Cybersecurity at the Heart of 5G and Open RAN

Colombia CRC Symposium
Cybersecurity: A Key Factor in Telecommunications Industry

Scott Poretsky, M.Sc., CISSP, CCSP
Director of Security Policy and Standards
Strategy and Technology
Ericsson Americas

FCC CSRIC Member
Co-Chair O-RAN Alliance WG11 for Security
Co-Chair ATIS Zero Trust for 5G Study Group
Advisory Board, IEEE ComSoc TC Communications Quality and Reliability

14 August 2025

AGENDA

- Threats to mobile critical infrastructure
- Zero Trust Architecture
- 5G and Open RAN
- Key Takeaways

Security for Critical Infrastructure is top of mind

Secure Communications Critical Infrastructure

Some regulators consider telecom networks as critical infrastructure (CI) and operators must meet requirements and regulations for securing CI

Threat actors

Sophisticated threat actors are targeting telecom networks for reconnaissance, data exfiltration, unauthorized control, and service disruption

Critical Infrastructure Threat Surface

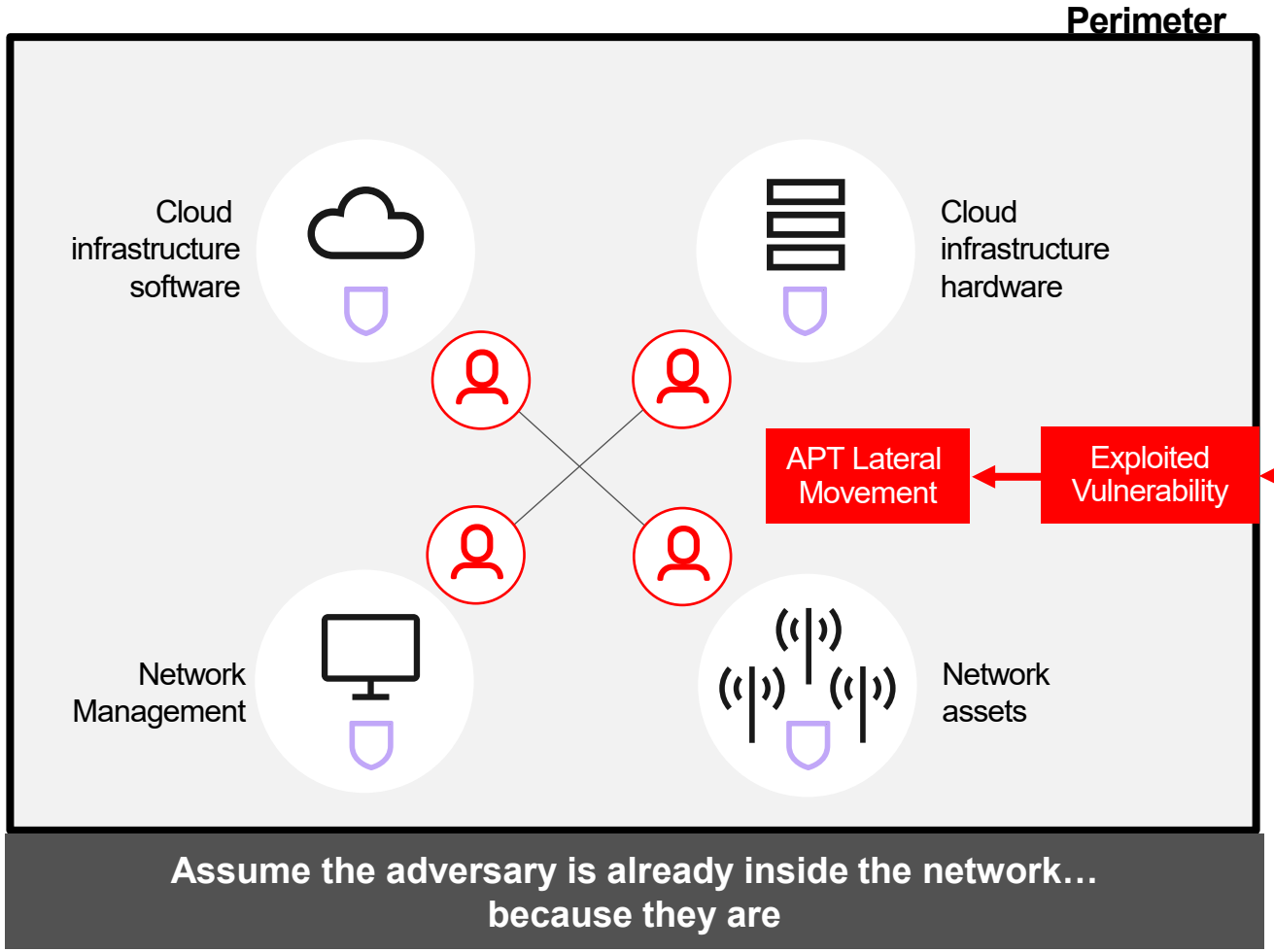
Traditional threats:

