CONTROL ANALYSIS ON SECURITY AS CYBER CRIME

Dr. RAJEEV KUMAR[1],ABHISHEK KUMAR [2]
[1]*Mtech Scholar-*[1]*CCSIT, TMU,MORADABAD*
[2]*Assistant Professor-CCSIT, TMU,MORADABAD*
[1]drrajeev.computers@tmu.ac.in
[2]ashu.shakya0@gmail.com

Abstract— **As we know cyber crime is a big problem in today's time. Every day a new crime is happening in cyber world. And cybercrime is done by people who are experts in computers. In this paper, we will tell how to control cyber crime. Cybercrime has a very dangerous effect. In cybercrime, the Criminal destroy its target completely, either steals some of its useful data from it or hacks its bank account and makes its entire money up. In this paper, we are telling you how cybercrime is different and how it affects them and how we can stop cyber crime.**

Keywords— cyber crime, cyber security

I. INTRODUCTION

As human society continues to grow, so much crime is increasing day by day. Cyber Crime is the most unique example of this! The convenience of computer and internet has now developed a cyber society by integrating the world into a circle, but like a conventional human society, this society is not even untouched by human weaknesses! Those who misuse their education and technical knowledge have given rise to such crimes, which are known as Cyber Crime! Cyber Crime is crime under crimes most prevalent - software piracy i.e. simulate real software at low prices and sell it in another computer and software Jiri intrusion (hacking) located on-site information in it to steal, the virus left in it or to delete the data in it with a rag-existing important files or information, however, and upon finding Prado Anon implement very difficult to get work.
The vicious criminals know that getting them caught or proven guilty is a very difficult task! In fact, there is no check post in the information super highway made with computer networking and internet facilities and neither an application nor an inspector!
There are many ways to cheat computer! The confluence of computers and telecommunication has given birth to new dimensions of crime such as theft of information, computer program change, duplication of information, dissemination of sensitive material, electronic money transactions, electronic felony and terrorism, sales and investment, fraud etc. ! By using all these methods, the use of computers is promoting wrong work. Thus, like a mobile phone, the computer has become an essential tool in the crime scene, which is a matter of great concern for us.

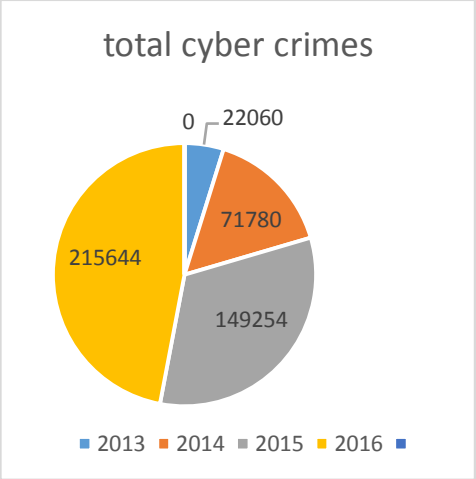

Fig.1

II. WHAT IS THE CYBER CRIME?

Cybercrime, also called computer crime, is any illegal activity that involves a computer or network-connected device, such as a mobile phone. The Department of Justice divides cybercrime into three categories: crimes in which the computing device is the target, for example, to gain network access; crimes in which the computer is used as a weapon, for example, to launch a denial of service (DoS) attack; and crimes in which the computer is used as

an accessory to a crime, for example, using a computer to store illegally-obtained data.

Fig.2

III. TYPES OF CYBER CRIMES

- HACKING
- Virus dissemination
- Denial-of-Service attack
- PHISHING
- Email bombing and spamming
- Web jacking
- Cyber stalking
- Data diddling
- Identity Theft and Credit Card Fraud
- Software Piracy
- Mobile Payment and Banking Hacks

IV. HACKING-

Hacking is a part of cybercrime in hacking, the hacker enters his system without the permission of the owner, and misuses it to steal some relevant information. In simple words, hacking is an act committed by an intruder. Hackers are basically computer programmers, who have advanced computer information and who have expert-level skills in a particular software program or language. And some people do this work for their interests. Hackers can use hacking to steal other people's bank accounts, some personal information, and other kinds of information against them against them.

