Journal of Advanced Zoology
ISSN: 0253-7214
Volume 44 Issue S-8 Year 2023 Page 73-78

Private 5G, "Not As Private As You May Think"

V. C. Nimkar[1*], S. A. Pingle[2], K. N. Bhagat[3]

[1]Assistant Professor, Department Of Information Technology, Changu Kana Thakur Arts, Commerce and Science College, New Panvel Email:-vinit.nimkar@gmail.com*
[2] Department Of Information Technology, Changu Kana Thakur Arts, Commerce and Science College, New Panvel Email:-vinit.nimkar@gmail.com
[3] Department Of Information Technology, Changu Kana Thakur Arts, Commerce and Science College, New Panvel Email:-vinit.nimkar@gmail.com

***Corresponding Author:** V .C. Nimkar*
[*]Assistant Professor, Department Of Information Technology, Changu Kana Thakur Arts, Commerce and Science College, New Panvel Email:-vinit.nimkar@gmail.com

Abstract

As the need grows for mobile solutions that can offer more data throughput with ultra-reliable low-latency communications and better connection density—albeit at risk—private 5G networks and the shift to Industry 4.0 are gaining pace. As 5G technology develops and enterprises start implementing it, they need to be cautious during this transitional phase to make sure they are cognizant of and control risk as their attack surface changes. Many private 5G deployments use 4G/LTE Core networks in Non-Stand-Alone mode, which keeps many of the same vulnerabilities that have been there for years. As a result, private 5G is frequently not fully 5G pure. In this research paper, a few of the present-day weaknesses in the Stream Control Transmission and GPRS Tunnelling protocols—as well as the Industrial Control System protocols—that businesses need to be aware of and safeguard while using these technologies are discussed and shown.

Keywords :-5G , Network , Technology, Private

1. Introduction

The next evolutionary step in scaling out large Industrial Control System (ICS) networks is likely to be Private 5G (P5G). However, as organizations start to realize the advantages, it won't be long before these networks scale out to include more than just ICS endpoints, increasing the attack surface and creating new vulnerabilities. Although there are hazards associated with this new technology, it has the potential to change numerous sectors. Businesses need to know how to safely incorporate it into their existing architecture. Enterprise networks and cellular services integration is the union of two distinct technologies, and a successful implementation requires careful consideration of a number of aspects by enterprises. Businesses have to deal with these elements while preserving security in a threat environment that is getting more and more dangerous due to hostile actors who are always looking for ways to exploit weaknesses.

The phrase "Private 5G" is deceptive as well because it isn't always either "5G" or strictly "Private." 5G that is private may not always be such since corporate dataflows may occasionally exit an organization's network.

Depending on the deployment option chosen, this data may travel in an unencrypted state via infrastructure that is not owned by the business. If P5G data is transmitted through infrastructure that is not owned by the company, it can potentially expose organizations to risks, as malicious individuals can exploit this situation to gather knowledge and information about a network that would otherwise be restricted. The term 5G is not completely precise because many Mobile Network Operators (MNOs) still use Non-Stand-Alone (NSA) mobile networks, in which 4G/Long Term Evolution (LTE) is used for the control channel and 5G channels are added to enhance the connection for increased data transmission capacity.

