“The increased speeds and lower latency of 5G networks are beginning to impact nearly every facet of life for consumers and enterprises. Fortunately, security has been built into 5G right from its inception and has been required throughout its development, planning and deployment.”

Chris Pearson, President, 5G Americas
“5G will allow operators to evolve toward new business models. For 5G to achieve its potential, organizations must embrace multi-layered security that goes far beyond 3GPP specifications by using a pragmatic, multi-layered approach. End-to-End Security should cater to RAN, SDN, MEC, and hybrid, multi-cloud deployments based on a cloud native architecture, secure CI/CD, and zero trust security for 5G.”

Pramod Nair
Technical Solutions Architect - Security
Cisco
“5G continues to integrate with other key technology enablers. In the cloud’s multi-stakeholder environment, cloud-native function software vendors, platform vendors, mobile network operators, hyperscale cloud providers, and system integrators must collaborate to clearly define requirements, roles and responsibilities for implementing security architecture and controls.”

Scott Poretsky
Director of Security, North America, Network Product Solutions at Ericsson
5G Deployment Models

On-premises

5G CNFs deployed only on Private Cloud, programmable routers, low footprint servers

Multi-stack
Public Cloud

5G CNFs deployed only on Public Cloud providers (GCP, AWS, Azure etc) & Public Cloud provided by 5G Equipment Vendors

Hybrid Cloud

5G CNFs deployed on mix of on-premises & Multi Stack Public Cloud
Evolution to 5G CNFs
Security risks within the 5G CNF deployments

- **5GC Container vulnerabilities**
  - Insecure container build
  - Container runtime vulnerabilities
  - Insecure container host
  - Malicious Container network traffic
  - Malicious 5GC CNFs
  - Insecure container management and orchestration
  - Improper access control
  - Insufficient isolation

- **Internal Interfaces**
  - API vulnerabilities within SBI communication
  - Insecure network leading to eavesdropping

- **External Interfaces**
  - Improper Isolation & Segmentation with enterprise network
  - API vulnerabilities
  - Vulnerabilities relates to non-3GPP MEC NFs
  - Insecure roaming interface & misconfigurations

- **Hardware**
  - NFVI Hardware & Software vulnerabilities
  - Improper Access control
API Security controls in the 5G Service Based Architecture (SBA)

1. SCP (optional 3GPP) for creating NF <-> NF communication mapping and high-level global access list etc

2. Secure API using mechanisms like token-based authorization using OAuth 2.0 and encryption using TLS

3. API GW / WAF to mitigate attacks exploiting API vulnerabilities by using mechanisms such as rate limiting etc

4. Secured API Signalling exchanges between roaming partners using IPsec or TLS

5G Packet Core CNFs:
- UDM
- NSSF
- NRF
- PCF
- AF
- NEF
- SEPP

HPLMN - VPLMN
Service, Orchestration, and Automation layers in a 5G network
### Layered 5G security controls

<table>
<thead>
<tr>
<th>Tier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orchestration</td>
<td>Securing Orchestration management &amp; interfaces, Securing Policy Enforcement and enhancing visibility within Orchestration and between Orchestration and network components</td>
</tr>
<tr>
<td>User</td>
<td>Segmentation, User Access based on Zero Trust principles, DNS protection</td>
</tr>
<tr>
<td>Network</td>
<td>Segmentation, Policy enforcement, Securing Network interfaces, Securing Cloud integrations and workloads, Securing Peering &amp; Roaming interface</td>
</tr>
<tr>
<td>Applications</td>
<td>Securing 3rd Party application interfaces, DDoS protection, Application security, DevSecOps practises, Segmentation, Cloud application policy sync and enforcement, securing API</td>
</tr>
<tr>
<td>VNFs and CNFs</td>
<td>Securing VNF / CNF, securing Software Lifecycle, Isolation between VNF’s / CNFs, detecting malicious virtual functions and vulnerabilities</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Hardening of NFVI, perimeter security, DDoS protection, securing – E-W traffic</td>
</tr>
</tbody>
</table>
Zero-Trust Architecture Logical Elements

Zero-Trust Architecture (ZTA)

Policy Engine (PE)
- PE offers the final decision in providing access to a resource

Policy Enforcement Point (PEP)
- PEPs serve as a system gateway for activating, monitoring, and terminating connections between authorized users and their accessed resources.

Policy Administrator (PA)
- PA establishes access to a resource

NIST SP 800-207
Overlay of NIST ZTA with 3GPP 5G Architecture

- **T1**: Each element in 5G is considered a resource.
- **T2**: Enable secure communication
- **T3**: Granted Access Between NFs over SBI
- **T4**: Dynamic Policy
- **T5**: Monitoring / Analytics
- **T6**: Resource authentication & authorization
- **T7**: ‘Risk-assess’ everything

Legend:
- **NIST Zero-Trust Logical Component**
- **NIST Zero-Trust Architecture Tenets**

- Continuous Diagnostics & Mitigation systems (CDM) - (NIST 800-207)
- Zero Trust Architecture should have risk supply chain management of its network functions.
  - Network functions should be compliant with GSMA NESAS.
Roles of 3GPP and GSMA in NESAS
NESAS High Level Overview

GSMA appoints Audit Team, which defines and provides Methodology and requirements to Audit Body. Audit Body writes Audit Report provided to Equipment Vendor, which builds Network Product evaluated by Evaluation Report. SCAS writes Test specifications applied provided to, by agreement. 3GPP SA3 defines and accredits.
# Open-source software security benefits and risks

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developers behave as “good citizens” in which consumers also contribute, provide useful feedback, and share fixes.</td>
<td>Intentional backdoors can be inserted by malicious developers.</td>
</tr>
<tr>
<td>Transparency of code. Many expert eyeballs reduces software complexity and the number of bugs. This crowdsourcing approach effectively produces quality software at low cost.</td>
<td>Attackers can review code to identify vulnerabilities.</td>
</tr>
<tr>
<td>Open source provides a platform for talented coders to openly collaborate and build software.</td>
<td>Developers do not spend sufficient time on security. Vulnerabilities can propagate through reuse.</td>
</tr>
<tr>
<td>Open source also reduces fragmentation and increases interoperability among different products by producing components and protocols that become the de facto standard.</td>
<td>‘Trees of dependencies’ make it difficult to ensure all uses of the code are patched.</td>
</tr>
</tbody>
</table>