MODULE: 1

INTRODUCTION TO SYSTEM SECURITY

Syllabus

Information Technology:

Introduction to Computer Security

Vulnerabilities, Threats and Attacks.
Public Key Cryptography and Cryptanalysis, Knapsack Cryptosystem (included in Module 2 – Cryptography)

Computer Engineering:

Security Attacks, Security Goals, Computer criminals, Methods of defense, Security Services, Security Mechanisms

Hello everyone! Welcome to the most interesting and simple subject in Engineering. The words like **"interesting", "simple"** doesn't suite for engineering students! Isn't it?

As the name suggest, the subject deals with some security aspects of computing. Let us take an example of earthquake. Suppose you are at your home with your friends. Say, some night-out plan is going on. Suddenly you feel that some *kind of vibration* happened at your home. After few seconds you realized that it is an earthquake! What you will do:

- You will inform your friends and recommend them to find some place which is safe to hide.
- You immediately switch off all electric switch board.
- You will find safe places like under the table or bed OR out of your home.
- At the worst situation, you will pray to god to save your life! Obviously, we engineering students always go to god for some serious issues like semester exams, viva, submissions etc.

Jokes apart! The points mentioned above are the counter measures about a particular problem (earthquake)

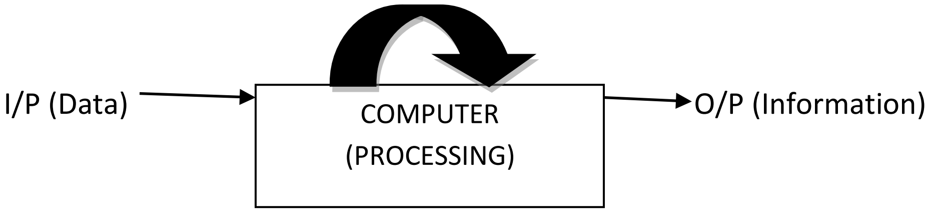
In computing also, there are many attacks or threats introduced into the system. We need to have some countermeasures or precautions which can save your system from unknown problems.

The central questions are: What is System? What is computing? Why attack is possible? What are the countermeasures of attack? How to overcome the problem of attacks?

The answer to all these questions is your Subject.

1.1 Prerequisite – INFORMATION AND SYSTEM:

The term “Information” is a collection of relevant data, which gives us meaningful knowledge about a particular entity. The information is always formed after processing of data.



Processing of data can be done in many ways .The important thing is that: It cannot be directly used however it should be processed in computer to get relevant information. For example suppose person “Ronny” has 5 pens say ‘red’, ’blue’, ’green’, ’black’, ’pink’.

How can we form information? It depends on particular person.

- One might create a picture of Ronny having 5-colour pens with him.
- The another ways is simple English sentence - “ My friend Ronny has 5 pens namely ‘red’, ’blue’, ’green’, ’black’ and ’pink’.

The example might be funny and useless in meaning but it will be easy for you to understand the difference between “data” and “information” .The “data” in this example is nothing but list of 5 colures viz. ‘red’, ’blue’, ’green’, ’black’ and ’pink’ and ‘Ronny’ itself. We have **processed** the **data** either by **creating a picture of Ronny** OR by **converting it into simple English language** which forms an Information**.**

The term “SYSTEM” is collection of components working together to provide a specific mechanism. Your system consists of collections of components like input (data), Processing components, output (information)

Set of components can be routers, cables, host where the mechanism are nothing but program execution, operating systems, browser access etc. The information is the base of all these mechanisms. In other words **SYSTEM provides a platform for information to process.**

1.1 Introduction to SYSTEM security:

In life, we always want to become secure! Isn’t it? We always implement some kind of procedure which will ensure security. We use “security” in many was in our daily lives. Security may be of different types. for example financial security involves the set of investment that are adequately funded .we hope the investment will grow in value over time, so that we have enough money to survive later in life .

The term **“SECURE”** means a state which *‘remains safe throughout a particular period of time.’* The entire subject deals with the theory about the security aspects of data, system and information.

The computer-related system has both theoretical and real weaknesses. The purpose of computer security is to devise ways to prevent the weaknesses from being exploited. In simple words, computer security specifically refers to safety of data and information which is stored in disks, tapes etc. with the increase in use of computers and digital storage in day-to-day life, there is a great need of safety of information. The use of system security becomes an essential part in corporate world where two computers can communicate with each other and may use the private information with each other. Such information should not be leaked or observed by the intruder or an attacker. Many of the industries have started recognizing the computers and their data valuable and vulnerable resources that should be protected.

Let us take previous example of my friend “Ronny” but with some modification. Suppose with the same story, Ronny wants to keep his information to be private that is - no one knows that he has 5 pens except his own desktop PC where he stored the same information. The interesting case is “what happened if someone tries to open his PC?” .It might be possible that someone has gained access to the information stored and can spread the wrong news also .

With this, you might have understood why we require our system to be secure? Let us define the term **“SYSTEM SECURITY”**

The SYSTEM SECURITY is the study of theoretical and real weaknesses and threats in computer-related system so that we can implement various protection mechanisms to protect the system.

The study of system security involves:

1. Examine the risk of security in computing

2. Consider available controls

3. Stimulate areas where more work is needed.

Cast of characters:

As mentioned earlier, entire subject deals with the secure communication between two hosts. I have kept the same example throughout the subjects so that it will be easier for you to understand. Let’s assume that “Ronny” and “Patrick” are good guys and they are communicating with each other in some way. Occasionally we also require additional good guy say “Jerry”. “Tom” is bad guy who is trying to attack the system in some way. “Ronny”, “Patrick” *and rest of the other gang need not to be humans. For example one possible scenario would be that Ronny is client computer, Patrick is sever where tom is human .*

1.2 SYSTEM security goals - CIA:

Expected Questions:

- Explain the goals of security
- Explain the terms with suitable example : Confidentiality , Integrity, Availability
- Explain CIA triad
- You are sending an e-mail to your friend. The email contains confidential information. How would you achieve the goals of security regarding to sending mail to your security.

The obvious question that one may ask: "when I say my system is secure? "

The answer looks difficult because no one has implemented a perfect security mechanism yet because attackers are always smarter than programmer's .In general, system is said to be "SECURE" if there is proper control of: **Confidentiality, Integrity, Availability (CIA).** The major challenge is to achieve proper and right balance among these three goals.

The diagram shown below is CIA. If these three goals are achieved then we can say that system is secure.

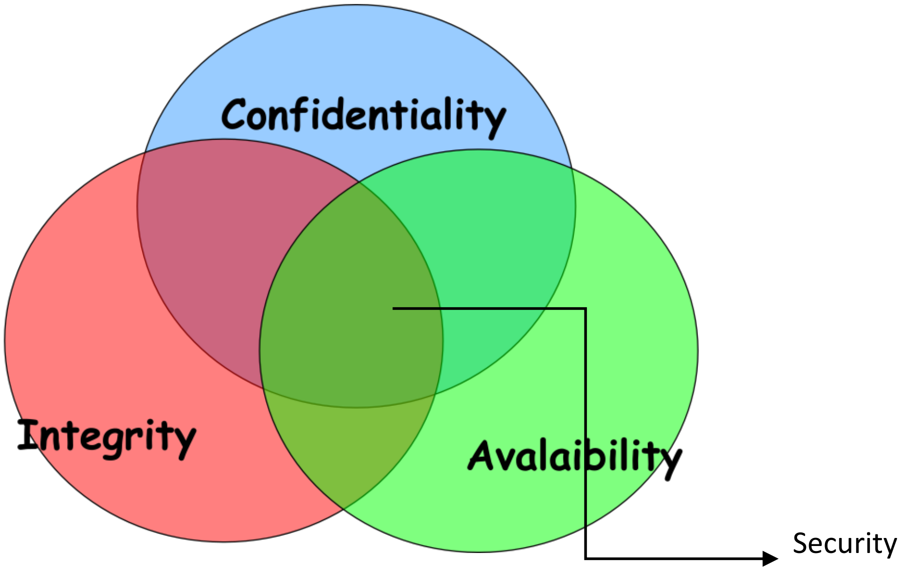
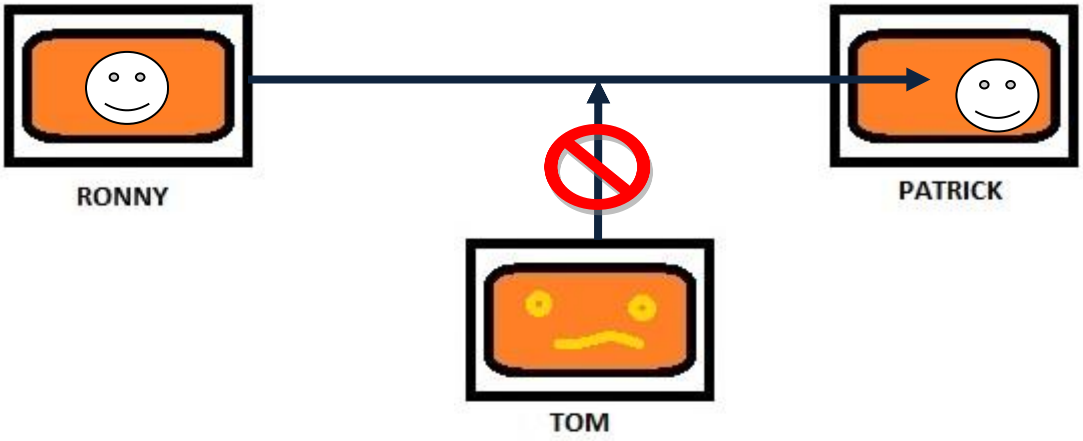


