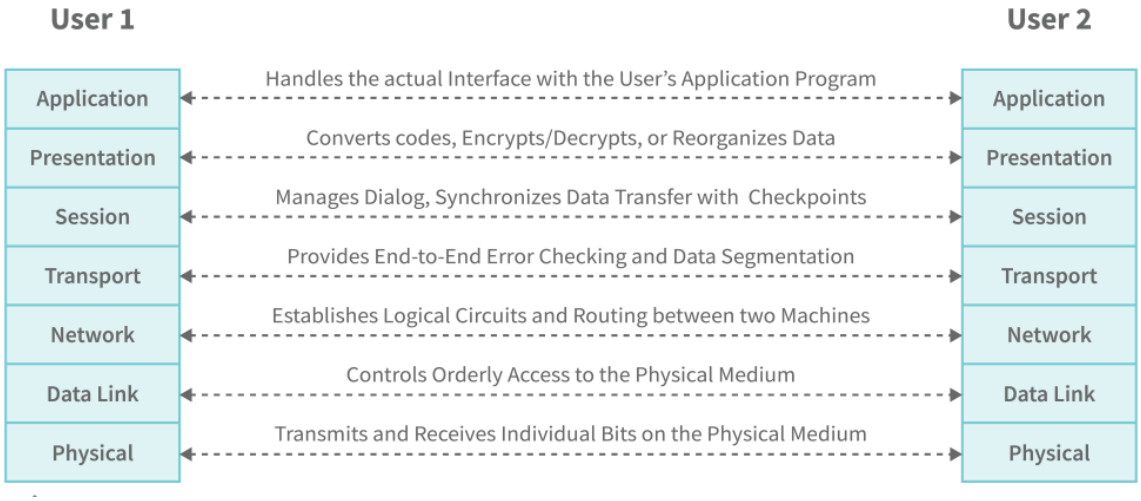
UNIT-I

OSI Security Architecture

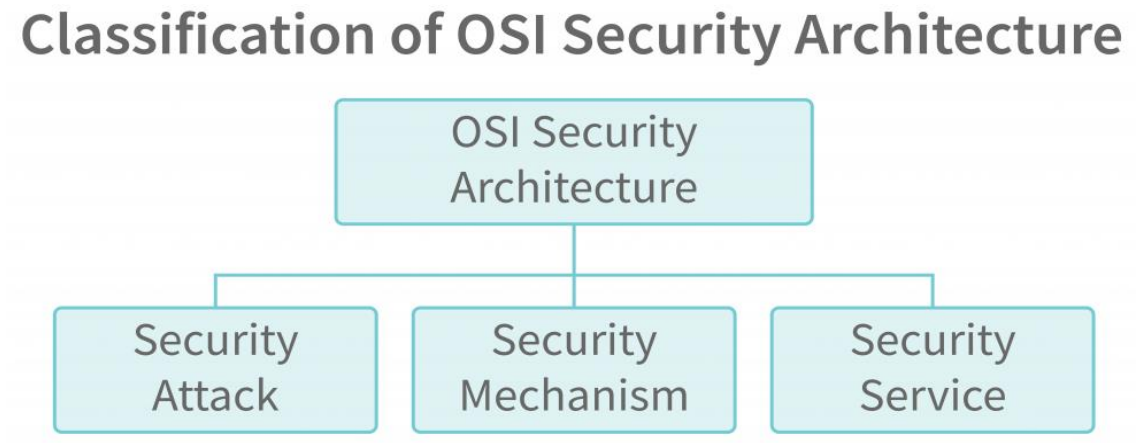
The **OSI security architecture** helps the managers responsible for the security of an organization in defining the requirements for security. The OSI security architecture was introduced as an 'international standard' which let the computer and communication vendor develop the products that have security features based on this architecture.

The OSI security architecture has a structure definition of services and mechanism for providing security to the organization's information.



OSI Security Architecture Defines:

1. Security Attacks
2. Security Mechanism
3. Security Services



Security Attacks

Security attacks can be defined as an action that risks the security of information owned by the company. X.800 and RFC 4949 classifies the security attack into two types as discussed below:

1. **Passive Attack**

In a passive attack, the attacker monitors or eaves drops the transmission between and sender and receiver and the attacker try to retrieve the information being transmitted. In passive attack neither the sender nor the receiver is aware of the attack as the attacker only retrieves the message, he doesn't perform any alteration to the captured message. The message is sent and received in the normal fashion.

