Security Measures in Cellular Networks: How Good Are They

***Abstract*—Numerous applications, including online banking, mobile payments, and real-time information sharing, are made possible by cellular networks, which are becoming an essential component of contemporary communication systems. But the increased dependence on these networks has made them vulnerable to serious security threats. The security features and weaknesses of the three main cellular network generations—GSM, LTE, and 5G—are surveyed in this study. We analyze the architecture of these networks, and investigate the attacks which are possible against these networks such as eavesdropping, rogue base stations, and cryptographic breaches and survey the security mechanism of these networks. Finally, we have reviewed the security mechanism of all the networks.**

I. Introduction

The growth of cellular networks, from GSM to LTE and now 5G, has transformed worldwide communication by providing quicker and more dependable access. However, this advancement has created severe security challenges. Protecting user privacy, preserving data integrity, and ensuring service availability are vital since these networks power critical systems such as healthcare and finance. GSM established the groundwork for basic encryption, LTE enhanced security with mutual authentication and stronger protocols, and 5G brought sophisticated safeguards to solve earlier flaws and counter emerging threats from increasing connectivity and IoT integration. Despite these developments, cellular networks remain vulnerable to assaults such as eavesdropping, impersonation, and denial-of-service. This article discusses GSM, LTE, and 5G networks, examines their security measures, assesses their effectiveness in reducing attacks, and analyses their weaknesses. It examines the strengths and shortcomings of each generation, using real-world examples, and analyses how future networks can improve security.

II. GSM

A. Overview of GSM Network Architecture

The architecture of a GSM network is divided into several functional components, each designed for specific purposes. Figure 1 illustrates the key components of the GSM network, which can be broadly categorized into three main sections: the Mobile Station (MS), the Base Station Subsystem (BSS), and the Switching System (SS). [1]

- **Mobile Station (MS)** : The Mobile Station consists of two essential parts:
  - **Mobile Equipment (ME)**: A portable, handheld, or vehicle-mounted device uniquely identified by its IMEI (International Mobile Equipment Identity).

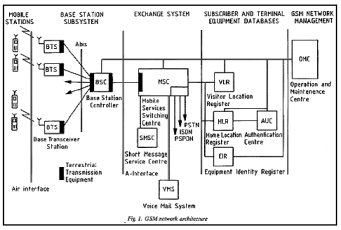

Fig. 1. GSM Architecture [1]

  - **Subscriber Identity Module (SIM)**: A smart card that contains the IMSI (International Mobile Subscriber Identity). It enables users to make and receive calls and access subscribed services. The SIM card is secured by a PIN and can be transferred between devices, carrying the necessary information to activate the phone.
  - **Base Station Subsystem (BSS)**: A smart card that contains the IMSI (International Mobile Subscriber Identity). It enables users to make and receive calls and access subscribed services. The SIM card is secured by a PIN and can be transferred between devices, carrying the necessary information to activate the phone.
- **Base Station Subsystem (BSS)** : The BSS is responsible for managing radio-related functions and comprises the following components:
  - **Base Station Controller (BSC)** : This component manages control functions and physical connections between the MSC and BTS. It acts as a high-capacity switch, handling tasks like handovers, cell configuration data, and regulating RF power levels in the BTS. A single MSC can serve multiple BSCs.
  - **Base Transceiver Station (BTS)**: This equipment establishes the radio interface with the mobile station. It includes the necessary transceivers and antennas to serve individual cells in the network. A BSC controls a group of BTSs.
- **Switching System (SS)** : The Switching System handles call processing and subscriber management tasks. It includes the following units:
  - **Home Location Register (HLR)**: A critical database for storing and managing subscription data. It main-

tains permanent subscriber information, including service profiles, location data, and activity status. When a user subscribes to a network operator, their details are recorded in the operator's HLR.

- **Mobile Services Switching Center (MSC)**: The MSC is the core telephony switch, managing call routing between different telephone and data systems. It also oversees functions like toll ticketing, network interfacing, and common channel signaling.
- **Visitor Location Register (VLR)**: A temporary database integrated with the MSC that stores information about roaming subscribers. When a mobile device enters a new MSC area, the VLR requests details from the HLR. This ensures call setup can occur without repeatedly querying the HLR.
- **Authentication Center (AUC)**: The AUC generates authentication and encryption parameters to verify subscriber identity and maintain call confidentiality. It also safeguards operators against fraud.
- **Equipment Identity Register (EIR)**: The EIR is a database containing details about mobile equipment to prevent unauthorized, stolen, or faulty devices from accessing the network. The AUC and EIR can be implemented as standalone units or combined into a single node.

