Developing Security Information and Events Management Use Cases for 5G Specific Vulnerabilities and Attacks

Anna Bánáti

John von Neumann Faculty of Informatics, Óbuda University, Bécsi út 96/b, 1034 Budapest, Hungary, banati.anna@nik.uni-obuda.hu

Abstract: The number of cybersecurity attacks and sensitive data breaches in businesses and organizations has increased significantly in recent years, and companies that are increasingly using or providing 5G technology are no exception. The impact of these incidents not only results the sensitive data breaches, financial losses and unexpected operational patterns for the targeted companies or organizations but can also extend to their peers in the same industry. Therefore, prevention and early detection of cyberattacks is also a key issue for IT infrastructures extended with emerging 5G technology. At the same time, detecting different types of attacks has become extremely challenging as attacks have become more sophisticated, distributed and stealthy with the help of artificial intelligence and other modern technologies. Detecting and managing such attacks requires sophisticated intrusion detection systems running on high-performance hardware and managed by expert security personnel. However, these resources are expensive to deploy, especially for small and medium-sized enterprises (SMEs). Therefore, in many cases, open source and free solutions are needed that allow SMEs to operate a security information event management (SIEM) system. Thanks to the low cost of implementation, it is affordable for SMEs and, after a short configuration and learning phase, it is self-sufficient and stable. Our goal is to provide detection solutions for attacks and vulnerabilities specific to 5G networks that provide effective detection and response for open source SIEM systems. Alerts on detected anomalies notify security personnel, who can efficiently and quickly implement incident response through graphical and visual dashboards.

Keywords: 5G networks; vulnerability; attack detection; SIEM

1 Introduction

The prevalence of cybersecurity attacks and breaches targeting businesses and organizations has experienced a significant surge in recent years. This trend does not spare organizations increasingly integrating or providing 5G technology, as 5G, despite its numerous advantages, arises many new, unknown and unexpected cyberthreats [1]. This trajectory is poised for further acceleration, particularly

considering projections indicating a staggering 22.3 billion interconnected devices globally by 2024 within the Internet of Things ecosystem. [2], [3]. The repercussions of these incidents can produce sensitive data breaches, financial losses and abnormal operational patterns for the targeted entities. Moreover, the impact can reverberate throughout the industry, affecting peers within the same sector. Consequently, the imperative of preventing and early detecting cyberattacks is paramount for IT infrastructures extended with the evolving landscape of 5G technology.

Simultaneously, the identification of diverse attack types has evolved into an exceptionally intricate task due to the increasing sophistication, distribution, and stealthiness of attacks facilitated by artificial intelligence (AI) and modern technologies. Effectively detecting and managing such advanced attacks necessitates sophisticated intrusion detection systems operating on high-performance hardware, overseen by special security professionals. However, the deployment of such resources incurs substantial costs, particularly burdensome for small and medium-sized enterprises (SMEs). Considering this, there is a compelling need for open-source and free solutions enabling SMEs to implement a security information event management (SIEM) system. The affordability stemming from a cost-effective implementation renders it accessible for SMEs, ensuring self-sufficiency and stability following a brief configuration and learning phase [4].

The overarching objective is to furnish detection solutions tailored to attacks and vulnerabilities specific to 5G networks, offering efficient detection and response capabilities for open-source SIEM systems. Anomalies are promptly communicated through alerts to security personnel, empowering them to execute incident responses efficiently and expeditiously, facilitated by graphical and visual dashboards. Defining use cases for 5G SIEM is an ongoing research effort. In this paper, we do not cover the detection of every presented attack, as some are planned for future development phases.

The structure of this paper is outlined as follows: The following subsections give a brief introduction to Stand Alone 5G (5G SA) networks and Security Information and Event Management Systems (SIEM). Section 2 describes related research and case studies about vulnerability assessment of 5G networks from the different point of view and SIEM solutions. Section 3 provides background information of our simulated and research environment. Section 4 introduces domain specific vulnerabilities and attacks. In Section 5 we describe our solutions about the different detection methods and SIEM use cases of 5G specific attacks. Finally, in conclusion we summarize our findings and outline potential areas for improvement, as well as future research directions.

1.1 Security Information and Event Management

The term SIEM refers to a comprehensive technological framework combining security information management (SIM) and security event management (SEM). It functions as the linchpin of a Security Operation Center (SOC), orchestrating the collection, aggregation, correlation, and analysis of vast volumes of security data generated across an enterprise's digital infrastructure. By collecting, normalizing and correlating log files, network traffic and event data from diverse sources like network devices, servers, applications, and endpoints, SIEM furnishes security professionals within the SOC with a holistic view of the organization's security posture. Moreover, SIEM systems facilitate the identification of anomalous patterns, discerning potential security threats or breaches that evade conventional signature-based detection mechanisms. This capability to scrutinize historical data and detect deviations from established baselines equips security analysts with the foresight to preemptively counter emerging threats. In essence, the synergy between a SOC and a sophisticated SIEM system fortifies an organization's resilience against an evolving threat landscape. The main components and processes of a SIEM system can be seen in Figure 1.

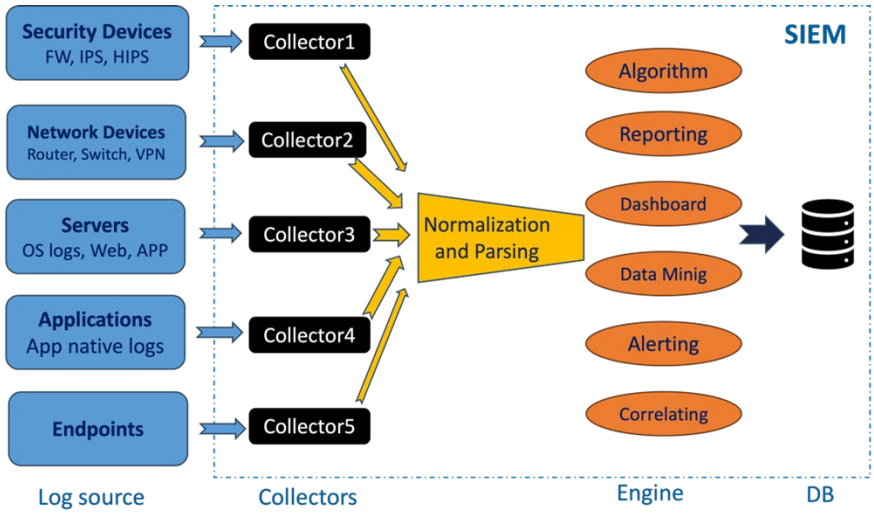

Figure 1
The components of a SIEM system

While the SIEM system yields considerable advantages, it bears inherent drawbacks. The exigencies of real-time processing and monitoring demand substantial resources. Furthermore, the rule-centric operation necessitates copious data for accurate functioning, rendering its implementation less favorable in smaller environments. Tailoring the SIEM system to individual requirements can be achieved by leveraging diverse components and functionalities. Although basic use cases remain consistent across different SIEM systems, exploiting distinct features

allows further customization for specific needs. These varied use cases formulate a set of rules, spanning from general scenarios common in Security Operations Centers (SOCs) to specially tailored regulations pertinent solely to our network. Crafting numerous rules is viable; however, emphasis rests on ensuring alerts focus solely on singular, precisely defined threats. Precisely delineating the affected elements and the relevant dataset for calculation is essential in this regard.

