International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 770-772 Jan 2019-June 2019 www.csjournals.com

A Review on Cyber Crime Prevention Using Steganography

[1]Lajja, [2]Priyanka
[1]Research Scholar, [2]Asst. Professor
Deptt. Of computer science and application, Chaudhary Ranbir Singh University, Jind, Haryana, India

Abstract: This paper is describing the cyber crime with its type. Cyber Crime is a different type of the crimes that are performed with the use of internet. Such crimes involve a plethora of criminal actions. Cyber crime has been referred as an umbrella. Under this umbrella several illegal activities are performed. Nowadays, several disturbing actions are performed in cyberspace due to anonymous nature of the Internet. Several users of Internet are grossly misusing this feature of the Internet. Along with the positive uses of internet, there is the misuse of internet to perform the criminal activities in cyberspace. This paper also provides a review of several existing researches in the field of cyber crime. Cryptography with Steganography is used to stop the cyber crime.
Keyword: Cyber crime, Steganography, Cryptography, Virus, Cyber Stalking, Spoofing, Phishing, Cyber Terrorism, Spamming, Hacking, fraud, Offences, Visual cryptography.

[1]Introduction: The Cyber Crime is a type of crime. In cyber crime the digital technologies are used to commit the crime. These illegal activities includes the activities like attacking on Data System, theft of goods online etc. the child pornography, create graphics, online fraud dealing. There are also deployments in internet illegal activities. Illegal activities may be virus, worm, and any third person mistreatment as phishing and email scams etc. For this purpose the firewall, virtual private networks and encryption algorithms are used. In this method of security, the virtual private network has an essential to stop the crackers from entering in networks. VPN offers the end users a way to personally get the information on the network.

Cyber crime: The advancement in technology always brought with it increasing criminal activities and increasing opportunities for committing crime and internet is not exception to this there is no doubt that computer technology has opened the door to preparation of crime in the fields of cyber. The effect of such crimes is so serious that it poses a great threat to public as well as personals.
Cyber: Cyber is just prefix used or compute work "as in cyberspace, the electronic medium in which online communication takes place. Cyber is just like an umbrella under which misleads are performed. While the technology to operate and protect these networks is expensive but the means and mode required to attack them are relatively inexpensive one with destructive mind should have computer.
Crimes: Crime means some activity which is not under parliament acts made for social welfare.

Reasons of Crimes: Computer systems are very soft to crimes because of open data available via some communication i.e. network. One gets connected to other resource easily and due to advancement in it system are easily accessed (gaining of any device, data)
Computer Crimes: Computer crimes are usually indulged in by students, computer programmers, some destructive mind, some business rivals, these persons gets motivation by advancement in tools and techniques some of the criminal behavior observes that people enjoy braking of codes and key used for security purpose.

[2] Type of Cyber Crime: - a lot of varieties of crimes are there. There are several *actions* determined to be cyber offence globally.

(a) Unauthorized Access: In this type of crime, a person attempts to access a secured and protected system. This crime has been completed when one get success to access a computer, computer system or computer network having not authorization of the owner.

(b)Intellectual Property Crime: Other kind of cyber offence is the crimes which are against of intellectual property of someone.

