Chapter 1: Introduction to Computer Security

Definition:
Computer security is the protection of computer systems from theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.

Attacks, Services and Mechanisms

- **Security Attack:** Any action that compromises the security of information.
  Passive attack: unauthorized reading of a message or a file.
  Active attack: modification of messages or files, and denial of service.
- **Security Mechanism**: A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service:** A service that enhances the security of data, information, systems or network.
  e.g. Authentication, Authorization, confidentiality, integrity etc.
  A security service makes use of one or more security mechanisms.

Basic Components & Objectives of Security

1. Confidentiality

Preserving authorized restrictions on information access and disclosure.

- Data Confidentiality: It assures that private or secret information is not made available or disclosed to unauthorized individuals.
- Privacy: What information to collect, who should collect and store the information and to whom the information may be disclosed.

2. Integrity

Guarding against improper information modification or destruction.
Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
System Integrity: Assures that a system performs its intended function in appropriate manner, free from unauthorized manipulation of the system.

3. Availability

- Assures that systems work normally and service is not denied to authorized users.
- Ensuring timely and reliable access to intended users.

CIA Triad

Other Security Services

Authenticity:

- The property of being genuine and being able to be verified and trusted.
- Authenticity is assurance that a message, transaction, or other exchange of information is from the source it claims to be from i.e. proof of identity.

Accountability:

- It means that every individual who works with an information system should have specific responsibilities for information assurance.
- The tasks for which a individual is responsible are part of the overall information security plan and can be readily measurable by a person who has managerial responsibility for information assurance.

Security Threats

A threat is a potential violation of security which might or might not occur.

Snooping

- It is the unauthorized interception of information and disclosure.
- Passively listening(or reading) to communications or browsing through files or system information.
- e.g. passive wiretapping-a form of snooping in which a network is monitored.

Modification or Alteration:

- Unauthorized change of information
- If modified data controls the operation of the system, threats of failure may arise
- Active form of security attack

E.g. Man-in-the-middle attack in which intruder reads messages from sender and sends modified data to the receiver without knowing the changes.

Masquerading or Spoofing:

- One entity pretends to be a different entity.

e.g. If a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one.

Or if a user tries to read a file, but an attacker has arranged for the user to be given a different file.

Repudiation of origin:

A false denial that an entity sent or created something.

e.g. A customer sends a letter to a vendor agreeing to pay a large amount of money for a product. The vendor ships the product and then demands payment. The customer denies having ordered the product and by law is therefore entitled to keep the unrequested shipment without payment. If the vendor cannot prove that the letter came from the customer, the attack succeeds.

Denial of receipt:

A false denial that an entity received some information or message.
e.g. A customer orders an expensive product with earlier payment and the vendor ships it. If the customer has already received the product, the attacker may deny that the product is delivered. The vendor can defend against this attack only by providing that the customer did, despite his denials, receive the product.

Delay:

- Usually delivery of a message or service requires some time t.
- If an attacker can force the delivery to take more than time t, the attacker has successfully delayed delivery.
- This involves manipulation of system control structures, such as network components or server components which is a form of attack.

Denial of service:

- The attacker prevents a server from providing a service.
- The denial may occur at the source (by preventing the server from obtaining the resources), at the destination (by blocking the communications from the server) or along the intermediate path (by discarding messages from either the client or the server, or both).
- It poses the same threat as an infinite delay.

Issues and Challenges of Computer Security

- Providing security is not as easy as it seems to be. The requirements for providing security (confidentiality, authentication, integrity) are quite complex, and understanding them involves complex reasoning.
- In developing a particular security mechanism or algorithm, potential attacks should be considered. But unexpected attacks may occur.
- The procedures used to provide particular services are complex. The security mechanisms should be updated regularly to adapt to the changes.
- Having designed various security mechanisms, it is necessary to decide where to use them: both in terms of physical and logical sense.

- Security mechanisms typically involve more than a particular algorithm or protocol. It also requires the knowledge of system and network.
- Strong security as burden to efficient and user friendly environment and operations.
- Computer and Network security is a battle between the intruder and the designer and administrator.
- The users or system managers hesitate to invest on security due to little benefits until a security failure occurs.
- Security requires regular and constant monitoring which is a difficult in today's short-term and overloaded environment.
- Security is implemented after the system design rather than as a part of the design process.

Operational Issues

1. Cost-benefit analysis

- Balance between benefits of the protection and the cost of designing, implementing and using the mechanism.
- If the data or resources cost less than their protection, adding security mechanisms or procedures is not cost-effective.

e.g. Database of salary information system in banks: main office and branch offices.

2. Risk analysis

- Priority should be given to the tasks that have higher importance
- Potential threats and possible effects of attack should be analyzed

e.g. network with internet and without internet

3. Laws and Customs

- Any policy or mechanism for security must consider legal constraints
- Restrictions affect procedural controls

Human Issues

1. Organizational Problems

- Unless the loss occurs, organization believes that they are wasting effort in security
- Security adds added complexity to simple operations, which may cause decrease in productivity
- Comparison between loss caused due to security attack and financial loss due to added security mechanisms

2. People problem

- Technological controls depends on human operations
- Risk of human intervention

e.g. A computer system authenticates a user by asking that user for a secret code. If the correct code is supplied, the computer assumes that the user is authorized to use the system. So, unauthorized person can masquerade the system.

Security Policies

- Security policy defines the goals and elements of an organization's computer systems that specifies what is allowed to do and what is not.
- With respect to confidentiality, security policy identifies the leakage of information flow.
- With respect to integrity, a security policy identifies authorized ways in which information may be altered and entities authorized to alter it.
- With respect to availability, a security policy describes what services must be provided.

Types of Security Policies:

1. Military Security Policy or Governmental Security Policy

- Developed primarily to provide confidentiality
- The name comes from military's need to keep information secret
- Confidentiality is one of the primary concerns in governmental agencies

2. Commercial Security Policy

- It is a type of security policy developed primarily to provide integrity.
- The name comes from the need of commercial firms to prevent tampering with their data
- If the confidentiality of a bank's computer is compromised, a customer's account balance may be revealed.
- But, if the integrity of the computer holding the accounts is compromised, the balances in the customers' accounts could be altered, which has vulnerable effects.

3. Confidentiality policy:

- A confidentiality policy is a security policy dealing only with confidentiality.
- Both Military policies and Confidentiality policies deal with the confidentiality. However, a confidentiality policy does not deal with integrity at all whereas a military policy may.

4. Integrity Policy:

- An integrity policy is a security policy dealing only with integrity.
- Commercial policy may deal with confidentiality also but integrity policy does not.

Access Control

- Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment.
- Access control is a way of limiting access to a system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information.

Types of Access Control

Mandatory Access Control

- Mandatory access control (MAC) refers to a type of access control by which the operating system constrains the ability of a user to access or generally perform some sort of operation.
- Each user and device on the system is assigned a similar access.
- When a person or device tries to access a specific resource, the OS checks the entity's credentials to determine whether access will be granted.
- Any operation by any subject on any object is tested against the set of authorization rules to determine if the operation is allowed.
- A database management system, in its access control mechanism, can also apply mandatory access control; in this case, the objects are tables, views, procedures, etc.

Discretionary Access Control

- Discretionary access control (DAC) is a type of security access control that grants or restricts object access via an access policy determined by an object's owner.
- DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username and password.
- DACs are discretionary because the subject (owner) can transfer authenticated objects or information access to other users.
- In other words, the owner determines object access privileges or an object's access policy is determined by its owner.
- A typical example of DAC is Unix file mode, which defines the read, write and execute permissions.

Originator Controlled Access Control

- An originator controlled access control bases access on the creator of an object (or the information it contains).
- Information is controlled by originator or creator of information not owner.
- Sometimes creator may be owner too. In that case, it is similar to discretionary access control.
- The goal of this control is to allow the originator of the file (or of the information it contains) to control the broadcasting of the information.
- This security access control is the combination of MAC and DAC.

Role based Access Control

- Role-based access control is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise.
- In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file.
- Roles are defined according to job competency, authority, and responsibility within the enterprise.
- In RBAC, roles can be easily created, changed, or discontinued as the needs of the enterprise evolve.
- The components of RBAC such as role-permissions and user-role relationships make it simple to perform user assignment.
- It is used by the majority of enterprises with more than 500 employees.

Bell-LaPadula Model

- The Bell–LaPadula Model (BLP) is a state machine model used for enforcing access control in government and military applications.
- The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects.
- The Bell–LaPadula model focuses on data confidentiality and controlled access to classified information.
- This module introduces the concept of state machine with a set of allowable states in security of a computer system.
- The security labels are Top secret, Secret, Confidential and Unclassified.
- The concept of state machine is used for the state transitions between these labels.
- This model is the combination of Mandatory Access Control and **Discretionary Access Control.**
- The bell-lapadula model stands on the basis of 3 properties.

Property 1: No read-up

- This is a property which says an associate cannot read any documents prepared by his/her higher officials. The documents are highly confidential or may be strategic and cannot be disclosed to lower level officials.

Property 2: No write-down (property)*

- A user is not allowed write (alter) access to object with lower security level than the current security level of subject.

Property 3: The Discretionary Security Property

- This is an access control which is based on the identity of the subjects. If a subject has certain type of access on the object, he/she can transfer rights to other subject of their choice.

Strong Star Property:

- The Strong Star Property is an alternative to the *-Property, in which subjects may write to objects with only a matching security level. Thus, the write-up operation permitted in the usual *-Property is not present, only a write-to-same operation.

Tranquility principle:

- This principle states that the classification of a subject or object does not change while it is being referenced.
- Principle of strong tranquility: This principle says that the security labels or classifications cannot change during the normal operation of the system.
- Principle of weak tranquility: It states that security levels may never change in such a way as to violate a defined security policy.

Limitations:

- Addresses confidentiality but limits integrity.
- Tranquility principle limits the applicability of the model where security levels do not change dynamically.
- The overall process may take more time due to the transitions between the states.

Biba Integrity Model

- Biba Integrity Model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity.
- Data and subjects are grouped into ordered levels of integrity.
- The levels of integrity are Untrusted, Slightly trusted, Trusted, Highly trusted and Unimpeachable.
- The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.
- Read up, write down (in contrast to Bell LaPadula model).

- In the Biba model, users can only create content at or below their own integrity level (a monk may write a prayer book that can be read by commoners, but not one to be read by a high priest).
- Conversely, users can only view content at or above their own integrity level (a monk may read a book written by the high priest, but may not read a pamphlet written by a lowly commoner).
- Consider a military chain of command. A General may write orders to a Colonel, who can issue these orders to a Major.
- In this fashion, the General's original orders are kept integral and the mission of the military is protected (thus, "read up" integrity).
- Conversely, a Private can never issue orders to his Sergeant, who may never issue orders to a Lieutenant, also protecting the integrity of the mission ("write down").
- In the context of a computer system, privileged processes having the highest levels of integrity are able only to read data with the highest integrity level, while being shielded from all data with a lower level of integrity.
- The Biba model defines a set of security rules, the first two of which are similar to the Bell–LaPadula model but reverse in nature.
- The Simple Integrity Property states that a subject at a given level of integrity must not read data at a lower integrity level (read up).
- The * (star) Integrity Property states that a subject at a given level of integrity must not write to data at a higher level of integrity (write down).
- Invocation Property states that a process from below cannot request higher access. The property whereby a subject at one integrity level is prohibited from invoking or calling up a subject at a higher level of integrity.

Limitations

- Focuses only on integrity
- System performance and monitoring is difficult due to the denied access to lower level information.

Unit 2: Cryptography and Cryptographic Algorithms

Cryptography:

- Cryptography is the technique of converting ordinary plain text into unintelligible text and vice-versa.
- It is the practice and study of techniques for secure communication in the presence of third parties.
- It is also referred by the terms Cryptology and Cryptanalysis.

- It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.
- Cryptology is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.
- Cryptography is most often associated with scrambling plaintext into cipher text (a process called encryption), then back again (known as decryption).

Encryption:

- Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.
- Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor.

Decryption:

- Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand (original form).
- It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

Plain text:

Plaintext or cleartext is unencrypted information.

Cipher text:

Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result. The term “cipher” is sometimes used as a synonym for ciphertext, but it more properly means the method of encryption rather than the result.

Transposition cipher:

A transposition cipher rearranges the characters in the plaintext to form ciphertext. The letters are not changed.

e.g. HELLO WORLD

HLOOL

ELWRD

The rearrangement of the text is based on the permutation. It just rearranges the given information without modifying it.

Substitution cipher:

A substitution cipher changes characters in the plaintext to produce the ciphertext.
e.g. HELLO WORLD

KHOOR ZRUOG

(key 3)

Data Encryption Standard

- The Data Encryption Standard(DES) works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key.
- DES is an outdated symmetric-key method of data encryption.
- **DES has been upgraded by the more secure Advanced Encryption Standard (AES) algorithm.**
- Originally designed by researchers at IBM in the early 1970s, DES was adopted by the U.S. government as an official Federal Information Processing Standard (FIPS) in 1977 for the encryption of commercial and sensitive yet unclassified government computer data.
- It was the first encryption algorithm approved by the U.S. government for public disclosure.
- The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time.
- To encrypt a plaintext message, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit ciphertext by means transposition and substitution.
- The process involves 16 rounds and encrypting blocks individually or making each cipher block is dependent on all the previous blocks.
- DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).
- The check bits or parity bits are used to check if the key was indeed correctly retrieved.
- The output text of each round is the input to next round.
- The keys for each round is separate which is just the result of left circular shift operation of the original key.

- The round key generator is the component which is responsible to generate 16 sub keys for 16 rounds.
- The round operation is nothing but the XOR operation between the plain text and the key.
- The final key to the cipher text is the resulting key at the end of 16 rounds.
- Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied.
- It would take a maximum of 2^56, or 72,057,594,037,927,936 attempts to find the correct key.
- For any cipher, the most basic method of attack is brute force, which involves trying each key until you find the right one.

- Even though few messages encrypted using DES encryption are likely to be subjected to this kind of code-breaking effort, many security experts felt the 56-bit key length was inadequate even before DES was adopted as a standard.
- **Thus, DES is upgraded to more secure Advanced Encryption Standard (AES).**
- Symmetric-key algorithms are the algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.
- Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way.
- Public-key cryptology, which utilizes two keys - a public key to encrypt messages and a private key to decrypt them.

Stream Cipher:

- A stream cipher is a symmetric key cipher where plaintext digits are combined with a keystream.
- A keystream is a stream of random characters that are combined with a plaintext message to produce an encrypted message.
- In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream.

Block cipher:

- A block cipher is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time.
- Block cipher is widely used to implement encryption of bulk data.

- A block cipher consists of two paired algorithms, one for encryption, E, and the other for decryption, D.
- Both algorithms accept two inputs: an input block of size n bits and a key of size k bits; and both yield an n-bit output block.
- The decryption algorithm D is defined to be the inverse function of encryption.
- Symmetric-key encryption can use either stream ciphers or block ciphers.
- Stream ciphers encrypt the digits or letters of a message one at a time. e.g. **Vigenere Cipher.**
- Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size. e.g. DES
- Blocks of 64 bits are commonly used.
- The Advanced Encryption Standard(AES) uses block cipher mode of operation use 128-bit blocks.
- The problem is providing the key to the receiver-key distribution problem.
- Copy of the key can't be sent along with the message. Thus, people at the source and destination must physically meet prior to communicating or any alternative delivery method to provide the key is required.
- This will be a problem if the communication is taking place between entities at long distance or multiple entities are participated in the communication.

Asymmetric key Cryptography

- Asymmetric cryptography, also known as Public key cryptography, uses public and private keys to encrypt and decrypt data.
- The keys are simply large numbers that have been paired together but are not identical (asymmetric).
- One key in the pair can be shared with everyone; it is called the public key.
- The other key in the pair is kept secret; it is called the private key.
- "Public key" cryptography has the following property: "There is no single key but rather a key-pair.
- Doesn't that just add complexity to the problem of key distribution?
- There is still a need for key distribution. But in this case, we intend to distribute the public key to anyone.
- One part (the public key) is available to be given away and the other part (the private key) is intended to be kept secret
- To encrypt something for another person, you need to get a hold of their public key and use it as the encryption key. Then, despite the fact that the public key can be seen by anyone, the only person that can decrypt your message is the person with the private key.

RSA Algorithm

- RSA is one of the first public-key cryptosystems and is widely used for secure data transmission.
- In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret.
- RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978.
- RSA involves a public key and a private key. The public key can be known by everyone, and it is used for encrypting messages.
- The intention is that messages encrypted with the public key can only be decrypted by using the private key.
- The public key is represented by the integers n and e; and, the private key, by the integer d(although n is also used during the decryption). m represents the message.
- A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret.
- The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption.

Key Generation:

The keys for RSA algorithm are generated in the following way:

- Choose two different large random prime numbers p and q
- Calculate n=p*q, n is called modulus
- Calculate the totient: $\Phi(n)=(p-1)(q-1)$

4. Choose an integer e such that $1<e<\Phi(n)$, where e and $\Phi(n)$ do not share factors other than 1

   (e,n) is released as the public key

5. Compute d to satisfy the relation:

   $de\{\text{mod } \Phi(n)\}=1$ or $d=(1+k*\Phi(n))/n$

   k is an integer which should be chosen in such a way that value of d should not be in fraction, k<e

- The totient of a positive integer is the number of integers smaller than n which are coprime to n(they share no factors except 1).

  e.g. $\Phi(8)=4$, because the four numbers:1,3,5 and 7 don't share any factors (Euler's Totient function)

- The public key is made of the modulus n and the encryption exponent e i.e. (e,n)

- The private key is made of the modulus n and the decryption exponent d which must be kept secret i.e. (d,n)

Key Distribution:

- Suppose that Bob wants to send information to Alice. If they decide to use RSA, Bob must know Alice's public key to encrypt the message and Alice must use her private key to decrypt the message.
- To enable Bob to send his encrypted messages, Alice transmits her public key (e,n) to Bob via a reliable, but not necessarily secret, route. Alice's private key (d,n) is never distributed.

Encryption:

- After Bob obtains Alice's public key(e,n), he can send a message m to Alice by computing the cipher text c, using Alice's public key (e,n).

  c=m^e (mod n)
- Bob then transmits c to Alice.

Decryption:

- Alice can recover the original message m form c using her private key (d,n) by computing m= c^d (mod n)

Example:

- Pick two prime numbers: p=3, q=5
- n=p*q=3*5=15
- Φ(n)=(p-1)(q-1)=(3-1)(5-1)=2*4=8
- Choose e satisfying 1<e<Φ(n).

  Let us choose e=3, which do not share any common factors with 8 rather than 1.
- Compute d satisfying: de{mod Φ(n)}=1

  So, d*3{mod 8}=1

  Let us choose d=11 which satisfies the relation.
- So public key (e,n) is (3,15) which is released publicly and the persons that want to send the message use this key to encrypt the message and send it to the receiver .
- Private key (d,n) is (11,15) which is kept secret by the receiver.
- Let us consider the message be 2.
- So, at encryption process, the sender uses the public key to encrypt the message. Resulting cipher text will be:

  c=m^e(mod n)

  =2^3(mod 15)= 8 mod 15=8
- At decryption process, the private key is used to decrypt the cipher text. Plain text is obtained as:

m=c^d(mod n)
=8^11(mod 15)
=2

- Hence, the original message 2 is obtained at receiver end after decryption.

Hashing

- Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.
- Hashing is one way to enable security during the process of message transmission when the message is intended for a particular recipient only. A formula generates the hash, which helps to protect the security of the transmission against tampering.
- Hashing is generating a value or values from a string of text using a mathematical function.
- It is an algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function, that is, a function which is infeasible to invert.
- The only way to recreate the input data from an cryptographic hash function's output is to attempt a brute-force search of possible inputs to produce a match.
- The input data is often called the message, and the output (the hash value or hash) is often called the message digest or simply the digest.
- Hashing is also a method of sorting key values in a database table in an efficient manner.
- Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value.
- When a user sends a secure message, a hash of the intended message is generated and encrypted, and is sent along with the message.
- When the message is received, the receiver decrypts the hash as well as the message. Then, the receiver creates another hash from the message.
- If the two hashes are identical when compared, then a secure transmission has occurred. This hashing process ensures that the message is not altered by an unauthorized end user.
- The ideal cryptographic hash function has five main properties:
- It is deterministic so the same message always results in the same hash.
- It is quick to compute the hash value for any given message.
- It is infeasible to generate a message from its hash value except by trying all possible messages.

- A small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value.
- It is infeasible to find two different messages with the same hash value.
- Cryptographic hash functions have many information-security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication.
- They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption.

Message Digest 5

- The MD5 hashing algorithm is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message.
- The MD5 algorithm is a widely used hash function producing a 128-bit hash value.
- The MD5 hash function was originally designed for use as a secure cryptographic hash algorithm for authenticating digital signatures.
- MD5 has been deprecated for uses other than as a non-cryptographic checksum to verify data integrity and detect unintentional data corruption.
- Although originally designed as a cryptographic message authentication code algorithm for use on the internet, MD5 hashing is no longer considered reliable for use as a cryptographic checksum because researchers have demonstrated techniques capable of easily generating MD5 collisions on commercial off-the-shelf computers.

Message Authentication Code(MAC)

- Message authentication code (MAC), sometimes known as a tag, is a short piece of information used to authenticate a message.
- In other words, to confirm that the message came from the intended sender (its authenticity) and has not been changed.
- The MAC value protects both a message's data integrity as well as its authenticity, by allowing receivers (who also possess the secret key) to detect any changes to the message content.
- MAC algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K.
- Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.

