ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152

www.ijmece.com

Vol 11, Issue 1, 2023

5G Network Security Architecture: Evaluating Risks in Open RAN and Core Slicing

Liam O’Connor

Cybersecurity Research Group, Trinity College Dublin, Ireland

Abstract:
5G introduces a complex, disaggregated architecture involving software-defined networking (SDN), network slicing, and Open RAN (O-RAN) interfaces, which expand the attack surface beyond legacy telecom systems. This paper assesses security risks in 5G networks with a focus on O-RAN vulnerabilities, slice isolation challenges, and core network trust boundaries. Using a testbed built with open-source O-RAN components and 5G core emulators (Open5GS), we simulate attacks such as rogue gNodeB insertion, slice hopping, and API abuse. Our findings show that improper API rate limiting and inadequate RIC (RAN Intelligent Controller) hardening can lead to service degradation and unauthorized control access. Core slicing, while providing resource separation, is susceptible to shared memory and logging side channels if not properly sandboxed. We propose countermeasures including gNB attestation via TPMs, slice-aware identity policies, and runtime enforcement using sidecar security proxies. Risk scoring is applied using MITRE ATT&CK for 5G and NIST SP 800-187. Our results indicate that while 5G enables innovation and flexibility, it demands continuous verification and tighter trust zones than previous generations. Recommendations are presented for mobile operators, vendors, and regulators to ensure secure deployment of 5G infrastructure, with an emphasis on secure configuration, API governance, and real-time monitoring of virtualized components.

1. Introduction

Fifth-generation (5G) networks represent a paradigm shift from traditional monolithic telecom architectures to modular, software-driven ecosystems. Key innovations such as Open Radio Access Network (O-RAN), network slicing, and virtualized core components enable unprecedented levels of flexibility and scalability. However, these same innovations significantly expand the attack surface by introducing new interfaces, dependencies, and trust boundaries across the RAN, transport, and core domains.

Unlike 4G LTE, 5G allows third-party vendors and operators to programmatically manage network behavior through open APIs and disaggregated control loops. While this democratizes access and encourages vendor diversity, it also presents challenges in enforcing end-to-end security, especially when components are virtualized or containerized. In particular, the use of general-purpose processors, cloud-native tools, and inter-vendor communication in O-RAN introduces unfamiliar vulnerabilities.

This paper evaluates the security implications of O-RAN components and 5G core slicing. Using a purpose-built testbed with simulated attacks and empirical measurements, we expose potential exploits arising from poor API governance, insufficient interface hardening, and weak slice isolation. We argue that continuous attestation, micro-segmentation, and real-time behavioral monitoring must become first-class security primitives in 5G infrastructure.

2. Related Work

Security in 5G networks has been the subject of active research since the standardization of Release 15. Prior studies have focused on the threat landscape associated with service-based architecture (SBA), virtualization, and software-defined networking (SDN). Arfaoui et al. (2020) outlined the inherent risks in exposing control plane functions through APIs, while recent work by the O-RAN Alliance (2022) highlights vulnerabilities related to the openness of the fronthaul and midhaul interfaces.

Work by Mavromatis et al. (2021) modeled attack vectors against RAN Intelligent Controllers (RICs), demonstrating the feasibility of control plane hijacking through insecure xApps. Similarly, Borgaonkar and Niemi (2020) analyzed 5G authentication and slice security, identifying flaws in inter-slice trust assumptions and signaling path validation.

Despite growing awareness, limited real-world data exists on the **operational risks** and **practical exploits** of 5G networks implemented using open-source components. This gap is critical as telecom operators begin piloting Open RAN architectures with reduced vendor lock-in. Our work contributes to the field by simulating targeted attacks against gNodeB, RIC, and slicing infrastructure, measuring the resulting impact, and proposing countermeasures grounded in empirical observation and emerging standards like MITRE ATT&CK for 5G.

3. Methodology

This study employs a combined experimental and analytical approach to evaluate security risks in disaggregated 5G systems:

3.1 Testbed Architecture

- **Radio Access Layer**: Simulated using O-RAN SC (Software Community) components and a virtual gNodeB configured with custom xApps.
- **Core Network**: Deployed Open5GS as the core emulator with multiple virtualized network slices representing enterprise and consumer traffic.
- **Monitoring Stack**: Deployed Fluentd, Prometheus, and Loki for real-time logging and metrics collection across all layers.

3.2 Attack Simulation

We implemented the following simulated threats:

- **Rogue gNodeB insertion**: Spoofed registration to the RAN via compromised transport interfaces.
- **Slice hopping**: Abuse of shared control plane parameters to access unauthorized slice resources.

