Privacy and Security Issues in Cyber World

Arun Dabas
Lecturer
Integrated Institute of Technology, Dwarka, Delhi, India
dabas99@yahoo.com

Abstract : *the Internet connectivity and speed is increasing over a period of time . Improved hardware with enhanced computational capatibility is being designed. Many small portable devices search as hand held devices are becoming popular with Internet support. With the increase in Internet connectivity the risk of various cyber attacks are increasing. Issues related to data and privacy are matter of concern. with the increased Internet services the data storage may be with third party service providers which increases the risk of data privacy and data theft at large. with enhanced Internet services the popularity of using e- commerce and banking services using cyber devices is increasing. These services may involve financial transactions which makes innocent users a soft target for cyber attacks. In this paper I am trying to identify the privacy and security issues involved in present day cyber world.*

Key words : Cyber , Privacy, data security, cyber crime.

1. Introduction:

The commercial use of Internet started sometime in January 1990. the usage of Internet is increasing rapidly since 1990. The Internet is capable of providing information required by the user without many efforts, in early days of Internet, the most of Internet services were paid and more costly as compared to today. As the time passed, the Internet services start becoming cheaper. Moreover many companies start working to introduce Internet services in hand held devices. With the increase in Internet ready hardware, the popularity of using Internet increased in a big way. With the increase in usage of Internet services, the risk of cyber crimes start increasing. People of every age group are indulging in usage of Internet services. the Internet services can be accessed anywhere around the world. There are various Internet services available worldwide such as banking services, e- commerce, e- learning , tour and travel, healthcare services, communication etc. To operate these services, the Internet connectivity may be required.

A little broader, cyber world or cyberspace which comprises services using digital systems to share, store, and process the information. These services are having no boundaries, and maybe accessed and used from anywhere irrespective of physical location. Since these services are Open Access, many people are using these services simultaneously. There are different types of users' categories, some users are ethical users and a few users may be threat to the whole Internet usage community. There is different kind of threat to different set of users. Since the Internet operations are global in nature, the cyber crime may be committed from anywhere irrespective of country, location etc. Any crime committed using computer or electronic device, peripheral or

involvement of any such device is termed as cyber crime. With the exponential growth of Internet usage, cyber crime is also growing at equal pace or even faster than usual.

Any crime needs to be booked under certain law of the land. Similarly the cyber crimes also need to be booked under appropriate cyber laws of the land along with IPC and CrPc in India. To handle cyber crimes information technology act 2000 came in to effect in the year 2000. the information technology amendment act 2008 also known as IT AA act 2008. It was an amendment to IT act 2000. Any crime related to cyber crime committed in India is booked under the provisions of IT act 2000 and IT AA act 2008.

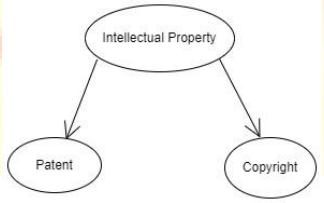
There are various provisions in IT Act. Such as Section 43A. Specifies the "Compensation for failure to protect data", it is the duty of corporate or person who is managing or storing the data to protect and secure the data. Section 65 "Tampering with computer source documents", any person who tempers or tries to temper any code of a program or source code etc. Section 66 mentions "Computer related offences". Section 66 A deals with the sending offensive messages over electronic devices. There are many other important provisions in the act.

2. Issues in Cyber World

There are different types of cyber crimes such as data theft, identity theft, impersonation, copyright, child abuse, online bullying, data privacy, virus threats, password related issues etc. even after having the law in place, there are many challenges to handle such cases.

Domain name issues - there are increasing cases where disputes related to domain names exist. Practically domain names are registered to anyone who applies for that specific domain name depending upon the availability. These domain names are used for commercial purpose to access the information. The issue or dispute arises when someone acquires the domain name and the same trademark lies with someone else. Many people register domain names of different brands and famous commercial establishments in bulk and then resale them after negotiations and getting lots of money. In the case of failed negotiations the matter goes to the court of law, in many cases it takes lots of time to decide the case and the litigation charges involved in it.

Intellectual Property -



Intellectual property is the creation of mind, art work, literature written by someone, design made by an individual or any other work which is creation of someone's mind comes under intellectual property. An individual has the sole right on such work. There are two categories of intellectual property, Patent and Copy right. Patent is the exclusive rights over some creation, design research work etc. And copy right is exclusive rights given to someone to copy, distribute etc.

There are certain issues related to intellectual property. Many people who are not having appropriate rights, misuse intellectual property rights and copy rights. Such persons are liable for prosecution. But the issue is that such people are very difficult to be caught and prosecuted.