- The receiver can check the MAC and be sure that the message hasn't been modified by the third party.
- The sender forwards the message along with the MAC. Here, we assume that the message is sent in the clear, as we are concerned of providing message origin authentication, not confidentiality. If confidentiality is required then the message needs encryption.
- On receipt of the message and the MAC, the receiver feeds the received message and the shared secret key K into the MAC algorithm and re-computes the MAC value.
- The receiver now checks equality of freshly computed MAC with the MAC received from the sender. If they match, then the receiver accepts the message and assures himself that the message has been sent by the intended sender.
- If the computed MAC does not match the MAC sent by the sender, the receiver cannot determine whether it is the message that has been altered or it is the origin that has been falsified. As a bottom-line, a receiver safely assumes that the message is not the genuine.
- The primary disadvantage of this method is the lack of protection against intentional modifications in the message content.
- The intruder can change the message, then calculate a new checksum, and eventually replace the original checksum by the new value.

Unit 3: Introduction to Network Security

Network Security:

- Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
- "Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network."- Cisco

The top network security fundamentals are:

- Keep patches and update current versions
- Use strong passwords
- Don't use any words from the dictionary
- Don't use anything related to your name, nickname, family members or pets

- Don’t use any numbers someone could guess by looking at your mail like phone numbers and street numbers
- Choose a phrase that means something to you, take the first letters of each word and convert some into characters.
- Secure your VPN
- Actively manage user access privileges
- Clean up inactive accounts

Principal methods of protecting Network:

(Encryption, Decryption, Encryption in network)

- Network encryption is the process of encrypting or encoding data and messages transmitted or communicated over a computer network.
- It is a broad process that includes various tools, techniques and standards to ensure that the messages are unreadable when in transit between two or more network nodes.
- Network encryption is primarily implemented on the network layer of the OSI model.
- Network encryption implements one or more encryption algorithms, processes and standards to encrypt the data/message/packet sent over the network.
- The encryption services are generally provided by encryption software or through an integrated encryption algorithm on network devices and/or in software.
- On an IP-based network, network encryption is implemented through Internet Protocol Security (IPSec)-based encryption techniques and standards.
- Each message sent is in an encrypted form and is decrypted and converted back into plain text/original form at the recipient's end using encryption/decryption keys.
- Using the existing network services and application software, network encryption is invisible to the end user and operates independently of any other encryption processes used.
- Data is encrypted only while in transit, existing as plaintext on the originating and receiving hosts.
- Network encryption products and services are offered by a number of companies, such as Cisco.

Network Organization

Firewalls and Proxies

- A firewall is a host that mediates access to a network, allowing and disallowing certain types of access on the basis of a configured security policy.

- A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.
- Firewall accepts or rejects messages on the basis of external information rather than on the basis of the contents of the message.
- A filtering firewall performs access control on the basis of attributes of the packet headers, such as destination addresses, source addresses, and options.
- Routers and other infrastructure systems are typical examples of filtering firewalls.
- They allow connections through the firewall, usually on the basis of source and destination addresses and ports.
- This contrasts with the second type of firewall, which never allows such a direct connection. Instead, special agents called proxies control the flow of information through the firewall.
- A proxy is an intermediate agent or server that acts on behalf of an endpoint without allowing a direct connection between the two endpoints.
- A proxy (or applications level) firewall uses proxies to perform access control.
- A proxy firewall can base access control on the contents of packets and messages, as well as on attributes of the packet headers.

- A proxy firewall adds to a filtering firewall the ability to base access on content, either at the packet level or at a higher level of abstraction.
- A different point of view is to see the firewall as an audit mechanism.
- It analyzes the packets that enter. Firewalls can then base actions on this analysis, leading to traffic shaping (in which percentages of bandwidth are reserved for specific types of traffic), intrusion response, and other controls.

Demilitarized Zone (DMZ)

- In computer networks, a DMZ (demilitarized zone) is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet.
- External-facing servers, resources and services are located in the DMZ so they are accessible from the Internet but the rest of the internal LAN remains unreachable.
- A DMZ is now often referred to as a perimeter network.
- This provides an additional layer of security to the LAN as it restricts the ability of hackers to directly access internal servers and data via the Internet.

- Any service that is being provided to users on the Internet should be placed in the DMZ.
- The most common of these services are: Web, Mail, DNS, FTP, and VoIP.
- The term DMZ comes from the geographic buffer zone that was set up between North Korea and South Korea at the end of the Korean War.
- There are various ways to design a network with a DMZ. The two most common methods are with a single or dual firewalls as shown in the figure.
- A single firewall with at least three network interfaces can be used to create a network architecture containing a DMZ. The external network is formed from the ISP to the firewall on the first network interface, the DMZ is formed from the second network interface and the internal network is formed from the third network interface.
- Different sets of firewall rules for traffic between the Internet and the DMZ, the LAN and the DMZ, and the LAN and the Internet tightly control which ports and types of traffic are allowed into the DMZ from the Internet, limit connectivity to specific hosts in the internal network, and prevent unrequested connections either to the Internet or the internal LAN from the DMZ.

- A more secure approach is to use two firewalls to create a DMZ.
- The first firewall also called the perimeter firewall is configured to allow traffic destined to the DMZ only.
- The second or internal firewall only allows traffic from the DMZ to the internal network.
- This is considered more secure since two devices would need to be compromised before an attacker could access the internal LAN.
- For example, a network intrusion detection and prevention system located in a DMZ that only contains as Web server can block all traffic except HTTP and HTTPS requests on ports 80 and 443.

Analysis of Network Infrastructure:

- The security policy distinguishes “public” entities from those internal to the corporation, but recognizes that some corporate resources must be available to the public.
- The public entities may enter the corporate perimeter (bounded by the “outer firewall”) but are confined to the DMZ area (bounded inside by the “inner firewall”).
- The key decision is to limit the flow of information from the internal network to the DMZ.

- The public cannot communicate directly with any system in the internal network, nor can any system in the internal network communicate directly with other systems on the Internet (beyond the "outer firewall").
- The systems in the DMZ serve as mediators, with the firewalls providing the guards.
- The firewalls and the DMZ systems control all access to and from the Internet and filter all traffic in both directions.
- The first step is to hide the addresses of the internal network.
- In general, the internal network addresses can be any IP addresses, and the inner firewall can use a protocol such as the Network Address Translation protocol to map these internal host addresses to the firewall's Internet address.
- A more common method is to assign each host an address but not allow those addresses to leave the corporate network.
- All services are implemented as proxies in the outer firewall. However, electronic mail presents a special problem.
- The DMZ mail server must know an address in order for the internal mail server to pass mail back and forth.
- This need not be the actual address of the internal mail server. It could be a distinguished address that the inner firewall will recognize as representing the internal mail server.

- Similarly, the internal mail server must know an address for the DMZ mail server. These addresses can be fixed (in which case the DMZ DNS server is unnecessary).
- The Web server lies in the DMZ for the same reasons that a mail server lies in the DMZ. External connections to the Web server go into the DMZ and no farther.
- If any information is to be transmitted from the Web server to the internal network (for example, the customer data subnet), the transmission is made separately, and not as part of a Web transaction.
- The goals of the outer firewall are to restrict public access to the Drib's corporate network and to restrict the Drib's access to the Internet. This arises from the duality of information flow.
- In the Bell-LaPadula Model, for example, one cannot read information from a higher level (here, by restricting public access to the Drib's network), but one cannot write information to a lower level, either (here, by restricting the Drib's employees' access to the Internet).

- To implement the required access control, the firewall uses an access control list, which binds source addresses and ports and destination addresses and ports to access rights.
- The public needs to be able to access the Web server and mail server, and no other services. The firewall therefore presents an interface that allows connections to the WWW services (HTTP and HTTPS) and to electronic mail (SMTP).
- Sites on the Internet see the addresses of the Web and mail servers as the same—that of the firewall. No other services are provided to sites on the Internet.
- The firewall is a proxy-based firewall. When an electronic mail connection is initiated, the SMTP proxy on the firewall collects the mail. It then analyzes it for computer viruses and other forms of malicious logic. If none is found, it forwards the mail to the DMZ mail server.
- When a Web connection (or datagram) arrives, the firewall scans the message for any suspicious components (such as extraordinarily long lines or other evidence of attacks) and, if none is found, forwards it to the DMZ Web server.
- These two DMZ servers have different addresses, neither of which is the address of the firewall.
- Attackers trying to penetrate the firewall have three methods of entry.
- The first is to enter through the Web server ports.
- The unsecured (HTTP) port proxy checks for invalid or illegal HTTP requests and rejects them.
- The second is to enter through the SMTP port.
- The mail proxy will detect and reject such attempts.
- The third is to attempt to bypass the low-level firewall checks by exploiting vulnerabilities in the firewall itself.

•The internal network is where the Drib's most sensitive data resides.
•It may contain data, such as proprietary information, that the Drib does not want outsiders to see.
•For this reason, the inner firewall will block all traffic except for that specifically authorized to enter.
•All such information will come from the DMZ, and never directly from the Internet.
•Like the outer firewall, the inner firewall allows a limited set of traffic through (using the same type of access control mechanism as does the outer firewall).
•It allows SMTP connections using proxies, but all electronic mail is sent to the DMZ mail server for disposition.
•It allows limited transfer of information to the DNS server in the DMZ.

•It also allows system administrators to access the systems in the DMZ from a trusted administrative server. All other traffic, including Web access, is blocked.
•The Mail server in the DMZ performs address and content checking on all electronic mail messages.
•The goal is to hide internal information from the outside while being transparent to the inside.
•The Web server accepts and services requests from the Internet. It does not contact any servers or information sources within the internal network.
•This means that if the Web server is compromised, the compromise cannot affect internal hosts.
•The DMZ DNS host contains directory name service information about those hosts that the DMZ servers must know.
• It contains entries for the following.
• DMZ mail, Web hosts
• Internal trusted administrative host
• Outer firewall
• Inner firewall
Types of Firewalls

Packet filtering firewall:

- A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet
- The firewall is typically configured to filter packets going in both directions (from and to the internal network).
- Filtering rules are based on information contained in a network packet.

- Source IP address: The IP address of the system that originated the IP packet (e.g., 192.178.1.1)
- Destination IP address: The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2)
- Source and destination transport-level address: The transport-level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELNET
- IP protocol field: Defines the transport protocol.
- Interface: For a firewall with three or more ports, which interface of the firewall the packet came from or which interface of the firewall the packet is destined for.
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.

- If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken.

Two default policies are possible:
- Default = discard: That which is not expressly permitted is prohibited.
- Default = forward: That which is not expressly prohibited is permitted.
- Advantage of a packet filtering firewall is its simplicity. Also, packet filters typically are transparent to users and are very fast.
- Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions.

State-full packet filtering
- State-full packet filtering is a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.
- It is also known as dynamic packet filtering and Stateful inspection filtering.
- Only packets matching a known active connection are allowed to pass the firewall.
- It is a security feature often included in business networks.
- A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections.
- There is an entry for each currently established connection.
- The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.
- By recording session information such as IP addresses and port numbers, a dynamic packet filter can implement a much tighter security posture than a static packet filter can.
- In a firewall that uses stateful inspection, the network administrator can set the parameters to meet specific needs.
- In a typical network, ports are closed unless an incoming packet requests connection to a specific port and then only that port is opened.
- This practice prevents port scanning, a well-known hacking technique.

Application Level Gateway
- An application-level gateway, also called an application proxy, acts as a relay of application-level traffic.
- The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.

- When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.
- If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall.
- Application proxy filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered.
- Application-level gateways tend to be more secure than packet filters.
- In addition, it is easy to log and audit all incoming traffic at the application level.
- Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only examine a few allowable applications.
- A prime disadvantage of this type of gateway is the additional processing overhead on each connection.
- In effect, there are two spliced connections between the end users, with the gateway at the splice point, and the gateway must examine and forward all traffic in both directions.

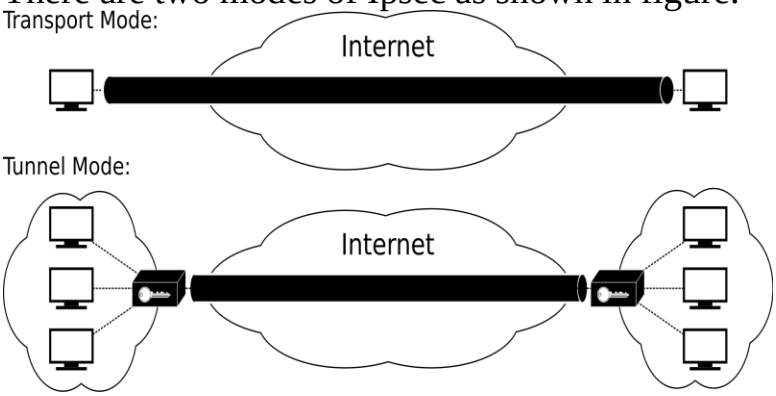
Circuit Level Gateway

- A fourth type of firewall is the circuit-level gateway or circuit-level proxy.
- The circuit level gateway firewalls work at the transport and session layer of the OSI model. They monitor TCP handshaking between the packets to determine if a requested session is legitimate.
- As with an application gateway, a circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.
- Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents.
- The security function consists of determining which connections will be allowed.
- A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users.
- The gateway can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections.
- In this configuration, the gateway can suffer the processing overhead of examining incoming application data for forbidden functions but does not suffer from that overhead on outgoing data.

Internet Protocol Security(IPSec)

- Internet Protocol Security (IPsec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network.
- Internet protocol security (IPsec) is a set of protocols that provides security for Internet Protocol. It can use cryptography to provide security.
- IPsec can be used for the setting up of virtual private networks (VPNs) in a secure manner.
- IPsec involves two security services:
- Authentication Header (AH): This authenticates the sender and it discovers any changes in data during transmission.
- Encapsulating Security Payload (ESP): This not only performs authentication for the sender but also encrypts the data being sent.
- IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

There are two modes of Ipsec as shown in figure:



- **Tunnel Mode:** This will take the whole IP packet to form secure communication between two places, or gateways.
- **Transport Mode:** This only encapsulates the IP payload (not the entire IP packet as in tunnel mode) to ensure a secure channel of communication.

Virtual Private Network (VPN)

- A virtual private network extends a private network across a public network, and 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.

- A VPN consists of a set of computers that interconnect by means of a relatively unsecure network and that make use of encryption and special protocols to provide security.
- At each corporate site, workstations, servers, and databases are linked by one or more local area networks (LANs).
- The Internet or some other public network can be used to interconnect sites, providing a cost savings over the use of a private network and offloading the wide area network management task to the public network provider.
- That same public network provides an access path for telecommuters and other mobile employees to log on to corporate systems from remote sites.
- A fundamental requirement for VPN is security.
- Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users.
- To counter this problem, a VPN is needed. In essence, a VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.
- VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends.
- The encryption may be performed by firewall software or possibly by routers.
- The most common protocol mechanism used for this purpose is at the IP level and is known as Ipsec.
- An organization maintains LANs at dispersed locations.
- A logical means of implementing an IPsec is in a firewall which is shown in the figure.

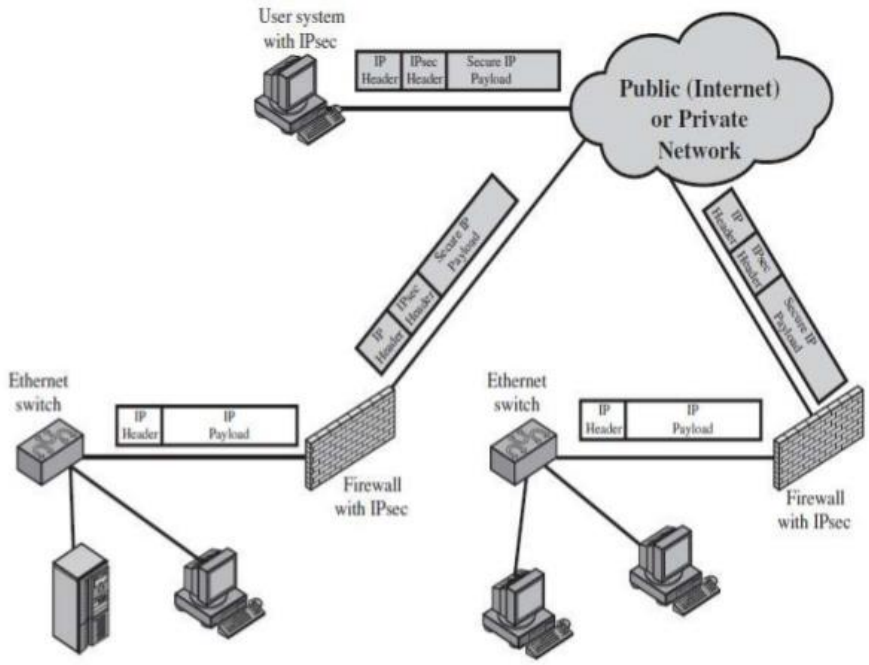


Figure 22.4 A VPN Security Scenario

- If IPsec is implemented in a separate box behind (internal to) the firewall, then VPN traffic passing through the firewall in both directions is encrypted.
- In this case, the firewall is unable to perform its filtering function or other security functions, such as access control, logging, or scanning for viruses.
- IPsec could be implemented in the boundary router, outside the firewall.
- However, this device is likely to be less secure than the firewall and thus less desirable as an IPsec platform.

Unit-4: Digital Signatures and Authentication Protocols

Authentication Basics

- Authentication is the verification of the credentials of the connection attempt.
- Authentication is the binding of an identity to a subject.
- This process consists of sending the credentials from the remote access client to the remote access server in an either plaintext or encrypted form by using an authentication protocol.
- The external entity must provide information to enable the system to confirm its identity.
- This information comes from one (or more) of the following.
- What the entity knows (such as passwords or secret information)
- What the entity has (such as a badge or card)

- What the entity is (such as fingerprints or retinal characteristics)
- Where the entity is (such as in front of a particular terminal)
- The authentication process consists of obtaining the authentication information from an entity, analyzing the data, and determining if it is associated with that entity.
- This means that the computer must store some information about the entity.
- We can represent these requirements in an authentication system consisting of five components.
- The set A of authentication information is the set of specific information with which entities prove their identities.
- The set C of complementary information is the set of information that the system stores and uses to validate the authentication information.
- The set F of complementation functions that generate the complementary information from the authentication information. That is, for $f \in F$, $f: A \rightarrow C$.
- The set L of authentication functions that verify identity. That is, for $l \in L$, $l: A \times C \rightarrow \{ \text{true, false} \}$.
- The set S of selection functions that enable an entity to create or alter the authentication and complementary information.

Passwords

- A password is an information associated with an entity that confirms the entity's identity.
- Passwords are an example of an authentication mechanism based on what people know: the user supplies a password, and the computer validates it.
- If the password is the one associated with the user, that user's identity is authenticated.
- If not, the password is rejected and the authentication fails.
- The goal of an authentication system is to ensure that entities are correctly identified.
- If one entity can guess another's password, then the guesser can impersonate the other.
- The authentication model provides a systematic way to analyze this problem.
- The goal is to:
- Hide authentication information
- Prevent access to the authentication functions.

Attacking a Password System

- The simplest attack against a password-based system is to guess passwords.

- Attackers can guess passwords locally or remotely using either a manual or automated approach.
- Most networks aren't configured to require long and complex passwords, and an attacker needs to find only one weak password to gain access to a network.
- Automated password guessing programs and crackers use several different approaches.
- **A Dictionary attack** is the guessing of a password by repeated trial and error.
- A hacker uses a program or script to try to login by cycling through combinations of common words.
- Dictionary attacks work on the assumption that most passwords consist of whole words, dates, or numbers taken from a dictionary.
- Dictionary attack tools require a dictionary input list.
- **In Brute Force attack**, a hacker uses a computer program or script to try to log in with possible password combinations, usually starting with the easiest-to-guess passwords until the result is obtained.
- The most time consuming—and most successful—attack method is the brute-force attack, in which the attacker tries every possible combination of characters for a password, given a character set (e.g., abcd…ABCD…1234…!@#$) and a maximum password length.

- **Hybrid password** guessing attacks assume that network administrators push users to make their passwords at least slightly different from a word that appears in a dictionary.
- **Hybrid guessing** rules vary from tool to tool, but most mix uppercase and lowercase characters, add numbers at the end of the password, spell the password backward or slightly misspell it, and include characters such as @!# in the mix.
- **Keystroke logging**, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard secretly so that the person using the keyboard is unaware that their actions are being monitored.
- Data can then be retrieved by the person operating the logging program.
- Attackers often find it much easier to reset passwords than to guess them.
- Many password cracking programs are actually password resetters.
- In most cases, the attacker boots from a floppy disk or CD-ROM to get around the typical Windows protections.
- Most password resetters contain a bootable version of Linux that can mount NTFS volumes and can help you locate and reset the Administrator's password.
- A widely used password reset tool is the free Petter Nordahl-Hagen program.

Phishing:

- Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels.
- The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims.
- Phishing is popular with cybercriminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate phishing email than trying to break through a computer's defenses.
- Phishing attacks are very simple to avoid.
- When you are asked to put your personal information into a website, look up into the URL bar. If for example you are supposed to be on gmail.com and in the URL bar it says something completely different like gmail.randomsite.com, or gamilmail.com, then you know this is a fake.
- When you are on the real gmail website, the URL should begin with www.gmail.com, everything else is a fake.

Countering password guessing

- Password guessing requires either the set of complementation functions and complementary information or access to the authentication functions.
- In both approaches, the goal of the defenders is to maximize the time needed to guess the password.

