A Survey of Cyber Crimes

Dr. K. Kiran Kumar
HOD, Department of Computer Science & Engineering
Chalapathi Institute of Engineering & Technology
Guntur, Andhra Pradesh, India

Sk. Mahaboob Basha
Student, Third Year, Department of Computer Science & Engineering
Chalapathi Institute of Engineering & Technology
Guntur, Andhra Pradesh, India

S. Nividitha
Student, Third Year, Department of Computer Science & Engineering
Chalapathi Institute of Engineering & Technology
Guntur, Andhra Pradesh, India

***Abstract*— With the advancement of computer and information technology, cyber crime is now becoming one of the most significant challenges facing law enforcement organizations.Cybercrimes are generally referred as criminal activities that use computers or networks. An understanding of the characteristics and nature of cyber crimes is important in helping research communities find ways to effectively prevent them. Most existing research focuses more on attacks and attack models, including either actual attacks or imaginary/possible attacks over all layers of networks or computers, but there has been less work carried out on a comprehensive survey of cyber crimes. This paper provides a survey of cyber crimes that have actually occurred.we also notice that some cyber crimes are actually traditionally non- cyber crimes that are facilitated by computers or networks. It is surprising that there are so many recurrent cyber crimes. More efforts are needed to protect people from cyber crimes.**

Keywords*— *Cybercrimes; forensics

1. INTRODUCTION

With the advancement of computer and information technology, cyber crime is now becoming one of the most significant challenges facing law enforcement organizations.Cybercrime generally is described as criminal activities that use modern information technology, such as computer technology, network technology, and so forth. Usually, the term cyber crime refers to criminal behavior carried out through a computer or network.There are all kinds of cybercrimes, including illegal access(such as hacking), illegal interception, data interference, systems interference, misuse of devices, forgery (ID theft), electronic fraud, etc. Security on Internet is challenging. Security on an Internet is important because information has significant value. Implementing security involves assessing the possible threats to one's network, servers and information.

Cyber crime is now becoming a serious concern. Many researchers put a great deal of energy into protecting society and human beings from cyber crimes. This developing world of information technology has a negative side effect. It has opened the door to antisocial and criminal behavior. Our motivation for writing this paper is to help people realize the comprehensive classifications and examples of cyber crimes. We expect that this paper can help reduce the number of cyber crimes listed in this paper significantly in the near future. In this paper, we provide a comprehensive survey of cyber crimes that have actually occurred.

2. DEFINITION OF CYBER CRIME

Cybercrime is defined as a crime in which a computer is the object of the crime or is used as a tool to commit an offense. Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime

3.REASONS FOR CYBER CRIME

Capacity to store data in comparatively small space

The computer has unique characteristics of storing data in a very small space. This affords to remove information either through physical or virtual medium makes it much easier.

Easy to access

The problem encountered in guarding a computer system from unauthorized access is that there is possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system**.**

Complex

The computers work on operating system & these operating systems in turn are composed of millions of codes. Human mind is fallible&is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

Negligence

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the

computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

Loss of evidence

Loss of evidence is a very common & obvious problem as all the data areroutinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

4.TYPES OF CYBER CRIMES

1.HACKING

2.CYBER TERRORISM

3.MALWARES

4.ONLINE GAMBLING

5.CYBER STALKING

6.VIRUS DISSEMINATION

7.PHISHING

8.SALAMI ATTACK

9.CHILD PORNOGRAPHY

10.SPOOFING

1.HACKING

Hacking involves gaining unauthorized access to a computer and altering the system in such a way as to permit continued access, along with changing the configuration, purpose, or operation of the target machine, all without the knowledge or approval of the systems owners.

EXAMPLE:

Koobface

An anagram of Facebook, Koobface was a hybrid, or blended threat, malware. It used the trickery aspect of a Trojan and the autonomously replicating nature of a computer worm – a type of standalone virus that does not need to attach itself to another program to spread the infection. Koobface penetrated systems of unsuspecting Facebook users by tricking them into believing they were clicking on a video. As in other scams, hackers used the compromised account of a Facebook friend by sending a private message through the Facebook platform.

The user, believing that it was a genuine message from an acquaintance, would take the bait and click on the video. This would cause users to be redirected to a site claiming they needed to upgrade their Adobe Flash Player software. The bogus site would then provide them with a link to download the update. The download was actually Koobface, and once it was installed it gave an attacker complete access to the victim's personal data, including passwords and banking information.Since the Koobface virus was neutralized just a few years after it first came out in 2008, it is difficult to estimate the full extent of damage it caused. According to Kaspersky Lab, as cited by Reuters, the Koobface virus "afflicted between 400,000 and 800,000 computers during its heyday in 2010."

