Worrying Cybersecurity Security Concerns: The Present and Future

Dylan Anderson

01172654

POLS426: Cyber War

The internet since its creation in the early 1980s has undergone rapid innovations and changes. Comparing the internet and our technology from now to a few years ago and it's astounding how fast innovations are coming. With these rapid innovations and the age of the internet of things with all sorts of devices being connected to the internet, cybersecurity and internet security practices must maintain and be ahead. This has not been the case however, during our rapid innovations to the internet and massive technological creations, computer and cybersecurity became a footnote for a long time. Though as the internet has begun to become further understood, cybersecurity attention and avocation has begun making the attempt to catch up.

While most know cybersecurity encompasses security for all devices connected to the internet, be that computer, mobile phone, toaster, etc; most do not know cybersecurity also encompasses safe internet habits and proper internet security understanding. This less known aspect of cybersecurity is one of the most direct links towards one of the most common types of cyber crimes: cyber attacks. Cyber attacks involve any malicious intrusion into a computer system or network to either steal or destroy data. These intrusions known as breaches or hacks into systems can be done in a multitude of ways. The most common intrusion method being malware, which will be gone over in more detail later on. To better understand why cyber attacks so frequently, it must first be understood the existing security concerns that allow these cyber attacks to occur.

One of the most common security weaknesses and concerns is little to no security in place whatsoever. If there is no security or open ports and weak firewalls, cybercriminals have free reign over the system and network with little to no effort. Public connections with no

passwords are also extremely unsafe and pose a threat to the business and the public who actively uses them, as they are prone to be monitored by malicious users looking for personally identifiable information. As our society shifts to the internet of things with millions of connected, unsecured devices, the general public has become extremely more susceptible to cyber attacks from anywhere (Abdalrahman, 2023). These open ports, unsecured networks along with most cybercriminals' intrusion method of choice, malware, have made cyber crimes rise to an unprecedented level.

Malware, software created to either damage or gain access to a computer, is sprinkled through random pop ups and downloads. Most malware is sent without targeting a specific network or computer and can be found and destroyed with simple antiviruses, but is so widely sent throughout the internet, websites, and emails, that enough devices will be infected. Malware usually comes in three forms: Spyware, the most common type of malware usually found, which monitors infected systems for personal information; Viruses, which spread and infect themselves throughout a host device and usually destroy devices; and Worms, which can survive without host systems and spread drastically through networks and systems (Abdalrahman, 2023).

It can be argued both of these main security concerns all stem from the biggest security concern which cannot necessarily be fixed is human error. As it is known, human beings aren't perfect, and will constantly make mistakes. Computers and devices, if created correctly, will not make mistakes, as most problems originate from the human being operating them. Human error as the name suggests is an unintended action performed by a human being either through negligence, manipulation, or a multitude of different reasons as to why a mistake was made. In

a 2014 IBM Security Services Cyber Security Intelligence Index report, it was found that human error played a role in more than 95% of all security breaches as opposed to those caused strictly by unanticipated vulnerabilities in system security (Coffey, 2023). In terms of cybersecurity, human error results in cyber attacks through two main ways: negligence and social engineering. Negligence involves the overlooking of a mistake like either an unseen breach into a system, irregular event logs or system activity, outdated software, and downloading of unsafe file attachments. These are usually not out of spite, but either through boredom and laziness. A far more malicious method of human error, known as social engineering, which malicious entities manipulate a specific employee of a targeted entity to either make the target reveal information, or allow access into the target system through malware. One of the best examples of human error which encompasses both types of human error is phishing. Phishing involves duping a target into entering login details or other access credentials into an email that is made to look like it is either from the company, ceo, or a partner company. This type of human error was placed as the most common type of incident at 34%, with other employee errors and actions accounting for 24% of all incident reports in a 2016 report by BakerHosteler's (Coffey, 2023). Again, human beings are not perfect and human error can not be fully stopped unless humans are taken out of the question of cybersecurity and defense, though human error can be mitigated.

Though what if there was a way to almost completely mitigate human error across the board? Enter artificial intelligence. Artificial Intelligence (AI) in the past few years has undergone extreme advancements and innovations leading to extremely worrying computer security concerns in the future. While AI is currently being used for jokes and to write papers, it has

already grown enough to be able to accurately mimic human voices, write code, and text documents which accurately convey a person's writing style or topic. It's important to note that AI is still in its infancy, think about how highly advanced AI may become in 5 years time. It's entirely possible all forms of cybersecurity both defensive and offensive, criminal and warfare may be through AI.