Some common password guessing are:

- Random selection of passwords
- Pronounceable passwords
- User Selection of passwords
- Passwords based on account and user names
- Dictionary words
- Patterns from keyword
- Passwords shorter than six characters
- Passwords containing only digits
- Passwords containing only uppercase or lowercase letters, or letters and numbers, or letters and punctuation
- Passwords used in the past
- Passwords with too many characters in common with the previous (current) password

- Reusable Passwords and Dictionary Attacks
- Password reuse is a problem where people try to remember multiple passwords for everything they interact with on a regular basis, but instead use the same password on multiple systems, tiers of applications, or even social sites.
- Guessing Through Authentication Functions

Password Aging

- Password aging is the requirement that a password be changed after some period of time has passed or after some event has occurred.
- Guessing of passwords requires that access to the complement, the complementation functions, and the authentication functions be obtained.
- If none of these have changed by the time the password is guessed, then the attacker can use the password to access the system.
- Assume that the expected time to guess a password is 180 days.
- Then changing the password more frequently than every 180 days will, in theory, reduce the probability that an attacker can guess a password that is still being used.
- In practice, aging by itself ensures little, because the estimated time to guess a password is an average; it balances those passwords that can be easily guessed against those that cannot.
- If users can choose passwords that are easy to guess, the estimation of the expected time must look for a minimum, not an average.
- There are problems involved in implementing password aging.
- The first is forcing users to change to a different password.
- The second is providing notice of the need to change and a user-friendly method of changing passwords.
- Password aging is useless if a user can simply change the current password to the same thing.
- One technique to prevent this is to record the n previous passwords.
- When a user changes a password, the proposed password is compared with these n previous ones.
- If there is a match, the proposed password is rejected.
- The problem with this mechanism is that users can change passwords n times very quickly, and then change them back to the original passwords.
- This defeats the goal of password aging.
- An alternative approach is based on time. In this implementation, the user must change the password to one other than the current password.

Challenge Response

- Passwords have the fundamental problem that they are reusable.
- If an attacker sees a password, she can later replay the password.
- The system cannot distinguish between the attacker and the legitimate user, and allows access.
- An alternative is to authenticate in such a way that the transmitted password changes each time.
- Then, if an attacker replays a previously used password, the system will reject it.
- Let user U desire to authenticate himself to system S.
- Let U and S have an agreed-on secret function f.
- A challenge-response authentication system is one in which S sends a random message m (the challenge) to U, and U replies with the transformation r = f(m) (the response).
- S validates r by computing it separately.
- Challenge-response algorithms are similar to the IFF (identification—friend or foe) techniques that military airplanes use to identify allies and enemies.

Pass Algorithms

- Let there be a challenge-response authentication system in which the function f is the secret. Then f is called a pass algorithm.
- Under this definition, no cryptographic keys or other secret information may be input to f.
- The algorithm computing f is itself the secret.

One-Time Passwords

- A one-time password is a password that is invalidated as soon as it is used.
- The ultimate form of password aging occurs when a password is valid for exactly one use.
- In some sense, challenge-response mechanisms use one-time passwords.
- Think of the response as the password.
- As the challenges for successive authentications differ, the responses differ.
- A mechanism that uses one-time passwords is also a challenge-response mechanism.
- The challenge is the number of the authentication attempt; the response is the one-time password.
- The problems in any one-time password scheme are the generation of random passwords and the synchronization of the user and the system.
- The former problem is solved by using a cryptographic hash function or enciphering function such as the DES, and the latter by having the system inform

the user which password it expects—for example, by having all the user's passwords numbered and the system providing the number of the one-time password it expects.

Hardware-Supported Challenge-Response Procedures

- Hardware support comes in two forms: a program for a general-purpose computer and special-purpose hardware support.
- Both perform the same functions.
- The first type of hardware device, informally called a token, provides mechanisms for hashing or enciphering information.
- With this type of device, the system sends a challenge.
- The user enters it into the device. The device returns the appropriate response.
- Some devices require the user to enter a personal identification number or password, which is used as a cryptographic key or is combined with the challenge to produce the response.
- The second type of hardware device is temporally based.
- Every 60 seconds, it displays a different number.
- The numbers range from 0 to 10^n – 1, inclusive.
- A similar device is attached to the computer.
- It knows what number the device for each registered user should display.
- To authenticate, the user provides his login name. The system requests a password.
- The user then enters the number shown on the hardware device, followed by a fixed (reusable) password.
- The system validates that the number is the one expected for the user at that time and that the reusable portion of the password is correct.

Challenge-Response and Dictionary Attacks

- Whether or not a challenge-response technique is vulnerable to a dictionary attack depends on the nature of the challenge and the response.
- In general, if the attacker knows the challenge and the response, a dictionary attack proceeds as for a reusable password system.
- Suppose a user is authenticating himself using a challenge-response system.
- The system generates a random challenge r, and the user returns the value Ek(r) of r enciphered using the key k.
- Then the attacker knows both r and Ek(r) and can try different values of k until the encipherment of r matches Ek(r).

- In practice, it is not necessary to know the value of r.
- Most challenges are composed of random data combined with public data that an attacker can determine.

Biometrics

- Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics.
- Identification by physical characteristics is as old as humanity.
- Recognizing people by their voices or appearance, and impersonating people by assuming their appearance, was widely known in classical times.
- Efforts to find physical characteristics that uniquely identify people include the fingerprints, and DNA sampling.
- Using such a feature to identify people for a computer would ideally eliminate errors in authentication.
- Biometrics is the automated measurement of biological or behavioral features that identify a person .
- When a user is given an account, the system administration takes a set of measurements that identify that user to an acceptable degree of error.
- Whenever the user accesses the system, the biometric authentication mechanism verifies the identity.
- Lawton points out that this is considerably easier than identifying the user because no searching is required.
- A comparison to the known data for the claimed user's identity will either verify or reject the claim.
- Common characteristics are fingerprints, voice characteristics, eyes, facial features, and keystroke dynamics.

Fingerprints

- A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger.
- Fingerprints can be scanned optically, but the cameras needed are bulky.
- A capacitive technique uses the differences in electrical charges of the patterns on the finger to detect those parts of the finger touching a chip and those raised.
- The data is converted into a graph in which ridges are represented by vertices and vertices corresponding to adjacent ridges are connected.
- Each vertex has a number approximating the length of the corresponding ridge.
- At this point, determining matches becomes a problem of graph matching.

- This problem is similar to the classical graph isomorphism problem (similarity between graphs), but because of imprecision in measurements, the graph generated from the fingerprint may have different numbers of edges and vertices.
- Thus, the matching algorithm is an approximation.

Voices

- Authentication by voice, also called speaker verification or speaker recognition, involves recognition of a speaker's voice characteristics or verbal information verification.
- The former uses statistical techniques to test the hypothesis that the speaker's identity is as claimed.
- The system is first trained on fixed passphrases or phonemes that can be combined.
- To authenticate, either the speaker says the pass-phrase or repeats a word (or set of words) composed of the learned phonemes.
- Verbal information verification deals with the contents of utterances (loud voice expression).
- The system asks a set of questions such as "What is your mother's maiden name?" and "In which city were you born?"
- It then checks that the answers spoken are the same as the answers recorded in its database.
- The key difference is that speaker verification techniques are speaker-dependent, but verbal information verification techniques are speaker-independent, relying only on the content of the answers.

Eyes

- Authentication by eye characteristics uses the iris and the retina. Patterns within the iris are unique for each person.
- Hence, one verification approach is to compare the patterns statistically and ask whether the differences are random.
- A second approach is to correlate the images using statistical tests to see if they match.
- Retinal scans rely on the uniqueness of the patterns made by blood vessels at the back of the eye.
- This requires a laser beaming onto the retina, which is highly intrusive.
- This method is typically used only in the most secure facilities.

Faces

- Face recognition consists of several steps. First, the face is located.
- If the user places his/her face in a predetermined position (for example, by resting her chin on a support), the problem becomes somewhat easier.
- However, facial features such as hair and glasses may make the recognition harder.
- Techniques for doing this include the use of neural networks and templates.
- The resulting image is then compared with the relevant image in the database.
- The correlation is affected by the differences in the lighting between the current image and the reference image, by distortion, by "noise," and by the view of the face. The correlation mechanism must be "trained."
- Several different methods of correlation have been used, with varying degrees of success.
- An alternative approach is to focus on the facial features such as the distance between the nose and the chin, and the angle of the line drawn from one to the other.

Keystrokes

- Keystroke dynamics refers to the automated method of identifying or confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard.
- Keystroke dynamics requires a signature based on keystroke intervals, keystroke pressure, keystroke duration, and where the key is struck (on the edge or in the middle).
- This signature is believed to be unique in the same way that written signatures are unique.
- Keystroke recognition can be both static and dynamic.
- Static recognition is done once, at authentication time, and usually involves typing of a fixed or known string.
- Once authentication has been completed, an attacker can capture the connection (or take over the terminal) without detection.
- Dynamic recognition is done throughout the session, so the aforementioned attack is not feasible.
- However, the signature must be chosen so that variations within an individual's session do not cause the authentication to fail.
- For example, keystroke intervals may vary widely, and the dynamic recognition mechanism must take this into account.

- The statistics gathered from a user's typing are then run through statistical tests (which may discard some data as invalid, depending on the technique used) that account for acceptable variance in the data.

Combinations

- Several researchers have combined some of the techniques described above to improve the accuracy of biometric authentication.

- Plankensteiner and Wagner combined voice sounds and lip motion with the facial image.
- Duc, Bigun, Maire, and Fischer describe a "supervisor module" for melding voice and face recognition with a success rate of 99.5%.
- The results indicate that a higher degree of accuracy can be attained than when only a single characteristic is used.

Caution

- Because biometrics measures characteristics of the individual, people are tempted to believe that attackers cannot pose as authorized users on systems that use biometrics.
- Two assumptions underlie this belief.
- The first is that biometric device is accurate in the environment in which it is used.
- For example, if a fingerprint scanner is under observation, having it scan a mask of another person's finger would be detected.
- But if it is not under observation, such a trick might not be detected and the unauthorized user might gain access.
- The second assumption is that the transmission from the biometric device to the computer's analysis process is tamperproof.
- Otherwise, one could record a legitimate authentication and replay it later to gain access.

Location

- Denning and MacDoran suggested an innovative approach to authentication.
- The reason that if a user claims to be Anna, who is at that moment working in a bank in California but is also logging in from Russia at the same time, the user is impersonating Anna.
- Their scheme is based on the Global Positioning System(GPS), which can pinpoint a location to within a few meters.

- The physical location of an entity is described by a location signature derived from the GPS satellites.
- Each location (to within a few meters) and time (to within a few milliseconds) is unique, and hence form a location signature.
- This signature is transmitted to authenticate the user.
- The host also has a location signature sensor (LSS) and obtains a similar signature for the user.
- If the signatures disagree, the authentication fails.

- This technique relies on special-purpose hardware.
- If the LSS is stolen, the thief would have to log in from an authorized geographic location.
- Because the signature is generated from GPS data, which changes with respect to time, location, and a variety of unpredictable actions resulting from the nature of the electromagnetic waves used to establish position, any such signature would be unique and could not be forged.
- Moreover, if intercepted, it could not be replayed except within the window of temporal uniqueness.
- This technique can also restrict the locations from which an authorized user can access the system.
- An interesting point is that the authentication can be done continuously.
- The LSS simply intermingles signature data with the transmitted data, and the host checks it.
- If the connection were hijacked, the data from the LSS would be lost.

Multiple Methods

- Authentication methods can be combined, or multiple methods can be used.
- Authenticating by location generally uses special-purpose hardware.
- Although the key feature of this technique is physical location, without the LSS it will not work.
- Techniques using multiple methods assign one or more authentication methods to each entity.
- The entity must authenticate using the specific method, or methods, chosen.
- The specific authentication methods vary from system to system, but in all cases the multiple layers of authentication require an attacker to know more, or possess more, than is required to spoof a single layer.
- Some versions of the UNIX operating system provide a mechanism called pluggable authentication modules (PAM).

- A pluggable authentication module is a mechanism to integrate multiple low-level authentication schemes into a high-level application programming interface.
- It allows programs that rely on authentication to be written independently of the underlying authentication scheme.
- When a program authenticates a user, it invokes a library routine, pam_authenticate, that accesses set of configuration files.

Mutual(Symmetric, Public Key)

- Mutual authentication, also called two-way authentication, is a process or technology in which both client and server authenticate each other's identities before actual communication occurs.
- In a network environment, the client authenticates the server and vice-versa.
- This authentication process is common in web-based and online applications. This is to ensure that clients are communicating exclusively with legitimate entities or servers and so the servers can be certain that the client attempting access has a legitimate purpose.
- Mutual authentication is gaining acceptance as a tool that can minimize the risk of online fraud in e-commerce.
- The identities can be proven using trusted third parties and by using shared secrets or through cryptographic methods like a public key infrastructure.
- So in a web-based mutual authentication process, communication can occur only if the client and the server trust each other's digital certificates.
- The certificate exchange is done through Transport Layer Security (TLS) protocol.
- The core essence of this process is that neither party trusts the other until identities are proven.
- This simply means that the server must be sure of who the client is and the client must be sure of the server.
- This prevents security from being compromised through simple attacks like impersonation.

Establishing the authentication using certificate-based 2-Way SSL involves:

- A client requests access to a protected resource.
- The server presents its certificate to the client.
- The client verifies the server's certificate.
- If successful, the client sends its certificate to the server.
- The server verifies the client's credentials.
- If successful, the server grants access to the protected resource requested by the client.

One-Way(Symmetric, Public Key)

- One-way authentication is a process or technology in which only client authenticates server's identity before actual communication occurs.
- This is to ensure that clients are communicating exclusively with legitimate servers.
- Establishing the authentication using certificate-based 1-Way SSL involves:
- A client requests access to a protected resource.
- The server presents its certificate to the client.
- The client verifies the server's certificate.
- If successful, the client authenticates the server as legitimate.

Digital Signature:

- A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature.
- A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.
- The signature guarantees the source and integrity of the message.
- The most important development from the work on public-key cryptography is the digital signature.
- Typically the signature is formed by taking the hash of the message and encrypting the message with the creator's private key.
- The digital signature provides a set of security capabilities that would be difficult to implement in any other way.
- The digital signature must have the following properties:
- It must verify the author and the date and time of the signature.
- It must authenticate the contents at the time of the signature.
- It must be verifiable by third parties, to resolve disputes.
- Thus, the digital signature function includes the authentication function.

- Digital signatures are based on public key cryptography, also known as asymmetric cryptography.
- Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public.
- To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed.

- The private key is then used to encrypt the hash.
- The encrypted hash is the digital signature.
- The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter.
- This saves time since hashing is much faster.
- The value of the hash is unique to the hashed data.
- Any change in the data, even changing or deleting a single character, results in a different value.
- This attribute enables others to validate the integrity of the data by using the signer's public key to decrypt the hash.
- If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed.
- If the two hashes don't match, the data has either been tampered with in some way (integrity) or the signature was created with a private key that doesn't correspond to the public key presented by the signer (authentication).

Direct Digital Signature

- The term direct digital signature refers to a digital signature scheme that involves only the communicating parties (source, destination).
- It is assumed that the destination knows the public key of the source.
- Confidentiality can be provided by encrypting the entire message plus signature with a shared secret key (symmetric encryption).
- Note that it is important to perform the signature function first and then an outer confidentiality function.
- In case of dispute, some third party must view the message and its signature.
- If the signature is calculated on an encrypted message, then the third party also needs access to the decryption key to read the original message.
- However, if the signature is the inner operation, then the recipient can store the plaintext message and its signature for later use in dispute resolution.

Arbitrated Digital Signature

- Implementing an arbitrated digital signature invites a third party into the process called a "trusted arbiter."
- The role of the trusted arbiter is usually twofold: first this independent third party verifies the integrity of the signed message or data.

- Second, the trusted arbiter dates or time-stamps the document, verifying receipt and the passing on of the signed document to its intended final destination.
- This approach requires suitable level of trust in arbiter to ensure that the arbiter is not biased and unauthorized modification won't be done.
- This can be implemented with either private or public-key algorithms.

Digital Certificate

- A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI).
- A digital certificate may also be referred to as a public key certificate or identity certificate.
- A digital certificate authenticates the Web credentials of the sender and lets the recipient of an encrypted message know that the data is from a trusted source (or a sender who claims to be one).

- A digital certificate is issued by a certification authority (CA).
- A person (sender), who is sending an encrypted message may obtain a digital certificate from a CA to ensure authenticity.
- The CA issues the digital certificate with the applicant's public key, along with other information such as holder name, serial number, date of expiration and a digital CA signature.
- It also issues its own public key in the public domain via the Web.
- When a Web message is transmitted, a digital certificate serves as an encrypted attachment containing the public key and other relevant identifying data.
- When the recipient receives the message, the digital certificate is decoded using the CA's public key.
- Using various information residing in the digital certificate, the recipient can send an encrypted reply back to the sender.
- Digital certificates verify website authenticity and legitimacy.
- A browser may display an unsafe digital certificate alert but still permit user entry.
- This warning signals that the website is a threat and security risk.
- The most common digital certificate standard is X.509.

X.509 Certificate

- An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure (PKI) standard to verify that a public

key belongs to the user, computer or service identity contained within the certificate.

- An X.509 certificate contains information about the identity to which a certificate is issued and the identity that issued it.
- Standard information in an X.509 certificate includes:
- Version – which X.509 version applies to the certificate (which indicates what data the certificate must include)
- Serial number – the identity creating the certificate must assign it a serial number that distinguishes it from other certificates
- Algorithm information – the algorithm used by the issuer to sign the certificate
- Issuer distinguished name – the name of the entity issuing the certificate (usually a certificate authority)
- Validity period of the certificate – start/end date and time
- Subject distinguished name – the name of the identity the certificate is issued to
- Subject public key information – the public key associated with the identity
- Extensions (optional)

Many of the certificates that people refer to as Secure Sockets Layer (SSL) certificates are in fact X.509 certificates.

Authentication Protocols

- An authentication protocol is a type of cryptographic protocol specifically designed for transfer of authentication data between two entities.
- It allows the receiving entity to authenticate the connecting entity (e.g. Client connecting to a Server) as well as authenticate itself to the connecting entity (Server to a client) by declaring the type of information needed for authentication.
- The task of the authentication protocol is to specify the exact series of steps needed for execution of the authentication.
- It has to comply with the main protocol principles:

 A Protocol has to involve two or more parties and everyone involved in the protocol must know the protocol in advance.

 All the included parties have to follow the protocol.

 A protocol has to be unambiguous - each step must be defined precisely.

 A protocol must be complete - must include a specified action for every possible situation.

- Authentication Protocols are used mainly by Point-to-Point Protocol (PPP) servers to validate the identity of remote clients before granting them access to server data.
- Most of them are using a password as the cornerstone of the authentication.
- The password has to be shared between the communicating entities in advance.
- Some common types of authentication protocols are:

PAP- Password Authentication Protocol

- Password Authentication Protocol is one of the oldest authentication protocols. Authentication is initialized by client/user by sending packet with credentials (username and password) at the beginning of the connection.
- It is highly insecure because the credentials are being transmitted over the network in plain ASCII text thus it is vulnerable even to the most simple attacks like Eavesdropping and man-in-the-middle based attacks.

- Server sends a random string (usually 128B long).
- Client uses his password and the string received as parameters for MD5 hash function and then sends the result together with username in plain text.
- Server uses the username to apply the same function and compares the calculated and received hash.
- An authentication is either successful or unsuccessful.

EAP - Extensible Authentication Protocol

- EAP was originally developed for PPP(Point-to-Point Protocol) but today is widely used in IEEE 802.1x authentication framework.
- The advantage of EAP is that it is only a general authentication framework for client-server authentication - the specific way of authentication is defined in its many versions called EAP-methods.
- More than 40 EAP-methods exist, the most common is EAP-MD5.

Authentication Service: Kerberos V4

- Kerberos is a protocol for authenticating service requests between trusted hosts across an untrusted network, such as the internet.
- Kerberos is built in to all major operating systems including Microsoft Windows, Apple OS and Linux.
- Kerberos was originally developed for Project Athena at the Massachusetts Institute of Technology (MIT).

- The name Kerberos was taken from Greek mythology; Kerberos was a three-headed dog who guarded the gates of Hades.
- The three heads of the Kerberos protocol represent a client, a server and a Key Distribution Center (KDC), which acts as Kerberos' trusted third-party authentication service.
- KDC provides two services: an authentication service and a ticket granting service.
- KDC "tickets" provide mutual authentication, allowing nodes to prove their identity to one another in a secure manner.
- Kerberos authentication uses DES cryptography to prevent packets traveling across the network from being read or changed and to protect messages from eavesdropping and replay attacks.
- To start the Kerberos authentication process, the initiating client sends a request to an authentication server for access to a service.
- The initial request is sent as plaintext because no sensitive information is included in the request.
- The authentication server retrieves the initiating client's private key, assuming the initiating client's username is in the KDC database.
- If the initiating client's username cannot be found in the KDC database, the client cannot be authenticated and the authentication process stops.
- If the client's username can be found in the KDC database, the authentication server generates a session key and a ticket granting ticket.
- The ticket granting ticket is timestamped and encrypted by the authentication server with the initiating client's password.
- The initiating client is then prompted for a password; if what is entered matches the password in the KDC database, the encrypted ticket granting ticket sent from the authentication server is decrypted and used to request a credential from the ticket granting server for the desired service.
- The client sends the ticket granting ticket to the ticket granting server, which may be physically running on the same hardware as the authentication server, but performing a different role.
- The ticket granting service carries out an authentication check similar to that performed by the authentication server, but this time sends credentials and a ticket to access the requested service.
- This transmission is encrypted with a session key specific to the user and service being accessed.
- This proof of identity can be used to access the requested "kerberized" service, which, once having validated the original request, will confirm its identity to the requesting system.

- The timestamped ticket sent by the ticket granting service allows the requesting system to access the service using a single ticket for a specific time period without having to be re-authenticated.
- Making the ticket valid for a limited time period makes it less likely that someone else will be able to use it later.

