Cyber Security.

WHY ARE WE TALKING ABOUT CYBER SECURITY??

Case Studies:

1. ACCUSESD IN RS 400 MILLION SMS SCAM ARRESTED IN MUMBAI.

2. CITY PRINCIPAL SEEKS POLICE HELP TO STOP CYBER CRIME.

3. UTI BANK HOOKED UP IN A PISHING ATTACK.

4. ONLINE CREDIT CARD FRAUD ON E-BAY.

5. INDIAN WEBSITES ARE NEW TARGET OF HACKERS.

6. TAMIL TIGER CREDIT CARD SCAM SPREADS TO CHENNAI, INDIA.

7. TWO BANKS WEBSITE HACKED.

8. ORKUT: THE NEW DANGER.

Cybersecurity is the most concerned matter as cyber threats and attacks are overgrowing.

Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

Gone are the days when passwords were enough to protect the system and its data. We all want to protect our personal and professional data, and thus Cyber Security is what you should know to ensure data protection.

So, lets being with defining the term Cyber Security….

Introduction

Cyber Security is the process and techniques involved in protecting sensitive data, computer systems, networks and software applications from cyber attacks.

Cyber security is the protection of Interconnected System including Hardware, Software and Program or data from cyber attack.

# Cyber Café– Hardware, Software, Internet

To Understand

What is the meaning of the word CYBER

What is the need of Cyber Security

What are the security problems in Cyber field

How to implement and maintain Security of a Cyber field around us.

Meaning of the Word CYBER

- It is a combining form relating to computer system, Network, Program or Data

Need of cyber security

- **Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.**

Major security problems

- Virus
- Hacker
- Malware
- Trojan horses
- Password cracking

Viruses and Worms

- **A Virus is a “program that is loaded onto your computer without your knowledge and runs against your wishes**

Solution

- Install a security suite that protects the computer against threats such as viruses and worms.

Hackers

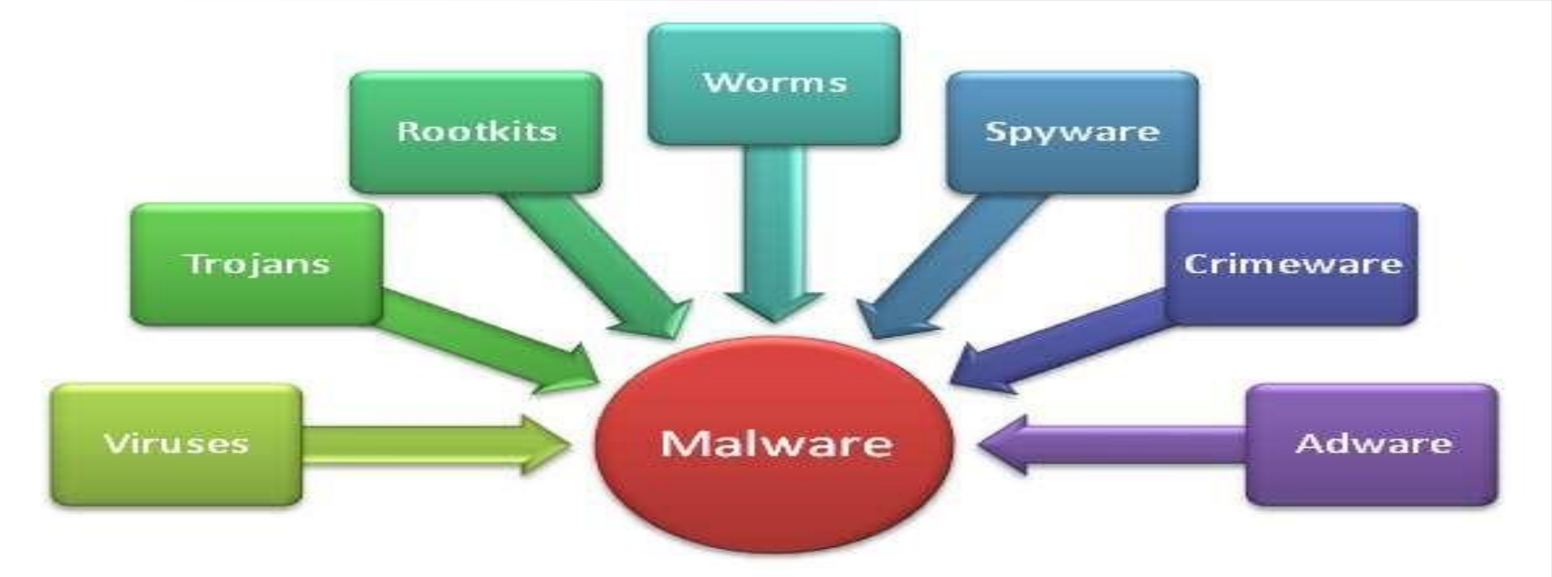
- In common a hacker is a person who breaks into computers, usually by gaining access to administrative controls.

How To prevent hacking

- It may be impossible to prevent computer hacking, however effective security controls including strong passwords, and the use of firewalls can helps.

Malware

- The word "malware" comes from the term "MALicious softWARE."
- Malware is any software that infects and damages a computer system without the owner's knowledge or permission.



