eclypses

WHITE PAPER

Why You Should Be Concerned About Quantum Computing

www.eclypses.com

Document ID: 736(6
Version No.:

Contents

Introduction

Quantum Computing is a different technology than what we use today which is known as Classical Computing. It is an emerging technology and in a very short time it will have the potential to render most current data protection mechanisms highly vulnerable to being compromised.

This brief paper describes at a very high level why that should be a concern to today's business environment, and it outlines a high-level strategy to begin to grapple with this issue.

Most of this information comes from a document published by the Accredited Standards Committee X9, Inc. The entire document is available for free download from that organization at https://x9.org/download-qc-ir/ and is quite detailed and in some cases very technical.

Background

According to the executive summary of the Accredited Standards Committee X9, Inc report:

> *A Cryptographically Relevant Quantum Computer (CRQC) is a computer that harnesses quantum mechanical phenomena as computing elements and has operating parameters sufficient to break some of today's most commonly used cryptographic algorithms in a short period of time. In some cases, the time to break a code is expected to be measured in minutes or hours. Much smaller and less able quantum computers exist today, but the creation of a CRQC is beyond the ability of current technology. However, tens of billions of dollars a year are being spent on research to achieve a CRQC. For decades, the question was "can the issues and technological barriers preventing the creation of a cryptography-breaking quantum computer ever be overcome". Now it is generally accepted that the question is "when" will the issues be solved. (ASC X9 Inc., 2022 – All Rights Reserved, 2022)*

In even simpler terms, Quantum Computing is a computer system that uses Qubits rather than the standard bits of a classical computer. Normally, a bit in a classical computer always has the value of zero or one (off or on) whereas a Qubit has an unknown value until it is measured. In comparison, the Qubit derives its value from a number of external stimuli and, due to its nature, a Quantum Computer can exploit certain characteristics of quantum mechanics to solve specific and highly complex math problems in a way that a classical computer cannot. Since all modern cryptography is based on solving these kinds of very complex math problems, it is a potential target for an adversary to be able to decipher even the best current cryptography.

Why is this important?

This matters to us since a large number of communications over public and private networks relies on cryptographically secure methods to protect the information contained in those communications. This includes information between systems (especially in today's modern micro-services environment) as well as information from web based and mobile based applications that communicate over the internet with processing servers via APIs.

Encrypted information can be thought of as valuable items in a safe. Assuming the safe is not otherwise able to be breached, only a single key can open that safe to retrieve the contents. An attacker would need that single key, or they would have to take key blanks and try every possible combination of grinding the key by hand, trying each one until something finally worked. This requires a lot of time, patience, skill, and a bit of luck. Applying that to encrypted information, if a key size was 256 bits, there is a possibility of 1.158e+77 (a very large number) of keys that would need to be tried to reveal the protected information. This is virtually impossible with today's classical computers, but soon, (some estimates are by 2030), commercially available Quantum computers will be able to find the "needle in the haystack" and be able to compromise and steal your protected information.

As we have seen, the secure mechanism for transmitting data over the internet (TLS) has been compromised multiple times. TLS V1.0 was published in 1999. In 2006, it was updated to TLS 1.1 due to security flaws. Just two years later in 2008, it was again updated with TLS 1.2. That was also replaced in 2018 with the current version of TLS 1.3. TLS 1.3 is currently not allowed through China's "Great Firewall" which is evidence that its security profile is an improvement, yet it still relies on underlying cryptography methods that will be in danger as Quantum Computing progresses.