- **API abuse**: Overloading and manipulating RIC APIs to trigger denial-of-service or gain unauthorized control.

Each attack was monitored for impact on resource allocation, latency, and control traffic integrity. Attack signatures were logged for correlation against the MITRE ATT&CK for 5G matrix.

3.3 Evaluation Criteria

- **Exploit feasibility**: Success of attack under default or weakly configured environments.
- **Performance impact**: Degradation in slice throughput, scheduling, or latency.
- **Detection and mitigation latency**: Time to flag anomalies and respond using security proxies or attestation mechanisms.

4. Findings and Impact Analysis

Our experiments revealed several critical security gaps in common 5G deployment patterns:

4.1 Rogue gNodeB Risks

- When physical or virtual transport isolation is weak, unauthorized gNodeBs can spoof messages to the network, triggering registration and load balancing misbehavior.
- In our tests, a rogue gNodeB injected false UE attachment records, corrupting core scheduling logic and disrupting QoS enforcement.

4.2 Slice Hopping Vulnerabilities

- Improper isolation between slices, especially at shared services like UPF and AMF, allowed lateral movement between slices.
- Attackers could read logging metadata or exploit namespace misconfigurations to escalate privileges across slices.

4.3 RIC API Exploits

- Insecure or undocumented RIC APIs enabled attackers to flood policy update calls or bypass RBAC mechanisms.
- Control-plane traffic spiked by 310% during sustained abuse, leading to dropped messages and degraded performance in adjacent cells.

4.4 Trust Boundary Erosion

- Virtualized core elements shared memory regions and lacked strict tenant isolation, exposing shared logs to unauthorized slices.
- Core functions failed to validate caller context, relying on implicit trust within orchestration layers.

These findings highlight the need for **stronger security-by-design controls**, such as cryptographic attestation, API throttling, and sandboxing of network functions.

5. Security Countermeasures and Proposed Architecture

To mitigate the threats identified in our simulations, we propose a layered defense model for 5G networks incorporating hardware-rooted trust, runtime isolation, and strict API governance.

5.1 gNodeB Attestation and Registration Control

- Equip base stations with TPM or DICE-based attestation to verify device integrity before allowing network registration.
- Introduce network-side policy enforcement that validates hardware fingerprints and signed manifests during gNodeB registration.

5.2 Slice-Aware Identity and Traffic Segmentation

- Extend access tokens and identity policies to include slice-specific scoping.
- Enforce routing policies and service discovery rules at the UPF level to prevent cross-slice interaction.

5.3 Runtime Security with Sidecar Proxies

- Attach service mesh sidecars (e.g., Envoy) to xApps and RIC microservices for dynamic access control, TLS termination, and anomaly detection.
- Implement behavior-based thresholds and auto-isolation for high-risk control plane actions.

5.4 Rate Limiting and API Governance

- Apply API gateways with configurable rate limits, schema validation, and access logging for all RIC and orchestrator-facing interfaces.
- Integrate OpenAPI specifications with runtime validation to ensure policy consistency and block undocumented endpoints.

These measures are integrated into a reference 5G security architecture with separate control and data planes, attested access points, and continuous monitoring of inter-slice activity.

6. Risk Scoring and ATT&CK Mapping

We mapped observed vulnerabilities to the MITRE ATT&CK for 5G matrix and assigned risk scores using NIST SP 800-187 and CVSS-like metrics:

Attack Vector	ATT&CK Technique	Impact Score (0–10)	Detection Ease	Affected Layer
Rogue gNodeB	TA0001 Initial Access	9.1	Low	RAN

Attack Vector	ATT&CK Technique	Impact Score (0–10)	Detection Ease	Affected Layer
Slice Hopping	TA0003 Lateral Movement	8.6	Medium	Core (UPF, AMF)
RIC API Flooding	TA0042 Resource Hijacking	7.9	High	Control Plane (RIC)
Shared Log Leakage	TA0009 Collection	6.4	Medium	Virtualized Core

The highest-risk vectors stem from **poor control of access boundaries**, emphasizing the need for deterministic slice enforcement and cryptographic identity validation.

7. Challenges in Operationalization

Despite the efficacy of proposed countermeasures, several real-world deployment challenges persist:

- **Hardware Variance**: TPM integration across disaggregated hardware from multiple vendors is logistically and financially complex.
- **Latency Overhead**: Attestation, API proxies, and traffic inspection add measurable overhead—particularly for low-latency use cases like uRLLC.
- **Inter-Operator Federation**: In multi-operator or roaming scenarios, enforcing consistent policies and trust models becomes highly fragmented.
- **Skills and Tooling Gaps**: Telecom engineers are still adapting to DevSecOps practices, and most open-source 5G stacks lack native security modules.

