NASK institute in Poland advances quantum encryption

As a national research institute, NASK tackles some of Poland's biggest information, cybersecurity and communications technology challenges. NASK also manages the Nationwide Education Network and maintains National Domain Registry (.pl).

As part of its advanced cybersecurity research, NASK is involved in the development of new encryption techniques that can safeguard data in a world of growing cyberthreats and use Juniper switches and firewalls as part of its testbed.

OVERVIEW

Company	NASK
Industry	Government and Non-Profit
Products Used	QFX5120, SRX1500
Region	

CUSTOMER SUCCESS AT-A-GLANCE

Two

Interconnected data centers protected by QKD and PQC systems

Operates

Nationwide Education Network (OSE) and Warsaw MAN (WARMAN)

2.5 million

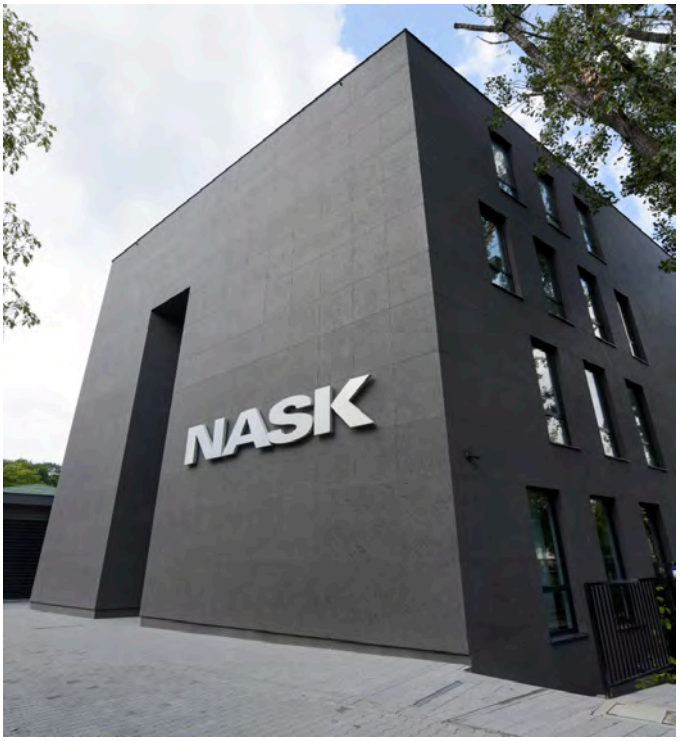
Domain names managed as national registrar

One

Of three nationwide computer security incident response teams for Poland

CHALLENGE

Create quantum-safe cryptography



"NASK is on the forefront of innovation in encryption," says Michael Marks, head of cloud computing and intelligent networks at NASK. The institute is developing, in consortium with Military University of Technology (leader) and TELDAT (project funded by NCBiR -competition 1/SZAFIR/2020), a quantum key distribution (QKD) system that could become standard across military, government or financial institutions in Poland.

QKD involves the exchange of hacker-resistant cryptographic keys that can both encrypt and decrypt messages. A quantum random number generator is used to securely generate entropy, where the outcome or states and random numbers are decided only by a physical process. The information is carried on single photons, which can be transmitted by fiber. Due to the principles of quantum mechanics, the act of observing the key exchange over the network will cause a disturbance, which can be detected by a QKD system, making it extremely secure.

"Not only do our QKD prototypes detect disturbances at the quantum level, but also they can detect even the slightest touch of the fiber," Marks says.

SOLUTION

Prove out quantum encryption systems

QKD architectures leverage three communication channels: crypto, key exchange, and quantum. First, in the crypto channel, quantum keys are shared and then fed into the crypto algorithm, which encrypts massive amounts of data in a separate channel. AES256, which is considered quantum-safe, is used by MACsec to encrypt and decrypt flows. Second, the devices at the end of the quantum channel communicate the quantum keys over the key exchange channel.

The third channel is where the QKD system comes into play. Since quantum mechanics describe objects in the physical world such as photons, devices that deal with quantum keys must be physical transmitters and receivers. In contrast, math-based cryptography can be distributed via software download. Consequently deploying QKD requires the presence of physical equipment.

NASK needed a secure connection to test the effectiveness of the QKD systems beyond the research lab.

Marks began to consider the use of Juniper switching for future testing purposes after meeting a quantum security expert from Juniper at an event in Switzerland several years ago.

Marks knew Juniper solutions well: The NASK engineering and operations team have deep experience in designing and managing large-scale Juniper networks, including the nationwide education network in Poland, which connects more than 20,000 schools and 5 million students. NASK uses Juniper MX Series Universal Routers, Juniper QFX Series Switches, and Juniper SRX Firewalls in this network.

NASK chose the QFX5120 Switch for the first test of its QKD solution in a live environment.

OUTCOME

Protect data privacy now and in the future

As a research institute, NASK is innovating new encryption methods that can safeguard data against today's sophisticated attacks but also potentially protect against devastating quantum attacks in the future.

NASK plans to conduct the first test of its QKD system in a live environment in Q4 2023. QFX5120 switches, which support MACsec, will be used to establish a secure, 200GbE connection between the QKD systems in different locations (primary and backup data center). In the second scenario the Juniper SRX1500 Firewalls will provide a secure IPSec channels using keys exchanged by the QKD system. Moreover NASK researchers plan to test interoperability between Juniper and other providers in a QKD-powered IPSec scenario.

"I am excited that this is the first time QFX switches will be used as part of our QKD solution," says Marks.

NASK also looking forward to more collaboration, including participating in a bigger proof-of-concept test with other universities and institutes in Europe planned for 2024.

"We plan to use Juniper networking to support testing of our first QKD system prototype, but our solution will work with other network vendors," says Marks. "From my perspective, the most important thing is the wide adoption of the QKD solution. We want to help create an ecosystem of partners in different countries to protect national security."

"NASK will use QFX switches as part of our quantum key distribution solution in September 2024."

Michal Marks
Head of Cloud Computing and Intelligent Networks, NASK

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240 1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.207.125.700

Copyright 2023 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.