Examining hacking and cyber ethics philosophy essay

With technology taking the forefront in communication, world has virtually shrunk! Distance and time are no more any hindrances for effective interactions and communications. Internet has so much invaded our day to day lives that without internet, we feel we are almost without bread!

As any advances bring in good , not so good and bad with it-take auto mobiles, electricity, movies whatever-even the communication technology has its own goods and bads.

Hacking is something that has shocked the world that is so much dependent on the cyber for its day to day affairs, may it be individual corporate or education fields.

Hacking and Hacker

Hacking is an action of trying to gain access to a computer or computer network without any legal authorization [1]. The entity who tries the act of hacking is the hacker. The new hacker dictionary defines hacker as below:

A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.

One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.

A person capable of appreciating hack value.

A person who is good at programming quickly.

An expert at a particular program, or one who frequently does work using it or on it.

An expert or enthusiast of any kind. One might be an astronomy hacker, for example.

One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.

[deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence ‘ password hacker’, ‘ network hacker’. The correct term for this sense is cracker.

Hacker is someone who has an intention to damage a system and hence invades it illegally [2]. He or she might invade into the system to get illegitimate access to resources.

As hacking becomes easier, a vulnerable computer will be the earlier target. Hacker invariably tries to hide his or her identity for launching attacks on the main site, which is generally more secure. The attack is made with an intention of gaining control of the targeted system so that the hacker can execute, edit or delete any file on the user’s directory. This is achieved generally by gaining access to the ‘ super-user’ account. This helps the hacker hide his presence and provides him maximum authority to access the data. Software bugs are generally used in the attacks which give the hacker super-user status.

Ethics and Cyber Ethics

That branch of art which looks with wonder at the marvels and mysteries of the world is philosophy. It leads to life with passion, moral and intellectual integrity. Socrates had once stated “ the unexamined life is not worth living”. In philosophy. Everything related to life is critically and comprehensively inquired in to. The branch of philosophy that deals with how we ought to live, with the ideas as to what is right and wrong, and with idea of Good is ethics [3].

The field of ethics that examines legal, moral and social issues in the use and development of cyber technology is cyber ethics [4]. A broad spectrum of technologies that range from standalone computers to a cluster of network computing, information and communication technologies is referred to as cyber technology. Computer ethics has been the general usage term for cyber ethics until recently. Computer ethics however suggests the study of ethical issues associated primarily with computing profession or computing machines. Cyber ethics however attempts to address ethical issues that are more wider and deeper. Other terminologies like “ internet ethics” or “ information ethics” are in use but cyber ethics has wider coverage than “ internet ethics”.

1. 3 Legal and Illegal Hacking

The informal trespassing into a computer is termed as hacking by many people. Hacking in general has formed a meaning of breaking into computers [5]. The term hacking clouds ethical and legal complexities of law that administrates use of computers. Some hacking is legal and valuable while some are illegal and destructive. Learning the way to get access is legal

while using this information to access the system and misuse it is illegal hacking. It is very important to understand the difference between legal and illegal hacking. This could be understood considering an example. For example, the security researcher of the system will learn a number of ways to get into the system without authorization. While learning this information is not illegal, using the information to access a system unauthorisedly is illegal. An action can be considered legal or illegal based on the scenario and the access and authorisation for the particular scenario.

1. 4 Ethical Theories

Ethical issues are based on morals which are subjective. The ethical theories offer direction for the moral analysis to be made. These are the scientific theories that provide the framework for the analysis of moral issues.

We may look into ethical theories relevant to the case in hand.

1. 4. 1 Consequence Based ethical theories (consequentialism)

Consequence based theories judge actions based on results. Proponents of these theories assume that certain state of affairs are better than many others. Actions that lead to better state for maximum number of people are better actions. In simple words, an action that makes the world better is a good action and that worsens the world is bad. Hence here, result is most important.

“ Three subdivisions of consequentialism emerge based on who is benefited by the action:

Ethical Egoism: an action is morally right if the consequences of that action are more favorable than unfavorable only to the agent performing the action.

Ethical Altruism: an action is morally right if the consequences of that action are more favorable than unfavorable to everyone except the agent.

Utilitarianism: an action is morally right if the consequences of that action are more favorable than unfavorable to everyone".(QuoteIEP)

Types of Utilitarianism

Two types of Utilitarianism are there namely Act Utilitarianism and Rule Utilitarianism. Under Act Utilitarianism, an action is considered good or bad based on its consequences while under Rule Utilitarianism, a code or rule of conduct is more acceptable if the consequences of it are beneficial than not beneficial to every one. For ex. If one steals, it may be beneficial to him but not to all. So the rule is not to steal.

Intended Consequentialism

Intended consequentialism is a consequence based ethical theory. Here, intended consequence is given importance over actual consequence in judging an action.

1. 4. 2 Duty Based ethical theories

Duty based ethics is otherwise called deontological theory. Deon is a Greek word meaning necessary, binding, obligatory. Immanuel Kant is the main proponent of this theory. It gives importance to sticking to ones duty and principle rather than the consequences. When most stick to Deontological

principles, naturally, consequences will be good. The focus is on duty and principle and not on consequences.

An other famous philosopher W. D. Ross who supported Kant's theory, summarized basic duties as below:

Duty of beneficence: A duty to help other people (increase pleasure, improve character)

Duty of non-maleficence: A duty to avoid harming other people.

Duty of justice: A duty to ensure people get what they deserve.

Duty of self-improvement: A duty to improve ourselves.

Duty of reparation: A duty to recompense someone if you have acted wrongly towards them.

Duty of gratitude: A duty to benefit people who have benefited us.

Duty of promise-keeping: A duty to act according to explicit and implicit promises, including the implicit promise to tell the truth.(M2)

Character based Ethical Theories

Character based virtue ethics is also called Virtue ethics. These theories are mostly based on Aristole'philosophy. Here, individual's character takes prime place over duty or consequence, in contrast Deontology and Consequentialism respectively. Here, the tenet is once the person has strong value system which has stabilized, he would be conscious of what is wrong and what is right, what are his duties to his children, family, society and his

master, so, action taken by such persons tend to have good consequences only. An ethical individual is therefore necessarily disposed to do good things acceptable to himself and for society.

1. 5 Role of software/Hardware/Application Engineers

Hacking has become a threat to modern world which is over dependent on information technology. It is easier done than said that, as you keep your valuable protected in house against thieves and robbers by locking the almirah or the house or safe keeping in banks or covering by insurance. As we use lot of IT services through public domains and distant server based technologies, the risks are even more. Professionals in the field can do their bit based on their knowledge and experience to reduce damages by hacking.

Objectives

The objectives of this case study are:

Highlight the main critical issues that this case brings out light and to critically apply consequence-based, Duty-based and character-based ethical theories to discuss whether the FBI were correct in attempting to capture and prosecute Mitnick.

Briefly discuss the general of asoftware/hardware/application engineer in terms of the use dof their knowledge and expertise in regard to hacking.

Facts of the case

While dealing with the case in hand from the point of the objectives of the case study, we have to critically observe the facts from the following angles.

Actions of Mitnick that are subject of ethical and moral nature