CRYPTOGRAPHY
and
NETWORK SECURITY

PEC-CS801B, UNIT 1

By
CHINMOY GHOSH
Assntt. Professor,
Deptt. Of CSE, JGEC

What is security?

- Security: prevent bad things from happening
  - Confidential information leaked
  - Important information damaged
  - Critical services unavailable
  - Clients not paying for services
  - Money stolen
  - Improper access to physical resources
  - System used to violate law
  - Loss of *value*

A definition of computer security

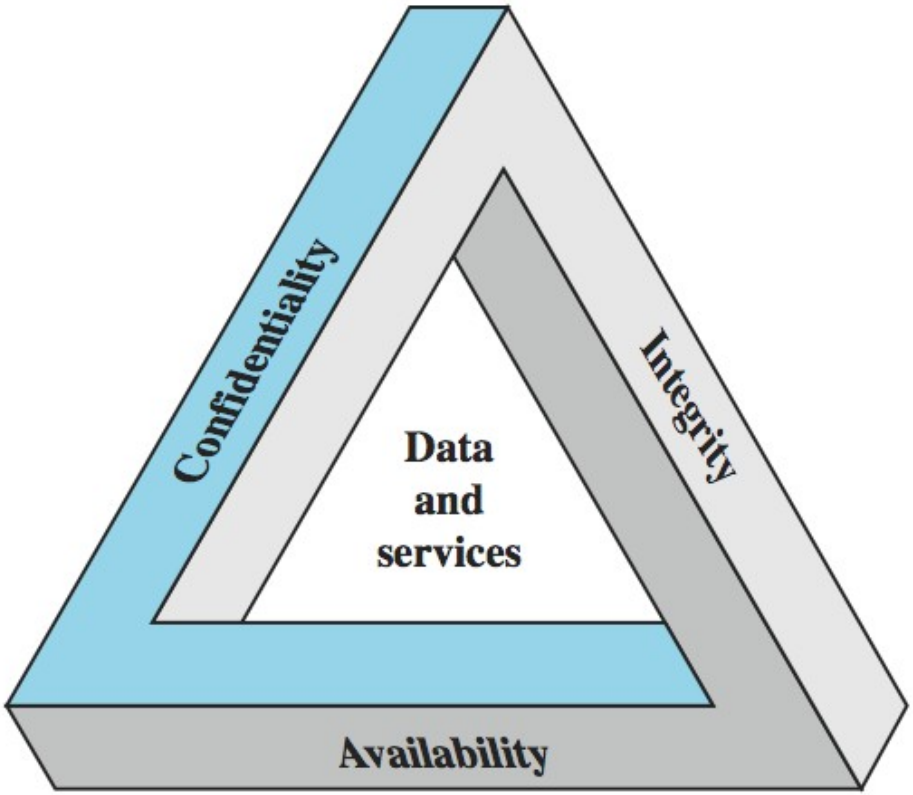
- **Computer security:** The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

Principles of Security (Security Properties)

- Confidentiality
- Integrity
- Availability

- Authenticity
- Non- repudiation

the CIA triad



Confidentiality

- It specifies that only the sender and the intended recipients should be able to receive the data.
- In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes"
- Two aspects of confidentiality
  - Privacy: protection of personal data
    - e.g., personal medical records, student grade information
  - Secrecy: protection of data belonging to an organisation
    - e.g., Formula for a new drug, plans for the company for the next 5 years, Student Records

Integrity

- Specifies No improper modification of data
- Assures that information and programs are changed only in a specified and authorized manner.
- E.g., account balance is updated only by authorized transactions, only you can change your password

Availability

- Specifies that resources (i.e information) should be available to authorized parties at all time.
- Denial of Service is the prevention of authorised access of resources or the delaying of time-critical operations

Authenticity

- Authentication mechanism help establish proof of identities.
- the property of being genuine and being able to be verified and trusted; confident in the validity of a transmission, or a message, or its originator.

Non-repudiation

- Ability to convince a third party that an event occurred (e.g., sales receipt)
- Non-repudiation does not allow the sender of a message to refute the claim of not sending the message.

