Vulnerabilities: (Megan)

**** First being the highest ranked vulnerability and last being the least ****

IoT Devices

- Internet of Things refers to devices other than, for instance, a phone transmitting data through 5G networks. Nowadays devices such a security systems, cars, sensors, and many many more, transmit data through the internet, which can provide an environment for data breaches and security risks for all of these devices

Data Collection

- Since 5G networks have huge connectivity and transfer capabilities, devices collect large amounts of data, which creates issues with privacy and personal information breaches.

Network Vulnerabilities

- As 5G networks have many moving parts, some of these provide a means of vulnerability, such as network slicing and virtualization. At the base level of the network core, these new features can also create data breaches and vulnerabilities to the system within

Location Tracking

- Most devices have some sort of location tracking capabilities and since 5G requires more base stations even the location of the base station can cause a threat to individuals as it shows a more precise

Supply Chain Risks

- Since 5G is so widespread, there are very few suppliers aside from the main companies. Additionally since 5G networks are more heavily software oriented as opposed to hardware, if a large supplier has a data breach it will affect large amounts of devices.

Attacks: (Megan)

**** First being the highest ranked attack and last being the least ****

Denial-of-service (DoS) attacks

- These attacks involve an attacker flooding the targeting host or network until it crashes or can no longer be used. This creates an environment where users are unable to access the system as it is no longer accepting requests due to the overload.

Configuration attacks

- These types of attacks involve not encrypting files or software allowing hackers to access and potentially your entire network.

Man-in-the-middle attacks

- This involves a third party introduced into the middle of two communicating parties. The two parties attacked usually are computer systems with a server or a server and a web app. When the third party “jumps in the middle” it now can access the information being transmitted between the two parties.

Distributed denial-of-service (DDoS) attacks

- These are similar to DoS attacks except there are multiple machines flooding the resource instead of a single one. DDoS are harder to track as the location is coming from multiple servers. Additionally, the attack is faster and can flood the system with more things as there are multiple systems in play.

SQL injection

- These attacks involve SQL code being inserted into a vulnerable system. These types of files are able to collect query results and give new commands that are able to perform originally prohibited actions.

DNS Tunneling

- This attack exploits the DNS protocol to bring malware through the client server model. A domain is made that brings individuals to the attackers server which has malware installed. The malware is able to access through a firewall and gain access to critical data. These attacks are hard to track as there is no direct connection between the attacker and the victim.

Phishing

- This attack typically involves messages or emails that have corrupted links or offers. They usually involve some sort of incentive to click said link and enter information so the intruder can steal information and eventually infiltrate your system or an account of some sort.

Malware

- This attack involves inserting corrupted software into a targeted system. Some of the types of malware involve spyware and ransomware.

Social engineering

- This type of attack is less software based and involves emotional and psychological manipulation to the target. After the manipulation, typically the attacker is able to gain enough information to sensitive private information to allow them to gain access to their systems