Robotic Vacuums and the Deontological and Teleological Moral Frameworks

Author: 2344104 Date: 27 March 2023

The proliferation of the Internet of Things (IoT) has revolutionized the way in which we live, work, and interact with each other. In the next decade, the IoT will increase in prevalence and will permeate in many more aspects of our lives (Lam , 2022). However, as the connectivity and conveniences increase so too will the cybersecurity risks and subsequent ethical concerns. As a qualifying electrical engineer, the cybersecurity industry is a potential career path, where knowledge of both the associated software and hardware domains are advantageous. Therefore, this essay aims to examine the moral dilemmas faced by ethical hackers in the IoT industry, using both the deontological and teleological ethical frameworks as the basis for analysis.

Within the cybersecurity industry, the use of hacking skills in an ethical framework has been categorised using a coloured hat metaphor. A 'white hat' is someone who utilizes their hacking skillset within a legal context and is responsible for finding any security flaw before a malicious hacker or 'black hat' can exploit them (Froehlich & Bacon, 2021). Therefore, given the rise in cybersecurity threats and advent of the IoT devices, the demand for white hats have skyrocketed (Terra, 2023).

However, the role and the responsibility of an ethical hacker is challenging. By gaining access and analysing the private system of the employed company i.e. passwords, network architecture, private databases etc, the white hat is essential in ensuring the company's continuity. Any mishap, data leak or successful attack will immediately start investigation(s) and scrutiny. Hence, the way in which a white hat behaves will constantly be evaluated and is of utmost importance.

Furthermore, the ethical outline and tough moral decisions of a white hat can be difficult to navigate. Ethical hackers must balance the benefits of identifying vulnerabilities and improving security against the potential harms that may result from their actions. Likewise, the employer is not only trusting the technical abilities of the white hat but also relying on the loyalty, secrecy, and fundamental ethical principles.

Robotic vacuums have become a popular and ubiquitous IoT device which allows people to effortlessly clean their houses and provide better usage of their time (Awa-abuon, 2021). In the next decade, the IoT devices which provide cleaning assistance will become more affordable, accessible and complex (Awa-abuon, 2021). Nevertheless, an audio-hack of the robotic vacuum from Xiaomi, a Chinese consumer electronics manufacturer, was exposed in 2020 (O'Donnell, 2020). Researchers were able to eavesdrop on the homeowners' private conversations utilizing the robotic vacuum's light detection and ranging technology also known as "Lidar" (O'Donnell, 2020). The so called 'LidarPhone' Hack represents the new technological challenges posed for future engineers. Correspondingly, the "LidarPhone" hack

embodies the pervasive IoT devices and thus the ethical challenges of engineers in the future working as white hats.

The teleological ethical outline which is also known as consequentialism evaluates the morality of an action based solely on its consequences. It assesses actions based on their ability to achieve the greatest good for the greatest number of people . The assumption is that people are rational beings who can weigh the potential outcomes of their actions, and ultimately, they will choose the actions which maximise the overall good and limit the overall harm. Within the teleological framework, there are several categories. Namely, utilitarianism which views that right action is the one that brings about the greatest overall pleasure for everyone involved (Mill & Sher, 2002). This leads to the principle of utility which states that actions should be evaluated on the basis of their ability to maximize total pleasure and minimize overall pain (Mill & Sher, 2002).

In contrast, deontology emphasizes the inherent rightness or wrongness of actions, irrespective of the consequences (Green, 2016). Immanuel Kant, the prominent 18th century philosopher associated with deontology, proposed that morality can be based on the principle of the categorical imperative. The categorical imperative can be understood using formulations. Firstly, the universalizability principle which states that one should make a decision or act by considering whether it would be acceptable for everyone else in similar conditions (Green, 2016) . Secondly, the "formula of humanity" which specifies that we should respect the inherent value and dignity of every person and thus never treat them as mere tools to achieve our own interests (Green, 2016).

Using the robotic vacuum hack as an example, the discrepancy between the deontological and teleological frameworks can be explored. The complexity to distinguish between right and wrong given the potential consequences, employment contracts and data sensitivity creates a rift between the deontological and teleological ethical framework.

For instance, suppose the white hat who works for Xiaomi mistakenly doesn't observe the "LidarPhone" security flaw. The actions or lack of defensive measures allowed for the customer's intimate conversations to be spied on. However, the intention of the white hat was to protect and follow the known guidelines and regulations. Perhaps, the white-hat never detected the security flaw or couldn't predict with certainty the outcomes of using the lidar technology. Analysing this hypothetical but realistic zero-day hack highlights the discrepancy between the teleological and deontological perspectives.

