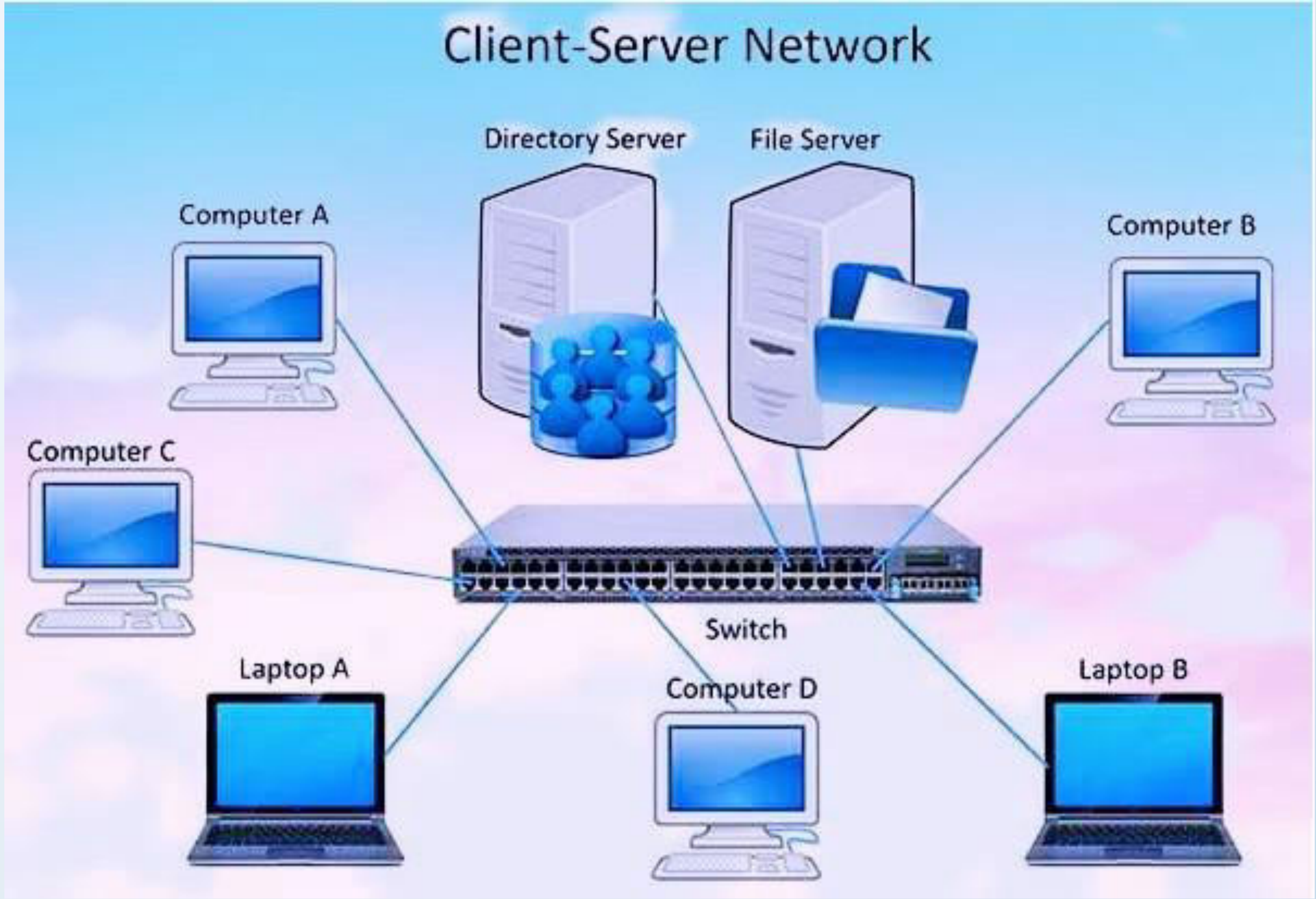
CSC-370
E - Commerce

(BSc CSIT, TU)

Ganesh Khatri
kh6ganesh@gmail.com

8. Client/Server Security



8. Client and Server Security

- A client-server network is a network consisting of a central computer, also known as a server, which hosts data and other forms of resources and clients such as laptops and desktop computers contact the server and request to use data or share its other resources with it

- A network security is defined as a circumstance, condition with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse

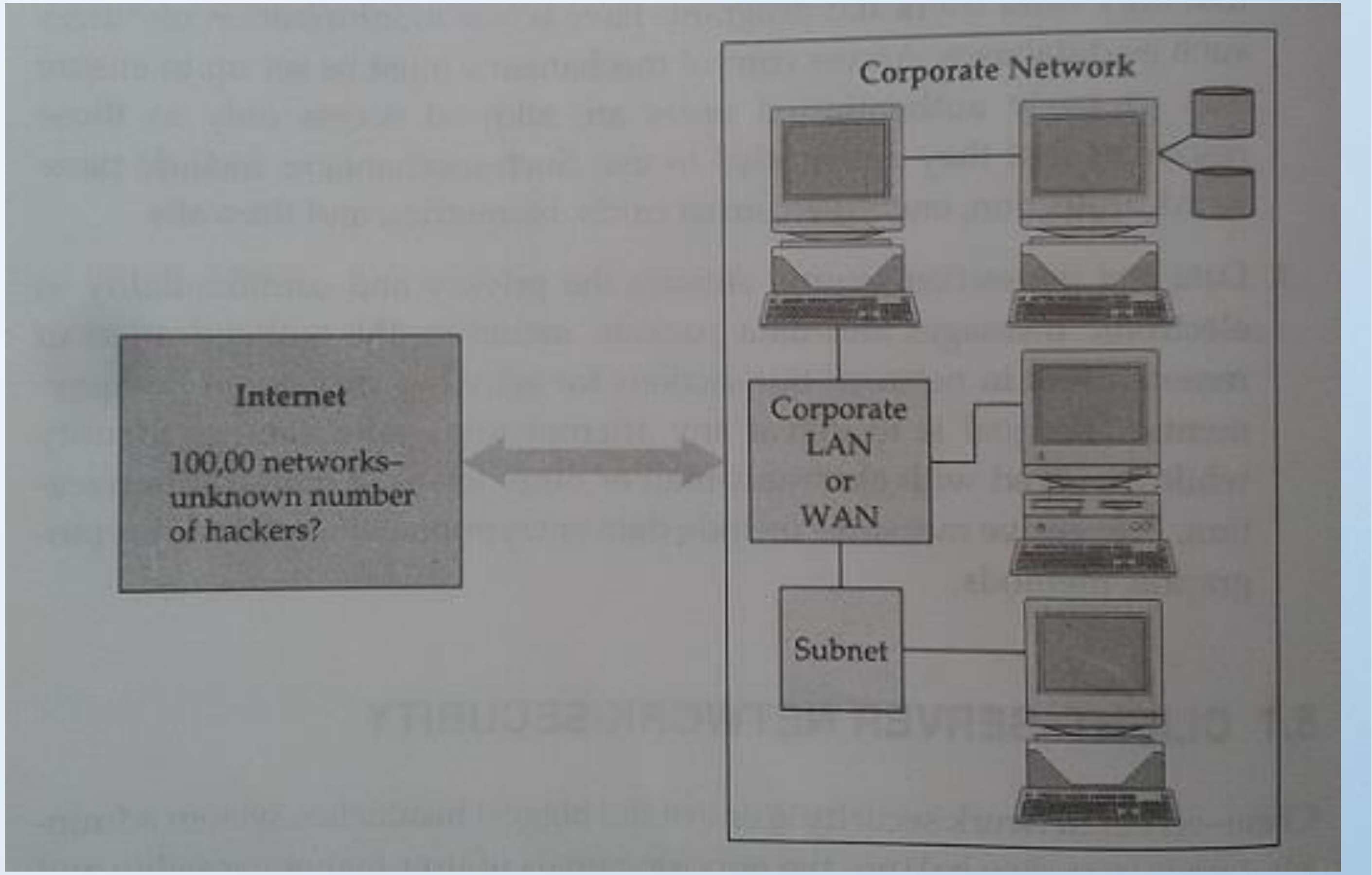
- uses various authorization methods to make sure that only valid user and programs have access to information resources such as databases.

- Access control mechanisms must be set up to ensure that properly authenticated users are allowed access only to those resources that they are entitled to use.

