Overview of 5G Security and Vulnerabilities

Shane Fonyi

ABSTRACT

The 5G wireless standard is currently in development and is slowly being rolled out to a few cities in the United States. There has been a concern for the security and overall architecture of the 5G standard from industry professionals and government officials. This paper will summarize the research done in the 5G security space and will provide an overview of the technologies used in 5G, the security built into 5G, and the vulnerabilities of 5G. The specific vulnerabilities researched are classified into the three pinnacle components of information security: confidentiality, integrity, and availability. The use of Internet of Things devices, medical collection devices, and massive device-to-device communications will also be discussed.

Keywords– 5G, security, wireless, vulnerabilities, LTE

I. INTRODUCTION

Launched in 1979 in Tokyo, Japan, the first generation (1G) cellular wireless network was established. By 1983, the United States had launched its first 1G network and several other countries followed suit. Fast forward 30 years and 4G Long Term Evolution (LTE) had been deployed to select cities in Norway, Sweden, and Finland. According to Statista, the number of LTE subscriptions in 2019 are estimated to reach 4.7 billion.[36] Throughout the evolution of wireless technology, the push to increase bandwidth and transmission speeds has been a catalyst for creating new wireless technology standards. Because of the increased abundance of transmission and technologies, wireless subscriptions are projected to rise. The large demand pushes industries to produce new technology that allows for greater innovation. Wireless speeds are tapering off worldwide as more devices come online and the allocated spectra in the respective countries are not able to keep up.[38] With this latest push for faster speeds and better coverage comes the 5G wireless standard. The speed of different generations over the years are shown in Table 1.[9]

The largest increase in bandwidth is from 4G LTE to 5G by looking at the table. Carriers are working to determine what 5G will look like as far as bandwidth goes. Verizon's current tests give an idea of what the standard user might be able to expect from 5G.[18] The 5G standard also includes a decrease in latency speed from 10 milliseconds to 1 millisecond.[4] With this jump in speed and a lower round trip time, new uses for wireless networking will come. A common phrase in the information security community is that innovation moves at the speed of light and security is often left behind. The rise of Internet of Things (IoT) devices brings its own set of confidentiality and availability issues.

When developing a newer, faster technology, it is imperative to determine the changes that need to be made to allow for its successful integration. In the case of 5G, there are several changes to the current 4G infrastructure that will be discussed. It is important to note that while 5G is being deployed, much of the 4G infrastructure will remain in place. The following will be discussed throughout the paper: an overview of 5G; security for 5G features; and possible vulnerabilities identified within 5G. The paper concludes with an accounting of the information presented and a summary of the most important outcomes of 5G and the security built into the standard.

Table 1: Wireless Generation Speeds

Generation	Dates	Speed
1G	1980s	Voice Only
2G	1990s	SMS (text only messages) introduced
2.5G	2001-2003	Data below 100 kbps, Multimedia Messaging introduced
3G	2003-2010	1-2 megabits per second download
4G	2010	2-10 megabits per second download
4G LTE	2010	10-20 megabits per second download
5G	2019	200-634 megabits download*

*Table information retrieved from [9]. *From [18]*

2. OVERVIEW OF 5G

At this time, there are no concrete standards for 5G. There are currently several organizations working on finalizing these standards, including the 3rd Generation Partnership Project (3GPP), the International Telecommunication Union (ITU), and the Internet Engineering Task Force (IETF). The 3GPP is an organization that brings together seven telecommunication standard development bodies into one group.[5] The IETF is an open international community of network professionals and researchers concerned with the future of internet architecture and operation.[29] The ITU is an international specialized agency, that is a part of the United Nations, for information and telecommunication technologies.[6] The ITU is the organization leading the charge for 5G standardization and has defined a timeline and project for submis-

sion and approval of 5G requirements called IMT-2020. The project was intended to determine and scope the requirements for the next generation networks in 2020 and the future. The 3GPP developed Release 15 for its 5G Phase 1 specifications and submitted to the ITU.[4] The 3GPP is currently working on Release 16: 5G Phase 2 specifications and soon plans to submit to the ITU before the proposal submission window closes in mid-2019. A timeline produced by a 3GPP partner, ETSI, can be viewed in Fig. 1 that displays the current 5G standards proposed timeline from the ITU and how the 3GPP plans to incorporate their findings. Currently, the minimum requirements for technical performance related to IMT-2020 were set in ITU-R M.2410 and are the following [32]:

- Peak Data Rate: 20 gigabits per second (Gbps) Download/10 Gbps Upload
- Peak Spectral Efficiencies: 30 bits per second per Hertz Downlink/15 bits per second per Hertz Uplink
- User Latency: 4 ms for enhanced mobile broadband (eMBB), 1 ms for ultra-reliable low latency communications (URLCC)
- Control Plane Latency: 10-20 ms
- Maximum Aggregated Bandwidth: 100 MHz for frequency bands <1 GHz/1 GHz for bands > 6 GHz
- Mobility: Usable up to 500 KPH in rural eMBB

