A 5G and Beyond Testbed for Cybersecurity Research and Education

Ibrahim Almazyad
Department of ECE
University of Arizona
Tucson AZ, United States
almazyad@arizona.edu

Safwan Elmadani
Department of ECE
University of Arizona
Tucson AZ, United States
safwanelmadani@arizona.edu

Salim Hariri
Department of ECE
University of Arizona
Tucson AZ, United States
hariri@arizona.edu

***Abstract*—The advent of 5G technology marks a pivotal advancement in mobile communications, enhancing broadband connectivity, enabling low-latency connections, and facilitating a broader range of diverse applications. Although advantageous, the introduction of 5G also introduces greater infrastructure complexity and increased cybersecurity vulnerabilities. This paper addresses these issues by developing a comprehensive 5G testbed for research and education purposes. The testbed integrates open-source software with physical hardware components to create a realistic environment for simulating and analyzing cyberattacks. Through various scenarios, including Denial of Service attacks and database exploits, we demonstrate the susceptibility of 5G core networks to these threats. Our findings reveal critical vulnerabilities in the Access and Mobility Management Function (AMF) and MySQL database, which can disrupt 5G network operations and compromise data integrity. The practical approach presented in this paper identify and mitigate 5G security threats provides valuable insights for enhancing the resilience of 5G/6G networks.**

***Index Terms*—5G, Beyond 5G, Cybersecurity, DoS, MySQL, Penetration Testing, Testbed, Telecommunication.**

I. Introduction

The rollout of 5G technology represents a transformative shift in mobile communications, ushering in a new era for autonomous vehicles, smart cities, agriculture, and remote sensors. This progress is anticipated to drive substantial economic growth and innovation across various industries worldwide. Nevertheless, the growing complexity of 5G infrastructure presents significant cybersecurity challenges. The intricate architecture of 5G networks leads to a rapid proliferation of potential vulnerabilities on a global scale, highlighting the utmost importance of robust security measures. Addressing these vulnerabilities is crucial for enhancing both reliability and safety standards for 5G networks that become increasingly indispensable in global communication and large-scale industrial operations.

The rapid expansion of 5G networks emphasizes the importance of fully understanding potential security risks and finding ways to mitigate them. A recent report highlighted over 160,000 telecommunications networks worldwide are exposed to internet attacks due to misconfigurations or lack of firewalls for nodes like the User Plane Function (UPF) [1]. This underscores the critical need for strong protective measures. Even major corporations are vulnerable; for instance, Azure Private 5G Core experienced a Denial-of-Service (DoS) vulnerability in 2024 due to mishandling length parameter inconsistency [2], demonstrating how widespread 5G security challenges can be.

Despite the availability of open-source 5G tools like OpenAirInterface (OAI) and Open5GS, they frequently lack comprehensive end-to-end security testing capabilities. Current tools mainly prioritize network functions over their cybersecurity aspects, resulting in unattended vulnerabilities. To address this gap, our study presents a comprehensive 5G network security test platform suitable for both research and educational purposes, while addressing these shortcomings.

This testbed platform integrates open-source software with physical hardware components to create a realistic environment for studying cyberattacks and evaluating defensive strategies. Scholars can use this controlled setting to measure the impact of harmful attacks and experiment with recommended defense measures before real-world implementation. Additionally, it enables practical cybersecurity training, including penetration testing methods on 5G networks without disrupting operational systems. The proposed research makes the following key contributions:

1) *5G Experimentation Platform*: An end-to-end 5G testbed that integrates open-source software with physical hardware components, supporting extensive research and testing in 5G technology and cybersecurity. Offering an insights into 5G performance metrics gained by exploring realistic deployment options.
2) *Security Evaluation*: Rigorous evaluation of physical 5G networks under various attack scenarios, such as DoS and data injection, enabling thorough evaluation of malicious attack impacts.

The organization of the paper as follows: Section II covers related work, Section III describes the design and implementation of the 5G testbed, Section IV presents our experimental evaluation, Section V presents cybersecurity recommendations and Section VI concludes the paper.