<u>Why do hackers hack?</u>

- Just for fun
- Show off
- Hack other system secretly
- Notify many people their thought
- Steal important information
- Destroy enemy's computer during the war

V. VIRUS DISSEMINATION

Virus is a process of malicious software. The virus adds itself to other software. (Viruses, worms, Trojan horses, time bombs, logic bombs, rabbits, and bacterial are examples of malicious software that destroys the system of prey. The virus program is automatically run before the other program runs. Viral dispersion is a very big problem. Viruses are a computer program that engages itself or influences the files of a system, and can be used to help with virus network from one computer to another. Some of these viruses are such that our computer performance slows and some of us share the information of our computer without knowing it.

VI. DENIAL-OF-SERVICE ATTACK

DoS (denial of service) attack is simple: send more request to the machine than it can not handle. There are toolkit available in the underground community that make it easy for the program and tell it which host to blast with request. The attacker's program simply make a connection on some service port, perhaps forging the packet header information that say where the packet came from, and then dropping the connection. If the host is able to answer 20 request per seconds, and the attacker is sending 50 request per seconds, obviously the host will be unable to service all of the attacker's requests.

- Symptoms of DoS attack-
- Unusually slow network performance (opening file and accessing web site)
- Unavailability of a particular web site

- Dramatic increase n the number of spam mails received. This type of DoS attack is known as "Mail-Bomb".

VII. PHISHING

Similarly, crimes committed through the Internet are increasing and since banking is happening through the internet nowadays due to which if you take a little more carelessness, then there may be a victim of fraud. Fishing means any brand or anybody Also, make a duplicate website that is similar in appearance to the website you use everyday, somehow by sending it to you by email or through some other way And the email is written in such a way that if you do not read it properly and click on it, then the password and details of the fake format for which you have been prepared for that website is requested. Such fake emails are cited for security reasons and you get trapped and you enter your user ID and password and by doing so, that detail comes to the hacker who created that page.

VIII. EMAIL BOMBING AND SPAMMING-

In e-mail, Criminal sends a large amount of email to its goal. And the message is meaningless and the network resources need to be consumed. If multiple accounts of the mail server are targeted, then there may be a negation-off-service effect, such mails can be easily detected by spam filters. DDOS attacks are used as an email bombardment (personal computers connected to the computer whose security has been compromised by malware and under attack control).

This kind of attack is more difficult to control due to multiple source addresses and bots, which are programmed to send enough spam messages. "Spamming" is a form of email bombardment, where unwanted messages are sent without any counting. Opening links in spam mail can help you phishing websites that host malware. In spam mail, infected files may also be attached as an attachment, email spam may get worse when the recipient answers the email for all the original remittances. Spammers collect email addresses from the list of customers, newsgroups, chat rooms, web sites and viruses, as well as crop users' address booklets and sell them to other spammers. There is a large amount of spam.

IX. WEB JACKING

Web jacking derives its name from "hijacking". Here, the hacker takes control of a web site illegally. He may modification the content of the original site or even forward the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish comforts. Cases have been reported where the attacker has asked for deal, and even posted obscene material on the site.

The web jacking process attack may be used to create a duplicate of the web site, and present the victim with the new link saying that the site has progressed. Unlike usual phishing methods, when you hang your cursor over the link provided, the URL presented will be the original one, and not the attacker's site. But when you click on the new link, it opens and is fast swapped with the malicious web server. The name on the address bar will be somewhat different from the original website that can trick the user into thinking it's a real site. For example, "Gmail" may direct you to "gmai1". Notice the one in place of 'L'. It can be easily overlooked.

X. CYBER STALKING

Cyberstalking is a big crime in which the attacker harasses a victim using electronic communication, such as e-mail and instant

messaging (IM), and messages sent to a Web site and a conversation group. A cyberstalked relies upon the privacy afforded by the Internet to allow them to follow their victim without being noticed. Cyberstalking messages change from regular spam in that a cyberstalked targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with simply annoying messages.

