Hackers analysis essay

kaygusuz1

It is the weekend you have nothing to do so you decide to play around on your computer .

You turn it and than start up , calling people with your modem , conneciting to another world

with people. This is all fine but what happens when you start getting into other peoples

computer files , then it becomes a crime and who are the criminals. To begin i will start

with hacking and hackers.

Hacking is the act of breaking into computers and network of other poeples with out

any permission . Hacking is like drugs or any other substance , its an addiction for the mind

and once started it is diffucult to stop . Hacker is a person who enjoy learning details of a

programming language or system , who tries to break into computer systems . There is two

types of hackers. On is the benign hackers , who likes get into his or her own computer and

understand how it works . The malicious hackers is the person who likes getting into other

peoples system . Black hat is used to discribe a hacker who break into a computer system

or network with malicious intent . Unlike white hat , the black hat takes advantage of the

break in perhaps destroying files or stealing data for some future purpose. White hat hackers

describes a hacker who identifies a security weakness in a computer system or network but

instead of taking malicious advantage of it . They will allow the systems owners to fix it

before can be taken advantage by others . But U. S law does not see differences between black

hat hacker and white hat hacker.

Many of the poeple in our society today often think that computer hackers are very smart

individuals who have special talents and abilities and enabiling them to crack passwords ,

send viruses , cancel your cable tv , raid your social security and crash computer systems.

Most people in our society do not spend the time to break into computer systems but all

studies indicate that hackers are genarlly young and not haave full time jobs or own property

kaygusuz2

They have so much time and energy to break into computers. Hackers learn hacking from

reading different kind of computer books , they find many available tools on the internet ,

they spend so much time on the computer to learn the techniques of hacking . Some of the

hackers hack for to gain highest prestige within the comunity. Some of them hack just for fun,

more they hack more fun they have . Hacking is just another way to recieve a build up of

adranaline in the body. They also gain great deal of power from learning confidential

information. Hacking involves accumulation of knowledge which is accompanied by the

greater status and power . Some of the hackers say that they only punish people an companies

that they do not like and to show weakness of companies which have poor security. Some feel

that if they put others down they will elevate to higher level. Most of the young hackers do

not know the implication of what they are doing , they do not consider that if they do get into

a system and start to hack they could costs the company thousands millions of dollars. Every

computer proffesionals have made mistakes thatr has caused the loss of data , service and

money but some hackers have never been in real situation to understand this issue. These

people are displaying situational morailtiy.

Many professionals argue that the cause why hackers hack is about the same as any other

criminal. It mostly has to deal with their familes and friends and the enviroment they grew

up in. I agree with professionals at this point and belive that the issue goes back to how they

are raised . I am not saying that these people have bad parents . I think that while parents go

around telling their children not to use drugs or any other substance , to study hard in school,

probably they do not their children not to break other peoples computer systems or hacking

is bad and illegal. Information security professions must be more visible in a way that set

children before the hackers community sets them . They get together to teach children about

hacking before somebody else does.

kaygusuz3

Some hackers are not really terrorist in a way they help companies find out flows in their

systems. And real hackers do not delete or destroy any information on the system they hack.

Best hackers end up with high-paying security consulting jobs because of their expertise.

Hackers may use any types of systems to access information depending on way they intend

on doing in the system. The methods hackers use attack your machine or network are fairly

simple. If hacker experienced and smart he will use telnet to access shell on other machine so

that the risk of cought is lower than doing it using their onw system. A hacker scan vulnerable

system by using a demon dialer which will redial a number repeatedly until a connection is

made. Or use wardialer , is an application that uses a modem to dial thousands random phone

numbers to find another modem connected to a computer. Hackers also use the Net to share

lists of vulnerable IP addresses- the unique location of internet connected computers with

unpatched security holes.

Once hacker find a machine , he uses a hacker tool such as Whistler to identify in less than

a second what operating system the machine is using and whether any unpatched holes exist

in it . Whistler also provide a list of exploits the hacker can use to take advantage of these

holes. Once hacker crack into a system , his next goal is to get root , or give himself the

highest level of access on the machine. The hacker can use little-known commands to get or

can search the documents in the system s hard drive for a file or e-mail message that contains

the system adminstrators password. Hacker can create legistimate user account and log in

whenever he wants without attracting attention. He can also alter or delete system logs to

erase any evidence such as command lines that he gained access to the

system.

