

Investigating kevin mitnick and computer hacking philosophy essay



**ASSIGN
BUSTER**

The main character of this case study Kevin Mitnick is known to be an expert in computer technology. The main theme of this case study is how he uses his expertise to exploit the utilization of his field. The case study explains how Kevin goes against the key ethical behaviors by misusing his skills causing disturbance to privacy and also immense security problems. Hence from the perspective of three ethical theories namely, consequence based, duty based and the character based ethical theories, the actions of Kevin are analyzed in this coursework.

The following part of the course work then aims at analyzing the role of an engineer with regard to hacking. It explains the limitations that an engineer is bound by and also how an engineer has to make use of his skills keeping in mind the interests of public. The role of an engineer becomes more significant as the engineering and technological segments have rapid advancements and improvements. The advancements and improvements can be of the entities associated with these segments in terms of quality and quantity. One of the reasons for this rapid development is the dependency of the world on communication. Though there are fast advancements the contrary part is that, these advancements can be ethical or unethical.

One of the classic examples for this is cyber space, on which even the case study is based on. Due to high demand for communication, rapid developments are made in the field of internet and networking which gives easy path for the hackers to produce consequences that can be catastrophic for an entire section of society or thousands of people. This problem of technology having the capacity of both good and ill (i. e. ethical or unethical) has been called the dual use dilemma [2]. The dual-use dilemma arises as a <https://assignbuster.com/investigating-kevin-mitnick-and-computer-hacking-philosophy-essay/>

consequence of the fact that the same piece of scientific research sometimes has the potential to be used for harm as well as for good. The below sections evaluate the different ethical issues which the case study presents with respect to the three different ethical theories.

1. 1 About the case study:

The case study illustrates how Kevin utilizes his skills for several illegal works which raises the question of ethical issues. Most of Mitnick's actions show that he has performed hacking only for challenges or sometimes to take revenge on people. None of his actions illustrate that he was greedy about financial gain but he has had a very long history of computer misuse.

When he was a teenager he learnt to hack the public school district's computer system and also he had hacked into a telephone company's computer system and altered the phone bills. When he was punished for this offense he hacked into the company's system again and disconnected the probation officer's phone line. He also stole software from the companies by hacking and also changed his conviction records in the police computer files. He made use of companies' networks to make free long distance phone calls and also tried to plant a false story against a company which refused to offer him a job.

Mitnick had even hacked into computers of North American Air Defence Command (NORAD) in Colorado Springs. NORAD was a warning system which could detect missile attacks directed towards United States. Damages made by hacking into such systems can have catastrophic effects on a very large geographic area [1]. But however the biggest blunder which Mitnick

committed was breaking into the San Diego Supercomputer Centre which led to his arrest.

1. 2 About Hacking:

Computer hacking is broadly defined as intentionally accesses a computer without authorization or exceeds authorized access. Also various states and federal laws govern computer hacking [3]. Usually people who engage in computer hacking activities are known as Hackers. Computer hacking can be ethical or unethical based on the scenario, how the hackers skills are being used. If a hacker is employed by a company to find flaws in the company's security system by trying to hack to the companies system then the hacking is ethical since the hacker has been employed by the company themselves. This kind of ethical computer hacking helps to prevent identity theft and many other computer crimes. The skills which the hackers have can be used in a constructional way for developments of technology. An example for this is, Dennis Ritchie and Ken Thompson who were previously hackers developed the UNIX operating system [4].

In [1] the hacker code of ethics from Levy [2001] provides an illustration of origin of hacking. The origin of hacking trails back to gaining access to the computers which were faulty to set the problem right which were common in those computers. All the information of the computers was required by the hackers to analyze, identify and fix the problem. This initiated the drift for hacking computers which are now being misused. This case study shows how Mitnick misused hacking.