Figure 1 SECURITY goals: CIA

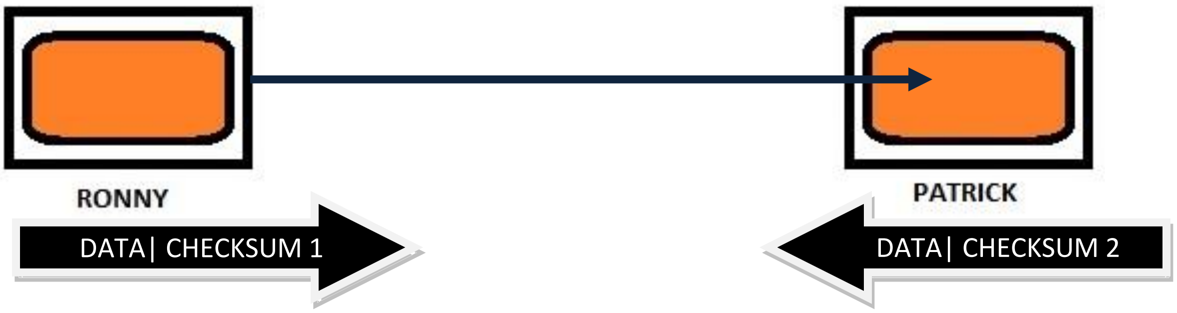
- **Confidentiality :**

- The term Confidentiality means only authorized people or system should access the data, Otherwise it is consider as Unauthorized Access.
- Access doesn't mean only reading; it also means viewing, printing or simply knowing that particular asset exists.
- To achieve confidentiality we used the "Encryption" technique that is message send by sender is encoded and then transmitted.
- In fig. below Ronny sends message X to Patrick .Message X is encrypted before transmission so that even if Tom tries to attack on communication channel he will not get information.



- **Integrity :**

- The term Integrity means only authorized party should modify the data send by receiver in authorized way and data should not be changed by attacker.
- The modification includes writing, changing, deleting the data from database.
- The data should be precise, accurate, unmodified, modified only by authorized people and authorized way – to achieve Integrity.
- To preserve integrity we implement "Checksum". Checksum is the binary block added with data part before transmission. The value of checksum should be preserved after transmission.
- In fig. below Ronny sends data X to Patrick. Checksum is appended before transmission. Patrick will calculate checksum. If both checksums are not same then Patrick will come to know that data is modified.



- For successful transmission data without modification , Checksum 1 = Checksum 2

- **Availability :**

- The principle of availability states that data or resources should be available to authorized parties at all times. In other words, data or resources should reach to receiver as it is.
- The goal of availability is preserved only

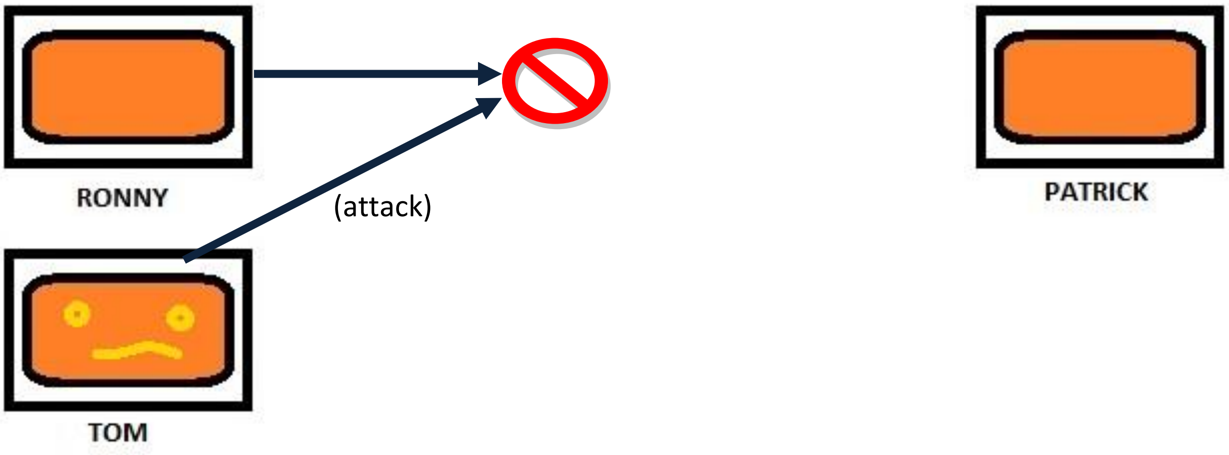
✓ If there should be appropriate response to request made by receiver.

✓ If the resources are available and no requester should be favored over others and system/service should be fault tolerance.

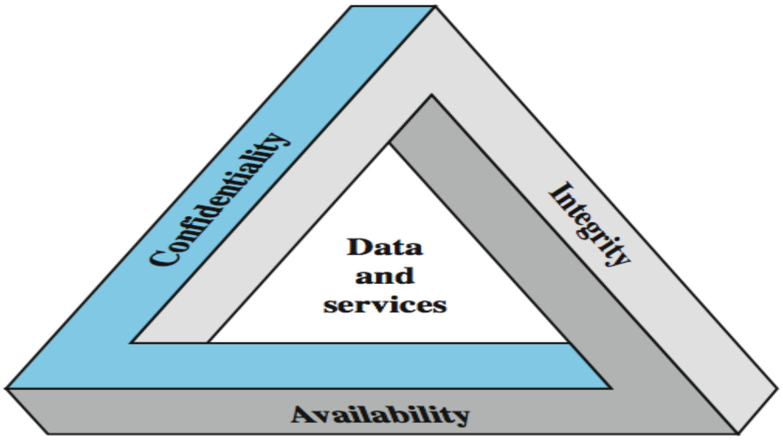
✓ If Hardware and software are properly configured so that they can able to transmit data properly.

✓ There should concurrency control for every Transaction. Deadlock management should be properly implemented.

- In fig. below Ronny and Patrick shares resources say sharing of some files. Tom interrupted in between so that sharing of file is unavailable for Patrick. (Attack on resources is called as **Denial of Service.**)

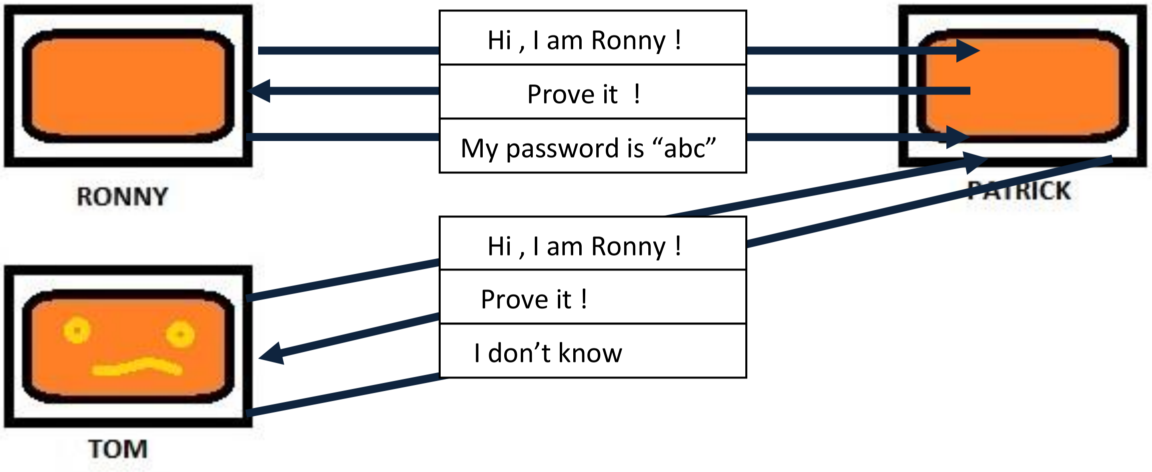


- **CIA Triad:**



- **Authenticity (Apart from CIA)**

- One of the secondary goals of security is Authentication .which means user should provide his own identity for accessing the resources.
- Authentication is simply implemented by password techniques, biometrics (finger prints, retina scan etc.), digital signature etc.
- Authentication process prevents “unauthorized access”. An unauthorized user may hide his own identity and can send malicious content/data to receiver .in order to prevent such access , sender is asked to prove his identity (often called ‘Entity Authentication’)
- In fig. Ronny is Authenticated user and Patrick is a Server .Ronny wants to access the resources from Patrick .Ronny has to prove his identity by unique password. After the password verification, Patrick allows him to access the resource. Whereas Tom who don’t know Ronny’s password, he is not able to access the resources as shown in the fig.



