P1 SECURITY

FRNOG #38 - 2023

5G Stand Alone Security

Real 5G with Real Attack Surface

Philippe Langlois

P1 Security

Mobile, Telecom & Infrastructure Security

2023-10-06

Agenda

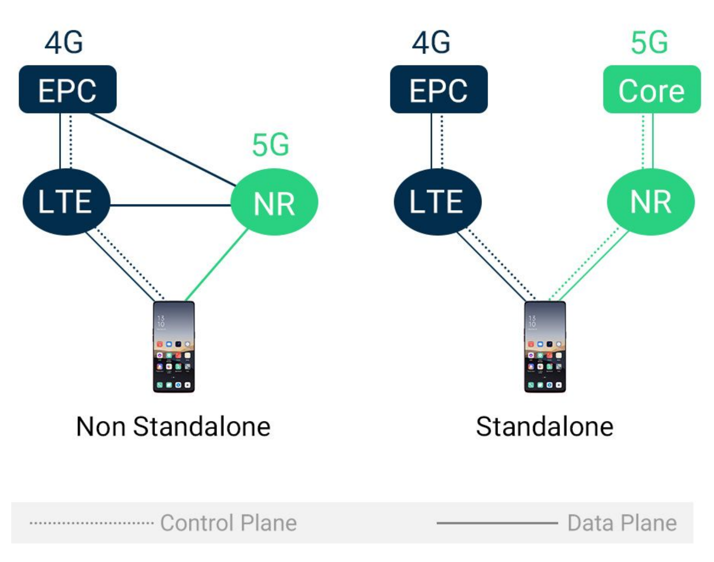
- What is 5G Stand Alone (5G SA) and its Security?
  - 5G Stand Alone technology
  - 5G Network usage and security overview
  - 5G Network attack surface
- Real cases from Pentests & Audits
  - How are vendors performing with Product Security?
  - Is Hybrid (Phy + Software + Cloud) affecting security?
  - How Cloud speed-up vs. Sovereignty is arbitrated?
- Is Telecom & Mobile security improving?
- Conclusion

5G Stand Alone technology

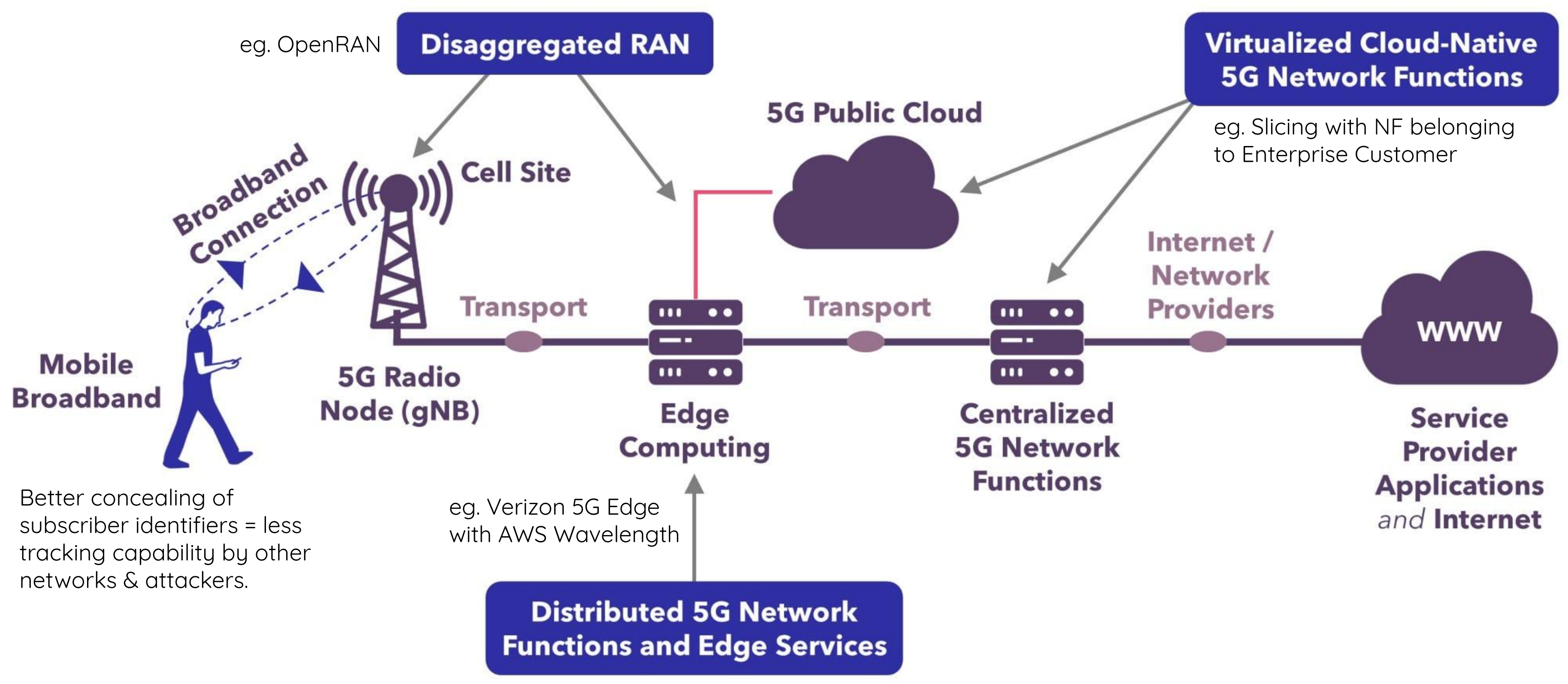
- This presentation focuses on **5G StandAlone** (5G SA) infrastructures
  - Different from 5G Non StandAlone (5G NSA): relying on a 4G Core Network