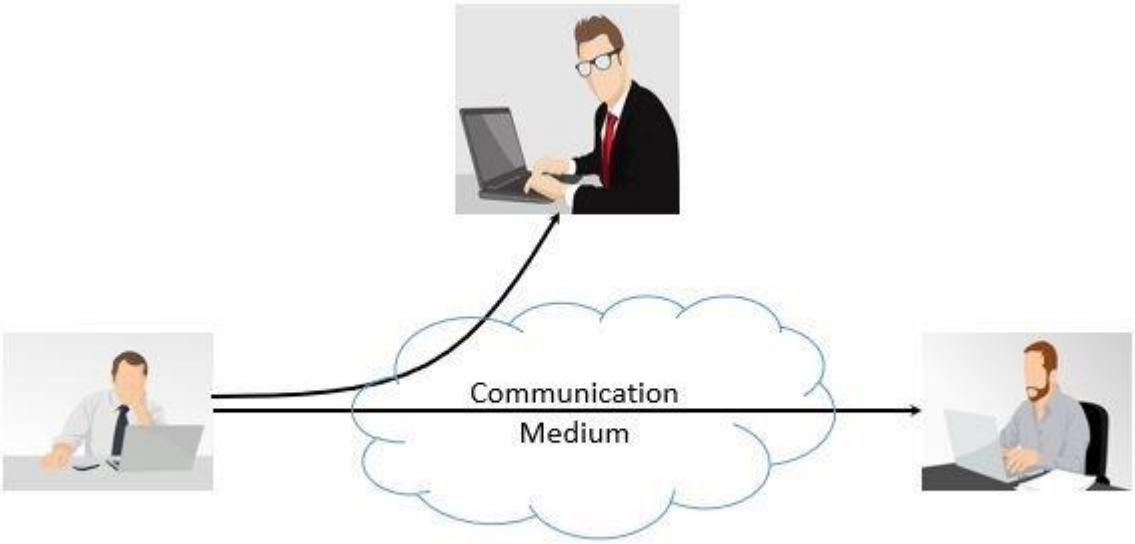


Figure 1. Passive Attack

Therefore, is more difficult to identify the passive attack. Though identification of passive attack is tedious, you can definitely implement encryption in order to prevent the success of this attack which means even if the attack happens the attacker is unable to extract the information.
The passive attack is further classified into two types.

Release of message content
The release of the message content is a kind of attack where the attacker listens to the telephone conversation, tracks electronic mail or the transferred file to retrieve the confidential message being transmitted. The opponent is quite interested in the content of the released message.

Traffic analysis
To protect the released message content the organization may apply a mask over the content of the message so that even if the attacker captures the message, he would not be able to understand the message. This technique of masking the released message is termed as encryption.
In traffic analysis passive attack, the attacker monitors the pattern, length and frequency of the released message to guess the original message.

Active Attack
We have seen that in the passive attack the attacker does not alter the message, but in the active attack the attacker alters, modify the transmitted message by creating a false data stream.

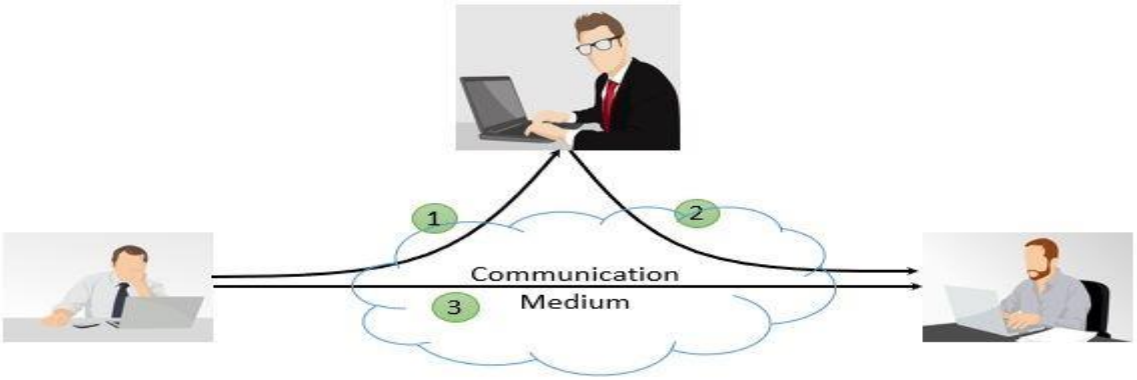


Figure 2. Active Attack

1. It is quite difficult to prevent the active attack instead the goal is to identify the source of active attack and apply a recovery measure.
   The active attack is further classified into four types