1.3 Vulnerability, Threats, attacks and Control:

```
Expected Question:

-  Explain  Threat,  Vulnerability  and  Control  in  computing  with
   suitable example
-  Differentiate Threats, vulnerabilities and control.
-  Short note on : Types of Vulnerabilities in security
-  Short note on : Threats possible in computing
-  Explain   the   following   terms   with   suitable   example:
   modification, fabrication, interception and interruption.
-  Difference between active and passive attacks.
-  Explain the types of attacks with suitable example
```

The basic questions regarding to security that can arise in our mind are-

- Why attackers attack our system?
- Is there any weak component present in our system?
- What are the precautions we need to take against attack?

The security of the system revolves around three concepts: Vulnerability, Threats, attacks and Control.

Vulnerability is nothing but the **Weakness in the system.** Weakness in the system may exploit an attack. Weakness can be in coding, design or can be anything related to software development. For instance system is vulnerable to unauthorized to resource access because your system does not verify the User-id entity before allowing resource access. In other words, the attack is only possible if System is vulnerable.

A threat is a set of activity that has ability to cause harm. The threat can be either generated by Human or Computer .Threat is purposely created by an attacker to attack on the system. In other words, an exploitation of vulnerability is attack on the system. **The threat in action** is called as Attack.

Control is an **action, device, procedure or technique** that removes or reduces vulnerability. Using Methods of defense the vulnerability in the system can be either removed or reduced in some way.

In order to understand these concepts let's take an example:

Ronny is new user on face book. He has created his own face book account and saved his User-id and password in notepad file as he could not remember his own User-id and password .His Friend Tom opens his PC and found the same password file with user-id. Tom is a bad guy. He managed to open Ronny's face book account every day. Tom Uses Ronny's face book account every day and chat with Ronny's friends on behalf of Ronny. However Ronny is unaware about overall scenario.

The above example will let you understand the difference between control, vulnerability, attack and threat in a better way.

- Ronny is saving his own User-id and password in his PC. Host PC is password unprotected – *vulnerability*
- Someone may hack his account by getting his password – *Threat*
- Tom is managing his account and Ronny doesn't have any idea- *attack*
- Ronny should either remember his password in his memory OR his PC should be password protected (in which the Facebook password) so that no one can open his PC without knowing the password- *Action*.

1.3.1 Vulnerability:

- As stated earlier, Vulnerability is nothing but the **Weakness in the system.** Weakness in the system may exploit an attack.

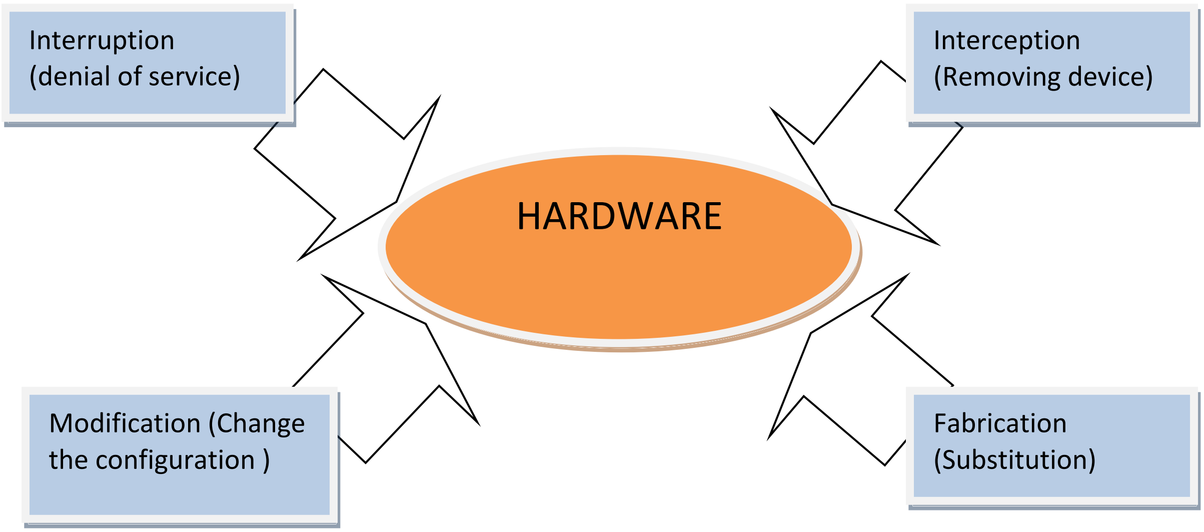
- Weakness can be in coding, design or implementation for the system. For instance system is vulnerable to unauthorized to resource access because your system does not verify the User-id entity before allowing resource access.

- In other words, the attack is only possible if System is vulnerable. An exploitation of vulnerability is attack on the system.

- A computer-based system has three separate vulnerable components viz. Hardware, Data, Software.

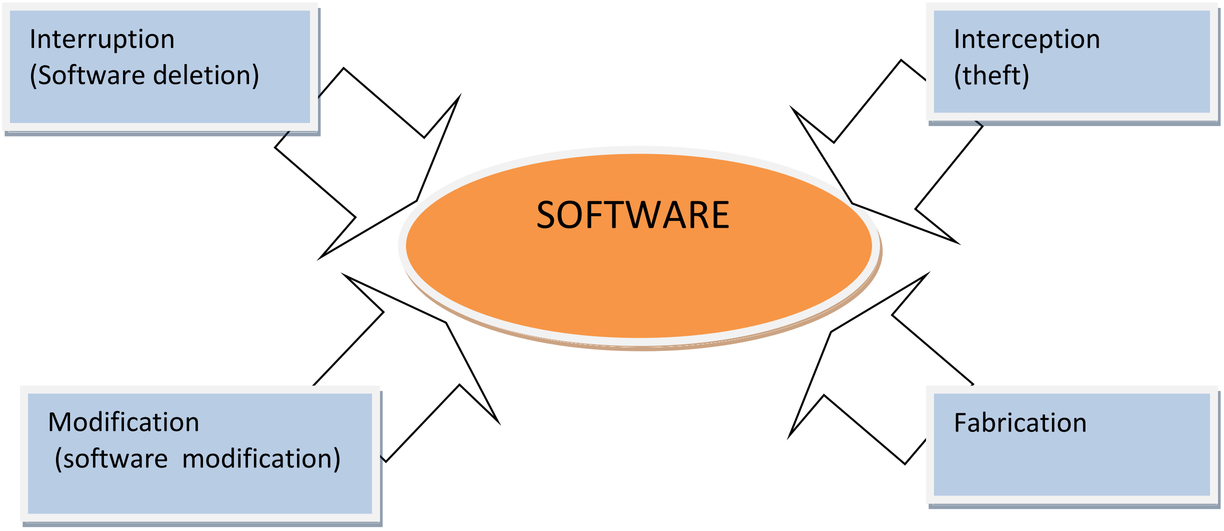
- **Hardware Vulnerability**

- Hardware is something which is visible and legal than software because it is composed of physical objects.
- The obvious vulnerability that can be seen on hardware is – adding device, changing them or sometimes forcefully changing their configurations or flooding them with traffic so that data can be blocked.
- Computers may have been drenched with water, burned, frozen, gassed and electrocuted with power surges. Such an accidental act is not intentionally done which cause serious damage to hardware.
- The only solution to prevent such vulnerability is to take care of computer and related devises. We can also put safeguards so that in future our hardware will be free from damage.
- The probability of hardware vulnerability is very low as this vulnerability can be easily detected and also it will not cause more harm as compared to software and data vulnerability.



