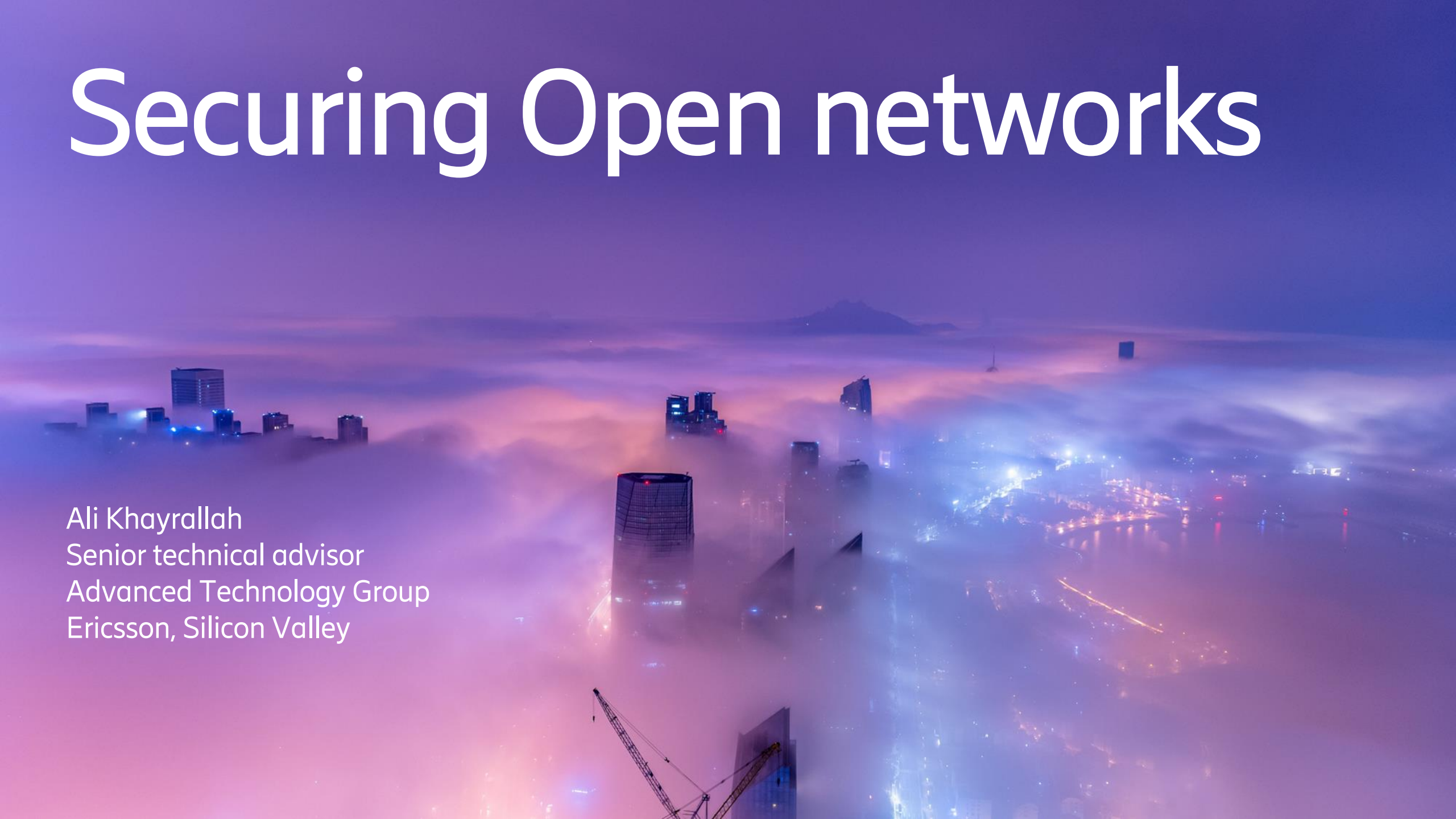
Securing Open networks



Ali Khayrallah
Senior technical advisor
Advanced Technology Group
Ericsson, Silicon Valley

