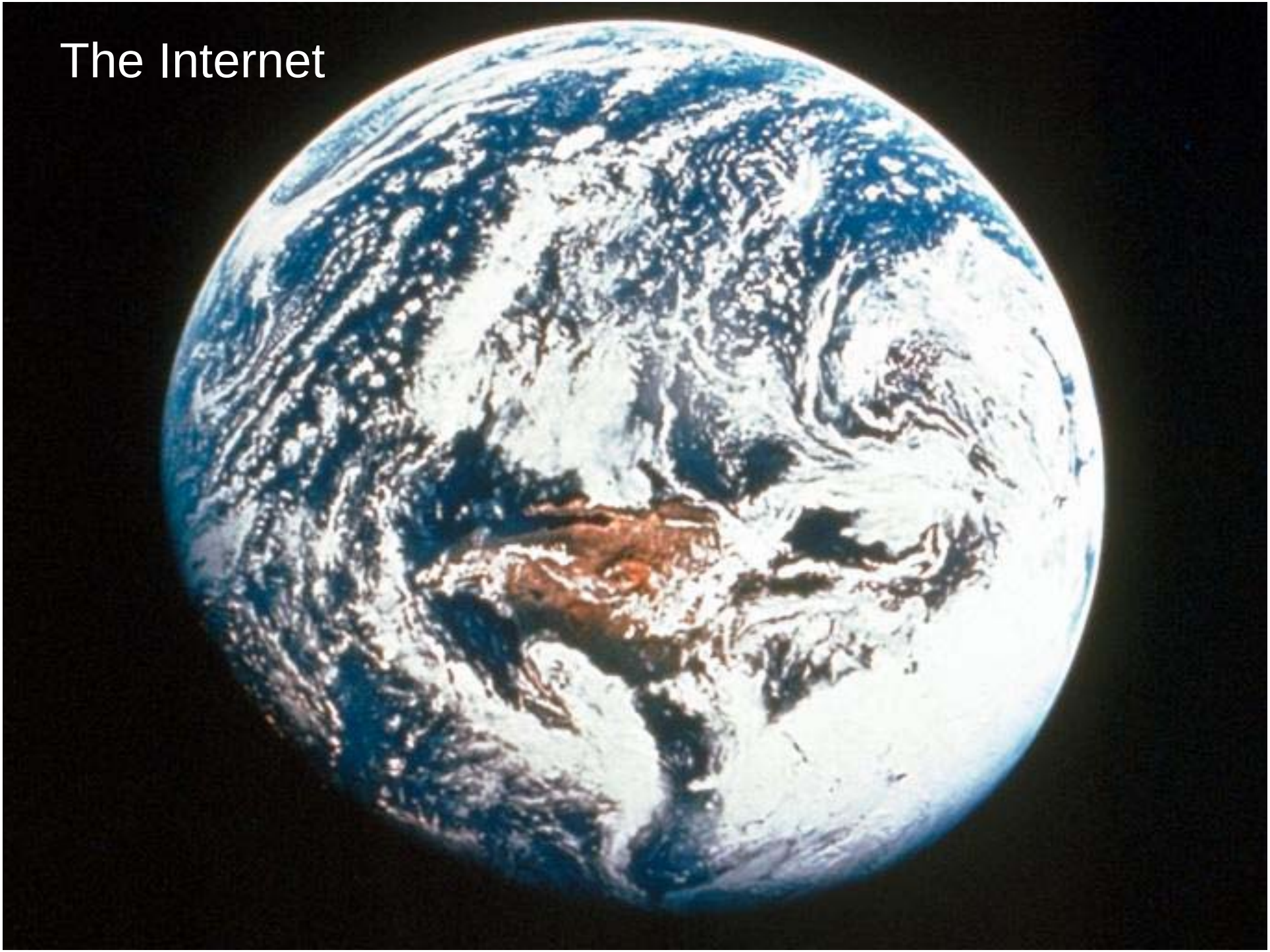
The Internet



What is the Internet ?

- It is a worldwide network of tens of millions of computers
- These computers communicate with each other in a consistent fashion
- Users on one computer can access services from other computers
- You can access a wide variety of services, most of which are free
- Each service can give you many kinds of information

What are its origins ?

