Hacking: An In-depth Exploration of a Hacker's Morality & Ethics

Garrett Bates

AMU (Dept. of Cybersecurity)

ITMG481 Ethics in Information Technology

Dr. Sherrilyn Magby

March 20th, 2024

Introduction

In the constantly evolving digital world, hacking has become a subject of profound intrigue and significant concern. In this paper, I will explore the moral intricacies and ethical dimensions of hacking, revealing the complexities that define a hacker's sense of right and wrong in today's interconnected society. Some topics that will be covered throughout this paper are what hacking is and ethics in general, what some of the main drivers are for a hacker to perform hacking, the difference society sees in hackers (ethical hackers vs. malicious hackers), ambiguities in hacking ethically (the grey areas). I will then investigate why ethical hacking is good for societal advancements in IT and examine why people think hacking (ethically and maliciously) should just be illegal. Finally, I will provide further thoughts in my conclusion.

Hacking & Ethics

So, what exactly is hacking? While there isn't one simple way to define hacking, I would define it as the act of acquiring access to a computer system or network without permission (unauthorized), usually intending to steal information or cause damage. But as I'll explain later in this paper, it can also involve finding and fixing security weaknesses to make the system more secure. Hacking can be either good or bad, depending on its intent. Ethical or white-hat hacking involves finding and fixing security weaknesses to improve cybersecurity. Ethical hackers work within legal boundaries and aim to protect assets such as systems & sensetive data from cyber threats.

On the other hand, nonethical hacking, or black-hat hacking, involves exploiting vulnerabilities for malicious purposes, like stealing information or causing harm. In ethical hacking, it's crucial to get permission before testing systems, prioritize data security, and use hacking tools responsibly. Looking ahead, advancements in AI may lead to more sophisticated cyber threats, making it crucial for ethical hackers to stay updated and collaborate with others to stay ahead of evolving risks. Their responsibilities include identifying vulnerabilities, conducting security tests, and educating others about cybersecurity.

In IT and Cybersecurity, ethics can refer to "the principles & values that guide the responsible and socially beneficial use and development of technology" (Tavani, 2015). Ethical considerations play significant roles in providing security & privacy of user data and addressing intellectual disputes regarding the moral implications of emerging technologies such as artificial intelligence and cyber weapons. It is vital for IT professionals and cybersecurity experts to be aware of these ethical issues and to work towards developing solutions that align with moral principles and values. Ethical hacking is often misinterpreted by the stereotype of a sinister

figure in a dimly lit room writing a Matrix-like code. Regardless, ethical hacking is vital for strengthening cybersecurity. Ethical hackers utilize their skills to identify and address vulnerabilities, aiding companies in protecting against cyber threats. But they must adhere to strict ethical guidelines. This entails "never using their knowledge for harm or personal gain, consistently questioning the morality of their actions, and refraining from breaching networks without proper authorization" (Meredith, 2020). Additionally, ethical hackers must avoid using pirated software and refrain from exploiting sensitive data. By committing to ethical standards and planning, they uphold integrity while ensuring their reputation remains trustworthy in the cybersecurity community.

Different Kinds of Hackers: Motivations

Unsurprisingly, hackers know a lot about computers and use their knowledge to get into computer systems or networks they shouldn't be in. There are three main types of hackers: White hat, black hat, and grey hat hackers. White hat hackers are the good guys. They help companies secure their computer systems and networks by looking for and reporting weaknesses. Black hat hackers are the bad guys. They use their knowledge to do bad things, like stealing information. Grey hat hackers are somewhere in between. They may help companies improve their security, but they might also use their knowledge for personal gain. There are also other types of hackers, including red, green, and blue hat hackers.

Over the years, hackers have been identified by different colored hats. "Green hats refer to aspiring hackers with little technical knowledge but are eager to learn. In the context of Microsoft, blue hats are like white hats and are employed to identify vulnerabilities in unreleased products. However, in some circles, blue hats are hackers seeking revenge. Red hats target Linux

systems and are often characterized as vigilantes" (Shea, 2019). Unlike white hats, who work with authorities, they aim to take down black hats using aggressive attacks. It's important to know that not all hackers are evil. Some are good and work to make computer systems and networks more secure. Hackers do things on computers for different reasons. Some do it to get famous or to create problems, while others do it to help their country or make money. Some don't understand that what they do can hurt people, while others think it's okay if it helps their country or makes them rich. Even though they have different reasons for doing it, they can hurt people and organizations by stealing information, causing money problems, or hurting their reputation when they attack computers. Hackers might start attacking things like smart devices or online stores as computers advance. Society should take computer security seriously, not click on suspicious links, and ensure they stay updated through their IT teams or other means.

