Cybersecurity and Cyberattacks: Creating the Impenetrable Bunker

Author: Haitian Huang

March 3, 2022

Author Bio: As of March 2022, Haitian Huang is 17 years old and is a high school junior. He has been fascinated with technology at a very young age and likes to tinker with technology. His passion for technology has led to many areas of pursuit in STEM fields. These include taking his school's most rigorous STEM courses, qualifying for the American Invitational Mathematics Examination through the American Mathematics Competition 12, winning Science Olympiad awards for many events, including Circuit Lab and Codebusters, leading the school math club to success in Math League, leading the app design club to create meaningful group projects, creating a technology YouTube channel and newsletter, while also leading a group to inform the

community about technology, helping to teach a Java programming class, as well as conducting independent research and writing a research paper on the effects of artificial intelligence and quantum computing on cybersecurity and cyberattacks.

Abstract

This paper attempts to analyze the different types of cybersecurity measures currently in use, as well as the different types of cyberattacks that currently pose threats, through observing significant trends, like those of technological advancements, including artificial intelligence and quantum computing. In addition, it aims to determine the potential strengths and weaknesses of current cybersecurity measures, like AES and RSA, and cyberattacks, particularly methods based on the emerging fields of artificial intelligence and quantum computing, like reinforcement learning and Shor's algorithm. Finally, using the information obtained through the research and analysis, the paper works towards providing further insight into what can be done to improve current cybersecurity for a more secure digital world for all, despite all the potential threats technological advancements could bring. The results show that using similar AI and quantum techniques in a different way could be effective in improving cybersecurity due to the nature of the methods.

Keywords: Cybersecurity, Cyberattacks, Artificial Intelligence, Quantum Computing, Reinforcement Learning, Shor's Algorithm, Threats, Improvement

Introduction

In the advent of the information era pioneered by computer related technologies, many different cybersecurity measures have been created to protect sensitive data. Some are encryption ciphers, like RSA (Rivest-Shamir-Adleman), an asymmetric cipher based on prime numbers, and AES (Advanced Encryption Standard), a symmetric block cipher based on permutations, while others are networks centered around cybersecurity, like Tor (The Onion Router), an anonymity centered network based on multiple layers of encryption (McKay, 2021). However, where there is security there is an attack to compromise the protected system, giving rise to many different cyberattacks. Some examples include worms, based on exploiting holes in cybersecurity by replicating itself to spread to other computers, ransomware, based on demanding ransom for encrypted data, and operating principle attacks like Spectre, based on exploiting the training nature of the branch predictor of the CPU (Central Processing Unit), which predicts what the CPU will need for future tasks to improve efficiency. Due to the interconnectedness of cybersecurity and cyberattacks, it is necessary to analyze them together to further improve cybersecurity in the future, which this study aims to achieve.

Status

The current status of cybersecurity appears stable, without too many major breakthroughs like achieving complete current cybersecurity or cracking current encryption methods. However, that does not mean that there is not potential for significant improvement or significant danger, as technology is one of the fastest changing industries. There is always the possibility that some under the radar cybersecurity researcher comes up with a way to achieve complete current

cybersecurity or some unknown cyberattacker creates a way to get around current encryption methods. The possibility of drastic change is the nature of the extremely volatile technology industry, and as a result the cybersecurity industry, where cybersecurity workers and cyberattackers fight for domination. Two potential threats to the apparent stability of the field of cryptography are quantum computers, threatening from the hardware side due to its exponentially increasing nature of computing power, and artificial intelligence, threatening from the software side due to its much more efficient attack creation and refinement potential. Now that the use of cryptocurrency is on the rise, as well as the number of people interacting digitally using computers, digital security is becoming increasingly important for everyone.

Motivation

There are many things that motivated the following research on cybersecurity measures and cyberattacks, including past experiences, previous research, and circumstantial motivators to varying degrees. Previous research that motivated the research include many years of learning about the inner workings of computers and how all the different parts, from hardware to software and everything in between, come together to create a functional and effective electronic computer. Tinkering with obtainable components of computers and conducting extensive online research provided the background knowledge and interest in technology that greatly influenced the research. In particular, the enthusiasm and knowledge of technology media content creators motivated and supported me to continue pursuing more knowledge in the field, starting from the very first video watched. Circumstantial motivators that motivated the research include an unexpected online code breaking challenge with potential technology related rewards that gave

