Summary of "Open RAN Security Report"

The recent release of the "Open RAN Security Report" concludes that the use of Open Radio Access Networks (Open RAN) does not fundamentally alter the security risk landscape for telecommunications, compared to more traditional RAN. Most security threats analyzed in the report affect both traditional network deployments and Open RAN deployments, with only four percent found to be unique to Open RAN. Mitigation measures make it feasible to ensure equivalent levels of security between traditional and Open RAN deployments. The report notes that Open RAN also offers potential advantages relevant both to security and to objectives like operational efficiency, interoperability, and innovation.

Key findings include:

- Open RAN is expected to increase the network "attack surface" by a small degree compared to traditional RAN;
- Risks stemming from utilization of cloud-based infrastructure can affect both traditional and Open RAN deployments similarly, along with any technological solutions that leverage cloud services; and
- Concerns related to use of artificial intelligence, machine learning, and open-source software (OSS) are neither unique to Open RAN nor immitigable.

Open RAN presents various security benefits. Open specifications allow operators to test and verify associated security controls, rather than mainly trusting their RAN vendor to adequately protect non-standard interfaces. Security issues can be addressed much more efficiently in virtualized, cloud-enabled environments than with traditional deployments. Open RAN makes it possible to automate many tasks now done manually, improving operational visibility and configuration management. The report also outlines other advantages of Open RAN, such as enhanced vendor competition and likely cost and performance benefits resulting from it; reduction of vendor lock-in and other supply chain risks; and energy efficiency optimization.

As with any newer approach, Open RAN presents additional security dynamics that operators should remain fully aware of in order to manage. The presence of more vendors within telecommunications supply chains is expected to make vendor coordination more complex than with traditional RAN. While parties external to the operator can be made responsible for implementing appropriate security controls, it is ultimately the operator's role to ensure its supply chain is reliable and trusted. Relatedly, Open RAN vendors, systems integrators, and operators alike should analyze and test their technology interdependencies and "harden" any components against potential vulnerabilities. Diversification of suppliers and technology components used in the RAN may also make it more difficult to keep track of all software in use in deployments.

Finally, the report presents and contextualizes numerous mitigation measures, both for operators now deploying Open RAN and those considering it. It explains that, while progress has been made, technical specification of Open RAN security requirements remains ongoing. Supplementary controls should be instituted to ensure comprehensive security during all stages of the Open RAN lifecycle. Open RAN stakeholders should also consider utilizing widely adopted industry standards and best practices, as well as conduct security checks on equipment.