Chapter:1 Introduction and Security Threats

1. Computer network security consists of measures taken by some organizations or bu siness to monitor and prevent unauthorized access from the outside attackers/hack ers .
2. Different approaches to computer network security management have different req uirements depending on the size of the computer network. For example, a home off ice requires basic network security while large businesses require high maintenance to prevent the network from malicious attacks.
3. There are numerous perspectives that make up organize security – the main components are prevention, protection and security. The ultimate goal of network security is to create a connected network that protects against illegal/abno rmal activity while simultaneously allowing you to perform the activities you need t o.

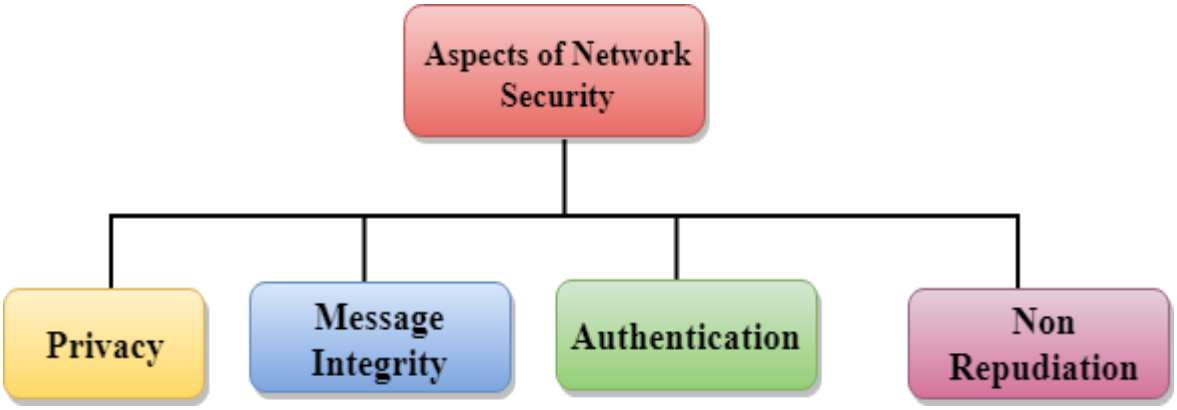

Fig 1[1]google

1. **Privacy:** Privacy implies both the sender and the receiver expects confidentiality. The transmitted message ought to be sent uniquely to the planned receiver whi le the message ought to be misty for different clients.

2. **Message Integrity:** Data integrity means that the data must arrive at the receive r exactly as it was sent. There must be no changes in the data/message content during transmission, either maliciously or accident, in a transit.

3. **authentication:** Authentication means that the receiver is sure of the sender id entity, i.e., no unauthorised person has sent the message

4. **Non-Repudiation:** Non-
   Repudiation means that the receiver must be able to prove that the received me ssage has come from a specific sender. The sender must not deny sending a mes sage that he or she send.

1.1THREATS TO SECURITY

- Viruses and Worms
- Intruders, Insiders
- Criminal organizations
- Terrorists
- Information warfare

VIRUS

- **Virus** is hidden code that spreads by infecting another program and inserting a copy of itself into that program.
- A virus requires its host program to run before the virus can become active and gen erally requires human interaction to activate.
- Viruses deliver a payload which could contain a simple message or image thus consu ming storage space and memory, and degrading the overall performance of a comp uter, or in the case of a more malicious payload, destroy files, format a hard drive, or cau se other damage.

WORMS:

Worm is similar/like to a virus by design and is considered to be a sub-
class of a virus. Worms spread from computer to computer, but' unlike a virus, it has the c apability to travel without any human action.

INTRUDERS AND INSIDERS

One of the two most publicized threats to security is the intruder (the other is viruses), ofte n referred to as a hacker or cracker.
Intruders can be classified in three Classes:'

1. **Masquerade**r:' An individual who is not authorized to use the computer and who sp ike a system's access controls to exploit a legitimate user's account
2. **Misfeasor:**' A authorized user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his o r her privileges

3. **Clandestine user**:′ An individual who takeover supervisory control of the system and uses this control to suppress audit collection.

INSIDERS

A insider threat to an organization is a current or former employee, or other business partn er who has or had authorized access to an organization's network, system, or data. He is in tentionally exceeded or misused that′ access in a manner that negatively affected the confi dentiality, integrity, or availability of the organization's information or information systems.