Unit-1
Introduction to Cyber Security

- Concept of Cyber Security
- Cyber Crimes
- Types of Attacks in cyber
- Hacker Techniques

Introduction/ (Why cyber security is important?)

- We live in a digital era which understands that our private information is more vulnerable than ever before.
- We all live in a world which is networked together, from internet banking to government infrastructure, where data is stored on computers and other devices.
- A portion of that data can be sensitive information that can be intellectual property, financial data, personal information,
- An unauthorized access or exposure to that data could have negative consequences.
- Cyber-attack is now an international concern.
- And cybercrime is a global problem that's been dominating the news cycle.
- It poses a threat to individual security and an even bigger threat to large international companies, banks, and governments.
- Hacks and other security attacks could endanger the global economy and sensitive data is transmitted across networks and to other devices frequently.
- As the volume of cyber-attacks grows, companies and organizations, need to take steps to protect their sensitive business and personal information.
- And cybersecurity describes to protect that information and the systems used to process or store it.

Cyber:

- Merriam Webster defines cyber as:
  : of, relating to, or involving computers or computer networks (such as the Internet).

- "Cyber" is a prefix used to describe a person, thing, or idea as part of the computer and information age.
- The word "cyber" denotes a relationship with information technology (IT), i.e., computers. (It can relate to all aspects of computing, including storing data, protecting data, accessing data, processing data, transmitting data, and linking data.)
- The common words related with cyber are Cyber-attack, Cyber Crime, Cyber Space, Cyber Security etc.

Cyber Security:

- Cyber Security is the process of detecting and preventing any unauthorized use of our laptop/computer.
- It involves the process of safeguarding against hacker from using our personal or office-based computer resources with malicious intent or for their own gains, or even for gaining any access to them accidentally.
- Cybersecurity is the protection of Internet-connected systems, including hardware, software, and data from cyber-attacks.
- It is made up of two words one is cyber and other is security. Cyber is related to the technology which contains systems, network and programs or data.
- Whereas security related to the protection which includes systems security, network security and application and information security.
- It is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access. It may also be referred to as information technology security.
- A strong cybersecurity strategy can provide a good security against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data.

Ethics:

- Ethics is a system of moral principles.
- Ethics is concerned with what is good for individuals and society and is also described as moral philosophy.
- Ethics is the discipline concerned with what is morally good and bad and morally right and wrong.

Professional Ethics:

- Professional ethics are principles that govern the behavior of a person or group in a business environment.
- Like values, professional ethics provide rules on how a person should act towards other people and institutions in such an environment.

Cyber Crimes

- Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network.

- It is criminal activity that either targets or uses a computer, a computer network or a networked device.
- In this, computer is the object of the crime or is used as a tool to commit an offense.
- The illegal activities such as committing fraud, harassment, abuse, stealing identities and intellectual property, or violating privacy etc. are the example of cyber-crime.
- Cybercrime may threaten a person, company or a nation's security and financial health.
- A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device.
- Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.
- Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money.
- Cybercrime can also be carried out by individuals or organizations.
- Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others might be novice hackers.
- Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

Types of cyber-crime:

Hacking

- It is an illegal practice by which a hacker breaches the computer's security system of someone for personal interest. **Unwarranted mass-surveillance**
- Mass surveillance means surveillance of a substantial fraction of a group of people by the authority especially for the security purpose, but if someone does it for personal interest, it is considered as cybercrime.

Child grooming

- It is the practice of establishing an emotional connection with a child especially for the purpose of child-trafficking and child prostitution. **Copyright infringement**
- If someone infringes someone's protected copyright without permission and publishes that with his own name, is known as copyright infringement.

Money laundering

- Illegal possession of money by an individual or an organization is known as money laundering. It typically involves transfers of money through foreign banks and/or legitimate business. In other words, it is the practice of transforming illegitimately earned money into the legitimate financial system. **Cyber-extortion**
- When a hacker hacks someone's email server, or computer system and demands money to reinstate the system, it is known as cyber-extortion.

Cyber-terrorism

- Normally, when someone hacks government's security system or intimidates government or such a big organization to advance his political or social

objectives by invading the security system through computer networks, it is known as cyber-terrorism.

Online Scams

- These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

Types of attacks in Cyber/ Hacker Techniques

The most common types of attacks are given below:

1. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
2. Man-in-the-middle (MitM) attack
3. Phishing and spear phishing attacks
4. Drive-by attack
5. SQL injection attack
6. Cross-site scripting (XSS) attack
7. Malware attack
8. Ransomware attack
9. Brute Force attack
10. Session Hijacking
11. DNS Spoofing
12. Dictionary attack

1. **Denial-of-service (DoS) and distributed denial-of-service (DDoS) attack**

   It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash.

2. **Man-in-the-middle (MitM) attack**

   A MitM attack occurs when a hacker inserts itself between the communications of a client and a server.

3. **Phishing attacks**

   Phishing attack is the practice of sending emails, web pages or links that appear to be from trusted sources which attempts to steal sensitive information like user login credentials and credit card number etc.

4. **Drive-by attack**

   Drive-by download attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages.

5. **SQL injection attack**

SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server.

6. **Cross-site scripting (XSS) attack**

   XSS attacks use third-party web resources to run scripts in the victim's web browser or scriptable application. Specifically, the attacker injects a payload with malicious JavaScript into a website's database.

7. **Malware attack**

   Malicious software is an unwanted software that is installed in our system without our knowledge. The software is injected with malicious code and after installing it can send data to the attacker or damage our system.

8. **Ransomware attack**

   With ransomware, the victim's system is held hostage until they agree to pay a ransom to the attacker. After the payment has been sent, the attacker then provides instructions regarding how the target can regain control of their computer. The name "ransomware" is appropriate because the malware demands a ransom from the victim.

9. **Brute Force attack**

   It is a type of attack which uses a trial-and-error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number.

10. **Session Hijacking**

    It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

11. **DNS Spoofing**

    Domain Name System (DNS) poisoning and spoofing are types of cyberattack that exploit DNS server vulnerabilities to divert traffic away from legitimate servers towards fake ones.

12. **Dictionary attack**

    This type of attack stored the list of a commonly used password and validated them to get original password.

Unit-2
Security Technologies

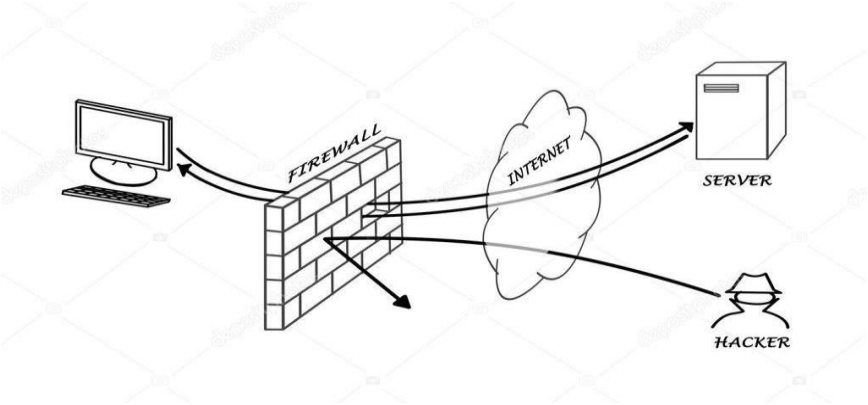
- Firewalls
- Virtual Private Networks
- Encryption
- Intrusion Detection

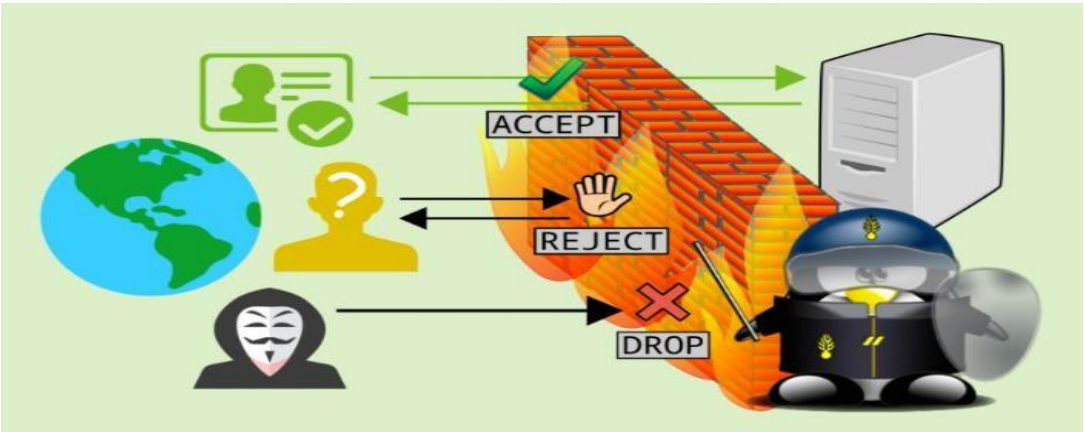
- Anti-Malicious Software
- Secure Software & Browser Security
- SSL and IPsec

Security technologies

- It is known to everyone that everything had two sides: pros and cons, and the same applies to the Internet as well.
- With the fast increase in Internet usage, the attacks happening in organizations have also been increased.
- For current business or organizations, a new challenge has been evolved that protects their body from cyber-attacks.
- So, we need security technologies to protect the organizations from cyberattacks so that the flow of their operations remains smooth.
- In this chapter some of the few securing technologies/techniques are discussed below.

