing (Agrawal et al., 2015). These limitations were mitigated through the introduction of GPRS (General Packet Radio Service). Also known as 2.5G, GPRS added IP packet transmission capability to 2G networks, allowing users to access web browsing. GPRS was the link between 2G and 3G networks (Pereira, 2014).

3G (Third Generation)

As wired telephones became obsolete, the need for faster Internet access on wireless mobiles led to the development of UMTS (Universal Mobile Telecommunications System). UMTS combined international roaming with GSM, providing higher data speeds and aiming to enable teleconferencing on mobile devices (Zontou, 2023). 3G includes standards like IMT2000, CDMA2000, and WCDMA, allowing global roaming.

UMTS Architecture: The MS underwent some upgrades as Li-ion battery mobile phones became common. The SIM card also evolved to USIM but the functionalities as well as the contents (MSISDN and IMSI) remained the same.

- *RNC (Radio Network Controller):* Chief governing entity of the UMTS network, replacing the BSC from GSM architecture. Manages handover, encryption, and packet scheduling.
- *PS Domain (Packet Switch Domain):*
  - SGSN (Serving GPRS Support Node): Manages connectivity to the Internet or other packet-switched networks.
  - GGSN (Gateway GPRS Support Node): Routes information from the GSM part of the network to the IP network.

    IMS (IP Multimedia Subsystem) is a Standardized framework for delivering IP multimedia services, acting as a precursor to VoIP.
- *CS Domain (Circuit Switch Domain):* The CS domain is based on the GSM architecture. The GMSC (Gateway MSC) is the MSC which is the first connecting point to the RNC. It determines the location of the receiving subscriber's MSC and routes the call to that MSC. The rest of the architecture follows the GSM architecture.

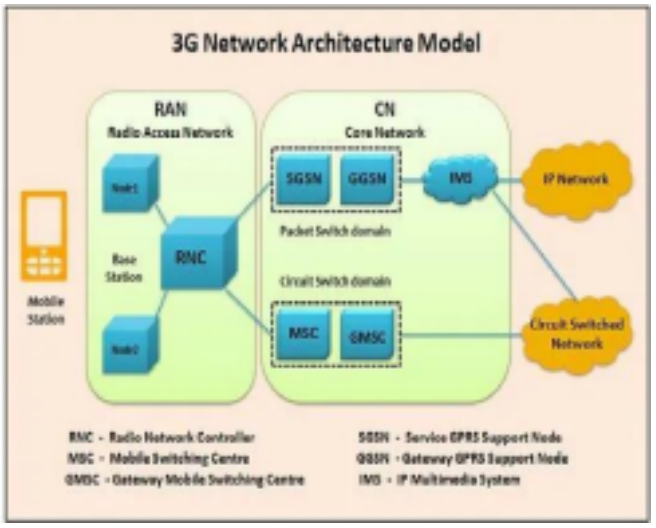


Fig 2. The UMTS architecture (Köksal, 2021)

4G (Fourth Generation)

4G, introduced commercially in 2009 with a data speed of 60Mbps, aimed for higher data rates and low latency over existing third-generation networks. It utilizes orthogonal frequency division multiple access in the air interface for efficient and simultaneous transmission of data. In its advanced version, LTE-A employs various frequency bands and advanced modulation schemes for data rates up to 90Mbps. LTE is a fully IP-based system, using a packet-switched core network. Evolution-wise, LTE shifted to efficient VoIP communication, departing from the circuit-switched processes of 3G. Architecture-wise, it is streamlined to handle packet-switched data, ensuring seamless connectivity between user equipment and packet data networks like the Internet (Kheddar, 2022).

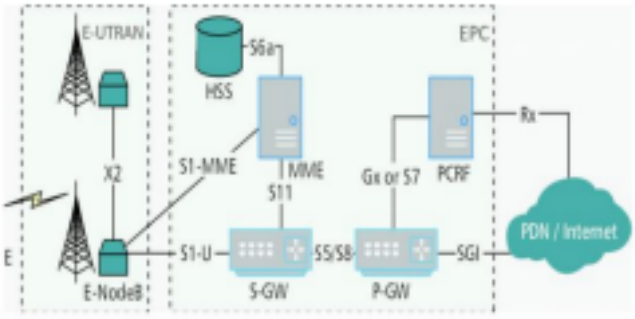


Fig 3. LTE Network Architecture (Kheddar, 2022)

In an LTE network, the E-NodeB facilitates connectivity between the User Equipment (UE) and the Evolved Packet Core (EPC) network, managing call handovers and processing radio signals (Kheddar, 2022).

Key components include (Kheddar, 2022):

- *Mobility Management Entity (MME):* Handles authentication, location update, mobility management, handover support, and bearer establishment functions, ensuring integrity and confidentiality.
- *Home Subscriber Server (HSS):* Stores subscriber information, QoS profiles, roaming restrictions, and MME IDs, including the generation of security key vectors.
- *Serving Gateway (S-GW):* Manages connections while the UE moves between different E-NodeBs and monitors data for legal purposes.
- *PDN Gateway (P-GW):* Assigns IP addresses, ensures QoS for the UE, handles billing, acts as a filter for downlink traffic, and serves as a translator between different technologies.
- *Policy and Charging Rule Function (PCRF):* A part of P-GW responsible for measuring and controlling data and speed according to the subscription plan.

5G (Fifth Generation)

The fifth generation (5G) cellular network, introduced globally in 2019, represents cutting-edge technology providing data rates ranging from 10 to 50 Gbps. It employs massive multiple input multiple outputs (MIMO) and nonorthogonal multiple access to enhance spectrum efficiency and reduce latency in smaller regions. 5G utilizes millimeter-wave technology for high-speed wireless communication, addressing interference issues present in 4G through the implementation of hybrid beamforming. Architecturally, it features a newly designed service-based structure (Dangi et al., 2021).

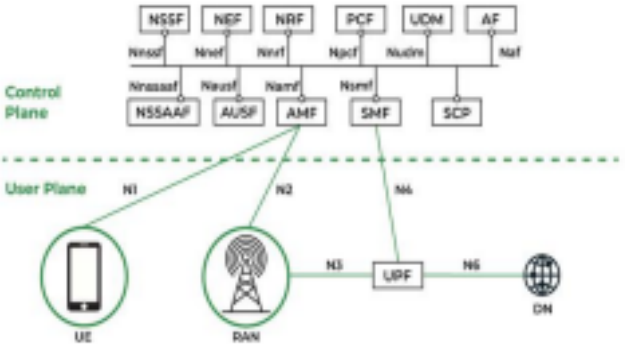


Fig 4. 5G Architecture (GeeksforGeeks, 2022)

- *NSSF (Network Slicing Selection Function):* Selects network slices based on application needs, considering factors like latency and quality of service (Skill Lync, 2022a).
- *AMF (Access and Mobility Management Function):* Core network component serving as an entry point, performing functions like 4G's MME. Supports NAS signaling and mobility management (Skill Lync, 2022b).
- *UPF (User Plane Function):* Establishes direct connectivity between RAN and data networks, controlling the quality of services through enforced packet deduction rules (Skill Lync, 2022d).
- *NEF (Network Exposure Function):* Successor of 4G's SCEF, supports third-party applications to connect with the network, influencing user traffic based on policies (Skill Lync, 2022b)
- *PCF (Policy Control Function):* Like 4G's PCRF, manages the quality of services and policies. Collaborates with NEF to create customized policies for third-party requirements (Skill Lync, 2022a).
- *SMF (Session Management Function):* Manages sessions, acting as SGW from 4G, mediating between UPF and PCF to control traffic flow through packet deduction rules (Skill Lync, 2022c).
- *UDM (Unified Data Management):* Equivalent to 4G's HSS with cloud-native design, handling data for authentication, network profiles, and user registration (Skill Lync, 2022e).
- *AUSF (Authentication Server Function):* Provides secondary user authentication with the assistance of UDF (Skill Lync, 2022f).
- *NRF (NF Repository Function):* Provides data on all available network functions and supplies service producer data upon request from service consumers like AMF (Skill Lync, 2022b)
- *NSSAAF*: Provides authentication authorization services for UE for specific slices, capable of triggering and revoking authentication (ETSI, 2023).
- *SCP (Service Communication Proxy):* Resolves network functions like DNS, akin to 2G and 3G's STP (Monem, 2023).

Overall 5G is a state-of-the-art communication technology with a high-speed data rate, low latency, and many more

features.

III. Security Protocols Used At Different Stages/Versions

Mobile network security has been an evolving field since the inception of 1G. The initial generations (1G and 2G) had minimal security, primarily focused on preventing fraud. With the advent of 3G, security measures became more advanced, introducing mutual authentication and encryption. However, it is the leap to 4G and the transition to 5G that have marked the most significant advancements in mobile network security. This section examines these changes, highlighting how each generation has built upon the lessons of its predecessors to enhance user privacy, data integrity, and secure access.