- ARPANET - Department of Defense 1969
  - The Internet began as a United States Department of Defense network to link scientists and university professors around world.
- NSFNET - National Science Foundation 1973
- World Wide Web - 1990s

Who owns the Internet ?

- No one person or entity owns the Internet and it has no formal management organization
- Some companies own the network and cabling
- Other companies own the servers connected to the network
- Other companies own the content shown on the sites
- Still other companies develop software for running the sites
- Some specific organizations are in charge of centralized registration of sites.

Who owns the Internet ?

- To join the Internet an existing network need only pay a small registration fee and agree to certain standards based on the TCP/IP reference model.
- Regional Internet companies have been established to which member networks forward all transmissions. These Internet companies route and forward all traffic, and the cost is still that of a local phone call.
- Due to this, the Internet is the fastest and least expensive method of communication available today.

Value of the Internet ?

- The value of the Internet lies precisely in its ability to easily and inexpensively connect so many diverse people from so many places around the globe.
- Anyone who has an Internet address can log onto a computer and reach virtually any other computer on the network, regardless of location, computer type, or operating system.

What use is it to you?

- Mail - the Killer App
- Information
- FTP - for getting software and files
- News
- Telephony
- Video conferencing
- Conducting Commercial Transactions

What you need to start using?

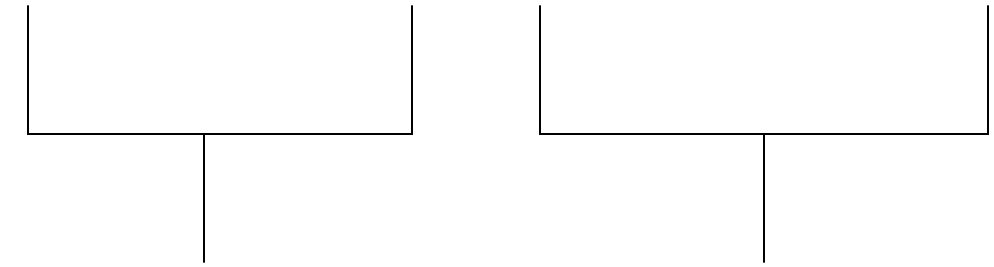
- Computer
- Connection Hardware
- Internet Service Provider account
- Specific accounts at paid subscription sites

Fundamental Parts of the Web

- Content - stuff you read, see, and hear on the Web
- Client Software - what you run on your computer to access the content on the Web
- Web Servers - Computers to which you connect; these computers store the Web content

