quantropi

CASE STUDY

How a Top-Tier Global Telco OEM is Securing its 5G Network from the Quantum Threat

VERTICAL
- Telecommunications
- 5G Networks

CHALLENGE
- Low entropy in wireless backhaul nodes exposes a potential vulnerability to future attack and exploitation

SOLUTION
- QiSpace™ Platform

BENEFITS
- Quantum entropy supplied to wireless backhaul enables full security of AES to be utilized
- Software solution offers significant cost savings compared to hardware alternatives

Overview

'Steal now and crack later' is real. Bad actors are harvesting encrypted data today, just waiting for the quantum computing power to decrypt its secrets. A top-tier multinational tele-communications OEM — keenly aware of the threat posed by quantum computers — collaborated with Quantropi, the world's only provider of "TrUE" quantum-secure data communications solutions, to enhance the security of its 5G wireless backhaul infrastructure via secure distribution of Quantum Entropy.

Challenge

5G wireless backhaul nodes (network connection points) are low entropy data sources, meaning they are unable to produce truly unpredictable random numbers. Because these nonces (arbitrary numbers usable just once in a cryptographic communication) are relied on for cryptographic algorithms like AES (Advanced Encryption Standard, the symmetric encryption standard for securing data communications), low quality nonce generation reduces overall backhaul security.

For the OEM, such vulnerabilities imply unacceptable risk, today and even more so in future. And while hardware solutions exist to upgrade backhaul nodes using entropy generators, they are costly, time consuming and difficult to maintain. The OEM was seeking an inexpensive, easy-to-implement software alternative capable of provisioning strong ultra-random numbers for nonce generation. →

Why are random numbers important?

An AES key is a random number used to determine how the algorithm will encrypt data. But if the same AES key is used to encrypt identical data, the encrypted form of the data will also be identical. This lowers security and creates vulnerabilities to exploitation, such as replay attacks. To protect against this, an additional type of random numbers, called nonces, are used in the encryption process. A random nonce is generated each time a secure communication link is established, enabling the same AES key to be used for multiple sessions without creating vulnerabilities to replay attacks.

V11/2021.08.17

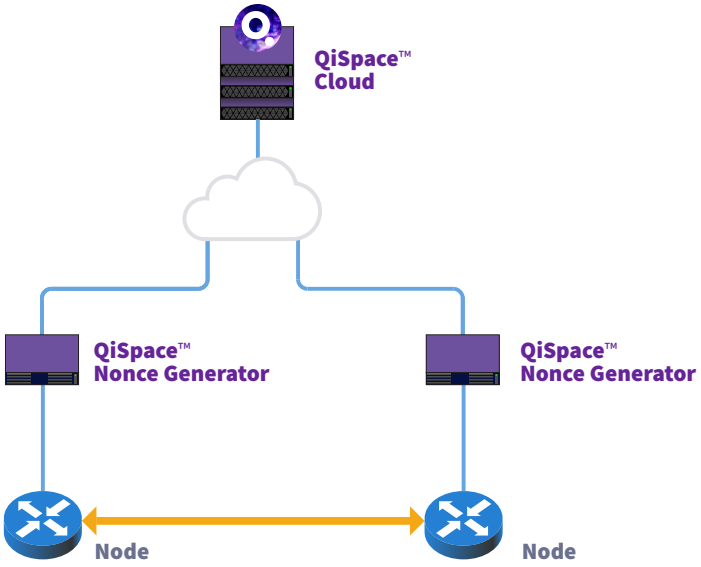
www.quantropi.com

quantropi

Proof of Concept

We leveraged our QiSpace™ software platform — specifically, our SEQUR™ Quantum Entropy as a Service — within the OEM's 5G backhaul infrastructure, in order to securely distribute Quantum Entropy (true random numbers generated in QiSpace™ Cloud) to all backhaul nodes over existing connections. This enabled the generation of high quality nonces — immediately enhancing overall backhaul security.

The upgrade was executed seamlessly, with zero requirement to change telco hardware or network policies, showcasing how a telco can rapidly and cost-effectively overcome the security weaknesses stemming from low-entropy 5G backhaul nodes.



Conclusion

By choosing Quantropi's TrUE quantum-secure QiSpace™ enterprise software platform over hardware alternatives to securely distribute Quantum Entropy to its 5G backhaul nodes, the OEM saved time and considerable capital investment, while benefitting from an enhanced security profile. That's because Quantropi is the only company in the world capable of quantum-secure entropy and key distribution via the existing Internet — including *wireless* networks — over unlimited distances, at network speeds. Moreover, our cloud-based cryptographic platform requires minimal investment in new technology infrastructure.

"We were very impressed with this collaboration. Quantropi exceeded our expectations, not only by presenting an elegant solution, but also through its professionalism and efficiency — rare qualities in a start-up. The project was a pleasure from start to finish."

— M.S., Senior Manager,
Technology Strategy & Partnerships

What's next?

With Quantropi and QiSpace™, customers like our telco OEM, who begin by first securely distributing SEQUR™ Quantum Entropy, can progress to adding a quantum-secure layer to AES encryption — and thereby ensure quantum *resilience* — before proceeding on a seamless evolutionary upgrade path towards 100% quantum *security*, forever.

Bring it on.