Secure Critical Infrastructures via QKD: the Madrid QKD Network.

A. Aguado[1], V. Martin[1], D. Lopez[2], V. Lopez[2], A. Pastor[2], H. Brunner[3], S. Bettelli[3], C-H. F. Fung[3], A. Poppe[3] and M.Peev[3]
[1]Center for Computational Simulation - Universidad Politecnica 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, Munich Research Center, Riesstrasse 25, 80992 Munchen. Germany
(a.aguado@fi.upm.es, vicente@fi.upm.es, diego.r.lopez@telefonica.com, momtchil.peev@huawei.com)

***Abstract*—The nature of network services is drastically affecting the way the infrastructure is evolving. New demands require new capabilities, forcing the infrastructure to dynamically adapt to new scenarios. Novel network paradigms, such as Software-Defined Networking (SDN) and Network Functions Virtualization (NFV), have appeared to provide flexibility for network management and services. On the other hand, traditional cryptographic protocols rely on certain mathematical problems (e.g. integer factorization, discrete logarithms or elliptic curves) that are believed not to be efficiently solvable using conventional computing. This assumption is being revisited because of quantum computing, which may put at risk the traditional schemes used for network security. Quantum Key Distribution (QKD) is a technique for providing synchronized sources of random and secure symmetric keys between two separated locations. Its security is based on the fundamental laws of quantum physics, according to which it is not possible to copy the quantum states transmitted between endpoints. Therefore, if implemented properly, QKD generated keys are immune against any algorithmic cryptanalysis. This work describes techniques to implement such new 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 planes, providing a whole quantum-safe network environment. This was demonstrated at the Madrid SDN-QKD network, 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.**

I. Introduction

Quantum Key Distribution (QKD) [1], [2] allows for the unlimited and secure growth of a private key between two points that are connected by a quantum channel. This channel, typically implemented using an optical fiber, is used to transport the quantum signals: weak light pulses embodying the quantum properties on which the security of the protocol relies. QKD technology allows to upper-bound the maximum information that is leaked out, independently of the computational power or resources available to the attacker, i.e. QKD is an Information-Theoretic Secure primitive. Thus, the keys produced by a correct QKD implementation are of the highest possible quality. On the other hand, factors such as noise or absorptions that do not impact classical cryptography, are important for QKD, potentially reducing its performance. However, QKD brings an additional physical security layer to an optical network that is qualitatively different from all classical techniques. In consequence, QKD is an opportunity to enhance the security in current networks to keep safe both data and control plane communications.

The Software Defined Networking (SDN) [3] paradigm, created to cope with the network dynamicity, has the capability to control network resources on demand. Similarly, NFV [4] allows the replacement of network functions by software running in a virtual image on commodity servers, thus reducing the amount of hardware appliances to be deployed. Virtualization brings simplicity to the network and reduces costs for both the deployment and the operation of the infrastructure. Nonetheless, these solutions entail certain vulnerabilities, as management architectures are usually abstracted in a single centralized management platforms (the MANO orchestrator, SDN controller), and critical configuration data traverses the infrastructure to distributed points-of-presence (PoP). In addition, also the communications among enterprises premises must be secured. These locations are usually connected via business to business services, implemented as virtual private networks (VPNs) connecting the sites. Technology advances, including but not restricted to quantum computing, are on their way to compromise the crypto primitives currently used to secure these remote communications. When speaking about critical infrastructures and private enterprise information exchange, the security is a must, as all traffic from control and data planes must be secured.

We demonstrate how QKD can bring an additional physical security layer for network infrastructure, showcased in the Madrid's QKD network. The network, described in more detail elsewhere in this meeting, consists of three locations: Almagro (Telefonica's R&D laboratory shared with a Telefonica Spain Point of Presence), Norte and Concepcion (both are large Telefonica Spain facilities). The three nodes and the three connections are part of the Telefonica Spain production network. Almagro hosts a Continuous Variables QKD transmitter built by Huawei and tailored to the requirements of SDN networks (i.e. exposes part of its characteristics to the network so that it can be controlled by the SDN), while Norte and Concepcion host the two receivers. The QKD network, following SDN principles, is optimized in such a way that the transmitter can generate keys with the two receivers having minimum (even none) performance penalties. The link between Norte and Concepcion uses QKD keys for securing multiple channels, provided in a multi-hop scheme by a SDN-based QKD network management (key management layer), while the other two links have direct QKD links.

II. Securing Control and Data Planes via QKD

As mentioned above, the so-called software-networks (i.e. SDN and NFV but also SDWAN or IBN) 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. The latter integration also facilitates QKD adoption in operator's infrastructures. However, this proposal, depending on the layer where it will be integrated, will require to utilize different security schemes.

