5G SECURITY

Curtis Norris
Kaylin Martin

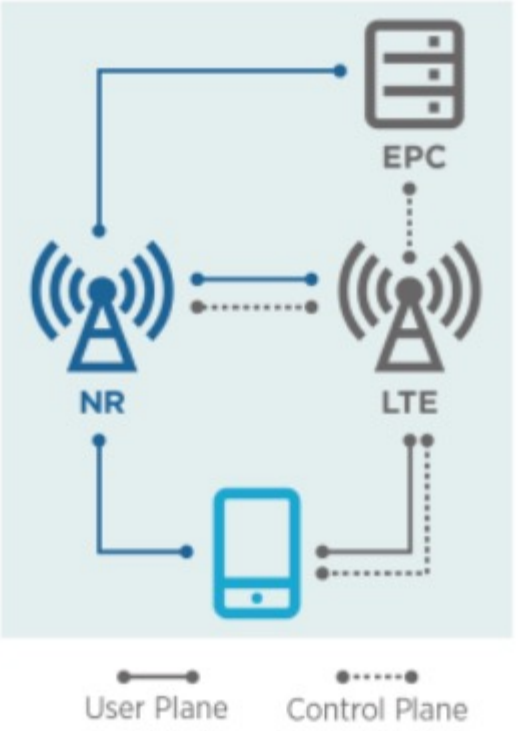
DSCI 519

WHAT IS 5G SECURITY

- 5G security is security controls for 5G radio networks or mobile network operators (MNOs)
- There are two 5G deployment methods
  - non-standalone (NSA) mode
  - standalone (SA) mode
- NSA mode has 5G base stations that are integrated with an existing 4G network working in tandem with LTE base stations and connected to the LTE core and relies on the measures and protections that the LTE core provides
- SA mode has built-in security controls that address many threats that are faced by the previous 4G/3G/2G networks and is connected to a 5G core network

