I J C T A, 9(17) 2016, pp. 8693-8701
© International Science Press

Network-based Attacks and its Correlation with Indian Cyber Laws

Navpreet Kaur[*] and Jaswinder Singh[*]

ABSTRACT

With the expansion in the growth of technology, issues like information warfare, cyber warfare, and cyber espionage have raised the concern over the new forms of conflict. In order to keep a check on the criminals who compromise cyber security of nations, a distinct field of law i.e. cyber laws made its way in the cyber world. All these transformations are leading to the emergence of techno-legal community where the legal fraternity allies with cyber professionals in an attempt to integrate the challenges posed by cyber criminals. This paper puts forward techno-legal approach in context to Indian scenario. First various network-related attacks are discussed briefly along with various attacking techniques mapped to the OSI model. Second, Information Technology Act, 2000 is scrutinized section wise on the basis of aforementioned attacks. Furthermore, different circumstances under which a cyber attack can be legally targeted at and performed are discussed from different perspectives. Also, a list of the hacking tools used by the attackers to launch these cyber attacks along with different laws applicable at different scenarios with a case study of each is detailed.

Keywords: IT Act 2000, MAC, ARP, MITM, DoS/DDoS

I. INTRODUCTION

With billions of computers and tons of network devices existing in the world, connected virtually by the new medium of fuel i.e. electricity, human beings created a new artificial domain called cyberspace. Cyberspace has become a new realm for the last decade of the twentieth century where wide range of activities such as exchange of digital information, electronic business, telecommuting, online shopping, entertainment, online learning are taking place on a single platform. Simultaneously, the terms ‘cyber espionage’, ‘information warfare’, ‘cyber warfare’ and ‘cyber attack’ have been commonly used since the mid-1990s raising the concern over the new forms of conflict such as, information stealing, corruption, or its distribution by illicit means. In an Information Age, the prime objective of the organizations is information dominance due to the fact that information is both a ‘weapon’ and a ‘target’ which entails that information should be exploited and defended for success.

Computers and internet have become mission-critical infrastructure for governments, organizations, and financial institutions as they are used for regulating power and water supplies, managing manufacturing processes, controlling air-traffic control systems, supervising stock market systems, and many more. Any disruption in functioning of the above mentioned entities comes directly under the category of cyber attacks provided it involves political and national security issues.

As mentioned in [1] the national-critical infrastructure, national information infrastructure, and the nation itself are always on the verge of Information warfare, Cyber warfare and Electronic warfare, setting up relevant policies and laws to govern and protect these mission-critical infrastructure not only for governments but also for other organizations and financial institutions is the need of an hour. All the techno-savvy countries have given ample significance to this issue by drafting global and national policies and laws.

[*] Department of Computer Engineering, Punjabi University, Patiala, Punjab, India, *E-mail: kaur.17navpreet@gmail.com; jaswindersinghmtech@gmail.com*

This paper is divided into three equal parts. Section II gives a brief introduction to various network attacks and their layer-wise distribution. Section III presents the applicability of Indian cyber legislative to these network attacks. Further, Section IV discusses the extent to which these attacks can be launched legally bearing in mind the technical background and legal knowledge acquired from previous sections. Finally, different scenarios are presented which gives an idea about the laws applicable and tools used to commit cyber crimes by the criminals along with case study of each attack. Section V concludes this paper.

II. NETWORK BASED ATTACKS

Networks are the nerve of all organizations. Network vulnerabilities are such a delicate link which once exposed to the attackers can not only take control of your network, but also can control how your data travels over the medium and to whom. In most of the cases, supervising the network means listening to sensitive information, such as email or financial data, or even redirecting traffic to unauthorized systems. Attackers can do this in a myriad of ways, including routing all your traffic through their own systems. Some of the most commonly performed network attacks are discussed below:

2.1. DoS/DDoS Attacks

Denial of Service attacks [2] [3] is one among the most prevalent cyber attacks that have the potential of affecting almost all the computers connected to the internet. In these attacks, integrated set of zombies inundates the servers by methodically visiting the designated websites. There are different techniques of launching DoS/DDoS attacks like SYN flood, Smurf attacks, TCP RST attacks, buffer overflows etc.