B. Security Measures in GSM

- **Authentication**:
  - **Generating authentication vectors**: Before understanding how the authentication works in GSM, we need to understand how the authentication vectors or security parameters are generated. The two key elements in our network dealing with authentication are
    - SIM - Subscriber Identity Module
    - AuC - Authentication Center

    Inside both elements we use 2 mathematical algorithms called A3 and A8. These algorithms are secret and are specific to given service providers. There is also a 128 bit subscriber authentication key which is present in both of them which is called Ki.
    In AuC, a random number termed RAND is generated, which is fed to A3 and A8 algorithms to generate SRES (Signal Response) and Kc (cipher key) respectively. (Please refer to the image below). Thus, SRES, Kc and RAND together are termed as authentication vector. [1]
  - **Working of Authentication in GSM**:
    1) Initiating the Authentication Process: When a mobile device (user) attempts to connect to the network, it sends its IMSI (International Mobile Subscriber Identity).
    2) Processing at AuC: Upon receiving the IMSI, the network checks its database to retrieve the subscriber's secret key (Ki) from the Authentication Center (AuC) and calculate the Random number (RAND), Signal response (SRES) and Cipher Key (Kc).
    3) Processing at SIM: The MSC sends the authentication request to the Mobile station and this request message contains RAND. This RAND is used by SIM along with Ki to generate the SRES and KC using A3 and A8 algorithms. These values which are generated by the SIM card are sent back to MSC as a response.
    4) Verification at MSC: MSC then compares SRES generated by the SIM with the SRES which it got from AuC. If they are the same then the subscriber is authenticated.
    5) Establishing secure connection: The derived ciphering key Kc is used for encrypting communication between the mobile device and the network.

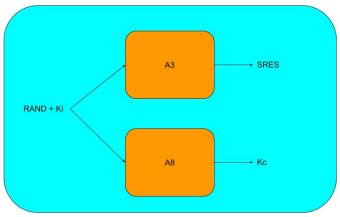

Fig. 2. Generation of SRES and Kc

- **Encryption**: Once the subscriber is authenticated, the cipher key Kc which is generated by SIM using RAND (Number generated by AuC) and Ki (subscriber authentication key) when fed to A8 Algorithm, is now used for encrypting the communication between mobile device and the network. Encrypted voice and data communication between the mobile station (MS) and the network is achieved using the A5 ciphering algorithm. The MSC will additionally store the encryption key in the base station (via the BSC) for use in encryption and decryption processes if the authentication result is accepted. The mobile system is then given an encryption mode command, or "test signal," by the BSC. The mobile system should respond by sending out an encrypted signal (encryption mode complete), which, if deciphered by the BSC, allows for ongoing communication and signalling. [3]

C. Attacks in GSM

- SIM Attacks: The GSM SIM is intended to be copy proof and tamper proof. But over the period of time, as more and more vulnerabilities of SIM are getting discovered, it no longer remain secure. The SIM cloning is possible and the attacker needs certain hardware and physical access to the target SIM. In particular, the attacker must have a SIM reader, a SIM software program, and a SIM chip writer [4] [6]. Physical SIM cloning is limited to the common and basic encryption algorithm called COMP128V1

[4] [6]. The COMP128v1 algorithm has weaknesses which allow an attacker to successfully mount a brute force attack and then extract the secret individual subscriber authentication key (Ki) of the SIM, along with the International Mobile Subscriber Identity (IMSI) and Integrated Circuit Card Identifier (ICCID). [7]

