ATTACKS ON COMPUTER NETWORKS IN INDIA: PROBLEMS AND POSSIBLE ANSWERS

Dhananjay Prakash Das, C. S. Raghuvanshi, Hari Om Sharan

Faculty of Engineering & Technology, Rama University, Uttar Pradesh, Kanpur, India, 209217

drcsraghuvanshi@gmail.com

Abstract

People frequently refer to the internet as a fantastic tool, an interesting environment, and a liberated experience; yet, for whom is this true? There is a rising population of criminals that are adept at navigating the Internet, and there is a possibility that many of us may fall prey to them. Cyberspace, more often referred to as the web, is an environment that is both ephemeral and ever-changing. This article makes the case that cyber crime, sometimes known as e-crime, is a new sort of high-tech criminal enterprise. The purpose of this study is to investigate a general overview of cybercrimes, as well as the individuals who commit these crimes and the reasons they do so. also I would like to go into detail about the various types of cybercrimes, as well as the one-of-a-kind difficulties and response issues that may arise during the process of preventing, detecting, and investigating these crimes. I will also outline the various sections of India's Information Technology Act of 2000 and propose new provisions for that act. People are becoming increasingly dependent on cyberspace as a result of the fast growth of information technology, and cyberspace links billions of users from all over the world. It gives individuals a great deal of convenience, but it also gives criminals a lot of possibilities to conduct crimes by making use of the new information tools. People benefit greatly from it. Several threats to cyberspace's security, such as identity theft, tracking stolen identities, online terrorism, and virtual warfare, have been encountered in recent years. In this study, our primary focus is on doing an analysis of these many security concerns, and we discuss some potential remedies that may be provided by legislation and technological advancement.

Key words: *Cyber Space, Cyber Crime, Hacking, Intellectual Property Rights,*

Introduction

The satisfactions of fundamental wants or archetypal aspirations are not longer the most significant or urgent difficulties facing modern technology; rather, the most important and urgent problems facing modern technology are the restoration of the ills and harms caused by technology from the past. A parallel may be drawn between the current state of affairs in cyberspace and the growth of the Internet and low-cost wireless communication with the history of thalidomide, which was a wonder medicine that went horribly wrong. The computer and the internet are without a doubt the very first amendment to be brought into existence, and they are also justly regarded as one of the greatest innovations. Yet this modification was unable of self-control inside the confines of safe hands, much like an uncontrolled chain reaction that was unaware of any restrictions. The Internet is the first thing that mankind has constructed that humanity does not comprehend. It is also the biggest experiment in anarchy that we have ever had. The introduction of the Internet and the growing prevalence of the usage of information systems have both had a significant impact on the ways in which people live their lives. It is revolutionizing the growth of many nations, tearing down obstacles to business, and enabling individuals all over the world to connect, cooperate, and share ideas despite the conventional constraints of class, geographical location, and time. The combination of the internet, information systems, and people has given rise to what is commonly referred to as cyberspace, which has resulted in the creation of a worldwide virtual domain with the purpose of gaining a competitive edge. Cyberspace technologies are progressively being used by governments, enterprises, organizations, and individuals all around the world in order to increase their levels of production and profitability. It is, in fact, causing changes in socioeconomic activity and security postures, as well as opening up prospects for innovation and economic growth. Also, it has increased the available tools to enhance general governance and the welfare of people all around the world. Certainly, the advent of cyberspace has paved the way for improved opportunities for research, development, and innovation, which is, in the end, resulting in remarkable economic growth and wealth, in addition to enabling informed societies all over the world at an incredible rate (WEF, 2014). Accelerating innovation is being driven by the growing significance of cyberspace in maintaining economic growth, delivering governance to the people, ensuring national security, and ensuring general prosperity. As a result, almost every activity that was traditionally done now has a digital equivalent. We may now conduct business online, pay bills and other bills, play games, perform financial operations, and connect with individuals, corporations, and governments. On top of that, individuals may receive an education online, cooperate and share resources, host workshops, seminars, and conferences online, and in actuality, one can control faraway places by utilizing internet infrastructure. A balance of good and evil is what life is all about. The Internet is as well. Cyberspace, for all the good it provides for us, also has some negative aspects to it. The information superhighway, on the other hand, is not regulated by law enforcement in the same way that traditional communities are.