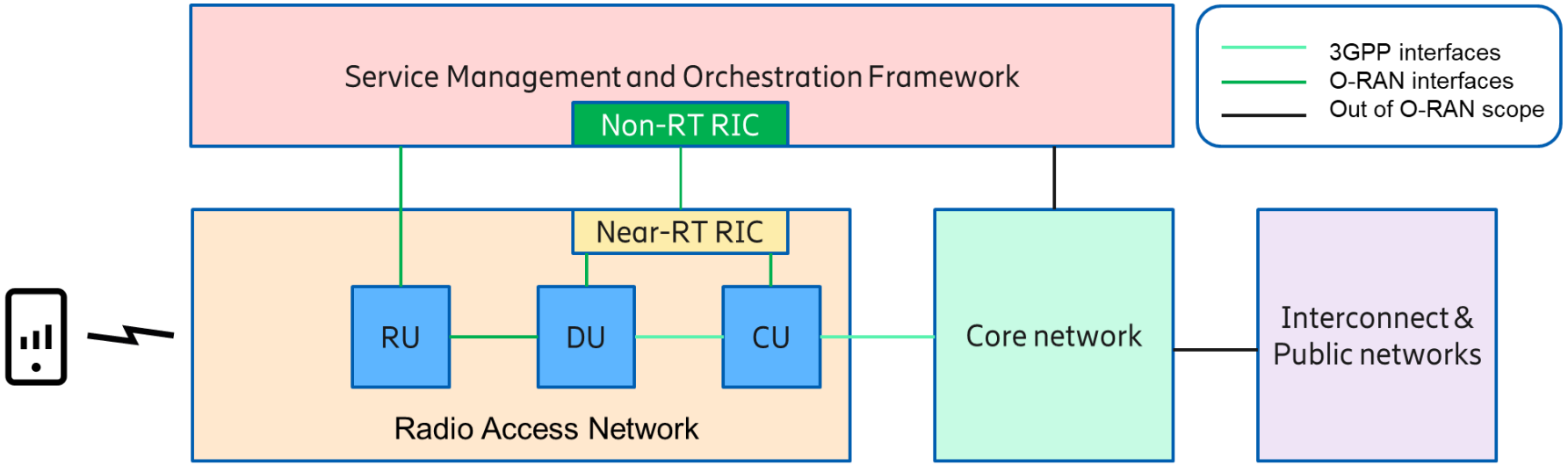
Architecture and interfaces in 5G

3GPP

- Interfaces between Core and Radio Access Network (RAN), Centralized Unit (CU) and Distributed Unit (DU)

O-RAN

- Interfaces between SMO and RAN
- Lower layer split (LLS) between DU and Radio Unit (RU)



Security challenge

Cloud RAN

- Security has to adapt to changes in network technology and architecture
- We cannot claim security by virtue of physical isolation, as in a network box

Interface as attack surface

- Interface enables observability into network state and controllability of network functions
- Critical with third party access to network control, or external data coming into network

Zero trust approach

- Security must be baked into the network
- Explicit verification of every entity
- Can be achieved in incremental phases

NIST

"There is no implicit trust granted to an asset based upon its ownership, physical location, or network location"

Security in O-RAN

Interfaces are always there

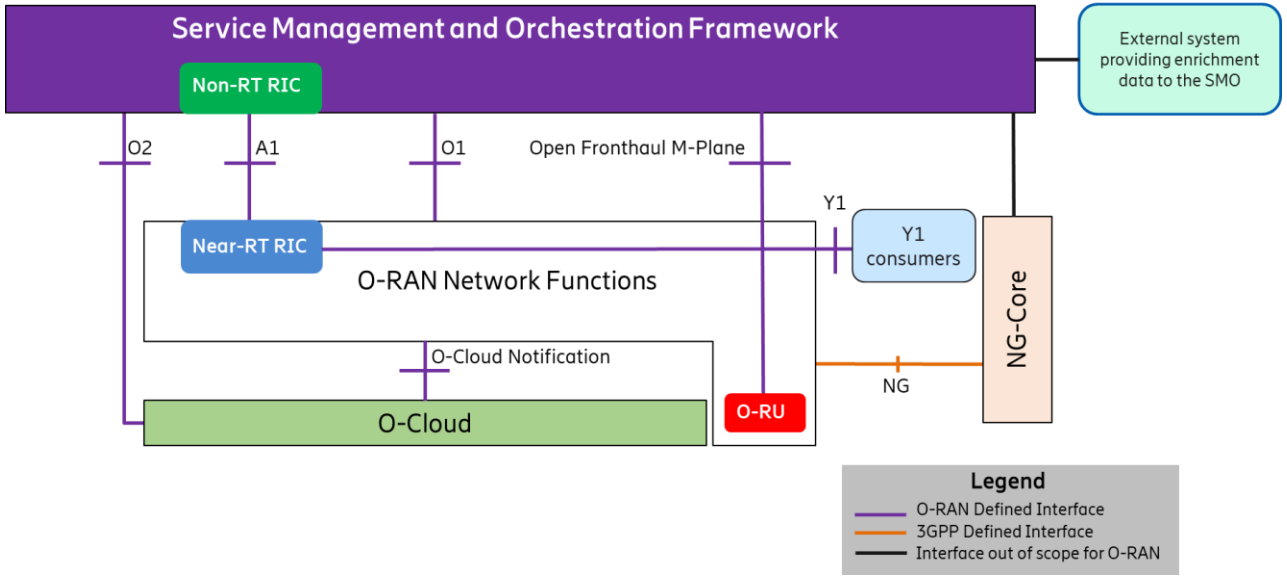
- Whether standardized, proprietary, or implicit

O-RAN Alliance WG11

- Enhance security posture
- Address new risks that come with new features
- Ericsson co-chair (Oct 2023)

Similar challenges likely with network APIs

- CAMARA project from GSMA and LF
- Ericsson supports



Securing open source

Open source more secure?

- Rationale that more transparency and visibility improve chances of catching vulnerabilities
  - Opposite of "security by obscurity"
- In practice need to incentivize contributions on securing code, versus features

O-RAN Software Community (OSC)

- Ericsson Software Technology (EST) contributor

DoD strong proponent of open source

- DARPA AI Cyber Challenge
  - "Secure Nation's Most Critical Software" (August 2023)

OpenSSF under LF

- Improve open source supply chain security
- Ericsson premier member

OpenSSF supports AI Cyber Challenge

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Some conclusions

- Move to cloud-based networks requires revamped security
- Zero trust architecture needs to be baked into networks
- Crucial to enable openness in networks, which are critical infrastructure
- Mechanisms for securing open source needed to achieve its promise of security