- **Software Vulnerability**

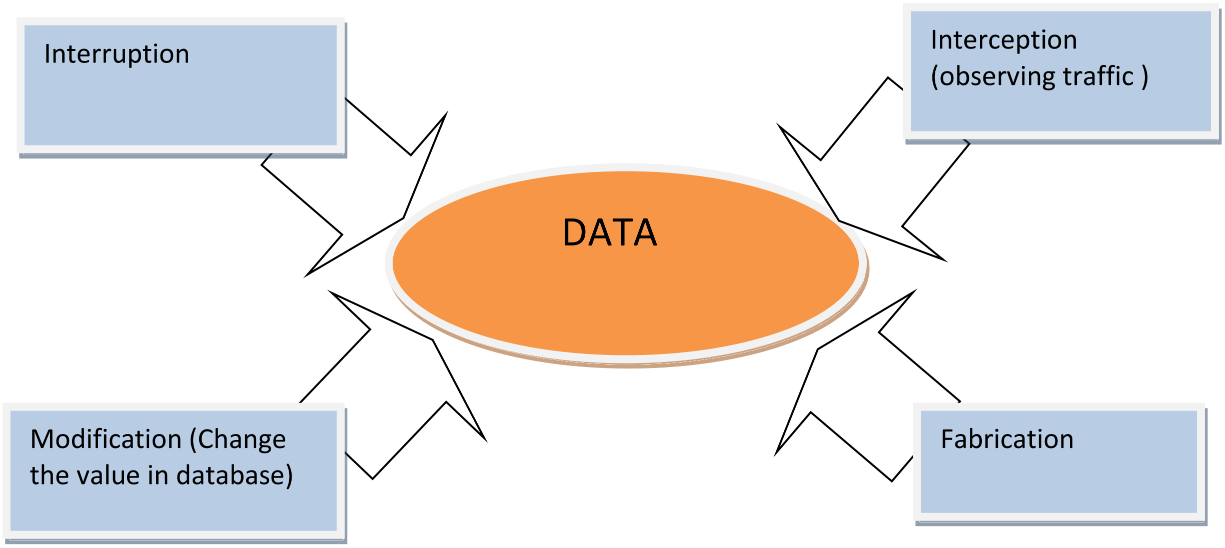
- Software is basically heart of any computing system. By software we mean utility programs, application programs, operating systems etc.
- Software can be changed; replaced, destroyed maliciously .Sometimes reverse Engineering techniques can be used to change the software code. For example the validity of Winrar can be changed using anti-debugging tool and can be made available lifetime.
- Sometimes software is unintentionally deleted. Some software act as a drivers to many functionalities like Audio, flash players etc. deleting such software may lead to stopping of such accessories.
- Software is sometimes modified to perform unintended tasks. For example a program can be modified to fail when certain condition is fulfilled or certain time is reached.(often called as *'Logic Bombs'*)
- Software also can be pirated for illegal use.
- Software vulnerability can be difficult to reduce. Because causes that are responsible to become a software vulnerable are many and for different purposes.

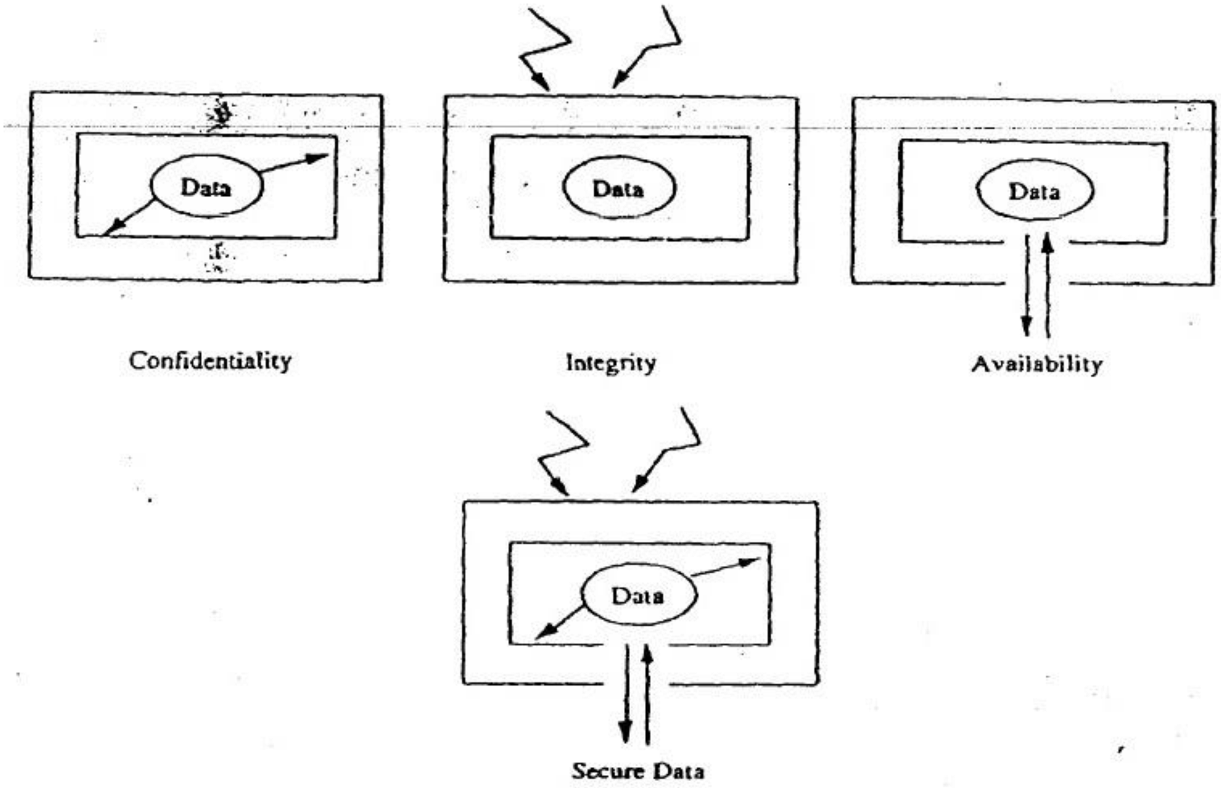


- **Data Vulnerability**

- Data items have greater public value as compared to software and hardware because they are easily identified. Because of visible nature of data ,attack on data is easily possible
- It is important to maintain data **confidentiality, availability and integrity** so that data can be seen to authorized people and system only.

- Confidentiality is the prevention of unauthorized disclosure of information. As data can be gathered from many physical devices (such as tapes, disks etc.) it is important to maintain the data confidential.
- Data integrity prevents data to modify from unauthenticated people or system. Small and most of the time skillful modification in data values can be ignored by people.
- Data vulnerability is most harmful than software and hardware vulnerability hence it should be properly handled.


Interruption
Interception (observing traffic)
DATA
Modification (Change the value in database)
Fabrication



1.3.2 Threats:

- A threat is a potential for violation of security or a possible danger that might exploit vulnerability.

- In other words a threat is a set of activity that has ability to cause harm. The threat can be either generated by Human or Computer.

- Threat is purposely created by an attacker to attack on the system. In other words, an exploitation of vulnerability is attack on the system.

- There are four kinds of threats possible: Interception, Interruption, Modification, and Fabrication.

- **Interception** :
  - Interception is keeping track of traffic without modification. In other words, some unauthorized system has gained access to an asset.
  - The unauthorized party can be a person, program or any computing device.
  - However Interception is very difficult to trace as silent interceptor leaves no traces while intercepting the data.

- **Interruption :**

- In interruption, the data may be lost or unavailable due to some unauthorized party.
- There are various ways by which attacker can achieve interruption. Either attacker can break the line so that communication cannot be completed further.
- The attacker can purposely send additional data on communication channel (called as Traffic) which will cause congestion on communication link.
- Interruption can be easily detected because of acknowledge system. (If data acknowledge for particular data is not reached to receiver, he will come to know that data is lost during transmission.)

- **Modification :**

- In modification, instead of intercepting or interrupting data is modified in some way. Receiver doesn't have any knowledge of this modification.
- Modification can be changing the values in particular database, altering the program execution flow, creating virus codes and appending it into program etc.
- Modification can be even possible by changing some configuration of hardware.
- By simple measures, Modification can be easily detected.

- **Fabrication :**

- In fabrication, attacker might hide his own identity and can send the data to receiver from some trusted host.
- This can be done skillfully by an attacker so that receiver will get to know that data is coming from trusted host.
- Fabrication is generally achieved by copying digital signature of trusted host and can append new malicious data.
- Sometimes fabrication is detected easily but if done skillfully then it is almost impossible to detect.