Attacks

- In *computer* and *computer networks* an **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset
- Attack is a threat that is accrued out
  - Active or passive; from inside or from outside
- Active
  - Interruption (Availability)
  - Fabrication (DOS) (Authentication)
  - Modification (Integrity)
    - Replay Attacks
    - Alterations
- Passive
  - Wiretapping
  - Interception- release of message content (Confidentiality)

Programs that attack

- **Virus**
  - A **computer virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, logging their keystrokes, or even rendering the computer useless. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without user consent.

Worm

- Worm
  - A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers.[1] Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.[2] Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Trosan Horse

- A **Trojan horse**, or **Trojan**, in computing is any malicious computer program which misrepresents itself as useful, routine, or interesting in order to persuade a victim to install it.
- Its attemts to reveal confidential information to an attacker.

Examples of threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Eavesdropping

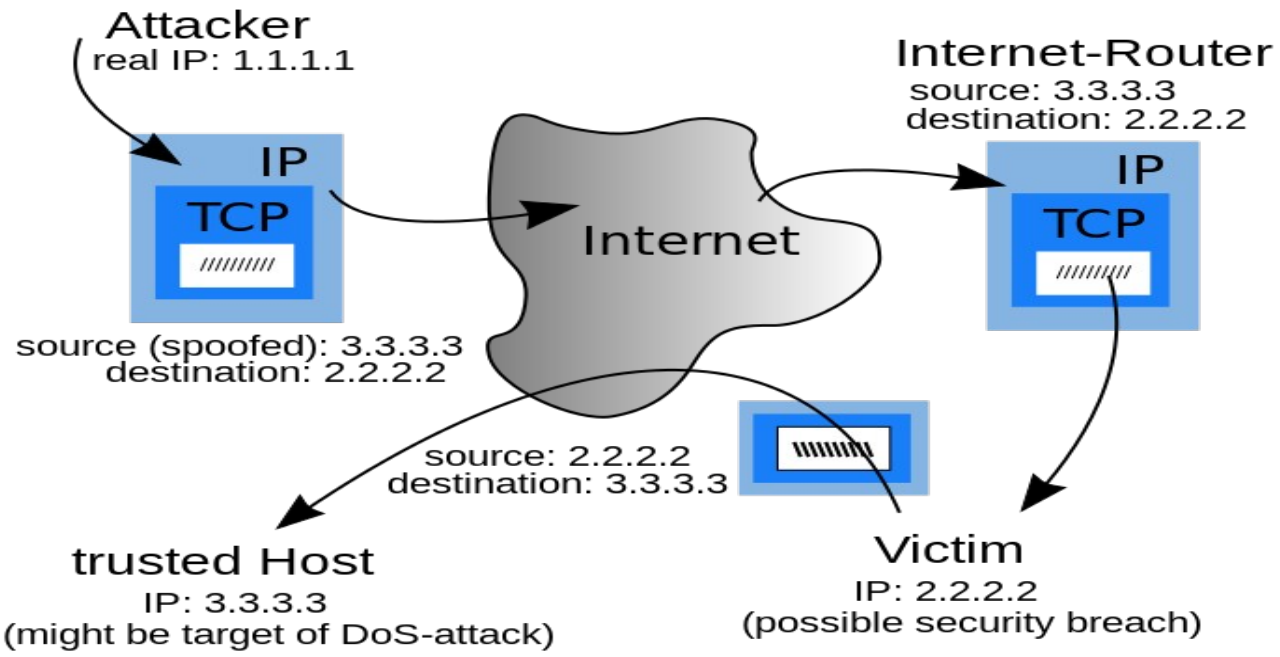
- **Eavesdropping** is secretly listening to the private conversation of others without their consent.
- It can be conducted on ordinary telephone systems, emails, instant messaging or other Internet services. Since eavesdropping activities do not affect the normal operation of network transmission, both the sender and the recipient can hardly notice that the data has been stolen, intercepted or defaced.