Crucial to reliable operation is the avoidance of false alarms. The system triggers alerts to the SOC upon threat or error detection, gauged against deviations from the norm. Establishing a threshold value becomes pivotal in delineating acceptable deviations and mitigating alarms stemming from single outliers. Precise definition of this threshold is indispensable to discerning actual threats from false positives.

1.2 SA 5G Networks

The fifth-generation mobile network, 5G, epitomizes a wireless communication standard technology established under the auspices of the 3rd Generation Partnership Project (3GPP) [5]. Recognized officially as IMT-2020 by the International Telecommunication Union (ITU), its genesis stems from the escalating demands of burgeoning mobile traffic and the concurrent emergence of the Internet of Things (IoT). Commencing in 2010, 3GPP initiated the standardization process for 5G technology, leading to the completion of Releases 15, 16, and 17, each iteration enhancing the standard's capabilities [5]. Presently, Release 18 is in progress, marking the inception of efforts toward 5G Advanced, with a pledge to augment network velocities and conserve energy across network devices [6]. In a Standalone architecture (SA 5G), 5G operates independently and does not rely on any existing 4G infrastructure. It includes a new 5G core network (5GC) and supports all 5G features, offering enhanced capabilities and performance. In a Non-Standalone 5G (NSA 5G), on the other hand, relies on the existing 4G LTE infrastructure for certain functions. The 5G radio access network (RAN) is deployed, but the core network. The foundational framework of the 5G network is delineated by three principal domains: the User Equipment (UE) domain, the Radio Access Network Domain (RAN), and the Core domain. The structure of the 5G network can be seen in Figure 2.

The 5G Core Network (CN) serves as the backbone of the 5G infrastructure, orchestrating essential network functions for seamless connectivity and diverse services. This domain includes various architectural components such as the Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF), and Authentication Server Function (AUSF), each governing specific operations. The CN integrates Network Function Virtualization (NFV) and Software Defined Networking (SDN) technologies for scalability and flexibility. The Core Network focuses on efficient service delivery, resource optimization, and robust security measures to ensure effective operations and protection against cyberthreats.

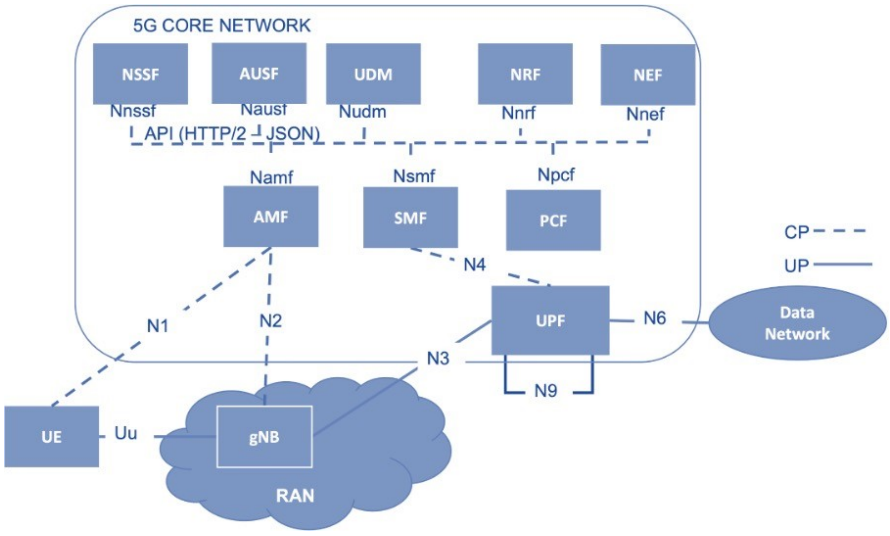

Figure 1
The architecure of 5G network

The Radio Access Network (RAN) domain establishes wireless connectivity between User Equipment (UE) and the Core Network. This includes elements like the New Radio (NR), which forms the 5G air interface technology, and the gNodeBs (gNBs) responsible for wireless communication with UEs. The RAN also encompasses Centralized Units (CU) and Distributed Units (DU), which manage radio resource management and connection mobility. The RAN faces specific security challenges, such as vulnerabilities in radio interfaces, which require robust encryption techniques, secure authentication mechanisms, and intrusion detection systems.

The User Equipment (UE) domain comprises end-user devices accessing the 5G network, including smartphones, IoT devices, and various equipment. This domain handles the User Plane, responsible for data transmission, and the Control Plane, responsible for managing communication. The diversity of devices introduces security challenges, necessitating stringent authentication protocols, encryption methods, and device-level security measures to prevent unauthorized access and data breaches.

2 State of the Arts

2.1 5G Attacks and Vulnerabilities

Many researchers discuss and analyze the cybersecurity challenges of 5G, this emerging technology [8]. Several surveys have been conducted on the whole research field as an overview [9] [10] [11] or categorizing security gaps according to different aspects, e.g. Core, RAN and UE domain, security services or even "Standalone" and "Non-Standalone" [12] [13] [14] or focusing on a specific domain or category, typically 5G Core [15] [16] [17]. Several in-depth studies highlight vulnerabilities in different technologies, tools, protocols and methods used. However, much less information is available on the analysis of specific attacks exploiting the vulnerabilities identified and on the implementation of defensive solutions against these attacks. This is even more true for detection methods, for a comprehensive SIEM methodology providing a solid security foundation or for solutions supporting the SOC approach, which to the best of our knowledge are still scarce in the literature on 5G technology. The various cybersecurity (ENISA, EU) and regulators (5G PPP, 3GPP) are also trying to provide appropriate frameworks, expectations and support, but in most cases, these remain at the level of recommendations [17].

Fang et al. in their paper [18] provide a comprehensive examination of the recent developments in 5G wireless security, emphasizing the security services like authentication, availability, data confidentiality, key management, and privacy. The study considers emerging technologies such as HetNet, D2D, massive MIMO, SDN, and IoT, highlighting their implications for security. The authors propose a 5G wireless security architecture, emphasizing identity management and flexible authentication. The advantages of the proposed architecture are demonstrated through a handover procedure and performance analysis. The paper concludes by addressing challenges and outlining future directions for 5G wireless security, aiming to guide research and implementation efforts in the field.

Park et al. in [19] investigate the Non-Standalone (NSA) 5G networks threats. Their paper's primary contribution lies in providing valuable insights into the security challenges present in real 5G NSA networks and suggesting mitigation strategies. The authors categorized 5G NSA security threats into Radio Access Network (RAN) and Core Network (CN) segments, constructing an attack tree and formulating 15 test cases applicable to real networks. They validated these test cases on three mobile carriers' networks, identifying eight valid vulnerabilities. For five of these vulnerabilities, they proposed equipment PKG software patches or configuration changes, and for the remaining three, they suggested relevant countermeasures.

In paper [17] the authors highlight the significant contributions of the 5G Infrastructure Public Private Partnership (5G PPP) to 5G security research and

development. These projects encompass standardization efforts, investigation of advanced 5G Cloud-RAN architecture, reliable network services for industrial use cases, adoption of post-Quantum cryptosystems, exploration of Distributed Ledger Technologies (DLT), and advancements in security leveraging Trusted Execution Environments (TEEs), Remote Attestation, Root Cause Analysis, and emerging trends like AI/ML and Blockchains.