Firewall





- A firewall is a network security system designed to prevent unauthorized access to or from a private network.
- A firewall can be hardware, software, or both.
- Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets.
- Firewall monitors and controls incoming and outgoing network traffic based on predetermined security rules.

- A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.
- Firewalls are used in both personal and enterprise settings, and many devices come with one built-in, including Mac, Windows, and Linux computers.
- They are widely considered an essential component of network security.

What Firewalls Do?

Basically, firewalls need to be able to perform the following tasks:

- Defend resources
- Validate access
- Manage and control network traffic
- Record and report on events

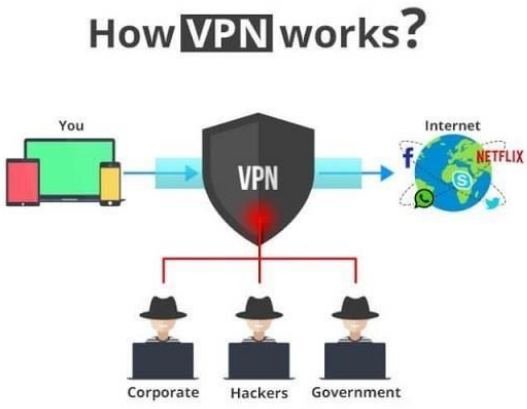
Advantages of firewall

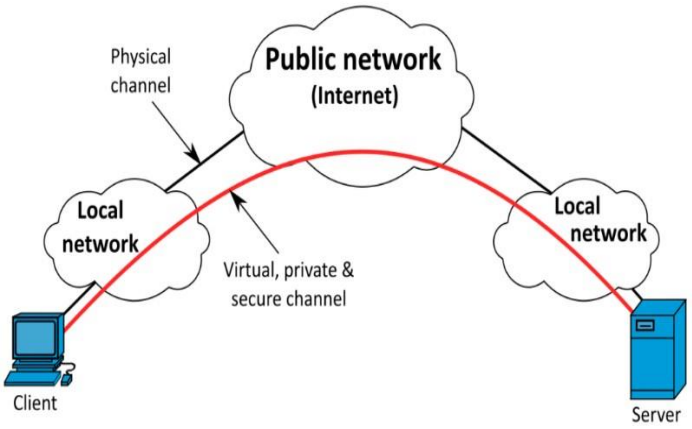
1. Network Isolation
2. Monitor Network Traffic
3. Protection against Trojans
4. Prevent Hackers
5. Access Control
6. Better Privacy

Disadvantages of firewall

1. Costly implementation
2. User Restriction
3. Reduced Performance
4. Defenseless against few other Malware Attacks

Virtual Private Network (VPN)





- A Virtual Private Network is a service that allows us to connect to the Internet via an encrypted tunnel to ensure our online privacy and protect our sensitive data.
- A virtual private network (VPN) extends a private network across a public network.
- It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
- Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network.
- VPN technology was developed to provide access to corporate applications and resources to remote or mobile users, and to branch offices.
- For security, the private network connection may be established using an encrypted layered tunnelling protocol, and users may be required to pass various authentication methods to gain access to the VPN.

What does VPN do? Application/Advantages of VPN

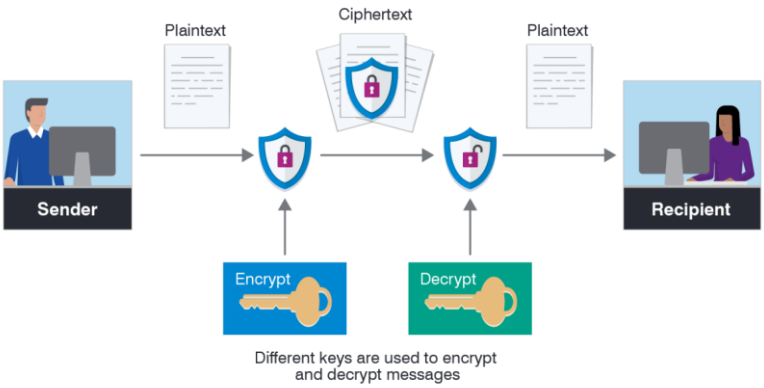
- **Hides IP address:** Masking our IP address is essential to becoming private online. A VPN makes sure that our city, country, and torrent download history aren't linked to our identity.
- **Protects us on public Wi-Fi**: A VPN encrypts our online data and helps to secure our personal information when we use free Wi-Fi in airports or anywhere else.
- **Unlocks blocked websites**: We can unblock sites by connecting to a VPN server in a different country. Access to various websites is restricted in many countries due to growing internet censorship or geo-blocking.
- **Protects online identity:** With VPN we can protect ourself from data theft, tracking, surveillance, and commercial targeting.
- **Secures crypto assets:** Encrypt our data and avoid malware. Make sure our wallet cannot be traced and identified via our IP address.
- **Access a Business Network While Traveling:** VPNs are frequently used by business travelers to access their business' network, including all its local network resources, while on the road. The local resources don't have to be exposed directly to the Internet, which increases security.

- **Access Home Network While Travelling:** we can also set up our own VPN to access our own network while travelling. This will allow us to access a Windows Remote Desktop over the Internet, use local file shares, and play games over the Internet as if we were on the same LAN (local area network).
- **Hides our Browsing Activity From our Local Network and ISP:** If we want to hide our browsing activity for a bit more privacy, we can connect to a VPN. The local network will only see a single, secure VPN connection.
- **VPN makes online gaming better.**
- **It protects against cyber-attack.**
- **VPN offers secure torrenting.**
- **VPN can bypass firewall.**
- **VPNs Might Help us Avoid Online Price Discrimination**

Disadvantages of VPN

- VPNs can sometimes slow down our online speeds.
- Using wrong VPN can put our privacy in danger.
- Quality VPN will cost more money.
- Not all devices natively support VPNs.
- VPNs may have legality issues in some regions.

Encryption:



- Encryption helps us to secure data that we send, receive, and store.
- It can consist text messages saved on our cell-phone, logs stored on our fitness watch, and details of banking sent by our online account.

- **Encryption** is the transformation of information from one form (plain-text) to another (cipher-text).
- **Decryption**, the opposite of encryption, is the transformation of encrypted information (cipher-text) back into an intelligible form (plain-text).

Types of Encryptions:

There are two types of encryptions schemes as listed below:

- Symmetric/Private Key encryption
- Asymmetric/Public Key encryption

Symmetric Key encryption

- Symmetric key encryption algorithm uses same cryptographic keys for both encryption and decryption of cipher text.

Public Key encryption

- Public key encryption algorithm uses pair of keys, one of which is a secret key and one of which is public. These two keys are mathematically linked with each other.

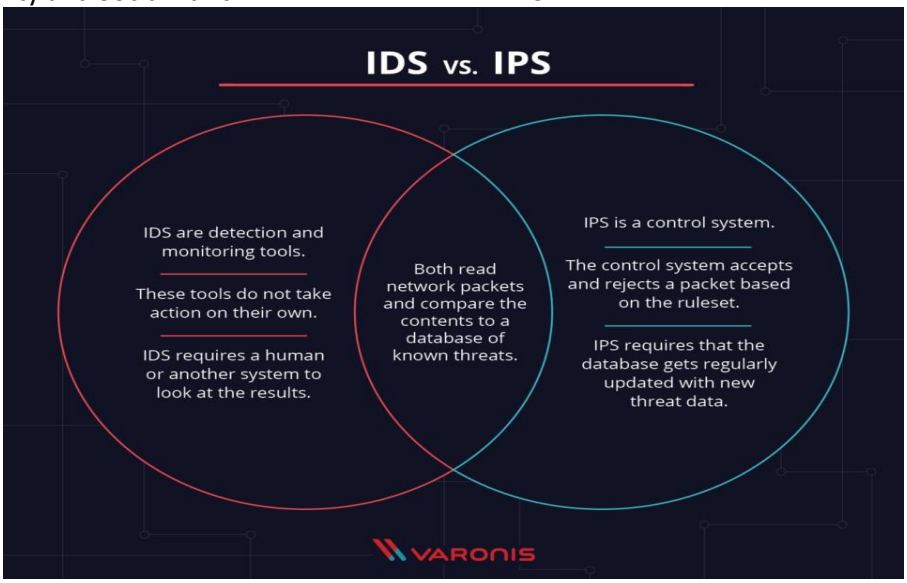
Advantages of encryption:

1. Encryption provides privacy.
2. Encryption helps move to the cloud.
3. When you own the keys, you can easily decommission/deprovision.
4. Encryption key services prevent service providers from accessing your data.
5. Encryption provides confidence that your backups are safe.

Intrusion Detection

- An intrusion detection is the process of monitoring network traffic for suspicious activity and issues alerts when such activity is discovered.
- Intrusion detection is usually performed with the system called Intrusion Detection System (IDS).
- IDS is a software application or hardware appliance that scans a network or a system for harmful activity or policy breaching.
- Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system.
- A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.
- These are classified as intrusion prevention systems (IPS).

Intrusion detection system vs Intrusion prevention system



Anti-Malicious Software

- An anti-malicious is a software that protects the computer from malware such as spyware, adware, and worms.
- It scans the system for all types of malicious software that manage to reach the computer.
- An anti-malicious program is one of the best tools to keep the computer and personal information protected.
- An anti-malicious is designed to eliminate malware from the computer.
- Although it has similarities with antivirus, an anti-malware program is different from antivirus.
- An anti-malware program has more advanced features and broader coverage. It addresses spyware, spam, and other threat issues that antivirus doesn't.
- Anti-malicious software is designed to find known viruses and oftentimes other malware such as Ransomware, Trojan Horses, worms, spyware, adware, etc., that can have a detrimental impact to the user or device.

