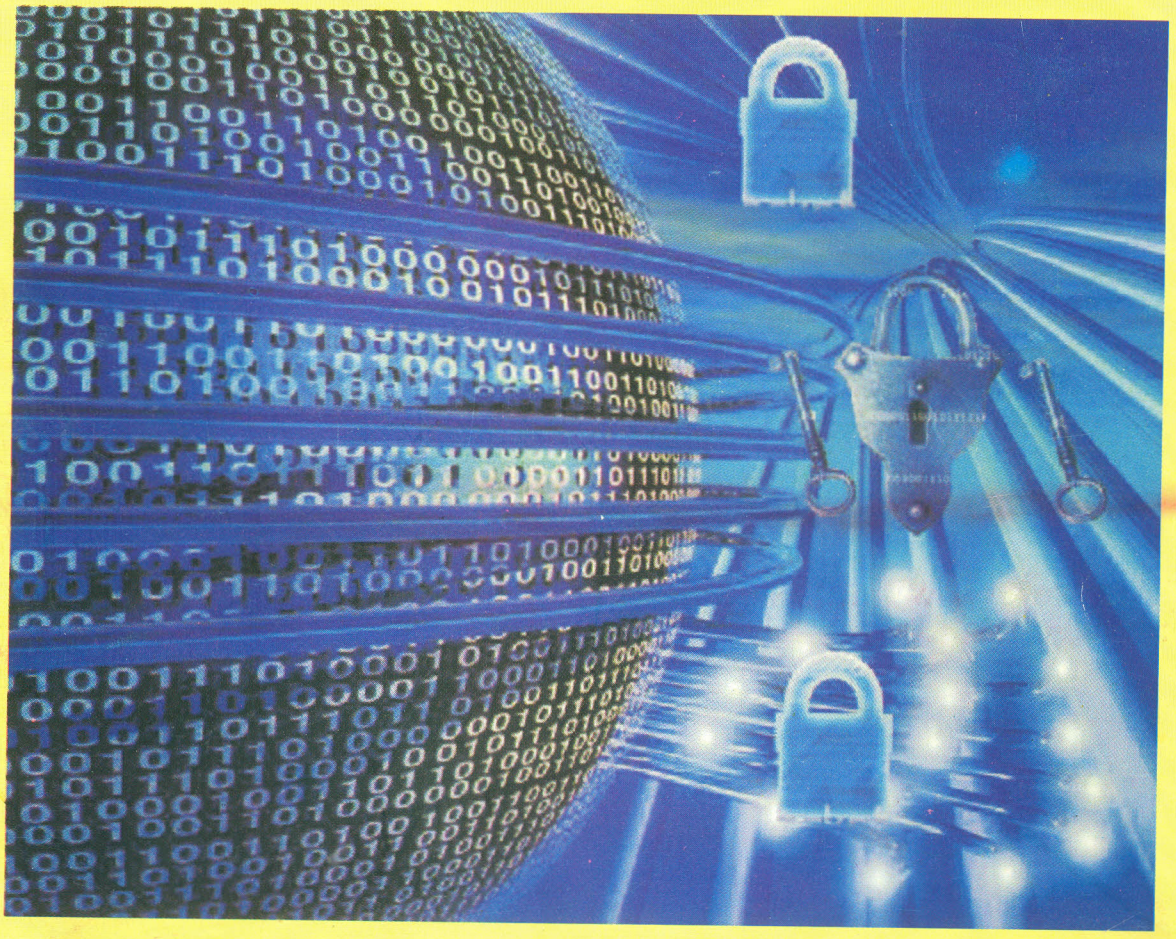
ignou
THE PEOPLE'S
UNIVERSITY
Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-027
Digital Forensics



Security Issues in Wireless Technologies

4

"शिक्षा मानव को बन्धनों से मुक्त करती है और आज के युग में तो यह लोकतंत्र की भावना का आधार भी है। जन्म तथा अन्य कारणों से उत्पन्न जाति एवं वर्गगत विषमताओं को दूर करते हुए मनुष्य क़ो इन सबसे ऊपर उठाती है।"

– इन्दिरा गांधी

"Education is a liberating force, and in our age it is also a democratising force, cutting across the barriers of caste and class, smoothing out inequalities imposed by birth and other circumstances."

—Indira Gandhi

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-027
Digital Forensics

Block

4

SECURITY ISSUES IN WIRELESS TECHNOLOGIES

Programme Expert/ Design Committee of Post Graduate Diploma in Information Security (PGDIS)

Prof. K.R. Srivathsan
Pro Vice-Chancellor, IGNOU

Mr. B.J. Srinath, Sr. Director & Scientist 'G',CERT-In, Department of Information Technology, Ministry of Communication and Information Technology, Govt of India

Mr. A.S.A Krishnan, Director, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Mr. S. Balasubramony, Dy. Superintendent of Police, CBI, Cyber Crime Investigation Cell Delhi

Mr. B.V.C. Rao, Technical Director, National Informatics Centre, Ministry of Communication and Information Technology

Prof. M.N. Doja, Professor, Department of Computer Engineering, Jamia Milia Islamia New Delhi

Dr. D.K. Lobiyal, Associate Professor, School of Computer and Systems Sciences, JNU New Delhi

Mr. Omveer Singh, Scientist, CERT-In Department of Information Technology Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Dr. Vivek Mudgil, Director, Eninov Systems Noida

Mr. V.V.Subrahmanyam, Assistant Professor School of Computer and Information Science IGNOU

Mr. Anup Girdhar, CEO, Sedulity Solutions & Technologies, New Delhi

Prof. A.K. Saini, Professor, University School of Management Studies, Guru Gobind Singh Indraprastha University Delhi

Mr. C.S. Rao, Technical Director in Cyber Security Division, National Informatics Centre, Ministry of Communication and Information Technology

Prof. C.G. Naidu, Director, School of Vocational Education & Training, IGNOU

Prof. Manohar Lal, Director, School of Computer and Information Science, IGNOU

Prof. K. Subramanian, Director, ACIIL IGNOU, Former Deputy Director General National Informatics Centre, Ministry of Communication and Information Technology Govt of India

Prof. K. Elumalai, Director, School of Law IGNOU

Dr. A. Murali M Rao, Joint Director Computer Division, IGNOU

Mr. P.V. Suresh, Sr. Assistant Professor School of Computer and Information Science, IGNOU

Ms. Mansi Sharma, Assistant Professor School of Law, IGNOU

Ms. Urshla Kant
Assistant Professor, School of Vocational Education and Training, IGNOU
Programme Coordinator

Block Preparation

Unit Writers

Dr. Neeru Mundra
Associate Professor
Banarsidas Chandiwala Institute of Professional Studies, Dwarka
New Delhi
(Unit 1,2,3 &4)

Block Editors

Prof. Ajith Kumar R
Professor, Indian Institute of Information Technology and Management-Kerala (IIITM-K) ,Trivandrum Kerala

Ms. Urshla Kant
Assistant Professor
School of Vocational Education and Training
IGNOU

Proof Reading and Format Editing

Ms. Urshla Kant
Assistant Professor
School of Vocational Education and Training
IGNOU

PRODUCTION

Mr. B. Natrajan	Mr. Jitender Sethi	Mr. Hemant Parida
Dy. Registrar (Pub.)	Asstt. Registrar (Pub.)	Proof Reader
MPDD, IGNOU	MPDD, IGNOU	MPDD, IGNOU

Feb,2012

ISBN 978-81-266-5925-8

Further information on the Indira Gandhi National Open University courses may be obtained from the University's office at Maidan Garhi, New Delhi-110 068 or the website of IGNOU www.ignou.ac.in

Printed and Published on behalf of the Indira Gandhi National Open University, New Delhi, by the Registrar, MPDD.

Printed at: Berry Art Press A-9, Mayapuri, Phase-I New Delhi-64

BLOCK INTRODUCTION

This block deals with Security issues in wireless technologies. Security is an important issue for wireless networks, especially for those security sensitive applications. Many users of data transmission devices (such as laptops, PDAs, PCs, phones, etc.) demand for Protecting data residing within devices, protecting the transmission network, protecting transfer of data, and ensuring proper transfer. One of the goals of current wireless standard was to provide security and privacy that was 'Wired equivalent' and to meet this goal, several security mechanisms were provided for confidentiality, authentication, and access control. Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. Without properly setting up, a user sets themselves up for certain risks that could be prevented or at least halted. Using even the most basic form of protection is better than nothing. This block comprises of four units and is designed in the following way;

The **Unit One** deals with the "Introduction to Wireless Technologies". For a specific design, the most important issue to note is what type of wireless technology is required. One must therefore select the right protocol for the application and the selection criteria will be based on speed, cost, power consumption, reliability and setup time. At the moment WLANs, WMANs and WPANs provide service to different markets with different needs. They are also competing against cellular technologies such as third generation (3G). With each of these technologies rapidly improving there will be a fine difference between them until there will be a time when they will overlap.

The **Unit two** covers Wireless Devices. Wireless devices continue to change rapidly. While no one is quite sure what the ultimate wireless device(s) will be, there is definitely a need to ensure that devices can function with one another. There is also the need for a truly global wireless communication infrastructure with sufficiently high bandwidth to satisfy the needs of wireless applications.

The **Unit three** covers securing wireless network. Organizations and individuals benefit when wireless networks and devices are protected. After assessing the risks associated with wireless technologies, organizations can reduce the risks by applying countermeasures to address specific threats and vulnerabilities. These countermeasures include management, operational, and technical controls. While these countermeasures will not prevent all penetrations and adverse events, they can be effective in reducing many of the common risks associated with wireless technology.

Unit four explains about the Ethical Hacking-Wireless Security. It must be reiterated that the ethical hacker is an educator who seeks to enlighten not only the customer, but also the security industry as a whole. By thinking like the enemy, the ethical hacker is able to ferret out issues in security which others may not even be aware of. Corporations and other entities are faced with the unenviable task of trying to defend their networks against various types of intrusive attacks. Although traditional methods of deterrence, (i.e. firewalls, intrusion detection devices, etc.) have their place in this battle, there has arisen the need to utilize specialists who are adept at exploiting both known and unknown vulnerabilities in networks in order to determine the security posture of an organization. These "Ethical Hackers" have created a niche for themselves in the "defense in-depth" spectrum.

Hope you benefit from this block.

