Hackers for a Greater Good

Ivelyn Gomez, Kristian Lewis, Joseph Osgood

Binghamton University

Introduction

The world of technology has revolutionized everyday life, including the way people communicate, research, and interact with one another. Along with the rapid increase in technology came various concerns regarding people's privacy, protection and rights. One of these specific ethical issues is hacking. Most people tend to see hacking as something malicious, ignoring its usefulness in society. Gray hat hackers are those who commit questionably legal Internet activities but without malicious intent. White hat hackers, usually paid professionals, have permission to hack companies for a specific purpose. Lastly, the most notorious kind of hacker, known as a black hat hacker, is one who hacks for malevolent purposes. The film, *Hackers Wanted,* accurately portrays gray hat hackers as both useful and maltreated by the law. While hacking is a real threat, ethical hacking is our best defense against malicious hackers, and it is a defense that the government ought to protect rather than prosecute. *Hackers Wanted* gives insight into the ethics of hacking and the legality of different hackers.

Main Source

There a numerous examples of nefarious black hat activities in the film, including attacks on physical infrastructure, disruptions of the economy, and biological warfare. Criminals use emails to fool victims into giving up their personal information, while others may break into bank systems (Brunetti et al., 2009). While black hat hackers who act individually pose a serious threat, hackers become even more dangerous when they join together with governments and organizations. The Chinese People's Liberation army prepared for information warfare against foreign countries by simulating attacks on infrastructure, stock markets, and electricity grids (Brunetti et al., 2009, 0:29:35). In the film, John Arquilla, an expert in terrorism at The Center on

Terrorism and Irregular Warfare, describes how terrorist groups, such as Al Qaeda, are gaining hacking skills which could feasibly be combined with physical attacks in order to seriously damage another country (Brunetti et al., 2009, 0:04:00). In light of the threat malicious hackers pose, it is vital that governments and corporations increase their security.

Hackers Wanted devotes much of its time to discussing the threat of cyberterrorism. Brunetti, Spacey, and Bozzo started creating the documentary in response to Adrian Lamo's arrest in 2003, only two years after the September 11 terrorist attacks (Nym, n.d.). Terrorism was a widely discussed topic during the years immediately following these attacks, which explains the documentary's emphasis on the threat of terrorism and cyberwarfare. While terrorism may not be as much of a common discussion topic today, it is still a threat. Moreover, there will always be some kind of criminal activity in the world, and the Internet is a convenient platform to carry it out. The documentary proves the threat posed by malicious hackers by giving numerous examples of those threats and by interviewing security professionals and existing gray hat hackers. The risks of online attacks further demonstrates the need for gray hat hackers to protect the world from cyber criminals and terrorists.

The film gives the example of two gray hat hackers known as "the Deceptive Duo." After seeing the tragedy of 9/11, the Deceptive Duo saw the threat that terrorists posed to the free world, so they decided to start simulating terrorist attacks on the government's computer systems in order to make sure they were secure (Brunetti et al., 2009, 0:42:55). They were ultimately arrested, imprisoned, and fined thousands of dollars for their actions, even though their original motives were altruistic (Brunetti et al., 2009, 1:04:30; Rohde, 2004). In their efforts to protect the government from terrorist attacks, the Deceptive Duo was prosecuted. Like most gray hat hackers, the Deceptive Duo wanted to secure the government's computer systems, not harm them. Hackers will find vulnerabilities in virtually every computer system. It is far better that gray hat hackers discover these vulnerabilities than black hats.

The film also focuses on the story of Adrian Lamo as an exemplary gray hat hacker. Lamo discovered that Yahoo News had a vulnerability allowing anybody to edit articles, which he used to make minor punctuation changes and insert false quotations in articles (Brunetti et al., 2009, 0:40:15). Lamo was shocked to realize that Yahoo did not notice his intrusion into their system (Brunetti et al., 2009, 0:41:20). Gray hat hackers try to break into computer systems out of both curiosity and a concern for security, which is why the apathy of technology companies regarding the security of their products often surprises hackers. Lamo's curiosity ultimately got him arrested when he found the social security numbers of New York Times employees through a security hole on their website (Brunetti et al., 2009, 0:56:00). Many people worried that Lamo's arrest would set a dangerous precedent that any hacker who intrudes into a computer systems could face legal consequences, regardless of the hacker's original intent (Brunetti et al., 2009, 0:57:30). The controversial arrest of Lamo reveals the tension within the law regarding hackers. While the government wants to take a strict position against the unlawful intrusion of black hat hackers, if it takes too strict of a stand against hacking, ethical hackers will cease their work in protecting and defending cyberspace from criminals.