Features of Anti-malicious Software

- Real Time Scanning
- Automatic Updates
- Protection for Multiple Apps
- Auto Clean
- Fight against all types of malwares
- Web and e-mail Protection

Benefits of Anti Malware Software

An anti-malware program has many benefits, particularly keeping your computer secure. But that's not all anti malware has to offer, you can benefit from anti malware in many ways.

- **You're protected from hackers** - hackers gain access to your computer through malware. With the anti-malware installed, you can browse the web safely.

- **Your privacy is protected** - cyber criminals use your personal information to their advantage. An anti-malware prevents any software that steal personal from installing.
- **Your valuable files are secured** - if malware and viruses are out of the computer, you can be assured that your data are protected.
- **Your software is up-to-date** - nobody wants outdated software. An anti-malware keeps your software updated. It will remind you if a new version or an update is available online.
- **Your computer is free of junk** - an antimalware notifies you if junks are consuming your computer memory, so you can free up some space. This eliminates useless files stored in your computer.

Secure software and Browser Security:

Secure Software

- The protection of data and programs used in computer system is known as software security.
- Software security provides barriers and other cyber-tools that protect programs, files, operation systems and the information flow to and from a computer.
- Software security is an idea implemented to protect software against malicious attack and other hacker risks so that the software continues to function correctly under such potential risks.
- Security is necessary to provide integrity, authentication and availability.

How to keep software safe

1. Protect Your Database from SQL Injection.
2. Validate Input Data Before You Use It or Store It.
3. Patch your software and systems.
4. Educate and train users.
5. Enforce least privilege (Permissions).
6. Monitor user activity.
7. Encrypt the data.
8. Use antivirus.

Browser Security:

Browser security is the application of Internet security to web browsers in order to protect networked data and computer systems from breaches of privacy or malware. Security exploits of browsers often use JavaScript, sometimes with cross-site scripting (XSS).

How to keep browser secure

- Keep your browser software up-to-date.
- Review your browser's security settings and preferences.
- If you do not need pop-ups, disable them or install software that will prevent pop-up windows. Pop-ups can be used to run malicious software on your computer.
- Install an adblocker.

- Install browser add-ons, plug-ins, toolbars, and extensions sparingly and with care.
- Private Web Browsing.
- Use VPN.

SSL and IPSec

SSL

- SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol.
- It is a networking protocol designed for securing connections between web clients and web servers over an insecure network and transmitting private documents via the Internet.
- It was first developed by Netscape in 1995 for the purpose of ensuring
  - Privacy
  - Authentication
  - Encryption
  - Integrity
  - Non-repudiability
- SSL is the predecessor to the modern TLS encryption used today.
- SSL has not been updated since SSL 3.0 and has been replaced by the Transport Layer Security (TLS) protocol.

SSL can be used to secure:

- Online credit card transactions or other online payments.
- Intranet-based traffic, such as internal networks, file sharing, extranets and database connections.
- Webmail servers like Outlook Web Access, Exchange and Office Communications Server.
- The transfer of files over HTTPS and FTP(s) services, such as website owners updating new pages to their websites or transferring large files.

IPsec

- IPsec is suite of protocols to provides security services during communications between networks.
- It supports network level peer authentication, data origin authentication, data integrity, data encryption and data decryption.

Key Features of IPsec are:

1. **Confidentiality**: by encrypting our data, nobody except the sender and receiver will be able to read our data.
2. **Integrity**: we want to make sure that nobody changes the data in our packets. By calculating a hash value, the sender and receiver will be able to check if changes have been made to the packet.
3. **Authentication**: the sender and receiver will authenticate each other to make sure that we are really talking with the device we intend to.
4. **Anti-replay:** even if a packet is encrypted and authenticated, an attacker could try to capture these packets and send them again. By using sequence numbers, IPsec will not transmit any duplicate packets.

Differences between IPSec and SSL

Sr. No.	Key	IPSec	SSL
1	Concept	IPSec, Internet Protocol Security, is a suite of protocols to provide security for internet protocol.	SSL, is a secure protocol to send information securely over internet.
2	Layer	IPSec works in internet layer of OSI model.	SSL works in transport and application layer of OSI model.
3	Configuration	IPSec is complex to configure.	SSL is simple to configure.
4	Usage	IPSec is used to secure VPN, Virtual Private Network.	SSL is used to secure web based communications/ transactions.
5	Installation	Installation is vendor neutral.	Installation is vendor specific.
6	Changes in OS	Changes required to OS during implementation.	No changes required to OS during implementation.
7	Changes to Application	No changes required to Application during implementation.	Changes are required to Application during implementation.
8	Location	IPSec is present in OS space.	SSL is present in User space.

Unit - 3
Information Security and Cryptography

- Classical Encryption Methods
- Asymmetric Key Cryptography
- Confidentiality, Integrity, Authentication and Non-Repudiation
- Digital Signature

Information security:

- Information security, sometimes shortened to infosec, is the practice of protecting information by reducing information risks.

- It is part of information risk management. It typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information.

Cryptography:

- The word 'cryptography' was coined by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing.
- Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it.
- Thus, preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".

Some Basic Terminology Some Basic Terminology

- **Plaintext** - original message.
- **Ciphertext** - coded message.
- **Cipher** - algorithm for transforming plaintext to ciphertext.
- **Key** - info used in cipher known only to sender
- **Encipher (encrypt)** - converting plaintext to ciphertext
- **Decipher (decrypt)**- recovering ciphertext from plaintext
- **Cryptography** - study of encryption principles/methods
- **Cryptanalysis (code breaking)**- study of principles/ methods of deciphering ciphertext without knowing key.
- **Cryptology** - field of both cryptography and cryptanalysis.

Classical Encryption Methods

1. Substitution Method
2. Transposition Method
3. Rotor Machines
4. Steganography

Substitution Method:

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

i. Caesar Cipher:

- This is the earliest known example of a substitution cipher.
- Each character of a message is replaced by a character three position down in the alphabet.
- plaintext: are you ready
- ciphertext: DUH BRX UHDGB

ii. Monoalphabetic and Polyalphabetic Cipher

- **Monoalphabetic cipher** is a substitution cipher, where the cipher alphabet for each plain text alphabet is fixed, for the entire encryption.
- In simple words, if the alphabet 'p' in the plain text is replaced by the cipher alphabet 'd'. Then in the entire plain text wherever alphabet 'p' is used, it will be replaced by the alphabet 'd' to form the ciphertext.

- **Polyalphabetic cipher** is far more secure than a monoalphabetic cipher. As monoalphabetic cipher maps a plain text symbol or alphabet to a ciphertext symbol and uses the same ciphertext symbol wherever that plain text occurs in the message. But polyalphabetic cipher, each time replaces the plain text with the different ciphertext.

iii. Playfair Cipher

- Playfair cipher is a substitution cipher which involves a 5X5 matrix. Let us discuss the technique of this Playfair cipher with the help of an example:
- Plain Text: meet me tomorrow
- Key: KEYWORD
- **Step 1:** Create a 5X5 matrix and place the key in that matrix row-wise from left to right. Then put the remaining alphabets in the blank space.

K	E	Y	W	O
R	D	A	B	C
F	G	H	I/J	L
M	N	P	Q	S
T	U	X	Y	Z

- Note: If a key has duplicate alphabets, then fill those alphabets only once in the matrix, and I & J should be kept together in the matrix even though they occur in the given key.
- **Step 2**: Now, you have to break the plain text into a pair of alphabets.
- **Plain Text**: meet me tomorrow
- **Pair**: me et me to mo rx ro wz Note
  - Pair of alphabets must not contain the same letter. In case, pair has the same letter then break it and add 'x' to the previous letter. Like in our example letter 'rr' occurs in pair so, we have broken that pair and added 'x' to the first 'r'.
  - In case while making pair, the last pair has only one alphabet left then we add 'z' to that alphabet to form a pair as in our above example, we have added 'z' to 'w' because 'w' was left alone at last.
  - If a pair has 'xx' then we break it and add 'z' to the first 'x', i.e. 'xz' and 'x_'.

▪ **Step 3**: In this step, we will convert plain text into ciphertext. For that, take the first pair of plain text and check for cipher alphabets for the corresponding in the matrix. To find cipher alphabets follow the rules below. Note

- If both the alphabets of the pair occur in the same row replace them with the alphabet to their immediate right. If an alphabet of the pair occurs at extreme right then replace it with the first element of that row, i.e. the last element of the row in the matrix circularly follows the first element of the same row.
- If the alphabets in the pair occur in the same column, then replace them with the alphabet immediate below them. Here also, the last element of the column circularly follows the first element of the same column.
- If the alphabets in the pair are neither in the same column and nor in the same row, then the alphabet is replaced by the element in its own row and the corresponding column of the other alphabet of the pair.