- Encryption : The A5/1 or A5/2 encryption algorithms are used to encrypt data in the GSM network. A5/0 is used in nations with political barriers to the provision of cryptographic hardware and does not employ encryption. The former Soviet Union and a few Middle Eastern nations are two examples of this. Mathematicians and cryptography experts have examined A5/1, which is supposedly the more robust of the two algorithms in use, and found it to be extremely vulnerable to cryptanalytic attacks. Several researchers such as M. Briceno, R. Anderson, M. Roe and J. Golic 9 also explored different aspects of the algorithm as well as different types of attacks on it. And these attacks have become the most widespread among those that are directed at the algorithm. Some examples of these attacks are the Baised Birthday Attack and the Random Sub graph Attack. The first attack requires two minutes of data and one minute of processing while the second attack two seconds of data and several minutes of processing. [2]
  The COMP 128 algorithm used for A3/A8 has many vulnerabilities and this makes it possible to obtain the Ki and the IMSI and these can be successfully used to program another [5]
- SMS Spoofing : SMS spoofing is a significant and realistic threat as it allows attackers to inject fraudulent SMS messages into the network using fake originator IDs. By sending an SMS from the internet with the correct headers, an attacker can impersonate a legitimate Mobile Equipment (ME). Since the ME cannot differentiate between a genuine message and one originating from the internet, it processes the message as legitimate, enabling the attacker to manipulate transactions as desired.
- Denial-of-Service (DoS) Attack : In mobile networks, flooding a device with SMS messages can render it ineffective by overloading the signaling layer, which handles essential network tasks. A specific form of this, the ”Silent” SMS DoS attack, goes unnoticed by the victim. Its symptoms include rapid battery drain and an inability to receive calls, as the signaling channel becomes clogged. This type of attack may be used for economic gain, to prevent communication between parties, or to ensure critical notifications are missed.

III. Conclusion

Security on a cellular network has advanced throughout the generations with each generation building on the weaknesses of the previous involving new security measures to counter new threats.

Mobile security was developed alongside the second-generation network, GSM which provided encryption and authentication features, however, these algorithms such as A5/1 and A5/2 are now susceptible, while self-authentication put users at risks such as. man-in-the-middle and IMSI catchers attacks. Its features security while great for that period has become obsolete with the gradual development of cyber threats.

LTE, fourth-generation network, has certainly advanced greatly from where GSM stood by providing features such as mutual authentication, more secured encryption protocols like AES and SNOW 3G and better key management strategies. The establishment of a secure signaling channel and IMSI exposure further guarded against the risks. Nonetheless, particular weaknesses remain flooding signaling member sessions, attacks on networks via downgrade to GSM and little safeguards against DoS attacks.

5G, being the most recent generation of cellular technology, represents a step forward regarding cellular security. It utilizes the progress made by LTE and includes impressive features like complete data encryption, improved mutual authentication, and privacy of identity through concealed subscription identifiers (SUCI). The deployment of network slicing security combined with a zero-trust architecture also enhances the security posture. Moreover, as growing threats like rogue base stations and attacks at the protocol level arise, 5G is made to be able to deal with those. It’s true that no one can say that it is invulnerable against sophisticated attacks, but the 5G security framework is the best so far.

The journey from GSM proceeds all the way to the fifth generation, which clearly suggests a trend that is quite clear: security mechanisms have certainly evolved and become more stronger. Every generation has dealt with the problems of the last, as the need for cybersecurity has risen in an interconnected world. However, advancing the technology comes with it a new set of problems such securing a complex IoT network in the 5th generation and AI assisted network management systems.

As much as it is true that GSM was an important stage in mobile security but its measures by today’s standards are not adequate. LTE represented an impressive step forward but still had gaps that had to be filled. This 5G era is characterized by a mature, at times even dynamic, security architecture, which goes a long way in advancing security in cellular networks. However, the majority of them are not impervious, and therefore augmenting the system constantly with research and monitoring through the boundaries of technology makes it ideal in relying on cellular networks in the current cyber threat environment.

REFERENCES

[1] Gurjeet Kaur, Pawansupreet Kaur, and Krishan Kumar Saluja. A review of security issues and mitigation measures in gsm. *International Journal of Research in Engineering & Applied Sciences*, 2(2):16, 2012.

[2] S Lord. Modern gsm insecurities. *X-Force Security Assessments White Paper*, 2003.

[3] David Margrave. Gsm security and encryption. *George Mason University*, pages 1–5, 1999.

[4] Jeremy Quirke. Security in the gsm system. *AusMobile, May*, pages 1–26, 2004.

[5] Josyula R Rao, Pankaj Rohatgi, Helmut Scherzer, and Stephane Tinguely. Partitioning attacks: or how to rapidly clone some gsm cards. In *Proceedings 2002 IEEE Symposium on Security and Privacy*, pages 31–41. IEEE, 2002.

[6] S Sidharsan. A complete guide to sim cloning.

[7] Jaspreet Singh, Ron Ruhl, and Dale Lindskog. Gsm ota sim cloning attack and cloning resistance in eap-sim and usim. In *2013 International Conference on Social Computing*, pages 1005–1010. IEEE, 2013.