MODULE (II)

Session-1: **OWASP Privacy preserving**: attacks to privacy, (spyware & backdoors, browser, email etc.)

Attacks to Privacy Overview

The emergence of the Internet in the late 1980s led to the evolution of cyberspace as a fifth domain of human activity and in last two decades, Internet has grown exponentially worldwide. India too has witnessed significant rise in cyber space activities and usage of internet so much so that it has not only become one of the major IT destinations in the world but has also become the third largest number of Internet users after USA and China. Such phenomenal growth in access to information and connectivity has on the one hand empowered individuals and on the other posed new challenges to Governments and administrators of cyberspace.

Cyber space has unique characteristics viz. anonymity and difficulty of attribution, coupled with enormous potential for damage and mischief. This characteristics not only adds to the vulnerabilities but also makes cyber security a major concern across the globe since it is being exploited by criminals and terrorists alike to carry out identity theft and financial fraud, conduct espionage, disrupt critical infrastructures, facilitate terrorist activities, steal corporate information and plant malicious software (malware) and Trojans. The emergence of cloud and mobile technology has further complicated the cyber threat landscape. Moreover, with the advent of sophisticated and malicious cyber tools physical damage on critical infrastructure and systems are inflicted and systematically information from targeted systems are stolen. All this makes cyber security an issue of critical importance with profound implications for our economic development and national security. Given the growing threats to cyber assets and all pervasive inter-connected information systems, countries around the world are engaged in actions for ensuring security of their cyber space.

Cyber security, a complex issue, cuts across domains and national boundaries and makes it difficult to attribute the origin of cyber-attacks. It, therefore, calls for a strategic and holistic approach requiring multi-dimensional and multi-layered initiatives and responses.

Nature of Cyber Space

The Cyber Space comprises of computer systems, computer networks and Internet. The latter includes Local Area Networks and Wide Area Networks. The Internet is a network of networks spread across the globe. Commercially, these computer systems are called servers, desktops, laptops, Personal Digital Assistants (PDAs), mobile computing platforms etc.

Unlike physical space, cyber space is anonymous and borderless. Once anybody is on Internet, he can access any system on Internet spread across the globe from anywhere. The cyber space offers virtual environment where anyone can hide his identity on the network and creates a pseudo name or can acquire some other identity. The security of the computer infrastructure is of greater importance under these conditions.

Risks in Cyber Space

As per the Background Note furnished by the Department, the risks in cyber space are manifold. They threaten personal data security-that is to say, they may undermine the individual's ability to control the information that they have entered into or stored on connective devices such as PCs, mobile telephones, or databases operated by commercial organizations, Government agencies and others. Victims typically suffer financial loss through fraud, though in cases of identity theft they may also suffer loss of reputation, or, in extreme cases, may be accused of crimes they did not commit. Online risks may also impact upon personal safety – it means that they may lead to direct physical or psychological harm to the individual. One recent high-profile threat is the one posed to children by predatory pedophiles, which conceal their true identity whilst using the Internet to "groom" potential victims. Probably far more common is the online bullying of children by their peers, while even adults who injudiciously disclose personal information online have found that their personal physical safety has been compromised and abused. As of now, it can be said that the benefits, costs and dangers of the Internet, are poorly understood and appreciated by the general public. The current assumption that it is end users' responsibility for security bears little relation either to the capabilities of many individuals or to the changing nature of the technology and the risk. The key contributors to online risks for an individual can be summarized as follows:

- Lack of knowledge
- Carelessness
- Unintentional exposure of or by others
- Flaws in technology – for instance, in the services offered online
- Criminal acts.

Types of Cybercrime/attack - methodology and impact

Most of the Internet frauds reported in the country are relating to phishing, usage of stolen Credit Cards / Debit Cards, unauthorized fraudulent Real Time Gross Settlement (RTGS) transactions, fictitious offers of funds transfer, remittance towards participation in lottery, money circulation schemes and other fictitious offers of cheap funds etc. When the Committee desired to know the mode of occurrence and prevention of various types of cyber-crimes existing/emerging around the world and in our country, the Department, in their written reply, furnished the following information: -

(spyware & backdoors, browser, email etc.)