Digital Signature Standard(DSS)

- Digital Signature Standard (DSS) is the digital signature algorithm (DSA) developed by the U.S. National Security Agency (NSA) to generate a digital signature for the authentication of electronic documents.
- The Digital Signature Standard is intended to be used in electronic funds transfer, software distribution, electronic mail, data storage and applications which require high data integrity assurance.
- The algorithm used behind the Digital Signature Standard is known as the Digital Signature Algorithm.
- The algorithm makes use of two large numbers which are calculated based on a unique algorithm.
- The digital signatures can be generated only by the authorized person using their private keys and the users or public can verify the signature with the help of the public keys provided to them.
- However, one key difference between encryption and signature operation in the Digital Signature Standard is that encryption is reversible, whereas the digital signature operation is not.
- Another fact about the digital signature standard is that it does not provide any capability with regards to key distribution or exchange of keys.
- In other words, security of the digital signature standard largely depends on the secrecy of the private keys of the signatory.
- The Digital Signature Standard ensures that the digital signature can be authenticated and the electronic documents carrying the digital signatures are secure.
- The standard also ensures non-repudiation with regards to the signatures and provides security for improper tampering.
- The standard also ensures that digital signed documents can be tracked.

DSS Approach vs RSA Approach

- The above figure contrasts the DSS approach for generating digital signatures to that used with RSA.

- In the RSA approach, the message to be signed is input to a hash function that produces a secure hash code of fixed length.
- This hash code is then encrypted using the sender's private key to form the signature.
- Both the message and the signature are then transmitted.
- The recipient takes the message and produces a hash code.
- The recipient also decrypts the signature using the sender's public key.
- If the calculated hash code matches the decrypted signature, the signature is accepted as valid.
- Because only the sender knows the private key, only the sender could have produced a valid signature.
- The DSS approach also makes use of a hash function.
- The hash code is provided as input to a signature function along with a random number generated for this particular signature.
- The signature function also depends on the sender's private key and a set of parameters known to a group of communicating principals.
- We can consider this set to constitute a global public key.
- The result is a signature consisting of two components, labeled s and r.
- At the receiving end, the hash code of the incoming message is generated.
- This plus the signature is input to a verification function.
- The verification function also depends on the global public key as well as the sender's public key , which is paired with the sender's private key.
- The output of the verification function is a value that is equal to the signature component if the signature is valid.
- The signature function is such that only the sender, with knowledge of the private key, could have produced the valid signature.

UNIT 5

Design Principles and Common Security related programming problems

Principles for the design and implementation of security mechanisms

- Saltzer and Schroeder describe eight principles for the design and implementation of security mechanisms.
- The principles draw on the ideas of simplicity and restriction.
- Simplicity makes designs and mechanisms easy to understand.
- More importantly, less can go wrong with simple designs.
- Minimizing the interaction of system components minimizes the number of sanity checks on data being transmitted from one component to another.

- Simplicity also reduces the potential for inconsistencies within a policy or set of policies.
- Restriction minimizes the power of an entity. The entity can access only information it needs.
- Entities can communicate with other entities only when necessary, and in as few and narrow ways as possible.

Principle of Least Privilege

- The principle of least privilege states that a subject should be given only those privileges that it needs in order to complete its task.
- If a subject does not need an access right, the subject should not have that right.
- Furthermore, the function of the subject (as opposed to its identity) should control the assignment of rights.
- If a specific action requires that a subject's access rights be increased, those extra rights should be withdrawn immediately on completion of the action.
- This is the analogue of the "need to know" rule: if the subject does not need access to an object to perform its task, it should not have the right to access that object.
- More precisely, if a subject needs to append to an object, but not to alter the information already contained in the object, it should be given append rights and not write rights.
- E.g. The UNIX operating system does not apply access controls to the user root.

- That user can terminate any process and read, write, or delete any file. Thus, users who create backups can also delete files.
- The administrator account on Windows has the same powers.

Principle of Fail-Safe Defaults

- The principle of fail-safe defaults states that, unless a subject is given explicit access to an object, it should be denied access to that object.
- This principle requires that the default access to an object is none.
- Whenever access, privileges, or some security-related attribute is not explicitly granted, it should be denied.
- Moreover, if the subject is unable to complete its action or task, it should undo those changes it made in the security state of the system before it terminates.
- This way, even if the program fails, the system is still safe.

- E.g. If the mail server is unable to create a file in the spool directory(waiting queue for printing), it should close the network connection, issue an error message, and stop.
- It should not try to store the message elsewhere or to expand its privileges to save the message in another location, because an attacker could use that ability to overwrite other files or fill up other disks (a denial of service attack).

Principle of Economy of Mechanism

- The principle of economy of mechanism states that security mechanisms should be as simple as possible.
- This principle simplifies the design and implementation of security mechanisms.
- If a design and implementation are simple, fewer possibilities exist for errors.
- The checking and testing process is less complex, because fewer components and cases need to be tested.
- Complex mechanisms often make assumptions about the system and environment in which they run.
- If these assumptions are incorrect, security problems may result.

Principle of Complete Mediation

- The principle of complete mediation requires that all accesses to objects be checked to ensure that they are allowed.
- This principle restricts the caching of information, which often leads to simpler implementations of mechanisms.
- Whenever a subject attempts to read an object, the operating system should mediate the action.
- First, it determines if the subject is allowed to read the object.
- If so, it provides the resources for the read to occur.
- If the subject tries to read the object again, the system should check that the subject is still allowed to read the object.
- Most systems would not make the second check.
- They would cache the results of the first check and base the second access on the cached results.
- E.g. When a UNIX process tries to read a file, the operating system determines if the process is allowed to read the file.
- If so, the process receives a file descriptor encoding the allowed access.
- Whenever the process wants to read the file, it presents the file descriptor to the kernel.

- The kernel then allows the access.
- If the owner of the file disallows the process permission to read the file after the file descriptor is issued, the kernel still allows access.
- This scheme violates the principle of complete mediation, because the second access is not checked.
- The cached value is used, resulting in the denial of access being ineffective.

Principle of Open Design

- The principle of open design states that the security of a mechanism should not depend on the secrecy of its design or implementation.
- This principle suggests that complexity does not add security.
- Designers and implementers of a program must not depend on secrecy of the details of their design and implementation to ensure security.
- If the strength of the program's security depends on the ignorance of the user, a knowledgeable user can defeat that security mechanism.
- The term "security through obscurity" captures this concept exactly.
- This is especially true of cryptographic software and systems.
- Because cryptography is a highly mathematical subject, companies that market cryptographic software or use cryptography to protect user data frequently keep their algorithms secret.
- Experience has shown that such secrecy adds little if anything to the security of the system.
- Worse, it gives an quality of strength that is all too often lacking in the actual implementation of the system.

- Keeping cryptographic keys and passwords secret does not violate this principle, because a key is not an algorithm.
- However, keeping the enciphering and deciphering algorithms secret would violate it.

Principle of Separation of Privilege

- The principle of separation of privilege states that a system should not grant permission based on a single condition.
- This principle is restrictive because it limits access to system entities.
- The systems and programs granting access to resources should do so only when more than one condition is met.
- This provides a fine-grained control over the resource as well as additional assurance that the access is authorized.

- E.g. On Berkeley-based versions of the UNIX operating system, users are not allowed to change from their accounts to the root account unless two conditions are met.
- The first condition is that the user knows the root password.
- The second condition is that the user is in the wheel group (the group with GID 0).
- Meeting either condition is not sufficient to acquire root access; meeting both conditions is required.

Principle of Least Common Mechanism

- The principle of least common mechanism states that mechanisms used to access resources should not be shared.
- This principle is restrictive because it limits sharing.
- Sharing resources provides a channel along which information can be transmitted, and so such sharing should be minimized.
- In practice, if the operating system provides support for virtual machines, the operating system will enforce this privilege automatically to some degree.
- Otherwise, it will provide some support (such as a virtual memory space) but not complete support (because the file system will appear as shared among several processes).
- E.g. A Web site provides electronic commerce services for a major company.
- Attackers want to deprive the company of the revenue it obtains from that Web site.
- They flood the site with messages and tie up the electronic commerce services.
- Legitimate customers are unable to access the Web site and, as a result, take their business elsewhere.
- Here, the sharing of the Internet with the attackers' sites caused the attack to succeed.
- The appropriate countermeasure would be to restrict the attackers' access to the segment of the Internet connected to the Web site.

Principle of Psychological Acceptability

- The principle of psychological acceptability states that security mechanisms should not make the resource more difficult to access than if the security mechanisms were not present.
- This principle recognizes the human element in computer security.

- Configuring and executing a program should be as easy and as intuitive as possible, and any output should be clear, direct, and useful.
- If security-related software is too complicated to configure, system administrators may unintentionally set up the software in a non-secure manner.
- Similarly, security-related user programs must be easy to use and must output understandable messages.
- If a password is rejected, the password changing program should state why it was rejected rather than giving a cryptic error message.
- If a configuration file has an incorrect parameter, the error message should describe the proper parameter.
- On the other hand, security requires that the messages impart no unnecessary information.
- In practice, the principle of psychological acceptability is interpreted to mean that the security mechanism may add some extra burden, but that burden must be both minimal and reasonable.

Common Security Related programming problems

- Programmers make mistakes sometimes and those errors can have disastrous consequences in protection domains.
- Attackers who exploit these errors may acquire extra privileges (such as access to a system account such as root or Administrator).
- They may disrupt the normal functioning of the system by deleting or altering services over which they should have no control.
- They may simply be able to read files to which they should have no access.
- So the problem of avoiding these errors, or security holes, is a necessary issue to ensure that the programs and system function as required.

Improper Choice of Initial Protection Domain

- Flaws involving improper choice of initial protection domain arise from incorrect setting of permissions or privileges.
- There are three objects for which permissions need to be set properly: the file containing the program, the access control file, and the memory space of the process.

Process Privileges

- The principle of least privilege dictates that no process have more privileges than it needs to complete its task, but the process must have enough privileges to complete its task successfully.
- Ideally, set of privileges should meet both criteria.

- In practice, different portions of the process will need different sets of privileges.
- Implementation Rule: Structure the process so that all sections requiring extra privileges are modules. The modules should be as small as possible and should perform only those tasks that require those privileges.
- Management Rule: Check that the process privileges are set properly.

Access Control File Permissions

- Biba's models emphasize that the integrity of the process relies on both the integrity of the program and the integrity of the access control file.
- The former requires that the program be properly protected so that only authorized personnel can alter it.
- The system managers must determine who the "authorized personnel" are.
- Verifying the integrity of the access control file is critical, because that file controls the access to role accounts.
- Management Rule: The program that is executed to create the process, and all associated control files, must be protected from unauthorized use and modification. Any such modification must be detected.
- Implementation Rule: Ensure that any assumptions in the program are validated. If this is not possible, document them for the installers and maintainers, so they know the assumptions that attackers will try to invalidate.

Memory Protection

- Consider sharing memory: If two subjects can alter the contents of memory, then one could change data on which the second relies.
- Unless such sharing is required (for example, by concurrent processes), it poses a security problem because the modifying process can alter variables that control the action of the other process.
- Thus, each process should have a protected, unshared memory space.
- If the memory is represented by an object that processes can alter, it should be protected so that only trusted processes can access it.
- Access here includes not only modification but also reading, because passwords reside in memory after they are typed.
- Implementation Rule: Ensure that the program does not share objects in memory with any other program, and that other programs cannot access the memory of a privileged process.
- Management Rule: Configure memory to enforce the principle of least privilege. If a section of memory is not to contain executable instructions, turn execute permission off for that section of memory. If the contents of a section of memory are not to be altered, make that section read-only.

- **Trust in the System**

- This analysis overlooks several system components.
- For example, the program relies on the system authentication mechanisms to authenticate the user, and on the user information database to map users and roles into their corresponding UIDs.
- It also relies on the inability of ordinary users to alter the system clock.
- If any of this supporting infrastructure can be compromised, the program will not work correctly.
- The best that can be done is to identify these points of trust in the installation and operation documentation so that the system administrators are aware of the dependencies of the program on the system.
- Management Rule: Identify all system components on which the program depends. Check for errors whenever possible, and identify those components for which error checking will not work.
- Implementation Rule: The implementers should identify the system databases and information on which the program depends, and should prepare a list of these dependencies. They should discuss these dependencies with system managers to determine if the program can check for errors.

- **Improper Isolation of Implementation Detail**

- The problem of improper isolation of implementation detail arises when an abstraction is improperly mapped into an implementation detail.
- The first rule is to catch errors and failures of the mappings.
- This requires an analysis of the functions and a knowledge of their implementation.
- The action to take on failure also requires thought.

- In general, if the cause cannot be determined, the program should fail by returning the relevant parts of the system to the states they were in when the program began.
- Implementation Rule: The error status of every function must be checked. Do not try to recover unless the cause of the error, and its effects, do not affect any security considerations. The program should restore the state of the system to the state before the process began, and then terminate.
- The abstractions in this program are the notion of a user and a role, the access control information, and the creation of a process with the rights of the role.

- **Resource Exhaustion and User Identifiers**

- The notion of a user and a role is an abstraction because the program can work with role names and the operating system uses integers (UIDs).
- The question is how those user and role names are mapped to UIDs.
- Typically, this is done with a user information database that contains the requisite mapping, but the program must detect any failures of the query and respond appropriately.

Validating the Access Control Entries

- The access control information implements the access control policy (an abstraction).
- The expression of the access control information is therefore the result of mapping an abstraction to an implementation.
- The question is whether or not the given access control information correctly implements the policy.
- Answering this question requires someone to examine the implementation expression of the policy.

Restricting the Protection Domain of the Role Process

- There are two approaches.
- Under UNIX-like systems, the program can spawn a second, child, process.
- It can also simply start up a second program in such a way that the parent process is replaced by the new process.
- This technique, called overlaying, is intrinsically simpler than creating a child process and exiting.
- It allows the process to replace its own protection domain with the (possibly) more limited one corresponding to the role.
- The new process inherits the protection domain of the original one.
- Before the overlaying, the original process must reset its protection domain to that of the role.
- The programmers do so by closing all files that the original process opened, and changing its privileges to those of the role.

Improper Change

- This category describes data and instructions that change over time.
- The danger is that the changed values may be inconsistent with the previous values.
- The previous values dictate the flow of control of the process.
- The changed values cause the program to take incorrect or non-secure actions on that path of control.

- The data and instructions can reside in shared memory, in non-shared memory, or on disk.
- The disk includes file attribute information such as ownership and access control list.

Memory

- First comes the data in shared memory. Any process that can access shared memory can manipulate data in that memory.
- Unless all processes that can access the shared memory implement a concurrent protocol for managing changes, one process can change data on which a second process relies.
- A second approach applies whether the memory is shared or not. A user feeds bogus information to the program, and the program accepts it.
- The bogus data overflows its buffer, changing other data, or inserting instructions that can be executed later.

Changes in File Contents

- File contents may change improperly.
- In most cases, this means that the file permissions are set incorrectly or that multiple processes are accessing the file, which is similar to the problem of concurrent processes accessing shared memory.
- Components that may change between the time the program is created and the time it is run should not be used.

Race Conditions in File Accesses

- A race condition in this context is the time-of-check-to-time-of-use problem.
- As with memory accesses, the file being used is changed after validation but before access.
- To oppose it, either the file must be protected so that no untrusted user can alter it, or the process must validate the file and use it indivisibly.
- This program validates that the owner and access control permissions for the access control file are correct (the check).
- It then opens the file (the use).
- If an attacker can change the file after the validation but before the opening, so that the file checked is not the file opened, then the attacker can have the program obtain access control information from a file other than the legitimate access control file.
- Presumably, the attacker would supply a set of access control entries allowing unauthorized accesses.

- **Improper Naming**

- Improper naming refers to an ambiguity in identifying an object.
- Most commonly, two different objects have the same name.
- The programmer intends the name to refer to one of the objects, but an attacker manipulates the environment and the process so that the name refers to a different object.
- Avoiding this flaw requires that every object be unambiguously identified.
- This is both a management concern and an implementation concern.
- Objects must be uniquely identifiable or completely interchangeable.
- Managing these objects means identifying those that are interchangeable and those that are not.
- Management Rule: Unique objects require unique names. Interchangeable objects may share a name.
- Implementation Rule: The process must ensure that the context in which an object is named identifies the correct object.

- **Improper Deallocation or Deletion**

- Failing to delete sensitive information raises the possibility of another process seeing that data at a later time.
- In particular, cryptographic keywords, passwords, and other authentication information should be discarded once they have been used.
- Similarly, once a process has finished with a resource, that resource should be deallocated.
- This allows other processes to use that resource, inhibiting denial of service attacks.
- A consequence of not deleting sensitive information is that dumps of memory, which may occur if the program receives an exception or crashes for some other reason, contain the sensitive data.
- If the process fails to release sensitive resources before creating unprivileged sub-processes, those unprivileged sub-processes may have access to the resource.
- Implementation Rule: When the process finishes using a sensitive object (one that contains confidential information or one that should not be altered), the object should be erased, then deallocated or deleted. Any resources not needed should also be released.
- Our program uses three pieces of sensitive information.
- The first is the cleartext password, which authenticates the user.
- The password is hashed, and the hash is compared with the stored hash.

- Once the hash of the entered password has been computed, the process must delete the cleartext password.
- So it overwrites the array holding the password with random bytes.
- The second piece of sensitive information is the access control information.
- Suppose an attacker wanted to gain access to a role account.
- The access control entries would tell the attacker which users could access that account using this program.
- To prevent the attacker from gaining this information, the developers decided to keep the contents of the access control file confidential.
- The program accesses this file using a file descriptor.
- File descriptors remain open when a new program overlays a process.
- Hence, the program closes the file descriptor corresponding to the access control file once the request has been validated (or has failed to be validated).
- The third piece of sensitive information is the log file. The program alters this file.
- If an unprivileged program such as one run by this program were to inherit the file descriptor, it could flood the log.
- Were the log to fill up, the program could no longer log failures.
- So the program also closes the log file before spawning the role's command.

Improper Validation

- The problem of improper validation arises when data is not checked for consistency and correctness.
- Ideally, a process would validate the data against the more abstract policies to ensure correctness.
- In practice, the process can check correctness only by looking for error codes (indicating failure of functions and procedures) or by looking for patently incorrect values (such as negative numbers when positive ones are required).
- As the program is designed, the developers should determine what conditions must hold at each interface and each block of code. They should then validate that these conditions hold.
- What follows is a set of validations that are commonly overlooked.

- Each program requires its own analysis, and other types of validation may be critical to the correct, secure functioning of the program, so this list is by no means complete.

Bounds Checking

- Errors of validation often occur when data is supposed to lie within bounds.
- For example, a buffer may contain entries numbered from 0 to 99.
- If the index used to access the buffer elements takes on a value less than 0 or greater than 99, it is an invalid operand because it accesses a nonexistent entry.
- The variable used to access the element may not be an integer (for example, it may be a set element or pointer), but in any case it must reference an existing element.
- Implementation Rule: Ensure that all array references access existing elements of the array. If a function that manipulates arrays cannot ensure that only valid elements are referenced, do not use that function.

Type Checking

- Failure to check types is another common validation problem.
- If a function parameter is an integer, but the actual argument passed is a floating point number, the function will interpret the bit pattern of the floating point number as an integer and will produce an incorrect result.
- Implementation Rule: Check the types of functions and parameters.
- Management Rule: When compiling programs, ensure that the compiler flags report inconsistencies in types. Investigate all such warnings and either fix the problem or document the warning.

Error Checking

- A third common problem involving improper validation is failure to check return values of functions.
- For example, suppose a program needs to determine ownership of a file.
- It calls a system function that returns a record containing information from the file attribute table.
- The program obtains the owner of the file from the appropriate field of the record.
- If the function fails, the information in the record is meaningless.
- So, if the function's return status is not checked, the program may act erroneously.
- Implementation Rule: Check all function and procedure executions for errors.

Checking for Valid, invalid Data

- Validation should apply the principle of fail-safe defaults.
- This principle requires that valid values be known, and that all other values be rejected.

- Unfortunately, programmers often check for invalid data and assume that the rest is valid.
- Implementation Rule: Check that a variable's values are valid.
- Management Rule: If a trade-off between security and other factors results in a mechanism or procedure that can weaken security, document the reasons for the decision, the possible effects, and the situations in which the compromise method should be used. This informs others of the trade-off and the attendant risks.

Checking Input

- All data from untrusted sources must be checked.
- The checking done depends on the way the data is received: into an input buffer (bounds checking) or read in as an integer (checking the magnitude and sign of the input).
- Implementation Rule: Check all user input for both form and content. In particular, check integers for values that are too big or too small, and check character data for length and valid characters.

Designing for Validation

- Sometimes data cannot be validated completely.
- For example, in the C programming language, a programmer can test for a NULL pointer (meaning that the pointer does not hold the address of any object), but if the pointer is not NULL, checking the validity of the pointer may be very difficult (or impossible).
- Implementation Rule: Create data structures and functions in such a way that they can be validated.

Improper Indivisibility

- Improper indivisibility arises when an operation is considered as one unit (indivisible) in the abstract but is implemented as two units (divisible).
- The checking of the access control file attributes and the opening of that file are to be executed as one operation.
- Unfortunately, they may be implemented as two separate operations, and an attacker who can alter the file after the first but before the second operation can obtain access illegally.

- Another example arises in exception handling.
- Often, program statements and system calls are considered as single units or operations when the implementation uses many operations.

- An exception divides those operations into two sets: the set before the exception, and the set after the exception.
- If the system calls or statements rely on data not changing during their execution, exception handlers must not alter the data.
- Implementation Rule: If two operations must be performed sequentially without an intervening operation, use a mechanism to ensure that the two cannot be divided.

Improper Sequencing

- Improper sequencing means that operations are performed in an incorrect order.
- For example, a process may create a lock file and then write to a log file.
- A second process may also write to the log file, and then check to see if the lock file exists.
- The first program uses the correct sequence of calls; the second does not (because that sequence allows multiple writers to access the log file simultaneously).
- Implementation Rule: Describe the legal sequences of operations on a resource or object. Check that all possible sequences of the programs involved match one (or more) legal sequences.

Improper Choice of Operand or Operation

- Preventing errors of choosing the wrong operand or operation requires that the algorithms be thought through carefully (to ensure that they are appropriate).
- At the implementation level, this requires that operands be of an appropriate type and value, and that operations be selected to perform the desired functions.
- The difference between this type of error and improper validation lies in the program.
- Improper implementation refers to a validation failure.
- The operands may be appropriate, but no checking is done.
- In this category, even though the operands may have been checked, they may still be inappropriate.
- If the program can not open the user information database file, it assumes that the database does not exist.
- This is an inappropriate choice of operation because one can block access to the file even when the database existed.