Email IDs

byfordconsulting@yahoo.com

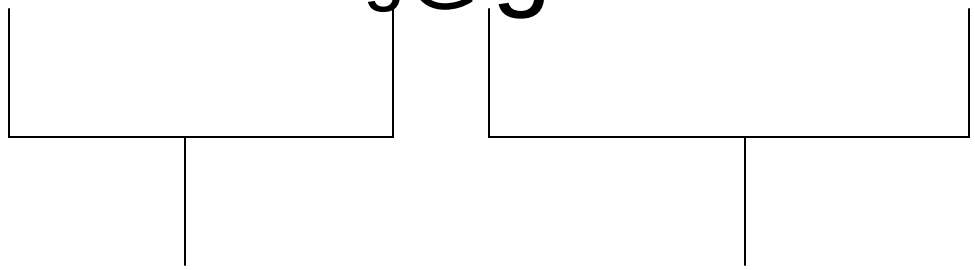


Personal ID

Server Name

Email IDs

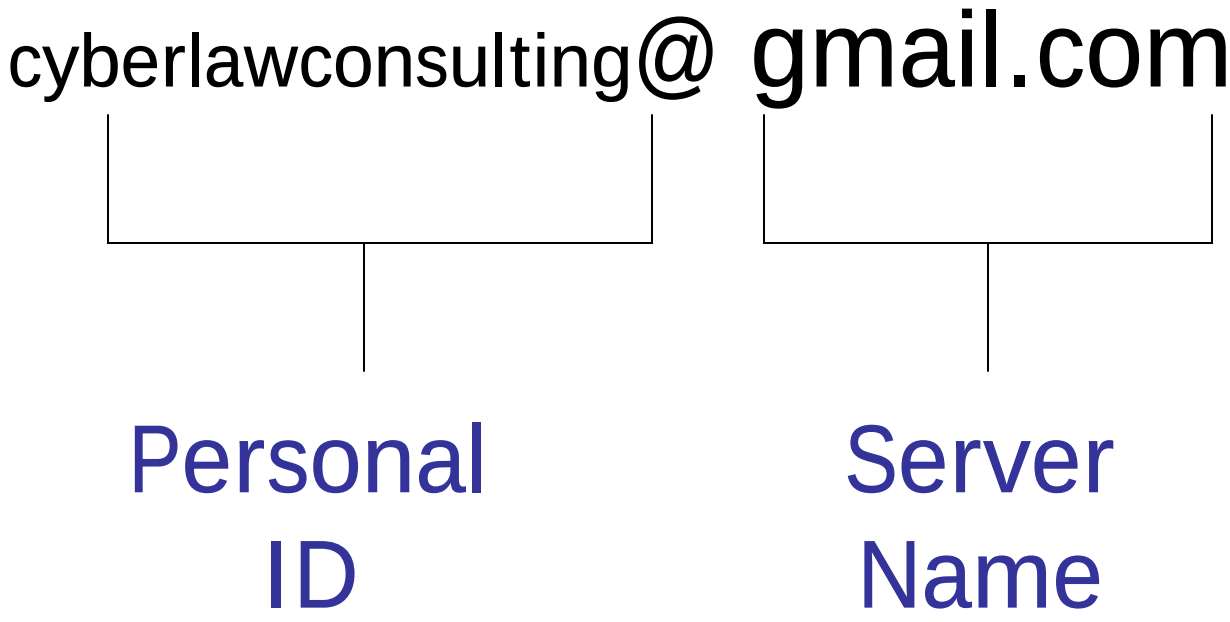
byfordconsulting@gmail.com



Personal ID

Server Name

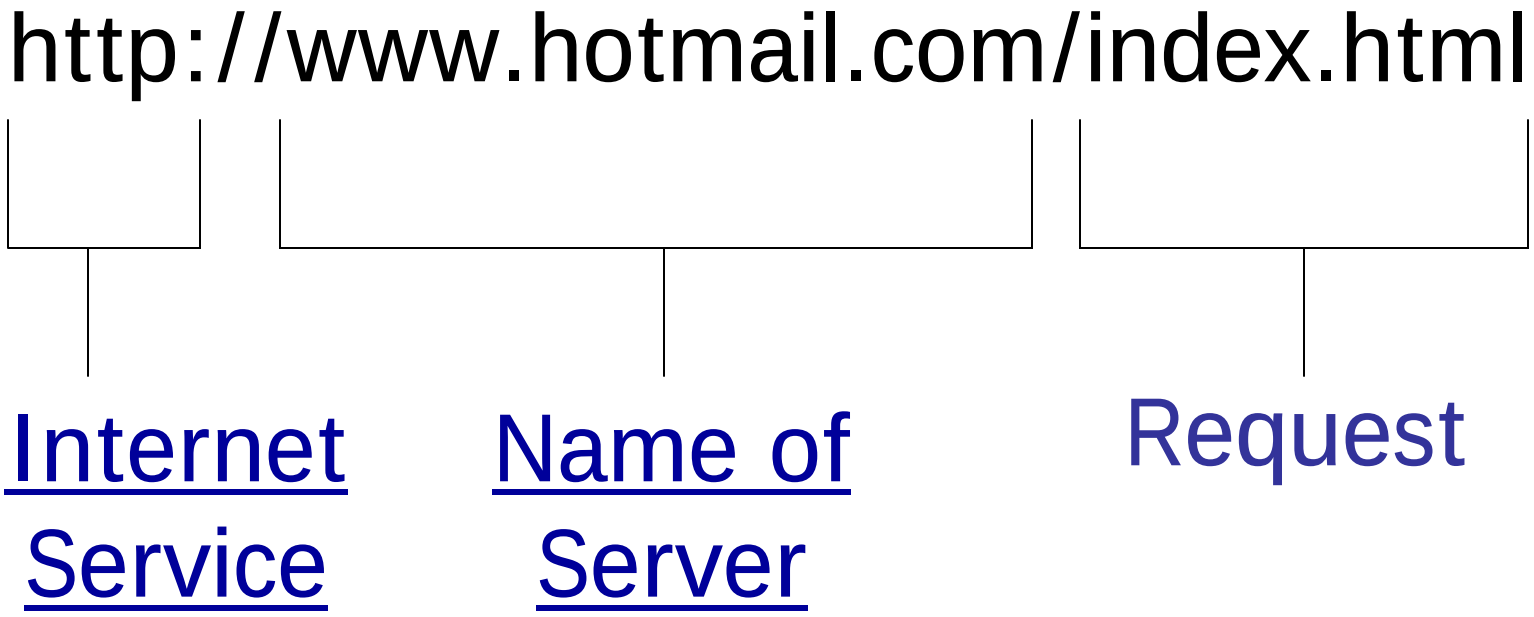
Email IDs



Email Software

- Internet Explorer
- Netscape Messenger
- Eudora
- Pine

Uniform Resource Locator



Keyword Sites

- Web Search Sites
- Web indexes
- Web crawlers, worms, spiders
- Download Engines, Accelerators
- Search Engines

Web Pages

- Create a Web page using a text editor like MS Word or a HTML editor
- Test the page with the most common browsers to see if it works well.
- Upload the page to the web site and file it in the proper place
- Pages can be updated frequently to reflect latest news, etc.
- Same procedure can be followed for photos, videos, etc.

Web Sites

- Servers which host the Web pages
- Supply pages to the client software or browsers that demand it.
- Should be connected all the time to the Internet

Web Directories

- Used to locate sites of interest
- Wide variety of directories are available.
- Differentiated by ease of use and scope of directories.

Search Engines

- Web searching facilities
- Search by particular keyword
- Yahoo, Lycos, Excite are directories with built-in search engines
- Google, Altavista, Inktomi are search engines without directories
- Search engines have to be updated regularly to be of any value.

Proxy Servers

- A server which is empowered to act on behalf of other computers is called a proxy server. The proxy server acts as a mediator between two systems attempting to communicate with each other over the network.
- A computer running a proxy server is commonly referred to as an Application Gateway.

Proxy Servers

- A user connects to the proxy server via software that tells the proxy about the system, the connection request, and the reason for the connection such as a web page request.
- The gateway checks the users IP address and accepts it or rejects it based on access criteria put in place by the administrator and creates a connection between the two systems.
- As the proxy server passes data between two systems, it logs the connection information.

Common Gateway Interface

- CGI scripts perform server side tasks
- Could be used for search, verification, validation tasks.
