QuLore: An Adaptive Security Framework to Extend Quantum-Safe Communications

Eduardo Jacob, University of the Basque Country (EHU), eduardo.jacob@ehu.eus

Abstract

The setup will demonstrate the feasibility of deploying secure connectivity solutions and networks that implement a security-in-depth approach by providing the best connectivity solution taking into account the underlying key distribution solution which is available between network locations: Quantum Key Distribution (QKD) or Post Quantum Cryptography (PQC).

This is possible by using the QuLore[1] framework developed by EHU and two R&E developed KMS: edukms developed by SURF [2], [3] and vMKS[4] by EHU. We will demonstrate Quantum Safe communications at three different layers: at the network layer between two enterprise networks using IPsec, at the optical layer over DWDM systems and at the application layer finally between end user applications.

The demonstration will involve several links:

- Two pairs of DWDM systems deployed between CIENA and PCCS booths at the SuperComputing Exhibition Floor and between two locations in the University of the Basque Country Bizkaia campus: The Faculty of Engineering of Bilbao and the Advanced Aeronautical Manufacturing Center (CFAA) in Zamudio. These links will co-propagate quantum and data channels over a shared fiber.
- Two IPsec-secured links with PQC cryptographic protocols between PCSS booth and SURF location in Amsterdam and between this same place and CFAA in Zamudio.
- IP links between different end-user applications. in this case, an Open-Source videoconferencing application has been modified to make use of quantum-safe keys for encrypting the audio and video traffic. These keys can be both direct QKD or relayed QKD using PQC keys for the relay, depending on the endopints.

The demonstration brings together Ciena's Waveserver quantum-safe encryption and LuxQuanta's QKD technology featuring a WaveLogic 6 Extreme (WL6e) 1.6Tb/s encrypted channel in Chicago and a WaveLogic 5 Extreme (WL5e) 800Gb/s encrypted channel in in Bilbao. Both locations showcase a hybrid quantum-safe security architecture, combining NIST-certified PQC algorithms implemented in the Waveserver optical encryption solution, with QKD-generated keys from LuxQuanta NOVA LQ systems, to demonstrate how complementary quantum-safe technologies can be integrated with proven high-capacity optical encryption to ensure the confidentiality of critical in-flight data. Two QRNG will provide true random numbers for PQC Key Establishment Mechanism (KEM) secure implementation.

Goals

The demonstration goals are:

- The seamless integration of PQC and QKD protected links under the management of a lightweight framework, namely, the EHU developed QuLore.
- The simple and transparent integration of two standard-aware KMS systems developed by SURF and EHU made possible by the QuLore Framework, guaranteeing interoperability of the systems.
- The use of the resources of the Smart Quantum Technologies for Everything research infrastructure, (https://i2t.ehu.eus/resources/smartquant4E) which is part of EHU Quantum Center (https://www.ehuqc.eus/)

[1] "QuLore: An Adaptive Security Framework to Extend Quantum-Safe Communications to Real-World Networks", ArXiv, by Ane Sanz, Eire Salegi, Asier Atutxa, David Franco, Jasone Astorga & Eduardo Jacob. https://doi.org/10.48550/arXiv.2511.22416

[2] https://gitlab.com/surfquantum/eduqkd/edukms

[3] https://events.geant.org/event/1949/contributions/2271/attachments/1279/1941/eduQKD.pdf

[4] "Toward Quantum-Safe Scalable Networks: An Open, Standards-Aware Key Management Framework" by Ane Sanz; Asier Atutxa; David Franco; Jasone Astorga; Eduardo Jacob; and Diego López https://ieeexplore.ieee.org/document/11299406

- The seamless connectivity between equipment, sites, domains, or end-nodes connected by either QKD or PQC links.
- Show that the use of commercial ready-to-go DWDM, QKD and QRNG equipment which adheres to standards eases the integration in standard-aware networks.

Impacts

EHU, SURF and the Network Development Work Package (WP6) of the GÉANT GN5-2 project are deeply involved in QKD deployment and applications. EHU is involved in the deployment of hybrid key distribution solutions that solve the challenges of Key Management System (KMS) identification, relay path discovery, and scalability of QKD networks to deploy Quantum-Safe networks and services, while SURF has developed eduQKD dedicated to providing a fully open-source software stack for Quantum Key Distribution (QKD).

Our objective is to improve network security-in-depth as well as to validate theoretical approaches in an R&E environment and NREN use cases. We have secured support and expressed interest from regional (Basque Government), national (with RedIRIS acting as technical stakeholder and observer), and European stakeholders, through the GÉANT project and representative of European NRENs, which supports both the experiment and its potential application to its community.

In the days of scattered quantum deployment, this lightweight solution can seamlessly integrate QKD islands in a quantum safe connectivity solution, showcasing future state where interconnectivity would need to be provided for future non-QKD islands or end-nodes in the quantum-safe world.

SCinet, and the specialized networking solutions it employs, gives the opportunity to demonstrate the QuLore framework and R&E-developed KMS systems interoperability both in a large-scale high-tech network and in a highly specialized conference which includes potential users that will analyze, criticize and propose new functionalities, for QuLore evolution and deployment. In this context, the expected feedback is far broader and more practical than that obtained through paper reviews or conference presentations and will help prioritize among these planned targets

While our research targets are somewhat fixed (improving QuSeC controller, supporting new devices, integrating in the framework point-to-multipoint optical switching-based solutions…), as mentioned above, we expect to receive significant feedback.