Kristian Lewis

Hackers can take advantage of vulnerabilities in corporate, government, and individual systems, as well as devices. Vulnerabilities may allow a black hat hacker to hack into corporation or government databases and steal user information, such as social security and credit card numbers. In a Ted talk by Avi Rubin, he describes how many devices have security vulnerabilities (Rubin, 2011). Avi Rubin begins with anecdotal stories about the general public's ignorance towards computer security before delving into examples of hackable devices. A team was able to hack into a pacemaker to change treatments and patient information (Rubin, 2011, 2:00). The relative ease with which they were able to hack into the device is alarming. Not only is hacking a medical danger, but so are devices like cars, iphones, and government radios (Rubin, 2011). Being a professor specializing in computer security, his talk is intended to inform and protect his viewers of the vulnerabilities of their devices. Since any device a hacker can access is subject to hacking, and many devices are run by computers, there are not enough security protections put in place for these devices to protect them from black hat hackers.

New technology increases efficiency and user satisfaction, but also increases vulnerabilities in systems. Simon Byers mentions this in his paper “Defending Against an Internet-Based Attack on the Physical World,” published in 2004 in the *ACM Transactions on Internet Technology.* Byers has had many peer-reviewed articles submitted through ACM Transactions on Internet Technology, and IEEE Security & Privacy showing he is an active researcher in cybersecurity. Although this specific paper is dated, the basic theme is still relevant. Byers produced this article to improve security and allow users to better prepare themselves for an attack (Byers, Rubin, & Kormann, 2004).

“Defending Against an Internet-Based Attack on the Physical World” describes an attack where a hacker sends large amounts of junk mail to an individual’s physical address, and attempts to access sensitive data (Byers et al., 2004, 242). The authors provide a variety of solutions, many of which involve not using or limiting use of technology with vulnerabilities.

One of the solutions is using a system similar to CAPTCHA, where a user must input text from an image and into a website in order to gain access, but the image is designed so that a computer program cannot read it (Byers et al., 2004, 249). The authors found that new technology often comes with vulnerabilities, and in order to protect computer systems, one must either limit one's use of the new technology or design new ways to protect oneself from them. The authors encountered an ethical issue of whether or not to distribute this information. They discovered the vulnerability first-hand in 2000 and decided not to release the details of its security weakness until 2004, when they felt there was enough protection available for individuals who may encounter this problem (Byers et al., 2004, 240-241). The authors waited four years to distribute the information, as it would have been detrimental to public safety to distribute it any sooner. This confirms the motives of the authors, as their ultimate goal was to protect other people. It also shows that there is a gap in time between when a technology is created and when the vulnerabilities created by that technology are resolved, putting the public at risk for black hat hackers.

Many vulnerabilities in systems are due to lack of education and poor practices. Hyung-Jin Mun and Kun-Hee Han describe a hacking method in their paper, "Blackhole attack: user identity and password seize attack using honeypot." They are affiliated with the Division of Information and Communication at Baekseok University in Cheonan, Korea. The paper was published in a peer reviewed journal specializing in computer virology and hacking techniques. This paper's motive is to present a potential hacking method for educational purposes.

In this article the authors provide a phishing method that relies on the idea that users use similar or the same passwords and IDs for accounts in different services (Mun & Han, 2016).

They developed a phishing using a fake website to obtain a user's information. The user attempt to log into the account, but it fails, saving the information they submit each time (Mun & Han, 2016, 186). The users enter their information multiple times, likely changing it each try, giving hackers multiple variations to work with (Mun & Han, 2016, 188). This highlights common vulnerabilities that black hat hackers can take advantage of. If hackers obtain one ID and password, they can likely use or guess the user’s ID or password on another website. This brings up some ethical issues concerning the responsible for the user's safety. It is the user’s responsibility to be appropriately educated on internet safety, but it is the software developer’s responsibility to use thorough authentication measures to ensure the identity of users. Their solutions suggest that their motives are to educated people on the dangers of user identification, and that we should change the ways websites authenticate users. This article highlights methods hackers use that have low detection, which is dangerous for the general public (Mun & Han, 2016, 189-190). Although there are a number of vulnerabilities for black hat hackers to take advantage of, gray hat hackers can be utilized in protecting our systems.

