Unit 5 : Basics of Network Security, Internet connection & Sharing

LECTURER : NANDAN PANDYA

COURSE: BACHELOR OF COMPUTER APPLICATIONS (BCA)

SEMESTER: 4TH

SUBJECT: NETWORK TECHNOLOGY AND ADMINISTRATION

SUBJECT CODE: CS-21

COLLEGE: KAMANI SCIENCE COLLEGE, AMRELI

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Topics

- Fundamental of Network Security
- Network Security :Policies, Standard, Procedures, Baselines, Guidelines
- Security Principle –CIA Model
- Security methods and Encryption, Cryptography, Authentication
- Basics of Internet: How internet is connecting with computer
- Technology related internet : Dial up ,ISDN , Lease line
- VPN: types and use of VPN
- VPN protocols (PPTP, L2TP, IPsec.)
- Proxy server, Firewall
- GPS, GPRS, CCTV

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Network Security

- Network Security protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.
- Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption and more.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Requirements of Network Security

- The main objective of the network is to share information among its users situated locally or remotely. Therefore, it is possible that undesired user can hack the network and can prove to be harmful for the health of the network or user.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Policy

- A network security policy delineates guidelines for computer network access, determines policy enforcement, and lays out the architecture of the organization's network security environment and defines how the security policies are implemented throughout the network architecture.
- Network security policies describes an organization's security controls. It aims to keep malicious users out while also mitigating risky users within your organization. The initial stage to generate a policy is to understand what information and services are available, and to whom, what the potential is for damage, and what protections are already in place.
- The security policy should define the policies that will be enforced – this is done by dictating a hierarchy of access permissions – granting users access to only what they need to do their work.
- These policies need to be implemented in your organization written security policies and also in your IT infrastructure – your firewall and network controls' security policies.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Standards

- Standards are industry-recognized best practices, frameworks, and agreed principles of concepts and designs, which are designed to implement, achieve, and maintain the required levels of processes and procedures.
- Like security policies, standards are strategic in nature in that they define systems parameters and processes.
- Standards vary by industry. There are two notable standards in security information management—ISO 17799 and COBIT.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Procedures

- Procedures are low-level documents providing systematic instructions on how the security policy and the standards are to be implemented in a system.
- Procedures are detailed in nature to provide maximum information to users so that they can successfully implement and enforce the security policy and apply the standards and guidelines of a security program.
- Employees usually refer to procedures more often than other policies and standards because procedures provide the actual details of the implementation phase of a security program.

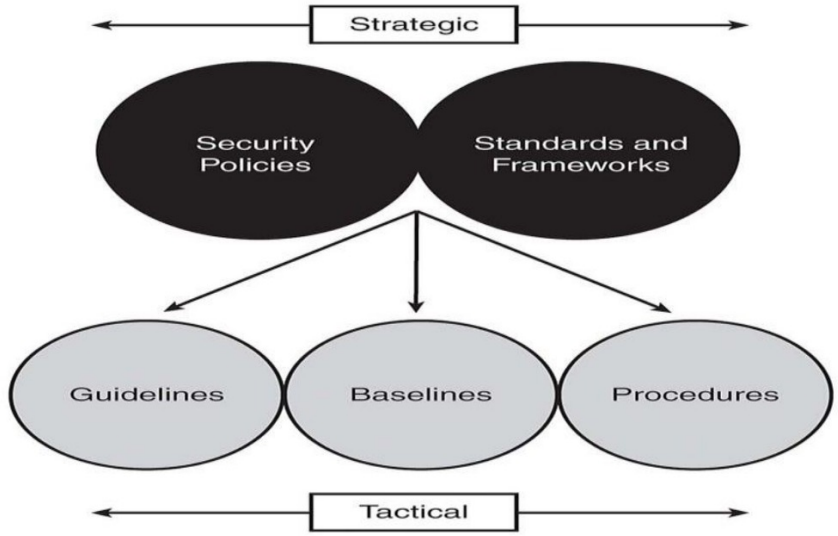
Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Baselines

- A baseline is the minimum level of security requirement in a system. Baselines provide users the means to achieve the absolute minimum security required that is consistent across all the systems in the organization.
- For example, a company might have a baseline for Windows 2000 servers to have Service Pack 4 installed on each server in the production environment. The procedure document would supplement the baseline by spelling out step-by-step instructions on where to download Service Pack 4 and how to install it to comply with this security level.

