Security Considerations in 5G

ETSI Security Week
June 12 – 16, 2017
Marcus Wong
Agenda

- 5G Motivation and Security Drivers
- Flexible Service Architecture
- Trust Model
- Slicing, On-demand, Flexible Policy
- User Plane Security
- Public Key for 5G
- Authentication
- Privacy
- 5G Security Standards Landscape
5G Security Motivations and Drivers

Evolutionary rather than Revolutionary

Things that worked:

- UE Provisioning: USIM and UICC
- Authentication: UE mutual authentication, home operator control (AKA)
- Crypto Algorithms: AES, ZUC, public-key algorithms
- Security Termination: UP terminating in access network
- Domain Security: backhaul, IPsec
- Service Security: one-size fits all

Things that need improving:

- UE Provisioning: eUICC
- Authentication: protocol enhancements, efficiency, device authentication
- Crypto Algorithms: quantum-ready, larger key sizes, expanding use of public-key algorithms
- Security Termination: flexibility, application layer security
- Domain Security: mid-haul security, end-to-end backhaul security
- Forward Security: long term key protection, public-key assisted key derivation
- Service Security: on-demand, network slicing, third-party
- Privacy: IMSI protection
Flexible Service Oriented Architecture

1. IoT device Identity Management & access security
2. Unified authentication framework for different access technologies
3. Physical infrastructure security
4. Virtualization Security
5. CP/UP separation security
6. Opening for third-party service security
7. On-demand slice security mechanism for vertical services

SOR: Service Oriented RAN
SOC: Service Oriented Core

Legacy Security

5G Specific Security

SOR: Service Oriented RAN
SOC: Service Oriented Core
Trust Model

Traditional Trust Model:

New Trust Model:

- Operator to retain more home control
- Reduce reliance on SN trust
- Reduce potential fraud due to unauthorized location update
**Network Slicing**

**Isolation Between Slices**
Protection from unauthorized network slice access, between slices within and outside of operator network.

**Isolation within Slices:**
Protection from unauthorized access of private data area among UEs within the slice.

- **Permanent Isolation**
- **Conditional Access**
- **Global Access**

**Common Resources/Device not in any slice:** globally accessible
On-Demand Framework & Flexible Security Policy

Flexible security features
Flexible security policy

<table>
<thead>
<tr>
<th>Security Features</th>
<th>Security Policies Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isolation</td>
<td>between slices</td>
</tr>
<tr>
<td></td>
<td>inside slice</td>
</tr>
<tr>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Privacy</td>
<td>Aware of user data</td>
</tr>
<tr>
<td></td>
<td>Not aware of user activities</td>
</tr>
<tr>
<td></td>
<td>Not aware of user’s ID</td>
</tr>
<tr>
<td>Integrity</td>
<td>Integrity Protection</td>
</tr>
<tr>
<td></td>
<td>No integrity Protection</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>256bit key</td>
</tr>
<tr>
<td></td>
<td>128bit key</td>
</tr>
<tr>
<td></td>
<td>Dedicate cipher algorithm</td>
</tr>
<tr>
<td>Authentication</td>
<td>Multi-factor authentication</td>
</tr>
<tr>
<td></td>
<td>Biometric authentication</td>
</tr>
</tbody>
</table>

- **Isolation**: Medium, Medium, High
- **Privacy**: Medium, High, Medium
- **Integrity**: On, On, Off
- **Confidentiality**: Medium, High, High
- **Authentication**: High, High, Medium
User Plane security

- Ciphering (and integrity protection) use common crypto synchronization from LTE PDCP protocols.
- Header compression capabilities (e.g., ROHC) support.
- In-sequence delivery support.
- Traffic-type aware and QoS support
- Faster to market
- Lawful Intercept support at CN consistent with solutions in LTE

UP terminates @ (R)AN
Use of Public Key

3G and 4G use of public key:
- certificates and certificate enrolment
- security between network entities (e.g. establishment of IPsec)
- ProSe/V2X application security
- EAP-TLS, Internet browser security

New 5G potential Public Key use cases:
- certificates requiring PKI and public-private key pairs without PKI
- device authentication
- over-the-air signaling protection
- IMSI and privacy protection
- remote provisioning
- long term key protection
Authentication

- Network Access Authentication
  - Support backward compatibility
    - EPS–AKA**
  - Support EAP authentication Framework
    - EAP–AKA’
- Device authentication
  - device public-key/certificate
- Slice authentication
  - service authentication
  - Authentication to external networks
    - secondary / third-party authentication
  - alternative credential
Privacy

- IMSI Privacy
  - UE tracking
  - IMSI Leakage
  - initial authentication protection
- Use of privacy enhancing technology
  - Pseudonym
  - access token
  - encrypted IMSI (using public key or shared key)
  - temporary identities
- Need to support lawful interception in the serving network
  - Serving Network can get target identity from Home network
  - Serving Network can get target identity from UE
  - Need to be done consistently (based on operator policy) for all UEs to avoid detectability
“Option 3”

- Non-standalone 5G deployment
  - 5G UE + 4G AN + 5G AN + 4G CN
  - Support faster deployment while migrating to full 5G CN gradually
- Security of “Option 3”
  - modelled after dual-connectivity in LTE where UE connects to two eNBs simultaneously
  - anchored via eNB (i.e. MeNB)
  - gNB access by UE is considered as secondary (i.e. SgNB)
  - RRC signalling support between UE and gNB reusing PDCP security
5G Security Standards: Current Landscape

Key 3GPP Working Groups

SA1: 5G requirements
SA2: 5G architecture
SA3: 5G security

RAN: 5G access network
CT: 5G core and terminal

Phase 1 considerations key points
- Security Architecture
- Unified Authentication Framework
- Key Hierarchy
- UE/Network Authorization
- Slicing Security

Phase 2 considerations key points
- Low latency
- IoT
- Small Data
- Slicing security enhancement
- etc.
Copyright © 2012 Huawei Technologies Co., Ltd. All Rights Reserved.
The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.