Wireless Cellular Network Security: Part 8

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- S. Velrajan, *“An Introduction to 5G Wireless Networks: Technology, Concepts & Use Cases*”, Saravanan Velrajan, 2020.

5G Network Security

Need for Security in 5G Networks

- 5G RAN has support for Massive IoT services
  - ❑hackers could potentially overload the RAN through DDoS attacks, if the network is left unprotected
- 5G uses edge computing and small cells that get deployed close to subscribers and devices
  - ❑this creates new means by which hackers can attack the network
- 5G caters to mission critical use cases such as robotic surgeries
  - ❑so preventing hackers from exploiting zero-day vulnerabilities is critical

Security Features in 5G Networks

- 5G achieves network segmentation through network slicing
  - ❑ so attacks or faults occurring in one slice do not have an impact on other slices
- 5G supports “Home Control” features for preventing network spoofing attacks
  - ❑ home control feature authenticates device location in roaming scenarios
  - ❑ when a device is roaming, home network verifies if device is actually present in serving network, before allowing the user to roam in visited network
  - ❑ this fixes a known vulnerability in the previous generation networks- 3G and 4G, where networks could be spoofed: sending false signaling messages to the home network to request the International Mobile Subscriber Identity (IMSI) and device location- data that could be used to intercept voice calls and text messages
- 5G provides native support for Extensible Authentication Protocol (EAP)
  - ❑ allows new authentication methods to be plugged into network by the service provider
  - ❑ also homogenizes the authentication method for 3GPP and non-3GPP systems (e.g., 5G and Wi-Fi systems)

Security Features in 5G Networks (contd.)

- 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
- SEAF is now part of the Access and Mobility Management Function (AMF) in the 5G core
- 5G network supports mutual authentication between UE and network

Security Features in 5G Networks (contd.)

- 5G supports Subscriber Identifier Privacy
  - ❑In 3G and 4G networks, the IMSI is shared with the network during connection establishment process
  - ❑In 5G network, a globally unique Subscriber Permanent Identifier (SUPI) is allocated for each subscriber
  - ❑SUPI is not shared during the connection establishment process
  - ❑Instead, a temporary Subscriber Concealed Identifier (SUCI) is shared with network until subscriber or device is authenticated
  - ❑This feature protects subscribers from rogue BSs in the network

Protecting the Edge Computing Infrastructure

- Edge computing infrastructure is one of the vulnerable entities in 5G networks since it is deployed at edge of network
- Risk can be minimized by deploying endpoint protection software in edge computing nodes
- Also, monitoring can be implemented to provide enhanced visibility of the edge computing applications, services and infrastructure components, e.g.,
    - ❑keeping track of activities of various logged-in administrators
    - ❑collection of system resource utilization
    - ❑system performance snapshots at various time intervals, etc.
- Since edge computing services are open to several third parties for running their own custom applications:
    - ❑it is better to deploy firewalls for DDoS protection, malware protection and API protection

Protecting the Core Network

- Core network can be protected using several mechanisms, which are as follows
- Micro segmentation helps in protecting the core network:
  - ❑allowing administrators to control the communication between different components in the core network
- Data exchanged over network can be protected by encrypting data using traditional methods, e.g.:
  - ❑IPsec and VPN
- NAT allows network administrators to isolate select internal networks and prevents access to those networks from external world
- Also, service providers can deploy firewalls to protect the network and implement monitoring of the end-to-end core network functions

Protecting the Virtualized Infrastructure

- Several 5G components are deployed in virtualized infrastructure
- Service providers need to deploy security software that:
  - ❑blocks compromised Virtualized Network Functions (VNFs), and
  - ❑prevents VM hopping
- In addition, virtualized infrastructure components must be continuously monitored for added protection

Protecting the CPE and Small Cell Devices

- In 5G, several equipment such as Customer Premise Equipment (CPE) and small cells are deployed close to user or at user premises
- In such cases, encryption of sensitive data stored in non-secure physical locations is required
- All the CPE or small cell devices connecting to service provider’s 5G network should validate firmware and software packages cryptographically at the time of booting
  - ❑When vulnerable software packages are detected, security teams must be alerted and the software must be rolled back to a trusted version
- Each device connecting to network should authenticate itself at the time of connecting to the network
  - ❑This can be achieved through certificate-based authentication
  - ❑Service providers can pre-provision device credentials in certificate and install them on device, before shipping the device to the field