From the requirements, the focus of the next generation network is adding more devices and increasing speeds to the user equipment.[32] User equipment (UE) includes home nodes, cell phones, computers, SCADA, ICS, IoT, etc. Any device that uses the cellular network to connect to the internet or to voice communications is UE in terms of wireless specifications. This broad range of devices makes it difficult to create specifications that allows the flexibility to incorporate the wide spectrum of devices. The proposal outlines an environment that will allow high speed communications from an end device to the internet and also very fast transactions between devices. This is where the URLCC comes into the fold to facilitate that type of quick communication. The timeline shown in Figure 1 shows that the expected finalization of the 5G standards will be early to mid 2020.[19] There are still proposal submissions that will be reviewed for final concurrence on whether they will be added to the final specification. This means that 5G is not a complete specification whether or not it is being deployed as changes will likely need to be made in order to keep with the requirements.

2.1 Changes to 4G Architecture

While 5G deploys to large cities, it will be configured in a mode called 5G NR Non-Standalone (NSA). This mode will use the 5G NR (New Radio) standards and continue to utilize the existing 4G core infrastructure.[40] The 5G NR standards include using spectrum sub-1 GHz, 1–6 GHz and above 6 GHz, including the mmWave frequencies above 24 GHz.[25] The FCC has made

offering mmWave frequencies available a priority.[10] The implementation of NSA is highly dependent on the carrier. From an interview with a 5G research group for major network provider in the US, their company plans to provide broadband internet to households and businesses using the 5G NR standards. These standards include the use of millimeter wave radio, multiple-input and multiple-output (MIMO), and beamforming to increase bandwidth and capacity of the radio link. During the transition to 5G, the current 4G bands (below 1 GHz) will still be utilized along with bands in the 6 GHz range and the bands above 24 GHz.

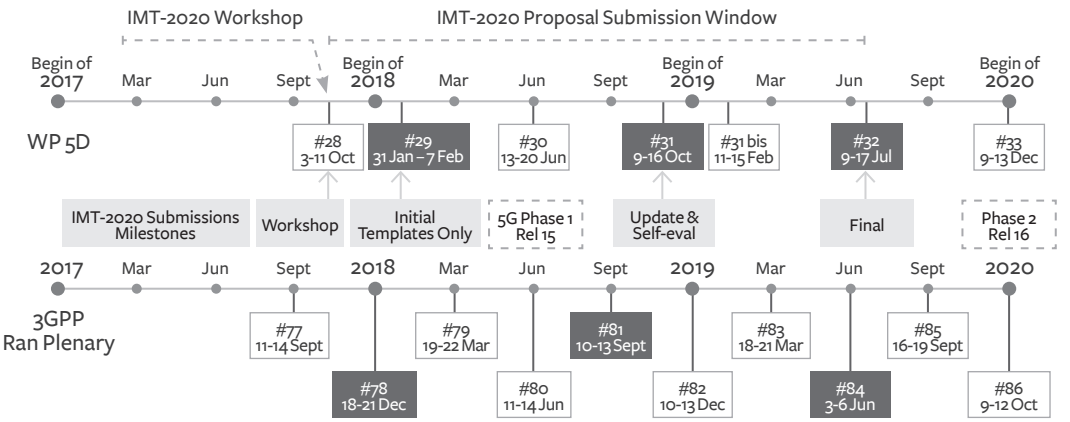

Figure 1: Timeline for 5G roll out and standards finalization. [19]

5G UE will also authenticate to the base stations differently using new authentication and key agreement methods (AKA). Where the UE authenticates will be important for the security analysis of 5G. Currently in 3G and 4G, mobile subscribers are equipped with Universal Subscriber Identity Module Cards (USIM) or colloquially known as SIM cards.[13] The idea for the use of USIM cards was for mutual authentication of UE to the networks it connects to in order to secure future communications.

5G architecture in standalone mode will include systems that will not be present in the current NSA model. The complete system will have eMBB, URLLC, and a massive Machine Type Communications (mMTC) like device-to-device communication. Mobile edge computing (MEC) will be added to the architecture in order to allow computational and storage intensive operations to be offloaded on these computing nodes attached to base stations.[21] This allows smaller hand-held and IoT devices to push graphic processing for augmented reality (AR) and other similar tasks to the network saving energy and CPU cycles.

5G will also be deployed using small cell radios. These access nodes operate in both licensed and unlicensed frequency spectra and have a range of 10 meters to several kilometers.[43] Due to the use of millimeter waves in the small cells, signal propagation is poor, therefore the distance radio waves can travel will be heavily limited, especially in densely populated areas.

To combat the issue of propagation, proposals have been made to integrate existing building wireless access, using the 2.4 GHz and 5 GHz IEEE 802.11 standards, to carry 5G data and allow UE equipment to connect to the cellular network without the need for extra equipment. Another feature of the 5G radios to help combat poor propagation is beamforming, a method of operating an antenna array to produce calculated signals that create constructive and destructive interference that form a concentration of signal in a specified location as represented in Fig. 2. Beamforming allows for improved signal and better data transfer speeds. The 5G networks will also include software defined networking (SDN) for hands-off, improved quality of service, and allowing device-to-device communications. With new architecture comes the ability to create much faster and more resilient networks. It also comes with challenges which are discussed in the next section.