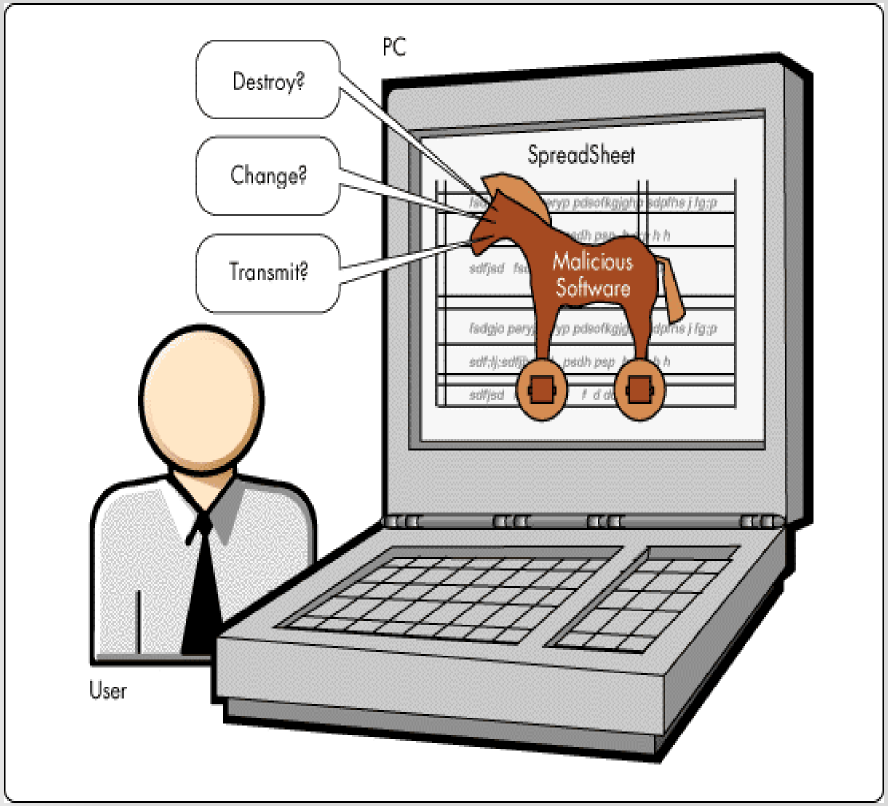
To Stop Malware

- Download an anti-malware program that also helps prevent infections.

- Activate Network Threat Protection, Firewall, Antivirus.

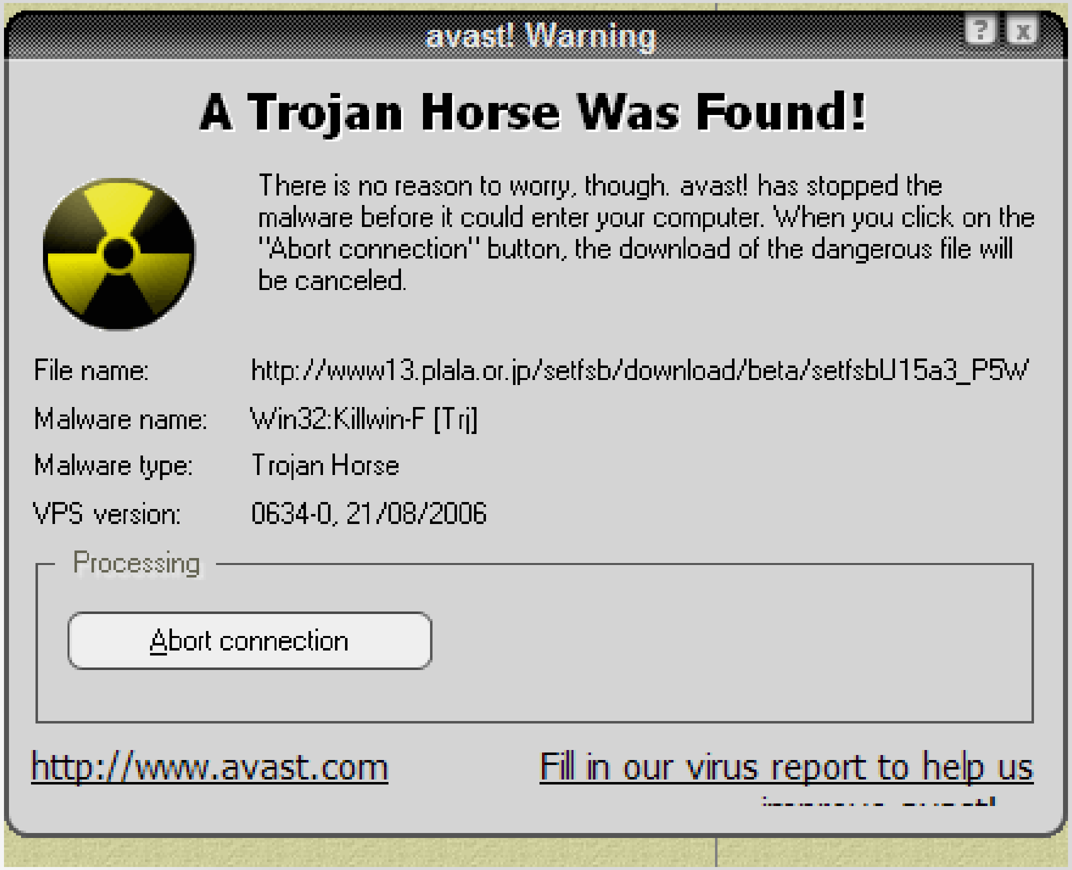
Trojan Horses

- Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.
- These viruses are the most serious threats to computers



How to Avoid Trojans

- Security suites, such as Avast Internet Security, will prevent you from downloading Trojan Horses.