Software always has bugs , system adminstrators and programmers can never eliminate all

possible software vulnerabilities. Hackers find a hole to break in. Hackers also crach

kaygusuz4

passwords. Cracking password is coming very easy to hackers because most of the people use

the names of themselves , their children , pet or car model as their passwords. so smart hackers

easily crack their passwords. Or hacker use a program that will try every possible word in the

dictionary. hacker usually have a copy of the english dictionary as well as foreign language

dictionaries for this purpose. Hackers main goals is to hide evidence of the attacks and

make sure they can get back in again. One of the other main attcak is DOS attacks but do not

involve breaking into a system or network unusable. It can be local or network based and

have always been diffucult to defend against. A firewall (is a program which stops other

connection s from different servers to the firewall server) can not prevent all of these attacks

because some of the attacks are outside the firewall and they are all diffucult to distinquish

from normal traffic. The effects of these attacks were to make sites inaccessible such as

yahoo.

Hackers always find hole in every security systems and they get what they want , they

can travel through the internet without restriciton. One of the hackers who was situated in an

east coast brokage house wa interested in the stocks market so he purchased 100, 000 dollars

worth of shares in the stock market. Then he hacked into stocks markets main computer and

stole 80 million dollars. The hacker was cought although 53 million dollars was not recovered

The homepage of United States Air Force was recently hacked and the contents had been

changed . The webpage has been changed completly as the hacker had inserted pornographic

pitures sayingtihs is what are we doing to you and had under the image screwing

you. The hackers have changed it and shown their views on the political system . Kevin

Mitnick who broke into a North America Air Defence command computer , Kevin Paulsen

who cracked goverment and milatary systems of America. Another major hack which was

committed was by a 16 year old boy in Europe. This boy hacked into the British Airforce

kaygusuz5

and downloaded confidential information on Ballistic missiles. Security experts agree that the

best way to combat these attacks is simply with better security practices or not having

connected to the internet.

As computer technologies have become more a more integral part of our daily lives , the

perceived govermental / legal responsibility to protect those technologies has increased . It

is quite obvious that the criminal implication of technological advancement have cought

goverments , legal system as well as the public of guard . Bureaucracy is slow , technology is

fast . If they can , it will take time for the public regulatory system to catch up. There are many

legal diffuculties that the goverment and the courts have to work through concerning computer

crime regulation in order to for the law to be effective while many computer crimes are

variations an old crime , there are new activities that are just started to be considered criminal .

One example is the case of R. Maclaughlen which had to do with a student who obtained

unothorized access to a computer system and escaped legal consequencesbecause the law did

not have an applicable section. Fitting computer crime into laws is also very diffucult. Another

problem with law is the people that make the law. Legaislators have to be familiar with high-

tech metarials that the hackers are using but most of them know very little about computer

systems. Current law system is unfair ; it tramples over the rights of the individual , and is not

productive.

New uses of computer technologies have caused established legal definitions to come under

review. For example , should data be considered property ? Even so there is the realization

that computer crime laws shoul have technologically neutral meanings. Laws thar are not

technologically neutral may become absolete they are even passed. Legal definition also

become an issue when involved regulators have limited understanding of the technologies

through the crimes can be committed. There is also diffuculty of determining sentences or

kaygusuz6

penalties for crime committed. Goverment and members of the court have take into

consideration factors as the following .

? the intend of the accused

? the previous record of the offender

? the extent or potential extent of the offence

? appropriate punishment to fit the crime

? the concept of providing to deterrent to the crime act

? compensatioin for the victim in civil cases

What can be considered acceptable evidence in computer crime cases has also come into

question. For example the court have sssumed that agreements or contracts require paper

records. Electronic records to date have been admitted in court cases but the results have been

inconsistent. The federal goverment and the provinces are considering amending their

respective evidence acts to allow the admission of electronic records where the record system

is deemed reliable. U. S law enforcement leaders said the computer attacks were one of the

fastest growing areas of crime.

Computer Emergency Response Team at Carnegic Mellon University has been taking

Internet attacks since 1988. Their statistics reveal an alarming growth in computer attacks:

YearAttacks

19886

1989 132

1990 252

1991 406

1992 773

19931, 334

19942, 340

19952, 412

19962, 573

19972, 134

19983, 734

19999, 859

200021, 756

Having knowingly accessed a computer without authorization or exceeding authorized

kaygusuz7

access , and by means of such conduct having obtained information that has been determined

by the United States Goverment pursuant to an Executive order or statute to require protection

against unauthorized dicslosure for reasons of natinal defense or foreign relations, or any

restricted data , as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954 ,

with reason to believe that such information so obtained could be used to the injury of the

United States, or to the advantage of any foreign nation willfully communicates , delivers ,

transmits , or causes to be communicated, delivered, or transmitted, or attempts to

communicate, deliver, transmit or cause to be communicated, delivered, or transmitted thesame

to any person not entitled to receive it , or willfully retains the same and fails to deliver it to tha

officer or employee of the United States entitled to receive it;

1) Intantionally access a computer without autohorization or exceeds authorized access.

a) Information from any deparment or agency of the United States; or

b) Information from any protected computer if the conduct involved an interstate or foreign communication

c) Information contained in a financial record of a financial institution , or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency are defined in the Fair Credit Reporting Act (15 U. S. C 1681 et seq)

2) Intantionally, without authorization to access any nonpublic computer of a department or

agency of the United States , accesses such a computer of that department or agency that is

exclusively for such use , is use by or for the Goverment of the United States and such

conduct affects that use by.