   - **Masquerade**
     In masquerade active attack, the attacker pretends to be the sender. To understand it better consider that in the above figure 2 only path 2 is active in masquerade attack.
   - **Replay**
     In the replay, the message is captured in a passive way and is retransmitted to produce an unauthorized effect. To understand replay, consider that in figure 2 path 1, 2 and 3 are active.
   - **Modification of message**
     Modification of message means some data stream of the message is altered or modified to create an unauthorized effect. Path 1 and 2 are active in this kind of attack.
   - **Denial of services**
     The attacker suppresses all the messages directed to a particular receiver by overloading the network to degrade the network performance

Security Mechanism
The security mechanism is an entire process that is specifically designed to identify the attack and develops a strategy to recover or prevent the attack.

Security Services
Considering X.800's security services the services can be classified into five categories as discussed below.

- **Authentication:** It assures that the entity involves in the communication is the one it is claiming for.
- **Access Control:** This service assures that only the authorized entities are accessing the resources and prevents unauthorized access.
- **Data Confidentiality:** This service manages to maintain the confidentiality of data by preventing the exposure of the message content to the attacker.

- **Data Integrity:** This service makes it sure that the data received at the receiver end is from an authorized entity.
- **Nonrepudiation:** This service restricts the sending and receiving entity from denying the transmitted message.

In all the OSI security architecture the things that need to be concentrated are security attack, service and mechanism to prevent the risk to the security of information of an organization.

Fundamental Security Design Principles

List of fundamental security design principles:

1. Economy of mechanism
2. Fail-safe defaults.
3. Complete mediation
4. Open design
5. Separation of privilege
6. Least privilege
7. Least common mechanism
8. Psychological acceptability
9. Isolation
10. Encapsulation
11. Modularity
12. Layering
13. Least astonishment

Brief Explanations:

1. **Economy of mechanism:**
Economies of mechanisms dictate that embodied security measures should be as simple, and as small as possible, both in hardware and software. The core principle of designing a simple security mechanism is to avoid unnecessary complexity.

2. **Fail-safe Defaults:**
The idea of fail-safe defaults means that access decisions should be driven by permission rather than exclusion. In other words, access is denied by default, and the protection scheme establishes conditions under which access is allowed.
The advantage of this approach is that it shows better failure modes than the alternatives.

3. **Complete mediation:**
In a complete mediation, every access must check with the access control mechanism. It is not recommended that systems rely on access decisions retrieved from caches.

4. **Open design:**
An open design for a security mechanism means that the design should be transparent rather than secret. As an example, while encryption keys must be secret, encryption algorithms should be open to public scrutiny.

5. **Separation of Privilege:**

In the separation of privilege Obtaining access to restricted resources requires multiple privilege attributes.
For example, with multifactor authentication, a user must verify his or her identity with more than one method, such as using a password and a smart card

6. **Least privilege:**
Each process and every user of the system should operate with the least amount of privileges necessary to accomplish the task.

7. **Least common mechanism:**
According to the least common mechanism, the design should minimize the functions shared by users while providing mutual security

8. **Psychological acceptability:**
A psychologically acceptable security system would not interfere with the work of users, while still meeting the requisites of those who authorize access

9. **Isolation:**
Isolation is a principle that applies in three contexts.
Firstly, public access systems should be separated from critical resources (data, processes, etc.) to prevent disclosure or tampering.
Second, individual users' processes and files should be isolated from one another, unless this is explicitly requested.
Last but not least, security mechanisms should be isolated so that they cannot be accessed.

10. **Encapsulation:**
Encapsulation can be stated as some specific form of isolation centered on object-oriented functionality.
It means the protection is provided by enclosing the collection of data and procedures in its domain and made only accessible to its internal calls within that system.
And these procedures are called only at designated domain entry points.

