Volume 6, Issue 4, April 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Cyber Crime and Security

Soumya Tiwari*, Anshika Bhalla, Ritu Rawat
CSE, Graphic Era University, Dehradun,
Uttarakhand, India

Abstract— Cybercrime is inescapable, ubiquitous and increasingly linked with different parts and areas of criminal environs. This evolution and network gave rise to cyber space which controls and manages to provide equal opportunities and facilities to all the people to access any kind of information. Due to gradually increase of the internet users and netizens, abusage of technology is broadening gradually which tends to cyber crimes. Cyber crime is basically an unlawful act that leads to criminal activity. Cyber Security, a mechanism by which computer information and the equipments are protected from unauthorized and illegal access. This paper illustrates and focuses on cybercrime, its impact on society, types of threats, and cyber security. Nowadays Computer crime issues and thefts have become tremendously high-profile, particularly those surrounding copyright infringement, hacking, child pornography, child grooming, and spoofing.

Keywords— Cybercrime, Cyber security, Hackers, Fraud, Privacy.

I. INTRODUCTION

Computer fraud can be a untrustworthy misrepresentation of the fact proposed to prompt another to abstain from doing something that causes loss. Computer crime can be summarized as a criminal activity which involves information technology infrastructure, in addition to unauthorized access, illegal interception, any data interference, computer or systems interference, abusage of devices, forgery, blackmail, embezzlement, and some electronic fraud. There exits privacy issues whenever any confidential information or data is hijack or lost, either lawfully or otherwise. The very first crime that was recorded, took place in 1820 in France, Joseph-Marie Jack quad, a textile manufacturer, produced a device namely loom which allowed the continuous repetition of series of steps involved in the weaving of some special fabrics. This leads to a kind of fear in employee's minds and they committed sabotage. Cyber crime cells are there in states basically to handle these crimes, and to expel or punish the netizens or criminals committing any of the cyber crime[1]. It basically ranges from theft of an individual's identity entire disruption of a particular country's Internet and network connectivity due to massive attacks across its networking resources. In this digital age, online communication now become a norm, the internet users and the government are at a enlarged risk of becoming the bull's-eye of the cyber attacks. Cyber crime can cause harm to any organisation.

To fight the fast-spreading cybercrime, governments and businesses must have collaboration globally basically to develop any impressive model that somehow controls the threat. The internet is basically used for the betterment of life, to make people aware of world-wide activities, enhances the speed of life as well and makes users technically strong and up-to-the-mark. As the use of technology is increasing day-by-day, the crime is also increasing gradually. It covers all the forms of crimes and thefts related to computer networks. Some of the criminals are technically expert and educated having deeper and remarkable knowledge regarding the technology. Hacking of the ATM password, transferring the money by hacking the bank account details of the victim's account to theirs, some pornography issues etc are some of the thefts that are handled by educated people [2]. There is an urge to implement some of the rules and regulations, to tackle and handle these crimes governing cyber space particularly known as Cyber Law.

Cyber security requires global co-operation to deal with the security of cyber space [3]. It protects computer equipments, resources of computer or system, information and data from any unauthorized access and the disclosure [1]. During this paper different kinds of attacks and threats are overviewed. Each and every attack is described firmly, category of hackers are also reviewed. In section II, cyber crime is detailed along with its two classifications of forms of crimes. In section III different types of attacks are briefly overviewed. In the next section, section IV, category of hackers is acknowledged. Then cyber crime's impact is detailed in section V. Last section, that is section VI, there is a short overview of cyber security is organised.

II. CYBERCRIME

Computer crime, cybercrime, electronic crime or hi-tech crime basically a criminal activity where a network or computer is the target, source, or place of the crime [1],[5],[9]. Network crime encloses a wide range of illegally potential active activities. Whenever a person tries to steal information, or cause damage to computer network, this is assumed to be entirely virtual in which the particular information exists in digital form but the damage caused is real, which ceases the machine and has no physical consequence. A computer may act as a source of evidence, even though not directly or completely used for the criminal purposes, it acts as an excellent device for keeping the record and has given the in charge to encrypt data[5]. If the evidences are obtained and decrypted, it will be assumed to have a greater value to the criminal investigators. Generally, it is classified into two forms of categories:

(1) Crimes targeting computer devices or network directly.

Examples of crimes targeting computer devices or network directly would include,

[1] Malicious and Malware code
[2] Denial-of-service
[3] Computing viruses

(2) Prime target is independent of device or computer network.

