5G Standardization, 5G Security Enhancements, and Supporting Infrastructure Security Considerations.
Foundational Standards Developing Organizations

**Internet Engineering Task Force**
- Internet Protocols
  - TCP/IP, TLS, IPSEC

**European Telecommunications Standards Institute**
- Virtualization Standards
- ICT Standards

**3rd Generation Partnership Program**
- Cellular Systems
  - 3G, LTE, VOLTE, 5G

**Institute of Electrical and Electronics Engineers**
- 802.11 – WiFi
- 5G Related work
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.
3GPP Overview Cont.

- 3 overarching groups – Radio Access Network (RAN), Service and System Aspects (SA), and Core Network and Terminals (CT)
- Each group has a plenary group associated responsible for setting priorities, timelines, coordination

<table>
<thead>
<tr>
<th>Radio Access Network (RAN)</th>
<th>Service &amp; Systems Aspects (SA)</th>
<th>Core Network &amp; Terminals (CT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAN 1 - Radio Layer 1 (Physical)</td>
<td>SA 1 - Services</td>
<td>CT 1 – User equipment &amp; Core network radio protocols</td>
</tr>
<tr>
<td>RAN 2 - Radio Interface architecture and protocols</td>
<td>SA 2 - Architecture</td>
<td>CT 3 - Interworking between a 3GPP networks and external nodes or networks</td>
</tr>
<tr>
<td>RAN 3 - Radio architecture and Interface protocols</td>
<td><strong>SA 3 - Security</strong></td>
<td>CT 4 – Core network aspects</td>
</tr>
<tr>
<td>RAN 4 - Radio performance and protocol aspects</td>
<td>SA 4 - Codec</td>
<td>CT 6 – Smart card application aspects (SIMS)</td>
</tr>
<tr>
<td>RAN 5 - Mobile terminal conformance testing</td>
<td>SA 5 - Telecom Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SA 6 – Mission Critical</td>
<td></td>
</tr>
</tbody>
</table>
3GPP Overview Cont.

• The RAN groups are responsible for the definition of the functions, requirements and interfaces of the Radio Network.
• The SA groups are responsible for the overall architecture and service capabilities of systems based on 3GPP specifications.
• The CT groups are responsible for specifying terminal interfaces (logical and physical), terminal capabilities (such as execution environments) and the Core network part of 3GPP systems.
• 3GPP works using a three-stage methodology that is applied in 3GPP as follows;
  • Stage 1 is an overall service description from the user’s standpoint.
  • Stage 2 is an overall description of the organization of the network functions to map service requirements into network capabilities.
  • Stage 3 is the definition of switching and signaling capabilities needed to support services defined in stage 1.
## 3GPP Working Groups

<table>
<thead>
<tr>
<th>Radio Access Network (RAN)</th>
<th>Service &amp; Systems Aspects (SA)</th>
<th>Core Network &amp; Terminals (CT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAN 1 - Radio Layer 1 (Physical)</td>
<td>SA 1 - Services</td>
<td>CT 1 – User equipment &amp; Core network radio protocols</td>
</tr>
<tr>
<td>RAN 2 - Radio Interface architecture and protocols</td>
<td>SA 2 - Architecture</td>
<td>CT 3 - Interworking between a 3GPP networks and external nodes or networks</td>
</tr>
<tr>
<td>RAN 3 - Radio architecture and Interface protocols</td>
<td><strong>SA 3 - Security</strong></td>
<td>CT 4 – Core network aspects</td>
</tr>
<tr>
<td>RAN 4 - Radio performance and protocol aspects</td>
<td>SA 4 - Codec</td>
<td>CT 6 – Smart card application aspects (SIMS)</td>
</tr>
<tr>
<td>RAN 5 - Mobile terminal conformance testing</td>
<td>SA 5 - Telecom Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SA 6 – Mission Critical</td>
<td></td>
</tr>
</tbody>
</table>
3GPP Process (SA3 Perspective)

• General approach: Study document (TR), followed by technical specifications (TS)
  • TR analyzes security issues and potential solutions
  • TS presents definitive solutions
  • Leverages protocols from other SDOs (e.g. IETF, IEEE)