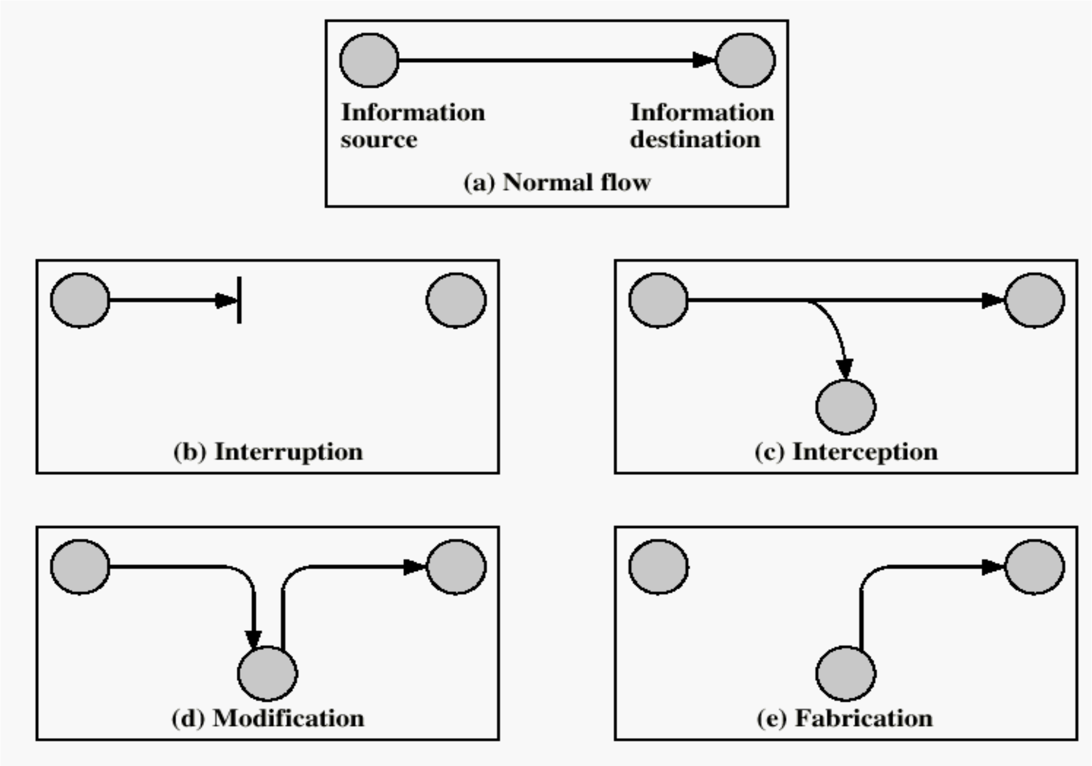


Figure 1.1 Security Threats

The fig. shows the four types of threats possible. Let us stick to our old example of Ronny, Patrick and Tom. Fig (a) shows a normal communication between Ronny and Patrick.

In fig (b) data is interrupted by an attacker Tom so that data become unavailable for Patrick.

In fig (c) Ronny is sending data to Patrick and Tom intercepted the data .data also reaches to Patrick.

In fig (d) data is modified by Tom and send to Patrick .As Patrick has not checked the authenticity of Tom.

In fig (e) Tom is copying the signature of Ronny and appending new malicious data which shows fabrication.

1.3.3 Attacks:

- We know that, an exploitation of vulnerability is attack on the system. **The threat in action** is called as Attack.

- There are two types of attacks – Active and Passive Attacks

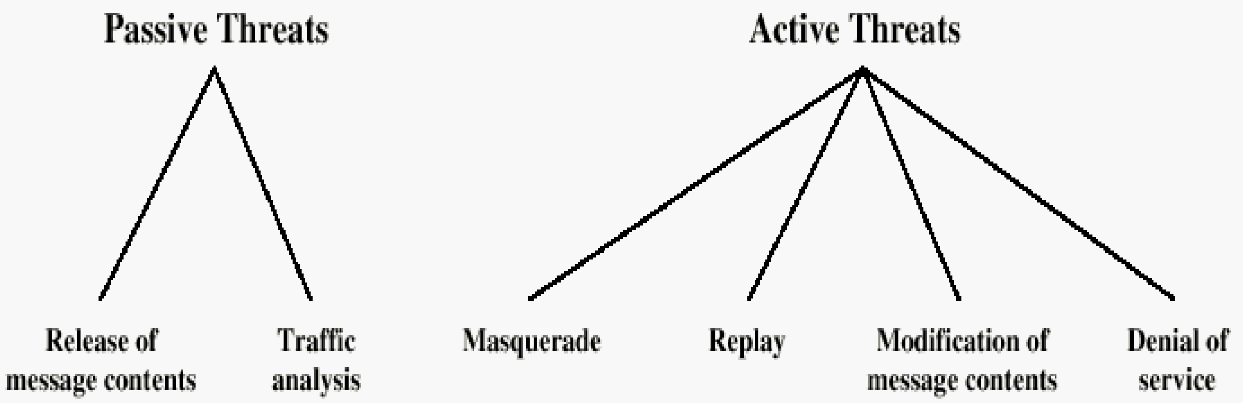


Figure 1.2 Active and Passive Security Threats

1. Active attacks:

- If there is change being made to system then the attack is called as Active attack.

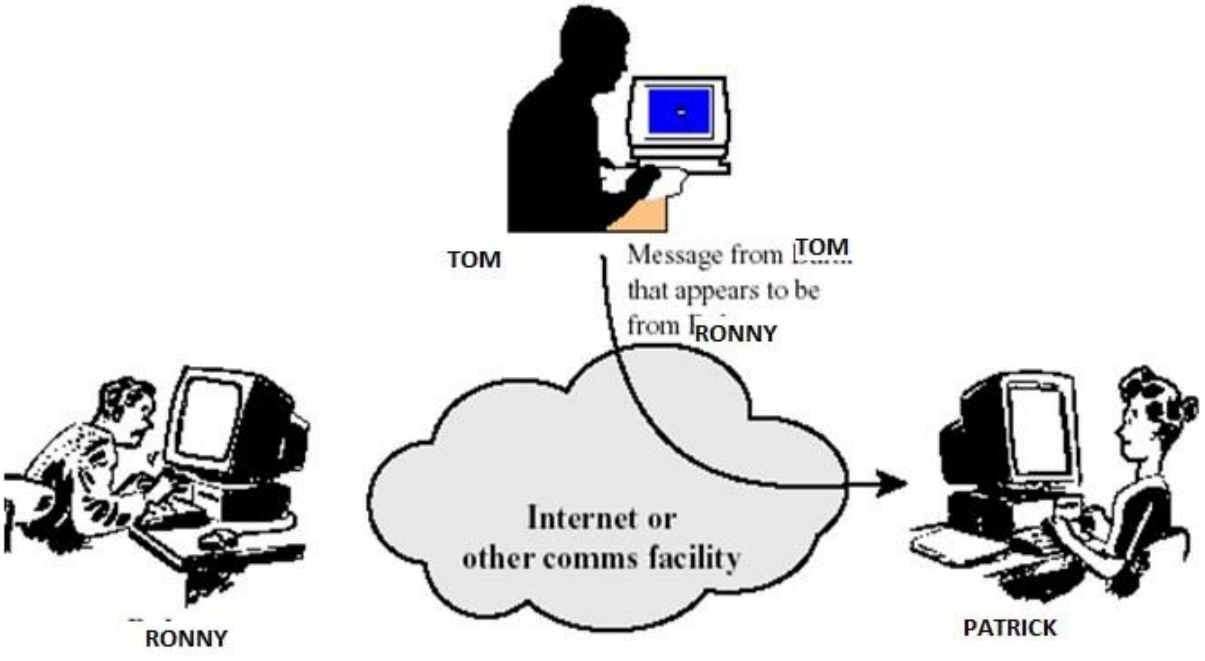
- Active attacks are actually attacks on Integrity and Availability

-Active attacks are normally easier to detect than to prevent , because an attacker can launch them in various variety of ways .

-some of the active attacks are: Masquerading, Reply , Modifications on message contents, Denial of services (DOS).

➢ <u>Masquerading:</u>

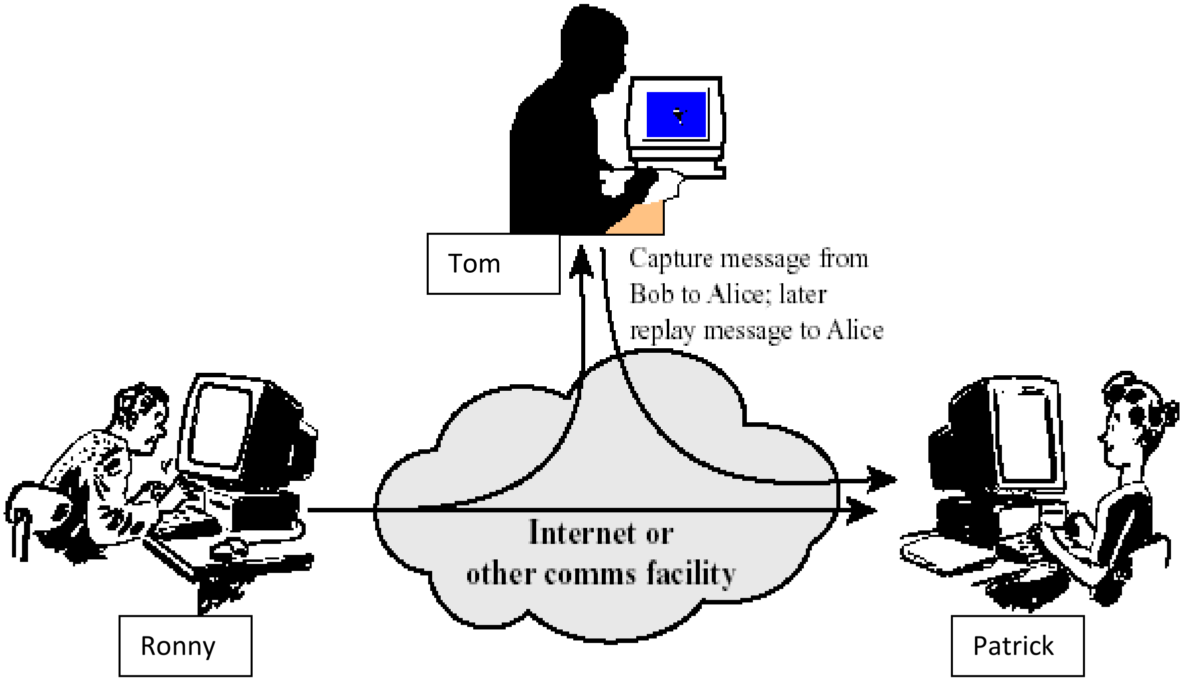
- In Masquerading, an entity is pretends to be some other entity .in other words entity always hides its own identity.
- In Fig below Patrick is receiving message from Tom pretending that he is Ronny



