International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XI, Nov 2018- Available at www.ijraset.com

A Study & Brief Description on Communication Systems, Wireless Network and Network Security

K. B. Mohd. Umar Ansari[1], Abhinaw Kumar Tripathi[2], Manjeet Singh[3]
[1]*MTech (Electrical Power & Energy Systems), Ex- Engineer, GET, Tata Motors Limited, IIE, Sidcul, Rudrapur, Pantnagar, UK, India.*
[2]*BTech (IT), Engineer (IT Administrator), Northern Express Infra Developers Pvt. Ltd., Gomti Nagar, Lucknow, Uttar Pradesh, India.*
[3]*BTech (Electrical & Electronics Engg.), Ex-Engineer, PE, Flowmore Limited, Sahibabad, Ghaziabad, Uttar Pradesh, India.*

Abstract: Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become ``wired'', an increasing number of people need to understand the basics of security in a networked world.
This document was written with the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them.
Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor.
The most common wireless technologies use electromagnetic wireless telecommunications, such as radio. With radio waves distances can be short, such as a few metres for television remote control, or as far as thousands or even millions of kilometres for deep-space radio communications.
It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking.
Keywords: Communication, Communication systems, Network security, Networking devices, Topologies, Wireless network, Wireless Technology.

I. INTRODUCTION

Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together.

A. What is a Network?

A network has been defined as any set of interlinking lines resembling a net, a network of roads an interconnected system, a network of alliances.

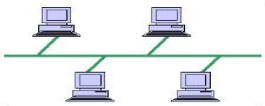
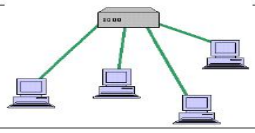
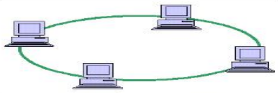
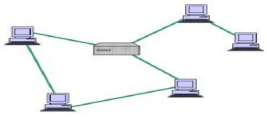
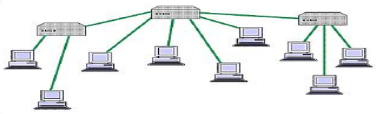
B. The ISO/OSI Reference Model

The International Standards Organization (ISO) Open Systems Interconnect (OSI) Reference Model defines seven layers of communications types, and the interfaces among them. (See Figure 1.) Each layer depends on the services provided by the layer below it, all the way down to the physical network hardware, such as the computer's network interface card, and the wires that connect the cards together.
The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the
internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO).

7	**APPLICATION LAYER** (Network Process to Application)	Data
6	**PRESENTATION LAYER** (Data Representation & Encryption)	Data
5	**SESSION LAYER** (Inter-host Communication)	Data
4	**TRANSPORT LAYER** (End-to-end connections & reliability)	Segments
3	**NETWORK LAYER** (Path Determination and IP)	Packets
2	**DATA LINK LAYER** (Physical Addressing)	Frames
1	**PHYSICAL LAYER** (Media, Signal and Binary Transmission)	Bits

Fig. 1. ISO Reference Model

1) *Network topology* is the arrangement of the various elements (links, nodes, etc.) of a computer network. There are two basic categories of network topologies: Physical topologies and Logical topologies.
2) *Physical topology* is the placement of the various components of a network, including device location andcable installation, while
3) *Logical topology* illustrates how data flows within a network, regardless of its physical design. Various types of topologies are:

Bus Topology		Every computer and network device is connected to single cable.
Star Topology		All the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.
Ring Topology		Each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.
Mesh Topology		It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other
Tree Topology		It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology.

4) *Hybrid topology* uses a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies.
5) *Cloud computing* is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand.
6) *Public clouds* are owned and operated by companies that offer rapid access over a public network to affordable computing resources.
7) *A private cloud* is infrastructure operated solely for a single organization, whether managed internally or by a third party, and hosted either internally or externally.
8) *A hybrid cloud* uses a private cloud foundation combined with the strategic integration and use of public cloud services. Google Drive is a personal cloud storage service from Google which gives every user 15 GB of Drive storage space. OneDrive is Microsoft's service for hosting files in the "cloud computing". OneDrive offers 5GB of storage space for free.

