Cyber Crime and Security- Challenges and Security Mechanisms

Niral Shah [#1], Naveen Vaswani [*2]

[#]Student, Department of Computer Engineering, Watumull Institute of Electronics Engineering and Computer Technology, Worli, Mumbai, Maharashtra, India

[*]Assistant Professor, Department of Computer Engineering, Watumull Institute of Electronics Engineering and Computer Technology, Worli, Mumbai, Maharashtra, India [2]

Abstract: *Man has reached a long way since inception and during the course of time he has managed to develop and invent technology for his own benefits. One can't deny the fact that the computer by far is one of the finest creations of the humans. It has become an indispensable part of our life and it has become a very important tool in this information era. Computers with internet connections have enabled the man to perform any job or activity with just one click. Ordering food, online shopping, performing bank transactions, getting any kind of information at any time and at any given place has become very easy, thanks to the internet. So this proves that undoubtedly computers and internet are omnipresent and are linked directly or indirectly in almost every activity we do.*

Everything has its equal share of pros and cons. And computers and internet networks are no such exception. The internet has been used by many miscreants for all the wrong purposes. The issue of cyber crime has risen considerably in the last decade or so. Many people have fallen prey to the cyber crime. This problem has been in the market since long and since its arrival, methods and strategies are constantly invented on how to tackle the cyber crime. Many security mechanisms have also been developed to avert the cyber crime. This presentation will concentrate on the challenges faced to tackle cyber crime and also briefly discuss about the security mechanisms employed for the same.

Keywords: *Computer crime, Identity crime, Cyber crime, Cyber Security, Security Mechanisms for Cyber Security.*

I. Introduction to Cyber Crime.

Since the invention of computer has been done, it has made man's life much easier and simple. Almost everything what he wishes is just a click away. With the advent of the internet, human communication across continents is now easily achievable. It has become one of the most used and most convenient forms of communication. The internet has grown at a tremendous rate since its establishment, and more and more people are depended on the services provided by it. Internet has managed to reach almost every corner of the world. Up to June 2008, the Internet has distributed to over 233 countries and world regions, and has more than 1.46 billion users [1]. Now based on the statistics up to November 30, 2015 the internet has distributed to over 243 individual countries and world regions and has more than 3.36 billion users [2].

The most fundamental definition of Cyber Crime is the activites performed with the help of internet by the people with the intention of attacking someone's reputation or stealing unauthorized information. Debarati Halder and K. Jaishankar define cybercrime as: "Offences that are committed against individuals or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)" [3]. Cyber crimes have increased to a great extent be it in the form of Trojan attacks, salami attacks, etc. A survey conducted by ISACA revealed that the total number of security incidents detected by respondents grew to 42.8 million around the world, up 48% from 2013 [4].These crimes are not just restricted to a person or a group of persons, but it also is a threat to the nation's security as well. Crimes committed with this regard are considered high profile as the security of a whole country becomes vulnerable. In Cyber crime the computer can either be used as target or can be used as a tool. Cyber Crime has been profitable than most of the trades including the drug trade. According to the 2008 CSI computer crime & security survey by Computer Security Institute (CSI), cyber attacks cause a lot of money losses each year [5]. It has thus become a humongous threat in this modern age of computers.

The history of cyber crime goes to almost 30 years back. The first incident to indicate the potential of computer crime occurred in 1986. An investigation in the matter later revealed that a German hacker had hacked military database using only a computer and modem to obtain sensitive information [6].Initially the hackers hacked only to get information about the other systems. But as time flew, hackers became more skillful and efficient and started using their skills to victimize and exploit other people.

II. Related Work

Since the first case of cyber crime has ever been reported, people and ethical hackers have been striving hard for discovering ways on how to prevent the criminals from getting the data and information. The internet is such a such a vast field that even after finding ways to stop cyber crime from occurring, the criminals find out newer and efficient ways to steal important data and information. There are various traditional ways and preventions proposed by many people in order to not fall a victim to cyber crime. These ways include detection of the crime after it has occurred and taking the necessary action. This method has been in the market for a long time and most of the companies focus on deploying the antivirus as soon as the threat is detected. Now detection should not be the only step taken by the companies, considering the level and intensity of cyber crime committed now a days.

