ISSN No. 0976-5697

Volume 7, No. 1, January-February 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Understand and Curb Cybercrime by Understanding Computer Network Basics

Dr.P.B.Pathak
Assistant Professor & Head,
Department of Computer Science & Information Technology
Yeshwant Mahavidyalaya Nanded
Maharashtra, India

Abstract: Computer networks and Internet are proving to be a free playground for Cybercriminals to commit Cybercrimes. To prevent ourselves becoming victim of cybercrime and face the severe consequences we must understand computer network, its working and components both hardware and software. To understand computer networks we need to know of how data is converted to electrical or light pulses, is sent across wires and cables or over the airwaves, the processes used on the sending and receiving ends to prepare data for sending and to translate received data back into a form usable by applications and, ultimately, computer users. Once one gets acquainted with network basics can easily proceed to investigate exploit of computer network vulnerabilities by cybercriminals and safeguard ourselves. The present research paper discusses computer network basics, types, topologies, hardware and software and protocols.

Keywords: Computer Network; Hardware; Software; Topologies; Protocols Cybercrime; Cybercriminal

I. INTRODUCTION

Data broken into manageable chunks are packets, and are transmitted across a network for greater efficiency. The packet structure and size may vary, depending on the protocols in use. Network protocols are rules that govern the sending and receiving data. Networking models and specifications are developed as guidelines to ensure compatibility and bring about uniform standard in systems using different hardware and software platforms and can communicate with one another. The OSI and DoD models are layered to define specific tasks to be performed by protocols at different layers in the network communication process. At the physical level, each computer requires network interface, in the form of a network interface card (NIC). In complex network configurations, devices like hubs, switches, bridges, and routers operate at different levels to provide increased efficient connectivity. Gateways operate at the highest levels and provide translation between different protocols. Modern operating systems come with networking capabilities built in, and expensive server operating systems providing network services like authentication, name resolution, remote access, and ability to function as a router. Authentication servers provide centralized network security and management of resources.

Different operating system platforms rely on different file sharing protocols and authentication schemes, and needs interoperability due to heterogeneous nature of networks. Regardless of operating system or hardware platform, the majority of networks today run on the Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is the most routable protocol stack and thus the most appropriate for large routed networks; it is required for connecting to the Internet. There are various ways to network computers at the physical level using different types of media and different topologies. There are various methods of controlling access to the media and directing traffic at the data link level. There are diverse ways to handle addressing and routing of messages between computers at the network level. There are several methods for dealing with the transfer of data at the transport level. There are multiple protocols and file sharing mechanisms for computer communication at the higher levels.[1]

II. COMPUTER NETWORK BASICS

The Computer Network allows computers to share data, application programs, hardware peripherals, common authentication mechanism. The start of networking with sneakernet involved physically transporting the data, software, or hardware to the remote computer. Physical transportation can be avoided by connecting the computers via wires and cable so that data can be sent from one computer to another. Since all data processed by computers is ultimately reduced to binary bits 0 and 1, all network communication involves transmitting and receiving this binary data. This binary information can be sent across copper cables as electrical pulses, across optical fiber cable as pulses of light, or through the air as radio or microwave signals, infrared, or laser pulses. Irrespective of the medium, the signals represent the 0 and 1 that comprise all computer data. The process of transforming the 0 and 1 into these energy pulses is called signal encoding or signal modulation. There are a ample encoding methods. The signaling having two possible states off or on t representing two specific values 0 or 1, is called discrete state signaling. Digital signals are discrete state, whereas analog signals are non discrete state. Analog signals change state gradually, from one discrete state to another. Performance, cost effectiveness, reliability and security are advantages of digital transmissions over analog transmissions. Analog signals are generally easier to multiplex. Multiplexing is using a single link to send multiple streams, or channels, of information. Signals can be multiplexed in several different ways.

- Frequency Division Multiplexing (FDM): Different streams of information can be sent on separate frequencies. This method can be used for multiplexing analog signals.
- Time Division Multiplexing (TDM): Breaking of each signal into small pieces, and these are transmitted over the link one by other. This method can be used for multiplexing digital signals.
- Dense Wavelength Division Multiplexing (DWDM): If the transmission medium is fiber optical cable, light can be separated into different wavelengths, separate signals can be transmitted using separate wavelengths.