As a result, it is vulnerable to a wide variety of threats, including cyber stalking, counterfeiting of trademarks, and cyber terrorism. The expansion of information and communications technologies has resulted in a shift in how crimes are classified. A simple click of the mouse has given an anonymous index finger so much power that it may pilfer millions of dollars, bring down an entire corporation, and even jeopardize a country's ability to defend itself. The nature of conflict and war has been altered as a result of the development of technology. The concept of a "no contact war," in which there is no "physical" or "kinetic" activity across boundaries, is one of the more recent developments in the art of engaging in battle. The concept of cyberspace as a potential fifth battlefield, in addition to land, sea, and air, has an essential element that should not be overlooked. Cybercrime, which represents the pinnacle of human intellect, is the result of a fusion between two areas of application of human intelligence that are at opposite extremes (the trough of human intelligence) The human species is having more trouble sleeping as a direct result of cybercrime. The dangers are never-ending, and our laws are now weak in their response.

Issues that are faced in cyber space

In the contemporary climate, the rate of cybercrime is quickly escalating, paralleling the quickening pace of technological advancement. Hence, conducting an investigation into computer crimes is becoming a highly challenging undertaking in the absence of an appropriate framework. Today, there is a diverse selection of online criminal activities to choose from. The following is a list of the main categories that may be used to classify the legal challenges that are encountered in cyberspace:

Typo squatting:

Typo squatting, also known as URL hijacking, is a type of cyber squatting that targets Internet users who incorrectly type a website address into their web browser (for example, "Gooogle.com" instead of "Google.com"). This type of cyber squatting is a form of sitting on sites under someone else's brand or copyright. Typo squatting is also known as URL hijacking. When consumers make such a typographical error, they run the risk of being sent to an alternate website that is often developed for malevolent intentions and is owned by a hacker. This is a common tactic in cyberspace that takes advantage of the fact that users frequently make typographical errors when looking for the domain name of a website. In this scenario, a person registers a domain name that is nearly identical to that of a website that receives a significant amount of online traffic, but with a single letter changed. These websites are rife with connections to sponsored adverts that create cash for the typo squatter, and the vast majority of the time, the web surfer will fool or deceive you into believing that you are on the appropriate website. This redirects visitors away from the site that was meant for them, and frequently they end up on the website of a rival or a pornographic website instead.

Cyber squatting : Cyber squatting is the practice of registering an Internet domain name that is likely to be desired by another person, business, or organization in the hope that it can be sold to them for a profit. This is done in the hope that the person, business, or organization will then register the domain name for their own use. It includes the registration of trademarks and trade names by third parties as domain names, despite the fact that these third parties do not own any rights to such names. Simply put, cybersquatters are people who register the trade-marks, trade names, business names, and so on, that belong to third parties with the intention of trading on the reputation and goodwill of such third parties by either confusing customers or potential customers, and sometimes even to sell the domain name to the rightful owner at a profit. Bad faith imitators are also known as cybersquatters. Someone has committed cybersquatting when they intentionally register a domain name with the intention of breaching the rights of the owner of the trademark. They often have the intention of blackmailing the owner of the trademark for cash while hoarding the names to sell at a later date to the highest bidder.

Page jacking: Page jacking is a method that is used to divert traffic from the websites that were supposed to receive it to other websites on the internet, most of which contain pornographic content. After a user has entered the site, it may be difficult for them to exit because pressing the "back" button on their computer may just lead them to other pornographic sites. According to the Federal Trade Commission (FTC), the practice of pagejacking is illegal since it is considered to be an unfair and misleading business activity that inhibits trade. Pagejacking is when a criminal replicates sections of a website that already exists, and then uploads those sections to a new website in an effort to make that website appear to be the original. Phishing tactics frequently make advantage of pagejacking. When there is a disagreement over a domain name that has to be addressed, the Universal Domain Name Dispute Resolution Policy (UDRP) offers a faster and more cost-effective alternative to filing a lawsuit. The Internet Corporation for Assigned Names and Numbers (ICANN), the organization that is in charge of the registration of domain names, is the one that established this.