11. **Modularity:**
With the use of separate security modules, we aim to provide common security functions and services, such as cryptography, as common modules.
For example, Cryptographic functions are used in a variety of protocols and applications.
The development of a common cryptographic module that can be invoked by a variety of protocols and applications provides a more secure design than implementing these functions in every protocol or application

12. **Layering:**
Multi-layered protection refers to multiple, overlapping protection approaches that address the people, technology, and operational aspects of information systems.
By using this approach, protection failure at any point in the stack of functions will not expose and affect the whole system.
Multiple barriers are often used between a piece of protected information or service and an opponent. This method is commonly referred to as defence in depth.

13. **Least astonishment:**

In this principle, a program or user interface should always respond in a way that will be least likely to surprise the user.
For example, authorization mechanisms should be transparent enough to the user that he or she has a clear understanding of how the security goals map to the available security mechanisms.

Attack Surface and Attack Tree

Attack Tree: The main theme of attack tree is to structure the process of identifying threats in information security. In these attack tree we have several nodes like AND, OR and Leaf nodes which illustrates the process of identifying threats. Firstly we have to know the goals to complete an attack tree because these goals form trees with sub trees and nodes. This attack tree can be complex which depends upon the type of attacks.

Attack Surface: Attack surface is the total sum of separate points which can be easily accessible for a hacker or attacker. If a hacker wants to access the system he has to do by scanning the target's attack surface. These attack surfaces has three categories they are network, software, and physical attack surface. These attack surfaces can be reduced by reducing the codes.

Difference between Attack Surface and Attack Tree: Attack tree is very hard to understand when compared to Attack surface it's because of sub trees which we have in attack tree. Attack tree's structure can be long depending upon the goal and target whereas attack tree can be reduced by reducing the codes and by reducing access to untrusted users. Even though it is analyse understand attack tree provides simplest way for 6 analysing the security of systems. In attack trees we have AND, OR and Leaf nodes which describes the possible ways of goal. The more large attack surface is the more we have to make sure that the code is excellent and defensive.

A Model for Network Security

A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

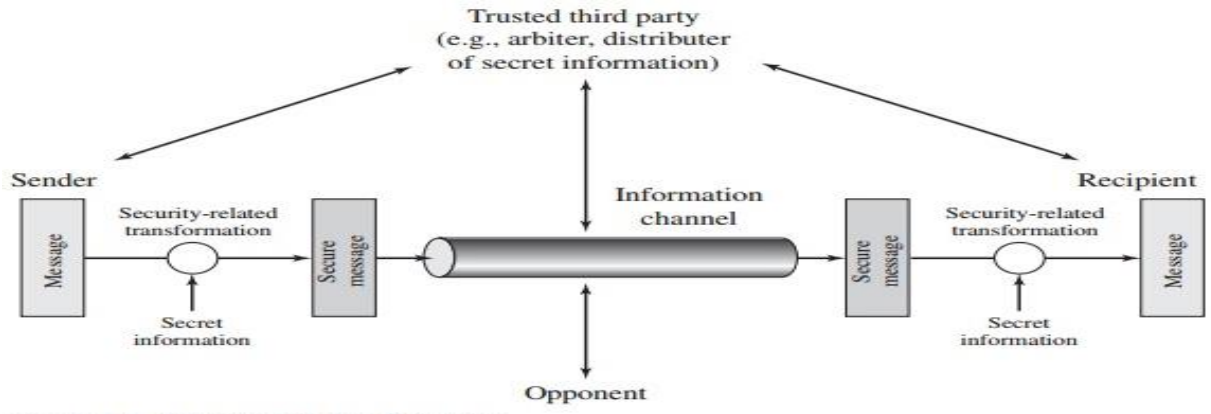


Figure 1.4 Model for Network Security

Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.6

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

- Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
- Generate the secret information to be used with the algorithm.
- Develop methods for the distribution and sharing of the secret information.
- Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

The types of security mechanisms and services that fit into the model shown in Figure 1.4. However, there are other security-related situations of interest that do not neatly fit this model but are considered in this book. A general model of these other situations is illustrated by Figure 1.5, which reflects a concern for protecting an information system from unwanted access. Most readers are familiar with the concerns caused by the existence of hackers, who attempt to penetrate systems that can be accessed over a network. The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system. The intruder can be a disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain
(e.g., obtaining credit card numbers or performing illegal money transfers).

