A REVIEW ON USE OF STEGANOGRAPHY FOR CYBER CRIME PREVENTION

Shivneet Singh

Email id :- redhu.shivneet3@gmail.com

Abstract: The many forms of cybercrime are categorized here. Internet-based criminal activity, or "cyber crime," is distinct from traditional crime. This kind of crime encompasses a wide range of illegal conduct. The term "cyber crime" has been used to describe a broad category of illegal activity. Several unethical pursuits are carried out under this guise. The anonymity of the Internet has led to some terrible acts being committed in cyberspace recently. Many online users are abusing this service in egregious ways. While the internet has many beneficial applications, it may also be used for illegal purposes. In addition, this study summarizes various previous studies on the topic of cybercrime. Steganography and other forms of cryptography are employed to combat online criminal activity.

Keyword: Cyber crime, Steganography, Cryptography, Virus, Cyber Stalking, Spoofing, Phishing, Cyber Terrorism, Spamming, Hacking, fraud, Offences, Visual cryptography

[1]Introduction: A new category of criminal activity has emerged in recent years: cybercrime. In the realm of cybercrime, electronic means of communication are used. Child pornography, graphic design, and online fraud transactions are all part of this category of illicit behavior, as are attacks on data systems and theft of products over the internet. Deployments may also be seen in cybercrime. Viruses, worms, and any kind of abuse of a third party, such as phishing and email scams, are all illegal practices. The deployment of a firewall, VPN, and encryption techniques all serve this goal. The VPN plays a crucial role in this security strategy by obstructing would-be hackers. Users may have direct access to network resources using VPN.

Cyber crime: There is no question that computer technology has opened the door to the preparation of crime in the realms of cyber, as the development of technology has always been accompanied by an increase in criminal activities and an increase in opportunity to conduct crime. Such acts have far-reaching consequences that endanger both the general populace and individual victims.

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: Open data accessible through some connection i.e. network makes computer systems very vulnerable to crimes. Due to technological advancements, connections can be made quickly and resources may be accessed with ease (gaining of any device, data)

Computer Crimes:. Students, computer programmers, people with destructive minds, and even business rivals often commit computer crimes; they are inspired to do so by the development of new technologies and methods, and researchers have found that some criminals even take pleasure in cracking the codes and keys used for security.

[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: A hacker is someone who tries to break into a protected and locked system. When someone gains access to a computer, computer system, or computer network without the owner's permission, they have committed this offense.

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

(c)Virus: Any time an unauthorized user creates problems on another's computer. When a virus is present, the system becomes corrupted, and it becomes difficult to run the system normally. Viruses may be broken down into a number of categories depending on their intended function.

(d) Child Pornography and Luring:.
Internet is used by pedophiles to distribute illicit images of youngsters. These young people find one other in online communities like newsgroups and chat rooms. People who are abused by pedophiles often become victims because of a lack of home security.

(e) Cyber Stalking/ Harassment: There are many individuals there who interact with one another in various online communities, such as message boards and online bulletin boards. These online interactions allow individuals to feel like they belong to a community. However, this is not achieved in reality.

(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: What has been done is called "spoofing," "phishing," or "mimicking," and it is used to create fake websites that seem like the real thing. To gain unauthorized access to a computer system, spoofing is a method that may be used.

(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:. It's common knowledge that terrorists are adept computer users. A user like that receives and gives out internet marketing materials, etc. There are several instances of the ways in which terrorists use the Internet and its many features. In order to disseminate the dangers, people have resorted to using this new form of communication. However, it has also been used to spread really disturbing visual

(j)Spamming:. Unsolicited email is known as spam. The majority of online advertisements are found on commercial websites. This kind of website mass-mails to thousands of email addresses simultaneously. As a result, such texts flooded people's inboxes. Usually, scammers use spam as a distribution channel. Possible malicious software and inappropriate material are listed below.

(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

Several studies have been conducted on the topic of cyber security. In order to combat cybercrime, many methods have been developed. IP spoofing was a topic explored in some of these studies, while others focused on P2P network security. Many scholars have analyzed the cyber danger to Network safety. Security technology to counter distributed denial of service (DDoS) attacks and IP spoofing has been the subject of academic discussion. Several studies have suggested encryption mechanisms to safeguard data during

network transmission. Multiple studies by many authors are mentioned here.

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

Cybercrime investigation and prevention in India at the present time: problems and technological hurdles.

Cybercriminals, often known as hackers or crackers, come in many forms. Anyone with the ability to breach a system might be considered a black hat. He accessed it without the owner's permission. Especially if it was done on purpose to do harm. Depending on local regulations, such actions might be prohibited. software cracking is a common term for this practice. A Grey Hat is a hacking expert. On occasion, he even acts within the law. However, there are a few instances when he engages in criminal behavior. As a compromise between white and black hat hackers, "Grey Hat" hackers have characteristics of both. They seldom launch attacks for the sake of glory. Cybercriminals, often known as hackers, commit crimes using the Internet. Kidnapping minors, fraud, and cyberterrorism are all part of this. Criminals use computers to carry out these acts..

[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.