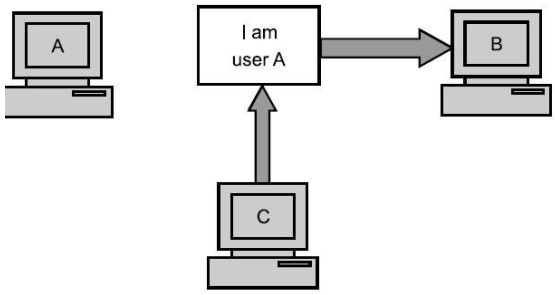
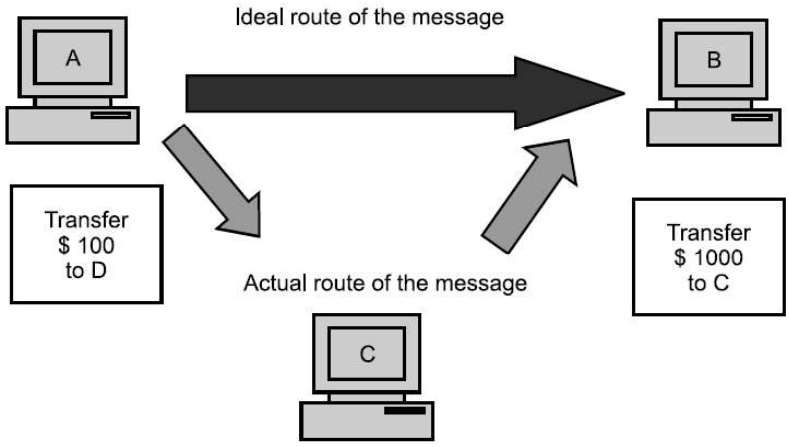
PRINCIPLES OF SECURITY

- Confidentiality
- Integrity
- Authentication
- non-repudiation

- Confidentiality- only the sender and the intended recipient should be able to access the contents of a message. Any user gets access to a message, which is not for that user defeats the purpose of confidentiality.
- Authentication – The authentication process ensures that the origin of an electronic message or document is correctly identified. Fabrication is possible in absence of proper authentication mechanisms.



- **Integrity-** When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, the integrity of the message is lost. This type of attack is called modification.



- **Non-repudiation**- when a user sends a message, and later on refuses that he/she had sent that message. Non-repudiation does not allow the sender of a message to refute the claim of not sending that message.
- **Access Control-** Access control determines who should be able to access what. For instance, we should be able to specify that user A can view the records in a database, but cannot update them. However, user B might be allowed to make updates as well.
- **Availability**-resources (i.e. information) should be available to authorized parties at all times.

Few programs that attack computer systems:

- Malicious software or malware is software that is intentionally included or inserted in a system for a harmful purpose.
- Malicious software can be divided into two categories: those that need a host program, and those that are independent.
- The former are essentially fragments of programs that cannot exist independently of some actual application program, utility, or system program. Viruses, logic bombs, and backdoors are examples. The latter are self-contained programs that can be scheduled and run by the operating system. Worms and zombie programs are examples.

- **Virus-** Avirus is a piece of program code that attaches itself to legitimate program code, and runs when the legitimate program runs. It can then infect other programs in that computer, or programs that are in other computers but on the same network.
- Viruses can also be triggered by specific events
- virus embed itself 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.
- it 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.

WORMS-A worm is a program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.

- Network worm programs use network connections to spread from system to system.
- A virus modifies a program. A worm, however, does not modify a program. Instead, it replicates itself again and again. The replication grows so much that ultimately the computer or the network on which the worm resides, becomes very slow, ultimately coming to a halt.
- A worm does not perform any destructive actions, and instead, only consumes system resources to bring it down.

- **Trojan Horse-**A Trojan horse. is a hidden piece of code, like a virus.
- the main purpose of a virus is to make some sort of modifications to the target computer or network, a Trojan horse attempts to reveal confidential information to an attacker.
- a Trojan horse could silently sit in the code for a Login screen by attaching itself to it. When the user enters the user id and password, the Trojan horse could capture these details, and send this information to the attacker without the knowledge of the user who had entered the id and password.

Attacks

- **Packet/IP Sniffing(snooping)-** An attackersimply observe (i.e. sniff) packets as they pass by. the information that is passing needs to be protected in some ways:
  - (i) The data that is traveling can be encoded in some ways.
  - (ii) The transmission link itself can be encoded.

- **Packet/IP Spoofing-** An attacker sends packets with an incorrect source address. When this happens, the receiver would inadvertently send replies back to this forged address (called spoofed address).
  - The attacker can intercept the reply.
  - The attacker's intention was a Denial Of Service
  - The attacker does not want the reply

Phishing

- The attacker decides to create his/her own Web site, which looks very identical to a real Web site.
- The attacker sends an email to the legitimate customers of the bank.
- This fake email warns the user that there has been some sort of attack on Citibank's computer systems and that the bank wants to issue new passwords to all its customers, or verify their existing PINs, etc. For this purpose, the customer is asked to visit a URL mentioned in the same email.
- When the customer (i.e. the victim) innocently clicks on the URL specified in the email, he/she is taken to the attacker's site, and not the bank's original site.

Denial Of Service (DOS) attack

- attacks make an attempt to prevent legitimate users from accessing some services, which they are eligible for. For instance, an unauthorized user might send too many login requests to a server using random user ids in quick succession, so as to flood the network and deny other legitimate users to use the network facilities.
- A DOS attack can be launched in many ways. The end result is the flooding of a network or change in the configurations of routers on the network.
- It is up to the server to detect that certain packets are from an attacker and not from a legitimate user and take an appropriate action. This is not an easy task. Failing this, the server would fall short of resources (memory, network connections, etc.

Impersonation

Impersonation refers to the act of pretending to be another person for a purpose or fraud. Impersonation attacks are a form of **cyber-attacks** where attackers send emails that attempt to **impersonate** an individual or company for gaining access to sensitive and confidential information.

- It is done in order to gain access to target's sensitive information, such as financial data.

Why are Impersonation Attacks Hard to Detect?

- Users ignorance and lack of attention to detail.

  Look at the email address written twice

  eeryaeel@reveantivirus.com

  eeryaeel@reventivirus.com

  It is hard to figure out the irregularity, especially when you have a hectic schedule at work and many distractions.