Importance of Cyber Security

Rajesh Kumar Goutam
Department of Computer Science
University of Lucknow, Lucknow

ABSTRACT
Governments, military, organizations, financial institutions, universities and other businesses collect, process and store a large amount of confidential information and data on computers and transmit that data over networks to other computers. With the continuous rapid growth of volume and sophistication of cyber attacks, quick attempts are required to secure sensitive business and personal information, as well as to protect national security. The paper details about the nature of cyberspace and shows how the internet is unsecure to transmit the confidential and financial information. We demonstrate that hacking is now common and harmful for global economy and security and presented the various methods of cyber attacks in India and worldwide.

Keywords
Cyber security, Cyberspace, Cybercrime.

1. INTRODUCTION
Cyber security is defined as technologies and processes constructed to protect computers, computer hardware, software, networks and data from unauthorized access, vulnerabilities supplied through Internet by cyber criminals, terrorist groups and hackers. Cyber security is related to protecting your internet and network based digital equipments and information from unauthorized access and alteration. Internet is now not only the source of information but also has established as a medium through which we do business, to advertise and sell our products in various forms, communicate with our customers and retailers and do our financial transactions. The internet offers lots of benefits and provides us opportunity to advertise our business across the globe in minimum charges and in less human efforts in very short span of time. As internet was never constructed to track and trace the behavior of users [1]. The Internet was actually constructed to link autonomous computers for resource sharing and to provide a common platform to community of researchers [1]. As internet offers on the one hand huge number of benefits and on the other hand it also provides equal opportunities for cyber-terrorists and hackers. Terrorist organizations and their supporters are using internet for a wide range of purposes such as gathering information and dissemination of it for terrorist purpose, recruiting fresh terrorists, funding attacks and to motivate acts of terrorism [2]. It is often used to facilitate communication within terrorist groups and gathering and dissemination of information for terrorist purposes [2].

2. NATURE OF CYBERSPACE
Cyberspace is virtual space that use electronics and electromagnetic spectrum to store, modify and exchange information through the use of networked system and concerned physical structure [3]. It is intangible where communications and internet related activities take place. Cyberspace is imaginary where contained objects are neither exist nor representation of physical world [4]. It is totally virtual environment wherein information exchange and communication occurs that connects about 2.7 billion people around the world to provide a common platform to share ideas, views, services and friendship. It is expandable and borderless in nature and growing sharply without considering any physical or political border.

3. NEED OF CYBER SECURITY
Cybersecurity is now considered as important part of individuals and families, as well as organizations, governments, educational institutions and our business. It is essential for families and parents to protect the children and family members from online fraud. In terms of financial security, it is crucial to secure our financial information that can affect our personal financial status. Internet is very important and beneficial for faculty, student, staff and educational institutions, has provided lots of learning opportunities with number of online risks [5]. There is vital need for internet users to understand how to protect themselves from online fraud and identity theft. Appropriate learning about the online behavior and system protection results reduction in vulnerabilities and safer online environment. Small and medium-sized organizations also experience various security related challenges because of limited resources and appropriate cyber security skills [5]. The rapid expansion of technologies is also creating and making the cyber security more challenging as we do not present permanent solutions for concerned problem. Although, we are actively fighting and presenting various frameworks or technologies to protect our network and information but all of these providing protection for short term only. However, better security understanding and appropriate strategies can help us to protect intellectual property and trade secrets and reduce financial and reputation loss [5]. Central, state and local governments hold large amount of data and confidential records online in digital form that becomes primary target for a cyber attack [5]. Most of time governments face difficulties due to inappropriate infrastructure, lack of awareness and sufficient funding. It is important for the government bodies to provide reliable services to society, maintain healthy citizen- to-government communications and protection of confidential information [5].