In below figure distribution of various DDoS attacks by type in the fourth quarter of 2015 is compared with the first quarter of 2016. The ranking of the most popular attack methods remained constant from quarter to quarter. Those used most often were the SYN DDoS method, although its share fell compared to the previous quarter (57.0% vs. 54.9%), and TCP DDoS which fell by 0.7 percentage point. The proportion of ICMP DDoS attacks grew significantly, rising to 9%; however, it did not affect the order of the Top 5. Noticeably, the figure for UDP DDoS has fallen continually over the last year: from 11.1% in Q2 2015 to 1.5% in Q1 2016 [4].

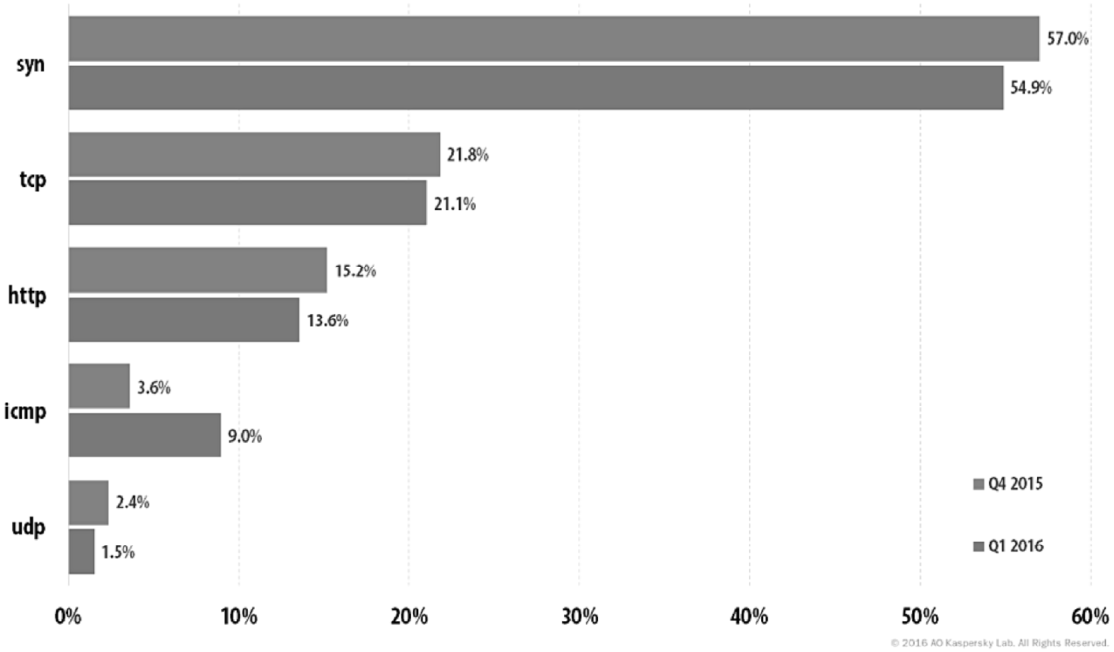
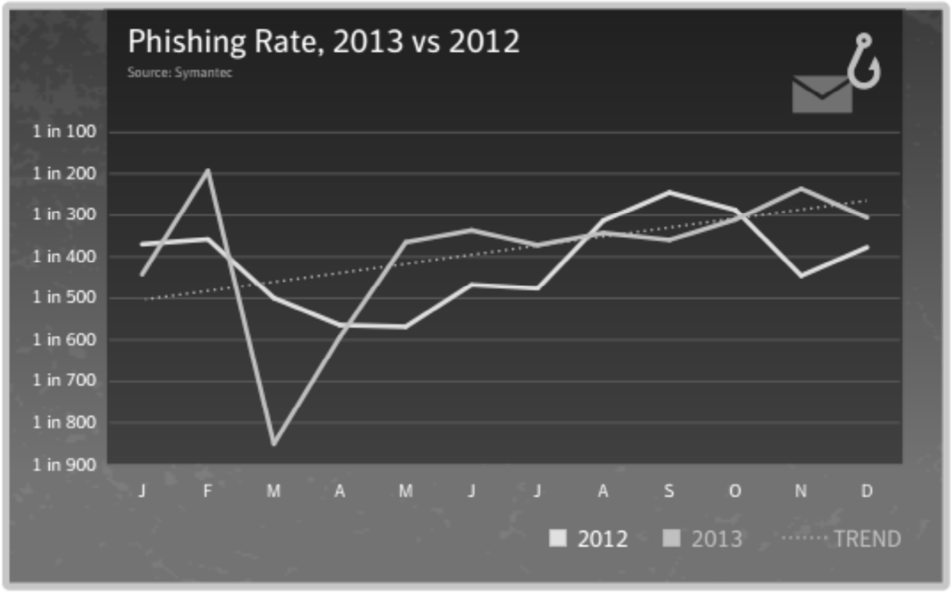