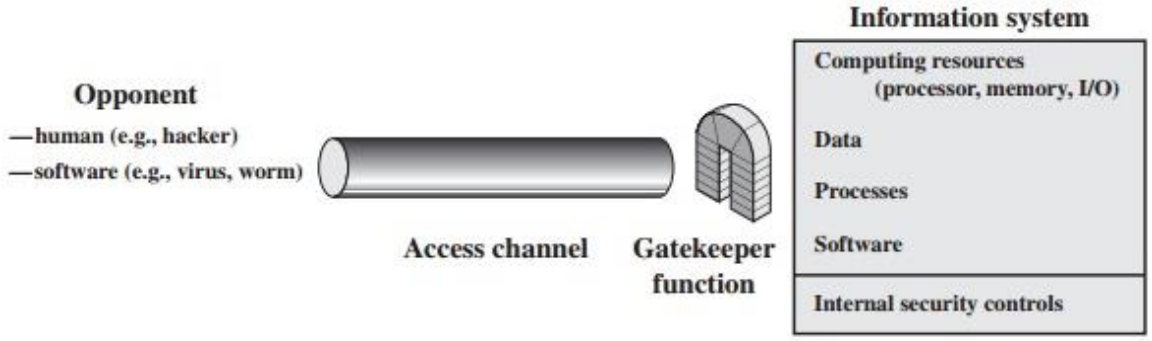


Figure 1.5 Network Access Security Model

Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application pro-grams as well as utility programs, such as editors and compilers. Programs can present two kinds of threats:

- **Information access threats:** Intercept or modify data on behalf of users who should not have access to that data.
- **Service threats:** Exploit service flaws in computers to inhibit use by legitimate users.

Viruses and worms are two examples of software attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic con-cealed in otherwise useful software. They can also be inserted into a system across a network; this latter mechanism is of more concern in network security.

The security mechanisms needed to cope with unwanted access fall into two broad categories (see Figure 1.5). The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyse stored information in an attempt to detect the presence of unwanted intruders.

Introduction to Cybercrime

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.

- Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.
- Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.
- Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

Most cybercrime falls under two main categories:

- Criminal activity that targets
- Criminal activity that uses computers to commit other crimes.

Cybercrime that targets computers often involves viruses and other types of malware. Cybercriminals may infect computers with viruses and malware to damage devices or stop them working. They may also use malware to delete or steal data. Cybercrime that stops users using a machine or network, or prevents a business providing a software service to its customers is called a Denial-of-Service (DoS) attack. Cybercrime that uses computers to commit other crimes may involve using computers or networks to spread malware, illegal information or illegal images. Sometimes cybercriminals conduct both categories of cybercrime at once. They may target computers with viruses first. Then, use them to spread malware to other machines or throughout a network. Cybercriminals may also carry out what is known as a Distributed-Denial-of-Service (D-Dos) attack. This is similar to a DoS attack but cybercriminals use numerous compromised computers to carry it out.

Nature and Scope of Cyber crime

Nature – Cybercrime is Transnational in nature. These crimes are committed without being physically present at the crime location. These crimes are committed in the im-palpable world of computer networks.

To commit such crimes the only thing a person needs is a computer which is connected with the internet. With the advent of lightning fast internet, the time needed for committing the cybercrime is decreasing. The cyberspace, being a boundary-less world has become a playground of the perpetrators where they commit crimes and remain conspicuously absent from the site of crime. It is an Open challenge to the law which derives its lifeblood from physical proofs and evidence. The cybercrime has spread to such proportion that a formal categorization of this crime is no more possible. Every single day gives birth to a new kind of cybercrime making every single effort to stop it almost a futile exercise. Identification possesses major challenge for cybercrime. One thing which is common it comes to identification part in cybercrime is Anonymous identity. It is quite an easy task to create false identity and commit crime over internet using that identity. Cybercrime being technology driven evolves continuously and ingeniously making it difficult for cyber investigators in finding solution related to cyber law crimes. Crimes committed over internet are very different in nature when compared to the physical world. In crimes relating to cyber space there is nothing sort of physical foot prints, tangible traces or objects to track cyber criminals down. Cybercrimes possess huge amount complications when it comes to investigation. There can be scenario where crimes committed over internet involve two or more different places in completely different direction of the world. This complicates the jurisdictional aspect of crimes relating to internet.