- Assurance techniques help detect these problems.

- The programmer documents the purpose of each function and then checks (or, preferably, others check) that the algorithms in the function work properly and that the code correctly implements the algorithms.
- Management Rule: Use software engineering and assurance techniques (such as documentation, design reviews, and code reviews) to ensure that operations and operands are appropriate.

UNIT 6
Malicious Programs and Protection

- Malicious logic is a set of instructions that cause a site's security policy to be violated.
- Malicious software, commonly known as malware, is any software that brings harm to a computer system.
- Malware can be in the form of worms, viruses, Trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user.
- Malware is software designed to cause harm to a computer and user.
- A Trojan horse is a program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function.
- A Trojan horse is a program with an overt (documented or known) effect and a covert (undocumented or unexpected) effect.
- Trojan horses fit into one of three models:

Continuing to perform the function of the original program and additionally performing a separate malicious activity

Continuing to perform the function of the original program but modifying the function to perform malicious activity (e.g., a Trojan horse version of a login program that collects passwords) or to disguise other malicious activity.(e.g., a Trojan horse version of a process listing program that does not display certain processes that are malicious)

Performing a malicious function that completely replaces the function of the original program.

Viruses

- A computer virus is a program that inserts itself into one or more files and then performs some (possibly null) action.
- When the Trojan horse can propagate freely and insert a copy of itself into another file, it becomes a computer virus.
- A computer virus is a piece of software that can "infect" other programs by modifying them; the modification includes injecting the original program with a routine to make copies of the virus program, which can then go on to infect other programs.

- Biological viruses are tiny scraps of genetic code—DNA or RNA—that can take over the machinery of a living cell and trick it into making thousands of flawless replicas of the original virus.
- Like its biological counterpart, a computer virus carries in its instructional code the recipe for making perfect copies of itself.
- The typical virus becomes embedded in a program on a computer.
- Then, whenever the infected computer comes into contact with an uninfected piece of software, a fresh copy of the virus passes into the new program.
- Thus, the infection can be spread from computer to computer by unsuspecting users who either swap disks or send programs to one another over a network.
- In a network environment, the ability to access applications and system services on other computers provides a perfect culture for the spread of a virus.
- A virus can do anything that other programs do.
- The difference is that a virus attaches itself to another program and executes secretly when the host program is run.
- Once a virus is executing, it can perform any function, such as erasing files and programs that is allowed by the privileges of the current user.
- A computer virus has three parts:
- **Infection mechanism:** The means by which a virus spreads, enabling it to replicate. The mechanism is also referred to as the infection vector.
- **Trigger:** The event or condition that determines when the payload is activated or delivered.
- **Payload:** What the virus does, besides spreading. The payload may involve damage or may involve safe but noticeable activity.
- During its lifetime, a typical virus goes through the following four phases:
- **Dormant phase:** The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.

- **Propagation phase:** The virus places a copy of itself into other programs or into certain system areas on the disk. The copy may not be identical to the propagating version; viruses often morph to evade detection. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
- **Triggering phase:** The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.
- **Execution phase:** The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.
- Most viruses carry out their work in a manner that is specific to a particular operating system and, in some cases, specific to a particular hardware platform.
- Thus, they are designed to take advantage of the details and weaknesses of particular systems.

```
beginvirus:
if spread-condition then begin
for some set of target files do begin
if target is not infected then begin
determine where to place virus instructions
copy instructions from beginvirus to endvirus into target
alter target to execute added instructions
end;
end;
end;
perform some action(s)
goto beginning of infected program
endvirus:
```

Worms

- A worm is a program that can replicate itself and send copies from computer to computer across network connections.
- A computer virus infects other programs. A variant of the virus is a program that spreads from computer to computer, spawning copies of itself on each one.
- Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.

- An e-mail virus has some of the characteristics of a worm because it propagates itself from system to system.
- However, we can still classify it as a virus because it uses a document modified to contain viral macro content and requires human action.
- A worm actively seeks out more machines to infect and each machine that is infected serves as an automated launching pad for attacks on other machines.
- Network worm programs use network connections to spread from system to system.
- Once active within a system, a network worm can behave as a computer virus or bacteria, or it could implant Trojan horse programs or perform any number of disruptive or destructive actions.
- To replicate itself, a network worm uses some sort of network vehicle.
- Examples include the following:
- Electronic mail facility: A worm mails a copy of itself to other systems, so that its code is run when the e-mail or an attachment is received or viewed.
- Remote execution capability: A worm executes a copy of itself on another system, either using an explicit remote execution facility or by exploiting a program flaw in a network service to subvert its operations.
- Remote login capability: A worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other, where it then executes.
- The new copy of the worm program is then run on the remote system where, in addition to any functions that it performs at that system, it continues to spread in the same fashion.
- A network worm exhibits the same characteristics as a computer virus: a dormant phase, a propagation phase, a triggering phase, and an execution phase.

Rabbits and Bacteria

- Some malicious logic multiplies so rapidly that resources become exhausted. This creates a denial of service attack.
- A bacterium or a rabbit is a program that absorbs all of some class of resource.
- Resources of a specific class, such as file descriptors or process table entry slots, may not affect currently running processes. They will affect new processes.
- Viruses not carrying a logic bomb, often referred to by experts as “bacteria” or “rabbits,” are not significantly destructive.
- Bacteria, or rabbit programs, make copies of themselves to overwhelm a computer system's resources.

- Bacteria do not explicitly damage any files. Their sole purpose is to replicate themselves.
- A typical bacteria program may do nothing more than execute two copies of itself simultaneously on multiprogramming systems, or perhaps create two new files, each of which is a copy of the original source file of the bacteria program.
- Both of those programs then may copy themselves twice, and so on.
- Bacteria reproduce exponentially, eventually taking up all the processor capacity, memory, or disk space, denying the user access to those resources.

Defenses:

- Defending against malicious logic takes advantage of several different characteristics of malicious logic to detect, or to block, its execution.
- The defenses hamper the suspect behavior.
- They may allow malicious logic that does not expose the given characteristic to proceed, and they may prevent programs that are not malicious but do affect the given characteristic from proceeding.

Sandboxing

- Sandboxing is a computer security term referring to when a program is set aside from other programs in a separate environment so that if errors or security issues occur, those issues will not spread to other areas on the computer.
- Programs are enabled in their own isolated area, where they can be worked on without posing any threat to other programs.
- Sandboxes can look like a regular operating environment.
- Virtual machines are often used for what are referred to as runtime sandboxes

Information Flow Metrics

- This approach is to limit the distance a virus can spread.
- Define the flow distance metric fd(x) for some information x as follows:
- Initially, all information has fd(x) = 0. Whenever x is shared, fd(x) increases by 1. Whenever x is used as input to a computation, the flow distance of the output is the maximum of the flow distance of the input.
- Information is accessible only while its flow distance is less than some particular value.
- The limitation of this approach is disallowance for sharing.
- It defeats the purpose of multi-user systems.

Reducing the rights

- The user can reduce the associated protection domain when running a suspect program.
- This follows from the principle of least privilege.

- Although effective, this approach begs the question of how to determine which entries should be in the authorization denial subsets.
- When the subsystem is invoked, it checks that the access is allowed.
- If not, it either denies the access or asks the user whether to permit the access.
- Also, the access right information is used to determine the user's intent to access files and the type of access.
- This technique does not protect these files, but instead prevent other files not named on the command line from being accessed.

Malicious Logic Altering Files

- Mechanisms using manipulation detection codes (or MDCs) apply some function to a file to obtain a set of bits called the signature block and then protect that block.
- If, after re-computing the signature block, the result differs from the stored signature block, the file has changed, possibly as a result of malicious logic altering the file.
- This mechanism relies on selection of good cryptographic checksums.
- An assumption is that the signed file does not contain malicious logic before it is signed.
- All integrity-based schemes rely on software that if infected may fail to report tampering.
- Performance will be affected because encrypting the file or computing the signature block may take a significant amount of time.
- The encrypting key must also be secret because if it is not, then malicious logic can easily alter a signed file without the change being detected.

Proof-Carrying Code

- Necula has proposed a technique that combines specification and integrity checking.
- His method, called proof-carrying code (PCC), requires a "code consumer" (user) to specify a safety requirement.
- The "code producer" (author) generates a proof that the code meets the desired safety property and integrates that proof with the executable code.
- This produces a PCC binary.

- The binary is delivered (through the network or other means) to the consumer.
- The consumer then validates the safety proof and, if it is correct, can execute the code knowing that it honors that policy.
- The key idea is that the proof consists of elements drawn from the native code.
- If the native code is changed in a way that violates the safety policy, the proof is invalidated and will be rejected.

Notion of Trust

- The effectiveness of any security mechanism depends on the security of the underlying base on which the mechanism is implemented and the correctness of the implementation.
- If the trust in the base or in the implementation is misplaced, the mechanism will not be secure.
- Thus, "secure," like "trust," is a relative notion, and the design of any mechanism for enhancing computer security must attempt to balance the cost of the mechanism against the level of security desired and the degree of trust in the base that the site accepts as reasonable.
- Research dealing with malicious logic assumes that the interface, software, and/or hardware used to implement the proposed scheme will perform exactly as desired, meaning that the trust is in the underlying computing base, the implementation, and (if done) the verification.

Antivirus

- The ideal solution to the threat of viruses is prevention: Do not allow a virus to get into the system in the first place, or block the ability of a virus to modify any files containing executable code or macros.
- This goal is, in general, impossible to achieve, although prevention can reduce the number of successful viral attacks.
- The next best approach is to be able to do the following:
- Detection: Once the infection has occurred, determine that it has occurred and locate the virus.
- Identification: Once detection has been achieved, identify the specific virus that has infected a program.
- Removal: Once the specific virus has been identified, remove all traces of the virus from the infected program and restore it to its original state.
- Remove the virus from all infected systems so that the virus cannot spread further.

- If detection succeeds but either identification or removal is not possible, then the alternative is to discard the infected file and reload a clean backup version.

- Advances in virus and antivirus technology go hand in hand.
- Early viruses were relatively simple code fragments and could be identified and purged with relatively simple antivirus software packages.
- As the virus arms race has evolved, both viruses and, necessarily, antivirus software have grown more complex and sophisticated.
- There are four generations of antivirus software:
- First generation: simple scanners
- Second generation: heuristic scanners
- Third generation: activity traps
- Fourth generation: full-featured protection
- A first-generation scanner requires a virus signature to identify a virus.
- The virus may contain "wildcards" but has essentially the same structure and bit pattern in all copies.
- Such signature-specific scanners are limited to the detection of known viruses.
- A second-generation scanner does not rely on a specific signature.
- Rather, the scanner uses heuristic rules to search for probable virus infection.
- One class of such scanners looks for fragments of code that are often associated with viruses.
- For example, a scanner may look for the beginning of an encryption loop used in a polymorphic virus and discover the encryption key.
- Once the key is discovered, the scanner can decrypt the virus to identify it, then remove the infection and return the program to service.
- Third-generation programs are memory-resident programs that identify a virus by its actions rather than its structure in an infected program.
- Such programs have the advantage that it is not necessary to develop signatures and heuristics for a wide array of viruses.
- Rather, it is necessary only to identify the small set of actions that indicate an infection is being attempted and then to intervene.
- Fourth-generation products are packages consisting of a variety of antivirus techniques used in conjunction.
- These include scanning and activity trap components.
- In addition, such a package includes access control capability, which limits the ability of viruses to penetrate a system and then limits the ability of a virus to update files in order to pass on the infection.

- With fourth-generation packages, a more comprehensive defense strategy is employed, broadening the scope of defense to more general-purpose computer security measures.

Features of Antivirus:

Features that make a good antivirus program are mentioned below:

- **Malware Detection & Removal:** Any good antivirus program will be able to detect different types of viruses and malware in compressed or uncompressed form. This should be the first and foremost deciding factor for your anti-virus program. Besides that, see that your robust antivirus program doesn't consume a lot of the system resources. If these qualities match, then the program is a real winner.
- **Firewall:** Few of the free antivirus programs like Comodo free antivirus, after removing all the threats from a device ensures the continual safety with the help of a powerful firewall. The powerful firewall helps in keeping away all the incoming threats.
- **Auto SandBoxing Technique**: An effective anti-virus program provides a secure environment to run files in real time to check for foul play. The Comodo free antivirus is a perfect example of one such platform that provides virtual space to run and analyze untrusted, unknown and malicious applications.
- Sometimes, this feature is also known by the names 'virus cleanup' mode, or 'virtual sandbox'. The best part of the feature is that it provides safe removal of the virus from the computer.
- **Virus Scan:** A good anti-virus program automatically runs virus scan at regular intervals to make sure the system is safe from all dangers. The virus scan will help spot on all the new threats that sneaked into your computer bypassing the usual authorizations.
- **Identity protection:** Identity theft has become common these days.
- With more and more paper facts getting converted into digital forms, it has paved the easy access for online thieves to steal the identity of known and unknown personnel. The online criminals make use of this information for their personal gains.
- A good antivirus program will safeguard your personal information in the best possible ways. For instance, it will make sure your system is safe and secure by verifying every time the user inputs the credit card or banking information online.
- **Backup:** During bad times, especially when your computer is under attack, it is better to run the backup without taking any chances. Any good antivirus

program will sport this feature by default and will help you in restoring that backup when all the issues have settled down.

- **Email Protection:** Emails also carry viruses and malware in the attachments. Even though you might be extra cautious, an impersonator email can cause the damage to your computer. Sometimes, all it requires to do the harm is opening without clicking on anything.
- In such worse case scenarios, a good antivirus program protects your computer from being the victim of scans or phishing schemes.
- **Social media Protection:** More and more people use social media accounts rigorously on a daily basis. Multiple number of times they open and close their accounts on a single day.
- These actions of a user provide an advantageous platform for hackers to implant viruses and malware on the computers.
- The intentions of hackers may vary but they never do any good to the computer user.
- A good antivirus software will send alerts to the user when a Facebook phishing scam or a Twitter malicious link has been detected.

UNIT 7
Intrusion Detection

Intruders & Intrusion Techniques

- Intrusion is a phenomenon that performs an activity that compromises a computer system by breaking the security or causing it to enter into an insecure state.
- A set of attempts to compromise a computer or a computer network resource security is regarded as an intrusion.
- The entity involved to perform such activity is called intruder.
- Intruders are also referred as attackers, interceptors or hackers.

Types of Intruders:

Masquerader

- An unauthorized user who penetrates a system's access control to exploit other's account
- Most likely an outsider to the system

Misfeasor

- A legitimate user but accesses data, program or resources for which he/she is not authorized. Generally an insider

Clandestine

- An individual who seizes supervisory control and evades auditing and access control
- May be an insider or outsider

Again there are two levels of Intruders:

- People with high level of system expertise: personally constructed methods for breaking into systems.
- Others are "foot soldiers", uses cracking programs developed and distributed by others: willing to spend countless hours looking for weakest links.

- Another classification scheme, based on intrusion types, classifies intrusions into the following six types:
- **Attempted break-in:** often detected by atypical behavior profiles or violations of security constraints.
- **Masquerade attack:** often detected by a typical behavior profiles or violations of security constraints.
- Penetration of the security control system: usually detected by monitoring for specific patterns of activity.
- Leakage: often detected by a typical usage of I/O resources.
- Denial of Service: often detected by atypical usage of system resources.
- Malicious use: often detected by a typical behavior profiles, violations of security constraints, or use of special privileges.
- Some common techniques for intrusion are:
  - Buffer overflows
  - Unexpected combinations
  - Unhandled inputs
  - Race conditions

Intrusion Detection:

- In addition to security services (e.g. data confidentiality, integrity, authentication, etc.), intrusion detection (ID) techniques are used to strengthen the system security and increase its resistance to internal and external attacks.
- These techniques are implemented by an intrusion detection system (IDS).
- Generally, IDS main task is to detect an intrusion and, if necessary or possible, to undertake some measures eliminating it.

- The goals of intrusion detection system are:
  - Detect a wide variety of intrusions.
  - Detect intrusions in a timely fashion.
  - Present the analysis in a simple, easy-to-understand format.
  - Be accurate.

- Formalizing this type of analysis provides a statistical and analytical basis for monitoring a system for intrusions.
- Three types of analyses—anomaly detection, misuse (or signature) detection, and specification detection.

Anomaly Modeling:

- Anomaly detection analyzes a set of characteristics of the system and compares their behavior with a set of expected values.
- It reports when the computed statistics do not match the expected measurements.
- Anomaly detection uses the assumption that unexpected behavior is evidence of an intrusion.

There are three different statistical models.

- The first model uses a threshold metric. A minimum of m and a maximum of n events are expected to occur (for some event and some values m and n).
- If, over a specific period of time, fewer than m or more than n events occur, the behavior is considered anomalous.
- Determining the threshold complicates use of this model.
- The threshold must take into account of differing levels of characteristics of the users.
- The second model uses statistical moments. The analyzer knows the mean and standard deviation (first two moments) and possibly other measures of correlation (higher moments).
- If values fall outside the expected interval for that moment, the behavior that the values represent is considered anomalous.
- Because the profile, or description of the system, may evolve over time, anomaly-based intrusion detection systems take these changes into account by aging (or weighting) data or altering the statistical rule base on which they make decisions.
- The statistical moments model provides more flexibility than the threshold model.
- Administrators can tune it to discriminate better than the threshold model.
- But with flexibility comes complexity.
- Third model is a Markov model.
- Examine a system at some particular point in time.
- Events preceding that time have put the system into a particular state.
- When the next event occurs, the system transitions into a new state.

- Over time, a set of probabilities of transition can be developed.

- When an event occurs that causes a transition that has a low probability, the event is deemed anomalous.
- This model suggests that a notion of "state," or past history, can be used to detect anomalies.
- The anomalies are now no longer based on statistics of the occurrence of individual events, but on sequences of events.
- This approach promoted misuse detection and was used to develop effective anomaly detection mechanisms.
- The effectiveness of Markov-based models depends on the adequacy of the data used to establish the model.
- This data (called training data) is obtained experimentally, usually from populations that are believed to be normal (not anomalous).

Misuse Modeling:

- Misuse detection determines whether a sequence of instructions being executed is known to violate the site security policy being executed.
- If so, it reports a potential intrusion.
- In some contexts, the term "misuse" refers to an attack by an insider or authorized user.
- In the context of intrusion detection systems, it means "rule-based detection."
- Modeling of misuse requires a knowledge of system vulnerabilities or potential vulnerabilities that attackers attempt to exploit.
- The intrusion detection system incorporates this knowledge into a rule set.
- When data is passed to the intrusion detection system, it applies the rule set to the data to determine if any sequences of data match any of the rules.
- If so, it reports that a possible intrusion is underway.
- Misuse-based intrusion detection systems often use expert systems to analyze the data and apply the rule set.
- These systems cannot detect attacks that are unknown to the developers of the rule set.
- Previously unknown attacks, or even variations of known attacks, can be difficult to detect.

Specification Modeling:

- Specification-based detection determines whether or not a sequence of instructions violates a specification of how a program, or system, should execute. If so, it reports a potential intrusion.
- Anomaly detection has been called the art of looking for unusual states.

- Misuse detection, similarly, is the art of looking for states known to be bad.
- Specification detection takes the opposite approach; it looks for states known not to be good, and when the system enters such a state, it reports a possible intrusion.
- For security purposes, only those programs that in some way change the protection state of the system need to be specified and checked.
- For example, because the policy editor in Windows NT changes security-related settings, it needs to have an associated specification.

Architecture of IDS:

- An intrusion detection system consists of three parts.
- The agent corresponds to the logger. It acquires information from a target (such as a computer system).
- The director corresponds to the analyzer. It analyzes the data from the agents as required (usually to determine if an attack is in progress or has occurred).
- The director then passes this information to the notifier, which determines whether, and how, to notify the requisite entity.
- The notifier may communicate with the agents to adjust the logging if appropriate.

Agent:

- An agent obtains information from a data source (or set of data sources).
- The source may be a log file, another process, or a network.
- The information, once acquired, may be sent directly to the director.
- Usually, however, it is preprocessed into a specific format to save the director from having to do this.
- Also, the agent may discard information that it considers irrelevant.
- The director may determine that it needs more information from a particular information source.
- In that case, the director can instruct the agent to collect additional data, or to process the data it collects differently.
- The director can use this to cut down on the amount of processing it must do, but can increase the level of information it receives when an attack is suspected.
- An agent can obtain information from a single host, from a set of hosts or from a network.

Host-Based Information Gathering:

- Host-based agents usually use system and application logs to obtain records of events, and analyze them to determine what to pass to the director.
- The events to look for, and to analyze, are determined by the goals of the intrusion detection mechanism.
- The logs may be security-related logs or other logs such as accounting logs.
- A variant of host-based information gathering occurs when the agent generates its own information.
- Policy checkers do this. They analyze the state of the system, or of some objects in the system, and treat the results as a log (to reduce and forward).

Network-Based Information Gathering:

- Network-based agents use a variety of devices and software to monitor network traffic.
- This technique provides information of a different flavor than host-based monitoring provides.
- It can detect network-oriented attacks, such as a denial of service attack introduced by flooding a network.
- It can monitor traffic for a large number of hosts. It can also examine the contents of the traffic itself (called content monitoring).
- Network-based agents may use network sniffing to read the network traffic.
- In this case, a system provides the agent with access to all network traffic passing that host.
- If the medium is point-to-point (such as a token ring network), the agents must be distributed to obtain a complete view of the network messages.
- If the medium is a broadcast medium (such as Ethernet), typically only one computer needs to have the monitoring agent.