1G Security Protocols

There was no data service available for 1G, only voice services were provided. 1G mobile networks were primarily analog systems, they barely had any digital security features like encryption. Calls could easily be dropped by a third party, anybody with a radio scanner could drop in on a call. The reliability of the handoff was likewise fairly low. Since a specific frequency had to be assigned to each user, 1G technology's capacity was severely constrained. They were vulnerable to eavesdropping, and there were minimal security mechanisms in place. Security was mainly focused on voice encryption to prevent eavesdropping, using techniques like frequency hopping. According to (Njoroge, 2019) at the mobile phone and the base station were also used for encryption which prevented call interceptions despite not being a strong encryption method.

- ***Frequency Hopping****:* Frequency-hopping spread spectrum (FHSS) is a technique for delivering radio signals that quickly switches the carrier frequency among numerous frequencies distributed across a wide spectral band. The narrow-band signal is dispersed using this technique as a function of time. Multiple times every second, the transmitted frequency is "hopped," changing to a different pre-assigned channel (CableLabs, 2019).

2G Security Protocols

The **Global System for Mobile Communications** (**GSM**) is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) mobile networks. As discussed by Njoroge (2019), in the GSM network architecture, two security procedures are performed: authentication and encryption.

- ***Authentication*** takes place in the Authentication Centre (AuC) located in the Home Location Register (HLR). Each subscriber has an individual 128-bit key (Ki) stored secretly in the AuC, which matches the Ki on the SIM card. During authentication, the IMSI is sent to the AuC, which uses Ki and the A3 algorithm to produce a signed response (SRES) and a cipher key (Kc) for encryption. Multiple triplets are generated and stored in the AuC for faster subsequent connections. The RAND is sent to the SIM, which generates a parallel signed response (SRES*) using Ki and A3. If SRES equals SRES*, authentication is successful. The COMP128 algorithm executes A3 and A8 simultaneously and produces a 96-bit output consisting of SRES and Kc.

- ***A5 encryption algorithm***: To achieve encryption, an A5/x algorithm uses ���� a unique frame number (22 bits) as input parameters. Here, "x" stands for 1, 2, 3, and so on. to protect data and voice communications. The four A5 encryption methods that are available in GSM are A5/0, A5/1, A5/2, and A5/3 [21]. Since A5/0 did not use any encryption techniques, it is essentially plaintext. The GSM standard's strong encryption method is called A5/1. The weak variant, A5/2, has no export restrictions. As a component of the Third Generation Partnership Project, the robust encryption algorithm A5/3 was developed. A5/2 was shown to be vulnerable in real-time and was breached more than a decade ago.

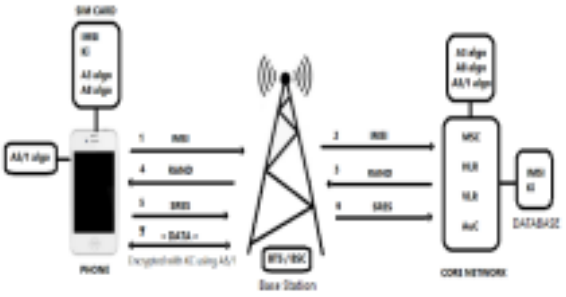


Fig 5. Encryption Process for 2G (Bhis, 2022)

3G Security Protocols

The 3rd Generation Partnership Project, or 3GPP, establishes two sets of standard encryption and integrity algorithms that must be used in third-generation mobile communication systems.

The **KASUMI block cipher** serves as the foundation for the first set, UEA1 and UIA1. The second set of algorithms, UEA2 and UIA2, is based on the **SNOW 3G stream cipher** as the primary cryptographic primitive.

- ***Kasumi Block Cipher****:* 3G networks improved security by introducing stronger encryption algorithms, such as KASUMI for voice. KASUMI works with a 64-bit input operated on by a 128-bit key and gives out a 64-bit output. This algorithm features in the newer GSM systems too as A5/3 algorithm. The eight-round Feistel network at the core of the KASUMI cipher is powered by a round key that is made up of eight 16-bit subkeys that are obtained from the 128-bit key according to a predetermined key schedule for each round (P Halagali and V Desai, 2017).

- ***UMTS AKA Protocol***: Another notable security

protocol used in 3G networks is the Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement (AKA) protocol. It provides a framework for authenticating both the mobile device (subscriber) and the network. The AKA protocol uses Challenge-Response mechanisms to verify the identities of both parties. It generates session keys for secure communication between the device and the network. UMTS AKA helps protect against various security threats, including eavesdropping, man-in-the-middle attacks, and impersonation. While Kasumi was used for ciphering voice traffic in 3G networks, UMTS AKA played a crucial role in ensuring the overall security of the network by establishing secure communication channels and verifying the authenticity of the devices and the network itself.

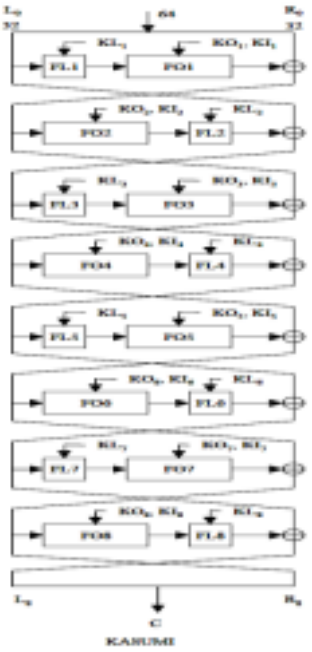


Fig 6. Kasumi Block Cipher (Shaker et al., 2013)

- ***SNOW3G Stream Cipher****:* With an internal state of 608 bits, SNOW3G is a two-component stream cipher that is started by a 128-bit key and a 128-bit initialization vector IV. It is made up of two interconnected modules: a finite state machine (FSM) and a linear feedback shift register (LFSR). The LFSR is made up of sixteen stages, each of which has thirty-two bits. A primitive polynomial over a finite field defines the feedback in each step. The FSM employs two substitution box ensembles that make use of XOR and modulo- 2^32 addition operations. It is built on three 32-bit registers (P Halagali and V Desai, 2017).

4G(LTE) Security Protocols

Based on the Long-Term Evolution (LTE) standard, 4G networks made significant security advancements over earlier 3G networks (Bartock et al., 2013).

- *EPS-AKA (Evolved Packet System Authentication and Key Agreement):* This is the primary authentication mechanism in LTE, an enhancement over the UMTS AKA used in 3G. It involves a challenge-response mechanism that ensures mutual authentication between the user and the network. The user's SIM card (containing a secret key) and the network both possess this secret key used to generate cryptographic responses (CableLabs, 2019).

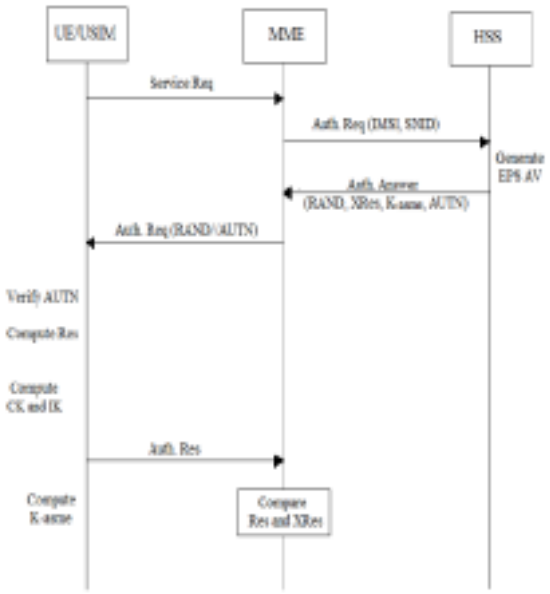


Fig 7. LTE Authentication Procedure (Ramadan et al., 2016)

- *NAS (Non-Access Stratum) Security:* The NAS layer encapsulates the signaling between the device and the core network for session and mobility management. Two sets of keys are derived from the EPS-AKA process: one for encryption (NAS encryption key) and another for integrity protection (NAS integrity key).
- *AS (Access Stratum) Security:* AS security is responsible for protecting the data that is transmitted over the air. It uses a pair of keys derived from the initial key agreement process: the RRC (Radio Resource Control) encryption key for ciphering the data and the RRC integrity key for ensuring the integrity of the control plane.
- *IPsec for S1-MME and X2 Interfaces:* IPsec is used to secure the backhaul links, particularly for the signaling traffic on the S1-MME interface between the eNodeB and the MME (Mobility Management Entity) and the X2 interface between eNodeBs.

5G Security Protocols

5G networks have further advanced the security measures, addressing some of the weaknesses in 4G and introducing

new concepts to cater to the expansive use cases of 5G (Ericsson, 2023).

- *5G-AKA (Authentication and Key Agreement):* Like EPS-AKA but includes additional measures to protect the user's privacy and to resist tracking and identity theft. Sequence number synchronization and home network control features are added to prevent replay attacks and enhance security against rogue base stations.