Depending on the signaling method, signals can travel in one direction only, unidirectional or in both directions, bidirectional. Bidirectional signals can either travel in both directions but not simultaneously or in both directions simultaneously. Following three different methods of signaling are identified as:

- Simplex Transmissions: These are unidirectional transmissions.
- Half-duplex Transmissions: These are bidirectional transmissions, but the signal can travel only one direction at a time.
- Full-duplex transmissions: These are bidirectional transmissions, and signal can travel simultaneously.

When a network adapter or other network device receives an incoming signal, it needs timing information to interpret the signals correctly called synchronization. There are two basic ways for synchronization and the transmission method is said to be either synchronous or asynchronous. The difference is as follows:

- Asynchronous: A start bit is included at the beginning of each message; this bit is used as a signal for the receiving device to synchronize its clock with that of the sending device.
- Synchronous: A timing mechanism built into the transmission synchronizes the clocks of the sending and receiving devices.

Signals represent individual bits, and group of bits forms bytes for convenience, but computers send data across the network in larger units like packets, segments, datagram's, or frames.

- A packet is a bunch of data.
- Segment: At the transport (TCP/IP) level, a unit of data is called a segment.
- Datagram: At the network (IP) level, the chunks of data are called datagram.
- Frame: At the data link level, the unit of data is called a frame.

When signals are transmitted on a network, a mechanism for directing traffic to ensure that all the data packets make it safely to their destinations, when multiple computers are sending signals, called the access control method. There are three popular access control methods contention methods, token passing, and polling methods. [2]

- Contention Methods: These include Carrier Sense Multiple Access Collision Detection (CSMA/CD), used in Ethernet networks, and Carrier Sense Multiple Access Collision Avoidance (CSMA/CA), used in Appletalk networks.
- Token-passing Methods: These eliminate the possibility of collision by using a circulating signal called a token to determine which computer can transmit.

Polling Methods: These are similar in some ways to token passing, except that instead of the group of computers policing it by passing around a token.

III. COMPUTER NETWORK TYPES

The Networks can be categorized in various ways. Broadly Networks may be classified either based on their physical scope or their architecture, standards and specifications. Networks classification based on their physical scope:

- Local Area Network (LAN): Limited to one geographic area.
- Wide Area Network (WAN): Limited locations in widely dispersed areas.
- Metropolitan Area Network (MAN): Limited to an area about the size of a typical city.

Networks classification based on their architecture, standards and specifications for type of media, physical and logical topology, access method, distance limitations, packet sizes, and headers and other criteria:

- Ethernet based on the CSMA/CD access method.
- Token Ring based on the token-passing access method.

A network protocol is a set of rules computers use to communicate with each other. Protocols are needed for two computers to understand one another, attempting to transfer data back and forth. The U.S. Department of Defense (DoD) developed the original networking model on which TCP/IP is based. Later, the International Organization for Standardization (ISO) refined and expanded on this model, creating the Open System Interconnection (OSI) model.

The OSI Networking Model: The OSI model consists of seven layers. The data is passed from one layer to the next layer below it at the sending computer, until the physical layer finally puts the data out onto the network cable. At the receiving end, the data travels back up the stack in reverse order. Though the data travels down the layers on one side of the transmission and up the layers on the other, the logical communication link is between each layer and its matching peer. As the data propagates down through the layers, it is encapsulated, within a larger unit, as each layer adds its own header information. When the encapsulated data reaches the receiving computer, the process occurs in exactly reverse; the information is passed upward through each layer, and as it travels, the encapsulation information is stripped off, one layer at a time. After processing, each layer removes the header information that was added by its corresponding layer on the sending side. When the application layer finally presents the incoming data to the user application at the receiving computer, the data is once again in approximately the same form it was in when sent by the user application at the originating machine.

- Physical layer interacts with the hardware to provide the actual stream of bits as signals at the electrical and mechanical levels.
- Data link layer is divided into two sub layers: media access control (MAC), which handles how computers access and transmit data on the network, and logical link control (LLC), which handles frame synchronization, flow control, and error checking at the link level.
- Network layer handles routing and switching using logical addresses by creating virtual circuits. Responsible for congestion control and packet sequencing.
- Transport layer provides for transfer of data between hosts; handles acknowledgment, error checking, and recovery and flow control.
- Session layer establishes, manages, and terminates connections between applications at each end.
- Presentation layer deals with heterogeneousness in the way data is represented, translating from application to network format or vice versa.
- Application layer supports application and end user processes; provides services for file transfer, e-mail, and other network software services.

