Benjamin McDonnough

Ethics and Computer and Network Security

Computer and network security is a critical aspect of modern life, encompassing various threats such as hacking, malware, and vulnerabilities in voting systems. Without computer and network security, there is no confidence that technology is safe or even useful. There would be the constant threat of black-hat hackers (hackers who have illegal motivations and strategies in hacking) coming in and stealing personal information and systems failing for various reasons with no hope of protection for users of the internet. This lack of security would result in inadequate safeguards for technology. This would cause financial losses, reputational damage, and threats to democratic processes. On a larger scale, having inadequate safeguards can cause high-scale terrorism and technological warfare. Countries will no longer have to spend large amounts of time hacking into security systems of other nations.

Moreover, there are significant ethical implications associated with cybersecurity breaches, raising questions about privacy, fairness, and social justice. These include things such as government involvement and punishments for tampering with technological security. Other questions arise as well: what is considered “ethical hacking” and how should it be implemented, what level of security is considered to be a national threat if tampered with, and what measures should be taken to prevent this tampering. There are also questions about the ethics of protecting against security threats from other nations. These questions include things like, how far can ethical methods of dealing with security threats be carried out before the security of the nation becomes more important than remaining completely ethical.

The ramifications of inadequate safeguards for technology within computer and network security are profound and far-reaching. Data breaches can result in financial losses, reputational damage, and legal liabilities for affected organizations. For example, the Equifax data breach in 2017 compromised the personal information of millions of individuals, leading to significant financial penalties and damage to the company's reputation. Moreover, cyber-attacks on critical infrastructure, such as power grids or transportation systems, can disrupt essential services and pose risks to public safety and national security. In the realm of elections, tampering with voting systems can erode public trust in the electoral process and undermine the legitimacy of democratic institutions.

To push further into the ramifications of inadequate security, recent, real-world examples can be dissected. A good example of inadequate security can be seen with the Capital One Breach in 2019. In this breach, the individual who hacked into the system, using “a number of well-understood vulnerabilities” gained access to over 100 million peoples’ information (Khan et al, 2022). This person gained access to “about 140,000 social security numbers” and “80,000 linked bank account numbers” of Capital One users (Capital One, 2022). This hacker then posted all of this leaked data to GitHub, meaning that millions of people had access to this information. Thankfully, the hacker was caught quickly due to their open boasting in what they had done. However, the damaged caused in such a short amount of time was catastrophic.

The threat landscape in computer and network security is constantly evolving, driven by advancements in technology and the sophistication of cybercriminals. Hacking, the unauthorized access to computer systems or networks, remains a prevalent threat, with attackers exploiting vulnerabilities in software and infrastructure to gain access to sensitive information or disrupt services. Malware, including viruses, worms, and ransomware, poses significant risks to individuals, businesses, and governments by infecting systems and stealing data or demanding ransom payments. Furthermore, vulnerabilities in voting systems raise concerns about the integrity and fairness of elections, potentially undermining democratic processes.

This evolution in the threat landscape is growing at an exponential rate. The advancements in technology that are being implemented into society are creating more vulnerabilities. This includes things like smart TVs, smart fridges, smart washers and dryers, smart cars, and any small trinket that has the ability to connect to internet or communicate with some kind of server. An example of this can be seen with robot vacuums with a LiDAR sensor. LiDAR sensors are how a robot vacuum can “see” what is around it. The sensor sends out a laser and measures the time that it takes the reflected light to make it back to the receiver. Hackers have figured out how to use this sensor to be able to “[capture] sound signals by obtaining its reflections off of objects that minutely vibrate due to nearby sound sources (e.g., victim’s computer speaker or TV soundbar)” (Sami et al, 2020). Hackers can use this to gather and personal information that is said while a vacuum is running. Similar events can happen with other smart appliances.

Cybersecurity breaches raise significant ethical concerns, touching upon principles of privacy, fairness, and social justice. Individuals have a fundamental right to privacy and security, and organizations have a moral obligation to protect the data entrusted to them. However, the pursuit of profit or geopolitical agendas may tempt actors to engage in unethical behavior, such as exploiting vulnerabilities for personal gain or engaging in cyber warfare. Moreover, the disproportionate impact of cyber-attacks on marginalized communities raises questions of fairness and equity in the digital age. For example, vulnerable populations may lack access to resources or information needed to protect themselves from cyber threats, exacerbating existing inequalities.

There are several different paths that can be taken to ethical combat these breaches. For the common citizen, the idea of the Categorical Imperative (second formulation) is the best. The idea of this is to treat everyone as people, and not tools to achieve something, which is the entire idea of unethical hacking. If people follow this, then hacking attacks like phishing attacks will be mitigated. However, there are people that will not follow this idea as they don’t care about who they are using to get the desired outcome. In this case, government and company involvement is more of a necessity. In full irony, one of the most effective ways for the government and companies to prevent these breaches is to get other hackers to find the vulnerabilities first and fix them. This is called ethical hacking. Companies, and the government, will hire white-hat hackers (hackers who follow the “guidelines” of ethical hacking and don’t illegally hack) to attempt to find vulnerabilities in their systems. These white-hat hackers will go through, find the vulnerabilities, and fix them. Not only does this prevent black-hat hackers from getting into vulnerable systems, but it also encourages hackers to do so in a legal environment and to benefit society instead of just themselves.