II. WHAT IS NETWORK SECURITY?

The networks are computer networks, both public and private, that are used every day to conduct transactions and communications among businesses, government agencies and individuals. The networks are comprised of "nodes", which are "client" terminals (individual user PCs) and one or more "servers" and/or "host" computers. They are linked by communication systems, some of which might be private, such as within a company, and others which might be open to public access. The obvious example of a network system that is open to public access is the Internet, but many private networks also utilize publicly-accessible communications. Today, most companies' host computers can be accessed by their employees whether in their offices over a private communications network, or from their homes or hotel rooms while on the road through normal telephone lines.

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

A. Comparison With Information Security

The terms network security and information security are often used interchangeably, however network security is generally taken as providing protection at the boundaries of an organization, keeping the bad guys (e.g. hackers, script kiddies, etc.) out. Network security systems today are mostly effective, so the focus has shifted to protecting resources from attack or simple mistakes by people inside the organization, e.g. with Digital Leak Protection (DLP). One response to this insider threat in network security is to compartmentalize large networks, so that an employee would have to cross an internal boundary and be authenticated when they try to access privileged information. Information security is explicitly concerned with all aspects of protecting information resources, including network security and DLP.

B. Network Security Concepts

Network security starts from authenticating any user, most likely a username and a password. Once authenticated, a stateful firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the network. An intrusion prevention system (IPS) helps detect and prevent such malware. IPS also monitors for suspicious network traffic for contents, volume and anomalies to protect the network from attacks such as denial of service. Communication between two hosts using the network could be encrypted to maintain privacy. Individual events occurring on the network could be tracked for audit purposes and for a later high level analysis. Honey pots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis could be used to further tighten security of the actual network being protected by the honey pot. A useful summary of standard concepts and methods in network security is given by in the form of an extensible ontology of network security attacks.

1) Threats To Network Security Include Viruses, Trojan Horse Programs, Vandals, Attacks, Etc

a) Viruses: Computer programs written by devious programmers and designed to replicate themselves and infect computers when triggered by a specific event

b) Trojan Horse Programs: Delivery vehicles for destructive code, which appear to be harmless or useful software programs such as games

c) Vandals: Software applications or applets that cause destruction.

d) Attacks: Including reconnaissance attacks (information-gathering activities to collect data that is later used to compromise networks); access attacks (which exploit network vulnerabilities in order to gain entry to e-mail, databases, or the corporate network); and denial-of-service attacks (which prevent access to part or all of a computer system).

e) Data interception: Involves eavesdropping on communications or altering data packets being transmitted

f) Social engineering : Obtaining confidential network security information through nontechnical means, such as posing as a technical support person and asking for people's passwords

2) Network Security Tools Includes Packages, Services, Security Management, Secure Network Infrastructure

a) Antivirus Software Packages: These packages counter most virus threats if regularly updated and correctly maintained.

b) Secure Network Infrastructure: Switches and routers have hardware and software features that support secure connectivity, perimeter security, intrusion protection, identity services, and security management. Dedicated network security hardware and

software-Tools such as firewalls and intrusion detection systems provide protection for all areas of the network and enable secure connections.

c) *Virtual Private Networks:* These networks provide access control and data encryption between two different computers on a network. This allows remote workers to connect to the network without the risk of a hacker.

d) *Identity Services:* These services help to identify users and control their activities and transactions on the network. Services include passwords, digital certificates, and digital authentication keys.

e) *Encryption:* Encryption ensures that messages cannot be intercepted or read by anyone other than the authorized.

f) *Security Management:* This is the glue that holds together the other building blocks of a strong security solution. Security Management for networks is different for all kinds of situations. A small home or an office would only require basic security while large businesses will require high maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

III. WIRELESS NETWORK

Wireless network refers to any type of computer network that uses wireless (usually, but not always radio waves) for network connections. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.

