PQC for IKEv2 in strongSwan

28/03/2019, IETF 104, Prague

Motivation

- Applications dealing with highly sensitive data will require PQC in the near future
- “Store now, decrypt later” attack
- Considerable time required for standardization, implementing, testing etc.
- We support quick adoption of INTERMEDIATE exchange and hybrid IKEv2
- Our idea: Demonstration of hybrid IKEv2 based on INTERMEDIATE exchange

Hybrid IKEv2 in strongSwan

- Implemented by Andreas Steffen and Tobias Bruner (ikev2-qske-notify)
- Based on **draft-smyslov-ipsecme-ikev2-aux-00** (January 2018)
- Implementation details:
  - New IKEv2 QSKE_MECHANISM transform type
  - New IKEv2 QSKE payload
  - QSKE initially transported via IKE_AUX/INTERMEDIATE
  - QSKE can be transported in CREATE_CHILD_SA (multiple child SAs, rekeying)
  - New INVALID_QSKE_PAYLOAD notify message
  - liboqs library (NewHope, Frodo, Kyber, BIKE, SIKE, SABER, LIMA)
- Test scenarios: https://www.strongswan.org/testing/ikev2-qske/swanctl/

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

Leonie Bruckert
Consulting Defence

secunet Security Networks AG
Ammonstraße 74
01067 Dresden
Telefon +49 201 5454-3819
leonie.bruckert@secunet.com