- Pair: me et me to mo rx ro wz
- Cipher Text: kn ku kn kz ks ta kc yo

iv. Hill Cipher

- Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26 with a scheme A = 0, B = 1, …, Z = 25
- To encrypt a message, column vector n x 1 is multiplied key n × n matrix, against modulus 26.
- To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

Example:

- Plain Text: Hello
- Key: four

Step 1: create a matrix based on key $\begin{matrix} F & O \\ U & R \end{matrix}$ = $\begin{bmatrix} 5 & 14 \\ 20 & 17 \end{bmatrix}$

Step 2. Write the plain text as a column vector and write their corresponding number

- [h] [l] [oz] = [7 4] [11 11] [14 25] e l

Step 3: multiply each column vector with key matrix and find the mod 26 of each element

- $\begin{bmatrix} 5 & 14 \\ 20 & 17 \end{bmatrix} * \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 91 \\ 208 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 13 \\ 0 \end{bmatrix}$
- $\begin{bmatrix} 5 & 14 \\ 20 & 17 \end{bmatrix} * \begin{bmatrix} 11 \\ 11 \end{bmatrix} = \begin{bmatrix} 209 \\ 407 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 1 \\ 17 \end{bmatrix}$
- $\begin{bmatrix} 5 & 14 \\ 20 & 17 \end{bmatrix} * \begin{bmatrix} 14 \\ 25 \end{bmatrix} = \begin{bmatrix} 420 \\ 705 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 4 \\ 2 \end{bmatrix}$

Example
91/26=3.5-3=0.5*26=13
208/26=8-8=0*26=0

Step 4: convert the result column vector to their respective characters

- [13 0] = [na], [17 1] = [br], [4 2] = [ec]

Cipher Text = NABREC

v. One-time Pad

- One-time Pad (Vernam Cipher) is a method of encrypting alphabetic text
- In this mechanism we assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, … z = 25).
  In this algorithm, the length of the should be equal to the length of the plain text.

Example:

Plain text: Are you there
Key this is hello

Step 1: Assign the number for both plaintext and the key

Plain text:	A	R	E	Y	O	U	T	H	E	R	E
	0	17	4	24	14	20	19	7	4	17	4

Key:	T	H	I	S	I	S	H	E	L	L	O
	19	7	8	18	8	18	7	4	11	11	14

Step 2 : Add the number of plain text and number of key.

19	17	12	42	22	38	26	11	15	28	18	

Step 3: If the number is greater than or equal to 26 then subtract from 26 and rewrite

19	17	12	16	22	12	0	11	15	2	18	

Step 4: Write the alphabets for the corresponding character

T	R	M	Q	W	M	A	L	P	C	S

Cipher text= TRMQWMALPCS

2. Transposition Method

- Transposition Ciphers are a bit different to Substitution Ciphers.
- In a Transposition cipher, the letters are just moved around.
- The letters or words of the plaintext are reordered in some way, fixed by a given rule (the key).
- One of the examples for the transposition is given below **Plain Text:** meet me Tomorrow
- The plain text is written in diagonal form as given below

The first row : memtmro
The second row: eteoorw

- Combine first row and second row.
- **Cipher Text**: MEMTMROETEOORW

3. Rotor Machines

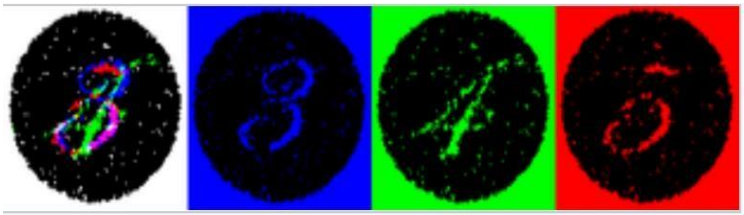
- Electric rotor machines were mechanical devices that allowed to use encryption algorithms that were much more complex than ciphers, which were used manually.
- They were developed in the middle of the second decade of the 20th century.
- They became one of the most important cryptographic solutions in the world for the next tens of years.
- The main idea that lies behind rotor machines is relatively simple.
- One can imagine a simple device, similar to a typewriter, with a number of keys used to input text produces some random text based on the machine's algorithm.

4. Steganography

- Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection.
- The secret data is then extracted at its destination.
- The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write).
- Since steganography is more of an art than a science, there is no limit to the ways steganography can be used. Below are a few examples:

i. Playing an audio track backwards to reveal a secret message

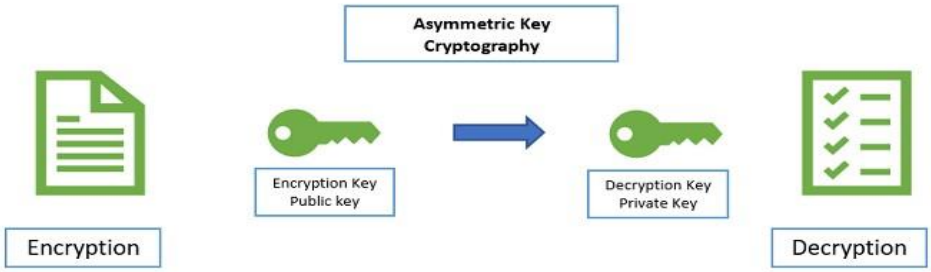
ii. Playing a video at a faster frame rate (FPS) to reveal a hidden image iii. Embedding a message in the red, green, or blue channel of an RGB image



The same image viewed by white, blue, green, and red lights reveals different hidden numbers.

Asymmetric Key Cryptography:

- Asymmetric Encryption, also known as Public-Key Cryptography is a relatively new concept.
- Unlike "normal" (symmetric) encryption, Asymmetric Encryption encrypts and decrypts the data using two separate yet mathematically connected cryptographic keys.
- These keys are known as a 'Public Key' and a 'Private Key.'
- One key, the Public Key, is used for encryption and the other, the Private Key, is for decryption.
- As implied in the name, the Private Key is intended to be private so that only the authenticated recipient can decrypt the message.



Goals of cryptography:

- Confidentiality
- Integrity
- Authentication
- Non-Repudiation

Confidentiality

- Confidentiality is most commonly addressed goal.
- The meaning of a message is concealed by encoding it.
- The sender encrypts the message using a cryptographic key.
- The recipient decrypts the message using a cryptographic key that may or may not be the same as the one used by the sender.

Integrity

- Integrity Ensures that the message received is the same as the message that was sent.
- Uses hashing to create a unique message digest from the message that is sent along with the message.

- Recipient uses the same technique to create a second digest from the message to compare to the original one.
- This technique only protects against unintentional alteration of the message.
- A variation is used to create digital signatures to protect against malicious alteration.

Authentication

- Authentication is verifying the identity.
- In other word you prove to the system that you are the person you claim to be by showing some evidence. For example, entering user id and password to login.

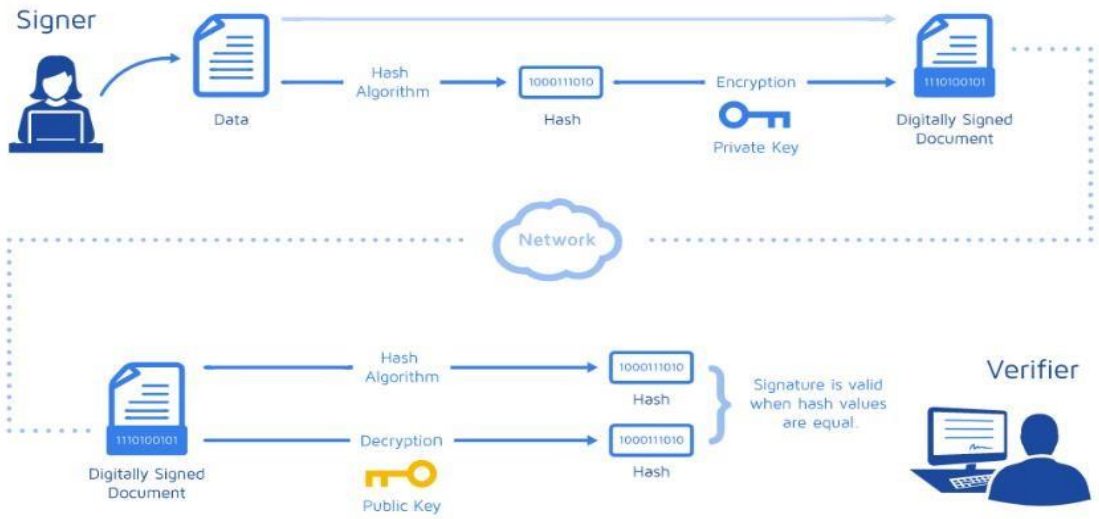
Non-Repudiation

- Nonrepudiation is the assurance that someone cannot deny something.
- Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Digital Signature:

- A digital signature is an electronic, encrypted, stamp of authentication on digital information such as email messages or electronic documents.
- A signature confirms that the information originated from the signer and has not been altered.
- It provides the highest levels of security and universal acceptance.

Working of Digital Signature



Sender's side

- When the sender electronically signs a document two keys are generated: Public and Private.
- The private key is kept by the signer and it should be kept securely. On the other hand, the receiver must have the public key to decrypt the message.
- Then the Hash function is used on the document to create Hash, which is also known as digest.
- Then the private key is used to encrypt hash.
- The document is sent to the recipients along with the sender's public key.

Receiver's side

- The recipient receives the document and decrypts the encrypted hash with the sender's public key certificate.
- A cryptographic hash is again generated on the recipient's end using the same hash function that the sender used.
- Both cryptographic hashes(of sender and receiver) are compared to check its authenticity.
- If they match, the document hasn't been tampered with and is considered valid.

Unit-4
Legal Issues in Cyber Crime

- Legal Issues in Information Security
- Cyber Law in Nepal
- Security Policy
- Managing Risk
- Information Security Process
- Information Security Best Practice

Legal issues in Information Security:

- It is true that any business operates in a legal environment.
- Liability, copyright, jurisdiction etc. are some of the legal issues related to information security.

Issues of copyright and trademarks:

- Internet Copyright and trademark violation fall under intellectual property law.
- Intellectual property includes software, music, videos, books, trademarks, copyright and web pages.
- Copyright is ownership of an original work created by the author.
- Trademark represents a symbol or picture that identifies the product or service is intellectual property.

