

OPEN
LIGHT
COMM

AIRQKD

Experimentations with the CQP Toolkit

Alexandros Stavdas, Christos
Matrakidis, Evangelos Kosmatos
(OpenLightComm)

Testing the CQP Toolkit with Dummy QKD Drivers (network deployment)

- ❑ Objective: to use the CQP Toolkit and “dummy” CQP QKD drivers to setup a mock key exchange between two nodes (laptops) located in different locations in the network
 - Deploy the dummy CQP QKD drivers on both ends (laptops)
 - Use the CQP Toolkit to synchronize the generated keys
 - Set-up a connection between the two nodes
 - Exchange encrypted data using this connection



AIRQKD

Results (I)

A dummy QKD driver on Alice laptop

```
root@user-lab-01: /home/user/build-cqptoolkit/src/Drivers/DummyQKDDriver

user@user-lab-01:~$ sudo su
[sudo] password for user:
root@user-lab-01:/home/user#
root@user-lab-01:/home/user# cd build-cqptoolkit/src/Drivers/DummyQKDDriver
root@user-lab-01:/home/user/build-cqptoolkit/src/Drivers/DummyQKDDriver# sudo ./DummyQKDDriver -r localhost:8000 -a
DEBUG: LoadChannelCredentials: Using insecure credentials
DEBUG: LoadServerCredentials: Using insecure credentials
INFO: StartControlServer: Control interface available on user-lab-01:35895
INFO: StartControlServer: Registering with site agent localhost:8000
DEBUG: RegisterWithSiteAgent: Registering device dummyqkd_0_16_alice with localhost:8000
INFO: Main: My device id is dummyqkd_0_16_alice
DEBUG: SessionStarting: Connecting to peer at user-lab-02:41369
```

A dummy QKD driver on Bob laptop

```
root@user-lab-02: /home/user/build-cqptoolkit/src/Drivers/DummyQKDDriver

user@user-lab-02:~$ sudo su
[sudo] password for user:
root@user-lab-02:/home/user# cd build-cqptoolkit/src/Drivers/DummyQKDDriver
root@user-lab-02:/home/user/build-cqptoolkit/src/Drivers/DummyQKDDriver# sudo ./DummyQKDDriver -r localhost:8001 -b
DEBUG: LoadChannelCredentials: Using insecure credentials
DEBUG: LoadServerCredentials: Using insecure credentials
INFO: StartControlServer: Control interface available on user-lab-02:41369
INFO: StartControlServer: Registering with site agent localhost:8001
DEBUG: RegisterWithSiteAgent: Registering device dummyqkd_0_16_bob with localhost:8001
INFO: Main: My device id is dummyqkd_0_16_bob
WARN: Start: Thread already started
WARN: Start: Thread already started
```

AIRQKD

Results (III)

The s/w module Site Agent on Bob laptop

```
root@user-lab-02: /home/user/build-cqptoolkit/src/Tools/SiteAgentRunner
user@user-lab-02:~$ sudo su
[sudo] password for user:
root@user-lab-02:/home/user# cd build-cqptoolkit/src/Tools/SiteAgentRunner
root@user-lab-02:/home/user/build-cqptoolkit/src/Tools/SiteAgentRunner# sudo ./SiteAgentRunner -p 8001 &
[1] 1831
root@user-lab-02:/home/user/build-cqptoolkit/src/Tools/SiteAgentRunner# DEBUG: GrpcAllowMACOnlyCiphers: Setting GRPC_SSL_CIPHER_SUITES to DHE-PSK-NULL-SHA256:ECDSA-PSK-NULL-SHA256:DHE-PSK-NULL-SHA384:ECDSA-PSK-NULL-SHA384:ECDSA-ECDSA-AES128-GCM-SHA256:ECDSA-ECDSA-AES256-GCM-SHA384:ECDSA-RSA-AES128-GCM-SHA256:ECDSA-RSA-AES256-GCM-SHA384
DEBUG: LoadChannelCredentials: Using insecure credentials
DEBUG: CreateBackingStore: Creating a backing store for
DEBUG: LoadServerCredentials: Using insecure credentials
INFO: SiteAgent: My address is: user-lab-02:8001
DEBUG: RegisterDevice: Device registering: dummyqkd_0_16 bob
INFO: RegisterDevice: New Bob device: dummyqkd_0_16 bob at 'user-lab-02:41369' on switch '' port ''
DEBUG: StartNode: user-lab-02:8001 is starting node with user-lab-01:8000 user-lab-02:8001
DEBUG: LoadChannelCredentials: Using insecure credentials
DEBUG: GetKeyStore: Creating keystore from user-lab-02:8001 to user-lab-01:8000
DEBUG: KeyStore: New key store from user-lab-02:8001 to user-lab-01:8000
WARN: PrepHop: No key available for bootstrap. Either populate the keystores or provide a fallback key in the configuration.
DEBUG: SecretPath is now user-lab-02:8002 - user-lab-01:8000
INFO: StartNode: Node setup complete
DEBUG: GetNewDirectKey: Reserved original key 3
```

QKD driver connected

Node setup done

QKD keys generated and used

AIRQKD

Results (V)

