Research Article **ISSN: 2393 – 9532**

International Journal of Arts and Science Research

Journal home page: www.ijasrjournal.com

AN ANALYSIS OF CYBER CRIME AND INTERNET SECURITY

V. Shoba*[1]

[1*]Department of Computer Science, SRM Arts and Science College, Kattankulathur, Kancheepuram, Tamil Nadu, India.

ABSTRACT

This study is to be review the issues involved of internet security and cyber crime. Apparently this possessed a paradox since the technological advances made in both of software and hardware to increased internet security measures are also available to cyber criminals who immediately use of them to counteract these measures of cyber crime. Cyber crimes have progressed into serious threat and proper legislation and prosecution is badly needed to combat them. Cyber crime legislation are always lagging behind those fast-growing technological advances which are used by the criminals as well as those who wish to combat them. There is also a needed to consider the competing interested between individual rights of privacy and free speech, and the integrity of both public and private networks system.

KEYWORDS

Cyber crime, Internet security, Technology, Network, Software and Hardware.

Author for Correspondence:

Shoba V,

Department of Computer Science,

SRM Arts and Science College,

Kattankulathur, Kancheepuram, Tamil Nadu, India.

Email: sho13velfam@gmail.com

INTRODUCTION

Cyber crimes is crime that progressed into a serious threat and proper legislation and prosecution are badly needed to combat them. Cyber crime legislation is always lagged behind the fast-growing to technological advances which are used by the criminals as well as those who wish to combat of them. There is also a needed to consider the competing interests between individual rights to privacy and free specking, and the integrity of public and private networks systems. The potential threats to cyber crime, their socioeconomic costs have become as a large that demand and special attention to both legislative aspects of cyber crimes and

technical aspects of data security systems. A best approach to the issue of cyber crimes is the analysis of the types of cyber crimes, the legislative aspects of fighting such crimes, and the technological improvements required in the field of data security to hinder these crimes.

CYBER CRIMES AND CYBER ATTACKS

Any use of a computer and the internet to the some act that would be considered a crime is called a cyber crime since of crime is usually defined in terms of the end result. There are many types of cyber crimes including hacking, cracking, extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage. He term 'hacker' usually refers to a computer user who wants to gain unauthorized access to the computer system while the term of 'cracker' is used to the refer to a hacker with criminal intentions. Software to detect cyber attacks has been developed as cyber threats have evolved. Sophisticated anti-spyware and anti-virus solutions capable of detecting very complex viruses have been developed as security tools and are easily available over the internet. These programs automatically scan for computer security weaknesses and quickly probea computer network, an entire network for hundreds of weaknesses. However, some of these tools may be used by attackers (a person). Moreover, there are some readily available programs of the internet whose only function is to attack computer network. Computer users should be cautious of potential vulnerabilities in their computer system due to the availability of potentially malicious security tools and high-quality attack ware.

CYBER WARFARE

Cyber warfare includes cyber espionage, web vandalism, political propaganda Distributed denial of service, equipment disruption, cyber attack on critical infrastructures such as power, water, fuel, communications, etc. Cyber warfare is another instance of the cyber crimes committed by one of the country against another. The recent cyber attacks in the Middle East and particularly Estonia as a result of which the country was almost brought to a standstill were presented. Information Technology security specialists worldwide were called in for help and on adhoc digital rescue team was formed. After a few days, frontline defences were set up which mainly involved implementing BCP 38 network ingress filtering techniques across affected routers to prevent source address spoofing of internet traffic. In the days it took to fight off the attack, Estonia lost billions of Euros in reduced productivity and business downtime.