Before talking about the potential benefits of AI towards cybersecurity, it's first important to realize how new cyber attack methods and updates to existing intrusion methods can be made. On the aspect of social engineering, AI can almost perfectly recreate human voices, paired with hard to hear phone calls, ill-informed workers and personal information from anyone can be accidentally given to malicious vendors. Highly accurate phishing emails can be made that suit the company being targeted. These phishing emails, which normally are hard to exactly replicate from human attackers, can quickly and accurately be made through AI, and mass sent to companies differing just enough to not cause alarm. AI can also accurately recreate studied behaviors, creating personalized phishing emails suited to each target. Theoretically, if anyone has access to AI, they can launch a cyber attack through the creation of code without any knowledge of coding. This AI is indispensable in allowing hackers who wouldn't have the knowledge or access to commit cyber crimes they wouldn't have ever been able to before.

AI also can currently be used for cyber defensive strategies that humans cannot currently detect and prevent. AI can constantly and accurately monitor computer systems and can detect extremely slight disturbances which humans would not be able to. Take for example a type of AI cyber defensive technique known as a Conventional Neural Network (CNN). The neural network is a feed-forward type of network which can respond to surrounding elements.

This model can potentially detect malware through slight disturbances in the network almost invisible to humans (Li, 2019). These tools can also be used to fix most of the current pitfalls in cybersecurity, those being the low detection and response rate. A currently used model in cybersecurity is the Artificial Neural Network (ANN) which seeks to imitate the function of the human brain. Regarding cybersecurity, ANNs have been used to encapsulate the entire cyber kill chain and network traffic (Wirkuttis, 2018). It cannot be overstated the sheer speed AI is able to perform these functions and detections compared to how methods are used now.

One of the current pitfalls of AI currently is the lack of autonomy and inability to make some human decisions, requiring human intervention to operate efficiently (Wirkuttis, 2018). Though in the distant future, it's entirely possible for these AI to run completely autonomously. In a hypothetical but entirely possible future world, systems would be run by these AI which would defend, monitor, and scale systems against other AI. AI would be used by both sides to breach into networks through millions of possible methods all of which must be prevented quick enough by defending AI.

It is imperative that AI is properly regulated, secured, and monitored in its own right in cybersecurity to better prevent security risks. A few things to take important notice of is data collection, and AI code. The data collection and analysis the AI uses must be relevant to the defensive strategy, have an expandable amount of data, variety, and accurate velocity of data reading. It is important that these four ways of reading in AI for the defensive strategy constantly increase as the AI expands. While this makes sure created AI accurately and optimally works within its bounds, it is also extremely necessary for the code of the AI to be properly secured. If your AI is able to be intruded upon and changed by malicious actors and then

construed into something potentially harmful, it will pose extreme challenges to both a company and many more. Take for example an AI which is used to monitor an entire cloud system network. This monitoring AI was maliciously changed to harmful malware throughout the cloud network to the system itself and any consumers who used the cloud service. This monitoring AI has also been changed to report normal behavior with this breach essentially being invisible. If this breach was ever detected, not mentioning the ramifications of a cloud service sending malware for who knows how long to millions of other systems, it's possible the AI has so completely rooted around it that it may not be fixed. What is a way to mitigate this? That is with the addition of human monitors of the AI to notice discrepancies and to report and fix them. Another way is to properly secure AI with up to date encryption methods, some common ones currently being RSA and AES-256 bit encryption to name a few.

Regarding encryption, a potential future security concern may break our current best encryption methods. Our current society fundamentally relies on encryption methods that are practically impossible, but theoretically possible to break (Kirsch, 2015). That new worrying concern is the advent of quantum computing. Quantum computing in the most basic sense, allows for calculations extremely quicker than a normal computer. This is due to how a quantum computer works. A current computer solves most problems one at a time, however a quantum computer is capable of solving a multitude of problems simultaneously. A quantum computer can factor a 300 digit number in the same amount of time that an ordinary computer could multiply the factor together (Kirsch, 2015). In essence all current forms of encryption are impossible to break through brute force due to the time it would take a computer to decrypt the code, however with the extreme processing power of quantum computing, these

