| Author: Justin Martel | Instructor: IH |
| --- | --- |
| Date: Dec 02, 2021 | Subject: Risk Assessment |

1. Executive Summary

*“For there is nothing covered, that shall not be revealed; neither hid, that shall not be known.”*

There is no small probability that quantum computers will be sufficiently stable in the future, and that certain quantum algorithms known to have significant speedup over classical algorithms will be readily capable of breaking standard encryption schemes like RSA, AES, and Elliptic Curve Cryptography (ECC). This risk assessment considers various threats, vulnerabilities, and measures which can be enacted in the near future to mitigate the threats of quantum-enabled decryption in the next ten years.

2. Scope

The scope of this assessment is to consider which best practices can be employed at present to minimize the threat of future quantum capabilities. This is extremely broad subject, and we limit ourselves to some basic problems at this stage. We do not consider any post-quantum cryptoschemes in detail, e.g. the very interesting lattice-based methods. We expect that the standard encryption schemes will eventually be replaced with a quantum-secure method. But meanwhile we consider auxiliary methods that can securely be used in combination with the current standard schemes.

3. Summary of Findings

Security has excessively relied on the standard cryptographic schemes, and auxiliary cryptographic techniques have been mostly neglected. Thus the possibility of quantum computers readily breaking this layer has potentially catastrophic consequences. Especially vulnerable is encrypted information with a “long lifetime”, e.g. information obtained today which will retain utility in the future. For example, personal private information has long lifetime on the scale of ~50 years. Another example is legacy industrial control systems, whose encryption standard cannot be updated.

4. Background

Cryptography is necessary when private information needs to be transmitted over insecure channels. A secure cryptography scheme needs expect worst-case scenarios with adversaries readily intercepting encrypted communications.

The standard cryptography schemes (AES, RSA, ECC) depend on the computational hardness of certain problems, specifically of factoring large numbers and the so-called discrete log problem. This is the cornerstone of standard encryption. Using classical computers, there is abundant evidence that an exponential amount of time is required to break these schemes, and therefore they have been considered secure and widely deployed.

Yet the development of quantum algorithms, e.g. Edwards’ order finding, Grover’s unordered search, and Shor’s algorithm reveals that quantum computers can (in certain special cases, and especially involving number-theoretic multiplication) offer significant speedups over the presently best known classical methods.

It is widely publicized that Shor discovered how to fast factorize numbers using quantum computation, i.e. using wave coherence and resonance. To date, quantum computers are extremely sensitive, need be kept at ~0 Kelvin (absolute zero refrigerator), and are extremely sensitive to thermal noise and decoherence. There is no small possibility that 1000 qubit quantum machine in series with state-of-the-art supercomputers will be constructed in ten years.

Therefore the situation is that information which is encrypted and secure *today*, need not be secure in *future.* The problem faced in this risk assessment is to determine which actions can be taken today to minimize risk and damages in future.

The most vulnerable assets today are those whose utility will not expire in the future. This includes:

* Private personal information (whose lifetime is proportional to the persons’ lifetime);
* Permissions and Passwords on legacy software in industrial utilities, nuclear power stations, hydro dams, water filtration facilities, factories;
* Budgets, R&D, Infrastructure;
* Legacy systems which cannot or will not be updated or modified in near future.

5. Risk Identification

5.1 Business Impact Assessment

This assessment concerns all digital assets which are sufficiently sensitive to require encryption, which is the bulk of data being transmitted today. Every business is potentially impacted by the fact that their past and present encrypted packets will be open to brute-force decryption by sufficiently stable quantum computers at some future date unknown.

Thus far the integrity and availability of business’ assets are not *yet* directly impacted by the potential of quantum capabilities, but theft and exfiltration of such encrypted assets *is* increasingly active. [ref]. In other words, bad actors are collecting and hoarding the encrypted data in anticipation of either selling or quantum brute-forcing and decrypting. After this future time, the confidentiality is severely impacted.

5.1.1. Network Diagram

%% Incomplete %%

5.2 Threat and Vulnerability Assessment

5.2.1 Threat Assessment

| Threat # | Threat Descriptions | Threat Likelihood |
| --- | --- | --- |
| T1 | Exfiltration or interception of encrypted data with long lifetime. | High. |
| T2 | Exfiltration or interception of encrypted data which has short lifetime. | Low. |

5.2.2. Vulnerability Assessment

| Vulnerability # | Vulnerability Descriptions |
| --- | --- |
| V1 | Unencrypted Catalogues, or Servers, Files Names, Headers, etc., reveals the nature of the files contents. For instance, the values in an SQL tableaux consisting of Name|DateOfBirth|SIN might be encrypted, but if the file is openly named “Sensitive Personal Information”, or the columns of the table have the conventional names, then that data will be target of exfiltration. Once obtained, the data will be potentially decrypted in future. |
| V2 | Contiguous data streams. If encrypted data is transmitted in contiguous streams, then a single listening post or sniffer will be capable of intercepting the complete encrypted data stream, and potentially decrypt in future. Furthermore, contiguity frequently reveals how the encrypted message is to be reassembled for decryption. |
| V3 | Legacy systems whose encryption is hard-coded to follow the standard cryptographic schemes. Their hardware might even be optimized for the specific standards. These legacy systems will eventually require replacement. |

5.3. Security Control Selection

5.3.1. Assess and Evaluate Risk

| Threat Type | Threat Description | Threat Likelihood | Impact Rating | Risk Exposure Rating |
| --- | --- | --- | --- | --- |
| T1 | Exfiltration or interception of encrypted data with long lifetime. | High | High | High |
| T2 | Exfiltration or interception of encrypted data which has short lifetime. | Low | Medium | Medium |

5.3.2. Recommendations

(a) We first recommend all parties to expect and prepare for the standard encryption schemes to become nonsecure in the future, and for a new standard (likely lattice-based) to be implemented.

(b) We recommend that all parties clearly identify those assets which have a long lifetime, and to immediately “pad” or augment the cryptographic standards used in both the storage and transmission of these assets. This means combining the standard schemes with some classical obfuscation and steganographic techniques, I.e. pre-composing and post-composing the standard encryption with *nonstandard* techniques. As a very elementary example, when transmitting encrypted data, one might implement a dynamic Caesar shift depending on the date and time of transmission. This is intended to complicate any future analysis of decrypted information.

(c) We recommend that long lifetime data never be contiguously transmitted or stored, and for non encrypted meta-data to never be included in the transmission. Concretely this includes obfuscating even the *names* and *paths* of the directories. The idea again is that any attacker who wants to exfiltrate encrypted data will need exfiltrate the *global* directory. In otherwords, the *nature* of the encrypted data needs be obfuscated. This forces attackers to collect exceedingly large amounts of (mostly useless) data. (“Needle in a needle stack”).

(d) %% Incomplete %%