exposure to many technology related fields, mainly problem solving using techniques in the field of cryptography, like decoding messages encrypted with many fundamentally different ciphers, observation skills like finding hidden aspects of a problem by looking at it from a different perspective, and synthesis skills like piecing together the full intention of a puzzle through gathering multiple hidden clues. Solving these challenges with an enthusiastic and dedicated community provided the more specific background knowledge and interest in cryptography that made the research possible, as well as increasing the interest level. Finally, there were also past experiences that motivated the research, which include winning an award for the Science Olympiad cryptography event that provided deeper understanding in how different types of ciphers work, including both historical substitution ciphers and current encryption ciphers like RSA. Researching the working principles of many historic and current ciphers provided the fundamental cryptography knowledge and motivation that helped drive the research forward. A core component of the motivation for the research was the fact that there were many different cases of cyberattacks of varying levels of severity over the years that together affected a large number of people, like the Colonial Pipeline ransomware attack, warranting extra research to help the world become more secure and a better place to live.

Methods

The research was conducted through extensive online research, with the general idea being to essentially attempt to analyze current cybersecurity measures, thoroughly dissect the potential cybersecurity threats, and come up with a method to counter those threats. The online research was based on past research and analysis done by others, as well as past trends observed,

creating a foundation for this research to be built on. It mainly involved using a large amount of data from many different sources to draw deep, meaningful, and informative conclusions, as well as thoroughly understanding emerging technologies that could potentially be catalysts for change, among many other things.

Discussion

It was found that a likely software technique that could cause a monumental shift in the technology industry is the relatively new artificial intelligence, a superset of machine learning that was used for this research, and a likely hardware invention that could cause a monumental shift in the technology industry is the relatively new quantum computers, which employs quantum states instead of binary. Both possibilities arise because they both fundamentally change the way technology is thought about and used, making them extremely potent catalysts of change in the industry.

For artificial intelligence, it has the potential to make cyberattacks much more efficient in the future by allowing the cyberattacks to first practice on training targets to improve its effectiveness through reinforcement learning using deep learning neural networks, similar to how AlphaGo by Google worked (See Figure 1), among other techniques before targeting a larger scale target like important servers without requiring the full time and attention of the attacker (Granter et al., 2017). Basically, it could be possible to create a system in which the attacker can create a project to attack a specific target that they have in mind, like a large social media company's server, and once they have the fundamental core and structure working, they could rely on verification and modification that could be implemented by the cyberattacks themselves,

among other benefits, instead of needing to do all the tedious checking and improving themselves. This approach makes it possible for the attackers to make a much more dangerous and destructive cyberattack in a lot less time with minimal effort. It could work somewhat like how current email spam detection works by learning keywords that are likely to be spam in emails (See Figure 2), but for cybersecurity vulnerabilities instead, found through analyzing trends that could hint at what current and future trends could be. Essentially, the machine learning could enable the cyberattack to learn the likely vulnerabilities that either have not been found yet or have not been patched yet through analyzing trends of certain metrics, like the type, location, and reach of the vulnerability, to name a few. It makes sense that cyberattacks could work better using these techniques when compared to not using them, as cybersecurity measures like previous methods of spam detection that did not use machine learning were evidently not nearly as effective as current methods of spam detection that do, and the interconnectedness between cybersecurity and cyberattacks suggest that there is not an inherent roadblock in using similar machine learning techniques in reverse to better cyberattacks instead. Currently, cyberattacks are only tailored for a specific target, like a particular operating system, particular hardware configuration, or a particular network, giving them limited reach. Examples include Spectre and Meltdown, extremely dangerous attacks that compromised the data of many through exploiting the way CPUs increase their effectiveness and efficiency through proper memory allocation, prediction, and management. Impactful as these types of attacks may be, they cannot be easily transformed to effectively attack a different type of system, requiring a lot of effort on the part of the attacker. However, due to the self-improving nature of reinforcement learning, that could be in the past since the attack could figure out some possible solutions instead of relying

solely on the attacker. Despite the possible increased difficulty of creating a self-adapting attack, once it is achieved, the update cycle will be much facilitated, compromising the cybersecurity of everyone (Soni, 2020).