- Such mechanisms include password protection, encrypted smart cards, biometrics, and firewalls

8. Client and Server Security

- According to the National Center for Computer Crime Data, computer security violations cost U.S. businesses half a billion dollars each year
- Network security on the Internet is a major concern for commercial organizations, especially top management.
- Recently, the Internet has raised many new security concerns.
- By connecting to the Internet, a local network organization may be exposing itself to the entire population on the Internet.
- As given figure illustrates, an internet connection opens itself to access from other networks comprising the public Internet



unprotected internet connection

8. Client and Server Security

- Client/server network security problems manifest themselves in three ways
  - **Physical security holes**
  - **Software security holes**
  - **Inconsistent usage holes**
- **Physical Security Holes**
  - result when individuals gain unauthorized physical access to a computer.
  - A good example would be a public workstation room, where it would be easy for a hacker to reboot a machine into single-user mode and tamper with the files, if precautions are not taken.
  - On the network, this is also a common problem, as hackers gain access to network systems by guessing passwords of various users

8. Client and Server Security

- **Software Security Holes**
  - result when badly written programs or "privileged" software are "compromised" into doing things they shouldn’t.
  - The most famous example of this category is the "sendmail" hole, which brought the Internet to its knees in 1988.
  - A more recent problem was the "rlogin" hole in the IBM RS-6000 workstations, which enabled a cracker (a malicious hacker) to create a "root" shell or superuser access mode.
  - This is the highest level of access possible and could be used to delete the entire file system, or create a new account or password file etc.

8. Client and Server Security

- **Inconsistent Usage Holes**
  - result when a system administrator assembles a combination of hardware and software such that the system is seriously flawed from a security point of view.
  - The incompatibility of attempting two unconnected but useful things creates the security hole.
  - Problems like this are difficult to isolate once a system is set up and running, so it is better to carefully build the system with them in mind.
  - This type of problem is becoming common as software becomes more complex
- To reduce these security threats, various protection methods are used.
- At the file level, operating systems typically offer mechanisms such as access control lists that specify the resources various users and groups are entitled to access
- Protection, also called authorization or access control - grants privileges to the system or resource by checking user-specific information such as passwords.

8. Client and Server Security

- Over the years, several protection methods have been developed :
  - **Trust-Based Security**
  - **Security through Obscurity**
  - **Password Schemes**
  - **Biometric Systems** etc
- **Trust-Based Security :**
  - trust-based security means to trust everyone and do nothing extra for protection.
  - It is possible not to provide access restrictions of any kind and to assume that all users are trustworthy and competent in their use of the shared network.
  - This approach assumes that no one ever makes an expensive breach such as getting root access and deleting all files (a common hacker trick).
  - This approach worked in the past, when the system administrator had to worry about a limited threat. Today, this is no longer the case

8. Client and Server Security

- **Security through Obscurity :**
  - Most organizations in the mainframe era practiced a philosophy known as security through obscurity (STO) - the notion that any network can be secured as long as nobody outside its management group is allowed to find out anything about its operational details and users are provided information on a need-to-know basis.
  - Hiding account passwords in binary files or scripts with the presumption that "nobody will ever find them" is a prime case of STO (somewhat like hiding the housekey under the doormat and telling only family and friends).
  - In short, STO provides a false sense of security in computing systems by hiding information

8. Client and Server Security

- **Password Schemes :**
  - a password scheme, creates a first-level barrier to accidental intrusion.
  - In actuality, however, password schemes do little about deliberate attack, especially when common words or proper names are selected as passwords.
  - The simplest method used by most hackers is dictionary comparison - comparing a list of encrypted user passwords against a dictionary of encrypted common words.
  - This scheme often works because users tend to choose relatively simple or familiar words as passwords.
  - To beat the dictionary comparison method, experts often recommend using a minimum of eight-character length mixed-case passwords containing at least one non - alphanumeric character and changing passwords every 60 to 90 days

8. Client and Server Security

- **Biometric Systems :**
  - Biometric systems, the most secure level of authorization, involve some unique aspect of a person's body.
  - Past biometric authentication was based on comparisons of fingerprints, palm prints, retinal patterns, or on signature verification or voice recognition.
  - Biometric systems are very expensive to implement : At a cost of several thousand dollars per reader station, they may be better suited for controlling physical access where one biometric unit can serve for many workers than for network or workstation access.
  - Many biometric devices also carry a high price in terms of inconvenience; for example, some systems take 10 to 30 seconds to verify an access request