International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

RELEVANCE OF CYBERSECURITY IN 5G NETWORK

Amulya Pathak[1], Tripti Dhote[2]

[1,2]Symbiosis Institute of Digital and Telecom Management,
Symbiosis International (Deemed University), Pune, India.
[2] tdhote@sidtm.edu.in

Abstract

As the world is moving fast-paced, the telecommunication sector is also under pressure of transforming and launching a new generation of the network to serve the changing needs of subscribers. The introduction of the 5G network will be an entirely new generation of technology having revolutionary characteristics like impressive speeds, fewer latency issues, and increased reliability over previous mobile technologies. As the 5G network is based on the software-defined network, cyberattack vulnerabilities will be the key issue. The success of this network will be determined by how well the Telecom companies are planning to combat the cyber-related risks by taking care of security challenges introduced by SDN, NFV, and 5G applications

Key words: 5G, Cloud Native Architecture, Cyber-security, SDN, NFV, IoT devices

Introduction

As countries are planning to roll out the 5G network, the shifting of the network from centralized, hardware-based to software network will be the stepping stone for creating a new ecosystem of applications and smart devices in this 21st century. The organizations have started developing 5G enterprise solutions leading to more innovations in the respective industry as digital transformation is unfolding and various technologies like cloud and IoT are becoming drivers for change. In this chain, 5G will act as an enabler as:

- It can expand its capacity to connect more people and devices.
- It will provide high data bandwidth which will have a range of 1GB-20GB and latency of 1 millisecond.

The key element of the 5G network is cloud virtualization technologies such as SDN (Software Defined Network) and NFV (Network Function Virtualisation) which will transform the landscape of the human-environment as 5G will easily support AR/VR applications, smart cities, autonomous vehicles, etc. But this will introduce a new kind of security concern. SDN/NFV is flexible and programmable. In SDN, the control plane and data plane for network elements are differentiated which leads to the open environment favourable for cyber-attacks. Another major component of having a security risk in the 5G network is unmanaged IoT devices.

According to Nokia's Threat Intelligence Report 2019, IOT devices contribute 78% in malware events happens in the communication service provider network.[1] Network security is the key issue that is to be resolved to strengthen the foundation of the 5G network and national security consequently. These cyber-threats in the 5G network will also cause effects on other dependent industries like financial services, automobiles, healthcare, gaming, etc.

Objective

Primarily, this paper seeks to study the importance of cybersecurity in the relevance of changing paradigms in the telecommunication industry as well as the probable hindrances on the way of 5G to be a success in this industry.

Review Of Literature And Framework Development

The literature review has been done extensively for this paper and covers the aspects of the changed architecture of 5G network and technological upgradations in the hardware as well as software. A thorough study of the role and relevance of these new elements has been done based on the previous research done in this field.

As everyone is in the race to introduce and adopt 5G technology for numerous benefits that are tagged along with new technology but a US report reveals that it is not a race just for 5G. It is a race to secure our nation, our citizens, and our economy. [2]

ITU specifies some key challenges for 5G rollout on a global scale. [3]

A published report suggests that the fourth Industrial Revolution will be fuelled by 5G communication and cybersecurity is going to be the direct threat for the expansion through it. [4]

Many companies underestimate the threat of DDoS, but 5G's faster speeds and greater mobility will undoubtedly make attacks even more destructive. [5]

Distributed Denial of Service (DDoS) threat might arise out of 5G devices due to a compromised Radio Access Network (RAN). [6]

Research also reveals that security improvements have been done in 5G over 4G [7]:

- Unified authentication
- Flexible security policy to address more use cases
- Encrypted transmission (SUPI) to avoid IMSI leakage and protect user privacy

Research suggests that the application of novel approaches to 5G security like Authentication and Key Agreement (AKA), Extensible Authentication Protocol (EAP)-based authentication and trust models. [8]

Stronger encryption, additional defence at the edge of the network, and introduction of technologies such as network function virtualization, mobile edge computer, and network slicing can make networks more secure. [9]

According to the standards set up by 3GPP, the security architecture of 5G technology gives us a review of the specifications about the technology which will affect the final performance.