The first integration use case comes from the control plane. In [5] 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 though the certification of this technology is still a work in progress. The QKD key inherits

the certification from DHE, while DHE also inherits the physical layer security brought by QKD. This solution, integrated in SSH, is used to create the virtual topology distributed among the three PoPs, retrieve the topological information and configure the virtual nodes and create the final services (e.g. a VPN).

The second use case comes from the data plane. The final integration used IPsec as a protocol to secure the traffic between the endpoints. While the implementation within this field trial provided VPN services as depicted in [6], we proposed in [7] the necessary control plane extensions to provide such services in a point-to-point way (rather than in a VPN). In this test, the MANO instance coordinated the creation of the IPsec-based VPN service by orchestrating both VCA instances to provide the same key stream IDs (generated by one of the endpoints). When required, the MANO instance configures one of the ends with no IDs. When configured (and after extracting the necessary keys) the orchestrator receives the IDs, which are then forwarded to the other end, successfully configuring the VPN service. The obtained keys are used for bidirectional authentication and encryption.

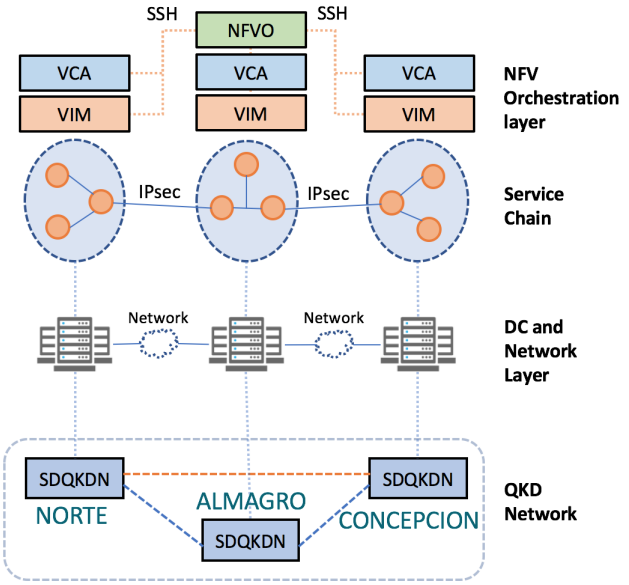

Fig. 1. Logical view **for** the network architecture comprising the QKD, network, virtualization and management layer

III. Experimental Testbed and Results

The experimental testbed is physically distributed as described above. To showcase the different scenarios, we have implemented the stack and the required extensions using different software and hardware platforms. The VIM is a container platform-based on Docker allocated in the three PoPs. It allows to create virtual networks using containers and OpenVSwitches. Among other functionalities, it allows users to control their networks via the SDN controller, enable STP, to attach to physical interfaces, to create VLAN networks, VXLAN tunnels, etc. The VCA is composed of a set of scripts and processes, which are remotely controlled by the NFVO. 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 OSNs 1800 by Huawei 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, they contain the key stores and the SDN software for managing the QKD network as well as the virtualization platforms and the crypto plugins for securing the channels using QKD-derived keys.

The results show how the QKD-keys are integrated in two different layers: in the network control plane, by using a hybrid solution combining the QKD and DHE keys [5] and; in the network data plane, by providing QKD-keys to virtual network functions (routers) to create quantum-safe VPNs based on IPsec protocol [6].

```
aa 1c c2 b8 d3 f2 34 e5  93 9e 00 00 00 82 71 6b   ......4. ......qk
64 2d 64 69 66 66 69 65  2d 68 65 6c 6c 6d 61 6e   d-diffie -hellman
2d 67 72 6f 75 70 31 2d  73 68 61 31 2c 64 69 66   -group1- sha1,dif
66 69 65 2d 68 65 6c 6c  6d 61 6e 2d 67 72 6f 75   fie-hell man-grou
70 2d 65 78 63 68 61 6e  67 65 2d 73 68 61 31 2c   p-exchan ge-sha1,
64 69 66 66 69 65 2d 68  65 6c 6c 6d 61 6e 2d 67   diffie-h ellman-g
72 6f 75 70 31 34 2d 73  68 61 31 2c 64 69 66 66   roup14-s ha1,diff
69 65 2d 68 65 6c 6c 6d  61 6e 2d 67 72 6f 75 70   ie-hellm an-group
2d 65 78 63 68 61 6e 67  65 2d 73 68 61 32 35 36   -exchang e-sha256
```

Fig. 2. Preferref key exchange algorithms within the SSH channel.

```
▼ SSH Version 2 (encryption:aes128-ctr mac:hmac-sha2-256 compressi
    Packet Length: 180
    Padding Length: 5
  ▼ Key Exchange
      Message Code: Diffie-Hellman Key Exchange Init (30)
      Multi Precision Integer Length: 129
      DH client e: 00ae176571d2ff47983ce7aa494a591dfdc3fad1ec6ac82
      Payload: 0000001039626130336261633465623032623165000000010...
      Padding String: 0000000000
```

Fig. 3. Payload (key stream IDs) during the key agreement process using DHE.