1) *Types of wireless networks:* Different types of network are: LAN, MAN and WAN.
2) *A LAN (local area network)* is a group of computers and network devices connected together, usually within the same building. By definition, the connections must be high speed and relatively inexpensive (e.g., token ring or Ethernet).
3) *A MAN (metropolitan area network)* is a larger network that usually spans several buildings in the same city or town.
4) *A WAN (wide area network),* in comparison to a MAN, is not restricted to a geographical location, although it might be confined within the bounds of a state or country. A WAN connects several LANs, and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive. The Internet is an example of a worldwide public WAN.
5) *A personal area network (PAN)* is a computer network used for data transmission amongst devices such as computers, telephones, tablets and personal digital assistants.
6) *Campus Area Network or corporate area network* is a computer network made up of an interconnection of local area networks (LANs) within a limited geographical area.
7) *A Storage Area Network (SAN)* is a specialized, high-speed network that provides block-level network access to storage.
8) *A virtual private network (VPN)* extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network
9) *Networking Devices*
10) *Modem:* Modem stands for Modulator-Demodulator. It is used to connect computers for communication via telephone lines.
11) *Hub:* It works at the Physical layer. It just acts like a connector of several computers i.e. simply connects all the devices on its ports together. It broadcasts all the data packets arriving at it with no filtering capacity.
12) *Switch:* It works at the Data Link Layer. It is used for dividing a network into segments called subnets. It provides filtering of data packets and prevents network traffic also.
13) *Repeater:* It operates at the Physical Layer. It is used to amplify a signal that has lost its original strength so as to enable them to travel long distances.
14) *Router:* It works at the Network Layer and is used to connect different networks that have different architectures and protocols. It sends the data packets to desired destination by choosing the best path available thus reducing network traffic.
15) *Gateway:* It operates in all the layers of the network architecture. It can be used to connect two different networks having different architectures, environment and even models.
16) *Bridge:* They are used two connect two LANs with the same standard but using different types of cables. It provides an intelligent connection by allowing only desired messages to cross the bridge thus improving performance. It uses physical addresses of the packets for this decision.

IPv4 - 32 bits numeric address
IPv6 - 128 bits hexadecimal address

IPv6 does not use broadcast messages and has three types of addresses, which are categorized as :
Unicast addresses. A packet is delivered to one interface.
Multicast addresses. A packet is delivered to multiple interfaces.
Anycast addresses. A packet is delivered to the nearest of multiple interfaces (in terms of routing distance).
With an IPv4 IP address, there are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used. Each class allows for a particular range of valid IP addresses. Class D is reserved for multicast groups and Class E is reserved for future use, or Research and Development Purposes.

17) *Data Communication* deals with the transmission of digital data from one device to another. Data is transferred through a pathway called as communication channel which can be physical wire connecting the devices or may be unguided media like laser, microwave etc. A communication channel has a source or transmitter at one side and a designation or receiver at another side of the network. The source of data origination is single but there may be multiple receivers. A communication channel is of 3 types:
18) *Simplex:* This, communication is unidirectional i.e. one of the two devices can transmit the data and the other can only receive the data. For e.g. Radio broadcasting, television broadcasting etc.
19) *Half duplex:* This communication is bidirectional. Either of the devices can act as transmitter or receiver but only one device can transmit the data at one time. For e.g. Walkie-Talkie.
20) *Full Duplex:* Here the communication is in both directions and both the devices can simultaneously transmit the data. For e.g. Telephone conversation.

A. *Cellular network*

A cellular network or mobile network is a radio network distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station. In a cellular network, each cell characteristically uses a different set of radio frequencies from all their immediate neighbouring cells to avoid any interference.

B. *Modes*

Wireless communications can be via

1) radio communication,
2) microwave communication, for example long-range line-of-sight via highly directional antennas, or short-range communication,
3) Light, visible and infrared (IR) for example consumer IR devices such as remote controls or via Infrared Data Association (IrDA).
4) sonic, especially ultrasonic short range communication
5) electromagnetic induction short range communication and power
6) Wi-Fi technology.

C. *Cordless*

The term "wireless" should not be confused with the term "cordless", which is generally used to refer to powered electrical or electronic devices that are able to operate from a portable power source (e.g., a battery pack) without any cable or cord to limit the mobility of the cordless device through a connection to the mains power supply.
Some cordless devices, such as cordless telephones, are also wireless in the sense that information is transferred from the cordless telephone to the telephone's base unit via some type of wireless communications link. This has caused some disparity in the usage of the term "cordless", for example in Digital Enhanced Cordless Telecommunications.