ACKNOWLEDGEMENT

The material we have used is purely for educational purposes. Every effort has been made to trace the copyright holders of material reproduced in this book. Should any infringement have occurred, the publishers and editors apologize and will be pleased to make the necessary corrections in future editions of this book.

UNIT 1 INTRODUCTION TO WIRELESS TECHNOLOGIES

Structure

1.0 INTRODUCTION

Wireless Networks

Today's global workforce is extremely mobile. Workers are accessing the Internet from any location including coffee shops, at their homes, in offices, in vehicles and trains, in airplanes, and literally almost every corner of a city. This mobile global environment has put a great deal of strain on both wired and wireless

networks. Wireless Communication is an application of science and technology that has come to be vital for modern existence. From the early radio and telephone to current devices such as mobile phones and laptops, accessing the global network has become the most essential and indispensable part of our lifestyle. Wireless communication is an ever-developing field, and the future holds many possibilities in this area. One expectation for the future in this field is that, the devices can be developed to support communication with higher data rates and more security. **Wireless** telecommunications is the transfer of information between two or more points that are not physically connected. Distances can be short, such as a few meters for television remote control, or as far as thousands or even millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of wireless technology include GPS units, Garage door openers or garage doors, wireless computer mice, keyboards and Headset (telephone/computer), headphones, radio receivers, satellite television, broadcast and cordless telephones.

Wireless networking (i.e. the various types of unlicensed 2.4 GHz WiFi devices) is used to meet many needs. Perhaps the most common use is to connect laptop users who travel from location to location. Another common use is for mobile networks that connect via satellite. A wireless transmission method is a logical choice to network a LAN segment that must frequently change locations. The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling,
- To provide a backup communications link in case of normal network failure,
- To link portable or temporary workstations,
- To overcome situations where normal cabling is difficult or financially impractical, or
- To remotely connect mobile users or networks.

Wireless operations permit services, such as long range communications, that are impossible or impractical to implement with the use of wires. The term is commonly used in the telecommunications industry to refer to telecommunications systems (e.g. radio transmitters and receivers, remote controls, computer networks, network terminals, etc.) which use some form of energy (e.g. radio frequency (RF),acoustic energy, etc.) to transfer information without the use of wires. Information is transferred in this manner over both short and long distances.

Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these are also sometimes classified as wireless.

The first wireless transmitters went on the air in the early 20th century using radiotelegraphy. Later, as modulation made it possible to transmit voices and music via wireless, the medium came to be called "radio." With the advent of television, fax, data communication, and the effective use of a larger portion of the spectrum, the term "wireless" has been resurrected.

As the Internet and the World Wide Web have exploded into our culture and are replacing other media forms for people to find news, weather, sports, recipes, yellow pages and a million other things, the new struggle is not only for time on the computer at home, but for time on the Internet connection.

The hardware and software vendors have come forth with a variety of solutions allowing home users to share one Internet connection among two or more computers. They all have one thing in common though- the computers must somehow be networked.

To connect your computers together has traditionally involved having some physical medium running between them. It could be phone wire, coaxial cable or the ubiquitous CAT5 cable. Recently hardware has been introduced that even lets home users network computers through the electrical wiring. But, one of the easiest and least messy ways to network computers throughout the home is to use wireless technology.

The Internet connection comes in from your provider and is connected to a wireless access point or router which broadcasts the signal. Connect wireless antenna network cards to the computers to receive that signal and talk back to the wireless access point and you are in business.

The problem with having the signal broadcast though is that it is difficult to contain where that signal may travel. If it can get from upstairs to your office in the basement then it can also go that same 100 feet to your neighbours living room. Or, a hacker searching for insecure wireless connections can get into your systems from a car parked on the street. That doesn't mean one shouldn't use wireless networking. Only we need to take some basic precautions to make it more difficult for curiosity seekers to get into the personal information.

1.1 OBJECTIVES

After going through this Unit, you should be able to:

- describe the need of wireless technology;
- identify modes of operation;
- classify wireless network;
- describe applications of Wireless Technology; and
- explain need to build Wireless Network.

1.2 NEED OF WIRELESS TECHNOLOGY

There are two main advantages of using wireless technology for computer networks - mobility and cost-savings. Using a wireless network means that you can move about freely, within your home, business or even your city, and still maintain a connection to other computers on the same network. Installing cabling can be expensive, especially over long distances, in difficult terrain, or in established buildings, so it can mean considerable cost-savings to use a wireless network instead, provided the environment is suitable. For WANs, using wireless technology also removes the need to pay for access to existing telecommunications infrastructure.

Typical uses of wireless technology include:

- a home or small business wireless access point that gives access to the internet for one or more computers
- linking two buildings (business premises, farm buildings, temporary or mobile sites) that are physically separate
- hot spots in public places such as hotels, restaurants, marinas, caravan parks
- wireless ISP infrastructure (network backbones and customer services)

Remote access to equipment, such as remote sensors or device controllers (e.g. irrigation systems, temperature sensors, security cameras)

Wireless can be divided into:

- **Fixed wireless** -- the operation of wireless devices or systems in homes and offices, and in particular, equipment connected to the Internet via specialized modems
- **Mobile wireless** -- the use of wireless devices or systems aboard motorized, moving vehicles; examples include the automotive cell phone and PCS (personal communications services)
- **Portable wireless** -- the operation of autonomous, battery-powered wireless devices or systems outside the office, home, or vehicle; examples include handheld cell phones and PCS units
- **IR wireless** -- the use of devices that convey data via IR (infrared) radiation; employed in certain limited-range communications and control systems

Wireless technology uses radio waves to transmit information without cables or wiring. Although wireless communications have been used since 1876, the technology is becoming widely used in the creation of wireless computer networks. There are many standards for wireless communications, including Bluetooth, DECT and WiMax. WiFi or 802.11 is a set of standards designed for

wireless ethernet LANs and is the protocol used by all of the mini PCI wireless cards.

1.3 MODES OF OPERATION

Wireless technology can operate in one of two modes. The first is known as infrastructure networks, i.e., those networks with fixed and wired gateways. The bridges for these networks are known as base stations. A mobile unit within these networks connects to, and communicates with, the nearest base station that is within its communication radius. Typical applications of this type of network include office wireless local area networks (WLANs). The second type of mobile wireless network is the infrastructure less mobile network, commonly known as an ad-hoc network. A 'mobile adhoc network' is an autonomous system of mobile hosts which are free to move around randomly and organise themselves arbitrarily.

These two modes have advantages and disadvantages which must be examined carefully to determine which mode of operation is best suited for the task at hand.

1.3.1 Infrastructure Mode

As the name states, this mode of operation requires infrastructure in the form of base stations similar to cell phone towers. This mode also requires access points (AP) so that a device can connect to the wireless network. This makes this mode very dependent on the hardware and also very prone to the networking collapsing if the base station is damaged.

1.3.2 Ad hoc Mode

In this mode of operation the devices that form the wireless in a peer-to-peer manner such that routing from one device to the other is done via the other devices in the network. Fig.1 below shows a typical mesh topology.

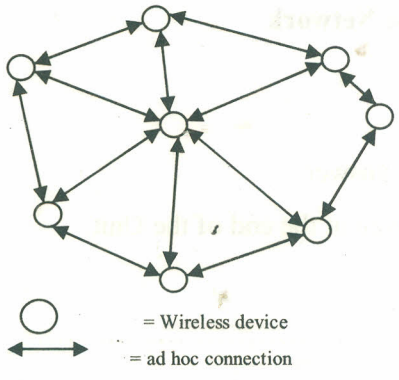


Fig. 1: Ad hoc network

In an ad hoc network, connections are made spontaneously such that a connection is made from the transmitting device to the receiver. This has the advantage of making the network very robust and independent of a single base station which

can cause the entire network to collapse if it is damaged. Ad hoc networks cost less than infrastructure networks and are faster to setup. These advantages make ad hoc mode networks a very compelling choice to use but the disadvantage of using this network is that it cannot be implemented with many users. This problem can be overcome by using smaller ad hoc networks called cells that can connect to other cells thereby forming a large community of ad hoc networks with as many users as desired. Fig. 2 shows how ad hoc cells are linked.

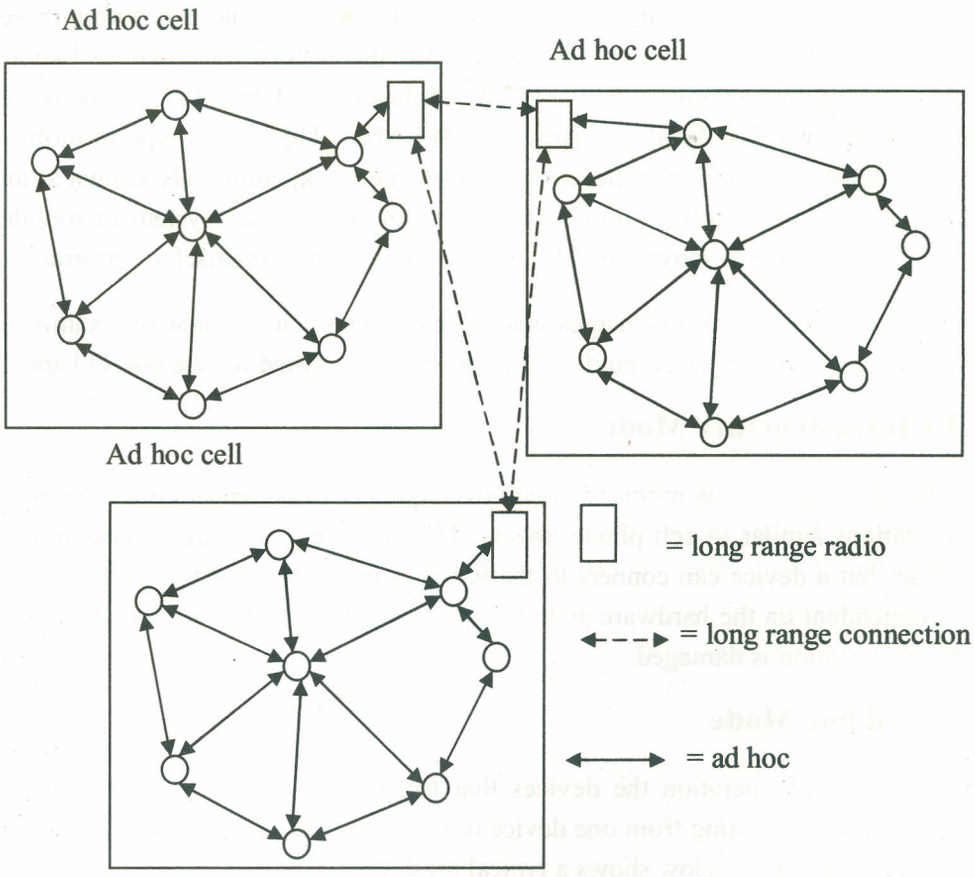


Fig. 2: Multicell ad hoc Network

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What are the uses of wireless technology?