- Ransomware
- DDoS
- False Base Stations
- MiTM for Eavesdropping

New threats:

Solarwinds	**Supply chain attack** during software build process to enable remote access when deployed
Log4j	**Open-source software vulnerability** exploited API vulnerability for RCE attacks
Colonial Pipeline	Ransomware attack that resulted in **service outage of critical infrastructure** impacting citizens
Advanced Persistent Threats (APT)	Sophisticated attack exploiting multiple vulnerabilities for lateral movement and undetected long dwell time

Advanced Persistent Threats (APTs) attack critical infrastructure



APTs target critical infra

- Tier-1 mobile networks
- Regional carriers
- Utilities
- Mission-critical

APT goals

- Reconnaissance
- Data exfiltration
- Unauthorized Control
- Disruption/Damage

Foundation for APT defense

Zero Trust Architecture

- Perimeter security alone is insufficient
- ZTA protects against external and internal threats
- ZTA secures the network as if the adversary is already inside

Secure Software Development

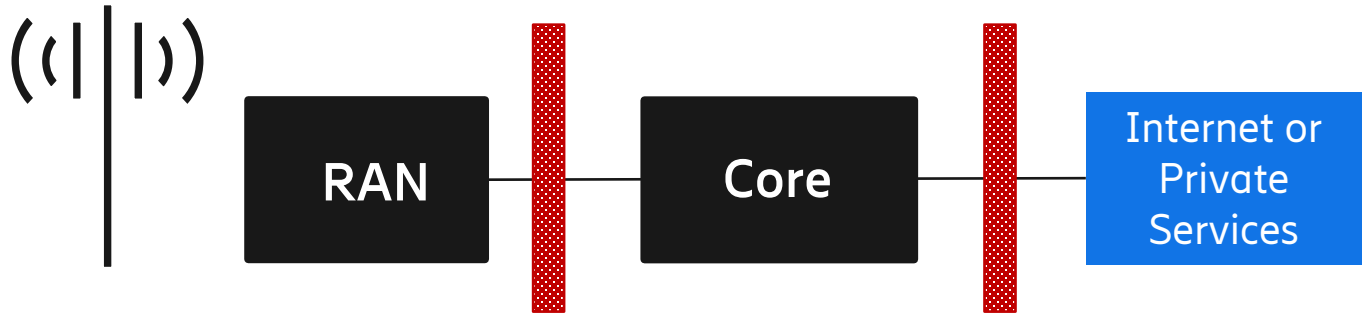
- Enhance software development lifecycle to include secure design, development, build, and delivery
- Follow established industry best practices from OWASP and SAFECode
- Software Bill of Materials (SBOM)
- Measurable goal is to reduce number of vulnerabilities and impact from exploitation

Network and Product Hardening

- Secure credentials
- Replace EOL products
- Apply software upgrades
- Patch vulnerabilities
- Use secure protocols with approved cipher suites
- Validate security configurations
- Continuously audit for configuration drift