Issue of jurisdiction:

- Jurisdiction is the official power to make legal decisions and judgements.
- The internet is beyond geographic borders, there are no laws or border on the internet.
- Different countries have a different legal system, criminal laws and consumer protection laws which makes e-commerce business difficult to run business over the internet.

Cyber Law in Nepal

Cyberlaw is the area of law which concerns computers and computer-related crimes.
It merges many legal sides including

- Internet law and regulations
- Telecommunication laws
- Software laws
- International laws
- Criminal law
- Intellectual property law etc.

And puts them into the context of computers.

Generically, cyber law is referred to as the Law of the Internet.

- Nepal's Cyberworld is ruled by the Electronic Transaction Act (ETA) 2063 that protects users online against cybercrimes.
- The Act is dived into 12 sections and 80 clauses. This law keeps an eye on issues which are related to computer networks and cybercrime.
- It brings cyber criminals under the justice of law and penalizes them just like other crimes. As per the Act, if anyone is found violating cybercrime, he/she will be punished for a minimum of 6 months to a maximum of 3 years in jail and has to pay minimum 50 thousand to maximum 3 lakhs as a penalty.

Some of the major provisions are:

1. It has the provision relating to electronic records and digital signature.
2. It has the provision relating to dispatch, receive an acknowledgement of electronic records.
3. It has the provision relating to government use of the digital signature.
4. It has a provision relating to the computer network and network services providers.
5. It has the provision relating to computer-related crimes and punishments.

Security Policy

- A security policy is a written document in an organization outlining o how to protect the organization from threats, including computer security threats, o and how to handle situations when they do occur.
- A security policy must identify all of a company's assets as well as all the potential threats to those assets.
- Thus, an effective IT security policy is a unique document for each organization, cultivated from its people's perspectives on risk tolerance, how they see and value their information, and the resulting availability that they maintain of that information.

Need of Security policies-

1) It increases efficiency.

- The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources.
- The policy should inform the employees about their individual duties, and telling them what they can do and what they cannot do with the organization sensitive information.

2) It upholds discipline and accountability

- When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also supporting a case in a court of law.
- The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.

3) It can make or break a business deal

- It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information.
- It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place.

4) It helps to educate employees on security literacy

- A well-written security policy can also be seen as an educational document which informs the readers about their importance of responsibility in protecting the organization sensitive data.
- It involves on choosing the right passwords, to providing guidelines for file transfers and data storage which increases employee's overall awareness of security and how it can be strengthened.

There are some important cybersecurity policies recommendations describe below-

1. Virus and Spyware Protection policy

- This policy provides the following protection:
  - It helps to detect, removes, and repairs the side effects of viruses and security risks by using signatures.
  - It helps to detect the threats in the files which the users try to download by using reputation data from Download Insight.

2. Firewall Policy

- This policy provides the following protection:
  - It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
  - It detects the attacks by cybercriminals.
  - It removes the unwanted sources of network traffic.

3. Intrusion Prevention policy

- This policy automatically detects and blocks the network attacks and browser attacks.
- It also protects applications from vulnerabilities. It checks the contents of one or more data packages and detects malware which is coming through legal ways.

4. Application and Device Control

- This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system.

5. Exceptions policy

- This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans.

6. Host Integrity policy

- This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure.
- This policy requires that the client system must have installed antivirus.

Managing Risk

- Risk management is the action of prioritizing cybersecurity measures in regards to possible consequences of vulnerabilities within the process.
- IT professionals depend on technologies and combinations of strategies to protect their organization against cybercrime.
- Cybersecurity risk management is similar to real-world risk management, but takes place in the cyber world.
- The need for cybersecurity risk management grows as the volume of compromised systems, stolen data, and damaged reputation increases with hundreds of cybercrimes happening every day.

The cyber risk management process

Although specific methodologies vary, a risk management program typically follows these steps:

1. **Identify** the risks that might compromise our cyber security. This usually involves identifying cyber security vulnerabilities in our system and the threats that might exploit them.
2. **Analyze** the severity of each risk by assessing how likely it is to occur, and how significant the impact might be if it does.
3. **Evaluate** how each risk fits within your risk appetite (your predetermined level of acceptable risk).
4. **Prioritize** the risks. Decide how to respond to each risk.
5. **Treat** – modify the likelihood and/or impact of the risk, typically by implementing security controls.
    - Tolerate – make an active decision to retain the risk (e.g. because it falls within the established risk acceptance criteria).
    - Terminate – avoid the risk entirely by ending or completely changing the activity causing the risk. o Transfer – share the risk with another party, usually by outsourcing or taking out insurance.
6. Since cyber risk management is a continuas process, **monitor** risks to make sure they are still acceptable, review controls to make sure they are still fit for purpose, and make changes as required. Remember that risks are continually changing as the cyber threat landscape evolves, and systems and activities change.

Information Security Process

- Information security process is a process that moves through phases building and strengthening itself along the way.
- Although the Information Security process has many strategies and activities, we can group them all into three distinct phases **- prevention, detection, and response**. Each phase requiring strategies and activities that will move the process to the next phase.
- The ultimate goal of the information security process is to protect three unique attributes of information. They are:

Prevention: Preventing an incident requires careful analysis and planning. Information is an asset that requires protection commensurate with its value. Security measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional. During the prevention phase, security policies, controls and processes should be designed and implemented.
Detection: Detection of a system compromise is extremely critical. With the ever-increasing threat environment, no matter what level of protection a system may have, it will get compromised given a greater level of motivation and skill. Intrusion detection systems (IDS) are utilized for this purpose. IDS have the capability of monitoring system activity and notifies responsible persons when activities warrant investigation.

Response: For the detection process to have any value there must be a timely response. The response to an incident should be planned well in advance. Making important decisions or developing policy while under attack is a recipe for disaster. Many organizations spend a tremendous amount of money and time preparing for disasters such as tornados, earthquakes, fires and floods. A Computer Security Incident Response Team (CSIRT) should be established with specific roles and responsibilities identified. These roles should be assigned to competent members of the organization. A team leader/manager should be appointed and assigned the responsibility of declaring an incident, coordinating the activities of the CSIRT, and communicating status reports to upper management.

Information Security Best Practice

1. Install anti-virus software and keep all computer software patched. Update operating systems, applications, and antivirus software regularly.
2. Use a strong password and don't reuse same passwords for different accounts.
3. Log off (Log out) from public computers such as office, hotel or café etc.
4. Back up important information and verify that you can restore it.
5. Keep personal information safe.
6. Be wary of suspicious e-mails and never ever respond to emails asking you to disclose any personal information.
7. Pay attention to browser warnings and shop smart online and don't click everywhere.
8. Download files legally.
9. Secure your laptop, smart phone or other mobile devices
10. Consider biometric security

Unit-5
Forensics and Incident Analysis

- Forensic Technologies
- Digital Evidence Collection
- Evidentiary Reporting
- Incident Preparation
- Incident Detection and Analysis
- Containment, Eradication, and Recovery
- Proactive and Post Incident Cyber Services

Forensics

- Forensics is related to scientific methods of solving crimes, involving examining the objects or substances are involved in the crime.
- Cyber forensics/ Digital Forensics/ Computer Forensics is the process by which experts collect, examine, and analyze all of the data from compromised computer systems and storage devices.
- This is done in a manner consistent with best-practices so that the evidence could be admissible in a court of law if necessary.
- Evidence collection includes identifying and securing infected devices and all data, including latent data, from the systems.

Forensic Technologies

- Digital forensics is a relatively new branch of forensic science.
- This involves the identification, validation, investigation, recovery, and presentation of facts during criminal cases regarding digital evidence found on computers and other digital devices.
- With help from advanced technology, information moves very fast.
- Additionally, the information could be stored or in this case hidden in different apps or software.
- Traditional criminal justice workers may not have the skills or capability to recover this information and use it to prosecute criminals.
- This creates the need for skilled personnel such as digital forensics technologists and forensics technologies.
- Such technologies are explained below.

The Sleuth Kit and Autopsy:

- This is a kit of commands lines for system analysis.
- This valuable forensic software helps us to navigate through the files from the suspect computer without altering anything on the computer.
- In addition, this forensic tool like many others is able to show us a detailed list of deleted files and hidden files.
- However, a disadvantage of this forensic tool is that you must to memorize all commands, and it is tedious but is here in this part when Autopsy can help.

- Autopsy is a forensic tool with a graphical user interface and browser to analysis evidence.
- Autopsy can analysis different types of data format such as FAT, Ext2 / Ext3, NTFS, etc.
- Autopsy is based on HTML, So, this feature permits the connection with the server of Autopsy employing a web browser.
- Also, deleted files and data are shown by an interface of Autopsy called "File Manager".

ProDiscover Basic:

- ProDiscover Basic is a free digital forensic tool that like Autopsy has a graphical user interface.
- This forensic tool is designed to make copies of the hard disk without altering any data on this.
- ProDiscover Basic also permits to create images of USB flash memory, RAM memory images, BIOS image and hard drives images. Once the image is ready, we can analyze in detail the evidence found for this wonderful software. Some features of this digital forensic tool are:
    - View Deleted files
    - Search for contents of a disk
    - Retrieve a file that was accidentally deleted
    - Registry view

- Event log view
- Internet history view

EnCase Enterprise:

- EnCase is an instinctive tool that has a useful user interface and amazing performance.
- EnCase forensic digital analysis in deep investigations with accuracy and safety.
- It is a software that ensures the full integrity of the information, even deleted data.
- Some features of this forensic tool are:
  - Support for multiple images systems such as Linux, Windows, MAC OS etc.
  - Full Support for Unicode
  - The ability of multiple systems analysis
  - Search tools
  - Gets data from disk or RAM, documents, pictures, email, web mail, Internet appliances, cache and web history, reconstruction of HTML websites, chat sessions, archives, backup files, and encrypted files.