- Normally, in the root directory of the server a sub-directory cgi-bin would be created. The server instead of just reading and sending the file, executes a file requested from the cgi-bin directory.
- The output of the executed program is sent to the browser that requested the page.

Cookies

- A cookie is a piece of data that is stored on your machine by the server the first time you visit it.
- Each site stores a different cookie.
- The next time you visit the site, the server will recognize you.
- Can be customized for your likes and dislikes.
- Security risk ?

Communications on the Web

- One-to-one
- Peer group
- Different Group
- Organizational
- Mass communications

Protocols

Following are some of the protocols used in internet technology:

- POP
- SMTP
- ICMP
- SSL
- SET
- SNMP

POP

Post Office Protocol

- POP is a protocol that is applicable to the offline model of client-server email.
- POP is a hypothetical machine state that can react only in three predetermined states :
  - Authorization state
  - Transaction state
  - Update state

SMTP

Simple Mail Transfer Protocol

- SMTP is a protocol used to transfer email from a client to server as well as from a server to another server. SMTP is a request-response protocol.
- The SMTP server takes the receivers address and breaks it into two parts:
  - The receivers name
  - The domain name
- These two parts are used to divert the message to the correct receiver.

ICMP

Internet Control Message Protocol

- ICMP is designed to send error or control messages from one machine to the other in a network.
- ICMP packets are usually small and relatively simple.
- It returns information like “the destination to which the packet was intended for is not available.

SSL

Secure Socket Layer

- SSL is a protocol developed by Netscape for transmitting private documents over the internet.
- SSL works by encrypting the data that is transferred over the SSL connection.
- Both Internet Explorer and Netscape Navigator support SSL.

SET

Secure Electronic Transactions

- SET is an internationally recognized standard for protecting and safeguarding credit card payments over the internet.
- SET focuses on maintaining confidentiality of information, ensuring message integrity, and authenticating parties involved in a transaction.
- Virtually all the major players in the electronic commerce arena including Microsoft, Netscape, Visa and Mastercard have endorsed SET.