2. Consequence Based Ethical Theories:

In this segment all the ethical issues are analyzed based on the perspective of Consequence based ethical theories. According to Consequence based theories [5] a person's action is said to be morally right if the best attainable consequences are obtained in the situation or if the best attainable consequences are obtained if everyone performs the action in that sort of situation. What makes it right or wrong is just the goodness or badness of the consequences of action. These theories are often known as utilitarian theories because these theories usually involve the notion of utility in producing good consequences.

In [1] a moral system is described to be informal where as co-existing by respecting each other's moral value is found in a society. Hence one should not go beyond the moral limits which can create dreadful consequences for the others in the society. For example, a person playing music for him with very soft sound would not affect others but if he plays the music very loudly then that can become noise to the rest of his neighbors and disturb them. Similarly in this case study as well, Mitnick though he does not hack computers for financial gain, he trespasses the privacy of other people in the society.

Several consequences raised because of Mitnick's action have given a harsh blow to the privacy and security of the people in the society. Though in some cases Mitnick hacked the company's database to take revenge on the companies or just as a challenge, the personal information about the customers which are stored in the company's database was intruded and

exposed which was a major security breach. Hence Mitnick's actions which in turn created some consequences had adverse effects on the society.

One of Mitnick's major action which could have had a large impact on the society was he had planted a false story against a company which had refused to offer him a job. But fortunately this false story was sensed before it reached the society and it was terminated. If this false story had reached the society then it would have created a negative impression for the employees and the investors of the company against the company. In terms of consequences, the recent development of internet and the search engines can give way to easy spread of information and also easy access to databases worldwide. These can in turn give way to disasters which are caused by criminal and terrorist activities.

Tavani in [2] also gives us another feature of consequence based theory which is explained by Moore. Moore explains which values are essential for the survival of the society. Those values are happiness, life and autonomy. Moore also says that, for an individual to attain these core values, a proper balance has to be maintained in the society. If the individual's actions disturb any one of these values then it creates an imbalance in the society and hence directly affecting to loss of any of these three core values which in turn creates several problems.

Even in countries where individualism is given more importance, Mitnick's actions are considered to be not morally correct. When we consider his hacking scenarios, it goes against his own (or an individual's) moral boundary. A responsible citizen of a society has his own moral duties towards

the society in order to co-exist with the other citizens in the society which Mitnick did not fulfill. His actions like hacking into a company's database to make long distance calls, planting false story against a company and using false identity for getting driver's license could have had severe effects on the society. As an individual Mitnick failed to distinguish between the good and bad, also he failed to judge what consequences his actions could create for him as well as the society. Hence we can conclude that Mitnick has gone against his ethical principles with respect to Consequence based theories.

Another consequence based theory is Utilitarianism. This philosophy of utilitarianism was developed by John Stuart Mill (1806-1873) as stated in [2]. The theory of utilitarianism [6] states that " the belief that the right act in any situation is the one that produce the best overall outcome which gives equal consideration on everyone's interest". The utilitarian approach [7] assumes that the utility principle can be expressed as " the greatest good of the greatest number" should be the basis for determining the property entitlements. Utilitarian theories can be divided into 2 types. They are

Act Utilitarian theory

Rule Utilitarian theory

2. 1 Act utilitarianism:

According to Act utilitarianism, any consequences produced due to an action performed, which in turn does the greatest good to great number of people then such an action is said to be ethically correct [1]. In order to define the right act, we have to first find the entire alternative act for that situation and also the net utility function for them [5]. From the entire acts, the act which <https://assignbuster.com/investigating-kevin-mitnick-and-computer-hacking-philosophy-essay/>

has the greater net utility can be defined as the right act. To do any of these other alternatives would be wrong because to do any of them would not be to maximize the balance of positive over negative value in the world, and a person's duty is always to do that which has such maximization as its consequence. Sometimes the Act utilitarianism can be known as Situation ethics.

According to act utilitarianism, hacking (unethical hacking- without the permission of the owner) is morally incorrect. Hacking only gives personal gain to the hacker while it destroys the privacy and data of the entire society and also destroys the entire security system set up by the company. Hence hacking cannot be a permissible act in act utilitarianism theory.