II. Related Work

The development approach builds upon our previous research efforts to create cybersecurity testbed for educational and research purposes. These efforts include projects aimed at detecting abnormal behavior in smart water treatment facilities [3], integrating blockchain techniques for Zero Trust in 5G

Networks [4], [5], and implementing the Federated Cybersecurity Testbed As A Service (FCTaaS) to offer cybersecurity testbeds [6].

Recent studies highlight 5G vulnerabilities that underscore the need for robust cybersecurity measures and testing [7], [8]. Open-source projects like Open5GS [9], Free5GC [10], and OAI [11] have been crucial in assessing new deployment structures, services, and protocols within 5G networks. While some research focuses on the Radio Access Network (RAN) tools like O-RAN [12], others such as Open5GS and Free5GC have integrated the 5G core [13]. However, current tools often lack complete end-to-end deployment capabilities and prioritize network functionalities over comprehensive security assessments.

VET5G is a virtual testing platform designed to ensure the security of 5G networks [14]. It integrates 5G core network, RAN and Android emulators, providing comprehensive simulation capabilities for 5G networks. However, its reliance on emulated environments may not fully represent the complexities of real-world 5G implementations, potentially limiting its practical applicability in scenarios that require physical infrastructures. The absence of physical hardware components can result in discrepancies between the simulated environment and real-world deployments, particularly in terms of network latency, interference, and hardware-induced vulnerabilities. Several studies utilize penetration testing techniques to reveal vulnerabilities in the 5G Core, comparing open-source options like Open5GS, Free5GC, and OAI [15], [16]. These investigations aim to recommend the most secure 5G core and propose strategies for addressing identified vulnerabilities. While these endeavors lay a foundation for future research into 5G Core security, they are limited by focusing only on virtualized environments and specific network functions without fully deploying and testing other components of the 5G network, including the physical User Equipment (UEs) and real-world attack vectors.

Management and Orchestration (MANO) frameworks, both commercial and open-source, have been created to supervise the efficient operations of Virtual Network Functions in different fields. For instance, the Open Network Automation Platform (ONAP) [17] and Open Source MANO (OSM) [18] oversee physical and virtual resources throughout the entire lifecycle of network services. However, it is essential to perform penetration testing within these MANO frameworks to detect and resolve possible security vulnerabilities, underscoring the importance of enhancing security protocols across diverse infrastructures. The work presented in [19] offers a detailed overview of potential attack paths targeting the 5G core and assesses current security measures. This review emphasizes the complexity and risks associated with implementing 5G networks, highlighting the importance of robust mitigation strategies. Furthermore, an empirical assessment of security risks within operational 5G networks [20] identifies significant vulnerabilities through practical experimentation and evaluates the effectiveness of existing mitigation methods. These findings underscore the critical needs for comprehensive security assessments and effective protection measures for ensuring 5G network Security.

Our research aims to expand on previous studies by developing a comprehensive 5G security evaluation testbed that can be used for both research and education. By incorporating 5G hardware components we can evaluate and experiment with broad network deployment capabilities. This approach addresses the shortcomings in existing tools and frameworks by providing a realistic environment for analyzing cyber threats and evaluating strategies to detect these threats and how to effectively mitigate their impacts on the operations of 5G networks and their services.

III. Design and Implementation of the 5G Testbed

The 5G testbed integrates open-source software and physical hardware components such as Software-Defined Radio (SDR) that will enable us to carry extensive research and experimentation in 5G technology, cybersecurity, and penetration testing. This testbed provides researchers with a flexible, cost-effective, and customizable environment to explore real-world applications and vulnerabilities of 5G networks.