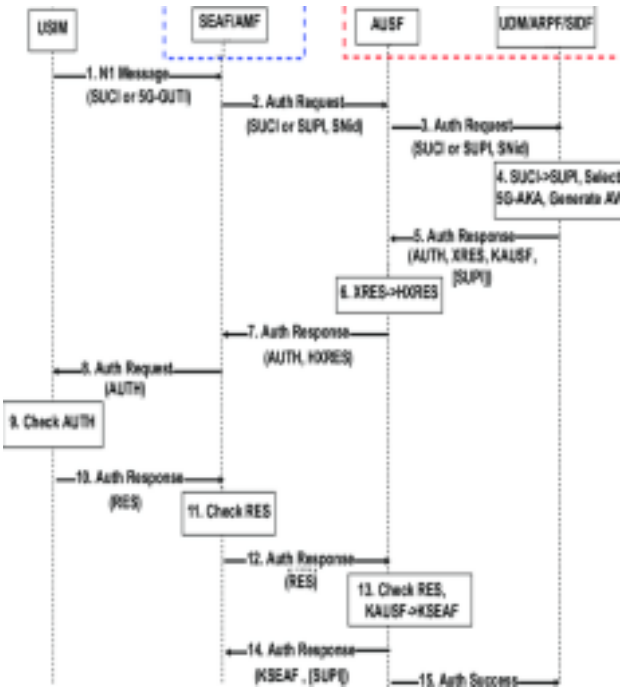


Fig 8. 5G-AKA Authentication Procedure (Abdel-Malek et al., 2022)

- *Enhanced Subscriber Privacy:* Uses Subscription Concealed Identifier (SUCI) to protect the subscriber's permanent identifier (SUPI) from being exposed and potentially intercepted or tracked by adversaries.
- *Service-Based Architecture (SBA) Security:* Utilizes a service-based architecture in the core network, where network functions communicate over HTTP/2 (N. Singh, 2023).
- *SEAF (Security Anchor Function):* SEAF is a functional entity within the Access and Mobility Management Function (AMF). It plays a pivotal role in the security of the 5G network by participating in the initial security procedures when User Equipment (UE) attaches to the network.
- *Network Slicing Security:* Each network slice in 5G can have its security parameters, meaning different slices can employ different security mechanisms tailored for specific service requirements.
- *Security Edge Protection Proxy (SEPP):* SEPPs are introduced in 5G to secure the interconnect between different operators' networks, particularly to protect against risks arising from signaling plane exposure to other networks (ETSI, 2020).

As mobile networks have become integral to our personal, social, and economic activities, the need for robust security protocols has never been greater. The advancements in 4G and especially in 5G reflect a commitment to continuous improvement and adaptation in the face of evolving threats.

IV. Attacks On Security Protocols

Attacks on security protocols of 1G:

1G, also known as the Analog Era
The Beginning of Wireless Communication
When 1G first appeared in the 1980s, it revolutionized mobile communication and brought cellular networks to a global audience. This technology was mainly intended for voice communication and ran on analog transmissions (Galazzo, 2022).

Principal Weaknesses:

- *Unencrypted Communications*: The absence of encryption in 1G was the most obvious security vulnerability. Voice calls were clearly transmitted as analog signals, so anyone with even a basic radio scanner could easily intercept them. This weakness was like conducting talks over an unprotected landline where anyone may listen in (PortSwigger, 2023).
- *Phone Cloning*: One of the main vulnerabilities in 1G was the unencrypted transmission of identifying information, such as the IMEI number. Competent persons might be able to intercept this data and replicate phones, which would allow for fraudulent operations and unapproved charges to be made against the gullible original user (Sonal & Upasna, 2018).
- *Simplicity and Insecurity*: 1G's technology was intrinsically vulnerable due to its general simplicity. The network was vulnerable to new technical threats since it only used rudimentary authentication techniques.

Fig 9. The Cloner (AI-Generated)

Security Aspects (Rao et al., 2023)**:**

- *No Encryption*: One of the most significant drawbacks of 1G was the lack of encryption. Calls could be easily intercepted and overheard using basic radio scanners.
- *Vulnerability to Fraud*: The transmission of identifying information (like IMEI) without encryption made 1G phones easy targets for cloning, leading to widespread fraud.

Attacks on security protocols of 2G:

Due to serious security flaws, the GSM (Global System for Mobile Communications)-based 2G (Second Generation) cellular network technology was finally phased out in favor of more secure alternatives.

The following are the main causes of the deprecation of 2G security protocols:

- *Weak Encryption*: To protect voice and data transmission, 2G networks employed the A5/1 and A5/2 encryption algorithms. It was discovered that these algorithms were weak and vulnerable to cryptographic assaults. In particular, the A5/2 algorithm was very prone to assault and could be defeated instantly (Ekdahl & Johansson, 2003).
- *Unencrypted Signaling Data*: While the content of calls and messages was encrypted, the signaling data (used for setting up and managing calls) was not. This allowed attackers to intercept and manipulate this data, leading to privacy breaches and unauthorized tracking of users (Wickr, 2023).
- *No Integrity Protection*: 2G protocols lacked mechanisms for ensuring the integrity of the data being transmitted. This made it possible for attackers to alter the content of communications without detection (Muppavaram et al., 2023).
- *Limited Key Management*: The key management practices in 2G were not robust enough, leading to vulnerabilities in how encryption keys were distributed and managed.
- *Technology Advancements*: As technology advanced, newer generations of cellular networks (3G, 4G, and 5G) introduced improved security features that addressed many of the vulnerabilities found in 2G. These advancements made the older 2G technology obsolete both in terms of functionality and security.
- *Regulatory and Compliance Issues:* With increasing awareness and regulatory requirements around data protection and privacy, the inherent security weaknesses of 2G became unacceptable, prompting network operators to upgrade to more secure technologies (Muppavaram et al., 2023).

Fig 10. 2G Tower Signal Disruption (AI-Generated)

Attacks on security protocols of 3G:

1) **KASUMI Cipher Attacks:**
   a) Known-Key Attack: Employing known-key attacks, which enable an attacker to decode communication with only an awareness of a specific key, researchers were able to reveal flaws in KASUMI (J. Singh, 2023).
   b) Related-Key Attack: KASUMI was found to have certain cryptographic flaws that left it open to related-key attacks, which degrade security by taking advantage of links between keys (Nguyen et al., 2011).

2) **SNOW 3G Stream Cipher Attacks**:
   a) Bitwise Attack: SNOW 3G was susceptible to bitwise attacks, which gave hackers the ability to change specific bits in the stream and possibly jeopardize the authenticity of encrypted data (Gong & Zhang, 2021).

b) Linear Approximation Attack: SNOW 3G's cryptographic framework was found to have vulnerabilities due to the discovery of linear approximation attacks by researchers (Gong & Zhang, 2021).

3) **UMTS Authentication and Key Agreement (AKA) Protocol Attacks**:

a) Man-in-the-Middle (MitM) Attacks:
Man-in-the-Middle (MitM) abuses were a threat even with the Challenge-Response method in place. An attacker could pretend to be the network or the mobile device if they are able to intercept and modify the request and response communications (Proofpoint, 2023).

b) Cryptanalysis of AKA Protocol: Current cryptanalysis research may reveal flaws that jeopardize the creation of strong and protected session keys within the UMTS AKA protocol (T. S. Kumar & Prabakaran, 2019).

There are several important reasons why 3G security techniques are becoming outdated. First, the unrelenting advancement of cryptographic analysis methods revealed flaws in the algorithms used by 3G, undermining trust in their resistance to complex assaults (Evans, 2023). The need for enhanced and powerful security mechanisms was highlighted by the introduction of 4G and the subsequent developments in mobile communication technologies. The transition to 4G and beyond required more robust security measures to keep up with the constantly changing cybersecurity threat ecosystem.

Furthermore, the option to phase out 3G security techniques was largely influenced by adherence to changing security standards and legal requirements. The demand for improved security options increased as standards changed to handle new dangers and privacy issues. After these weaknesses were identified, and after increased security became necessary, new generations of mobile communication technologies—4G and 5G in particular—introduced sophisticated security measures. These protocols attempted to provide a more robust basis for the safe transfer of voice and data in the constantly changing mobile communication ecosystem, reducing the risks brought about by emerging security concerns (Salahdine et al., 2022).

Attacks on security protocols of 4G:

1. EPS-AKA (Evolved packet system authentication and key agreement):
Possible vulnerabilities that attackers could exploit include (Lu et al., 2023):

a) **Impersonation (man in the middle):** An attacker may attempt to place himself between the equipment (UE) and the network to intercept and alter communication.
They may be the UE or network that exposes unauthorized or sensitive information.

b) **Denial of Service (DoS) attack:** An attacker may attempt to disrupt the EPS AKA or LTE network through multiple requests, causing a denial of service to the target user.

c) **Conflicting keys:** If the keys used for encryption and decryption are not adequately protected, attackers with access to these keys can decrypt and control the transmitted data.

2. NAS (Non-access Stratum) Security: Here are some potential attacks on the NAS in 4G (Rupprecht et al., 2020): a. **Data tampering:** The attacker will try to alter the integrity of the message, causing no change or interrupting the communication between the UE and the network.

b. **Location tracking**: Attackers can use notifications to track the movements of specific users, thus compromising privacy.

c) **SMS interception:** An attacker may attempt to intercept SMS sent between the network and the UE.

