P1 SECURITY

ENISA Digital Forum - May 2024

Security Needs of Mobile as a Bell shape: from 5G Standalone to 4G-2G legacy

Speaker

Philippe Langlois

Date

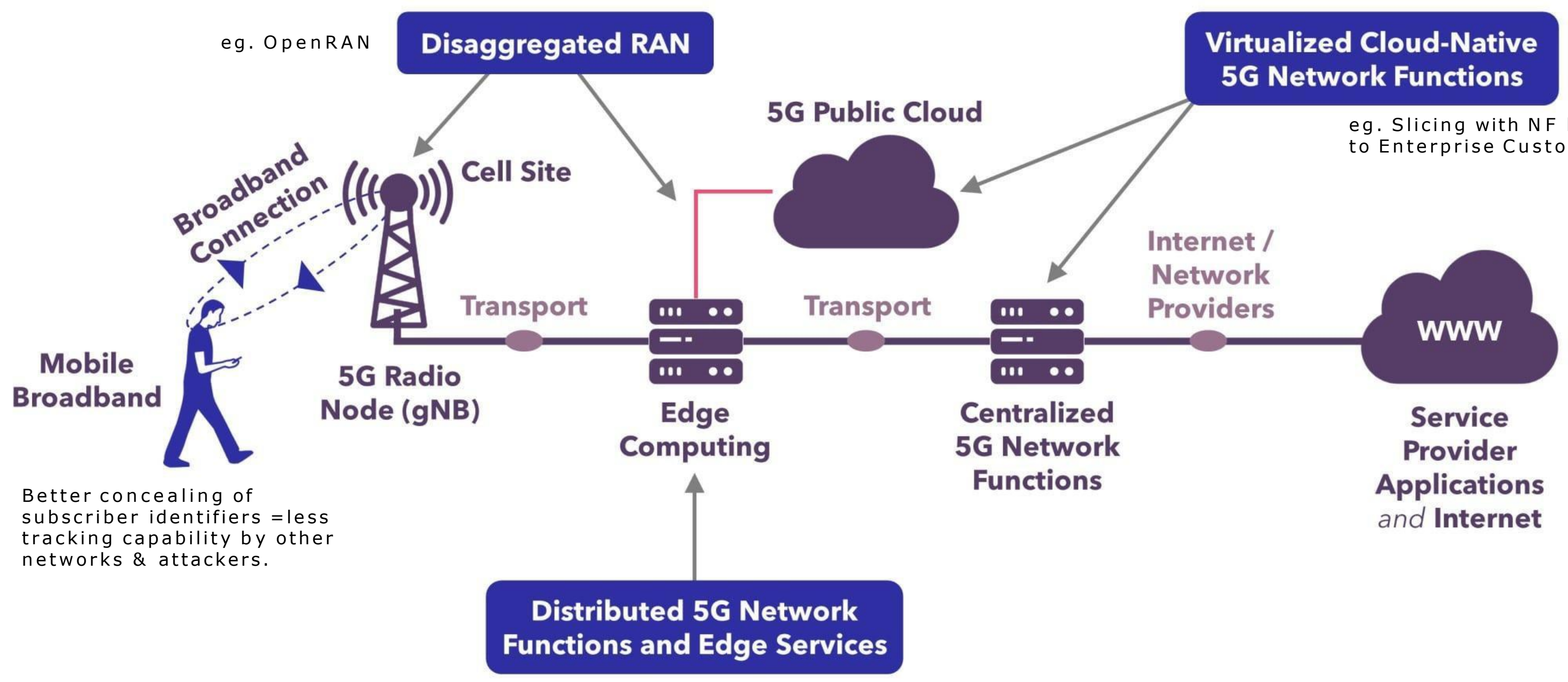
May 15th 2024

01

Who are we?

Cyber Defense in Telecom & Mobile Critical Infrastructure

5G Network: improvement… and Kill Chain


Disaggregated RAN
Virtualized Cloud-Native 5G Network Functions
5G Public Cloud
Broadband Connection
Cell Site
Internet / Network Providers
Transport
Transport
WWW
Mobile Broadband
5G Radio Node (gNB)
Edge Computing
Centralized 5G Network Functions
Service Provider Applications and Internet
Distributed 5G Network Functions and Edge Services

eg. OpenRAN

eg. Slicing with NF belonging
to Enterprise Customer

Better concealing of
subscriber identifiers =less
tracking capability by other
networks & attackers.