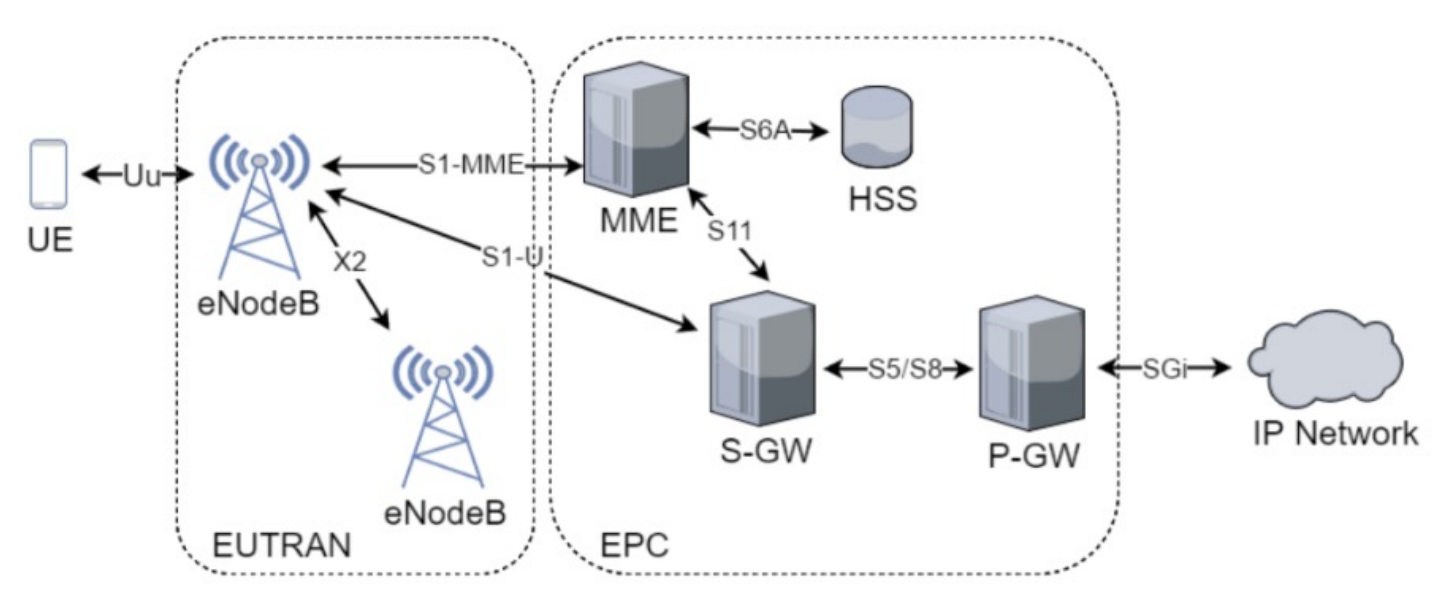
NON-STANDALONE (NSA) MODE

- 5G radio network (NR) relies on the measures and protections that the existing 4G LTE core provides
- Vulnerabilties (same as 4G)
  - DDoS- distributed denial of service attacks
  - Man in the middle attacks
    - faked base station can broadcast a different tracking area code with a stronger signal strength to lure user equipment (UE) away from its legitimate cellular network to register with the faked base station
    - IMSI catching



Non-Standalone (NSA) deployment

NON-STANDALONE (NSA) MODE CONT..