Figure 1: Distribution of DDoS attacks by type in Q4 2015 and Q1 2016[5]

2.2. Spoofing Attacks

Another form of network based cyber-attack is spoofing attack [6] [7], in which the attacker surreptitiously makes use of inaccurate information which helps him to successfully masquerade as another entity. There are a number of ways by which an attacker can impersonate as a legitimate entity. Some of common techniques include Internet Address (IP) spoofing, Address Resolution Protocol (ARP) spoofing, Domain Name Server (DNS) spoofing , Email Spoofing (phishing), Search Engine poisoning.

As shown in the chart below, the phishing rate added on in 2013, from 1 in 414 for 2012 to 1 in 392 in 2013. The busiest month of the year was February, where the rate rose to 1 in 193.0 emails [8].


Phishing Rate, 2013 vs 2012

Source: Symantec

Figure 2: The global average phishing rate, 2012 vs. 2013 [8]

2.3. Network/Packet Sniffing Attacks

With the advancement of network technology, it is crucial to protect the network against cyber attacks. Network sniffing is a technique of capturing and analyzing every packet on the network, used both by IT Professionals as well as by attackers. The packets are captured by attacker in search for the sensitive information like passwords, session tokens and confidential information.

2.4. Man in the Middle (MIMT) Attacks

MITM attack, also referenced as fire brigade attack, eavesdropping attack, or connection hijacking attack, makes the task of keeping data secure and private, particularly, challenging as it exploits inherent vulnerabilities of the authentication protocols being used at various layers. In technical terms, it is a derivative of packet sniffing and spoofing techniques [9] [10].

To understand what hackers get by launching these cyber attacks, it is necessary to know what they can get from the network. Table 1 shows the OSI layers and the attacks that a hacker can perform at each layer by successfully compromising a network [11].

III. NATIONAL LAW PERSPECTIVE

Cyber security of a nation is closely bound by the legal framework that is in practice to combat various cyber attacks. The amenability of cyber security desires to have cohesion with certain well established legal ethics. The moment cyber attack takes place; many legal issues are accordingly conjured [12]. However, cyber laws are distinct in itself by the nature of crimes covered in it. Cyber laws are principally of remedial

Table 1
Layer-wise Attack Distribution

	DOS	*Spoofing*	*Sniffing*	*MITM*
Application	Web DOS, Email Spam	Phishing, Web Spoofing	User ID/Password Sniffing	Wireless MITM, Cookie Injection
Presentation	Malformed SSLRequests	SSL Certificate Spoofing	SSL/TLS Session Sniffing	SSL Hijacking
Session	Telnet DDoS	DNS Poisoning	Telnet and FTPSniffing	Session Hijacking
Transport	SYN Flood, SmurfAttack	TCP Session Poisoning	TCP Session Sniffing, UDP sniffing	Flooding Attacks
Network	ICMP Flood	IP Spoofing, Port Spoofing	IP Sniffing, PortSniffing	ICMP MITM, IP and Port Spoofing/ Sniffing
Data Link	MAC Flood	MAC Address Spoofing	MAC/ARPSniffing	ARP Cache Poisoning and Flooding
Physical	Dummy Packet Attack	Route Spoofing	Surveillance Sniffing	Wiretapping

nature in the sense that they are drafted keeping in mind that the crimes have already taken place. As on date no country is safe from cyber attacks but to keep check on illegal activities in the cyber space, each nation has formulated its own technology laws.

India being the topmost ranked country in the world by making phenomenal rise in the Information Technology sector, witnessed heavy amount of cyber attacks. This compelled India to take required necessary steps in order to save its position in IT sector. As a result of this, Information Technology Act, 2000 [13] came into existence which is based on the UNCITRAL Model Law (United Nations Commission on Trade Related Laws) on Electronic Commerce framed by the United Nations Commission on International Trade Law in 1996. This section explains the applicability of IT Act on above stated cyber attacks.

2.1. DoS/DDoS Attacks

Law: DOS is considered as a severe cyber crime where the person committing this crime is held liable for punishment varying from three years to life term imprisonment or/and with fine which may extend to five lakh rupees under the following sections:

Section 66-F: This section of ITA-2000 states that if a person or group **denies or causes the denial of access to any authorized person to a computer resource** with the intent to threaten the unity, integrity, security or sovereignty of India, then he commits cyber terrorism.