Combining Sources:

- The goal of an agent is to provide the director with information so that the director can report possible violations of the security policy (intrusions).
- An aggregate of information is needed. However, the information can be viewed at several levels.
- The difference between application and system views (which is, essentially, a problem of layers of abstraction) affects what the agent can report to the director and what the director can conclude from analyzing the information.

- The agent, or the director, must either obtain information at the level of abstraction at which it looks for security problems or be able to map the information into an appropriate level.

Director:

- The director itself reduces the incoming log entries to eliminate unnecessary and redundant records. It then uses an analysis engine to determine if an attack (or the precursor to an attack) is underway.
- The analysis engine may use any of, or a mixture of, several techniques to perform its analysis.
- Because the functioning of the director is critical to the effectiveness of the intrusion detection system, it is usually run on a separate system.
- This allows the system to be dedicated to the director's activity.
- It has the side effect of keeping the specific rules and profiles unavailable to ordinary users.
- Then attackers lack the knowledge needed to evade the intrusion detection system by conforming to known profiles or using only techniques that the rules do not include.
- The director must correlate information from multiple logs.
- Many types of directors alter the set of rules that they use to make decisions.
- These adaptive directors alter the profiles, add (or delete) rules, and otherwise adapt to changes in the systems being monitored.
- Typical adaptive directors use aspects of machine learning or planning to determine how to alter their behavior.
- Directors rarely use only one analysis technique, because different techniques highlight different aspects of intrusions.
- The results of each are combined, analyzed and reduced, and then used.

Notifier:

- The notifier accepts information from the director and takes the appropriate action.
- In some cases, this is simply a notification to the system security officer that an attack is believed to be underway.
- In other cases, the notifier may take some action to respond to the attack.
- Many intrusion detection systems use graphical interfaces.
- A well-designed graphics display allows the intrusion detection system to convey information in an easy-to-grasp image or set of images.
- It must allow users to determine what attacks are underway (ideally, with some notion of how likely it is that this is not a false alarm).

- This requires that the GUI be designed with a lack of clutter and unnecessary information.
- The notifier may send electronic mail to the appropriate person or make entries into the appropriate log files.

Organization of Intrusion Detection Systems:

- An intrusion detection system can be organized in several ways.
- The organization of IDS explores three such paradigms using research intrusion detection systems.
- The first system examines network traffic only.
- The second explores how to combine network and host sources.
- The third system distributes the director among multiple systems to enhance security and reliability.

Monitoring Network Traffic for Intrusions: NSM

- The Network Security Monitor (NSM) develops a profile of expected usage of a network and compares current usage with that profile.
- It also allows the definition of a set of signatures to look for specific sequences of network traffic that indicate attacks.
- It runs on a local area network and assumes a broadcast medium.
- The monitor measures network utilization and other characteristics and can be instructed to look at activity based on a user, a group of users, or a service. It reports anomalous behavior.
- The NSM monitors the source, destination, and service of network traffic.
- It assigns a unique connection ID to each connection.
- The source, destination, and service are used as axes for a matrix.
- Each element of the matrix contains the number of packets sent over that connection for a specified period of time, and the sum of the data of those packets.
- NSM also generates expected connection data from the network.
- The data in the array is “masked” by the expected connection data, and any data not within the expected range is reported as an anomaly.
- The NSM is important for two reasons.
- First, it served as the basis for a large number of intrusion detection systems.
- Second, it proved that performing intrusion detection on networks was practical.

Combining Host and Network Monitoring: DIDS

- The Distributed Intrusion Detection System (DIDS) combined the abilities of the NSM with intrusion detection monitoring of individual hosts.

- It sprang from the observation that neither network-based monitoring nor host-based monitoring was sufficient.
- An intruder attempting to log into a system through an account without a password would not be detected as malicious by a network monitor.
- Subsequent actions, however, might make a host-based monitor report that an intruder is present.
- Similarly, if an attacker tries to telnet to a system a few times, using a different login name each time, the host-based intrusion detection mechanism would not report a problem, but the network-based monitor could detect repeated failed login attempts.
- DIDS used a centralized analysis engine (the DIDS director) and required that agents be placed on the systems being monitored as well as in a place to monitor the network traffic.
- The agents scanned logs for events of interest and reported them to the DIDS director.
- The DIDS director invoked an expert system that performed the analysis of the data.
- The expert system was a rule-based system that could make inferences about individual hosts and about the entire system (hosts and networks).
- It would then pass results to the user interface, which displayed them in a simple, easy-to-grasp manner for the system security officer.

Autonomous Agents: AAFID

- An autonomous agent is a process that can act independently of the system of which it is a part.
- In 1995, Crosbie and Spafford examined intrusion detection systems in light of fault tolerance.
- They noted that an intrusion detection system that obtains information by monitoring systems and networks is a single point of failure.
- If the director fails, the IDS will not function.
- Their suggestion was to partition the intrusion detection system into multiple components that function independently of one another, yet communicate to correlate information.
- Crosbie and Spafford suggested developing autonomous agents each of which performed one particular monitoring function.
- Each agent would have its own internal model, and when the agent detected a deviation from expected behavior, a match with a particular rule, or a violation of a specification, it would notify other agents.

- The agents would jointly determine whether the set of notifications were sufficient to constitute a reportable intrusion.
- The beauty of this organization lies in the cooperation of the agents.
- No longer is there a single point of failure.
- If one agent is compromised, the others can continue to function.

Intrusion Response:
- Once an intrusion is detected, how can the system be protected?
- The field of intrusion response deals with this problem.
- Its goal is to handle the (attempted) attack in such a way that damage is minimized (as determined by the security policy).
- Some intrusion detection mechanisms may be augmented to thwart intrusions.
- Otherwise, the security officers must respond to the attack and attempt to repair any damage.

Incident Prevention:
- Ideally, intrusion attempts will be detected and stopped before they succeed.
- This typically involves closely monitoring the system (usually with an intrusion detection mechanism) and taking action to defeat the attack.
- In the context of response, prevention requires that the attack be identified before it completes.
- The defenders then take measures to prevent the attack from completing.
- This may be done manually or automatically.

Intrusion Handling:
- When an intrusion occurs, the security policy of the site has been violated.
- Handling the intrusion means restoring the system to comply with the site's security policy and taking any actions against the attacker that the policy specifies.

Intrusion handling consists of six phases.
1. Preparation for an attack. This step occurs before any attacks are detected. It establishes procedures and mechanisms for detecting and responding to attacks.

2. Identification of an attack. This triggers the remaining phases.
3. Containment (confinement) of the attack. This step limits the damage as much as possible.
4. Eradication of the attack. This step stops the attack and blocks further similar attacks.

5. Recovery from the attack. This step restores the system to a secure state (with respect to the site security policy).
6. Follow-up to the attack. This step involves taking action against the attacker, identifying problems in the handling of the incident, and recording lessons learned (or lessons not learned that should be learned).

Containment Phase:

- Containing or confining an attack means limiting the access of the attacker to system resources.
- The protection domain of the attacker is reduced as much as possible.
- There are two approaches: passively monitoring the attack, and constraining access to prevent further damage to the system.
- In this context, "damage" refers to any action that causes the system to deviate from a "secure" state as defined by the site security policy.

- Passive monitoring simply records the attacker's actions for later use.
- The monitors do not interfere with the attack in any way.
- This technique is marginally useful.
- It will reveal information about the attack and, possibly, the goals of the attacker.
- However, not only is the intruded system vulnerable throughout, the attacker could attack other systems.
- The other approach, in which steps are taken to constrain the actions of the attacker, is considerably more difficult.
- The goal is to minimize the protection domain of the attacker while preventing the attacker from achieving her goal.
- But the system defenders may not know what the goal of the attacker is, and thus may misdirect the confinement so that the data or resources that the attacker seeks lie within the minimal protection domain of the attacker.

Eradication Phase:

- Eradicating an attack means stopping the attack.
- The usual approach is to deny access to the system completely (such as by terminating the network connection) or to terminate the processes involved in the attack.
- An important aspect of eradication is to ensure that the attack does not immediately resume.
- This requires that attacks be blocked.

- A common method for implementing blocking is to place wrappers around suspected targets.
- The wrappers implement various forms of access control.
- Wrappers can control access locally on systems or control network access.

Follow-Up Phase:

- In the follow-up phase, the systems take some action external to the system against the attacker.
- The most common follow-up is to pursue some form of legal action, either criminal or civil.
- The requirements of the law vary among communities, and indeed vary within communities over time.
- Counterattacking, or attacking the attacker, takes two forms.
- The first form involves legal mechanisms, such as filing criminal complaints.
- This requires protecting a "chain of evidence" so that legal authorities can establish that the attack was real (in other words, that the attacked site did not invent evidence) and that the evidence can be used in court.
- The precise requirements of the law change over time and jurisdictions, so this first form of counterattacking lies outside the scope of this discussion.
- The second form is a technical attack, in which the goal is to damage the attacker seriously enough to stop the current attack and discourage future attacks.
- This approach has several important consequences that must be considered.
  - The counterattack may harm an innocent party.
  - The counterattack may have side effects.
  - The counterattack is antithetical to the shared use of a network.
  - The counterattack may be legally actionable.

UNIT 8
Web security and Email Security

Web Security:

- Web security is the process of securing confidential data stored online from unauthorized access and modification.
- The aim of Web security is to identify the following:
  - Critical assets of the organization
  - Genuine users who may access the data
  - Level of access provided to each user

o Various vulnerabilities that may exist in the application
o Data criticality and risk analysis on data exposure
• Web application security aims to address and fulfill the four conditions of security, also referred to as principles of security:
 Confidentiality: States that the sensitive data stored in the Web application should not be exposed under any circumstances.
 Integrity: States that the data contained in the Web application is consistent and is not modified by an unauthorized user.
 Availability: States that the Web application should be accessible to the genuine user within a specified period of time depending on the request.
 Nonrepudiation: States that the genuine user cannot deny modifying the data contained in the Web application and that the Web application can prove its identity to the genuine user.

Web Threats:

• A web threat is any threat that uses the World Wide Web to facilitate cybercrime.
• Web threats are malicious software programs such as spyware, adware, trojan horse programs, bots, viruses, or worms, etc. that are installed on your computer without your knowledge or permission.

• These programs utilize the Web to spread, hide, update themselves and send stolen data back to criminals. They can also be combined to do the crime.
• Web threats use multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but may also employ other protocols and components, such as links in email or malware attachments or on servers that access the Web.
• The types of security threats faced when using the web can be grouped in two ways.
• One way to group these threats is in terms of passive and active attacks.
• Passive attacks include eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted.
• Active attacks include impersonating another user, altering messages in transit between client and server, and altering information on a Web site.
• Another way to classify Web security threats is in terms of the location of the threat: Web server, Web browser, and network traffic between browser and server.

- Common web threats to be considered are:

Security misconfiguration:

- A functioning web application is usually supported by some complex elements that make up its security infrastructure.
- This includes databases, OS, firewalls, servers and other application software or devices.
- All these elements require frequent maintenance and configuration to keep the web application running properly.
- Whenever possible, schedule penetration tests for the web applications to test out its capability of handling sensitive data.

Malware:

- The presence of malware is yet another one of the most common threats that companies commonly have to guard against.
- Upon downloading malware, severe repercussions like activity monitoring, access to confidential information and backdoor access to large scale data breaches can be incurred.
- Malware can be categorized in different groups since they work to achieve different goals- Spyware, Viruses, Ransomware, Worms, and Trojans.

Injection Attacks:

- Injection attacks are yet another common threat to be on the lookout for.
- These types of attacks come in a variety of different injection types and are primed to attack the data in web applications since web applications require data to function.
- The more data is required, the more opportunities for injection attacks to target. Some examples of these attacks include SQL injection, code injection and cross site scripting.
- SQL injection attacks usually hijack control over the website owner's database through the act of data injection into the web application.
- The data injected gives the website owner's database instructions that have not been authorized by the site owner themselves.
- This results in data leaking, removal or manipulation of stored data.
- Code injection, on the other hand, involves the injecting of source codes into the web application while cross site scripting injects code (javascript) into browsers.

- **Phishing Scam:**

• Phishing scam attacks are usually involved and interfere directly with email marketing efforts.
• These types of threats are designed to look like emails that are from legitimate sources, with the goal of acquiring sensitive information like login credentials, bank account numbers, credit card numbers and other data.
• If the individual is not aware of the differences and indications that the email messages are suspicious, it can be deadly since they may respond to it.
• Alternatively, they can also be used to send in malware that, upon clicking, may end up gaining access to the user's information.

- **Brute Force:**

• In brute force attacks, hackers attempt to guess passwords and forcefully gain access to the web application owner's details.
• There is no effective way to prevent this from occurring. However, business owners can deter this form of attack by limiting the number of logins one can undertake as well as making use of a technique known as encryption.
• By taking the time to encrypt data, this ensures that they are difficult for hackers to make use of it for anything else unless they have encryption keys.
• This is an important step for corporations who are required to store data that is sensitive to prevent further problems from occurring

Secure Socket Layer(SSL):

• Secure Sockets Layer (SSL) is a standard protocol used for the secure transmission of documents over a network.
• Developed by Netscape, SSL technology creates a secure link between a Web server and browser to ensure private and integral data transmission.
• SSL uses Transport Control Protocol (TCP) for communication.
• In SSL, the word socket refers to the mechanism of transferring data between a client and server over a network.
• When using SSL for secure Internet transactions, a Web server needs an SSL certificate to establish a secure SSL connection.
• SSL encrypts network connection segments above the transport layer, which is a network connection component above the program layer.
• SSL follows an asymmetric cryptographic mechanism, in which a Web browser creates a public key and a private (secret) key.
• The public key is placed in a data file known as a certificate signing request (CSR). The private key is issued to the recipient only.

- The objectives of SSL are:
  - Data integrity: Data is protected from tampering.
  - Data privacy: Data privacy is ensured through a series of protocols, including the SSL Record Protocol, SSL Handshake Protocol, SSL Change CipherSpec Protocol and SSL Alert Protocol.
  - Client-server authentication: The SSL protocol uses standard cryptographic techniques to authenticate the client and server.
- SSL is the predecessor of Transport Layer Security (TLS), which is a cryptographic protocol for secure Internet data transmission.

Architecture of SSL:

- SSL is designed to make use of TCP to provide a reliable end-to-end secure service.
- SSL is not a single protocol but rather two layers of protocols.
- The SSL Record Protocol provides basic security services to various higher layer protocols.
- In particular, the Hypertext Transfer Protocol (HTTP), which provides the transfer service for Web client/server interaction, can operate on top of SSL.
- Three higher-layer protocols are defined as part of SSL: the Handshake Protocol, The Change Cipher Spec Protocol, and the Alert Protocol

Handshake protocol:

- This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record.
- The Handshake Protocol is used before any application data is transmitted.
- It consists of a series of messages exchanged by client and server.
- The SSL Record Protocol provides two services for SSL connections:
- Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
- Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).
- The Record Protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment.
- Received data are decrypted, verified, decompressed, and reassembled before being delivered to higher-level users.
- The Change Cipher Spec Protocol is one of the three SSL-specific protocols that use the SSL Record Protocol, and it is the simplest.

- This protocol consists of a single message which consists of a single byte (initially 1).
- The sole purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.
- Cipher suite is a list that contains the combinations of cryptographic algorithms supported by the client, in decreasing order of preference.
- Each element of the list (each cipher suite) defines both a key exchange algorithm and a CipherSpec.
- The Alert Protocol is used to convey SSL-related alerts to the peer entity.
- As with other applications that use SSL, alert messages are compressed and encrypted, as specified by the current state.

Transport Layer Security:

- TLS (Transport Layer Security) is just an updated, more secure, version of SSL.
- Transport layer security (TLS) is a protocol that provides communication security between client/server applications that communicate with each other over the Internet.
- It enables privacy, integrity and protection for the data that's transmitted between different nodes on the Internet.
- TLS primarily enables secure Web browsing, applications access, data transfer and most Internet-based communication.
- It prevents the transmitted/transported data from being eavesdropped or tampered.
- TLS is used to secure Web browsers, Web servers, VPNs, database servers and more.
- TLS protocol consists of two different layers of sub-protocols:
- TLS Handshake Protocol: Enables the client and server to authenticate each other and select a encryption algorithm prior to sending the data
- TLS Record Protocol: It works on top of the standard TCP protocol to ensure that the created connection is secure and reliable. It also provides data encapsulation and data encryption services.

HTTP:

- Hyper Text Transfer Protocol (HTTP) is an application-layer protocol used primarily on the World Wide Web.
- HTTP uses a client-server model where the web browser is the client and communicates with the webserver that hosts the website.

- The browser uses HTTP, which is carried over TCP/IP to communicate to the server and retrieve Web content for the user.
- A basic HTTP request involves the following steps:
  - A connection to the HTTP server is opened.
  - A request is sent to the server.
  - Some processing is done by the server.
  - A response from the server is sent back.
  - The connection is closed.

Limitations of HTTP

- Integrity is not there, so someone can easily alter with the content.
- HTTP is insecure as there's no encryption methods for it. So, it's subjected towards man in the middle and eavesdropping of sensitive information.
- There's no authentication, so you will not have any clear idea with whom you are initiating a communication.
- Authentication is sent in the clear, anyone who intercepts the request and can know the username and passwords being used.

HTTPS:

- HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server.
- The HTTPS capability is built into all modern Web browsers.
- Its use depends on the Web server supporting HTTPS communication. For example, search engines do not support HTTPS.
- The principal difference seen by a user of a Web browser is that URL (uniform resource locator) addresses begin with https:// rather than http://.
- A normal HTTP connection uses port 80. If HTTPS is specified, port 443 is used, which invokes SSL.
- HTTPS is primarily designed to provide enhanced security layer over the unsecured HTTP protocol for sensitive data and transactions such as billing details, credit card transactions and user login etc.
- HTTPS encrypts every data packet in transition using SSL or TLS encryption technique to avoid intermediary hackers and attackers to extract the content of the data; even if the connection is compromised.
- When HTTPS is used, the following elements of the communication are encrypted:
  - URL of the requested document
  - Contents of the document
  - Contents of browser forms (filled in by browser user)

- Cookies sent from browser to server and from server to browser
- Contents of HTTP header

Secure Electronic Transaction:

- A secure electronic transaction (SET) is an open-source and cryptography-based protocol for secure payment processing via non-secure network.
- In 1996, SET was launched and backed by VISA, MasterCard and other payment processing industry leaders.
- SET's algorithm ensures data confidentiality, data integrity and cardholder/merchant authentication.
- An SET system includes the following components:
  - Merchant
  - Cardholder/acquirer
  - Card issuer
  - Payment gateway
  - Certification authority (CA)
  - Dual signature: A guaranteed SET data integrity innovation that links two different recipient messages

Working:

- Assume that a customer has a SET-enabled browser and that the transaction provider (bank, store, etc.) has a SET-enabled server.
- The customer opens a Mastercard or Visa bank account. Any issuer of a credit card is some kind of bank.
- The customer receives a digital certificate. This electronic file functions as a credit card for online purchases or other transactions. It includes a public key with an expiration date. It has been through a digital switch to the bank to ensure its validity.
- Third-party merchants also receive certificates from the bank. These certificates include the merchant's public key and the bank's public key.
- The customer places an order over a Web page, by phone, or some other means.
- The customer's browser receives and confirms from the merchant's certificate that the merchant is valid.
- The browser sends the order information. This message is encrypted with the merchant's public key, the payment information, which is encrypted with the bank's public key (which can't be read by the merchant), and information that ensures the payment can only be used with this particular order.

- The merchant verifies the customer by checking the digital signature on the customer's certificate.
- This may be done by referring the certificate to the bank or to a third-party verifier.
- The merchant sends the order message along to the bank. This includes the bank's public key, the customer's payment information (which the merchant can't decode), and the merchant's certificate.
- The bank verifies the merchant and the message. The bank uses the digital signature on the certificate with the message and verifies the payment part of the message.
- The bank digitally signs and sends authorization to the merchant, who can then fill the order.

Dual Signature:

- Dual signature is the use of encryption with two electronic signatures as a security measure for delivering an electronic message in a Secure Electronic Transaction (SET).
- The purpose of the dual signature is to link two messages that are intended for two different recipients.
- In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank.
- The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order.
- The customer is afforded extra protection in terms of privacy by keeping these two items separate.
- The customer takes the hash (using SHA-1) of the PI and the hash of the OI.
- These two hashes are then concatenated and the hash of the result is taken.
- Finally, the customer encrypts the final hash with his or her private signature key, creating the dual signature.

Payment processing:

- It is usually a third-party service that is actually a system of computer processes that process, verify, and accept or decline credit card transactions on behalf of the merchant through secure Internet connections.

- Payment processing is a service that allows websites to sell online by accepting payment via electronic methods such as credit cards, debit cards and bank transfers.

- Provided by payment service providers, payment processing is the technical connection or 'gateway' between a website and the financial institutions or 'acquirers' that govern different payment methods.

Email and Concept of Secure Email:

- Electronic mail (email) is a digital mechanism for exchanging messages through Internet or intranet communication platforms.
- Email messages are relayed through email servers, which are provided by all Internet service providers (ISP).
- Emails are transmitted between two dedicated server folders: sender and recipient.
- A sender saves, sends or forwards email messages, whereas a recipient reads or downloads emails by accessing an email server.

- Email security refers to the collective measures used to secure the access and content of an email account or service.
- It allows an individual or organization to protect the overall access to one or more email addresses/accounts.
- An email service provider implements email security to secure subscriber email accounts and data from hackers - at rest and in transit.
- Email security is a broad term that encompasses multiple techniques used to secure an email service.
- From an individual/end user standpoint, proactive email security measures include:
  - Strong passwords
  - Password rotations
  - Spam filters
  - Desktop-based anti-virus/anti-spam applications
- Similarly, a service provider ensures email security by using strong password and access control mechanisms on an email server; encrypting and digitally signing email messages when in the inbox or in transit to or from a subscriber email address.
- It also implements firewall and software-based spam filtering applications to restrict unsolicited, untrustworthy and malicious email messages from delivery to a user’s inbox.