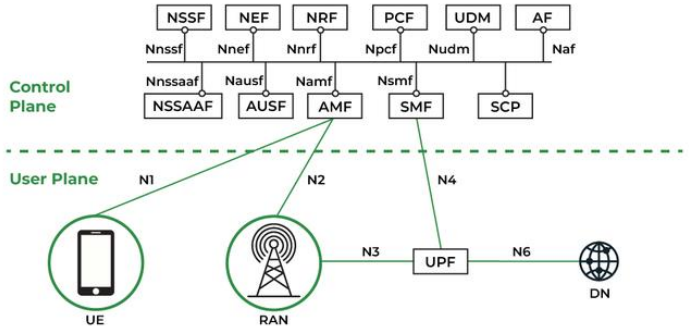

Fig 1. 5G Network Architecture

2. Methods and Equipment for Conducting Research

Advancements in the mobile phone industry have made it possible for security researchers to obtain readily available equipment and open-source software that can be used to test LTE/5G services. Although this assists in enhancing security in the industry, it also presents a two-sided situation as assailants can exploit the same methods to uncover weaknesses, create attacks, and potentially surveil cellular networks. Previously, due to the telecommunications industry's closed structure, the majority of security researchers faced great challenges in conducting independent tests on cellular technologies. This was primarily attributable to the high expenses involved in obtaining equipment and software, as well as the licensing requirements. Numerous open-source software projects and devices have resulted from the need for interoperable, open, and virtual solutions brought about by the growth of small mobile network operators (MNOs) serving rural areas and developing countries. The cellular industry is home to a number of open-source projects, including Magma, ORAN Alliance, srsRAN Project, and Open-Air Interface. Many software packages are available for free and can be integrated with software-defined radios that are easily accessible, like the low-cost LimeSDR produced by Lime Microsystems and the USRP family of radios from Ettus Research.

3. Research Limitations and Assumptions

The open-source software platform srsRAN was utilized in this experiment. Using the previous version of this program, known as srsLTE, in versions before to 21.04 (srsRAN 4G, 2023), was required due to compatibility constraints with the accessible LimeSDR. The Enterprise Packet Core (EPC) and Radio Access Network (RAN) suites needed to deliver cellular services can be operated using this software. The radios and antennas are connected to the RAN. Next, it transforms this radio data into General Radio Packet Service (GPRS) Tunnelling Protocol (GTP) Internet Protocol traffic, which it subsequently sends via Ethernet. the Core Network (CN) is reached. The CN is the system that establishes permission and authentication for mobile phones, also known as user equipment (UE). The Subscriber Identity Module (SIM) cards that the UEs use to authenticate themselves onto the mobile network are stored in a database that is maintained by the CN. Additionally, for UE data traffic traveling to the internet, the CN acts as the Packet Gateway (PGW).

4. Findings and Discussion

Before we begin, we must understand where we are and how we got here to set the stage for discussing existing and potential vulnerabilities within P5G. First, we will cover the history of cellular technologies and generations, followed by the evolution of LTE to the new 5G New Radio generation and the driver for the need to evolve current standards for use with new requirements and evolving Industry 4.0 use cases. Next, we will cover the two versions of P5G, NSA, and SA, the existing methods for deploying these services, either wholly

owned by the enterprise or wholly provided by an existing MNO, and the various hybrid deployment methods between the two. Following this, we will discuss the ports, protocols, use cases, and examples to demonstrate these protocols.

We will analyse the attack surface to discuss potential threats and vectors that attackers can use to inject traffic into the P5G network to manipulate ICS devices and create a Denial of Service. We will then provide proofs of concept to demonstrate the need for securing these vital communications and the need for in-depth consideration of the various deployment models and the pros and cons of each when integrating P5G into enterprise networks. While each has merit, additional factors must be evaluated and planned for during deployments to mitigate threats and control risk.

