

Cloud-Native 5G O-RAN Security Toolbox

Navid Nikaein
CEO, BubbleRAN
Professor, EURECOM



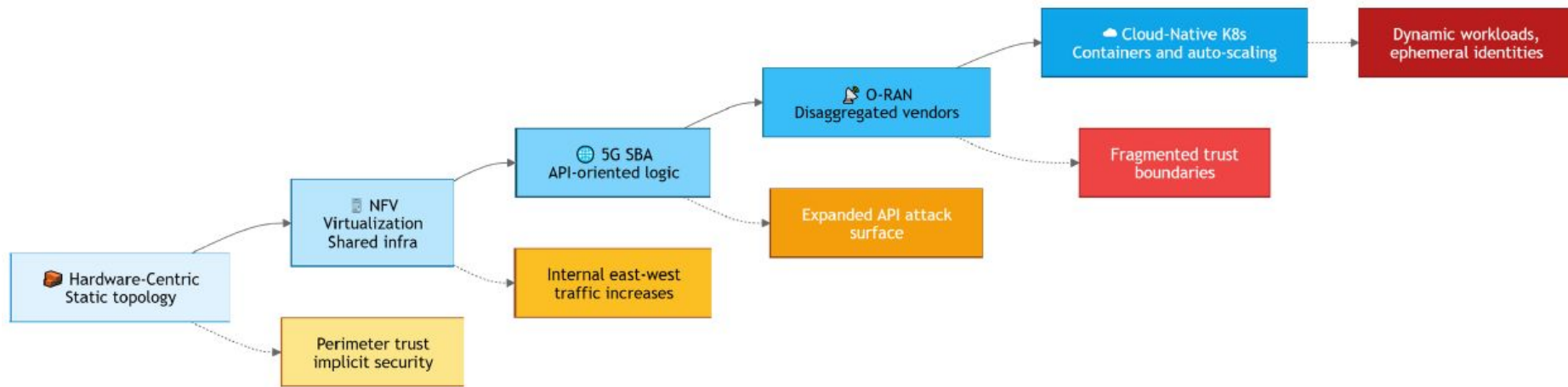
5G-TACTIC Training Workshop
Regulatory aspects of 5G networks Cybersecurity & Trust
26/05/2026, University of Athens



01

Introduction

Evolution of 5G Architecture and Emerging Security Surface



How does AI-driven runtime decision layer expand this attack surface?

Emerging Security Surface

- **Critical Planes**

- **Control Plane (AMF, UDR):** Sensitive user data
- **User Plane (UPF):** User services
- **Sync Plane (Fronthaul):** Network Service
- **Decision plane (xApp/rApp/AI):** Performance degradation
- **Wireless Plane:** jamming, sniffing, spoofing

- **Cloud Native dynamics**

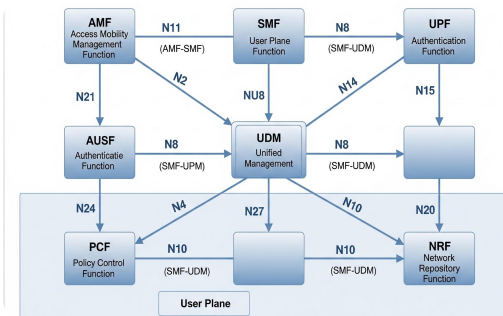
- Ephemeral Containerized Microservices
- Frequent updates
- Static policies

- **Lateral Movement Risk**

- **Rogue workloads** inside the network service / cluster
- Over-permissive network policies
- Misconfiguration drift

- **Open-source exposure**

- Publicly available projects can be analyzed by attackers to find exploitable bugs/crashes



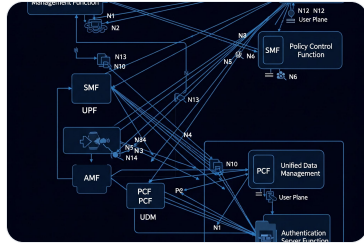
Security Paradigm



Legacy reactive measures are insufficient. Modern software-driven networks require proactive **"Security by Design"**.

Adaptive Zero Trust Security for Cloud-Native 5G

A progressive analysis of security threats in modern telecommunications.



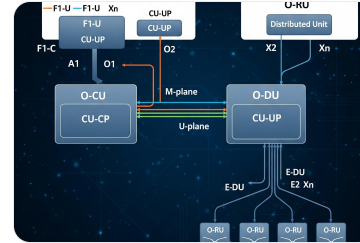
Foundational 5G

Analyzing vulnerabilities in initial 5G architectural standards.



Cloud-Native Shift

Securing deployments in containerized and dynamic environments.



Openness & APIs

Managing the attack surface of open and split RAN interfaces.



Runtime Decision

Implementing Zero Trust with real-time threat response.