.....

.....

.....

.....

2) What are the two modes of wireless technology?

.....

.....

.....

.....

1.4 CLASSIFICATION OF WIRELESS NETWORK

Wireless networks can be classified into three groups:

- wireless local area networks (WLANs),
- wireless metropolitan area networks (WMANs) and
- wireless personal area networks (WPANs)

Each of these groups is designed to accommodate the specific needs of the network which they provide. Wireless networks use high frequency radio waves to communicate and transfer data rather than using wires. WPANs are short range networks that provide high data transfer over short distances, WLANs are medium range networks that reduce data rate to accommodate for longer range while WMANs have a long range with a higher data rate than WLANs at the same range but is still less than WPANs. Power consumption plays a role in the range of each network. Refer to Fig. 3 below.

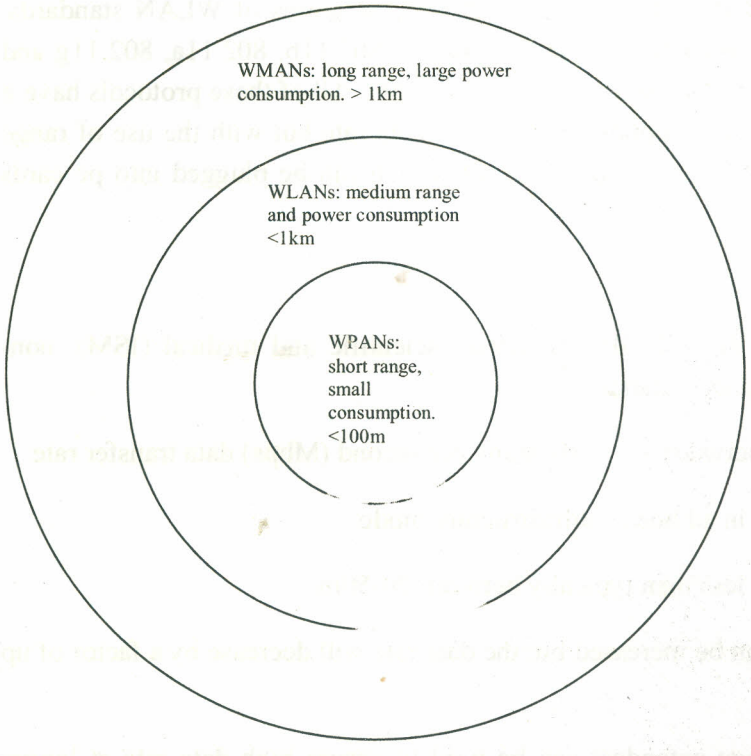


Fig. 3: Typical range for wireless networks

WMANs are used to network an area the size of a city and are used by municipality's public safety agencies such as the fire department, ambulance services and the police force. Once a WMAN is in operation, these agencies can communicate with each other within an area of up to 50 km radius given that the right technology is in use. WLANs network a small community of users, an example will be computer users on a campus, where medium range is required. WPANs are usually used for multimedia communications such as Bluetooth in cell phones which have a range of up to 10m. To choose the best network requires a balance between range, data rate, cost and power consumption. The organisation that sets the standard for wireless technology is the Institute for Electrical and Electric Engineers (IEEE). The IEEE classifies the various standards in wireless technology by their range, speed and purpose. These standards have been given a specific name by the IEEE but to the community of wireless users these standards have been grouped into names that classify a specific type of wireless technology into a larger group. Wireless Fidelity (Wi-Fi) is a name commonly given to the IEEE 802.11x standards; here the x denotes whether the standard is a, b, g. Wi-Fi is a WLAN standard. Worldwide Interoperability for Microwave Access (WiMax) is the name given to 802.16x, here the x specifies whether it is e, f, g, h and etc. WiMax is a WMAN standard. The IEEE 802.15x standard is a WPAN standard here the x denotes whether it is version .1 or .2 and etc. The 802.15.4 is commonly called ZigBee since ZigBee utilises the same radio as 802.15.4 but has additional software that enhances the 802.15.4 features.

1.4.1 WLANs

The 802.11 standard is broken up into different categories of WLAN standards. 802.11 was the first WLAN used, then came the 802.11b, 802.11a, 802.11g and the 802.11n which will be released in the year 2006. All of these protocols have a limited range which corresponds to its lowest data rate but with the use of range extenders such as omni directional antennas which can be plugged into pc cards the range can be increased up to 50%.

1.4.1.1 802.11

- Operates in the 2.4 GHz industrial, scientific and medical (ISM), non-licensed frequency band.
- Capable of between 1 – 2 Megabits per second (Mbps) data transfer rate.
- Can be used in ad hoc or infrastructure mode.
- The range is less than typically between 20-50m.
- The range can be increased but the data rate will decrease by a factor of up to two.
- Optional range extenders can be used to ensure high data rate at longer ranges e.g. WiDeFi's WLAN Xtender.

1.4.1.2 802.11b Wi-Fi

- Also operates in the unlicensed ISM band of 2.4 GHz.
- Data rate can be up to 11Mbps at a range of 50 m indoors and 250m outdoors.
- The outdoor range can increase to more than 500m with data rate dropping to 1 Mbps.
- Since it operates in the 2.4 GHz frequency band it can incur interference from household appliances and other devices that operate in the 2.4 GHz range.
- It is has an enhancement mode such that it can have a bit rate of 22Mbps with the correct equipment in place such as the Texas Instruments chipset; the ACX1000.
- Operates in ad hoc or infrastructure mode.
- Good penetration through walls because of its low frequency.
- Maximum transmitting power of 1W but typically operates at less than 30mW.
- Compatible with 802.11g.

1.4.1.3 802.11a Wi-Fi

- Operates in the 5 GHz unlicensed national information infrastructure (UNII) frequency band.
- Maximum data rate of 54Mbps.
- Typical range to achieve 54Mpbs 18m indoors and 30m outdoors.
- The range can be increased but the data rate will drop to the minimum specified of 6Mbps.
- Maximum transmitting power is between 40-800mW.
- Penetration through walls is low.
- Operates in ad hoc or infrastructure mode.
- Used mainly for short distance high data rate communication.
- Has an additional enhancement mode viz. "Turbo mode" that can increase data rate between 720-108Mbps by using chipsets by Atheros.
- Not compatible with 802.11b and 802.11g.

1.4.1.4 802.11g

- Optimises features from 802.11a and 802.11b.
- Operates in the ISM 2.4 GHz band.
- Data rate of 54Mbps.
- Backward compatible with 802.11b.
- Has a higher data rate than 802.11b and 802.11a when operating at the same range.
- At a range greater than approximately 50m; 802.11g will have the same data rate as 802.11b.

1.4.1.5 802.11n

- Data rate claimed to be up to 240Mbps.
- Only released in the year 2006 therefore not much information available.
- Many pre 802.11n products are launched and are claimed to have better performance that 802.11g.
- Uses multiple input multiple output (MIMO) antenna technology.

The table below summarises the features of the 802.11a, 802.11b, 802.11g and 802.11n standards, which are most commonly used in wireless networking.

Table 1: Features of the 802.11a, 802.11b, 802.11g and 802.11n standards

Standard	802.11a	802.11b	802.11g	802.11n
Frequency	5.8 GHz	2.4 GHz	2.4 GHz	2.4 GHz / 5.8 GHz
Max legal output power (EIRP)	4W / 36 dBm	4W / 36 dBm	4W / 36 dBm	4W / 36 dBm
Legal frequency range and output power	5.150 - 5.350GHz (up to 0.2W) 5.725 - 5.850GHz (up to 4W)	2.400 - 2.4835GHz (up to 4W)	2.400 - 2.4835GHz (up to 4W)	2.400 - 2.4835GHz (up to 4W) 5.150 - 5.350GHz (up to 0.2W) 5.725 - 5.850GHz (up to 4W)
Theoretical maximum rate (Mbps)	54	11	54	304

Practical maximum rate (Mbps)	~25	~7	~25	75-150
Modulation technology	Orthogonal frequency-division multiplexing (OFDM)	Complementary code keying (CCK, variation of CDMA)	Orthogonal frequency-division multiplexing (OFDM)	Multiple Input Multiple Output (MIMO), including OFDM with 16-QAM, 64-QAM, BPSK, BSSK, QPSK; DSSS with CCK, DQPSK, DBQPS; A-MPDU, A-MSDU
Typical distance	Less than 802.11b	~30m (indoor) ~8 km (outdoor point-to-point)	Slightly more than 802.11b at lower speeds, but much less than 802.11b at 54Mbps	Less than 100m
Advantages	Spectrum is less crowded so less interference.	Large range of hardware and software available.	Large range of hardware and software available.	Faster than all the other standards because it combines them.
Disadvantages	Less hardware and software available, especially antennas. Absorbed more readily. Need line-of-sight.	In a very crowded spectrum. Interference can occur between wireless adapters and microwaves, Bluetooth and cordless phones.	In a very crowded spectrum. Interference can occur between wireless adapters and microwaves, Bluetooth and cordless phones. Is interfered with by older 802.11b networks.	Less open-source support currently. Not intended to cover long distances. Interference can occur between wireless adapters and microwaves, Bluetooth and cordless phones.
Theoretical maximum rate (Mbps)	54	11	54	304

Practical maximum rate (Mbps)	~25	~7	~25	75-150
Modulation technology	Orthogonal frequency-division multiplexing (OFDM)	Complementary code keying (CCK, variation of CDMA)	Orthogonal frequency-division multiplexing (OFDM)	Multiple Input Multiple Output (MIMO), including OFDM with 16-QAM, 64-QAM, BPSK, BSSK, QPSK; DSSS with CCK, DQPSK, DBQPS; A-MPDU, A-MSDU
Typical distance	Less than 802.11b	~30m (indoor) ~8 km (outdoor point-to-point)	Slightly more than 802.11b at lower speeds, but much less than 802.11b at 54Mbps	Less than 100m
Advantages	Spectrum is less crowded so less interference.	Large range of hardware and software available.	Large range of hardware and software available.	Faster than all the other standards because it combines them.
Disadvantages	Less hardware and software available, especially antennas. Absorbed more readily. Need line-of-sight.	In a very crowded spectrum. Interference can occur between wireless adapters and microwaves, Bluetooth and cordless phones.	In a very crowded spectrum. Interference can occur between wireless adapters and microwaves, Bluetooth and cordless phones. Is interfered with by older 802.11b networks.	Less open-source support currently. Not intended to cover long distances. Interference can occur between wireless adapters and microwaves, Bluetooth and cordless phones.