Section 43: This section states that if any person without the permission of the owner or any other person who is in-charge of a computer, computer system or computer network-

d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or **computer network**;

e) disrupts or causes disruption of any computer, computer system or **computer network;**

f) denies or causes the denial of access to any person authorized to access any computer, computer system or **computer network** by any means;

2.2. Spoofing Attacks

Law: Person committing this crime is held liable for punishment varying from three years to life term imprisonment or with fine which may extend from two to five lakh rupees under the following sections:

Section 43: This section states that if any person without the permission of the owner or any other person who is in-charge of a computer, computer system or computer network-

i) Destroys, deletes or **alters any information** residing in a computer resource or diminishing its value or utility or affects it injuriously by any means

Section 65: This section states that anyone who intentionally conceals, destroys, or **alters** or causes the other person to do so will be held under this section.

Section 66C: This section states that whoever **steals other person's identity** by dishonestly making use of electronic signature, password or any other unique identification feature of any other person then he is liable for punishment.

2.3. Network/Packet Sniffing Attacks

Law: Anyone found guilty of illegally sniffing the packets of other's network shall be held punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both under the following section:

Section 43: This section states that if any person without the permission of the owner or any other person who is in-charge of a computer, computer system or computer network-

(a) **Accesses or secures access to** such computer, computer system or computer **network** or computer resource (ITAA2008)

(b) downloads **copies or extracts any data,** computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

2.4. Man in the Middle Attacks

Law: Person committing this crime is held liable for punishment varying from three years to life term imprisonment or with fine which may extend from two to five lakh rupees under the following sections:

Section 43: This section states that if any person without the permission of the owner or any other person who is in-charge of a computer, computer system or computer network-

(a) Accesses or secures access to such computer, computer system or computer network or computer resource

(b) downloads copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any computer, computer system or computer network;

(f) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder,

(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

(i) Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means

(i) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage

Section 65: This section states that anyone who intentionally conceals, destroys, or **alters** or causes the other person to do so will be held under this section.

Section 66C: This section states that whoever steals other person's identity by dishonestly making use of electronic signature, password or any other unique identification feature of any other person then he is liable for punishment.

IV. NETWORK RELATED CRIMES AND CYBER LAWS

Having taken a look at the various network related attacks and the relevant legislation, this section combines the knowledge of both the sections. Bearing in mind, the different cyber attacks and the relevant legislation of India, this section presents the cases that were booked in the court concerning the cyber crimes committed. Also, the different circumstances under which a cyber attack can be legally targeted at and performed are discussed from different perspectives. Later, a list of the hacking tools used by the attackers to launch these attacks is specified. In the end Cyber attacks along with different laws applicable at different scenarios are discussed and a case study of each is described.

1. Who may lawfully be targeted in a cyber attack [14]?

   Considering the international perspective, under the law of war, three types of individuals may be lawfully targeted: combatants, civilians directly participating in hostilities, and civilians acting in a continuous combat function such as programmers who work with military intelligence. This causes the civilians involved in cyber-attacks regarded as performing tasks that alter their status under the law of war, rendering them lawful targets of a counterattack [14].

   Taking into account the organizational perspective, any institution which has employed the penetration testers by legally signing a number of contracts and agreements to penetrate into their network for the purpose of exposing and later plugging up the known vulnerabilities comes under the category of being lawfully targeted. Any violation to the pre-defined and mutually agreeable contracts is subject to the matter of legal consequences.

2. Who may lawfully carry out a cyber attack [14]?

   From the global perspective, another important issue arises that of who may lawfully carry out a cyber attack and how the nations constitute their cyber-fighting forces. In context to cyber attacks, nations are more prompted to civilians due to many reasons such as using the civilians to carry out cyber attacks can mask their own involvement in such operations [14].

   Considering the organizational viewpoint, all the legal and technically certified companies which are involved in the business of penetration testing are lawfully sound to carry out cyber attacks keeping in notice that no agreements like confidentiality agreements, non-disclosure agreements, and other relevant contracts are violated in the due course interval.

3. Who may lawfully access the data?

   Section 29 of the IT Act [13] states clearly about who may lawfully access the data as follows:-

Access to computers and data give power to lawfully access the data as stated below:

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made there under has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system [13].