4G LTE (Long Term Evolution) technology has not been deprecated yet. It is also widely used worldwide to provide high-speed wireless communications for mobile devices. Although next-generation mobile networks such as 5G are used and expected to become widespread, 4G is still an important part of global communications.
It is also worth noting that 4G is still reliable and widely used on the Internet, providing high-speed data and efficient mobile communications (Remmert, 2020). Users with 4G-enabled devices will likely continue to use 4G networks in the future.

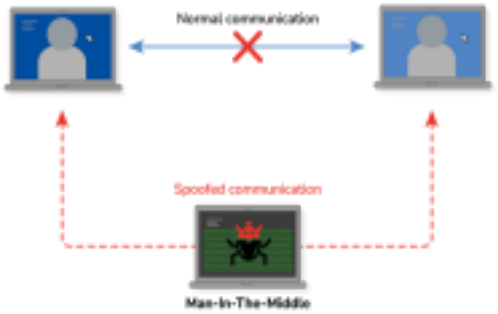
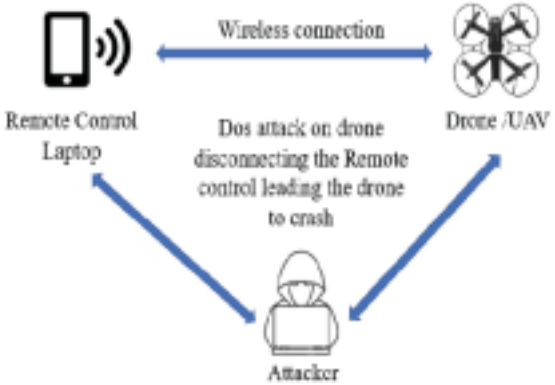


Fig 11. Man in the middle attack (Kumar, 2022)

Fig 12. Denial of Service attack (Dai & Nguyen, 2021)



Attacks on security protocols of 5G:

1) **5G-AKA (Authentication and Key Agreement):**

While this is designed to provide high security, like all communica tion methods, it will also be exposed to attacks. Here are some arguments against 5G-AKA: a) **Replay attack:** In a replay attack, the attacker intercepts and resends the correct authentication message. This may lead to credential reuse, which may lead to unauthorized access (Schamotta & Schamotta, 2023).

b) **Eavesdropping**: An attacker may attempt to eaves drop on communications between the UE and the network during authentication to obtain sensitive in formation that can be used to compromise security (Fortinet, 2023).

c) **Key Spoofing:** If an attacker controls the confident iality of keys exchanged during authentication, he will gain unauthorized access to secure communications between the UE and the net work.

2) **Service based architecture (SBA) Security:** Here are some considerations for specific attacks against 5G SBA (Singh, 2023):

a) **Service-Based Interface (SBI) Spoofing**: An attacker may attempt to exploit weaknesses in SBI to alter or control the communication of network functions. This may include impersonating a legitimate employee or injecting malicious content**.** b) **Dynamic network slice manipulation:** Since 5G SBA supports dynamic network manipulation, attackers may attempt to control the process of slices, resulting in unauthorized use or interfering with network connections.

c) **API exploits:** Services can be exposed to interest and APIs are targeted exploits. Attackers may attempt to exploit unsecured APIs to gain unauthorized access, insert malware, or perform other malicious actions (Walkowski, 2020).

3) Enhanced Subscriber Privacy: Here are some possible attacks that could target user privacy in 5G networks:

a) **Spoofing:** An attacker may attempt to impersonate a legitimate customer to access unauthorized services or obtain sensitive information, causing illegal activity, access to privacy-related information and services (Park et al., 2021).

b) **Interception of communication:** Interruption of communication between user equipment and the network to eavesdrop on sensitive data or control information. This affects the confidentiality and integrity of communications, leading to potential privacy breaches (McClanahan, 2022).

Fig 13. Eavesdrop attack (Illi, 2019)

V. Signalling System No. 7

Signaling System 7 (SS7) is a set of telecommunication protocols that are used to set up and manage telephone calls in a public switched telephone network (PSTN). Most of the public switched telephone network (PSTN) in the world is run by this set of signaling protocols (IEC, n.d.).

SS7 is used for various functions in telecommunication networks, including:

1. Call setup and teardown: SS7 is responsible for establishing, maintaining, and releasing connections for voice and data calls.
2. Number translation: It provides services such as local number portability, toll-free number translation, and short message service (SMS) signaling.
3. Mobility management: SS7 is used for tracking the location of mobile phone subscribers, enabling features like roaming.
4. Intelligent network (IN) services: It supports advanced telecommunication services, such as call forwarding, call waiting, and prepaid billing.
5. Packet-switched network access: SS7 can be used for signaling in packet-switched networks.

To transmit signaling messages between network nodes, SS7 uses a packet-switched network. The information in these messages is required for call setup and management.

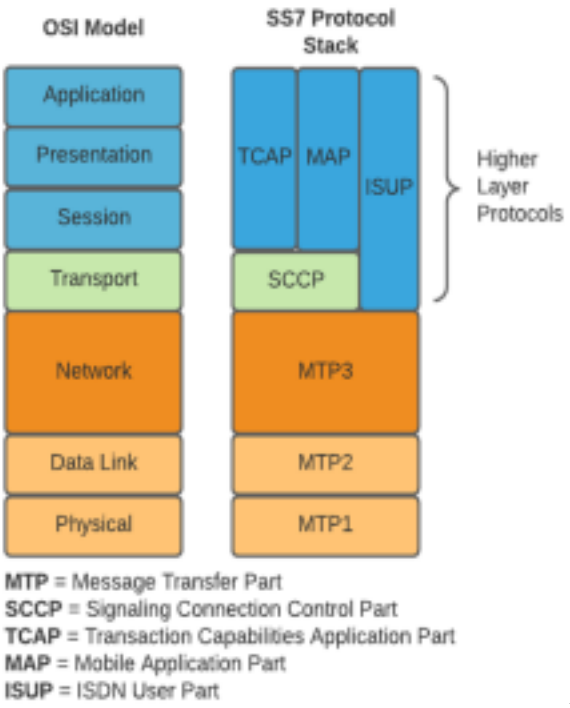


Fig 14. SS7 Protocol Layers (Nick, 2021)

SS7 Protocols:

SS7 comprises various protocols that operate within its layered architecture to facilitate different functionalities in telecommunications.

- *Message Transfer Part (MTP):*
  - MTP Level 1: Defines the physical layer characteristics, such as the electrical and mechanical properties of the signaling links (IEC, n.d.).
  - MTP Level 2: Provides error checking and correction functions for the reliable transmission of signaling messages. (IEC, n.d.).
  - MTP Level 3: Responsible for message routing and network management. It handles the signaling messages' routing through the network (IEC, n.d.).

- *Signaling Connection Control Part (SCCP):* SCCP provides additional routing and addressing capabilities beyond what MTP Level 3 offers. It allows more sophisticated addressing and message handling (IEC, n.d.).

- *ISDN User Part (ISUP):* ISUP is used for the setup, maintenance, and release of circuit-switched connections for voice calls on the PSTN. It operates between switches and is crucial for call related signaling (IEC, n.d.).

- *Transaction Capabilities Application Part (TCAP)*: TCAP is used for database queries and other transactional services in the SS7 network. It enables the exchange of non-circuit-related information between signaling points (IEC, n.d.).

- *Operations, Maintenance, and Administration Part (OMAP):* OMAP is responsible for managing, monitoring, and maintaining the SS7 network. It handles tasks related to the operational aspects of the network (IEC, n.d.).

- *Global Title Translation (GTT):* GTT is not a protocol itself but is part of the SS7 network. It involves the translation of global titles (phone numbers or other identifiers) into the corresponding signaling point code for routing purposes (IEC, n.d.).

These protocols work together to enable the various functions of SS7, including call setup, teardown, mobility management, and the provision of additional services. The structure and functions of SS7 protocols make it possible for different components in a telecommunication network to communicate and coordinate effectively.

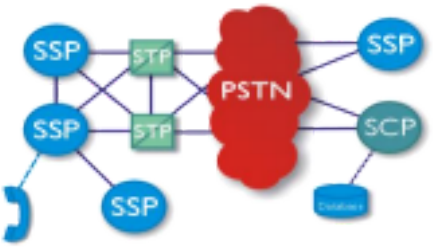


Fig 15. SS7 Nodes (Dialogic, 2018)

Service Switching Point (SSP):
Functionality: Initiates and terminates communication sessions (calls).
Role: Generates signaling messages to set up, manage, and release calls.

Signal Transfer Point (STP):
Functionality: Routes SS7 signaling messages between different signaling endpoints.
Role: Acts as a switch for SS7 messages, ensuring they reach their intended destination.

Service Control Point (SCP):
Functionality: Acts as a database or service logic provider.
Role: Provides information for call routing, service interactions, and other intelligent network functions.

These nodes collectively contribute to the proper functioning of SS7, enabling essential features such as call routing, subscriber authentication, and the provision of intelligent network services (IEC, n.d.).