3) Knowingly and with intent to defraud, accesses protected computer without authorization

or exceeds authorized access and means of such conduct furthers the intended fraud and

obtains anything of value , unless the object of fraud and the thing obtained consists only of

the use of the computer and the value of such use is not more than 5000 dollars in any 1 year

period.

kaygusuz8

4) Knowingly causes the transmission of a program , information , code, command, and as a

result of a such conduct, intentionally causes damage without authorization to a protected

computer.

5) Knowingly and with the intent to defraud traffics in any password or similiar information

through which a computer may be accessed without authorization, if such computer is used by

or for the Goverment of the United States.

6) With intent to extort from any person , firm , association , educational institution, financial

institution, goverment entity or other legal entity, any money or other thing of value transmits

in interstate foreign commerce any communication and threat to cause damage to protected

computer shall be punished.

In U. S. A. law , computer tampering penalties range from 500 dollars and 15 years in prison

depanding on the damage to the computer system. Computer fraud penalties are up to 7 years in

prison. Computer hackers also can be charged under federal law if the criminal activity stretches

over state lines , penalties up to 250, 000 dollars and 1 year in prison for the first offence.

Original hackers ethics was sort of informal ethical code developed by the original hackers

in the 50s and 60s. These hackers were the firt generation of programers. The ethics reflects

their ideology of the liberatory power of technology. These hackers were moraly thinkers

computer software and hardware. The first ethic code is Hands on Inperative: access to

computer and remove barriers between people and goverment and understanding of technology.

Information wants to be free: the computer has been in the hands of goverment and big

buisnesses. Goverment activities , corprate crime , illegitimate information needs to be

dissaminated. And hackers want to know when the goverment is killing people and they also

said everyone have right to gain information about goverment. Mistrust Authority: hackers

always shown distrust toward large institution coroperations. And they said PCs power move

kaygusuz9

away from large organizations to hands of individuals. No bogud Criteria: Hackers should be

judged by their hacking not by bogus criteria such as race , age , sex or position. You can

create truth and beauty on a computer : Hacking is equated eith artistry and creativity. This

element of the ethos raises to the level of philosphy (as opposed to simple pragmatism) which

is about hummanitys search for the good , the true and the beautifiul. Without question , good

programing hacking is art and as withart each person has their own signature and style.

Computer can change your life for the better : The world of cyber space is more real than the

real world itself. Because it is only within the virtual world that people are really to be free

themselves , to speak without fear , to paricipate in a dialogue where one is judged by the

merits of their words , not the color of their skin or the timbre of their voice.

Ethical principle of hsckers ethics suggest it is ethical duty of hackers to remove barriers ,

pwer and create things by using computers. Now there is new hackers ethics which developed

by 90s hackers. Above all else , do not harm : do not damage computers , data if it possible

hack must be safe , not damage anything and anyone (physically or mentally). Leave no trace :

do not leave trail or trace of your computer presence, , keep quite , keep low profile. Hackers

have to protect other hackers from being cought or loosing access. Share informaiton do not

hide. Just because it wants to be free does not mean you must give it to as many people as

possible. Protect privacy : people have a right to privacy , which means control over their own

personal information. The concept of privacy is something that is very important to a hacker.

Hackers know how fragile privacy is in todays world. Exceed Limitation : hacking is about the

continual transcendence of problem limitations. Telling something can not be done , is a moral

imperative for him to try. Hacking always seeks to surpass current limits. Limitations must be

overcome , for some hackers these kimitations might be unjust laws or outdated moral codes

Hackin help security : hacking is a positive force because it shows people how to mend weak

kaygusuz10

security or in some cases to recognize and accept that total security is unattainable without

drastic sacrifice. This ethical principle seems to be agreed upon by some menbers of the

industry . Trust but test : you must constantly test the integrity of system and find ways to

improve them . Do not leave maintenance and schematics to others , understand fully the

system you use or which affect you. If you can exploit certain systems (such as the telephone

network) in ways that their creators never intended or anticipated , thats all to the better. This

could help them create better system

Hackers ethics changes because computer are more powerful , more distributed , more

important now. Hackers ethics unnoticed before because fiddling with larger complex system

was so diffucult until recently. There have always thinkers but their explorations were very

local. We live in yhe age of computers. Everything is controled by massive mainframes

(electricity , water distribution , telephone systems). Also society has changed , old hackers

lived in a society which was based on trust and honesty thats why their behaviours was

different. Computer cominity is driven now not by knowledge but for money. Generation

changed too. Hackers are more pessimiste , thoughtless more careless and more self-centered.