(a) Masquerade

- <u>Reply:</u>

- Involves capture of a data unit and its retransmission to produce an unauthorized effect.
- The fig below shows simple reply attack where Tom captures message from Ronny and sends a reply on behalf of Ronny to Patrick.



(b) Replay

-

- ➢ <u>Modification of message contents :</u>
- In Modification, attacker may modify the content and make it beneficial for himself.
- Modification can be changing the values in particular database, altering the program execution flow, creating virus codes and appending it into program etc.

- ➢ <u>Denial of the Service (DOS) :</u>
- This is attack on resources which is made available to host by server .it is common attack.
- This attack may slow down or totally stops the system's service.

2. Passive attacks:

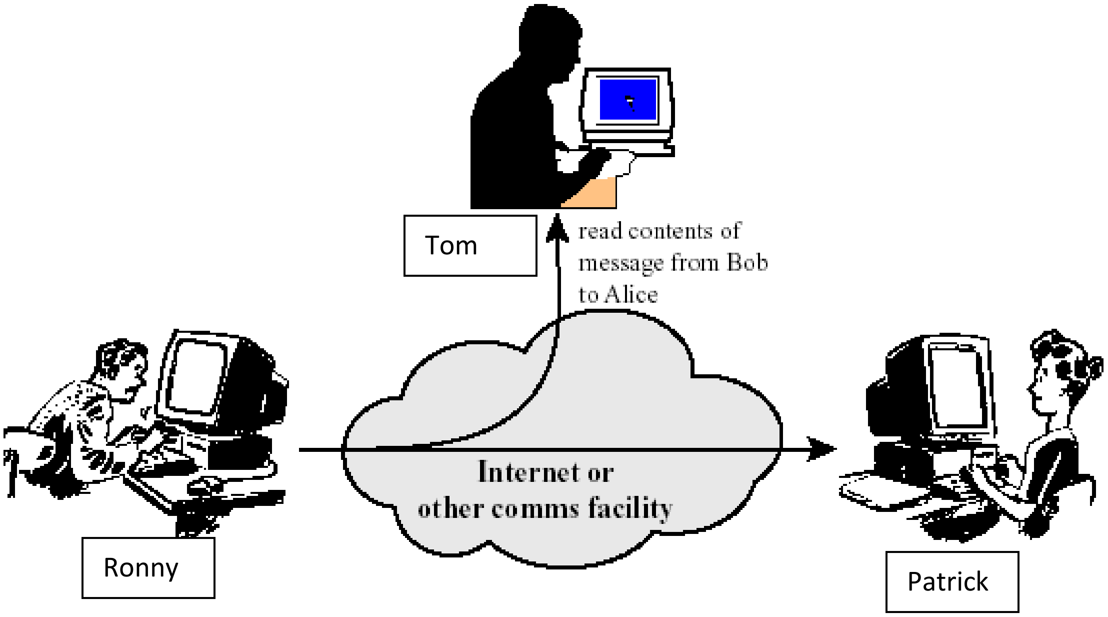
- In passive attack, there are no changes made in the system by an attacker. The attacker is interested in obtaining information.

- Passive attacks are harmless and difficult to trace.

- Some of the passive attacks are release of message contents, snooping etc

➢ <u>Release of message contents :</u>

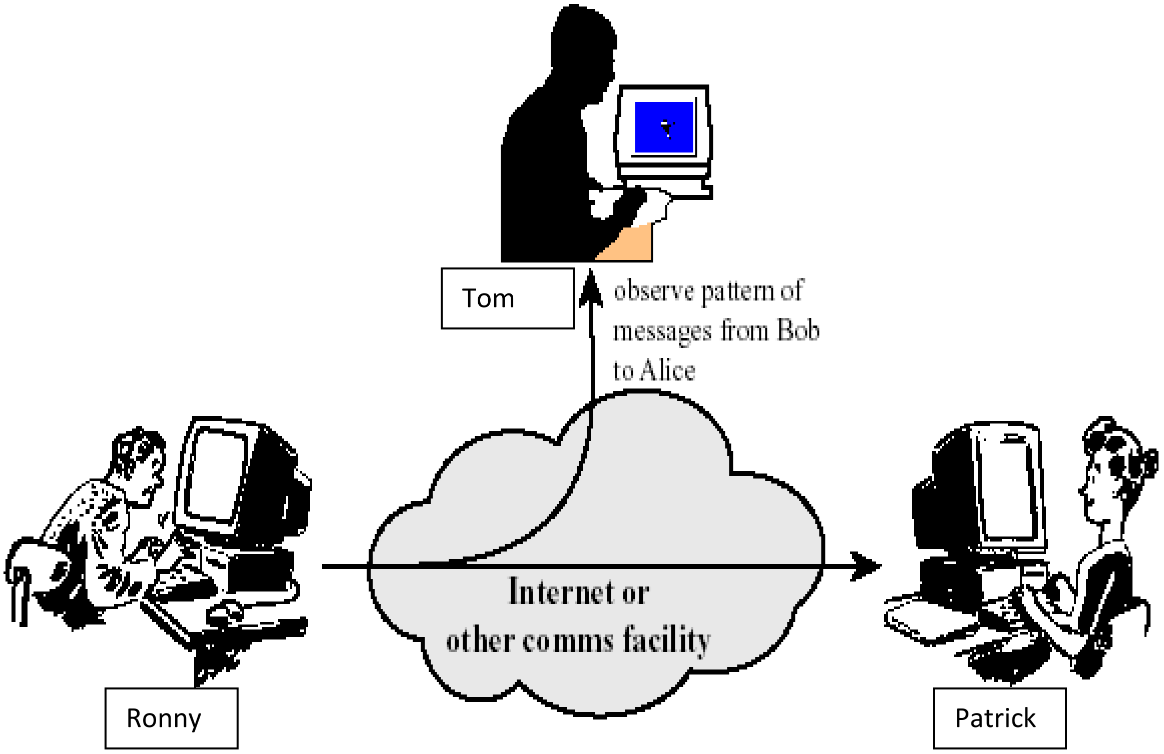
- This attack is also known as interception where data is observed by attacker.
- Some unauthorized system has gained access to an asset.
- The unauthorized party can be a person, program or any computing device.
- However Interception is very difficult to trace as silent interceptor leaves no traces while intercepting the data.


Tom
read contents of message from Bob to Alice
Internet or other comms facility
Ronny
Patrick

(a) Release of message contents

➢ <u>Traffic analysis :</u>

- This attack is somewhat similar to interception; the only difference is attacker may observe some patterns of sender.
- The pattern may observe by an attacker so that, next time he can spoof the receiver or capture some physical address of an sender. (ARP spoofing)
- the pattern of request and response is observed by an attacker so that nature of sender and receiver can be identified .


Tom
observe pattern of messages from Bob to Alice
Internet or other comms facility
Ronny
Patrick

(b) Traffic analysis

3. Difference between Active and Passive attacks:

Active Attacks	**Passive Attacks**
1.In active attacks, system can be changed	1. No changes being made in the system.
2. attacker's goal is to either modify or delete the data from communication channel	2. Attacker's goal is to just obtain information or observe the message pattern.
3. Active attacks are easy to detect.	3. Passive attacks are difficult to trace as compared to active attacks.
4. Active attacks are generally threatening on Confidentiality.	4. Passive attacks are generally threatening on Integrity and Availability .
5. Example : Modification, replying, masquerading	5. Example : Snooping, traffic-analysis

1.3.4 Method of defense – Control:

- Control is an **action, device, procedure or technique** that removes or reduces vulnerability. Using Methods of defense the vulnerability in the system can be either removed or reduced in some way.