(c)Virus: In the situation in which a person causes some issues on the system of someone without his permission. The virus in a system corrupts the system and induced some issues to operate the system. There are several kinds of viruses according to its use.
(d) Child Pornography and Luring: Pedophiles apply the Internet to share the not legal picture of small children. Newsgroups as well as the chat rooms are used to provide the meeting places of such entice children. The people that are suffered from Pedophiles get victims with security of their houses.
(e) Cyber Stalking/ Harassment: Several people are there who talk to each other via chat rooms, forums, newsgroups etc. Virtual connections provide them the feeling of relationship to each other. But such are not met physically.
(f) Identity Theft: Several criminals are there. The mimic sites are made by these criminals. Using such sites they get the payment made by the user of lure sites. Such sites have been made designed to unfairly theft the personal, financial information of user of lure sites.
(g)Spoofing and Phishing: Spoofing or Phishing is the action that has been made to construct a mimic site. Spoofing that is a technique applied to obtain the not legal access of systems.
(h)Dissemination of Offensive Materials: A large quantity of content is there on the Internet. Such content may be the objected by someone. Such content includes the sexually explicit materials, racist propaganda etc.
(h)Cyber Terrorism: Terrorists have been known as skilful user of internet. Such user gets and provides the online marketing etc. several examples is there which show how the terrorists apply the internet and its several feature. This new medium has been user to share the threats. It also has been used to disseminate terrible graphic.
(j)Spamming: Spam is the spontaneous email. Mostly the commercial sites make the advertisement of their product or service. Such sites send the mail to thousands of email addresses at a time. In this way the people's Inboxes filled with such messages. Generally the spam is a source of scams. Here are the chances of viruses as well as offensive content.
(k)Hacking: Hackers take theadvantage of technology according to the requirement. A lot of kind of hackers is there in cyber space.
(l)Fraud: Several kind of fraud is there made with the use of the Internet. Financial scams as well as get rich quick schemes are provided a new lease on Internet.
(m)Offences: There is a growing threat of attacks on computer systems via telecommunication networks, theft or telecommunication services and the user of computer to commit fraud and crimes of data manipulation.

[3]LITERATURE REVIEW
There have been several researches in field of cyber security. Several techniques are used to overcome the cyber crimes. Some of these researches considered IP spoofing, while other discussed threats in peer to peer networks. Lot of researchers have discussed cyber threat to Network security. Research has discussed security technology to handle DDOS attack, IP spoofing. Several researches have proposed encryption mechanism to provide security to information transferred over network. Here in this section the several existing researches made by different authors have been discussed.

In 2013, Abhishek Kumar Bharti [1] introduced detection of Session Hijacking and IP Spoofing Using Sensor Nodes and Cryptography.
In 2014, Hani Alshamrani [2] wrote research on Internet Protocol Security (IPsec) Mechanisms.
In 2011, ChanderDiwakar [3] et al. discussed security threats in peer to peer networks.
In 2014, HaroonShakiratOluwatosin [4] did research on Client-Server Model.
In 2014, Ms. Jasmin Bhambure[5] et al. proposed Secure Authentication Protocol in Client – Server Application using Visual Cryptography.
In 2015, Mohan V. Pawar [6] et al. discussed Security of network and Types of Attacks in Network
In 2015, Manjiri N. Muley [7] did study for analysis for exploring the scope of network security techniques in different era.
In 2013, Rupam [8] et al. introduced approach to detect packets using packet sniffing.
In 2013, Sharmin Rashid[9].et al proposed Methods of IP Spoofing Detection & Prevention.
In 2013, MukeshBarapatre [10] et al. made a review on Spoofing Attack Detection in Wireless Adhoc Network.
In 2014, Amandeep Kaur [11] et al. did a review on Security Attacks in Mobile Ad-hoc Networks.
In 2014, Md. Waliullah [12] et al. wrote a research on Wireless LAN Security Threats & Vulnerabilities.
In 2014, P. Kiruthika Devi [13] et al did research on spoofing attack detection & localization in wireless sensor network.
In 2014, BarleenShinh [14], did a review on Collaborative Black Hole Attack in MANET.
In 2014, Ms. VidyaVijayan [15] did review on Password Cracking Strategies.

[4] OBJECTIVES

- To identify the problems and challenges in cyber sector due to crime.
- To identify the trends of crime in cyber sector.
- Highlight present state of response to cyber offence in India;
- Highlight the level of main concern cyber crime for law enforcement association.
- To know the effectiveness of law regarding cyber crime.
- Set the recommendations for additional knowledge and feasible enhancement in state of give the answer to cyber crime in India.