Site Agent Controller software module on Bob laptop

```
root@user-lab-02: /home/user/build-cqptoolkit/src/Tools/SiteAgentCtl
user@user-lab-02:~$ sudo su
[sudo] password for user:
root@user-lab-02:/home/user# cd build-cqptoolkit/src/Tools/SiteAgentCtl
root@user-lab-02:/home/user/build-cqptoolkit/src/Tools/SiteAgentCtl# sudo ./SiteAgentCtl -d -c localhost:8001
DEBUG: GrpcAllowMACOnlyCiphers: Setting GRPC_SSL_CIPHER_SUITES to DHE-PSK-NULL-SHA256:ECDHE-PSK-NULL-SHA256:DHE-PSK-NULL-SHA
A384:ECDHE-PSK-NULL-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RS
A-AES256-GCM-SHA384
DEBUG: LoadChannelCredentials: Using insecure credentials
DEBUG: GetDetails: Getting Site details...
{
  "url": "user-lab-02:8001",
  "devices": [
    {
      "config": {
        "id": "dummyqkd__0__16_bob",
        "side": "Bob",
        "kind": "dummyqkd"
      },
      "controlAddress": "user-lab-02:41369"
    }
  ]
}

root@user-lab-02:/home/user/build-cqptoolkit/src/Tools/SiteAgentCtl#
```

Site Agent
configuration

Results (VI)

Establishing a connection (tunnel) on Alice side

```
root@user-lab-01: /home/user/build-cqptoolkit/src/Tools/QTunnelServer
user@user-lab-01:~$ sudo su
[sudo] password for user:
root@user-lab-01:/home/user# cd build-cqptoolkit/src/Tools/QTunnelServer
root@user-lab-01:/home/user/build-cqptoolkit/src/Tools/QTunnelServer# sudo ./QTunnelServer -p 9010 --keystore-url='user-lab-02':8001
INFO: Main: Loading blank configuration.
DEBUG: LoadChannelCredentials: Using insecure credentials
DEBUG: LoadServerCredentials: Using insecure credentials
DEBUG: Controller: Using keystore: user-lab-02:8001
INFO: Controller: Tunnelling controller started with ID: d879e195-fe46-4a8d-adee-ea350c736ddd
DEBUG: Controller: I have 0 tunnels defined.
DEBUG: LoadServerCredentials: Using insecure credentials
INFO: Main: My address is: user-lab-01:9010
DEBUG: CompleteTunnel: Waiting for keystore...
DEBUG: CompleteTunnel: Keystore ready
DEBUG: LoadChannelCredentials: Using insecure credentials
DEBUG: LoadServerCredentials: Using insecure credentials
DEBUG: TunnelBuilder: Cipher Mode=GCM, SubMode=Tables2K, BlockCypher=AES
DEBUG: TunnelBuilder: Server ready on user-lab-01:37437
DEBUG: ConfigureEndpoint: Endpoint details:
  Unencrypted port: tcpsrv://0.0.0.0:9001
  Far Keystore: user-lab-01:8000
INFO: TCPServerTunnel: Waiting for connection on tcpsrv://0.0.0.0:9001
INFO: CompleteTunnel: Tunnel setup complete
INFO: TunnelBuilder: Connection established
DEBUG: WriteEncrypted: Getting new shared key
DEBUG: ReadEncrypted: Getting key: 2
DEBUG: ReadEncrypted: Getting key: 4
DEBUG: ReadEncrypted: Getting key: 5
DEBUG: ReadEncrypted: Getting key: 6
```

Configuration completed

Encrypted data exchanged on the tunnel

Results (VII)

Establishing connection (tunnel) on Bob side

```
root@user-lab-02: /home/user/build-cqptoolkit/src/Tools/QTunnelServer
user@user-lab-02:~$ sudo su
[sudo] password for user:
root@user-lab-02: /home/user/build-cqptoolkit/src/Tools/QTunnelServer# ./QTunnelServer --keystore-url='user-lab-01':8000 --remote=192.168.1.14:9010 --start-node=tcpsrv://0.0.0.0:9000 --end-node=tcpsrv://0.0.0.0:9001-l
INFO: Main: Loading blank configuration.
DEBUG: LoadChannelCredentials: Using insecure credentials
DEBUG: LoadServerCredentials: Using insecure credentials
DEBUG: Controller: Using keystore: user-lab-01:8000
INFO: Controller: Tunnelling controller started with ID: 63d990a9-6279-4f7e-9dc7-e29ccccf915ea
DEBUG: Controller: I have 0 tunnels defined.
DEBUG: LoadServerCredentials: Using insecure credentials
INFO: Main: My address is: user-lab-02:43279
INFO: Main: Setting key lifespan to 65536 bytes or 10 seconds
INFO: Main: Starting tunnel simple-tunnel
DEBUG: StartTunnel: Waiting for keystore
DEBUG: StartTunnel: Keystore ready
DEBUG: StartTunnel: Defaulting encryption mode to GCM
DEBUG: StartTunnel: Defaulting sub mode to Tables2K
DEBUG: StartTunnel: Defaulting block cypher to AES
DEBUG: LoadChannelCredentials: Using insecure credentials
DEBUG: TunnelBuilder: Cipher Mode=GCM, SubMode=Tables2K, BlockCypher=AES
DEBUG: FindController: Connecting to 192.168.1.14:9010
DEBUG: StartTunnel: Found controller
DEBUG: StartTunnel: Configuring endpoint
DEBUG: ConfigureEndpoint: Endpoint details:
  Unencrypted port: tcpsrv://0.0.0.0:9000
  Far KeyStore: user-lab-02:8001
INFO: TCPSTunnel: Waiting for connection on tcpsrv://0.0.0.0:9000
DEBUG: EncodingWorker: Connecting to encrypted channel user-lab-01:37437
INFO: EncodingWorker: Waiting for client
DEBUG: WriteEncrypted: Getting new shared key
DEBUG: WriteEncrypted: Getting new shared key
DEBUG: WriteEncrypted: Getting new shared key
DEBUG: WriteEncrypted: Getting new shared key
```

Configuration completed

Encrypted data exchanged on the tunnel

Results (VIII)

Application's encrypted data exchange between Alice and Bob laptops



Thank You!!!