…and Legacy. Lets see in reality what it looks like in a real world engagement.

02

Red-Team story on a 5G 4G 3G 2G mobile operator

Why it’s hard to protect both bleeding edge and legacy

1. **Physical**

   From outside radio site.
   Weak locks & alarms usage (!)

2. **5G gNB and legacy 3G, 4G**

   Compromise Site Integration, multiple vulnerabilities

3. **Spread to RAN**

   Lateral movement, IPsec attack surface

4. **Spread to Core**

   Segmentation issues, management (OAM) takeover

5. **Core Compromise**

   VNFs, NFV Hypervisor hosts, CNF, Kubernetes and OSS MANO takeover

P1 SECURITY

MNO Security Coverage

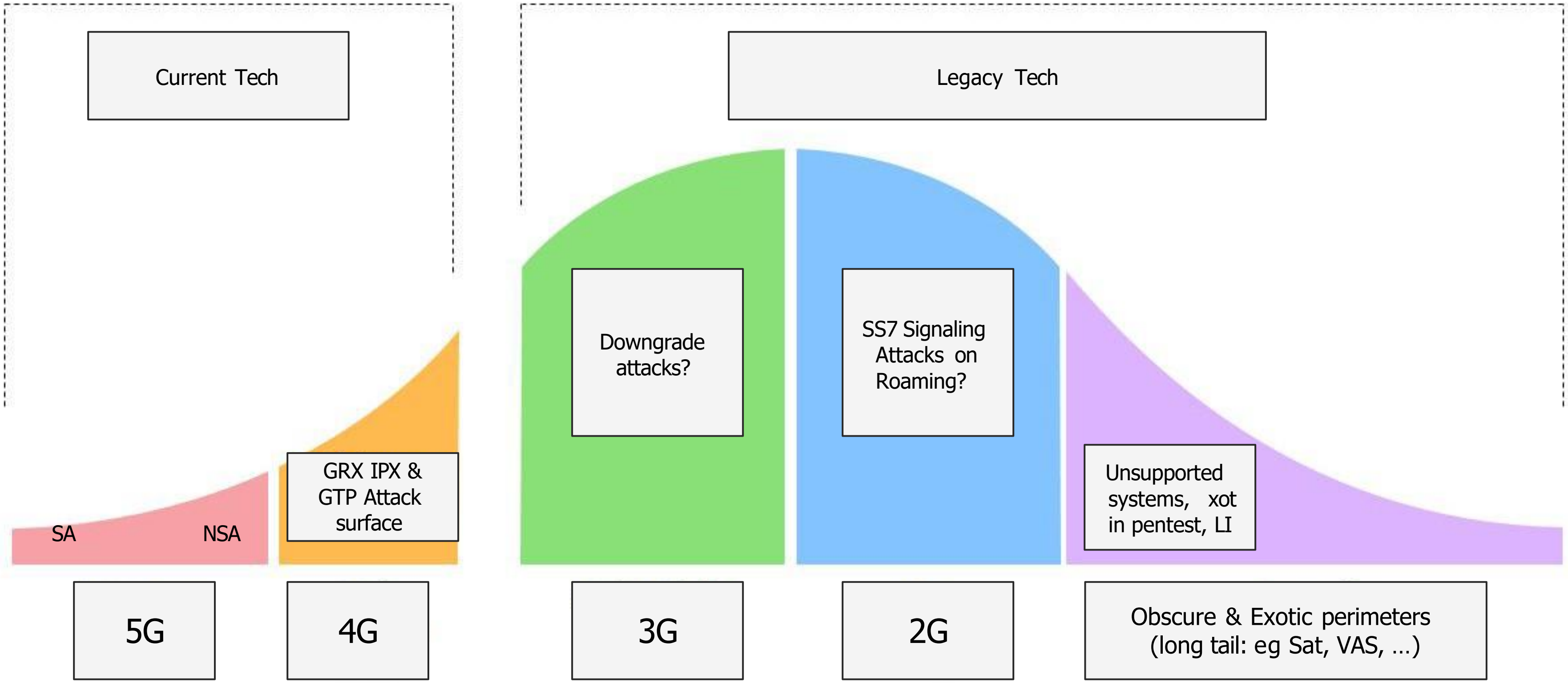
Activities \ Domains	5GC Telco	5GC NFV	2G/3G/4G Core	RAN	Roaming (2G,3G,4G)	IMS	LI	Fixed Infra	IPTV, OSS, BSS, VAS, Web portals, IT infra…
MNO Organisational audit Process and practices review	🟩 3	🟩 5	⬜	⬜	⬜	⬜	🟥	⬜	⬜
Architecture review HLD, LLD, product documentation	🟩 7	🟩 11	⬜	⬜	⬜	🟥	⬜	⬜	⬜
Product Vulnerability Research system / binary analysis	🟩 3	🟩 13	🟥	⬜	⬛	🟥	🟥	⬜	⬜
Pentest Network discovery & propagation	🟩 4	🟩 17	🟩 21	🟥	🟥	🟥	⬜	🟩	🟩
SoC / Monitoring validation	🟧 6	🟧 27	⬜	🟥	🟥	⬜	⬜	⬜	⬜
Physical Security	⬜	⬜	⬜	🟧 2	⬛	⬜	⬜	🟧 7	⬜
Compliance checks, Products configuration review, supply-chain integration verification	🟥	🟥	🟥	🟥	⬜	🟥	🟥	⬜	🟥

