ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

SOME EMERGING ETHICAL ISSUES IN COMPUTER SCIENCE AND TECHNOLOGY

Prashant
Assistant Professor
Amity Institute of Behavioural and allied Science
Amity University Rajasthan,
Jaipur (India)

Abstract

The rapid advance of information technology has brought modern society into information age. In this multifaceted world of the information society, traditional ethical question are being reexamined and new one arising as moral standards for human behavior evolve. Computer has become the principal tool for political power, authority as well as providing the opportunity for electronic crime, fraud, surveillance and security. Unique types of ethical problems are associated with computer ethics. The central ethical issues discussed in computer ethics are privacy, and anonymity, intellectual property, computer crime, security and control computer reliability, integrity of data, freedom of information, authenticity, dehumanization etc. This paper would focus light on ethical issues related to computer crime and privacy.

Key Words – Ethics, Computer Crime, Privacy, Security, Dehumanization

The term technology derives from the Greek words techne and logos. Techne was used for the art, craft or skill involved in deliberately producing something. The word techne referred not only to the practical skills of the crafts man but also intellectual activities and fine arts. For Aristotle, techne involves knowledge of the universals and causes, techne along with wisdom (Sophia) and Science (Episteme) is central in the acquisition of knowledge.[i]

Since antiquity man has been exploiting scientific approaches to ameliorate environment making it feasible to reduce human effort at one end while acquiring luxuries on the other. Needless to say the scientific and technical aspects are directly or indirectly linked to human brain and body where the former absorbs the scientific concepts utilizing numerous inventions and discoveries while the latter molds the knowledge to create different tools that finally serve the basic purpose of science-to serve humanity in the best possible manner.

Hans Jonas in his book continues Heidegger's enquiry but on an ethical basis, Jonas maintains that since technology expands human power, there must be an expansion in human responsibility. He argues that because technology changes human condition and life at local and global level, it engages humanity in a new perspective of ethics.

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal

Computer ethics is a field of enquiry originates from the work of Prof. Nobert Wiener, who first foresaw the revolutionary social and ethical consequences of Information Technology. Wiener, in his book Cybernetics: or control and communication in the animal and machine and the human use of Human Beings, establishes the theoretical background for computer ethics.

The term computer ethics was first introduced by Walter Maner in the mid 1970's referring to the field of philosophical inquiry that deals with ethical problems aggravated, transformed or created by computer technology. The first complete presentation of the nature of the computer ethics appears in the influential articles of James Moor (1985), entitled 'What is Computer Ethics'. According to Moor ' Computer Ethics' is to be defined as the analysis of the nature and social impact of computer technology and corresponding formulation and justification of policies for the ethical use of such technology (Moor 1985).[ii]

An organized and methodical study of the ethical and the social impact of computers on the society fall under Computer ethics involving the acquisition, distribution, storage, processing and dissemination of digital data in an information system besides the utility and interaction via different approaches amongst individuals and groups. The moral implications of computer ethics are include to the responsibility and accountability of computer users and professionals with regard to design and implementation of information system.

The computer technology has resulted in cropping up of many ethical issues including over amplification of traditional ethical issues and conversion of the earlier problems into corresponding new problematic zones. Further, creation of entirely new ethical problems also can't be ruled out.

An ethical action is inclusive of intentions turning to actions resulting in consequences. All aforementioned factors are pivotal in all three groups of ethical theories relevant to computer ethics: virtue ethics, deontological ethics and Consequentialist ethics for consequences.

The Aristotelian philosophy defines ethics as s a practical science that deals with character and behavior of the individual within any community whilst his moral theory rests on fundamental distinction between means and ends. Means are the actions done for sake of something else. There must be end of all means and the ultimate end of all the actions must lead to happiness and contentment. Happiness is the activity of the human soul in accordance with reason.

Coincidentally moral virtue is an intermediate state, i.e. falling between two extreme states: deficiency and excess. For instance, the virtue of courage is a mean between feeling of fear and indiscretion; hence all choices of the moral agent have to be for actions between alternatives based on the concept of golden mean – a mean relative to the abilities of the moral agent. Based on this rationale freedom is a presupposition for ethics. The moral agent becomes good and happy not only by choosing the right action but in ensuring its right execution

The Deontological ethics, declares or categorizes the right or wrong actions in their core of occurrence while completely ignoring any basis of their categorization on the basis of their consequences either for an individual or on the society as a whole. Good will determines our choices of action in accordance with the commands of duty. Only good will is good in itself and an action is good only if it is done from a sense of duty i.e. when it is based on good intentions that are rationally recognized by the moral agent independently of the consequences of the action or the preferences of the agent. A rational agent must rely on the objective moral principles of a universal moral law and not on subjective moral principles or personal preferences.