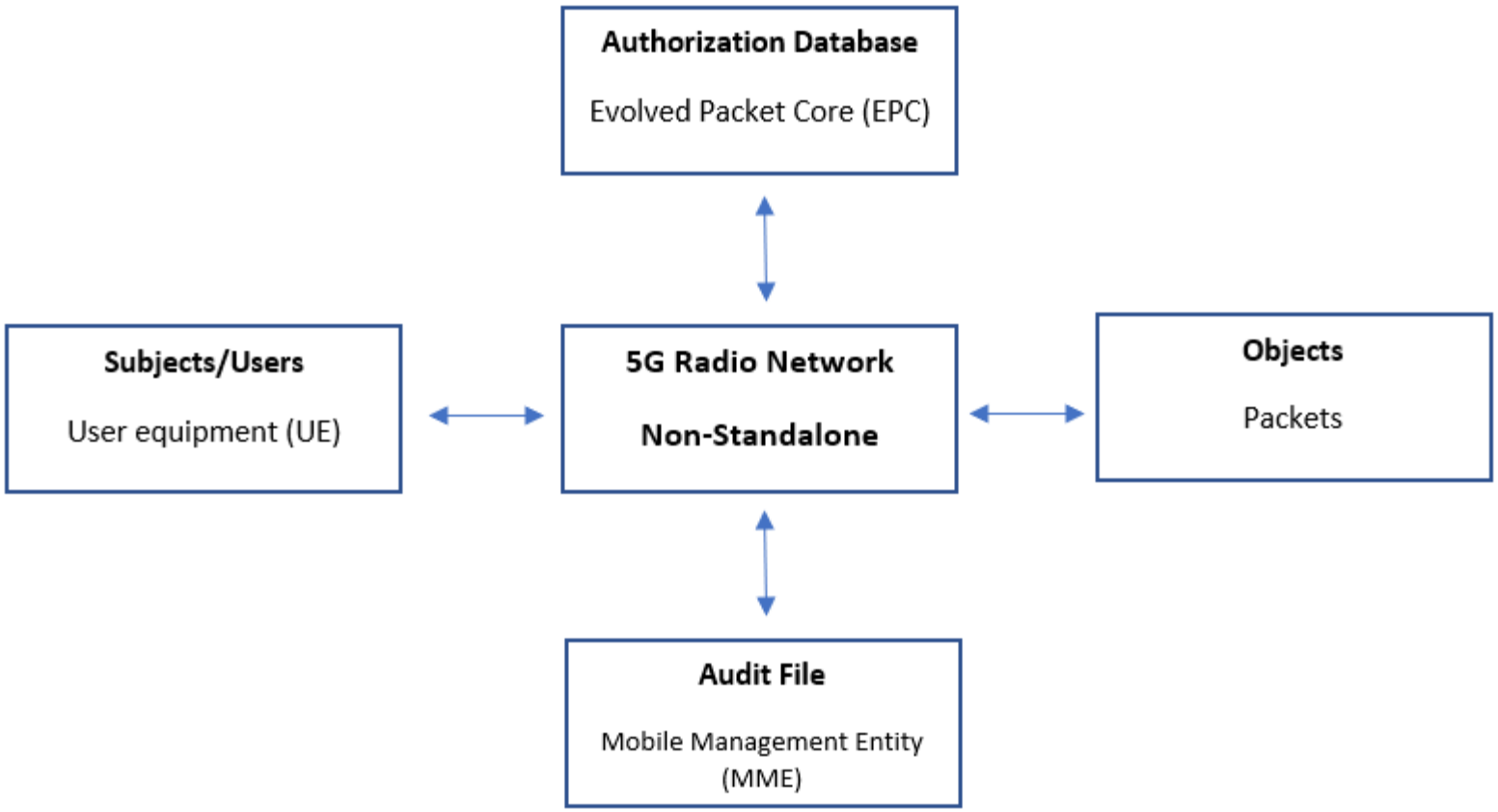


- In 4G LTE, the user equipment (UE) first connects with base stations (eNodeB) within the evolved universal terrestrial radio access network (EUTRAN) before the wider carrier network
- The eNodeB then connects with the mobile management entity (MME), which is responsible for authentication and management of UEs in the evolved packet core (EPC)
- Once the MME retrieves the private key of the UE from the home subscriber server (HSS) and authenticates the UE, the eNodeB connects with the serving gateway (S-GW) which communicates with the PDN gateway (P-GW)
- The P-GW can then communicate with the wider packet data network (IP network)

MAN IN THE MIDDLE ATTACKS

- Each SIM card for a mobile device has a unique identifier, known up to the 4G as an IMSI (International Mobile Subscriber Identity) and as a SUPI (Subscription Permanent Identifier) for 5G
- Authentication between a user and its network provider can only take place after user identification because it is based on a shared symmetric key
- The SIM card is also assigned temporary identifiers, TMSI (Temporary Mobile Subscriber Identity) until 3G systems and GUTI (Global Unique Temporary Identifier) for 4G and 5G systems, by a visited network that are used for identification purposes
- There are certain situations where authentication using temporary identifiers is not possible
  - when a user registers with a network for the first time (UE to eNodeB connection), the packets are sent unencrypted as plaintext and is not yet assigned a temporary identifier
  - when the visited network is unable to identify the IMSI/SUPI from the presented TMSI/GUTI
- An active man-in-the-middle attacker mimics a genuine eNodeB cell tower and gets targets to connect to it because an LTE device will always connect to the network cell with the strongest signal
- Once the attacker begins communication with a mobile device it will force the UE to disclose its IMSI or SUPI number as the fake cell tower represents a new network that the UE has not communicated with which is an IMSI catching attack
- Law enforcement use a surveillance device called a Stingray which is a IMSI catcher to identify or track a phone of suspects