Evolving the Security Posture

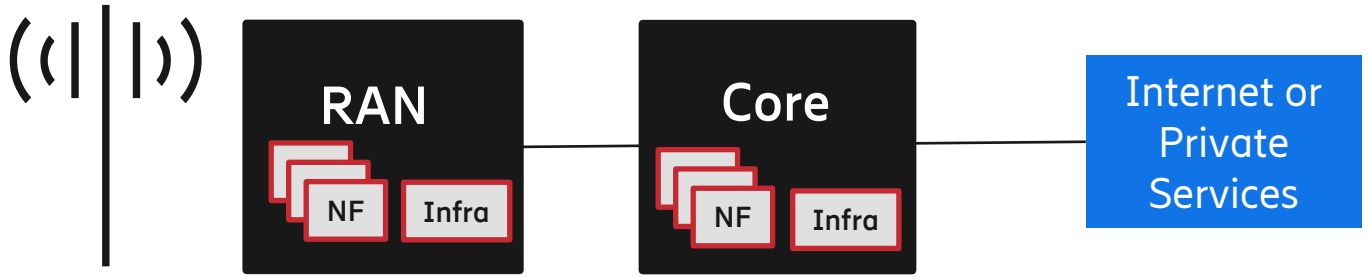
Traditional perimeter security



Traditional security

- Firewalls at perimeters
- Access controls at perimeters for external subjects to access internal resources
- Assets and users internal to network domains assumed to be trusted

... enhanced by complementary Zero Trust Architecture



Zero Trust Architecture

- Each network asset is secured as a micro-perimeter without assumption of sufficient perimeter security
- Protects from internal threats

ZTA for mobile critical infrastructure

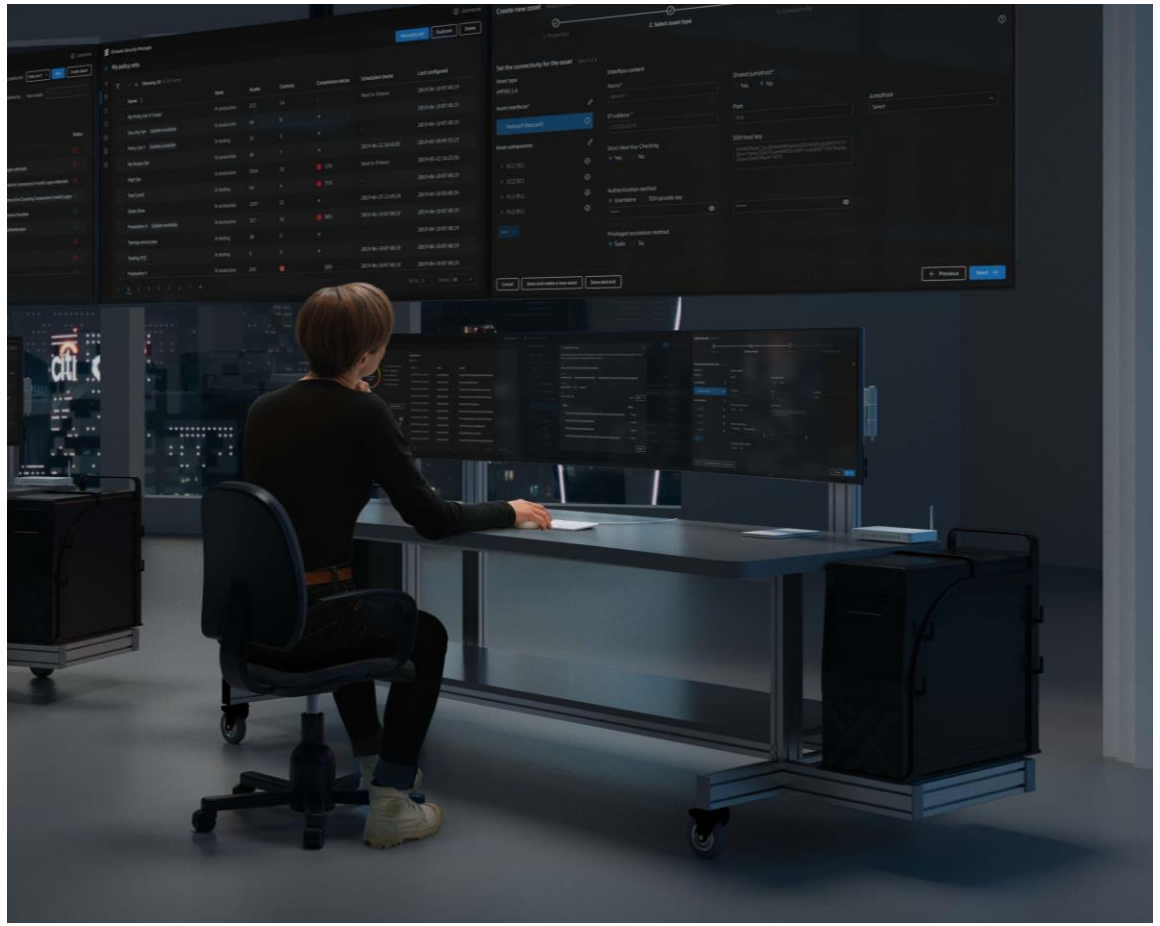
Four principles of a Zero Trust Architecture (ZTA) for mobile networks*