Necessity for cyber legislation Because of the pervasive and global nature of cybercrime, determining who has jurisdiction over a case of cybercrime is one of the most contentious questions. The application of traditional legal principles to the realm of cyberspace is fraught with challenges for a variety of reasons. Because of the ease with which a user may visit a website from virtually any location in the globe, the internet can be thought of as a multi-jurisdictional system. Each and every minute, millions of websites are browsed, and each and every day, millions upon millions of dollars are sent electronically from one bank to another throughout the world. Within a few of minutes, a person in India might hack into the electronic vault of a bank that was housed on a computer in the United States and transfer millions of rupees to another bank located in Switzerland. Since digital technology provide new ways of hiding information's inside other information's, steganography has made significant strides in recent years. This is useful in a variety of contexts, which has contributed to the field's rapid expansion. The theft of electronic information has emerged as the primary focus of cybercrime. Extreme mobility, which significantly exceeds the mobility of people, products, or other services, is one of the defining characteristics of this phenomenon.

RESEARCH HISTORY

The task of ensuring the safety of computer networks is a challenging one that is being taken into account on an increasingly regular basis by administrators of organizational centers. On this particular aspect, a considerable quantity of research has been carried out. "A security framework has been offered by the Hojaji study (2008), which should be listed as one of them because it applies to services in next-generation networks. According to his point of view, the replacement of simple and traditional infrastructure with integrated and multilayered infrastructure will cause service network operators to face challenges related to data privacy as well as security challenges, and suppliers from this platform will be exposed to new risks. Moreover, he believes that this will expose suppliers to new risks ". Research was done on symmetric encryption methods, which are applicable to a wide range of tasks in the secure network and communications infrastructure. The subject of the research was "symmetric encryption." Moreover, Azarpour et al. (2012) explored the relevance of Honey Pot technology in the process of building network security and how network experts have been successful in successfully enticing hackers into their traps. The interaction between people and computers has been problematic due to a lack of an appropriate user interface, according to the findings of an investigation that was carried out by Javadzadeh et al. (2013) into the design and building of the knowledge of systems experts for network security testing. The investigation was into the design and building of the knowledge of systems experts for network security testing. Gholipour et al. (2014) also propose a technique for evaluating the security of web-based applications that are housed within an organization's internal intranet. According to them, the security check needs to be carried out in an accurate way in line with a demanding protocol, which he and his colleagues conceived of as having 10 steps total. An information system that is able to point the systematic management of security devices through a well-defined processes is required in this area, according to the findings of an investigation that was conducted by Sayana (2003) on the methodology for auditing the approach taken to ensuring the network's security. Sayana's investigation was on the methodology for auditing the approach taken to ensuring the network's security. According to these findings, "that a high level of security cannot be attained only via the expenditure of a large amount of money and the employment of advanced equipment.

NETWORK SECURITY

computer networks, is another name for network security. In point of fact, security is made up of a number of various security dimensions, each of which is designed to represent and regulate a particular aspect of network security. These security dimensions are referred to together as security layers. The three main facets, which, when brought together, comprise the security triangle, are what need to be accomplished in order for security thinking in network design to be successful. Among these are the observance of stringent confidentiality and trust, the possession of steadfast honesty, and the availability to all parties at all times. These three fundamental principles are the building blocks of information security, whether it be inside the network or outside of it. As a consequence of this, all of the necessary precautions that have been taken for the security of the network or the equipment that has been made are all due to the need to apply these three parameters in the maintenance and exchange of information.

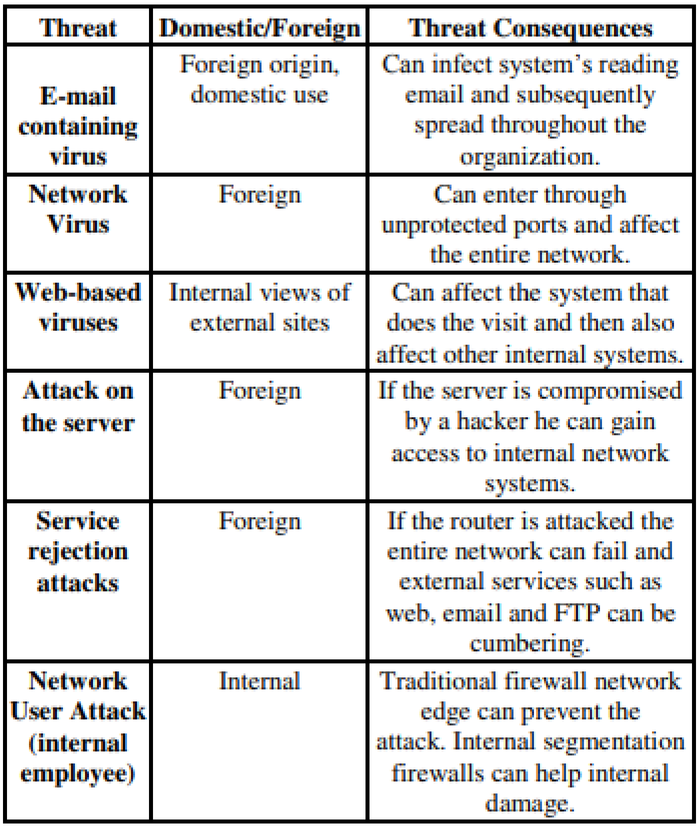
THREATS AND SECURITY VULNERABILITIES IN COMPUTER SECURITY