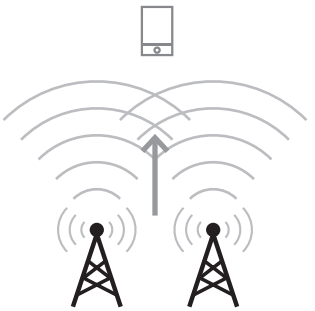

Figure 2: A basic visual representation of beam forming.

2.2 Challenges

With every new technology comes challenges that are inherent to the system or are newly introduced with the addition of features. Not all of the challenges faced are issues that will cause undue harm to the system. Some are merely items that, if left unattended, can cause the system to function erratically or cause further issues. Identifying these challenges ahead of time can have a significant positive impact on the total outcome of the introduced technology. In the case of 5G, there have been some items pointed out that need to be addressed before a stable system can be thoroughly vetted. With more devices being able to connect with the 5G network, there is a greater need for the ability to thwart attackers attempting to subvert authentication systems and causing a denial of service. These items are important to note and will be discussed below:

2.2.1 Trust Infrastructure

The architecture in 5G is based on a Public Key Infrastructure (PKI) system. A PKI system is one that uses cryptographic keys in order to establish identity. A public key and private key are created by a certification authority (CA) for each device. The private key should only ever be known to the device that needs an identity and the public key can be distributed to

any party that needs to encrypt messages to the device. The CA that creates these keys is trusted by all devices in the chain that need to check the validity of the certificates. When a device needs to connect, it will present a message signed by its private key to the authorization system. The authorization system will validate the message by decrypting it with the public key that corresponds to the private key of the device. The system will also verify that the public key it used was created by the trusted CA, so it knows the certificates are valid. If all these checks pass, the system will be able to confirm the identity of the device.

The PKI system is the current authentication mechanism in 4G with the cryptographic keys placed permanently on the USIM chips. The devices present their digital certificates to the base station, which then determines whether or not to allow the device on the network. Having permanent keys causes an issue when the number of UE increases substantially with the suspected adoption of 5G for IoT. If keys are compromised, carriers cannot reissue keys instantly. Replacing the USIM card is the only remediation for changing keys. In the current 4G space with an approximate 4.7 billion devices, it would be near impossible to replace even 10% of keys if a catastrophic event were to occur such as a breach that exposes the private keys of all the subscribers. Extrapolating to the proposed 5G space, that number becomes extremely large and even more unfeasible to handle. A solution would be a global adoption of a single large-scale PKI system.[33] It would be the responsibility of each carrier to opt into the global PKI in order to create a usable and seamless system. The specifics of issuing, replacing, recovering, and revoking keys has already been drawn out by the Internet Engineering Task Force.[15, 35, 23] The PKI system could also be used for devices to authenticate with each other before carrying out device-to-device communication that would not traverse through the carrier security equipment. Implementation could be baked into the 5G requirements and would add a significant layer of defense to the architecture.

2.2.2 Interconnection of Devices

One of the major milestones for 5G and one item of interest from mobile carriers is the introduction of IoT into the 5G space. IoT will allow for smart homes, smart cars, smart cities, or similar environments. These additions can make life easier in certain aspects; it also opens up the attack surface for abuse. There will now be more devices online and connected to the same network; this increases the number of potential eavesdropping devices, potential pivots for denial of service attacks, and potentially private data collection devices. If the current landscape of Industrial Control Systems (ICS) can be used as a guide, it should be noted that many of these devices very seldom get updates due to the need for thorough testing from manufacturers and end users.[37] Updates have to be planned and scheduled weeks, if not months, in advance. A significant amount of ICS equipment runs on old or outdated operating systems that cannot be patched due to the lack of support by the vendor.[37] Following that example would mean that many of these mass-produced devices will likely be left

without security updates and remain connected to home networks creating vulnerabilities and endangering the privacy and security of the people who live there.

3. SECURITY FOR 5G FEATURES

In the specifications for 5G, security was implemented at the beginning of its creation as all technologies developed in this day and age should strive to accomplish.[2] This is important for a couple of reasons. First, planning to add security on top of a product that already exists doesn't produce the best results. Think of an entrance to a house. A door is used to keep the elements out and segment different spaces. If security is not thought about before installing the door, it is added on after. This could be in the form of a chain or a latch. While these two components can help, having installed the door with a deadbolt and a metal frame would have been far more effective. Of course, this doesn't prevent a person from breaking in through a window or the roof. Second, it is harder to get users and providers to accept the security changes if they are used to operating without them. If a person enters their home without a key and all of sudden needs to use and keep track of a key, it can be hard to convince the person that it is useful without breaking into their home. So, while security is incorporated in the beginning, it is important to look for holes in the protocols.