Examples of crimes whose prime target is independent of device or computer network would include,

- Cyber stalking
- Fraud and identity theft
- Phishing scams
- Information warfare

III. THREATS TO BE AWARE OF

A. Botnets

Botnets are defined as a set of compromised systems ("zombies" or "bots") under the particular unified command along with the control of the “bot-master” commands are sent through a command and a control channel to bots. Botnets are largely undetected. Botnet is basically a network of malicious computers or systems (bots, known as zombies or drones) under the control of central controller through the commands and the control servers[4]. The goal is to make use of the infected or malicious computers for criminal activities such as attacking a network, or generating spam. Botnets are considered as the most hilarious form of network-based attack as they make use of large, and coordinated group of hosts basically for both subtle attack and brute-force.

A. It may send any spam email having viruses attached.
B. Spread malware.
C. It may your system as a part of denial of service attack across other systems.

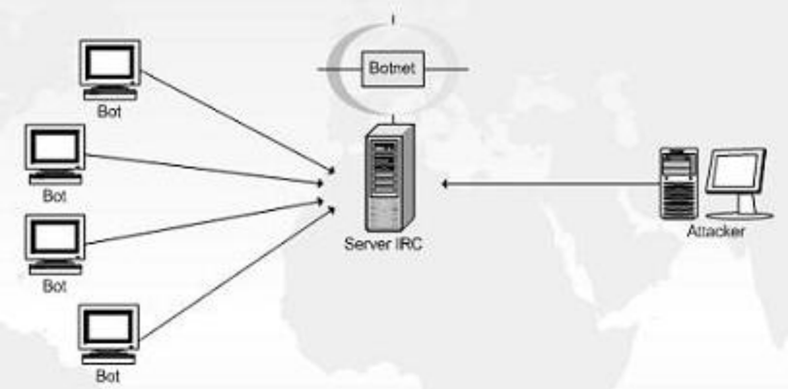

Fig. 1 A sample structure of botnets

B. Denial-of-service

It is an act in which criminal sends numerous spam mails to the victim's mail box depriving him/her of the entitled services to be provided. It is particularly an attempt to make the resources unavailable to users. Denial of Service (DoS) is basically produced by unintentional failure of nodes[10]. This attack is a pervasive threat. The DoS attack attempts to exhausts the available resources by sending unnecessary packets to victim node. An attacker may take control of a system by taking the advantage of security weaknesses or vulnerabilities [6],[8]. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses.

We can follow these steps to reduce the possibilities that an attacker can make use of your system to attack other system:

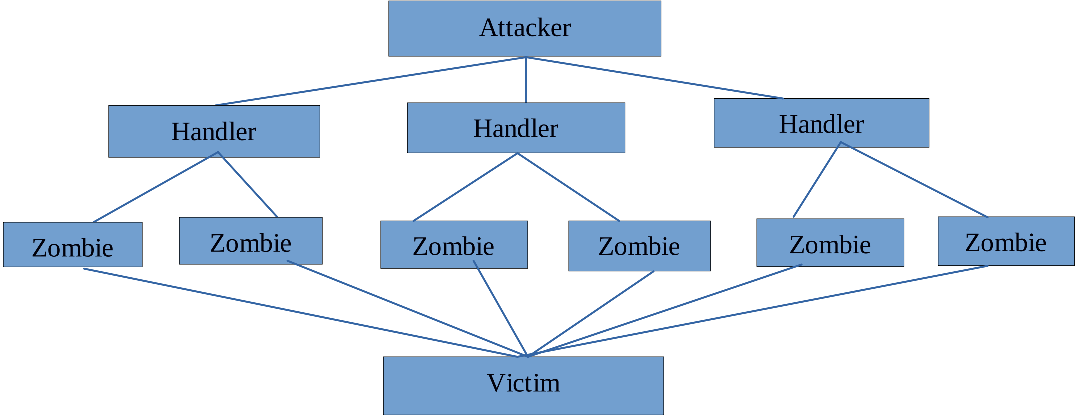

Fig. 2 A Denial of Service attack functioning

1) Install anti-virus software.
2) Install a firewall to configure it and restrict traffic.
3) Follow remarkable security practices by applying email filters to manage unwanted emails.
4) Do not open email attachments, if they are from unknown people.