XI. DATA DIDDLING

Data diddling arises when someone with access to information of some sort changes this information before it is arrived into a computer. This is complete to deliver some sort of benefit to the data diddling , generally financial, and is a common method of computer-related crime.

XII. IDENTITY THEFT AND CREDIT CARD FRAUD

Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name. The imposter may also use your identity to commit other crimes. "Credit card fraud" is a wide ranging term for crimes involving identity theft where the criminal uses your credit card to fund his transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is your pre-approved card falling into someone else's hands.
He can use it to buy anything until you report to the authorities and get your card blocked. The only security measure on credit card purchases is the signature on the receipt but that can very easily be forged. However, in some countries the merchant may even ask you for an ID or a PIN. Some credit card companies have software to estimate the probability of fraud. If an unusually large transaction is made, the issuer may even call you to verify.

XIII. SOFTWARE PIRACY

The unauthorized copying of software. Most retail programs are licensed for use at just one computer site or for use by only one user at any time. By buying the software, you become a ***licensed user*** rather than an owner . You are allowed to make copies of the program for backup purposes, but it is against the law to give copies to friends and colleagues.

Software piracy is all but impossible to stop, although software companies are launching more and more lawsuits against major inflators. Originally, software companies tried to stop software piracy by copy-protecting their software. This strategy failed, however, because it was inconvenient for users and was not 100 percent fool proof. Most software now requires some sort of registration, which may discourage would-be pirates, but doesn't really stop software piracy.

XIV. MOBILE PAYMENT AND BANKING HACKS

Every online communication is possibly weak, even mobile payments and online payments. With millions of attacks against financial organizations daily, the core defence most banks have is "generating money" out of thin air using credit based on the assumed resolution of the problem in the future. It's a bubble that security experts are scrambling to stabilize before it bursts.

XV. CAUSES OF CYBER CRIMES

A. *Ease of access*: The problem encountered in protecting a computer system from unauthorised access is that there is every chance of violating the technology by stealing access codes, recorders, pins, retina imagers etc. that can be used to fool biometric systems and bypass firewalls to get past many a security system.

B. *Cyber Hoaxes*: Cyber Crimes can be committed just to reason threats or damage one's character. This is the most risky of all causes. The complex believe in fighting their cause and want their goal to be succeeded. They are called cyberterrorists.

C. *Negligence*: There are possibilities of not paying attention in defensive the system. This negligence gives the criminals control to damage the computer.

D. *Revenge or Motivation*: The greed to master the complex system with a want to inflict loss to the victim. This includes youngsters or those who are driven by desire to make quick money and they damage with data like e-commerce, e-banking or fraud in transactions.

E. *Poor law Enforcing Bodies*: Due to lack in cyber laws of many countries, many criminals get away without being punished.

F. *Cyber Crimes committed for publicity or recognition*: Generally committed by youngsters where they just want to be noticed without heartbroken someone's feelings.

1. Specific Cyber Security Technologies

1.1 ACCESS CONTROL AND IDENTITYMANAGEMENT User Name / Password Combination Since the beginning of 1960, computer has been the key to access control. Only the owner of that system can open the system and our system is safe from other people.

1.2AUTHENTICATION documents need to be certified as being generated from a trusted source and that they have not been changed later.

1.3 MALWARE SCANNERsoftware that scans files and messages regularly for malicious code. Our software is safe with the help of this software and avoids our conflicts with further attack.

1.4 FIREWALL A firewall program will monitor a traffic both in and out of the computer and alert the user for unauthorized access. Firewalls keep our system safe from attack by network.

1.5 CRYPTOGRAPHY INFORMATION SECURITY It is used in two main ways: It is better known that encrypting the data and data stored in the transit is to provide privacy. With its help, we can send our data from Source to Destination Point without any troubles.

XVI. CYBER SECURITY CHALLENGES

1. HACKERS ARE NOT GOING TO QUIT THEIR ACTIVITIES.

In fact, according to more than one presenter, attacks on our digital systems are not only going to increase in number, but also in sophistication.

