Higly Secure Critical Infrastructures via QKD: the Madrid's QKD testbed

A. Aguado[1], V. Lopez[2], H. Brunner[3], C.-H. F. Fung[3], A. Pastor[2], S. Bettelli[3], D. Hillerkuss[3], L. Comandar[3], S. Mikroulis[3], D. Wang[3], D. Lopez[2], A. Poppe[3], M. Peev[3], V. Martin[1]

[1]Center for Computational Simulation - Universidad Politécnica de Madrid. Campus de Montegancedo. Boadilla del Monte, 28660 Madrid. Spain

[2]Telefónica Investigación y Desarrollo, Ronda de la Comunicación s/n 28050 Madrid. Spain

[3]Huawei Technologies Duesseldorf GmbH, Riesstrasse 25, 80992 Munchen. Germany

(a.aguadom@fi.upm.es, vicente@fi.upm.es)

ABSTRACT.— This work describes techniques to implement and additional QKD security layer in current and novel network architectures. Our work shows how QKD can be integrated in standard security protocols and network architectures for securing control and data channels, providing a whole quantum-safe network environment. This demonstration was carried out over the Madrid's SDN-QKD tested, comprising 3 remote nodes connected through standard optical devices in an operational environment and with the physical links among sites being shared between classical and quantum signals.

Securing Control and Data Planes via QKD.— The so-called software-networks (i.e. SDN and NFV) come together with associated vulnerabilities, since now there are management entities that need to remotely communicate. To solve this problem, we have integrated QKD in existing security protocols and schemes to facilitate its adoption by operators.

The first integration comes from the control plane. In (1) we proposed and demonstrated the integration of QKD-keys with DHE keys by XORing them. This technique, if properly implemented, allows to bring the best capabilities from each key exchange solution, as both have been demonstrated to be composable. From a legal perspective, this allows QKD to be installed even although the certification of these kind of devices is still a work in progress. The QKD device inherits the certification from DHE, while DHE also inherits the physical layer security brought by QKD. This solution, integrated in SSH, is used to secure the control plane among the three PoPs (virtual network and service creation).

The second use case comes from the data plane. In (2) and (3) we show how the service can be automated using NFV and SDN principles respectively. Here, the management and orchestration (MANO) instance coordinated the synchronization of both VNF control and abstraction (VCA) instances to use the same key stream IDs. When required, the MANO instance configures one of the ends with no IDs. When this is finished, the orchestrator receives the valid IDs which are then forwarded to the other end, successfully configuring the VPN service. The obtained keys are used for bidirectional authentication and encryption, using IPsec as the transport protocol.

The prototypes are integrated in the Madrid's QKD network. The network consists of three locations: Almagro (Telefonica's R&D laboratory shared with Telefonica of Spain PoP), Norte and Concepcion (both two are large Telefonica of Spain PoP), all part of Telefonicaś production network. Almagro hosts a Continuous Variables QKD transmitter, while Norte and Concepcion host the two receivers, all made by Huawei. They expose part of its chracteristics to the network so they can be controlled by the SDN controller. The QKD network, via SDN, is optimized in such a way that the transmitter can generate keys with the two receivers having minimum performance penalties. The link between Norte and Concepcion uses multi-hop-generated QKD keys, while the other two links have direct QKD links.

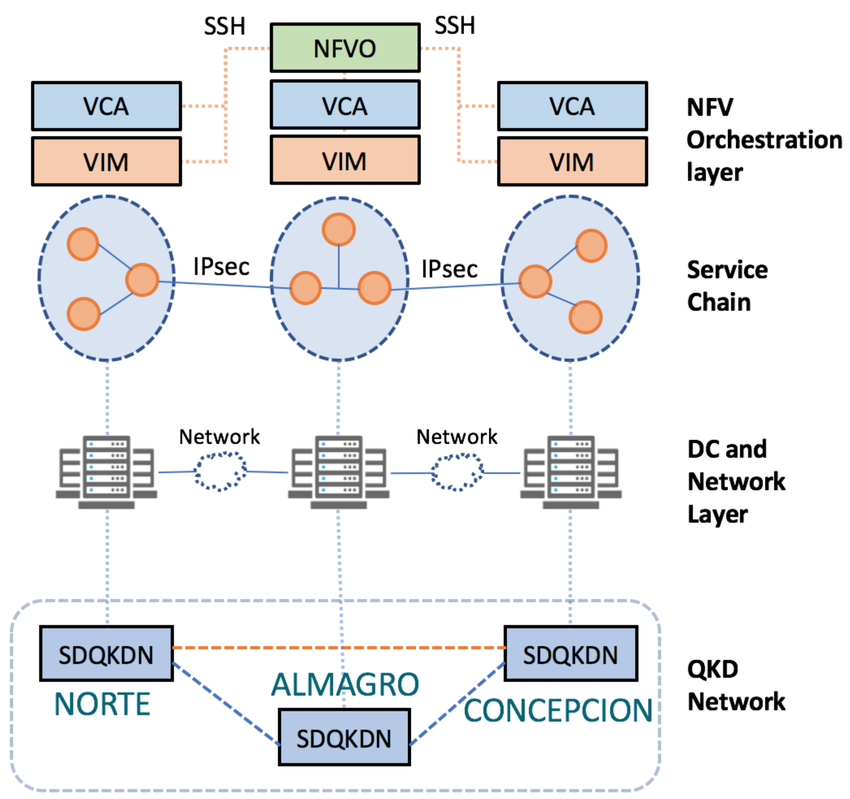

Fig. 1. Logical view fo the network architecture comprising the QKD, network, virtualization and management layer.

Experimental Scenario and Results.— The experimental testbed is physically distributed as shown in Fig.1. To showcase the use cases, we have implemented the stack and the required extensions using different software and hardware platforms. The virtual infrastructure manager (VIM) is a container platform-based on Docker allocated in the three PoPs. It allows to create virtual networks using containers and OpenVSwitches (OVS). The VCA is composed of a set of scripts and processes which are remotely controlled by the orchestrator. Finally, the orchestrator is implemented to receive requests, distribute them across the connected VIMs, gather topological information and forward configuration commands to the remote VIMs and VCAs. The orchestrator is located in Almagro's PoP.

The physical testbed comprises three servers, three OSN 1800 and the three QKD devices distributed as described above. The servers are used for multiple purposes: they integrate the post-processing and internal management of the QKD systems, it contains the key stores and the SDN software for managing the QKD network, they contain the virtualization platforms and the crypto plugins for securing the channels using QKD-derived keys.

Results show how the QKD-keys are integrated in two different layers: in the network's control plane, by using a hybrid solution combining the QKD and DHE keys and; in the network's data plane, by providing QKD-keys to virtual network functions (routers) to create quantum-safe VPNs based on IPsec protocol.