Hackers from Society's Point of View

Hacking has existed since the 1980s and has become a hot topic in tech. While movies like Black Hat and The Matrix or TV shows like CSI impact how hackers are viewed, the media often portray hackers as criminals; it's important to remember that not all hackers are bad. Technological advancements have made hacking more sophisticated; it's recommended that businesses and individuals remain vigilant to protect themselves from cyber threats. Hacking has led to legal complexities, media scrutiny, and widespread fear and mistrust in the past five years. Legal battles ensue as governments update cybersecurity laws, while media coverage shapes public perception. In the article "A Hacker's Mind," Bruce Schneier explains how the hacker's mindset can be used to analyze the systems that support our society, from tax laws to financial markets to politics. "Almost all systems have vulnerabilities that can be exploited by powerful

actors, which threatens our financial markets, democracy, and the way we think" (Schneier, 2023). However, by understanding the hacking mindset, we can rebuild systems and use tools such as AI to improve them and safeguard them against exploitation. Hackers face moral dilemmas, balancing privacy, and security concerns, considering intentions, consequences, and compliance with laws and regulations. Ethical hackers should prioritize responsibility and accountability, aiming to minimize harm, while malicious hackers usually try to exploit vulnerabilities for personal gain, undermining trust in digital systems.

After asking some friends who are non-IT majors and some people from my local coffee shop, almost all of them said hackers were bad. This interested me, considering how ethical hacking hasn't been pushed out as much as some would agree. As one stated, "hacking is cool," but didn't know what he was talking about and what the hacking process could achieve. When I asked others what they thought of when they heard the word hacker, they said something along the lines of someone "who has hacking skills," and they didn't say anything else other than that. When I asked if they thought hackers were good or bad, all of them answered "Bad!" except for one who watched the show Mr. Robot. It was rather intriguing to see just the small number of individuals, and I may continually ask this question in the future to analyze other responses.

Society often views hacking as inherently wrong, but not all hackers are "bad guys." Ethical hacking aims to find vulnerabilities before malicious hackers do so that they can be fixed, and data breaches prevented. Ethical hackers undergo specialized training and certification programs to carry out these tasks professionally and responsibly. Businesses and organizations can identify and mitigate risks, thus protecting sensitive data like personally identifiable information (PII) through ethical hacking. This is especially important since data breaches happen frequently in today's world since data breaches can severely affect individuals and

organizations. Ethical hacking also promotes better physical security, secure coding practices, and pen testing with advancements in fixes, which helps prevent data breaches from black hat hackers. Ultimately, ethical hacking is good for societal advancements because it helps protect against cyber threats increasingly prevalent in our interconnected world.

The Grey Areas

Let's talk about some of the juicier stuff (controversial). By now, you might see why hacking can be such a controversial topic regarding ethics. The legalities of hacking devices and software are controversial, with debates around who should be allowed to access hacking tools and technologies. The Flipper Zero is a recent example of a controversial hacking device reiterating this issue. Some argue that only trained professionals should have access to these tools, while others believe that anyone should be allowed to explore and learn about technology. Balancing innovation and protection against malicious activities is crucial for hacking tools and technologies. During the National Summit on Combatting Auto Theft on February 8, François-Philippe Champagne, the Canadian Minister of Innovation, Science, and Industry, introduced strategies to counter Canada's increasing car theft rate. Among the proposed measures, he suggested banning the Flipper Zero device, alleging its involvement in car theft through keyless entry systems—a claim that has been debunked. One prominent argumentative statement I found was, "The problem is not in the available radio hardware, but rather in the insecurity of outdated access control systems" (Zhovner, 2024). This reinforces the ongoing debate surrounding the positive aspects of hacking, showcasing how ethical hackers can reveal vulnerabilities in outdated control systems and networks, not to mention other applications used by individuals and organizations.

Image: Flipper Zero (Hacking Device)

"The Computer Misuse Act of 1990 makes unauthorized access to computer systems and data illegal. It aims to protect digital systems from misuse" (Popescu, 2021). Ethical considerations are crucial in developing hacking tools. Developers must ensure tools are used responsibly and transparently, preventing misuse, and promoting ethical hacking practices. Grey hat hackers have the skills and knowledge of black hat hackers but use their abilities for ethical reasons. However, there is ethical uncertainty associated with their motivations, as they may accidentally cause harm while uncovering vulnerabilities. Therefore, they need to be aware of the potential risks and be cautious in their activities.

Ethical decision-making in the IT world is paramount, particularly in the grey areas of hacking, where moral compasses guide professionals. IT experts bear significant responsibilities, recognizing that "with great power comes great responsibility" (Uncle Ben). They navigate complexities, understanding the fine line between cybercrime and activism in hacking activities. Upholding ethical standards involves ensuring legal clarity, such as filling out NDAs and pen-test forms and adhering to legal standards across industries; this all backs up how ethical

considerations are crucial in maintaining integrity, protecting data, and even fostering trust in the digital domain.