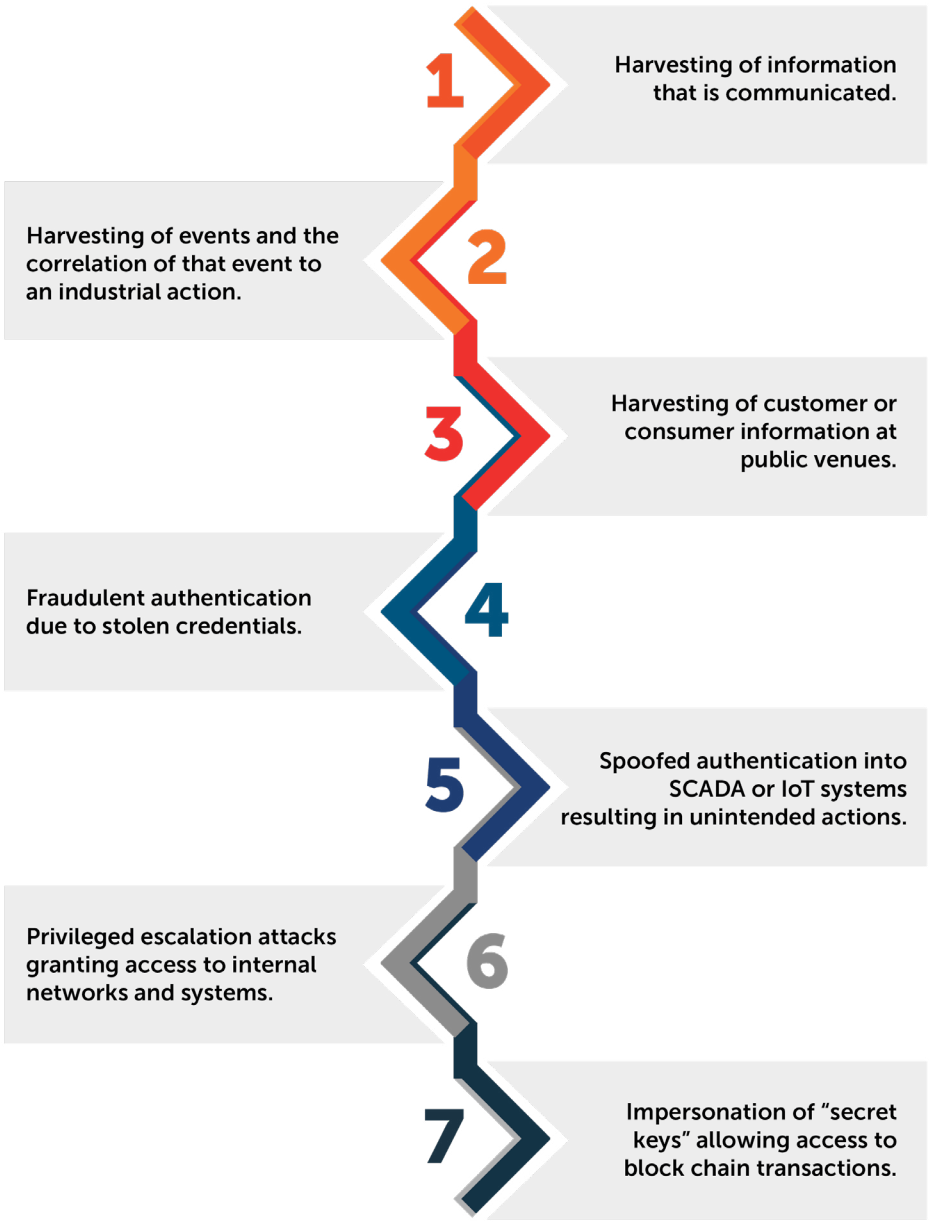
Fortunately, today, there are no Quantum Computers available to break the best current encryption. However, the amount of investment by nation-states (China, Russia, EU, England, The Netherlands, and the US) is staggering, so the question is not IF, but WHEN will this capability be available.

The above referenced document describes just how the current encryption methodologies are at risk. At risk ciphers such as 3DES, AES, RSA, ECC, DSA, and ECDSA are commonly used by application protocols like SSH, TLS, and IPSec. Secure web sites and applications use HTTPS and FTPS to exchange information which use one of these protocols. This makes most current "secure" web sites at risk. VPNs also rely on TLS and IPSec which makes them another target for compromise.

Every one of these rely on current encryption methodologies and can be compromised once Quantum Computers are readily available.