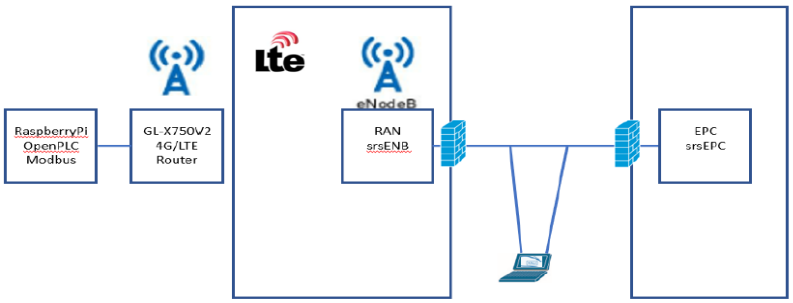

Fig 2. 5G Topology

a) Private 5G History and Future

Early Cellular Technologies: - Cellular technology has come a long way in the last 50 years since the first portable cellular phone call was placed by Martin Cooper from Motorola on April 3, 1973, to his rival, Joel Engel, at Bell Labs (Shiels, 2003). Later that year, they filed the first patent for the Radio Telephone System, paving the way for the future of mobile networks as we know them today (US Patent No. 3906166A, 1975). Although it took nearly ten years before this technology was available to the public if they could afford it, it was not long before they were affordable by the masses, and now there are very few people in developed nations who do not have a cellular device/smartphone on them. The 1st generation (1G) of cell phones, released in the early 1980s, supported voice-only using Frequency Division Multiple Access (FDMA) technology with direct connections to the existing Public Switched Telephone System (PSTN). With the evolution of the cellular industry, the 2nd generation, 2G, appeared in the 1990s. The industry became more complex with a split in technologies with Global System for Mobile Communications (GSM) and Carrier Division Multiple Access (CDMA) technologies, which continued through the 3rd generation until the technologies reconverged with the 4th generation, also referred to as Long Term Evolution (LTE) (Ghayas, 2020). The two tracks, GSM and CDMA, progressed separately, with GSM gaining prevalence as the most widely deployed technology in the US. Later in the evolution, the General Packet Radio Service (GPRS) and Enhanced Data for Global Evolution (EDGE) emerged, with this being referred to by some as generation 2.5 with data rates of up to 384 Kilobits per second (Kbps). This new development began to merge the cellular infrastructure with the nascent internet by introducing packet-switched networking. A primary focus of this research is this GPRS and the corresponding tunnelling protocol.5G-New Radio – Drivers, Benefits, and Industry 4.0 :- Since almost every adult in the developed world now owns a smart device, change is the only constant in life. As a result, the 5th generation of mobile networks has emerged to meet the demands of an always-connected and always-on society. With the release of Release 15, the technical specifications that steered the creation of the new 5G-NR standards, the 3GPP reemerged as the driving force behind the standardization and planning for the fifth generation. This new technology is needed to keep up with the proliferation of devices and the increasing bandwidth demands of mobile streaming and video due to the explosion of connected mobile devices and the Internet of Things (IoT).

b) Private 5G Architecture

5G Deployment Options :- There are two deployment options available for 5G regarding frequencies and channels used and the core networks that control the various authentication and network functions, the first being Non-Stand-Alone (NSA) and the second being Stand-Alone (SA) (3GPP, 2022). NSA refers to using 4G in conjunction with the new 5G-NR; 4G/LTE is the core network responsible for the initial connection establishment and control channels, while 5G-NR supplements the service with additional channels for increased bandwidth demands. NSA uses 4G eNB and 5th generation Node B (gNB)at the RAN and a 4G

Enhanced Packet Core (EPC), and configurations on the core network to interoperate with gNB. NSA allows MNOs to provide 5G services "over the top" of existing 4G infrastructure to facilitate faster deployment while providing mobility for users between 4G and 5G coverage areas. SA refers to a completely native 5G configuration with 5G-NR at the RAN with the new 5G Core Network (5G-CN) performing management functions.

Non-Public Network Deployment Scenarios :- The 3GPP refers to P5G as Non-Public Networks (NPN); there are, at the highest level, two types, Stand-Alone NPNs (SNPN), with entirely isolated networks that have dedicated infrastructure for Radios, RAN, and CN, and Public Network Integrated NPNs (PNI-NPN) of which there are several variations of resource sharing scenarios between private enterprises receiving the service and the MNOs that are providing (Ordonez-Lucena, Chavarria, Contreras, & Pastor, 2019). The type of deployment scenario used is based on several factors such as Capital/Operational Expenditures, frequency availability (such as licensed, unlicensed, or shared based on regions), infrastructure, and staff experience level deploying these solutions.

c) Protocols

GTP

As mentioned, GTP is responsible for both control and user plane traffic. GTP encapsulates various protocols in its payload, and according to 3GPP TS 23.060, the transport layer protocol used for user-plane traffic shall be User Datagram Protocol (UDP). While GTP is a tunnelling protocol and uses tunnel IDs, this traffic is unencrypted; therefore, anyone with access to this traffic in transit can capture and sniff traffic to view inner layers encapsulated in the GTP header to perform reconnaissance of target networks. The GTP header is only eight bytes, consisting of flags for version, protocol type, reserved, next extension header, sequence number presence, N-PDU presence, message type, payload length, and tunnel ID (TEID). Since GTP is transported using UDP, it has no inherent fault checking or sender authentication mechanism, and it is vulnerable to potential spoofing and replay attacks, as demonstrated in the proof of concept attacks in the following sections.