1) ***Architectural Overview:*** Our testbed architecture is built around the 5G Standalone (SA) core network that provides critical network functions and complex set of Core Network Functions and entities. Establishing communication services between the UE and the 5G core network relies on various network elements, each outlined in detail to offer a thorough comprehension of the functional components of the 5G SA network. The architectural diagram shown in Figure 1 provides a detailed overview of the testbed, and illustrates the data flows between UEs, RAN, and core network functions, as well as the integration points for cybersecurity tools and attacks implementation. An end-to-end 5G testbed refers to a fully integrated system that covers all essential elements and operations of a 5G network. This encompasses the following components:

- User Equipment: The UE, a user device connected to the 5G core network, includes both the Mobile Equipment (ME) and the Subscriber Identity Module (SIM). The UE examples include smartphones, tablets, and IoT devices.
- Next Generation NodeB (gNB): The gNB operates as the primary station that facilitates 5G New Radio (NR). It guarantees wireless access for users of 5G technology. Its main function involves overseeing radio resources, regulating user movement, and facilitating smooth and uninterrupted high-speed data transfer.
- Core Network Functions: Includes components such as AMF, SMF, AUSF, UDM, UDR, NRF, and UPF, each fulfilling essential roles in managing network sessions, authentication, data routing, and service access.

To demonstrate the interaction among the 5G network components, we use the 5G SA registration process shown in Figure 2. This process includes two key stages: Authentication and Session Establishment. The UE registers with the 5G core network, and an IP address is assigned during session establishment. The process involves sending a Registration

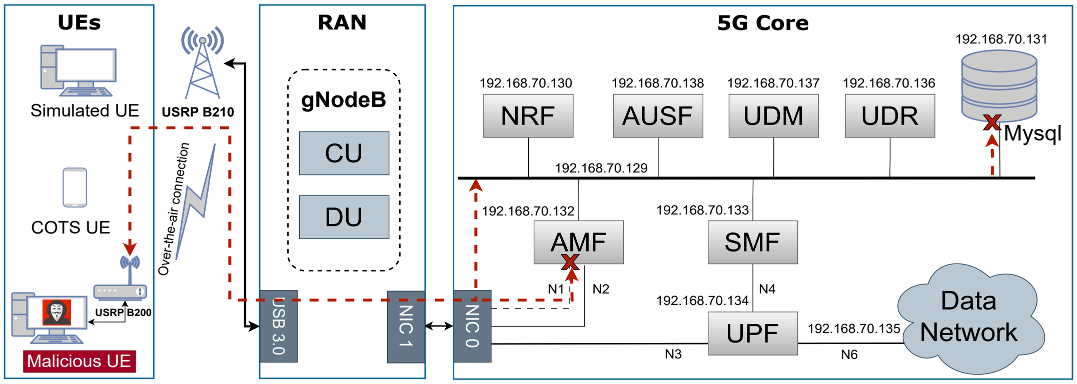

Fig. 1. 5G Cybersecurity Testbed Architecture and Main Layers.

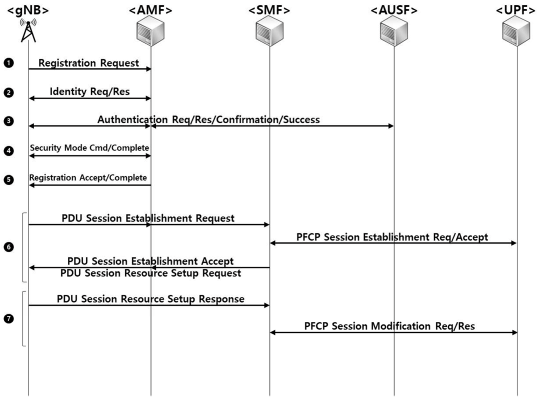
<gNB>
<AMF>
<SMF>
<AUSF>
<UPF>
1
Registration Request
2
Identity Req/Res
3
Authentication Req/Res/Confirmation/Success
4
Security Mode Cmd/Complete
5
Registration Accept/Complete
PDU Session Establishment Request
6
PFCP Session Establishment Req/Accept
PDU Session Establishment Accept
PDU Session Resource Setup Request
PDU Session Resource Setup Response
7
PFCP Session Modification Req/Res

Fig. 2. 5G SA registration procedure [21].