Jurisdiction - is one of the main issues in the cyber world. As mentioned earlier the cyber crimes are committed across the world. The victim is physically present in one country and the cyber criminal is present physically in another country to commit the crime. In that situation it is quite difficult to prosecute or book that person. This has become a major issue in cyber world. Geographic and country boundaries are major hindrances in registering legal case, prosecute and put on trial in different country. Many criminals are taking benefits of this issue and committing crimes in countries other than their own country, particularly financial frauds and economic offences.

Financial Frauds using Cyber media: Financial frauds are one of the leading crimes in cyber space worldwide. Many hacker and cyber fraudsters keep on identifying weak points or loop holes in software systems and misuse these weak points in financial frauds. In many cases they target vulnerable group of people, who are either less proficient in using computer systems or they steal / cheat login- password details from these people by putting them in trap using one method or another.

Data Theft – Data theft is an act in which the sensitive information related to a person or a group of persons is transferred or taken away illegally without legitimate permissions. Many times hackers illegally log into data servers of individuals and organisations and steal the information. Data is one of the prime components for operation of any organisation. Stealing operational information from any organisation directly impacts the credibility of any organisation. This is one of the sensitive issues. Organisations invest ample amount on security systems to safeguard their data. Financial institutions, research and development establishments, security agencies are most prone to data theft issues.

Identity Theft - identity theft occurs when someone steals the identity details of an individual and uses that information for identification purposes. The main moto of using this stolen identity is to commit crime or fraud activities. These criminals steal the identity so that they are not caught while committing the crime. The only way to prevent identity theft is to keep personal information secure and not to share with anyone.

Impersonation - is the act of pretending to be someone else. Social media is very prone to impersonation. Unethical persons use impersonation tactics on social media to laid trap on innocent people. They behave as if they are their colleagues, Friends etc. and attack them with bad intentions. Impersonation is difficult to notice at initial stages, when identified, it becomes too late and damages have already been done by then.

Cyber bullying - cyber bullying happens when someone harasses someone else using Internet. Cyber bullying is seen in young people and is a matter of concern in terms of psychological and emotional fronts. This is a serious issue. Appropriate cyber literacy of vulnerable group may reduce cyber bullying cases.

Data privacy - data privacy is one such issue, which allows organizations to share information with third parties. There are data privacy laws in many countries, which regulate the privacy of

data and allow how much information may be shared with others. If not monitored or controlled properly, the quantum of information sharing cannot be controlled and the individuals are at risk of misusing their information.

Virus attacks and threats- virus is a wilfully written code of malicious program to cause some predefined destruction. Many cyber attackers write viruses to steal information from target systems. A virus is written and transferred to target computer and with the help of that information from target computer it is stolen.

Password Theft - many hackers steal password and login details from different sources. using these stolen logins and passwords they perform destruction. Password theft is quite common in financial frauds and economic offences. Not sharing login details, with anyone may somehow be helpful in keeping login details safe. Moreover frequent change of passwords may keep the password in safe position.

Cyber Crime Investigation and cyber forensic- Is the process which is performed after the cyber crime takes place. The purpose of cyber crime investigation is to investigate, how the crime took place .While investigating cyber crime, sensitive information is collected to verify the traces of cyber crime. Cyber forensic is used to collect evidences used in a cyber crime to identify actual sequence of operations involved in the cyber crime and devices used to perform such actions. There are several cyber forensic tools which help in gathering the information. Some forensic tools are used to recover password, data recovery etc. There are several cyber forensic tools used for specific purposes.

S**oftware piracy** is one of the most vulnerable issues. Software development is a very costly, time consuming and effort oriented affair. The software developer invests lots of efforts and money in software development process such that he may gain benefits out of it. The developed software is the sole ownership of the developer organisation or individual as the case may be.The cyber pirates steal the software and sell the software illegally to gain profit out of it.

Privacy issues - while using cyber world, we provide so much information. That information may be operational information or personal information of individuals. We provide our personal details such as particular information, health information, financial information, educational information etc.

Ones the information has been provided to any organization by any individual, the protection and safety of that data lies with that organization only. These organisations could be any Govt. agency, hospital, school, university, departmental store etc. sometimes these organisations fail to protect the data lies with them. And many times the integrity of the data is compromised.

3. Conclusion and Future Work :

The increasing popularity of Internet applications and easy accessibility of services anywhere in the world makes internet applications popular and powerful. Being Internet based service, there are certain security and integrity issues which need to be considered and addressed. I tried to identify and address major issues involving privacy, data theft, identity theft, risk of cyber attacks etc. I also tried to find out how hackers or cyber criminals identify weak points in cyber domain and target the innocent users. In my future work, I have planned to suggest strong

measures to safeguard from cyber attacks and hacking particularly where financial and economic transactions take place in large volume.
In future I have planned to work on security issues and to suggest secure and robust solution on security of cyber systems.