• Iterative pipeline
  • SA3 (security) defines solutions based on SA1’s requirements and SA2’s architecture (for Mission Critical, SA6’s architecture)
  • Tight timelines require groups to work in parallel and re-work or add to solutions as needed

• SA3’s security solutions are concretized by CT1
  • Optimal/feasible solutions require back-and-forth between SA3 and CT1

• Consensus process
  • Resorting to a vote is rare, viewed as a process failure
Current 3GPP Timeline

- **R16**
  - stage 2 freeze
  - R16 stage 2 freeze
  - Q2/2019
  - 6/19
- **R16**
  - stage 3 & code freeze
  - SA#84 Q3/2019
  - 9/19
- **SA#85**
  - Q1/2020
  - 3/20
- **SA#86**
  - Q2/2020
  - 6/20
- **SA#87**
  - Q1/2021
  - 9/20
- **SA#88**
  - Q2/2021
  - 12/20
- **SA#89**
  - Q3/2021
  - 3/21
- **SA#90**
  - Q4/2021
  - 6/21
- **SA#91**
  - Q3/2022
  - 3/21
- **SA#92**
  - Q4/2022
  - 6/21
- **SA#93**
  - Q3/2022
  - 3/21
- **SA#94**
  - Q4/2022
  - 6/21

- **Rel-16 Schedule**
  - exceptions
  - R16 stage 2 freeze
  - 6/19

- **Rel-17 Planning**
  - RAN Rel-17 day
  - RAN/SA Rel-17 day

- **Rel-17 Schedule**
  - start/ongoing: S1 normative S2 studies
  - R17 stage 1 ~ 80%
  - R17 stage 1 freeze
  - R17 stage 2 freeze
  - R17 stage 3 freeze
  - R17 code freeze

- **Rel-18 (unknown)**
  - R18 stage 1 Initial input
  - Rel-18 schedule fix
  - Rel-18 schedule timeline fix

Mobile Network – The Basics

- 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.
Mobile Network Security

- Radio Access Network
  - Access Stratum Security
  - Non-Access Stratum Security
- Core Network
  - Network Domain Security
- Other Networks
  - Security Gateway
  - Gateway
5G System Security Architecture

User plane security
- AS (Radio) control plane security
- NAS security
- Interconnect security
- NDS/IP (IPsec)
- TLS

Home network
- UDM
- ARPF
- SEPP

Visited / home network
- AMF
- SEAF
- SMF
- UPF

gNB - Security Gateway

Other Networks

UP - Application Layer Security
Known Security Issues With LTE

- Subscriber tracking
- No user plane integrity protection
- Roaming issues (SS7 & diameter threats)
- False Base stations
New 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)
- CU performs security functions (confidentiality/integrity)
  - AS (air interface) security terminates at the CU.
  - Can be located closer to the core

Visibility
- Requirement to enable applications to check security being applied to the connection
5G Privacy Protections

Objectives;
- Protect permanent identifiers
- Cycle temporary identifiers regularly
- Avoid re-authentication

Outcomes;
- Encryption of SUPI with public key of home operator (SUCI)
- Routing information (home network ID) in clear
- SUPI revealed to VPLMN only after authentication
- Binding of SUPI into key
- Respond to identifier request with SUCI
- No SUPI based paging
- Reallocation of temporary IDs after security set up, on every periodic mobility registration update and after use in paging
5G Authentication Framework Enhancements

Credential storage on secure hardware (UICC)
  • Allows the use of integrated secure element (e.g. integrated UICC)

Same Primary authentication method can be used over both 3GPP & non-3GPP access
  • WiFi / fixed broadband networks
  • N3IWF – Non-3GPP Interworking Function

One security context for both access technologies

Native EAP support over 3GPP access networks
  • Enables operator to plug-in different credentials and authentication methods without impacting other intermediate network functions

Optional EAP based secondary authentication for access to specific data networks/services
  • Allows applications to use their own credentials & authentication before allowing access to their dedicated application/service specific data networks (e.g., Amazon, Facebook, Enterprises)
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.
Questions / Comments?