3.1 HetNet

A heterogeneous network, or HetNet, is a combination of different powered radio nodes that cover an area to provide high throughput for a large number of devices.[39] In order to cover densely populated areas and areas with poor reception (e.g., office buildings, rural areas, intercity spaces, etc.), a heterogeneous network of cells is deployed to create coverage. An example of a HetNet is shown in Fig. 3. This network approach is an important feature of the 5G infrastructure. It will allow an extraordinary number of devices to connect and transfer large amounts of data that is not possible in the current LTE environment. HetNets allow for the ability to connect a multitude of devices and allow for the smart-enclaves.

Since endpoints connect to the strongest node with the highest signal-to-interference-plus-noise ratio (SINR), it is trivial to find the geographical region of a device. From Yang et al., adding randomness to the SINR can prevent determining the location of a device on a network.[41] In a HetNet, there are high powered nodes (HPNs) and low powered nodes (LPNs). These nodes tend to overlap in high-density areas and can create a load balancing problem. Yang et al. propose incorporating security-oriented mobile association policies to monitor and balance the loads of HPNs and LPNs thus increasing the secrecy performance of the connection.[41]

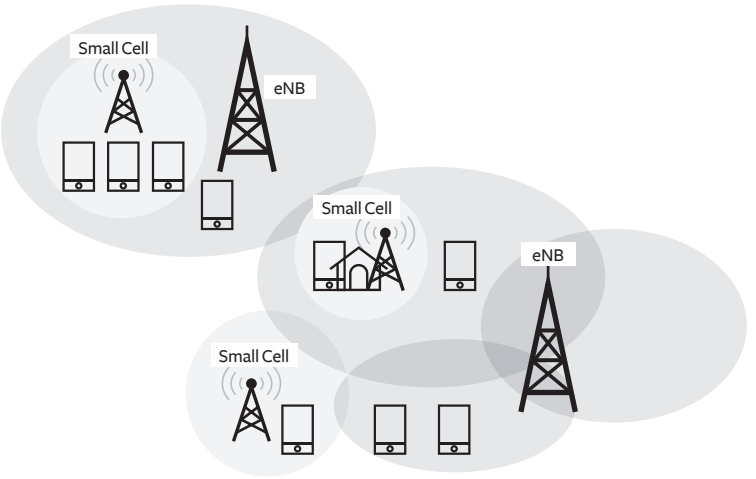

Figure 3: Illustration of a heterogeneous network.

3.2 Massive MIMO

Multiple Input Multiple Output (MIMO) is a technology that relies on several antennas to simultaneously transmit streams of data in wireless communications.[31] MIMO is currently in use on consumer-grade wireless access points and in the current 4G LTE architecture as well as GSM and CDMA communications.[26] Massive MIMO improves on its predecessor through the use of hundreds of antenna arrays allowing simultaneous access to several dozen endpoints in the same time-frequency domain.[31] Massive MIMO can allow for increased capacity on the frequency resource, significant reduction of latency over the air, and increases resiliency to intentional and unintentional interference.[31] Massive MIMO can produce beamforming as mentioned previously and allows for a shift in signal processing from the endpoint to the base stations (BS) and fits well within the specifications for 5G.[20] Massive MIMO can also increase the security of a connection. According to Chen et al., when a base station has a large enough number of antennas the proposed original symbol phase rotated secure trans- mission scheme can defend against an attacker with an unlimited number of antennas from decoding the original symbols.[14] This will keep a physical connection secure from eavesdropping.

3.3 Device-to-Device

The 5G standard introduces device-to-device communications (D2D). The purpose of D2D is to allow endpoints to communicate with each other without having to pass through base stations.[20] Communication traffic will be offloaded from base stations since no connection to the network infrastructure is needed. A primary application for this technology is the use of vehicle-to-vehicle (V2V) communication to facilitate self-driving cars and collision avoidance messages.[27] The V2V communication is also important for standard vehicles to communicate information to other drivers and even vehicles that are not self-driving. Security is a concern when allowing direct communication between UE. Taking into account all of the IoT devices that

will now be able to participate in D2D communications can cause concern. Several proposals attempt to improve the security of D2D communications. Ghanem and Ara produced a method of cooperation that takes into account distance between nodes as a security mechanism.[22] If a device believes that a connection to another based on distance can increase security, then it can make that request. The other end of the connection also calculates the path and decides to cooperate or suggests moving to keep the confidentiality of the connection intact and help avoid eavesdropping. The use of distance as a security parameter helps keep the connection more localized without having to pass through more network hops than needed. Using fewer network hops limits exposure to other devices that are also listening, but it does not completely solve that problem. Another solution proposed by Ghanem and Ara introduces a security scoring system (SeS) for measuring the protection of a connection.[7] The system calculates a score at the physical layer to detect attacks without needing to incorporate computation at higher levels of the software stack. The score produced is based on probabilistic characteristics of the transmitted data in a D2D connection. A few other solutions incorporate the use of a PKI system where devices create their own keys without the use of certificates. This form of verification would look more like a web-of-trust seen with PGP where devices verify each other removing the centralized management that is a single point of failure.