- There are few standard control techniques are :

1. Hardware control

2. Physical control

3. Software control

4. Encryption

1. Hardware control:

- In order to prevent the attacks, hardware is developed to provide computer security.
- These devices established between two network (secure or insecure) and can observe incoming and outgoing traffic (Intrusion Detection System). Some hardware may block the malicious data (For e.g. Firewall).some hardware may check the authenticity of user (ATM card)
- The devices are: Intrusion Detection System (IDS), Firewall, ATM card, smartcard implementation of encryption etc.

2. Physical Control:

- The control which is very easiest and least expensive in nature are the Physical control.

- we always say “precautions are always better than cure” therefore instead of waiting for the attack to happen we should physically protect the data .

- For example –

✓ to prevent from unauthorized access our PC should be password protected and also password should not be remembered.

✓ We can also store the backup files or data in case of loss.

✓ our PC should be free from virus therefore antivirus must be installed on our PC.

- Physical controls are in our hand we can easily protect ourselves by an attacker.

3. Software Control:

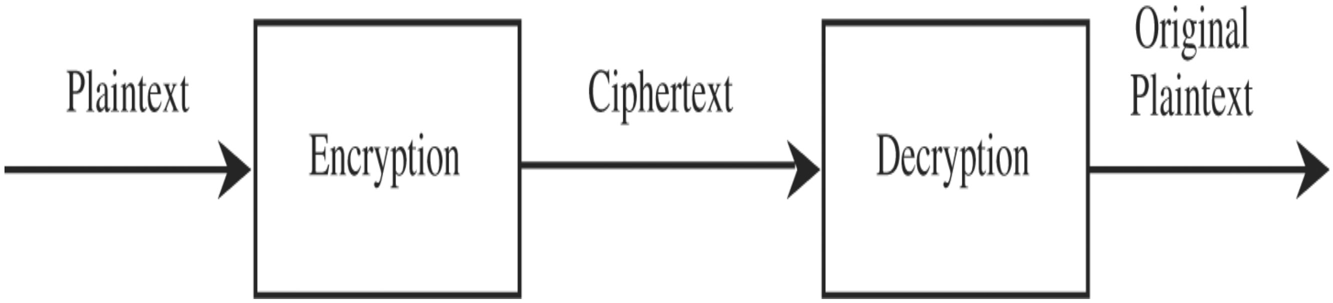
- Software is composed of many programs. Where Program is composed of Code and data (code +data = program). The attacker may change anything in the program may lead in failure of that software.

- The program controls should be managed in such a way that there should be least probability of modification. Even if modification occurs it should be easily detected.

- The program that controls operating and network system should be confidential enough such that no one can change program control using reverse engineering techniques.

4. Encryption:

- **Encryption** is nothing but transforming the data into some other form so that the data become meaningless for user.
- One of the best way to fool an attacker is to create some confusion in data or to purposely scramble the data so that interpretation of such data is almost meaningless without intruders knowing how the transformation was done.
- Encryption always provide Confidentiality as original data is converted into some other form so that attacker will not get hint easily .
- Additionally it also preserve integrity; data cannot be read and cannot be changed.
- The data before transformation is called as ‘Plain text’ where data after transformation called as Cipher text.
- There are various transformation techniques available (symmetric key, RSA) . the study of all these transformations is nothing but “Cryptography”.
- Weak encryption is similar to no encryption because it may give false results.



1.4 Computer Criminals:

```
Expected Question:

What are the types of attacker in security?
```

- Computer Criminals are human being who purposely wants to destroy the security systems. They may have illegal access to software, data or hardware.
- Computer criminals are of four types: Amateurs, Crackers, Career Criminals and Terrorists.

➢ **Amateurs**

These are the people who only observe the weakness in our system. Amateur's not necessarily bad people, they can be software developers also who observe vulnerability in their own software so that in future their software will be free from malicious attacks.

➢ **Crackers**

These people are high-school or university students who have knowledge about security mechanisms. In other word all engineering student can be in this category.

Let's take an example of my normal practical batch of Operating system! . As face book is strictly blocked by college firewall, I was using some proxy sites to unblock face book site. I was using it for entire practical session without knowing the subject teacher or LAB assistant!

If my subject teacher is reading this book, He might throw me out of class! Anyways, Jokes apart! The point is I am cracker at this point who doesn't cause much harm.

➢ **Career criminals**

These people are dangerous who understand targets of computer crime. They begin as computer professionals who engage in their crime, finding the prospects and pays off good.

➢ **Terrorists**

These are the person who breaks security mechanisms in following ways.

1. *Target of attack:* web - site attacks and Denial of Service attack are popularly used for any political organizations because they want to bring undesired negative attention.

2. *Propaganda vehicles:* Using web-logs, email-lists are used to get message to many people.

3. *Methods of attack:* To launch offensive attacks requires use of computers.

1.5 Security Services and Mechanisms:

[This topic is only for Computer Engineering Students]

```
Expected question:

What are the security services and mechanisms?
```

- *The International Union-Telecommunication Standardization Sector (ITU-I)* defines the framework for the architecture (Services) and dimensions **(Mechanisms)** in achieving end-to-end security of distributed applications.

- The general principles and definitions apply to all applications, even though details such as threats and vulnerabilities and the measures to counter or prevent them vary based on the needs of an application.

-The security architecture is defined in terms of two major concepts, layers and planes. Security layers address requirements that are applicable to the network elements and systems that constitute the end-to-end network.

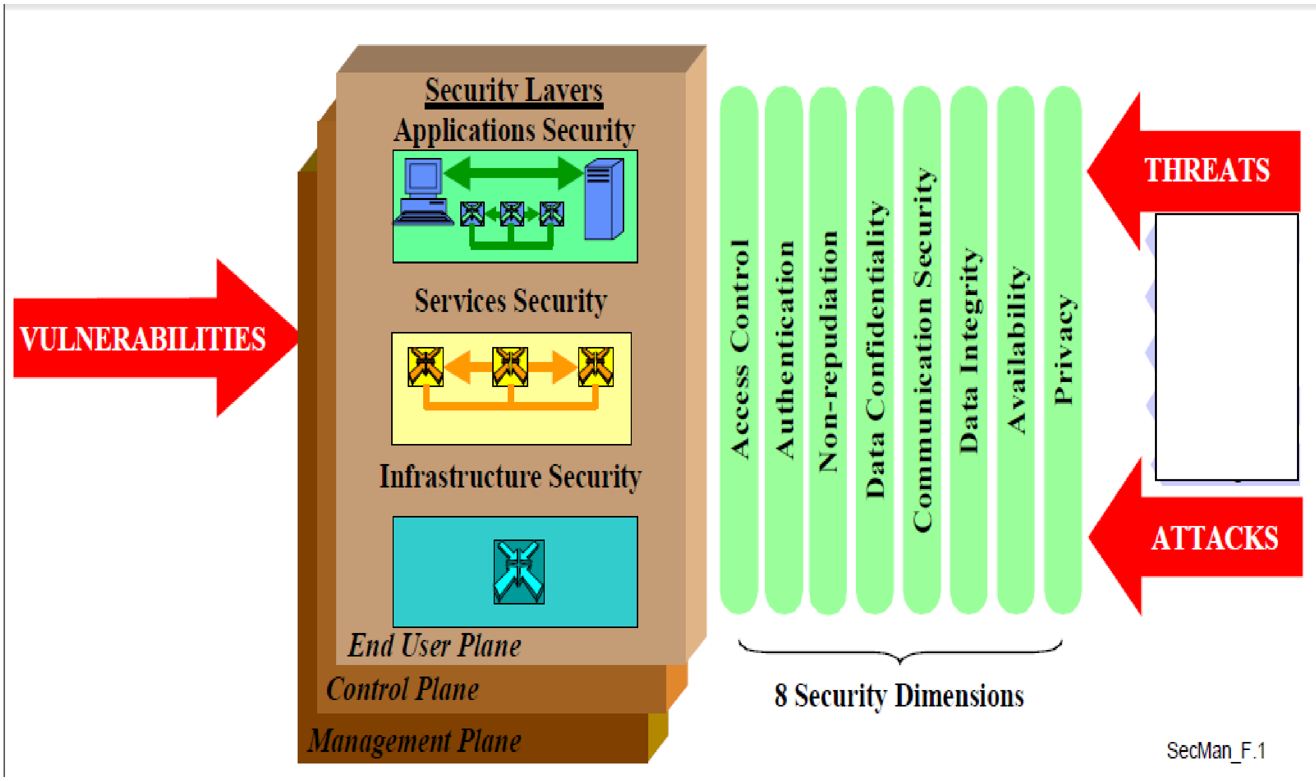
-One of the advantages of defining the layers is to allow for reuse across different applications in providing end-to-end security.

- The vulnerabilities at each layer are different and thus counter measures are to be defined to meet the needs of each layer. The Infrastructure layer consists of the network transmission facilities as well as individual network Elements.