SNMP

Simple Network Management Protocol

- SNMP is a tool for network managers to continuously monitor the network and is simple to implement.
- SNMP works independently on the network with one connection gathering reliable information from the network.
- SNMP requires low overhead and requires just 64K RAM.

Internet Threats

- Denial of Service (DoS)
- Disclosure
- Loss of Integrity
- Masquerade
- Theft of services or resources
- Unauthorized access

Risk Analysis

Risk Assessment:

- What is to be protected
- Who it is to be protected against
- how well is it to be protected

Potential attacks:

- Penetration by unauthorized persons
- Disruption of networks
- Loss of confidential information

General rules

What do we mean by authorized use of systems:

- No getting into outside systems
- No capturing passwords
- No reading or tampering of other people's files
- No sharing your account with other people or staff
- No copying copyright software.

General rules

What are the duties of the users:

- Keep passwords secret
- Change passwords regularly
- Make backup copies of your own files
- Keep secret data secret
- Follow the guidelines for using system resources
- Follow guidelines for using the Internet
- Monitor your own account for unauthorized use.

Securing Hardware

- Physical access control over critical network components (servers, root terminals, router, bridges)
- Physical security of remote terminals
- Theft protection of PCs/terminals
- Interruption free power supplies
- Excess voltage protection
- Storage of backup copies
- Storage of confidential data

Security Guidelines

- Any internet services not expressly authorized must be disabled
- Registered and authorized users have access to the following Internet services:
  - WWW
  - FTP
  - Email
  - Gopher
  - Archie
- Access management is via a dedicated firewall system.

Security Guidelines

- There must be no direct links between the company's network and the Internet. The only access should be through the firewall system.
- The firewall system must have monitoring and alarm systems for detecting breaches or impending breaches of security rules (outside attacks, changes in configurations, breaches in data integrity, etc.)

Dealing with Security Breach

Make safe and Continue

- Data and system are inadequately protected.
- Further breaches of security are an incalculable risk
- You are not prepared to put resources into bringing charges against the offender.
- Users are unfamiliar with computing

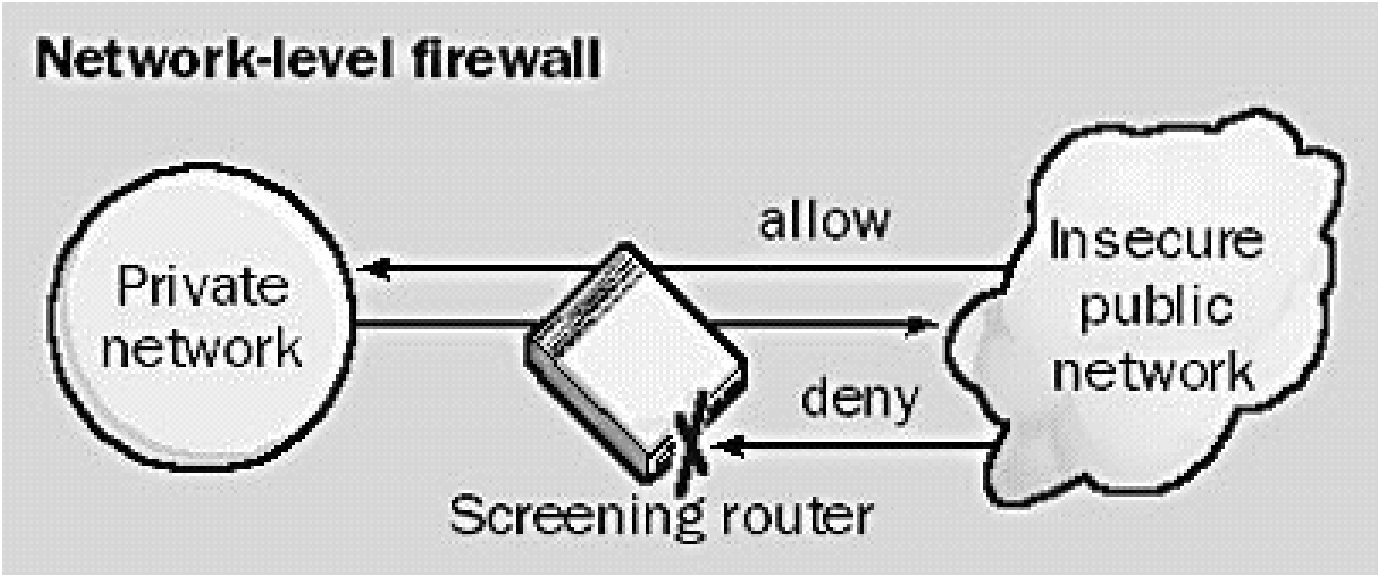
Dealing with Security Breach

Catch and Punish policy:

- Data and systems are adequately protected
- You have backup copies available for all the areas concerned
- Risk of damage from future breaches of security is to be weighed against the possibility of catching the offender
- Company is a attractive target for hackers

Firewalls

A firewall is a hardware, software, and management policies solution that protects all traffic between an “inside” network and a less trustworthy “outside” network.



Firewalls

The objectives of Firewalls are:

- Enforce an access control policy
- Allows only authorized traffic to pass
- Helps prevent unauthorized access
- Protects sensitive data
- Provides audit and logging information
- Authenticate all server access

Characteristics of a Firewall

The characteristics of a Firewall are:

- All traffic from inside to outside and from outside to inside shall pass only through the firewall. There should be no other alternate route.
- The overall security policy of the organization shall determine what traffic must be permitted to pass through the firewall. All other traffic must be blocked.
- The firewall must be resilient and immune to attacks and penetration.

Types of Firewalls

Different types of Firewall Architectures available:

- Packet filtering router
- Application level gateway or proxy server
- Circuit level gateway
- Bastion Host

Firewalls Rules

Some typical filtering rules include:

- Permit incoming Telnet sessions only to a specific list of internal hosts.
- Permit incoming FTP sessions only to specific internal hosts.
- Permit all outbound Telnet sessions
- Permit all outbound FTP sessions
- Deny all incoming traffic from specific external networks

Packet Filtering Router

- Fast and cost effective firewall configuration.
- The firewall examines the header of each incoming packet to determine whether it matches one of its packet filtering rules.
- If a match is found and the rule permits the package, the packet is forwarded according to the information in the routing table.
- If a match is found and the rule denies the package, the packet is rejected.
- If there is no matching rule, a user configurable default parameter setting determines what action to take.

Packet Filtering Router

Disadvantages

- Source IP Address spoofing attacks
- Source routing attacks
- Tiny fragment attacks

Application level Gateways

- An Application level gateway offers more security
- A special purpose code (a proxy service) is installed on the gateway for each desired application.
- If the proxy code for a particular application is not installed, the service is not supported.
- Users are allowed access only to the proxy services.

Application level Gateways

Advantages

- Provide complete control over each service, since the proxy application limits the command set and determines which internal hosts may be accessed by the service.
- There is complete control over services that are permitted.
- Support strong user authentication
- Detailed logging information can be obtained which is of immense use as an audit trail.

Circuit level Gateways

- Circuit level gateway is a specialized form of an application level gateway.
- Often used for outgoing connections where the administrator trusts the internal users.
- The firewall can be configured as a hybrid gateway supporting proxy services for inbound connections and circuit-level functions for outbound connections.

Bastion Hosts

- Bastion Host is a point of high security in a network through which all incoming and outgoing traffic is allowed to pass.
- The Bastion Host hardware platform executes a tamper proof and secure version of an operating system.
- Each proxy service maintains detailed audit information by logging all traffic, each connection, and the duration of each connection.
- A proxy generally performs no disk access other than to read its initial configuration file.
- Each proxy runs as a non-privileged user in a private and secured directory on the bastion host.

Firewalls

Common implementations structures of a Firewall:

- Packet filtering router
- Single homed firewall
- Dual homed firewall
- DMZ or screened subnet firewall

Firewalls

A Firewall cannot:

- Guarantee protection against malicious intruders
- Protect a connection that does not go through it.
- Protect against completely new threats
- Protect against viruses, trojan horses, and such variants

Firewall Problems

The problems faced by an organization that has implemented a firewall solution are:

- Activities are not monitored regularly
- Firewalls and their capabilities are not clearly understood (a mere screening router cannot be a real deterrent against a determined attack)
- Firewalls are not configured properly
- Firewalls are circumvented by using modems
- Once hackers are inside a network, firewalls cannot do anything against them.