01 Each network function is a resource secured as micro-perimeter

02 Confidentiality and integrity protection is provided for all data

03 Authentication and authorization are enforced on a per-session basis for external and internal subjects

04 Continuous monitoring, logging, and alerting is implemented to detect and respond to security events



* Based on US NIST 7 Tenets of Zero Trust

ZTA evolution using Zero Trust Maturity Model*

Don’t wait for perfect security. Take the incremental journey in stages…

Traditional	Initial	Advanced	Optimal
• Perimeter-based security • Perimeter-based monitoring • Static network policies • Manual processes	• First steps toward ZTA • External controls and some security controls to protect against internal threats • Monitoring with known indicators • Tailored policies • Some automation	• Security controls to protect against internal and external threats • Centralized visibility • Continuous monitoring of network • Tailored policies • Security automation	• Security controls to protect against internal and external threats • Visibility with situational awareness • Continuous Monitoring of network, applications, and users • Dynamic policies by AI • Automation with AI

* Based on US DHS CISA ZTMM v2.0

Enabling Technologies for Strong Security Posture

ERICSSON

5G

Open RAN

Continuous security monitoring

AI/ML-based security automation

5G Security enhancements

Each "G" mobile generation has been more secure than its predecessor. 5G is most secure to date.

5G

3GPP R15

- Subscriber privacy with SUCI
- Subscriber authentication with EAP-TLS
- Home network control
- User-Plane Integrity Protection
- Service-Based Architecture (SBA) security with TLS and OAuth
- Secure interconnect and transport

3GPP R16

- Inter-PLMN User Plane Security
- Network Slice Specific Authentication and Authorization
- Secure Non-Public Network (NPN) for Private 5G

3GPP R17

- Enhanced Security against False Base Stations
- Security for Industrial IoT (IIoT)
- Secure Multicast and Broadcast Service (MBS)

5G Advanced

3GPP R18

- Certificate Management Protocol (CMP) for certificate enrolment and lifecycle in SBA
- Home network triggered primary authentication to refresh the KAUSF key
- Extend SBA security to authorize access to AI/ML model and data storage and sharing used for analytics

O-RAN WG11 protects attack surface

THE SECURITY CHALLENGE – Security and interoperability as O-RAN opens the RAN architecture to enable a multi-vendor ecosystem

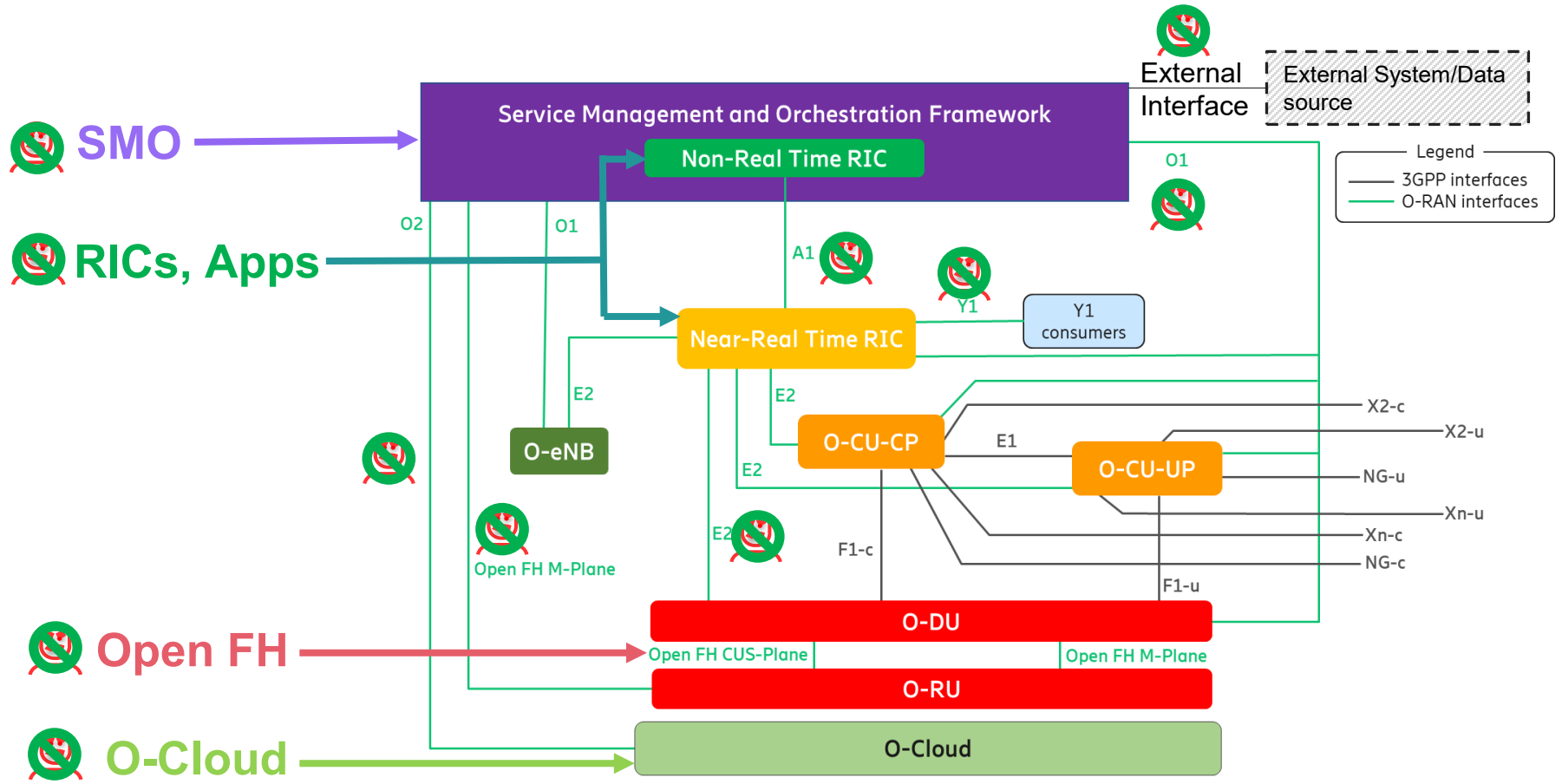
- Decoupled Service Management and Orchestration (SMO) with Service-Based Architecture (SBA)
- Third-party rApps and xApps in the RICs
- Lower Layer Split (LLS) at the O-RU and O-DU with Open Fronthaul interface
- O-Cloud with hardware and software infrastructure to run O-RAN CNFs

O-RAN security controls and mitigations are now standardized

- O-RAN Alliance WG11 has progressed the O-RAN security posture
- O-RAN Alliance WG11 for Security continuously pursues a ZTA based upon NIST SP 800-207 in its Security Requirements and Controls Specification
- Industry has advanced multi-vendor interoperability

Open RAN is secure and ready for deployment

The O-RAN security posture is now at the level expected by mobile operators for 5G



O-RAN Security Specifications for a ZTA

Security Principles	Non-Fronthaul Interfaces				Open Fronthaul Interfaces		
	A1	O2	O1	R1	C/S-planes	U-plane	M-plane
Confidentiality	TLS	TLS	TLS (SSH optional)	TLS	MACsec (optional)	PDCP, MACsec (optional)	TLS or SSH
Integrity	TLS	TLS	TLS (SSH optional)	TLS	MACsec (optional)	PDCP, MACsec (optional)	TLS or SSH
Authentication [1, 2]	mTLS	mTLS	mTLS (SSH optional)	mTLS	802.1X PNAC	802.1X PNAC	mTLS or SSH/ 802.1X PNAC
Authorization	OAuth	OAuth	NACM	OAuth	802.1X PNAC	802.1X PNAC	NACM/ 802.1X PNAC

NOTE 1: mTLS with PKI X.509 certificates. SSH with Password or Pre-Shared Keys
NOTE 2: CMPv2 is specified for certificate management

Looking ahead to security for evolving threats*

AI data and models

APIs

Quantum Computing

*These are not mobile specific

Key Takeaways

Critical infrastructure increasingly attacked by sophisticated threat actors

5G is the most secure generation of mobile technology to date

Open RAN is as secure as 5G and ready for deployment

Zero Trust Architecture is a strategic plan to protect against evolving threats

ERICSSON

scott.poretsky@ericsson.com
Scott Poretsky | LinkedIn