- Examples of components that belong to the Infrastructure layer are individual routers, switches and servers as well as the communication links between them.

- The Services layer addresses security of network services that are offered to customers. These services range from basic connectivity offerings such as leased line services to value added services such as instant messaging.

- The application layer addresses requirements of the network-based applications used by the customers.



- The second axis of the framework addresses the security of activities performed_in a network.
- The security framework defines three Security Planes to represent the three types of protected activities that take place on a network.
- The Security Planes are: (1) the Management plane, (2) the Control plane, and (3) the End-User plane.
- These Security Planes address specific security needs associated with network management activities, network control or signaling activities, and end-user activities.
- The management plane is concerned with Operations, Administration, Maintenance & Provisioning (OAM&P) activities.
- The control plane is associated with the signaling aspects for setting up (and modifying) the end-to-end communication through the network irrespective of the medium and technology used in the network.
- The end-user plane addresses security of access and use of the network by customers. This plane also deals with protecting end-user data flows.

1.5.1 Security Dimensions (Services)

- **Data Confidentiality** :

The concept of privacy is a fundamental motivation for security. Privacy is associated with certain technical means (e.g. cryptography) to ensure that this information is not disclosed to anyone other than the intended parties, so that only the explicitly authorized parties can interpret the content exchanged among them.

- **Authentication :**

Authentication is the provision of proof that the claimed identity of an entity is true. Entities here include not only human users but also devices, services and applications. Authentication also provides for assurance that an entity is not attempting a masquerade or an unauthorized replay of a previous communication.

There are two kinds of authentication: data origin authentication (i.e. authentication requested in a connection-oriented association) and peer entity authentication (i.e. authentication in a connectionless association).

- **Integrity :**

Data integrity is the property that data have not been altered in an unauthorized manner. By extension, data integrity also ensures that information is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities.

- **Non-Repudiation:**

Non-repudiation is the ability to prevent users from denying later that they performed an action. These actions include content creation, origination, receipt, and delivery, such as sending or receiving messages, establishing or receiving calls, participating in audio and video conferences, etc.

- **Access Control**

The *Access Control* security dimension protects against unauthorized use of network resources. Access Control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications.

- **Availability :**

The principle of availability states that data or resources should be available to authorized parties at all times. In other words data or resources should reach to receiver as it is.

1.5.2 Security Mechanisms

To implement all these services, we have certain techniques which ensure security of Data, Information and System. Some of the techniques are widely used are mentioned below .

1. **Encipherment :**

- In Encipherment data Confidentiality is achieved so that any unauthorized user should not gain the access on an asset. For E.g., Cryptography and Stenography.
- In Cryptography cipher is the algorithm which performs encryption or decryption -a series of well-defined steps that can be followed as a procedure.
- Stenography, now a days are widely used in order to provide Encipherment .

(Please note: Stenography is the art and science of writing hidden messages in an image such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.)

2. **Digital Signature :**

- A **digital signature** or **digital signature scheme** is a mathematical scheme for demonstrating the authenticity of a digital message or document.
- A valid digital signature gives a recipient reason to believe that the message was created by a known sender such that they cannot deny sending it (authentication and non-repudiation) and that the message was not altered in transit (integrity).
- Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

3. **Authentication**

- Authentication is the process of proving identity of one party to another.
- The party which proves its identity is called as “claimant” where the party which accepts/rejects the identity is called as verifier.
- Claimant and verifier may be person, machine or any other security program in a network. Once the party is authenticated , it will be allowed to access the recourses available on the system .
- Password techniques or Biometrics (retina scan , fingerprint scan) are the example of authentication .

4. **Traffic padding :**

- This is a security mechanism which inserts or appends bits of information inside the gaps between streams or chucks of data making harder to the attacker to perform a traffic analysis.

- Traffic padding is implemented in order to create confusion for an attacker in case of traffic analysis. (Even if attacker observing the traffic between two host , due to addition of some dummy data he cannot identify what the exact information is .)

5. Routing Control :

- Routing control is switching routing path continuously in order to avoid attacks like eavesdropping on particular routing path.
- A routing control mechanism is composed of hardware and software, which monitors all the outgoing traffic through its connection with the Internet service providers (ISPs), and helps in selecting the best path for efficient delivery of the data.
- The switching is performed when the routing control calculates the performance and security of all the ISPs and selects only those that have performed optimally in these areas.

6. Data Integrity :

- Verify that the data received is the same as the data being send and assure that it was not modified by an unauthorized entity.

7. Access Control :

- Security mechanisms that provide a way to enforce access right to resources.
- For example, in Linux, every file, folder, and/or resource have three set of permissions. These permissions indicate who have the right to read, write, and/or execute a specific file, folder, and/or resource.

1.6 About This Book :

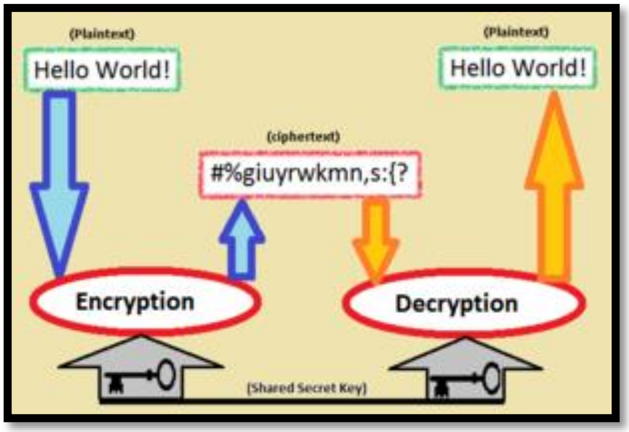
As stated earlier, Security in the system becomes an important issue in corporate industry. We have already wasted a lot of time to learn what exact “Security” means. Let’s review some fundamental implementations of security parameters that can help to protect the data as well as information.

In fact the goal of any developer or programmer is to achieve top level security mechanism in his system. However, no one in the world can provide guarantee that my system is 100% secure. Someone said - “Attackers are always smarter than programmers.”

There are 4 more modules we will study as a part of our syllabus. Let’s have an idea in brief.

- **CRYPTOGRAPHY (MODULE 2) :**

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. The original data is encoded in some form and then transmitted towards receiver. The purpose of encryption is to provide data confidentiality so that attacker, even if gets the message –he cannot understand what it means. At receiver side the entire message is decoded to original message.



Cryptography is rooted in mathematics: groups and field theory, computational complexity and even real analysis, not to mention probability and statistics. With this, there is something called as “Symmetric Key Cryptography” and “Public Key Cryptography”. The entire chapter plays around these two techniques. We will also learn some cryptographic algorithms like RSA, AES, DES etc. The chapter might be difficult if you mug up the concepts therefore I will personally suggest you to understand the concepts and algorithms so that in examination you can write the answers in own words.

- **AUTHENTICATION AND AUTHORIZATION (MODULE 3):**

Computer security authentication means verifying the identity of a user logging onto a network. Passwords, digital certificates, smart cards and biometrics can be used to prove the identity of the user to the network. Computer security authentication includes verifying message integrity, e-mail authentication and MAC (Message Authentication Code), checking the integrity of a transmitted message. There are human authentication, challenge-response authentication, password, digital signature and biometrics. In simple words, authentication is proving the identity of one party to server or some other party (claimant and verifier).

Authorization is the function of specifying access rights to resources, which is related to information security and computer security in general and to controlling particular. More formally, "to authorize" is to define access policy. For example, human resources staff are normally authorized to access employee records, and this policy is usually formalized as access control rules in a computer system. During operation, the system uses the access control rules to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected). Resources include individual files' or items' data, computer programs, computer devices and functionality provided by computer applications.

Examination point of view this chapter is simple and important. I suggest not to leave a single topic from this chapter.

- **SOFTWARE SECURITY (MODULE 4):**

What makes it so easy for attackers to target software is the virtually guaranteed presence of vulnerabilities, which can be exploited to violate one or more of the software's security properties. Most successful attacks result from targeting and exploiting known, non-patched software vulnerabilities and insecure software configurations, many of which are introduced during design and code.

In this chapter we will learn various types of malicious/non-malicious codes, types of software attacks, the critical conditions in code (like buffer overflow) .we will also learn Digital Rights Management which provides remote control to distributed contents.

Anyways let us not go into its detail. You might feel this chapter is boring but again like chapter 3 it is scoring. The typical questions are asked in examination so that you can prepare well.

- **NETWORK SECURITY (MODULE 5) :**

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources .

In this chapter we will learn all Network threat, Network security mechanisms (Like IDS , firewall),study of secure communication channels (like IPSec),Honeypots, Firewalls etc.. We are going to see the attacks possible on resources which is made available to client (called as Denial of Service attacks)

Well, it is second largest MODULE in this subject. The chapter is simple if you understand the concepts. In VIVA also, more focus of external will be this chapter only.