Simple Mail Transfer Protocol (SMTP):

- Simple Mail Transfer Protocol (SMTP) is the standard protocol for email services on a TCP/IP network.
- SMTP provides the ability to send and receive email messages.
- It is an application-layer protocol that enables the transmission and delivery of email over the Internet.
- SMTP clients and servers have two main components.
  - **User Agents:** prepares the messages, encloses it in an envelope
  - **Mail Transfer Agent:** transfers the mail across the internet
- The limitations of SMTP are:
  - Transmission of executable files and binary files using SMTP is not possible without converting into text files. Use MIME to send mail in other format.
  - It cannot transmit text data that contains national language characters.
  - It is limited to 7-bit ASCII characters only.
  - SMTP servers may reject mails beyond some specific length.

Privacy-Enhanced Mail (PEM):

- Privacy-Enhanced Mail (PEM) is an Internet standard that provides for secure exchange of electronic mail.
- PEM employs a range of cryptographic techniques to allow for confidentiality, sender authentication, and message integrity.
- The message integrity aspects allow the user to ensure that a message hasn't been modified during transport from the sender.
- The sender authentication allows a user to verify that the PEM message that they have received is truly from the person who claims to have sent it.
- The confidentiality feature allows a message to be kept secret from people to whom the message was not addressed.
- PEM does not require the use of a specific algorithm.
- On the contrary, it allows use of several algorithms for data encryption, key management, and data integrity.
- PEM provides a range of security features. They include originator authentication, message confidentiality, and data integrity.

Pretty Good Privacy (PGP):

- Pretty Good Privacy (PGP) is a methodology used for encrypting and decrypting digital files and communications over the Internet.
- PGP was initially designed for email security.

- PGP works on the public key cryptography mechanism, where users encrypt and decrypt data using their respective public and private keys.
- PGP uses a symmetric encryption key to encrypt messages, and a public key is used with each sent and received message.
- First, the receiver must use its private key to decrypt the key and then decrypt the message through the decrypted symmetric key.
- PGP also provides data/file integrity services by digitally signing messages, allowing receivers to learn whether or not message confidentiality is compromised.
- PGP is also used to encrypt files stored on a computer and/or complete hard disk drives.
- PGP can be used basically for 4 things:
- Encrypting a message or file so that only the recipient can decrypt and read it.

- Clear signing a plain text message guarantees that it can only have come from the sender and not an impostor.
- Encrypting computer files so that they can't be decrypted by anyone other than the person who encrypted them.
- Really deleting files (i.e. overwriting the content so that it can't be recovered and read by anyone else) rather than just removing the file name from a directory/folder.
- PGP provides two services: encryption and digital signatures.
- Encryption allows a user to encode a file for storage locally or for transmission as an e-mail message.
- The local storage option is handy if you are worried about other people having access to files on your machine.
- The e-mail option enables PGP to be used for private exchanges over a network.
- PGP encrypts the entire contents of the message in such a way that only the intended recipient can decode and read the message.
- Anyone else who attempts to capture or copy the message in route will receive meaningless garbage.
- The digital signature service allows a user to 'sign' a document before transmission in such a way that anyone can verify that the signature is genuine and belongs with a particular document.
- If someone alters the message or substitutes a different message, the signature will no longer be valid.
- And any recipient can verify that the message has been signed by its true creator and not an imposter.

UNIT 9
Database security

- Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks.
- It is a broad term that includes a multitude of processes, tools and methodologies that ensure security within a database environment.
- Database security covers and enforces security on all aspects and components of databases. This includes:
  - Data stored in database
  - Database server
  - Database management system (DBMS)
  - Other database workflow applications

- Database security is generally planned, implemented and maintained by a database administrator and/or other information security professional.
- Some of the ways database security is analyzed and implemented include:
  - Restricting unauthorized access and use by implementing strong and multifactor access and data management controls.
  - Load/stress testing and capacity testing of a database to ensure it does not crash in a distributed denial of service (DDoS) attack or user overload.

  - Physical security of the database server and backup equipment from theft and natural disasters.
  - Reviewing existing system for any known or unknown vulnerabilities and defining and implementing a road map/plan to mitigate them.

Issues regarding the right to access information:

- Information access is the freedom or ability to identify, obtain and make use of data or information effectively.
- Freedom of information is a fundamental human right .
- Right to access information depends upon the information policy and access control mechanisms of an organization.

- Information access covers many issues including copyright, open source, privacy, and security.

System Related Issues:

- Databases are a key target for cybercriminals due to the often valuable nature of sensitive information locked away inside.
- Whether the data is financial or holds intellectual property and corporate secrets, hackers worldwide can profit from breaching a businesses' servers and plundering databases.
- The top ten vulnerabilities often found in database-driven systems, whether during the creation phase, through the integration of applications or when updating and patching, are:

 Deployment Failures

- The most common cause of database vulnerabilities is a lack of due care at the moment they are deployed. Although any given database is tested for functionality and to make sure it is doing what the databases is designed to do, very few checks are made to check the database is not doing things it should not be doing.

 Broken databases

- Malicious programs are able to infect vulnerable computers within minutes of deployment, taking down thousands of databases in minutes.

 Data leaks

- Databases may be considered a "back end" part of the office and secure from Internet-based threats (and so data doesn't have to be encrypted), but this is not the case.
- Databases also contain a networking interface, and so hackers are able to capture this type of traffic to exploit it.
- To avoid such a pitfall, administrators should use SSL- or TLS-encrypted communication platforms.

 Stolen database backups

- External attackers who infiltrate systems to steal data are one threat, but what about those inside the corporation?
- Insiders are also likely to steal archives — including database backups — whether for money, profit or revenge.
- This is a common problem for the modern enterprise, and businesses should consider encrypting archives to mitigate the insider-risk.

 A lack of segregation

- The separation of administrator and user powers, as well as the segregation of duties, can make it more difficult for fraud or theft undertaken by internal staff.
- In addition, limiting the power of user accounts may give a hacker a harder time in taking complete control of a database.

SQL injections

- A popular method for hackers to take, SQL injections remain a critical problem in the protection of enterprise databases.
- Applications are attacked by injections, and the database administrator is left to clean up the mess caused by unclean variables and malicious code which is inserted into strings, later passed to an instance of SQL server for parsing and execution.
- The best ways to protect against these threats are to protect web-facing databases with firewalls and to test input variables for SQL injection during development.

Database inconsistencies

- The common thread which brings all of these vulnerabilities together is a lack of consistency, which is an administrative rather than database technology problem.
- System administrators and database developers need to develop a consistent practice in looking after their databases, staying aware of threats and making sure that vulnerabilities are taken care of.
- This isn't an easy task, but documentation and automation to track and make changes can ensure that the information contained in enterprise networks is kept secure

System Levels:

- To protect the database, we must take security measures at several levels:

Physical hardware:

- The sites containing the computer systems must be secured against armed or surreptitious entry by intruders.
- Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution.
- This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism
- Physical security has three important components: access control, surveillance and testing.
- Obstacles should be placed in the way of potential attackers and physical sites should be hardened against accidents, attacks or environmental disasters.

- Physical locations should be monitored using surveillance cameras and notification systems, such as intrusion detection sensors, heat sensors and smoke detectors.
- Disaster recovery policies and procedures should be tested on a regular basis to ensure safety and to reduce the time it takes to recover from disruptive man-made or natural disasters.

Operating System:

- No matter how secure the database system is, weakness in operating system security may serve as a means of unauthorized access to the database.
- Each operating system provides security measures that you can use to protect your database.

- Operating system command level does not allow the access to the database.
- But, if the operating system itself is non-secure, then there is a possibility for violation of security of database.
- Thus, security of operating system also plays vital role for protecting the database.
- OS security may be approached in many ways, including the following:
  - Performing regular OS patch updates.
  - Installing updated antivirus engines and software.
  - Inspecting all incoming and outgoing network traffic through a firewall.
  - Creating secure accounts with required privileges only (i.e., user management)

DBMS Level:

- Security within the DBMS protects the integrity of the data, records and databases.
- Major elements of DBMS security include user authentication, user authorization, encryption of data and/or user-id and password, and the auditing user actions.
- It can provide encryption protection at the data level and allows organizations to have another layer at which to manage and control all access to the information.
- Some database-system users may be authorized to access only a limited portion of the database. Other users may be allowed to issue queries, but may be forbidden to modify the data.
- It is responsibility of the database system to ensure that these authorization restrictions are not violated.

- Security at all these levels must be maintained if database security is to be ensured.
- A weakness at a low level of security (physical or human) allows violation of strict high level (database) security measures.

Multiple Security Level:

- Multilevel security or multiple levels of security (MLS) is the application of a computer system to process information with classifications (i.e., at different security levels), permit access by users with different security clearances and needs-to-know, and prevent users from obtaining access to information for which they lack authorization.
- In MLS, users are cleared at different clearance levels such as Unclassified, Confidential, Secret and TopSecret.
- Data is assigned depending upon different sensitivity levels such as Unclassified, Confidential, Secret, and TopSecret.
- Multilevel security provides the capability to prevent unauthorized users from accessing information at a higher classification than their authorization, and prevents users from declassifying information.
- Multilevel security offers the following advantages:
  - Multilevel security enforcement is mandatory and automatic.
  - Multilevel security can use methods that are difficult to express through traditional views or queries.
  - Multilevel security does not rely on special views or database variables to provide security control.
  - Multilevel security controls are consistent and integrated across the system.
  - Multilevel security does not allow users to declassify information.

Categorization of data:

- Data categorization is the process of organizing data into categories for its most effective and efficient use.
- Data classification enables the separation and classification of data according to data set requirements for various business or personal objectives. It is mainly a data management process.
- This is generally done through a database or business intelligence software that provides the ability to scan, identify and separate data.
- Some examples and applications of data classification include:
  - Separating customer data based on gender
  - Identifying and keeping frequently used data in disk/memory cache
  - Data sorting based on content/file type, size and time of data

o Sorting for security reasons by classifying data into restricted, public or private data types.
• To be effective, a classification scheme should be simple enough that all employees can execute it properly.

• Here is an example of what a data classification scheme might look like:
• Category 4: Highly sensitive corporate and customer data that if disclosed could put the organization at financial or legal risk.
o Example: Employee social security numbers, customer credit card numbers
• Category 3: Sensitive internal data that if disclosed could negatively affect operations.
o Example: Contracts with third-party suppliers, employee reviews
• Category 2: Internal data that is not meant for public disclosure.
o Example: Sales rules, organizational charts
• Category 1: Data that may be freely disclosed with the public.
o Example: Contact information, price lists

Categorization of Database users:
• There are two classes of DBMS users:
 Actors on the Scene: Person whose job involves daily use of a large database are:
 Database administrator
 Database designer
 End users
 System Analysts
 Application programmers.
 Workers behind the scene: Persons whose job involves design, development, operation and maintenance of the DBMS software are:
 DBMS designers and implementers
 Tool developers
 Operator and maintenance personnel

(Database Threats)
Loss of Integrity:
• Data integrity is the maintenance of, and the assurance of the accuracy and consistency of, data over its entire life-cycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data.

- Database integrity refers to the requirement that information be protected from improper modification which includes creation, insertion, modification, changing the status of data and deletion.

- Any unintended changes to data as the result of a storage, retrieval or processing operation, including malicious intent, unexpected hardware failure, and human error, is failure of data integrity.
- If the changes are the result of unauthorized access, it may also be a failure of data security.
- Integrity lost if authorized changes are made to the data by either intentional or accidental acts.
- If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data would result in inaccuracy, fraud or erroneous decisions.
- Physical integrity deals with challenges associated with correctly storing and fetching the data itself.
- Challenges with physical integrity may include electromechanical faults, design flaws, corrosion, power outages, natural disasters, acts of war and terrorism, and other special environmental hazards.
- Logical integrity is concerned with the correctness or rationality of a piece of data, given a particular context.
- This includes topics such as referential integrity and entity integrity in a relational database or correctly ignoring impossible sensor data in robotic systems.
- These concerns involve ensuring that the data "makes sense" given its environment.
- Challenges include software bugs, design flaws, and human errors.
- Common methods of ensuring logical integrity include things such as a check constraints, foreign key constraints, program assertions, and other run-time sanity checks.

Loss of availability:

- Database availability refers to making objects available to a human user or a program to which they have a legitimate right.
- Primary methods that organizations use to protect against loss of availability are fault tolerant systems, redundancies, and backups.
- Fault tolerance means that a system can develop a fault, yet tolerate it and continue to operate.
- This is often accomplished with redundant systems such as redundant drives or redundant servers.

- Backups ensure that that important data is backed up and can be restored if the original data becomes corrupt.

Loss of confidentiality:

- Data confidentiality refers to the protection of data from unauthorized disclosure.
- The impact is of confidential information can range from violation of data privacy act.
- Unauthorized, unanticipated or unintentional disclosure could result in loss of public confidence, or legal action against the organization.
- Organizations protect against loss of confidentiality with access controls and encryption.
- For example, users are first required to authenticate and then access is granted to users based on their proven identity.
- In short, users are granted access to data via permissions. If users do not have permissions, they are denied access.
- However, there are many other instances where someone can access data without needing to prove their identity.
- For example, any data sent over the network can be captured with a sniffer.
- Additionally, any data at rest in the database(or on a hard disk drive, or a portable USB flash drive) could be stolen and easily accessed.
- You can protect this data from loss of confidentiality with encryption.

Database Security Control Measures:

- There are four main control measures used to provide security of data in databases. They are:

 Access Control:

- Access control is a way of limiting access to a system or to physical or virtual resources.
- In DBMS, access control is a process by which database users are granted access and certain privileges to systems, resources or information.
- Users must present credentials before they can be granted access.
- The security mechanism of a DBMS must include provisions for restricting access to the database as a whole.
- This function is handled by creating user accounts and passwords to control the login process by the DBMS.

 Inference Control:

- Inference is a database system technique used to attack databases where malicious users infer sensitive information from complex databases.
- In basic terms, inference is a technique used to find information hidden from normal users.
- It is possible to deduce or infer certain facts concerning individuals form queries that involve only summary on groups, consequently this must not be permitted either.
- An inference attack may endanger the integrity of an entire database.
- The more complex the database is, the greater the security implemented in association with it should be.
- If inference problems are not solved efficiently, sensitive information may be leaked to outsiders.
- Two inference vulnerabilities that appear in databases are data association and data aggregation.
- When two values taken together are classified at a higher level than one of every value involved, this becomes a data association.
- When a set of information is classified at a higher level than the individual level of data, it is a clear case of data aggregation.
- The sensitive data leaked through inference involves bound data, where an attacker finds out a range of data holding expected data or negative data, which is obtained as a result of certain innocent queries.

Flow control:

- Flow control is the mechanism that ensures the rate at which a sender is transmitting is in proportion with the receiver's receiving capabilities.
- Too much data arriving before a device can handle it causes data overflow, meaning the data is either lost or must be retransmitted.
- It prevents information from flowing in such a way that it reaches unauthorized users.

Data encryption:

- It is used to protect sensitive data that is transmitted via some type communication network.
- Encryption can be used to provide additional protection for sensitive portions of database.
- The data is encoded using some cryptographic algorithm.
- An unauthorized user who access encoded data will have difficulty deciphering it, but authorized users are given decoding or decryption algorithms to decipher data.

UNIT 10
Policy and Procedures

Computer Crime, Cyber Crime and Categories:

- Any illegal act involving a computer generally is referred to as a computer crime.
- Alternatively referred to as cyber crime, e-crime, electronic crime, or hi-tech crime.
- The term cybercrime refers to online or Internet-based illegal acts.
- Cybercriminals use computer technology to access personal information, business trade secrets or use the internet for malicious purposes.
- Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker, that illegally browses or steals a company's or individual's private information.
- In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.
- Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access.
- Some of the examples of computer crimes are copyright violation, cracking, cyber terrorism(threats and blackmails), cyberbullying or cyberstalking, creating malwares, DOS attack, identity theft, phishing, scam, software piracy etc.

Computer crime laws prohibit a person from performing certain acts without authorization, including:

- Improperly accessing a computer, system, or network;
- Modifying, damaging, using, disclosing, copying, or taking programs or data;
- Introducing a virus or other contaminant into a computer system;
- Using a computer in a scheme to fraud;
- Interfering with someone else's computer access or use;
- Using encryption in aid of a crime;
- Falsifying email source information; and
- Stealing an information service from a provider.

- There are primarily four general types of computer crimes.
- However, in practice, multiple crimes, that is, concurrent criminality or lesser offenses, can occur during any given criminal transaction, resulting in an overlap between the classifications.

- **Computer as the target:**

• Crimes in which the computer is the target include such offenses as theft of intellectual property, theft of marketing information (e.g., customer lists, pricing data, or marketing plans), or blackmail based on information gained from computerized files (e.g., medical information, personal history, or sexual preference).

- **Computer As the Instrumentality of the Crime**

• In common law, instrumentality refers to the diversion of a lawfully possessed item, that is, an instrument, to facilitate committing a crime.
• In this category, the processes of the computer, not the contents of computer files, facilitate the crime.
• The criminal introduces a new code (programming instructions) to manipulate the computer's analytical processes, thereby facilitating the crime.
• Another method involves converting legitimate computer processes for illegitimate purposes.

- **Computer Is Incidental to Other Crimes**

• In this category of computer crime, the computer is not essential for the crime to occur, but it is related to the criminal act.
• This means that the crime could occur without the technology; however, computerization helps the crime to occur faster, permits processing of greater amounts of information, and makes the crime more difficult to identify and trace.
• Such crimes include money laundering, unlawful banking transactions etc.

- **Crimes Associated With the Prevalence of Computers**

• The simple presence of computers, and notably the widespread growth of microcomputers, generates new versions of fairly traditional crimes.
• In these cases, technological growth essentially creates new crime targets.
• Software piracy/ counterfeiting, copyright violation of computer programs, counterfeit equipment, black market computer equipment and programs, and theft of technological equipment fall into this category of computer crime.
• Cybercrime encompasses a wide range of activities, but these can generally be broken into two categories:
o Crimes that target computer networks or devices. These types of crimes include viruses and denial-of-service (DoS) attacks.
o Crimes that use computer networks to advance other criminal activities. These types of crimes include cyberstalking, phishing and fraud or identity theft.

Digital Forensics:

- Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.
- Digital forensics is the process of uncovering and interpreting electronic data.
- The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.
- The context is most often for usage of data in a court of law, though digital forensics can be used in other instances.
- Digital Forensics may also feature in the private sector, such as during internal corporate investigations or intrusion investigation.

Digital Evidence:

- Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device.
- This evidence can be acquired when electronic devices are seized and secured for examination.
- Some properties of Digital evidence are:
  - Hidden, like fingerprints or DNA evidence
  - Crosses jurisdictional borders quickly and easily
  - Can be altered, damaged or destroyed with little effort
  - Can be time sensitive
- There are many sources of digital evidence but three major forensic categories of devices where evidence can be found: Internet-based, stand-alone computers or devices, and mobile devices.
- These areas tend to have different evidence-gathering processes, tools and concerns, and different types of crimes tend to lend themselves to one device or the other.
- Digital evidence is information stored or transmitted in binary form that may be relied on in court.
- Laws dealing with digital evidence are concerned with two issues: integrity and authenticity.
- Integrity is ensuring that the act of seizing and acquiring digital media does not modify the evidence (either the original or the copy).
- Authenticity refers to the ability to confirm the integrity of information; for example that the imaged media matches the original evidence.

Investigation procedures:

- With the increase of cyber crime, tracking malicious online activity has become crucial for protecting private citizens, as well as preserving online operations in public safety, national security, government and law enforcement.
- Tracking digital activity allows investigators to connect cyber communications and digitally-stored information to physical evidence of criminal activity; computer forensics also allows investigators to uncover premeditated criminal intent and may aid in the prevention of future cyber crimes.
- For the investigators, there are five critical steps in digital evidence investigation procedure, all of which contribute to a thorough and revealing investigation.

Policy and Procedure Development

- Whether related to malicious cyber activity, criminal conspiracy or the intent to commit a crime, digital evidence can be delicate and highly sensitive.
- Cybersecurity professionals understand the value of this information and respect the fact that it can be easily compromised if not properly handled and protected.
- For this reason, it is critical to establish and follow strict guidelines and procedures for activities related to computer forensic investigations.
- Such procedures can include detailed instructions about when computer forensics investigators are authorized to recover potential digital evidence, how to properly prepare systems for evidence retrieval, where to store any retrieved evidence, and how to document these activities to help ensure the authenticity of the data.

Evidence Assessment

- A key component of the investigative process involves the assessment of potential evidence in cyber crime.
- Central to the effective processing of evidence is a clear understanding of the details of the case at hand and thus, the classification of cyber crime in question.
- For instance, if an agency seeks to prove that an individual has committed crimes related to identity theft, computer forensics investigators use sophisticated methods to extract evidences through hard drives, email accounts, social networking sites and other digital archives to retrieve and assess any information that can serve as viable evidence of the crime.
- Prior to conducting an investigation, the investigator must define the types of evidence and have a clear understanding of how to preserve applicable data.

- The investigator must then determine the source and integrity of such data before entering it into evidence.

Evidence Acquisition

- Perhaps the most critical aspect of successful digital evidence investigation is a effective and detailed plan for acquiring evidence.
- Extensive documentation is needed prior to, during, and after the acquisition process; detailed information must be recorded and preserved, including all hardware and software specifications, any systems used in the investigation process, and the systems being investigated.
- This step is where policies related to preserving the integrity of potential evidence are most applicable.
- General guidelines for preserving evidence include: the physical removal of storage devices, using controlled boot discs to retrieve sensitive data and ensure functionality, and taking appropriate steps to copy and transfer evidence to the investigator's system.
- Acquiring evidence must be accomplished in a manner both deliberate and legal.
- Being able to document and authenticate the chain of evidence is crucial when pursuing a court case, and this is especially true for digital forensics given the complexity of most cybersecurity cases.