- **3GPP standards**
  - **Rel.15** (Q3 2019): focused on 5G NSA
    - NR radio interface (NR = 5G New Radio)
  - **Rel.16** (Q3 2020):, focused on 5G SA
    - 5GC and Service Based Interfaces

- Currently, **most of the 5G networks** worldwide **are still NSA**
  - MNOs struggle to deploy SA
    - A Core roll-out is complex
    - Many MNOs still have no strong business cases for 5G SA



5G Network usage and security overview


Disaggregated RAN
Virtualized Cloud-Native 5G Network Functions
5G Public Cloud
Cell Site
Broadband Connection
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

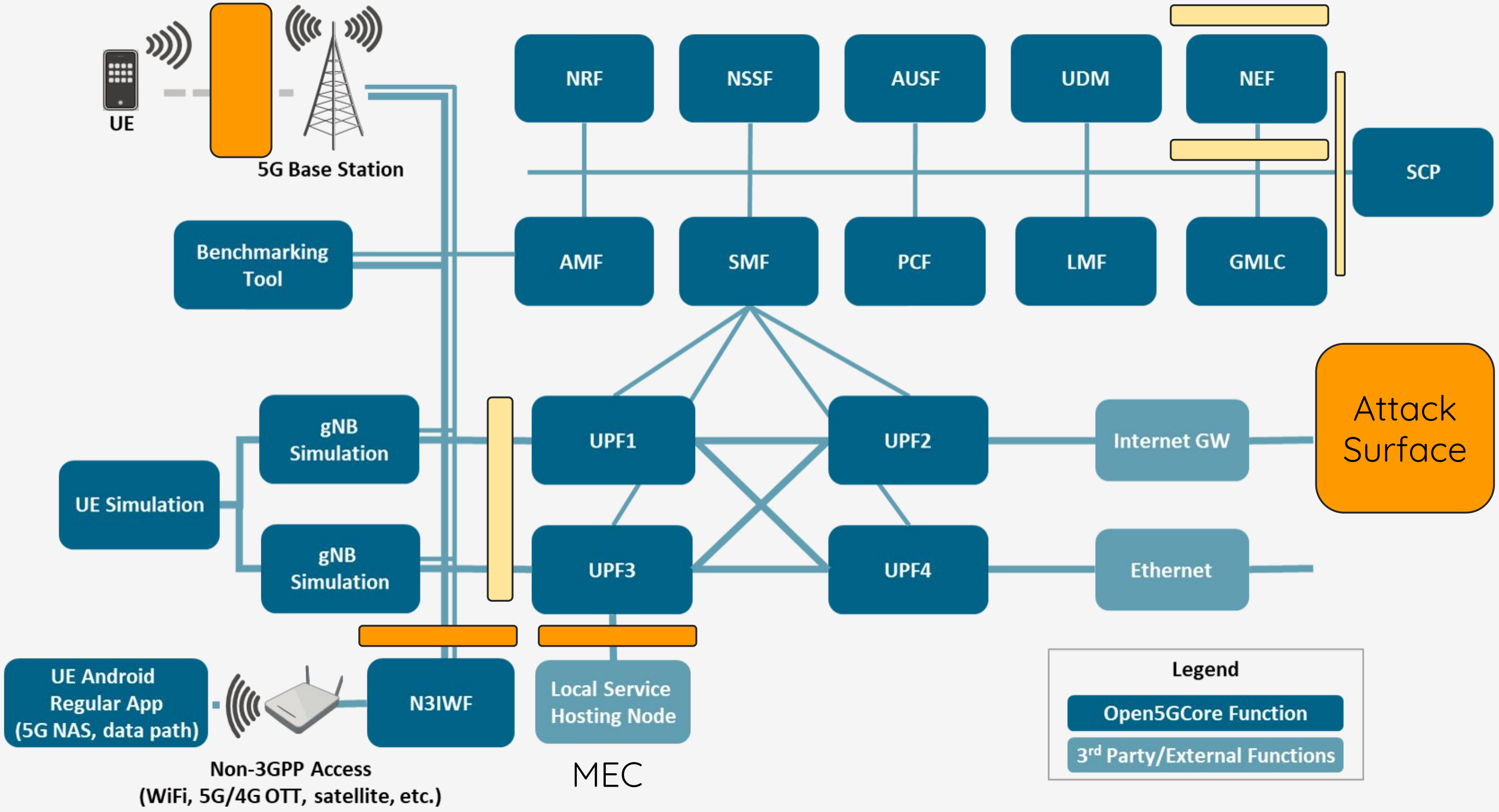
eg. OpenRAN

eg. Slicing with NF belonging to Enterprise Customer

eg. Verizon 5G Edge with AWS Wavelength

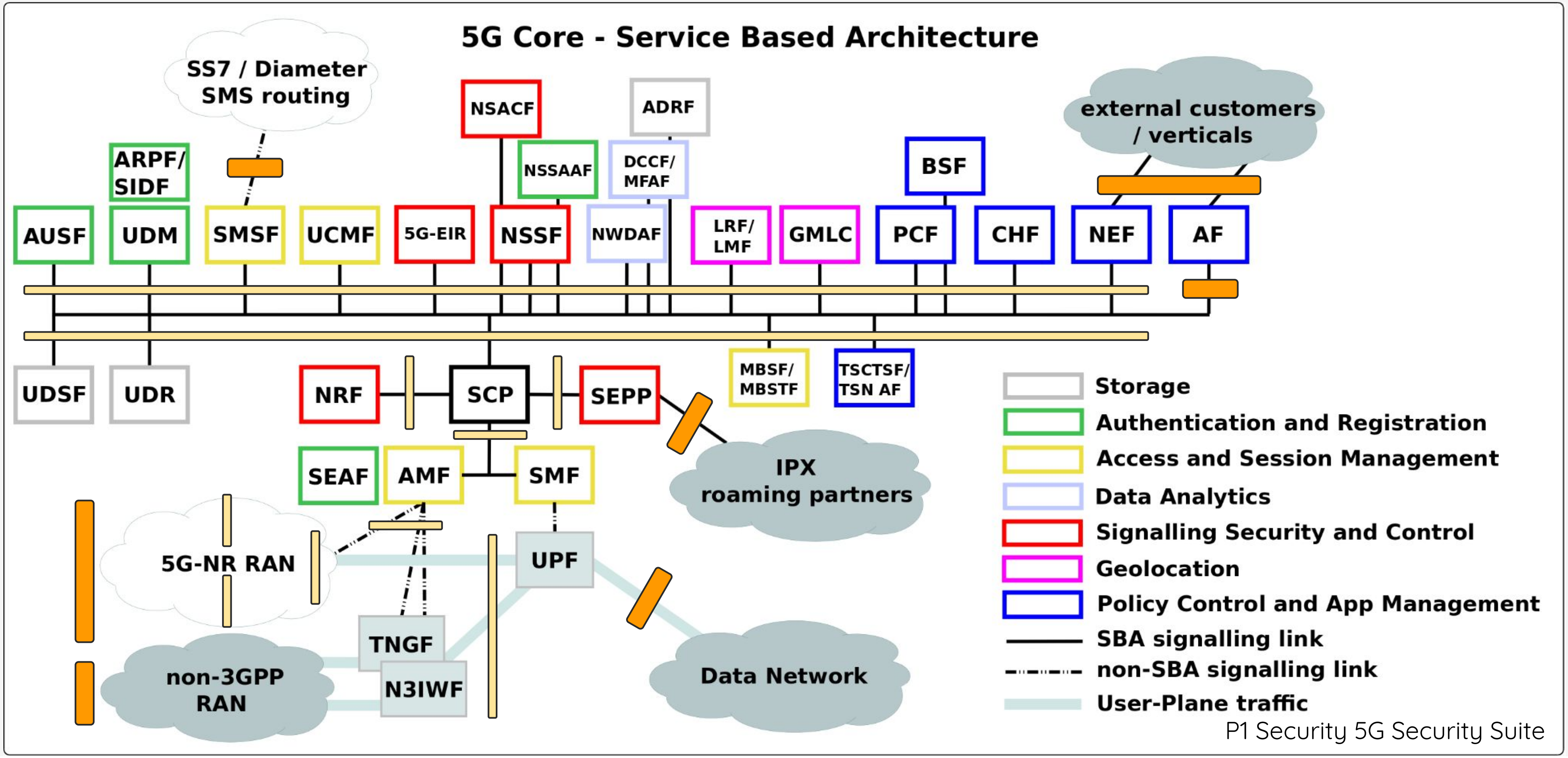
Better concealing of subscriber identifiers = less tracking capability by other networks & attackers.