(2) For the purposes of sub-section (1), the Controller or any person authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary [13].

In the following section real world cases with respect to the above discussed cyber attacks along with applicable laws in different scenarios are covered. In addition to this, different hacking tools used by the criminals to commit these crimes are discussed.

2.1. DoS/DDoS Attacks

Tools: Bonk, LAND, Smurf, Teardrop, Win Nuke

Scenarios:-

Scenario 1: Use of Internet and Computer by Terrorists

Laws: Sections 43 and 66F of IT Act

Scenario 2: Infrastructure disruption by corporate companies

Laws: Section 43 of IT Act

Case Study: Official website of Maharashtra government blocked

The denial of service attack took place in September 2007, when the official website of Maharashtra government, http://www.maharashtragovernment.in, remained blocked. The state government website contained detailed information about government departments, circulars, reports, and several other topics. The hackers identified themselves as “Hackers Cool Al-Jazeera” and claimed that they were based in Saudi Arabia. It should also be noted that the official website was affected by viruses on several occasions in the past, but was never blocked. Also, the website had no firewall implemented to keep it secure [15].

2.2. Spoofing Attacks

Tools: Scapy, Spoofer, Colasoft Capsa, Nmap, Yersinia, Hping, Nemesis, IRPAS, PacketExcalibur

Scenarios:-

Scenario 1: Fake profile cases

Laws: Sections 67 of IT Act and Sections 509, 153A, 500 of IPC

Scenario 2: Phishing Attacks

Laws: Sections 43, 66 of IT Act and Sections 419, 420,468 of IPC

Scenario 3: Virus Attacks

Laws: Sections 43, 66 of IT Act and Section 426 of IPC

Case Study: Phishing Case of Nasscom vs. Ajay Sood & Others

A landmark judgment was delivered in March, ‘05 in the case of National Association of Software and Service Companies vs. Ajay Sood & Others, where the Delhi High Court declared `phishing’ on the internet to be an illegal act, entailing an injunction and recovery of damages. The petitioner Nasscom alleged that the defendants, who were operating a placement agency, were involved in head-hunting and recruitment used the name of Nasscom by sending emails in order to obtain personal data. The defendants used fictitious identities to avoid recognition and legal action. This case achieves clear milestones by bringing the act of "phishing" within the range of Indian laws even in the absence of specific legislation [16].

2.3. Network/Packet Sniffing Attacks

Tools: Dsniff, Ethereal, Etherpeek, Network Associates's Sniffer, Cain and Abel, Ngrep, Sniffit, Snort, Tcpdump, Windump

Scenarios:

Scenario 1: Software and Music Piracy
Laws: Sections 43, 66 of IT Act and Section 63 of Copyright Act

Scenario 2: ID and Password Hacking
Laws: Sections 43, 65 of IT Act

Case Study: Software Piracy Case of Microsoft Corporation vs. Yogesh Papat, Delhi HC.

The Microsoft Corporation, the registered proprietor of the trademark MICROSOFT, registered a case concerning the infringement of copyright in software. It requested a permanent injunction restraining the defendant, its directors and agents from copying, selling, offering for sale, distributing or issuing to the public counterfeit or unlicensed versions of Microsoft's software program in any manner that amounts to infringement of Microsoft's copyright in the computer programs, related manuals and Microsoft's registered trademarks [16].

2.4. Man in the Middle Attacks

Tools: Mitmproxy, combination of Arpspoof, Driftnet and Urlsnarf, Cain and Abel, Wireshark, Sslstrip, Ettercap

Scenarios:

Scenario 1: Source Code Theft

Laws: Sections 43, 65, 66 of IT Act and Section 63 of Copyright Act

Scenario 2: Theft of Confidential Information

Laws: Sections 43, 66 of IT Act and Section 384, 426 of IPC

Case Study: Data Theft Case

One of the data theft cases registered in the country was that of Florida (USA) based firm. The firm registered the data theft case against Ahmedabad based BPO alleging that the latter had theft database from their server & illegally selling to company's clients & competitors. They also claimed that IT company owner had taken this step in response to cancellation of business contract of development & maintenance of the company's one of the portals [17].

