International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.05, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

CYBER SECURITY CHALLENGES FOR SOCIETY

Dr. Sudhakar Singh

Professor / Principal, Department of Physics and C.S.,
Sardar Patel College of Technology, Balaghat (M.P.), India

ABSTRACT

The 19th century saw development of competitive variety and excellence in mechanics and allied branches. First half of 20thcentury saw revolution in electricity and its applications. Second half of twentieth century saw revolution in semiconductor technology, electronics for obvious reasons. Initial stages of 21st century appear to be dominated by micro and "nano" domain research and their applications. Digital technique is its one of the most wonderful domain. Micro intelligent chips are capable of doing a lot, was never thought of. It's starting point being development of computer taking it from first generation to 4+ computer generations. Whereas, use of microelectronics and controlled em wave propagation. The perfect assimilation of generation of em wave and computer led to the development of mobile phone technology. Now with fast growth of technology we cannot imagine what is in our plate after 10 years. Using different peripherals and programmes the digitalisation of data feeding and recovering in desired for results are now on the fingertips. There are numerous welcome applications has made digital techniques indispensible. But the other face of this coin is horrifying and makes us to recall a proverb that says "you make rules I will show how to make it fail". It is affecting conceivable growth or damaging the desired output. In the name of intellectual property (IP) our top most bran in digital world are engaged for earning a few alms "some throw away money" for the top level managerial system. These people make a spectacular / unmatchable program and the virus is immediately developed to make system fail. The other aspect of digital technology, like almost all other technologies is to ensure that the system and core should fail or abuse-able to corruption and makes system fail. A more dangerous part is 'it can be similar to nuclear power which can be used as for power generation as well as in damaging the environment. Specifically, using digital technique can lead to human empowerment and handling those techniques to make the world full of fear and damaging the health of its user. So, who needs cyber security? Use of this technology has threats in some of the following areas. Malware may cause impact on cyber space, spyware, virus security, fishing attacks, cyber crimes, cyber law ethics etc. This paper will dwell on cyber crime, a few coding and decoding of secret messages. This has severed damages to persons and locates the location of target field, to terrorise people, in general and generate hatred.

Keywords - Cyberspace, Coding And Decoding, Malware, Hacker, Cybercrime

I INTRODUCTION

May be, for over 3 million years human species, like most of the other animals, were constantly learning and exerting physically and mentally to lead a safe and better life. But this is not certain that we at present excel in development, when life evolved. It is quite likely that culmination of development had occurred several times before in this long period. But if we look back, we find that restless human ventured to uncover nature for selfishness. We have evidences that human again started (some 4+ thousand of years) to discover things that directly affected their life. In spite of odds some dedicated philosophers and scientists did not deter in their pursuance of truth related to exploration of nature. As for as science is considered, Copernicus, Newton, Galileo and others did a spade work. The 19th century saw development of competitive variegation and excellence in mechanics and allied branches (by inventing principles of machines and their fabrication). First half of 20th century was dramatically different. It saw revolution in electricity and its applications. Second half of twentieth century saw revolution in semiconductor technology (electronics for obvious reasons). Initial stages of 21st century appear to be dominated by micro and "nano" domain research and their applications. Digital technique is its one of the most wonderful domain. Micro intelligent chips, now are capable of doing a lot that was never even thought of. Its starting point being (most probably) development of computer saw its rapid growth from first generation to 4+ generation computer. Whereas, use of microelectronics and guided em wave propagation, can be considered as foundation stone for increasing efficiency in terms of 'memory, storage capacity and ability to retrieve data and their analysis', the software was key to all such wonderful helps. The perfect assimilation of generation of em wave and computer analysis led to the development of mobile phone technology. Now with fast growth technology we can hardly imagine what would be there in our plate after 10 years. The mobiles are now part and parcel of our life, as is handling multi-tasking. Earlier it was simply a phone. Now in conjunction with internet mobiles are more users friendly and performing tasks is unique feature. It is handling so many task that it has reached every nook and corner of the world. Using different peripherals and programmes the digitalisation of data feeding and retrieving in desired form, the intended results are now on the fingertips. There are numerous welcome applications, has made digital techniques indispensible. Taking this thread let us develop a consistent tool in the study of cyber world.

II TYPES OF CYBER CRIME

2.1. HACKING

Hacking in simple terms means an illegal intrusion into a computer system and/or network. There is an equivalent term to hacking i.e. cracking, but from Indian Laws perspective there is no difference between the term hacking and cracking. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from some corporate giant threatening him to publish the stolen information which is critical in nature. Government websites are the hot targets of the hackers due to the press coverage, it receives. Hackers enjoy the media coverage.