3.4 Software Defined Networking

Software Defined Networking (SDN) is becoming more popular as organizations move infrastructure to the cloud and virtualize the systems and applications that remain on-premise. SDN allows for the rapid implementation of routing rules and protocols to support an ever expanding and contracting network. In traditional networks, access control lists (ACLs) and routing statements need to be updated on every hop in a routing chain to allow for creations of new networks inside a large enclave. SDN solves this problem through centralizing the management of a network and allows for automation that can greatly expand the flexibility of a network and reduces workload. One of the solutions with 5G is the inclusion of SDN. With 5G, SDN will be needed to rapidly adjust routing between devices and automate the creation and modification of access control lists. It will allow for centralized management and facilitate D2D communication. Some potential for abuse comes with the centralized control plane. There is also still the ability to attack individual devices operating in the SDN. Some malicious behavior on SDNs and their causes are outlined by Dabbagh et al.[17]

4. SUMMARY OF VULNERABILITIES

From the current published standards and research conducted in the 5G community, some notable vulnerabilities have come to light. These vulnerabilities can be addressed in future standards releases, and some are expected to have mitigations in place when 5G standards are finalized. The vulnerabilities addressed in this paper are broken down into three sections: Confidentiality, Integrity, and Availability (CIA). The CIA triad, as it is known, is the cornerstone of security policy and dictates the most crucial components of security. Some of the following

findings are hold overs from 4G LTE that have yet to be addressed in current published standards. It is likely that several of them will be addressed in the future, however, some of the findings will be difficult to mitigate and as of 3GPP Release 15, they are still vulnerable.[33] An overview of security threats and their impact from this report can be found in Table 2.

Table 2: Summary of 5G Threats and Impacts

Security Principle	Threat	Impact
Confidentiality	AKA Attack Unsecured DNS Paging Broadcast	Spoofing Malware dropping MITM Location Determination
Integrity	Silent Downgrade AKA Attack	Phone/SMS snooping Subscriber Impersonation
Availability	Spectrum Slicing Attack Botnet Attack Paging Attack	Performance Degradation Denial of Service

4.1 Confidentiality

Confidentiality is the principle that sensitive data will be prevented from being released to parties that have no need or authority to access. In the case of cellular communications, that can mean text messages, phone calls, and internet traffic. In the 5G space with IoT, that can mean medical devices that collect data for practitioners or building control equipment that allows entry into an area. It is essential that this data be safeguarded from threats in order to prevent unintended leaks of personal or security data.

4.1.1 AKA Attacks

Authentication and Key Agreement (AKA) for 5G security and attacks are heavily researched in Borgaonkar et al, Basin et al., and Cremers and Dehnel-Wild.[13, 11, 16] Privacy was built into the standard for 3G and 4G authentication.[1, 3] Unfortunately, there have been weaknesses found in the AKA system that allows for false base stations attacks and IMSI catchers through non-protected identity request mechanisms and authentication failure messages.[13] These flaws allowed for the creation of StingRays, a device used by law enforcement to track users through their cellular devices.[42] The protocol is extremely important for controlling devices that are allowed on the network and maintaining the confidentiality of communications. From Cremers and Dehnel-Wild, the 5G-AKA protocol does not meet its own security requirements. It is shown that an attacker can access a service network in the name of a legitimate user other than itself.[16] The attack is possible due to insecure transportation methods used to transfer secret keys between UE and a base station required for authentication while a device is roaming. A real-world application of the attack would be dependent on how the network carrier implements its authentication mechanism. There are other known attacks against AKA that have been inherited from the 4G protocol standards.[13] In order for carriers to provide backward compatibility, the architecture from 4G will still be operational, and even while the

shift to 5G occurs, devices will still need to communicate with a 4G network first before being upgraded to 5G. In the current 5G AKA specification, a vulnerability was found that would allow an attacker to learn about the cellular consumption of a user through a replay attack from lack of randomness in the sequence number (SQN).[13] The SQN can be thought of as a token that allows access to a resource. This has major privacy implications since an attacker will be able to determine the time spent on phone calls, SMS statistics, and some web traffic usage. This attack works even while a user is not in range of an attacker's fake base station since a device will update the statistics when it returns in range of the false base station. This could mean that an attacker could determine the location and schedule of a user while only knowing the target's phone number.

4.1.2 Man-In-The-Middle

In the 5G space, Man-in-the-Middle (MITM) attacks are mostly resolved in theory with two-way authentication for the UE and the base station as well as service providers that are in the middle. This can prevent a false base station from sniffing traffic of the UE that connect directly to it. However, a flaw in the 5G-AKA standard described in Section 4.1.1 will allow an attacker to reuse authentication keys from a previous session to create a false base station.[11] This would open the door to surveillance devices, like the StingRay and other ISMI catchers that are used currently in LTE networks.

Aside from the issues with authentication, there has been research on the insufficient protection of DNS traffic.[34] Intercepting or poisoning DNS entries can create a whole host of issues. Changing legitimate DNS requests to return malicious IP addresses can allow the attacker to perform MITM attacks, steal credentials, and deploy remote malware.