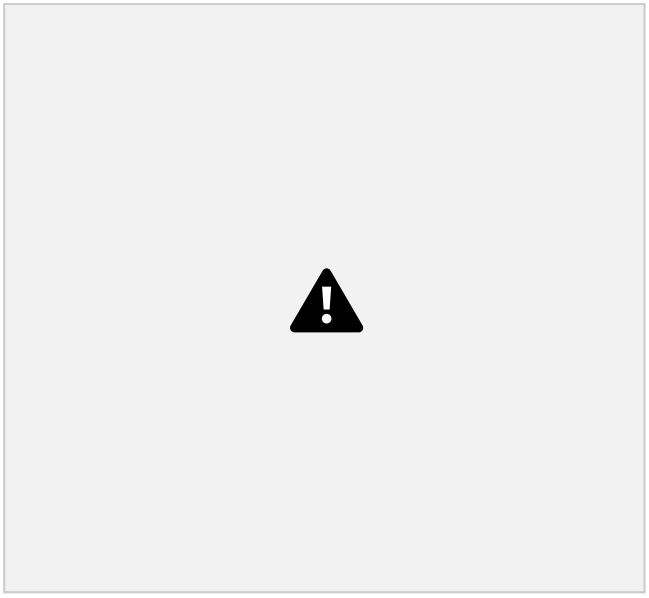


Fig 16. SS7 Working (Ullah et al., 2020)

- *Mobile Switching Center (MSC)*: The MSC is a central component in the GSM network that manages the switching functions for calls. It interfaces with the SS7 network for signaling purposes, handling call setup, teardown, and routing. The MSC communicates with other MSCs, Home Location Register (HLR), Visitor Location Register (VLR), and other network elements via SS7 signaling (Ullah et al., 2020).

- *Visitor Location Register (VLR):* The VLR is responsible for temporarily storing information about subscribers currently within a specific geographic area or under the jurisdiction of a particular MSC. It communicates with the HLR and other VLRs using SS7 signaling to retrieve subscriber information and update location information (Ullah et al., 2020).
- *Home Location Register (HLR):* The HLR is a central database that stores subscriber information, including subscriber profiles, current locations, and services subscribed to. It communicates with the VLRs and MSCs using SS7 signaling for call routing, subscriber authentication, and service provisioning (Ullah et al., 2020).

- *Authentication Center (AUC):* The AUC is responsible for subscriber authentication and generating encryption keys. It communicates with the MSC and HLR using SS7 signaling to provide secure authentication of mobile subscribers (Ullah et al., 2020).

- *Equipment Identity Register (EIR):* The EIR communicates with the MSC and HLR using SS7 signaling to exchange information about mobile devices, specifically their International Mobile Equipment Identity (IMEI) numbers. This helps prevent the use of stolen or unauthorized devices in the network (Ullah et al., 2020).

- *Short Message Service Center (SMSC):* The SMSC is responsible for handling SMS (Short Message Service) messages in the GSM network. It communicates with the MSC and HLR using SS7 signaling for SMS delivery and related functions (Ullah et al., 2020).

Vulnerabilities in Signaling System No. 7

SS7 (Signaling System No. 7) has gained notoriety due to a vulnerability that allows for SMS interception, posing a threat to the confidentiality of communications. In this exploit, attackers identify a target's phone number and then exploit weaknesses in the SS7 network to impersonate the target's mobile device. This involves sending deceptive signaling messages to the network (Kreitzman, 2023).

A trust model that presumes operator cooperation, weak authentication, restricted security measures, and an antiquated design make SS7 susceptible. Security against contemporary cyber threats was not given priority in its heritage design, which was created in a different era. Due to its intrinsic design flaws and the increasing interconnectivity of digital networks, SS7 is vulnerable to attack, enabling message and call interception by adversaries. While there are continuous efforts to resolve these vulnerabilities, putting in place thorough security measures is difficult due to the extensive worldwide infrastructure based on SS7.

Here's a simplified example of how this vulnerability can be exploited (Kreitzman, 2023):

1. Attacker identifies the target phone number: The attacker needs to know the target's phone number to intercept SMS messages.
2. Initiating the attack: The attacker leverages weaknesses in the SS7 network to impersonate the target's mobile device. This often involves sending fraudulent signaling messages to the network.
3. Intercepting SMS messages: Once the attacker has successfully impersonated the target, they can intercept and read SMS messages meant for the target. This can include two-factor authentication (2FA) codes and other sensitive information sent via SMS.
4. Unauthorized access: With access to the target's SMS messages, the attacker can potentially gain unauthorized access to various accounts and services associated with the target's phone number.

It's important to note that SS7 vulnerabilities have been widely discussed in the cybersecurity community, and telecommunications companies have been working on improving the security of their networks to mitigate these risks. However, these vulnerabilities serve as a reminder of the importance of securing the telecommunication infrastructure and using alternative methods, such as app based authentication, for sensitive communications and two factor authentication (Kreitzman, 2023).

Discovery of Subscribers Location

An illustrative example of SS7 Location Based Services involves the Location Based Service (LBS) application

initiating a MAP-Anytime-Interrogation (ATI) request to the subscriber's Home Location Register (HLR), using the Mobile Subscriber ISDN (MSISDN) as input. This prompts the HLR to send a MAP-Provide-Subscriber-Info (PSI) Request to the serving MSC/VLR. The MSC/VLR, in turn, initiates a paging procedure to obtain the most up-to-date location information. Following receipt of the updated location details in the paging response, the MSC/VLR generates a PSI Response and forwards it to the HLR. The HLR uses the PSI information to create an ATI Response, which is then transmitted to the requesting LBS application. The ATI Response contains Cell Global Identity (CGI) details, including Cell Id, Mobile Country Code (MCC), Mobile Network Code (MNC), and Location Area Code (LAC). This CGI information can be utilized to determine the longitude and latitude of the subscriber, with web applications available to map these coordinates. In urban areas, the location accuracy can be within a few hundred feet due to the proximity of cell sites.

.

Fig 17. Short Message service call flow (Cellusys, 2022)

According to the details provided in the depicted threat labeled "Subscriber Identity Disclosure," the location information of a subscriber can be acquired without resorting to the use of the ATI message.

Purpose of Attack:

1. Access to the SS7 Network – easily obtainable 2. Capability to generate SS7 messages – accessible through open-source means.
3. Knowledge of the IMSI of the target subscriber 4. Knowledge of the address of the Serving MSC/VLR

The basis for this attack involves the intruder masquerading as an HLR and sending a MAP-Provide-Subscriber-Info (PSI) Request message directly to the MSC/VLR currently serving the subscriber. This exploit is feasible because, in a prior threat scenario, the intruder obtained both the address of the MSC/VLR and the IMSI of the targeted subscriber.

Fig 18. Threat setup (Cellusys, 2022) **Attack Sequence:**

Attack Sequence: In this situation, the malicious actor assumes the role of an HLR with the intention of obtaining the current location details of a subscriber. The intruder generates a MAP-PSI (Req.) message and dispatches it to the Gateway STP, directing it toward the Serving MSC/VLR. This message contains the IMSI of the subscriber, specifying the targeted user. Subsequently, once the MSC/VLR updates the subscriber's location information, it formulates and transmits a MAP-PSI (Resp.) message, revealing the requested location information to the deceptive "Fake HLR."

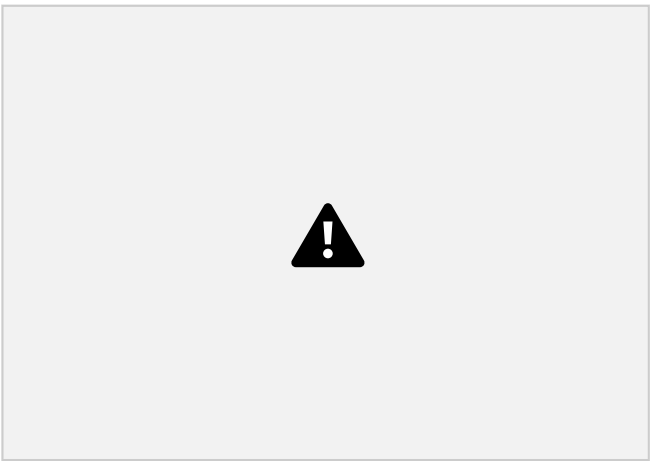


Fig 19. Subscriber Identity disclosure call flow (Cellusys, 2022)

Outcome of the Attack:

Following the attack, the intruder obtains the following details pertaining to the location of the targeted subscriber.

1. Cell Id.
2. Mobile Country Code (MCC)
3. Mobile Network Code (MNC)
4. Location Area Code (LAC)

VI. Implementation of Attacks on Signalling System No. 7

The SS7 protocol is not safe and is readily broken into by hackers. The SS7 network protocol does not yet have a well established security system, which means that a hacker with access to the network can read your texts, listen to your phone calls, and even track your whereabouts. Even the two-factor authentication can be circumvented by a hacker simply intercepting the user's allocated SMS.

In addition, the hacker has access to the user's online banking and social media accounts after intercepting the SMS message (Steiner et al., 2019).

SigPloit

A project called SigPloit intends to assist telecom security researchers, telecom pen-testers, and even operators who are eager to improve their posture so they can test against a variety of vulnerabilities related to infrastructure. The framework's objective is to give current risks for the many signalling protocols that are employed in a mobile network (Steiner et al., 2019).