Guidelines

- Guidelines are recommended actions and operational guides for users. Similar to procedures, guidelines are tactical in nature. The major difference between standards and guidelines is that guidelines can be used as reference, whereas standards are mandatory actions in most case
- Relationships among Security Policies, Standards, Procedures, Baselines, and Guidelines in diagram



Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Principles of Security: CIA Model

- A simple but widely applicable security model is the confidentiality, integrity, and availability (CIA) triad. These three key principles should guide all secure systems. CIA also provides a measurement tool for security implementations. These principles are applicable across the entire spectrum of security analysis—from access, to a user's Internet history, to the security of encrypted data across the Internet. A breach of any of these three principles can have serious consequences for all parties concerned.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Confidentiality

- Confidentiality prevents unauthorized disclosure of sensitive information. It is the capability to ensure that the necessary level of secrecy is enforced and that information is concealed from unauthorized users. When it comes to security, confidentiality is perhaps the most obvious aspect of the CIA triad, and it is the aspect of security most often attacked. Cryptography and encryption methods are examples of attempts to ensure the confidentiality of data transferred from one computer to another. For example, when performing an online banking transaction, the user wants to protect the privacy of the account details, such as passwords and card numbers. Cryptography provides a secure transmission protecting the sensitive data traversing across the shared medium.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Integrity

- Integrity prevents unauthorized modification of data, systems, and information, thereby providing assurance of the accuracy of information and systems. If your data has integrity, you can be sure that it is an accurate and unchanged representation of the original secure information. A common type of a security attack is man-in-the-middle. In this type of attack, an intruder intercepts data in transfer and makes changes to it.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Availability

- Availability is the prevention of loss of access to resources and information to ensure that information is available for use when it is needed. It is imperative to make sure that information requested is readily accessible to the authorized users at all times. Denial of service (DoS) is one of several types of security attacks that attempts to deny access to the appropriate user, often for the sake of disruption of service.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Security Models

- An important element in the design and analysis of secure systems is the security model, because it integrates the security policy that should be enforced in the system. A security model is a symbolic portrayal of a security policy. It maps the requirements of the policy makers into a set of rules and regulations that are to be followed by a computer system or a network system. A security policy is a set of abstract goals and high-level requirements, and the security model is the do's and don'ts to make this happen.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Cont..

- **The Bell-LaPadula Model (BLM)**, also called the multilevel model, was introduced mainly to enforce access control in government and military applications. BLM protects the confidentiality of the information within a system.
- **The Biba model** is a modification of the Bell-LaPadula model that mainly emphasizes the integrity of the information within a system.
- **The Clark-Wilson model** prevents authorized users from making unauthorized modification to the data. This model introduces a system of triples: a subject, a program, and an object. The Access Control Matrix is a general model of access control that is based on the concept of subjects and objects. The Information Flow model restricts information in its flow so that it moves only to and from approved security levels.

Cont..

- **The Chinese Wall model** combines commercial discretion with legally enforceable mandatory controls. It is required in the operation of many financial services organizations.
- **The Lattice model** deals with military information. Lattice-based access control models were developed in the early 1970s to deal with the confidentiality of military information. In the late 1970s and early 1980s, researchers applied these models to certain integrity concerns. Later, application of the models to the Chinese Wall policy, a confidentiality policy unique to the commercial sector, was developed. A balanced perspective on lattice-based access control models is provided.

Encryption

- In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor.
- In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudorandom encryption key generated by an algorithm.
- It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Cryptography

- Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense.
- The originator of an encrypted message (Alice) shared the decoding technique needed to recover the original information only with intended recipients (Bob), thereby precluding unwanted persons (Eve) from doing the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.
- Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Cont..

- There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.
- The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export.
- In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation. Cryptography also plays a major role in digital rights management and piracy of digital media.

Authentication

- In the context of computer systems, authentication is a process that ensures and confirms a user's identity. Authentication is one of the five pillars of information assurance (IA). The other four are integrity, availability, confidentiality and no repudiation.
- Authentication begins when a user tries to access information. First, the user must prove his access rights and identity. When logging into a computer, users commonly enter usernames and passwords for authentication purposes. This login combination, which must be assigned to each user, authenticates access. However, this type of authentication can be circumvented by hackers.
- A better form of authentication, biometrics, depends on the user's presence and biological makeup (i.e., retina or fingerprints).
- This technology makes it more difficult for hackers to break into computer systems. The Public Key Infrastructure (PKI) authentication method uses digital certificates to prove a user's identity. There are other authentication tools, too, such as key cards and USB tokens. One of the greatest authentication threats occurs with email, where authenticity is often difficult to verify. For example, unsecured emails often appear legitimate.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