From the consequentialist ethical framework, the consequences of the ethical hacker's actions are the determining factor in the moral dilemma. In this example, the white hat never intended for a such a hack to take place, nonetheless, the consequences were dire for all parties- both the customers and the company. Therefore, the circumstances of the mistake or the inadvertent actions are irrelevant, and the white hat is ethically at fault for the outcomes.

Conversely, from the deontological ethical framework, the white hat's actions themselves are judged in moral terms. The intention or motivation of the action itself is considered and is independent of the consequences. Moreover, accidents happen and given the complexity

of the system designed, there will always be unforeseeable consequences. Therefore, the white hat's mishap, from a deontological perspective does not automatically implicate the actions and further investigations would have to specify responsibility.

Similarly, imagine the circumstance where the white-hat, working for Xiaomi, finds the lidar vulnerability. The white hat has successfully performed the job, however, it comes with the realization that existing customers are at risk and any new customers who buy Xiaomi's robotic vacuum should be informed. Nonetheless, the job responsibilities of the ethical hacker is to notify the supervisors/owners of Xiaomi, however, is it ultimately their moral decision? Suppose they continue to sell the same robotic vacuum, what is the white-hat ethically expected to do?

In the teleological view, the white-hat is morally obligated to apply the principle of utility, meaning to act based upon what will produce the greatest good for the greatest number of people. Therefore, the white-hat must weigh the potential consequences caused by the vulnerability against the harm that could result from disclosing it, such as damage to the company's reputation, financial losses or ultimately the white-hat's employment status.

Cognitive dissonance describes the situation where a person has conflicting attitudes, beliefs, or behaviours (Mcleod, 2023).To resolve cognitive dissonance, humans have a natural tendency to rationalize or justify their behaviours and actions. This can consist of pursuing information or perspectives that support our existing beliefs, dismissing evidence that contradicts them, or finding alternative justifications for our actions (Mcleod, 2023).

Accordingly, the ethical hacker could justify that whistleblowing about the vulnerability would result in more harm than good. In order to protect personal interests and avoid cognitive dissonance, the white-hat will rationalize not disclosing the vulnerability by downplaying the potential harm to the customers of Xiaomi. Similarly, the white-hat may be influenced by the high value of loyalty to the employer or feeling of indebtedness to Xiaomi and thus decide that reporting the vulnerability would be deemed a betrayal.

Moreover, the white-hat could justify that the company has the expertise and resources to manage the vulnerability internally, without involving clients or the public. Therefore, given the high personal stakes, loyalty and desire to avoid cognitive dissonance , the ethical hacker could utilize the teleological ethical framework to turn a blind eye and substantiate not disclosing the lidar security flaw.

Additionally, the white-hat could be influenced by the contractarianism ethical framework, whereby the emphasis of upholding free and rational agreements defines right actions (Green, 2016). In a contractarian ethical framework, individuals are expected to behave in a way that respects the rights and interests of others, as outlined in mutually agreed-upon contracts (Green, 2016). Therefore, in this example of the ethical hacker who finds the lidar security vulnerability, the ethical response would be to consider the contractual obligations with Xiaomi. It is probable that the agreed upon contract of employment signed by the white-hat necessitates the preserving of confidentiality and protection of company information. Therefore, since the agreed-upon procedures likely conclude that the decision

is determined by executives, the white-hat ultimately is ethically forbidden to expose the security vulnerability.

In the deontological moral framework, the action of non-disclosure is inherently unethical. Despite how detrimental the consequences are for either the company or the white hat, the very action leading to a lack of transparency is morally forbidden. Both Xiaomi and the white-hat have the ethical obligation to act in the best interests of the customers.

Initially, the white-hat has the duty to report the security flaw to Xiaomi. Thereafter, Xiaomi has the responsibility to reveal the vulnerability to the customers and take crucial steps to mitigate it. Xiaomi has the duty to respect the privacy and safety of its customers. This is consistent with the principle of the categorical imperative, which requires the treatment of customers as ends in themselves. By failing to disclose the vulnerability, Xiaomi would be treating its customers as means to some other end, for instance in maintaining its reputation or avoiding financial losses. Therefore, according to Immanuel Kant , Xiaomi as well as all their employees have a categorical imperative in ensuring their customers are provided with full transparency , safety and security regardless of the impending consequences.

