ARQIT

Securing 5G & OpenRAN for Public & Private Networks

White paper

Introduction

The Telecom world around us is changing with new technologies like 5G and open deployment architectures such as OpenRAN being rolled out across the world to connect not only mobile subscribers but also billions of IoT devices.

5G is being delivered through a service and solution driven approach connecting critical services with very high availability requirements especially in automotive, smart city, healthcare and public safety. End to end security is key to such applications.

As standards for 5G and OpenRAN mature, security and resilience have been the focus for nations' public and private networks.

This paper highlights some of the known security issues. It also provides an overview of the security solutions developed within Arqit and how these can be integrated at any layer to provide cleaner and simpler protection for service providers.

Arqit's solutions can also provide transport / application layer security for the end users and service providers thereby securing networks around the world against a future quantum adversary.

As standards for **5G and OpenRAN mature**, security and resilience have been the focus for **nations' public and private networks**.

Security Challenges

On one hand 5G networks enable the introduction of new services across various industries, on the other hand it is also acknowledged that the attack surface increases as identified by the National Cyber Security Centre UK.[1]

Legacy 2G, 3G and 4G networks were modelled on hierarchical trust. This is different in the case of 5G where the network in between the uSIM/ eSIM on the subscriber end and the Unified Data Management (UDM) in the core, is untrusted[2], with services running on private and public cloud.

Although 3GPP has introduced security enhancements on standards (3GPP Rel15&16) to address some of these security challenges, compliance to the standards as proven historically will not be sufficient, as vendors are typically more focussed on delivering 5G's features than enhancing its security.

5G initially is being rolled out in Non-Standalone Access (NSA) Mode. This requires interaction between the High-Risk Vendor (HRV) supplying the 2G, 3G and 4G network elements and the non HRVs supplying the 5G elements. This interaction needs to be secured.

OpenRAN is based on an **open architecture** and on disaggregating hardware from software by using commercial off-the-shelf (COTS) hardware and software-defined technologies. **Open interfaces** between the different RAN elements from multiple hardware and software vendors ensure interoperability. However, the multi-vendor ecosystem will challenge service providers on how best to build efficient overall security management due to individual implementation vulnerabilities

OpenRAN also includes new interfaces and RAN functions where the integrity of the network and its data needs to be protected. The introduction of 5G services and technologies using the OpenRAN deployment architecture brings about many challenges for the communication providers, vendors and regulators across the world.[2]

As OpenRAN emerges as the standard of choice for wireless communication globally, security and resilience of these open networks become paramount in order to deliver the next generation of use cases.

In September 2020, Ericsson[3] raised the first alarm bells on the security vulnerabilities within the OpenRAN standard that was being developed by the O-RAN Alliance. Ericsson's security experts pointed out that new open interfaces like O1, O2, A1, and E2 defined by the O-RAN Alliance did not mandate the use of Transport Layer Security (TLS).

Subsequently the OpenRAN specifications were changed for the compulsory use of TLS. TLS itself is not future proof as it currently relies on non-quantum safe set of deployed algorithms including DH, RSA, DSA, ECDH and ECDSA.

Studies[4] have found that the OpenRAN specification does not specify security configurations between various RAN elements (for example between the Radio Unit and the Distributed Unit). This allows an adversary to mount Denial of Service (DoS) attacks from a compromised element.

In an OpenRAN ecosystem, 3rd party vendors provide services (example cV2x, UAVs) on Virtualised Network Function (VNF) on open platforms. This opens the door for malicious users.

In order to mitigate this risk, a centralised key management service is required to secure keys and secrets used by the VNFs along with a root of trust to enforce policies. Secure boot for all physical elements needs to be enabled by validating encryption keys and lifecycle.

The early O-RAN Alliance specifications lacked details for defining network security considerations[6] A security focus group involving the industry was established to address specifications to mitigate current & future threats including quantum attacks.

[1] *Summary of NCSC's security analysis for the UK telecoms... - NCSC.GOV.UK*

[2] *Telecoms security: proposal for new regulations and code of practice - GOV.UK (www.gov.uk)*

[3] *Avoiding risks in 5G - Ericsson*

[4] *Security in 5G RAN and core deployment Whitepaper - Ericsson*

Arqit's solution

Arqit's QuantumCloud™[6] is independent of the layer at which it operates making it cleaner and simpler for Service Providers to implement core security. At the same time, it can provide transport / application layer security for the end users and service providers.

It is an alternative for network security that addresses the shortcomings of PKI and delivers a host of new benefits to customers today, as well as protection against quantum attack. Our cloud-based symmetric key platform is easy to scale and allows customers to concentrate on security outcomes.

QuantumCloudTM provides an efficient way of agreeing symmetric keys with a trustless broker-based architecture, where the brokers are used instead of a hard mathematical problem to allow the 2 parties to agree a key.

QuantumCloudTM and Arqit's patented Autonomous Trustless Keyfill (ATK) processes solve the problem of end-to-end encryption, meaning that Quantum Safe symmetric encryption can be used to protect every part of the network without any change to the existing standards.

For OpenRAN, QuantumCloudTM agrees symmetric keys with the RU, DU and CU along with any firewalls/ gateways in the network. The entire management of the keys is taken care of by QuantumCloudTM , thereby freeing up the Service Provider and the vendors from the burden of key management.

In a 5G network, the SBA can benefit from the symmetric key agreement process by QuantumCloudTM in a virtualised cloud-based environment. Also, encryption between SEPPs of different Service Providers can be established using QuantumCloudTM thereby securing roaming between networks across the world.

Connected devices in the world including handsets, IoT sensors and CPEs can all benefit from QuantumCloudTM and the key bootstrap process using the ATK with equal simplicity, efficiency and security.

For more information on QuantumCloud™ read **QuantumCloud_Symmetric_Encryption_Reborn_for_the_Cloud_White_Paper**

Conclusion

As 5G networks using an open ecosystem for RAN and Core are rolled out across the world with services moved into the cloud and enterprises handling billions of IoT devices, it is time to redefine the way we implement security in Telecom networks.

The rigid PKI system with asymmetric keys needs to be replaced by a dynamic light touch QuantumCloudTM symmetric key agreement process.

Get in touch today to find out more.

contactus@arqit.uk

[5] *Germany reckons open RAN is risky business | Light Reading*

[6] *QuantumCloud_Symmetric_Encryption_Reborn_for_the_Cloud_White_Paper_April_2021_v3__.pdf (cloudinary.com)*