4. INTERNET USAGE IN INDIA
India has experienced tremendous growth of information technology and established itself as popular IT destination in world. It is ranked on number three position in world after China and United State in the usage of internet [6]. A report from IAMAI [7] revels that India is expected to be second largest by 2015 with 330 to 370 million internet users [7]. More than 200 million users started to use internet after 2010 [7]. The total number of internet users were 205 million in 2013, out of which 137 million internet users resides in urban areas while rest 68 million were from rural areas. Mumbai, Delhi and Hyderabad were rated as top cities in internet usage with 12 million, 8.7 million and 7.1 million internet users respectively [7]. About 75% internet users are below the age of 35 years. In India around 81% population is using mobile phones, out of which 10% using smart phone, 9% using multimedia phone and 3% use tablets. About 25 million

people accessing internet through mobiles. Indian believes in social networking 86% internet users visit social networking sites [7]. The target for broadband connections is projected to 22 million by 2014[6].

5. VARIOUS FORMS OF CYBERCRIME

Cybercrime denotes criminal activity including internet, computers or any other inter-connected infrastructure. The term that covers crimes like phishing, credit card frauds, illegal downloading, industrial espionage, child pornography, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on.

5.1 Cyber Stalking

It is defined as an act which is frequently done by intruding into individuals' personal life to cause distress, anxiety and fear [8]. Cyber Stalkers often take the advantages of anonymity of internet that allow them to continue their activities without being detected. Actually, an intrusion is possible in individuals' personal life by approaching to their friend circle, family members or sending fake letters and mails to targeted person electronically. Cyber stalking harasses a person psychologically therefore it is sometimes referred as "psychological rape" or "psychological terrorism" [8]. About 90% stalkers are male and around 80% females are victims of such kind of harassment [8].

5.2 Intellectual Property Theft

The Intellectual property is defined as an innovation, new research, method, model and formula that have an economic value. Intellectual property is protected with having patents and trademarks and with the copyright on videos and music as well. It is clear that market secrets and internal business information are highly attacked assets for any organization. This business information may be in various forms such as future product design, customer lists and price lists etc. the internet is the frequently used medium to facilitate the Intellectual property theft because it is easy to mask the identity on network.

5.3 Salami Attack

In the salami cyber attack, cyber criminals and attackers steal money in very little amount from several bank accounts to make a huge amount. The alteration becomes so insignificant that in a single case it would be difficult to notice. Suppose, a bank employee creates a program into banking software, that reduces a insignificant amount of money (say Rs. 3 a month) from the account of each customer. It is general perception that no customer will probably notice this unauthorized deduction, but it will be beneficial to cyber criminals that make large money.

5.4 E-Mail Bombing

It is sending of enormous amount of e-mails to a targeted person. A large amount of e-mails simply fill up the recipient's inbox on the server or, in some cases, server becomes fail to receive such large amount data and stops functioning [9]. There are many ways to create an e-mail bomb like "zombie" or "robot" which are capable to send continuous thousands or even millions of e-mails to recipients' e-mail address [10]. E-mail is bombing and e-mail flooding, both the terms are used interchangeably and represent the same phenomena. It is said e-mail bombing as the recipient's inbox gets filled up with large number of undesired mails and the targeted person does not become able to receive further important e-mails.

5.5 Phishing

It is a kind of fraudulent attempt that is made through email, to capture personal and financial information. Perpetrator sends e-mail that seems to come from well known and trustworthy address ask for your financial information such as bank name, credit card number, social security number, account number or password. It is common for phishing attempts that e-mails appear to come from sites and companies that do not even have a bank account.

5.6 Identity Theft

Identity theft is a type of fraud in which a person pretends to be someone else and does crime with the name of someone else [11]. Perpetrator steals key pieces of information such as name, address, credit card number, bank account number to impersonate a person and commits crimes in his/her name. Perpetrator can use stolen personal and financial information to access your bank accounts, opening new accounts, transferring bank balances or purchasing etc [12].

5.7 Spoofing

It refers to a technique to have unauthorized access to computers, whereby perpetrator sends messages to a networked computer with an IP address. At the recipient end it seems that messages are being transmitted from a trustworthy source. To conduct IP spoofing, a hacker first makes attempt to find an trusted host IP address and then modification and alteration of packets are done to show that the packets are being generated form original host.