DEFT:

- DEFT (Digital Evidence and Forensic Toolkit) is a distribution of Linux based tool with a GUI for forensic applications.
- DEFT is designed to police, researchers, system administrators or forensic specialists.
- DEFT is a useful forensic tool because it is able to provide accurate and reliable analysis to forensic investigators, and this is because DEFT ensures the integrity of data structures and metadata in the system that is being analyzed without altering the data.
- When the system is booting, the partition in the system that must be analyzed is not touched by DFET to make any changes.

Internet Evidence Finder:

- Internet Evidence Finder is a software tool that enables the recovery of data that has been deleted or that are currently stored on the hard drive, as a result of communications right through the internet.
- This means that Internet Evidence Finder can recover all types of social networks data, such as popular web mail applications, browsing the history, chat histories, instant messaging, and other online communications.

Digital Evidence Collection

- Digital evidence can be defined as the information or valuable data stored on a computer or a mobile device that was seized by a law enforcement organization as part of a criminal investigation.
- The information stored or transmitted in binary form on a computer hard drive, a mobile phone, or any other electronic device can be used as digital evidence by the forensic responders in a court of law.

- This evidence can include files on emails or mobile phones of the suspects, which could be critical to track their intent and location at the time of the crime and the searches they made on search platforms like Google or YouTube.

Typical Digital Evidence sources

- Web browser cache (LOCAL)
- Browsing History
- Web page program features
- Mobile phone (LOCAL & REMOTE)
- Sent and received calls/SMS
- Network logs

Steps to Collection

- Seizing the available electronic media.
- Acquiring and creating a forensic image of the electronic media for examination.
    - Find the evidence where is it stored.
    - Find relevant data using recovery techniques.
- Analyzing the forensic image of the original media to ensure the data is not modified.
- Create a good documentation of all the actions.

Evidentiary Reporting

- An Evidence is a piece of information that supports a conclusion.
- Digital evidence is an any data that is recorded or preserved on any medium in or by a computer system or other similar digital device.
- The digital evidence can be read or understood by a person or a computer system or other similar device.
- It is important that information about the investigation be limited to as few people as possible.
- Information should be given on a need-to-know basis, which limits the possibility of the investigation being leaked.

Process of evidentiary writing

- List every piece of evidence analyzed, including serial numbers, hash values, photographs, etc. Write thorough descriptions for photographs, including information on the camera type, date, timestamps and locations.
- Clearly show the steps taken to collect and analyze artifacts, including listing any software or hardware used to extract and analyze data.
- Create a timeline. It's helpful to create a visual that demonstrates the chronological sequence of events in a way that's easy for readers to grasp.
- Remember to put yourself in the shoes of the reader.
- What questions might you have about the evidence if you were in their position? If you can adequately answer these questions in your report, you may be released from testifying.

Incident Preparation

- Preparation is the key to effective incident response.

- Even the best incident response team cannot effectively address an incident without predetermined guidelines.
- A strong plan must be in place to support team. In order to successfully address security events, these features should be included in an incident preparation plan:
    - **Develop and Document IR Policies:** Establish policies, procedures, and agreements for incident response management.
    - **Define Communication Guidelines**: Create communication standards and guidelines to enable seamless communication during and after an incident.
    - **Incorporate Threat Intelligence Feeds**: Perform ongoing collection, analysis, and synchronization of threat intelligence feeds.
    - **Conduct Cyber Hunting Exercises:** Conduct operational threat hunting exercises to find incidents occurring within environment. This allows for more proactive incident response.
    - **Assess Threat Detection Capability:** Assess current threat detection capability and update risk assessment and improvement programs.

Incident Detection and Analysis

- Incident detection is the process of identifying, investigating and recovering from a cyber-attack.
- Sometimes, even the best defenses are breached and sensitive data is compromised.
- Incident detection and analysis process focuses on these key areas:
    o Ensuring threat actors are no longer present in the network, o Developing and implementing the incident response plan, o Identifying the scope of the breach and the data impacted, o Closing the vulnerability that allowed the data breach occur.

Questions to address during incident detection and analysis

- When did the event happen?
- How was it discovered?
- Who discovered it?
- Have any other areas been impacted?
- What is the scope of the compromise?
- Does it affect operations?
- Has the source (point of entry) of the event been discovered?
- Have artifacts/malware from the attacker been securely removed?
- Has the system been hardened, patched, and updates applied?
- Can the system be re-imaged?

Containment, Eradication, and Recovery
Write the topic of these three terms

Containment

- Once a threat has been identified, the IR (incident response) team should work to contain the threat to prevent further damage to other systems and the organization at large.

- The responder quickly isolates any infected machine and works on backing up any critical data on an infected system, if possible.
- Next, a temporary fix should be implemented on an infected machine to prevent the threat from escalating. The goal is to minimize the threat.
- Damaged systems removed from production; devices are isolated, compromised accounts are locked down — the bleeding stops here.

4. Eradication

- Eradication is removing and remediating any damage discovered in the identification phase.
- This is normally done by restoring systems from backup and re-imaging workstation systems.
- It's important to note that proper eradication of a cyber infection should be done by trained professionals and should only be done after comprehensive investigation into the incident is completed.
- During the eradication phase, the IR team should also be documenting all actions required to eradicate the threat.
- In addition, any defenses in the network should be improved so that the same incident doesn't occur again.

Recovery

- Recovery is the testing of the fixes in the eradication phase and the transition back to normal operations.
- Vulnerabilities are remediated, compromised accounts have passwords changed or are removed altogether and replaced with other more secure methods of access.
- At the recovery stage, any production systems affected by a threat will be brought back online.
- This includes any data recovery or restoration efforts that need to take place as well.
- To ensure that they are back to normal operation, test, check, and track the affected systems.

Proactive and Post Incident Cyber Services

- This step provides the opportunity to learn from our experience so we can better respond to future security events.
- Take a look at the incident with a humble but critical eye to identify areas for improvement.
- Then add those improvements to documentation.
- A central part of the incident response methodology is learning from previous incidents to improve the process.
- This helps analyze and document everything about the breach. Determine what worked well in response plan, and where there were some holes.
- Lessons learned from both mock and real events will help strengthen systems against the future attacks.

Unit-6
Ethics in Cyber security & Cyber Law

- Privacy
- Intellectual Property
- Professional Ethics
- Freedom of Speech
- Fair User and Ethical Hacking
- Trademarks
- Internet Fraud
- Electronic Evidence

Privacy

- Privacy is a word describing the condition of being free from being observed. Digital privacy is the lack of personal identification in the digital world and the internet.
- It refers to the protection of an individual's information that is used or created while using the Internet on a computer or personal device.
- Digital privacy is often used on behalf of individual and consumer privacy rights in e-services for the business practices of many e-marketers, businesses, and companies to collect and use such information and data.
- Digital privacy has increasingly become a topic of interest as information and data shared over the social web: social-media users are now considered unpaid 'digital labors', as one pays for 'free' e-services through the loss of their privacy.
- For example, between 2005 and 2011, the change in levels of disclosure for different profile items on Facebook show that, over the years, people want to keep more information private.
- However, observing the seven-year span, Facebook gained a profit of $100 billion through the collection and sharing of their users' data to the third-party advertisers.

Intellectual Property

- Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.
- It is a category of property that includes intangible creations of the human intellect.
- To protect the intellectual property, we have the intellectual property law.
- The main purpose of intellectual property law is to encourage the creation of a wide variety of intellectual goods.

Types of Intellectual Property

Patents

- A patent is a property right for an investor that's typically granted by a government agency.
- The patent allows the inventor exclusive rights to the invention, which could be a design, process, an improvement, or physical invention such as a machine.
- Technology and software companies often have patents for their designs.
- For example, the patent for the personal computer was filed in 1980 by Steve Jobs and three other colleagues at Apple Inc. **Copyrights**
- Copyright provides authors and creators of original material the exclusive right to use, copy, or duplicate their material.

- Authors of books have their works copyrighted as do musical artists.
- A copyright also states that the original creators can grant anyone authorization through a licensing agreement to use the work.

Trademarks

- A trademark is a symbol or phrase that is recognizable and represents a product that legally separates it from other products.
- A trademark is exclusively assigned to a company, meaning the company owns the trademark so that no others may use or copy it.
- A trademark is often associated with a company's brand. For example, the logo and brand name of "Coca Cola," is owned by the Coca-Cola Company (KO).

Trade Secrets

- A trade secret is a company's process or practice that is not public information, which provides an economic benefit or advantage to the company or holder of the trade secret.
- Trade secrets must be actively protected by the company and are typically the result of a company's research and development.
- Examples of trade secrets could be a design, pattern, recipe, formula, or proprietary process.
- Trade secrets are used to create a business model that differentiates the company's offerings to its customers by providing a competitive advantage.

Professional Ethics:

- Professional ethics are principles that govern the behavior of a person or group in a business environment.
- Like values, professional ethics provide rules on how a person should act towards other people and institutions in such an environment.
- Ethical principles underpin all professional codes of conduct. Ethical principles may differ depending on the profession; for example, professional ethics that relate to medical practitioners will differ from those that relate to lawyers or real estate agents.
- However, there are some universal ethical principles that apply across all professions, including:
- honesty
- trustworthiness
- loyalty
- respect for others
- adherence to the law
- doing good and avoiding harm to others
- accountability.

