Case study

Education

Protecting research and innovation sectors from cyber threats

Overview

Universities and research labs are prime targets for intellectual property theft due to their cutting-edge research across a multitude of fields. Attackers are known to capture large volumes of network traffic, for example using a wiretap on a cable, so that the data can be decrypted later. Defending against these attacks is made more challenging by the nature and complexity of university environments where intellectual property and research data must often be shared between the institution itself and thirdparty organisations like innovation hubs; start-ups and corporate partners.

The Challenge

Jisc manages the UK's national research and education network ("JANET") which is part of UK CNI. It serves hundreds of education customers including top universities, academic and research institutions, as well as major global research institutions like CERN and MIT.

Jisc is highly aware of Store Now Decrypt Later (SNDL) threat to sensitive research data either on its JANET network or shared within and between research institutions and corporate partners.

Jisc wanted to test a means of upgrading the encryption on data in transit to protect it from future decryption. PQAs such as CRYSTALS Kyber were considered not yet mature enough, so Jisc wanted to test a solution that could provide symmetric keys at scale to network endpoints.

> **The recent feature launches from leading network equipment vendors combined with Arqit's technology gives Jisc and its members the opportunity to test new features that hardens encryption on data links to a quantum-safe level. We are pleased to be at the forefront of piloting quantum safe cryptography within the academic and research sector to safeguard IP and innovation data.**
> – Simon Farr, Director of Innovation & IT, Jisc

Our Solution

NetworkSecure™ is a software application allowing network equipment to create quantum-safe levels of encryption for data links by using Arqit SKA-Platform™, Arqit's Symmetric Key Agreement platform. SKA-Platform is a cloudbased service that allows connected firewalls to use Arqit's patented protocol to create encryption keys on demand over a public channel without any risk of interception.

NetworkSecure is simple to deploy with industry-leading network devices and requires minimal ongoing management.

Jisc deployed NetworkSecure on two FortiGate NGFWs at either end of a critical point-to-point connection from Jisc's Bristol site and AWS Outpost location. Once installed, the Adaptors were registered with an Arqitmanaged cloud instance of SKA-Platform and acted as an interface between SKA-Platform and each FortiGate. The FortiGates were successfully able to agree symmetric pre-shared keys (PPKs) used in the IPSec tunnel creation without any distribution or transmission of the keys.
By using these PPKs (used in addition to the existing PKI method of key exchange between the firewalls) the data packets passing through the IPSec tunnel would contain insufficient key material for decryption, even if harvested.

Outcomes

- Quantum-safe level of security
- No negative effect on latency
- Conforms to NIST standards for cryptography