The TCP/IP Networking Model: The TCP/IP Networking Model consists of only four layers. The TCP/IP Model layers can be roughly mapped to layers of the OSI model. Various protocols in the TCP/IP suite fit nicely into the layers of the

TCP/IP model. The TCP/IP model was designed prior OSI model. [2,3]

- The Application/Process Layer: The top layer of the TCP/IP model encompasses all three OSI upper layers: application, presentation, and session.
- The Host to Host (Transport) Layer: The host to host layer maps to the transport layer on the OSI model. TCP, User Datagram Protocol (UDP), and DNS operate here.
- The Internetworking Layer: The internetworking layer corresponds closely to the OSI's network layer. IP, Internet Control Message Protocol (ICMP), and Address Resolution Protocol (ARP) function at this layer. IP deals with routing based on logical IP addresses. ARP translates logical addresses to MAC addresses. This translation is necessary since the lower layers can process only the MAC addresses.

The Network Interface Layer: The network interface layer maps to OSI's data link and physical layers. The TCP/IP suite itself has no protocols that operate at these lower layers but uses the standard Ethernet and Token Ring data link and physical layer protocols.

IV. COMPUTER NETWORK TOPOLOGIES

Wherever The network topology is the way in which the nodes of a network are linked together. It determines the data paths that may be used between any pair of nodes in the network. Though the number of possible network topologies is in bundle, the major ones are the: [4,11]

- Star Topology: All computers attach to a central point called hub. Many home networks use the star topology. All traffic originates from the hub of the star. The central site is in control of all the nodes attached to it. The central hub is usually a fast, self-contained computer and is responsible for routing all traffic to other nodes. A failure in any star network cable will only take down one computer's network access and not the entire LAN. If the hub fails, the entire network also fails.
- Ring Topology: Computers connected in a closed loop. Every device has exactly two neighbors for communication purposes. First passes data to second, second passes data to third, and so on. All messages travel through a ring in the same direction either clockwise or anticlockwise. A failure in any cable or device breaks the loop and can take down the entire network.
- Bus Topology: Use a common backbone to connect all devices. A single cable, functions as a shared communication medium that devices attach with an interface connector. A device interested to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message. If the backbone cable fails, the entire network effectively becomes unusable.
- Tree Topology: Also known as the Hierarchical topology, the tree topology is a combination of bus and star topologies. This bus and star hybrid approach supports future expandability of the network much better than a bus or a star alone. They are very common in larger networks.

Mesh Topology: Involve the concept of routes. Messages sent on a mesh network can take any of several possible paths from source to destination. Some WANs, employ mesh routing. A mesh network in which every device connects to every other is called a full mesh. Partial mesh networks also exist in which some devices connect only indirectly to others.

V. COMPUTER NETWORK HARDWARE

The network interface card (NIC) is the hardware device most essential for establishing communication between computers. The NIC is responsible for preparing the data to be sent over the network media. The network media are the wires and cable or wireless technologies on which the signal is sent. Cable types include thin and thick coaxial cable, twisted pair cable, or fiber optic cable. Wireless media include radio waves, laser, infrared, and microwave. Network connectivity devices connect two or more segments of cable. Complex connectivity devices can serve two seemingly opposite purposes, they are used to divide large networks into smaller parts called subnets, and they are used to combine small networks into a larger network called an internetwork.

Hubs and Repeaters: Hubs and Repeaters are connection devices. Repeaters connect two network segments and boost the signal so the distance of the cabling can be extended past the normal limits at which attenuation, or weakening, interferes with the reliable transmission of the data. Hubs can be categorized as follows:

- Passive hubs: These hubs serve as connection points only; they do not boost the signal. Passive hubs do not require electricity.
- Active hubs: These hubs serve as both a connection point and a signal booster. Data that comes in is passed back out on all ports. Active hubs require electrical power.
- Intelligent or Smart hubs: These are active hubs that include a microprocessor chip with diagnostic capabilities so that you can monitor the transmission on individual ports.
- Switching hubs: These hubs operate at the data link rather than the physical layer and are a switch.

Bridges: Bridges operate at the data link layer of the OSI model. Bridges can separate a network into segments, but they don't subnet the network.

Switches: Switches, or switching hubs, work at the data link layer, and they are installed in place of the active hubs that have been more typically used to connect computers on a UTP cabled network.