How internet is connect with computer

- Using a network connection, including connecting to the Internet, computers connect to each other to transmit data between them and communicate with each other using the TCP/IP (Transmission Control Protocol / Internet Protocol). Think of TCP/IP as a book of rules, a step-by-step guide that each computer uses to know how to talk to another computer.
- This book of rules dictates what each computer must do to transmit data, when to transmit data, how to transmit that data. It also states how to receive data in the same manner. If the rules are not followed, the computer will not be able to connect to another computer, nor send and receive data between other computers.
- Internet service providers (ISP), the companies that provide Internet service and connectivity also follow these rules. The ISP provides a bridge between your computer and all the other computers in the world, which are all a part of the Internet. The ISP uses the TCP/IP protocols to make computer-to-computer connections possible and transmit data between them. When successfully connected to an ISP you will be assigned an IP address, which is a unique address given to your computer or network and allows it to be found while on the Internet.

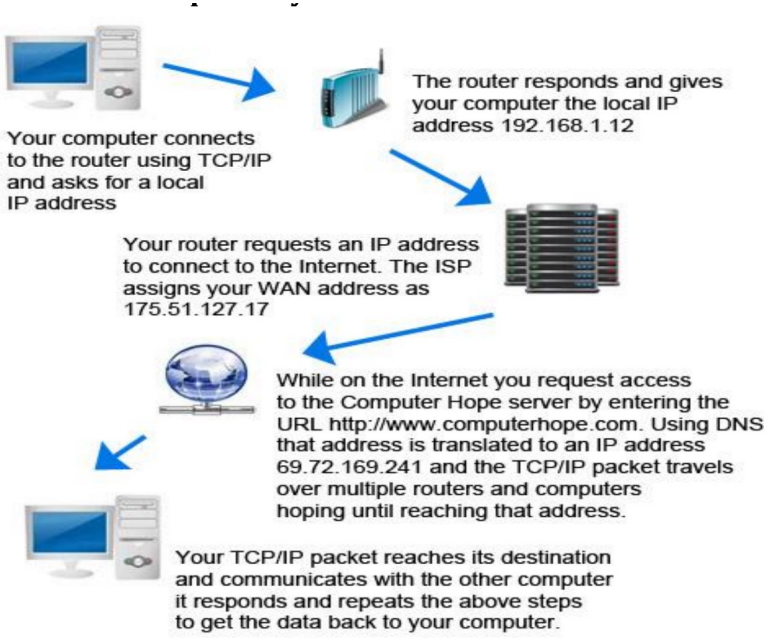
Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Cont..

- If you have a home computer network, the computers are also using TCP/IP to connect to each other. This protocol allows each computer to "see" the other computers on the network and share files between them and is what makes it possible for a printer to be shared on a network. When computers connect to each other on the same network, it is called a local area network, or LAN. When multiple networks are connected to each other, it is called a wide area network, or WAN. With this type of network, your home will have a network router that connects to your ISP.
- The router is given the IP address for your connection to the Internet and then assigns local IP addresses to each device in your network. These local addresses are often 192.168.1.2-255. When accessing a local computer in your own network, your router sends your TCP/IP packets between the local IP addresses. However, when you want to connect to the Internet your router communicates to the Internet with the IP address assigned to it from the ISP. This is why when on the Internet your IP address is not a 192.168.x.x address.
- When requesting information from a web page, such as Computer Hope you enter a URL that is easy to understand and remember. In order for your computer to access the computer containing the pages that URL must be converted into an IP address, this is done with DNS. Once DNS has converted the URL into an IP address the routers on the Internet will know how to route your TCP/IP packet.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Cont..



Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Dial up Technology

- Dial up networking technology provides PCs and other network devices access to a LAN or WAN via standard telephone lines. Dial up Internet service providers offer subscription plans for home computer users.
- Dial-up Internet access is a form of Internet access that uses the facilities of the public switched telephone network (PSTN) to establish a dialled connection to an Internet service provider (ISP) via telephone lines. The user's computer or router uses an attached modem to encode and decode Internet Protocol packets and control information into and from analogue audio frequency signals, respectively.
- The term was coined during the early days of computer telecommunications when modems were needed to connect terminals or computers running terminal emulator software to mainframes, minicomputers, online services and bulletin board systems via a telephone line.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Cont..