The authors in [20] have demonstrated that the 5G network is vulnerable to numerous different attack vectors. Mitigation is essential to ensure secure connections for users. The authors provide a comprehensive analysis of attack vectors found in various components of the network and suggest possible defense mechanisms. They conclude that each component has its vulnerabilities, and while some types of attacks are common, there is no single solution to address all risks, which supports and validates our objectives as well. However, this research focuses on deep packet inspection and anomaly detection-based solution rather than SIEM detection methods.

The study of Dolente et al. [7] is particularly relevant for us, as it examines protocol-based vulnerabilities and attacks in an open-source simulated environment (Open5GS), which is the basis of our simulation environment. The paper aims to experimentally investigate security vulnerabilities in open-source 5G projects focusing on the 5G core network's Service-Based Interface (SBI), emphasizing the most relevant network functions, such as the Access and Mobility Management Function (AMF) and Network Repository Function/Network Exposure Function (NRF/NEF) within the Service-Based Architecture (SBA) NFs. The central contribution lies in rigorously exploring security vulnerabilities in these components, highlighting potential gaps and emphasizing the role of 5G vendors and Mobile Network Operators (MNOs) in implementing robust security measures. The paper underscores the importance of secure development practices amid the transition to Network Function Virtualization (NFV).

2.2 SIEM and Monitoring Solutions

To detect the different attacks and threats in the realm of IT security, extensive research has focused on intrusion detection systems (IDS), classifying them primarily into signature-based and anomaly-based methods [21]. While signature-based methods rely on known attack scenarios, anomaly-based methods analyze normal behavior, detecting deviations to identify previously unknown attacks [22] [23]. Even so, there is solution in the case of 5G networks. Iavich et al. in [24] present a new cybersecurity model based on machine learning algorithms which contain Firewall and IDS/IPS as well. They use an extended 5G relevant data set to detect more efficiently the majority of 5G attacks.

In many times, to address the nowadays sophisticated and hiding intrusions, a comprehensive view of security-relevant data is essential, and Security Information

and Event Management (SIEM) systems serve this purpose by integrating and evaluating data, using static rules or anomaly detection and providing the possibility for the digital forensic of the incident. SIEM must handle heterogeneous data from different types of sources and higher volumes than IDS/IPS. The literature on general Security Information and Event Management (SIEM) solutions is also a widely researched area [25] [26] [27]. However, in the case of emerging technologies such as 5G, Edge computing, or IoT, there are no well-established solutions with extensive experience in place.

However, most research tends to focus more on network supervision and monitoring rather than on the detection use cases of SIEM systems. For example, the authors in [28] address the detection methods and use cases of SIEM, with the focus being on SDN networks, particularly on SDN switches. They describe how the reconnaissance of compromised switches disrupts networks. They propose several attack models and two detection algorithms for identifying compromised switches. Their detection mechanisms are based on existing OpenFlow protocols, allowing the mechanisms to be run online and practically applied in OpenFlow networks. As another example the authors in [29] also introduce a comprehensive network monitoring framework focusing on SDN-NFV networks, the results of which can be compared to non-virtualized network monitoring. While the solution is highly interesting and the results are undeniable, the authors do not focus on detecting attacks or cybersecurity incidents.

3 Background

At the John von Neumann Faculty of Informatics of Óbuda University we have developed an open-source Security Operation Center in a research environment. The basis of the SOC is a SIEM solution based on Wazuh and Opensearch which plays a crucial role in monitoring, analyzing, and responding to security events within networks, including 5G mobile networks. Due to the nature of the research test environment, our primary focus is on the technological pillars of the SOC. This involves testing various components of the SOC, such as IDS/IPS, Firewall, Honeypots, monitoring solutions, log- and traffic analysis, etc. We explore new technological solutions and conduct optimization research to develop effective solutions. The research and testing are performed using simulations and cyberexercises, given the absence of real-time incidents in the production environment. For this purpose, we have developed a Cyber Range infrastructure where controlled cybersecurity attack-defense and Capture the Flag exercises are organized. The traffic and log data generated during these exercises are used to feed the solutions applied in the SOC.

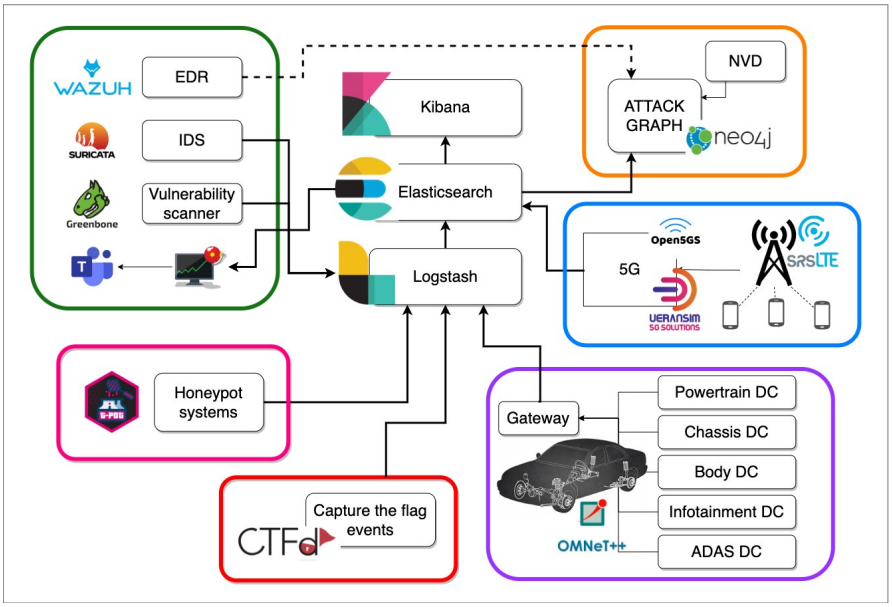

Figure 2
The High-Level Architecture of our extended Security Operation Center

Furthermore, we extended traditional solutions and methodologies designed for computer networks to encompass new directions and infrastructures increasingly used today, such as automotive electronic networks, IoT, or 5G mobile networks, where cybersecurity threats and measures play a prominent role. Additional simulation environments have been created to integrate these new infrastructures. The high-level design of our research environment can be seen in Figure 3.

For the setup of the 5G environment, we established two sites: one using a real test environment built by NOKIA provided devices explicitly for research purposes [30], and the other utilizing an open-source simulation environment where the 5G Core, RAN, and UE domains are based on virtualized solutions. To simulate attacks and threats, we employ physical 5G phones, 5G usb sticks, programmable SIM cards and Software Defined Radio devices. The high-level architecture of our 5G environment and SIEM can be seen in Figure 4. The initial step in the integration and establishment of 5G SIEM involved the strategic design and implementation of log data collection. The novel architecture had to adhere to the expectations of 5G mobile networks, requiring supervision of a significantly larger number and variety of endpoints compared to conventional setups. These endpoints now encompass not only computers but also phones, various sensors, and IoT devices. Accordingly, our log collection solution needed to be extended to accommodate communication via the MQTT protocol, enabling the gathering of information from specialized endpoints [31] [32].