Spoofing

- In the context of network security, a **spoofing attack** is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.
- **Spoofing** is the creation of TCP/IP packets using somebody else's IP address. Routers use the "destination IP" address in order to forward packets through the Internet, but ignore the "source IP" address. That address is only used by the destination machine when it responds back to the source.

IP address spoofing

- **IP spoofing** is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system.

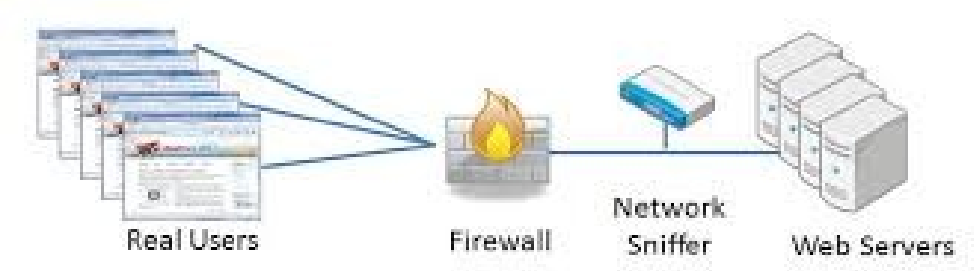


Caller ID spoofing

- Public telephone networks often provide Caller ID information, which includes the caller's name and number, with each call. However, some technologies (especially in Voice over IP (VoIP) networks) allow callers to forge Caller ID information and present false names and numbers. Gateways between networks that allow such spoofing and other public networks then forward that false information. Since spoofed calls can originate from other countries

Sniffing

- Sniffing is a passive attack on a ongoing conversation.
- Packet sniffing is a form of wire-tap applied to computer networks instead of phone networks.



Phishing

Phishing has become a big problem in recent times. In 2006, the estimated losses due to phishing were to the tune of USD 2.8 billion, according to a study. Attackers set up fake Web sites, which look like real Web sites. It is quite simple to do so, since creating Web pages involves relatively simple technologies such as HTML, JavaScript, CSS (Cascading Style Sheets), etc. Learning and using these technologies is quite simple. The attacker's modus operandi works as follows.

1. The attacker decides to create her own Web site, which looks very identical to a real Web site. For example, the attacker can clone Citibank's Web site. The cloning is so clever that human eye will not be able to distinguish between the real (Citibank's) and fake (attacker's) sites now.
2. The attacker can use many techniques to attack the bank's customers. We illustrate the most common one, as follows:

   The attacker sends an email to the legitimate customers of the bank. The email itself appears to have come from the bank. For ensuring this, the attacker exploits the email system to suggest that the sender of the email is some bank official (e.g. accountmanager@citibank.com). This fake email warns the user that there has been some sort of attack on the 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. This is conceptually shown in Fig. 1.27.
3. When the customer (i.e. the victim) innocently clicks on the URL specified in the email, she is taken to the attacker's site and not the bank's original site. There, the customer is prompted to enter confidential information, such as her password or PIN. Since the attacker's fake site looks exactly