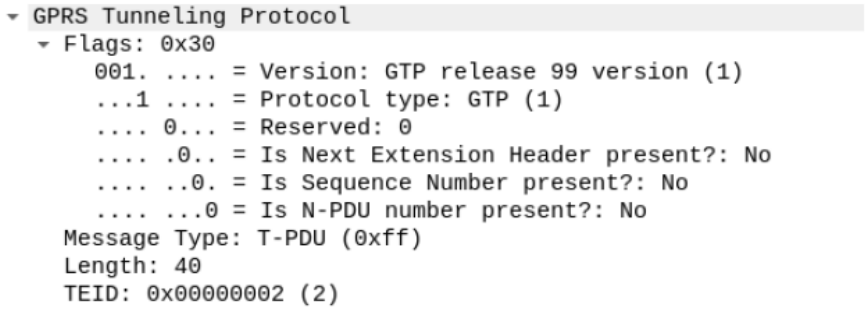

Fig 3. GTP GPRS Tunnelling Protocol

SCTP

As mentioned, SCTP is responsible for PSTN control messages, specifically for control messages between various elements within the cellular network infrastructure. SCTP replaced Transmission Control Protocol (TCP) as the new transport layer protocol for use in mobile networks due to many limitations of TCP, making it a poor candidate for cellular networks. SCTP comes with faults too because it is also unencrypted and, therefore, vulnerable to use by attackers for reconnaissance. A commonly known use of SCTP is in "Stingrays," which are commonly used by law enforcement, or "IMSI Catchers," which can force a UE to associate with it by offering the highest-level signal in the area with the proper codes to simulate valid cell towers. These types of attacks use data from the higher-level protocols carried within SCTP, namely the S1AP or S1 Application Protocol messages, which carry signals to the core for authentication of subscribers and attachment of UEs to the network. While the encapsulated S1AP messages are essential to the functioning of cellular networks, the proof-of-concept exploit demonstrated by this research uses the SCTP layer itself and therefore there is no need to cover S1AP control messages in more detail at this point.

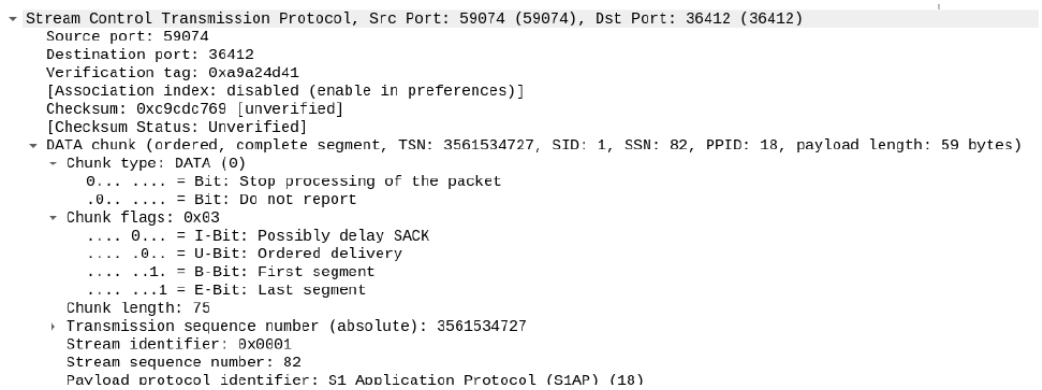

Fig 4. SCTP

5. Attack Proofs of Concept

The following attack proofs of concept are all based on the manipulation of GTP or, in one case, SCTP. There are examples provided of recon attacks using either Internet Control Messaging Protocol (ICMP) or TCP encapsulated in GTP. There is a TCP Syn Scan and an example of a X-MAS tree scan. All of these use simple manipulation of the Server script to incorporate different lower-level protocols inside the GTP flows. While other attacks outside of this research are certainly possible by a more advanced attacker, these attack proofs of concept demonstrate some simple attacks that can potentially disrupt business operations with simple scripting.

a) GTP–Modbus/TCP Sniffing and Spoofing Attack

This GTP–Modbus/TCP attack proof-of-concept takes advantage of weaknesses within the GTP and Modbus protocols and other standard practices observed in ICS environments. As illustrated in the lab topology earlier, this attack implies that an enterprise is deploying P5G using a PNI-NPN model with the RAN and CN separated, and the attacker has compromised a section of the transit network between the two. Depending on the type of network equipment in use in the environment, the attacker sniffs the transit network using the Switched Port Analyzer (SPAN) feature or port mirroring. After monitoring traffic, interesting GTP traffic is identified, and the attacker extracts the necessary data elements to populate the attack script provided in Appendix I. After populating the required data elements in the script, the attacker executes the script, which then injects spoofed GTP packets from another management workstation on the same subnet while sniffing for responses to perform a 3-way TCP handshake before injecting Modbus “Read Coils” and “Write Coils” commands. As seen below, the Modbus commands are encapsulated in the existing IP, UDP, and GTP layers.