In the case study, we can see many incidents of Mitnick hacking into different databases for different missions. Once he hacked into a company's network to make long distance calls and deceived the company of its bills. He also planted a false story of the financial conditions of a company which refused to offer him a job which made the company suffer huge losses. He also hacked into the security system of United States which was designed to detect missile attacks directed towards the country. The first two acts had adverse effects only on those companies but the third act had an impact on a whole country which had a very huge population. These actions of Mitnick made only Mitnick happy while the rest of the society had a negative impact which was very much against act utilitarianism. Hence we can again conclude that Mitnick had gone against the ethical principles with respect to Act Utilitarianism.

2. 2 Rule Utilitarianism:

Rule Utilitarianism [8] is the view that rightness or wrongness of an action is to be judged by the goodness and badness of the consequences of a rule that everyone should perform the action in like circumstances. This theory usually tells us how to act in a particular situation by simply framing a rule rather than thinking which action would create the best consequence for that particular situation. These rules have to be determined by retrospective calculation of which possible rules have the greatest net utility. Following the rules may seem right but sometimes it may not give the best consequence. Act Utilitarians use situation-by-situation calculations which are rejected by the rule utilitarians. This situation-by-situation may not precisely predict the consequences of the actions and also they are not very reliable and efficient.

When we try to apply rule utilitarianism to the case study, then we can observe again that Mitnick has gone against many rules and policies of the society. He tried to have false identity for himself for the driver's license and also posed as a police officer to get the driver's license information which was very much against the rules made by the society. Also Mitnick tried to hack into a company's network to make free long distance calls again trying to trespass others property without their permission. All of these acts show that Mitnick had gone against the rules and also the consequences of those actions had only negative impact on the society. Hence we can again conclude that Mitnick had gone against the ethical principles with respect to Rule Utilitarianism.

One of the main disadvantages of Consequence based theory is that it does not give importance to an individual's feelings or the minority people. Hence <https://assignbuster.com/investigating-kevin-mitnick-and-computer-hacking-philosophy-essay/>

there are many critics against utilitarianism and consequence based theory. Immanuel Kant argues against consequence based theories and says that importance has to be given to duty performed by the individual instead of the consequences which arise due to their actions.

3. Duty based Ethical theories:

Constitution of every country prescribes that it is the foremost duty of every citizen of that country to respect the laws and regulations of the country. In a similar way, it is the duty of every citizen to respect the other fellow citizens and also the confidentiality and privacy of other entities has to be protected as specified by the law of the country.

Duty based ethics are concerned with what people do and not with the consequences of their actions [9]. Duty based ethics is also known as Deontological ethics. The word 'Deontological' comes from the Greek word deon, which means 'duty'. These theories are sometimes called as nonconsequentialist as we cannot justify an action if it is going to produce good consequences or not [10].

Immanuel Kant (1724-1804) who was one of the greatest philosophers of all time standardizes deontology as categorical imperative. This system is based on two essential principles namely:

Universality

Impartiality

Universality implies that the rules and regulations implies to every person on this universe. Hence everybody has to follow the rules and going against the rules would imply that the person is unethical. Impartiality implies that the law is for everyone irrespective of the caste, religion or race. According to impartiality there should be zero distinction between all humans. It also states that everyone should treat others as equal and also abide by oneness.

In this case study Mitnick tries to have unauthorized access a company's database which has so many people's information, which is against the law of the country. By not fulfilling his duties and going against the law of the country, Mitnick is unethical with respect to the universality principle of deontology. Mitnick also tries to take revenge on a company which did not offer him a job by planting a false story about the company. From this false story the company had to suffer huge losses. These actions show that Mitnick never treated everyone equally. He distinguished between the common man and the people whom he hated. This action of Mitnick again shows that he was unethical with respect to the impartiality principle of deontology.

From the above actions of Mitnick, we can again conclude that Mitnick had gone against the ethical principles with respect to Deontological ethics.