02

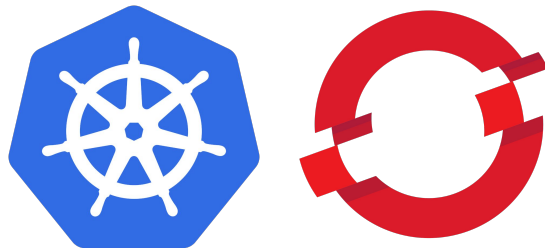
Cloud-Native 5G

The Shift to Cloud-Native 5G

- **Containerized Deployments:** 5G network functions are now deployed as containerized microservices managed by orchestration platforms like Kubernetes.
- **Dynamic Workloads:** Cloud-native 5G features ephemeral pods & Identities, continuous scaling, and frequent updates, for which static security policies are not sufficient
- **Fragmented Trust:** Moving to software-based APIs expands the attack surface and creates fragmented trust boundaries across the network



A GLOBAL INITIATIVE



The Illusion of Perimeter Security

Cloud-native 5G environments render traditional external-only defenses obsolete.

Internal Vulnerabilities



Traditional security focused on perimeter defense, but cloud-native 5G runs on shared infrastructure where internal, east-west traffic increases significantly.

Implicit Trust



By default, Kubernetes networking is flat; pods share an implicit trust and can freely communicate within the cluster unless actively restricted.

Failure of Static Rules



Legacy static controls protect the network before deployment but fail to reason about dynamic 5G behaviors at runtime.

End-to-End DevSecOps

- **Code**
 - Performs static analysis and scanning
 - CodeChecker (bug detection), Detect Secrets (secret scanning), ClamAV (malware detection)
- **Container**
 - Scan dependencies inside container images
 - Identify vulnerabilities (CVE, outdated packages)
- **Cluster**
 - Runtime Process and Network Security and policy reconciliation and enforcement .

Three Privilege Levels:

 - **Debugger:** audit/log only for debugging the microservices
 - **Secure:** predefined static policies (package manager disabling ...)
 - **Zero-trust:** dynamic policies discovery, and enforcement, and reconciliation
- **Cloud**
 - Secure Infrastructure
 - Hardware Vulnerability
 - Data Encryption

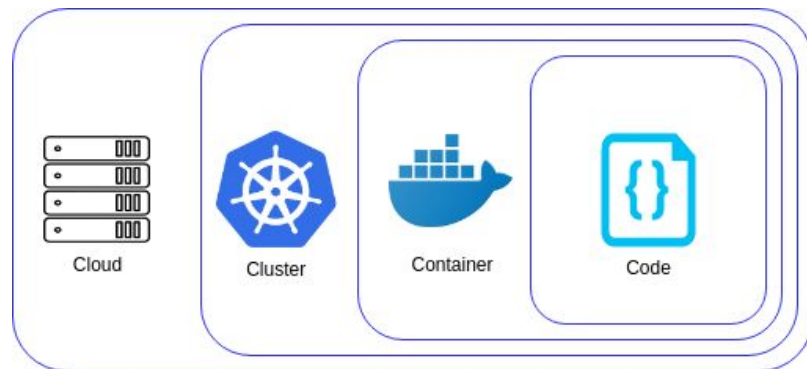


Image source can be found [here](#)



03

O-RAN

Openness via O-RAN

Breaking the Monolith with Openness: O-RAN extends the disaggregation concept introduced in 5G to foster innovation and multi-vendor interoperability.

O-CU (Central Unit)

O-DU (Distributed Unit)

O-RU (Radio Unit)



Non-Real-Time RIC and Service Management and Orchestrations

Operates in control (A1) and management (OEM) loops longer than 1 second, orchestrating third-party applications called **rApps**.



Near-Real-Time RIC

Operates in control loops between 10ms and 1s, orchestrating **xApps** to enforce policies and manage radio resources.

O-RAN Open Interfaces

Enabling multi-vendor interoperability through standardized communication planes.

R1 & A1 INTERFACE

RIC Coordination

Connects the non-RT RIC and near-RT RIC, enabling policy-driven guidance of xApps.

E2 INTERFACE

Telemetry & Control

Connects the near-RT RIC with E2 nodes (O-CUs and O-DUs) to stream telemetry and provide control feedback.

OPEN FRONTHAUL

O-DU to O-RU link

Synchronization, Management, and Communicates through C/U/S/M planes between distributed and radio units.

R1 & O1 INTERFACE

Management & Orchestration

Enables OEM Services and connects the SMO (Service Management and Orchestration) with O-RAN elements for operations, administration, and maintenance.

The Expanded Threat Surface of O-RAN

O-RAN expands the threat surface significantly compared to traditional 3GPP networks.



1. New Functions

Security risks within RIC, xApps, and rApps frameworks.