[5]PROBLEM STATEMENT

Present issues &technical challenges for investigation and prevention of cyber crime in India.
There are different type of hacker and crackers who are responsible for cyber crime. A black hat may be any person who is capable to access the computer system. He accesses the system having not authority to the owner of system. Especially it has been done by malicious intention. These activities may be legal or illegal according to the laws of a country. Generally is called software cracking. A Grey Hat is skilled hacker. Sometimes he plays his role legally. But in few situations he also acts illegally. A Grey Hat hacker is the amalgam of white with black hat hacker. Usually they don't attack for personal achievement. The Internet crime hackers perform the crime on the platform of internet. It also involves the kidnapping children, scams, cyber terrorism also commit by the internet. These offences are committed by computer.

[6] Future scope: The research work would stop the illegal actions. At the time of data sharing, there are the chances of attacks but the proposed work is capable to offer the best security. It is efficient to secure data in the case of RSA attack. The chances of Brute force attack are there if the RSA is applied. But the proposed work is also beneficial to limit the attacks in the case of Brute force attack as well as timing attack.

References

[1] Abhishek Kumar Bharti, "Detection of Session Hijacking and IP Spoofing Using Sensor Nodes and Cryptography"IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661, p-ISSN: 2278-8727 volume 13, Issue 2 (Jul. -Aug. 2013), PP 66-73
[2].Hani Alshamrani, "Internet Protocol Security (IPSec) Mechanisms", International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014, pp. 85-87.
[3].ChanderDiwakar, Sandeep Kumar, Amit Chaudhary, "SECURITY THREATS IN PEER TO PEER NETWORKS", Journal of Global Research in Computer Science, Volume 2, No. 4, April 2011, pp. 81-84.
[4]. HaroonShakiratOluwatosin, "Client-Server Model", Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 1, Feb. 2014, pp. 67-71.
[5]. Ms. Jasmin Bhambure, Ms. DhanashriChavan, Ms. Pallavi Band, Mrs.LakshmiMadhuri, "Secure Authentication Protocol in Client – Server Application using Visual Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014, pp. 556-560.
[6]. Mohan V. Pawar, Anuradha J, "Security of network and Types of Attacks in Network", International Conference on Intelligent Computing, Communication & Convergence, 2015, pp. 503 – 506.
[7]. MANJIRI N. MULEY, "ANALYSIS FOR EXPLORING THE SCOPE OF NETWORK SECURITY TECHNIQUES IN DIFFERENT ERA: A STUDY", International Journal of Advanced Computational Engineering and Networking, Volume-3, Issue-12, Dec.-2015, pp. 33-36.
[8]. Rupam, AtulVerma, Ankita Singh, "An Approach to Detect Packets Using Packet Sniffing, International Journal of Computer Science & Engineering Survey (IJCSES) ,Vol.4, No.3, June 2013, pp.21-33.
[9]. Sharmin Rashid, SubhraProsun Paul, "Proposed Methods of IP Spoofing Detection & Prevention, International", Journal of Science & Research (IJSR), Volume 2, Issue 8, August 2013, pp.438-444.
[10]. MukeshBarapatre, Prof. Vikrant Chole, Prof. L. Patil, "A Review on Spoofing Attack Detection in Wireless Adhoc Network", International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 6, November – December 2013, pp.192-195.
[11]. Amandeep Kaur, Dr. Amardeep Singh, "A Review on Security Attacks in Mobile Ad-hoc Networks", International Journal of Science & Research, Volume 3 Issue 5, May 2014, pp.1295-1299.
[12]. Md. Waliullah, Diane Gan, "Wireless LAN Security Threats & Vulnerabilities", International Journal of Advanced Computer Science & Applications, Vol. 5, No. 1, 2014, pp.176-183.
[13]. P. Kiruthika Devi, Dr. R. Manavalan "Spoofing attack detection & localization in wireless sensor network", International Journal of Computer Science & Engineering Technology, Vol. 5, No. 09, Sep 2014, pp.877-886.
[14]. BarleenShinh, Manwinder Singh, "A Review Paper on Collaborative Black Hole Attack in MANET", International Journal of Engineering & Computer Science, Volume 3, Issue 12, December 2014, pp. 9547-9551.
[15]. Ms. VidyaVijayan, Ms. Josna P Joy, Mrs. Suchithra M S, "A Review on Password Cracking Strategies", international Journal of Research in Computer & Communication Technology, 2014, pp.8-15.