Financováno Evropskou unií
NextGenerationEU

MINISTERSTVO PRŮMYSLU A OBCHODU

Grant Thornton

STUDY 15 · CYBERSECURITY AND OPEN RAN IN 5G NETWORKS

Cyber risks of 5G networks: the impact of Open RAN and Open Core

AT A GLANCE **Study 15 analyses the cyber risks of operating 5G networks** — both private (closed) networks and networks *used* to deliver public services — and assesses how the **Open RAN** and **Open Core** approaches affect 5G security. Fifteen chapters map vulnerabilities and attack types, examine identity and access management, propose ways to secure data in transit, resist DDoS and keep networks available under load, set out auditing, monitoring and incident response, check backup and recovery, and review how other technologically advanced countries support open architectures.

Prepared for the Czech Ministry of Industry and Trade by Grant Thornton Advisory k.s., August 2024. Approximately 100 pages, 15 chapters.

What the study covers

5G networks carry ever more information, including sensitive information. The study examines the cyber resilience of these networks and the vulnerabilities that arise where they are built on Open RAN or Open Core. The brief set nine tasks, regrouped here into eight themes:

Vulnerabilities & impact
Where Open RAN and Open Core introduce weak points — and what they mean for the security of the whole mobile network.

Attack types
Threats to the confidentiality, integrity and availability of data in private and public 5G networks built on Open RAN.

Identity & access
Opportunities and risks in IAM, and weak points in authentication and authorisation mechanisms.

Securing data in transit
How to keep data untouched and unaltered: encryption, integrity checks, mutual authentication, network slicing.

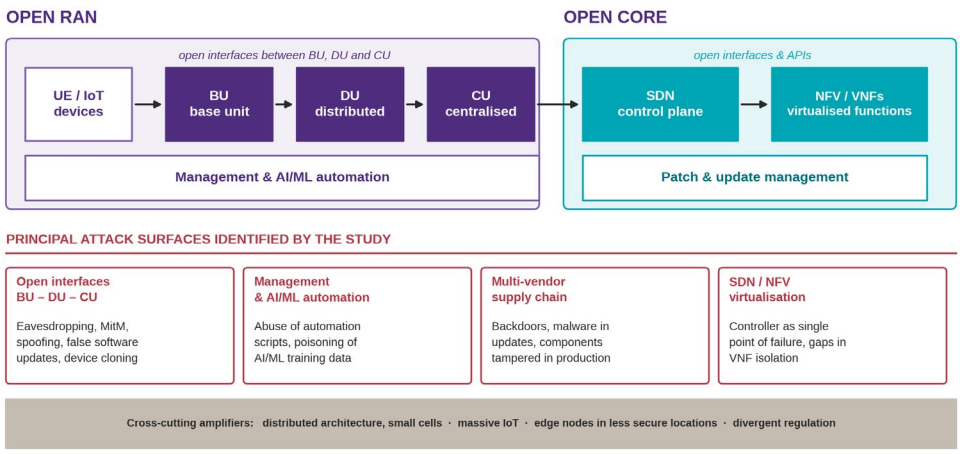
Unauthorised foreign traffic
Measures against unauthorised communication with foreign servers, and ways to detect it.

DDoS & availability
Resilience of Open RAN-based 5G to distributed denial of service, and availability under heavy load.

Audit, monitoring, response
A system for regular auditing and monitoring, and immediate reaction to security incidents.

Backup, recovery, best practice
Whether backup and recovery are at risk — and how other advanced economies support open architectures.

Where the attack surface sits



Open RAN and Open Core components and the principal attack surfaces identified in Chapters 2 and 3. "BU" (base unit) is the study's own term for the radio unit.

Five key cyber risks of 5G, as the study frames them

1. Network complexity
2. Distributed 5G architecture
3. Supply chain
4. Privacy and data protection
5. Jamming and attacks on the signal

Heterogeneity of devices and systems raises the probability of vulnerabilities; the distributed architecture widens the attack surface and can undermine the integrity and availability of services; multi-vendor dependence comes with insufficient control over the whole chain; more data in more places increases the risk of leaks; and 5G remains vulnerable to physical attacks such as jamming and interception.

