A Survey of Common Attacks on 5GNetworks

Mukul Biswas[1], Keshav Kishore[2]
[1,2]*Research Scholar and Guie, Alakh Prakash GoyalShimla University, Shimla*

***Abstract*— Mobile networks are prime target for cyberattacks as they serve as backbone for digital commmunictaion. Smartphones becomes universal device to access the data, connectivity and information. Security is always a significant issue that should be tended to in a time where user and administrator are putting preventive measures against digital wrongdoing that incorporates refusal of cyber assaults, altering data, and information misleading, listening in sensitive communication, among others. These attacks leads to confidential data will be downloaded, transferred and handled through the impending 5G networks. Besides, the development of the 5G time requires the incorporation of numerous current trend setting innovations with creative new methods, which will bring about numerous new security breaches. Accordingly, in this paper, we present instances of possible dangers and attack vectors against the principle parts of 5G to reveal insight into the future security issues and difficulties in the impending 5G period. We will study and list the most common attacks and their possible mitigations.**

Index Terms: **5GCybersecurity, Wireless network, Network security, Attack vectors, Mitigations.**

INTRODUCTION

5G innovation is intended to convey higher multi-Gbps top information speeds, ultralow idleness, greater dependability, monstrous organization limit, expanded accessibility, and a more uniform client experience to more clients. Better execution and further developed effectiveness engage new client encounters and interfaces new businesses. .Network protection is the utilization of innovations, cycles and controls to safeguard frameworks, organizations, projects, gadgets and information from digital assaults.

It means to diminish the gamble of digital assaults and safeguard against the unapproved double-dealing of frameworks, organizations and innovations.

Architecture:

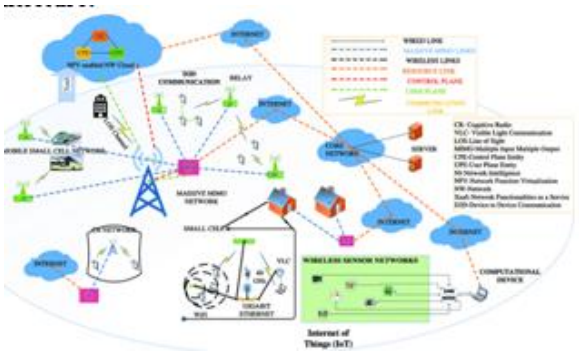

Fig: 1.1 commonly used structure of 5G Networks

The following elements are Example of 5G network 5Gnetwork are usually combination of one or more networks

1. Massive IoT
2. Internet
3. Enhance mobile broadband
4. VR/AR/MR
5. LTE/VOLTE
6. Cloud
7. Vehicular area network
8. Edge network

1 Massive IoT:5G networks extensively supports IoT. Smarts grids are one of the popular application of massive IoT. On IoT networks API manipulation and networks attacks are possible. The tools used for this attacks are Fiddler and malt go. For this attacks the security case study is botnet.

2 Internet.5G networks extensively support internet for better communication. WWW and website are the most popular platform of internet. On internet Dos/DDos, spoofing (DNS) are possible. The tools used for this attacks are NMAP and Metasploit. For this attacks the security case study is Russ and Ukraine cyber war

3 Enhance mobile broadband: 5G networks extensively supports enhance mobile broadband.

OTT is one of the popular application of enhance mobile broadband. On enhance mobile networks fishing and man in the middle attacks are possible .The tools used for this attacks are wire shark and Air cracking. For this attacks the security case study is credit card data thrifting.

4 VR/AR/MR:5G networks extensively supports VR/AR/MR. Gaming are one of the popular application of VR/AR/MR. On gaming piracy and impersonation attacks are possible. The tools used for this attacks are vomit and VoIP Crack. For this attacks the security case study is gamming station.

5 LTE/VOLTE: 5G networks extensively supports LTE/VOLTE. Video calling and video conferencing are the most popular application of LTE/VOLTE. On video calling and video conferencing Eps dropping and data thrifting attacks are possible. The tools used for this attacks are cloner (sim cloner/device), spy. For this attacks the security case study is video streaming.

6 Cloud: 5G networks extensively supports cloud. Pass, sash, ash are the most popular application of cloud. On cloud ransomware and hyper jackingattacks are possible. The tools used for this attacks are Scout Suite and gitops. For this attacks the security case study is data leak in cloud.

7 Vehicular area network:5G networks extensively supports Vehicular area network. Driverless car is the most popular platform of Vehicular area network. On Vehicular area network spamming and Broadcast Tampering attacks are possible. The tools used for this attacks are Spam Sieve and Mercury. For this attacks the security case study is data leak.

8 Edge network:5G networks extensively supports Edge network. Intelligence devices are one of the popular example of Edge network. On Edge network hardware hacking and privilege escalation attacks are possible. The tools used for this attacks are USB Kill and LAN turtle. For this attacks the security case study is smart device.

Cybersecurity is protecting your digital assets from hackers. It includes everything from securing your personal identity online to keeping your company's sensitive data safe. Cybersecurity professionals protect against cyber threats like viruses, hacking, phishing, ransomware, and other types of malware. They also help companies prevent data breaches and maintain compliance with regulations like HIPAA, PCI DSS, GLBA, FERPA, etc.

Network security involves protecting your computer network from unwanted access. This includes preventing unauthorized users from accessing your computer system, detecting attacks against your computer systems, and responding to those attacks.

Information security starts at the beginning of the development cycle. Security professionals should ensure that any code written will not compromise the integrity of the system. This means ensuring that all components are secure and that there are no vulnerabilities that can be exploited.

Operational Security is about making sure your data is safe and secure. It involves the processes and decisions for managing and protecting data assets. These include the permissions users have when accessing networks and the procedures that determine where and how data may be stored or accessed.