2. STAKEHOLDERS NEED TO COOPERATE WITH ONE ANOTHER ON A MASSIVE SCALE.

Business and academia must cooperate with government agencies and form partnerships to share information to help thwart cyberattacks.

3. THE NEEDS OF THE FUTURE IT WORKFORCE IS CHANGING RAPIDLY.

There is an ongoing lack of skilled professionals to fill the unoccupied seats in our IT departments.

4. AS WE INCREASE OUR GLOBAL CONNECTIONS THROUGH THE INTERNET OF THINGS (IOT), SO TOO WILL INCIDENTS OF ATTACKS.

As a myriad of chip-enabled products are released to consumers, the Internet of Things (IoT) will exponentially broaden the attack surface and increase our vulnerabilities.

5. LEADERS ARE AWARE OF CYBERSECURITY ISSUES, BUT DO NOT KNOW WHAT TO DO NEXT.

The entire issue of cybersecurity has gone from a back office nuisance to a major topic of conversation. Today's C-Suite executives now pay attention, but in many cases are not sure what to do.

6. SPECIALIZED CYBERSECURITY GROUPS WILL CONTINUE TO RISE.

'Hunt Teams', highly skilled and specialized cybersecurity groups that seek out attackers in a system, will continue to grow. These professionals have been seen in in increasing numbers in the cybersecurity operations centers of organizations.

7. MONEY DOES NOT EQUAL SECURITY.

Chief information security officers are coming to realize that simply throwing money at the issue may not provide the security they are seeking.

8. THERE IS SIGNIFICANT LAG TIME BETWEEN DATA BREACHES AND DETECTION.

On average, 146 days pass between the day an organization's digital system is attacked and breached and when the attack is detected.

9. ATTACKS ON OUR CRITICAL INFRASTRUCTURE WILL BECOME MORE FREQUENT.

Our critical infrastructure continues to be under mounting attack as bad actors in the form of individuals, groups and nation states probe for weaknesses in the cyber defences of these all-important sectors.

10. THE CYBERSECURITY INSURANCE INDUSTRY WILL EXPAND ITS ROLE.

Cybersecurity insurance will continue to balloon as organizations seek to shift financial and moral responsibility for breaches of their digital systems.

XVII. CONCLUSION

Cyber crime is now serious, common, forceful, developing, and increasingly sophisticated, and poses major effects for national and economic security. Many industries, institutions, public- and private-sector organizations (particularly those within the critical infrastructure) are at major risk. For businesses and governments alike, getting the Cyber Security posture right across all its elements will be vital for future growth, innovation and competitive advantage. There is no single answer for success, but by working across public and private sector partnerships and by advancing security measures particularly with regard to mission-critical systems, processes and applications that are connected into cyberspace, businesses will be able to work towards a future environment that is both open and secure and prosperous.

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to our principal **Dr.R.K.Dwivedi** and my teacher **Dr. Rajeev Kumar** who gave me the golden opportunity to do this wonderful research paper on the topic **CONTROL ANALYSIS ON SECURITY AS CYBER CRIME**, which also helped me in doing a lot of Research and i came to know about so many new things I am really thankful to them. Secondly i would also like to thank my parents and friends who helped me a lot in finalizing this research paper within the limited time frame.

REFERENCES

[1] " Challenges of cyber crimes in present time "http://blog.tesu.edu/10-critical-cybersecurity-challenges-for-2017-and-beyond
[2] "Introduction to Indian cyber laws", Asian School of Cyber Laws
[3] " Introduction of cyber crime and cyber crimes types" http://www.ijser.org
[4] http://en.wikipedia.org/wiki/computersecurity. Computer Security. Accessed on 08/03/2013
[5] S. Krasavin, What is Cyberterrorism?, Computer Crime Research Center, April 23, 2004. Accessed from http://www.crime-research.org/analytics/Krasavin/ on 12/03/2013.
[6] "Book information security & cyber law by Poonam Singh"
[7] "A Study on Cyber Crime and Security Scenario in INDIA" www.ijemr.net
[8] "Study of Latest Emerging Trends on Cyber Security and its challenges to Society"www.ijser.org