Exploring Positive Impacts of Ethical Hacking: Societal Advancements in IT

There are several real-world examples of Ethical Hacking Successes that I can think of. The first thing that comes to mind is penetration testers working for companies or contractors who use up-to-date penetration testing techniques to break into a company's/organization's network or applications. This ultimately results in a better-rounded security posture for companies that proactively help with vulnerability identification, thus strengthening cyber defense against evolving threats. "While cybersecurity experts have access to hacker typologies and their motivations, which help them gain a deeper understanding of cybercrime, it's worth noting that the hackers' motivations, attack methods, and sophistication are constantly evolving" (Chng, S., Lu, H. Y., Kumar, A., & Yau, D, 2022).

For ethical & nonethical hackers, Linux is one of the better options for performing a variety of different hacking techniques. "XSS is a vulnerability that can be found on websites and has been known for a long time. It can also be a risk for APIs, primarily if the data submitted to the API interacts with the website" (Ball, 2022). In an XSS attack, the attacker injects a harmful script into a web page by submitting user data interpreted as JavaScript or HTML by a user's browser. This script can cause pop-up messages or redirect the user to harmful content. Using a Linux distribution such as Kali Linux (I prefer Parrot OS), ethical hackers can test different APIs, find vulnerabilities, and patch them to strengthen the security of their APIs! To test APIs for XSS attacks, one must find an endpoint that lets you submit requests to the web application. If the application doesn't check the input, the XSS script can be executed when a

user visits the page. However, it's important to note that API defenders are aware of this vulnerability and have taken steps to prevent it. Additionally, if an API doesn't interact with a web browser, it's unlikely that an XSS attack will be successful.

"Ransomware is a form of malicious code that encrypts a machine's files and demands payment for the decrypted data. To comprehend ransomware, it is essential to learn about encryption algorithms and secure communications" (Graham, 2021). Cryptography provides ethical hackers with vital tools to bolster cybersecurity efforts. By using encryption algorithms, they can safeguard sensitive data from unauthorized access, ensuring it remains unreadable to potential attackers. Secure communication protocols, like SSL/TLS, enable them to protect data transmission over networks. Ethical hackers also utilize cryptographic hash functions to verify data integrity and detect unauthorized changes. Cryptography allows ethical hackers to identify vulnerabilities and strengthen defenses, contributing to a safer digital landscape and reducing attack surfaces. Ethical hacking improves incident response plans, considering updates with security vulnerabilities will most likely be found when ethical hackers step in. Without ethical hackers' vulnerabilities might be discovered by nonethical hackers, which you wouldn't want. In this sense, it creates jobs and can help a company align with legal requirements and improve stakeholder/client trust. International collaboration with ethical hackers varies, but through online communities and hack-the-box events, hackers (both ethical and nonethical) can gather skillsets.

Conclusion

In conclusion, I went over & explored the ethical and moral considerations of hackers. While hacking may have negative connotations, ethical hacking is a critical practice that helps to

mitigate risks and protect sensitive data. Society should start to recognize the value of ethical hacking and encourage its use to promote better cybersecurity practices and prevent data breaches. Ethical hacking helps organizations identify and fix security vulnerabilities, preventing cybercrime and improving overall security. While some argue that all hacking should be illegal, ethical hacking (with permission) can build a safer digital world.

References

Ball, C. (2022). *Hacking apis*. O'Reilly Online Learning. https://www.oreilly.com/library/view/hacking-apis/9781098130244/f08.xhtml

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022, January 19). *Hacker types, motivations and strategies: A comprehensive framework*. Computers in Human Behavior Reports. https://www.sciencedirect.com/science/article/pii/S245195882200001X

Graham, D. (2021, September). *Ethical Hacking*. O'Reilly Learning. https://help.oclc.org/Library_Management/EZproxy/EZproxy_database_stanzas/Database_stanzas_O/OReilly_Learning_(formerly_Safari_Books_Online)

Kisters, S. (2023). *The morality of hacking: Cyber ethics uncovered*. OriginStamp. https://originstamp.com/blog/the-morality-of-hacking-cyber-ethics-uncovered/

Meredith, D. (2020, May 7). *Ethics in hacking*. Pluralsight. https://www.pluralsight.com/blog/software-development/ethic-in-hacking

Popescu, F. (2021, January 25). *Grey area of hacking: Cyber security*. Flaviu Popescu. https://flaviu.io/the-grey-area-of-hacking/

Schneier, B. (2023). *A Hacker's mind: How the powerful Bend Society's rules, and how to bend them back*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/hackers-mind-how-powerful-bend-societys-rules-and-how-bend-them-back

Shea, S. (2019, October 21). *Different types of hackers, from Black Hat to red hat: TechTarget*. Security. https://www.techtarget.com/searchsecurity/answer/What-is-red-and-white-hat-hacking

Tavani, H. T. (2015). Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing (5th ed.). Wiley Global Education US. https://online.vitalsource.com/books/9781119186571

Zhovner, P. (2024, March 20). *Our response to the Canadian government*. Flipper Blog. https://blog.flipper.net/response-to-canadian-government/#:~:text=TLDR%3A%20The%20Canadian%20government%20has,and%20slow%20down%20technological%20progress.