5G Testbed Network attack surface (eg. Open5G Core)



5G Real Network architecture complexity & attack surface

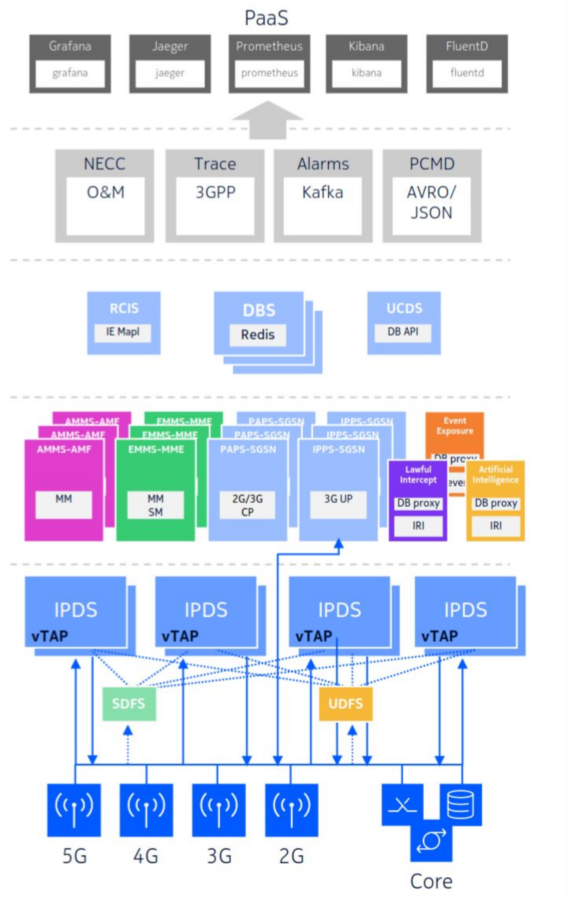
5G Security Suite's Risk Mapper, not spec

