Hayden Ackerman

Dr. Hayes

CSCI 235

February 11th, 2019

The Good Hacker?

According to Steven Levy, author of *Hackers: Heroes of the Computer Revolution*, what we know as hacking today originates from the MIT Tech Model Railroad Club. They were able to modify the punch cards that were fed into a TX-0 computer, and made the computer do something outside of its intended purpose such as converting numbers to Roman numerals, or making the speaker play Bach tunes (Levy 27-28). This technological advancement was originally meant for benign purposes, however, it opened the gateway for more malicious activities, such as phreaking. According to Wallace Wang, phreaking involved the modification of phone lines in order to make unlimited long distance phone calls (Wang). In fact, some of the most gifted technological wizards of our time, such as Steve Jobs and Steve Wozniak, were known phone phreakers (Wang 38). Phreaking was technically black hat hacking. Fast forward to today and the innovation of the personal computer, and we have the hackers and crackers. A hacker is a "person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular" (Internet Users' Glossary). On the other hand, a cracker is an "individual who attempts to access computer systems without authorization" (Internet Users' Glossary).

In regards to the terms, one can therefore deduce that a hacker stands for everything ethical while a cracker could care less. However, there are times where hackers ride a gray line of ethical actions, especially in regards to system-cracking. Of course, it naturally falls to one's perspective. If a hacker were to crack the password of a computer belonging to one of the world's most prolific child

molesters, the hacker sees it as ethical. However, the child molester sees it as unethical. Personally, I see it as ethical. If a hacker were to hack into a children hospital's network just for fun, utilizing a vulnerability, I would see it as unethical even if the hacker didn't steal, vandalize, or leak anything. If the hacker were to immediately report the vulnerability they utilized to the hospital, I would change my opinion. Say that John Smith hacks into the hospital's network for fun, utilizing an SMB port vulnerability. He pivots around, looks at some records, and quietly exits the system. Then comes the cracker a week later. Upon finding the SMB vulnerability, he gleefully exploits it, and starts to modify information in an attempt to help his friend get prescription drugs. Three floors above the server hosting the files, a day later, little Sally is resting in bed after having surgery on her knee. In order to prevent infection, a nurse gives Sally a shot of penicillin. However, Sally goes into anaphylactic shock, and dies. You see, the cracker deleted the bit of information detailing that Sally was extremely allergic to penicillin—along with other people's information—to throw the IT team off of his trail.

Had the hacker originally reported the SMB vulnerability, Sally could still be alive. A good hacker would've reported the vulnerability, and checked up on it. A cracker would continually exploit that vulnerability. In essence, a line between the two exists, showcasing the dichotomy of their actions. A good hacker's responsibility is to report this vulnerability, and check up on it, due to its severity. If the hospital understands the nature of the vulnerability, they would thank the hacker and reward him. They should not persecute him, such as the case of Allan Dumanhug. Dumanhug found a bug in an undisclosed company's network, but upon reporting it, Dumanhug was accused of trying to hack into their network (Kharpal). However, Dumanhug didn't lash out at them. 1 Peter 4:8-10 states, "Above all, love each other deeply, because love covers over a multitude of sins. Offer hospitality to one another without grumbling. Each of you should use whatever gift you have received to serve others, as faithful stewards of God's grace in its various forms" (*English Standard Version*, 1 Peter 4.8-10). Every hacker should use his or her gift for good, just like Dumanhug did.

Works Cited

"Internet Users' Glossary." *IETF Tools*, tools.ietf.org/html/rfc1392.

The Holy Bible: English Standard Version, Containing the Old and New Testaments, ESV. Crossway, 2016.

Kharpal, Arjun. "Are Companies Still Scared of 'Ethical' Hackers?" *CNBC*, CNBC, 19 June 2015, ` www.cnbc.com/2015/06/17/are-companies-still-scared-of-white-hat-hackers.html.

Levy, Steven. *Hackers: Heroes of the Computer Revolution: 25th Anniversary Edition*. OReilly, 2010.

Wang, Wallace. *Steal This Computer Book 4.0: What They Wont Tell You about the Internet*. No Starch Press, 2006.