- Motive Behind The Crime
- Greed
- Power
- Publicity
- Revenge
- Adventure
- Desire to access forbidden information
- Destructive mindset
- Wants to sell n/w security services

2.2. CHILD PORNOGRAPHY

The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The internet is very fast becoming a household commodity in India . Its explosion has made the children a viable victim to the cyber crime. As more homes have access to internet, more children would be using the internet and more are the chances of falling victim to the aggression of pedophiles. The easy access to the pornographic contents readily and freely available over the internet lower the inhibitions of the children. Pedophiles lure the children by distributing pornographic material, then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions. Sometimes Pedophiles contact children in the chat rooms posing as teenagers or a child of similar age, then they start becoming friendlier with them and win their confidence. Then slowly pedophiles start sexual chat to help children shed their inhibitions about sex and then call them out for personal interaction. Then starts actual exploitation of the children by offering them some money or falsely promising them good opportunities in life. The pedophiles then sexually exploit the children either by using them as sexual objects or by taking their pornographic pictures in order to sell those over the internet.In physical world, parents know the face of dangers and they know how to avoid & face the problems by following simple rules and accordingly they advice their children to keep away from dangerous things and ways. But in case of cyber world, most of the parents do not themselves know about the basics in internet and dangers posed by various services offered over the internet. Hence the children are left unprotected in the cyber world. Pedophiles take advantage of this situation and lure the children, who are not advised by their parents or by their teachers about what is wrong and what is right for them while browsing the internet.

2.3. CYBER STALKING

Cyber Stalking can be defined as the repeated acts harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously. It all depends on the course of conduct of the stalker. Both kind of Stalkers Online & Offline – have desire to control

the victims life. Majority of the stalkers are the dejected lovers or ex-lovers, who then want to harass the victim because they failed to satisfy their secret desires. Most of the stalkers are men and victim female.

2.4. DENIAL OF SERVICE ATTACK

This is an act by the criminal, who floods the bandwidth of the victimâ€™s network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide Short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCp/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker.

2.5. VIRUS DISSEMINATION

Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious.

2.6. SOFTWARE PIRACY

Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

2.7. IRC CRIME

Internet Relay Chat (IRC) servers have chat rooms in which people from anywhere the world can come together and chat with each other.

2.8. CREDIT CARD FRAUD

The unauthorized and illegal use of a credit card to purchase property.

2.9. NET EXTORTION

Copying the company's confidential data in order to extort said company for huge amount

2.10. PHISHING

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has.

III CYBER LAW AND CYBER CRIME

3.1. CYBER LAW IN INDIA

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous

nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyber laws in India.

3.2. IMPORTANCE OF CYBER LAW

Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives. As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyberlegal perspective. From the time you register your Domain Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails , to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyberlaw issues involved. You may not be bothered about these issues today because you may feel that they are very distant from you and that they do not have an impact on your Cyber activities. But sooner or later, you will have to tighten your belts and take note of Cyberlaw for your own benefit.

3.3. CYBER LAW ENCOMPASSES LAWS RELATING TO

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property
4. Data Protection and Privacy

3.3.1. CYBER CRIMES:

Cyber crimes are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber crime. These crimes are discussed in detail further in this chapter. A comprehensive discussion on the Indian law relating to cyber crimes and digital evidence is provided in the ASCL publication titled “Cyber Crimes & Digital Evidence – Indian Perspective”.

3.3.2. ELECTRONIC AND DIGITAL SIGNATURES :

Electronic signatures are used to authenticate electronic records. Digital signatures are one type of electronic signature. Digital signatures satisfy three major legal requirements – signer authentication, message authentication and message integrity. The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures. These issues are discussed in detail in the ASCL publication titled “Ecommerce – Legal Issues”.

3.3.3. INTELLECTUAL PROPERTY :

Intellectual property is refers to creations of the human mind e.g. a story, a song, a painting, a desi.gn etc. The facets of intellectual property that relate to cyber space are covered by cyber law.

3.3.4. DATA PROTECTION AND PRIVACY

Data protection and privacy laws aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc. These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

IV CYBER LAW AND POLICE

Availability of relevant and timely information is of utmost importance in conduct of business by Police, particularly in investigation of crime and in tracking & detection of criminals. Police organizations everywhere have been handling large amounts of information and huge volume of records pertaining to crime and criminals. Information Technology (IT) can play a very vital role in improving outcomes in the areas of Crime Investigation and Criminals Detection and other functioning of the Police organizations, by facilitating easy recording, retrieval, analysis and sharing of the pile of Information. Quick and timely information availability about different facets of Police functions to the right functionaries can bring in a sea change both in Crime & Criminals handling and related Operations, as well as administrative processes. Creation and maintenance of databases on Crime & Criminals in digital form for sharing by all the stakeholders in the system is therefore very essential in order to effectively meet the challenges of Crime Control and maintenance of public order. In order to achieve this, all the States should meet a common minimum threshold in the use of IT, especially for crime & criminals related functions. Cyber Crime Investigation M.P. Cyber Police, Police Headquarter, Bhopal India, to deal with Cyber crimes, and to enforce provisions of India's Information Technology Law, namely, The Information Technology Act, 2000 and various cyber crime related provisions of criminal laws, including the Indian Penal Code.