- Dial-up connections to the Internet require no infrastructure other than the telephone network. Where telephone access is widely available, dial-up remains useful to travelers. Dial-up is often the only choice available for rural or remote areas, where broadband installations are not prevalent due to low population density, and high infrastructure cost. Dial-up access may also be an alternative for users on limited budgets, as it is offered free by some ISPs, though broadband is increasingly available at lower prices in many countries due to market competition.
- Dial-up requires time to establish a telephone connection (up to several seconds, depending on the location) and perform handshaking for protocol synchronization before data transfers can take place. In locales with telephone connection charges, each connection incurs an incremental cost. If calls are time-metered, the duration of the connection incurs costs. Dial-up access is a transient connection, because either the user, ISP or phone company terminates the connection.

Cont..

- Internet service providers will often set a limit on connection durations to allow sharing of resources, and will disconnect the user—requiring reconnection and the costs and delays associated with it. Technically-inclined users often find a way to disable the auto-disconnect program such that they can remain connected for days.

ISDN

- ISDN (Integrated Services Digital Network) is a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media. Home and business users who install an ISDN adapter (in place of a telephone modem) receive Web pages at up to 128 Kbps compared with the maximum 56 Kbps rate of a modem connection. ISDN requires adapters at both ends of the transmission so your access provider also needs an ISDN adapter. ISDN is generally available from your phone company in most urban areas in the United States and Europe. In many areas where DSL and cable modem service are now offered, ISDN is no longer as popular an option as it was formerly.
- There are two levels of service: the Basic Rate Interface (BRI), intended for the home and small enterprise, and the Primary Rate Interface (PRI), for larger users. Both rates include a number of B-channels and a D-channels. Each B channel carries data, voice, and other services. Each D-channel carries control and signalling information.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Cont..

- The Basic Rate Interface consists of two 64 Kbps B-channels and one 16 Kbps D- channel. Thus, a Basic Rate user can have up to 128 Kbps service. The Primary Rate consists of 23 B-channels and one 64 Kpbs D-channel in the United States or 30 B-channels and 1 D-channel in Europe.
- ISDN in concept is the integration of both analog or voice data together with digital data over the same network. Although the ISDN you can install is integrating these on a medium designed for analog transmission, broadband ISDN (BISDN) is intended to extend the integration of both services throughout the rest of the end-to-end path using fiber optic and radio media. Broadband ISDN encompasses frame relay service for high-speed data that can be sent in large bursts, the Fiber Distributed-Data Interface (FDDI), and the Synchronous Optical Network (SONET). BISDN is intended to support transmission from 2 Mbps up to much higher, but as yet unspecified, rates.

Leased Line Technology

- A leased line is a service contract between a provider and a customer, whereby the provider agrees to deliver a symmetric telecommunications line connecting two or more locations in exchange for a monthly rent (hence the term lease). It is sometimes known as a 'Private Circuit' or 'Data Line' in the UK or as CDN (Circuit Direct Number) in Italy. Unlike traditional PSTN lines it does not have a telephone number, each side of the line being permanently connected to the other. Leased lines can be used for telephone, data or Internet services. Some are ring down services, and some connect two PBXes.
- Leased lines are used by businesses to connect geographically distant offices. Unlike dial-up connections, a leased line is always active. The fee for the connection is a fixed monthly rate. The primary factors affecting the monthly fee are distance between end points and the speed of the circuit. Because the connection doesn't carry anybody else's communications, the carrier can assure a given level of quality.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Cont..

- An internet leased line is a premium internet connectivity product, delivered over fiber normally, which is dedicated and provides uncondensed, symmetrical speeds, Full Duplex. It is also known as an Ethernet leased line, DIA line, data circuit or private circuit.

VPN

- A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.
- Types of VPN
  - Site-to-site VPN
  - DMVPN
  - Client VPN
  - SSLVPN

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Site-to-site VPN

- A site-to-site virtual private network (VPN) is a connection between two or more networks, such as a corporate network and a branch office network. Many organizations use site-to-site VPNs to leverage an internet connection for private traffic as an alternative to using private MPLS circuits.
- Site-to-site VPNs are frequently used by companies with multiple offices in different geographic locations that need to access and use the corporate network on an ongoing basis. With a site-to-site VPN, a company can securely connect its corporate network with its remote offices to communicate and share resources with them as a single network.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

DMVPN

- A dynamic multipoint VPN is not a protocol but more a technique using different protocols. One or more central hub routers are required, but the remote (spoke) routers can have dynamic IPs and more can be added without having to modify the configuration on the hub router(s), or any other spoke routers. The routers use a next-hop resolution protocol, combined with a dynamic routing protocol to discover remote peers and subnets. The VPN itself is a mGRE tunnel (GRE with multiple endpoints) which is encrypted. This way, traffic between spoke routers does not have to go through the hub router but can be sent directly from spoke to spoke.