V. CONCLUSION

In the era of twenty-first century, it is not very difficult to plot a scenario of cyber attacks against the critical information infrastructure run by Information and Communication Technology. These attacks can hamstring the entire global network if executed successfully. Since India is a late entrant in the cyber security world, a great deal is still needed to be done apart from implementing the sole cyber law of India known as Information Technology Act, 2000. In this paper, various network attacks are taken into account to have an idea how effectively and suitably the present Indian cyber laws are capable of dealing with the ever-increasing, fast changing technical cyber world. It is realized that IT Act alone is not sufficient to deal with the cyber space crimes, as the rules under the present law do not prescribe due diligence, internet intermediary liability, and reasonable security practices etc. Therefore, it is used as a substitute to other laws such as Indian Penal Code, Copyright Act, Income Tax Act, Prevention of Money Laundering Act, and Arms Act.

In India, the techno-legal fields such as cyber law, cyber security, cyber forensics, cyber warfare, cyber terrorism etc. takes a back seat because of lack of expertise to manage these complicated cyber security issues. Since, the techno-legal fields are growing in number Indian Government needs to act wisely and look into the matter seriously as cyber security has become an integral part of the national security.

REFERENCES

[1] Kramer, F.D., S.H. Starr, and L.K. Wentz. Eds. 2009. Cyberpower and national security, Washington, D.C: Center for Technology and National Security Policy.

[2] Gligor, V.D., M. Blaze, and J. Ioannidis. 2000. Denial of Service – Panel discussion. In *Security Protocols Workshop, Lecture notes in computer science*, vol. 2133, 194–203. Springer, Berlin.

[3] Carl, G., G. Kesidis, R.R. Brooks, and S. Rai. 2006. Denial-of-service attack – Detection techniques. *IEEE Internet Computing* 10(1): 82–89.

[4] K. Lab, "Securelist – information about viruses, hackers and Spam," 2015. [Online]. Available: *https://securelist.com/blog/research/70071/statistics-on-botnet-assisted-ddos-attacks-in-q1-2015/*. Accessed: May 28, 2016.

[5] K. Lab, "Distribution of DDoS attacks by type," (Quarterly Malware Reports), 2016. [Online]. Available: *https://securelist.com.*

[6] X. Hou, Z. Jiang, and X. Tian, "The Detection and Prevention for ARP Spoofing based on SNORT," in Proc. of IEEE International Conference on Computer Application and System Modeling (ICCASM'10), vol. 5, pp.V5-137.

[7] V Goyal, R Tripathy, An efficient solution to the ARP cache poisoning problem, in Proc of Australasian Conference on Information Security and Privacy (ACISP), vol. 1. Brisbane, Australia, pp. 40–51 (July 2005).

[8] S. Corporation, "Internet Security Threat Report 2014," vol. 19, Apr. 2014. [Online]. Available: *http://www.symantec.com*. Accessed: May 30, 2016.

[9] V. Networks, "Article: Cyber attacks explained: Man in the middle: Ethical hacking, pen test Pune, India," 2008. [Online]. Available: *http://www.valencynetworks.com/articles/cyber-attacks-explained-man-in-the-middle-attack.html*. Accessed: May 27, 2016.

[10] S. Gangan, (A Review of Man-in-the-Middle Attacks). [Online]. Available: *https://arxiv.org/ftp/arxiv/papers/1504/1504.02115.pdf*. Accessed: May 27, 2016.

[11] P. Phatak, "Cyber Attacks Explained," in *The complete portal on open source* (Concepts, Overview, Sysadmins). [Online]. Available: *http://opensourceforu.com/.*

[12] B. Singh, "Centre of excellence for Cyber security research and development in India (CECSRDI)," 2014. [Online]. Available: *http://perry4law.org/cecsrdi/?p=1095*. Accessed: May 30, 2016.

[13] [Online]. Available: *http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf*. Accessed: May 30, 2016.

[14] O. A. Hathaway *et al.*, vol. 100, no. 4, pp. 817–885. [Online]. Available: *http://www.jstor.org/stable/23249823*. Accessed: Apr. 10, 2016.

[15] V. Tripathi, "Latest cases of Cyber crime," 2007. [Online]. Available: *http://www.cyberlawsindia.net/cases.html*. Accessed: May 28, 2016.

[16] "Popular Cyber case law, IT act, 2000 case law, Cyber cases investigation reports, Cyber cases lawyer," 2009. [Online]. Available: *http://www.cyberlawconsulting.com/cyber-cases.html*. Accessed: May 28, 2016.

[17] "Cyber crime cases solved by Sunny Vaghela". [Online]. Available: *http://www.sunnyvaghela.com/casestudies.html*. Accessed: May 28, 2016.