C. Malware

Malware is the most common way to infiltrate or harm your computer. The term malware is nothing more than "malicious software". Different malwares are Trojan, key loggers, spyware.

1) Alter files or delete them.
2) Intimidate you with scare ware.
3) Reformat hard drive causing you to lose all the useful information.
4) Steal some sensitive information.
5) Send emails using your identity.
6) Take charge of your system.

D. Hacking

Hacking is a term used to describe actions taken by someone to gain unauthorized access to a computer. The availability of information online on the tools, techniques, and malware makes it easier for even non-technical people to undertake malicious activities. The process by which cyber criminals gain access to your computer. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location [10]. This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed.

- Find weaknesses (or pre-existing bugs) in your security settings and exploit them in order to access your information.
- Install a Trojan horse, providing a back door for hackers to enter and search for your information.

E. Phishing

Phishing is a crime mostly used by the criminals because it is one of the easiest ways to execute and it can produce the outcomes or results they're looking for with less effort. Websites, text messages, and fake emails are created to look as if they are from some authentic companies. Basically these are sent by some criminals to steal and acquire some personal and the financial information from you. This may also known as "Spoofing"[11]. Phishing is used by the strangers to "fish" or steal for information about you basically those that you would not disclose to a stranger, like your bank details, PIN, and some other personal details. What it does:

- Trick you into giving them information by asking you to update, validate or confirm your account. It is often presented in a manner than seems official and intimidating, to encourage you to take action.
- Provides cyber criminals with your username and passwords so that they can access your accounts (your online bank account, shopping accounts, etc.) and steal your credit card numbers.

F. Spam

Spam is the method of both sending the information out and then collecting it from any unsuspecting people. Spam, an unlawful act or unsolicited sending of numerous amount of or bulk email for commercial purposes. What it is:

- The huge distribution of some unsolicited messages, pornography or advertising to addresses that are easily available and found on Internet through things example social networking sites, personal blogs, and company websites.

What it can do:

- Unwanted junk mails annoy you.
- Phish for your data and information by tricking into some links or having details with soe very good and true offers and the promotions.
- Provide a vehicle for scams, malware, and fraud and threats to the privacy.

G. Sybil

Sybil attack can be defined as some malicious device illegitimately taking on some multiple identities. In Sybil attack, an malicious appears to be in multiple places at the same time. A single node may present few multiple identities to some nodes in sensor network either by stealing or fabricating the identities of the legitimate nodes. Figure 1 illustrates Sybil attack: in which an adversary node "AD" is present with multiple identities as well [13]. "AD" appears as node 'F' for node 'A', node 'C' for node 'B' and node 'A' as to node 'D' so whenever node 'A' wants and tries to communicate with the node 'F' and then it sends the message to node "AD". Sybil attack is somehow a very harmful threat and hazardous to the sensor networks. It has an significant threat to some geographic routing protocols. This attack can disrupt the normal functioning of sensor network, like multipath routing. It basically reduces the effectiveness of some fault tolerant schemes such as dispersity, multipath, and distributed storage. Basically, any peer-to-peer network is vulnerable to this attack.

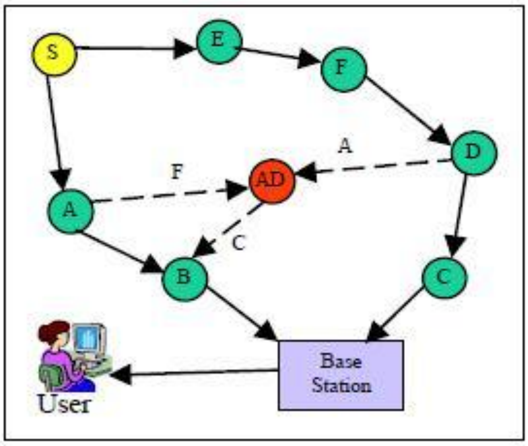

Fig. 3 A sybil attack

H. Wormhole

Wormhole is basically a critical attack in which hacker or attacker records the bits or packets at a particular one location in the network and tunnels them to another one(location). In this attack, the malicious nodes eavesdrop packets and may tunnel the messages that are received in one area of network over some low latency link and finally retransmits them in some other part[1],[7],[14]. This may generate a false scenario representing the original sender in the neighbourhood of remote location. Basically tunnelling procedure outlines the wormholes in the sensor network. One can selectively proceed to the scenario of tunneling or retransmitting of bits. Figure 2 demonstrates the wormhole attack in which the malicious node is "WH" which then creates the tunnel in between node 'E' and node 'I' because these two nodes are present at the most distances from each other. The easiest case of warm-hole attack is to basically have a malicious node which forwards the data in between the two legitimate nodes. Warm-hole attack can be launched by both the insiders and the outsiders.