Duty based ethical theories is also not completely accepted by everyone and there are critics for the same. In [11] a practice has been explained in which each other's duties are respected and it is known as contradictory beliefs.

Because of this it leads to many conflicts and confusion. Also another critic by name Ross argues that if two duties conflict with each other, there can be

confusions in the prioritization of both duties which are equally important.

Hence another theory has been made which gives more importance to moral virtues based on character.

4. Character Based Ethical Theories:

Character based ethical theory can also be known as virtue ethical theory which judges a person by his character rather than the person's action or the consequences that occur from the action [12]. In this theory, to judge various situations ethically the character of a person plays a very important role. The character of the person influences the decision taken. A person is said to have good character if he possesses good moral values such as love, kindness, honesty, courage and affection. Hence to take good ethical judgments one should have the right traits. The evolution of Character based theory evolved since the time of Aristotle. This theory was the reigning theory for ethical thinking during the ancient and medieval periods. The virtue theory contrasts with Consequentialism, which gives more importance to consequences which occur from the actions, and also Deontology which gives more importance to the rules and laws made rather than the outcome of the action.

In character based ethical theory, an individual is fully aware of his duties towards the society and he can decide whether he wants to be a responsible citizen or not. The reaction between talent and character of an individual is the main constraint for the emergence of character ethics. An individual can master the subjects in his area and reach a very high level due to his talents but it is the method how the individual will utilize the talent. He can make good use of it or a bad use. In other words the individual can create things which

<https://assignbuster.com/investigating-kevin-mitnick-and-computer-hacking-philosophy-essay/>

are constructive for the society or he can even create things which may be destructive for the society.

In the case study, character based ethical theory seems to be more appropriate to discuss the actions of Mitnick. We see that Mitnick is very well versed with computers i. e., has good talent to handle computers. Also he shines well in the field of cyber communication as well. Mitnick could have used his talents to do something best or constructive for the society but instead he chose to use his talents for his own benefits and to fulfill his desires. All the actions of Mitnick in the case study show that Mitnick did not have good character. A person with good character will try to help in welfare of the society keeping in mind everyone's interest but a person who is morally wrong will only create a havoc in the society. Similarly Mitnick also did not do anything for the society but instead he created many more problems to many people in the society. Again even in this theory it proves that Mitnick was unethical from the point of Character based ethical theory.

5. Prosecution of Kevin Mitnick:

To make a decision, all the ethical theories and their principles contribute some significant characteristics. Even though all the ethical theories try to validate themselves and also try to follow the ethical principles they will have some flaws and failings. On the other hand, all the ethical theories can be combined and used to provide the most ethically correct answer for the scenario. For example, if a person breaks speed limit rule, then a utilitarian will use the caustic theory and say if only somebody is hurt due to over speeding then the person has committed a mistake but a deontologist and rule utilitarian will say that the person has gone against the rule and hence <https://assignbuster.com/investigating-kevin-mitnick-and-computer-hacking-philosophy-essay/>

he is wrong. Hence in this way combining the ethical theories we can get variety of ways to analyze a problem and provide the most ethically correct solution.

In the case study we studied all actions of Mitnick and its outcome, applied all the three ethical theories to his actions to conclude what Mitnick did was ethically correct or wrong and also the prosecution of Mitnick. As we have discussed all the three ethical theories above, we see that one or the other actions of Mitnick is wrong with respect to all the three ethical theories from which we can conclude that he was ethically wrong. Mitnick did not care about his society or the consequences that the society has to face because of his actions. He never treated everyone equally and had the characteristic of taking revenge. He also went against the laws of the society. He did not possess the noble virtues when he committed the cyber crimes. Hence Mitnick was ethically wrong.

A piece of article is extracted from the United Nations Organization which is regarded as the world governing body. This law holds good for all the hackers irrespective of the country they commit the crime including Mitnick.

The Universal Declaration of the human rights, United Nations [13] states that:

“ Article 3

Everyone has the right to life, liberty and security of person.”