According to Utilitarianism, rightness or wrongness of an action is judged by its consequences rather than intention of the agent or any intrinsic rightness or wrongness of the act in itself. The fundamental imperative of utilitarian theory is: always act in a way that will produce the maximum number of good consequences and least number of bad consequences in the world as a whole. This imperative is known as principle of utility. On this basis, the aim of utilitarian ethics is to maximize good and minimize suffering for the greatest number of people.

The mushrooming of personal computers and advanced technical as well as informational technology besides earning new laurels to serve humanity has also opened an arena for vices that can easily surpass the virtues. This arena has resulted in numerous malpractices leading to electronic crime and illegal activities. The illegal activities related to computers and computer networks are usually classified as computer crime.

The national Institute of Justice defines computer crime as 'any illegal act for which knowledge of computer technology is used to commit the offence'.[iii] (McEwen 1989)
Forester and Morrison define computer crime as ' any criminal act that has been committed using computer as a principle tool.'[iv] By Forester and Morrison (1994)

Herman Tavani maintains that a 'criminal act is one that can be carried out only through the use of computer technology.'[v] (Tavani 2004)

In a computer crime, the computer can be involved actively (computer assisted crime) when computer is used to commit the crime (computer sabotage and hacking), or passively (computer related crime) when computer is used indirectly to commit the crime (e.g. record data for all illegal weapon dealing). Some computers crime are transformation of old crimes, such as espionage, theft, fraud and sabotage others are entirely new kinds of crimes such as trespassing in computer networks, cyber terrorism and computer sabotage.

The nature of computer crime is antiseptic, involves little physical danger for the computer criminal, has low risk of detection and can appear to be more like a game rather than a crime of the traditional kind. Hence most computer crimes are erroneously considered victimless crime with no serious consequences. As a result analyst believes that the actual amount of computer crime is much greater that reported.[vi](Cornwall 1986)

The difficulty in detection of crimes via computer and shielding of the same crimes for publicity reasons by the owner companies are the two main reasons that has lead into the deliberate or accidental crimes by the computers.

Computer crime is also related to computer abuse: the use of computer systems to perform irresponsible or unacceptable acts such as sending electronic messages with offensive language or pornographic material and spam, unsolicited or illegal electronic messages sent automatically to bulk recipients, usually for advertisements. This problem is more evident in internet community. Computer abuse may bring financial and managerial problems to companies and business by affecting the efficiency of computer system. (e. g. low performance of network server , introduction to viruses into systems) and by reducing the productivity of the employees (e.g. wasting time reading and deleting non work related materials , leaving work related material unread.)

In order to minimize the problem, Internet providers have established security measures, such as antivirus systems, filtering anti spam software and firewalls. Internet users are encouraged to block and report unsolicited messages.

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal

An inherent desire to earn quick money and to perform daring adventures remains the back bone behind all immoral practices done by the computer criminals the lit of which includes software experts, terrorists, student's and other fraudulent experts. The illegal activities of these lead to destruction of data in companies, especially financial firms like banks and sensitive organizations like the defense offices as well as many government organizations.

Computer fraud can be divided into computer related fraud in which computer is used unintentionally to commit the fraud and computer assisted fraud in which computer is used actively to commit the fraud.

Computer fraud may involve:

(a) Theft of money (e. g. unauthorized transfer of payments to different accounts)
(b) Theft of information (e. g. retrieval of data from database for illegal use)
(c) Theft of goods (e. g. redirection of goods in wrong destination)
(d) Theft of services (e. g. illegal use of cable T V channel)

Various techniques are used to perform such type of theft , the two most important are the ' salami technique' a program fraud that involves drag information over a large no. of transition like slices of salami, and the Trojan horse technique, which involve the insertion of false information into a program in order to profit from the outcome.[vii] Forester and Morrison (1994) Another technique is data diddling in which the fraudster swaps one piece of information for another of the same type.