Another approach in addressing the challenges of computer and network security requires technological, organizational, and regulatory measures. First and foremost, organizations must adopt a proactive stance towards cybersecurity, investing in robust defenses, conducting regular risk assessments, and implementing best practices for secure software development and network infrastructure. Collaboration between the public and private sectors is essential for sharing threat intelligence, coordinating responses to cyber incidents, and developing international norms and agreements to prevent cyber warfare and espionage. Furthermore, stronger regulations and enforcement mechanisms are needed to hold organizations accountable for lapses in data protection and incentivize them to prioritize cybersecurity.

In addition to the intranational cyber-attacks, the international cyber-attacks must be addressed as well. As countries are developing more technologically advanced weapons for their armies, hacking in warfare is becoming much more prevalent. Even in warfare, ethics must be considered. This is why there are “rules of war” put into place to prevent unnecessary destruction and merciless killing. However, the ethics look much different in warfare than in common, everyday life. The line of ethical versus unethical is much less clear in warfare. This is where Act Utilitarianism would be useful. For instance, if a situation similar to World War II arose, it would produce more “happiness” to hack into the worldly problematic country to get an advantage in the war. However, in wars that are only between two countries, there is not usually a clear “right and wrong” for each side. These scenarios will have to be decided on a case-by-case basis.

In the context of war, AI and machine learning models should not be used to make final decisions for security. Although they can be useful tools in mitigating cyber-attacks, they should not be used to decide when to “attack”. This is due to the fact that AI and machine learning models can be influenced by outside sources. For instance, another country can flood AI with false information to sway the information that it will output or the decision that it might make. This can lead to several complications, including harm of innocent people. A human being has to be the one to make the final decision on when to use hacking against other countries. This is due to the heavy devastation that a mistake can have in the context of warfare.

Mitigating the effects of cybersecurity breaches requires a combination of technological, legal, and educational interventions. Improved detection and response capabilities can help organizations minimize the impact of cyber-attacks and recover more quickly. For example, machine learning algorithms can analyze vast amounts of data to identify suspicious patterns and anomalies indicative of a cyber-attack. Moreover, stronger regulations and enforcement mechanisms can incentivize companies to prioritize cybersecurity and hold them accountable for lapses in data protection. Additionally, raising awareness about cyber threats and promoting digital literacy can empower individuals to protect themselves online and make informed choices about the technologies they use.

In order to promote digital literacy, governments should have some sort of requirement for a digital literacy class be taught. Since several, major scale breaches start with a phishing attempt or scam emails, it is imperative that people are taught about the dangers of cyber-attacks. There also needs to be some kind of incentive for people to care about cyber-attacks. People need to understand what is at stake so that they will desire to learn about how to prevent cyber-attacks. This can include things like showing examples of bank breaches and the effects that they have had on families that were affected. Also, understanding what can happen on an international scale is important as well. Another important topic for people to understand is the different types of hackers and what their goals are. As previously mentioned, there are white-hat hackers and black-hat hackers. However, another type of hacker is a gray-hat hacker. These hackers hack illegally; however, they are doing it for good reasons. They are not wanting monetary gain for themselves. They hack in order to bring down toxic companies or policies. Understanding the differences in the different types of hackers can be beneficial to people so that they have a greater understanding of what hacking is “good” hacking and what is bad.

Overcoming the challenges of computer and network security will require sustained effort and collaboration across different stakeholders. Governments, industry associations, academic institutions, and civil society organizations all have a role to play in advancing cybersecurity research, developing innovative technologies, and promoting responsible behavior in cyberspace. By fostering a culture of cybersecurity awareness and resilience, we can build a safer and more secure digital future for all.

In conclusion, safeguarding computer and network security is a complex and pressing challenge that requires collective action and a commitment to ethical principles. By understanding the threat landscape, recognizing the ramifications of inadequate safeguards, grappling with the ethical implications, and implementing strategies to address and mitigate the effects of cybersecurity breaches, we can overcome the challenges and build a more secure digital ecosystem. Only through concerted effort and collaboration can we ensure that technology serves as a force for good rather than a source of harm.

Works Cited

“2019 Capital One Cyber Incident: What Happened.” *Capital One*, www.capitalone.com/digital/facts2019/. Accessed 5 Apr. 2024.

Khan, Shaharyar, et al. “A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned.” *ACM Transactions on Privacy and Security*, 1 Feb. 2023, dl.acm.org/doi/10.1145/3546068#d6506706e1.

*UMD*, www.cs.umd.edu/~nirupam/images/2\_publication/papers/LidarPhone\_SenSys20\_nirupam.pdf. Accessed 5 Apr. 2024.