Cyber-security is about protecting your systems from attacks. You need to teach your employees what to do when they see something suspicious. For example, you should never click on links inside emails unless you trust them. If you plug in a USB drive, you should always unplug it immediately. And if you receive a suspicious attachment, you should report it to your IT department.

Cyber security is a major concern for organizations today. A cyber-attack could cause significant damage to an organization’s reputation, financial stability, and even physical safety. Organizations must therefore invest heavily in cybersecurity solutions to protect themselves against cyber-attacks. Cyber resilience is the ability of an organization to recover quickly after a cyber-attack. Business continuity plans help organizations mitigate the impact of a cyber-attack. These plans outline what steps will need to be taken to ensure that critical services continue to function during an emergency.

Endpoint security is a vital component of cybersecurity. Cybercriminals are constantly looking for ways to exploit vulnerabilities in software and hardware. Endpoints are the first line of defense against attacks. They are the entry point for hackers and malicious code. To prevent them from getting

through, you need to secure your system. You should always keep your operating system updated, install anti-malware programs, and run regular scans.

Elements	Example	Attacks	Tools	Security case study
1. Massive IoT	1.Smarts grids	1.Networks API manipulation 2.Networks attacks	1. Fiddler 2. malt go	Botnet
2. Internet	1. WWW 2. website	1. Dos/DDos 2. Spoofing (DNS)	1. NMAP 2. Metasploit	Russ and Ukraine cyber war
3.Enhance mobile broadband	1. OTT	1. Fishing 2. Man in the middle	1.wire shark 2.Air crack-ng	Credit card data thrifting.
4. VR/AR/MR	1.Gaming	1. piracy 2. impersonation	1. vomit 2.VoIP Crack	Gamming station.
5.LTE/VOLTE	1.Video calling 2.video conferencing	1. Eps dropping 2. data thrifting	1. cloner (sim cloner/device) 2. spy	video streaming
6. Cloud	1. Pass 2. sash 3.ash	1. ransomware 2. hyper jacking	1. Scout Suite 2. gitops	data leak in cloud
7.Vehicular area network	1. Driverless car	1. spamming 2.Broadcast Tampering	1.Spam Sieve 2. Mercury	data leak
8.Edge network	1.Intelligence devices	1.hardware hacking 2.privilege escalation	1. USBKill 2. LAN turtle	smart device

CONCLUSION

This review paper gives information about Common Attacks, used tools for the attacks and security case study on 5G Networks. The above-listed table describe the different element, example, attacks, used tools and the security case study. In this different way, the attacker can attacks in 5G networks elements and damage our confidential data and they also can leak our important information. The proposed work can also be extended to act as a guide for security specialist like, how we can secure our used networks elements more secure and how we can save our confidential data from attacker.

ACKNOWLEDGMENT

The authors would like to acknowledge the advice of the professors and those who previously worked in this area. The authors would also like to thank the reviewers for their suggestions to improve the quality of the paper.

REFERENCES

[1] https://resources.infosecinstitute.com/topic/top-19-tools-for-hardware-hacking-with-kali-linux/

[2] https://www.google.com/search?q=common+hardware+attacking+tool&sxsrf=ALiCzsaMJ2Pr-Tw5wTaxhyuYDXNKyFDi5A%3A1654782876287&ei=nPuhYu7wEP-VseMP26CyiA4&ved=0ahUKEwjurpXMwqD4AhX_SmwGHVuQDOEQ4dUDCA4&uact=5&oq=common+hardware+attacking+tool&gs_lcp=Cgdnd3Mtd2l6EAMyBQghEKABMggIIRAeEBYQHToHCCMQ6gIQJzoECCMQJzoFCAAQkQI6CgguEMcBENEDEEM6CwgAEIAEELEDEIMBOggIABCABBCxAzoECC4QQzoECAAQQzoFCAAQgAQ6CAgAELEDEIMBOgUILhCABDoKCAAQgAQQhwIQFDoGCAAQHhAWOggIABAeEA8QFjoHCCEQChCgATocECEQFUoECEEYAEoECEYYAFDoE1j3pAFgyakBaANwAXgAgAHDAogBrzWSAQkwLjEyLjE4LjGYAQCgAQGwAQrAAQE&sclient=gws-wiz

[3] Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020)

[4] IEEE Xplore Part Number:CFP20K25-ART; ISBN:978-1-7281-4889-2

[5] http://www.scribd.com/doc/84304292/Concepts-for-5g-Mobile-Networks
[6] Shameli-Sendi, A.; Aghababaei-Barzegar, R.; Cheriet, M. Taxonomy of Information Security Risk
[7] Assessment (ISRA). Comput. Secur. 2016, 57, 14–30.
[8] https://www.google.com/search?q=data+liksin+tool&sxsrf=ALiCzsZ3g24qGznbORR0UrB84oolwdhXVw%3A1654781833456&ei=ifehYtu-G_CBg8UPga2noAk&ved=0ahUKEwibp_TavqD4AhXwwKACHYHWCZQQ4dUDCA4&uact=5&oq=data+liksin+tool&gs_lcp=Cgdnd3Mtd2l6EAM6BQgAEJECOgcILhCxAxBDOgYIABAeEAc6BAgAEEM6BwguENQCEEM6BQgAEIAEOgoIABCABBCHAhAUOggIABAeEAcQCjoICAAQHhAIEAc6BggAEB4QDToICAAQHhAIEA06CAgAEB4QDxANOgoIABAeEA8QCBANSgQIQRgASgQIRhgAUABYypypgnzloAHABeACAAfQCiAGnFZIBBzAuNC43LjGYAQCgAQHAAQE&sclient=gws-wiz
[9] https://en.wikipedia.org/