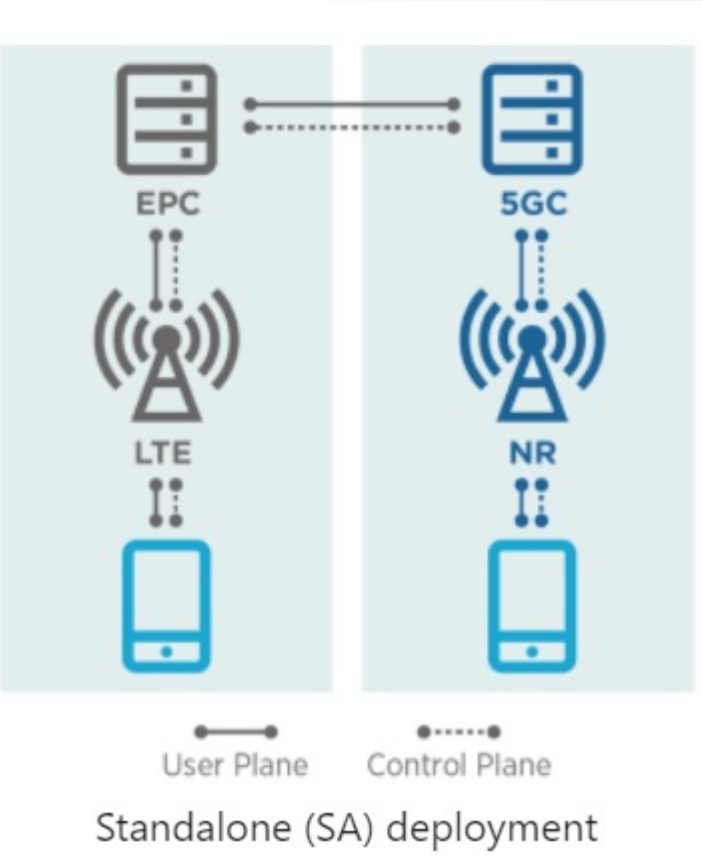
NSA MODE VS REFERENCE MONITOR



- Not tamperproof
- Not non-bypassable
- Not verifiable

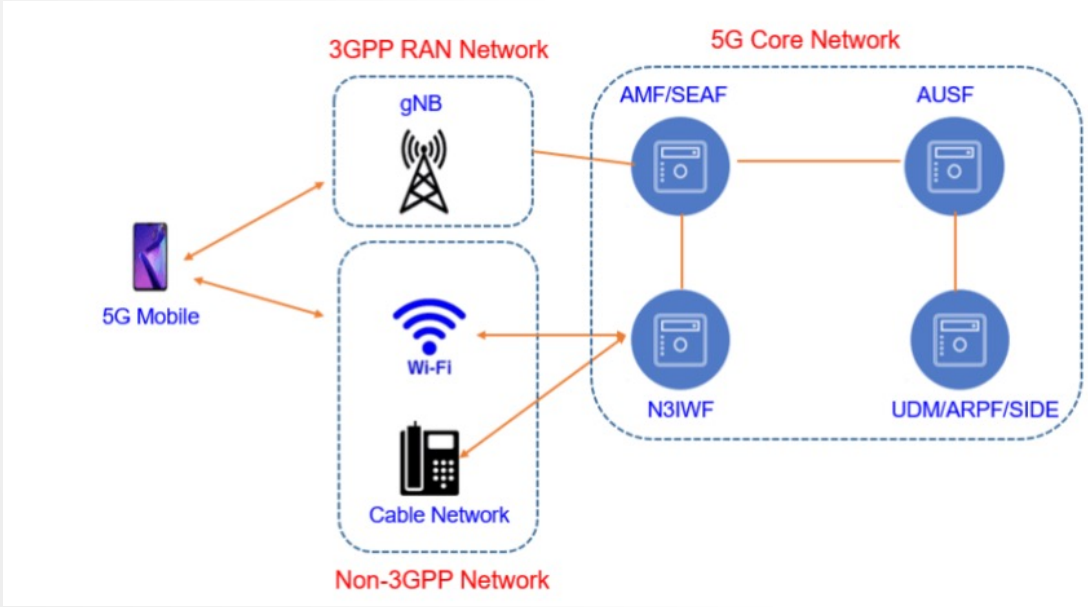
STANDALONE (SA) MODE

- UE is connected to separate 5G core network
- UE generates a SUCI (Subscription Concealed Identifier) using an ECIES (Elliptic Curve Integrated Encryption Scheme) to encrypt the SUPI (Subscription Permanent Identifier)
- When a user registers with a network for the first time (UE to gNB connection), the packets are sent encrypted and prevents IMSI catching attacks
- Encryption of the SUPI is optional, service provider could just opt for null encryption
- UE is vulnerable to downgrade attacks