A Trojan Horse Was Found!

There is no reason to worry, though. avast! has stopped the malware before it could enter your computer. When you click on the "Abort connection" button, the download of the dangerous file will be canceled.

File name: http://www13.plala.or.jp/setfsb/download/beta/setfsbU15a3_P5W
Malware name: Win32:Killwin-F [Trj]
Malware type: Trojan Horse
VPS version: 0634-0, 21/08/2006

http://www.avast.com
Fill in our virus report to help us

Password Cracking

- Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.

Securing Password

- Use always Strong password.
- Never use same password for two different sites.

Types of Attacks

- PassiveAttacks
- ActiveAttacks

PASSIVE ATTACKS

Passive Attacks

A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target.

In passive reconnaissance, an intruder monitors systems for vulnerabilities without interaction, through methods like session capture. In active reconnaissance, the intruder engages with the target system through methods like port scans.

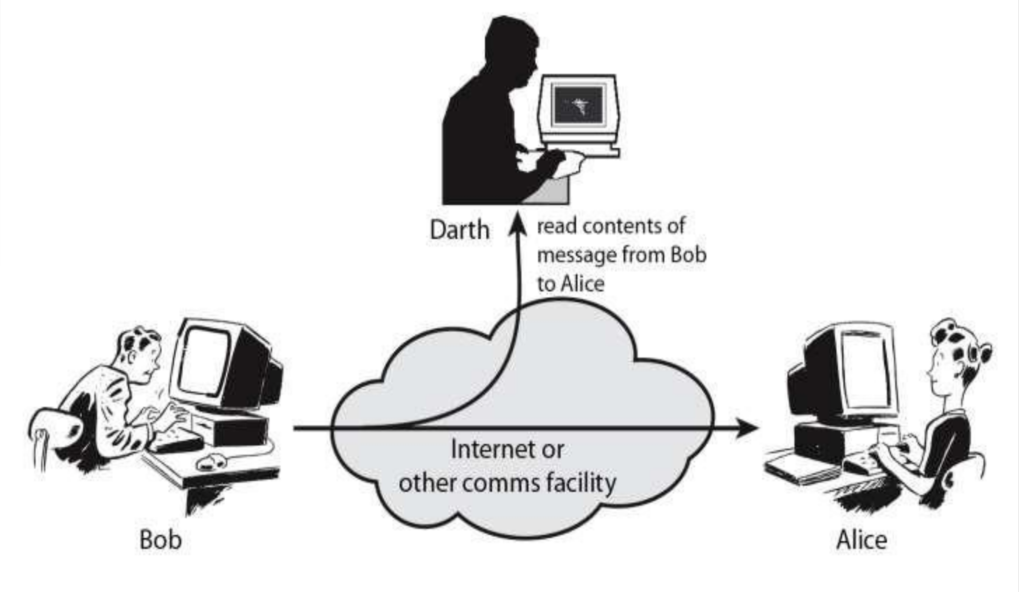
Types of Passive Attacks

- Interception Attack
- Traffic AnalysisAttack

Interception

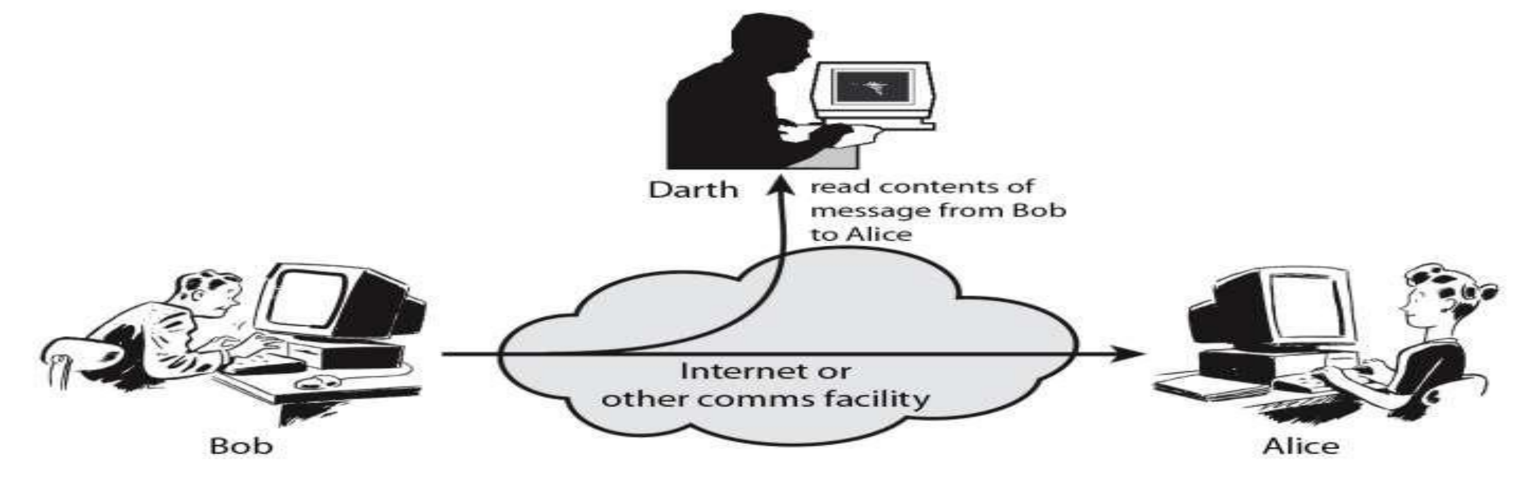
The phenomenon of confidentiality plays an important role in this type of attack. The data or message which is sent by the sender is intercepted by an unauthorized individual where the message will be changed to the different form or it will be used by the individual for his message is lost in this type of attack.