Scope – Cybercrime can be basically categorized into three parts:

- Cybercrimes against persons.
- Cybercrimes against property.
- Cybercrimes against government.

Cybercrimes against persons - Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be amplified.

Cybercrimes against property - The second category of Cyber-crimes is that of Cybercrimes against all forms of property. These crimes include computer vandalism (destruction of others' property), transmission of harmful programmes.

Cybercrimes against government - The third category of Cyber-crimes relate to Cybercrimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

Types of cybercrime

Here are some specific examples of the different types of cybercrime:

- **Email and internet fraud -** Email fraud (or email scam) is intentional deception for either personal gain or to damage another individual by means of email. Internet fraud is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them.
- **Identity fraud (where personal information is stolen and used) -** is the use by one person of another person's personal information, without authorization, to commit a crime or to deceive or defraud that other person or a third person.
- **Theft of financial or card payment data -** The purpose may be to obtain goods or services, or to make payment to another account which is controlled by a criminal.
- **Theft and sale of corporate data -** Data theft is the act of stealing information stored on corporate databases, devices, and servers. This form of corporate theft is a significant risk for businesses of all sizes and can originate both inside and outside an organization.
- **Cyberextortion (demanding money to prevent a threatened attack) -** Cyberextortion is a crime involving an attack or threat of an attack coupled with a demand for money or some other response in return for stopping or remediating the attack. Cyberextortion attacks start with a hacker gaining access to an organization's systems and seeking points of weakness or targets of value. While ransomware attacks can be automated through malware spread by email, infected websites or ad networks, these attacks tend to spread indiscriminately, and they may result in only a small percentage of victims paying the extortionists. More targeted attacks can produce less collateral damage while providing more lucrative targets for the extortion attempt.
- **Ransomware attacks (a type of cyber extortion) -** Ransomware is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever.
- **Cryptojacking (where hackers mine cryptocurrency using resources they do not own) -**Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency. Hackers do this by either getting the victim to click on a malicious link in an email that loads cryptomining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser.
- **Cyberespionage (where hackers access government or company data) -** Cyber espionage is a form of cyber-attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.

Cybercrime: An Indian Perspective.

REGULATIONS

There are five predominant laws to cover when it comes to cyber security:

Information Technology Act, 2000 The Indian cyber laws are governed by the Information Technology Act, penned down back in 2000. The principal impetus of this Act is to offer reliable legal inclusiveness to E-Commerce, facilitating registration of real-time records with the Government. But with the cyber attackers getting sneakier, topped by the human tendency to misuse technology, a series of amendments followed. The ITA, enacted by the Parliament of India, highlights the grievous punishments and penalties safeguarding the e-governance, e-banking, and e-commerce sectors. Now, the scope of ITA has been enhanced

to encompass all the latest communication devices. The IT Act is the salient one, guiding the entire Indian legislation to govern cybercrimes rigorously:

Section 43 - Applicable to people who damage the computer systems without permission from the owner. The owner can fully claim compensation for the entire damage in such cases.
Section 66 - Applicable in case a person is found to dishonestly or fraudulently committing any act referred to in section 43. The imprisonment term in such instances can mount up to three years or a fine of up to Rs. 5 lakh.
Section 66B - Incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years imprisonment. This term can also be topped by Rs. 1 lakh fine, depending upon the severity.
Section 66C - This section scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of three years might also be backed by Rs.1 lakh fine.
Section 66 D - This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.

Indian Penal Code (IPC) 1980
Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 - invoked along with the Information Technology Act of 2000. The primary relevant section of the IPC covers cyber frauds:

Forgery (Section 464)
Forgery pre-planned for cheating (Section 468)
False documentation (Section 465)
Presenting a forged document as genuine (Section 471)
Reputation damage (Section 469)
Companies Act of 2013

The corporate stakeholders refer to the Companies Act of 2013 as the legal obligation necessary for the refinement of daily operations. The directives of this Act cement all the required techno-legal compliances, putting the less compliant companies in a legal fix.