Green: Covered in this audit
Orange: Partly covered in this audit

Light Grey: Not covered in this audit
Dark grey: Not applicable

Red: Not covered in this audit, high-risk,
Number in cell: number of found vulnerabilities

Bell shape of Mobile Networks vulnerabilities



Current Tech
Legacy Tech
SA
NSA
GRX IPX & GTP Attack surface
Downgrade attacks?
SS7 Signaling Attacks on Roaming?
Unsupported systems, xot in pentest, LI
5G
4G
3G
2G
Obscure & Exotic perimeters (long tail: eg Sat, VAS, …)

Bleeding edge research: you don't know the stockpile of the attackers (P1 has 65 in VKB 5G)

Many vulnerabilities and attackers to be covered, how fast do you spot a problem? Are there Unknown domains?

Attacker arbitrage on Telecom & Mobile targets

Start with a story: 5G Black box Penetration Testing: Outside Radio site to Core compromise & Enterprise Subscriber geolocation attack: Commonality?

Infrastructure Security

Scope
s

5G (NSA, SA, MEC, Slices) | **4G** | **3G** (2G)

Issues

- End to End Compromises
- Hyper Layered Tech
- Downstream Security Model
- Security Economics
- Regional & Events security constraints
- Security Maturity

Solutions

- ENISA 5G SCM & others
- Superposition & Planning
- Maturity, Priorities & Phases
- Automation
- Active Measures

Audience

- Gov, NRAs, NISAs, LEAs
- Operators
- Vendors
- Security Providers, CSIRTs

Subscribers Security

Signaling | Messages | Content | Devices

- Dark Unmonitored Domains
- Scale of Devices
- Reach Impact of Usages
- Attackers Pressure
- Attack Creativity
- Attackers Fragmentation

- Mobile Enterprise SIEM
- Anti Smishing
- Mobile Response & Threat Hunt
- Fleet Alerts
- Privacy Apps & Regulations

And many others: Bug Bounties, Information Sharing,

- Enterprises
- HVTs VIPs
- Subscribers
- IoT
- Verticals

Budget vs Attacker Focus: Leveraging enterprise security for MNO security

Conclusion

- Protecting Mobile operator is a **hard job**:
    - **many perimeters** with both
        - **outdated** legacy technologies (VXworks !)
        - and **bleeding edge layered technologies** (Layer 8 Kubernetes to Layer 1 Optical ROADMs + Ethernet FlexE for SPN Transport)
- **Coverage** and **depth of audit**
- **Automation** of audits & remediation: many perimeters are not scanned nor monitored (SS7, Diameter, ...) -> **DevOps & CI for Mobile Security**
- **Investment vs Attack surface** : investment in **5G,** but a lot of **legacy** is **vulnerable and not going away**
- Leveraging **needs of Enterprise subscribers** to provide security services to their SIEM: eg **Anti-smishing threat management**, Agentless **Mobile Fleet Attack Surface Management** etc...
- Security is not anymore only cost center → **Revenue Generation ensures good security**

Thank you !

Questions?

contact@P1sec.com