Sl. No	**Type of Cyber Crime**	**Definition**	**Mechanism in which it is carried out**	**How it can be prevented/tackled**	
				Legal Measures as per Sections	**Technical and other Measures**

				Relevant in IT Act, 2000 and Amendments	
1.	Spyware	Stealthily following a person, tracking his internet chats.	By using electronic communication, such as e-mail instant messaging (IM), messages posted to a Web site or a discussion group.	43, 66 (Compensation and punishment of three years with fine)	Not disclosing personal information on Internet, chat, IM and interacting over electronic media with known people only. Taking up the matter with concerned Service Providers in stopping cyber stalking activities.
2.	Backdoors	Taking control of computer with the help of malware.	Compromising the computer systems	43, 66 (Compensation and punishment of three years with fine)	Securing computer systems and deploying anti-malware solution.
3.	email	Flooding an E-mail box with innumerable number of E-mails, to disable to notice important message at times.	Bulk email generation to target specific email account by using automated tools	43, 66 (Compensation and punishment of three years)	Implementing anti-spam filters
4.	Browser	Web Pages Defacing	Compromising the websites and adding or manipulating the web pages with some messages	43, 66 (Compensation and punishment of three years with fine)	Securing the websites and the IT infrastructure used for hosting and maintaining the websites

CYBER SECURITY AND RIGHT TO PRIVACY

As per the background note furnished on the subject, balancing cyber security, cybercrime and right to privacy is an extremely complex task due to the nature of the cyber space which is borderless. It requires the maturity and competence of seasoned professionals who have skills in multiple disciplines at the same time, namely technical (deep understanding of ICT and cyber security), protection (technical, process and administrative controls), legal and regulatory, constitutional, diplomacy, communication skills, public policy, psychology and economics to name a few.

Regarding measures that are in place for balancing privacy concerns while dealing with cyber threats, the Department, in the background note, submitted as under:-

"The Information Technology Act 2000 contains adequate provisions to deal with various cyber related offenses as well as protection of privacy of individuals. The following is a brief on such provisions in the Act:

• Section 43 and section 66 of the Information Technology Act, 2000 provides penalty and stringent punishment for hacking of website.

• Section 43A of the Information Technology Act, 2000 provides compensation to the affected person for failure to protect data

• The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 notified on 11th April, 2013 under section 43A of the Information Technology Act defines the sensitive personal data and reasonable security practices and procedures. The Rules require body corporate to provide policy for privacy and disclosure of information (Rule 4), obtain consent of user for collection of information (Rule 5), prior permission required from provider of information before disclosure of sensitive personal information (Rule 6)

• Section 72 of the Act provides penalty for breach of confidentiality and privacy

• Section 72A of the Act provides punishment for disclosure of information in breach of lawful contract."

In reply to an unstarred question (No.1969) replied in Lok Sabha on 5th December, 2012, as to whether the Government proposes to introduce relevant law/rules for unauthorized sharing of personal information and its disclosure and make it as a cognizable offence, the Minister of State for Communications and Information Technology stated as under:-

"Section 43A of the Information Technology Act, 2000 and Rules notified there under establishes a legal framework for data privacy protection in India. It mandates body corporate to implement reasonable security practices, framework for mode of collection, transfer and disclosure of sensitive personal data or information. Further, section 66C and 72A of the Information 45

Technology Act, 2000 provides for punishment and penalty for identity theft and breach of confidentiality and privacy respectively."

When the Committee desired to know the adequacy of the existing provisions in the law so as to address the issue of right to privacy, the Department in their written reply submitted as under: -

"xxx…xxx...xxx…Department of Personnel and Training is engaged in evolving legislation to address concerns of privacy, in general in country. The proposed legislation together with section 43A of the Information Technology Act, 2000 is expected to address all concerns of privacy in the cyberspace and in general."

Further, on being asked whether any study has been conducted by the Government to estimate the extent of privacy breach and type of breaches happening due to cyber-crime, the Department, in their written reply, submitted as under: -

"Government has not conducted any study to estimate the extent of privacy breach and type of privacy breach happening due to cybercrime. However, Data Security Council of India (DSCI), an industry association of NASSCOM has been engaged in conducting such a study focusing on privacy breach.