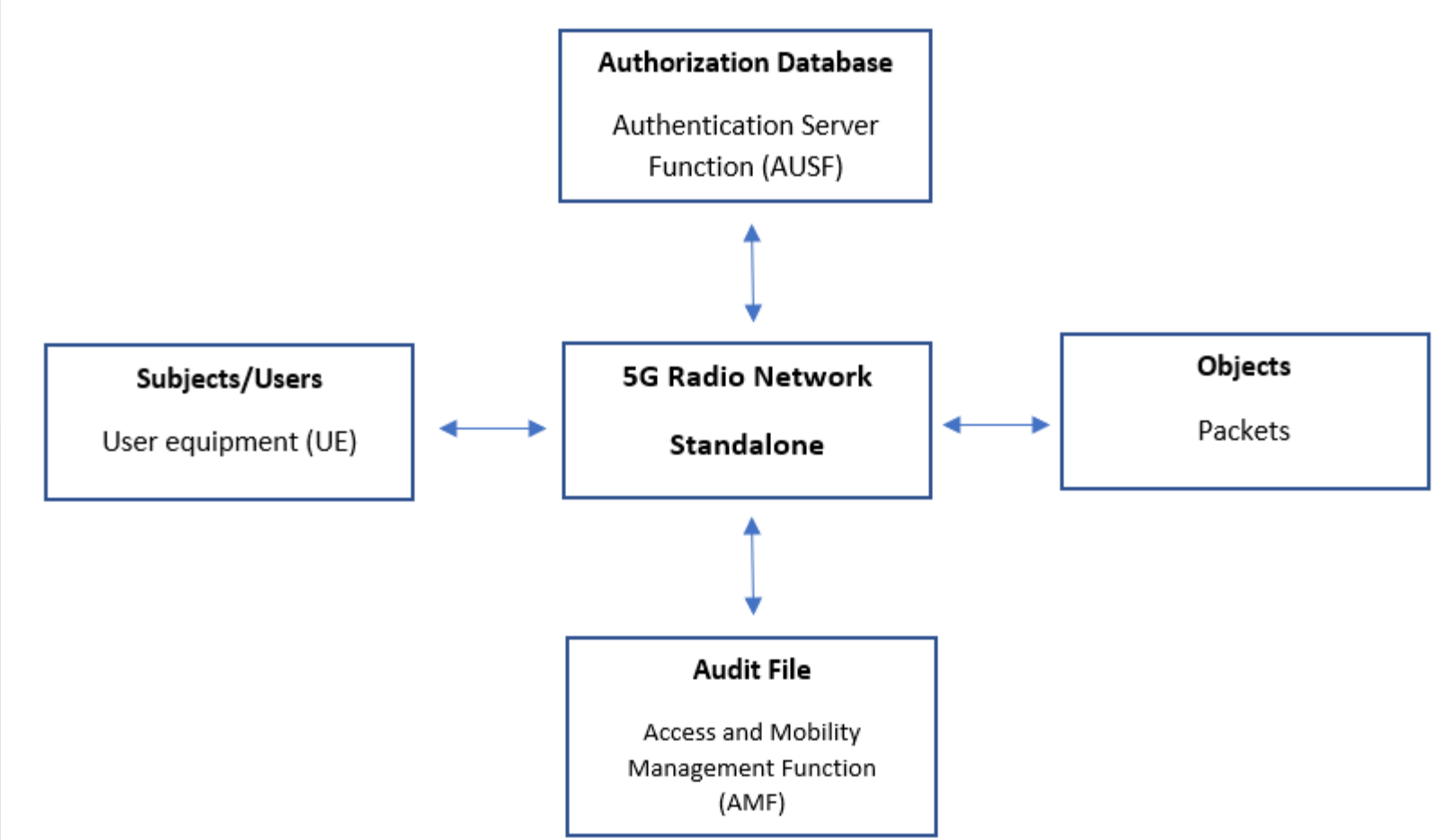
Standalone (SA) deployment

STANDALONE (SA) MODE CONT..



- In 5G, the user equipment (UE) first connects with base stations (gNB) before the wider 5G Core network
- The gNB then connects with the access and mobility management function (AMF), which receives all connection and session related information from the UE but is only responsible for handling connection and mobility management tasks for the 5G core network
- The authentication credential repository and processing function (ARPF) within the unified data management (UDM) selects an authentication method based on subscriber identity and configured policy and computes the authentication data and keys for the authentication server function (AUSF)
- The security anchor function (SEAF) within the AWF then confirms that the authentication of the UE has been accepted by the AUSF and the subscription identifier de-concealing function (SIDF) within the UDM decrypts the SUCI to obtain the SUPI
- If the UE is attempting to access the 5G core network over an untrusted, non-3GPP network, the non-3GPP interworking function (N3IWF) acts as a VPN server to allow access to the network

SA MODE VS REFERENCE MONITOR



- Not tamperproof
- Not non-bypassable
- Not verifiable

VULNERABILITIES OF 5G SECURITY

- Vulnerabilities relate to confidentiality, integrity, and availability
- Authentication and Key Agreement attack (AKA)
  - Current 5G networks have a PKI infrastructure, and these types of attacks are possible due to insecure transportation methods to transfer secret keys from UE and a base station
- Location Discovery
  - TSMI for devices are not changed as frequently as they should, making devices vulnerable to sniffing and tracking
- Message Alteration and message spoofing
  - An attacker can spoof a message acting as another device, and message alteration in the 5G space is not remediated
- DDoS attack
  - With the current amount of devices being used around the world, an attack like this could be devastating
- Man-in-the-Middle attacks

REFERENCES

- https://www.gsma.com/security/securing-the-5g-era/
- https://nse.digital/pages/guides/Wireless/lte-hacking.html
- https://en.wikipedia.org/wiki/Stingray_phone_tracker#Usage_by_law_enforcement
- https://www.mpirical.com/blog/5g-anonymity-and-the-suci
- https://www.kroll.com/en/insights/publications/cyber/a-5g-security-overview
- https://www.efani.com/blog/5g-security
- https://www.techplayon.com/5g-authentication-and-key-management-aka-procedure/
- https://www.techplayon.com/5g-nr-global-unique-temporary-identifier-guti/
- https://www.techplayon.com/5g-identifiers-supi-and-suci/
- https://www.nokia.com/sites/default/files/2021-05/Whitepaper-5G-security-Nokia-STC-March-31-2021.pdf
- https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%2008_%20Fonyi_WEB.pdf
- https://www.gsma.com/membership/wp-content/uploads/2019/11/5G-Research_A4.pdf