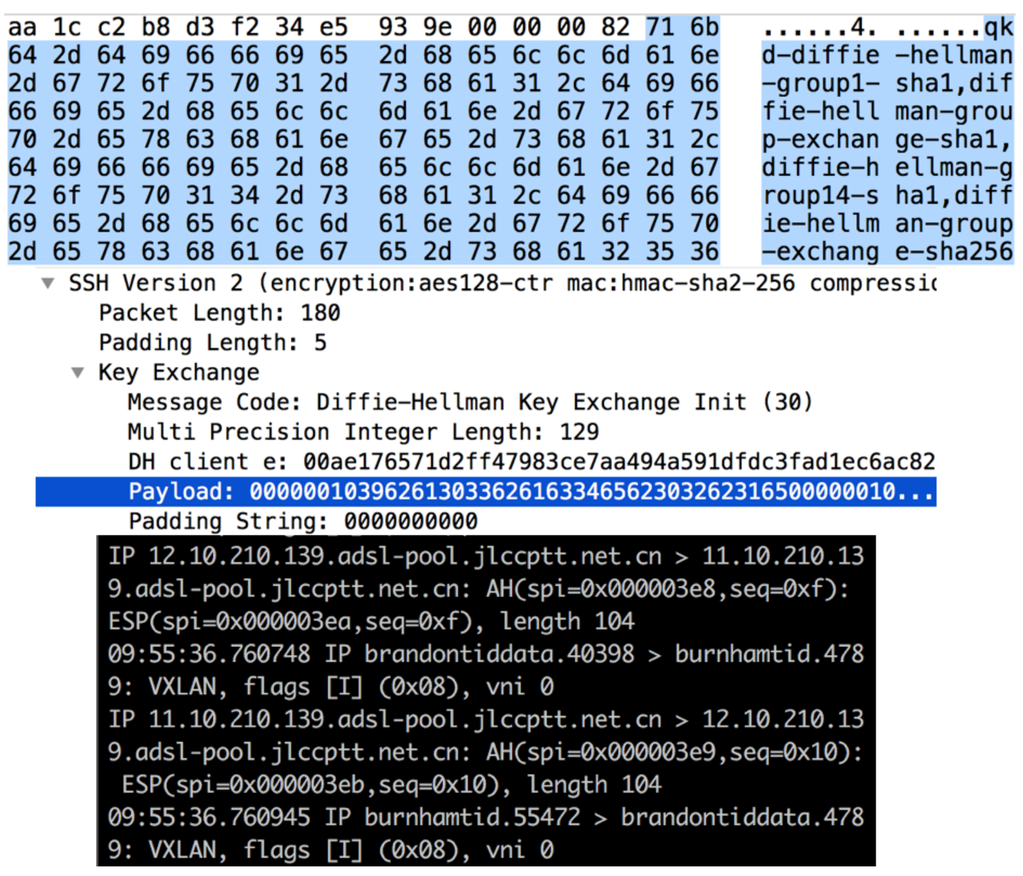

Fig. 2. (top) Preferref key exchange algorithms within the SSH channel; (middle) Payload (key stream IDs) during the key agreement using DHE;(bottom) IPsec and VxLAN traffic.

The first two figures (top and middle ones) show the extended DHE protocol, integrating the key stream IDs as a payload during the exchange. This technique is set as the first in the list of preferred key exchange algorithms. Finally, the last figure (bottom one) shows the traffic exchanged between the secure areas, captured at the physical interface of the server. This includes (among others) VXLAN traffic (the PoPs are connected via VXLAN tunnels from the OVSs) and the IPsec traffic between the virtual routers, shown as authentication header and encapsulating security payload.

CONCLUSIONS. We showcase a prototype of our whole quantum-safe ecosystem and network architecture, implemented on top of the first QKD field trial demonstration on a production network: the Madridś QKD testbed. Any communication channel from both, control and data plane, integrates QKD keys in different ways to provide quantum-safe services.

ACKNOWLEDGMENTS.— This work has been partially supported by the project CVQuCo, TEC2015-70406-R, funded by the Spanish Ministry of Economy and Competitiveness and QUITEMAD+, S2013-IC2801, funded by Comunidad Autonoma de Madrid.

References

(1) A. Aguado, *et al.*, 'Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks' in Journal of Optical Communications and Networking Vol. 9, Issue 10, pp. 819-825 (2017).

(2) A. Aguado, *et al.*, 'Vpn service provisioning via virtual router deployment and quantum key distribution,' in Proc. Optical Fiber Conference (OFC), 2018.

(3) A. Aguado, *et al.*, 'Virtual network function deployment and service automation to provide end-to-end quantum encryption,' J. Opt. Commun. Netw., vol. 10, no. 4, pp. 421430, Apr 2018.