The first two figures (2 and 3) 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.

```
IP 12.10.210.139.adsl-pool.jlccptt.net.cn > 11.10.210.13
9.adsl-pool.jlccptt.net.cn: AH(spi=0x000003e8,seq=0xf):
ESP(spi=0x000003ea,seq=0xf), length 104
09:55:36.760748 IP brandontiddata.40398 > burnhamtid.478
9: VXLAN, flags [I] (0x08), vni 0
IP 11.10.210.139.adsl-pool.jlccptt.net.cn > 12.10.210.13
9.adsl-pool.jlccptt.net.cn: AH(spi=0x000003e9,seq=0x10):
 ESP(spi=0x000003eb,seq=0x10), length 104
09:55:36.760945 IP burnhamtid.55472 > brandontiddata.478
9: VXLAN, flags [I] (0x08), vni 0
IP 12.10.210.139.adsl-pool.jlccptt.net.cn > 11.10.210.13
9.adsl-pool.jlccptt.net.cn: AH(spi=0x000003e8,seq=0x10):
 ESP(spi=0x000003ea,seq=0x10), length 104
09:55:37.337624 IP burnhamtid.48495 > brandontiddata.478
9: VXLAN, flags [I] (0x08), vni 0
STP 802.1d, Config, Flags [none], bridge-id 8000.42:11:3
c:db:e9:44.8002, length 35
```

Fig. 4. Traffic exchanged

Finally, the last figure (4) shows the traffic exchanged between the secure areas, captured at the physical interface of the server. This includes (among others, that have been omitted to improve readibility), VXLAN traffic (the PoPs are connected via VXLAN tunnels from the OVSs), STP (to avoid loops between OVSs) and the IPsec traffic between the virtual routers, shown as AH and ESP.

BRIEF GLOSSARY

NVF : Network Function Virtualization.
OpenFlow : Communications protocol to access the forwarding plane of the network devices (switches, routers...). It is a key SDN enabler.
SDN : Software defined network.
VNF : Virtualized Network Function. Describes an instance of a software image performing a network function in the NVF paradigm.
VIM : Virtualized Infrastructure Manager.
MANO : Management and Orchestration entity in an NFV environment
SSH: Secure Shell
VLAN : Virtual Local Area Network
VCA: VNF Configuration and Abstraction
VXLAN : Virtual Extensible Local Area Network
STP : Spanning Tree Protocol
IPsec : Internet Protocol security.
PoP : Point of Presence.
DHE : Diffie-Hellman exchange.

ACKNOWLEDGMENTS

This work has been partially supported by the project CVQuCo, TEC2015-70406-R, funded by the Spanish Ministry of Economy and Competitiveness (MINECO-FEDER) and QUITEMAD+, S2013-IC2801, funded by Comunidad Autónoma de Madrid.

REFERENCES

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sept. 2009.

[2] V. Martin, J. Martinez-Mateo, and M. Peev, "Introduction to quantum key distribution," in *Wiley Encyclopedia of Electrical and Electronics Engineering*, 2017, pp. 1–17. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8354

[3] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, March 2008.

[4] "Network functions virtualisation (nfv); architectural framework," in *ETSI GS NFV 002 V1.2.1*, 2014-12.

[5] A. Aguado, V. Lopez, J. Martinez-Mateo, T. Szyrkowiec, A. Autenrieth, M. Peev, D. Lopez, and V. Martin, "Hybrid conventional and quantum security for software defined and virtualized networks," *J. Opt. Commun. Netw.*, vol. 9, no. 10, pp. 819–825, Oct 2017.

[6] A. Aguado, V. Lopez, J. Martinez-Mateo, M. Peev, D. Lopez, and V. Martin, "Vpn service provisioning via virtual router deployment and quantum key distribution," in *Proc. Optical Fiber Conference (OFC)*, 2018.

[7] ——, "Virtual network function deployment and service automation to provide end-to-end quantum encryption," *J. Opt. Commun. Netw.*, vol. 10, no. 4, pp. 421–430, Apr 2018. [Online]. Available: http://jocn.osa.org/abstract.cfm?URI=jocn-10-4-421