Evidence Examination

- In order to effectively investigate potential evidence, procedures must be in place for retrieving, copying, and storing evidence within appropriate databases.
- Investigators typically examine data from designated archives, using a variety of methods and approaches to analyze information; these could include utilizing analysis software to search massive archives of data for specific keywords or file types, as well as procedures for retrieving files that have been recently deleted.
- Data tagged with times and dates is particularly useful to investigators, as are suspicious files or programs that have been encrypted or intentionally hidden.
- Analyzing file names is also useful, as it can help determine when and where specific data was created, downloaded, or uploaded and can help investigators connect files on storage devices to online data transfers (such as cloud-based storage, email, or other Internet communications).

Documenting and Reporting

- In addition to fully documenting information related to hardware and software specs, computer forensic investigators must keep an accurate record of all activity related to the investigation, including all methods used for testing system functionality and retrieving, copying, and storing data, as well as all actions taken to acquire, examine and assess evidence.
- Not only does this demonstrate how the integrity of user data has been preserved, but it also ensures proper policies and procedures have been applied to by all parties.
- As the purpose of the entire process is to acquire data that can be presented as evidence in a court of law, an investigator's failure to accurately document his or her process could compromise the validity of that evidence and ultimately, the case itself.

Categories of Evidence:

- The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files.
- The forms of digital evidences include the following categories:

Impressions:

- Impression evidences in cyber crime are the type of evidences that can be found on digital media devices or the physical location of the crime which includes fingerprints, tool marks, footwear marks, and other types of impressions and marks.

Bioforensics:

- The evidences that are found in the location of cyber crime including blood, body fluids, hair, nail scrapings, bloodstain patterns etc of the people being involved in the crime is called bioforensics.

Trace evidence:

- This includes residues of things used in the committing of a crime like arson accelerant, paint, glass, and fibers.

Material evidence:

- This includes physical materials such as folders, letters, and scraps of papers that are found in the crime location.

Intellectual Property Rights:

- Intellectual property (IP) is any intangible asset that is created from an original thought, such as an idea, name, content, design, invention or digital media.
- Intellectual property rights (IPR) refer to the rights of IP owners and authors.
- IP is divided into two categories:
  - Industrial property
  - Copyright

- **Industrial property covers:**
  - Patents (inventions): Require public registration and provide up to 20 years of protection against any unauthorized use, likeness and unfair competition.
  - Industrial design: Protects creations that define or describe a product, including trademarks and commercial names and logos.
  - Geographical source indications
- Copyright protects rights related to literary and artistic creations, including:
  - Art and literary works: Books, film, sound recordings, software, designs
  - Performances
  - Radio and TV broadcasters
  - Technology-based works, such as computer programs and databases
- Copyright law protects IP owners against unauthorized use or replication.
- The main purpose of intellectual property law is to encourage the creation of a large variety of intellectual goods.
- To achieve this, the law gives people and businesses property rights to the information and intellectual goods they create – usually for a limited period of time.
- This gives economic incentive for their creation, because it allows people to profit from the information and intellectual goods they create.

Copyrights:

- Copyright (or author's right) is a legal term used to describe the rights that creators have over their literary and artistic works.
- The creator has exclusive rights to determine and decide whether, and under what conditions, this original work may be used by others
- Works covered by copyright range from books, music, paintings, sculpture, and films, to computer programs, databases, advertisements, maps, and technical drawings.
- Under current law in the U.S., works created after Jan. 1, 1978, are afforded copyright protection for the life of the author plus an additional 70 years.

- For anonymous, pseudonymous and corporate-owned works, a copyright lasts 95 years from the year of its first publication or a term of 120 years from the year of its creation, whichever expires first.
- A major limitation on copyright on ideas is that copyright protects only the original expression of ideas, and not the underlying ideas themselves.

Trademarks:

- A trademark is a word, phrase, symbol, and/or design that identifies and distinguishes the source of the goods, products or services of one party from those of others.
- The trademark owner can be an individual, business organization, or any legal entity.
- 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.

Patents Licenses:

- A patent is a set of exclusive rights granted to an inventor or assignee for a limited period of time in exchange for detailed public disclosure of an invention.
- An invention is a solution to a specific technological problem and is a product or a process.
- Patents are a form of intellectual property.
- In basic terms, a patent allows the patent holder to stop others from building his invention.
- A license is an agreement between two parties. The licensor allows the licensee to do something (use the software, build an invention).

Agreements:

- A negotiated and usually legally enforceable understanding between two or more legally competent parties is called agreement.
- Although a binding contract can (and often does) result from an agreement, an agreement typically documents the give-and-take of a negotiated settlement and a contract specifies the minimum acceptable standard of performance.
- Agreement may refer to:

- Agreement (linguistics) , a change in the form of a word depending on grammatical features of another word
- Gentlemen's agreement, not enforceable by law
- Trade agreement, between countries

- Contract, enforceable in a court of law

e.g. Meeting of the minds (a.k.a. mutual agreement), a common understanding in the formation of a contract

Plagiarism:

- Plagiarism is the "wrongful appropriation" and "stealing and publication" of another author's "language, thoughts, ideas, or expressions" and the representation of them as one's own original work.
- Basically, plagiarism means:
  - to steal and pass off (the ideas or words of another) as one's own
  - to use (another's production) without crediting the source
  - to commit literary theft
  - to present as new and original idea or product derived from an existing source
- In other words, plagiarism is an act of fraud.
- It involves both stealing someone else's work and lying about it afterward.

Digital Rights Management:

- Digital rights management (DRM) is a set of access control technologies for restricting the use of proprietary hardware and copyrighted works.
- In other words, Digital rights management (DRM) is a systematic approach to copyright protection for digital media.
- DRM technologies try to control the use, modification, and distribution of copyrighted works (such as software and multimedia content), as well as systems within devices that enforce these policies.

- The purpose of DRM is to prevent unauthorized redistribution of digital media and restrict the ways consumers can copy content they've purchased.
- DRM products were developed in response to the rapid increase in online piracy of commercially marketed material, which proliferated through the widespread use of peer-to-peer file exchange programs.
- Typically DRM is implemented by embedding code that prevents copying, specifies a time period in which the content can be accessed or limits the number of devices the media can be installed on.

Privacy protection:

- Information privacy, or data privacy (or data protection), is the relationship between the collection and distribution of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.
- Privacy concerns exist wherever personally identifiable information or other sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues.

Cyber Law:

- Cyber law is the area of law that deals with the Internet's relationship to technological and electronic elements, including computers, software, hardware and information systems (IS).
- Cyber law is also known as Internet Law.
- Cyber laws prevent or reduce large scale damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property (IP) and freedom of speech related to the use of the Internet, websites, email, computers, cell phones, software and hardware, such as data storage devices.
- Cyber law applies to the internet and internet-related technologies.
- Cyber law provides legal protections to people using the internet.
- This includes both businesses and everyday citizens.
- Understanding cyber law is of the utmost importance to anyone who uses the internet.

Electronic Transaction Act(ETA):

Refer the document uploaded.
Preamble, Preliminary, Definitions (compulsory)
(Also see the different provisions and gather some knowledge, because you never know what might be asked.)

Electronic Transaction Rules(ETR)

- This rule, also called the Electronic Data Interchange, or EDI, specifies how certain electronic transactions are transferred from one computer to another.
- These Rules may be called Electronic Transaction Rules.
- Refer the document uploaded.
- Preliminary, Definitions and Procedures (compulsory)
- Read the whole document in case

Information Technology (IT)Policy:

(Refer to the document uploaded, this is not sufficient)

- The policies to be pursued for the implementation of IT strategies shall be as follows:
  - To declare information technology sectors a prioritized sector.
  - To follow a single-door system for the development of information technology.
  - To prioritize research and development of information technology.
- To create a conducive environment that will attract investment in the private sector, keeping in view the private sector's role in the development of information technology.
- To provide internet facilities to all Villages of the country in phases.
- To render assistance to educational institutions and encourage native and foreign training as a necessity of fulfilling the requirement of qualified manpower in various fields pertaining to information technology.
- To computerize the records of each governmental office and build websites for them for the flow of information.
- To increase the use of computers in the private sector.
- To develop physical and virtual information technology park in various places with the private sector's participation for the development of information technology.
- To use information technology to promote e-commerce, e-education, e-health, among others, and to transfer technology in rural areas.
- To establish National Information Technology Centre.
- To establish a national level fund by mobilizing the resources obtained from Nepal Government, donor agencies, and private sectors so as to contribute to research and development of information technology and other activities pertaining to it.
- To establish venture capital funds with the joint participation of public and private sectors.
- To include computer education in the curriculum from the school level and broaden its scope.
- To establish Nepal in the global market through the use of information technology.
- To draft necessary laws that provides legal sanctions to the use of information technology.

Cyber Law Issues in Nepal:

- Cyberlaw differs from different countries and is the issues related to the activities over the internet and other communication technology, including privacy, jurisdiction.
- Cyberlaw is very important since these days along with the use of internet the crimes over the internet has been increasing day to day.
- It also maintains the privacy of the end user so that they would be safe from being a victim of cybercrime.
- Cyber laws design a secure platform and also a standard model for the advancement of cybersecurity.
- In Nepal, cyber law is also known as ETA (Electronic Transaction Act) which deals with issues related to cybercrime and also help in making and implementing laws over cybercrime.
- It has made different laws so that if anyone found having cybercrime he/she will be punished according to the scene of the crime.
- He /she can be jailed for minimum from 6 months to maximum of 3 years and has to pay penalty according to the crime.
- However, the cybercrime has been growing rapidly in Nepal because of a poor tracking system and the advancement needs still to grow like in other developed countries.
- The lack of proper updates of ETA, the hackers still hacks the governmental confidentiality which is an embracing to tell.
- ETA still hasn't properly addressed Online payment, due to which we still don't have fast and reliable online payment system too.
- The strongest challenge in the field of cyberlaw in Nepal is the challenge of implement cyber laws.
- For the implementation of the law, people over the internet in Nepal should have proper knowledge about the cybercrime and its consequences.
- Without the knowledge of the cyber crimes and law people will have no awareness of them.
- Maintaining the privacy in the cyberspace, creating the strong passwords, updating the security software, updating password are some of the techniques to keep secure him /her.

Information security and policies:

- Information security policy is a set of policies issued by an organization to ensure that all information technology users within the domain of the organization or its networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organization's boundaries of authority.

- In business, a security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets.
- A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change.
- A company's security policy may include an acceptable use policy, a description of how the company plans to educate its employees about protecting the company's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.
- Every organization needs to protect its data and also control how it should be distributed both within and without the organizational boundaries.
- This may mean that information may have to be encrypted, authorized through a third party or institution and may have restrictions placed on its distribution with reference to a classification system laid out in the information security policy.
- An example of the use of an information security policy might be in a data storage facility which stores database records on behalf of medical facilities.
- These records are sensitive and cannot be shared, under penalty of law, with any unauthorized recipient whether a real person or another device.
- An information security policy would be enabled within the software that the facility uses to manage the data they are responsible for.
- In addition, workers would generally be contractually bound to comply with such a policy and would have to have sight of it prior to operating the data management software.
- A business might employ an information security policy to protect its digital assets and intellectual rights in efforts to prevent theft of industrial secrets and information that could benefit competitors.

UNIT 11
Issues with Internet in college

Cyberbullying:

- Cyberbullying is a practice where an individual or group uses the Internet to ridicule, harass or harm another person.
- In other words, cyberbullying or cyber harassment is a form of bullying or harassment using electronic means.

- Also known as online bullying.
- Cyberbullying is a prosecutable offense in some jurisdictions, but a globally uniform legal approach has not yet been established.
- Cyberbullies use social media and smartphones to harass victims from remote or local areas.
- Traditional bullying usually stops when a victim returns to the safety of his home, but cyberbullying is a continuous process maintained through email, texting, forum/blog posts and other communication mediums.
- Even if cyberbullying victims change profile settings and avoid certain websites, cyberbullies may easily continue public bullying activities.
- It has become increasingly common, especially among teenagers.
- Harmful bullying behavior can include posting rumors, threats, sexual remarks, a victims' personal information etc.
- Some recommendations for victims to avoid cyberbullying are:
  - Block cyberbullies on all social media sites.
  - Report cyberbullies to website administrators.
  - Avoid sharing personal details online.
  - If you are a minor, speak to a trusted adult about cyberbullying.

Cyberstalking:

- Cyberstalking is a form of online harassment in which the perpetrator uses electronic communications to stalk a victim.
- Stalking is unwanted or repeated surveillance by an individual or group towards another person.
- This is considered more dangerous than other forms of cyberbullying because it generally involves a credible threat to the victim's safety.
- They may encourage others to do the same, either explicitly or by impersonating their victim and asking others to contact them.

Curbing student use of technology to intimidate and harass others:

- Bullying in schools is hardly a new problem, but in today's "connected" world, it doesn't look like it once did.
- Face-to-face harassment incidents, once confined to the schoolyard, have moved to the cyber schoolyard.
- Students and teens are using technology to target one another.
- They take social media outlets, such as Facebook, Twitter and YouTube and turn them into powerful instruments to stalk and harass the victims.
- The biggest challenge to combating cyber bullying is leaning which students are dealing with cyberbullying because it is not usually reported.

- There will never be a complete “cure” for bullying and cyber bullying behavior.
- However, with continuous focus, energy, and commitment, there can be successful management of all forms of bullying, with significant minimization of the number of victims.
- However, experts suggest some simple steps that school administration can take to respond appropriately to cyber bullying.

The steps are:

- Develop clear rules and policies to prohibit the use of school technologies to bully others.
- Educate students and staff members about what types of behavior constitute cyber bullying and how the school’s policies apply to them.
- Provide adequate supervision and monitoring of student use of technology.
- Establish systems for reporting cyber bullying or misuse of technology.
- Establish effective responses to reports of cyber bullying.

Student use of Internet: Reducing inappropriate internet behaviors;

- Students must understand that internet searching and activity that involves inappropriate material is prohibited.
- Activities that are considered inappropriate include but are not limited to:
  - Visiting websites such as pornographic, obscene, sexually explicit, jokes, gambling, gossip etc., that are not work related.
  - Downloading of inappropriate material including pornographic, obscene, sexually explicit, music/audio that is copyright protected.
  - Internet surfing for personal purposes such as shopping, banking, research for personal purposes, online auctions, sports message boards, etc.
  - Using social medias to stalk and bully others.
- Students think of best practices only in the sense of electronic mail and internet use.
- It must be understood that any acceptable use also extends to: computer hardware and peripherals; software; network access; storage devices: databases, files, and other repositories of information in electronic form.

Components of comprehensive approach in schools and colleges to support safe and responsible use of internet is:

- Focus on educational purpose
- Clear policy that is well-communicated to students

- Safe internet places for younger students
- Education About the Safe and Responsible Use
- Supervision and Monitoring
- Appropriate Discipline

Staff use of the Internet: Drawing a Line between teacher's public and private lives;

- Social media have blurred the lines between teacher's public and private life.
- Every month, there are reports of students suspended and teachers disciplined for behaving badly online.
- While teachers should know better, some insist on posting status updates such as "I hate my students" after a rough school day.
- Teachers should be responsible and professional if they are using social media connected with students.
- Ontario college, Canada advised teachers to decline friend requests from students, avoid e-mailing with them from personal addresses and refrain from corresponding late at night - even about homework.
- The college also urged teachers to reflect on how they use Twitter, YouTube and other online channels, all with a mind to maintaining "the public trust."
- Teachers have their private lives too but should be careful enough in case of use of technology.
- This applies to other staffs of academic organizations too.
- There are many cases of teachers being suspended worldwide due to unusual and irresponsible behavior in social media.
- Its difficult to distinguish where to draw the line between public and private lives but is necessary to have certain boundary and responsibility to maintain it.

Privacy and Security: Protecting student information;

- It is the responsibility of any institution to protect the information related to its members.
- In case of academic institutions, educators should keep their students' records out of the wrong hands.
- Some ways to protect the student information are:
  - Assessing data collection practices
  - Identifying the security objectives
  - Appointing a data leader with responsibility for privacy and security compliance
  - Conducting risk assessment and identifying security needs
  - Data-mapping exercises

- Training
- Monitoring, Auditing and Reporting
- Accountability
- Managing third-party vendor relationships
- Establishing procedures to address breaches

The school as an Internet Service Provider: Providing access and protecting students;

- Use of safe, secure and appropriate online technologies in educational environment is important.
- Internet is essential for researches and other educational activities at higher levels of education.
- Even at lower levels, internet can be of significant importance for effective learning.
- Schools and colleges should provide internet to the students but with focus on educational purposes while reducing inappropriate behaviors.
- Schools that are leading the way in applying new information and communications technologies are finding that the Internet enables student access to a vast array of information resources that includes primary source material, subject specialist sites, materials from cultural institutions and current news media.
- The Internet also provides a compelling communication tool that enables students to link with students from across the globe, engage in collaborative curriculum project tasks online and publish their own materials on the web.
- Also, providing access to research papers and journals is necessary for students to explore the contents better and enhance their knowledge.
- However, the school administration should keep in mind that student privacy and protecting their information is of greater importance.
- Characteristically, Internet Access Management policies include:
  - guidelines to accessing good educational sites
  - support for developing critical skills in assessing Internet content
  - the need to supervise students appropriately
  - suggestions for acceptable use policies for students, codes of practice and establishing common sense classroom "rules"
  - information on tools to manage inappropriate material
  - advice on protecting students' privacy on the Internet, including through web-publishing
  - information on legal aspects

Copyright Law in the Classroom: steering clear of legal liability;

- Technology makes copying cheaper and the public display of copyrighted media easier than ever before.
- But the ease of reproducing copyrighted works is increasing copyright violation.
- When teachers and students use the Internet, they have access to a wide variety of material, much of which may be protected by copyright law.
- The primary copyright violations are of two types: illegal copying and illegal display or performance.
- Except for the occasional plagiarized passage or unattributed reference in student research papers, most educators have had little experience dealing with copyright issues in their classrooms.
- With the advent of the Internet, however, their need to know about copyright law and to understand its implications for such activities such as Internet research, downloading programs and documents, creating class Web sites, and installing software on school networks has increased dramatically.

Common classroom practices that should raise concerns about copyright violation include the following:

- Downloading copyrighted material from the Internet and using it in a way that violates the rights of the copyright owner.
- Allowing students to use the Internet system to download copyrighted material, such as MP3 files of popular music.
- Material posted on the public Web site in violation of copyright law.
- Software used in violation of copyright law.

- Recognizing and respecting the copyright status of works created by students is another important, and often neglected, aspect of copyright that schools need to consider.
- Students should learn about the rights they have as creators and about how copyright laws help protect those rights.
- All student-created works that are published by the school should include a copyright notice with the student's name or unique student identifier.
- When students understand that copyright laws protect their personal interests, they will be more inclined to respect the copyright rights of other creators.

Policies, procedures and contracts: communicating expectations to teachers, students and parents;

- Well crafted policies lay out expectations, define rights and responsibilities, describe procedures and detail the remedies available if policy is violated.
- Policies allow administrators to use contract law principles to create a kind of private law that governs the school community.
- Acceptable use policies, bullying policies, parent permission slips, school handbooks, disciplinary procedures are all contracts.
- All these contracts are binding to the school community.
- For example: a school with an anti-bullying policy, based on its findings of an increase in offensive text messaging and emailing among students may amend its policies to include a prohibition against cyberbullying.
- Schools should include policies on the following: cyber bullying policy, student privacy and Data security, Rights and responsibilities of students, teachers and staffs, Copyright compliance policy etc.
- To make these policies effective, schools should establish a policy describing the recommended chain of command for reporting incidents.
- They can craft age appropriate tests students must pass before being granted license to participate in less structured internet activities.
- Contracts establish the private law developed by and between parties which allows parties to create their own rules.
- Parties can amend the contract in light of changing circumstances.

Notification to parents should include:

- A copy of the user notification form provided to the student
- Description of Parent/Guardian responsibility
- Notification that parents have the option to request alternative educational activities not requiring internet access
- A statement that the Student Online Acceptable Use Contract Form must be signed by the student, parent/guardian and teacher prior to use by student.
- A statement that the school's acceptable use policy is available for parental review.

Ethical Issues: Developing responsible internet citizens;

- Responsible and ethical use of the Internet is not something that teenagers, in particular, consider to be important, and serious consequences are beginning to emerge as a result of careless and offensive online behavior.
- Digital citizenship can be defined as "the norms of appropriate, responsible behavior with regard to technology use".
- The Internet has evolved into a "participatory culture," allowing students to create, connect, and collaborate with a global audience.

- School administration should put in place Acceptable Use Policies, which are a set of computer rules to ensure appropriate student usage of the Internet and technology equipment at school.
- But educators need to think of ways to train today's generation to be responsible and ethical life-long learners of the digital age.
- Teachers must demonstrate, guide, and help students practice appropriate and professional behavior while actively participating in authentic learning experiences using blogs, wiki spaces, learning management systems, online research, and much more.
- Wiki spaces is a place where you can write, discuss, and build web pages together but unfortunately it is being closed.
- The following tips can prepare students to be TECH SMART when using technology. (Note that when put together the first letter of each of the following headings spell out TECH SMART.)

 Take care of Technology Equipment
 Explore Appropriate and Safe sites for Learning and Research
 Copyright Law, Fair Use Act, and Creative Commons Matter
 Help prevent Cyberbullying
 Self-image is important
 Make use of netiquette (Netiquette can be defined as rules for online communication which includes Be aware of your audience; respect other's privacy; apply real-world rules; be nice; use proper writing style; do not send unsolicited emails; avoid personal attacks; learn the rules of the community; refrain from profanity; and don't use electronic devices while engaging in face-to-face interaction)
 Always give credit to original source
 Remember to be effective, thoughtful and ethical digital creators
 Think (There's always a purpose for technology use. Think of how, when, why, and for what purpose you're using it. Think of ways to be creative and innovative.)