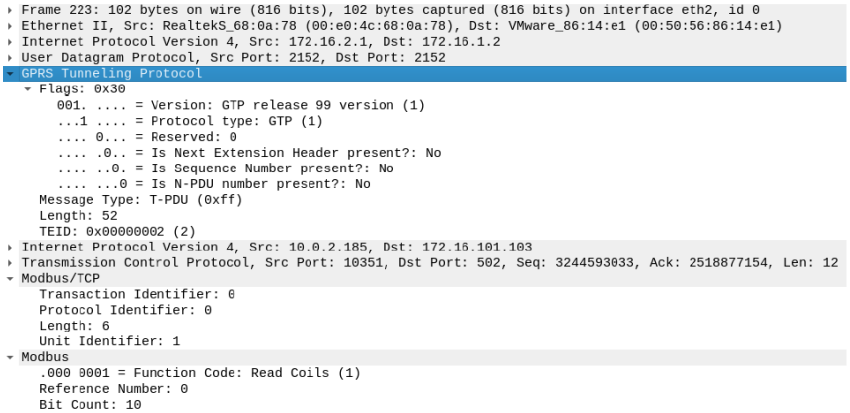

Fig 5. GTP–Modbus/TCP

6. Conclusion

Mobility is critical given the proliferation of ICS and IoT devices, as well as the growing demands on business networks and technology. These new capabilities come with a new set of threats in tandem with this greater demand for mobility. Businesses that want mobile solutions for ICS networks are turning to cellular solutions, namely P5G networks, to meet this requirement. ICS networks used to be isolated from traditional IT

infrastructure, sometimes on totally different infrastructure; however, this is no longer the case as OT and IT are merging to save costs and increase efficiency. In order to provide these extra capabilities and expand the network for new, demanding applications inside Industry 4.0, we are currently witnessing a shift to private cellular networks. Businesses implementing P5G networks as part of Industry 4.0 must exercise caution in assessing the impact this has on their attack surface and modifying safeguards as needed. Enterprises must continue to safeguard these assets while updating their infrastructure during this phase of transition since many older devices still employ easily manipulated, unsecure protocols. Since many MNOs and integrators market and offer these services on top of current LTE/4G networks using NSA deployment patterns, P5G is in a state of transition. Because cellular networks are closed, security was considered as an afterthought during the construction of the protocols, and these NSA deployment models still include weaknesses from those early generations.

7. References

1. 3GPP. (1999, April 23). 3rd generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface (3G TS 29.060 version 3.0.0). Retrieved from 3GPP: https://www.3gpp.org/ftp/Specs/archive/29_series/29.060/29060-300.zip
2. 3GPP. (1999, December 24). 3rd generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2. Retrieved from 3GPP Technical Specifications: https://www.3gpp.org/ftp/Specs/archive/23_series/23.060/
3. 3GPP. (2022, August 8). 5G System Overview. Retrieved from 3GPP: https://www.3gpp.org/technologies/5g-system-overview
4. 3GPP. (2023, June 26). Introducing 3GPP. Retrieved from 3GPP: https://www.3gpp.org/about-us/introducing-3gpp
5. 5G Alliance for Connected Industries and Automation (5G-ACIA). (2021, February). Security Aspects of 5G for Industrial Networks. Retrieved from 5g-acia.org/resources/whitepapers-deliverables/: https://5g-acia.org//wp-content/uploads/2021/05/5G-ACIA_Security_Aspects_of_5G_for_Industrial_Networks_single-pages.pdf
6. 5G-ACIA. (2023, June 26). 5G-ACIA Mission. Retrieved from 5G Alliance for Connected Industries and Automation: https://5g-acia.org/organisation/mission/.S