4.1.3 Location Discovery

A Temporary Mobile Subscriber Identity (TMSI) is a randomly assigned credential given to a device by a network operator's Mobile Management Entity (MME). It is recommended that the TMSI for a device should be changed frequently.[24] However, in practice, this TMSI does not change often. When there are one or more pending services for a device, the MME asks a nearby base station(s) to broadcast a paging message, which includes the TMSI of the device. This makes the process of locating a device in an area a much simpler process. The attack involves determining the paging interval of a target through the use of sniffing traffic on the network and placing calls or texts at known times and allowing for a delay. The network will broadcast the paging notification and slowly an attacker can find the target device. Once the paging interval is known, a device can be tracked in any cellular area that the attacker has a sniffer in.

4.2 Integrity

Integrity is the principle of maintaining the accuracy and consistency of data from end point to end point, and it is important in wireless communications to prevent data from being

manipulated due to environmental factors or malicious actors. Wireless specifications often incorporate methods to re-transmit data in order to overcome disconnects or interference and to continue connections. It is important that this data is verified that it is exactly the same as what the device sent. The consequences for altered data accepted can be as benign as a glitch in a phone conversation to as catastrophic as power plants receiving the wrong control codes.

4.2.1 Message Alteration

In the current model, message authentication provides the verification of the source; however, there is no protection against the duplication or modification of the message.[20] Data transfer is much easier to alter when compared to voice communications. Since much of the data transfer security is reliant on the application the device is communicating with, it is difficult to remediate in the 5G space.

4.2.2 Message Spoofing

From the AKA attacks in Section 4.1.1, an attacker can spoof a device on a cellular network. That will allow for the attacker to send SMS messages and phone calls as the subscriber they are impersonating.

4.2.3 Silent Downgrade

When a UE attempts to connect to a base station, there is a negotiation that occurs where the UE and base station determines authentication mechanisms, speeds, and encryption. A malicious base station may be able to force the UE to downgrade to GSM, an older and less secure communication protocol, exploiting the pre-authentication messages. All a false base station would need to do is broadcast a valid Mobile Country and Network Code (MCC-MNC) combination for a network that has no public key provisioned in the USIM. This will allow for MITM attacks, phone call snooping, and SMS message snooping.[33]

4.3 Availability

Availability is the third leg of the CIA triad. This principle requires that all information systems be functional and accessible at all times. It is an important objective because, without availability, nothing else matters. If a system is not available, it is of no use to anyone. When dealing with cellular networking, an area being out of coverage can have major consequences. In this day and age, most users do not have landline telephones, and there are very few public telephones around. When life safety is involved, and communication is critical, the system that carries communications is vital.

4.3.1 DDOS

A distributed denial of service (DDOS) attack occurs when a malicious actor attempts to disrupt service to a commodity through the use of overburdening the system with fake requests and data traffic from a large number of devices. This attack is hard to circumvent and difficult to track down to a single root cause. In the 5G space, the inclusion of IoT will make this style

of attack much more devastating and potentially easier to orchestrate. Right now, there is not an abundance of non-mobile operating systems in the 4G LTE ecosystem, so the bar to abusing and compromising these devices is higher. When wireless cameras that are running on outdated versions of Linux with web servers becomes more common, it is not out of the realm of possibilities that an attack like the one seen with the Marai botnet will make its way to the 5G space.[30] It is especially important to include DDOS protections and mitigations in the standards and for network operators to work to thwart such efforts.

Infrastructure. As stated previously in 3.4, having a 5G SDN can alleviate many foreseen problems with connecting a massive amount of devices to a network, but it also creates some single points of failure. The control plane and the individual switches in the core infrastructure are targets for attempts to disrupt service in a large area.[8] An attempt to locate the control plane for the SDN and go after individual network components can have major negative effects if not properly defended.

With radio spectrum being a scarce resource, the practice of leveraging unused radio frequencies in a geographical area to use for 5G communications is included in the 5G proposals. [28] Using the frequencies set aside for government operations can provide benefits in areas where there are many devices attempting to communicate over the same frequencies and causing connection issues.[12] There is potential for abuse with this method when looking at how the 5G infrastructure handles off-loading the connections when a control signal from the military or government operations system attempts to broadcast on the reserved frequencies. If the equipment that is attempting to use the spectrum allocated for it cannot properly reach the 5G infrastructure to allow it to broadcast over the 5G equipment, then it can potentially cause a denial of service and hamper critical communications. More research will need to be done to determine how feasible that attack would be from a well-resourced threat actor.

User Equipment. As with the infrastructure, user equipment is vulnerable to DDOS conditions at an even higher rate. This equipment is likely not made to handle extremely high rates of data traffic. In current network topologies, these devices do not normally take the brunt of a network attack. Routing and switching equipment along with firewalls and intrusion prevention systems (IPS) will absorb most of a large DDOS attack by protecting the endpoints. In 5G with D2D communications, these devices are potentially exposed to such attacks from malicious actors that are in the vicinity of a target and have the capability to use other user equipment as a part of a botnet. From following previous attacks that are able to determine the location of a user, a threat actor can set up an attack using the devices in an area to launch against a specific target using the paging occasion hijacking discussed in 4.1.3. Preventing such an operation would be difficult unless a network operator could detect indicators of an attempt and perform mitigation.