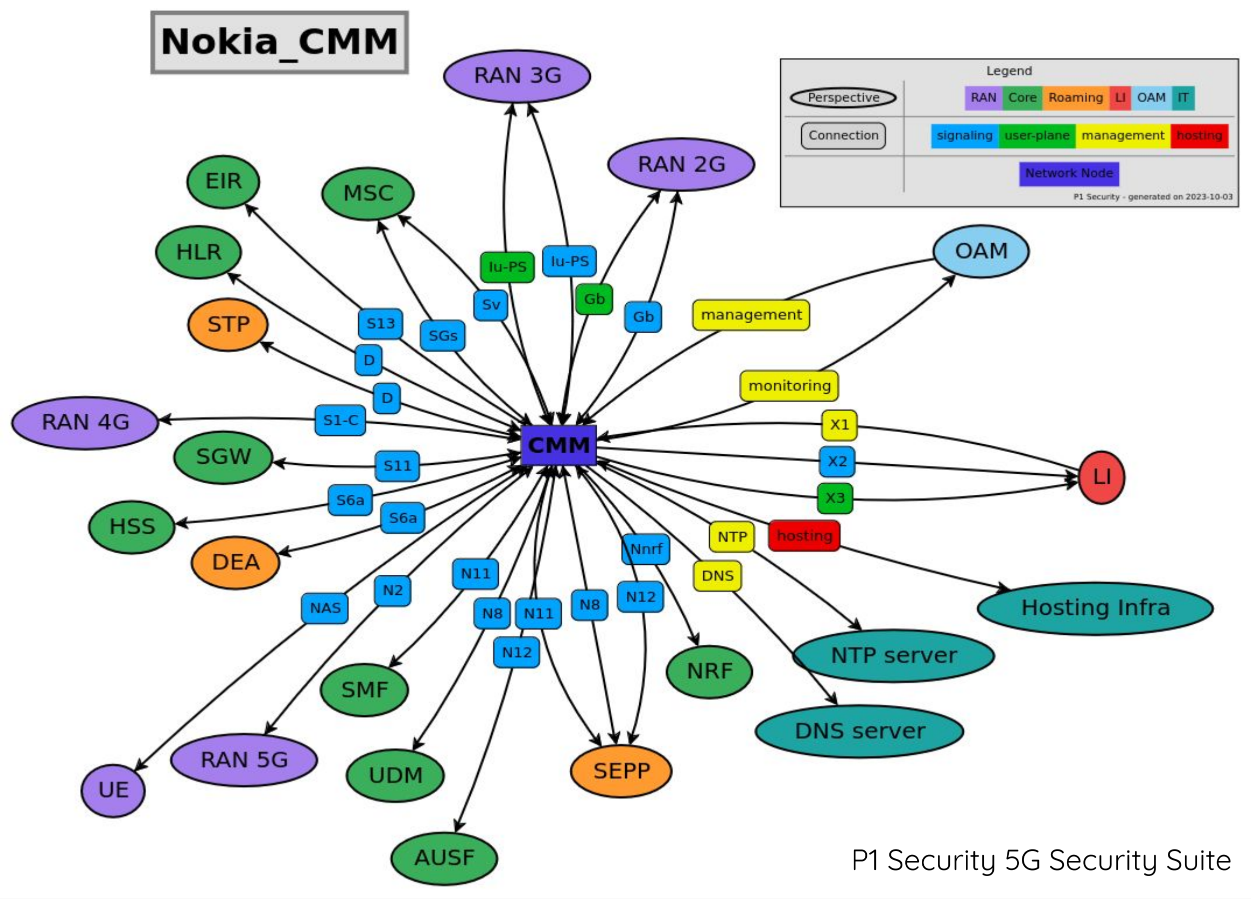


P1 Security 5G Security Suite

5G Network Function system complexity

Digging down into a single Network Function: Nokia CMM (5G AMF, 4G MME and 2G-3G SGSN) -> Complexity Explosion





P1 Security 5G Security Suite

5G pentests & security evaluations results

- **Linux** all-the-way !
    - **Data-plane** handled into **dedicated hardware** (i.e. for 10xM subs deployments)
    - Or **within network cards** in off-the-shelf servers
        - Controlled through DPDK / VPP
        - In rare cases, SCTP and part of signalling stack also run there
- Essential 5G network functions and features
    - No specific slicing configuration considered for production
        - But MNOs interested in testing slicing and NSSF in their 5GC
    - Inter-NF communications with **mTLS**, but no fine-grained authorizations (no OAuth)

Examples of vulnerabilities in 5G NF (1/2)

- **Physical** level
  - IP “hidden encapsulation” in eCPRI: compromise Antenna -> RAN / Core
- **Infrastructure** level: OpenStack, hypervisors, Kubernetes and containers environments
  - Some virtualized / containerized applications running privileged & extended capabilities
  - **Insecure Container** & Docker configuration
  - Missing network **micro-segmentation** between NF, virtual interfaces and sub-networks
  - **Hardcoded secrets** (private keys, passwords…) in **O&M binaries**
  - **LPE** often easy (insecure base configurations)
  - **Compromising a 5GC NF** system enables to **pivot to the rest of the MNO internal network**: subscriber profiles and charging / billing / CDRs, LI platform, O&M, internal IT / Active Directory…