In order to maximize the data security of a company or enterprise or nation, series of steps have to be implemented, and detection is just the first among them. A study about the working of the threat should be done so it will help to understand the gravity of the threat in a much better way. It will also help in formulating the solution based on study of the threat. After analyzing the capabilities of what the threat can do and in what way it can harm the company, the company or organization must be ready with the defense mechanisms if a similar threat attacks anytime in the future. Other ways which were suggested before are to not open the emails from unknown source. These emails might contain links in them which on clicking can install malicious software or key logger software. With the help of such software the criminals can get their hands on sensitive and personal information of the user.

These were some of the traditional and proposed ways to fight cyber crimes. But as time has progressed, the nature of cyber crime has also changed and improved over the years. So employing the traditional strategies just won't be enough. This presentation will enlighten on various ways to prevent cyber crimes for occurring and discover, detect and mitigate if the crime has already occurred. Preventing the cyber from occurring is always better than detecting the cyber crime and then fighting towards it.

III. Cyber Crime Examples

The crimes committed over the internet are referred to as cyber crimes or computer crimes. The various examples of cyber crimes are:

*1) **Financial Fraud*** [7] - This type of crime can be defined as an intentional act of cheating or deception in which financial transactions, which may amount to lots of money, are involved for purpose of personal gain. This type of fraud includes Tax Refund Fraud and account takeover frauds.

*2) **Hacking**-* This is a type of crime in which a person's computer is broken into virtually to retrieve his personal or sensitive information. Identity theft, theft of sensitivity data etc come under this category.

*3) **Cyber Extortion**-* In this type of crime, the individual sends company a threatening email or message stating that they have received confidential information about their company and will leak it online unless their demands are not met with.

*4) **Cyber Vandalism**-* Cyber vandalism means destroying or damaging the data or information stored in computer when a service provided by the network is stopped or disrupted. Physical harm done to the computer in any way also comes under this category.

*5) **Child Soliciting and Abuse**-* In this type of crime the criminals solicit minors via chat rooms for bad reasons.

Monitoring of the chat rooms has been frequented with the hopes of reducing and preventing child abuse.

IV. Types of Cyber Crime

In the recent times, the cases of credit card thefts, online money laundering and email spoofing crimes are doing the rounds. Cyber crime has also penetrated the field of e-banking. Piracy of music, videos and software has also risen to a great extent. In India there are less stringent laws in accordance with the cybercrime. The IT Act of 2000 was a welcoming move but it mainly concentrated on e-commerce.

Types of Cyber Crime are [8]:

Type 1: In this category, the cyber crime is confined to single user only. The user may accidently download a file or is duped to open a link send as attachment in the email. As soon as the user downloads this file, the Trojan horse enters the computer and acts like a backdoor in the computer. This enables the hackers to get unlimited access to the user's personal information and also enables them to delete or modify files in it. The Trojan horse is also capable of installing key logger in the user's machine or device. This enables the hackers to get sensitive information such as passwords and personal details.

Type 2: This category consists of series of events unlike category 1. In this, the target is contacted through social networking sites and tries to establish a friendly relation with him. Eventually the criminals misuse this friendship to commit a crime. The examples in this can be cyber stalking, harassment etc.

V. Cyber Security

Information Systems are complex and often require Network security. Automation has undoubtedly helped to bring smooth operation but it has also enabled risks of data breaches. It is indispensable that organizations introduce mechanisms and measures to protect their sensitive data from reaching to the people who are not authorized to use it. The information technology section of each organization must ensure that the necessary steps are taken so that the data is not lost to the wrong people. There are two aspects in introducing network security; the first is to deal with the hardware or equipment as well as the tools required such as authentication and encryption software, LAN analyzers tools and so on. The other aspect deals with the need of workforce or staff trained in aspects of network security for information systems. These people comprises of administrators, security officers and system analysts.