“ Article 12

No one shall be subjected to arbitrary interference with his privacy, family,

home or correspondence, nor to attacks upon his honour and reputation.

Everyone has the right to the protection of the law against such interference or

attacks.”

From the above stated laws and also the evidence obtained from Tsutomu Shimomura (the last hacking of Mitnick before his arrest), it clearly shows that Mitnick had gone against law and requires to be punished. In order to support this decision we have also discussed the three ethical theories which are again against Mitnick and proved that his actions were ethically wrong. Hence the FBI was correct in attempting to capture and prosecute Mitnick.

5. 1 Conclusion:

The case study gives us a clear image about Mitnick and his actions in the world of computers. In order to justify what Mitnick did was ethically right or wrong; we studied all the three ethical theories and applied the same to the case study. By doing so we could conclude that Mitnick’s action was ethically wrong. This case study also throws light on crimes happening in the cyber world. It also alerts us that if proper precaution is not taken in stopping such crimes then it could lead to terrible conditions. Hence appropriate steps have

to be taken to reduce cyber crime and to make the society safer. Another stimulating fact in the case study is Mitnick is punished for only 22 months and then kept under probation for 3 years after which he is free to use the computer and internet as he chooses. Is the 3 year probation period enough to reform Mitnick? Also is there any monitoring made on Mitnick after he is completely released? It also raises a question as to how long the hackers should be monitored.

6. Role of an Engineer with regard to Hacking:

As seen in Tavani [1], the engineer has the unique expertise of studying the theoretical aspects and implementing his knowledge in a practical manner. Engineers have extra ordinary talent to transform the given piece of work into a final product which can be used. To ensure success in both business and profession, good reputation is required. An ethical approach to work is consistent with this as it encompasses competence, integrity and the personal and professional values that support it [14]. The engineer's ongoing stand with the engineering community and the clients is enhanced by these values. The engineer has to keep in mind the below features while he creates the product according to the requirements of his clients. The features are:

Protection of life and safeguarding people

Professionalism, integrity and competence

Commitment to community well-being

Sustainable management and care for the environment

Sustaining engineering knowledge

Hacking as defined earlier is an intentional access to a computer without authorization or exceeds authorized access. The individual who performs this action is called a hacker. Earlier hackers were the individuals who were employed by a company to hack the security of that company to check how strong it is. This was ethical but now hacking is used mostly to gain access to unauthorized information which is against the privacy of the individuals.

In Tavani [1] it explains that hardware professionals design the system while application engineers analyzes the product with respect to its application and the software engineers are concerned only with development of the software for the product. The engineers who design this product from the start to the end should also be capable of finding the loopholes of the product as well which can give way to hacking and also they should be well aware of the consequences. From the above discussion of the case study we can see how damage hacking can cause on the individual and also the society, how it could tamper the privacy of the individuals. In order to stop these engineers should design much stronger system. Also a team of engineers can be set up to reduce the cyber crime rate and also have more strict laws and fines against the individuals who commit cyber crimes. In the given case study Kevin who was a computer security consultant used his skills to gain illegal access to many companies and changed many information. He misused his skills for his own benefit and to take revenge. Hence the role of an engineer plays a very important role in hacking. An engineer should develop technologies which are beneficial to the society as

well they should be fault proof, should not have any loopholes for hackers to access the data.

The Association of Computing (ACM) and the Institution of Electrical and Electronics Engineers (IEEE) together have recommended eight principles [15] which the engineers have to abide by in order to make the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. The engineers should adhere to these principles to maintain the health, safety and welfare of the public. Hence it becomes the moral duty of an engineer to protect the society against hacking which exploits the welfare of the society.

6. 1 Conclusion:

Computer hacking and the effects of hacking on the society is studied in detail with respect to three ethical theories in this coursework. Then the role of engineer with regard to hacking and its effects on the society is discussed in detail. From the above discussion we can wrap up by concluding engineering and welfare of society goes hand in hand. Hence the engineer has the prime responsibility in maintaining the welfare of the society.