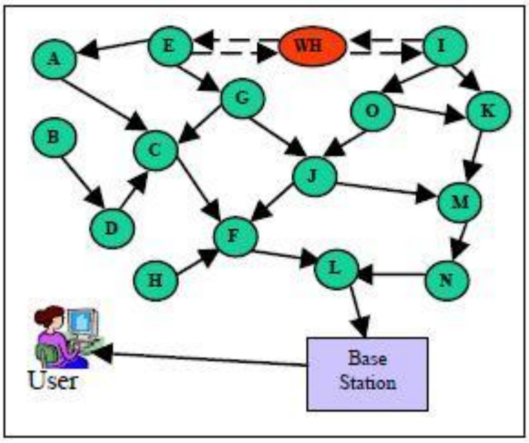

Fig. 4 A warm hole attack

I. Virus

Viruses are the malicious and harmful computer programs that infect your system or may harm your contact list, are sent as an e-mail attachment basically and sometimes by downloading a file may also infect your system. Visiting a site sometimes starts an automatic download of a virus. They can send spam mails, may hijack your browser, sometimes disable the security settings and display unwanted and useful ads [2],[4],[12]. They may also provide access of your system and contact lists to the criminals, and scan the personal information like bank account details, or passwords etc. When any of the programs might run, the viruses attached to that particular program could infiltrate the hard drive of the system and spread to the USB keys and also to the external hard drives. Now any attachment created by you using that particular program and sent to someone else may also infect them. Few things needs to be checked to know whether your system is infected or not:

- It takes more than usual time to launch a particular program.
- Some Files and data get disappeared.
- Your system may crash constantly.

J. Worms

Worms are basically a common form of threats that harms the computer or system or Internet as a whole. Unlike virus, worms directly attacks without any attachment of files, programs, images, text or something and works on its own. It resides in the memory of the system, doesn't cause harm to the hard drive and do not alter as well and propagates itself to other systems in a particular network. It may propagate by sending worm either within the company or to the internet itself. What they may do:

- They spread in your contact list.
- Tremendously causes damage by shutting down the parts of internet, and causes enormous amount of harm to the companies.
- Web pages now loaded slowly.
- Your system's screen looks like distorted.
- Programs run without any of your control.

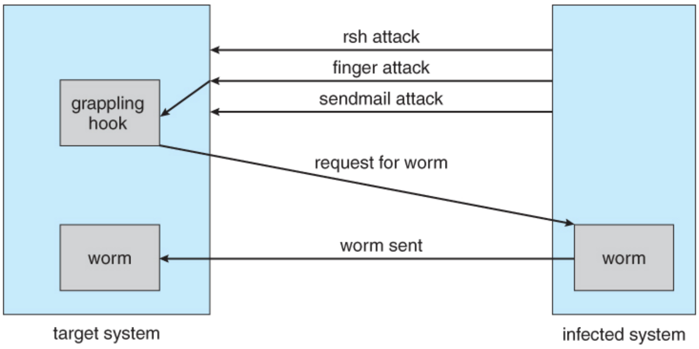

Fig. 5 A worm attack

IV. TYPES OF HACKERS

These criminals or hackers are usually engineers, doctors, MBA students etc all educated people who tries to gain the access of other's system. These are:

A. Script Kiddies

Script kiddies are non-technical expertise and hack the weakly secured systems. They cannot seriously harm the victim.

B. Scammers

Scammers sends the fake mails to the targeted victim like fraud prizes (lottery), discount pharmaceuticals, etc by which they access the victim's system and corrupts it.

C. Hacker Groups

They anonymously work and hacks the system for no criminal reasons. They are basically hired by government agencies, organizations, etc. to examine the security and handle the fraud cases.

D. Phishers

They request the confidential information over the network under false pretences to fraudulently get credit card details, passwords and other personal information. Phishing is carried out by mail spoofing and directs the users to get details at a fraud website that is almost identical to the legitimate one.

E. Political/religious/commercial groups

These types of hackers develop malicious threats or malwares for political concern ends and have no interest in any kind of financial gain. They tries to access the confidential information of the opponent groups.