Our Approach

Simulation Mode

You can use the simulation mode to gain an understanding of attacks in the event that you are unable to access the SS7 network. The server-side **.jar** files are under **"SigPloit/Testing/Server/Attacks/"**. In order to replicate an attack on the client, you must use the hard-coded values for each server-side attack (Mahar, 2021).

Determining the subscriber's location

To find a subscriber's location within the worldwide mobile network, there are at least two SS7 methods available. The first gets the subscriber's location parameters by using a message and process called Any Time Interrogation. A significant portion of network operators, nonetheless, have disabled their devices' ability to reply to these signals. Next, the attacker uses the standard MAP messages and procedures known as Provide Subscriber information while posing as a Fake Home Location Register. After this process, the target subscriber's current position is determined by the information obtained, which includes the Cell ID, Mobile Network Code (MNC), Mobile Country Code (MCC), and position Area Code (Cleary, 2020).

Sigploit Installation

Requirements:

1. Python 2.7
2. Java Version 1.7+
3. Linux Machine

We will be using this GitHub repository to simulate the attack:

https://github.com/ethicalhackeragnidhra/SigPloit-ss7

As we will use the machine both as server and client, we need to set two Ips' of the same network on localhost (Rifky The Cyber, 2022).

1. Location Tracking Attack

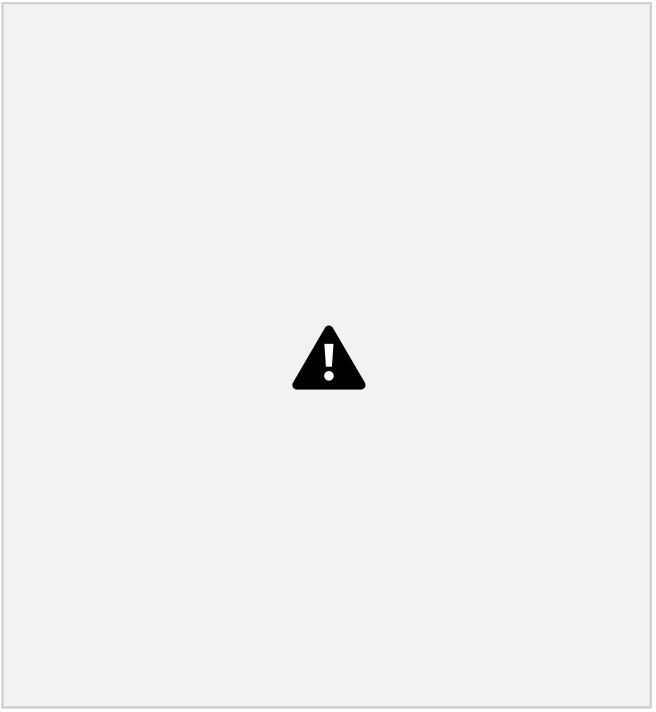


Fig 20. Location Tracking Attack using AnyTimeInterrogation

After initializing the attack, we will open Wireshark to intercept the location. We invoke AnyTimeInterrogation with the location request and we will get the acknowledgment SACK AnyTimeInterrogation with the Location of the target (Rifky The Cyber, 2022).

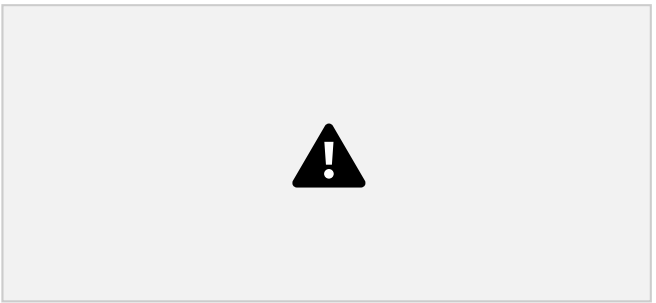


Fig 21. Wireshark output after initializing the location tracking attack

And the result is stored in HLR.