2.CYBER TERRORISM

Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

EXAMPLE:

In 1999,North Atlantic Treaty Organization Computers attacked by hackers.It was a DOS attack performed by hackers using flooding e-mails.The attack was motivated by political purposes and e-mails containing political contents along with viruses bombarding many institutes and Organizations.More recently, a distributed DOS attack was initiated when the Estonian Government tried to remove the Russian World War - 2 memorial in may 2007.some websites were inaccessible during the attack, especially the government websites. Peoplebelieved that the attack might have been related to Russian hackers and even the Russian government;however, no one was able to prove this.Hackers attacked the website of Ukrainian president victor Yushchenko in October 2007.The Eurasian Youth Movement, a radical Russian Nationalist Youth group, claimed responsibility.

3.MALWARES

According to the definition in malware refers to software designed to penetrate or destroy a computer system without the knowledge of the owner. The word malware combines the words malicious and software. As generally used by computer professionals, the expression refers to all kinds of software or program codes with hostile or intrusive purposes. However, the term "malware" is seldom used by computer users, and many people are confused by the terms "malware" and "virus". The term "virus" is inappropriately used in common parlance to describe all kinds of malware, but not all kinds of malware are actually viruses. Software is considered malware only if the creator's intent is malicious. There are many examples of malware,such as computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, and other malicious and unwanted software.

EXAMPLE:

cryptoLocker :-

This malware encrypts your data and displays a message which states that your private information can be decrypted for a sum of money in a limited period of time. Though CryptoLocker can be removed by various security solutions, there isn't any way yet to decrypt the locked files.CryptoLocker is one of the nastiest pieces of malware ever created. It's not just because it takes money from you or

because it can access your private data, but once it manages to encrypt your information, there is no way for you to decrypt those files. This ransomware is so dangerous because the affected users have their private information disclosed (and taken advantage from) and they also lose the files without having any chance of recovering them.CryptoLocker is a ransomware Trojan which can infect your system in different ways, but usually this happens through the means of an apparently legitimate e-mail attachment, from a well-known company or institution. Because it spreads through e-mail attachments, this ransomware is known to target companies and institutions through phishing attacks.

4.ONLINE GAMBLING

Online gambling generally refers to gambling over theInternet. In the following, we will introduce some forms ofonline gambling, as well as some general issues.

EXAMPLE:

In November 2002, sports betting with interstate electronic information transmissions was prohibited by the US Court of Appeals for the Fifth Circuit; however, there is a lower court ruling for the betting related to sports through the Internet. Any possible form of online gambling is prevented in some states by special laws for online gambling. Without a license, it is illegal for anyone to own an online game. However, there is currently no law on granting online gaming licenses in any state.

5.CYBER STALKING

The Criminal follows the victim by sending emails,entering the chat rooms frequently. In order to harass a woman her telephonenumber is given to others as if she wants to befriend males befriend males.

EXAMPLE:

Ritu Kohli (first lady to register the cyber stalking case) is a victim ofcyber-stalking. A friend of her husband gave her phone number and name on a chat site for immoral purposes

6.VIRUS DISSEMINATION

This category of criminal activity involves either direct or searchunauthorized access to computer system by introducing new programs known as viruses, worms or logic bombs. The unauthorized modification suppression or erasure of computer data or functions with the Internet to hinder normal functioning of the system is clearly a criminal activity and is commonly referred to as computer sabotage. Malicious code is computer code that is writtenwith the sole intent to cause damage to a machine or to invade the machine to steal information. The most common forms of malicious code are viruses, worms, and Trojan programs

VIRUS: (Vital information resources under seize). Virus is a series of program codes with the ability to attach itself to legitimate programs and propagate itself to other computer programs. Viruses are file viruses and bootsector viruses. It attacks the fat so that there is no sequence of file content and it destroys the data content.

WORMS:(Write Once Read Many)

They are just added to the files and they do not manipulate. It differs from a virus in that it does not have the ability to replicate itself.

LOGIC BOMB:

As it involves the programming the destruction or modification of data is at a specific time in the future.

Why do people Create These Viruses?