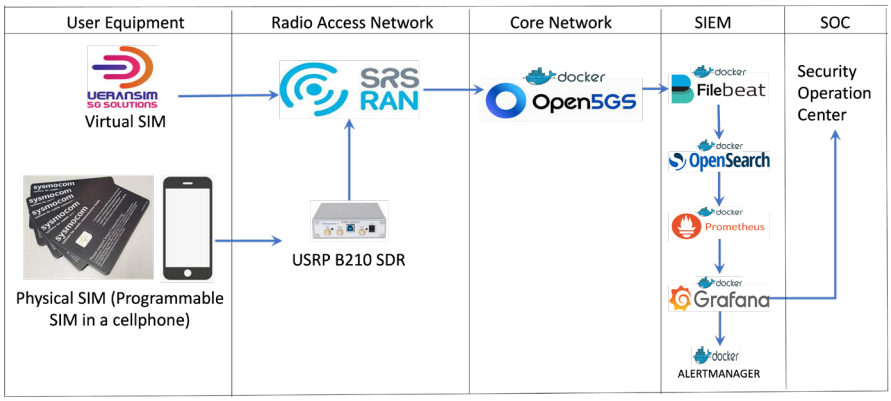

Figure 3
The high-level design of our 5F environment and SIEM

The second step entailed the identification of "normal" events in 5G mobile networks (such as registration processes, handover processes, authentication processes, cell switching, etc.) and their patterns based on log and traffic data. This process was indispensable in the development of anomaly-based intrusion detection solutions, which we concurrently initiated with the application of Artificial Intelligence tools [33].

To define various detection rules, it was also necessary to design appropriate monitoring solutions to generate statistics and thresholds for evaluating normal operation. For example, statistics on the process of registered devices, both successful and unsuccessful registrations, and the reasons for errors are required in cases where detecting a malicious attack involves identifying the registration or disconnection of devices with frequencies deviating from the norm [34].

4 Domain Vulnerabilities and 5G Specific Attacks

In this chapter, we present the vulnerabilities of 5G SA networks and malicious attacks against them, categorized based on the network domains of 5G. The classification can be seen in Figure 5.

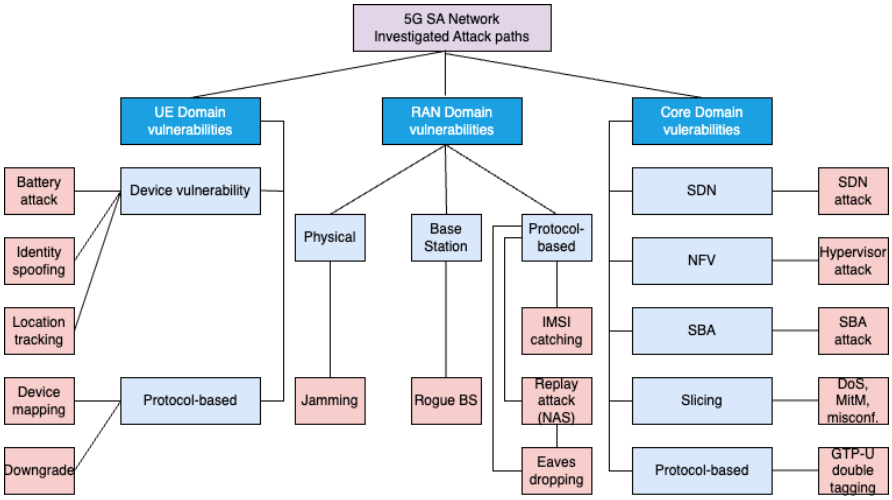

Figure 4
Attack Paths of our SIEM use cases

4.1 Core Network Vulnerabilities

Since in 5G SA core networks, the hardware-dependent architecture has been replaced by a "software-based" infrastructure, the communication between equipment has been replaced from the previous P2P-based interface communication to HTTP-based communication via API interfaces. The infrastructure is implemented by using 5G communication servers, network equipment and network slicing services, using SDN and NFV. Consequently, the most significant vulnerabilities in the core network stem from these changes [17] [7].

Software-based Infrastructure and API: The SBA uses HTTP-based web interfaces for service collaboration, streamlining communication services and data access among components. It exposes security vulnerabilities due to the familiarity of web technologies among attackers. The use of well-known web technologies and the security gaps in web application services can be exploited by attackers. Additionally, security concerns arise with open APIs, especially when providing access to external users for functions like SCEF and NEF. In 5G SA networks, signaling and data transmission protocols are expected to shift towards HTTP/2, JSON, and REST APIs instead of SS7 and Diameter in the control plane. However, the GTP protocol may remain for data transmission between the control and user planes [15]. The SBA includes various network functions (NF) and a special function called the NF Repository Function (NRF), responsible for maintaining NF profiles and supporting service discovery. While the SBA allows flexible and independent deployment of services, it introduces new security risks. Specifically, the potential transfer of security context or user privacy information between NFs poses a risk of eavesdropping when lacking confidentiality protection. Without

integrity protection, attackers may tamper with security context information, leading to inconsistencies between User Equipment (UE) and NFs. Authentication absence before signalling exchange between NFs could result in spoofing or man-in-the-middle attacks, particularly at the network edge with virtualized NFs. The lack of authorization in the new architecture raises concerns about potential unauthorized access to NF services, leading to privacy breaches such as obtaining subscriber data without permission.

NFV: The text highlights security threats to Network Function Virtualization Infrastructure (NFVI). Adversaries can upload malicious VM images, leading to data leakage and host OS compromise. Inadequate hypervisor configuration may result in DoS attacks on guest VMs. Malicious use of hypervisor power and injection of a malicious hypervisor pose risks. Virtualized Network Functions (VNF) are susceptible to software flaws and DoS attacks. The Management and Orchestration (MANO) system is a single point of failure, vulnerable to compromise. Multivendor integration complicates global security policies. Insecure interfaces expose sensitive information and may allow illegal access via embedded malicious code. These threats emphasize the need for robust security in the NFVI landscape [35][36].

SDN: In Software Defined Network (SDN), the control plane is centralized on an SDN controller, while the data plane is located on a physical or virtual switch in the case of NFV. This centralized control reveals security challenges, as attackers find the controller an attractive target. When it comes to SDN security, as SDN technology is used to control the network delivery function, it is especially vulnerable to traffic bypass attacks that exploit control protocol vulnerabilities between SDN controllers and switches, to unauthorized access between switches and controllers, and to DoS attacks aiming to deplete resources of SDN systems. These attacks can paralyze services and bring the network to a halt. The importance of implementing mitigation strategies - proper hypervisor security, controlled VM migration, proper authentication of applications running on virtualized network functionality and authorization for network functions including TLS and protections against ARP spoofing - is highlighted to enhance the overall security posture of SDN implementations [20].

Network Slicing: Vulnerabilities within network slicing configurations leading to inadequate isolation between slices or misconfigurations that compromise segmentation. Security Orchestration and Management Weaknesses: Vulnerabilities within the orchestration and management systems responsible for creating, configuring, or managing network slices, impacting the core network’s security posture.