- It is also known as “Release of message contents”.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Traffic Analysis

- Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

ACTIVE ATTACKS

Active Attacks

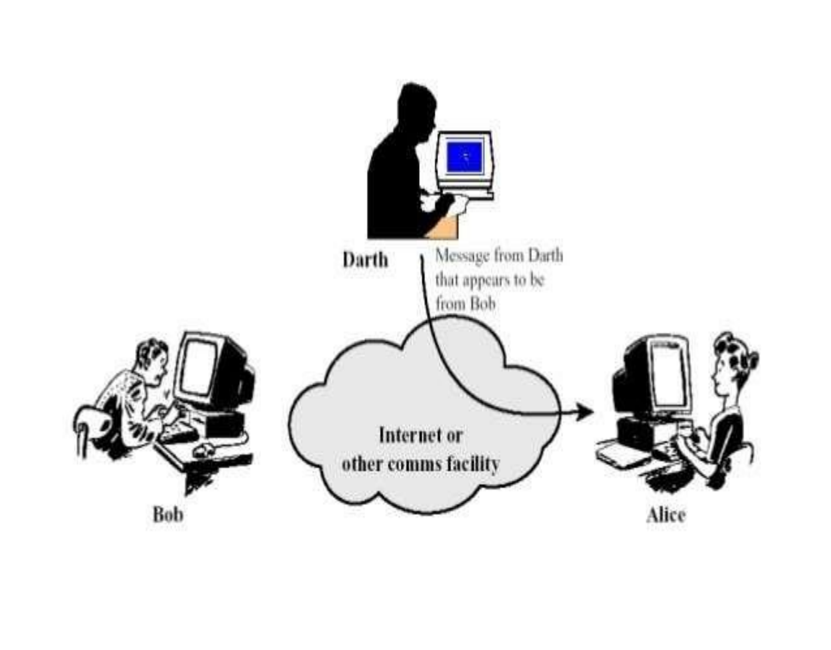
- An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en-route to the target.
- The purpose is to gain information about the target and no data is changed. However, passive attacks are often preparatory activities for active attacks.

Types of Active Attacks

- Masquerade Attack
- Interruption Attack
- Fabrication Attack
- Session Replay Attack
- Modification Attack
- Denial of Service (DOS) Attack