Freedom of Speech

- Freedom of Speech is the right to express information, ideas, and opinions free of government restrictions.
- The power or right to express one's opinions without censorship, restraint, or legal penalty.

When freedom of speech can be restricted

- In certain circumstances free speech and freedom of expression can be restricted.
- Governments have an obligation to prohibit hate speech and incitement.
- And restrictions can also be justified if they protect specific public interest or the rights and reputations of others.

  Any restrictions on freedom of speech and freedom of expression must be set out in laws that must in turn be clear and concise so everyone can understand them.

Fair User and Ethical Hacking

- Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data.
- Ethical hacking is used to identify potential data breaches and threats in a network unlike malicious hacking, this process is planned, approved, and more importantly, legal.
- Ethical hacking is performed by Security expert/professionals known as ethical hacker (white hat hacker)
- Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy.
- By doing so, they can improve the security of the system. **Key concepts of ethical hacking**

Hacking experts follow four key protocol concepts:

- **Stay legal**. Obtain proper approval before accessing and performing a security assessment.
- **Define the scope**. Determine the scope of the assessment so that the ethical hacker's work remains legal and within the organization's approved boundaries.
- **Report vulnerabilities**. Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.
- **Respect data sensitivity.** Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization.

Trademarks

- A trademark is an easily recognizable symbol, phrase, or word that denotes a specific product.
- A trademark exclusively identifies a product as belonging to a specific company and recognizes the company's ownership of the brand.
- Trademarks are generally considered a form of intellectual property and may or may not be registered.
- It legally differentiates a product or service from all others of its kind and recognizes the source company's ownership of the brand.
- A trademark may be located on a package, a label, a voucher, or on the product itself.
- For the sake of corporate identity, trademarks are often displayed on company buildings. It is legally recognized as a type of intellectual property.

Using the trademark symbols TM, SM, and ®

- The symbols "TM" is used for goods, "SM" for services even if you haven't filed an application to register your trademark.
- Once we trademark with, we can use an ® with the trademark.

Internet Fraud

- Internet fraud is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them.
- Internet fraud can also involve incorrect information for the purpose of tricking victims out of money.
- Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace.
- Several kinds of internet fraud include Data Breach, Denial of Service, malware, ransomware, phishing etc.

How to protect ourselves from the internet fraud?

- **Learn about the types of internet fraud.**
  The more you know about various fraud schemes, the better you can protect yourself from them.
- **Use common sense.**
  If something sounds too good to be true, it's probably a fraud.
- **Keep your personal information secure.**
  Do not give out any information regarding your savings, checking, credit, or other financial accounts.
- **Guard your Social Security number especially carefully.**
- **Deal only with legitimate, reputable companies and individuals.**
- **Obtain and verify addresses and phone numbers.**
- **Be sure to use an up-to-date major browser and avoid insecure websites.**

Electronic Evidence

- Electronic evidence is any electronically stored information (ESI) or transmitted in a digital form that may be used as evidence in a lawsuit or trial.
- Electronic evidence includes any documents, emails, or other files that are electronically stored. Additionally, electronic evidence includes records stored by network or Internet service providers.
- The use of digital evidence has increased in the past few decades as courts have allowed the use of following things as electronic evidence o Emails o Digital photographs o ATM transaction logs o Word processing documents o Instant messages history o Accounting files o Spreadsheets o Internet browser history
  - Databases
  - Contents in a computer memory o Computer backups & printouts o GPS Tracks o Digital video
  - Audio files

Assignment: Trademark vs Patent vs Copyright

Unit-7
Professional and Ethical Responsibilities

- Community values and the laws by which we live
- The nature of professionalism in IT
- Various forms of professional credentialing
- The role of the professional in public policy
- Maintaining awareness of consequences
- Ethical dissent and whistle-blowing
- Codes of ethics, conduct, and practice (IEEE, ACM, SE, AITP, and so forth) • Dealing with harassment and discrimination

Community values and the laws by which we live

- Ethics and laws are found in virtually all spheres of society. They govern actions of individuals around the world on a daily basis.
- They often work hand-in-hand to ensure that citizens act in a certain manner, and likewise coordinate efforts to protect the health, safety and welfare of the public.
- Though law often embodies ethical principles, law and ethics are not co-extensive.
- Based on society's ethics, laws are created and enforced by governments to mediate our relationships with each other, and to protect its citizens.
- While laws carry with them a punishment for violations, ethics do not. Essentially, laws enforce the behaviors we are expected to follow, while ethics suggest what we ought to follow, and help us explore options to improve our decision-making.

The nature of professionalism in IT

- Profession is any type of work that needs special training or a particular skill, often one that is respected because it involves a high level of education. Ex: Engineer, lawyers, doctors, dentists, accountants, architects & etc.
- Professionalism may be considered as behaving in an appropriate manner and adhering to accepted principles and practices.
- It is not only vital in the field of Information Technology but it is also very important in other fields. Some of the key aspects of IT Professionalism are competence in IT, knowledge, various skills such as soft skills, ethical behavior and certification.

Why IT professionalism is needed and why is it important?

- In order to enhance the growth and add value to an organization.
- It helps to provide better services to clients.
- It increases trust with employers and employees within an organization.
- Create company's own brand value.
- IT professionalism forms the pillar for company's own vision and mission.
- It improves customer satisfaction.

Nature of IT Profession

1. Self-directed & continuous learning about new technologies.
2. Communication skills & language proficiency.
3. Has honesty and performs his/her duties
4. Responsible and dedicated towards work.
5. Organizational skills.
6. Team contribution and leadership.

7. Has self-respect and treats others with respect.
8. Critical thinking and decision making
9. Customer relations
10. Long working hours and stress management
11. Competitive working environment with multi skilled colleagues

Various forms of professional credentialing

- A credential is a piece of any document that details a qualification, competence, or authority issued to an individual by a third party with a relevant or de facto authority or assumed competence to do so.
- Examples of credentials include academic diplomas, academic degrees, certifications, security clearances, identification documents, badges, passwords, user names, keys, powers of attorney, and so on.
- Professional credentialing is the process by which a person proves that he or she has the knowledge, experience and skills to perform a specific job and the tasks in which they have been trained.
- The proof comes in the form of a certificate which is earned by passing one or more exams that were developed by an organization or association that monitors and upholds the prescribed standards for the particular industry involved.

Various forms of professional credentialing

Diplomacy

- In diplomacy, credentials, also known as a letter of credence, are documents that ambassadors, diplomatic ministers etc. provide to the.
- It contains a request that full credence be accorded to his official statements. Until his credentials have been presented and found in proper order, an envoy receives no official recognition.

Medicine

- In medicine, the process of credentialing is a detailed review of all permissions granted a medical doctor, physician, assistant or nurse practitioner at every institution at which he or she has worked in the past, to determine a risk profile for them at a new institution.

Information technology

- Information systems commonly use credentials to control access to information or other resources.
- The classic combination of a user's account number or name and a secret password is a widely used example of IT credentials.
- An increasing number of information systems use other forms of documentation of credentials, such as biometrics (fingerprints, voice recognition, retinal scans), public key certificates, and so on.

Cryptography

- Credentials in cryptography establish the identity of a party to communication. Usually, they take the form of machine-readable cryptographic keys and/or passwords. Cryptographic credentials may be self-issued, or issued by a trusted third party.

Operator licensing.

- Operators of vehicles such as automobiles, boats, and aircraft must have credentials in the form of governmentissued licenses in many jurisdictions.
- Often the documentation of the license consists of a simple card or certificate that the operator keeps on his person while operating the vehicle, backed up by an archival record of the license at some central location.

- Licenses are granted to operators after a period of successful training and/or examination.

Journalism

- In many democratic nations, press credentials are not required at the national or federal level for any publication of any kind. However, individual corporations, and certain government or military entities require press credentials, such as a press pass, as a formal invitation to members of the press which grants them rights to photographs or videos, press conferences, or interviews.

Titles

- Titles are credentials that identify a person as belonging to a specific group, such as nobility or aristocracy, or a specific command grade in the military, or in other largely symbolic ways.
- They may or may not be associated with specific authority, and they do not usually attest to any specific competence or skill (although they may be associated with other credentials that do). A partial list of such titles includes o Personal titles, such as Lord, Knight, Right Honorable, indicating an earned or inherited rank or position within a formal power structure.
    - Command ranks, such as Captain, Sergeant, etc., indicating likewise a very specific position in a command hierarchy, e.g. police rank or military rank;
    - An academic degree or professional designation such as PhD, M.D., whether this be purely honorary or symbolic, or associated with credentials attesting to specific competence, learning, or skills.
    - Citizenship, as in the case of passports and birth certificates.

The role of the professional in public policy

- Public policy is a governmental decision to pursue a specific course of action in order to solve a problem or achieve a goal.
- More importantly, these governmental decisions express certain values and beliefs about different groups of people in society that impact policy design.
- Public policy professionals should have strong problem-solving, presentation, and oral and written communication skills. **Roles**

Public Administration

- Public policy helps to learn to plan, implement, and assess programs.
- They gain the skills needed to lead multidisciplinary teams, train employees, and allocate resources.
- They also learn to align an organization's policies with government regulations and standards.