Request using SUCI to encrypt the SUPI or re-access via 5G-GUTI. If AMF can't locate the number, it requests SUCI. Successful authentication, verified by AUSF and UDM, results in creating communication keys. The Security Mode determines encryption and integrity algorithms, ensuring data protection at the radio interface.

2) ***Testbed Implementation:*** The 5G testbed features four types of UEs that will enable us to evaluate several 5G communication setups and configurations: (1) USRP B200: A versatile SDR platform capable of adjusting communication setups and configurations, making it suitable for diverse testing scenarios. (2) Google Pixel Phone: An off-the-shelf commercial device that provides valuable insights into real-world interactions with the testbed. (3) Raspberry Pi with Quectel RM502Q-AE 5G Module: This setup enables cost-effective 5G connectivity on widely accessible platforms, facilitating extensive application testing. (4) Simulated User Equipment: Used for scalability testing and performance benchmarking under various virtual network conditions.

The OAI 5G core is deployed within Docker containers, allowing for efficient deployment and flexible management of core network functions such as AMF, SMF, and UPF. OSM is employed to manage and orchestrate various network segments that provides a comprehensive framework for overseeing the lifecycle of network services and components, enabling flexible and efficient resource allocation based on real-time network conditions and requirements.

The gNB, a key component of the RAN, integrates the OAI software stack on a USRP B210. This SDR platform offers a flexible and open-source solution for managing the 5G RAN, enabling extensive customization and optimization of network performance to meet diverse operational requirements. High-performance computers with low-latency kernels are used to host key components of the testbed and support communication with the RAN. These servers provide the necessary computational power and storage to support intensive network operations and data processing. The testbed's advanced hardware and software components work in concert to create a robust and flexible testing environment.

IV. Experimental Evaluation

In this section, we discuss the deployed use cases of the 5G testbed using the OAI 5G core implementation and physical hardware deployment. Figure 1 shows the testbed architecture and malicious actors for penetration testing. To illustrate the testbed functionality two cybersecuirty scenarios are explored: Denial of Service (DoS) and 5G database injection attacks. Both attacks are performed using Universal Software Radio Peripherals (USRPs) by a malicious UE to achieve over-the-air (OTA) realistic attacks for 5G networks.

1) ***Scenario 1: DoS Attacks on 5G Networks:*** DoS attacks pose a significant threat to the stability and reliability of 5G networks by overwhelming network resources and obstructing legitimate users from accessing network services. These attacks can disrupt 5G network services, exhaust network resources, and lead to significant financial loses. This scenario explores techniques for conducting DoS attacks on the AMF, a core component that ensures seamless user connectivity, in the 5G core network, as well as the attack impact resulting from a malicious UE, as illustrated in Figure 1.

The Stream Control Transmission Protocol (SCTP) protocol addresses specific limitations of TCP, particularly in telecommunication systems. Cellular networks like 4G/5G widely use SCTP to enable communication between base stations (e.g., eNB in 4G, gNB in 5G) and core network functions (e.g., MME in 4G, AMF in 5G). Key features of SCTP include supporting multiple streams within a single connection for independent message delivery that will reduce head-of-line blocking risks. Additionally, SCTP transmits chunks of packets that can span multiple IP addresses to implement redundant and fault tolerance opreations. SCTP uses a 4-step process to establish a connection between two endpoints: 1) INIT: The client initiates the connection by sending an INIT chunk to the server. 2) INIT ACK: The server responds with an INIT ACK chunk. 3) COOKIE ECHO: The client sends a COOKIE ECHO chunk. 4) COOKIE ACK: The server responds with a COOKIE ACK chunk, completing the handshake [22]. This process ensures that both parties are ready for communication and establishes a secure and reliable connection.

The handshaking and cookie exchange in SCTP require additional processing, potentially leading to higher resource utilization. An attack utilizing INIT flooding can disrupt server operations similar to SYN flooding attack in TCP protocol. While SCTP servers are theoretically not prone to memory depletion after transmitting INIT/ACK containing the cookie, attackers may exploit vulnerabilities such as variable message lengths or sending lengthy messages, causing service disruption or potential DoS attacks [23].