Routers: Routers are multiport connectivity devices. Routers are appropriate for use on large, complex networks because they are able to use the logical IP address to determine where packets need to go. [5,10]

VI. COMPUTER NETWORK SOFTWARE

The term network operating system (NOS) is used in three different ways:

- It is used to refer to any computer operating system that has built in networking components, as do all of today's popular operating systems.
- It is used to refer to the components of the operating system that make networking possible. These components, along with the protocol stacks on which the network operates, are sometimes referred to as the NOS.
- It is used to refer to the server operating system software, especially when functioning as an

authentication server that maintains a security accounts database for the network.

Client/Server Computing: The term client/server computing has different meanings, depending on the context in which it is used like applications in which the bulk of the processing is performed on a server and system in which database files are stored on a server, but a client query results in the entire file being transferred to the client machine, where the storing takes place.

Authentication Server-Based Networks: When a user wants to log onto the network, the client computer contacts this authentication server. The server checks its database to ensure that the user is authorized and to determine the level of access allowed that user. The authentication server is a centralized point of security and network resource management and must run special server software.

Peer to Peer Networks: Networks without an authentication server are called workgroups or peer to peer networks. This model is appropriate for small networks with only a few computers, in environments where high security is not required. In a workgroup, all computers can provide both client and server services.

Server Software: Server software is operating systems capable of providing network authentication services. There are also many server applications that can be installed only on a system running a server operating system.

Client Software: Most modern operating systems can also function as network clients. Client machines don't necessarily have to run an operating system made by the vendor of the network's server software.

Network File Systems and File Sharing Protocols: Network file systems and file sharing protocols allow users to access and update files on remote computers as though they were on the local computer. They can make different file systems on the remote machine irrelevant when accessing that machine's resources across the network. Network File System (NFS) is a client/server application developed by Sun Microsystems that runs on TCP/IP to allow remote file access. NFS uses the Remote Procedure Call (RPC) communication method. [6,2]

VII. COMPUTER NETWORK PROTOCOLS (TCP/IP)

Network communication to take place between computers it is necessary that the computers must be running a same network protocol. Protocols are simply sets of rules that govern the communication process. Networking protocols generally work together in protocol stacks or suites. A stack is two or more protocols working at different layers of the OSI or TCP/IP model. TCP and IP form a protocol stack, with TCP working at the transport layer and IP working at the network layer. A suite includes additional protocols such as the application-layer File Transfer Protocol (FTP) and Telnet protocols included in the TCP/IP suite. The most popular protocol stack today is TCP/IP, primarily because it is the protocol of the Internet and any computer that connects to the Internet must have TCP/IP installed. TCP/IP uses an addressing scheme that makes it extremely routable and suitable for the largest networks. It can also be run on the smallest networks. TCP/IP is the networking protocol stack of choice for most of today's networks.

TCP/IP on the Internet: The TCP/IP is a familiar, networking component to most modern network administrators and information technology professionals. Business networks need such a powerful but high overhead set of protocols like TCP/IP.

IP and IP Addressing: One of TCP/IP's great strengths and a primary reason that it has become the standard for large networks, including the Internet is its scalable addressing scheme, which can accommodate networks of all sizes. In order to communicate over a network using the TCP/IP protocols, a computer must have an IP address that is unique on that network. The IP address can be manually assigned by a network administrator or it can be automatically assigned by an automatic addressing service. In any event, there will be no IP communication without an address. IP specifications became standardized; a two level hierarchical addressing structure was imposed, consisting of the network ID and the host ID. Networks are divided into classes A, B, and C. This is referred to as classful addressing. A newer method of identifying networks via an IP prefix is called classless inter domain routing (CIDR).

Logical IP and Physical MAC Addresses: The IP address is a logical address assigned by the network administrator. It bears no direct relation to the network interface cards physical address or MAC address. Changing a computers IP address is a software function. If you have administrative privileges, it's as simple as clicking the mouse a few times to open the proper dialog box and typing in a new number. The MAC address is hardcoded into the chip on the network card in the typical Ethernet network. Some network cards provide a way to change the MAC address via jumper settings or by flashing the chip with special software, but in most cases, the MAC address stays the same.

- Static Addressing: This works fine when the network is small and is necessary when you have computers that need always the same IP address.
- Automatic Addressing: With very large networks, Automatic address assignment can be done by a server running the Dynamic Host Configuration Protocol (DHCP) service.

Routing: Computers on an internetwork exchange packets between one another in one of the two ways:

- Directly if the source and destination computers are on the same subnet.
- Indirectly if the source and destination computers are on different subnets by forwarding the packets to a router.