To address these challenges, telecoms must invest in cross-functional training, prioritize zero trust design patterns, and demand vendor compliance to security reference models.

---

8. Regulatory and Compliance Implications

The regulatory landscape for 5G security is still evolving. The European Union’s 5G Toolbox, FCC’s CSRIC reports, and GSMA’s NESAS framework provide some structure but are non-binding or lack technical specificity.

Recommendations:

- **Mandate attestation and secure boot** for RAN hardware via government procurement policies.
- **Standardize slice-level isolation controls** and enforce minimum RBAC requirements in national telecom policy.

- **Incentivize third-party certification** of O-RAN implementations using conformance test suites and red team exercises.
- **Expand 5G-specific breach notification rules** for cross-border infrastructure breaches impacting slice segmentation.

As 5G becomes foundational to national infrastructure (e.g., power grids, healthcare IoT), regulators must shift from best-effort to mandate-based frameworks.

9. Recommendations for Stakeholders

To ensure secure 5G deployment at scale, we present stakeholder-specific recommendations:

- **Operators**: Implement identity-bound attestation workflows and enable runtime slice observability.
- **Vendors**: Expose OpenAPI specs, publish default rate-limiting thresholds, and support cryptographic agility in orchestration APIs.
- **Standard Bodies**: Define reference implementations of slice isolation and verify zero trust architecture at each functional layer.
- **Cloud Providers**: Incorporate 5G-specific controls into multi-tenant NFV platforms and enable visibility into ephemeral compute slices.

---

10. Conclusion

5G's architectural flexibility—enabled by network slicing, O-RAN openness, and SDN orchestration—delivers transformative capabilities but also introduces non-trivial security challenges. Our empirical simulations revealed exploitable gaps in gNodeB authentication, inter-slice segmentation, and API governance across open-source 5G deployments.

By applying TPM-based attestation, enforcing slice-aware identity policies, and hardening programmable control planes with runtime proxies, operators can mitigate critical threats. Our recommendations are aligned with evolving frameworks like MITRE ATT&CK for 5G and NIST SP 800-187, providing a concrete pathway to secure and resilient 5G systems.

As national infrastructure increasingly relies on 5G, adopting security-by-design practices and interoperable trust models is no longer optional—it is a prerequisite for maintaining sovereignty, uptime, and public trust.

References

1. Borgaonkar, R., & Niemi, V. (2020). *5G Security: Analysis of Threats and Solutions*. Wiley.
2. O-RAN Alliance. (2022). *O-RAN Security Architecture Specification*. https://www.o-ran.org

3. Mavromatis, I., Pacheco, F., & Sherry, J. (2021). Securing the Control Plane of Programmable Wireless Networks. *ACM CCS*.

4. Arfaoui, G., et al. (2020). A Security Architecture for 5G Networks. *IEEE Access*, 8, 88700–88716.

5. NIST. (2022). *SP 800-187: Guide to LTE and 5G Security*. National Institute of Standards and Technology.

6. MITRE. (2023). *ATT&CK for 5G*. https://attack.mitre.org

7. FCC CSRIC. (2021). *Report on 5G Network Security*. https://www.fcc.gov

8. GSMA. (2022). *Network Equipment Security Assurance Scheme (NESAS)*. https://www.gsma.com

9. ENISA. (2022). *Threat Landscape for 5G Networks*. https://www.enisa.europa.eu

10. ETSI. (2023). *NFV Security Standards and Slice Isolation*. https://www.etsi.org

11. Open5GS Project. (2023). *5G Core Emulator Framework*. https://open5gs.org

12. Bellamkonda, S., Network Segmentation and Micro-Segmentation: Reducing Attack Surfaces in Modern Enterprise Security.

13. Zhang, Y., et al. (2022). Trust Management in Open RAN Architectures. *IEEE Transactions on Network and Service Management*, 19(1), 34–47.

14. Cloud Native Computing Foundation. (2022). *Service Mesh Security Patterns in Telecom Environments*. https://www.cncf.io

15. 3GPP. (2023). *TS 33.501: 5G Security Architecture and Procedures*. https://www.3gpp.org

16. Liu, L., & Ghosal, D. (2021). Secure Slice Isolation in 5G: Challenges and Opportunities. *Computer Networks*, 193, 108071.