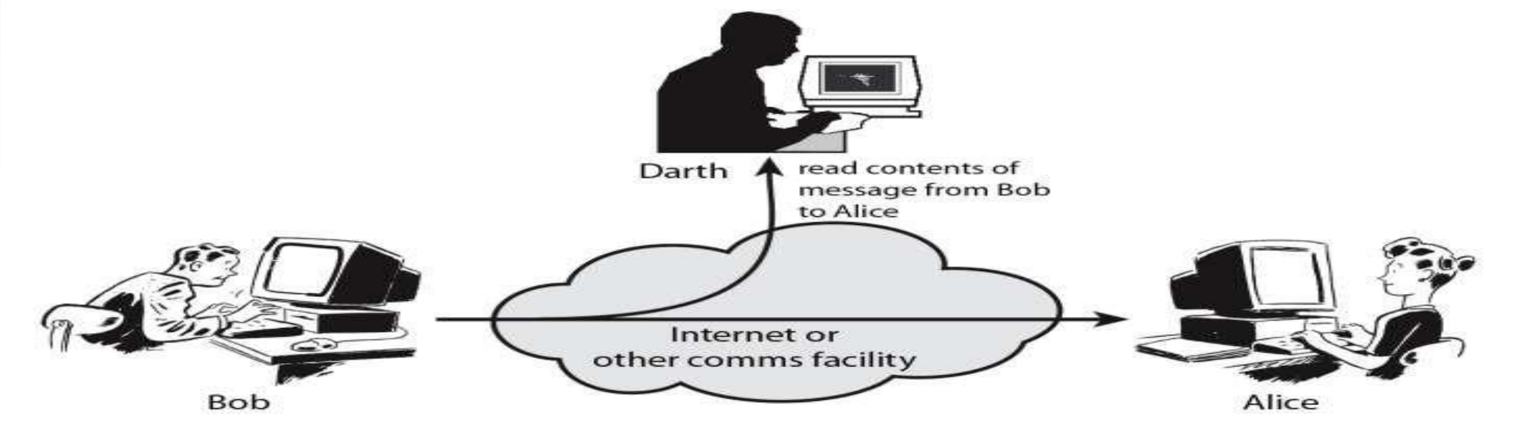
Masquerade

In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

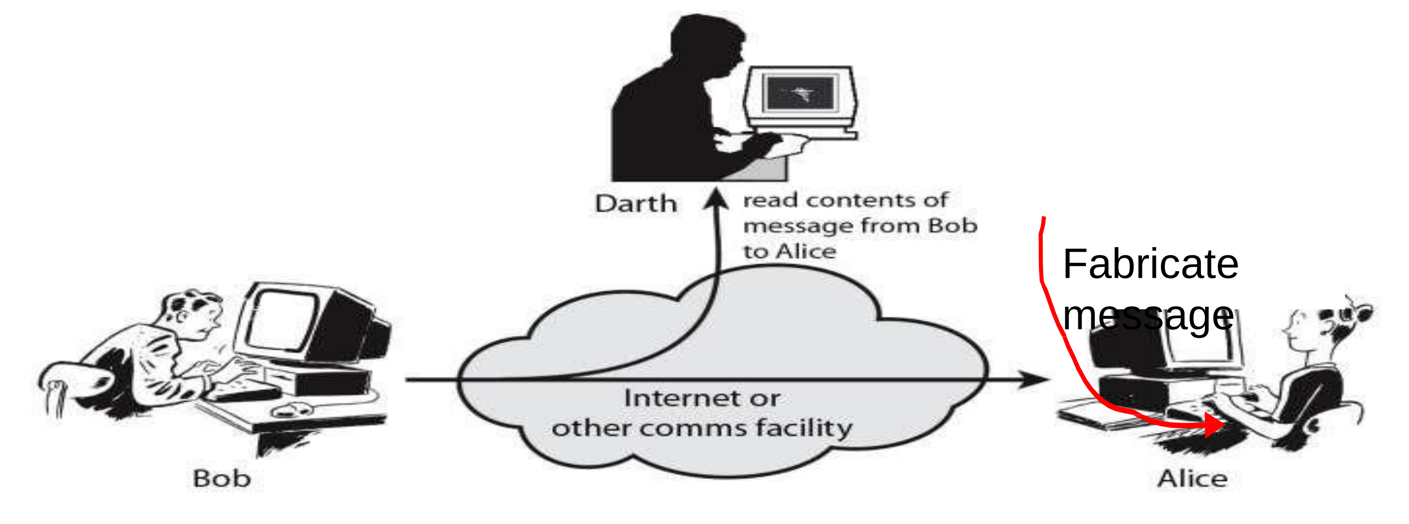
Interruption

This type of attack is due to the obstruction of any kind during the communication process between one or more systems. So the systems which are used become unusable after this attack by the unauthorized users which results in the wastage of systems.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

