ARQIT

Case study

Telecommunications

Enabling quantum-safe private networks

Overview

In October 2022, Arqit was selected to provide security by default for the Secure 5G project funded by the Department for Science, Innovation and Technology (DCMS) (now DSIT).

The Secure 5G project is building a flexible platform that will enable companies to roll out and maintain their own quantum-safe private networks, with targeted applications for Industry 4.0, mobile edge computing (MEC), the Internet of Things (IoT) and highly secure environments, such as defence.

Project partners include Compound Semiconductor Applications (CSA) Catapult, Lime Microsystems Ltd and Slipstream Engineering Design Ltd.

> **Harnessing the UK's innovation and technological expertise will deliver the world-leading digital infrastructure that is so fundamental to growing our economy.**
>
> **The Secure 5G project will pave the way for more secure and competitive telecoms networks in the UK, benefiting industries across the board.**
>
> **This cutting-edge technology will accelerate that process while cutting business costs, boosting communications security, and supporting UK supply chains.**
>
> – Sir John Whittingdale,
> Minister for Data and Digital Infrastructure

The Challenge

The UK's committed to see 35% of UK cellular traffic carried over open RAN by 2030. As Open RAN mobile networks become more prevalent, larger and more complex there is a need for solutions that are inherently more secure, while offering a level of flexibility which enables them to adapt to emerging threats with far greater agility.

Current software defined radio platforms for O-RAN are typically bespoke solutions able to cover only a narrowband of operation. With the opening of the spectrum towards 10GHz, there is a need to develop systems that are flexible in their frequency range but can output the power required by communications platforms in dense environments.

There are many security issues with existing O-RAN cybersecurity standards and the complexity of O-RAN with a wide range of incumben vendors will only introduce more. For example

1. The use of certificates across the entire network is difficult to manage, and certificate compromise can result in unauthorised access to the network without any mechanism of prevention. Certificate Authorities (CAs) must also be trusted and increase the attack surface.
2. Static pre-shared encryption keys (PSKs) on endpoints are often rarely or never refreshed, resulting in poor forward secrecy and potential limitless unauthorised access to the network if a key is compromised. These keys must also be physically distributed which is logistically challenging and increases the probability of compromise.
3. The implementation of public key infrastructure (PKI) across the entire network means data in transit is vulnerable to the harvest now, decrypt later attack. This is because PKI is inherently vulnerable to attack by quantum computers.

Our Solution

The Secure 5G project brings together a radio frequency (RF) power amplifier (Slipstream Engineering Design) with open-source network-in-a-box solution (Lime Microsystems), underpinned by Arqit SKA-Platform™, a quantum-safe symmetric key agreement platform (Arqit) and state-of-the-art test and evaluation support (CSA Catapult).

Arqit's lightweight software agent is embedded directly into the Lime Microsystems base station, allowing the device to securely register with SKA-Platform™. Strong authentication is then achieved by a symmetric link between the device and SKA-Platform, with a symmetric authentication key rotating on a frequent basis to ensure that only trusted devices may connect to the network. Previous authentication issues due to certificates and static PSKs are removed, strengthening the network against bad actors who aim to gain unauthorised access.

The IPsec-based backhaul connection from the Lime Microsystems device is then strengthened using Arqit SKA-Platform as it allows symmetric encryption keys to be generated directly on the endpoints. The final keys are zero trust as they are not known by any other third party, including SKA-Platform itself, and are rotated at an extremely high rate that can be defined by the customer to provide enhanced forward secrecy with zero downtime. The backhaul is therefore completely quantum safe, eliminating the threat of the harvest now, decrypt later attack, and vulnerable PKI is removed from the network.

Benefits

Allows industries to deploy their own private, flexible, and secure 5G networks across their business areas.

Brings many suppliers into the Open RAN ecosystem, diversifying and democratising 5G deployment using cost effective, programmable radio modules.

Empowers network owners with the flexibility to maintain and upgrade services by running their applications at the very edge of the network, from secure on-premises file sharing to low latency machine learning.

Flexibility and reconstruction of the system, coupled with processing power that is powerful enough to run resource intensive apps, will allow for further developments in hardware and services by the wider UK telecoms supply chain.

IET The Institution of Engineering and Technology

Excellence and Innovation Awards Winner 2023

Named as one of 2023's **top innovators** by the Institution of Engineering and Technology (IET), winning the institution's Excellence and Innovation Award for Communication and IT alongside project partners.