The most popular computer fraud is

(1) A T M fraud – This fraud is related to bank fraud. The fraudster requires only fake A T M card and P I N of the original customer to commit fraud.
(2) E F T Fraud - Fraudster uses the electronic fund transfer system to transfer money to private bank accounts.
(3) Credit card Fraud – The fraudster steals credit card numbers and the owner's authentication from the internet or a computerized network data base to make illegal purchase.
(4) Internet Stock Fraud – The fraudster pretends to be an investment expert who promises victims quick and easy big profits.

The above mentioned frauds are only some cases of computer fraud, but they clearly present the importance of this problem in the information society.

Hacking: The oxford dictionary of computing defines hacking as 'unauthorized access to computer material. The same dictionary also define hacker is a person who attempts to breach the security of a computer system by access from remote point, especially by guessing or otherwise obtaining a password. Hacker is a person who had an instinctive knowledge enabling him or her to develop software apparently by trial and error.

There is a basic difference between 'Hackers' and 'Cracker' based on intension of computer intruder. The term hacker does not always have a negative connotation / indication and it can equally refer just to a skillful programmer who is obsessive about programming, the term cracker always has negative meaning and it is associated with a person who gains unauthorized access to a computer system for malicious purpose.

A different kind of hacker is the cypherpunk: an intruder who wishes to create new regions of privacy where the system will not able to invade? Through cryptography and

cryptosystems, the cypherpunk aims to bungle the system by spreading hard to break coding schemes throughout the cyberspace.

There is a new term related to hacking is hactivism: the use of hacking for political purposes such as promoting a political cause or spreading anti war messages via the web.

A clear distinction can be made between modern hackers and old hackers. Where early hackers were gifted individuals who exercised their technical skills for self esteem, intellectual challenge and socialization, modern hackers use their skills in order to create malicious damages in computer system.

Steven Levy in his book hackers: Heroes of the computer Revolution, describe vividly the hacker ethics in the 1950's as follows:[viii] (Levy1984) Access to computers and anything that might teach about the way the world works should be unlimited and total.

Levy describes the original hackers of 50's as adventures, visionaries and risk takers who clearly recognized the computer as a revolutionary tool.[ix] (Levy 1984) He further observes that problem of hacking began when software became commercialized and controlled. When software was free and public, there was no reason to gain access and steal information.

Many modern Hackers do not regard hacking as a criminal act. In some cases, a hacker may illegally access a computer system just for curiosity without intending to cause any damage to the system. On the other hand, because computer based information remains copy righted, the event of the system break ins is actually copyright violation. In addition, any computer intrusion without the owner's permission is a clear invasion of the right privacy, from this perspective, hacking is not only illegal but immoral.

Some analysts relate hacking to computer addition and characterize hackers as people suffering from malady and social ineptitude. Hackers are described as people who feel less competent in face to face settings and prefer anonymity instead of publicity. Finally they are described as self taught adolescents who love intellectual games. These adolescents who love intellectual games.

On the other hand it must be admitted that hacking requires a great intellectual ability. Indeed many computer break ins demand incredible inventiveness and cleverness. The Hacker's Dictionary (1983) outlines the hacker persona as follows:

(1) A person who enjoys learning the details of computer system and how to stretch the capabilities as opposed the most users of computers, who prefer to learn minimum amount required.
(2) Who enjoys programming rather than just theorizing about programming.
(3) A person who appreciates hack value (e. g. someone who enjoys gaining unauthorized access to computers).
(4) A person who is good at programming quickly.
(5) An expert on a particular program or one who frequently does work using it or on it.
(6) An expert of any kind.
(7) A malicious inquisitive meddler who tries to discover information by poking around.

Another approach is that of Richard Rosenberg, who describes the hacker more as a skillful and determined programmer:[x] (Rosenberg 1997)

(1) A programmer who works long hours and seems to be strongly motivated by and infatuated with programming.

(2) A compulsive person who is driven to find solutions to problem that are claimed to be extremely difficult or even impossible.
(3) A programmer who produces programs that are not particularly elegant and represent a collection of patches or hacks rather than a coherent whole; such programs are difficult to maintain, modify or verify.
(4) A programmer who breaks into systems to prove that it is possible; no system can resist his or her efforts such a hacker is sometimes called crackers.
(5) A programmer who is a variant of no. 4, but in addition feels that society benefits by his or her actions, in that hidden information is brought to light or proprietary software is made available to the entire community of the programmers.

The last characteristic is very important for the reputation of a hacker and extremely influenced on public opinion. Due to this characteristic, some people regard hacker as heroic persona with rebellious attitude.