Policy Analysis

- Developing an understanding of the legislative process, including how social, political, economic, and technological factors affect government regulations and laws.
- Public policy professionals analyze the effects of public policies on individuals and communities. That also helps to guide policy formation by examining key legislative and executive institutional objectives.

Communication

- Communication skills enables to convey information clearly and persuasively in written, oral, and multimedia forms.
- Public policy professionals must communicate complex and technical ideas to individuals and teams. They also need to tactfully engage with government officials and community members to cultivate productive relationships. **Ethical Leadership**
- Public policy professionals must be able to assess the ethical implications of individual, organizational, and social actions. They analyze a leader's decisions, including how external and internal pressures affect decision-making processes.

Strategic Decision-Making

- Public policy professionals may be responsible for making decisions that have widespread and long-lasting effects.

- They should identify the most important features of a decision based on setting and context.
- They must also evaluate the psychological factors that impact a decision's quality.

Maintaining awareness of consequences

- Cybersecurity is a global phenomenon representing a complex socio-technical challenge for governments, but requiring the involvement of individuals.
- Although cybersecurity is one of the most important challenges faced by governments today, the visibility and public awareness remains limited.
- Almost everybody has heard of cybersecurity, however, the urgency and behavior of persons do not reflect high level of awareness.
- The Internet is all too often considered as a safe environment for sharing information, transactions and controlling the physical world.
- Yet, cyberwars are already ongoing, and there is an urgent need to be better prepared. The inability to frame cybersecurity has resulted in a failure to develop suitable policies.

Best practices for maintaining awareness

Implement basic cyber security training

- Conducting training sessions will ensure that employees use approved software, and have strong passwords.
- We could also look at implementing common sense practices surrounding technology access

Implementing secure technologies and following best practices

- Implementing the secure technologies reduces the risks of data loss in an organization.
- And we should always follow the best practices of the technologies to make good use of them.

Have a data backup and recovery strategy

- Many businesses don’t have a procedure or back-up plan, if their data get lost or damaged.
- With more and more businesses relying on the cloud, it’s crucial to ensure cloud-based data is adequately protected or not.

Detect and plan for what you can’t prevent

- Hackers will always try and find a vulnerability, and when they do, we need to make sure we have the resources and knowledge to detect their activities as quickly as possible.
- This way, you can contain the damage and get back to normal business without experiencing a massive loss event.

Ethical dissent and whistle-blowing

- Ethical dissent likely starts as the result of an employee noticing that things are not what they ought to be, and then attempting to get them changed by talking to people in the organization.
- It can end easily, with changes made quickly, or it can end by involving an unfolding number of agencies, lawyers, legal systems, and public proceedings.
- Sometimes, the direction it takes after the beginning is in your own hands.
- But ethical dissent does not need to go as far as making public allegations about wrongdoing in your company.
- It can involve as little as making a well-supported suggestion that policy be changed in your organization.
- Ethical dissent becomes whistleblowing when you make your dissent public by going outside the organization and contacting others such as media or any government agencies to convince them to help you reform the organization.
- Whistle blower is a person who exposes the misconduct or illegal activities occurring in an organization.

- The matters that are of substantial important to public interest only fall under the whistle blowing. It can also be done by a member or a former member of an organization.

Codes of ethics, conduct, and practice (IEEE, ACM, SE, AITP, and so forth)

IEEE: Institute of Electrical and Electronics Engineers.
ACM: Association for Computing Machinery
SE: Software Engineering
AITP: Association of Information Technology Professionals

- A number of resources help IT professionals searching for ethical guidance within the scope of their job duties.
- For example, IEEE has a code of ethics for its members; the Association of Information Technology Professionals (AITP) has a code of ethics and standards of conduct; and SANS has published an IT code of ethics.
- There are other examples beyond these three, and many elements in these codes could be useful to higher education IT professionals.
- Among other elements that describe ethical behavior in the profession, in general these codes assert that IT professionals need to commit to:
- Integrity
- Competence
- Professional responsibilities
- Work responsibilities
- Societal responsibilities

Dealing with harassment and discrimination

- Cyberbullying is the use of technology to harass, threaten, embarrass, or target another person.
- Online threats and mean, aggressive, or rude texts, tweets, posts, or messages all count. So does posting personal information, pictures, or videos designed to hurt or embarrass someone else.
- Cyberbullying also includes photos, messages, or pages that don't get taken down, even after the person has been asked to do so. In other words, it's anything that gets posted online and is meant to hurt, harass, or upset someone else.
- Intimidation or mean comments that focus on things like a person's gender, religion, race, or physical differences count as discrimination, which is against the law in many states. That means the police could get involved, and bullies may face serious penalties.

What Can I Do About Cyberbullying?

1. **Tell someone**. Most experts agree: The first thing to do is tell an adult you trust. This is often easier said than done. People who are cyberbullied may feel embarrassed or reluctant to report a bully. Some may hesitate because they're not 100% sure who is doing the bullying. But bullying can get worse, so speak up until you find someone to help. Sometimes the police can track down an anonymous online bully, so it's often worthwhile to report it.
2. **Walk away**. Ignoring bullies is the best way to take away their power, but it isn't always easy to do — in the real world or online.
3. **Resist the urge to retaliate or respond**. Walking away or taking a break when you're faced with online bullying gives you some space so you won't be tempted to fire back a response or engage with the bully or bullies. Responding when we're upset can make things worse.
4. **Report Harassment** Social media sites take it seriously when people post cruel or mean stuff or set up fake accounts. If users report abuse, the site administrator may block the bully from using the

site in the future. You can report to the police about the activities done by some one on the internet if things are getting serious.

5. **Block the bully**. Most devices have settings that let you electronically block the bully or bullies from sending notes. If you don't know how to do this, ask a friend or adult who does.
6. **Be safe online**. Password protect your smartphone and your online sites, and change your passwords often. Be sure to share your passwords only with your parent or guardian. It's also wise to think twice before sharing personal information or photos/videos that you don't want the world to see.

Unit - 8
Risks and Liabilities of Computer-Based Systems

- Software risks
- Safety and the engineers
- Implications of software complexity
- Risk assessment and management

Software risks

- Software risk encompasses the probability of occurrence for uncertain events and their potential for loss within an organization.
- Risk management has become an important component of software development as organizations continue to implement more applications across a multiple technology, multi-tiered environment.
- Typically, software risk is viewed as a combination of robustness, performance efficiency, security and transactional risk propagated throughout the system.
- Various risks related to software are:

1. Injection

- It is a code injection technique in which the data is injected through the input fields of the software.
- The way to protect from this is to enforce input type and length, ensure special characters are escaped, validate all input fields and use and input validation whitelist, and avoid dynamic queries or commands.

2. Weak Authentication and Session Management

- This is when attacks take advantage of improper authentication or session management practices and can lead to revealing sensitive information like passwords.
- This is why user management and authentication are important. You should perform user and role validation on all actions and use secure session cookie flags.

3. Cross Site Scripting (XSS)

- XSS is a technique that enables attackers to inject client-side scripts to the web pages.
- An unwanted script can lead to compromised credentials and sessions or redirection to malicious sites. To mitigate this, you should sanitize input.

4. Insecure Direct Object References

- It's scary when files are exposed. Insecure direct object references lead to unauthorized data access. The most common that most people have heard of is called Local File Inclusion. This is where a secure file shows up on the front end of a web page.
- You can ensure access control checks when using direct object references and use reference maps instead of direct references.

5. Security Misconfiguration

- If security configuration is outdated, or not set up properly this can lead to unintended access to data or application functions.

6. Sensitive Data Exposure

- This is caused by improper encryption of sensitive data like payment credentials or personal information. This can lead to fraud or a company being victim.
- To fix this you should encrypt data and avoid storing sensitive data.

7. Unvalidated Redirects and Forwards

- If site gets hacked, the hackers can redirect users visiting that site to malicious sites. Also, it can trick us to think the malicious site is our site. So, we should avoid redirects and forwards altogether.

Safety and the engineers

Implications of software complexity

- Early prediction of software quality is important for better software planning and controlling.
- In early development phases, design complexity metrics are considered as useful indicators of software testing effort and some quality attributes.
- Although many studies investigate the relationship between design complexity and cost and quality, it is unclear what we have learned beyond the scope of individual studies.
- With increasing demands on software functions, software systems become more and more complex.
- This complexity is one of the broadest factors affecting software development productivity.
- Assessing the impact of software complexity on development productivity helps to provide effective strategies for development process and project management.
- To produce reliable software, its complexity must be controlled by suitably decomposing the software system into smaller subsystems.
- A software complexity metric is developed that includes both the internal and external complexity of a module.
- This allows analysis of a software system during its development and provides a guide to system decomposition.

Risk assessment and management

- Risk assessment helps us identify and categorize risks. Plus, it provides an outline for potential consequences.
- Performing a risk assessment involves processes and technologies that help identify, evaluate and report on any risk-related concern.
- Risk assessment is a “key component” of the risk management process and is primarily focused on the identification and analysis phases of risk management.
- If we take the example of a security risk assessment, it involves the following steps:
- Identify the critical assets and sensitive data,
- Build a risk profile for each asset,
- Determine cybersecurity risks for each asset,
- Mapping how critical assets are linked,
- Prioritize which assets to address in case of a security threat,
- Continually monitor risks, threats, and vulnerabilities.

- Risk management involves the identification, analysis, evaluation, and prioritization of current and potential risks.
- This allows you to address loss exposures, monitor risk control and financial resources in order to minimize possible adverse effects of potential loss.
- Further, a solid risk management strategy gives you the ability to maximize the realization of available opportunities to avoid risk.