F. Insiders

These attackers are very dangerous as they reside in the organization only. By residing in the organization they acquire complete knowledge and details of the organization and easily corrupt the system attack and harm the security of the company.

G. Advanced Persistent Threat (APT) Agents

This is responsible for highly targeted attacks which are carried out by well organized and state-sponsored groups. They have higher technical skills and have access to the vast computing resources.

H. White Hat Hackers

They are ethical hackers who basically focus on securing and protecting IT systems. White hat hackers are those who attempts to break into network or system in order to help the holder of the system by making an effort to aware them of the security flaws. Many such kind of people are employed by the companies concerning about the computer security; these are professional sneakers and the collective group of them are often categorised as tiger teams.

I. Black Hat Hackers

An individual who compromises with the security of computer system without any acknowledgement from the authorized party. They uses their knowledge to exploit the systems.

J. Grey Hat Hackers

A Grey Hat Hacker is considered as a skilled hacker in the security community who at times acts legally, and sometimes not. They are considered as hybrid between black and white hat hackers. They basically do not hack with the malicious intentions.

V. IMPACT OF CYBERCRIME

Worms are the most strong form of cyber attack which causes severe disruption. In the month of September, in 2010, Stuxnet infected and affect the unknown number of industrial controls around the whole world, and stealthily give invalid instruction's to the machinery and some false readings to the operators [16]. Potentially, it destroys gas pipelines, causes nuclear plant to malfunction or causes boilers of factory to explode. This worm was known to be active mostly in Iran, on the same Indonesia, Pakistan, India also reported as infections [1].

A. Crime Against People

In this, the criminal provides numerous false promotions and gives the people an illusion of security by forcing them to administer their personal information. It includes child pornography, a dominant offence. Social networking sites and the chat groups can also be concluded as a serious cyber crime at times.

B. Crime Against Property

Criminals can easily with their techniques steal the personal information of the other people computer system and the theft gains the unauthorized access to an internet connection, can be a cyber crime.

C. Crime Against Business

In this crime, criminal basically hacks the system or machine of any business organization; they store and steal the confidential and the sensitive data of the system on the server. They acquire unauthorized access to the secured and confidential data of the company and via this, they transfer fund's of the company to their accounts that makes the organization bankrupt.

D. Crime Against Government

Cyber terrorism is a term used against government crime in which hackers hacks the secured and confidential database of the government with the urge to use sensitive and personal information of the government that reduces the faith of the citizens.

VI. CYBER SECURITY

A branch of technology basically known as cyber security or information security applied to networks and computers, the objective carries protection of data or information and the property from the thefts, natural disaster, or corruption, and allowing the property and information to remain productive and accessible to its users[1],[8],[15]. The Cyber security implies to the processes and the technologies which are designed to protect networks, computers and the data from the unauthorized access, attacks, and vulnerabilities delivered via the Internet by cyber criminals.

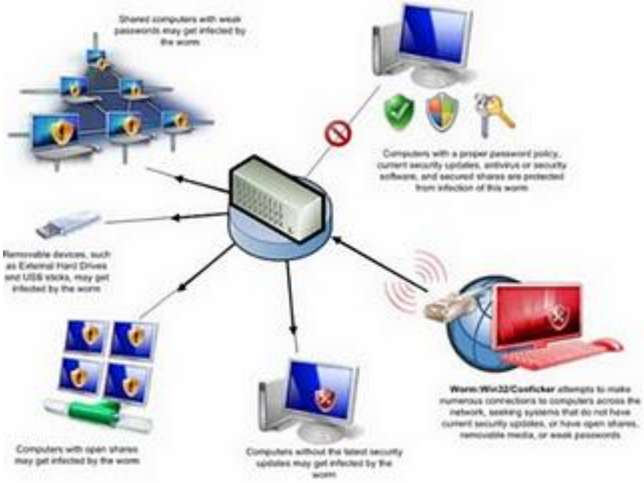
Shared computers with weak passwords may get infected by the worm
Computers with a proper password policy, current security updates, antivirus or security software, and secured shares are protected from infection of this worm
Removable devices, such as External Hard Drives and USB sticks, may get infected by the worm
Worm:Win32/Conficker attempts to make numerous connections to computers across the network, seeking systems that do not have current security updates, or have open shares, removable media, or weak passwords
Computers with open shares may get infected by the worm
Computers without the latest security updates may get infected by the worm

Fig. 6 Cyber Security

Prevention tips for cyber crime:

1. Do Keep your firewalls (infrastructure defence systems) up to date.
2. Make sure that your system is configured safely and securely.
3. Always choose strong passwords and security checks for social networking sites, email boxes, and for your systems.
4. Do not respond to unfamiliar mails.
5. Protect your system with some security software.

