How Quantum Computing is having a significant impact on Cyber Security

Nichita Maftei k2205319

Kingston University

1. Introduction

In an ever-growing online world, privacy and security are important but have been increasingly harder to protect. Data breaches exposed 22billion records in 2021 (Sobers, 2022). In an effort to protect transactions, data, passwords, records etc. The Cybersecurity sector has been evolving in conjunction with computers and their advancements. However, recent breakthroughs in Quantum Computing could shake the very foundation of today's Cybersecurity sector.

This report will explore how quantum computers will shape the future of online security. In section 2, the report explains what a Quantum Computer is and how it differs from classical computers. In section 3, the report goes into detail on how quantum computing can help encrypt data more securely than if we used classical computers. In section 4, the report goes in-depth about the risks Quantum Computing poses towards the security of current encryption. In section 5, there is a discussion on how quantum computing is in its early stages of development and how there are much-needed advancements before Quantum Computers will be used commercially in firms that would benefit.

2. What are Quantum Computers and how do they differ from classical computers?

Following the creation of the first computer in 1951, computer scientists have been improving computers exponentially. Their speed, power and efficiency have been doubling every one and a half to two years since the 1960s and 1970s (McCain, 2022) Although we continue to make transistors smaller and smaller, the core way in which computers operate at their most basic level has remained the same. However recent breakthroughs in Quantum Computing have been gaining traction. Quantum Computers calculate with Qubits which can be 1 and 0 simultaneously, qubits can also be entangled where a change in one qubit can directly affect the other (Dilmengani, 2022). These properties allow them to do several calculations at the same time, unlike long-established computers. This means Quantum Computers can drastically outperform certain tasks compared to traditional computers.

3. Benefits of Quantum Computers in Cyber Security

One benefit of Qubits is that it can be used for Quantum Key Distribution (QKD) (Idquantique, 2022), this is a more secure alternative to the traditional Public Key encryption which we use in today's world. This works by using the Observer effect, which happens when the observation of quantum operations affects their outcome (Bonderud, 2022). QKD is significant in Cybersecurity as the messenger and receiver of a message sent using QKD can know if their message has been

compromised as the state of the photos would have changed when observed by an attacker. This will massively improve upon existing Cybersecurity technology as classical computers could guess private keys and find ways around encryption but if attackers even attempt to view the message it will be rendered unreadable. Incorporating this new technology into today's cyber world will ensure major firms will not be the victim of large data leaks and help keep the public confidence in our financial sector. Everyone in society benefits from stronger defences put in place in order to prevent anything on the internet from being taken or ransomed.

4. Risks Quantum Computers poses to Cyber Security

A huge part of Cybersecurity is built on cryptography to which quantum computers pose the biggest threat. Cryptography is the most significant barrier between sensitive health, financial, and personal information. Almost all sensitive data shared over the internet is encrypted using Public Key Encryption, it is the most common form of internet encryption, built into every web browser and used by almost all organisations to secure their personal data (Bitdefender Enterprise, 2021). Public key encryption can be brute forced by traditional computers. However, it would take several months, years and beyond; it would take supercomputers a fraction of the time. This is because classical computers can do one calculation at a time, whilst quantum computers can do multiple calculations with multiple inputs at the same time. Given that public key algorithms such as RSA safeguard nearly the $4 Trillion Ecommerce Industry (Bonderud, 2022), it is likely that since Quantum Computers could break these algorithms orders of magnitude quicker than binary computers, it could pose a threat to financial systems like banks and even national security without proper precautions and misuse of this technology, it could be used not only for personal gain, but governments could weaponise this technology for espionage etc.

5. Quantum Computing is still in its infancy

Although Quantum Computing can help but also break our security, the truth is, it needs significantly more research and testing before ever making it for commercial use, even for huge firms, let alone for personal use. For example, a massive problem is that Quantum Computers are huge and very delicate, they are extremely sensitive to their surroundings like dust and temperature. Currently, quantum computers need to be stored at around 25mk (Irving, 2022) in order to function optimally. Moreover, Quantum Computers won't be available to the general public for the foreseeable future meaning that attacks using this technology won't instantly disrupt security in the entire web ranging from organisations to governments to regular citizens.

6. Conclusion

This report has provided a discussion on the risks Quantum Computing poses to Cybersecurity, and how this new technology has the ability to crack current widely adopted encryption methodologies and the significant consequences this has as a result. On the other side of the spectrum, this report has also discussed how we could utilise Quantum Computing to further improve our current encryption methods, to significantly protect against current ways in which hackers gain access to data.

In order to prevent a surge in significant cyber-attacks, it is the duty of lawmakers and the tech companies such as IBM to ensure that Quantum Computing doesn't get into the hands of the public in an effort to sustain the confidence of the public in every sector going digital.

References

Bitdefender Enterprise (2021) *How Quantum Computing will impact Cybersecurity*. Available at: https://businessinsights.bitdefender.com/how-quantum-computing-will-impact-cybersecurity (Accessed: 25 October 2022).

Bonderud, D. (2022) *Quantum Computing: How Qubits Could Change the World of Cybersecurity*. Available at: https://www.spiceworks.com/it-security/cyber-risk-management/articles/will-quantum-computing-change-cybersecurity/ (Accessed: 25 October 2022).

Dilmengani, C. (2022) *Quantum Entanglement: What is it & why is it important?* Available at: https://research.aimultiple.com/quantum-computing-entanglement/ (Accessed: 26 October 2022).

Idquantique (2022) *Quantum Key Distribution*. Available at: https://www.idquantique.com/quantum-safe-security/quantum-key-distribution/ (Accessed: 25 October 2022).

Irving, M. (2022) *IBM builds huge super-fridge colder than space to chill quantum computers*. Available at: https://newatlas.com/computers/ibm-goldeneye-super-fridge-quantum-computing/ (Accessed: 22 October 2022).

McCain, A. (2022) *How fast is technology advancing? [2022] Growing, Evolving, And Accelerating at Exponential Rates*. Available at: https://www.zippia.com/advice/how-fast-is-technology-advancing/ (Accessed: 21 October 2022).

Sobers, R. (2022) *166 Cybersecurity Statistics and trends*. Available at: https://www.varonis.com/blog/cybersecurity-statistics (Accessed: 26 October 2022).