IP routing refers to forwarding of packets from a source computer to a destination computer by going through routers that support IP routing. Every computer has a routing table. A gateway address is listed there for each network number, and the gateway is used to reach that network. The gateway doesn't have to connect directly to the destination network; it is just the starting point. Each gateway, or router, that the message must go through is called a hop. At each router, the destination IP address on the packet is compared to the routing table, and the best route is used to decide the endpoint of the next hop. Typically, a router is connected to two or more networks or subnets. The router, a dedicated device or a computer acting as a router, an interface to each network to which it is connected. Routing comes in two basic flavors, static and dynamic. [12,9]

- Static Routing: With static IP routing, the routing table must be constructed manually; an administrator must enter the IP addresses defining the routes to remote networks one by one. Static routing not only requires that you painstakingly set up the routing table; you also must manually enter every change, addition, and deletion that occurs. This reprogramming of the routers each time a change is made can be time consuming and tedious.
- Dynamic Routing: Using a dynamic routing protocol, the table is configured and maintained automatically because the dynamic router can communicate with

and learn from other routers on the network. This system saves the administrator a great deal of time. Two popular dynamic routing protocols are the, Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

The Transport Layer Protocols: The TCP/IP protocols that operate at the transport layer of the OSI model are the TCP and the UDP. These two protocols provide two different types of connection services: connection oriented and connectionless respectively.

- Connection Oriented Services: TCP first establishes a virtual connection between the sending and receiving computers. This is done through the use of acknowledgments and response messages.
- Connectionless Services: A connectionless transport protocol like UDP doesn't provide the service of dividing a message into packets and reassembling it at the other end so an application program that uses UDP has to be able to make sure that the entire message has arrived and is in the right order. To save processing time, network applications may use UDP instead of TCP.

TCP/IP is the common abbreviation used for the protocol suite which consists of the IP, the TCP and the UDP. All applications used on the Internet rely on either IP in combination with TCP or IP along with UDP. Today an ever growing number of systems are connected through the Internet and not all of them are playing along nicely. So it arise need of securing communications from eavesdropping and disruption. [7, 8]

VIII. CONCLUSION

The globalization has given rise to expanded criminal activity. Cybercrime has cross border dimensions and global implications. Networked technologies have created ample opportunities for criminal activity. There are various reasons for the rise in Cybercrimes like Global reach of the Internet, Lack of Information Security Management initiatives, Lack of awareness of Security Threats and Vulnerabilities, Misconception that only Firewalls and Antivirus Software's are adequate, Solid Information Security Policies and Procedures, Increasing Complexity of our Information Systems, Software written without security in mind, Lack of Information Security Integration into software projects, Widespread availability of attack scripts source code on the Internet, Ease of carrying out attacks, Poor chances of getting caught committing a Cybercrime due to kind of Anonymity provided by Computers and the Internet. Study of basics of Computer Networks will help us understand and curb Cybercrime.

IX. REFERENCES

[1] Windows 2000 Resource Kit "Internet Protocol Security.", http://www.microsoft.com

[2] Debra Littlejohn Shinder "Scene Of Cybercrime: Computer Forensics Handbook"

[3] Bluefire Security Technologies. (2003) "Mobile insecurity: A practical guide to threats and vulnerabilities." http://www.bluefiresecurity.com

[4] Jupitermedia Corporation. (2003). PDA security 101. http://www.intranetjournal.com

[5] Lyon D. M. (2002). "The dilemma of PDA security: An overview" (SANS Institute)

[6] Ben-Itzhak Y. (2009) "Organised cybercrime and payment cards", Card Technology Today

[7] Pfleeger, Charles P., and Pfleeger, Shari Lawrence (2003). "Security in Computing" – 3rd Edition. Upper Saddle River, NJ: Prentice Hall.

[8] W. Jansen and K. Scarfone (2008.) "Computer security, guidelines on cell phone and PDA security." Technical report, NIST- National Institue of standards and Technology, US Department of Comerce. Special Publication

[9] Cybercrime and Steganography Resources Website. "Computer forensics and steganography and data hiding" http://www.forensics.nl

[10] Anat H & John D. A. (2003) "The impact of denial-of-service attack announcements on the market value of firms." Risk Management and Insurance Review.

[11] Hlavaty P. (2003) "The Risk Involved With Open and Closed Public Key Infrastructure" SANS Institute. http://www.sans.org

[12] Rae A & Wildman L (2003). "A Taxonomy of Attacks on Secure Devices." Proceedings of the Australia Information Warfare and Security Conference 2003. Adelaide: Australia.