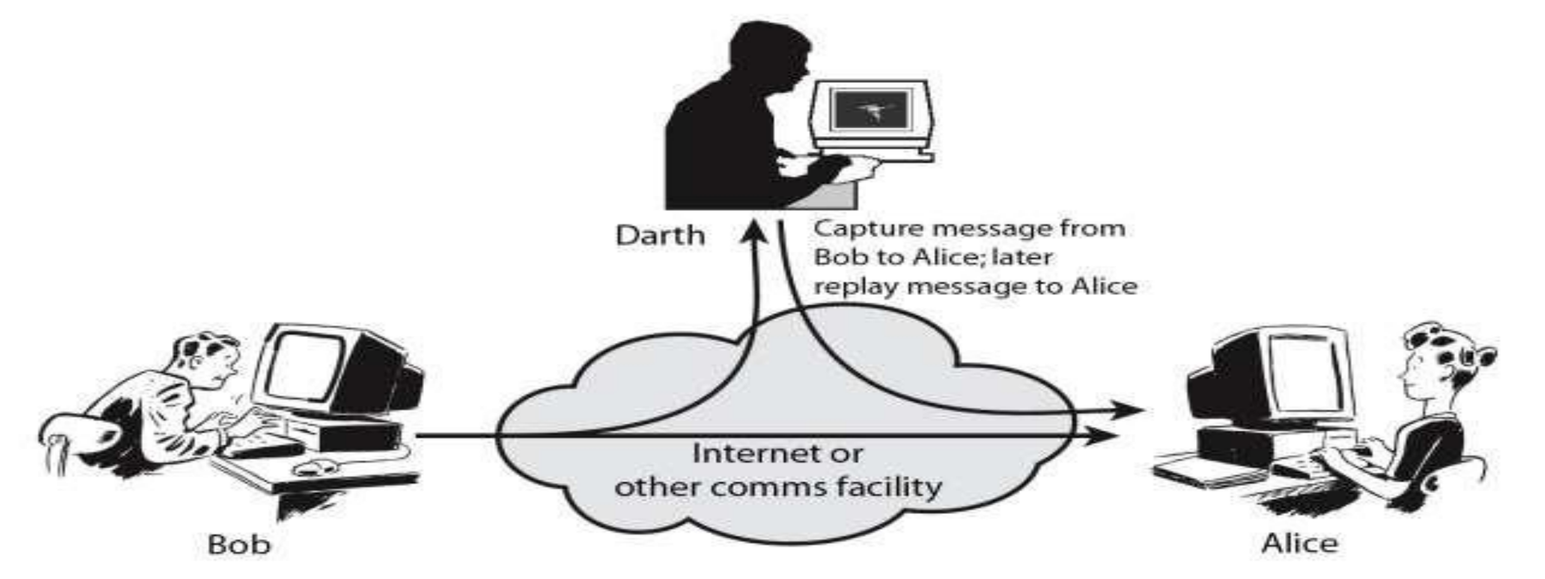
Fabrication

- In this type of attack a fake message is inserted into the network by an unauthorized user as if it is a valid user. This results in the loss of confidentiality, authenticity and integrity of the message.


Darth
read contents of message from Bob to Alice
Fabricate message
Internet or other comms facility
Bob
Alice