However, if Xiaomi does not adhere to its moral responsibility to divulge the security flaw, they are violating the categorical imperative and the moral accountability falls to the white-hat. Ensuring the transparency , safety and security of Xiaomi's products is paramount and cannot be superseded by other concerns such as reputation, financial losses or even unemployment. Kant would contend that every ethical hacker who finds a security vulnerability has a duty to ensure the customers are appropriately informed and protected. The white hat has an universal obligation to disclose the lidar vulnerability to both existing and potential customers of Xiaomi. Therefore, failure to adhere to the categorical imperative would deem the white hat as an immoral actor.

Likewise, within the deontological moral framework the white-hat's loyalty does not lie with the bosses at Xiaomi, but rather with the categorical imperative. Even if the white hat does not oblige to the contractual agreements, Xiaomi in essence has already broken their universal ethical duty. Furthermore, by following the clear and consistent guidelines of the deontological framework, the white-hat will not have to avoid cognitive dissonance , and as a result align all actions with that of the categorical imperative.

However, the deontological moral framework works in this example due to the evident lack of transparency and disregard of customers safety from Xiaomi. What if the security flaw is not discernible or is ambiguous? The white-hat would be required to do additional analysis, testing and research to ascertain the true extent of the vulnerability or if one even exists. Nevertheless, the rigid and absolute nature of the deontological framework might make the ethical hacker believe in the right to expose the security flaw to the public. However, this could be premature or misguided and thus with a lack of emphasis of consequences the white hat could ultimately cause more harm to both Xiaomi and its customers.

In conclusion, the example of IoT lidar hack of a robotic vacuum was explored to highlight the ethical dilemmas an engineer working in the cybersecurity could encounter. The specific ethical circumstances were investigated and argued form both the teleological and

deontological ethical guidelines. The teleological ethical framework did not account for the specific circumstances, intentions, or inner conflict of the ethical hacker. In contrast, the deontological ethical framework provided compelling and resolute principles yet could be regarded as unrealistic. In essence, as the field of engineering grapples with the complex ethical challenges associated with securing the Internet of Things , a hybrid approach that incorporates both deontological and teleological principles will be essential for future engineers.

Bibliography

1. Awa-abuon, J. (2021) *How does a robotic vacuum work?*, *MUO*. Available at: https://www.makeuseof.com/how-does-a-robotic-vacuum-work/#:~:text=What%20Is%20a%20Robotic%20Vacuum,own%20without%20any%20human%20intervention. (Accessed: March 16, 2023).
2. Froehlich, A. and Bacon, M. (2021) *What is a white hat hacker?*, *Security*. TechTarget. Available at: https://www.techtarget.com/searchsecurity/definition/white-hat (Accessed: March 14, 2023).
3. Green, H. (2016) *Contractarianism: Crash course philosophy #37*. YouTube. Available at: https://www.youtube.com/watch?v=2Co6pNvd9mc&t=177s (Accessed: March 20, 2023).
4. Green, H. (2016) *Kant & Categorical Imperatives: Crash course philosophy #35*, *Kant & Categorical Imperatives: Crash Course Philosophy #35*. YouTube. Available at: https://www.youtube.com/watch?v=8bIys6JoEDw&t=186s (Accessed: March 21, 2023).
5. Lam , J. (2022) *The future of IOT: What should we expect?*, *IoT For All*. Available at: https://www.iotforall.com/what-can-we-expect-for-the-future-of-iot (Accessed: March 11, 2023).
6. Mcleod, S. (2023) *What is cognitive dissonance? definition and examples*, *Simply Psychology*. Available at: https://simplypsychology.org/cognitive-dissonance.html (Accessed: March 21, 2023).
7. O'Donnell, L. (2020) *Robot vacuums suck up sensitive audio in 'LidarPhone' hack*, *Threatpost English Global threatpostcom*. Available at: https://threatpost.com/robot-vacuums-audio-lidarphone-hack/161421/ (Accessed: March 16, 2023).
8. Terra, J. (2023) *White Hat hacker - roles and Responsibilities*, *Simplilearn.com*. Simplilearn. Available at: https://www.simplilearn.com/white-hat-hacker-article (Accessed: March 16, 2023).
9. Mill, J.S. and Sher, G. (2002) *Utilitarianism*. Hackett Publishing Co, Inc.