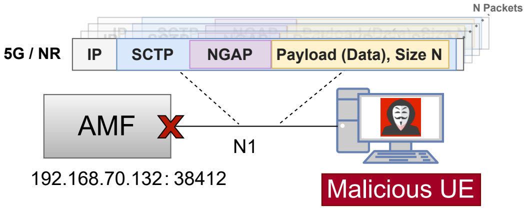

Fig. 3. SCTP-based DoS Attack on 5G AMF Network Function.

The DoS attack involves systematically creating and transmitting SCTP packets with varying payload sizes as shown in Figure 3. The steps to craft these packets include:

1) *Packet Header*: Each SCTP packet starts with a header that includes the source and destination ports, verification tag, and checksum.
2) *Chunks*: The packets contain data chunks designed to mimic control plane communication. Content sizes are adjusted to assess the AMF's capability to handle high volumes of traffic.
3) *Payload Content*: The payload is crafted to mimic genuine control messages but with increasing sizes to overwhelm the AMF's buffer and processing capabilities.

The scatter plot in Figure 4 displays the correlation between network Input/Output for AMF and payload size for SCTP packets across five different test cases. The observed findings are as follows: The blue dots illustrate the relationship between payload size and incoming network traffic, showing a positive correlation. Larger payload sizes correspond to higher network input. Similarly, yellow dots depict outgoing network traffic, also increasing with larger payload sizes.

Critical points of potential crashes are marked on the figure with red and green cross markers. Analysis shows that there were no reported crashes for payload sizes of 1000 and 2000 bytes, implying a 0% success rate in causing system failure. This indicates the system's capability to handle these payload sizes without encountering problems. However, when the payload size is increased to 3000 bytes, vulnerabilities become evident with a crash success rate of 5.56%, based on one crash out of a total of 18 occurrences.

The data shows that larger payload sizes are associated with a higher level of instability. For instance, at 4000 bytes, there is a significant increase in the frequency of crashes, leading to a success rate for attacks of only 25%. Of particular concern is the fact that at payload sizes of 5000 and 6000 bytes, every recorded instance led to system crashes, resulting in a 100% attack success rate, with an average time of 33.2 seconds from the start of the attack til crash point. This sharp rise underscores the system's inability to effectively handle higher payload sizes and inevitably leads to failures under these circumstances.

The analysis highlights the importance of monitoring network I/O metrics and payload sizes to predict and prevent system crashes. By identifying potential crash points, administrators can implement load balancing, traffic shaping, or resource adjustments to minimize crash risks.

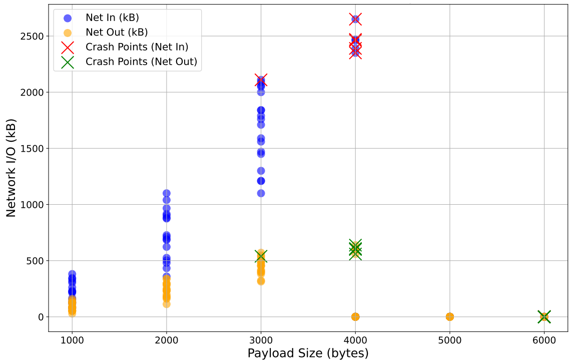

Fig. 4. Network Traffic Crash Points Correlation to DoS Attack Payload Size.

*2) **Scenario 2: Attacks on 5G Networks Database**:* This section illustrates how vulnerabilities in a 5G Standalone core network can be exploited by *physical implementation* of malicious UE for unauthorized access and data manipulation, as depicted in Figure 1. We focus on identifying accessible ports, exploiting vulnerabilities to gather system-specific details, conducting brute-force attacks to acquire credentials, and manipulating the data. This scenario highlights significant security threats in 5G core networks and emphasizes the need for robust security measures. Our attack follows these steps: network reconnaissance, vulnerability identification, credential acquisition, and data manipulation, as shown in Figure 5.