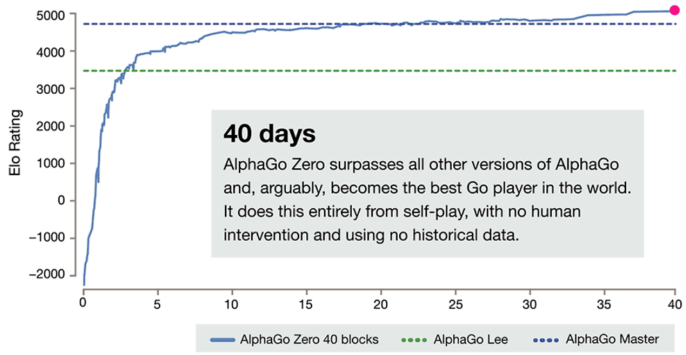

Figure 1: AlphaGo Zero Learning Speed Extremely High, Thanks To Reinforcement Learning (Silver & Hassabis, 2017).

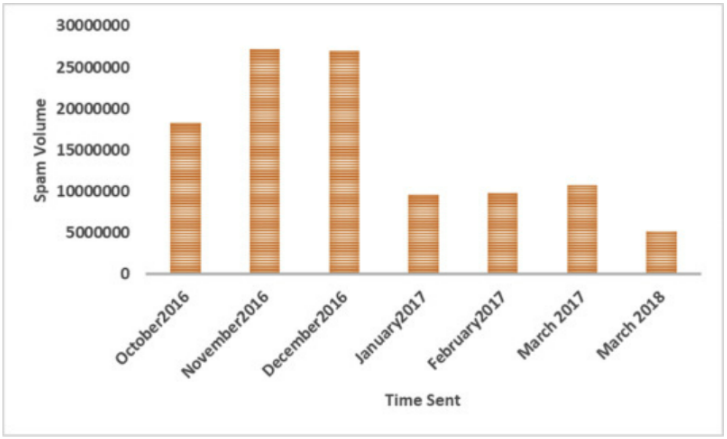

Figure 2: Spam Email Volume Seeing Downward Trend, Likely Due To Lowered Incentives For Spamming Caused By Improved Spam Detection Methods (Dada et al., 2019).

For quantum computers, they have the potential to make cyberattacks much more effective in the future by making it much more feasible to brute force attack current encryption ciphers, like RSA and AES, that mainly rely on the difficulty of effectively implementing a brute force attack through using very large quantities with a very large number of possible outcomes.

The main reason quantum computers are a threat is because of a quantum computer's ability to store 2 bits simultaneously in a single qubit, exponentially increasing computing power with respect to the number of qubits (See Figure 3), thanks to the underlying principles of quantum superposition, interference, and entanglement (Fischer, n.d.). Basically, since quantum computers do not have the same limitations as binary computers due to them relying on quantum mechanics, their computing power can scale up much quicker, making it extremely dangerous to the current encryption methods that rely on current computers not having enough raw computing power to effectively brute force attack, as it is very possible that quantum computers will have enough raw computing power to achieve a successful brute force attack. Further, through the use of Shor's algorithm, quantum computers can become even more effective at cracking encryption methods that rely on prime factorizing extremely large numbers (See Figure 4), like RSA, as it can be implemented such that the undesirable results are eliminated by the noise of the quantum computers and other techniques, leaving only the desired results, further compromising the security of everyone that uses computers for sensitive information (Reich, 2019).

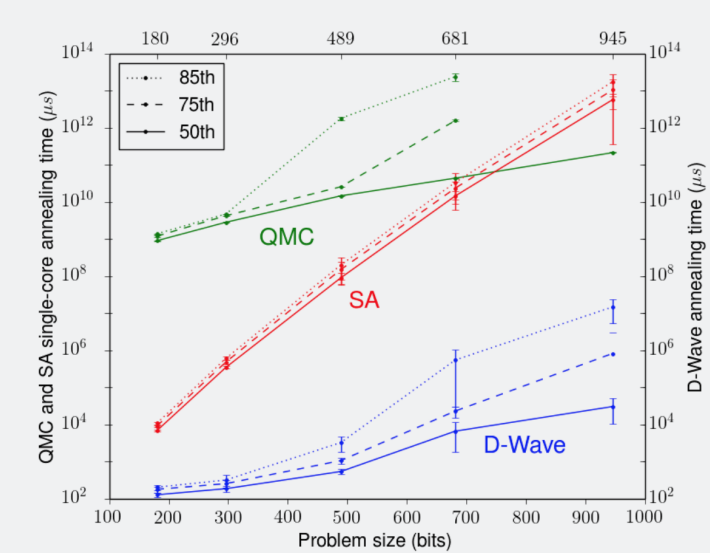

Figure 3: Multiple Binary And Quantum Computing Methods Working On Identical Computational Tasks, QMC Traditional Quantum, SA Classical Binary, D-Wave Quantum Annealing, Shows Quantum Speedups (Anthony, 2015).