V. CODING AND DECODING OF SECRET MESSAGES

The other aspect of digital technology, like almost all other technologies is to ensure that the system and core should fail or abuse-able to corruption and makes system fail. A more dangerous part is ‘it can be similar to nuclear power which can be used as for power generation as well as in damaging the environment’. Specifically, using digital technique can lead to human empowerment and handling those techniques to make the world full of fear and damaging the health of its user. So, who needs cyber security? Use of this technology has threats in some of the following areas. Malware (viruses and warms and spread unknowingly) may cause impact on cyber space and infect the system, spyware, virus fight, fishing attacks, cyber crimes, cyber law ethics etc. Cookies may misuse our personal data and information. This presentation dwells on cyber crime, a few coding and decoding of secret messages. This has severed damages to persons and locates the location of target field, to terrorize people in general and generate hatred.

Cyber theft is related to the culprits who steal financial and personal information to make illegal and fraudulent activity. Selected brains are appointed to make it realise. Hacking, damaging data, inputting virus etc, are their mode of operation. The so called activists conceal their identity and get protection from legal action. It is

capable of initiating cyber war to frighten the legal user. Here, I am giving an example how the activists misuse their learning. Everyone or one may be using this method but by some coded information. Though coding is done to lock the information for quite some time, but it let me design my own coding system. One may use it for own security not for any crime. I want to say meet me. Instructions are use binary number system. For first coded information use up to down sequence and for second use right to left. Significant figure is O in both cases. So, I can code and decode information for meet me.

m	z	J	7	S	E	E
x	N	O	P	E	E	R
J	A	M	S	U	N	N
O	M	E	C	O	I	R
2	2	E	7	3	C	1
Q	U	T	S	T	I	N
9	7	8	3	R	A	T

First I wrote what I want to convey by leaving gap to write O. For up to down there is following words. Since significant figure is O we need to start from there. One is 2 Q 9, next is M E E T, and third is 3 T R. For second word, the available words in the rows are P E E R, M E, I R. The word that should follow MEET is PEER or ME only. You can try to see what should be on the cards. Now if I want to convey my car/vehicle number in 4 columns. In binary system significant number is one and other symbols have zero value. My significant number is M.

3	S	D	C	B
Q	E	U	O	N
M	C	T	N	r
U	O	M	E	M
Q	N	9	p	M
R	d	M	M	M

We need to consider only four columns where M exist. The columns are 1, 3, 4 and 5. First column says 1 0 0 0 i.e., 8. Third column says 1 0 0, i.e.,3. Fourth column says 1 which is equal to 1. Fifth column is 111 i.e. 7. So my vehicle number is 8315. We need to know information and use it but not at the cost of problem to any individual or country. Spying for a country is as harmful as Jaichand, XXX, etc, who made loss to several kingdoms.

VI. CONCLUSION

Cyber space also called cybernauts is always prone to be in danger zone. Our device connected to internet is always vulnerable to cyber-attacks. Every day these attacks are comes in a variety of ways as attackers become more and more inventive. These attacks not only comes from the hackers but also from the various advertiser and e-commerce companies, who interested to know about our network access pattern, our internet habits, our choice, our preferences etc. Without the permission of user, even browser, search engines leaks our internet behavior and sends it to various interested groups. Cyber criminals, in variety of ways always try to find out our personal identification data, passwords etc. to make identity/ bank frauds. But the situation always be not such

disappointing, if we follow cyber-ethics. The word cyber ethics refers to a code of safe and responsible behavior in the internet. Changing the online habits by adopting safe browsing habits can prevent the user from cyber attacks. These safe browsing habits includes disabling the use of remembering password and other form information by the browser, beware of fake pop-ups, not to open unknown email attachments or respond to unknown emails, do not send personal data via email, cleaning browsing history from the public computer, not to access important account on public computer, use of two factor authentication to logging into any personal account, use of super strong and unique password, not to use the same password for the multiple services, not to click unknown links to prevent malicious software, use of authorized and authentic software and apps, careful reading of permissions before installing apps, keeping software up-to-date, not to access the unauthorized and/or porn websites to prevent phishing attempts etc.

REFERENCES

[1] Young A., Young M., "Crypto-virology: Extortion-Based Security Threats and Countermeasures," IEEE Symposium on Security & Privacy, pp. 129-141, 1996.

[2] Snorre Fagerland, Sylvia Moon, Kenneth Walls, Carl Bretteville, "The Norman Book on Computer Viruses", Published in October 2001.

[3] Peter Mell, Karen Kent, Joseph Nusbaum, "Guide to Malware Incident Prevention and Handling", NIST Special Publication November 2005,USA.

[4] Stalling ,William "Cryptography and Network Security", Fourth Edition, Pearson Prentice Hall, Published in 2006.

[5] Singh Brijendra, "Network Security and Management", Prentice Hall of India Private Limited, New Delhi-110001, Published in 2007.

[6] Stalling, William "Network Security Essentials application and standards", Third Edition, Pearson Prentice Hall, Published in 2008.

[7] www.wikipedia.org, Retrieved on August 2017.

[8] www.indiacode.nic.in, Retrieved on December 2017.

[9] https://digitalguardian.com/blog/what-cyber-security; Retrieved on 30 March 2018.

[10] https://www.itgovernance.co.uk/what-is-cybersecurity; Retrieved on 02 April 2018.