1.4.2 WMANs

WMANs are used to network an entire city such that various agencies that have 802.16 or WiMax technology can communicate with each other. This is due to the interoperability of the 802.16 standard. If a group or organisation has 802.16 technologies and it is certified by the WiMax Forum then their 802.16 technology can be used in conjunction with other 802.16 technology. With this in mind if a municipality employs the 802.16 infrastructure such as access points and base stations then anybody with 802.16 pc cards or network interface cards (NIC) can use this infrastructure to communicate. The WiMax working group is responsible for providing the standards for WMAN technology and are a branch of the IEEE. The current goal of the WiMax working group is to allow for mobility in WMANs. Although WiMax does not operate in ad hoc mode, it does allow peer-to-peer connections between users to allow for non line of sight (NLOS) transmittance from the base station this is an advantage of 802.16e.

1.4.2.1 802.16 WiMax

- Operates between 10-66 GHz frequencies.
- Up to 120Mbps data rate.
- Maximum range of up to 30miles with a single wired base station but the data rate drops significantly.
- Does not operate in ad hoc mode since a base station is required.
- Supports point to multipoint architectures.

1.4.2.2 802.16a WiMax

- Operates between 2-11 GHz i.e. unlicensed and licensed bands.
- Uses orthogonal frequency division multiplexing (OFDM) similar to 802.11a,g
- Accommodates for non line of sight (NLOS) transmittance.
- Range is between 2-40km which can be extended with improved antenna technology developed by Intel and Array COMM and other antenna manufacturers.
- Up to 70Mbps data rate.

1.4.2.3 802.16e WiMax

- Up to 15Mbps data rate
- 6GHz maximum frequency
- Range is between 1-3miles

- Mobility is provided for vehicular movement up to 75mph.
- Optimized for multimedia
- Does not operate in ad hoc mode.

1.4.2.4 802.20

- Up to 15km range
- Provides mobility up to 250 kmph
- Minimum data rate is greater than 1Mbps
- Operates at frequencies less than 3.5 GHz
- Does not operate in ad hoc mode.

1.4.3 WPANs

WPANs are used to provide data transfer in short distances. The 802.15.4 standard or ZigBee (since they both utilize the same radio) provides low data rate transfer to ensure long battery life and reliable communication. WPANs are also used in multimedia such digital video and audio, the standard that is used for fast data transfer in short distances is WiMedia or 802.15.3. The 802.15.1 and 802.15.2 standards were developed from the concept of Bluetooth. These two standards are just official standards for Bluetooth and most of their development is handled by the Bluetooth special interest group (SIG). WPANs have many applications which can be exploited in the home or in industry. An example would be the control of lighting, access control, monitoring of patients in hospitals, wireless keyboards and pc peripherals and DVD, VCR and TV remotes. ZigBee is termed "Wireless control that simply works" and provides reliable communication with battery life of up to a few years. In the future WPANs will be incorporated into many portable devices due to the competitiveness between Bluetooth and 802.15 since these wireless technologies are producing single chip devices with low cost. Companies producing Bluetooth claim that their single chip devices will be available for approximately $5. With the cost of this wireless technology so low it is predicted that WPANs will be incorporated into pens, cameras, headsets and various sensors and not just pda's, phones and laptops.

1.4.3.1 802.15.1 Bluetooth 1

- Operates in the 2.4 GHz band
- Up to 2.178Mbps data rate
- Maximum range up to 100m
- Compatible with Bluetooth v1.1

- Power consumption from as low as 0mW - 100mW
- Portable but only within its specified range

1.4.3.2 802.15.2 Bluetooth 2

- Designed to mitigate the interference with 802.11b and 802.11g
- Operates in the 2.4 GHz band
- Must be used if you want to use Bluetooth and Wi-Fi simultaneously

1.4.3.3 802.15.3 WiMedia

- Used for consumer devices such TV's and digital cameras.
- Data rate up to 55Mbps but the improved version; 802.15.3a has a data rate of 480Mbps. This is currently being tested by the WiMedia Alliance.
- Uses ultra wide band width (UWB) to reach high data rates.

1.4.3.4 802.15.4 ZigBee

- Designed for long battery life and low device cost.
- No support for voice.
- Operates in the 2.4 GHz frequency band.
- Data rate is as low as 9.6kbps to 250kbps.
- The range is between 70 – 300m depending on the placement of nodes.
- Extendable.
- Simple.

1.4.3.5 802.15.5

- Still under development
- Will enable networks to be formed without the need for ZigBee or internet protocols.

1.4.3.6 802.15.6

- Not yet official but will cover the terahertz frequency range i.e. 1000 GHz.
- This uses T-rays that use properties of both light and radio.
- Theoretical data rate is in the multi gigabit range

Table 2: Summary of Popular Wireless Technologies

	Data rate (Mbps)	Frequency	Range	Ad-hoc	Mobility
802.11a (Wi-Fi)	up to 54 max	5 GHz	20-30 m	yes	Low speed
802.11b (Wi-Fi)	11 max	2.4GHz	100m indoors 500 m outdoors	yes	Low speed
802.11g (Wi-Fi)	up to 54 max	2.4 GHz	Same as 802.11b at distances greater than 60m.	yes	Low speed
802.11n (Wi-Fi)	100 240 claimed	-	-	yes	-
802.16 (WiMax)	Up to120	10-66 GHz	30 miles max with a single wired base station	no	Low speed
802.16e	Up to 15	6 GHz max	1-3 miles	no	High speed
802.20	>1	Less than 3.5 GHz	Up to 15 km	no	Very high speed
ZigBee/ 802.15.4	0.25	2.4 GHz	70m typically. But depends on environment.	yes	Low speed

1.5 APPLICATIONS OF WIRELESS TECHNOLOGY

- Wireless technology is rapidly evolving, and is playing an increasing role in the lives of people throughout the world. In addition, ever-larger numbers of people are relying on the technology directly or indirectly. (It has been suggested that wireless is overused in some situations, creating a social nuisance.) More specialized examples of wireless communications and control include:
- Global System for Mobile Communication (GSM) -- a digital mobile telephone system used in Europe and other parts of the world; the de facto wireless telephone standard in Europe
- General Packet Radio Service (GPRS) -- a packet-based wireless communication service that provides continuous connection to the Internet for mobile phone and computer users
- Enhanced Data GSM Environment (EDGE) -- a faster version of the Global System for Mobile (GSM) wireless service
- Universal Mobile Telecommunications System (UMTS) -- a broadband, packet-based system offering a consistent set of services to mobile computer and phone users no matter where they are located in the world

- Wireless Application Protocol (WAP) -- a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access
- i-Mode -- the world's first "smart phone" for Web browsing, first introduced in Japan; provides color and video over telephone sets.
- Telemetry control and traffic control systems
- Infrared and ultrasonic remote control devices
- Modulated laser light systems for point to point communications
- Professional LMR (Land Mobile Radio) and SMR (Specialized Mobile Radio) typically used by business, industrial and Public Safety entities.
- Consumer Two way radio including FRS Family Radio Service, GMRS (General Mobile Radio Service) and Citizens band ("CB") radios.
- The Amateur Radio Service (Ham radio).
- Consumer and professional Marine VHF radios.
- Airband and radio navigation equipment used by aviators and air traffic control.
- Cellular telephones and pagers: provide connectivity for portable and mobile applications, both personal and business.
- Global Positioning System (GPS): allows drivers of cars and trucks, captains of boats and ships, and pilots of aircraft to ascertain their location anywhere on earth.
- Cordless computer peripherals: the cordless mouse is a common example; keyboards and printers can also be linked to a computer via wireless using technology such as Wireless USB or Bluetooth.
- Cordless telephone sets: these are limited-range devices, not to be confused with cell phones.
- Satellite television: Is broadcast from satellites in geostationary orbit. Typical services use direct broadcast satellite to provide multiple television channels to viewers.
- Home-entertainment-system control boxes -- the VCR control and the TV channel control.
- Hi-fi sound systems and FM broadcast receivers also use this technology.
- Remote garage-door openers -- one of the oldest wireless devices in common use by consumers; usually operates at radio frequencies.

- Two-way radios -- this includes Amateur and Citizens Radio Service, as well as business, marine, and military communications.
- Baby monitors -- these devices are simplified radio transmitter/receiver units with limited range.
- Satellite television -- allows viewers in almost any location to select from hundreds of channels.
- Wireless LANs or local area networks -- provide flexibility and reliability for business computer users.
- Mobile telephones (cellular phone) with more than 5 billion mobile cellular subscriptions worldwide. 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.
- 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.
- 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.
- Computer interface devices--Answering the call of customers frustrated with cord clutter, many manufactures 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. Initial concerns about the security of wireless keyboards have also been addressed with the maturation of the technology.

1.6 NEED TO BUILD WIRELESS NETWORK

In the last if we need to build wireless network, we need the following:

1. Computers

To make use of a wireless network, one will need wireless-capable computers and devices such as wireless access points or wireless routers. One can build own access point or router using dedicated hardware, like the **ALIX and net** computers, or can buy an off-the-shelf product.

2. Wireless cards

Wireless expansion cards (also called wireless adapters) handle the processing of the data that is transmitted or received over a wireless network. Each card supports one or more of the 802.11 standards, and has different characteristics with regard to the chipset used, maximum output power, speed, receive sensitivity, etc. Wireless adapters are available in a variety of formats, including mini PCI and PCI, PCMCIA (CardBus) and USB. All of the **wireless cards** are mini PCI type 3A or 3B.