5.8 Worms, Trojan Horses, Virus

A computer virus needs another medium to propagate. In other words the computer virus becomes effective only when it links itself with a malicious program or executable files. When we run or execute these supportive files then virus leaves its infections. In the field of computer science, as far as we know the virus generation is not natural phenomena. It always needs human efforts to get expansion. The existence of virus in your system does not harm computer until its related executable file or program run. A worm and virus both the terms used interchangeably but there is major difference as worm do not need supportive attached files while virus requires. Existence of worm in system alone can affect the performance of your system. It requires no human activity. The Trojan Horse, at first glance seems as useful software but actually damage computer and its software as it gets installed on. Some Trojans create backdoor for malicious users to control your computer remotely, allowing confidential and personal information theft [13].

5.9 DoS and DDoS

A denial of service (DoS) attack refers an attempt to make computer, server or network resources unavailable to its authorized users usually by using temporarily interruption or suspension of services. A Distributed Denial of Service (DDoS) attack refers a DoS attack that propagates from more than one infected system with malicious software at the same time. These infected systems are collectively called as "botnets" that control the target system remotely.

5.10 Pornography

Pornography refers to printed or video material such as books, magazines, photographs and video-clips that contain description or showing sexual organs or activity intended to encourage sexual excitement. More often same person gets involved in production, distribution and downloading in pornography. The motivation behind production and

distribution becomes to attain financial gain while third stage-downloading is performed by the end users to entertain them.

6. GROWTH IN CYBER CRIME

A large number of tasks now have been automated and now easier to handle with the help of information technology. Now, hardly any sector of society remains unaffected. By the end of 2013, over 2.7 billion people are using internet worldwide while 4.4 billions still needs to be connected. Now a day, our lives look incomplete without internet, mobiles and computers. Records are maintained digitally and transferred on communication lines. Banks and other financial institutions also use internet and connected network to carry out financial transactions. So it becomes necessary to secure our network from treats and hacking. According to report about 1,00,000 virus/ worms are reported to be active each day and out of which 10,000 are indentified as new and unique [14]. The report also describes the number of websites hacked (Fig. 1 and Fig. 2) in last six years across worldwide and in India as well [14].

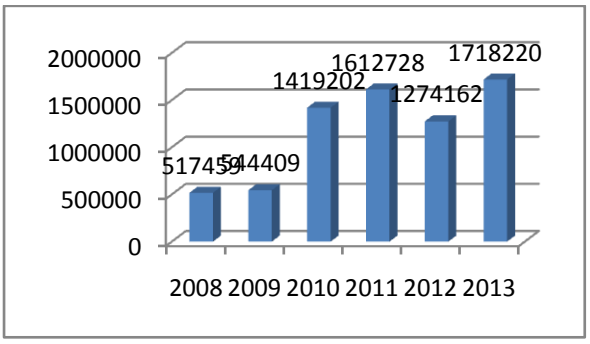

Fig 1: Websites hacking worldwide

ISTR highlight 2013 as the year of Mega Breach. In this year total number of breaches was about 62 percent which was larger than in 2012 with 254 breaches. It was also greater than in 2011 with 207 breaches [15]. Although, 2013 was the year in which eight breaches exposed greater than 10 million identities but in 2012 only one breach was capable to expose about the same number of identities. In 2013, about 552 million identities were breached that has transferred financial and credit card information, date of birth, contact number and IDs into criminal hands. Normally, cyber attackers seek vulnerability in legitimate websites to have control to plant malicious software.

Note: the data of Fig.1 and Fig.2 has been taken from Fifty Second Report. Cyber Crime, Cyber Security and Right to Privacy, Ministry of Communications and Information Technology, Department of Electronics and Information Technology, Govt. of India, February 2014.

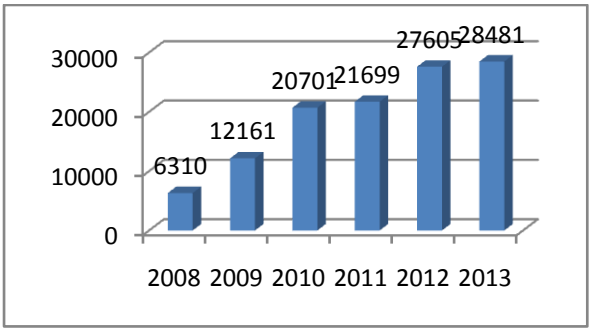

Fig 2: Websites hacking in India

ISTR [15] vulnerability assessment system found that about 82 percent websites have vulnerabilities that invite the terrorists for coordinated attack. In 2012, Malware was detected on 1 in 532 websites while it is found in 566 websites in 2013.

