5G Security Threats and Countermeasures: An Operator Perspective

Jasmina Baraković Husić[1], Sabina Baraković[2]

[1]University of Sarajevo – Faculty of Electrical Engineering, Zmaja od Bosne bb, 71000 Sarajevo, B&H

[2]University of Sarajevo – Faculty of Transport and Communication, Zmaja od Bosne 8, 71000 Sarajevo, B&H

Abstract

The fifth generation of mobile telecommunications (5G) is one of the most important novelties of our times due to its influence on the economy and society. The advent of 5G networks and services expands the security threats landscape and requires the implementation of adequate countermeasures. This paper presents a brief overview of 5G security threats and countermeasures from operators' perspective. The aim is to contribute to the 5G cybersecurity knowledge collection and dissemination by summarizing the key findings and identifying next steps.

***Keywords**: 5G, Cybersecurity, Threats, Technical measures, Operators*

1 Introduction

The fifth generation of mobile telecommunications (5G) is an inevitable, next generation transformation of the role that technology plays in the economy and society. 5G is designed to provide an opportunity to move beyond connectivity in order to meet the different needs of citizens and economy. It is an opportunity to collaborate between various sectors, such as transport, health, finance, and provide rich, innovative services.

Thanks to technology improvement in various fields, commercial 5G networks are widely deployed from 2020. The Groupe Speciale Mobile Association (GSMA) has expected that 5G networks are likely to cover one-third of the population by 2025 [1]. The implementation of 5G network could add up to €1 trillion to European gross domestic product (GDP) between 2021 and 2025 and potentially create up to 20 million jobs across all sectors of the economy [2]. Ensuring the cybersecurity and resilience of 5G networks is thus essential.

Introducing a 5G technology makes changes to the security threat landscape due to the combination of new technology and different service models being introduced. These threats are usually unknown at the time of launch since attackers need live environment to develop new threats. Security threat landscape will expand with the exposure of new industries and services, such as industry 4.0, smart cities, connected vehicles, etc. [3].

Operators are responsible for the secure rollout of 5G using equipment sourced from technology vendors, i.e., deployment of 5G networks, investment and funding, and security of 5G networks. Recent research activities showed that 32% of operators reported an increased attack surface as key challenge here, whereas 48% admit that they do not have enough knowledge or tools to deal with security threats. In addition, 39% of operators point to limited pool of security experts which further reduce in-house cybersecurity knowledge [4].

In order to identify a common set of countermeasures which can mitigate the main 5G security risks, the European Union (EU) toolbox on 5G cybersecurity has been created. It contains non-binding measures to be implemented by various actors including operators. In addition, there are supporting actions that have potential to enable and assist the strategic and technical measures. In this context, one of the actions obligates the operators to review or develop guidelines and best practices on network security [5].

In order to contribute to this supporting action, this paper aims to summarize 5G security threats and countermeasures. All security threats

mentioned in this paper can be used by operators as a basis to develop security controls and to complement any in-house security threat materials. The specific measures are recommended to reduce various vulnerabilities and minimize the exposure to these threats. The intention is to decrease or even eliminate the impacts of these threats and better manage 5G cybersecurity risks.

The rest of the paper is organized as follows. After introduction, section 2 provides a brief overview of 5G security threats and corresponding countermeasures to be taken by operators. Section 3 discuss the key findings and provides an insight into the next steps.

2 Security of 5G Network

5G security threats and countermeasures described in this paper are categorized to map to generic 5G network domains, i.e., user equipment threats, radio access network threats, core network threats, cloud threats, service and application threats, and operation and management threats. Table 1 contains description of each identified 5G security threat, whereas Table 2 gives an insight into the suggested countermeasures that can be taken by operators to reduce or eliminate the threat impact.

2.1 Security Threats

Security threat is defined as "*the potential cause of an incident that may result in a breach of information security or compromise business operations*" [6]. Threats can be accidental and intentional. Accidental threats exist with no premediated intent. Intentional threats are result of a harmful decision.

Table 1 gives an overview of identified 5G security threats to provide practical guidance to technical staff.

2.2 Security Countermeasures

According to EU toolbox on 5G cybersecurity, security measures can be divided into two groups, i.e., strategic and technical [5]. Strategic measures include regulatory powers, third-party suppliers, diversification of suppliers, and sustainability and diversity of 5G supply and value chain. On the other side, technical measures refer to network security, requirements related to suppliers' process and equipment, and resilience and continuity. Here we focus on technical measures. Table 2 summarizes countermeasures for each of identified threats that can be taken by operators.

3 Kye findings, Conclusions and Next Steps

The security of 5G networks is identified as a critical issue. Operators strive to provide security assurance described by the security triad, i.e., confidentiality, integrity, and availability (CIA). Security threats summarized in Table 1 have potential influence on all three elements of CIA triad. User equipment threats potentially affect confidentiality. Radio access network and cloud threats have impact on both confidentiality and availability, while core network threats mainly affect confidentiality. Operation and management threats mainly have influence on integrity, while service and application threats primary affect confidentiality. Furthermore, security threats listed in Table 1 affect the following assets:user equipment, user data, system data, and telecom services. User equipment is only affected by the service and application threats. User data are affected by the threats associated with all 5G network domains, while system data are influenced by the core network, cloud, and operation and management threats. Telecom services are mainly affected by the radio access network, core network, and cloud threats.

Operators are expected to further discover new security threats and addressed them as 5G network and services are used commercially. In addition, they may implement standards, guidelines, and best practices to achieve security objectives for the safe use, deployment, and operation of 5G networks and services. In this context, this paper contributes to creation of technical guidance on best practices related to 5G network security which can increase in-house cybersecurity knowledge.

Table 1. Overview of 5G security threats

Domain	Threat	Description	References
User equipment	SIM credential theft	SIM credentials are accessed by unauthorized actors to monitor mobile user communication.	[7]
Radio access network	UE DoS attack	Fake base station is used by attacker to pretend to be legitimate base transceiver station to send false system information causing DoS attack.	[8]-[13]
	Network DoS attack	High amount of connection requests is generated by radio air-interface to exhaust network resources causing DoS attack.	
	5G authentication vulnerabilities	5G authentication vulnerabilities include billing fraud, implicit authentication, and privacy violation against active attackers.	
	5G user location tracking	Media access layer information about carrier aggregation is used to passively locate and track 5G users.	
	Radio jamming	Fake base station blocks users trying to access the network.	
	Hijacked TCP connection eavesdropping	Traffic between victim user equipment and remote TCP server can be eavesdropped by hijacking TCP connection to inject malicious TCP packets.	
Core network	Core network DoS attack	Attacker initiates DoS attack against the core network and make service unavailable.	[14]-[17]
	Voice call eavesdropping	Unauthorized actors compromise the mobile switching center with malware to spy voice content using lawful interception functionality.	
	SMS eavesdropping	Unauthorized actors infect operator's short message service center with malware.	
	5G NEF API exploitation	API software can have vulnerabilities which can lead to tampering, spoofing, data theft, and service unavailability.	
	CDR harvesting	Call detail records are harvested from mobile networks by malware usage.	
Cloud	VM abusing	Virtual resources are abused/controlled by attacker which results in information leakage, interception, eavesdropping, or system unavailability.	[3]
	MEC DDoS attacks	DDoS attacks against MEC are initiated in order to consume network resources and make services unavailable.	
	MEC APIs abusing	MEC APIs are abused to cause network congestion, data leakage, or resource exhaustion.	
	Unauthorized access to the NS management plane	Security control mechanisms of network virtualization may be bypassed resulting in unauthorized access to the slice management plane.	
	NS resource preemption	Security control mechanism of network virtualization may be bypassed causing slice resource preemption.	
	NS data theft and tampering	Security control mechanism of network virtualization may be bypassed causing slice data theft and tampering.	
Operation and management	Detect theft or fraud	A legal identity of the management plane is illegally obtained by attacker in order to intrude into the network.	[3]
	Exploitation of NC data weakness	Critical network assets can be accessed by threat actors during different phases of the solution implementation lifecycle.	
	Log tampering	Attackers tamper with system logs, security logs, and operation logs.	
Service and application	Malicious applications	Malicious applications may use phone credit, tamper with personal data, intercept user traffic or copy applications to commit fraud.	[18]-[21]
	UE compromise	Malicious actor may compromise or hack user equipment through a range of exploit methods.	
	Personal data theft	Improper use of security controls causes vulnerabilities exploitation by malicious actors.	

Legend: SIM (*Subscriber Identity Module*); DoS (*Denial of Service*); UE (*User Equipment*); IP (*Internet Protocol*); TCP (*Transmission Control Protocol*); NEF (*Network Exposure Function*); API (*Application Programming Interface*); SMS (*Short Message Service*); CDR (*Call Detail Records*); VM (*Virtual Machine*); MEC (*Multi-access Edge Computing*); NS (*Network Slice*); NC (*Network Configuration*).

Table 2. Overview of 5G security countermeasures

Domain	Threat	Countermeasures	References
User equipment	SIM credential theft	Store SIM credentials within hardware security module. Detect data exfiltration and identify abnormal processes. Identify compromised SIM cards and consider the chance of remotely changing the credentials.	[7]
Radio access network	UE DoS attack	Implement two-way authentication and SUPI encryption. Use signaling monitoring or network management system to identify the presence of false base station.	[8]-[13]
	Network DoS attack	Use network management system to monitor network key performance indicators and enable network access control.	
	5G authentication vulnerabilities	Deploy solution for fake base station detection.	
	5G user location tracking	Check configuration and frequently refresh temporary identifiers.	
	Radio jamming	Identify radio jamming equipment by using fake base station detection. Use measurement reports for identifying signatures of false base station.	
	Hijacked TCP connection eavesdropping	Establish network domain security. Implement IP-spoofing and replay protection, and TCP proxy in the network infrastructure.	
Core network	Core network DoS attack	Ensure equipment has a baseline security level. Deploy anti-DDoS devices, security edge protection proxies, signaling firewall.	[14]-[17]
	Voice call eavesdropping	Apply the latest security patches at the mobile switching center. Use privileged account monitoring to identify unauthorized access. Forward access logs to SIEM system and perform the root cause analysis.	
	SMS eavesdropping	Apply the latest security patches at short message service center. Review the privileges of network equipment users. End-point security solution and internal firewalls should raise alarms.	
	5G NEF API exploitation	Ensure network equipment has a baseline level of security. Ask vendors to provide test reports and have emergency response.	
	CDR harvesting	Apply the latest security patches at network and IT systems. Review the privileges of call data records database. Call data records databases and internal firewalls should raise alarms.	
Cloud	VM abusing	Develop virtualization security development policies for intrusion detection, security isolation, and security hardening. Coordinate security solutions included in all virtualized components.	[3]
	MEC DDoS attacks	Filter the packets heading for the target site under attack, restrict communication ports, reduce the operation of target facilities.	
	MEC APIs abusing	Develop security management specifications to prevent apps with security risks and deploy abuse prevention solution.	
	Unauthorized access to NS management plane	Enable authorization and authentication mechanisms. Implement domain and privilege management.	
	NS resource preemption	Enable proper network resource management mechanisms.	
	NS data theft and tampering	Delete residual data when slice resources are released. Enable network resource isolation and authorization mechanism.	
Operation and management	Detect theft or fraud	Deploy privileged access management and perform security audits. Improve the access control and authentication of accounts and permission. Deploy authentication, antimalware, and least privilege control.	[3]
	Exploitation of NC data weakness	Purchase tools for checking device security configurations. Improve the training of operation and maintenance personnel. Implement domain- and rights-based management.	
	Log tampering	Manage logs in a unified and centralized way. Protect the integrity of logs to prevent tampering. Use the situational awareness system to detect real-time/previous attacks.	
Service and application	Malicious applications	Not applicable.	[18]-[21]
	UE compromise	Provide DoS indicators and quick location for compromised UE.	
	Personal data theft	Not applicable.	

Legend: SIM (*Subscriber Identity Module*); DoS (*Denial of Service*); UE (*User Equipment*); IP (*Internet Protocol*); TCP (*Transmission Control Protocol*); NEF (*Network Exposure Function*); API (*Application Programming Interface*); SMS (*Short Message Service*); CDR (*Call Detail Records*); VM (*Virtual Machine*); MEC (*Multi-access Edge Computing*); NS (*Network Slice*); NC (*Network Configuration*); SIEM (*Security Information and Event Management*); IT (*Information Technology*); VM (*Virtual Machine*); SUPI (*Subscription Permanent Identifier*); DDoS (*Distributed Denial of Service*); MEC (*Multi-access Edge Computing*).

More detailed overview of challenges in the security of 5G networks is given in the ENISA report on threat landscape for 5G networks [22] and its update that encompasses all novelties introduced, captures developments in 5G architecture and summarizes information found in standardization documents [3]. In addition, there is specific report which focuses on 5G cybersecurity standardization from a technical and organizational perspective [23]. To ensure 5G network security, it is important that security requirements defined in the relevant 3GPP specifications are fully implemented and utilized [24]. In general, 5G should consider a more flexible security [25].

Based on security threats to date, the following next steps can be made on 5G networks [3][22]:

- Conduct a detailed gap analysis of the limitations for the protection of 5G network. In addition to organizational issues, such gap analysis will be required for migration/mitigation options;
- Develop good practices or guidelines for the secure implementation of 5G network, since they are an important step towards maintaining the final security level of 5G network;
- Perform a systematic analysis of operational and general-purpose models for security assurance processes to test their 5G adequacy and fill the identified gaps;
- Engage in discussions on 5G matters since experience in technical, organizational, and business issues of a 5G deployment are important for the generation of security guidance;
- Contribute to the 5G cybersecurity knowledge collection and dissemination.

References

[1] GSMA. (2019). The 5G Guide: A Reference for Operators. [Online]. Available at: https://studylib.net/doc/25387786/the-5g-guide-gsma-2019-04-29-

[2] Accenture Strategy. (2021). The Impact of 5G on the European Economy. [Online]. Available at: https://www.accenture.com/_acnmedia/PDF-144/Accenture-5G-WP-EU-Feb26.pdf?_sm_au_=iVVZRW54FHZ10n2PVkFHNKt0jRsMJ

[3] ENISA. (2020). ENISA Threat Landscape for 5G Networks Report. [Online]. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

[4] Cabrera, E. (2021). With 5G coming, it's time to plug security gaps. [Online]. Available at: https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html

[5] EC (2021). EU toolbox for 5G security: a set of robust and comprehensive measures for an EU coordinated approach to secure 5G networks, Publications Office. [Online]. Available at: https://data.europa.eu/doi/10.2759/500089

[6] ISO/IEC (2018). ISO/IEC 27000: 2018 Information technology – Security techniques – Information security management system. [Online]. Available at: https://www.iso.org/standard/73906.html

[7] Begley, J. & Scahill, J. (2015). How Spies Stole the Keys to the Encryption Castle. [Online]. Available at: https://theintercept.com/2015/02/19/great-sim-heist/

[8] Kim, H., Lee, J., Lee, E., Kim, Y. (2019). Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane. *IEEE Symposium on Security and Privacy (SP)*. San Francisco, CA, USA.

[9] 3GPP. (2009). 3GPP 33.821 - Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE). (Release 9). [Online]. Available at: https://www.3gpp.org/ftp/Specs/archive/33_series/33.821/

[10] Brunker, M. (2016). GPS Under Attack as Crooks, Rogue Workers Wage Electronic War. [Online]. Available at: https://www.nbcnews.com/news/us-news/gps-under-attack-crooks-rogue-workers-wage-electronic-war-n618761

[11] Basin, D., Dreier, J., Hirschi, L., Radomirović, S., Sasse, R., Stettler, V. (2018). A Formal Analysis of 5G Authentication. *ACM SIGSAC Conference on Computer and Communications Security*. Toronto Canada.

[12] Lakshmanan, N., Budhdev, N., Min, S. K., Mun, C. C., Han, J. (2021). A Stealthy Location Identification Attack Exploiting Carrier Aggregation in Cellular Networks. *The 30th USENIX Security Symposium*.

[13] Yqqlm. (2020). Tencent demonstrates 5G security vulnerabilities: can send counterfeit bank text messages to users. [Online]. Available at: https://www.yqqlm.com/2020/10/tencent-demonstrates-5g-security-vulnerabilitiescan-send-counterfeit-bank-text-messages-to-users/

[14] Reuters Staff. (2020). Vodafone hit by three-hour mobile network outage in Germany. [Online]. Available at: https://www.reuters.com/article/uk-vodafone-group-germany-idUKKBN2831WE

[15] 3GPP. (2021). 3GPP 33.926 - Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes (Release 17). [Online]. Available at: https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_102Bis-e/SA_91e/33926-h00.doc

[16] Leong, R., Perez, D., Tyler, D. (2019). MESSAGETAP: Who's Reading Your Text Messages. [Online]. Available at: https://www.mandiant.com/resources/messagetap-who-is-reading-your-text-messages

[17] Spadafora, A. (2021). T-Mobile data breach sees phone numbers and call records leaked online. [Online]. Available at: https://www.techradar.com/news/t-mobile-data-breach-sees-phone-numbers-and-call-records-leaked-online

[18] Cimpanu, C. (2020). Google removes 17 Android apps caught engaging in WAP billing fraud. [Online]. Available at: https://techrander.com/google-removes-17-android-apps/

[19] Gandhi, V. (2020). Joker Playing Hide-and-Seek with Google Play. [Online]. Available at: https://www.zscaler.com/blogs/security-research/joker-playing-hide-and-seek-google-play

[20] Clover, J. (2017). Security Researchers Use Wi-Fi and Safari Exploits to Breach iPhone 7 at Annual Mobile Pwn2Own Contest. [Online]. Available at: https://www.macrumors.com/2017/11/01/iphone-7-exploits-mobile-pwn2own-contest/

[21] Davis, J. (2020). Walgreens Reports Data Breach from Personal Mobile Messaging App Error. [Online]. Available at: https://healthitsecurity.com/news/walgreens-reports-data-breach-from-personal-mobile-messaging-app-error

[22] ENISA (2019). ENISA threat landscape for 5G Networks. [Online]. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[23] ENISA (2022). 5G Cybersecurity Standards. [Online]. Available at: https://www.enisa.europa.eu/publications/5g-cybersecurity-standards

[24] ENISA (2021). Security in 5G Specifications. [Online]. Available at: https://www.enisa.europa.eu/publications/security-in-5g-specifications

[25] Baraković, S., Kurtović, E., Božanović, O., Mirojević, A., Ljevaković, S., Jokić, A., Peranović, M., and Baraković Husić. J. (2016). Security Issues in Wireless Networks: An Overview. *BiHTEL 2016.*