When we talk about network threats, we are referring to situations or individuals who have the potential to do damage to any data stored on a network. Threats to a network may originate from the elements, such as storms, lightning, or flooding, or they may be the result of human error, such as the deletion of files inadvertently. The disclosure of confidential information (also known as the threat of disclosure), damage to the integrity of information (also known as the threat of manipulation), and a lack of information are the three primary categories that can be used to classify threats to the security of information systems (damaging services threats). From one point of view, assaults may be broken down into two categories: passive and active. From another vantage point, they can be broken down into destructive and nondestructive categories. From still another viewpoint, they can be classed according to the base upon which they operate. The following is a list of the typical assaults launched against the network:

- Stop service attack (DOS): In this kind of assault, other users have access to the attacked system's resources, as well as its information and communication. This kind of assault is active, and it may be carried out by users both inside and outside the organization.
- Eavesdropping: During a passive attack, the attacker observes and listens in on the flow of information, data, and communications.
- Traffic Analysis: This is an example of a passive attack in which the attacker gathers useful information by analyzing the network traffic based on the total number of packets.
- Message and Data Manipulation: active attack, in which the attacker makes illegal modifications to the information, hence causing disruptions to the information's comprehensiveness and correctness.

Nonetheless, the vulnerability of computer networks as information technology infrastructure is the primary worry of this industry. The majority of security flaws are caused by improperly configured software and networks. Vulnerabilities, faults, and weaknesses in information systems typically manifest themselves during the design or implementation stages ("including the security procedures and security controls associated with the system"). These vulnerabilities can be harmful to an organization's operations or assets because they compromise the confidentiality, integrity, or availability of information. Organizations tend to see security as a technical issue or make the assumption that software and security solutions are effective, despite the fact that human error is the most common cause of security breaches. As a result, the majority of network invasions are the result of users' carelessness. Because of this, even blind people are susceptible to being deceived and mistreated on the network by means of social engineering. The dangers and the damage they cause are outlined in Table 1:

Table 1: An Overview of the Many Dangers and the Impacts They Might Have.



Threat	Domestic/Foreign	Threat Consequences
E-mail containing virus	Foreign origin, domestic use	Can infect system's reading email and subsequently spread throughout the organization.
Network Virus	Foreign	Can enter through unprotected ports and affect the entire network.
Web-based viruses	Internal views of external sites	Can affect the system that does the visit and then also affect other internal systems.
Attack on the server	Foreign	If the server is compromised by a hacker he can gain access to internal network systems.
Service rejection attacks	Foreign	If the router is attacked the entire network can fail and external services such as web, email and FTP can be cumbering.
Network User Attack (internal employee)	Internal	Traditional firewall network edge can prevent the attack. Internal segmentation firewalls can help internal damage.

Conclusion

Because of the complexity of the modern world, making use of the knowledge will invariably result in threats to one's safety. It has been asserted that one of the most important variables in establishing a competitive advantage is the level of protection that is afforded to the computer network of an enterprise. According to the findings of this study, any individual or event that posed a risk to the integrity of the data may be deemed a hazard to computer networks. This conclusion was reached as a result of the fact that computer networks were examined. There are three basic types of assaults that may be launched against computer networks: active assaults, passive assaults, and combined active and passive assaults "both internal and external assaults were made. Eavesdropping, traffic analysis, manipulation of messages and data, Web-based virus assaults on Web servers, attacks on RAID network users, and denial of service attacks are some of the most common types of cyberattacks that target computer networks. Other common types of cyberattacks include network viruses, e-mails containing viruses, and network viruses. There are methods accessible, such as encryption methods, which include encoding fundamental facts in language in such a way that it is difficult to read and decipher. These methods are available ". Encryption methods are one of the many defense mechanisms that may be utilized to protect against vulnerabilities and threats of this nature. As a result of this, there will be a significantly reduced risk of an intrusion into the network. On the other hand, the processes of intrusion detection and prevention systems (often referred to as IDS and IPS), govern the flow of information inside the network and prevent unauthorized access. Cyber security hazards can be difficult to spot due to the broad nature of these threats, which can result in a lack of awareness of numerous security problems. Despite the development in documenting cybercrimes under various sections of the IT act and the IPC, the vast majority of occurrences are still not reported for a number of reasons. This is despite the fact that the IT act and the IPC both provide provisions for recording cybercrimes. The severity of the cyber hazards that are currently existing is brought into focus by this. Informed decision making should be founded on an understanding of the actual risks and problems offered by cyberspace, and any plans or policies that are produced should use knowledge of the dangers, difficulties, and challenges posed by cyberspace as their foundation.