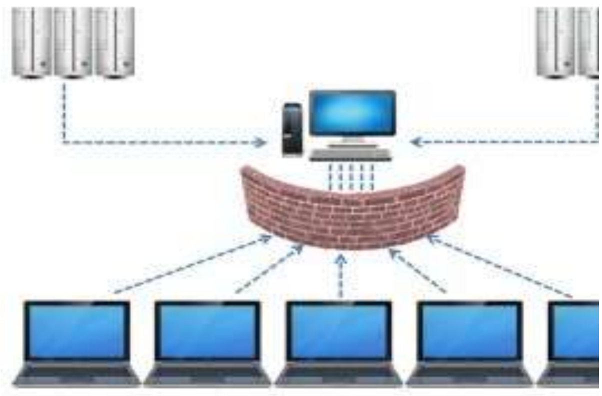

Fig. 1 Diagrammatic representation of the hackers trying to penetrate a personal computer and security mechanism trying to prevent them.

Cyber Security can be divided fundamentally into four strategies:

- Prevention Strategies
- Detection Strategies
- Recovery Strategies
- Mitigation Strategies

Prevention Strategies: Prevention is always better than cure. It is always better to take certain precautions before working on the net. Many attacks can be avoided by having some prior technical knowledge. The criminals committing cyber crime are desperate of making fast money. So the more difficult you make their job, there are bright chances of them sparing you and moving on to the next easier target. Apart from the ID3 algorithm with respect to data mining techniques and which reduces complication of calculation [9], prevention strategies can be further classified into two techniques [10]:

- Proactive Defense Technique
- Reactive Defense Technique

Proactive Defense Technique: - This technique includes following ways to prevent cyber crime activities:

- *Penetration testing, Ethical hacking and simulations*- This includes the imitation or simulation of an attack on a computer system to test for vulnerabilities. It also includes regular training exercises on social engineering techniques.
- *Keep computer updated* - The user must install the updates and other software fixes as soon as they are available. These updates eliminate the shortcomings in the existing system which the attackers could use to exploit the system. This won't protect the computer from all the attacks but it does block basic and automated attacks completely which might unnerve a less determined attacker to look for another vulnerable computer.
- *Configuring the Computer Securely*- It is very vital to configure Internet applications such as Web Browser and email software. This is because the settings in your Web Browser such as Chrome or Firefox will ascertain or verify what happens when you visit websites on the Internet- the strongest settings will give the most control over what happens but might frustrate some users by asking many questions (the site might not be safe, do you want to continue anyway?)
- *Vulnerability Assessment*- This includes identification, quantification and prioritization of vulnerabilities. All potential threats are assessed and all assets, equipment and infrastructure is indexed in order of the prioritization of threats.
- *Data Encryption*- Conversion of plain text and information into 'ciphertext' which is unreadable by anyone but the person who is intended to use it. So even if the information goes in wrong hands, it will be impossible to decipher the text or information.
- *Choosing Strong Passwords*- Selecting a password that cannot be easily predicted is the basic step in keeping your details secure. Nowadays passwords are used for simplest of things. Keeping the password in a safe place is equally important. Changing the passwords after some period of time is highly recommended as it can keep the damage within bounds which is caused by someone who has already gained access to your account.

***Reactive Defense Technique*: -** This technique includes following ways to prevent cyber crime activities:

- *Anti-DNos and Anti-bot Detection Systems*- This is software which detects bots and Distributed Denial of Service (DDNoS) attacks and can block communications.
- *Intrusion Prevention Systems*- These systems are often combined as Intrusion Detection and Prevention Systems. It is a software that is aimed at identifying, logging, reporting and blocking and risky or dangerous activity on computer systems. The actions initiated by these systems include resetting connections and blocking traffic from malicious IPs.
- *Reviewing bank and credit card statements periodically*- The impact of identity theft and online crimes can be curbed if you catch it shortly after your data is stolen or when the use of your information is first endeavored.
- *Firewalls and antivirus*- Firewalls are supposed to monitor open connections. This includes checking attachments in email, blocking unauthorized and unwanted traffic or disable

internet add-ons such as cookies, pop-ups etc. Antivirus scans the files or packages in your system for viruses. They clean or delete any such infected files if found.

