SAD LAB EXPERIMENT - 1

Aim: Study of different Laws and Standards of Cyber Security.

To do:

1. Cyber Security
2. Cyber Security Standards
    a. ISO used for computer networks
    b. ISO 2700 series
    c. IT Act
    d. Copyright Act
    e. Patent Law
    f. IPR
3. Cyber security Laws
    a. Indian Penal Code 1980
4. Payment Card Industry Data security Standards
5. General Data Protection Regulations
6. Cyber Security Guidelines
7. Cyber Attacks
8. Types of Cyber Attacks

Theory:

Cyber Security:

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- **Information security** protects the integrity and privacy of data, both in storage and in transit.
- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Disaster recovery and business continuity** define how an organisation responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organisation restores its operations and

information to return to the same operating capacity as before the event. Business continuity is the plan the organisation falls back on while trying to operate without certain resources.

- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organisation.

Cyber Security Standards:

A security standard is "a published specification that establishes a common language, and contains a technical specification or other precise criteria and is designed to be used consistently, as a rule, a guideline, or a definition." The goal of security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures. The Well-Written cybersecurity standards enable consistency among product developers and serve as a reliable standard for purchasing security products.

Security standards are generally provided for all organisations regardless of their size or the industry and sector in which they operate.

- ISO
- IT Act
- Copyright Act
- Patent Law
- IPR

Cyber Security Laws:

India has four predominant laws when it comes to cybersecurity:

- **Information Technology Act (2000):** Enacted by the parliament of India, the information technology act was made to safeguard the e-governance, e-banking, and e-commerce sectors; but now, its scope has been enhanced to encompass all the latest communication devices.
- **Indian Penal Code (IPC) (1980):** This cybercrime prevention act has primary relevance to cyber frauds concerning identity theft and other sensitive information theft.
- **Companies Act (2013):** With the companies act enacted back in 2013, the legislature ensured that all the regulatory compliances are covered, including e-discovery, cyber forensics, and cybersecurity diligence. The Companies Act provides guidelines for the responsibilities of the company directors and leaders concerning confirming cybersecurity obligations.
- **NIST Compliance:** The Cybersecurity Framework (NCFS), authorised by the National Institute of Standards and Technology (NIST), contains all the guidelines, standards, and best practices necessary to responsibly address cybersecurity risks.

ISO used for Computer Networks:

ISO refers to the International Organization for Standardization. The ISO is a non-governmental organisation that develops and publishes international standards to ensure consistency, compatibility, and interoperability in various industries, including computer networks.

ISO has defined several standards that are relevant to computer networks. Some of the key ISO standards used for computer networks include:

- **ISO/IEC 8802-x (IEEE 802.x):** This series of standards specify the local area network (LAN) and metropolitan area network (MAN) technologies. For example, IEEE 802.3 defines Ethernet, and IEEE 802.11 defines Wi-Fi.
- **ISO/IEC 11801:** This standard covers generic cabling for customer premises, including structured cabling systems used for Ethernet and other networking technologies.
- **ISO/IEC 7498-1:** This standard provides a framework for the Open Systems Interconnection (OSI) model, which defines a conceptual framework that standardises the functions of a telecommunication or computing system into seven distinct layers.
- **ISO/IEC 27000 series:** While not specifically related to networking protocols, this series of standards covers information security management systems (ISMS) and provides guidance on managing security aspects in networks and IT environments.
- **ISO/IEC 18000-6:** This standard deals with Radio Frequency Identification (RFID) for item management in supply chain applications, which has applications in certain types of computer networks.
- **ISO/IEC 10164:** This standard defines the Reference Model of Open Distributed Processing (RM-ODP), which is a framework for distributed systems and networks.

ISO 27000 series:

The need of ISO 27000 series arises because of the risk of cyber-attacks which the organisation faces. The cyber-attacks are growing day by day making hackers a constant threat to any industry that uses technology.

The ISO 27000 series can be categorised into many types. They are-

- **ISO 27001:** This standard allows us to prove the clients and stakeholders of any organisation to managing the best security of their confidential data and information. This standard involves a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving our ISMS.
- **ISO 27000:** This standard provides an explanation of terminologies used in ISO 27001.
- **ISO 27002:** This standard provides guidelines for organisational information security standards and information security management practices. It includes the selection, implementation, operating and management of controls taking into consideration the organisation's information security risk environment(s).
- **ISO 27005:** This standard supports the general concepts specified in 27001. It is designed to provide the guidelines for implementation of information security based on a risk management approach. To completely understand the ISO/IEC 27005, the knowledge of the concepts, models, processes, and terminologies described in

ISO/IEC 27001 and ISO/IEC 27002 is required. This standard is applicable for all kinds of organisations such as non-government organisations, government agencies, and commercial enterprises.

- **ISO 27032:** It is the international Standard which focuses explicitly on cybersecurity. This Standard includes guidelines for protecting the information beyond the borders of an organisation such as in collaborations, partnerships or other information sharing arrangements with clients and suppliers.