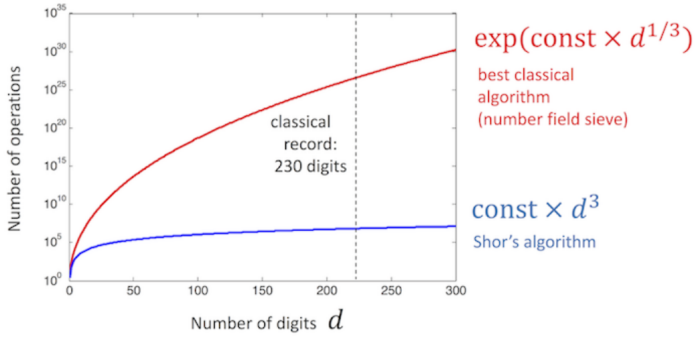

Figure 4: Classical Binary Computer Using Number Field Sieve Compared To Quantum Computer Using Shor's Algorithm Demonstrates Much Higher Efficiency Going Quantum (IBM, n.d.).

It was also found that historically, cyberattacks that target a specific group of people (like a large oil company that millions rely on) with a specific goal in mind (like taking the personal information from millions of people through compromising a large social media platform) are generally a lot more dangerous, likely because the attackers can better fine tune their attack and home in on the vulnerable loopholes and weaknesses in a security system. It was shown that an attack being widespread was also an important factor in its success potential. Additionally, the

attack's stealth was also very important. These trends are shown by infamous attacks like the WannaCry ransomware encryptor, the Stuxnet worm, and the Spectre attack (Cisco, 2022). All these attacks were extremely dangerous due to their extremely high transmissibility and extremely focused targets while remaining hidden until it was too late. Furthermore, it is important to note that as the internet increases in usage, the sheer amount of data that is required to be protected will increase as well, increasing the amount of computational power needed to protect all that data. If a clever loophole was found around the cybersecurity measures that was extremely efficient, like an attack method that implemented quantum computing with Shor's algorithm in conjunction with an extremely adaptable reinforcement learning improvement cycle, it can be conceivable that an entire group of data that utilizes RSA as its main encryption method collapses due to the attack. It wouldn't even necessarily need to scale up in computational power as much as the encryptor does (Dupont, 2013).

As to what could be done to improve current cybersecurity measures, one obvious way would be to counter the features that make cyberattacks so deadly, efficient, and effective, namely restricting access to important data by putting it behind more layers of security than other data and putting them in different locations to make it more likely to be overlooked when the other data is breached, similar to Tor but at the hardware level, directly countering the high transmissibility, focused targeting, and the hidden nature of the attacks. This would also more effectively thwart artificial intelligence-based attacks by confusing it in terms of where to look for vulnerabilities. Regarding the encryption methods themselves, one important thing to be improved upon is to not only make it extremely computational heavy, difficult, and time consuming to crack using standard binary computers, but also make them hard for newer

quantum computers by exploiting their weaknesses, like exploiting the relatively large amount of noise of quantum computers by purposely making the protection stronger when there are higher amounts of noise and computational error, for example, one way to counter quantum computing attacks implementing Shor's algorithm. A clever solution would be to use the attack design structure in reverse, essentially using quantum computing and artificial intelligence for bettering the cybersecurity system instead of the attack.

Future Work

Now that deeper research has been conducted on how cyberattacks compromise the cybersecurity in the digital information age and how quantum computing and artificial intelligence further threatens cybersecurity, as well as possible solutions, a logical direction to go would be to create a measure of how devastating a cyberattack is. Essentially, create something similar to the Common Vulnerability Scoring System, or CVSS, for the cyberattacks themselves instead of the vulnerabilities they exploit, allowing a gauge of not just the vulnerabilities' severity levels, like the recent Apache log4j, but also allowing a gauge of the cyberattacks that exploit them, like the VMWare hack by Conti ransomware. The process could be aided by machine learning, using machine learning techniques like linear regression, for analyzing the data, and gradient descent, for optimizing the function, coming together to provide an accurate and precise evaluation of how dangerous a cyberattack is. Data sets could be input into the machine learning algorithm, which then improves, allowing it to create more meaningful results. More specifically, the analyzing functions could take in many different variables with many different weights, like similarity to past methods (trojan delivery method, ransomware delivery

method, spyware delivery method), total effective coverage, and target size, and create outputs that represent the level of effectiveness of the cybersecurity measure or cyberattack, with a separate function to analyze each based on the input. Each function could aim to predict relatively accurately (within 5% of a 100% scale) what the effectiveness level would be of its specific input, using data sets of many cybersecurity measures and many cyberattacks with their corresponding information.