CONCLUSION

This paper discusses the current landscape of 5G networking and security and attempts to bring all aspects of the environment together to create a thousand-foot view of the topic. There are many places where security can be built into the specification, where it currently is missing, or lacking specific details. As the 3GPP, ITU, and IETF work to produce the final specifications, there will undoubtedly be changes made and the network carriers will adjust their deployments to follow. It would be beneficial to revisit this topic when the final publications are made available and more carriers are involved in rolling out their versions of 5G networking. Since it is up to each carrier to implement the standards and core infrastructure, there will be variations in what is produced. From a security standpoint, trusting a standard will not be enough to determine the overall resiliency of a solution. Further testing will surely be done when 5G networks are more available. With the availability and relatively low-cost of software-defined radios (SDRs), testing these cellular networks will not be as difficult as it once was. As of now, there is no actual silver bullet that makes 5G unfeasible or wildly insecure. It will take time before all the standards in 5G are worked out and a stable system is produced. Until then, there should be some hesitation in using the 5G network for enterprise communications.

DISCLAIMER

The views expressed in this work are those of the author and do not reflect the official policy or position of he Army Cyber Institute, the United States Military Academy, the Department of the Army, or the Department of Defense.

Author Bio

Shane Fonyi

Shane Fonyi is a Cyber Research Integrator for the Army Cyber Institute at West Point (ACI). He is responsible for consulting with research teams at the ACI and other organizations to determine requirements and provide guidance on projects as well as developing and building the necessary IT infrastructure. He has been a speaker at several IT and Information Security conferences including BSides KC and the Conference on Higher Education in Kansas for work involved in IoT research and security awareness. He currently holds a Bachelor of Science in Electrical Engineering from The University of Kansas as well as several industry certifications including the CISSP, SSCP, CySA+, and GCFA. He is also an NYU Cyber Fellow at the NYU Tandon School of Engineering.

NOTES

1. 3GPP. 3G Security; Security Architecture. 15th ed. 3GPP, 2018. url: http://www.3gpp.org/DynaReport/33102.htm.
2. 3GPP. Security Architecture and Procedures for 5G System. Tech. rep. TR 33.501 V 15.4.0. 3GPP, Mar. 2019. url: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx? specificationId=3169.
3. 3GPP. Service Requirements for the Evolved Packet System (ETS). TS 122.278. 3GPP, 2018. url: http://www.3gpp.org/DynaReport/22278- CRs.htm.
4. 3GPP TR 21.915, "Release Description; Release 15". https://www.3gpp.org/ftp/Specs/archive/21_ series/21.915/21915-100.zip. Accessed: 2019-04-19. 2018.
5. About 3GPP Home. Accessed: 2019-04-30. 2019. url: https://www.3gpp.org/about-3gpp/about-3gpp.
6. About International Telecommunication Union (ITU). Accessed: 2019-04-2019. url: https://www.itu.int/en/about/Pages/default.aspx.
7. 1. Abualhaol and S. Muegge. "Securing D2D Wireless Links by Continuous Authenticity with Legitimacy Patterns". In: 2016 49th Hawaii Inter- national Conference on System Sciences (HICSS). Jan. 2016, 5763– 5771. doi: 10.1109/HICSS.2016.713.
8. Ijaz Ahmad et al. "5G security: Analysis of threats and solutions". In: 2017 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE. 2017, 193–199.
9. Grudi Associates. The Facts about 3g, 4g & LTE Wireless Service. Grudi Associates, 2012. url: https://grudiassociates.com/wp-content/uploads/The-Facts-About-3G-4G-LTE-.pdf.
10. "Auction of Upper 37 GHz, 39GHz, and 47 GHz Bands Critical to Ensuring United States Leadership in 5G". In: (July 2019). url: https://docs.fcc.gov/public/attachments/DOC-358397A1.pdf.
11. David Basin et al. "A formal analysis of 5G authentication". In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM. 2018, 1383–1396.
12. S. Bhattarai et al. "An Overview of Dynamic Spectrum Sharing: Ongoing Initiatives, Challenges, and a Roadmap for Future Research". In: IEEE Transactions on Cognitive Communications and Networking 2.2 (June 2016), 110–128. doi: 10.1109/TCCN.2016.2592921.
13. Borgaonkar, Ravishankar, Lucca Hirschi, Shinjo Park, and Altaf Shaik. "New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols." Proceedings on Privacy Enhancing Technologies 2019, no. 3 (2019): 108–27, https://doi.org/10.2478/popets-2019-0039.
14. B. Chen et al. "Original Symbol Phase Rotated Secure Transmission Against Powerful Massive MIMO Eavesdropper". In: IEEE Access 4 (2016), 3016–3025. issn: 2169-3536. doi: 10.1109/ACCESS.2016.2580673.
15. S. Chokhani et al. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. RFC 3647. RFC Editor, Nov. 2003.
16. Cas Cremers and Martin Dehnel-Wild. "Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion". In: Network and Distributed Systems Security (NDSS) Symposium 2019 (2019). doi: 10.14722/ndss.2019.23394.
17. Mehiar Dabbagh et al. "Software-defined networking security: pros and cons". In: IEEE Communications Magazine 53.6 (2015), 73–79.
18. Jessica Dolcourt. Testing Verizon's early 5G speeds was a mess, but I'm still excited about our data future. 2019. url: https://cnet.co/2V3Dzun.
19. ETSI. 5G Timeline. 2019. url: https://www.etsi.org/technologies/5g.
20. D. Fang, Y. Qian, and R. Q. Hu. "Security for 5G Mobile Wireless Networks". In: IEEE Access 6 (2018), 4850–4874. issn: 2169-3536. doi: 10.1109/ACCESS.2017.2779146.
21. Alex Galis et al. Mobile Edge Computing – An Important Ingredient of 5G Networks. 2016. url: https://bit.ly/2S5eyST.
22. Samah AM Ghanem and Munnujahan Ara. "Secure communications with D2D cooperation". In: 2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15). IEEE. 2015, 1–6.
23. R. Housley. Internationalization Updates to RFC 5280. RFC 8399. RFC Editor, May 2018.
24. Syed Rafiul Hussain et al. "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information". In: Network and Distributed Systems Security (NDSS) Symposium 2019 (2019). doi: 10. 14722/ndss.2019.23442.
25. Pablo Iacopino et al. The 5G era in the US. Tech. rep. GSM Association, 2018. url: https://www. gsmaintelligence.com/research/?file=4cbbdb475f24b3c5f5a93a2796a4aa28&download.

