Post Quantum Cryptography for Real-Time Communication

The Quantum Threat

Encryption is widely used on IP networks to protect the confidentiality and integrity of everything from banking and on-line payments to real-time communication applications including audio and video phone services, static and mobile surveillance, augmented reality applications and IoT. All of these services rely on an encryption mechanism known as public/private key or asymmetric encryption to establish and authenticate a connection and generate a shared or symmetric key for protecting sensitive data.

Correctly implemented, the protocols used for asymmetric encryption are secure against an attack using even the most powerful conventional computer. It is estimated that a brute force attack against a 2048-bit RSA key would take 300 trillion years.

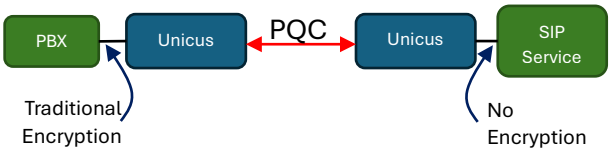
Quantum computers will change all this. An algorithm has been designed which can reduce the time to crack an RSA key to a few seconds. All that is needed is a suitable quantum computer. Recent advances mean that suitable computers could exist in a few years. This poses a threat to any sensitive information that requires future protection. An adversary can record communications today and decrypt it when a suitable quantum computer becomes available. This is an obvious problem in government and defence, but also applies to other sectors.

Fortunately, new post quantum algorithms have been designed to replace the existing vulnerable algorithms. These have now been standardised by the USA's NIST as FIPS 203, 204 and 205. These new algorithms are compatible with the protocols used to deliver real-time communication on IP networks providing effective Post Quantum Cryptography (PQC) to protect sensitive data.

Unicus®

Unicus, a real-time cybersecurity platform from UM Labs has implemented these new algorithms and is now the only solution to provide quantum safe encryption for real-time communication. Unicus protects SIP based services including voice and video calls, streaming video, augmented reality and IoT.

Unicus supports PQC and traditional cryptography enabling connections to systems supporting only traditional encryption or without encryption support.



As an example, two Unicus systems will provide encrypted SIP trunks and interconnections using Post Quantum Cryptography between IP-PBXs and SIP User Agents supporting traditional encryption, such as Cisco Call Manager, and services offering only unencrypted connections.

Web: https://www.um-labs.com
Email: info@um-labs.com