LEGISLATION AGAINST CYBER CRIME

The main question to be addresses regarding legislation against cyber crime is whether or not Existing penal law are adequate to deal with cybercriminals. Existing legislation regarding cybercrimes are different in various parts of the world. New laws and technology are needed to effectively combat cyber crimes. Existing legal framework for fighting cyber crimes is insufficient in many countries including Chinna and etc that has the most numbers of computer internet users in the world. The Computer Fraud and Abuse Act (1984) (CFAA) deals with a compelling federal interest, where computers of the federal government or certain financial institutions are involving, the crimes itself are interstates in the nature, or computers are used in interstate and foreign trade and commerce.

INTERNET SECURITY

The World Wide Web is constructed from programs called Web servers that make information available in the network system. Web browsers can be used to access the information that is stored in the servers to display it on the user's screen. Another use of the Web involves putting programs created with aprotocol called the Common Gateway Interface(CGI) and behind Web pages, such as a counter which increments every time of user’s looks at that time of pages or aguest books to let users sign in to a site.

DETECTION SYSTEMS

Intrusion detection was a first studied by an analysis of computer system audit Data. Intrusion detection systems (IDS) are that software and or hard ware

solutions meant to detect unwanted attempts at accessing, manipulating or disabling computer systems through networks. An Intrusion detection system (IDS) consists of several components including sensor to generate security events, a console to control of the sensors and monitor events and alerts. The IDS uses a system of rules to generate alerts from the security events received.

CYBER SYSTEMS SECURITY STANDARD

There is a growing need for information assurance and security since a sensitive information is an often stored in the computers that are attached to the internet. In addition to critical infrastructures, personal identity, important fiscal information, trade a secrets, proprietary information and the customers 'information must also be a safeguarded against as possible cyber attacks. Cyber security standards are developed to provide security techniques in order to minimize the number of successful cyber attacks and provide guidelines for the implementation of cyber security.

NETWORK FORENSICS

Digital and network systems deals with the discovering and retrieval of information about computer or cyber crimes to provide court-admissible digital evidence. The problem of network forensics is the huge network traffic that might crash the system if the traffic capture system is left unattended. Kim *et al.* Proposed afuzzy logic based expert system for network forensics to analyzed computer crimes in network environments and automatically provide digital evidence.

CONCLUSION

The paradox of internet security and cyber crime of due to the fact that both the researchers in the area of internet cyber crime security. Cyber security standards are developed to provide security techniques in order to minimize the number of successful cyber attacks and provide guidelines for the implementation of cyber security.

ACKNOWLEDGEMENT

The authors wish to express their sincere gratitude to Department of Computer Science, SRM Arts and Science College, Kattankulathur, Kancheepuram, Tamilnadu, India for providing necessary facilities to carry out this research work.

CONFLICT OF INTEREST

We declare that we have no conflict of interest.

BIBLIOGRAPHY

1. Ali Peiravi, Mehdi Peiravi. Internet security - cyber crime Paradox, *Marsland Press Journal of American Science,* 6(1), 2010, 15-24.
2. Aaron G, Bostik K A, Chung E, Rusmussen R. "Protecting the web: Phishing, malware, and other security, threats", Proceeding of the 17th International Conference on World Wide Web 2008, WWW'08, 2008, 1253-1254.
3. Ben-Itzhak Y. "Organised cybercrime and payment cards", *Card Technology Today,* 21(2), 2009, 10-11.
4. Bhatia J S, Sehgal R, Bhushan B, Kaur H. "Multilayer cyber attack detection through honeynet", Proceedings of New Technologies, *Mobility and Security Conference and Workshops, NTMS*, 2008.
5. Blakeley C J. "Cybercrime law: international best practices", *Doha information Security Conference, Doha, Qatar,* 2008, 10-11.
6. Dwyer D. "Chinese cyber-attack tools continue to evolve", *Network Security,* 2009(4), 2009, 9-11.
7. Gilman N. "Hacking goes pro", *Engineering and Technology,* 4(3), 2009, 26-29.

Please cite this article in press as: Shoba V. An analysis of cyber crime and internet security, *International Journal of Arts and Science Research,* 4(1), 2017, 38-40.