STATEMENT OF CASE FOR WHITELISTING QUANTUM VIRTUAL PRIVATE NETWORK CLIENT FOR E-TAB BASED ACCESS TO QUANTUM SECURE CAMPUS WIDE NETWORK AT MCEME

INTRODUCTION

1. Military College of Electronics and Mechanical Engineering (MCEME) is a premier training institute imparting technical training to Officers and NCOs. Over a period of time, the landscape of education and training has witnessed a paradigm shift with the increasing integration of technology into academic and administrative processes. Online learning has become pivotal in enabling to meet modern educational demands, facilitating efficient course delivery, resource sharing and collaboration. There is a need for an adaptable, scalable and secure architecture with robust systems for ensuring secure access to the training content on network.

2. As a pilot project, MCEME was tasked to implement a secure wireless access mechanism over College Wide Network (CWN) to provide access to training material for all trainees. To address the threats to networks emanating due to existence of Quantum Computers, a Post Quantum Cryptography based Quantum secure campus wide network setup has been designed and implemented within MCEME. The solution includes customised, secure and hardened BOSS operating system based client devices, a Quantum Virtual Private Network (QVPN) Server and a Quantum Random Number Generator (QRNG) device which together provide a secure access to the client (trainee) of the training content hosted within CWN. The client device has been embedded with a custom made QVPN client which is used to establish a secure connection with the QVPN server over the network. Being a third party custom made application, presently there is a requirement to whitelist the QVPN client of QVPN solution implemented in MCEME. Being a custom made unique application for the secure solution at MCEME, the whitelisting will provide a secure way to establish Quantum secure network (both physical and WiFi) across campus of training institutes within Indian Army.

AIM

3. The aim of Quantum Virtual Private Network Client is to establish a PQC based Quantum secure connection with QVPN server to extend access to training content hosted on CWN over network within MCEME.

SCOPE

4. The function of QVPN client is to establish secure QVPN tunnel with QVPN server.

DESCRIPTION

5. **Purpose**. To establish secure QVPN tunnel with QVPN server.

6. **Beneficiaries**. All users on Quantum Secure network in MCEME.

7. **Target User Base**.

   (a) **Students**. 800 (approx).

(b) **Faculty/ Staff**. 40(approx).

(c) **Administrative Staff**. 20(approx).

(d) **Total Users**. 860(approx).

8. **Features and Operating Procedure**.

(a) The tunnel uses TLS1.3 as transport protocol.

(b) The QVPN client uses PQC based Crystals Kyber (kyber1024) key exchange mechanism (KEM) algorithm.

(c) The QVPN client uses AEAD (Authenticated Encryption with Associated Data) using AES-256-GCM with SHA384.

(d) The QVPN client uses Quantum seed from QRNG source to generate cryptographic keys.

(e) If QRNG is not accessible from QVPN client, then a random seed is used from systems PRNG (Pseudo Random Number Generator) source within the client device.

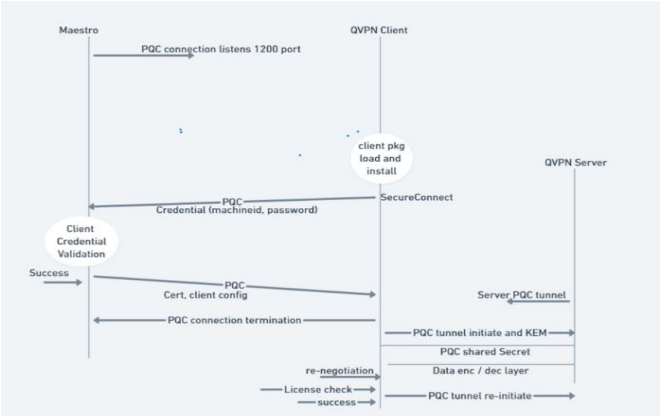
(f) QVPN client in client devices authenticates itself with Maestro server (provisioning, authentication and registration server for QVPN clients) over PQC channel established between the client and Maestro.

(g) QVPN client uses unique machine ID of the client device and client password as the credentials for validation and authentication. Both these parameters are registered with Maestro server during the initial process of onboarding of client device.

(h) On successful authentication, QVPN client receives client configuration file and PQC certificates (dilithium) from Maestro while creating the PQC tunnel.

(j) QVPN Client is configured to be re-negotiated periodically and the period is configurable. The re-negotiation ensures complete forward secrecy (complete new set of KEM and data cipher key generation). Presently it is configured for 5 minutes.

(k) QVPN Client retries to establish connection with the QVPN server for a configurable period in case of network fluctuation, reconnection or move of client devices across different Access Points.



QVPN Client interaction with Maestro & QVPN Server

(l) The QVPN Client connects to Maestro server for authentication on Port 1200. This is PQC enabled TLS/SSL port on Maestro server.

(m) QVPN client gets one client configuration file from Maestro after successful validation / authentication. The file contains server IP and port to which the client will establish PQC tunnel with the server.

(n) **Client's Interaction with OS**. The QVPN client interacts with OS only via standard system calls (syscall). The security of system APIs are guaranteed by Operating system.

(o) **Security of Open-Source Software and Libraries**. QVPN client uses two Open-Source libraries :-

(i) **OpenSSL**. The inherent security is provided by OpenSSL which is validated by the community.

(ii) **Open Quantum Safe (liboqs)**. The inherent security is provided by the OQS community.

(p) **Password Storing Mechanism**. The QVPN Client does not store any password. It takes the users input as password for client authentication with the Maestro. The password is stored in memory for the period only during processing and the memory is cleared and password is deleted post authentication.

9. **Requirements for Hosting Environment**. The QVPN Client is customised application installed in OS of client device.

10. **Security and Access Control**. The QVPN client is installed as part of OS and doesn't allow any access to users. The user can only use the client application to establish a QVPN connection.

11. **Cost**. The QVPN Client is a customised client application and has been installed as a part of the entire project of establishing campus wide quantum secure network at MCEME.

12. **Date of Completion**. 15 Oct 2023.

13. **Architecture**. QVPN client is installed on every client device accessing Quantum Secure Network in MCEME.

14. **Upgrade Mechanism**. Network based patch update mechanism has been implemented.

15. **Licensing**. 400 perpetual licenses have already been procured for the said project.

CONCLUSION AND RECOMMENDATIONS

16. The QVPN client is embedded in the Operating System of client devices for establishing a QVPN tunnel with QVPN server. The client package is a custom development as a part of entire solution for establishment of Campus wide Quantum Secure network across MCEME. The QVPN client is an application in client device which establishes the secure connection with QVPN server allowing all users to have secure access to training content over CWN.

17. Given its proven capabilities and customised configuration with client devices, it is recommended that QVPN client be whitelisted for installation on client devices for establishing QVPN tunnel to access Quantum Secure network in MCEME.