Fig 22. Output of the Target's Info and Location

Fig 23. Target's Location in Google Map using Latitude and Longitude

2. Phishing Mail (Fraud)

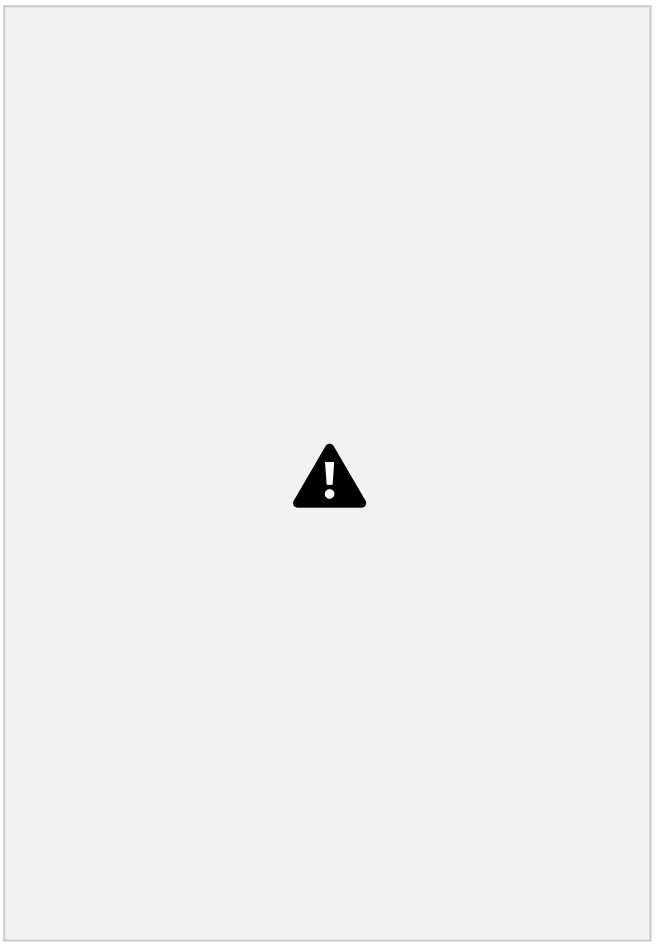


Fig 24. Phishing mail attack

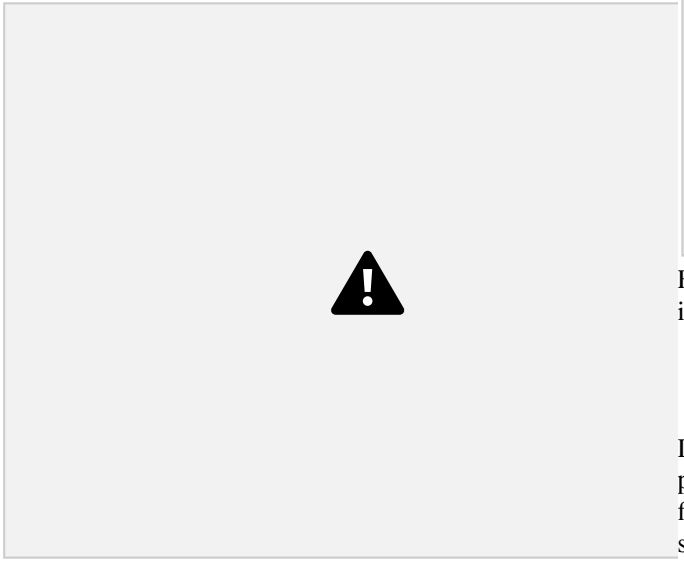


Fig 25. Wireshark output after initializing the phishing mail attack

3. SMS Interception:

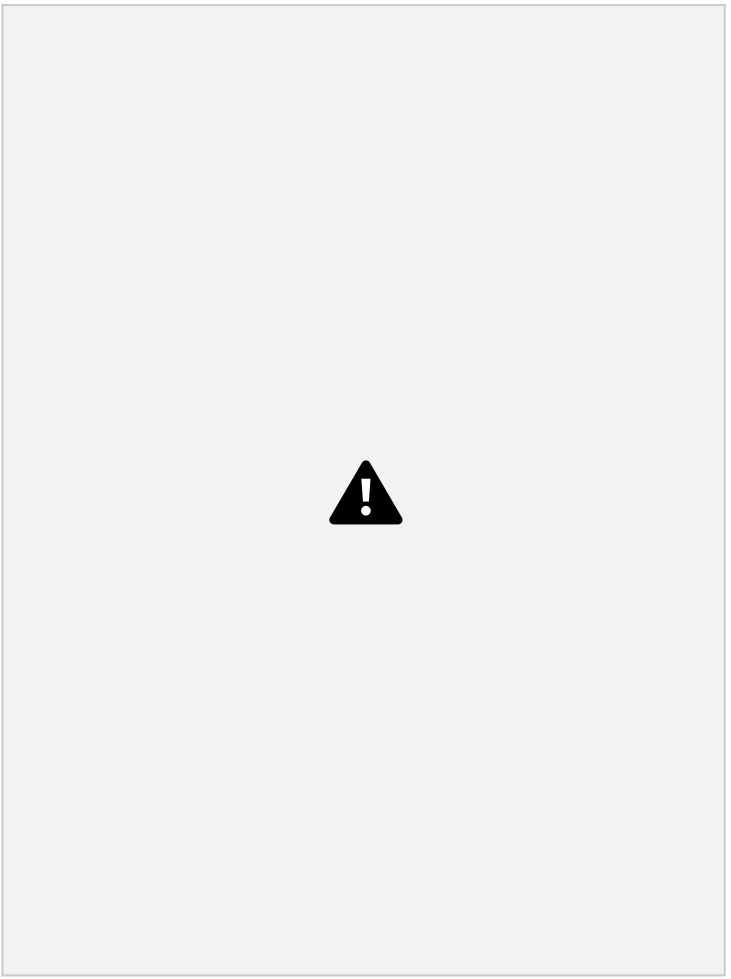


Fig 26. SMS Interception Attack

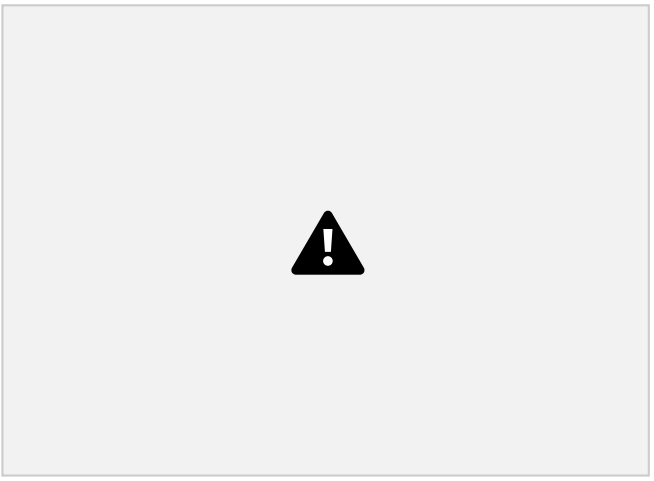


Fig 27. Wireshark output after initializing the SMS interception attack.

VII. Summary And Conclusions

Due to the vast worldwide infrastructure built around this protocol, even though SS7 vulnerabilities are well known, fixing them is a difficult undertaking. Work to improve the security of SS7 networks and add further protections is

being done by the telecommunications industry. As a result, industry and regulatory organizations are working to develop better secure signaling protocols for contemporary telecommunications. In the interim, industry understanding of these vulnerabilities is vital.

References

Abdel-Malek, M. A., Sayed, M. M., & Azab, M. (2022). UAV-Based Privacy-Preserved trustworthy seamless service agility for NextG cellular networks. *Sensors*, *22*(7), 2756. https://doi.org/10.3390/s22072756

Agrawal, J., Patel, R., Mor, P., Dubey, P., & Keller, J. (2015). Evolution of Mobile Communication Network: from 1G to 4G. *International Journal of Multidisciplinary and Current Research*, *3*. http://ijmcr.com/wp content/uploads/2015/11/Paper11100-11031.pdf

Bartock, M., Cichonsk, J., & Franklin, J. (2013). LTE Security – How Good Is It. In *csrc.nist*. NIST. https://csrc.nist.gov/CSRC/media/Presentations/LTE-Security-How-Good is-it/images-media/day2_research_200-250.pdf

Bhis. (2022, December 1). *GSM traffic and encryption: A5/1 Stream cipher*. Black Hills Information Security. https://www.blackhillsinfosec.com/gsm-traffic-and-encryption-a5-1-stream-cipher/

CableLabs. (2019, March 7). *A comparative introduction to 4G and 5G authentication - CableLabs*. https://www.cablelabs.com/insights/a comparative-introduction-to-4g-and-5g authentication#:~:text=4G%20EPS%2DAKA,-The%20EPS%2DAKA&text=An%20AV%20consists%20of%20an,UE%2C%20including%20the%20AUTH%20token

Cellusys. (2022, October 23). SS7 Firewall - Cellusys. https://www.cellusys.com/products/cellusys-protect/ss7-firewall/

Cleary, B. (2020, January 2). *8 SS7 vulnerabilities you need to know about*. Cellusys. https://www.cellusys.com/2015/10/20/8-ss7-vulnerabilities-you need-to-know about/?fbclid=IwAR12ukFS6LCfuX94tRJKWlSdWiXhQ5lxbS7RPj9gqlaa mtrtGQkSkIGxIx4

Comodo Security Solutions. (2022, June 16). DDoS attack Definition. *Cwatch Web Security*. https://cwatch.comodo.com/ddos-attack definition.php

Dai, N. H. P., & Nguyen, D. D. (2021). Drone Application in Smart Cities: The General Overview of security Vulnerabilities and Countermeasures for Data communication. In *Studies in systems, decision and control* (pp. 185–210). https://doi.org/10.1007/978-3-030-63339-4_7

Dangi, R., Lalwani, P., Choudhary, G., You, I., & Pau, G. (2021). Study and Investigation on 5G Technology: A Systematic review. *Sensors*, *22*(1), 26. https://doi.org/10.3390/s22010026

Dialogic. (2018). *Public Network Signaling Tutorial*. https://dialogicoriginal.na1.teamsupport.com/knowledgeBase/19010306

Ekdahl, P., & Johansson, T. (2003). Another attack on A5/1. *IEEE Transactions on Information Theory*, *49*(1), 284–289. https://doi.org/10.1109/tit.2002.806129

Ericsson. (2023). *A guide to 5G network security 2.0*. https://www.ericsson.com/en/security/a-guide-to-5g-network-security

ETSI. (2020). 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.3.0 Release 16). In *Etsi*. https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf

ETSI. (2023). 5G; 5G System; Network Slice-Specific Authentication and Authorization (NSSAA) services; Stage 3 (3GPP TS 29.526 version 16.0.0 Release 16). In *Etsi*. https://www.etsi.org/deliver/etsi_ts/129500_129599/129526/16.00.00_60/ts_129526v160000p.pdf

Evans, J. (2023). *Security challenges in the 3G sunset era: Protecting your IoT infrastructure*. Yourcommsgroup. https://www.yourcommsgroup.com/news/security-challenges-in-the-3g sunset-era-protecting-your-iot-infrastructure?hsLang=en

Fortinet. (2023). *What are eavesdropping attacks? | Fortinet*. https://www.fortinet.com/resources/cyberglossary/eavesdropping

Galazzo, R. (2022, July 28). *Timeline from 1G to 5G: A Brief History on Cell Phones - CENGN*. CENGN. https://www.cengn.ca/information centre/innovation/timeline-from-1g-to-5g-a-brief-history-on-cell-phones/

Gawas, A. U. (2015). An overview on evolution of mobile wireless communication networks: 1G-6G. *International Journal on Recent and Innovation Trends in Computing and Communication*, *3*(5). https://doi.org/10.17762/ijritcc.v3i5.4404

GeeksforGeeks. (2022, November 13). *5G Network Architecture*. https://www.geeksforgeeks.org/5g-network-architecture

Gong, X., & Zhang, B. (2021). Comparing large-unit and bitwise linear approximations of SNOW 2.0 and SNOW 3G and related attacks. *IACR Transaction on Symmetric Cryptology*, 71–103. https://doi.org/10.46586/tosc.v2021.i2.71-103

GSM Security. (2010). *What algorithm is utilized for encryption in GSM networks?* https://www.gsm-security.net/faq/gsm-encryption-algorithm-a5-cipher.shtml

IEC. (n.d.). *Signaling System 7 (SS7)*. The International Engineering Consortium. https://people.cs.rutgers.edu/~rmartin/teaching/fall04/cs552/readings/ss7.pdf

Illi, E. (2019). On the Performance Analysis of Optical Wireless Communication Systems [Ph. D. degree]. Mohammed V University Rabat. https://www.researchgate.net/publication/343239565_On_the_Performance_Analysis_of_Optical_Wireless_Communication_Systems

Kaur, K. (2022). *Signaling System 7*. Topcoder. https://www.topcoder.com/thrive/articles/signaling-system-7

Kheddar, H. (2022, October 2). *From 2G to 4G Mobile Network: architecture and key performance Indicators*. arXiv.org. https://arxiv.org/abs/2210.00642

Köksal, S. (2021, December 12). Evolution of Core Network(3G vs. 4G vs. 5G) - Sarp Köksal - Medium. *Medium*. https://medium.com/@sarpkoksal/core-network-evolution-3g-vs-4g-vs-5g 7738267503c7

Kreitzman, M. (2023). SS7 Attack: What is it, how SS7 attack works, and prevention techniques. https://www.efani.com/blog/ss7-attack

Kumar, P. (2022, August 24). *Man-In-The-Middle Attack (MITM)*. https://www.linkedin.com/pulse/man-in-the-middle-attack-mitm-pankaj kumar/

Kumar, T. S., & Prabakaran, S. (2019). Security and Privacy enforced wireless mobile communication using PI-MAKA protocol design. *Measurement & Control*, *52*(7–8), 788–793. https://doi.org/10.1177/0020294019842893

Lu, X., Yang, F., Zou, L., Lio, P., & Hui, P. (2023). An LTE Authentication and Key Agreement Protocol Based on the ECC Self Certified Public Key. IEEE/ACM TRANSACTIONS ON NETWORKING, 31(3). https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9903404

s

Mahar, B. (2021, July 7). *3G: Practical attacks against the SS7 signaling Protocol*. Kroll. https://www.kroll.com/en/insights/publications/cyber/3g practical-attacks-against-the-ss7-signaling-protocol