Joseph Osgood

While black hat hackers pose a significant threat to the world today, gray hat hackers offer protection from these criminals and a way to keep the Internet secure. Keren Elazari, a researcher at Blavatnik Interdisciplinary Cyber Research Center with a Masters of Arts in Security Studies from Tel Aviv University, compares gray hat hackers to “the Internet’s immune system” in her 2014 TED talk (“Keren Elazari,” n.d.; Elazari, 2014). Like an animal’s immune system, hackers may sometimes cause the entire body of Internet to become “sick” in order to fight off an infection, but these hackers are ultimately trying to help (Elazari, 2014). She gives many examples of hackers who discovered dangerous security flaws in computer systems and reported these bugs to the appropriate company, thus securing the product even further (Elazari, 2014). While Elazari generally favors hackers, she also acknowledges their unethical actions, explaining that oftentimes hackers need to break the law in order to find the vulnerabilities that could be exploited by malicious hackers (Elazari, 2014). Elazari's presentation supports an idea similar to that portrayed in *Hackers Wanted*, namely that gray hat hackers are necessary to protect the Internet from black hat hackers.

Many hackers naturally develop strong opinions about the importance of the work they do. Hafiz and Fang, researchers at the department of computer science in Auburn University, explored these opinions through an email survey that they sent hackers and vulnerabilities reporters (Hafiz & Fang, 2015, pp. 1920-1921). According to the responses they received, most bug reporters think companies ignore what they submit, compelling them to fully disclose - or publicly post online - these security holes (Hafiz & Fang, 2015, p. 1954). Disclosure is an ethical issue, as inappropriate disclosure can alert malicious hackers of existing security flaws. Even though vulnerability reporters may desperately want companies to secure their systems, the risk of black hat hackers finding those loopholes due to public disclosure is far greater than the risk of them finding these loopholes on their own. Hafiz and Fang conclude that hackers would be less likely to riskily expose security holes if companies were more responsive to their vulnerability reports (Hafiz & Fang, 2015, p. 1955).

The study relies primarily on a survey sent to the users of SecurityFocus, a website for hackers to discuss and report security issues for various programs ("SecurityFocus," n.d.). The opinions given in the survey are therefore first-hand accounts of what hackers think about finding and reporting bugs to companies. Hafiz and Fang recognize the bias of hackers by explaining that they often want recognition for their work, hence their desire to publicly disclose vulnerabilities, even if that recognition comes at the price of a company's reputation or malicious hackers exploiting the bugs (Hafiz & Fang, 2015, p. 1954). Nevertheless, this bias confirms the altruistic motives of the vulnerability reporters; they want to be remembered for making programs secure. Gray hat hackers have a choice of either telling the public about security holes or only telling companies about security holes, and the decisions these hackers make can reveal their true intentions.

One study aimed to secure the Internet by studying past security compromises. Vasek, the primary author of this article, is a researcher at the University of Tulsa, specializing in cyber security and malware (Vasek, 2015, p. 219). The study examines potential risk factors for web servers by comparing the circumstances of websites that became infected with the circumstances of those that did not, a method of study commonly referred to as case-control (Vasek, 2015, p. 208). Vasek acknowledges the difficulties of collecting a representative sample of websites and explains that that is why she gathered data from anti-phishing websites (Vasek, 2015, p. 208). Analyzing the data prompted Vasek to conclude that content management systems, certain plugins, and up-to-date software systems all increase a website's chance of being hacked (Vasek, 2015, p. 218). Once web developers are aware of the dangers that certain features present, they can better secure their websites from malicious hackers by avoiding those features. In contrast to gray hat hacking, this method of improving Internet security relies on analyzing past security compromises, rather than the discovery of current vulnerabilities. Thus, while it may not be necessary to break the law in order to find these security weaknesses, breaking the law is often a better way, as it can find vulnerabilities without letting websites be compromised.

Ivelyn Joyce Gomez

Hackers, malicious or not, end up in legal controversies. Nowadays, hackers are predetermined as vandals, where all hacking is portrayed as a crime. During the 1960s and 1970s hacking was a positive term, where a hacker was a programmer who wrote clever and elegant programs (Baase, 2013, p. 321). Society has gradually come to view a hacker as a nuisance or a malicious person due to the rise of Internet crimes like identity theft. Richard Hollinger, from the Department of Sociology and the Center for Studies in Criminology and Law at the University of Florida, conducts research in cybercrime. He gathers multiple articles and sources along with many of his own papers from varying conferences such as “Crime by computer: receptivity of computer science students occupationally related deviance.” A paper presented at the 1984 American Society of Criminology Annual Meetings in Cincinnati, titled, “Computer Heroes or Electronic Highwaymen?” discusses how cybercrime should be handled. He takes into account a hacker’s intent, effects, and other variables.