The most typical example of such a hacker persona is that of Kevin Mitnick[xi] (Baase 2003) . Mitnick was accused of hacking the computer system of international companies such as Motorola and Nokia and governmental agencies such as North American Aerospace Defence Command and FBI. He was arrested by the FBI in September 1995 and remained in prison until 2000.he was under supervision until 2003, and during this period he was prohibited in the use of any telecommunication technology. Although Mitnick's criminal actions can not be denied, his case raised legal and ethical issues about hacking. Supporters of Kevin Mitnick believed that most of charges against him were deceptive and that his break ins were not criminal actions. Today the name of Kevin Mitnick is synonymous with hacking and many people regard him as a kind of modern hero with an anti-conformist attitude.

Most popular hacking techniques:[xii] by Forester and Morrision (1994).

- **Piggybacking –** the hacker invades a computer system by pretending to be a legitimate user of the network. The hacker uses the user's identification and password and logs into the network illegally.
- **Scavenging –** the hacker searches through stray data for clues that might unlock the secrets of a targeted computer system. A similar technique is known as dumpster diving , wherein the hacker searches electronic garbage in order to find discarded documentation that may include user name and password.
- **Password Guessing –** the hacker aims just to crack the password. Guessing the password may involve various techniques such as **dictionary attacks** (searching with a dictionary file for words fitting to the password); **hybrid attacks** (adding numbers or symbols to the filename for to successfully guess the password); **brute force attacks** (long time guessing a password)
- **Autodialing –** the hackers systematically dials with his/her computer until answered by the computer on the other side of the line.
- **Zapping –** (a sabotage method) the hacker penetrates a computer system by unlocking the master key of its program, then self destroying it by activating its own emergency program. Zapping is a cracking technique with malicious purpose.

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal

Computer Sabotage:

Computer sabotage is one of the dangerous forms of computer crime. The saboteurs create tiny but destructive programs that cause serious hardware and software problems in a computer system, such as deleting files in the hard disk, blocking up mail servers by sending fake e mails to the address found in the address book of the victim and stealing the information from the computer of the victim and sending this information back to the saboteur. There are different kinds of these malicious programs the most popular are worms, viruses, bacteria, Trojan horse, logic bombs and spywares. A brief description of [xiii] by Forester and Morrision (1994).

- **Viruses –** A computer virus is a self replicating program reproduced by attaching executable copies of itself to other programs. The effects of a virus may range from irritating messages to complete destruction of the system. A virus can not run independently. Initially the virus requires a host program to infect and it is not executed until the host program is run. A virus can spread rapidly through hosts that share same infected programs or disks that include these programs. A computer virus is very difficult for a common user to detect. The most common type of viruses are (a) boot sector viruses : infect the system boot and whenever the system is loaded (b) e mail virus : spread through e mail attachments and (c) macro virus : spread through documents that contain macro programming instructions that perform automated tasks.
- **Worms –** A worm is virus like program that make copies of itself across network connections, seeking uninfected workstations in which to reproduce. In contrast to a computer virus a worm program can travel independently through different hosts and resides more in the computer memory of a system rather than on disk. The aim of worm is through continued reproductions to cause disk or memory overload through network. Inevitably, the network freezes and the system has to be reloaded, this process cause complete loss of memory data that have not been saved on disk. On the other hand , the consequences of a worm are not as destructive as that of virus . A worm is a memory virus thus it can be removed by shutting down the infected system.
- **Trojan horse –** A Trojan horse is a destructive program disguised to appear as something begins (mild). The name of this malicious program comes from famous wooden horse of Trojan War that Greeks left as a gift to the Trojans. The horse was full of Greek armed forces that caused the fall of troy when released into the city at the right moment. Likewise the electronic version of the Trojan horse resides in the code of program until the moment of its activation. The conditions of activation are determined by the computer programmer who designed the program. A Trojan horse is usually posted through the internet disguised as a harmless program or game. Trojan horse are also used to exchange secret information between hackers.
- **Logic bombs and Time Bombs –** logic bombs and time bombs are kinds of Trojan horses. A logic bomb inserts secretly into a system and causes a destructive action when a certain logical event or sequence of events happens. (e.g. if program x runs, then do destructive action y) . Similarly , a Time Bomb is triggered after a particular time related event.(e.g. if program x runs after date y, then do destructive action z)
- **Spy Ware –** A spyware is a type of surveillance program that is inserted into a computer system in order to monitor, store and analyze the electronic transmission of the system. A spyware is not itself destructive program.