3. Antennas

As with other radio devices, wireless computers can use antennas to improve reception and transmission quality. Each antenna has a distinctive pattern of radiation, with omni-directional (360°) being the most common. Antennas can also be directional or sectorised, with transmission and reception occurring in a narrower, more specific direction. The gain of an antenna in combination with the output power of the wireless card, determine the output power (**EIRP**) of a wireless device.

4. Pigtails

A pigtail is used to connect a wireless card to an antenna. Some pigtails connect directly from the wireless card to the antenna, while others connect from another pigtail to the antenna, allowing for more distant placement of the antenna from the wireless card. With these longer pigtails, loss of signal can occur, so using special low-loss cable (LLC or LMR) is recommended.

It's important to make sure one has compatible connectors on the card, pigtail and antenna.

5. Software

Lastly need of software to run wireless hardware. We need drivers for the wireless card and a network-capable operating system.

1.7 FUTURE OF WIRELESS TECHNOLOGY

The future of wireless technology is bright due to it being very cost efficient and very easy to use and the best part about it is you don't have to worry about being tangled up in wires. We have seen wireless technology in cell phones and radios.

However, this technology has many other practical uses which can be seen to revolutionize the future. In straightforward and simple words wireless technology is low cost and simple to handle technology. We are standing in the era where it is possible to have voice chats and video conferencing in even remote areas but still there are many challenges that hinder the way of wireless success. The main challenge is that how to make current network architecture compatible with next generation technologies like 4 G. this is the reason why 4G has not been widely adopted. The next generation technologies are modified to provide long term benefits to the technology carriers. If we look at the current Korea e would find that this region is entirely different from our world. They can make use pervasive communications throughout their country. While most of the courtiers in the world including USA is also looking forward to adapt to these changes in future. Hence we can say the wireless technology challenges can be overtaken without additional network modifications even in our country.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) List three classifications of wireless networks?

.....

.....

.....

.....

2) What is range of 802.20.

.....

.....

.....

.....

3) 802.15.2 Bluetooth 2 operates in ..... band.

.....

.....

.....

.....

4) Define i-Mode.

.....

.....

.....

.....

5) What are the main advantages of using wireless technology for computer networks?

.....

.....

.....

.....

6) What are the different formats in which Wireless adapters are available?

.....

.....

.....

.....

7) WPANs are used.

.....

.....

.....

.....

1.8 LET US SUM UP

For a specific design the most important issue to note is what type of wireless technology is required. One must therefore select the right protocol for the application and the selection criteria will be based on speed, cost, power consumption, reliability and setup time. Clearly wireless technology in ad hoc mode will reduce cost and setup time but the power consumption and speed depends on what IEEE standard is used. For a large scale network which will incorporate many users in a large area, the right protocol to use will be WiMax or for a small scale project that requires transfer of data over a short distance then ZigBee will be used. This leaves Wi-Fi which is a compromise between the two. The 802.11g is versatile in the sense that it has good range like the 802.11b with a low data rate and a high data rate like 802.11a at short range. Since 802.11n will be released in 2006, the only feasible choice of wireless technology to use for a medium scale project is the 802.11g. At the moment WLANs, WMANs and WPANs provide service to different markets with different needs. They are also competing against cellular technologies such as third generation (3G). With each of these technologies rapidly improving there will be a fine difference between them until there will be a time when they will overlap. When this happens then all the different wireless technologies will be interoperable and co-exist. At the moment Wi-Fi will continue to grow in public spaces called "Hot Spots", at home

and in industry. In the future it is hoped that 3G and Wi-Fi will compliment each other and provide a low cost networking services to developing countries.

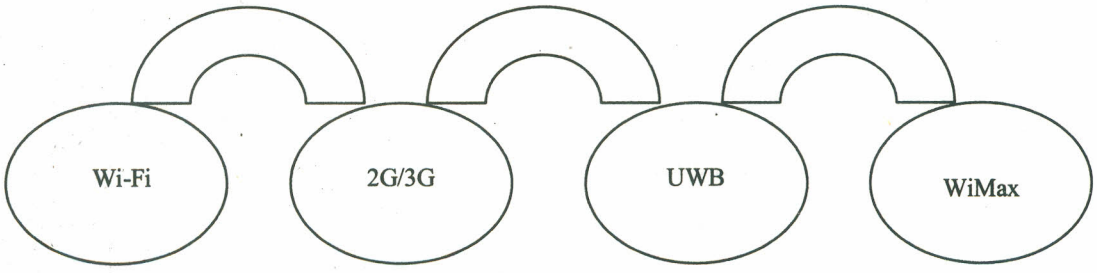


Fig. 4: Convergence of wireless technologies

1.9 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Uses of wireless technology include:

- a home or small business wireless access point that gives access to the internet for one or more computers
- linking two buildings (business premises, farm buildings, temporary or mobile sites) that are physically separate
- hot spots in public places such as hotels, restaurants, marinas, caravan parks
- wireless ISP infrastructure (network backbones and customer services)
- remote access to equipment, such as remote sensors or device controllers (e.g. irrigation systems, temperature sensors, security cameras

2) There are two modes –

1. Infrastructure Mode

As the name states, this mode of operation requires infrastructure in the form of base stations similar to cell phone towers. This mode also requires access points (AP) so that a device can connect to the wireless network. This makes this mode very dependent on the hardware and also very prone to the networking collapsing if the base station is damaged.

2 Ad hoc Mode

In this mode of operation the devices that form the wireless in a peer-to-peer manner such that routing from one device to the other is done via the other devices in the network.

Check Your Progress 2

1) Wireless networks can be classified into three groups:
   - wireless local area networks (WLANs),
   - wireless metropolitan area networks (WMANs) and
   - wireless personal area networks (WPANs)
2) Up to 15km range
3) Operates in the 2.4 GHz band
4) The world's first "smart phone" for Web browsing, first introduced in Japan; provides color and video over telephone sets
5) There are two main advantages of using wireless technology for computer networks - mobility and cost-savings
6) miniPCI and PCI, PCMCIA (CardBus) and USB
7) to provide data transfer in short distances

1.10 SUGGESTED READINGS

- Gen- X –PC, "Wireless standards (Wi-Fi) 802.11b vs. 802.11a", http://www.gen-x-pc.com/wireless_home2.htm.
- Grier, J.; 802.16: A Future Option for Wireless MANs, http://www.wi-fiplanet.com/tutorials/article.php/2236611.
- Grier, J.; Understanding Ad hoc mode, http://www.wi-fiplanet.com/tutorials/article.php/1451421.
- Geier, Jim (2001). *Wireless LANs*. Sams. ISBN 0672320584.
- Goldsmith, Andrea (2005). *Wireless Communications*. Cambridge University Press. ISBN 0521837162.
- http://www.bluetooth.com.
- I.E.E.E., Get IEEE 802, http://standards.ieee.org/getieee802.
- Jain, R. Wireless data networking, http://www.cse.ohio-state.edu/~jain/cis788-97/ftp/h_cwir.pdf.
- Kargl, F.; Lawrence E. and Zarumba, G.V. *Introduction to the Minitrack on Wireless Personal Area Networks (WPANs)*.

- Molisch, Andreas (2005). *Wireless Communications*. Wiley-IEEE Press. ISBN 047084888X.
- Pahlavan, Kaveh; Levesque, Allen H (1995). *Wireless Information Networks*. John Wiley & Sons. ISBN 00471106070.
- Pahlavan, Kaveh; Krishnamurthy, Prashant (2002). *Principles of Wireless Networks - a Unified Approach.* Prentice Hall. ISBN 0130930032.
- Rappaport, Theodore (2002). *Wireless Communications: Principles and Practice.* Prentice Hall. ISBN 0130422320.
- Rhoton, John (2001). *The Wireless Internet Explained.* Digital Press. ISBN 1555582575.
- Tse, David; Viswanath, Pramod (2005). *Fundamentals of Wireless Communication*. Cambridge University Press. ISBN 0521845270.
- Wi-Fi Alliance, What is Wi-Fi? http://www.wi-fi.org/OpenSection/index.asp.
- WiMax forum, Welcome to the WiMax Forum, http://www.wimaxforum.org/home.
- ZigBee Alliance, Control that simply works http://www.zigbee.org/en/index.asp.

UNIT 2 WIRELESS DEVICES

Structure

2.0 INTRODUCTION

In today's world, where people put a premium on staying connected to the Internet and to each other, there are several types of wireless technologies. In the home and office, wireless routers with built-in modems, hubs and switches broadcast a local area network (LAN) for computers in the area to join. Broadcasting distance varies widely depending on many factors, but a LAN generally spans 300 feet (91.44 m) or more. Any computer on the network can share resources that are connected to the network, including a high-speed Internet connection, printer or other office equipment. A wireless device can refer to any kind of communications equipment that does not require a physical wire for relaying information to another device. Wireless headphones fitted with a receiver use either radio frequency (RF) or infrared technology to

communicate with a transmitter that is connected to the sound source, say a television.

In most cases, however, when someone refers to a wireless device, they are speaking of a networking device that can pass data to other wireless network gear without being physically connected. Ultimately, one must determine what tasks users really want to perform anytime from anywhere and decide how to ensure that information and functionality to support those tasks are readily available and easily accessible.

The solution for this is WIRELESS DEVICE.

In the computing world, the term wireless can be rather ambiguous, since it may refer to several different wireless technologies.

The two most common types of wireless capabilities computers have are Wi-Fi and Bluetooth.

Wi-Fi is the technology used for wireless networking. If your computer has a wireless card, it is most likely Wi-Fi compatible. The wireless card transmits to a wireless router, which is also based on the Wi-Fi standard. Wireless routers are often connected to a network, cable modem, or DSL modem, which provides Internet access to anyone connected to the wireless network.

In order to join a wireless LAN (WLAN), a computer must have a wireless network card or adapter installed.

A network card is an internal wireless device manufactured to use the same language or protocol that wireless routers use. These protocols periodically evolve into new standards, however, causing compatibility issues in the interim. If a router uses a protocol that is not supported by an internal wireless device, an external wireless adapter can be used in an external port. The most common type is a USB dongle, but wireless network adapters are also available in Express Card formats, giving laptop users a choice as to which port they would rather use.

Another type of wireless device might be part of a Personal Area Network (PAN). A PAN is created with Bluetooth technology, designed to connect personal digital devices over very short distances of just a few feet, though the standard extends to 30 feet (9.14 m).