To uncover potential access points to the 5G core network, we conducted an extensive network reconnaissance. Using

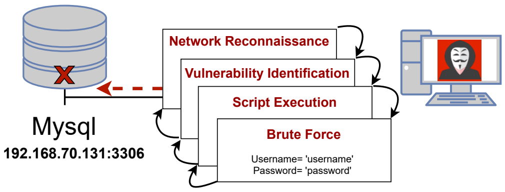

Fig. 5. Attack Stages to Takeover MySQL Database.

TABLE I
MALICIOUS UE OTA RECONNAISSANCE SCAN FOR OAI CORE

Scaned IP	latency	Port	Service
192.168.70.129	0.036s	22/tcp	ssh
192.168.70.130	0.035s	8080/tcp	http-proxy
192.168.70.131	0.036s	3306/tcp	**mysql**
192.168.70.132	0.036s	8080/tcp & **38412/sctp**	http-proxy
192.168.70.133	0.028s	8080/tcp	http-proxy
192.168.70.134	0.030s	ports are closed	N/A
192.168.70.135	0.034s	ports are closed	N/A
192.168.70.136	0.036s	8080/tcp	http-proxy
192.168.70.137	0.027s	8080/tcp	http-proxy
192.168.70.138	0.036s	8080/tcp	http-proxy
192.168.70.139	0.036s	5060/tcp	sip

tools such as *nmap tool*, we scanned the network to identify active hosts and accessible ports. The findings, detailed in Table I, revealed numerous open ports for 5G core network functions, including:

- Port 22/tcp open (SSH)
- Port 8080/tcp & **38412/sctp** open (HTTP Proxy)
- Port 3306/tcp open (**MySQL**)

These open ports indicate potential vulnerabilities, particularly within the MySQL database service, crucial for storing and managing subscription data. In order to delve deeper into the MySQL service, a detailed scan was performed to identify the exact version and any potential vulnerabilities. The scan results revealed that the MySQL service was operating on version *8.0.36*. Additionally, this procedure enabled us to successfully identify several valid usernames including *'root'*, *'sysadmin'* and *'admin'*. These identified usernames could serve as important access points for potential future exploitation and assessment activities. After obtaining the usernames, we initiated a brute-force attack to acquire valid credentials. We employed tools like *Hydra* and leveraged a standard password list for this purpose. Following multiple attempts, we managed to obtain the '*root*' user's password, granting us full access to the MySQL database and enabling extraction of valuable information.

After gaining valid access credentials, we were able to enter the MySQL database and examine and modify different types of user data. Once inside the database, we performed various activities to manipulate data. For instance, we removed legitimate user entries from the '*authentication_subscription*' table, thereby revoking their authorization to use the network. Even after deletion, active sessions persisted due to session caching mechanisms embedded within OAI 5G core network components until session drooped. Furthermore, we demonstrated our ability to inject malicious data into the database by adding a new user with elevated privileges. This injected account could then be exploited for unauthorized access to network resources and potentially enable additional attacks. This highlights the severe impact of inadequate security measures in the 5G core network; a malicious actor could potentially gain access to sensitive subscriber information, compromise user privacy, and facilitate further attacks.

Figure 6 depicts the network traffic dynamics from a 5G SA gNB. The graph illustrates incoming network traffic in Gigabit per second (Gbit/s) and highlights significant phases during the attack phases that impact network traffic. It starts with legitimate UE generating traffic, followed by a connection drop event marked with a red dashed line. Next, the brown line shows retry attempts made by valid UE to re-establish connections after authentication was revoked as part of an attack. Then, there is an orange phase indicating the injection of malicious UE. Finally, the red line represents the period during which malicious UE successfully connects and extensively consumes network resources. Vertical dashed lines clearly delineate these critical transitions for each phase's commencement. This detailed visualization emphasizes how various MySQL attacks can impact network activities in 5G and provide valuable insights into 5G data security.