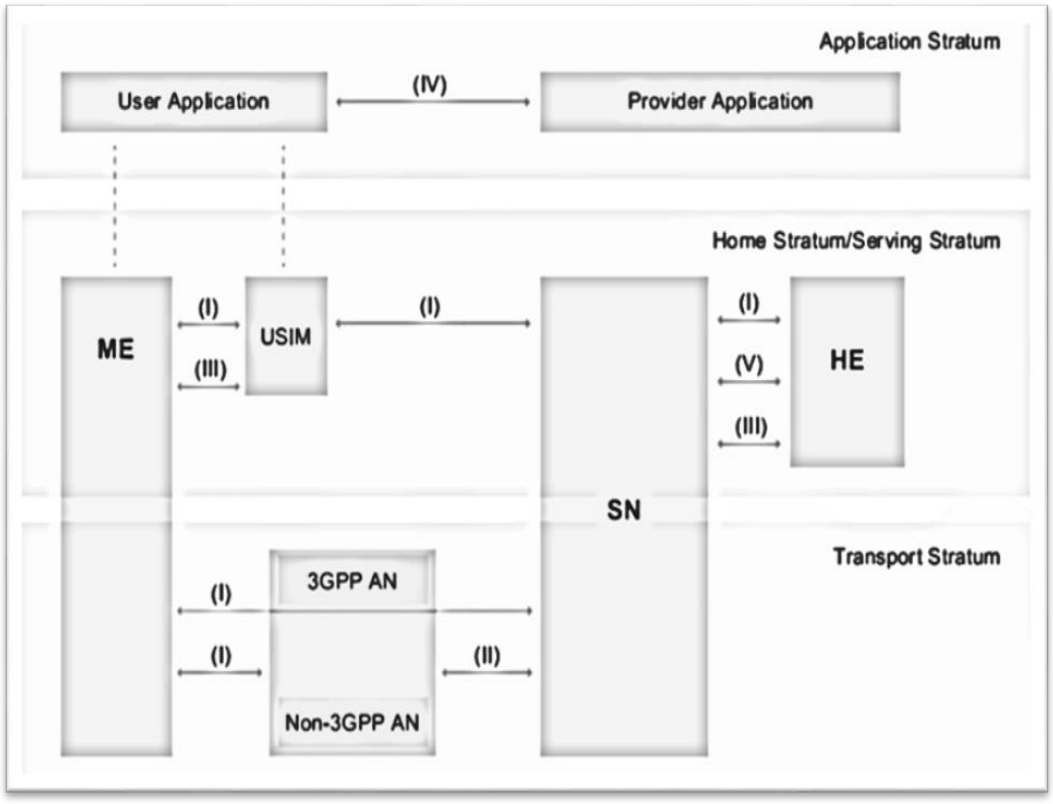

Fig.1: Security architecture of 5G network (Source: ETSI) [7]

Security domains of 5G network set up by 3GPP:

- Network access protection – Security features that allow a UE to securely access services through the network, and in to protect against attacks by wireless interfaces. It also requires transmission of the security background from SN to UE for the security of access.
- Network domain security – Security features set allowing network nodes to securely exchange signals, user plane data.
- Safety of the user domain - Security features collection which secures users to access mobile devices.
- Application domain security - The collection of security features that allow for the secure exchange of messages between applications in the user and the service provider domain.
- SBA domain security – Security apps set relating to SBA Safety. These include the security aspects of registration of the network application, discovery, and authorization, as well as the safety of the service-based interfaces.
- Visibility and configurability of protection - Collecting functionality to tell the user whether a security feature is in operation.

The study suggests that regulators should focus on all four strata. Rest every other stratum should be monitored based on the needs such as application stratum by the service provider, transport, serving, and home strata to be monitored by operators, underlying network equipment should be monitored by equipment vendors. These security challenges generated through the evolvement of technologies and architectures will be tackled by the synergy of all industries. [10]

Hence in this paper, we are aiming at finding all the possible threats attached to the 5G network in the era of technologies and IoT devices. We are also aiming at studying the application of IoT devices in connection with the 5G network and analysing the cyber-risks attached within.

Security Threats Vulnerabilities And Attacks

Various advancements in the network architecture of 5G such as cloud-native functions, decomposed RANs, network slicing, and virtualization is introducing the key concerns, not for service providers only but network operators, customers, and businesses. These advancements are contributing to the expansion of threats associated with every element of 5G network architecture.

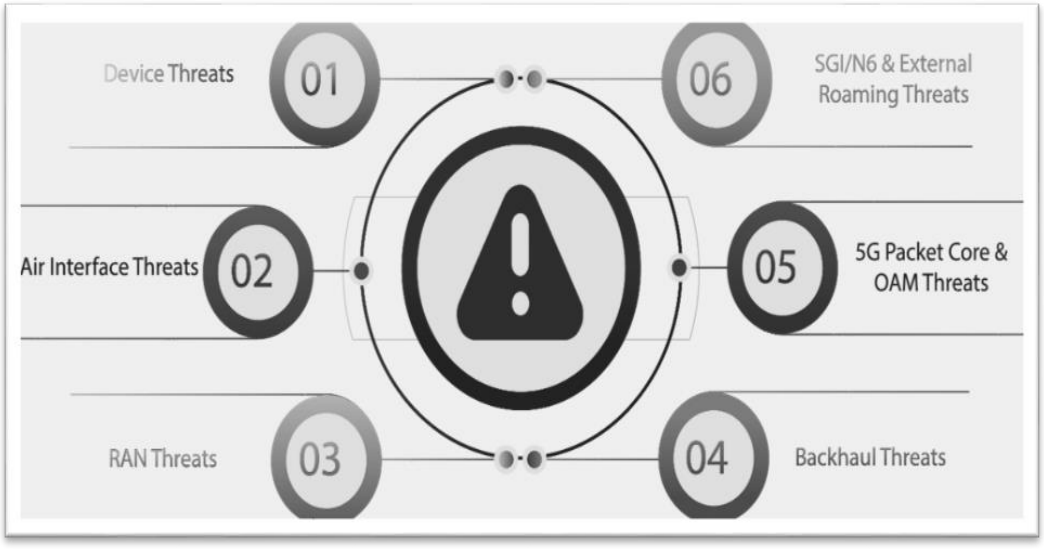

Fig.2: Security Threats (Created by the researcher)

These threats are categorized into three broad categories mainly:

Core Network Threats

These threats are associated with the parts of the network which is the core element of the network and includes SDN, NVF, NS, and MANO. These threats can result in severe cyber-attacks:

- Having remote access to the core network can lead to tampering the configuration data and malware attack.
- Loss of connectivity due to traffic spikes for authentication or authorization of any IoT device.
- The abuse done by a third party hosted network.
- Usage of APIs to exploit the different layers of the core network by targeting roaming interfaces, internal network functions, inter-networking interfaces, etc.
- The exploitation of design flaws in the architecture
- Fraud scenarios during roaming connections as the visited network ask the home network to authenticate the user.
- Extraction of sensitive information from SDN application servers known as memory scraping malware.
- Manipulation or flooding of network traffic and abuse of network configuration data
- Altering the settings in network orchestration
- Misuse of audit tools used by MNOs for monitor, optimization, and security purposes.
- Traffic sniffing of network data in SDN to get access to unencrypted valuable data.
- Threat on network elements of the data plane from side-channel attacks.
- Fraudulent usage of shared resource or end to end keys of centralized servers.

Access Network Threat

These threats refer to the threats associated with the wireless medium and radio transmission technology. In the 5G network, elements like 5G radio access technology (RAT), non-3GPP access technologies, radio access network (RAN) are in a vulnerable state for threats.[11]

- Attackers can use the ARP cache spoofing technique which helps the attacker to associate his MAC address with the IP address of any host to send ARP messages to do malicious actions.
- Other malicious tasks can be done by tampering the communication between UE and the network.
- Sending excessive requests on radio interfaces and flooding it.
- The exploitation of the victim's soft identity by exploiting cellular paging protocols.
- Intentional interference in the network radio frequency makes the services related to the core network unreachable for the victim users.
- Attacks like DoS can be done by forging the configuration data and hampering the working of base stations.
- Attackers can make the network resource unavailable by disrupting 5G RAN temporarily or indefinitely.
- Attackers plan to conduct other types of attacks by having full control over the specific traffic and stealing the legitimate authenticated conversation session ID.
- Bandwidth can be overloaded by the attacker's intentional signaling requests onto the network by using malware or apps.

Hardware &Other Common Threats

Threats related to underlying IT infrastructure or ICT system of a network falls under this category.

- Activities like Data breach, manipulation of information, leak, theft, etc., are possible threats to harming data security.
- Various network elements paves way for attackers to tamper the communication layers of these elements and helps them to do eavesdropping.
- The exploitation like a spectre, meltdown, and buffer flow, etc can be done in hardware element and software element.
- Malicious activities to be done to disrupt the services of a product by injecting software like ransomware, virus, SQL injections, virus, etc.
- Unauthorised access of user accounts, improper use of user identity, stealing user credentials, password cracking, and unauthenticated usage of devices by IoT group authentication.
- Natural calamity such as fires, floods, and earthquakes can make a huge impact on the equipment of the 5G network as a whole.
- Physical assets of the 5G network are aimed at stealing, disrupting, and disabling the services by doing deliberate physical attacks.
- DoS, fraud, etc, can be done on new protocols introduced for new UICC components in the new generation devices like eUICC, iUICC, soft SIM, etc.
- Data privacy and integrity are sacrificed because of low-cost insecure IoT devices which can be exploited by the attacker for misuse of data of users.
- Abuse of powerful computing infrastructure.
- Improper implementation of network slicing or improper isolation can hamper the integrity and confidentiality of data connected to the network and users.
- Unfair access of applications running on virtualized hosts, and abuse of shared resources on a shared virtualized environment.
- Certain vulnerabilities are attached to the Data Centres Interconnect (DCI) protocols which can be exploited by attackers.

Use Case

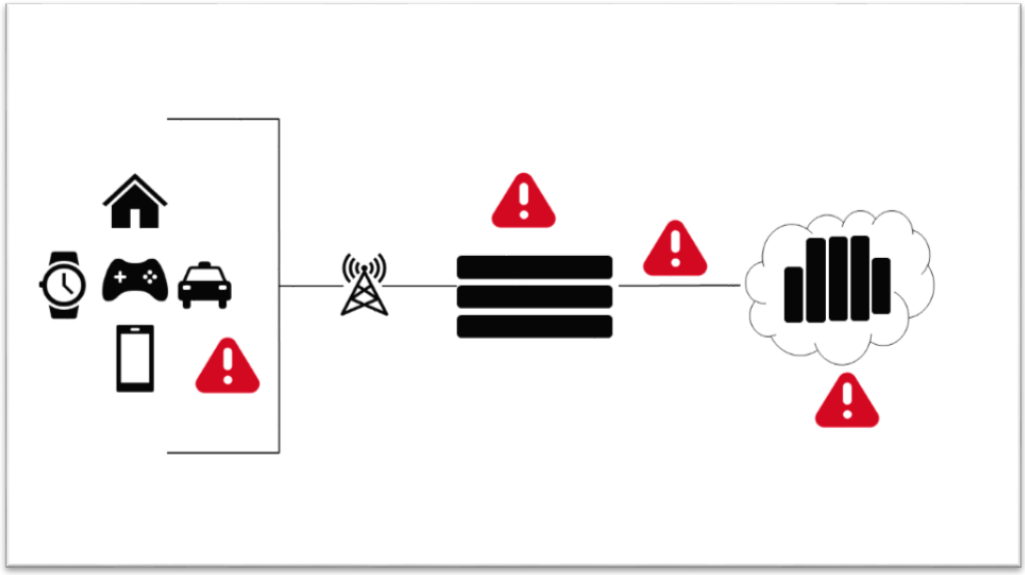

Fig 3: IoT architecture connected to the 5G network (Created by the researcher)

As the above picture reveals that the chances of threats are linked to different places in the architecture.

