The main cyber threats to 5g

Sociology, Communication

There has been an exponential increase in technology innovation and an equivalent incline in the number of threats that consistently take advantages of the vulnerabilities in these innovations. Unfortunately, cyber security is nowhere at par with these malicious hackers. 5G is another improved service that has been built and is set to be launched for year 2020. This technology poses vast amount of various threats. This write up will analyze these threats and try to proffer solutions and examine a number of potential 5G security mechanisms. We conclude this section with some proposals for the next steps towards specifying the 5G security architecture.

Explaination Of The Threat Exposure Brought In By 5g

5G is a state of the art innovation that supersedes its predecessor (4G) in more than one way, such as faster speed, lower latency, better coverage, higher connectivity density, better throughput and better efficiency. The enhancements also presents better platforms for threats to be propagated.

The question now is what are the new security threat that 5G will bring and what are the mitigations to reduce the risk of its user being attacked since it has also provided open doors for malicious actors to carry out their activities?

5G brings a devastating advantage for cyberattacks such as eaves dropping, Denial of service, Rogue devices, Equipment cloning, Impersonation attacks, data manipulation, unprotected endpoint entry, to mention a few. 5G aims to reduce latency to 1ms and increase speed to 10Gbps, which unfortunately gives hackers the fastest malware delivery opportunity and the ability to create better persistent threats. The technology presents a platform for operation of the Internet of Things, virtual reality, cloud, autonomous driving, e-health, and many others, which implies that so many devices are coming in to the network. Therefore the internet is not just going to contain an exponentially increased number connected human users but machine to machine communication will take the lead. The huge amount of data that will gush out of this usage will be good news to the bad actors as this equates an increased probability of creating the largest scaled attack. Device cloning can be done to cause a denial of service attack or even worse a distributed denial of service. Weaponisation of these machines can be done such that they begin to operate in ways they are not built to do, to the detriment of the user and the world at large. More human users' leads to more phishing attacks and with humans being a weak link in a network, it is sure that 3 out of 10 phishing attacks will be successful.

Solutions To The Threats

The solution however, is that security is built into the core of 5G as it evolves. Such that it will be able to withstand all of these attacks. Therefore, all security rules for 4G and 3G still remain, but, the fact that it serves as a bases for some new technologies would imply that the security dynamics will change. Security focus areas should spans across: Identity management, IoT security, Data intergrity, and building trust worthy cloud.

Identity management

Identity management is the process of, authenticating and authorizing users to have access to applications, information systems or networks and mapping rights and limitations with the established identities. Simply put, it's the ability of the system to confirm that a user is who he/she claims to be or not. One of the fore front security measures is to control who can access or manage a resources on your network. The process of identity management includes: single authentication or 2 way authentication, authorization, role based identity, directory, single sign on, the use of tokens, provisioning, de-provisioning and managing the identities life cycle.

Securing Internet of Things

Internet of things are devices that have a toggle switch for on or off that can be connected to the internet. There are so many devices that are being manufactured that fall into this category such as smart headset, smart fridge, Television, toaster, microwave, webcam, door, etc. The implication is that people will rely on these items to run both their personal and work life, thus, so many data will be generated and stored safely. The question is how safe is the data, or the device itself? Securing IoT requires 3 steps.

securing the devices where data is collected

securing the cloud where it is sent

securing lifecycle management of the various components.

IoT products that are sold off the shelf are mostly with the unpatched operating system. Futhermore, user often don’t change the password or use very weak passwords that can be hacked. Therefore to improve the security, IoT should be placed in an isolated network that have restricted network access. The Isolated network should be contantly monitored for any malicious traffic. The use of Application Programming Interface (API) to secure IoT by monitoring the traffic between all communicating devices and protects the IoT from misuse by covering it with security procedures and policies.

5g data security

4G has been able to come up with very strong encryption for data. It is therefore expected for 5G to use 4G as a bases for data encryption. The European Telecommunications Standards Institute (ETSI) Technical Committee on Cybersecurity released two encryption specifications that could be key for access control in IoT and 5G, since they are highly distributed systems. It employs Attribute Based Encryption (ABE) technique that combines both encryption and access control together to ensure security. ABE is a public form of encryption that can be used in a multiparty data transfer. It inputs attributes of the receivers into the Internal Vector that is added to the encryption mechanism to produce a cipher text. However, an access control process is done before decryption can take place. The receivers has to satisfy the attributes and the access control attribute before he can begin decryption. This attributes cannot be determined by the hacker and since he doesn’t have any of the attribute, the message can never be decrypted. ABE is use when there are more than two users involved and it has proven to be very secure as it first of all defines personal data protection on IoT devices, Wireless Land Area Network, Cloud, and mobile services, Secondly, a trust models, functions, and protocols to control access to data for decryption is built.

Security at the organizations level

Organisations that have evolved to support the 5G network would have ensure their security is upgraded. Some of the upgrade can include: a. The conventional use of anti virus, fire walls and upgraded access controls such as biometrics, to minimize user-induced risk. Intrusion detection and prevention tools to block basic security threats. All of these form part of the basic filters for the networkb. The used of behavior based tools to check endpoints for malware attacks that could have been built to evaded the first set of basic filters. After which an action to remove all instances of this detected malware be automatically expunged from the network and noted to be blocked going forwardc. Using anomaly detection in your network switches and routers has proven to be effective because, it converts these devices to security sensors. d. Domain name servers are major threat vector as at today. Monitoring the activities of the DNS is very germane to protecting networke. Ensure thrusted sources are gotten to provide instant and accurate information on current cyber threat worldwide.

Building a thrust worthy cloud

The huge wave of data we are expecting in the nearest future as a result of the explosion of IoT and 5G networks will have to be saved some where safe – cloud. Cloud can be attacked with data breaches, Denial of service, data loss, account hijacking, and so on. Therefore, users and companies should be worried about the safety of their private data. It is therefore paramount that 5G help to build a secure cloud to store all of the data that will be generated. Securing a cloud requires the following: Data encryption, key management, Media protection, Identification, authentication, authorization, virtualization and resource abstraction, Application security, security risk assessment and management, privacy, contingency planning, maintenance, Incident response, Compliance, audit and accountability, awareness and training.