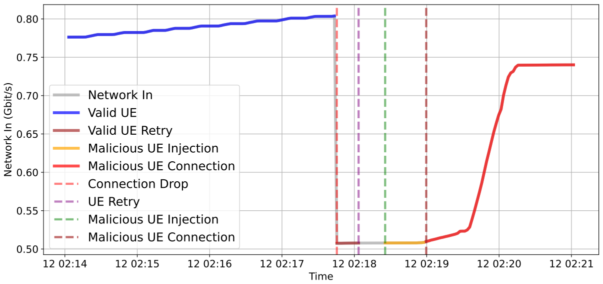

Fig. 6. MySQL Attack Stages Reflected on Network Traffic.

V. CYBERSECURITY RECOMMENDATIONS

The study findings highlight the critical need for robust security measures in 5G networks softwares, especially concerning control plane traffic in 5G core. The presensted examples of AMF susceptible to SCTP-based DoS and MySQL to data manipulation attacks demonstrate the necessity for improved resilience to ensure uninterrupted service provision. The following strategies are recommended for preventing these types of attacks:

1) Proper firewall configuration: It is critical to restricting access to only essential network ports and protocols, and thus minimizing the attack surface. Implementing stateful inspection to monitor active connections and block suspicious activity further enhances protection. Additionally, configuring network devices to use stealth techniques, such as avoiding responses to ICMP and TCP/UDP probes, can reduce their visibility to potential attackers. A regular internal and external vulnerability assessments is essential to identify and address potential weaknesses before they can be exploited by adversaries.

2) Network segmentation: It can be leveraged to constrain the impact of potential attacks. For instance, critical core networks should be logically isolated from user plane network infrastructure. Techniques such as virtual LANs and subnetting can be utilized to segregate different traffic types and enforce access restrictions. Deploying Intrusion Detection and Prevention Systems (IDS/IPS) enables the detection and mitigation of unauthorized reconnaissance activities, including rogue scanning and probing of network services. Additionally, robust password policies that mandate the use of complex, lengthy passwords, as well as regular password change requirements, can effectively deter brute-force attack attempts.

3) Zero Trust security model: This operates on the principle that no user, device, or application is inherently trusted, regardless of their location within or outside the network, thereby strengthening cybersecurity for the 5G core. By continuously authenticating identities, verifying access privileges, and assessing the legitimacy of all activities, it enables real-time monitoring that enhances privacy and security.

VI. Conclusion

In this paper, we introduced a comprehensive 5G security testbed designed to assess and mitigate cybersecurity risks in 5G networks. Through two 5G attack scenarios, we demonstrated the susceptibility of OAI 5G core networks to DoS attacks and MySQL database injection vulnerability. Specifically, we identified that the Access and Mobility Management Function (AMF) in the 5G core is vulnerable to SCTP-based DoS attacks, which can significantly disrupt network operations and halt user connection completely. Additionally, exploiting vulnerabilities in the MySQL database can lead to unauthorized access and data manipulation, compromising user privacy and network integrity. Future work will focus on broadening the scope of attack scenarios and integrating advanced detection methods into the testbed to achieve autonomous zero-trust architecture. These efforts aim to strengthen 5G networks against evolving cyber threats, contributing to the development of secure next-generation communication systems.

Acknowledgment

This work is supported by National Science Foundation (NSF) projects 1624668 and 1921485, the Department of Energy/National Nuclear Security Administration under Award Number DE-NA0003946, and the AGILITY project 4263090, sponsored by Korea Institute for Advancement of Technology (KIAT South Korea)

References

[1] "Outside Looking In How a Packet Reflection Vulnerability Could Allow Attackers to Infiltrate Internal 5G Networks With Contributions From."

[2] "CVE-2024-20685 - Security Update Guide - Microsoft - Azure Private 5G Core Denial of Service Vulnerability." [Online]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20685

[3] I. Almazyad, S. Shao, S. Hariri, and H. A. Kholidy, "Anomaly Behavior Analysis of Smart Water Treatment Facility Service: Design, Analysis, and Evaluation," *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, 2023.

[4] S. Elmadani, S. Hariri, and S. Shao, "Blockchain Based Methodology for Zero Trust Modeling and Quantification for 5G Networks," *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, vol. 2022-December, 2022.