Bluetooth is a very flexible and convenient type of network. It can be used to send print jobs from a laptop to a nearby printer without the hassle of setting up shared resources over a LAN. It is also used to connect Bluetooth-enabled cell phones, personal digital assistants (PDAs), or Apple products to each other or to other Bluetooth-enabled equipment including headsets, external speakers, or computers. Since Bluetooth uses a different frequency range than LANs, one can use a Bluetooth network within a LAN without interference. Bluetooth is

the technology often used for wireless keyboards and mice, wireless printing, and wireless cell phone headsets. In order to use a device such as a Bluetooth keyboard or mouse, your computer must be Bluetooth-enabled or have a Bluetooth adapter installed.

Computers may also use other wireless technologies aside from Wi-Fi and Bluetooth. Products such as remote controls and wireless mice may use infrared or other proprietary wireless technologies. Because of the many wireless options available, it is a good idea to check the system requirements of any wireless device you are considering buying.

A wireless network device can be best defined as a network device used to connect computers and computer hardware together without cables, normally through radio signals. The term wireless network device itself is very broad, and applies to a wide variety of different devices and technologies. A wireless network device can be anything from a large broadcasting tower to a USB adapter.

Example:

Common wireless network device is a wireless router. Wireless routers are used not only by at home laptop users, but large businesses and colleges as well. This type of device works in cooperation with very specific wireless signals. In order to take advantage of newer wireless signals and technologies, a wireless network device must be compatible and up to date with that specific signal.

Basic wireless routers are a good example of how devices rely on specific signals.

Wireless routers are available for a range of prices, the difference being largely due to the different signals that the router is capable of using. Wireless routers can operate on band signals such as 802.11a, 802.11b, 802.11g, and 802.11n. 802.11n requires a router with specific built-in technology. It offers a stronger signal and greater range compared to other wireless router networks.

2.1 OBJECTIVES

After going through this Unit, you should be able to:

- describe the Technologies Required for Wireless Devices;
- identify the Categories of Wireless Devices;
- describe Advantages of Wireless Devices;
- describe Applications of Wireless Devices; and

- explain health issues related to wireless devices.

2.2 TECHNOLOGIES REQUIRED FOR WIRELESS DEVICES

Wireless devices have been available to consumers for many years, starting with the first infrared remote controls. Wireless technology is still prevalent in many forms. Within the past 15 years, the other primary types of wireless devices created for the consumer market have been 802.11-based wireless computer networking components and Bluetooth peripherals.

2.2.1 802.11

Wireless devices based on the different 802.11 standards--including wireless cards and routers--are typically associated with computer networking. Many other types of devices use 802.11 wireless technology, however, including Blu-Ray players and smart phones. As of December 2010, the most common 802.11 wireless standards are A, B, G and N. 802.11 technology runs on both the 2.4 gigahertz (GHz) and 5 GHz range of radio frequencies, depending on the sub-standard. 802.11b and 802.11g use 2.4 GHz, while 802.11a uses 5 GHz. 802.11n uses both sets of frequency ranges. The different sub-standards utilize different connection speeds. 802.11b connects up to 11 megabits per second (Mbps). 802.11a and 802.11g connect up to 54 Mbps, while 802.11n connects up to 300 Mbps.

2.2.2 Bluetooth

Bluetooth is the name given to 802.15-based technologies. Bluetooth operates in the 2.4 gigahertz (GHz) range of radio frequencies and is designed for short distance point-to-point connections of up to 30 feet. The most common device associated with Bluetooth is the headset designed for cell phones. Many other devices are designed to use Bluetooth, however, such as wireless keyboards and mice.

2.2.3 Infrared

Infrared is one of the oldest wireless technologies associated with the consumer market. Infrared is primarily used for remote control devices and requires a direct line-of-sight connection for proper operation.

2.3 CATEGORISATION OF WIRELESS DEVICES CAN BE DONE IN TWO WAYS

Wireless technology has come a long way since 1880 when Alexander Graham Bell and Sumner Tainter invented the photo phone. The photo phone was an early wireless telephone device that transmitted sound over a beam of light.

Unlike the photo phone, modern wireless technology relies on the use of radio frequency signals. Wireless technology makes it possible for consumers worldwide to use several types of devices.

2.3.1 Usage of Services

According to usage of services Wireless Devices are categorized into following ways:

2.3.1.1 Communication Equipment

The modern world has several types of wireless devices that allow humans to communicate.

E.g. The singer sang into a wireless microphone. The children might spend hours running around playing with walkie-talkies. Perhaps the most widely used of all wireless communications devices is the cell phone. It's almost impossible to go anywhere in America without seeing at least one person using a cell phone. However, wireless communication first received worldwide recognition in 1949 when Al Gross, the inventor of the walkie-talkie, invented the telephone pager. A telephone pager has a wireless receiver inside that responds to certain signals. When a person dials the pager number, whoever is wearing the pager hears a sound.

2.3.1.2 Computer Peripherals

Computers play an important role in modern society. We can see computers in schools, homes and business establishments. When it comes to wireless devices, many of them fit into the computer-peripheral category. A computer peripheral is a device made for a computer, but it's not a part of the computer. A wireless printer is an example of a wireless computer peripheral. It works like a traditional printer, except you print without having to physically connect the printer to the computer. Other wireless computer peripherals include the wireless keyboard and mouse.

2.3.1.3 Household Items

Wireless devices aren't only for computers and communications. We probably use several wireless household items everyday. Now every household have at least one television remote control. If you have a DVD player or cable box, those usually have a remote control as well. One might even have a remote garage door opener which, is one of the oldest wireless devices in common use. Some parents also use wireless baby monitors, which make it possible to monitor activity in a child's room from a distance.

2.3.1.4 Security Concerns

Wireless technology makes life easier in many ways. However, it also poses a threat in some situations. According to Internal Auditor, wireless technology

makes use of a broadcast medium. Anyone with the proper device can intercept information you might think is private. For example, some households have wireless networks that allow multiple computers to share one Internet connection. If the network isn't password-protected, any computer within range with wireless connectivity can connect to the network.

2.3.2 Flexibility of Movement

According to flexibility of movement Wireless Devices can be divided into:

2.3.2.1 Fixed Wireless

The operation of wireless devices or systems in homes and offices, and in particular, equipment connected to the Internet via specialized modems.

This refers to wireless devices or systems that are situated in fixed locations, such as an office or home, as opposed to devices that are mobile, such as cell phones and PDAs. Fixed wireless devices normally derive their electrical power from utility mains, as opposed to portable wireless devices that normally derive their power from batteries.

The point-to-point signal transmissions occur through the air over a terrestrial microwave platform rather than through copper or fiber cables; therefore, fixed wireless does not require satellite feeds or local phone service. The advantages of fixed wireless include the ability to connect with users in remote areas without the need for laying new cables and the capacity for broad bandwidth that is not impeded by fiber or cable capacities.

Fixed wireless is the operation of wireless devices or systems used to connect two fixed locations (e.g., buildings) with a radio or other wireless link, such as laser bridge. Usually, fixed wireless is part of a wireless LAN infrastructure. The purpose of a fixed wireless link is to enable data communications between the two sites or buildings. Fixed wireless data (FWD) links are often a cost-effective alternative to leasing fiber or installing cables between the buildings.

The point-to-point signal transmissions occur through the air over a terrestrial microwave platform rather than through copper or optical fiber; therefore, fixed wireless does not require satellite feeds or local telephone service. The advantages of fixed wireless include the ability to connect with users in remote areas without the need for laying new cables and the capacity for broad bandwidth that is not impeded by fiber or cable capacities.

Fixed wireless devices derive their electrical power from the public utility mains, unlike mobile wireless or portable wireless devices which tend to be battery powered.

Types of Fixed Wireless Devices are:

a. Antennas

Fixed wireless services typically use a directional radio antenna on each end of the signal (e.g., on each building). These antennas are generally larger than those seen in Wi-Fi setups, and are designed for outside use.

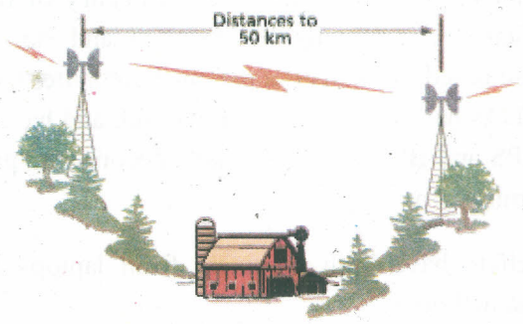
Several types of radio antennas are available that accommodate various weather conditions, signal distances and bandwidths. They are usually selected to make the beam as narrow as possible and thus focus transmits power to their destination, increasing reliability and reducing the chance of eavesdropping or data injection. The links are usually arranged as a point to point setup to permit the use of these antennas. This also permits the link to have better speed and or better reach for the same amount of power.

These antennas are typically designed to be used in the unlicensed ISM band radio frequency bands (900 MHz, 1.8GHz, 2.4 GHz and 5 GHz), however, in most commercial installations, licensed frequencies may be used to ensure quality of service or to provide higher connection speeds.

b. Fixed Wireless Broadband

With the growing infrastructure of the GSM wireless networks, fixed wireless has also become a viable solution for broadband access. Using the 3G speed and reliability, businesses and homes can use fixed wireless antenna technology to access broadband internet and Layer 2 networks using fixed Wireless broadband. Because of the redundancy and saturation of the GSM network, antennas that can aggregate signal from multiple carriers are able to offer fail-over and redundancy for connectivity not otherwise afforded by wired connections. In rural areas where wired infrastructure is not yet available, fixed wireless broadband has become a viable option for internet access.

The terms wireless broadband and broadband wireless are not used consistently, but generally both apply to carrier-based services in which multiple data streams are multiplexed onto a single radio-carrier signal. Some vendors also use the terms to refer to privately deployed networks.



2.3.2.2 Mobile Wireless

The use of wireless devices or systems aboard motorized, moving vehicles; examples include the automotive cell phone and PCS (personal communications services).

A **mobile device** (also known as a **handheld device**, **handheld computer** or simply **handheld**) is a small, hand-held computing device, typically having a display screen with touch input and/or a miniature keyboard and less than 2 pounds (0.91 kg). Early pocket sized ones were joined in the late 2000s by larger but otherwise similar tablet computers. As in a personal digital assistant (PDA), the input and output are often combined into a touch-screen interface.