Firewall General Controls

- Physical security controls
- Operating system security
- Change control procedures
- Verification of documents
- Examination of logs

Firewall implementation

- Definition of security policy
- High level design
- Selection of firewall components
- Implementation
- Review and Testing
- Maintenance

Computer

- Any kind of computer with the appropriate connectivity software is good enough
- Could be a Mainframe, Minicomputer, or PC.
- No restriction on the operating system used - UNIX, Windows, Linux, Macintosh, BeOS……

Connection Hardware

- Many kinds of Connection Hardware
- Modems - telephone line *Rs. 20/hr*
- Digital Modems - ISDN telephone line
- Cable Modems - Cable line
- Radio Towers - Radio waves
- Microwave Links - Microwaves
- Satellite Dishes - Satellite communications
- VSATs - Satellite communications

Internet Service Providers

- VSNL, Mantra Online, Net Cracker, Satyam Online
- Cost depends on the speed of the connection and the type of connection used
- Additional costs for any equipment that needs to be set up.
- Provision of leased lines to other countries

Internet Service Providers

Choice of ISP is based upon:

- Service Area
- Types of connections offered
- Target market of ISP
- Support
- Training
- Reliability
- Security
- Cost

Mail Servers

A mail server is required to send and receive email. Mail servers perform the following functions:

- Houses a list of email accounts
- Contains a text file for each email account.
- It accepts the sender information, receiver information and the body or content of the message from the email client.
- It formats the information and appends it to the bottom of the text file of the receiver account.
- When the receiver connects to the mail server, the messages are shown to him.

Paid Subscription Sites

- Newspapers like Wall Street Journal, The New York Times, etc.
- Magazine sites
- Consultancy Sites - Arthur Andersen
- Software sites - software downloads
- Freeware or Shareware sites

Content

The Web is very much like a well-stocked library

- It houses materials on an incredibly wide variety of topics
- Contains material in variety of forms - articles, books and magazines, videos, CDs, tapes, databases, etc.
- All the material is mostly 

- Ads pay for most of the services that you use.

Client Software or Browsers

All Browsers do certain things

- Access files on HTTP (hypertext)
- Show HTML documents from HTTP servers with some formatting
- Move between links in hypertext documents
- Save files to your computer hard disk
- Fill in interactive forms on some sites
- Remember places that you have been to so that you can return there easily.

Web Servers

Servers make services available to the clients.

- Also known as host computers
- Servers must follow the same protocols (must speak the language) as the Browsers
- Domain name - *www.hotmail.com*
- University Servers
- Commercial Servers
- Web Societies - *www.geocities.com*

Internet Services

Service	Name in URL
hypertext	http:
gopher	gopher:
ftp	ftp:
Usenet News	news: and nntp:
email	mailto:
Telnet	telnet:
files	file:

http

Hypertext Transfer Protocol

- Used by browsers to transfer hypertext documents.
- http represents a document from the World Wide Web.
- http://www.netscape.com/download/index.html