IT Act:

The Information Technology Act also known as ITA-2000, or the IT Act main aims is to provide the legal infrastructure in India which deal with cybercrime and e-commerce. The IT Act is based on the United Nations Model Law on E-Commerce 1996 recommended by the General Assembly of the United Nations. This act is also used to check misuse of cyber networks and computers in India. It was officially passed in 2000 and amended in 2008. It has been designed to give the boost to Electronic commerce, e-transactions and related activities associated with commerce and trade. It also facilitates electronic governance by means of reliable electronic records.

IT Act 2000 has 13 chapters, 94 sections and 4 schedules. The first 14 sections concerning digital signatures and other sections deal with the certifying authorities who are licenced to issue digital signature certificates, sections 43 to 47 provides penalties and compensation, section 48 to 64 deal with appeal to high court, sections 65 to 79 deal with offences, and the remaining section 80 to 94 deal with miscellaneous of the act.

Copyright Act:

The Copyright Act 1957 amended by the Copyright Amendment Act 2012 governs the subject of copyright law in India. This Act is applicable from 21 January 1958. Copyright is a legal term which describes the ownership of control of the rights to the authors of "original works of authorship" that are fixed in a tangible form of expression. An original work of authorship is a distribution of certain works of creative expression including books, video, movies, music, and computer programs. The copyright law has been enacted to balance the use and reuse of creative works against the desire of the creators of art, literature, music and monetize their work by controlling who can make and sell copies of the work.

<u>The copyright act covers the following:</u>

- Rights of copyright owners
- Works eligible for protection
- Duration of copyright
- Who can claim copyright

<u>The copyright act does not covers the following:</u>

- Ideas, procedures, methods, processes, concepts, systems, principles, or discoveries
- Works that are not fixed in a tangible form.
- Familiar symbols or designs
- Titles, names, short phrases, and slogans
- Mere variations of typographic ornamentation, lettering, or colouring

Patent Law:

Patent law is a law that deals with new inventions. Traditional patent law protects tangible scientific inventions, such as circuit boards, heating coils, car engines, or zippers. As time increases patent laws have been used to protect a broader variety of inventions such as business practices, coding algorithms, or genetically modified organisms. It is the right to exclude others from making, using, selling, importing, inducing others to infringe, and offering a product specially adapted for practice of the patent.

In general, a patent is a right that can be granted if an invention is:

- Not a natural object or process
- New
- Useful
- Not obvious

IPR:

Intellectual property rights is a right that allows creators, or owners of patents, trademarks or copyrighted works to benefit from their own plans, ideas, or other intangible assets or investment in a creation. These IPR rights are outlined in the Article 27 of the Universal Declaration of Human Rights. It provides for the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions. These property rights allow the holder to exercise a monopoly on the use of the item for a specified period.

Payment Card Industry Data security Standards:

The primary goal of PCI DSS is to safeguard and optimise the security of sensitive cardholder data, such as credit card numbers, expiration dates and security codes. The standard's security controls help businesses minimise the risk of data breaches, fraud and identity theft.

Compliance with PCI DSS also ensures that businesses adhere to industry best practices when processing, storing and transmitting credit card data. In turn, PCI DSS compliance fosters trust among customers and stakeholders.

The PCI Security Standards Council (PCI SSC) has created six major goals for PCI DSS:

- **Build and maintain a secure network and systems.** Credit card transactions must be conducted in a secure network. The security infrastructure should include firewalls that are strong and complex enough to be effective without causing inconvenience to cardholders or vendors. Specialised firewalls are available for wireless local area networks, which are highly vulnerable to eavesdropping and malicious attacks. Vendor-provided authentication data, such as personal identification numbers and passwords, should not be used on an ongoing basis.
- **Protect cardholder data.** Organisations adhering to PCI DSS must protect cardholder information wherever it's stored. Repositories with vital data, such as birth dates, mothers' maiden names, Social Security numbers, phone numbers and mailing addresses, must be secure. The transmission of cardholder data through public networks must be encrypted.

- **Maintain a vulnerability management program.** Card services organisations must institute risk assessment and vulnerability management programs that protect their systems from the activities of malicious hackers, such as spyware and malware. All applications should be free of bugs and vulnerabilities that might enable exploits in which cardholder data could be stolen or altered. Software and operating systems must be regularly updated and patched.
- **Implement strong access control measures.** Access to system information and operations should be restricted and controlled. Every person who uses a computer in the system must be assigned a unique and confidential identification name or number. Cardholder data should be protected physically, as well as electronically. Physical protection can include the use of document shredders, limits on document duplication, locks on dumpsters and security measures at the point of sale.
- **Regularly monitor and test networks.** Networks must be regularly monitored and tested to ensure security measures are in place, functioning properly and up to date. For example, antivirus and antispyware programs should be provided with the latest definitions and signatures. These programs frequently scan all exchanged data, applications, RAM and storage media.
- **Maintain an information security policy.** A formal information security policy must be defined, maintained and followed by all participating entities. Enforcement measures, such as audits and penalties for noncompliance, might be necessary.