4.2 Core Network Attacks

Attacks against SDN: The control plane is susceptible to various attacks, such as message spoofing between APIs. Successful spoofing can enable attackers to activate new flows, granting them control over the SDN and the ability to disable policies, allowing for further penetration through the network. SDN, handling critical network components, is vulnerable to diverse attacks [20]. Address Resolution Protocol (ARP) spoofing, where attackers replicate identity information to authenticate as a destination device, potentially gaining unauthorized access to the network. Man-in-the-Middle (MitM) attacks leveraging ARP spoofing to intercept data in the forwarding-control link. Furthermore, the Denial of Service (DoS) attacks, aiming to flood the host with traffic to render it unresponsive or slow down traffic, causing resource exhaustion and potential network disruption.

Attacks against Network slicing: Numerous threats pose risks to a 5G network slice. These include denial-of-service (DoS) attacks on the signalling plane, misconfiguration attacks, and Man-in-the-Middle (MITM) attacks. DoS directly targets the availability of the system and its functionalities, potentially leading to loss of access to the 5G infrastructure, remote data access, or compromised communication services.

Protocol-based attacks: Despite the transitions between generations in mobile networks, network operators need to maintain support for legacy technologies to support users who have not upgraded their equipment. However, this intention perpetuates vulnerabilities inherent in previous generations from one generation to the next. Older protocols like the GPRS Tunnelling Protocol (GTP), used since 2G, facilitate the transport of data packets between different wireless networks and networks, and suffer from several security weaknesses [15] [37]. One such weakness is that GTP does not verify the physical location of the user, making it susceptible to attackers spoofing user traffic's location. Another known type of attack is PDCP (Packet Data Convergence Protocol) spoofing, where the manipulation of the PDCP header allows for eavesdropping on user data or SMP (Session Management Protocol) fuzzing.

4.3 Radio Access Network Vulnerabilities

Physical vulnerabilities: the physically open nature of the Radio Access Network (RAN) in 5G make its infrastructure elements susceptible to physical access, tampering, or attacks. Unlike core network components that are typically housed in secure data centers, RAN components such as base stations, antennas, and transmission equipment are distributed across various locations, including rooftops, poles, and street cabinets. This distributed and decentralized nature exposes RAN elements to a higher risk of physical vulnerabilities due to their accessibility in public spaces. RAN elements are deployed in diverse locations to provide coverage across urban, suburban, and rural areas. Remote or unmanned sites, such as rural

base stations or roadside cabinets, may have limited monitoring or supervision, increasing the risk of physical attacks or sabotage.

Vulnerability of Base station: the 5G RAN ecosystem also faces risks associated with rogue base stations. A rogue base station, also known as a fake base station or IMSI catcher, is an unauthorized device that impersonates a legitimate base station to intercept, monitor, or manipulate wireless communications. Rogue base stations exploit security weaknesses in cellular networks to deceive mobile devices into connecting to them instead of genuine base stations operated by licensed network operators. Rogue base stations exploit security vulnerabilities in the cellular network infrastructure to gain unauthorized access to the radio access network. By broadcasting fake signals that mimic legitimate base stations, rogue devices trick nearby mobile devices into connecting to them, allowing attackers to intercept communication traffic and collect sensitive information. Once connected to a rogue base station, mobile devices become vulnerable to man-in-the-middle (MitM) attacks, where attackers intercept and modify data exchanged between the device and legitimate network services. Attackers can eavesdrop on communication sessions, capture sensitive information such as voice calls or text messages, and inject malicious payloads into network traffic. In addition, rogue base stations can track the physical location of connected mobile devices by triangulating their signal strength and calculating their approximate position. This capability poses significant privacy risks as attackers can monitor the movements of individuals, track their whereabouts, and gather intelligence for surveillance or criminal purposes. Rogue base stations can disrupt legitimate wireless communication services by broadcasting interference signals or jamming the radio frequency spectrum. Throughoverwhelming nearby base stations with fake signals or noise, attackers can cause network congestion, degrade signal quality, and trigger service outages, impacting the availability and reliability of cellular connectivity.

Protocol-based and signaling vulnerabilities: The Control Signal Manipulation related to the manipulation or tampering of control signals exchanged between RAN components, such as gNBs (Next Generation NodeBs). These vulnerabilities have the potential to disrupt connectivity and service provisioning within the network. Vulnerabilities within RAN-specific protocols, such as NGAP (Next Generation Air Interface Protocol), that, when exploited, could result in unauthorized access, data breaches, or disruptions to services operating within the RAN. These vulnerabilities, whether specific to the Core Network or the Radio Access Network within 5G infrastructure, underscore critical weaknesses that adversaries may exploit to compromise the integrity, availability, or confidentiality of the network.

4.4 Attack against Radio Access Network

Jamming: Jamming attacks pose a significant threat to the reliability and performance of 5G networks, particularly targeting the Radio Access Network (RAN). These attacks involve deliberate interference with wireless communication

signals, disrupting the transmission and reception of data between user devices and base stations. This interference not only affects the communication links between UEs and base stations but also interferes with synchronization mechanisms crucial for maintaining network stability. One specific type of RAN jamming attack targets the synchronization of base stations with each other and with global navigation satellite systems (GNSS). Base stations rely on precise timing synchronization to coordinate transmission and reception activities seamlessly. However, jamming attacks can disrupt this synchronization by emitting interfering signals that interfere with the reception of timing signals from GNSS satellites or neighboring base stations. As a result, base stations may lose synchronization, leading to service degradation or outages in the affected areas [38].

Rogue Base Station: A rogue base station attack involves the unauthorized deployment of a malicious base station or cell tower by an attacker. For example, a rogue base station can be implemented with the help of a software defined radio. These rogue stations mimic legitimate network infrastructure, such as those operated by mobile network operators (MNOs), to deceive mobile devices into connecting to them instead of genuine networks. Once connected, the rogue base station can intercept, monitor, or manipulate communications between mobile devices and the network, enabling various malicious activities. These attacks can lead to several security threats such as traffic Interception, message phishing, blocking of legitimate network access or eavesdropping. Eavesdropping is an attack type where an attacker intercepts and listens to the communication traffic between UE devices, aiming to obtain confidential information. To enhance privacy in the 5G network, Subscriber Permanent Identifiers (SUPI), Subscriber Concealed Identifiers (SUCI), and 5G Globally Unique Temporary UE Identity (5G-GUTI) are employed. A potential threat to GUTI involves an incoming call or message, where the network pages the UE to its last known location. This paging message lacks authenticity or integrity protection, making it susceptible to exploitation for location tracking. Implementing a strict GUTI refreshment mechanism can mitigate such exploits [20].

