THE EU CYBERSECURITY AGENCY

5G TOOLBOX AND OPEN RAN

Marnix Dekker, Head of Sector NIS
Policy unit, ENISA

TIMELINE AND CONTEXT

Toolbox preparation

March 2019
Commission Recommendation

April-July 2019
National risk assessments

October 2019
ENISA Threat landscape
EU Coordinated risk assessment

January 2020
EU Toolbox of mitigating measures

Toolbox implementation

July 2020
Progress report on Toolbox implementation

December 2020
Report on the impacts of the Recommendation of March 2019 and new EU Cybersecurity Strategy

June 2021
Cybersecurity Strategy implementation report

May 2022
Report on the cybersecurity of Open RAN

OPEN RAN - BACKGROUND

- **EU Cybersecurity Strategy** (December 2020): "Monitor existing and expected market trends and assess the risks and opportunities in the field of Open RAN"

- Open RAN = new paradigm for building the RAN:

1. **Open interfaces** = interfaces using open standards
2. **Cloudification, virtualisation, softwarisation**
3. **Automation** (AI, Machine Learning)

- Limited number of Open RAN deployments globally
- Maturity of Open RAN specifications varies

OPEN RAN PAPER – METHOD/INPUT

Open RAN Security analysis by EU MS:

- The impact of Open RAN on security risks
- Assessing new security risks
- Assessing security opportunities

ENISA Review of publicly available information sources on **technical security aspects of Open RAN**

Analysis of the **O-RAN Alliance specification development process**, conducted by ENISA

BEREC survey addressed to MNOs on **Open RAN market aspects**

OPEN RAN PAPER - OUTCOME

- A technical paper with risks and opportunities, drafted together with authorities from all EU Member States

- Continuing the 5G Toolbox approach

- Contents of the paper:
  - Impact of Open RAN on identified security risks (EU Coordinated risk assessment
  - New security risks with Open RAN
  - Security opportunities with Open RAN
  - Guidance for MS on 5G toolbox implementation wrt Open RAN

OPEN RAN RISKS

Key risks amplified or brought by Open RAN:

- More **entry points for malicious actors**, irrespective of the supplier
- **Expanded threat surface** and more complex environment
- Increased **risk of misconfiguration of networks**
- **Insufficiently mature technical specifications** and **deficiencies in the O-RAN Alliance governance**
- New or increased **dependency on cloud service/infrastructure providers**
- Decreased sustainability of the EU 5G supply chain and **potential dependencies on non-EU capacities**

OPEN RAN - OPPORTUNITIES

Security opportunities of Open RAN, *depending on a certain number of factors and associated with counter-risk:*

- Greater **diversification of suppliers** within networks in the same geographic area
- **Visibility** and **transparency** of the network, facilitating auditing and security testing
- **Automation** which could help to decrease threats related to human error *(not specific to Open RAN)*
- **Virtualisation** and **cloud-based solutions** which allow for greater flexibility and make managing network resources easier *(not specific to Open RAN)*

OPEN RAN - RECOMMENDATIONS

With the 5G Toolbox as baseline, reinforce certain areas:

- Authorities to **scrutinise any large-scale Open RAN deployment**;
- **Address issues** in the **O-RAN technical specifications**;
- **Look at dependencies from a broader perspective** and not just the RAN;
- **Strengthen technical controls in networks**.
- Include Open RAN components in future **EU certification scheme** on 5G

Recommending a cautious approach to this new architecture

WHAT IS COMING UP

ENISA TELECOM SECURITY FORUM

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Brussels, Belgium
29 June 2022
09.30 - 17.30 CET

- Integrating NFV controls into the 5G matrix (ongoing)
- Consultation about the 5G matrix (Q3)
    - first NRAs then MNOs
- Deep-dive on security of 5G edge and fog computing
- Deep-dives on SS7 (a checklist), submarine cables, etc.

ENISA Telecom security week – end of June

- Several working groups of MS meeting in Brussels
    - ECASEC (formerly Article 13a), NIS CG 5G work stream, NIS CG WS 10 core internet, NIS CG WS 5 Digital services
- 29 June ENISA Telecom security forum
- 1 July ENISA 5G knowledge building seminar

THANKS

ENISA-NIS-Directive@enisa.europa.eu

Directions, suggestions, ideas, very welcome

☎ +30 6956610736

✉ marnix.dekker@enisa.europa.eu

🌐 enisa.europa.eu