Richard Hollinger clarifies that law enforcement usually misunderstands hackers due to their classification as a “computer illiterate profession,” thus catalyzing society’s collective fear and ignorance of technology (Hollinger, 1991, p.11). These aspects show how the offense is automatically associated with the crime of malicious hacking. Furthermore, Hollinger traces and identifies how law enforcement branches and agencies are assigned to certain court cases and crimes. Ultimately, “the most sophisticated law enforcement agencies in the land are chasing the least powerful and least prevalent computer criminals” (Hollinger, 1991, p.13). Overall, Hollinger accurately shows how both hackers and law enforcement misunderstand one another due to their characteristics. The dissecting of hackers and their personalities helps depict a new perspective of cyber crime. Hackers who society once praised for their sophistication in technology have now come into conflicts with the law. *Hackers Wanted* depicts different hackers and their classifications, a majority of whom are gray hat hackers. These gray hat hackers have come to be seen as malicious and Hollinger helps clarify why this is the case.

The film, *Hackers Wanted,* follows and debates court cases of hackers, like Adrian Lamo and the Deceptive Duo, who were prosecuted even though they had good intentions. Similarly, Aaron Swartz, hacktivist and co-founder of Reddit, managed to hack into a paid journal database, JSTOR without harming anyone (Sangkyo Oh & Kyungho Lee, 2014, p.1). He was consequently prosecuted with the "maximum penalty of one million dollars in fines along with 35 years in prison and asset forfeiture" (Sangkyo Oh & Kyungho Lee, 2014, p.1). Unfortunately, this court case led Swartz to commit suicide. Due to this controversial event and many others, the United States government has modified its laws to prevent excessive punishments of hackers.

The study, "The Need for Specific Penalties for Hacking in Criminal Law," explains the relationship between cybercrime and the provisions of laws in various countries, including the United States. Sangkyo and Kyungo conduct research at the Center for Information Security Technologies at Korea University in the Republic of Korea. This study is an academic article published on the Scientific World Journal. It cites 21 different sources relating the hacking laws of various countries to ethical standpoints of hacking. This article shows that hacking laws are abused in court cases and excessively punish hackers, even those who have no malicious intentions and cause no harm. The article shows that the government mistreats gray hat hackers.

Furthermore, Sangkyo and Kyungo analyze the principles common to the laws and penalties. They compare the series of laws and regulations relating to cybercrime internationally to those of the United States. Additionally, Sangkyo and Kyungo mention that misuse and abuse of the Computer Fraud and Abuse Act led to excessive punishment of hackers (Sangko et al., 2014, p.1). Usually, the laws set forth to punish hackers are meant to impose fear and prevent people from hacking. However, this method of keeping hackers from illegal Internet activity is inefficient due to its side effects, such as the suicide of Swartz. Instead of preventing hacking, many believe hackers should use their intelligence and potential for better things like keeping the Web safe, thus solidifying *Hackers Wanted's* depiction of some hackers as useful.

Between advising countries about Internet policies and reporting current events in Europe, Misha Glenny knows about cybercrimes and has shared his thoughts through books and television programs ("Misha Glenny," n.d.). TED talks have the potential to be subjective, as the speakers can present any reasonable claim they would like to, so long as they can support it with some evidence. Glenny backs up his argument by examining the lives of six unique cybercriminals, all of which shared impressive intelligence and underdeveloped moral compasses (Glenny, 2011). Governments need to train hackers like the ones Glenny describes to keep our Internet safe rather than jailing them for using their talents.

Glenny suggests in his TED talk "Hire the Hackers!" that hackers are extremely intelligent people whose potential should not be wasted by convicting them as criminals (Glenny, 2011). He gives an example of different hackers who all share certain qualities: they are smart, they have underdeveloped social skills, and they grow up in poor environments (Glenny, 2011). Unpleasant upbringings leave some hackers with a poor sense of morality (Glenny, 2011). Other countries take advantage of these bright individuals, according to Glenny, rather than incarcerating them for doing something questionable, as might happen in the United States (Glenny, 2011). Glenny's talk suggests that the governments of the world should tap into this valuable resource of talented hackers and teach them how to direct their energy towards beneficial activities (Glenny, 2011).

