5G: Security status and opportunities

Marc Kneppers
Chief Security Architect
Me == Blue team

- Long-term architectural strategy
- Architectural overview
- Academic research
- Critical infrastructure
- Industry collaboration and influence
What is mobility
What is 5G

5G is just the latest evolution of wireless tech

- 50 Mbps <> 10 Gbps
- Sub-millisecond latency
- Support for more devices
- Energy efficiency
# 3GPP: Release 15 & Release 16 ‘NR’ milestones

<table>
<thead>
<tr>
<th>RAN #79</th>
<th>RAN #80</th>
<th>RAN #81</th>
<th>RAN #82</th>
<th>RAN #83</th>
<th>RAN #84</th>
<th>RAN #85</th>
<th>RAN #86</th>
<th>RAN #87</th>
<th>RAN #88</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
<td>Q1</td>
<td>Q2</td>
<td></td>
</tr>
</tbody>
</table>

- **Rel-15 NSA ASN.1**
- **Rel-16 Package Approval**
- **Rel-15 Freeze**
- **Rel-16 Freeze**
- **Rel-15 Late Drop Freeze**
- **Rel-15 Late Drop ASN.1**
- **Architecture Option 2 & 5 (LTE): ASN.1 Freeze Sept 2018**
- **The late drop is to exclusively contain NR architecture options that were not completed by September ASN.1 drop**
- **Options 4, 7 are part of the late drop**
- **If Option 5 is not completed by Sept ASN.1 drop, it will be part of the late drop**

**RAN#79 endorsed the freeze of NSA ASN.1 and approved the corresponding CRs**

**Until June WGs shall prioritize Option-3 stabilization (only essential corrections allowed), and Option-2 specification work**

Source: 3GPP, RAN Chairman’s Summary from RAN#79, March 2018
5 years of work culminating in 5G standard

3 Specification Groups
- RAN
- SA
- CT

1260+ Specifications

16 Sub-Groups
- SA3

170 Security-specific

Overall Security Architecture
Why 5G?

Broadband access in dense areas
PERVERSIVE VIDEO

Broadband access everywhere
50+MBPS EVERYWHERE

High user mobility
HIGH SPEED TRAIN

Massive Internet of Things
SENSOR NETWORKS

Extreme real-time communications
TACTILE INTERNET

Lifeline communications
NATURAL DISASTER

Ultra-reliable communications
E-HEALTH SERVICES

Broadcast-like services
BROADCAST SERVICES

Source: NGMN
Some key differences in 5G

- Web services
- De-centralization
- Virtualization
Web services – the “Service Based Architecture”

Policy
- NSSF
- NEF
- NRF
- PCF
- AF
- vSEPP
- hSEPP

Authentication
- Access & Session Management
  - AMF
  - SMF
- Resource Catalogue
  - UDM
  - NRF
  - AUSF
  - PCF
  - NEF

Access & Session Management
- UE
- (R)AN
- UPF
- DN
- HPLMN
- VPLMN
De-centralization
Virtualization

- De-couple software from hardware for service agility
- Containers and VMs
- ... maybe the base-station
Does 5G fix all mobile security problems?
From an operator perspective
The RAN protocols have expanded ...

Virtualization at the tower

Separation of the user and control plane

eCPRI/xRAN
- “Generic data transfer”
- “Remote reset”
- “Remote memory access” (symmetric)
- VLAN tagging

xRAN
- Beamforming
- Timing (PTP)

PFCP
- Packet matching templates
- QoS, charging, data LI, …
And the security model remains the same

IPSec
4G attacks may still be possible in 5G

But can be mitigated via vendor/operator
The Service Based Architecture is a new model

Source: XKCD.com
Virtualization will require new software management

- May require specialized hardware
- Have implications for IPSec
- And need new patching/upgrade procedures (CI/CD?)

Source: XKCD.com
The overall perimeter is controlled by 3 functions

- De-centralization of the user-plane should improve DoS risk
- Abuse via API will have to be monitored
- There are opportunities for better inter-operator signaling security

But still for future study
From a user perspective
Secondary authentication is nice
With improved privacy protection
... but it all depends on the key
Security can be customized in slices

Source: 3GPP
As IoT requirements vary

Urgent

Not urgent
Key takeaways

- 5G will be transformative
- Many security improvements have been made
- Implementation will not be immediate
- There is room for improvement in Phase 2
We mean business