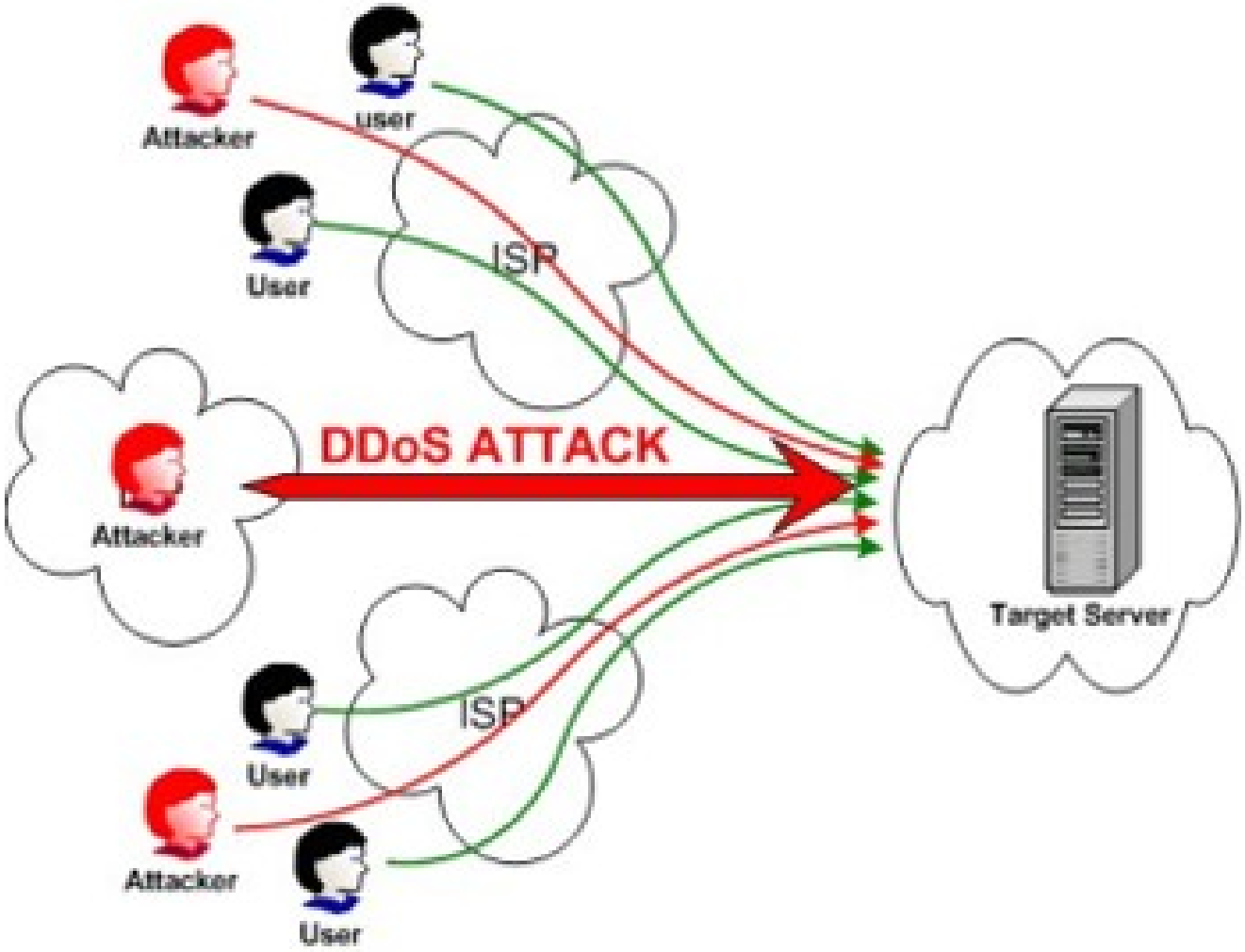

www.lolomgz.a.gp/?_fb_noscript=1
Google URL Shortener
Like Button - Faceboo...
Welcome to Windows ...
Blogger Buzz: Tweet ...
tweetburner - track li...
twitterfeed
facebook
Sign Up
Facebook helps you connect and share with the people in your life.
This is a Phishing Scam. This web site looks like Facebook.com, but if you note the web address in the the browsers address bar you can clearly see this is not Facebook.
Facebook Login
Email:
XXX
Password:
Keep me logged in
Login
or Sign up for Facebook
Forgot your password?
??????? English (US) Español Português (Brasil) Français (France) Deutsch Italiano ?????? ??(??) ??? »
Facebook © 2010
About · Advertising · Develope

Denial-of-service attack

- A **denial of service** (**DoS**) **attack** is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

symptoms of denial-of-service attacks to include:

- Unusually slow network performance (opening files or accessing web sites)
- Unavailability of a particular web site
- Inability to access any web site
- Dramatic increase in the number of spam emails received—(this type of DoS attack is considered an e-mail bomb)[4]
- Disconnection of a wireless or wired internet connection
- Long term denial of access to the web or any internet services


Attacker
user
User
ISP
DDoS ATTACK
Attacker
Target Server
User
ISP
Attacker
User