6. Shield or protect your personal information from unknown people or strangers.
7. Safe browsing, and do maintain some good system hygiene.
8. Keep updating your passwords, and login id's at least once or twice in one or two months and make them strong.
9. Do protect your data and personal information and avoid being scammed.
10. Never send personal information and data via mail or any other means.
11. Make your system clean time to time and review your social media sites as well.
12. Do not respond to any spam email and be cautious.

VII. CONCLUSION

In this modern era of technology, the role and usage of internet is increasing worldwide rapidly, therefore it becomes easy for cyber criminals to access any data and information with the help of their knowledge and their expertise. Cyber crime is an unlawful act or a menace that needs to be tackled firmly and effectively. There is a need to create more awareness among the people and basically users of internet about cyber space, diverse forms of cyber crime and some preventive measures as “Prevention is always better than cure”, so it is seriously advised to take some previous precautions while operating the internet. Security nowadays is becoming a prominent and major concern. In the following paper, some security issues are introduced, threats, Trojans, and attacks over internet. Computer security becomes critical in many of the technology-driven industries which operate on the computer systems. Computer security is nothing more than computer safety. Countless vulnerabilities and computer or network based issues are acts as an integral part of maintaining an operational industry.

ACKNOWLEDGMENT

We would like to thank everyone, especially faculty members and our respected mentors, friends, and family members who provided support and followed up with us for such a long period, and trusted us regarding the content of the paper.

REFERENCES

[1] Pooja Aggarwal , Neha, Piyush Arora , Poonam , “REVIEW ON CYBER CRIME AND SECURITY”, IJREAS, Vol. 02, Issue 01, Jan 2014.

[2] Ammar Yassir and Smitha Nayak, “Cybercrime: A threat to Network Security”, IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012.

[3] Atul M. Tonge, Suraj S. Kasture, Surbhi R. Chaudhari, “Cyber security: challenges for society- literature review”, IOSR Journal of Computer Engineering (IOSR-JCE) , Volume 12, Issue 2 (May. - Jun. 2013), PP 67-75.

[4] C. Catlett (ed.), “A Scientific Research and Development Approach to Cyber Security”, Report submitted to the U.S. Department of Energy, December 2008.

[5] Seema Vijay Rane & Pankaj Anil Choudhary, April 2012-September 2012, “Cyber Crime and Cyber Law in India”, Cyber Times International Journal of Technology and Management, Vol. 5 Issue 2.

[6] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. London: Academic Press, 2011: Pp. 5-19.

[7] Richards, James. Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators. Boca Raton, FL: CRC Press, 1999: Pp. 21-54.

[8] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012.

[9] BinaKotiyal, R H Goudar, and Senior Member, A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India PritiSaxena, IACSIT International Journal of Information and Education Technology, Vol. 2, No. 2, April 2012.

[10] B.T. Wang and H. Schulzrinne, “An IP traceback mechanism for reflective DoS attacks”, Canadian Conference on Electrical and Computer Engineering, Vol. 2, 2-5 May 2004, pp. 901 – 904.

[11] Y. C. Hu, A. Perrig, and D.B. Johnson, “Packet leashes: A defense against wormhole attacks in wireless networks”, in Proceedings of the 22 nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM ’03), vol. 3, San Francisco, CA, Mar. 2003, pp. 1976-1986.

[12] Shio Kumar Singh, M P Singh, and D K Singh, “A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks”, International Journal of Computer Trends and Technology- May to June Issue 2011.

[13] M. Cagalj, S. Capkun, and J.P. Hubaux, “Wormhole-based Anti-Jamming Techniques in Sensor Networks” from http://lcawww.epfl.ch/Publications/Cagalj/CagaljCH05-worm.pdf.

[14] A. T. Zia, “A Security Framework for Wireless Sensor Networks”. 2008, http://ses.library.usyd.edu.au/bitstream/2123/ 2258/4/02whole.pdf.

[15] en.wikipedia.org/wiki/Cyber_security_standards.

[16] en.wikipedia.org/wiki/Cyber_crime.