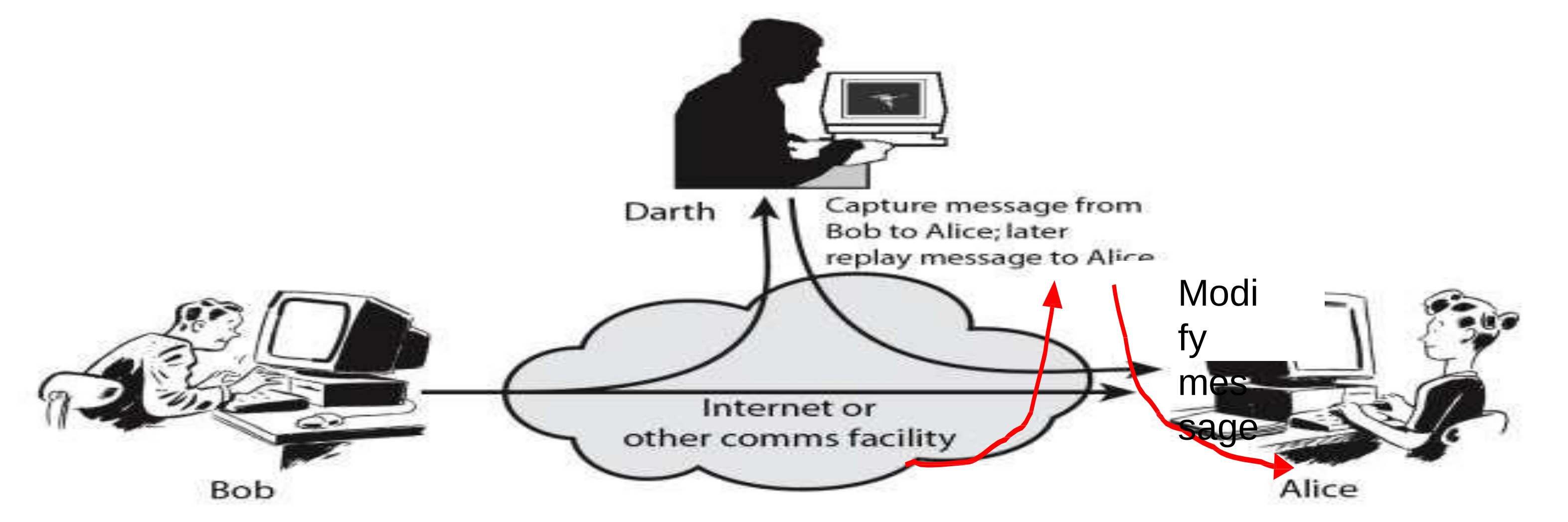
Session Replay

In a session replay attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

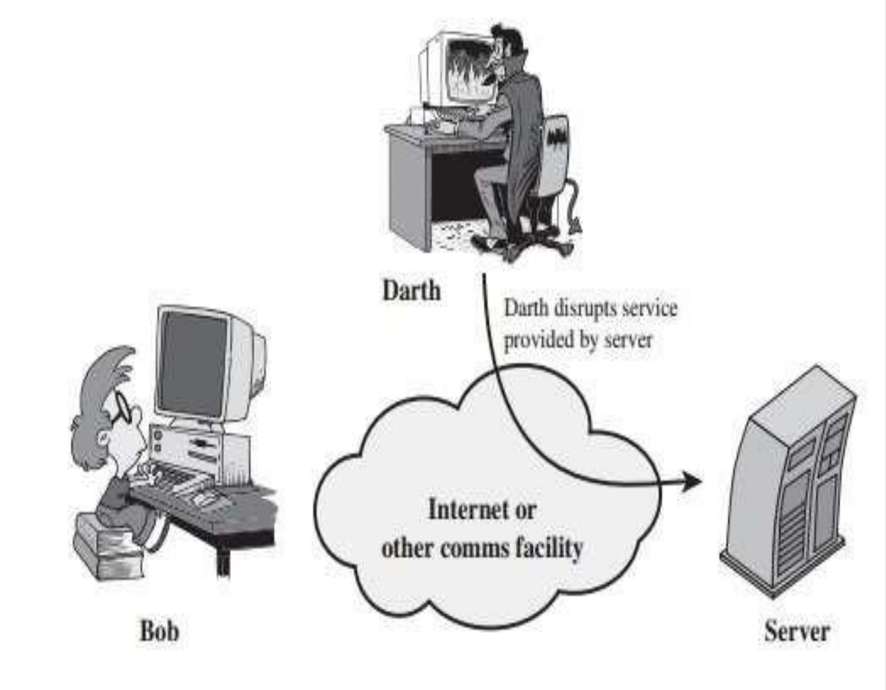
Modification

- In a message modification attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.



Denial of Service (DOS)

In a denial of service (DoS) attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.


Darth
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server

Cyber Security Is Everyone's Responsibility

Cyber Security Strategy – India

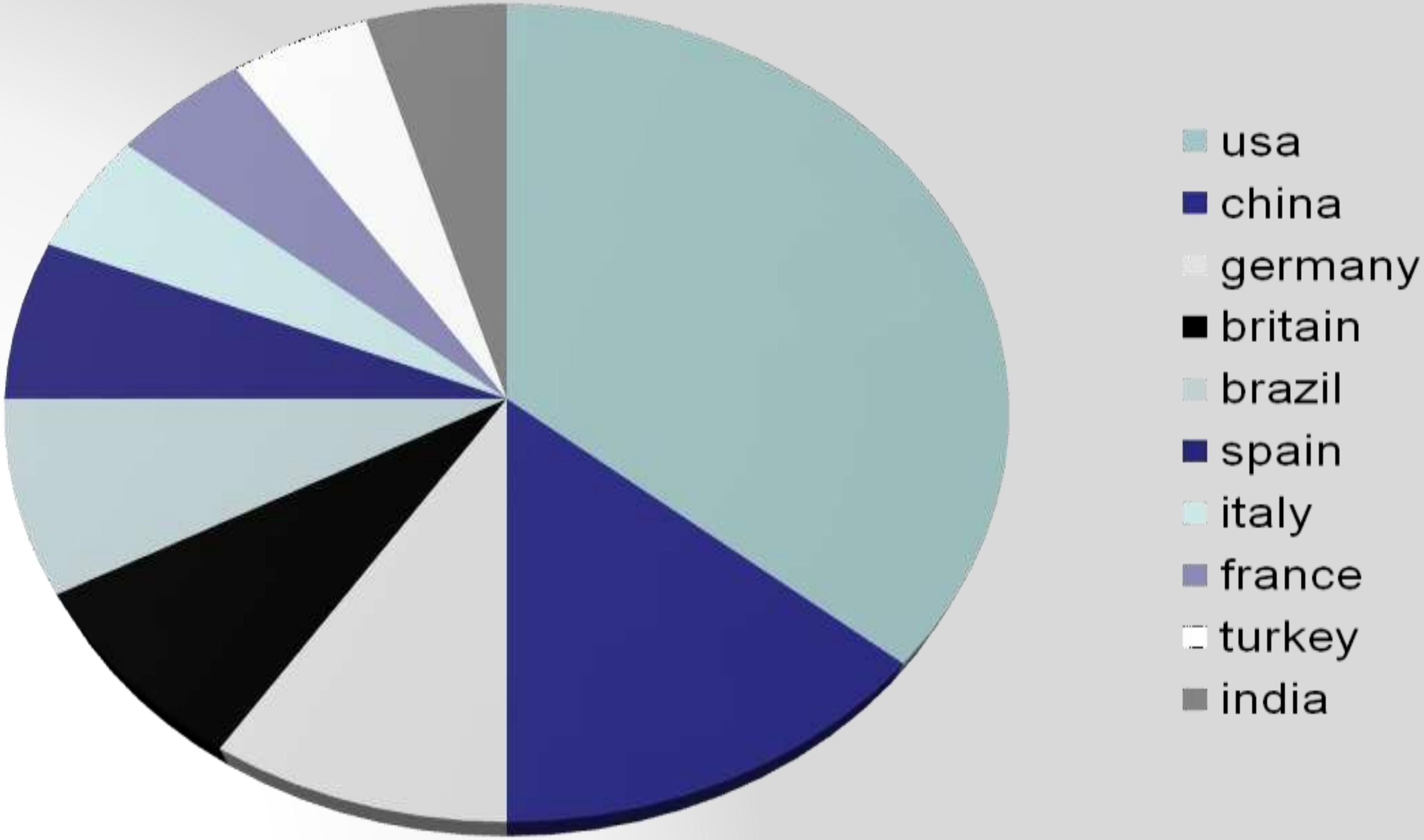
- **Security Policy, Legal Framework**
  - IT Act, 2000
  - IT (Amendment) Bill, 2006 – Data Protection & Computer crimes

- **Capacity building**
  - Skill & Competence development

- **Research and Development**
  - Cyber Monitoring
  - Network Security

- **International Collaboration**

India stands 10th in the cyber crime in the world



Need Of Cyber Security--

1. To Protect Private Data
2. To protect Intellectual Data. (Research, Copyright, Patent Material)
3. To Protect Banking & Financial Data.
4. National Security. (Eg. Russia can attack any country’s defence data.)
5. Global Economy.
6. Protect Sensitive Data. (of any company’s or govt’s data)

History Of Cyber Security--

1969 : Professor of UCLA SENT MSG to standard Research Institute.
(“LOGIN → “LO”)

1970 : Robert Thomas created first Virus Namely “CREPER”
“I AM CREPER CATCH ME IF YOU CAN”

1986 : Russia used Cyber Power as Weapons.