Eavesdropping: Eavesdropping is an attack type where an attacker intercepts and listens to the communication traffic between UE devices, aiming to obtain confidential information. To enhance privacy in the 5G network, Subscriber Permanent Identifiers (SUPI), Subscriber Concealed Identifiers (SUCI), and 5G Globally Unique Temporary UE Identity (5G-GUTI) are employed. A potential threat to GUTI involves an incoming call or message, where the network pages the UE to its last known location. This paging message lacks authenticity or integrity protection, making it susceptible to exploitation for location tracking. Implementing a strict GUTI refreshment mechanism can mitigate such exploits [20],

IMSI Catching: User devices establish network connections through a registration procedure where device data is logged in the core network for expedited reconnection. This enrollment involves transmitting technical specifications and capabilities to the most proximate and proficient tower. This action is crucial for

equitable power distribution among devices to prevent resource monopolization. However, the conveyed data is susceptible to interception as it moves from the endpoint to the tower without encryption, allowing unauthorized access with appropriate tools. Through imitating base stations, attackers can obstruct communication between the parties. Upon device activation, it seeks the nearest tower for network connection, choosing the most efficient Radio Access Network (RAN) among multiple potential connection points. An attacker's counterfeit tower endeavors to consistently surpass surrounding base stations, coaxing the endpoint into connecting with it. The device initiates the registration process, manipulated by the attacker to exploit the base station. A distinct scenario unfolds when a device, already connected and registered, necessitates a tower switch due to movement or performance issues. This transition occurs via an update message to prevent network overload from re-registration. As these messages are concise and the core network retains device data from the initial registration, they hold minimal exploitable information from an attacker's perspective. Attempting to sustain the attack, the user device futilely sends territorial or periodic update messages to the counterfeit base station. However, the attacking tower dismisses these messages, compelling the endpoint to re-register. Subsequently, the device begins the registration sequence with the counterfeit tower, thereby successfully reinstating the attack [39].

4.5 User Equipment Domain Vulnerabilities

Device vulnerability: The 5G User Equipment (UE) domain encompasses a diverse array of devices, ranging from smartphones and tablets to Internet of Things (IoT) sensors and connected vehicles. Despite advancements in technology, these devices remain susceptible to vulnerabilities that may compromise the integrity, confidentiality, and availability of data and services within the 5G network. Device vulnerabilities within the UE domain stem from a multitude of sources, including software vulnerabilities, hardware weaknesses, and insecure configurations. Such vulnerabilities may be exploited by malicious actors to gain unauthorized access to user devices, intercept sensitive information, disrupt communications, or launch other nefarious activities. Understanding and mitigating device vulnerabilities in the 5G UE domain are imperative for network operators, device manufacturers, and cybersecurity professionals. By comprehensively assessing and addressing these vulnerabilities, stakeholders can bolster the overall security posture of 5G networks, safeguard user privacy, and ensure uninterrupted service delivery.

To mitigate the impact of device vulnerabilities, various security measures can be implemented, including robust device authentication mechanisms, encryption protocols, secure boot processes, and timely software updates. Additionally, ongoing research and development efforts are essential to stay abreast of emerging threats and evolving attack vectors targeting devices in the 5G UE domain.

Protocol-based vulnerability: In the UE domain, communication between the User Equipment (UE) and the Radio Access Network (RAN) as well as the Core Network (CN) typically involves several protocols. These protocols facilitate various functions such as authentication, signaling, and data transfer. In this way the protocol-based vulnerabilities within the UE domain cannot be distinctly or unequivocally separated from vulnerabilities within the RAN or Core domains. Authentication protocols such as EAP-AKA and EAP-TLS may exhibit weaknesses that adversaries could exploit to impersonate legitimate users or conduct man-in-the-middle attacks, compromising the security of the UE's interactions with the network. Similarly, vulnerabilities within RAN-specific protocols like RRC and NGAP create opportunities for attackers to disrupt communication sessions, manipulate control signals exchanged between the UE and network elements, or eavesdrop on user data, thereby compromising network integrity.

Session management protocols like SIP and Diameter are also susceptible to exploitation, with flaws potentially enabling attackers to hijack sessions, intercept sensitive information, or tamper with signaling messages, leading to unauthorized access or service disruptions. Furthermore, vulnerabilities in data transmission protocols such as TCP/IP, UDP, and HTTP/2 can be leveraged by attackers to intercept, modify, or inject malicious data into communication streams, resulting in data leakage or service interruptions.

At the network layer, weaknesses in protocols like IPv6 and ICMPv6 expose devices to various threats, including address spoofing, router advertisement spoofing, or denial-of-service attacks. Addressing these vulnerabilities requires comprehensive security measures such as encryption, authentication, access control, intrusion detection, and regular security updates. Moreover, ongoing monitoring, vulnerability assessments, and threat intelligence sharing are crucial for detecting and mitigating emerging threats in the dynamic landscape of the 5G UE domain.

4.6 Attacks against User Equipment

Battery attack: The battery attack poses a significant threat primarily to IoT (Internet of Things) devices. This form of attack specifically targets low-usage, basic, sporadically active devices that conserve power due to infrequent use. These endpoints, tailored for intermittent tasks, employ a timer mechanism, periodically communicating with the base station to limit continuous network connections and disconnections. In this scenario, the attacker manipulates the transmission registration process by erasing the timer message. Consequently, despite the device awaiting acknowledgment from the tower in a uninterrupted manner, it depletes its energy resources, unaware of the altered transmission state [39].

Downgrade attack: The primary aim of a downgrade attack is to diminish service quality, resulting in a deterioration of the user's experience. This is accomplished

by altering the device's capabilities within the registration process. Such alterations might encompass reducing data rates or disabling functionalities, such as Voice over LTE (VoLTE). The core network stores and handles this modified device information accordingly. This attack disrupts the user experience as the endpoint's functionality remains compromised until re-registration with the network occurs. Re-registration typically occurs infrequently, potentially lasting several days. Under more favorable circumstances, users can expedite this process by rebooting the device, prompting immediate self-registration [39].

Device Mapping: During the registration process, devices communicate a lot of information to the core network so that it can identify and serve them properly. This data is sent unencrypted from the device to the base station. By themselves, this data does not reveal much information about a particular endpoint. Due to the specificities of hardware manufacturers and their narrow product groups, their combination of technologies is very limited. Thus, the devices are distinctive. If the attacker has a large enough database of these devices and their specifications, he can easily identify the user device from this data. This will allow it to map the surrounding endpoints within the range of the fake base station [39].

5 Detection Methods and SIEM Use Cases

Notably, 3GPP security specifications are mandatory for vendors, yet optional for 5G service providers. This flexibility in implementation has led to varying security levels across different 5G networks. This approach caters to the varied regulations of different countries, some of which opt not to mandate certain security features for national telecommunications providers to preserve privacy [7]. In this section, the design and implementation of detection methods, we primarily focused on the RAN and UE domains, with the analysis of the Core domain slated for the next phase of our research.

5.1 RAN Network

The enumerated attacks are detectable through a SIEM system, particularly by monitoring the registration of devices. The pivotal point across these attacks resides within the registration process, rendering it imperative for the attacker's access to or manipulation of sensitive data. Through analyzing logged data samples, the system can quantify daily device registrations and updates within each Tracking Area. Detection hinges on identifying outliers, specifically a notable surge in the number of registrations. If a false tower exists in each zone, update messages in the area will decline markedly while registration messages will proportionately escalate. The deceptive stations, operating akin to regular endpoints, mimic routine and innocuous registration processes, making detection challenging.