References:

[1] Cem Kaner, Department of Computer Sciences, Florida Institute of Technology, kaner@kaner.com, Holger Kienle, Department of Computer Science, University of Victoria, kienle@cs.uvic.ca, Scott Tilley, Department of Computer Sciences, Florida Institute of Technology, stilley@cs.fit.edu, *1st Workshop on Legal Issues of Documentation, SIGDOC '04,* October 10–13, 2004, Memphis, Tennessee, USA.
ACM 1-58113-809-1/04/0010.
[2] Nigel Wilson Barrister , Bar Chambers ,34 Carrington Street ,Adelaide South Australia 5000 Australia nigel.wilson@barchambers.com.au, *Forensics in Cyber-Space – The Legal Challenges, e-Forensics 2008*, January 21-23, 2008, Adelaide, Australia. © 2008 ICST 978-963-9799-19-6.
[3] Elisa Boschi ,Hitachi Europe, Zurich, Switzerland, elisa.boschi@hitachi-eu.com, *Panel Abstract: Legal Requirements and Issues in Network Traffic Data Protection, NDA'08,* October 31, 2008, Fairfax, Virginia, USA. ACM 978-1-60558-301-3/08/10.
[4] Maria Luisa Damiani Department of Informatics and Comunication University of Milan, Italy
damiani@dico.unimi.it, Pierluigi Perri School of Law University of Milan, Italy pierluigi.perri@unimi.it, *Privacy issues in location-aware browsing*
[5] Jody R. Westby, Esq.* Global Cyber Risk LLC 5125 MacArthur Blvd, NW; Third Floor Washington, DC 20016 USA + 1.202.255.2700 westby@globalcycberrisk.com, *Legal Issues Associated With Data Collection & Sharing.*
[6] Steven Fraser Independent Consultant Research Relations & Tech Transfer sdfraser@acm.org, Djenana Campara CEO and Co-Founder KDM Analytics djenana@kdmanalytics.com, Michael C. Fanning Principal Security Development Lead Microsoft Michael.Fanning@microsoft.com, Gary McGraw CTO *Cigital gem@cigital.com*, Kevin Sullivan Associate Professor University of Virginia sullivan.kevinj@gmail.com, *Privacy and Security in a Networked World*
[7] Hendrik Drachsler Open University of the Netherlands Welten Institute hendrik.drachsler@ou.nl ,Gábor Kismihók University of Amsterdam Center of Job Knowledge Research Amsterdam Business School G.Kismihok@uva.nl ,Weiqin Chen Oslo and Akershus University College of Applied Sciences Weiqin.Chen@hioa.no , Tore Hoel Oslo and Akershus University College of Applied Sciences tore.hoel@hioa.no Alan Berg University of Amsterdam ICT Services a.m.berg@uva.nl Adam Cooper University of Bolton CETIS a.r.cooper@bolton.ac.uk
Maren Scheffel Open University of the Netherlands Welten Institute Maren.Scheffel@ou.nl
Rebecca Ferguson The Open University Institute of Educational Technology rebecca.ferguson@open.ac.uk Jocelyn Manderveld SURF Jocelyn.Manderveld@surfnet.nl *Ethical and Privacy Issues in the Application of Learning Analytics*
[8] Anand Shah Tata Consultancy Services TRDDC, Hadapsar, Pune, Maharashtra +91 20 66086378 shah.anand@tcs.com Shishir Dahake Tata Consultancy Services

MIDC SEZ, Hinjewadi, Pune, Maharashtra +91 20 67940972 shishir.dahake@tcs.com Sri Hari Haran J Tata Consultancy Services TRDDC, Hadapsar, Pune, Maharashtra +91 20 66086204 sriharihara n.j@tcs.com , *Valuing Data Security and Privacy using Cyber Insurance*

[9] Isabel Borges Alvarez Universidade Autónoma de Lisboa Rua Santa Marta 56 1169-023 Lisboa, Portugal +351213177600 ialvarez@ual.pt Nuno S. Alves Silva Universidade Lusíada de Lisboa Rua da Junqueira, 188 a 194 1349-001 Lisboa, Portugal +351213611502 nsas@lis.ulusiada.pt Luisa Sampaio Correia ISCTE - Instituto Universitário Av. das Forças Armadas 1649-026 Lisboa, Portugal +351217903000 correia.mluisa@gmail.com, *Cyber Education: towards a pedagogical and heuristic learning*

[10] IT Act 2000

[11] IT Amendment Act 2008