Attacks on Open RAN — and the countermeasures the study proposes

CONFIDENTIALITY	INTEGRITY	AVAILABILITY	OPEN RAN SPECIFIC
THREATS Eavesdropping Man-in-the-middle Supply-chain exposure	**THREATS** Injection attacks Identity spoofing Supply-chain tampering	**THREATS** DDoS Attacks on power resources Exploiting Open RAN complexity	**THREATS** Side-channel Interface / API attacks SDN & NFV attacks Insider abuse
COUNTERMEASURES Strong encryption at every level Secure tunnelling (VPN, IPSec) Mutual authentication Segmentation, zero-trust	**COUNTERMEASURES** Input validation Security protocols, encryption Network policies + monitoring Certification, EDR at key nodes	**COUNTERMEASURES** Load balancing, redundancy DDoS protection services Rate limiting, traffic filtering Energy monitoring, efficiency Advanced monitoring, sharing	**COUNTERMEASURES** Physical security, isolation Hardened API security protocols Secured virtualisation layer Least privilege, audits, logging

Attack types and the countermeasures the study proposes for them (Chapter 4)

Five risks specific to implementing Open RAN and Open Core

Unclear split of security responsibility
Modular, multi-vendor architectures blur who secures what. Gaps nobody owns, and slower incident response.

Incompatibility and configuration errors
More configurable components mean more room for human error; uncoordinated updates cause gaps or outages.

Supply-chain risk
Hidden vulnerabilities or deliberate backdoors, vendors not meeting the same standards, dependence on a single supplier.

Expanded entry points and attack vectors
Openness that enables interoperability also helps attackers understand internal mechanisms and find ways in.

Unauthorised access, weak authentication
Identity management across heterogeneous networks is hard; inconsistent access policies open the way in.

From individual controls to a continuous cycle

IDENTIFY	PREVENT	DETECT	RESPOND	RECOVER	IMPROVE
Asset & risk assessment	Encryption, IAM, segmentation, patching	IDS/IPS, SIEM, AI/ML anomalies	Incident response team, comms plan	Backup, restore, service continuity	Post-incident review, training, sharing

Continuous loop — the study stresses that testing, validation and review of policies must be an ongoing process covering people and procedures, not only technology

Structure follows the auditing and monitoring system proposed in Chapter 12, with incident response from Chapter 13

How other advanced economies support open architectures

European Union
Horizon 2020 and Horizon Europe funding, the 5G Public Private Partnership, support for open standards and the Cybersecurity Act, innovation hubs, and sustainability as part of climate neutrality by 2050.

United States
Federal funding and grants (NTIA's BTOP, DoD 5G test beds and Trusted Capital Marketplace, NSF programmes), the Open RAN Policy Coalition, and an active — often leading — role in 3GPP standardisation.

Japan & South Korea
Government initiatives with leading operators: pilot projects and demonstration tests in Japan (NTT Docomo, Rakuten Mobile) and government R&D investment in Korea (SK Telecom, KT, LG Uplus), plus active work in international standards bodies.

Standards and frameworks referenced: O-RAN Alliance (Architecture Description, Security Focus Group, Fronthaul Interface Specifications) · 3GPP · ITU-T X-series · GSMA · ISO/IEC 27001 · GDPR · the EU Cybersecurity Act, the NIS Directive and the EU 5G Toolbox.

KEY TAKEAWAY Open RAN and Open Core offer flexibility and interoperability, but open interfaces and dependence on third-party software also raise the potential security risk. The study concludes that safe deployment needs a package of measures — stronger security standards, monitoring and anomaly detection, security audits of suppliers, data and privacy protection, and regular staff training. A carefully balanced approach to security lets 5G networks realise their full potential while minimising the associated cyber risks.