The Companies Act 2013 vested powers in the hands of the SFIO (Serious Frauds Investigation Office) to prosecute Indian companies and their directors. Also, post the notification of the Companies Inspection, Investment, and Inquiry Rules, 2014, SFIOs has become even more proactive and stern in this regard.

The legislature ensured that all the regulatory compliances are well-covered, including cyber forensics, e-discovery, and cyber security diligence. The Companies (Management and Administration) Rules, 2014 prescribes strict guidelines confirming the cyber security obligations and responsibilities upon the company directors and leaders.

NIST Compliance

The Cyber security Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), offers a harmonized approach to cyber security as the most reliable global certifying body.

NIST Cyber security Framework encompasses all required guidelines, standards, and best practices to manage the cyber-related risks responsibly. This framework is prioritized on flexibility and cost-effectiveness.

It promotes the resilience and protection of critical infrastructure by: Allowing better interpretation, management, and reduction of cyber security risks – to mitigate data loss, data misuse, and the subsequent restoration costs Determining the most important activities and critical operations - to focus on securing them Demonstrates the trust-worthiness of organizations who secure critical assets Helps to prioritize investments to maximize the cyber security ROI Addresses regulatory and contractual obligations Supports the wider information security program By combining the NIST CSF framework with ISO/IEC 27001 – cyber security risk management becomes simplified. It also makes communication easier throughout the organization and across the supply chains via a common cyber security directive laid by NIST.

Final Thoughts As human dependence on technology intensifies, cyber laws in India and across the globe need constant up-gradation and refinements. The pandemic has also pushed much of the workforce into a remote working module increasing the need for app security. Lawmakers have to go the extra mile to stay ahead of the impostors, in order to block them at their advent.

Cybercrimes can be controlled but it needs collaborative efforts of the lawmakers, the Internet or Network providers, the intercessors like banks and shopping sites, and, most importantly, the users. Only the prudent efforts of these stakeholders, ensuring their confinement to the law of the cyber land - can bring about online safety and resilience.

ROLE OF INTERNATIONAL LAWS

In various countries, areas of the computing and communication industries are regulated by governmental bodies

- There are specific rules on the uses to which computers and computer networks may be put, in particular there are rules on unauthorized access, data privacy and spamming
- There are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes
- There are laws governing trade on the Internet, taxation, consumer protection, and advertising
- There are laws on censorship versus freedom of expression, rules on public access to government information, and individual access to information held on them by private bodies
- Some states limit access to the Internet, by law as well as by technical means.

INTERNATIONAL LAW FOR CYBER CRIME

Cybercrime is "international" that there are ‘no cyber-borders between countries’

- The complexity in types and forms of cybercrime increases the difficulty to fight back fighting cybercrime calls for international cooperation
- Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale

THE INDIAN CYBERSPACE

Indian cyberspace was born in 1975 with the establishment of National Informatics Centre (NIC) with an aim to provide government with IT solutions. Three networks (NWs) were set up between 1986 and 1988 to connect various agencies of govt. These NWs were, INDONET which connected the IBM mainframe installations that made up India's computer infrastructure, NICNET (the NIC NW) a nationwide very small aperture terminal (VSAT) NW for public sector organisations as well as to connect the central government with the state governments and district administrations, the third NW setup was ERNET (the Education and Research Network), to serve the academic and research communities.

New Internet Policy of 1998 paved the way for services from multiple Internet service providers (ISPs) and gave boost to the Internet user base grow from 1.4 million in 1999 to over 150 million by Dec 2012. Exponential growth rate is attributed to increasing Internet access through mobile phones and tablets. Government is making a determined push to increase broadband penetration from its present level of about 6%1. The target for broadband is 160 million households by 2016 under the National Broadband Plan.

NATIONAL CYBER SECURITY POLICY

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology. It aims at protecting the public and private infrastructure from cyber-attacks. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This was particularly relevant in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. Ministry of Communications and Information Technology (India) defines Cyberspace as a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

VISION

To build a secure and resilient cyberspace for citizens, business, and government and also to protect anyone from intervening in user's privacy.

MISSION

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

OBJECTIVE

Ministry of Communications and Information Technology (India) define objectives as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

- To create an assurance framework for the design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
- To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.
- To enhance and create National and Sectorial level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.