- To distribute political message.
- To attack the products of specific companies.
- Some consider their creations to be works of art, and see as a creative hobby

7.PHISHING

In computing, phishing refers to attempts to criminally and fraudulently gain sensitive information, such as usernames, passwords, and credit card details, by means of some public entities that run on electronic systems, such as online banks, PayPal, and eBay. Typically, phishing uses e- mail or instant messaging and directs users to enter their detailed information on the Web site. Nowadays, efforts have been made to protect people from phishing, including legislation, user training, and technical measures. The phishing technique has been used since 1987, and the first recorded phishing was in 1996, although the term existed on hacker- related print publications even earlier. In these years, phishing- related reports increased dramatically. Recently, such crimes have been more likely to target customers of banks and payment services. E- mail is also a critical way to steal customers' sensitive information. Initially, phishers send e- mails indiscriminately to many people expecting some to respond. Thereafter, criminals determine which bank the users used and begin to send bogus e- mails, responsively. Phishers also target social networks; through which they can gain a customer's personal information for identity theft. It has been reported that such attacks have reached a success rate of over 70%.

EXAMPLE:

ONLINE CREDIT CARD FRAUD ON E-BAY

Bhubaneswar: Rourkela police busted a racket involving an online fraud worth Rs 12.5 lakh. The modus operandi of the accused were to hack into the eBay India website and make purchases in the names of credit cardholders.Two persons, including alleged mastermind Debasis Pandit, a BCA student, were arrested and forwarded to the court of the sub divisional judicial magistrate, Rourkela. The other arrested person is Rabi Narayan Sahu.Superintendent of police D.S. Kutty said the duo was later remanded in judicial custody but four other persons allegedly involved in the racket were untraceable. A

case has been registered against the accused under Sections 420 and 34 of the Indian Penal Code and Section 66 of the IT Act and further investigation is on, he said.
While Pandit, son of a retired employee of Rourkela Steel Plant, was arrested from his Sector VII residence last night, Sahu, his associate and a constable, was nabbed at his house in Uditnagar.Pandit allegedly hacked into the eBay India site and gathered the details of around 700 credit cardholders. He then madepurchases by using their passwords. The fraud came to the notice of eBay officials when it was detected that several purchases were made from Rourkela while the customers were based in cities such as Bangalore, Baroda and Jaipur and even London, said V. Naini, deputy manager of eBay. The company brought the matter to the notice of Rourkela police after some customers lodged complaints. Pandit used theaddress of Sahu for delivery of the purchased goods, said police. The gang was involved in train, flight and hotel reservations. The hand of one Satya Samal, recently arrested in Bangalore, is suspected in the crime. Samal had booked a room in aBangalore hotel for three months. The hotel and transport bills rose to Rs 5 lakh, which he did not pay. Samal was arrested for non-payment of bills, following which Pandit rushed to Bangalore and stood guarantor for his release on bail, police sources said.

8.SALAMI ATTACK

In such crime criminal makes insignificant changes in such a manner that such changes would go unnoticed. Criminal makes such program that deducts small amount like Rs.2.50 per month from the account of all the customer of the Bank and deposit the same in his account. In this case no account holder will approach the bank for such small amount but criminal gains huge amount.

EXAMPLE:

The Ziegler case wherein a logic bomb was introduced in the bank's system, where deducted 10% from every account and deposited it in a particular account.

9.CHILD PORNOGRAPHY

Child pornography is the term used to describe the sexualabuse of children by means of pornographic material. With the help of the Internet, it is quite easy to spread images and video.Child pornography is illegal all over the world. Related production of such material is also prohibited. The main reason that such criminal activities continue is the profit that can be generated from the sale of such images. Photographs and movies are still being produced and purchased. From a statement by the UK Children's charity NCH, child pornography cases have undergone a 1500% rise since 1988.As such, more and more children are becoming the victims of such crimes. According to a review in 2008, exposure to child pornography stimulates and provokes criminal sexual intentions that otherwise would have lie buried or was inaccessible. Exposure to child pornography may heighten desires and motivate people to act on urges by lowering internal restraints. Anonymity (or the belief that anonymity exists) may further loosen these internal restraints, such that the individual "practices" molestation intheir imagination that is facilitated by still or moving images. This makes actual criminal sexual behavior with children more probable if the person was already sexually motivated toward children and creates new sexual interest in children. The review article states that these are plausible hypotheses, while there is a lack of clarity as to the general applicability of these mechanisms. The review article mentioned in the former paragraph further indicates that, when child pornography users go on to commit sexual offenses, the offenses are characterized by the exploitation of a relationship that is bent by the offender in the direction of sexuality and by the absence of violence. The most common charges are statutory rape and other types of sexual crimes in which the victim has cooperated. Additionally, some materials (such as images) relatedto child pornography are created artificially. In these cases, the children involved are not the actual persons.Therefore, there is a dispute on whether such a form falls under thescope of child pornography.