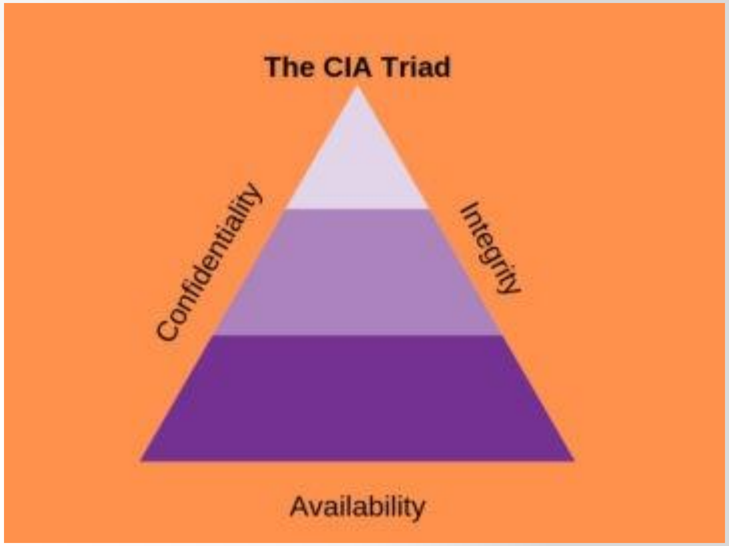
1988 : American Scientists created program to check the size of Internet.

We started understanding the concept of cyber crime and then started working on cyber security.

Principles of Cyber Security --

The Cyber Security on a whole is a very broad term but is based on three fundamental concepts known as “**The CIA Triad**“.

It consists of **Confidentiality, Integrity and Availability**. This model is designed to guide the organization with the policies of Cyber Security in the realm of Information security.



Confidentiality

It defines the rules that limits the access of information. Confidentiality takes on the measures to restrict the sensitive information from being accessed by cyber attackers and hackers.

In an organization, peoples are allowed or denied the access of information according to its category by authorizing the right persons in a department. They are also given proper training about the sharing of information and securing their accounts with strong passwords.

They can change the way data is handled within an organization to ensure data protection. Various ways to ensure confidentiality, like: two-factor authentication, Data encryption, data classification, biometric verification, and security tokens.

INTEGRITY--

This assures that the data is consistent, accurate and trustworthy over its time period. It means that the data within the transit should not be changed, altered, deleted or illegally being accessed.

Proper measures should be taken in an organization to ensure its safety. File permissions and user access control are the measures controlling the data breach. Also, there should be tools and technologies implemented to detect any change or breach in the data. Various Organizations uses a checksum, and even cryptographic checksum to verify the integrity of data.

To cope with data loss or accidental deletion or even cyber attacks, regular backups should be there. Cloud backups are now the most trusted solution for this.

Availability--

Availability in terms of all necessary components like hardware, software, networks, devices and security equipment should all be maintained and upgraded. This will ensure the smooth functioning and access of Data without any disruption. Also providing constant communication between the components through providing enough bandwidth.

It also involves opting for extra security equipment in case of any disaster or bottlenecks. Utilities like firewalls, disaster recovery plans, proxy servers and a proper backup solution should ensure to cope with DOS attacks.

For a successful approach, it should go through multiple layers of security to ensure protection to every constituent of Cyber Security. Particularly involving computers, hardware systems, networks, software programs and the data which are shared among them.

NON- REPUDIATION

To repudiate means to deny. For example, a legal document typically requires witnesses to signing so that the person who signs cannot deny having done so.

After a message has been sent and received, the sender and the receiver should not be able to deny about the sending and receiving of the message, respectively. The receiver should be able to prove that the message has come from the intended sender and not from anyone else. In Addition, the receiver should be able to prove that the received message's contents are the same as sent by the sender.

On the Internet, a digital signature is used not only to ensure that a message or document has been electronically signed by the person , but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature.

Access Control

The term "access" involves writing, reading, executing and modifying. Thus, access control determines and control *who* can access *what*. It regulates which user has access to a resource, under what circumstances the access is possible and which operations the user can perform on that resource.

For Example, we can specify that user A is allowed to only view the records in a database but not to modify that. However, user B is allowed to read as well as update the records.

AUTHENTICATION

Authentication is concerned with determining whom you are communicating with. Authentication is necessary to ensure that the receiver has received the message from the actual sender, and not from the attacker. That is, the receiver should be able to authenticate the sender, which can be achieved by sharing a common secret code word, by sending digital signatures or by the use of digital certificates.