D. *Applications Of Wireless Technology*

1) *Mobile Telephones:* One of the best-known examples of wireless technology is the mobile phone, also known as a cellular phone, with more than 4.6 billion mobile cellular subscriptions worldwide as of the end of 2010. These wireless phones use radio waves to enable their users to make phone calls from many locations worldwide. They can be used within range of the mobile telephone site used to house the equipment required to transmit and receive the radio signals from these instruments.
2) *Wireless data Communications:* Wireless data communications are an essential component of mobile computing. The various available technologies differ in local availability, coverage range and performance, and in some circumstances, users must be

able to employ multiple connection types and switch between them. To simplify the experience for the user, connection manager software can be used, or a mobile VPN deployed to handle the multiple connections as a secure, single virtual network. Supporting technologies include:

Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to the Internet. Standardized as IEEE 802.11 a,b,g,n, Wi-Fi approaches speeds of some types of wired Ethernet. Wi-Fi has become the de facto standard for access in private homes, within offices, and at public hotspots. Some businesses charge customers a monthly fee for service, while others have begun offering it for free in an effort to increase the sales of their goods.

Cellular data service offers coverage within a range of 10-15 miles from the nearest cell site. Speeds have increased as technologies have evolved, from earlier technologies such as GSM, CDMA and GPRS, to 3G networks such as W-CDMA, EDGE or CDMA2000. Mobile Satellite Communications may be used where other wireless connections are unavailable, such as in largely rural areas or remote locations. Satellite communications are especially important for transportation, aviation, maritime and military use.

E. Wireless Energy Transfer

Wireless energy transfer is a process whereby electrical energy is transmitted from a power source to an electrical load that does not have a built-in power source, without the use of interconnecting wires.

F. Computer Interface Devices

Answering the call of customers frustrated with cord clutter, many[] manufacturers of computer peripherals turned to wireless technology to satisfy their consumer base. Originally these units used bulky, highly limited transceivers to mediate between a computer and a keyboard and mouse; however, more recent generations have used small, high-quality devices, some even incorporating Bluetooth. These systems have become so ubiquitous that some users have begun complaining about a lack of wired peripherals. Wireless devices tend to have a slightly slower response time than their wired counterparts; however, the gap is decreasing. Concerns about the security of wireless keyboards arose at the end of 2007, when it was revealed that Microsoft's implementation of encryption in some of its 27 MHz models was highly insecure.

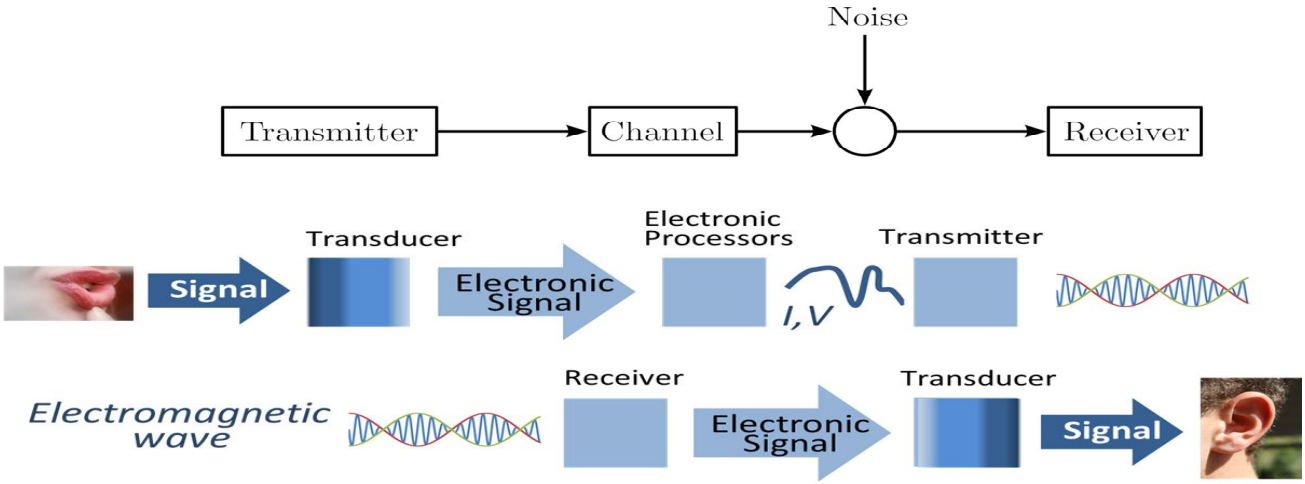
G. Categories Of Wireless Implementations, Devices And Standards