I tihnk the truth of the matter is everyone has their own hacker ethics.

No one plans to arrested but the hackers have several rules that they apply when they are

arrested. They do not try to convince the officer of their innocence it is useless. Because they do

not care hackers are innocent or not . It is the job of the judge or jury to free hackers if he is

right . Hackers must keep quite because police will ask questions. Don not give permission to

search anywhere. If law enforcement ask , it probably means they do ont believe they have

the right to search and need your consent. If the police are searching your home or computer

do not look at the places you wish they would not search . Do not react to the search at all , and

especially not to questions like who does this belongs to Hackers do not belive what

kaygusuz11

the police tell them in order to get them talk. The law permits them to lie to a suspect in

order to get him to make admission. For example they will seperate two firends who have ben

arrested and tell the first one that second one sequealed on him. The first one then sequeals on

the second though in the truth second one never said anything . If at home , never invite the

police inside nor should you step outside. If the police believe you have committed a felony ,

they usually need an arrest warrant to go into your home to arrest you. Probably they have not

got warrant to enter or to arrest you in your home. And if the hacker arrested outside their

home do not accept any offers to let him go inside to get dressed , change their clothes , get

jacket , call your wife or any other reason. The police will of cource escort you inside and then

search everywhere they want without any warrant .

I give some information in my research paper about hacking , hackers and about their world

I try to understand who are the hackers , how their mentality work and their lifestyle and also

goverment regulations against these smart indivuduals. nformation security professions must

be more visible in a way that get children before the hackers community gets them . They get

together to teach parents and schools and also they must teach children about hacking and

hackers before somebody else does. And also goverment takes to find a way to stop hackers. If

the goverment does not hurry up they are going to get buried by hackers and when that

happens the world will not be a fun places to live in and aslo the cyberspace.

kaygusuz12

WORK CTED

Cert Coordination Center Computer Crime in todays Society

Retrieved: November 10, 2000 from the World Wide Web:

http:// www. cert. org//

Choas Computer Club (januvary 05 , 1995) Hacker Bible

The New Hackers Dictionary (online education)

Retrieved November 10 , 2000 from the Worl Wide Web

A non-technical artical from business web zine about Distrbuted Denial Service Attacks:

http://www. cert. org/advisories /Ca-99-17-denial-of-service-tools. html

Tool from the FBIs National Infrastructure Protection Center :

http://www. nipc. gov/

The Criminal Heroes Of Cyberspace And Law That Apply Against Their Attacks

The internet is one of the newest form and effective tools of technology. The world would

be lost without it. Millions of people would be using the internet to share information , make

new association and communicate. From individuals and students to businesses and journalist

using the internet to share information. The internet would allow people to send and receive

data , notes , messages , documents , pictures.

But there is considerable drawback of the internet . The problem is hackers , they have

tremendous knowledge on the subject and use it to steal confidential informaiton for the sake

of fun or profit and they use computer technology as a weapon. It is called cyber terrorism ,

they threat the global security. People who are responsible from their informaiton security on

the internet try to improve their systems , find new ways to protect their informaitons against

hackers. But hackers are still making trouble and breaking in the computer systems. Hacking

is presenting problems for companies , universities and law-enforcement officials in every

industry country.

Why do hackers go through all the trouble to do what they do ? Why they spend so much

of their time and energy accomplishing these feats of techonlogical wizadary ? What is the

cause that turns those mostly above-avarage intelligent people to purpose a criminal career ,

and destroy their otherwise very succesful career ? why do hey commit these computer related

crimes as an obession. What they want ? I try to find answers to these questions.

Information on hacking and hackers can be found in several popular magazines and

through web sources. However , it is hard to find books on hacking and hackers available at

libraries. I will mainly use the internet and it will play the biggest part in my paper. I will use

popular search engines , online journals and magazines, and databases to conduct my internet

research. Once all the source are gathered i will carefully read through each one and highlight

significant parts that will be used in the research paper.

The Criminal Heroes Cyberspace And Law That Apply Against their Attacks

Introduction

I The nightmares of our computer and their mentality

A Who are hackers and reasons for their attacks

B – How they hack the systems

II Preventive systems that apply to the hackers and rules of hacking

A — U. S. A goverment precoution against hackers

B Hackers ethics and their defence against US law

Conclusion

Words

/ Pages : 7, 049 / 24