Resources

Regarding connectivity, we will only need the routed connections available in the CIENA and PCCS booths and a dark fiber link between both locations. The remaining resources, as described will be made available by the partners:

CIENA Booth

- Ciena Waveserver 6 with WL6e 1.6Tbs encryption sleds.
- Ciena MUX/DEMUX CMD24
- Ciena 5166 router
- Luxquanta LQ QKD system
- EHU QuLore server

PCSS Booth

- Ciena Waveserver 6 with WL6e 1.6Tbs encryption sleds.
- Ciena MUX/DEMUX CMD24
- Ciena 5166 router
- Luxquanta LQ QKD system
- EHU QuLore/IPsec Server with QRNG

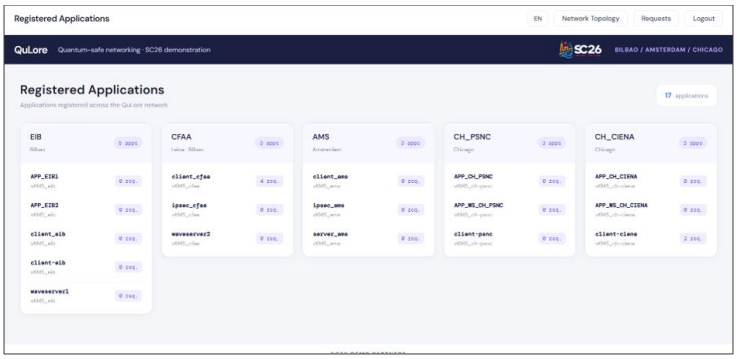
In EHU nodes of Bilbao and Zamudio:

- Ciena/EHU Waveserver 5 with WL5E 800Gbs encryption sleds.
- Ciena/EHU MUX/DEMUX CMD42
- Luxquanta/EHU LQ QKD system
- Routers
- EHU QuLore/IPsec Server with QRNG

In SURF (Amsterdam)

- SURF VM with IPsec/QuLore/eduKMS

QuLore is deployed with microservices over a Kubernetes cluster. See interface below:



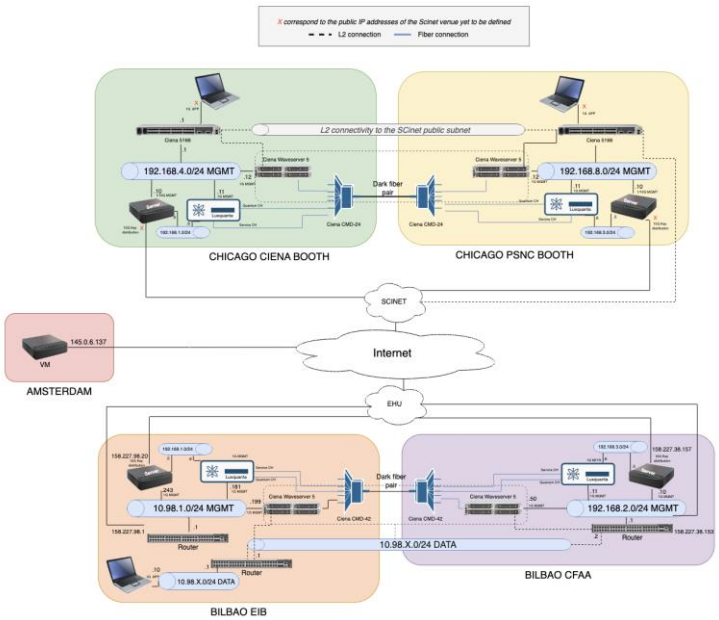
There is a management interface that is very useful to show in real time the key exchanges happening.



The general view of the experiment is shown here:



A network topology schema is shown in next figure:



Involved Parties

- Eduardo Jacob, EHU/EHU Quantum Center, eduardo.jacob@ehu.eus
- Ane Sanz, EHU/EHUQC, ane.sanz@ehu.eus
- Eire Salegi, EHU/EHUQC, eire.salegi@ehu.eus
- Jorge Sasiain, EHU/EHUQC, jorge.sasiain@ehu.eus
- Asier Atutxa, EHU/EHUQC, asier.atutxa@ehu.eus
- Jasone Astorga, EHU/EHUQC, jasone.astorga@ehu.eus
- Esther Robles, RedIRIS, esther.robles@rediris.es
- Vanesa Diaz, LuxQuanta, vanesa.diaz@luxquanta.com
- Bartomeu Heer, LuxQuanta, bartomeu.heer@luxquanta.com
- Scott Kohlert, CIENA, skohlert@ciena.com
- José Eduardo Goncalves, CIENA, jgoncalv@ciena.com
- Nacho Carcas, CIENA, ncarcas@ciena.com
- Ivana Golub, PCSS/GÉANT, igolub@man.poznan.pl
- Piotr Rydlichowski, PCSS, prydlich@man.poznan.pl
- Migiel de Vos, SURF, migiel.devos@surf.nl
- Wojciech Kozlowski, SURF, wojciech.kozlowski@surf.nl
- Susanne Naegele-Jackson, FAU/DFN, susanne.naegele-jackson@fau.de