Rogue Base station: Detecting the presence of a rogue base station involves analyzing various types of log data originating from UE, RAN, or Core domains. The process begins by examining signal strength information reported by UE devices. Sudden drops or fluctuations in signal strength, as recorded in UE logs, may indicate interference from unauthorized base stations. In addition to signal strength discrepancies, abnormal cell ID changes observed in RAN logs can also raise suspicion. Instances where UE devices unexpectedly switch to different Cell IDs or sectors within a short time frame might suggest the presence of rogue base stations. Furthermore, analyzing Core domain logs can reveal unauthorized handovers of UE devices to unrecognized or unauthorized base stations. Any such handover events could be indicative of rogue base station interference with legitimate network operations. Network traffic logs provide another valuable source of information for rogue base station detection. Unusual patterns in network traffic, such as unexpected spikes or drops in data usage, anomalous protocols or port numbers, or suspicious increases in network activity, may suggest the presence of rogue base stations attempting to disrupt communication. Geolocation data can also be leveraged by correlating UE location information with expected base station locations. Any deviations or discrepancies in reported UE positions relative to known base station locations could signal the presence of rogue base stations. Finally, Core domain logs should be monitored for instances where UE devices register with unauthorized network identifiers or attempt to establish connections with unrecognized network entities. Such registration attempts may be indicative of rogue base station activity attempting to gain unauthorized access to the network.

Table 1
Alert statistics after Syncronization issue

Alarm title	Information	Created time	Severity	Type
Cell service problem	Phase error exceeds the interference limit. 5G cells were disabled because either phase error exceeded 1.5 µs or holdover of PPS provider expired	10.25.2023. 11:25	critical	QoS
BS information	Top reference missing	10.25.2023. 11:10	minor	QoS
BS information	NTP Server192.168.250.250 unavailable	10.25.2023. 10:20	minor	QoS
BS security problem	Service account root access is enabled	10.25.2023. 9:27	minor	QoS
BS security problem	Ethernet port security is disabled	10.25.2023. 9:27	minor	QoS

Jamming: 5G networks, like any wireless networks, are built on open sharing, making them susceptible to interference. When the interference level is high, receivers are unable to properly decode transmitted signals. Exploiting this weakness, attackers can intentionally disrupt communication on specific wireless

channels for legitimate users. This type of attack, known as jamming, is a denial-of-service attack. As more base stations and cells are deployed for adequate coverage and performance, it is crucial that they synchronize with each other and share the same time reference as the surrounding macrocell towers, user devices, and RAN elements. Timing precision is required to support technologies like Time Division Duplex (TDD), where the uplink and downlink connections are on the same frequency band [12]. In 5G networks, synchronization comes not only from neighboring base stations but also from various Global Navigation Satellite Systems (GNSS) sources. Our experimental 5G Standalone network at the university operates in isolation with two base stations, obtaining synchronization data solely from satellites. Therefore, the synchronization within the network ceases by jamming the reception antennas. As synchronization errors can lead to further damage, the base station shuts down its services upon detecting the problem [38]. The alerts statistics after the crash can be seen in Table 1, in addition in the traffic captured by wireshark was detected.

IMSI catching: Reducing the interlinkage of authentication responses can prevent IMSI Catching by concealing the cause of the error in authentication rejection. However, in many cases, the attack is not based on the cause of the error, but rather on the message type (rejection or acceptance) perceived by the user equipment, so concealing the cause of the error often does not provide protection against IMSI catching; the attacker can observe whether the connection establishment continues or not. The attacker uses the legitimate network to generate new authentication vectors. Throttling mechanisms effectively reduce the scalability of the attack and require minimal effort for acceptance. Operators can detect large-scale IMSI Catcher attacks by tracking known IMSI numbers, such as storing them in a database. In such a scenario, the reappearance of IMSI numbers would likely stem from an attack. However, this detection method fails if the attacker knows the IMSI number and the scheme must also be aware of the freshness and authenticity of the IMSI, for example, with a counter and the endpoint's private-public key pair. As an additional option, the user equipment can detect an IMSI Catcher attack by detecting abnormal protocol behavior, such as observing multiple repeated authentication requests. The endpoint can limit or delay responses, thereby compromising the scalability of the attack: if the number of responses is limited, the attacker only has a few attempts to guess the correct authentication token. In summary, continuous monitoring of log data from the registration process allows for the detection of attacks in both the RAN and UE domains. Based on the statistics of "normal" daily traffic (number of successful registrations, number of unsuccessful registrations, knowledge of the cause of failure), a significant deviation from these statistics in most cases likely indicates an attack (or at least an error).

5.2 UE Domain

In scenarios where the false base station's coverage slightly differs from the legitimate station, update messages persist in the area during an attack. However, an alternative strategy is essential when the attacker deploys their station in a confined area or with extensive overlap, obscuring significant differences in registration numbers. Yet, in such cases, detection of downgrade and battery attacks remains feasible.

Downgrade Attack: For a downgrade attack, the registry logs serve to discern the capabilities of connected devices. Analyzing average values for diverse device capabilities per area, like data transfer rates, facilitates detection. A noteworthy increase in significantly lower-than-average values may indicate an ongoing attack.

Battery Attack: Similarly, in detecting a battery attack, targeted analysis of registry log files can pinpoint IoT devices based on vendor specifications during registration. Scrutinizing the receipt of timer messages from identified endpoints, observing substantial outages—beyond sporadic message corruption—suggests an ongoing attack.

Conclusion

The cybersecurity aspects of 5G networks remain largely obscure, covering many areas that require thorough investigation. Beyond existing risks, the emergence of new threats inherent in this novel technology necessitates their identification and mitigation wherever possible. While many attacks stem from improper network configuration, others are related to the architecture or communication protocols. Consequently, a deeper understanding of network operations, functions, communication mechanisms, data transmission processes, and associated vulnerabilities is crucial.

In critical and general IT systems, the necessity of Security Information and Event Management (SIEM) systems is increasingly acknowledged, where well-established detection rules and mechanisms trigger alerts following suspicious events. These are reinforced by comprehensive Security Operations Center (SOC) technologies to enhance efficiency. However, in 5G networks, these methods are still relatively underdeveloped, necessitating the rapid design and implementation of effective solutions.

Our research focuses on developing a 5G-specific SIEM system, involving a detailed analysis of known vulnerabilities and attacks according to the architecture of 5G networks. Initially, we concentrated on the Radio Access Network (RAN) and User Equipment (UE) domains, with plans to extend to the core network in the future. We employ open-source solutions for SIEM development and have created an open-source simulation environment. Our research prioritizes common every day attacks, while considering open-source and cost-effective options to support the capabilities and constraints of small and medium-sized enterprises (SMEs).

At this stage of our research, it is evident that collecting and analyzing log and traffic data within the network can significantly enhance our understanding of network operations. Patterns of normal and abnormal events and processes can be identified, facilitating the detection of suspicious activities.

The research on developing a 5G-specific SIEM system also has several limitations that need to be considered for future improvements. Firstly, the vast amount of data generated within 5G networks poses significant technological challenges in terms of accurate and real-time collection and analysis. Secondly, while open-source simulation environments are useful, they may not fully reflect the complexity and dynamics of real-world 5G networks, which can limit the practical applicability of the research findings. Thirdly, the scalability and adaptability of the SIEM system developed during the research may be constrained when applied to different 5G network architectures and various environmental conditions. Implementing the system in larger networks may require additional fine-tuning and optimization.

Acknowledgment

The research was supported by the Ministry of Culture and Innovation NRDI Office within the framework of the Infocommunication and Information Technology National Laboratory Program.

