Implementation of Post Quantum Encryption with Linux on Z

James Nelson
VM Workshop 2024, Richmond, VA

What is post quantum cryptography?

- A series of encryption algorithms that are designed to not be weak to attacks by quantum computers

Quantum computers?

- A novel way of working with numbers and number sets that rely on advanced physics understanding
- Are capable of solving certain classes of problems that are essentially impossible to solve in a reasonable time frame with traditional computing
- Currently are just coming out of the research lab, at least in smaller configurations

Why do we need it?

- All attacks are currently theoretical since quantum computers large enough to do these attacks currently do not exist
- However, there is a significant amount of effort being made to make quantum computers with enough qbits to attack current key strengths
- The number of qbits in existing quantum computers keep getting bigger, and...

Fear, Uncertainty, Doubt

- At a certain point, quantum computers will get to the point that they will be able to break existing crypto algorithms
- We do not know when that will happen - and you can make the argument that it never will
- From a risk assessment point of view, this is BAD - some very smart people are being funded by very big companies to make this happen
- When this happens, the risk assessment calculation gets very complex if you have not prepared.

RSA and EC attacks

- Shor's Algorithm is the technique used to attack RSA keys.
- Elliptic Curve (EC) algorithms were intended to make calculation of the private key much more difficult.
- However, crypto researchers were able to create a modified Shor's Algorithm implementation to attack the elliptic curve calculations

Q-day - there will be multiple

- The fundamental issue is that we do not know when quantum computers will have enough qbits to break modern encryption
- The weaker keys will fall first - current exploit models rely on X qubits for X bits of key length

The new cyphers

- Current algorithms include:
- SPHINCS+
- CRYSTALS-Dilithium
- CRYSTALS-Kyber - key exchange
- NTRU
- FALCON
- There are many more, relying on the NIST standardization process is critical for non-cryptographers to keep up

The hybrid cypher: X25519Kyber[x]Draft00

- In order to get some protection against store-and-decrypt-later attacks, there is an effort to use a hybrid traditional / quantum algorithm
- X25519Kyber is implemented in a number of modern browsers as well as by vendors like Cloudflare

Software: OpenSSL 3.x and liboqs

- OpenSSL 3 includes the infrastructure to include and configure liboqs, an open source implementation of a large number of post-quantum algorithms
- The liboqs library includes bindings for a number of languages, including Go, Java, C++, Rust, and Python

Software: OpenSSH 9

- OpenSSH 9 has NTRU Prime algorithm as a supported algorithm

Hardware: CryptoExpress

- CEX7S (z15) has hardware support for CRYSTALS-Dilithium per IBM documentation
- CEX8S (z16) Supports CRYSTALS-Dilithium, CRYSTALS-Kyber, FALCON, and SPHINCS+
- libica does not support any post quantum algorithms

Hardware: DASD, Fiber Channel, Tape

- Encryption at rest, management interfaces, secure fiber channel will be up to the vendor as well as z/VM
- Since all modern disk and tape systems have a major software component, this technically can be addressed with firmware updates

OS: z/VM

- No publicly available information on implementation of post quantum algorithms in OS functions
- HTTPS, TN3270E, FTPS all contain confidential information

OS: VSEn

- Per 21st Century Software, updating to OpenSSL 3.0 is underway
- VSE Connector, CICS Transaction Gateway contain confidential information
- JCL can also contain calls to insecure network targets and those utilities will have to be tested

OS: Linux

- SLES15 provides OpenSSL 3 but applications are not built against it - command line interface unless you custom build applications
- Fedora 39 has OpenSSL 3 as its base version, with applications built against it. Also has OpenSSH 9 included.
- Ubuntu 24.04 has OpenSSL 3 and OpenSSH 9 included.
- Even with the new OpenSSL version, many applications are not written to handle post quantum algorithms in SSL negotiation

Auditing SSL configuration

- This can be an entire presentation on its own
- First requirement is creating an inventory of places encryption is being used
- The nmap Linux utility has scripts to enumerate ssl and ssh ciphers being used - it currently does not recognize pqc algorithms
- This allows you to identify systems and applications that are badly configured - disabling weak algorithms and turning off obsolete SSL protocols is part of standard system hardening

Potential mitigations - FIPS 140-2

- FIPS 140-2 is a federal standard used to define cryptographic standards for systems handling sensitive but not confidential information
- It can cause breaking changes turning it on in an existing system - the minimum key length requirements will show you where your weak keys are
- In Linux it also precludes the use of some software - RADIUS and Samba both include weak algorithms in their implementation and cannot be run in a system in FIPS 140-2 mode
- Even without enabling FIPS mode, you can use the guidance on key strength and protocol configuration to protect yourself if your industry has not provided guidance or regulation

Risk assessment

- VPNs are a great mitigation against network sniffing by outside attackers - encrypted tunnels are an easy first place to go
- The use of HTTPS for large portions of new software's API interfaces means properly configuring those services are also paramount
- Encryption at rest is going to be a huge exposure that isn't clearly defined - encrypted backup tapes *were* as safe as possible

Risk assessment

- Other network protocols that live inside your system are, frankly, less of a risk but should not be ignored
- Any environment large enough to use network routing protocols can be used by an internal bad actor to redirect your inside traffic, and modern networks include a lot of ways to sniff traffic
- Once quantum computers become available for crypto breaking, encrypted communications that are "safe in our network" can be exploited

Final thoughts

- There is no such thing as a small operation running a mainframe - every system we run contains valuable data
- We cannot assume that obscure protocols and network firewalls protect us
- Modern threat actors can be incredibly skilled, and the increasing visibility of mainframes in fintech can definitely motivate attackers
- Quantum computing will be as disruptive as Y2K for our industry, and even more complicated to manage due to the massive number of moving parts