Client VPN

- A client VPN is an encrypted connection from one device towards a VPN router. It makes that one remote device appear as a member of a local subnet behind the VPN router. Traffic is tunneled from the device (usually a computer or laptop of a teleworker) towards the VPN router so that user has access to resources inside the company. It requires client software that needs to be installed and configured.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

SSLVPN

- This type of VPN works like a client VPN. The difference is that the remote client does not need preconfigured software, but instead the browser acts as VPN software. The browser needs to support active content, which every modern browser supports, either directly or through a plug-in. Traffic is tunneled over SSL (or TLS) to the SSLVPN router. From a networking perspective, traffic is tunneled over layer 4 instead of layer 3. The benefit is that the remote user does not need to configure anything and can simply log in to a web page to start the tunnel. The drawback that you'll likely need a dedicated device as SSLVPN endpoint because this is not a standard feature.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

VPN Protocols

- VPN protocols determine exactly how data is routed through a connection. These protocols have different specifications based on the benefits and desired circumstances; for example, some VPN protocols prioritize data throughput speed while others focus on masking or encrypting data packets for privacy and security.
- Types:
  - PPTP
  - L2TP/IPSec
  - OpenVPN

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

PPTP

- Point-to-Point Tunneling Protocol is one of the oldest VPN protocols in existence. Developed in the mid-90s by Microsoft, PPTP was integrated into Windows 95 and specifically designed for dial-up connections. But as technology advanced, PPTP's basic encryption was quickly cracked, compromising its underlying security. However, because it lacks many of the security features found in other modern protocols it can deliver the best connection speeds for users who may not need heavy encryption. But while PPTP is still used in certain applications, most providers have since upgraded to faster more reliable protocols.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

L2TP/IPSec

- Layer 2 Tunnel Protocol is a replacement of the PPTP VPN protocol. This protocol does not provide any encryption or privacy out-of-the-box and is frequently paired with security protocol IPsec. Once implemented, L2TP/IPsec is extremely secure and has no known vulnerabilities.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

OpenVPN

- OpenVPN is an open source protocol that allows developers access to its underlying code. This protocol has grown in popularity due to its use of (virtually unbreakable) AES-256 bit key encryption with 2048-bit RSA authentication and a 160-bit SHA1 hash algorithm.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Proxy Server

- During a HTTP connection, the IP address of the client machine is necessarily transmitted in order to get the information back. This allows a server to identify the source of the web request. Any resource you access can gather personal information about you through your unique IP address your ID in the Internet.
- They can monitor your reading interests, spy upon you and log your requests for third parties. Also, owners of the Internet resources may impose some restrictions on users from certain countries or geographical regions.
- An anonymous proxy server acts as a middleman between your browser and an end server. Instead of contacting the end server directly to get a web page, the browser contacts the proxy server, which forwards the request on to the end server. When the end server replies, the proxy server sends the reply to the browser.
- No direct communication occurs between the client and the destination server, therefore it appears as if the HTTP request originated from the intermediate server. The only way to trace the connection to the originating client would be to access the logs on the proxy server (if it keeps any). So an anonymous proxy server can protect your identity by stripping a request of all identifying information.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Firewall

- A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.
- **Packet filtering**
- A small amount of data is analysed and distributed according to the filter's standards.
- **Proxy service**
- Network security system that protects while filtering messages at the application layer.
- **Stateful inspection**
- Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.
- **Next Generation Firewall (NGFW)**
- Deep packet inspection Firewall with application-level inspection.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Firewall working

- A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Firewall need

- Firewalls, especially Next Generation Firewalls, focus on blocking malware and application-layer attacks. Along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls are able to react quickly and seamlessly to detect and combat attacks across the whole network. Firewalls can act on previously set policies to better protect your network and can carry out quick assessments to detect invasive or suspicious activity, such as malware, and shut it down. By leveraging a firewall for your security infrastructure, you're setting up your network with specific policies to allow or block incoming and outgoing traffic.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

GPS

- Global Positioning System was developed by the United States' GPS is often used by civilians as a navigation system. On the ground, any GPS receiver contains a computer that "triangulates" its own position by getting bearings from at least three satellites. The result is provided in the form of a geographic position - longitude and latitude - to, for most receivers, within an accuracy of 10 to 100 meters. Software applications can then use those coordinates to provide driving or walking instructions.
- Getting a lock on by the GPS receivers on the ground usually takes some time especially where the receiver is in a moving vehicle or in dense urban areas. The initial time needed for a GPS lock is usually dependent on how the GPS receiver starts. There are three types of start - hot, warm and cold.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Cont..