1) Low-cost insecure IoT devices which may be exploited by threats like firmware and OS hacks to target user data confidentiality and integrity. Spoofing of another device can be done on the network. Malware injection causing DoS will be another threat to IoT devices.
2) Flooding radio interface with requests to do other nefarious activities.
3) Shutdown due to malware injection and Usage of APIs to exploit the core network.
4) IoT Applications are injected with malicious code leading to Data Privacy leaks. Virtualised Mobile networks are arising chances of DoS & DDoS attacks on network slices due to artificial resource exhaustion, side-channel attacks across slices due to class attacks.

Research Methodology

This paper has a research strategy to explain the various challenges and threats associated with the security framework of 5G architecture with the evolution and implementation of ubiquitous 5G technology. A qualitative research approach and use case approach have been chosen for this study as qualitative methods are useful in getting insights about experiences from the implementation of technology in any given event. A thorough study of the network diagram is useful to understand and extract inferences that would be beneficial in understanding the challenges involved; considered as parameters in this qualitative study and how they would be crucial in the implementation of the 5G network. The methods used for this study include analysis of secondary data such as White Papers, Articles, Conference Papers, Research Papers, and Blogs. This research paper is based on a few important questions:

1. What are the threats that 5G is introducing along with the benefits?
2. Will 5G call for newer security requirements?
3. Are previous design approaches still valid?
4. How businesses and governments should think about these cybersecurity concerns?

Limitations And Scope Of Future Research

In this paper, the study of governmental aspects in the context of cybersecurity in 5G technology has not been included. The issue of cybersecurity will be resolved or can say lessened by the synergy of government regulators, network operators, service providers, and businesses. They should work towards the enhancement in the 5G infrastructure at all levels of supply chain management to ensure the best practices are to be followed by them to cater to the citizens and their privacy. 5 areas for best practices in cybersecurity management:

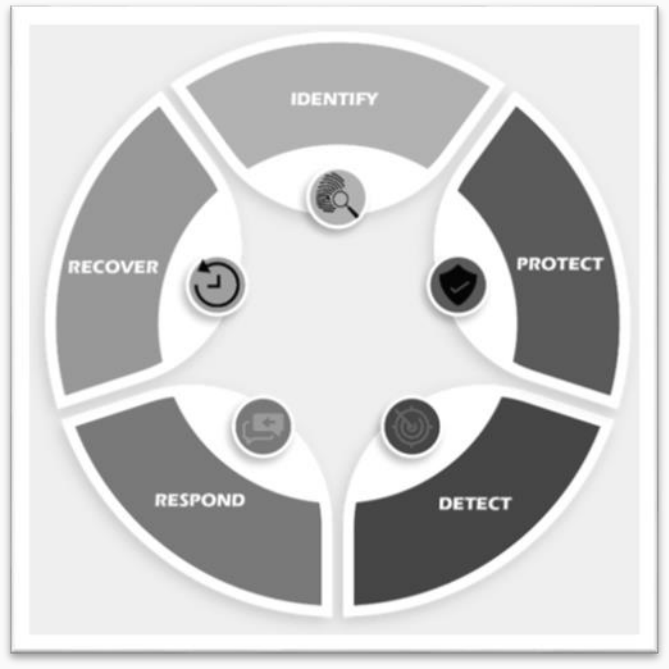

Fig. 4: Five best practices for cybersecurity (Created by the researcher)

As India is still working for introducing 5G technology, so the government regulators should do a balanced risk assessment having a focus on threat probabilities and their impacts on every level of the supply chain to get a broader perspective for formulating policies and standards in the field of cybersecurity. Cybersecurity is the issue related to national security and if compromised, can lead to severe cyber-crimes. Tensions between countries such as China and India will lead to thinking about the risk associated with tie-ups with Chinese industries. As claimed by US, various privacy issues and cyber-risk have been aroused due to the usage of Chinese equipment in U.S. networks. Is India self-sufficient enough to cope up with the cyber risks?