brute-force attacks are able to be completed extremely quickly. With quantum computing, our current methods would be just about as effective as holding the door open to your house with a “rob us” sign out front with blinking lights. It is also important to note due to how much quantum computing is still in its infancy, most attacks considered are guess work. Some potential concerns of cyber attacks using quantum computing are time lag between incident and response, interceptions, and most algorithms for destroying our current encryption methods will be finished by the time quantum computing is a reality. Time lag involves how long it takes from an incident to be reported and how quickly it is responded to, patched, and fixed. In this window of time, the system is still extremely vulnerable. With the advent of quantum computing, this vulnerable technology may be stuck in an extreme time lag. It is theorized most quantum computing attacks will be interceptions of messages without notification to either party of the message being viewed by a third party. This would make almost all messages sent from anywhere to anything unsecure and unsafe. It is also possible these interceptions could be taken from almost anywhere, not just messages between two human parties. Take for example authentication servers with login details or credit cards. Almost anything would have a high degree of uncertainty. Mathematicians are already currently devising quantum algorithms to breach some of the most widely used encryption methods, RSA and ECC (Kirsch, 2015). By the time these algorithms are finished, it is extremely likely we will be on the cusp of finalizing quantum computing.

Why are our current encryption methods so hard to break? This is due to how their encryption and decryption processes work. Most of our current encryption methods use large prime numbers, which are extremely easy to multiply together and encrypt, but extremely hard

to factor the semiprime, the product of two primes, into the two factors used. Most of our current encryption methods use a form of this, most notably being RSA, AES, and public-key encryptions. The currently used methods to break these semiprimes and encryption methods have been extremely ineffective. With most taking an exorbitant amount of time to successfully brute force and decrypt, or utterly improbable. Take for example RSA encryption. RSA currently is impossible to break, as it takes far too much time. However, with extreme processing power or a fast semiprime factoring algorithm was discovered, RSA can be broken (Kirsch, 2015).

There are a few ways to defend against quantum computing if it ever becomes a reality in the distant future, with some encryptions already being created to work in a “post-quantum society”. These encryptions use methods like hashing, resistant to quantum computing and commonly used already; and quantum cryptography. Quantum cryptography and quantum key distribution is a type of encryption that relies on quantum mechanics like quantum computers. This type of encryption is impossible to silently intercept, and virtually unbreakable, making this type of encryption potentially the “most powerful data encryption scheme ever developed” (Kirsch, 2015). Quantum computing can potentially destroy our current way of life if we fail to properly act against it, however it looks like we are already currently making strides towards a post-quantum computing world.

Quantum computing, while being an extreme cybersecurity concern, also brings on extreme innovations which are almost too good to be true. As stated earlier, while it would fundamentally break most currently used encryption methods, it also serves to create the most secure type of encryption in existence, quantum cryptography. Quantum cryptography’s

potential future uses towards preventing cyber attacks and potential encryptions of things like AI or full on network systems is astounding.

Our current cyberspace and internet is host to thousands of security concerns per person, device, network, and system. It is important these concerns are properly detected, mitigated, and understood for the future. These current concerns mixed with potentially extreme security concerns in the future, like artificial intelligence and quantum computing, must actively be prepared to have the best chance of mitigation. Artificial intelligence and quantum computing, while potentially being extreme security concerns, allow for some of the most beneficial contributions to cybersecurity and the internet as a whole if they are implemented properly. It is important to turn these cybersecurity risks into benefits for a better future.

References

Abdalrahman, G. A., & Varol, H. (n.d.). *Defending Against Cyber-Attacks on the Internet of Things* . IEEE Xplore. Retrieved April 28, 2023, from https://ieeexplore.ieee.org/document/8757478

Li, J.-hua. (2019, January 10). *Cyber Security Meets Artificial Intelligence: A Survey - Frontiers of Information Technology & Electronic Engineering*. SpringerLink. Retrieved April 28, 2023, from https://link.springer.com/article/10.1631/FITEE.1800573#citeas

Coffey, J. W. (n.d.). *Ameliorating Sources of Human Error in Cybersecurity* . Retrieved April 28, 2023, from https://www.iiis.org/CDs2017/CD2017Spring/papers/ZA253LY.pdf

Wirkuttis, N., & Klein, H. (2018, March 27). *Artificial Intelligence in Cybersecurity*. Academia.edu. Retrieved April 28, 2023, from https://www.academia.edu/36264684/Artificial_Intelligence_in_Cybersecurity

Kirsch, Z. (2015, December 15). *Quantum Computing: The Risk to Existing Encryption Methods*. Tufts University . Retrieved April 28, 2023, from https://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf