**Communication Quantum Attack Resistance Scanner**

Edit By Liu Yuancheng 13/01/2022

**Program Design Purpose**:  We want to check/test whether the communication between two point (such as 2 servers) has the resistance ability for Quantum Crypto Attack.

**Introduction**

This project is aimed to develop a probe/scanner program to analysis the network packets of communication channel between two points to give the confidence level of the resistance ability for Quantum Crypto Attack.

As we don’t have the way to simulate the quantum crypto attack, so what we want is parsing the network packet from the host/dist side or in the mid to analysis the network communication protocol to identify whether the communication is quantum safe. We will compare the protocol with our data base Quantum Attack standard to give a value.

The standard we want to use is NSA\_Suite\_B\_Cryptography ‘s Quantum resistant suite.

For example:

If we find the packet is using protocol OpenSSH 2.3.1(SSH2), as its encryption use aes128-ctr, we say it doesn’t have the resistance ability for Quantum Crypto Attack.

If we find the packet is using WireGuard protocol, as it is using Curve25519 for key exchange, ChaCha20 for symmetric encryption, Poly1305 for message authentication codes, SipHash for hashtable keys and BLAKE2s for cryptographic hash function, so we are 80% confident about it have the resistance ability for Quantum Crypto Attack.

**Program Design**

The program contents three main parts:

* Network traffic packet collection module.
* Protocol parsing and matching module.
* Result visualization module.

**1. Packet Collection Module**:

The Network traffic packet collection module have two kinds of design: collect in one side or collect in the mid.

Collect in one side:

Install our collection program (wireShark, tshark or pyshark) in the source or destination machine.

Diagram

Description automatically generated

Advantage: easy to implement.

Disadvantage: need servers’ permit and install the program in the server side.

Collect in one side:

Install our collection program (ettercap) in a computer and plug in their network.

Diagram

Description automatically generated with medium confidence

Advantage: Can make a plug and play device, not make any influence for the system.

Disadvantage: May be blocked by some of the firewall (Ettercap packet capture can also be used for mim attack, if the firewall defined it as a malware, it may be blocked.)

**2.Protocol parsing and match module**.

Parsing the protocol detail from the TCP/UDP layer. Match the primitives used by the protocol then generate the confidence level of the resistance ability for Quantum Crypto Attack. Our database need to continuous update during our research.

For example we paring these data from the packet:

Text

Description automatically generated

=> Not quantum safe

Graphical user interface, text, application

Description automatically generated with medium confidence

=> May be quantum safe

Text

Description automatically generated

=>quantum safe

**3. Result visualization module.**

We want to design some UI/Dashboard to show all the communication between A and B in a list , then categorized all the packet by protocol types and highlight the result we calculated to give the user a conclusion.

**Program Workflow Diagram:**

Diagram

Description automatically generated