Examples of vulnerabilities in 5G NF (2/2)

- **Signalling** level
  - **Crash** of network services found with P1sec fuzzing products (PTF)
    - C / C++: memory management issues, may be turned to **RCE**
    - Java / GO: plain crash
    - Can lead to few seconds to minutes of downtime: complete **deny of service** if looped
  - **Bypass access control** on SBA APIs, enabling e.g.: subscribers tracking
- **Subscriber facing** application level
  - Security procedure bypasses e.g., AMF accepting insecure NAS connections
  - Generation of predictable subscribers' TMSI
  - Un-met 3GPP SCAS security profiles (e.g. for AMF)
  - Put subscribers' communications and **privacy at risk**

Security Posture & Balance

Is Telecom & Mobile security posture improving?

Positive

- **Compliance** & Education improves (ENISA, 5GCTF, NIST, …)
- SUCI Concealed Identifier & **resistance to bad networks** (roaming)
- Internal core network traffic can be encrypted (**mTLS**)
- 3GPP understood that IPsec is not really scalable nor adapted
- Kubernetes, CNCF, OpenRAN, ONAP Technology **can be hardened**
- **OpenRAN still rare**, less complexity in RAN
- **Slicing** QoS includes Radio & resources

Negative

- Old code base in **Memory unsafe** languages (security “**Rule of 2**” not respected)
- **Signaling abuses** still (5G SBI)
- Kubernetes, CNCF, OpenRAN, ONAP **complexity**
- **Reluctance of vendors** to change Network Functions’ base images (eg to include EDR)
- **Authentication & Crypto** Security Management is not great (no Oauth2, fixed certificates)
- **Vendor Security & SCRM is still bad** and not open to collaboration with security community
- **Hard-coded** or undocumented unchanged authentication is still frequent, **legacy**

Ecosystem Security Considerations

- **Vendor** & supplier level (NEV / NEP)
  - **Vendors** are a new kind of attack surface
    - **Upstream** compromise at vendor or CVE in FLOSS package
    - **SCRM** : Supply Chain Risk Management (SBOM, VEX, sigstore, SLSA)
    - **Threat-centric** security: many APTs focus on Telco (Regin), Threat Intel
  - **Bypass access control** on SBA APIs, enabling e.g.: subscribers tracking
- **Hybrid:** Physical + Software + Cloud
  - Attack surface is not a single perimeter
  - Zero Trust Network Access (ZTNA) requires maturity, vendor nogo
- **Cloud** speed-up vs **Sovereignty** arbitration
  - Testbed plans <> National Critical Infrastructure Security Requirements
  - Going to production becomes very hard.

Conclusion

- Network compromise is **feasible from many perspectives**: attack surfaces needs to be defended (incl. physical attack surface & signaling)
- **Supply chain risk is high** : Some vendors are better than others at securing their product. **Upstream is an attack surface**.
- Network using **Kubernetes and CNCF technologies**: Complexity, Attack Surface, Vulnerabilities, Compromises
- Need **threat-centric defensive & deceptive security** (honeypots): Seamless Audit, Monitor, Harden, Trap helps a lot. Needed for upcoming sensitive events (Paris JO 2024, WEF, G7, …) & sensitive regions (Ukr, TW)
- **Compliance is helping**: regulators pushing for more security, harder to deliver (so much to audit -> Audit & Monitoring automation)
- **Edge Computing & Enterprise Exposure** is a huge entry point (SA6).
- **Private 5G (and 4G)** is coming fast, security problems too.

P1 SECURITY

Questions?

Thank You !

ontact@p1sec.com

https://www.p1sec.com

Thank you !

Do not hesitate to reach out: contact@p1sec.com

P1 SECURITY

BACKUP SLIDES

Security complexity (6k-20M postures)

Technology: 2G-3G, 4G, 5G	2-4 Technos
Plane: Physical, User-plane, Signaling-Plane, Infrastructure-plane, LI,	x 4-10 planes
Network Functions	x 15-40 NFs
System Design & Components	x 10-100 Components
NF Instances	x 5-500 NF Instances
Configurations	x 5-20 Configurations