McClanahan, P. (2022, November 1). *1.4 Attacks - Types of attacks*. Engineering LibreTexts. https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.4_Attacks_-_Types_of_Attacks

Monem, M. A. (2023, March 17). *What is Service Communication Proxy (SCP) in 5G? - Moniem-Tech*. Moniem-Tech. https://moniem tech.com/questions/what-is-service-communication-proxy-scp-in-5g

Muppavaram, K., Govathoti, S., Kamidi, D., & Bhaskar, T. G. (2023). Exploring the Generations: A Comparative Study of Mobile Technology from 1G to 5G. *SSRG International Journal of Electronics and Communication Engineering*, *10*(7), 54–62. https://doi.org/10.14445/23488549/ijece-v10i7p106

Nguyen, P. H., Robshaw, M. J. B., & Wang, H. (2011). On Related-Key attacks and KASUMI: the case of A5/3. In *Lecture Notes in Computer Science*. https://doi.org/10.1007/978-3-642-25578-6_12

Nick. (2021). *Demystifying SS7 & Sigtran Networks (With Labs!) – Part 1 – Intro | Nick vs Networking*. https://nickvsnetworking.com/practical-ss7-sigtran-with-labs-part-1-intro/

Njoroge, F. (2019). A Survey of Cryptographic Methods in Mobile Network Technologies from 1G to 4G. *Jkuat*. https://www.academia.edu/38873002/A_Survey_of_Cryptographic_Methods_in_Mobile_Network_Technologies_from_1G_to_4G

P Halagali, B., & V Desai, V. (2017). Review Paper on Cryptosystems used in Cellular Networks. *International Journal of Computer Science and Mobile Computing*, *6*(4), 385–388. https://ijcsmc.com/docs/papers/April2017/V6I4201799a5.pdf

Park, S., Kim, D., Park, Y., Cho, H., Kim, D., & Kwon, S. (2021). 5G Security Threat Assessment in real networks. *Sensors*, *21*(16), 5524. https://doi.org/10.3390/s21165524

Pereira, V. (2014). *Evolution of Mobile Communications: from 1G to 4G*. https://www.semanticscholar.org/paper/Evolution-of-Mobile Communications%3A-from-1G-to-4G-Pereira Sousa/2d2a30bc1824ceb732b22288af82baa732d5c0e9

PortSwigger. (2023). *Unencrypted communications*. https://portswigger.net/kb/issues/01000200_unencrypted-communications

Prasad, A. R., Arumugam, S., Sheeba, B., & Zugenmaier, A. (2018). 3GPP 5G Security. *Journal of ICT Standardisation*, *6*(1), 137–158. https://doi.org/10.13052/jicts2245-800x.619

Proofpoint. (2023, October 12). *What is a Man-in-the-Middle Attack? MITM Attacks explained | ProofPoint US*. https://www.proofpoint.com/us/threat-reference/man-in-the-middle-attack mitm

Ramadan, M., Li, F., Xu, C., & Abdalla, A. (2016). User-to-user mutual authentication and key agreement scheme for LTE cellular system. *ResearchGate*. https://www.researchgate.net/publication/290482085_User to user_mutual_authentication_and_key_agreement_scheme_for_LTE_cellular_system

Rao, S. P., Holtmanns, S., & Aura, T. (2023). Threat modeling framework for mobile communication systems. *Computers & Security*, *125*, 103047. https://doi.org/10.1016/j.cose.2022.103047

Remmert, H. (2020, May 20). 4G to 5G: How Long Will 4G LTE Be Available? *Digi*. https://www.digi.com/blog/post/4g-to-5g-how-long-will 4g-lte-be-available

Rifky The Cyber. (2022, September 30). *Part 1: how to trigger SS7 AnytimeInterrogation from our computer* [Video]. YouTube. https://www.youtube.com/watch?v=-_7_wKhzY2A

Rupprecht, D., Kohls, K., Holz, T., & Pöpper, C. (2020). IMP4GT: IMPersonation Attacks in 4G NeTworks. Network and Distributed Systems Security (NDSS) Symposium 2020. https://doi.org/10.14722/ndss.2020.24283

Salahdine, F., Han, T., & Zhang, N. (2022). Security in 5G and beyond recent advances and future challenges. *Security and Privacy*, *6*(1). https://doi.org/10.1002/spy2.271

Schamotta, J., & Schamotta, J. (2023, November 10). *What is a replay attack?* Comparitech. https://www.comparitech.com/blog/information security/what-is-a-replay-attack/

Shaker, N. H., Issa, H. H., Shehata, K., & Hashem, S. N. (2013). Design of F8 encryption algorithm based on customized Kasumi Block Cipher. *International Journal of Computer and Communication Engineering*, 398–402. https://doi.org/10.7763/ijcce.2013.v2.213

Singh, J. (2023, August 24). *Known-plaintext attacks, explained*. Cointelegraph. https://cointelegraph.com/explained/known-plaintext attacks-explained

Singh, N. (2023). *What is the 5G Service-Based Architecture (SBA)?* TECHCOMMUNITY.MICROSOFT.COM. https://techcommunity.microsoft.com/t5/azure-for-operators-blog/what-is the-5g-service-based-architecture-sba/ba-p/3831367

Skill Lync. (2022a, December 16). 5G Service Based Architecture & Network Functions (EP.1) | 5G Architecture Explained | Skill-Lync [Video]. YouTube. https://www.youtube.com/watch?v=-v7gISwfm9I

Skill Lync. (2022b, December 20). *What does the AMF do? (Ep.3) | 5G Architecture Explained | Skill-Lync* [Video]. YouTube. https://www.youtube.com/watch?v=21LHZMD0hsE

Skill Lync. (2022c, December 23). *What is the role of SMF in 5G Core Networks? (Ep.4) | 5G Architecture Explained | Skill-Lync* [Video]. YouTube. https://www.youtube.com/watch?v=j8s8fodbn_4

Skill Lync. (2022d, December 25). *UPF in 5G Core Networks (EP.5) | User Plane Function | 5G Architecture explained | Skill-Lync* [Video]. YouTube. https://www.youtube.com/watch?v=zcvFsb0v32c Skill Lync. (2022e, December 27). UDM in 5G Core Networks? (EP.6) | Unified Data Management | 5G Architecture Explained | Skill-Lync [Video]. YouTube. https://www.youtube.com/watch?v=PCqFLN2N_ps

Skill Lync. (2022f, December 29). *What is AUSF in 5G Core Networks? (Ep.8) | 5G Architecture Explained | Skill-Lync* [Video]. YouTube. https://www.youtube.com/watch?v=HLRxbWgGgMI

Sonal, & Upasna, U. (2018). Mobile phone cloning. *IJERT*, *3*(10). https://doi.org/10.17577/IJERTCONV3IS10043

Steiner, B., Escoto, L., Sefa, E., & George, J. (2019). Exploring the inherent vulnerabilities in SS7 technology using SigPloit. In *Cysecure.org*. http://cysecure.org/560/online/project/sigploit_brianSteiner_joyGeorge_louisEscoto_emmanuelSefa.pdf

Report Contribution :

Role 1: Evolution of Cellular Networks

Ullah, K., Rashid, I., Afzal, H., Iqbal, W., Bangash, Y. A., & Abbas, H. (2020). SS7 Vulnerabilities—A Survey and Implementation of Machine Learning vs Rule Based Filtering for Detection of SS7 Network Attacks. *IEEE Communications Surveys and Tutorials*, *22*(2), 1337–1371. https://doi.org/10.1109/comst.2020.2971757

Walkowski, D. (2020, August 6). *Securing APIs: 10 Best practices for keeping your data and infrastructure safe | F5 Labs*. F5 Labs. https://www.f5.com/labs/learning-center/securing-apis-10-best-practices for-keeping-your-data-and-infrastructure-safe

Wickr. (2023, February 28). *Why Your 2G Cellphone Network Data Encryption was Intentionally Weakened*. AWS Wickr. https://wickr.com/why-your-2g-cellphone-network-data-encryption-was intentionally-weakened/

Wright, G. (2021, June 4). *Signaling System 7 (SS7)*. Networking. https://www.techtarget.com/searchnetworking/definition/Signaling-System 7

Zontou, E. (2023). Unveiling the evolution of mobile networks: from 1G to 7G. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2310.19195

https://github.com/SigPloiter/SigPloit

Mohik Jaswal (40224737), Jaykit Rameshbhai Kukadiya (40261905)

Role 2: Security Protocols Used at Different Stages/Versions

Rhea Sharma (40221493), Sanjana Farial Oishee (40276253)

Role 3: Attacks on Security Protocols

Taran Ahuja (40258445), Sidharth Sunil (40279959), Muhammad Bilal ALi (40259265)

Role 4: Signaling System No. 7

Sriprada Sridhara Murthy (40202429), Tashlima Rashid (40218648)

Role 5: Implementation of Attacks on Signaling System No. 7

Salahuddin Ahmed Sabbir (40118011), Damandeep Singh (40232416)