Conclusion

While the world of technology will continue to advance and expand, hackers will continue to increase in numbers. Consequently, governments will need to continually modify laws and legislations to fit the crimes of hackers – both those who do illegal activity online and those that do not. *Hackers Wanted* depicts various hackers who are malicious, ethical, and professionally paid. Along with these identifications, the documentary uses court cases to show that laws should be appropriate for the hacker and their specific intentions. The constant misunderstanding between hackers, society, and law enforcement causes hackers to be punished to a greater extent than is needed. As a result of the controversy of hackers, their practices continue to exist. Devices and systems are riddled with vulnerabilities which black hat hackers can take advantage of. However, not all hackers are malicious, especially since many have skills that are useful for protecting society from cyber criminals. Gray hat hackers do not need to wait for the compromises that researchers need to study the security of a system. Gray hats can even find and report security flaws before black hat hackers find them. The definition of a hacker should change to reflect the varying characteristics and activities of different hackers. The film, *Hackers Wanted,* accurately portrays gray hat hackers as both useful to society and maltreated by the law.

Hackers will continue to seek new challenges regardless of how the law treats them, a pursuit that will continue and evolve as technology progresses. Since hackers can use the their skills for both good or bad purposes, it is vital that governments consider their motives before convicting or rewarding them. If governments do not redirect and appropriately reward questionably ethical hackers, the world will have no defense against malicious hackers. Tools have power, but it is people who use them. Ethical hackers are those who wield the tools of their trade for defense and not for personal gain, and they are also the best defense the world has against those would use this tool for evil.

References

Baase, S. (2013). A gift of fire: social, legal, and ethical issues for computing technology (4th ed.). Upper Saddle River, NJ: Pearson.

Brunetti, D., Spacey, K. (Producer), & Bozzo S. (Director). (2009). *Hackers wanted* [Motion

Byers, S., Rubin, A., D., & Kormann, D. (2004). Defending against an Internet-based attack on the physical world. *ACM Transactions on Internet Technology,* 4(3), 239-254. doi: 10.1145/1013202.1013203

Elazari, K. (2014, March). *Hackers: the Internet's immune system* [Video file]. Retrieved from https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system/transcript#t-318546

Glenny, M. (2011, July). *Hire the hackers!* [Video file]. Retrieved from https://www.ted.com/talks/misha_glenny_hire_the_hackers#t-282815

Hafiz, M., & Fang, M. (2015, Sept.). Game of detections: how are security vulnerabilities discovered in the wild? *Empirical Software Engineering, 21*(5), 1920-1959. doi: 10.1007/s10664-015-9403-7

Hollinger, R. C. (1991). Hackers: computer heroes or electronic highwaymen? *ACM SIGCAS Computers and Society, 21*(1), 6-17. doi:10.1145/122246.122248 https://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked/up-next

Keren Elazari. (n.d.). Retrieved from http://premierespeakers.com/keren_elazari/bio

Mun, HJ. & Han, KH. (2016, August). Blackhole attack: user identity and password seize attack using honeypot. *Journal of Computer Virology and Hacking Techniques*, 12(3), 185-190. doi: 10.1007/s11416-016-0270-6

Nym. (n.d.). *Hackers Wanted (2009) plot summary*. Retrieved from http://www.imdb.com/title/tt2292707/plotsummary#summaries

Oh, S., & Lee, K. (2014). The need for specific penalties for hacking in criminal law. *The Scientific World Journal, 2014,* 1-6. doi:10.1155/2014/736738

picture]. United States: Trigger Studio Production.

Rohde, L. (2004, July 20). 'Deceptive duo' hacker charged. *PC World.* Retrieved from https://www.pcworld.com/article/116957/article.html

Rubin, A. (2011, October). *All your devices can be hacked* [Video file]. Retrieved from https://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked

SecurityFocus. (n.d.). Retrieved from http://www.securityfocus.com/about

Vasek, M., Wadleigh, J., & Moore, T. (2015, April 19). Hacking is not random: a case-control study of webserver-compromise risk. *IEEE Transactions on Dependable and Secure Computing 13*(2), 206-219. doi: 10.1109/TDSC.2015.2427847