Network Security
Professor Gaurav S. Kasbekar
Department of Electrical Engineering
Indian Institute of Technology, Bombay
Week - 08
Lecture - 50
Wireless Cellular Network Security : Part 8

Hello, in the previous several lectures, we discussed the security of 2G, 3G, and 4G cellular systems. In this lecture, we will discuss 5G network security. Since we have already devoted a lot of time to discussing 4G security in detail, this discussion of 5G network security will be brief. There are many similarities between the security systems in 4G and 5G, so we will only discuss the salient features of 5G security. So first, what is the need for security in 5G networks?

5G radio access networks support massive IoT services, or Internet of Things services. Here, a large number of resource-constrained devices, such as sensors and actuators, send their traffic to the network. Typically, there are hundreds of IoT devices present in an area. So, information is sent from a large number of IoT devices to the network.

Hackers could exploit this to potentially overload the radio access network through Distributed Denial of Service (DDoS) attacks if the network is left unprotected. So, this is one reason for adding security features to 5G networks. Another reason is that 5G uses edge computing and small cells that are deployed close to the subscribers and devices. Hence, this infrastructure needs to be protected. It can be tampered by subscribers and users or some hackers who are present in the vicinity of the subscribers.

This creates new means by which hackers can attack the network. Another reason is that 5G caters to mission critical use cases such as robotic surgeries. So, these are mission critical use cases and there is an additional need for security in such cases. Preventing hackers from exploiting zero-day vulnerabilities is critical. So, zero-day vulnerabilities are those which are discovered by hackers but which are not known to the security community.

So, one needs to prevent hackers from exploiting such zero-day vulnerabilities. So, what are the security features in 5G networks? One feature is that 5G achieves network segmentation through network slicing. So, we'll not discuss network slicing in detail, but the idea is that the network right from the core network to the radio access network is divided into logical parts called slices or network slices. So, different network slices are allocated to different applications or to different users.

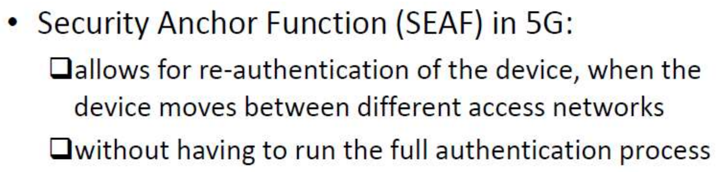
Because of this network slicing, attacks or faults that occur in one slice do not have an impact on other slices. So, this creates a separation between different parts of the network. Even if there are attacks or faults in one slice, since the different slices are isolated from each other, these attacks or faults do not have an impact on other slices. Another security feature in 5G networks is that 5G supports “Home Control” features for preventing network spoofing attacks. An attacker creates a false base station and sends signaling messages to the UE to try to extract information from the UE.

The home control feature authenticates the device location in roaming scenarios. When the user moves from the range of their home network to the range of another network—that is, when they roam to a foreign network. In that case, the home control feature is used to authenticate the device location to find out where the user actually is roaming. When a device is roaming, the home network verifies if the device is actually present in the serving network before allowing the user to roam in the visited network. So, this fixes a known vulnerability in the previous generation networks, namely 3G and 4G, where networks could be spoofed.

In particular, the vulnerability is this: sending false signaling messages to the home network to request the IMSI and device location. This is data that could be used to intercept voice calls and text messages. So, because of this home control feature, this vulnerability in 3G and 4G systems is mitigated. Another feature in 5G is that it provides native support for EAP, or Extensible Authentication Protocol. Recall that we discussed EAP in the context of Wi-Fi.

It is not one authentication protocol but a framework in which many authentication protocols can be supported. So, the use of EAP allows new authentication methods to be plugged into the network by the service provider. So, if some flaws or vulnerabilities are discovered in one authentication method, then it can be replaced with another authentication method. Another advantage of using EAP in 5G is that it homogenizes the authentication method for 3GPP and non-3GPP systems, such as 5G and Wi-Fi systems. We already discussed that EAP is used for authentication in Wi-Fi systems.

5G is a 3GPP system and Wi-Fi is a non-3GPP system. In particular, it’s based on an IEEE standard. Since EAP is used in Wi-Fi as well as in 5G, hence, the authentication method used in 3GPP and non-3GPP systems is homogenized. Another important security feature in 5G networks is Security Anchor Function (SEAF). It allows for efficient re-authentication of the device when the device moves between different access networks.

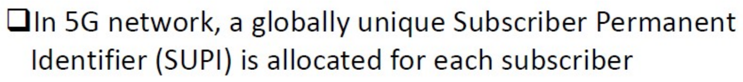


- Security Anchor Function (SEAF) in 5G:
  - ❑allows for re-authentication of the device, when the device moves between different access networks
  - ❑without having to run the full authentication process

It is not necessary to perform the authentication process from scratch. So, the full authentication process doesn't have to be run all over again. So, the SEAF function allows for efficient re-authentication of the device when it moves between different access networks. SEAF is now part of the Access and Mobility Management function (AMF) in the 5G core. Just like 4G, the 5G network also supports mutual authentication between the UE and the network.

That is, the UE authenticates the network and the network authenticates the UE. 5G also supports subscriber identifier privacy. So, we discussed the use of IMSI and TMSI in 3G networks and then we discussed that GUTI is an identifier used in LTE as a placeholder in place of the IMSI. Similarly, 5G supports subscriber identifier privacy. In 3G and 4G networks, the IMSI is shared with the network during the connection establishment process.