NOTES

26. "IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput". In: IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k- 2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009) (Oct. 2009), 1–565. doi: 10. 1109 / IEEESTD. 2009. 5307322.
27. National Instruments. Applications of Device-to-Device Communication in 5G Networks. 2019. url: https://spectrum.ieee. org/computing/networks/applications-of-devicetodevice-communication-in-5g- networks.
28. T. Irnich et al. "Spectrum sharing scenarios and resulting technical requirements for 5G systems". In: 2013 IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC Workshops). Sept. 2013, 127–132. doi: 10.1109/PIMRCW.2013.6707850.
29. ITEF | Who We Are. Accessed: 2019-04-30. 2019. url: https://www.ietf.org/about/who/.
30. Brian Krebs. Who Makes the IoT Things Under Attack? — Krebs on Security. 2019. url: https:// krebsonsecurity. com/2016/10/who-makes-the-iot-things-under-attack/.
31. Erik G Larsson et al. "Massive MIMO for next generation wireless systems". In: arXiv preprint arXiv:1304.6690 (2013).
32. Minimum requirements related to technical performance for IMT-2020 radio interface(s). Accessed: 2019-03-26. 2017. url: https://www.itu.int/pub/R-REP-M.2410-2017.
33. R. Piqueras Jover and V. Marojevic. "Security and Protocol Exploit Analysis of the 5G Specifications". In: IEEE Access 7 (2019), 24956–24963. issn: 2169-3536. doi: 10.1109/ACCESS.2019.2899254.
34. David Rupprecht et al. "Breaking LTE on layer two". In: IEEE Symposium on Security & Privacy (SP). 2019.
35. S. Santesson et al. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 6960. http:// www.rfc-editor.org/rfc/rfc6960.txt. RFC Editor, June 2013. url: http://www.rfc-editor.org/rfc/rfc6960.txt.
36. Statista. LTE subscriptions worldwide 2018-2023. 2019. url: https://bit.ly/2JkOe1B.
37. Keith A. Stouffer, Joseph A. Falco, and Karen A. Scarfone. SP 800-82. Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC). Tech. rep. Gaithersburg, MD, United States, 2011.
38. The State of LTE (February 2018). Feb. 2018. url: https://www.opensignal.com/reports/2018/02/state-of-lte.
39. Jeanette Wannstrom and Keith Mallinson. HetNet/Small Cells. 2019. url:https://www.3gpp.org/hetnet.
40. Cisco Wireless. 5G Non-Standalone Solution Overview. Accessed: 2019-04-2018. url: https://www.cisco.com/c/en/us/ td/docs/wireless/asr_5000/21-5_N5-8/5G-NSA/21-5-5G-NSA-Solution-Guide/21-5- 5G-NSA-Solutions-Guide_chapter_01.pdf.
41. Nan Yang et al. "Safeguarding 5G wireless communication networks using physical layer security". In: IEEE Communications Magazine 53.4 (2015), 20–27.
42. Kim Zetter et al. Florida Cops' Secret Weapon: Warrantless Cellphone Tracking. 2014. url https://www.wired.com/2014/03/ stingray/.
43. Haijun Zhang et al. "Coexistence of Wi-Fi and heterogeneous small cell networks sharing unlicensed spectrum". In: IEEE Communications Magazine 53.3 (2015), 158–164.