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal

The normal functioning of the computer is disrupted as soon as the destructive program enters in the computer. The user can be identified the presence of a destructive program by annoying messages on the screen, strange behavior of the system, problem in the system performance or partial destruction of the data . in this case user is recommended to use an anti virus that searches for malicious program throughout the system , informs the user about possible infections and usually clean the infected files. The user is also able to select a safeguard option of the program that protects the system from unexpected virus attacks on line. This option helps the user monitor all suspicious virus like activities. An antivirus program must be frequently updated with the new virus fighting data base and if there is network, must be installed in all network nodes.

Some additional actions to minimize the risks of infection:

(1) Make sure all purchased software comes in sealed tamper proof packages.
Be careful about software received from friends as well as files downloaded from web, e mail attachments and other forms of shareware and free ware programs.
(2) Be particularly careful with software of unknown origin.
(3) Avoid using disks from the office computer at the home computer and vice versa.
(4) Make backup copies of software and data.

Good practice aims to improve the security of computer system and protect programs and in case of destruction, misuses and malfunctions. The backup copies must be kept in different versions. If a recent version is corrupted, the user must able to retrieve data from an earlier version.

Three different approaches could be suggested to prevent computer crime:

(1) Computer Security and Management
(2) Appropriate policies & standards
(3) Education and Morals

Computer security involves protection of hardware, software, machines and networks from unauthorized e attacks, misuses and malfunctions. Security is very important and is especially so for business because the degree of security determines not only the reliability of information and the integrity of data, but also the confidence of the public in the computer systems.

Security measures may involve restricted physical and digital access as well as backup of data and encryption of sensitive information. High – tech security systems include encryption devices that protect the transmission of data by scrambling the transmission, firewalls and anti - virus programs that prevent unauthorized access, and tools for authentication that identify users electronically with dial – back systems , audit control devices and biometrics.

Here it should be mentioned that a user's authentication is one of the central problem both for business security and national security. While authentication affects seriously the computerized collaboration between companies and institutions and brings the demand of a justified digital identity of the user in electronic transactions, it is also essential to the protection of public security in the fight against terrorism and cyber terrorism. The most fool proof solution to this problem is biometrics – digitizing individual's biological characteristics such as fingerprints, voices, patterns of blood vessels in the retina, wheel pattern of iris and lip prints.

Despite of such vital and sensitive responsibility in the security issues of finance, defense, education, medical and various other sensitive domains it is quite astonishing and unfortunate that most of the companies and organizations do not follow the appropriate computer security measures. Only creation of awareness to such sensitive issues remains the only option as preparation is better than cure.

Work Cited

1. Aristotle metaphysics I.1, Nicomachean ethics
2. Moor, J.H. (1985) What Is Computer Ethics? *Metaphilosophy, 16(4),* 266-75
3. McEwen, J. T.(1989) *Dedicated Computer Crime Units* Washington, D.C.: National Institute of Justice.
4. Forester, T. & Morrison, P. (1994). *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. New York: M I T Press.
5. Tavani, H. T. (2004). *Ethics and Technology: Ethical Issues in Information and Communication Technology*. New York: John Wiley & Sons.
6. Cornwall , H.(1986). *The Computer Hacker's Handbook* . E. A. Brown Company.
7. Forester , T. & Morrison, P. (1994*). Computer ethics: Cautionary tales and eethical dilemmas in computing.* New York: M I T Press.
8. Levy, S. (1984) *Hackers: Heroes of the computer revolution.* New York: Doubleday Press.
9. Levy, S.(1984) *Hackers: Heroes of the computer revolution.* New York: Doubleday Press.
10. Rosenberg , R.(1997) *The social impact of computers*. 2nd ed. Burlington, MA: Academic Press.
11. Baase , S.A(2003) *Gift of fire : Social , legal and ethical issues for computers and the internet* . 2nd ed. Upper Saddle River, NJ: Prentice Hall.
12. Forester , T. and Morrision, P. (1994). *Computer ethics: Cautionary tales and eethical dilemmas in computing.* New York: M I T Press.
13. Forester , T., & Morrision, P. (1994*). Computer ethics: Cautionary tales and eethical dilemmas in computing.* New York: M I T Press.