What is at risk?

Today's business world is highly connected and the information that we transmit over public and private networks is extremely valuable. Some of the risks that one must consider are:



All of these should be of concern to any enterprise today, and prudent organizations should begin to formulate a strategy to be prepared for these eventual scenarios.

What steps should I take?

The good news is that we have some time. Michele Mosca of the University of Waterloo has developed what is known as Mosca's XYZ Theorem. X is the shelf life of an asset or system that must be protected. Y is the amount of time we can estimate it will take to migrate the asset from a Quantum vulnerable technology to one that is safe. Z is the amount of time we feel before a Cryptographically Relevant Quantum Computer (QRQC) will be able to compromise the asset. If X + Y > Z, then we have a problem. However, we must also factor in the legal, financial, and reputational risk of a system. Some systems may not pose any substantial risk, and migration of these might not be necessary. Some systems will not be able to migrate due to underlying technologies and their age – these systems (if they contain high value information) may need to be targeted for replacement. Deciding which systems or assets to focus on is a risk-management decision that should be evaluated with senior management at an enterprise.

The steps one could take in protecting from future risks of disruption by Quantum Computing should roughly follow this process.

1. Assemble a team of researchers and engineers to form a working group that is tasked with addressing these risks for your organization.
2. Gain a general understanding of Quantum Computing and its potential impact on information security (start by reading the referenced document).
3. Research available tools and techniques for future protection.
4. Conduct an inventory of all assets and systems that may require better protection – this involves cataloging the current methods that these systems use.
5. Prioritize these based on Mosca's XYZ Theorem, the risk of exposure, and your own perceived risk tolerance.
6. Determine which tools (from step 3) are appropriate for which risks (from step 4).
7. Authorize Proof of Concept (POC) projects on your most valuable and vulnerable assets from step 5.
8. You may need to try multiple POCs using various tools to find which combinations will provide the best protection at a reasonable investment.
9. Plan for and execute the various projects to take your most vulnerable and important assets to a new level of protection that will be future proofed from the adversaries that will acquire Quantum Computing power in the near future.

This process is not without some expense, but that must be weighed against the consequences of doing nothing and in a few short years finding your organization in a compromised position with valuable assets stolen and used against you and / or your customers.

How can Eclypses help?

Eclypses has a patented, FIPS 140-3 validated solution (Eclypses MTE) that can easily be incorporated into not only new, but existing legacy systems. This technology protects data in transit at an application level making that information totally obscured to any attacker. It is an excellent addition to the list of tools gathered in Step 3 of your process as it resistant to the commonly known techniques that an attacker with quantum capabilities may have.

Even today, attackers do not always just attempt to break into real-time communications, but they quite often use a “Harvest-and-Decrypt Attack” where data is captured, analyzed, decrypted, and then used for various attacks at a later date. Eclypses MTE uses instantly obsolete token replacement to ensure that no discernable pattern can be discovered and that replay attacks (as in Harvest, Decrypt, Reuse) are totally useless. For more information, contact us at www.eclypses.com and request an in-depth discussion.

ABOUT ECLYPSES

Eclypses has a disrupting cyber technology, offering organizations with an advanced data security solution not seen in today's environments, called MTE®.

Founded in 2017, Eclypses originated as a subsidiary of Secure Cloud Systems, Inc. with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies, websites, and IoT devices. The development of this technology led to the MTE toolkit, as we know it today.

Eclypses' patented MTE technology was developed through their technical team in Colorado Springs, CO, where they continue to innovate and expand on this cutting-edge security technology. The MTE technology generates a random string of values that is used to replace any form of structured or unstructured data. This replacement string of values is referred to as MTE, which provides innovative security against man-in-the-middle cyber-attacks.

This technology allows for a higher level of security to protect against man-in-the-middle cyber-attacks in products and applications that may have limited resources, such as battery life, processor, or throughput.

CONTACT

contact@eclypses.com
www.eclypses.com
(719) 323-6680