Smart phones and PDAs are popular amongst those who wish to use some of the powers of a conventional computer in environments where carrying one would not be practical. Enterprise digital assistants can further extend the available functionality for the business user by offering integrated data capture devices like barcode, RFID and smart card readers.

Mobile devices such as the iPhone, iPad, Android and others are revolutionizing the way information can be disseminated. Contrast this with the older generation mobile devices such as Personal Data Assistants (PDAs) which primarily focused on data storage and display. An increasingly large number of devices are focusing not only on data storage and display, but also on communication and processing.

Types of mobile Wireless devices are:

Mobile devices have been designed for many applications and include:

a. Computer

It is the predominant term used to describe a category of mobile computer designed or modified to specifically be installed and run in automobiles. Originally these were based on industrial personal computer technology, but as smart phones and PDAs have become more powerful, and have included useful technologies like GPS and Bluetooth, they have become the predominant base platform for developing carputers.

Many do-it-your-selfers have built carputers from laptops and small form factor computers like netbooks.

The recent popularity of carputers has caused the creation of more advanced units that use touch screen interfaces, integrate with vehicles via OBD-II link, and offer a variety of other add-ons like rear-view cameras and GPS. It is now possible to find assembled carputers complete with wireless capabilities and built-in microphones for sale on the internet.

Police cars often have carputers, known as Mobile data terminals.

b. Personal Digital Assistant (PDAs)

A personal digital assistant (PDA), also known as a palmtop computer, or personal data assistant is a mobile device that functions as a personal information manager. Current PDAs often have the ability to connect to the Internet. A PDA has an electronic visual display, enabling it to include a web browser, but some newer models also have audio capabilities, enabling them to be used as mobile phones or portable media players. Many PDAs can access the Internet, intranets or extranets via Wi-Fi or Wireless Wide Area Networks. Many PDAs employ touch screen technology.

c. Tablet computer

A tablet computer, or a tablet, is a mobile computer, larger than a mobile phone or personal digital assistant, integrated into a flat touch screen and primarily operated by touching the screen rather than using a physical keyboard. It often uses an onscreen virtual keyboard, a passive stylus pen, or a digital pen.

A tablet computer that lacks a keyboard (also known as a non-convertible tablet) is shaped like slate or a paper notebook, features a touch screen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.

d. Ultra-Mobile PC

Ultra-mobile personal computer or UMPC is a small form factor version of a pen computer, a class of laptop whose specifications were launched by Microsoft and Intel in spring 2006. Sony had already made a first attempt in this direction in 2004 with its Vaio U series, which was however only sold in Asia. UMPCs are smaller than subnotebooks, have a TFT display measuring (diagonally) about 12.7 to 17.8 cm, and are operated like tablet PCs using a touch screen or a stylus. There is no clear boundary between subnotebooks and ultra-mobile PCs.

e. Wearable Computer

They are miniature electronic devices that are worn by the bearer under, with or on top of clothing. This class of wearable technology has been developed for general or special purpose information technologies and media development. Wearable computers are especially useful for applications that require more complex computational support than just hardware coded logics.

One of the main features of a wearable computer is consistency. There is a constant interaction between the computer and user, i.e. there is no need to turn the device on or off. Another feature is the ability to multi-task. It is not necessary to stop what you are doing to use the device; it is augmented into all other actions. These devices can be incorporated by the user to act like a prosthetic. It can therefore be an extension of the user's mind and/or body.

f. Mobile Internet Device

(MID) is a multimedia-capable mobile device providing wireless Internet access. They are designed to provide entertainment, information and location-based services for personal use, rather than for corporate use. They allow 2-

way communication and real-time sharing. An MID is larger than a smart phone but smaller than an Ultra-Mobile PC (UMPC). They have been described as filling a niche between smart phones and Tablet PCs. They are an easy way to stay in contact with others wirelessly.

g. Calculator

An electronic calculator is a small, portable, usually inexpensive electronic device used to perform the basic operations of arithmetic. Modern calculators are more portable than most computers, though most PDAs are comparable in size to handheld calculators.

h. Handheld Game Console

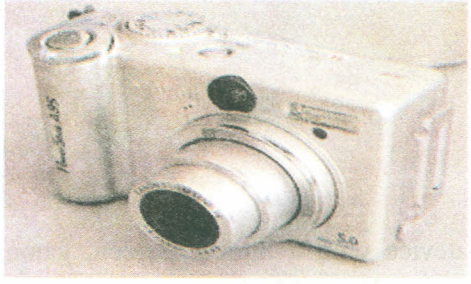
It is a lightweight, portable electronic device with a built-in screen, game controls, speakers and replaceable and or rechargeable batteries or battery pack. Handheld game consoles are run on machines of small size allowing people to carry them and play them at any time or place. Unlike video game consoles, the controls, screen and speakers are all part of a single unit.

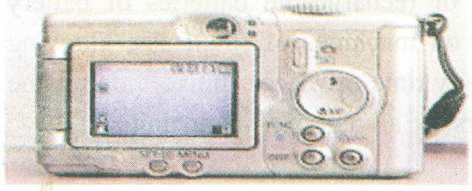
i. Portable Media Player

A portable media player (PMP) or digital audio player, (DAP) is a consumer electronics device that is capable of storing and playing digital media such as audio, images, video, documents, etc. the data is typically stored on a hard drive, micro drive, or flash memory. In contrast, analog portable audio players play music from cassette tapes, or records. Often digital audio players are sold as MP3 players, even if they support other file formats.

j. Digital Still Camera

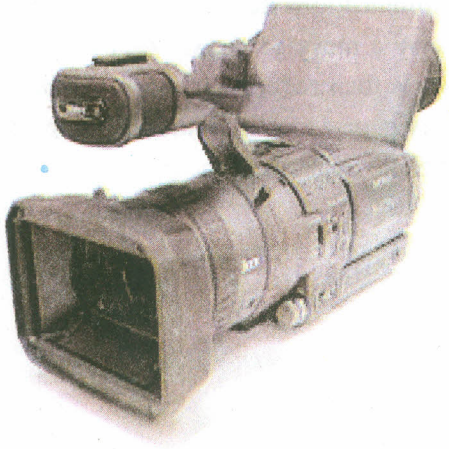
A digital camera (or digicam) DSC is a camera that takes video or still photographs, or both, digitally by recording images via an electronic image sensor. It is the main device used in the field of digital photography. Most 21st century cameras are digital.





k. Digital Video Camera

DVC or digital camcorder: A video camera is a camera used for electronic motion picture acquisition, initially developed by the television industry but now common in other applications as well Video cameras are used primarily in two modes. The first, characteristic of much early broadcasting, is live television, where the camera feeds real time images directly to a screen for immediate observation. In the second mode the images are recorded to a storage device for archiving or further processing; for many years, videotape was the primary format used for this purpose, but optical disc media, hard disk, and flash memory in tapeless camcorders are all increasingly used.



l. Mobile Phone

A mobile phone (also known as a cellular phone, cell phone and a hand phone) is a device that can make and receive telephone calls over a radio link whilst moving around a wide geographic area. It does so by connecting to a cellular network provided by a mobile phone operator, allowing access to the public telephone network. By contrast, a cordless telephone is used only within the short range of a single, private base station.

m. Smartphone and Feature Phone

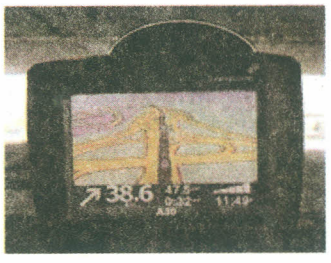
A smart phone is a high-end mobile phone built on a mobile computing platform, with more advanced computing ability and connectivity than a contemporary feature phone. The first smartphones were devices that mainly combined the functions of a personal digital assistant (PDA) and a mobile phone or camera phone. Today's models also serve to combine the functions of portable media players, low-end compact digital cameras, pocket video cameras, and GPS navigation units. Modern smartphones typically also include high-resolution touch screens, web browsers that can access and properly display standard web pages rather than just mobile-optimized sites, and high-speed data access via Wi-Fi and mobile broadband.

n. Pager

A beeper is a simple personal telecommunications device for short messages. A one-way numeric pager can only receive a message consisting of a few digits, typically a phone number that the user is then requested to call. Alphanumeric pagers are available, as well as two-way pagers that have the ability to send and receive email, numeric pages, and SMS messages

o. Personal Navigation Device

It is known as Personal Navigation Device or Portable Navigation Device (PND) is a portable electronic product which combines a positioning capability (such as GPS) and navigation functions.



2.3.2.3 Portable Wireless

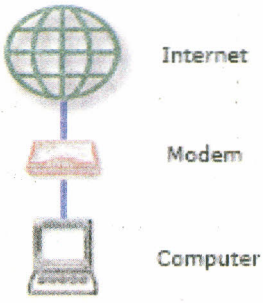
The operation of autonomous, battery-powered wireless devices or systems outside the office, home, or vehicle; examples include handheld cell phones and PCS units.

Portable wireless device can be anything which is small in size and work without wire.

Some computer portable devices are explained below:

a. Wireless Router

A standard modem allows you to connect one computer to the internet at a time.



A **Wireless router** is a device that performs the functions of a router but also includes the functions of a wireless access point and a network switch. They are commonly used to allow access to the Internet or a computer network without the need for a cabled connection. It can function in a wired LAN (local area network), a wireless only LAN (WLAN) or a mixed wired/wireless network. Most current wireless routers have the following characteristics:

LAN ports which function in the same manner as the ports of a network switch. A WAN port connects to a wide area network, typically one with Internet access. External destinations are accessed using this port. If it is not used, many functions of the router will be bypassed.

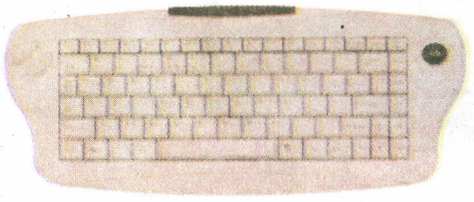
A wireless antenna allows connections from other wireless devices (NICs (network interface cards), wireless repeaters, wireless access points, and wireless bridges, for example), usually using the Wi-Fi standard.

b. Wireless Mouse

Cordless or wireless mice transmit data via infrared radiation or radio (including Bluetooth). The receiver is connected to the computer through a serial or USB port. The newer nano receivers were designed to be small enough to remain connected in a laptop or notebook computer during transport, while still being large enough to easily remove.

c. Wireless Keyboard

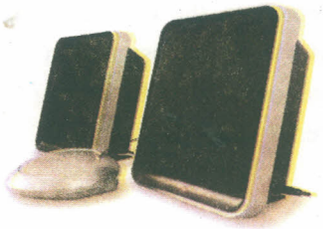
A wireless keyboard works just like a television remote or wireless video game controller. There is something on the computer which receives input signals and sends them to the CPU for quick processing and then finally it's displayed on the computer monitor as the appropriate result.



d. Wireless Speakers

Wireless speakers are very similar to traditional (wired) loudspeakers, but they transmit audio signals using radio frequency (RF) waves rather than over audio cables.