General Data Protection Regulation:

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live and outside of the European Union (EU). Approved in 2016, the GDPR went into full effect two years later. Its aim is to give consumers control over their own personal data by holding companies responsible for the way they handle and treat this information. The regulation applies regardless of where websites are based, which means it must be heeded by all sites that attract European visitors, even if they don't specifically market goods or services to EU residents.

- The General Data Protection Regulation is a law that sets guidelines for the collection and processing of personal information from individuals.
- The law was approved in 2016 but didn't go into effect until May 2018.
- The GDPR provides consumers with more control over how their personal data is handled and disseminated by companies.
- Companies must inform consumers about what they do with consumer data and every time it is breached.
- GDPR rules apply to any websites regardless of where they are based.

Cyber Security Guidelines:

Cybersecurity guidelines are sets of best practices and recommendations designed to help individuals, organisations, and governments protect their digital systems, networks, and data from cyber threats and attacks.

Use Strong Passwords: Encourage users to create strong and unique passwords for each account, consisting of a mix of uppercase and lowercase letters, numbers, and special characters. Implement multi-factor authentication (MFA) wherever possible to add an extra layer of security.

- **Keep Software Up-to-Date:** Regularly update operating systems, applications, and security software to patch known vulnerabilities and protect against emerging threats.
- **Employee Training:** Educate employees and users about cybersecurity best practices, phishing awareness, and how to recognize suspicious activities or emails.
- **Data Encryption:** Encrypt sensitive data both at rest and during transmission to safeguard it from unauthorised access.
- **Network Security:** Implement firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor and control network traffic.
- **Regular Backups:** Regularly backup critical data and store it offline or in a separate location to ensure data recovery in case of a ransomware attack or data loss.
- **Mobile Device Security:** Enforce security measures on mobile devices, such as password protection, encryption, and remote wipe capabilities.
- **Incident Response Plan:** Develop a comprehensive incident response plan that outlines steps to be taken in case of a cyber incident and assigns responsibilities to team members.
- **Secure Wi-Fi:** Secure wireless networks with strong passwords, encryption (WPA2/WPA3), and use separate guest networks when needed.
- **Vendor Security:** Ensure that third-party vendors and suppliers follow cybersecurity best practices to prevent supply chain attacks.
- **Regular Security Assessments:** Conduct periodic security assessments, vulnerability scans, and penetration testing to identify and address weaknesses in the infrastructure.
- **Restrict Privileges:** Limit user access to systems and data based on the principle of least privilege to minimise potential damage from insider threats or compromised accounts.
- **Secure Development Practices:** Implement secure coding practices to prevent common software vulnerabilities.
- **Monitor and Audit:** Monitor network activity and log events to detect and respond to potential security incidents in real-time.
- **Compliance and Regulations:** Stay updated with relevant cybersecurity laws, regulations, and industry standards that apply to your organisation.

Cyber Attacks:

A cyber attack is an attempt to disable computers, steal data, or use a breached computer system to launch additional attacks. Cybercriminals use different methods to launch a cyber attack that includes malware, phishing, ransomware, man-in-the-middle attack, or other methods.

Types of Cyber Attacks:

- **Malware**

Malware is a term that describes malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then instals risky software.

- **Phishing**

  Phishing is the method of sending fraudulent communications that seems to come from a reputable source, usually through email. The goal is to steal or get sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is an increasingly common cyberthreat.

- **Man-in-the-middle attack**

  Man-in-the-middle (MitM) attacks, also called eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

- **Denial-of-service attack**

  A denial-of-service attack fills systems, servers, or networks with traffic that exhaust resources and bandwidth. That makes the system incapable of fulfilling legitimate requests. Attackers also use multiple compromised devices to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.

- **SQL injection**

  A Structured Query Language (SQL) injection happens when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

- **Zero-day exploit**

  A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. Zero-day vulnerability threat detection requires constant awareness.

- **DNS Tunnelling**

  DNS tunnelling utilises the DNS protocol to communicate non-DNS traffic over port 53. It sends HTTP and other protocol traffic over DNS. There are various, legitimate reasons to utilise DNS tunnelling. However, there are also malicious reasons to use DNS Tunnelling VPN services. They can be used to disguise outbound traffic as DNS, concealing data that is typically shared through an internet connection. For malicious use, DNS requests are manipulated to exfiltrate data from a compromised system to the attacker's infrastructure. It can also be used for command and control callbacks from the attacker's infrastructure to a compromised system.

Conclusion:

The study of different laws and standards of cybersecurity is essential for creating comprehensive and effective security measures, ensuring legal compliance, and safeguarding against cyber threats in an increasingly interconnected digital landscape.By understanding and implementing these laws and standards, organisations and individuals can better protect their sensitive data, mitigate risks, and foster a safer online environment for everyone.