7. CYBER CRIMES IN INDIA

In 2013, total 4,356 cases were reported under IT Act while this figure was 2,876 in 2012. In other words, there was rapid growth about 51.5% from 2012 to 2013. 681 cases about 15.6% were registered from Maharashtra. In Andhra Pradesh 635 cases were registered under same Act, followed by Karnataka (513 cases) and Uttar Pradesh with 372 cases. About 45.1% (1,966 cases) were related to hacking of websites and damage of computer resources [16]. There were 1,337 cases related to cybercrime, registered under different sections of IPC during 2013 while this figure was around 601 in 2012. This shows a rapid increase, around 122.5% in a year [16]. Only in Uttar Pradesh 310 cases were registered from 1,337 cases. Maharashtra holds second positions with 226 cases followed by Haryana with 211 cases. Most of the cases, out of total 1,337 cases were related to forgery and financial fraud. From the 1,337 cases, 747 cases were registered under forgery category while 518 cases fall in fraud.

Table 1. Cyber Crime Growth in India

Year	Cases Registered Under IT Act	Person Arrested
2010	966	799
2011	1,791	1,184
2012	2,876	1,522
2013	4,356	2098

Although, All these (1,337) offences were put in traditional IPC crimes but somewhere these were related to cyber crime wherein computer systems and internet were used to conduct such offences [16]. Uttar Pradesh was the state with the highest number (219) of cyber forgery followed by Maharashtra with 215. Statistics depicted in the table 1.show that cyber crimes are rapidly growing in numbers and sophistication as well. We still require a technique or procedure to control cyber crimes. As the statistics of the arrested people show that there is a huge gap between cases registered and the person arrested. It means we are not reaching and arresting all the criminals who commit such types of cyber crimes.

Note: the data of table 1 has been taken from A Report on,Crime in India 2013 compendium, National Crime records Bureau, Ministry of Home affairs, Govt. of India.

8. CONCLUSION

In this paper, we have detailed about the nature of cyberspace and defined the cyber security with its necessities across the world. Significant statistics show that India stands on third position in the usage of internet and also experiencing the problem of cyber security. We have also explained various methods of cyber attacks and showed how the websites hacking incidents are common and growing with time worldwide.

9. REFERENCES

[1] Lipson. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Carnegie Mellon Software Engineering Institute, Pittsburgh, November 2002.

[2] A Report from United Nations offices on drugs and crime (UNODC), the use of the Internet for terrorist purposes, New York, USA, 2012.

[3] A Report available on http://searchsoa.techtarget.com/definition/cyberspace.

[4] A Report available on http://www.businessdictionary.com/definition/cyberspace.html.

[5] A Report form CISCO, Cybersecurity: Everyone's Responsibility, 2010.

[6] A Fifty Second Report. Cyber Crime, Cyber Security and Right to Privacy, Ministry of Communications and Information Technology, Department of Electronics and Information Technology, Govt. of India, February 2014.

[7] A Report, Digital India 2014, IAMAI 2013.

[8] Gisela Wurm, Stalking, A Report before Committee on Equality and Non-Discrimination, June 2013.

[9] A Report available at http://searchsecurity.techtarget.com/definition/mail-bomb.

[10] A Report available at http://www.businessdictionary.com/definition/e-mail-bomb.html

[11] A Report availale at http://www.sse.gov.on.ca/mcs/en/pages/identity_theft.aspx

[12] A Report available at http://www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-eng.htm.

[13] A Report available at http://www.webopedia.com/DidYouKnow/Internet/virus.asp.

[14] A Fifty Second Report. Cyber Crime, Cyber Security and Right to Privacy, Ministry of Communications and Information Technology, Department of Electronics and Information Technology, Govt. of India, February 2014.

[15] A Report on Internet Security Threat Report 2014, Symantec Corporation, Volume 19, April 2014.

[16] A Report on, Crime in India 2013 compendium, National Crime records Bureau, Ministry of Home affairs, Govt. of India.