- The **hot** start is when the GPS device remembers its last calculated position and the satellites in view, the almanac used (information about all the satellites in the constellation), the UTC Time and makes an attempt to lock onto the same satellites and calculate a new position based upon the previous information. This is the quickest GPS lock but it only works if you are generally in the same location as you were when the GPS was last turned off.
- The **warm** start is when the GPS device remembers its last calculated position, almanac used, and UTC Time, but not which satellites were in view. It then performs a reset and attempts to obtain the satellite signals and calculates a new position. The receiver has a general idea of which satellites to look for because it knows its last position and the almanac data helps identify which satellites are visible in the sky. This takes longer than a hot start but not as long as a cold start.

Cont..

- the cold start is when the GPS device dumps all the information, attempts to locate satellites and then calculates a GPS lock. This takes the longest because there is no known information. The GPS receiver has to attempt to lock onto a satellite signal from any available satellites, basically like polling, which takes a lot longer than knowing which satellites to look for.
- This GPS lock takes the longest. In an attempt to improve lock times, cell phone manufacturers and operators have introduced the Assisted GPS technology, which downloads the current ephemeris for a few days ahead via the wireless networks and helps triangulate the general user‘s position with the cell towers thus allowing the GPS receiver to get a faster lock at the expense of several (kilo)bytes.

GPRS

- GPRS is a cellular networking service that supports WAP, SMS text messaging, and other data communications. GPRS technology is integrated into so-called 2.5G mobile phones designed to provide faster data transfer speeds than older 2G cellular networks. General packet radio service (GPRS) is a packet oriented mobile data service available to users of the 2G cellular communication systems global system for mobile communications (GSM), as well as in the 3G systems. In 2G systems, GPRS provides data rates of56-114kbit/s.
- GPRS data transfer is typically charged per megabyte of traffic transferred, while data communication via traditional circuit switching is billed per minute of connection time, independent of whether the user actually is using the capacity or is in an idle state. GPRS is a best-effort packet switched service, as opposed to circuit switching, where a certain quality of service (QoS) is guaranteed during the connection for non-mobile users.
- 2G cellular systems combined with GPRS are often described as 2.5G, that is, a technology between the second (2G) and third (3G) generations of mobile telephony.
- It provides moderate speed data transfer, by using unused time division multiple access (TDMA) channels in, for example, the GSM system. Originally there was some thought to extend GPRS to cover other standards, but instead those networks are being converted to use the GSM standard, so that GSM is the only kind of network where GPRS is in use. GPRS is integrated into GSM Release 97 and newer releases.
- It was originally standardized by European Telecommunications Standards Institute (ETSI), but now by the 3rd Generation Partnership Project (3GPP). GPRS was developed as a GSM response to the earlier CDPD and i-mode packet switched cellular technologies.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

CCTV Technology

- Closed-circuit television (CCTV) is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted, though it may employ point to point (P2P), point to multipoint, or mesh wireless links. Though almost all video cameras fit this definition, the term is most often applied to those used for surveillance in areas that may need monitoring such as banks, casinos, airports, military installations, and convenience stores. Videotelephony is seldom called "CCTV" but the use of video in distance education, where it is an important tool, is often so called.
- In industrial plants, CCTV equipment may be used to observe parts of a process from a central control room, for example when the environment is not suitable for humans. CCTV systems may operate continuously or only as required to monitor a particular event. A more advanced form of CCTV, utilizing digital video recorders[3] (DVRs), provides recording for possibly many years, with a variety of quality and performance options and extra features (such as motiondetection and email alerts). More recently, decentralized IP-based CCTV cameras, some equipped with megapixel sensors, support recording directly to network-attached storage devices, or internal flash for completely stand-alone operation. Surveillance of the public using CCTV is particularly common in many areas around the world

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli