Computer Abuse and Crime

Ahmad Bahaitham and Mohammad Felemban

***Abstract*— In this paper, we have discussed computer ethics and their importance in this age where computer technology grows and develops rapidly. Then, we have listed out the ten commandments of computer ethics which have been defined by Computer Ethics Institute. After that, we have presented some examples of computer crimes e.g. malicious software and hacking. Then, we have defined who hackers are in details. Finally, we have introduced anti-hacking laws that have been adopted by Saudi Arabia.**

***Index Terms*— Computer ethics, Computer crime, Hacking, Saudi Arabia Cybercrime laws.**

I. Introduction

ETHICS deals with placing a "*value*" on acts according to whether they are "*good*" or "*bad*", "*right*" or "*wrong*". Every society has its rules about whether certain acts are ethical or not. These rules have been established as a result of agreements in society and are often written into laws.

II. Computer ethics

Computer ethics is a new branch of ethics that is growing and changing rapidly as computer technology also grows and develops. So, computer ethics is the analysis of the nature and the social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of technology. Social and personal policies for the ethical use of technology are both covered by ethics.

Recently, this strong new field has led to new university courses, conferences, workshops, professional organizations, curriculum materials, books, articles, journals, and research centers. And in the age of the world-wide-web, computer ethics is quickly being transformed into "global information ethics".

Ethics about the usage of computers is a discipline, which depends on science and ethics, a field in between them, which facilitates both conceptualizations for understanding and policies for the effectual use of computer technology.

When computers first began to be used in society at large, the absence of ethical standards about their use and related issues caused some problems. However, as their use became widespread in every facet of our lives, discussions in computer ethics resulted in some kind of an agreement. Today, many of these rules have been formulated as laws, either national or international. Computer crimes and computer fraud are now common terms. There are laws against them, and everyone is responsible for knowing what constitutes computer crime and computer fraud.

The *Ten Commandments of computer ethics* have been defined by the *Computer Ethics Institute* which are:

1) Thou shalt not use a computer to harm other people.
2) Thou shalt not interfere with other people's computer work.
3) Thou shalt not snoop around in other people's files.
4) Thou shalt not use a computer to steal.
5) Thou shalt not use a computer to bear false witness.
6) Thou shalt not use or copy software for which you have not paid.
7) Thou shalt not use other people's computer resources without authorization.
8) Thou shalt not appropriate other people's intellectual output.
9) Thou shalt think about the social consequences of the program you write.
10) Thou shalt use a computer in ways that show consideration and respect.

III. Computer crime

Computer crime can broadly be defined as criminal activity involving the information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

Malicious kinds of software, or "programmed threats", provide a significant challenge to computer security. These include "*viruses*", which cannot run on their own, but rather are inserted into other computer programs; "*worms*" which can move from machine to machine across networks, and may have parts of themselves running on different machines; "*Trojan horses*" which appear to be one sort of program, but actually are doing damage behind the scenes; "logic bombs"

Ahmad. Bahaitham is with the Computer Engineering Department, KFUPM, Saudi Arabia (e-mail: s224594@kfupm.edu.sa).

Mohammad Felemban is with the Computer Engineering Department, KFUPM, Saudi Arabia (e-mail: s232571@kfupm.edu.sa).

which check for particular conditions and then execute when those conditions arise; and "bacteria" or "rabbits" which multiply rapidly and fill up the computer's memory.

Computer crimes, such as embezzlement or planting of logic bombs, are normally committed by trusted personnel who have permission to use the computer system. Computer security, therefore, must also be concerned with the actions of trusted computer users.

IV. Hackers

Another major risk to computer security is the so-called "*hacker*" who breaks into someone's computer system without permission. Some hackers intentionally steal data or commit damages, while others merely "explore" the system to see how it works and what files it contains. These "explorers" often claim to be benevolent defenders of freedom and fighters against rip-offs by major corporations or spying by government agents. These self-appointed vigilantes of cyberspace say they do no harm, and claim to be helpful to society by exposing security risks. However every act of hacking is harmful, because any known successful penetration of a computer system requires the owner to thoroughly check for damaged or lost data and programs. Even if the hacker did indeed make no changes, the computer's owner must run through a costly and time-consuming investigation of the compromised system.

A "computer hacker," then, is someone who lives and breathes computers, who knows all about computers, who can get a computer to do anything. Equally important, though, is the hacker's attitude. Computer programming must be a hobby, something done for fun, not out of a sense of duty or for the money.

There are specialties within computer hacking. An algorithm hacker knows all about the best algorithm for any problem. A system hacker knows about designing and maintaining operating systems. And a "password hacker" knows how to find out someone else's password.

V. Cybercrime laws adopted in Saudi Arabia

Saudi Arabia's legislation body, the Shoura, has adopted its first set of laws designed to combat the growing threat of cybercrime. In a session of the 120-strong Shoura Council four months ago the new law that deals with offences such as hacking or the use of online resources to spread terrorism was approved. It now awaits enactment following publication in the official gazette.

The Saudi law establishes that website defacing is a crime worthy of punishment, while data theft could carry a significant fine of more than $130 thousand or even a maximum one year prison sentence. The same punishment could apply to those found guilty of defamation using electronic means or those who unlawfully break into private electronic networks. Anyone found guilty of unauthorized possession of electronic documents will face three years in prison, and a sentence of one year in prison will be given to anyone convicted of gaining unauthorized access to electronic networks, hacking into web sites to change or damage their contents. Users spreading malware could find themselves paying out $800 thousand and spending up to four years in a Saudi jail, less than those found guilty of spreading vice and immorality. People setting up websites with pornographic content or content that defames humanity, or sites with information promoting drug use may be punished with fines of up to $1.3 million and five years of jail time.

The heaviest punishment in the new law is reserved for individuals who break into government networks or steal data relating to national security. Those found guilty of using the Internet as a medium for spreading terrorist views or share terrorism-related knowledge will also be facing the toughest sentences of fines up to $1.3 million and ten years imprisonment. Accomplices of those found guilty of committing cybercrimes will also be punished, with their sentences halved. The new law is expected to come into force within next month.

VI. Conclusion

Computer ethics is a growing branch of ethics as the rapid development in computer information and technology. Social agreement in computer ethics is then translated into laws that govern the ethical usage of computers. This led the Computer Ethics Institute to define the Ten Commandments of computer ethics. Illegal accessing, writing malicious software's and hacking are justified as computer crimes which deserve punishments. Such laws have been adopted by Saudi Arabia's government.

Acknowledgment

The authors gratefully acknowledge the support of King Fahd University of Petroleum & Minerals in this work and Dr. Aiman El-Maleh for his help.

References

[1] Computer Ethics by Laith Murad. http://www.geocities.com/lool95/computer_ethics1.htm
[2] Computer Ethics article by Anna Elizabeth Kuruvilla. http://itoutsourcingindia.com/resources/computer_ethics.asp
[3] Computer Ethics: Basic Concepts and Historical Overview. http://plato.stanford.edu/entries/ethics-computer/#3.2
[4] What is a Hacker? By Brain Harvey, University of California, Berkeley. http://www.cs.berkeley.edu/~bh/hacker.html
[5] Computer Abuse. http://en.wikipedia.org/wiki/Computer_abuse
[6] Cybercrime laws adopted in Saudi Arabia by Konstantin Kornakov. http://www.viruslist.com/en/news?id=202181770