Derrick Lee
Homework 1
CSCI 180
November 5, 2019

1

Depending on the process of discussing the vulnerability with the manufacturers, I believe the 2016 Rose presentation could be ethical. It seem like the manufacturers did not care to fix their vulnerabilities and continued to sell their products online regardless. Disclosing the vulnerability puts pressure on these companies to improve their products, as without disclosure, a malicious user can still eventually come across the same thing and use it privately without the companies knowing it. Also, it provides the general public knowledge of such attacks which in turn allows for them to try to mitigate the risks and provides other companies knowledge to prevent such attacks in their products. This is a very big problem in the lock industry, many big companies like Master Lock provides a wide variety of locks that are extremely easy to pick or bypass with low skill attacks. Master Lock is willingly producing locks that are not secure even when their vulnerabilities are known. For example, a new Master Lock 3 released over 75 years after the Master Lock 77 (made in the 1930s) has zero improvements in resistance to lock picking. Only when consumers are educated about these issues would companies like Master Lock innovate more on security and releasing these attacks put pressure on them to do so.

I think if Rose released the vulnerabilities without contacting the manufacturers to let them create a fix first, it would have been unethical and a deliberate act to let people exploit the specific locks.

2

I believe the presentation was ethical. The security team members did not have malicious intent in releasing Meatpistol. Similar to disclosing vulnerabilities, providing these offensive security tools can allow companies and others to improve their security countermeasures. Preventing such security tools only makes it harder for people to protect against such attacks. While there may be malicious actors that may benefit from such tools, many other ones benefit those who are protecting their systems as it is much easier to test with malware generated in a few seconds compared to a several days. Keeping such a tool private may be seen as for selfish reasons, to monetize and profit from it. Making it public would reduce the barrier for users to test their systems without having to spend a lot of money.