5G Security - Evolution not Revolution

Jeff Cichonski
Cybersecurity Engineer
NIST

#PSCR2020
Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately.

Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

* Please note, unless mentioned in reference to a NIST Publication, all information and data presented is preliminary/in-progress and subject to change.
The 5G Capabilities

5G has been envisioned and designed to provide capabilities focused on three core use cases.

High Speed
Massive IoT
Low Latency
Ultra-Reliable
3GPP Overview

• 3GPP is a global initiative responsible for mobile communications specifications.

• 3GPP partners with regional SDO organizations (ETSI, ARIB, ATIS, CCSA, etc.) to set cellular telecommunications standards.

• TLDR; 3GPP wrote (is writing) the technical specifications for 5G, defining interoperable interfaces, protocols, and security features.
A device connects to a network of base stations or Radio Access Network (RAN)
- The RAN connects to a 3GPP Packet Core (Core)
- The Packet Core provides connectivity to the internet or other IP network.
Types of Security Provided by LTE & 5G Networks

Access Stratum Security
Security between the device and base station
- Encryption and integrity protection AS signaling
- Encryption and integrity* protection of User Plane traffic

Non-Access Stratum Security
Security of signaling traffic between a device and the network function supporting mobility

Network Domain Security
Provides security by utilizing IPSEC tunnels
Mobile Network Security in a Nutshell

DU: Distributed Unit of gNodeB
CU: Central Unit of gNodeB
AMF: Access Management Function
SMF: Session Management Function
UPF: User Plane Function
UDM: Unified Data Management
ARPF: Authentication credential
Repository and Processing Function
UDR: Unified Data Repository

Radio Access Network
Access Stratum Security
Non-Access Stratum Security

Core Network
Network Domain Security

Other Networks
### 5G System Security Architecture

- **Home Network**
  - UDM
  - ARPF
  - SEPP

- **Visited / Home Network**
  - AMF
  - SEAF
  - SMF
  - Security Gateway

- **Other Networks**

#### Security Protocols:
- User Plane security
- AS (Radio) control plane security
- NAS security
- Interconnect security
- NDS/IP (IPsec)
- TLS

#### Security Areas:
- **User Plane**
- **AS (Radio) Control Plane**
- **NAS Security**
- **Interconnect Security**
- **NDS/IP (IPsec)**
- **TLS**

#### Diagram Annotations:
- **gNB**
- **UPF**
- **UP - Application Layer Security**
Known Security Issues With LTE

- Subscriber Tracking
- No User Plane Integrity Protection
- SS7 Threats
- False Base stations
New 3GPP Security Features

- User Plane Traffic Integrity
- Subscriber Privacy
- Security Edge Protection Proxy
- Increased Home Control
- Unified Authentication Framework
- CU / DU Separation
Radio Network Security

Integrity protection for User Plane
- Finally!
- Control plane integrity protection was available since UMTS

Split of gNB into Central and Distributed Unit (CU/DU)
- Centralized Unit performs security functions such as confidentiality and integrity protection
- Access Stratum security terminates at the CU
- Centralized unit can an be physically located closer to the core in more trusted environment

Visibility
- 3GPP requirement in 5G security specification to enable applications to assess the security being applied to the connection
AKA is the only supported authentication method

- AKA is slightly different in all generations
- Pre-Shared key is stored in the device and in the home network
- AKA is generally made up of two parts
  - Generation of the authentication vector (AV)
  - Authentication of Device using AV to generate shared session keys between network and device
Authentication Enhancements in 5G

Credential storage on secure hardware (UICC)

Allows the use of integrated secure element (e.g. integrated UICC or eSIM)

Same Primary authentication method can be used over both 3GPP & non-3GPP access

WiFi / fixed broadband networks

Native EAP support over 3GPP access networks

Enables operator to plug-in different credentials and authentication methods without impacting other intermediate network functions
5G Subscriber Privacy

Prevention of subscriber identity from being sent over the air unprotected
- Fixes issues associated with IMSI catching in LTE
- Routing information like mobile country code (MCC) and mobile network code (MNC) still sent unprotected

Cycle temporary identifiers regularly

Terminology!
**Unprotected** 5G Subscriber Identity -> **SUPI** Subscriber Unique Permanent Identifier
**Protected** 5G Subscriber Identity -> **SUCI** Subscriber Concealed Permanent Identifier
5G Non-Standalone (NSA) Deployment Option

- 5G NSA Utilizes a 4G Core
- Device has Dual Connectivity to LTE and 5G base stations
- 5G radio is used to increase capacity
- LTE radio is master node; 5G Radio is secondary
- Security is same as 4G
• The 5G system introduces the concept of a service-based architecture (SBA) for the first time in cellular networks.

• Moving past the traditional network functions as boxes and network functions as VM.

• SBA is pushing the 5G core to look more like a cloud native application and less like a legacy telecommunication stack.
Mobile Network – A 5G World

- gNB: 5G base station
- AMF: Access Management Function
- SEAF: Security Anchor Function
- SMF: Session Management Function
- UPF: User Plane Function
- UDM: Unified Data Management
- ARPF: Authentication credential Repository and Processing Function
- N3IWF: Non-3GPP InterWorking Function
- UDR: Unified Data Repository

Home network

Visited / Home network

- DU, CU: DU, CU
- gNB: gNB
- Non-3GPP Access (e.g. WLAN)
- AMF
- SEAF
- SMF
- UPF
- N3IWF

external AAA for secondary authentication

Internet
Beyond the 3GPP System

• 5G networks are comprised of many components utilizing different modern information technologies

• 3GPP Network Functions are ONLY one piece of the evolution to 5G deployments

• Cybersecurity best practices used for the various components of the technology stack
Supporting Infrastructure and Security Protocols

- Cloud computing platforms
  - Virtualization
  - Containerization
  - Orchestration
- Internet security protocols
  - IPSec
  - TLS
  - JOSE, etc.
The Full Stack Architecture

Over the Top Services

3GPP Network

Supporting Infrastructure

Cloud Platform
Virtualization
Container Orchestration
Commodity Hardware
SDN

IP Network
5G Cybersecurity at The NCCoE

Enhanced Security Capabilities
Demonstrate increased cybersecurity protections in 5G networks from the addition of standards-based features

Modern supporting Technologies
Increased use of modern information technologies Supporting the 5G System to allow for the addition of modern cybersecurity best practices

Practical Approach
As 5G technologies are still being specified and developed, it’s important to effectively scope and prioritize this effort
Project Phases and Associated Security Characteristics

Phase 1: 5G Non-Standalone

- Trusted Infrastructure & 5G Non-Standalone Deployment

Phase 2: 5G Standalone

- 5G Standalone Deployment

Infrastructure Security Capabilities
- Trusted Hardware
- Isolation & policy enforcement
- Visibility into trust status & operations
- Compliance

5G NSA Deployment Security Capabilities
- Enable EPC based security features
- False base station detection
- Serving network disable legacy RATs
  - Network / UE based

5G SA Deployment Security Capabilities
- Subscriber privacy
- User plane integrity protection
- CU/DU Split
- Authentication enhancements
- Roaming security
- Network exposure function

Continuation from previous
- Service based architecture security
  - TLS certificate management
  - VM & Container Orchestration
Current Status

The National Cybersecurity Center of Excellence is soliciting industry collaborators for this project…

Join our Community of Interest—By joining the 5G Community of Interest (CoI), you will receive periodic updates and the opportunity to share your expertise to help guide this project. Join the CoI by emailing us at 5G-Security@nist.gov.
Contact Us

jeffrey.cichonski@nist.gov
THANK YOU

#PSCR2020