REFERENCES

[1] New Generation of angry & Youthful hackers join the hacktivism wave, adding to cyber-security woes. Available at https://economictimes.indiatimes.com/magazines/panache/new-generation-of-angryyouthful-hackers-join-the-hacktivism-wave-adding-to-cyber-security-woes/articleshow/81707844.cms. Last assessed on 30 March, 2021.

[2] Justice K.S.Puttaswamy(Retd) vs Union Of India And Ors. on 24 August, 2017.Available at https://indiankanoon.org/doc/91938676/. Last assessed on 30 March, 2021

[3] Report on Cyber Security & Right to Privacy submitted by the Parliamentary Standing Committee on Information Technology Act presented on Feb 12th 2014, under the chairmanship of Rao Inderjit Singh to the fifteenth of the Lok Sabha.

[4] The categories of the crimes have been adapted from the article found in https://www.lawctopus.com/academike/cyber-crimes-other-liabilities/ Last assessed on 30 March, 2021

[5] Cyber space available at: https://www.britannica.com/topic/cyberspace. Last assessed on 28 March, 2021

[6] Barkha, Rama Mohan, U. (2011) Cyber Law and Crimes, IT Act 2000 & Computer Crime analysis. (3rd ed.), ISBN: 978-93-81113-23-3.

[7] India: Key Features Of The Personal Data Protection Bill, 2019 available at https://www.mondaq.com/india/data-protection/904330/key-features-of-the-personal-data-protectionbill-2019. Last assessed on 28 March, 2021

[8] Examining the importance of Stenography information technology essay. Available at https://www.ukessays.com/essays/information-technology/examining-the-importance-of-steganographyinformation-technology-essay.php. Last assessed on 28 March, 2021

[9] Introduction to Cyber Crime, Available at: http://cybercrime.planetindia.net/cybercrime_cell.htm. Last assessed on 28 March, 2021.

[10] F. Hohaji, "providing a framework of security for services in next generation networks," the Third National Conference on Information and Communication Technology, Tehran, 2008.

[11] Vizandan, A. Mir Ghadri, J. Sheykh Zadegan, "passive defense in infrastructure communications networks with an emphasis on the security assessment of flow encryption algorithms," Journal of passive defense, pp. 47-52, summer and fall of 2011.

[12] M. Azar Poor, A. Dahar, M. Jahani Mir, “the assessment of computer network security by Honey Pot technique in IDS & IPS systems”," journal of information technology era, pp. 78-84, 2012.

[13] F. Gholi Poor, N. Modiri, M. Riahi Kashani, Providing a process for testing the security of webbased intranet applications," the National Conference on Advances in science, engineering and basic electronics, Tehran, 2014.

[14] Sayana, "Approach to Auditing Network Security," INFORMATION SYSTEMS CONTROL JOURNAL, 2003.

[15] S. Alabady, "Design and Implementation of a Network Security Model for Cooperative Network," International Arab Journal of e-Technology, pp. 26- 36, 2009

[16] B. Daya, "Network Security: History, Importance, and Future," University of Florida Department of Electrical and Computer Engineering, 2010.

[17] S. Farahmand, "IT security and computer networks," Processor Monthly, pp. 32-36, 2010.

[18] N. Mashayekhi, M. Ashoorian, M. Riahi Nasab, “Providing the security matrix as a layer in NGN networks" the Third National Conference on Information and Communication Technology, Tehran, 2008.

[19] M. Azar Poor, A. Dahar, M. Jahani Mir, “the assessment of computer network security by Honey Pot technique in IDS & IPS systems”," journal of information technology era, pp. 78-84, 2012.