1.100Elaborating on the issue of cyber security and Right to privacy, the Secretary, DeitY, during evidence, submitted as under: -

"Regarding personal information and the right to privacy already, the IT Act, section 43A and 72A has got provisions to safeguard the personal information in the sense that if any organization which is in possession of the private personal information of the individuals, reveals to other without consent of the individual, it is a punishable offence under the IT Act with imprisonment of up to three years. If any such case comes to the notice, immediately cognizance can be taken. It is already provided under section 72A. So, the companies are obliged to keep confidentiality of the personal information of individuals. Apart from the legal provisions, more workable and more operative thing is the fact that India is one of the top most countries in the world in terms of business processes outsourcing (BPO) operations.

So, a large number of IT companies in this country are receiving personal data of people from all over the world and they are processing that data as per their client's requirement without any major concerns or complaints. It is a question of survival also. If this information is traded by these companies, then obviously the reputation of the company as well as the country will be on stake. Hence, there is also available a commercial safeguard, a professional safeguard apart from the legal safeguard. That I would say regarding the privacy.

The third point is the fact that the Government of India is considering the enactment of a privacy law in the country. At present, it is at a draft stage. It is being piloted by the Department of Personnel for all the Ministries put together. So, it has substantive provisions relating to the personal data pertaining to the 46

residents of India. How the privacy of such information should be and shall be protected and what are the consequences if it is not protected – the provisions in this regard are also going to be enlarged, which are available to some extent in Section 43 of the IT Act."

The Director- General, CERT-In, during evidence, added as under: -

"With regard to right to privacy, ..x.x.x... Section 43A mandates the body corporates or the service providers to implement the best practices to protect the data leakage from their servers. As part of the Act we have defined what reasonable security practices the body corporate will have to implement. In the rules we have defined 'sensitive personal data information'. There are about ten parameters. There are credit card numbers, health details, financial details, biometric data, password, etc. Those ten parameters have defined.

As regard to personal information, ..x.x.x.. DoPT is evolving a general framework for the privacy law. So, personal information is a little wider aspect which may not come under the purview of Department of Electronics and Information Technology because it contains personal data which is not part of DeitY. We can be concerned only with the digital data. So, all those parameters which are seen as part of digital data, as part of the mandate of this Ministry, have been addressed in rules under Section 43A of the IT Act."

The reasonable best practices have been notified on 11th April, 2011 and many of the body corporates are implementing best practices. In case there is a leakage of data the victim again can file compensation or claim damages and the lower courts can award compensation up to Rs.5 crore and for the higher compensation the case can go to the higher courts or other competent courts there. That is Section 43. So, Section 43A and the rules published under that Section cover the entire privacy in case of digital data. These are being followed by UIDAI also and other organizations.

The entire Section 43A is based on self-regulation. Companies will have to implement those best practices, not only the notified best practices but if a cluster of organizations want to have their own best practices suitable for their business, they can get the best practices approved by the Department and they can implement those, notify on their website that these are the best practices they will follow and those practices can be audited by independent auditors, either those 44 or others. So, it is a complete process of self-regulation. Government does not want to come into the picture."

In the context of privacy of data, the Committee desired to know the Department's stand on the issue of surveillance by US and interception of data sent through e-mails. To this, the Secretary, DeitY, responded during the evidence as under: -

"Sir, about the US surveillance issue, there has been a debate, as you are aware, this morning in the Rajya Sabha itself and the hon. Minister has addressed this issue. He also emphasized that as far as the Government data and Government 47

mails are concerned, the policy, the copy of which I have given to the Committee earlier, is going to address a large part of it. Hopefully, by the end of this year, if it is implemented, the things will be absolutely safe and secure…x.x.x.x…In the reply, the Hon. Minister also said that we have expressed our serious concern about the reported leakages and in the name of surveillance, the data that has been secured from various private sources, internet resources by the US Government. We have expressed it formally to the Government of the US and also during the Secretary of State's visit a few weeks ago in India, this has been reinforced on a person to person basis. We have been assured that whatever data has been gathered by them for surveillance relates only to the metadata. It has been reiterated and stated at the highest

level of the US President that only the metadata has been accessed, which is, the origin of the message and the receiving point, the destination and the route through which it has gone, but not the actual content itself. This has been reiterated by them, but we expressed that any incursion into the content will not be tolerated and is not tolerable from Indian stand and point of view. That has been mentioned very clearly and firmly by our Government.