[5] H. A. Kholidy, K. Disen, A. Karam, E. Benkhelifa, M. A. Rahman, A. U. Rahman, I. Almazyad, A. F. Sayed, and R. Jaziri, "Secure the 5G and Beyond Networks with Zero Trust and Access Control Systems for Cloud Native Architectures," *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, 2023.

[6] M. Mamun, Y.-Z. Lin, I. Almazyad, S. Shao, S. Satam, S. Hariri, and P. Satam, "Federated Cybersecurity Testbed as a Service (FCTaaS): A framework to federate cybersecurity testbeds." [Online]. Available: https://ssrn.com/abstract=4643053

[7] S. FONYI, "Overview of 5G Security and Vulnerabilities," *The Cyber Defense Review*, vol. 5, no. 1, 2020.

[8] A. Shaik, R. Borgaonkar, S. Park, and J. P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols : Exposing device capabilities," *WiSec 2019 - Proceedings of the 2019 Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 221–232, 5 2019. [Online]. Available: https://dl-acm-org.ezproxy2.library.arizona.edu/doi/10.1145/3317549.3319728

[9] "Documentation - Open5GS." [Online]. Available: https://open5gs.org/open5gs/docs/

[10] "free5GC." [Online]. Available: https://free5gc.org/

[11] "OpenAirInterface – 5G software alliance for democratising wireless innovation." [Online]. Available: https://openairinterface.org/

[12] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges," *IEEE Communications Surveys and Tutorials*, vol. 25, no. 2, 2023.

[13] J. E. Hakegard, H. Lundkvist, A. Rauniyar, and P. Morris, "Performance Evaluation of an Open Source Implementation of a 5G Standalone Platform," *IEEE Access*, vol. 12, pp. 25 809–25 819, 2024.

[14] Z. Wen, H. S. Pacherkar, and G. Yan, "VET5G: A Virtual End-to-End Testbed for 5G Network Security Experimentation," in *ACM International Conference Proceeding Series*, 2022.

[15] F. Dolente, R. G. Garroppo, and M. Pagano, "A Vulnerability Assessment of Open-Source Implementations of Fifth-Generation Core Network Functions," *Future Internet 2024, Vol. 16, Page 1*, vol. 16, no. 1, p. 1, 12 2023. [Online]. Available: https://www.mdpi.com/1999-5903/16/1/1/htm https://www.mdpi.com/1999-5903/16/1/1

[16] D. Granata, M. Rak, and W. Mallouli, "Automated Generation of 5G Fine-Grained Threat Models: A Systematic Approach," *IEEE Access*, vol. 11, pp. 129 788–129 804, 2023. [Online]. Available: https://ieeexplore-ieee-org.ezproxy2.library.arizona.edu/document/10318093

[17] "Home - ONAP." [Online]. Available: https://www.onap.org/

[18] "OSM." [Online]. Available: https://osm.etsi.org/

[19] Q. Tang, O. Ermis, C. D. Nguyen, A. De Oliveira, and A. Hirtzig, "A Systematic Analysis of 5G Networks With a Focus on 5G Core Security."

[20] S. Park, D. Kim, Y. Park, H. Cho, D. Kim, and S. Kwon, "5G Security Threat Assessment in Real Networks," *Sensors 2021, Vol. 21, Page 5524*, vol. 21, no. 16, p. 5524, 8 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/16/5524/htm https://www.mdpi.com/1424-8220/21/16/5524

[21] S. Park, S. Kwon, Y. Park, D. Kim, and I. You, "Session Management for Security Systems in 5G Standalone Network," *IEEE Access*, vol. 10, 2022.

[22] C. F. Tai, L. H. Chang, and T. W. Hou, "Improvement of SCTP performance during handshake process," in *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 2008.

[23] E. P. Rathgeb, C. Hohendorf, and M. Nordhoff, "On the robustness of SCTP against DoS attacks," in *Proceedings - 3rd International Conference on Convergence and Hybrid Information Technology, ICCIT 2008*, vol. 2, 2008.