Case study

Telecommunications

Delivering quantum-safe security for Private 5G networks

The Security Enhanced Virtualised Networking for 5G (SEViN-5G) project, funded by Innovate UK, the UK Government's innovation agency, leveraged Ampliphae's network security analytics technology and Arqit SKA-Platform™ Symmetric Key Agreement (SKA) platform to deliver a quantum-secure Private 5G testbed that can protect against both current and future cyber threats. Athonet, a Hewlett Packard Enterprise acquisition, provided the Radio Access Network (RAN) equipment for the project with a cloud core hosted on AWS.

The Challenge

Private enterprise networks based on 5G cellular technology are accelerating digital transformation across industries including manufacturing, healthcare, defence and smart cities. Private 5G gives enterprises access to high-speed, massively scalable, and ultra-reliable wireless connectivity, allowing them to implement innovative IoT and mobile solutions that enhance productivity, drive automation and improve customer engagement.

The security of these networks will be paramount as they will support safety-critical infrastructure and carry highly sensitive data. 5G comes with potential new threats and security risks including the threat from quantum computing and is especially vulnerable because most 5G solutions rely on public key infrastructure (PKI) to encrypt data-in-transit across the network, but cryptographic algorithms such as RSA 2048 and ECC 256 will soon be unfit for purpose as quantum computers will be powerful enough to break the mathematical functions that are used to form the encryption keys. Bad actors are harvesting critical data now, including that transmitted across 5G infrastructure, for decrypting at a later date.

In addition to the threat of "harvest now, decrypt later", 5G networks also rely on certificates and static preshared keys for authentication. If these components are compromised, an attacker has the potential to gain uninhibited access to the network without detection. Distributing new certificates and static pre-shared keys is a risk and is also logistically challenging, resulting in many networks containing secrets that are unchanged for long periods of time (and they are never refreshed in the worst-case scenario). This increases the attack surface further and provides poor forward secrecy.

Our Solution

Arqit SKA-Platform™ is Arqit's unique Symmetric Key Agreement platform that enables quantum-safe encryption which makes the communications links or data at rest of any networked device or cloud machine secure against current and future forms of attack – even from a quantum computer. SKA-Platform, enables any device to download a lightweight software agent, which can create encryption keys in partnership with any number of other devices.

In the context of SEViN-5G, Arqit's lightweight software agent was integrated with Athonet's RAN equipment and AWS cloud core to enable secure registration with Arqit's SKA-Platform. The RAN and core connect to each other via an IPsec VPN tunnel, but rather than a typical PKIbased approach, symmetric keys are generated directly on the endpoints to establish the tunnel and encrypt the data. All data passing between the RAN and core is now verifiably secure even against quantum attack, future-proofing the 5G network. No third-party aside from the RAN and core know the final keys, including Arqit SKA-Platform, and the keys refresh regularly to massively improve forward secrecy. This rotation rate is customisable to the needs of the end customer.

Additionally, encryption inventory analysis is provided by Ampliphae, a leader in network cyber security solutions, providing software products and consultancy services to the networking industry. SaaSGuard, Ampliphae's innovative network analytics platform, is deployed as a physical probe alongside the RAN, enabling deep encryption analysis of the network traffic flowing between the RAN and the core network. For SEViN-5G, the traffic can be observed to be provably quantum secure, and each key rotation tracked. A cloud-based SaaSGuard probe was also deployed directly within the cloud core, allowing further analysis within the core network itself. Alerts are set up to identify weak encryption, allowing action against threats and weaknesses to be taken in real time.

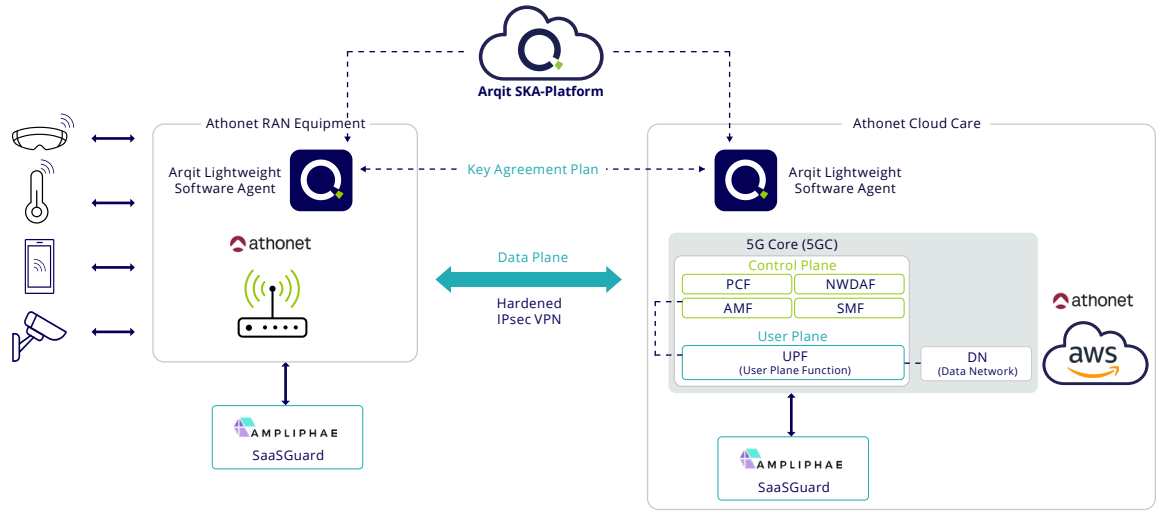

Figure 1: High-level architecture of a quantum-safe 5G private network with Arqit, Ampliphae and Athonet.

Benefits

Strong authentication – The 5G network components are securely registered with Arqit-SKA platform with unique rotating authentication keys. Third parties and bad actors cannot gain unauthorised access to the network, removing the threats due to static pre-shared keys and PKI. In addition, we also reduce the threat of base station spoofing and man-in-the-middle (MITM) attacks.

Forward secrecy – Symmetric keys rotate at an extremely high rate, enhancing forward secrecy and reducing the threat surface significantly compared to static keys and certificates.

Quantum-safe encryption – The PKI is removed from the connection between the RAN and the core network, with all traffic now protected by symmetric keys that are provably secure against threats including quantum computers. The IPsec VPN uses RFC 8784 as a standard to ingest symmetric keys,e nsuring compliance with the NSA Commercial Solutions for Classified (CSfC) Symmetric Key Management Requirements Annex.

Plug-and-play architecture – The network can be stood up at a fast pace, removing the logistical issues of certificate and key distribution. Arqit's endpoint software is embedded into the RAN and core for rapid deployment, and Ampliphae offer physical and cloud-based versions of SaaSGuard to allow flexibility across the network.

Awarded the 2024 GLOMO awards for:

Best Mobile Security Solution

The award recognizes the best use of technology to safeguard customers' personal data and help network operators and service providers' combat fraudulent access to networks.

CTO Choice: Outstanding Mobile Technology Award

The award is selected from GLOMO's panel of distinguished industry experts (comprised of more than 20 CTOs, from every continent) for the overall technology winner from the nine best 'Mobile Tech' in 2024 award winners.