- *Ensuring Clean Pipe*- Clean Pipe is the term for communication channel through which the user employs or delivers services. It should be made sure that the communication channel does not subsume any kind of malicious content which can alter the information passed to the end user.

Detection Strategies [11]: The typical Intrusion Detection techniques are as follows:

- *Tripwires*: These software programs take snapshots of key system attributes and behavior which can be used to compare with the previous behavior or characteristics to detect file changes. This enables to provide evidence against the hackers as they make alterations while installing backdoor entry points.
- *Honey pots*- They are employed so that they can help to keep the criminal occupied long enough for identification of the intruder. They create bogus files, administrative accounts and various other files which appear to contain sensitive information.
- *Anomaly Detection System*- These systems focus on odd patterns of activity. They analyze user profiles and user activity and immediately informs if there is something different than the usual activity.
- *Intrusion Detection Systems*- These systems detect hacker attempts e.g. a file integrity checker which detects when a system file has been altered.
- *Security Operation Centres (SOC)* - There must be a centralized unit in organization that monitors the organization’s technological infrastructure and access to the infrastructure.

***Recovery Strategies*:** The recovery strategies after cyber crime attack are as follows:

- *Backup systems and data loss prevention software*- This software enables to automatically detect and secure confidential and sensitive information which is stored on different systems.
- *Redundancy and Disaster Recovery Sites*- Storage facilities or data centres located in a separate physical location from the main network help in restoring the vital information as soon as possible.

Mitigation Strategies:

- *Disconnect Immediately*- One must unplug the network cable, phone, or cable line from the computer. This can prevent data from being leaked to the attacker. Disconnecting the network connection is also a very effective way to put stop to immediate damage.
- *Scan the Computer*: Scan the computer as soon as possible with the antivirus installed in your computer. It will enable to detect and remove threats that would otherwise remain hidden in the computer.
- *Back Up Critical Information*- Backing up the data is a surest way of ensuring that all your personal details and information are safe as there is a high probability of the data being leaked or lost or destroyed in the cyber attack.

VI. CHALLENGES OF FIGHTING CYBER CRIME

Fighting against cyber crime is not just an activity of fortnight. It is a continuous activity. As the cases of cyber crime arise everyday with newer forms, the challenges to curb them also increase considerably. The challenges in cyber crime can be broadly classified into two types:

General Challenges [12]:

1] ***Reliance on ICTs***- Most of the communications that is being used by us depends on Information and Communication Technology (ICT). The dependence on ICT is likely to grow in the coming years. This growing dependency on ICTs makes the systems weaker to attacks. Minor attacks or interruptions can cause huge financial damages to big companies. This is not only just limited to big companies, but also to government and military communications. Every infrastructure has some or the other weakness. If there are large numbers of people using the same operating system, then the hackers can design effective attacks by targeting a single person.

2] ***Number of Users***- The popularity of the internet is growing at a fast rate and the people using internet has crossed almost 3.36 billion by November 2015 [2]. As the number of people using the internet services increases, the number of people falling victim to it and the number of criminals also rise. Among so many people it is hard to extrapolate how many people are using the internet for wrong purposes.

3] ***Identification of Network and Devices***- The basic equipment required to commit a cyber crime is a computer and internet access. Criminals usually use those hardware and software which are available for a very cheap price. Software can be downloaded for free from various sites. Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices. Criminals mostly use only those internet facilities in which their registration is not required so their chances of being caught reduces considerably for example public networks or open networks.