In a 5G network, a globally unique Subscriber Permanent Identifier called SUPI is allocated to each subscriber. The SUPI is not shared during the connection establishment process. Instead, a temporary identifier called SUCI, which stands for Subscriber Concealed Identifier, is shared with the network until the subscriber or device is authenticated. This helps prevent attackers from tracking a subscriber. This feature also protects subscribers from rogue base stations in the network.



❑In 5G network, a globally unique Subscriber Permanent Identifier (SUPI) is allocated for each subscriber

These rogue base stations may try to steal the identities of subscribers. So, sending the temporary SUCI instead of the permanent SUPI, that helps in protecting subscribers from rouge base stations. Next, 5G also has features for protecting the edge computing infrastructure. The edge computing infrastructure is a vulnerable entity in 5G networks since it is deployed at the edge of the network. It is away from the core network and can be accessed by hackers.

The risk can be minimized by deploying endpoint protection software in edge computing nodes. So, this is software that can be used to defend against several attacks. Monitoring can also be implemented to provide enhanced visibility of edge computing applications, services, and infrastructure components. For example, one can track the activities of various logged-in administrators to detect any malicious actions by them. One can also collect system resource utilization.

So, this helps in monitoring and managing the network. Another example is system performance snapshots at various time intervals. So, these help in debugging, monitoring, and maintenance. Since edge computing services are open to several third parties for running their own custom applications, it's better to deploy firewalls for distributed denial-of-service protection, malware protection, and API protection. We will discuss firewalls and intrusion detection systems in future lectures.

Then, we also need to protect the core network in 5G. The core network can be protected using several mechanisms, which are as follows. One mechanism is micro-segmentation, which helps in protecting the core network. This segments the network into different parts, so any security flaws or vulnerabilities in one part do not transit to the other part of the network or other segments. Micro-segmentation allows administrators to control the communication between different components in the core network.

Data exchange over the network can be protected by encrypting data using traditional methods, for example, IPsec and VPNs, which we discussed earlier. Network address translation allows network administrators to isolate select internal networks and prevents access to those networks from the external world. So, NAT stands for Network Address Translation. It is used in several networks. The primary purpose was that there was a shortage of IPv4 addresses.

So, instead of assigning a separate IP address to every host in the network, the same IP address was assigned to all the hosts, but they were distinguished by the use of port numbers. So, network address translation ensures that a single IP address is used to access all the hosts in the network, but their port numbers are different. So, this NAT feature allows network administrators to isolate select internal networks and prevents access to those networks from the external world. There is a gateway between the internal network and the external world. And this can be used to isolate the internal networks and to prevent access to them from the external world.

Also, service providers can deploy firewalls to protect the network and implement monitoring of the end-to-end core network functions. It is also important to protect the virtualized infrastructure. What does virtualized infrastructure mean? In the case of 5G, several networking functions are outsourced to the cloud or data centers. This is known as virtualization.

That is, network functions such as load balancing, firewalls, and so on. Instead of being run on custom hardware, these are run on virtualized infrastructure. That is, on general-purpose processing and storage devices in the cloud or data center. Several 5G components are deployed in virtualized infrastructure. That is, these are general purpose processors and storage elements, but they run different networking functions.

Service providers need to deploy security software, which blocks compromised Virtualized Network Functions (VNFs), and also prevents VM hopping. So, virtualized network functions are different network functions which are run on general purpose processors and storage elements. If some of these VNFs are compromised then they need to be blocked. And also the hopping of malware between different virtual machines, this needs to be prevented. So, that is done by deploying security software.

In addition, virtualized infrastructure components must be continuously monitored for additional protection. It is also important to protect the CPE and small cell devices. CPE stands for Consumer Premise Equipment. So, CPEs are deployed at the residences of users typically. A CPE connects with the 5G base station and it provides connectivity locally to the users in the residence via some technology, such as Wi-Fi.

So, the CPE connects over the 5G network to a base station and locally provides connectivity over Wi-Fi. In 5G, several equipment, such as customer premise equipment or CPE and small cells are deployed close to the user or at user premises. So, in such cases, encryption of sensitive data stored in non-secure physical locations is required. All the CPE or small cell devices connecting to the service providers 5G network should validate firmware and software packages cryptographically at the time of booting. And in case some vulnerabilities are detected in the firmware or software then one needs to roll back to the previous version which is known to be stable.

So, when vulnerable software packages are detected then security teams must be alerted and the software must be rolled back to a trusted version. Each device connecting to the network should authenticate itself at the time of connecting to the network. So, how can this authentication take place? It can be done using one of the techniques that we have discussed. In particular, it can be achieved through certificate based authentication.

Recall that a certificate binds a public key to a name and address. So, certificate based authentication can be used to authenticate devices connecting to the network. In particular, service providers can pre-provision device credentials in certificates and install them on the device before shipping the device to the field. So, in this way, devices that connect to the network can authenticate themselves using this certificate-based authentication. This concludes our brief discussion of 5G network security.

We discussed various aspects of 5G network security including protecting the core network, protecting virtualized infrastructure, protecting small cells and edge computing infrastructure, and so on. This concludes our discussion of cellular network security. We started with discussion of the security of 2G networks, then we discussed 3G networks, 4G and finally 5G cellular networks. So with this, we conclude our discussion of cellular network security. Thank you.