Securing 5G and evolving architectures
2020 Cisco Knowledge Network

Pramod Nair
Security – EMEAR Architecture
September 2020
Discussion topics

- Evolution of networks – 4G to 5G
- Key 3GPP security enhancements for 5G
- Key 5G Security challenges
- Industry views on 5G security
- E2E threats in 5G
- E2E threat mitigation for 5G networks
Some tips

This symbol on top right corner means the slide has a link which can be used for further reading after the session.

This symbol on the top right corner means the slide contains more information on the topic discussed in previous slide.
Legend & Abbreviations

- = UE = User equipment (mobile phone etc)

- Radio base station (eNB = 4G, gNB = 5G)

- Indicates DC (centralised & distributed)

- Generally indicates another SP partner

CU = Centralised Unit
DU = Distributed Unit
RU = Radio Unit
AAU = Active Antenna Unit
DDoS = Distributed Denial of Service
NSA = Non-Standalone (LTE network with software upgrades
SA = Standalone
3GPP = 3rd Generation Partnership Programme
ETSI = European Telecommunications Standards Institute

3GPP vocabulary & Abbreviations:
Evolution from 4G to 5G

- **4G**
  - eNB
  - Internet & SP Services
  - Roaming and Interconnect

- **5G**
  - gNB
  - Front Haul / Mid Haul
  - MEC (Multi-access Edge Compute)
  - Backhaul
  - Centralised Packet Core
  - Internet & SP Services

- Roaming and Interconnect
3GPP Key security enhancements

Subscriber Security

4G Authentication mechanism for user equipment:
- EPS-AKA - USIM

5G Authentication mechanism for user equipment:
- 5G-AKA - USIM
- EAP-AKA' - USIM
- EAP-TLS - USIM / Non-USIM

Roaming & Interconnect

Reference: 3GPP TS 33.501
http://www.3gpp.org/ftp/specs/archive/33_series/33.501/
Key security challenges in 5G

- IoT & M2M
- Virtualization
- Unprotected interfaces & API’s
- Convergence with Legacy technologies
Security challenges in 5G

- **IoT & M2M**: Weak inbuilt security in IoT devices, peer to peer attacks, V2X use cases
- **Virtualization**: Increased complexity in cloud native deployments and vulnerability in open source components
- **Distributed architectures**: New unprotected interfaces and API based interfaces
- **Convergence - Legacy technologies**: Improper isolation between technologies
Industry views on 5G threats

https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSC%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf

https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF

https://fas.org/sgp/crs/natsec/IF11251.pdf

.... and many others
End to End threats - 5G

Device Threats
- Malware
- Bots
- DDoS
- Firmware Hacks
- Device Tampering
- Sensor Susceptibility
- TFTP MitM attacks

Air Interface Threats
- MitM attack
- Jamming

RAN Threats
- Rogue Nodes
- Insecure S1, X2
- Insecure Xx, Xn

MEC Functions
- CU
- vBBU
- UPF

MEC & Backhaul Threats
- DDoS attacks
- LI Vulnerabilities
- Insecure Sx
- Insecure N6
- CP / UP Sniffing
- MEC Backhaul sniff
- Side Channel attacks
- NFVi Vulnerabilities

Centralized 5G Core

5G Packet Core & OAM Threats
- Virtualisation
- LI Vulnerabilities
- Improper Access Control
- Network Slice security
- API vulnerabilities
- NEF vulnerabilities
- IoT Core integration
- Roaming Partner
- DDoS & DoS attacks

SGi / N6 & External Roaming Threats
- IoT Core integration
- VAS integration
- App server vulnerabilities
- Application vulnerabilities
- API vulnerabilities
Securing your multi-vendor 5G network

- Security control evolution
- Trust as a foundation
- Security control evolution
- Secure 5G RAN, Transport
- Secure workloads (MEC & 5GC)
- Secure Roaming interfaces
- Secure 5G access control (Ops & management)
- E2E monitoring for 5G networks
### Security Control Evolution

<table>
<thead>
<tr>
<th>Security Control</th>
<th>2G</th>
<th>2G + 3G</th>
<th>2G + 3G + 4G</th>
<th>2G + 3G + 4G + 5G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralised Security Gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Security Gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIAMETER Inspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCTP Inspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GTP Inspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carrier Grade NAT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Application Firewall (WAF)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DDoS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi- Firewall</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS7 Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visibility on Packet Core</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-Factor Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Slice Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Security Endpoints</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Internet Gateway (SIG)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>API Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbuilt Hardware Security (ex: Trust Anchor)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Micro-Segmentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management / DCN Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Trust as a foundation

Cisco Trust center: https://trust.cisco.com
Secure 5G RAN & Transport

- gNB
- Front Haul / Mid Haul
- MEC
- Backhaul
- Centralised Packet Core
- Anti-DDoS controller
- IPS
- SecGW
- Internet & SP Services
- 4G VPLMN
- 5G VPLMN
- SEPP
- Signaling & GTP FW
- Proprietary / 3GPP / IPsec Depending on mode of deployment
- IPsec

Depending on mode of deployment
Securing 4G network evolution towards 5G

LTE NW: Secure S1 & X2 interfaces
LTE CUPS NW: Secure S1, X2, Sx interfaces
5G NSA NW: Secure Xx, N2, N3, N4 & N6
5G SA NW: Secure Xn, N2, N3, N4 & N6
Secure Roaming – 5G NSA & SA
Secure 5G Access control based on Zero Trust principles
Securing access to 5GC network components

Remote Users
- VPN (Cisco Anyconnect)

Internal Users
- Primary Authentication (Cisco ISE /AAA)
- MFA & Device check (Cisco DUO)
- RBAC (Inbuilt Cisco)

Service Provider 5GC components
- Orchestration Layer
- Network Functions & Applications
- App Infrastructure
- Cloud Infrastructure
- Data Center Infrastructure

© 2020 Cisco and/or its affiliates. All rights reserved.
Securing virtualised deployments
E2E monitoring for multi-vendor 5G networks
E2E Threats mitigation

Device Threats | Air Interface Threats | RAN Threats | Backhaul / Remote DC Threats | 5G Packet Core & OAM Threats | SGI / N6 & External Roaming Threats
---|---|---|---|---|---
Enhanced Visibility & Threat detection Layer | Stealthwatch
DNS Protection Layer | Umbrella
Application Protection & Policy enforcement | Tetration, Radware
NGFW & DDoS protection Layer | Firepower, Radware
Segmentation & Isolation Layer | ISE, Duo
Advanced Malware Protection Layer | AMP

CU - Centralized Unit
DU - Distributed Unit
UPF - User Plan Function
RAT - Radio Access Technology
vBBU - Virtualized BaseBand Unit

Application & Direct Internet Access
Key Takeaways

- Design your 5G network with **layered security controls** in mind
- Ensure **End to End visibility** – including the encrypted traffic
- Ensure **multi-layered access control** from Day 0
Interesting reads on 5G security..

**EU coordinated risk assessment of 5G networks security:**

**5G security blog:** https://blogs.cisco.com/sp/5g_secure


**Innovation in 5G security:**
That was fun, let’s do it again sometime 🙂