4] ***Easy Availability of Information***- The internet is a storehouse of millions of web pages which contains latest up to date information. Anyone can access those web pages. This information can be used for both constructive and destructive purposes. Before the internet, it was quite difficult to access any information. But now the internet has made a lot of things easy. Using the internet search engines, information about a particular individual can also be obtained which can be later used by criminals to target them.

5] ***Automation***- ICTs have enabled us to automate certain processes thereby reducing the time consumed and speeding up of processes. This has proved to be very useful in many technologies. But the criminals have used this technology to send millions of spam messages or technical support messages in bulk. According to a report from Symantec, they blocked over 100 million of fake technical support scams in 2015 [13]

Long term Challenges [14]:

1] ***Design***- The integral part of any ICT design should be effective security. But due to economic reasons, the developers concentrate more on the features than the security aspect. As the future needs cannot be predicted, it becomes a difficult challenge for designers to come up with an efficient design.

2] ***Incentives***- Committing cyber crime is much cheaper than employing means for cyber security. Cyber security is very unpredictable as the criminals can come up with newer means of committing crimes. Thus the return on investments is also unsure.

VII. CONCLUSION

In this paper, we have discussed about cyber crime and have catalogued various effective strategies for its prevention, detection, recovery and mitigation. The contributions of this paper are as follows:

- Several effective ways have been listed out which can be used to avert or prevent cyber crimes.
- Several strategies have been proposed as to how to tackle Cyber Crimes if one is a victim of it.
- Several challenges for fighting cybercrime have been enlightened.
- After doing the study on various strategies of prevention, detection, recovery and mitigation, we can conclude that prevention is better than the rest. We should strive our best to avert those attacks as much as possible and if at all we are a victim of cyber crime attacks then we must religiously follow the mitigation and recovery techniques mentioned above.

VIII. FUTURE WORK

1] Presenting a detailed paper on the working of the mechanisms stated in prevention, detection and mitigation techniques.

2] Developing innovative and efficient algorithms to detect cyber crimes beforehand.

3] Taking each of the challenges individually and finding effective techniques to overcome or at least reduce them.

REFERENCES

[1] Zhang, Linfeng, "*Effective techniques for detecting and attributing cyber criminals*", (2008). Graduate Theses and Dissertations Paper 11953.

[2] Internet World Stats. [Online]. Available: http://www.internetworldstats.com

[3] Halder, D., & Jaishankar, K. (2011) *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations.* Hershey, PA, USA: IGI Global. ISBN 978 160960-830-9

[4] ISACA. [Online]. Available: http://www.isaca.org/cyber/Documents/State-ofCybersecurity_Res__Eng_0415.pdf

[5] R. Richardson, 2008 CSI "*computer crime & security survey*," 2008. [Online]. Available: http://www.gocsi.com/forms/csi survey.jhtml

[6] Britz, Marjie T. , "*Computer Forensics and Cyber Crime, An Introduction*", Pearson.

[7] Dr. Mike McGuire and Samantha Dowling, "*Cyber Crime: A review of the evidence*", (2013), Home Office Research Report.

[8] Norton by Symantec [Online]. Available: http://in.norton.com/cybercrime-definition

[9] Mohit M.Patel , Shailendra K.Mishra. "*Design and Development of Efficient Algorithm in Web Usage Mining For Web Personalization*". International Journal of Engineering Trends and Technology (IJETT). V4(4):1101-1104 Apr 2013. ISSN:2231-5381. www.ijettjournal.org. published by seventh sense research group.

[10] Richard Steinberger, "*Proactive vs Reactive Security*".

[11] LogRhythm-The Security Intelligence Company. [Online]. https://logrhythm.com/solutions/security/

[12] Dr. Marco Gercke, "*Understanding cybercrime: phenomena, challenges and legal response*", (2012). ITU

[13] Symantec [Online] Available: https://www.symantec.com/security-center/threat-report

[14] Eric A. Fischer, "*Cybersecurity Issues and Challenges: In Brief*", (2014) , Congressional Research Service.