gopher

Gopher

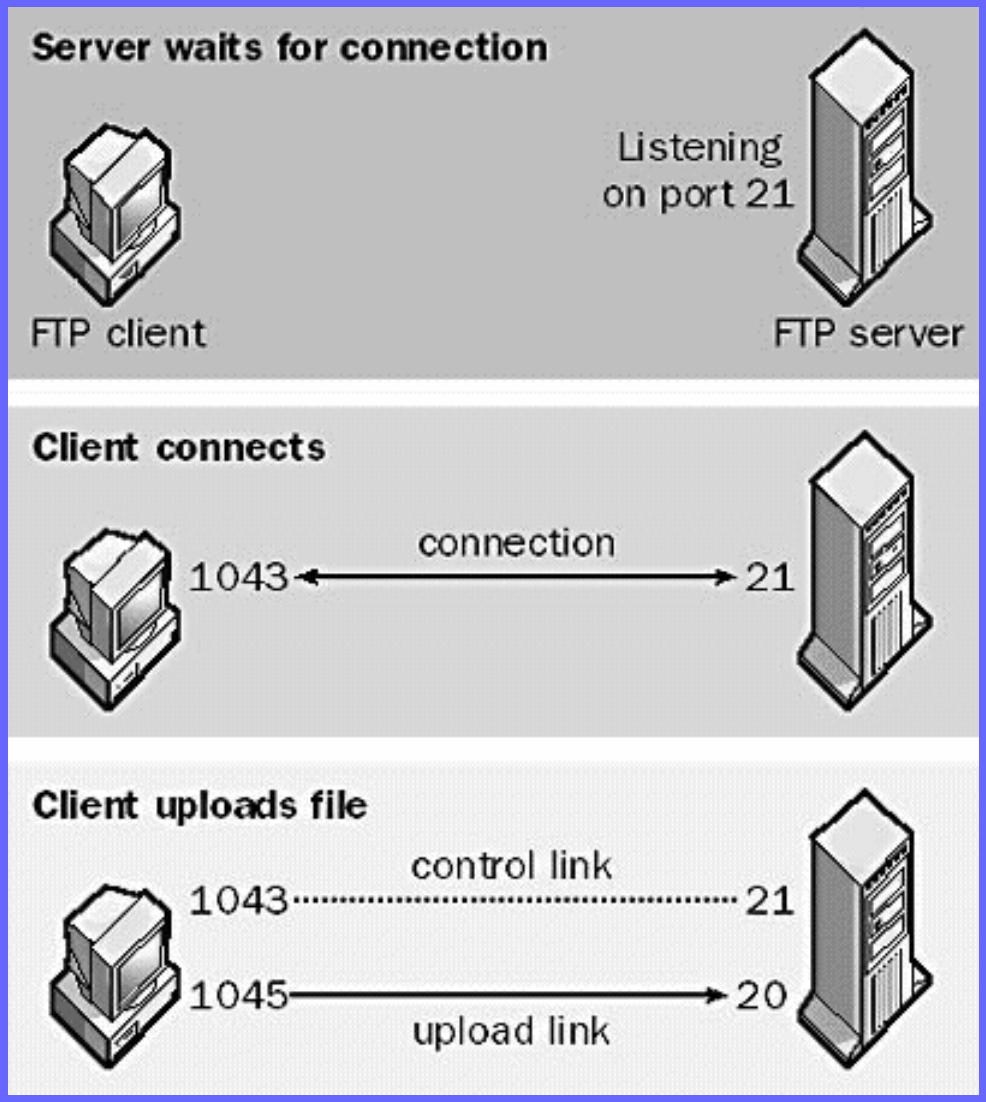
- Gopher is an information browser just like FTP with enhancements for ease of use and flexibility.
- By connecting to gopher sites, we can search databases, read text files, transfer files and navigate around the collection of information called gopher space.
- One of the special features of gopher is that it provides access to FTP, WAIS resources available only via telnet and special data types such as pictures and sounds.

ftp

The objectives of FTP are:

- To encourage indirect or implicit use of remote computers
- To promote sharing of files
- To shield a user from variations in file storage systems among hosts
- To transfer data reliably and efficiently.
- Used widely by organizations and individuals

FTP process


Server waits for connection
Listening
on port 21
FTP client
FTP server
Client connects
1043
connection
21
Client uploads file
control link
1043
21
1045
20
upload link

news

Usenet News

- Usenet news is interpersonal news. It comes from several individuals and is aimed at thousands of people around the world.
- Posting a message to Usenet is like writing a letter to the editor of a magazine or newspaper.
- News:computer-infosystems.www.authoring.html

mailto

Email service

- mailto refers to the internet electronic mail service.
- We can use a mailto address in our html documents so that people can send email simply by clicking on the hyperlink.
- Mailto:prashant.mali@cyberlawconsulting.com

file

Local Files

- file refers to the files located on our own computer.
- file://internet/documents/test.htm

telnet

Telnet

- Telnet allows a user to connect to a remote system using his local screen and keyboard as a terminal.
- Allows direct connection to the services provided by the host computer.
- telnet://tech.science.computer.edu

Name of Company

Name in URL	IP Address
www.yahoo.com	152.4.101.50
www.hotmail.com	202.54.35.109
www.microsoft.com	201.30.56.987
www.cmu.edu	203.43.34.119

Name of Company

Zone in URL	Type of Organization
.com	Commercial Organizations
.edu	Educational Institutions
.net	Networking Organisations
.gov	Government Organizations
.mil	Military Organizations
.biz	Business Organisations

OM

Thank You

prashant.mali@cyberlawconsulting.com