Managerial Implications

This paper is beneficial to the businesses and industries in forming a vision towards how to combat the key concerns arising due to threats associated with 5G. They should look out for the cybersecurity solutions to secure and strengthen their business system as well as their contribution to the privacy and security of the whole nation. This research can be taken forward by the Government to strengthen the cybersecurity of the nation. This may prove helpful for students and other researchers to get to know about the need for cybersecurity for every individual who is associated with or using 5G technology.

Conclusion

Security is the keystone of 5G technology towards catering to the widened threat surface by introducing enhanced security tools and mechanisms. The presence of IoT seems to raise more security issues, specifically in terms of privacy. As software advancements such as SDN, NFV, and cloud-native functions are introduced in the architecture of the 5G network, the vulnerabilities are increased on the software part. Data breach, DDoS attacks, eavesdropping, tampering the data, traffic sniffing of network data in SDN all these are the aftereffects of changed elements in the architecture. But these software upgradations can also be useful in solving these concerns by implementing the system of need-based security and proactive network forensics in the network. So, a careful approach should be adopted to improve the security which will be the deciding factor in terms of successful deployment as well as the functioning of this technology at large

References

1. Nokia, "Nokia Threat Intelligence Report 2019", Nokia, Espoo, Finland, 2019.Available:https://pages.nokia.com/T003B6-Threat-Intelligence-Report-2019.html.[Accessed 8-July 2020]

2. D. Simpson and T. Wheeler, "Why 5G requires new approaches to cybersecurity", Brookings online publication, 2019.

3. International Telecommunication Union, "Setting the Scene for 5G: Opportunities & Challenges", International Telecommunication Union, 2018.

4. P. Nair, "Why 5G is Changing our Approach to Security - Cisco Blogs", Cisco Blogs, 2020. [Online]. Available: https://blogs.cisco.com/sp/5g_secure. [Accessed: 22- Jun- 2020].

5. M. Sirbu, "Security concerns in a 5G era: are networks ready for massive DDoS attacks?", Scmagazineuk.com, 2019. [Online]. Available: https://www.scmagazineuk.com/security-concerns-5g-era-networks-ready-massive-ddos-attacks/article/1584554. [Accessed: 10- Jul- 2020].

6. What Are the Top 5G Security Challenges?", Sdxcentral, 2017. [Online]. Available: https://www.sdxcentral.com/5g/definitions/top-5g-security-challenges/. [Accessed: 02- Jul- 2020].

7. ETSI, "5G;Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.4.0 Release 15)", ETSI 3rd Generation Partnership Project (3GPP), 2019.

8. A. Prasad, S. Arumugam, S. B and A. Zugenmaier, "3GPP 5G Security", Journal of ICT Standardization, vol. 6, no. 1, pp. 137-158, 2018. Available: 10.13052/jicts2245-800x.619 [Accessed 22 May 2020].

9. "5G Security: How 5G will Impact Network and Cybersecurity", Verizon, 2020. [Online]. Available: https://www.verizon.com/about/our-company/5g/security-network-cybersecurity. [Accessed: 25- Jun- 2020].

10. Huawei, "Partnering with the industry for 5G security assurance", Huawei, 2019.Available: https://www-file.huawei.com/-/media/corporate/pdf/trust-center/huawei-5g-security-white-paper-4th.pdf

11. European Union Agency for Cybersecurity (ENISA), "ENISA Threat landscape for 5G networks", European Union Agency for Cybersecurity (ENISA), 2019.