References

[1] M. Bogdanoski, T. Shuminoski, M. Hadji-Janev, A. Risteski, T. Janevski, "Future 5G Mobile Broadband Networks Using Cloud-based Services with Advanced Security and QoS Framework," Acta Polytechnica Hungarica, 17(10), 20, 2020

[2] "EuropeanConsilium," www.consilium.europa.eu/en/policies/cybersecurity,accessed:2024-02-02

[3] P. T. Mai, A. Tick, "Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam," Acta Polytechnica Hungarica, 18(8), 67-89, 2021

[4] T. Laue, T. Klecker, C. Kleiner, K.-O. Detken, "A SIEM Architecture for Advanced Anomaly Detection," Open Journal of Big Data, 6(1), 26-42, 2022

[5] "The 3rd Generation Partnership Project," https://www.3gpp.org/technologies/rel-18, accessed: 2024-02-02

[6] X. Lin, "An overview of 5G advanced evolution in 3GPP release 18," IEEE Communications Standards Magazine, 6(3), 77-83, 2022

[7] F. Dolente, R. G. Garroppo, M. Pagano, "A Vulnerability Assessment of Open-Source Implementations of Fifth-Generation Core Network Functions," Future Internet, 16(1), 1, 2023

[8] R. Khan, P. Kumar, D. N. K. Jayakody, M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements,

and future directions," IEEE Communications Surveys & Tutorials, 22(1), 196-248, 2019

[9] S. Fonyi, "Overview of 5G security and vulnerabilities," The Cyber Defense Review, 5(1), 117-134, 2020

[10] S. Sullivan, A. Brighente, S. A. Kumar, M. Conti, "5G security challenges and solutions: a review by OSI layers," IEEE Access, 9, 116294-116314, 2021

[11] F. Shokoor, W. Shafik, S. M. Matinkhah, "Overview of 5G & beyond security," EAI Endorsed Transactions on Internet of Things, 8(30), 2022

[12] G. Holtrup, W. Lacube, D. P. David, A. Mermoud, G. Bovet, V. Lenders, "5g system security analysis," arXiv preprint arXiv:2108.08700, 2021

[13] J. A. Khan, M. M. Chowdhury, "Security Analysis of 5G Network," in 2021 IEEE International Conference on Electro Information Technology (EIT), 001-006, 2021, doi:10.1109/EIT51626.2021.9491923

[14] C. Suraci, G. Araniti, A. Abrardo, G. Bianchi, A. Iera, "A stakeholder-oriented security analysis in virtualized 5G cellular networks," Computer Networks, 184, 107604, 2021

[15] H. Kim, "5G core network security issues and attack classification from network protocol perspective." J. Internet Serv. Inf. Secur., 10(2), 1-15, 2020

[16] J. H. Park, S. Rathore, S. K. Singh, M. M. Salim, A. Azzaoui, T. W. Kim, Y. Pan, J. H. Park, "A comprehensive survey on core technologies and services for 5G security

[17] Taxonomies, issues, and solutions," Hum.-Centric Comput. Inf. Sci, 11(3), 2021

[18] Q. Tang, O. Ermis, C. D. Nguyen, A. De Oliveira, A. Hirtzig, "A systematic analysis of 5G networks with a focus on 5G core security," IEEE Access, 10, 18298-18319, 2022

[19] D. Fang, Y. Qian, R. Q. Hu, "Security for 5G mobile wireless networks," IEEE access, 6, 4850-4874, 2017

[20] S. Park, D. Kim, Y. Park, H. Cho, D. Kim, S. Kwon, "5G security threat assessment in real networks," Sensors, 21(16), 5524, 2021

[21] S. A. Bjerre, M. W. K. Blomsterberg, B. Andersen, "5G Attacks and Countermeasures," in 2022 25th International Symposium on Wireless Personal Multimedia Communications (WPMC), 285-290, IEEE, 2022

[22] R. Ferdiana, et al., "A systematic literature review of intrusion detection system for network security: Research trends, datasets and methods," in 2020 4th International Conference on Informatics and Computational Sciences (ICICoS), 1-6, IEEE, 2020

[23] A. Thakkar, R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," Artificial Intelligence Review, 55(1), 453-563, 2022

[24] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Transactions on Emerging Telecommunications Technologies, 32(1), e4150, 2021

[25] M. Iavich, S. Gnatyuk, R. Odarchenko, R. Bocu, S. Simonov, "The novel system of attacks detection in 5G," in International Conference on Advanced Information Networking and Applications, 580-591, Springer, 2021

[26] S. Dorigo, "Security information and event management," Radboud University, Nijmegen, 2012

[27] M. Vielberth, G. Pernul, "A security information and event management pattern," 2018

[28] G.-S. Jeon, S.-H. Chun, J.-B. Kim, "A Study on the Methods for Establishing Security Information & Event Management," Applied Computing and Information Technology, 33-45, 2020

[29] P.-W. Chi, C.-T. Kuo, J.-W. Guo, C.-L. Lei, "How to detect a compromised SDN switch," in Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft), 1-6, 2015, doi:10.1109/NETSOFT.2015.7116184

[30] G. Yang, H. Jin, M. Kang, G. Jun Moon, C. Yoo, "Network Monitoring for SDN Virtual Networks," in IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, 1261-1270, 2020, doi: 10.1109/INFOCOM41043.2020.9155260

[31] P. J. Varga, L. Nádai, A. B. Tóth, E. Kail, T. Wührl, S. Gyányi, G. Kún, R. Kovács, A. Bánáti, M. Kozlovszky, "5G RAN research in Óbuda University," in 2022 IEEE 20th

[32] Jubilee World Symposium on Applied Machine Intelligence and Informatics (SAMI), 000359-000366, 2022, doi:10.1109/SAMI54271.2022.9780721

[33] M. Orsós, M. Kecskés, E. Kail, A. Bánáti, "Log collection and SIEM for 5G SOC," in 2022 IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics (SAMI), 000147-000152, IEEE, 2022

[34] M. V. Kecskés, M. Orsós, E. Kail, A. Bánáti, "Monitoring 5g networks in security operation center," in 2021 IEEE 21st International Symposium on Computational Intelligence and Informatics (CINTI), 000223-000228, IEEE, 2021

[35] Á. Puskás, S. Laczi, E. Kail, A. Bánáti, "Neural Network-based Log Analysis Methods for 5G network," in 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics (SISY), 000589-000594, IEEE, 2023

[36] M. V. Kecskés, M. Orsós, E. Kail, A. Németh, A. Bánáti, "5G registration tracking based on logdata," in 2022 IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC), 000129-000134, IEEE, 2022

[37] S. Zhang, Y. Wang, W. Zhou, "Towards secure 5G networks: A Survey," Computer Networks, 162, 106871, 2019

[38] T. Madi, H. A. Alameddine, M. Pourzandi, A. Boukhtouta, "NFV security survey in 5G networks: A three-dimensional threat taxonomy," Computer Networks, 197, 108288, 2021

[39] R. P. Jover, V. Marojevic, "Security and protocol exploit analysis of the 5G specifications," IEEE Access, 7, 24956-24963, 2019

[40] T. Wührl, P. J. Varga, S. Gyányi, M. Baross, A. Németh, "5G RAN synchronization vulnerability," in 2022 IEEE 20th Jubilee International Symposium on Intelligent Systems and Informatics (SISY), 000139-000144, IEEE, 2022

[41] A. Shaik, R. Borgaonkar, S. Park, J.-P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities," in Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, 221-231, 2019