2. Open Interfaces

Exposure via R1, A1, E2, O1, and Open Fronthaul.



3. Distributed Architecture

Complex disaggregated nodes increase entry points.



4. Fragmented Trust

Multi-vendor environments split security ownership.



6. Open-Source Code

Risks from third-party libraries and code reuse.



04

ToolBox for Cloud-Native O-RAN Networks

Static analysis

Code & Container Static Analysis
Leaked Secret Analysis
SBOM Analysis
Malware Analysis

Network Security

Continuous Network Observability
Continuous Policy Reconciliation & Enforcement
(Role-Based Communication, Least-Privilege
Microsegmentation, Drift detection)

Runtime Security

Continuous Process Observability (Exec, Access)
Continuous Policy Reconciliation & Enforcement
Post-incident investigation & Forensics

DevSecOps: SBOM & Supply-Chain Security

- **Software Bill of Materials (SBOM):** Extracting SBOMs from 5G images using tools like **Syft** to enumerate all runtime dependencies and system libraries.
- **Vulnerability Correlation:** Tools like **Grype** match these components against databases to expose supply-chain risks introduced by third-party code.
- **Malware Gatekeeping:** Utilizing signature-based scanning (**ClamAV**) to block the CI pipeline immediately if malware is detected in compiled binaries

A screenshot of a security dashboard with a dark theme. At the top, there are five colored boxes showing counts: 212 (blue), 0 (red), 0 (orange), 135 (yellow), and 77 (green). Below these is a table with columns: CVE ID, Severity, Product, Fix available, Status, and Time to resolve. The table lists several CVEs with their severity levels (Critical, High, Medium, Low) and whether a fix is available.

CVE ID	Severity	Product	Fix available	Status	Time to resolve
CVE-2020-13422	Critical	libcrypto	Yes	Fixed	0.0h
CVE-2020-13422	Critical	libcrypto	Yes	Fixed	0.0h
CVE-2020-13422	Critical	libcrypto	Yes	Fixed	0.0h
CVE-2020-13422	Critical	libcrypto	Yes	Fixed	0.0h
CVE-2020-13422	Critical	libcrypto	Yes	Fixed	0.0h
CVE-2020-13422	Critical	libcrypto	Yes	Fixed	0.0h
CVE-2020-13422	Critical	libcrypto	Yes	Fixed	0.0h

Runtime Network Security

Zero-Trust Microsegmentation



cilium



Hubble



eBPF

- **Runtime Network Enforcement:**
To prevent lateral movement, cloud-native 5G requires strict, **least-privilege traffic restrictions**.
- **Cloud-native tools:**
CNI such as **Cilium** offers an eBPF-based technology integrated natively with Kubernetes that **enforces L3/L4 microsegmentation**.
- **Identity based confinement:**
Only entities that are meant to communicate are **whitelisted over specific ports**.

Interface	Connected Nodes	Protocol	Application Protocol	Default / Standard Port
A1	Non-RT RIC – Near-RT RIC	TCP	HTTP/2	Port 8443
E2	Near-RT RIC – E2 Nodes	SCTP	E2AP (E2 Application Protocol), ASN.1	Port 36422
R1	SMO –rApps	TCP	HTTP/2	Port 443 / 8443