10.SPOOFING

Getting one computer on a network to pretend to have the identity of another computer, usually one with special access Privileges, so as to obtain access to the other computers on the network.

EXAMPLE:

Pranab Mitra, former executive of Gujarat Ambuja Cement posed as a woman, Rita Basu, and created a fake e-mail ID through which he contacted one V.R. Ninawe an Abu Dhabi businessmen. After long cyber relationship and emotional massages Mitra sent an e-mail that ''she would commit suicide'' if Ninawe ended the relationship. He also gave him ''another friend Ruchira Sengupta's'' e-mail ID which was in fact his second bogus address. When Ninawe mailed at the other ID he was shocked to learn that Mitra had died and police is searching Ninawe. Mitra extorted few lacs Rupees as advocate fees etc. Mitra even sent emails as high court and police officials to extort more money. Ninawe finally came down to Mumbai to lodge a police case.

5. PRECAUTIONS TO PREVENT CYBER CRIME

Nobody's data is completely safe. But everybody's computers can still be protected against would-be hackers. Here is your defense arsenal.

1. Firewalls:
These are the gatekeepers to a network from the outside. Firewall should be installed at every point where the computer system comes in contact with other networks, including the Internet a separate local area network at customer's site or telephone company switch.

2. Password protection:
At minimum, each item they logon, all PC users should be required to type-in password that only they and network

administrator know. PC users should avoid picking words, phrases or numbers that anyone can guess easily, such as birth dates, a child's name or initials. Instead they should use cryptic phrases or numbers that combine uppercase and lowercase. Letters such as the "The Moon Also Rises". In addition, the system should require all users to changepasswords every month or so and should lockout prospective users if they fail to enter the correct password three times in a row.

3. Viruses:

Viruses generally infect local area networks through workstations. So anti-virus software that works only on the server isn't enough to prevent infection. You cannot get a virus or any system-damaging software by reading e-mail. Viruses and other system-destroying bugs can only exist in files, and e-mail is not a system file. Viruses cannot exist there. Viruses are almost always specific of the operating system involved. Meaning, viruses created to infect DOS application can do no damage to MAC systems, and vice versa. The only exception to this is the Microsoft Word "macro virus" which infects documents instead of the program.

4. Encryption:

Even if intruders manage to break through a firewall, the data on a network can be made safe if it is encrypted. Many software packages and network programs – Microsoft Windows NT, Novel NetWare, and lotus notes among others- offer and – on encryption schemes that encode all the data sent on the network. In addition, companies can buy stand alone encryption packages to work with individual applications. Almost every encryption package is based on an approach known as public-private key. Scrambled data is encoded using a secret key unique to that transmission. Receiver's use a combination of the sender's public key and their own private encryption key to unlock the secret code for that message decipher it.

5. Never send your credit card number to any site which is not secured.

6. Uninstall unnecessary software

6. CONCLUSION

With the great advance of computer technology, there now exist many different kinds of cybercrimes.Anyone could be attacked by a cybercriminal. Serious attacks happen every day and we should have basic preparation and principles to protect ourselves awareness is the best defense. In this paper we categorized Cyber Crimes intodifferent types and explained each type. The main purpose of this paper is to help people realize the Threats and potential attacks and to learn from these attacks in order to better protect themselves.

7. REFERENCES

[1] Moore R. Cybercrime: investigating High-Technology Computer Crime. Anderson publishing: Cleveland, Mississippi 2005.
[2] IT magazine (dec. 2008)
[3] Pc quest(dec.2008)
[4] Englund H,Johansson T.Three ways to mount distinguishing attacks on irregulary clocked stream ciphers. International Journal of Security and 2006;
[5] Cyber Crimes .April 2008.Available from:http://theviewspaper.net/cyber_crimes [accessed on 25 april 2010]
[6] Deng J,Han R,Mishra S.Limiting DoS attacks during multihop data delivery in wireless sensor networks. International Journal of Security and Networks 2006;
[7] Guo Y,Perreau S.Detect DDoS flooding attacks inmobile adhoc networks. International Journal of Security and Networks 2010.