Conclusion

Two major threats to current cybersecurity measures include the use of artificial intelligence from the software standpoint and quantum computers from the hardware standpoint, due to their radically different approaches to technology. More specifically, reinforcement learning of cybersecurity vulnerabilities could facilitate the making of more potent cyberattacks, while quantum computing with Shor's algorithm could make brute force cracking current encryption methods feasible in a reasonable time frame. In addition, despite cyberattacks that have the properties of high transmissibility, high target focus, and high stealth being more devastating, they can be countered by putting important data behind extra layers of differing security, both hardware and software, and in more different locations to increase the likelihood of being overlooked by both current cyberattack methods and reinforcement learning of cybersecurity vulnerabilities. Preventing quantum computers from breaking current encryption methods with their extremely high processing power used in tandem with Shor's algorithm could be achieved as well, potentially by exploiting their weaknesses of relatively high noise and thus chance of computational error through making it more difficult to breach cybersecurity measures

when errors occur. In conclusion, reinforcement learning of cybersecurity vulnerabilities and quantum computing with Shor's algorithm may pose significant threats to current cybersecurity, but if proper adjustments are made, they can be conquered, just like the many previous cybersecurity hurdles in the past.

References

Anthony, S. (2015, December 9). *Google, NASA: Our quantum computer is 100 million times faster than normal PC*. Ars Technica. https://arstechnica.com/information-technology/2015/12/google-nasa-our-quantum-computer-is-100-million-times-faster-than-normal-pc/

Cisco. (2022, February 24). *What Is a Cyberattack?* Cisco. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#%7Etypes-of-cyber-attacks

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

Dada, E. G., Bassi, J. S., Chiroma, H., Abdulhamid, S. M., Adetunmbi, A. O., & Ajibuwa, O. E. (2019). Machine learning for email spam filtering: review, approaches and open research problems. *Heliyon*, *5*(6), e01802. https://doi.org/10.1016/j.heliyon.2019.e01802

Dupont, B. (2013). Cybersecurity Futures: How Can We Regulate Emergent Risks? *Technology Innovation Management Review*, *3*(7), 6–11. https://doi.org/10.22215/timreview/700

Fisher, C. (n.d.). *IBM | What is Quantum Computing?* IBM Quantum. https://www.ibm.com/quantum-computing/what-is-quantum-computing/

Granter, S. R., Beck, A. H., & Papke, D. J. (2017). AlphaGo, Deep Learning, and the Future of the Human Microscopist. *Archives of Pathology & Laboratory Medicine*, *141*(5), 619–621. https://doi.org/10.5858/arpa.2016-0471-ed

IBM. (n.d.). *Shor's algorithm*. IBM Quantum. https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm

Kaur, J., & Ramkumar, K. R. (2021). The recent trends in cyber security: A review. *Journal of King Saud University - Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2021.01.018

Li, S. S., Long, G. L., Bai, F. S., Feng, S. L., & Zheng, H. Z. (2001). Quantum computing. *Proceedings of the National Academy of Sciences*, *98*(21), 11847–11848. https://doi.org/10.1073/pnas.191373698

McKay, D. (2021, July 27). *What Is Encryption, and How Does It Work?* How-To Geek. https://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/

Nadikattu, R. R. (2016, December 15). *The Emerging Role of Artificial Intelligence in Modern Society*. Papers.ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3652429

Reich, H. (2019, May 1). *How Quantum Computers Break Encryption | Shor's Algorithm Explained*. YouTube. https://www.youtube.com/watch?v=lvTqbM5Dq4Q

Silver, D., & Hassabis, D. (2018, February 14). *AlphaGo Zero: Starting from scratch*. Deepmind. https://deepmind.com/blog/article/alphago-zero-starting-scratch

Soni, V. D. (2020). Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3624487

Wallden, P., & Kashefi, E. (2019). Cyber security in the quantum era. *Communications of the ACM*, *62*(4), 120. https://doi.org/10.1145/3241037