Runtime Network Security

Zero-Trust Microsegmentation



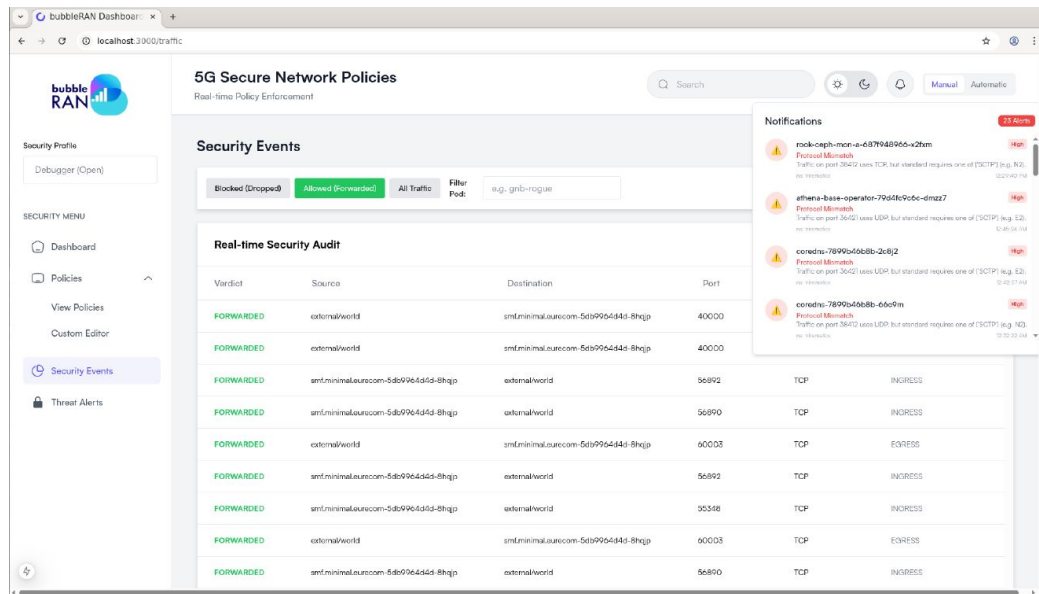
cilium



Hubble



- **Runtime Network Enforcement:**
To prevent lateral movement, cloud-native 5G requires strict, **least-privilege traffic restrictions**.
- **Cloud-native tools:**
CNI such as **Cilium** offers an eBPF-based technology integrated natively with Kubernetes that **enforces L3/L4 microsegmentation**.
- **Identity based confinement:**
Only entities that are meant to communicate are **whitelisted over specific ports**.

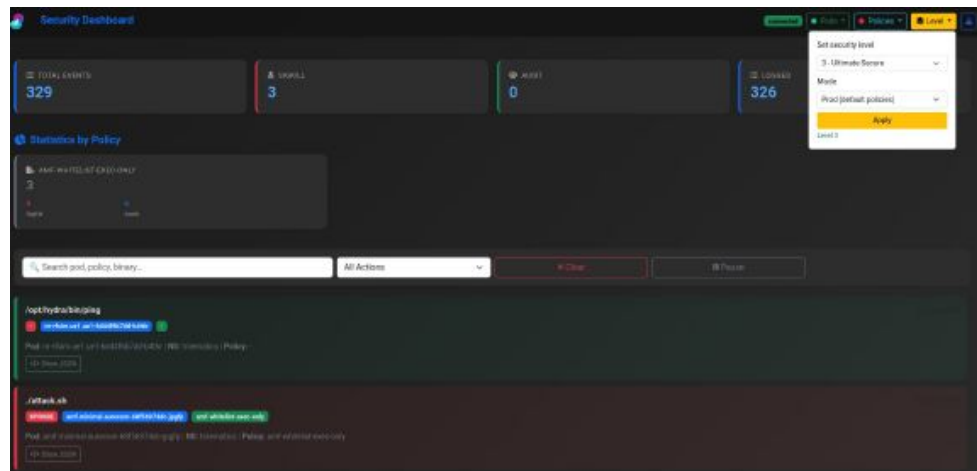


19

Runtime Process Security Kernel-Level Protection



- **Beyond Networking:**
Containerized 5G workloads interact intensively with kernel resources, necessitating **deep behavioral monitoring**
- **Cloud-native tools:**
Tools such as **Tetragon** provides **kernel-level tracing of process executions, file access, and network sockets without requiring container restarts**
- **Process whitelisting and monitoring:**
containers can be monitored at the process level to block any potential malicious behaviour.



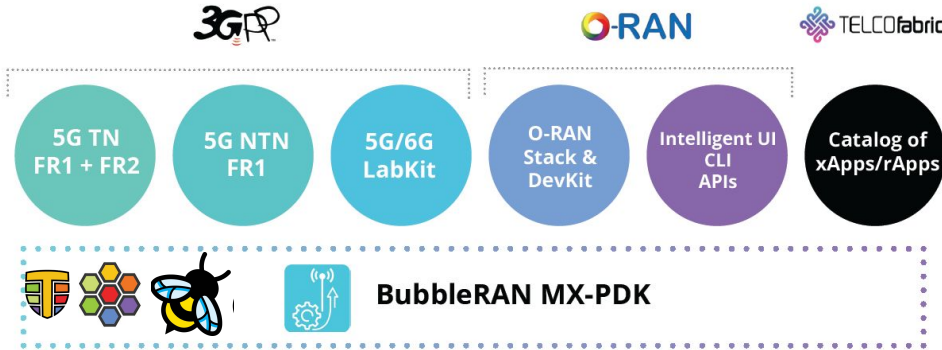


05



Secure All-in-One 5G O-RAN Solution

Secure All-in-One 5G O-RAN Solution Provided by BubbleRAN





06

Final Remarks

Best practices



**Risk = *Probability of Occurrence* x
*Consequence Severity***

Subject to *Available Resources*

- 1. Controlled Trusted Parties**
- 2. Runtime Process & Network Policy Discovery, Reconciliation & Enforcement**
- 3. Current Technologies provides tools to minimize attack surface for Cloud-native 5G O-RAN**
- 4. AI brings a new challenge and attack surface that are yet to be discovered and addressed**



Thanks!

Do you have any questions?

contact@bubbleran.com

bubbleran.com