1) Radio communication system
2) Broadcasting
3) Amateur radio
4) Land Mobile Radio or Professional Mobile Radio: TETRA, P25, OpenSky, EDACS, DMR, dPMR
5) Cordless telephony:DECT (Digital Enhanced Cordless Telecommunications)
6) Cellular networks: 0G, 1G, 2G, 3G, Beyond 3G (4G), Future wireless
7) List of emerging technologies
8) Short-range point-to-point communication: Wireless microphones, Remote controls, IrDA, RFID (Radio Frequency Identification), TransferJet, Wireless USB, DSRC (Dedicated Short Range Communications), EnOcean, Near Field Communication.
Wireless sensor networks: ZigBee, EnOcean; Personal area networks, Bluetooth, TransferJet, Ultra-wideband (UWB from WiMedia Alliance).
9) Wireless networks: Wireless LAN (WLAN), (IEEE 802.11 branded as Wi-Fi and HiperLAN), Wireless Metropolitan Area Networks (WMAN) and (LMDS, WiMAX, and HiperMAN).

IV. COMMUNICATION SYSTEMS

In telecommunication, a communications system is a collection of individual communications networks, transmission systems, relay stations, tributary stations, and data terminal equipment (DTE) usually capable of interconnection and interoperation to form an integrated whole. The components of a communications system serve a common purpose, are technically compatible, use common procedures, respond to controls, and operate in unison. Telecommunications is a method of communication (e.g., for sports broadcasting, mass media, journalism, etc.).

Communication is the act of conveying intended meanings from one entity or group to another through the use of mutually understood signs and semiotic rules.



1) *Examples:* An optical communication system is any form of telecommunication that uses light as the transmission medium. Equipment consists of a transmitter, which encodes a message into an optical signal, a channel, which carries the signal to its destination, and a receiver, which reproduces the message from the received optical signal. Fiber-optic communication systems transmit information from one place to another by sending light through an optical fiber. The light forms an electromagnetic carrier wave that is modulated to carry information. A radio communication system is composed of several communications subsystems that give exterior communications capabilities. A radio communication system comprises a transmitting conductor[4] in which electrical oscillations or currents are produced and which is arranged to cause such currents or oscillations to be propagated through the free space medium from one point to another and a receiving conductor at distant point adapted to be excited by the oscillations or currents propagated from the transmitter. A duplex communication system is a system composed of two connected parties or devices which can communicate with one another in both directions. The term *duplex* is used when describing communication between two parties or devices. Duplex systems are employed in nearly all communications networks, either to allow for a communication "two-way street" between two connected parties or to provide a "reverse path" for the monitoring and remote adjustment of equipment in the field.

A. Examples of communications subsystems include the defense communications system (dcs).

A tactical communications system is a communications system that (a) is used within, or in direct support of, tactical forces, (b) is designed to meet the requirements of changing tactical situations and varying environmental conditions, (c) provides securable communications, such as voice, data, and video, among mobile users to facilitate command and control within, and in support of, tactical forces, and (d) usually requires extremely short installation times, usually on the order of hours, in order to meet the requirements of frequent relocation.

An Emergency communication system is any system (typically computer based) that is organized for the primary purpose of supporting the two way communication of emergency messages between both individuals and groups of individuals. These systems are commonly designed to integrate the cross-communication of messages between are variety of communication technologies.

V. CONCLUSION

Future wireless networks will need to support diverse IP multimedia applications to allow sharing of resources among multiple users. There must be a low complexity of implementation and an efficient means of negotiation between the end users and the wireless infrastructure. The fourth generation promises to fulfill the goal of PCC (personal computing and communication) a vision that affordably provides high data rates everywhere over a wireless network. The provision of megabit/s data rates to thousands of radio and mobile terminals per square kilometer presents several challenges. The key enablers are:

1) Sufficient spectrum, with associated sharing mechanisms.
2) Coverage with two technologies: parent (2G, 3G, and WiMAX) for real-time delivery, and discontinuous Pico cell for high data rate delivery.
3) Fixed-mobile convergence (for indoor service).
4) Network selection mechanisms.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XI, Nov 2018- Available at www.ijraset.com

REFERENCES

[1] Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257
[2] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317–323.
[3] "Introduction to Network Security". Interhack.net. Retrieved 2011-12-09.
[4] Hansell, Clarence W., U.S. Patent 2,389,432, "Communication system by pulses through the Earth".