Next Generation Mobile Networks

NGMN Liaison Statement on Security consideration of Low Layer Split in O-RAN

Title: NGMN Security Consideration of Low Layer Split in O-RAN

Source: Next Generation Mobile Networks (NGMN) Security Competence Team and RAN Functional Split & X-Haul Project

To: O-RAN Standards Development Focus Group and Security Task Group

Date: March 16th, 2020

Contacts:
Feifei Lou (feifei.lou@ngmn.org)
Klaus Moschner (klaus.moschner@ngmn.org)
Minpeng Qi (qiminpeng@chinamobile.com)
Charles Hartmann (charles.hartmann@orange.com)
Richard Mackenzie (richard.mackenzie@bt.com)

1. About the NGMN Alliance

The NGMN Alliance is an industry organization of leading world-wide Telecom Operators, Vendors and Research Institutes (see www.ngmn.org) and was founded by international network operators in 2006. Its objective is to ensure that the functionality and performance of next generation mobile network infrastructure, service platforms and devices will meet the requirements of operators and, ultimately, will satisfy end user demand and expectations. The NGMN Alliance will drive and guide the development of all future mobile broadband technology enhancements with a focus on 5G. The targets of these activities are supported by the strong and well-established partnership of worldwide leading operators, vendors, universities, and successful co-operations with other industry organisations.

2. Introduction about NGMN Project on RAN Functional Split and Security Competence Team

The NGMN “RAN Functional Split and X-Haul” project has the objective to understand the RAN decomposition for 5G networks. This covers understanding the various RAN functional splits and the transport requirements to support the various deployment options. As a wide number of industry activities are related to this subject, we also look to encourage industry alignment.

NGMN Security Competence Team (SCT) is responsible for 5G security analysis, 5G security related topics raised by other NGMN projects or teams, and revising and updating deliverables produced by the previous security work stream.

3. Intention of the LS and required actions

The current version of the O-RAN Working Group 4 specifications include security requirements for the management plane (MP) and specifies SSHv2 for authentication, key exchange, encryption and integrity protection.
The latest ORAN specifications mentions “no requirement” for security for the low layer split control and user plane. However, the latest eCPRI specification does mention using MACSEC or IPSEC as a non-mandatory option. It is not well understood if these options can be used in the field, as there are potential impacts on performance (bandwidth, latency, fronthaul transport link length, etc.).

The security of low layer split in O-RAN needs to be globally considered as, for example, some eCPRI message types convey critical information (reset commands, Real Time Control Information, etc).

The considerations on threats depend on the deployment model and use case. For example:

- O-RU and O-DU may be located on the same physical site or located at different premises.
- O-RU and O-DU may be provided by the same vendor or may be provided by different vendors, needing some interoperability of security features.
- Management Plane architectural options (hierarchical or hybrid model).
- Wireless technology may be used to support the fronthaul link
- High bit rate interfaces impose strict performance requirements that limit the use of some security features, due to the increased processing delay.

These different deployment models and use cases may help attackers to achieve their goals. For example, there could be attackers who lack the capability to attack the air interface but can tap the fronthaul link, especially in configurations where the O-RU and O-DU are not located on the same physical site. The threat is not only about sniffing, but about changing or inserting traffic. This could be easier with access to a wire, if the attacker can loop-in an attack device, like a man in the middle (MITM), or inner attacker. That being said, similar impacts can be achieved by attacks at the air interface, by ‘overshadowing’.

SCT delegates propose security requirements and proposals in order to mitigate such threats. Discussions have happened among security experts inside the SCT and between SCT and the RAN Functional Split & X-Haul project. The security enhancements and their impact on latency and complexity are both considered. With such discussion, it is recommended to enhance security in two phases. In phase 1, some incremental security requirements for O-RAN are proposed, which has no major impact on or require any changes to the existing O-RAN specifications. In phase 2, we propose to identify in more detail the threat scenarios, then to study effective security enhancements for further versions of O-RAN.

For phase 1, it is proposed to cover security enhancements on equipment security, network operations, and some security guidelines/configurations for management tools:

1. On the equipment security aspect, it should cover enhancements on physical security, hardening, security assurance, secure interfaces and other related security mechanisms such as secure boot, secure runtime, secure updates and secure configuration, etc.
2. On network operation security enhancements, it should cover how to utilize security for mass upgrades, unified security requirements, secure verification tools and some security guidelines for virtualization.
3. On security guidelines/configurations, it should cover how to utilize SSH based on NIST IR 7966 or BSI TR 02102 best practices, and to secure NETCONF with enhanced configuration and testing. The configuration shall be able to validate inputs, to enhance RBAC policy, to log security issues, to limit extensions, to mitigate security attacks against buffer overflow attacks and API attacks. The tests are recommended to include penetration testing and the need for appropriate management of administrator rights with some flexibility to take into account operational requirements.

Besides the main security proposal above, some other related security enhancement proposals are on PKI, resiliency, anti-DDoS, and more inter-operability testing for security.

In addition, with a view to a possible phase 2, we propose O-RAN to address the remaining security related open points, including the benefits and impacts of MACSEC at RU-DU interface, mitigation features on the user and control plane attacks over the fronthaul link, false base station detection, and synchronization measurement and testing features.

In another aspect of the proposed phase 2, as there are different network deployment models and use cases, it needs to make further analysis in order to check security proposals are fit for specific network deployments. These security proposals may have to be considered with other non-security factors, e.g., latency, complexity and so on in specific use cases, and therefore may become optional rather than mandatory proposals.

Actions: It is kindly requested that O-RAN take the above information into consideration. NGMN RAN Functional Split & X-Haul project would welcome feedback on the liaison statement and is looking forward to further possible/potential collaboration with O-RAN on security aspects that would have an impact on the 5G RAN architecture.

References

None.