Wireless speakers are composed of two units: a main speaker unit combining the loudspeaker itself with an RF receiver, and an RF transmitter unit. The transmitter connects to the audio output of any audio devices such as hi-fi equipment, televisions, computers, mp3 players, etc. An RCA plug is normally used to achieve this. The receiver is positioned where the listener wants the sound to be, providing the freedom to move the wireless speakers around without the need of using cables. The receiver/speaker unit generally contains an amplifier to boost the audio signal to the loudspeaker; it is powered either by batteries or by an AC electric outlet. Batteries may last for three to four hours; some wireless speakers operate on rechargeable batteries.



2.3.2.4 IR Wireless

The use of devices that convey data via IR (infrared) radiation; employed in certain limited-range communications and control systems.

The Infrared Data Association (IrDA) defines physical specifications communications protocol standards for the short-range exchange of data over infrared light, for uses such as personal area networks (PANs).

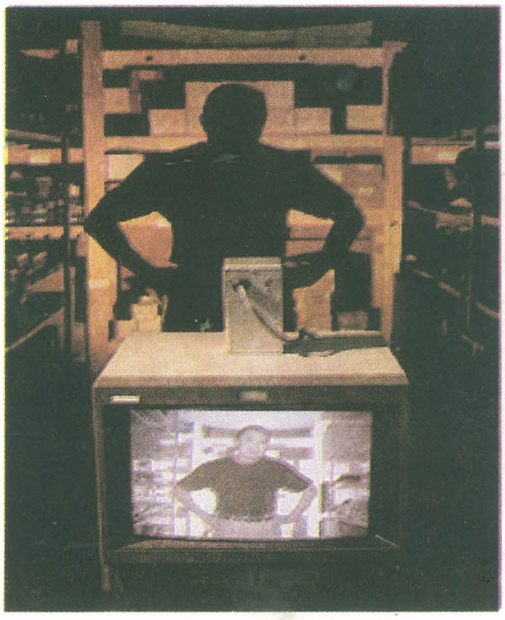
- IrDA is a very short-range example of free space optical communication.
- IrDA interfaces are used in medical instrumentation, test and measurement equipment, palmtop computers, mobile phones, and laptop computers (most laptops and phones also offer Bluetooth but it is now becoming more common for Bluetooth to simply replace IrDA in new versions of products).
- IrDA specifications include IrPHY, IrLAP, IrLMP, IrCOMM, Tiny TP, IrOBEX, IrLAN and IrSimple. IrDA has now produced another standard, IrFM, for Infrared financial messaging (i.e., for making payments) also known as Point & Pay.

For the devices to communicate via IrDA, they must have a direct line of sight similar to a TV remote control.

Some of the Infrared devices are as follows:

a. Night Vision Camera

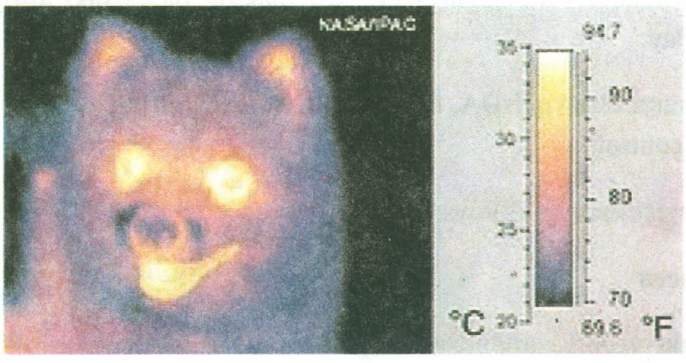
Infrared is used in night vision equipment when there is insufficient visible light to see. Night vision devices operate through a process involving the conversion of ambient light photons into electrons which are then amplified by a chemical and electrical process and then converted back into visible light. Infrared light sources can be used to augment the available ambient light for conversion by night vision devices, increasing in-the-dark visibility without actually using a visible light source.



Active-infrared night vision: the camera illuminates the scene at infrared wavelengths invisible to the human eye. Despite a dark back-lit scene, active-infrared night vision delivers identifying details, as seen on the display monitor.

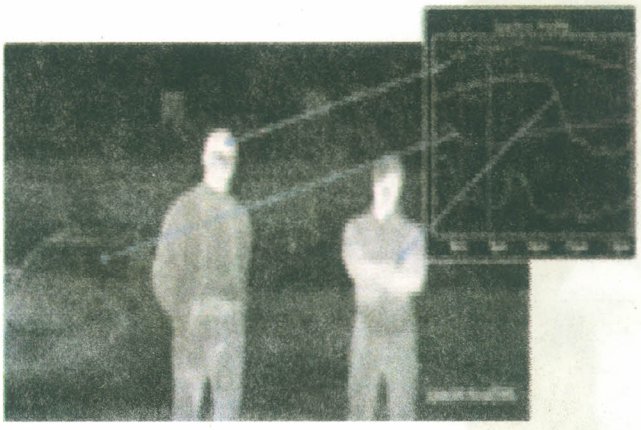
b. Thermographic Cameras

This detects radiation in the infrared range of the electromagnetic spectrum (roughly 900–14,000 nanometers or 0.9–14 μm) and produce images of that radiation. Since infrared radiation is emitted by all objects based on their temperatures, according to the black body radiation law, thermography makes it possible to see one's environment with or without visible illumination. The amount of radiation emitted by an object increases with temperature, therefore thermography allows one to see variations in temperature.



c. Hyperspectral Camera

Thermal Infrared Hyperspectral Camera can be applied similarly to a Thermographic camera, with the fundamental difference that each pixel contains a full LWIR spectrum. Consequently, chemical identification of the object can be performed without a need for an external light source such as the Sun or the Moon. Such cameras are typically applied for geological measurements, outdoor surveillance and UAV applications.



Hyperspectral thermal infrared emission measurement, an outdoor scan in winter conditions, ambient temperature -15°C, image produced with a Specim LWIR hyperspectral imager. Relative radiance spectra from various targets in

the image are shown with arrows. The infrared spectra of the different objects such as the watch clasp have clearly distinctive characteristics. The contrast level indicates the temperature of the object.

2.4 ADVANTAGES OF WIRELESS DEVICES

Many consumer electronics can be purchased in cordless or wireless versions, giving individuals more freedom. Wireless devices require little effort to use and give consumers a great deal of flexibility with less clutter and fuss.

Less Clutter

- Devices such as printers, mice, keyboards, and game controllers all can be found in wireless versions.
- When you are at your desk studying or working, you do not have to untangle all of the wires from your mouse, keyboard or your printer if you purchase a device that uses a wireless connection.
- Game controllers are also wireless now, which gives other people the freedom to walk past the TV without tripping over the remote control's cabling.

Freedom and Flexibility

- Devices such as wireless headphones, WiFi computers, cordless land-line phones, and cell phones are all very flexible, especially if you are a busy person.
- Buy wireless headphones if you do not want a cord interfering with your work while doing chores such as cooking, cleaning, and doing laundry.
- Cordless phones and cell phones have already been popular for some time. Cordless phones are portable land-line phones which you can carry a short distance from their base station. Cell phones can be used just about anywhere you can receive a signal. You can go just about anywhere with your laptop or netbook and stay connected to a network via a wireless signal.
- Wireless routers provide Internet access for your portable computer without the hassle of attaching cables to your laptop. You can also go anywhere you like within the range of a wireless router while on the Internet.

Handy

- Garage door openers gives you the ease of not having to get out of your car just to open your garage door. All you need to do is keep the garage door opener/remote in your car and press the button on the remote and the garage will open. Alarm systems such as Life Alert for seniors is a convenient way for them to get help for emergencies. It only takes a quick click of a button and then help is on the way.

2.5 APPLICATIONS OF WIRELESS DEVICES

Applications of Wireless Devices are:

- Global System for Mobile Communication (GSM) -- a digital mobile telephone system used in Europe and other parts of the world; the de facto wireless telephone standard in Europe
- General Packet Radio Service (GPRS) -- a packet-based wireless communication service that provides continuous connection to the Internet for mobile phone and computer users
- Enhanced Data GSM Environment (EDGE) -- a faster version of the Global System for Mobile (GSM) wireless service
- Universal Mobile Telecommunications System (UMTS) -- a broadband, packet-based system offering a consistent set of services to mobile computer and phone users no matter where they are located in the world
- Wireless Application Protocol (WAP) -- a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access
- i-Mode -- the world's first "smart phone" for Web browsing, provides color and video over telephone sets.
- Telemetry control and traffic control systems
- Infrared and ultrasonic remote control devices
- Modulated laser light systems for point to point communications
- Professional LMR (Land Mobile Radio) and SMR (Specialized Mobile Radio) typically used by business, industrial and Public Safety entities.
- Consumer Two way radio including FRS Family Radio Service, GMRS (General Mobile Radio Service) and Citizens band ("CB") radios.
- Airband and radio navigation equipment used by aviators and air traffic control.

- Cellular telephones and pagers: provide connectivity for portable and mobile applications, both personal and business.
- Global Positioning System (GPS): allows drivers of cars and trucks, captains of boats and ships, and pilots of aircraft to ascertain their location anywhere on earth.
- Cordless computer peripherals: the cordless mouse is a common example; keyboards and printers can also be linked to a computer via wireless using technology such as Wireless USB or Bluetooth.
- Cordless telephone sets: these are limited-range devices, not to be confused with cell phones.
- Satellite television: Is broadcast from satellites in geostationary orbit. Typical services use direct broadcast satellite to provide multiple television channels to viewers.
- Home-entertainment-system control boxes -- the VCR control and the TV channel control.
- Hi-fi sound systems and FM broadcast receivers also use this technology.
- Remote garage-door openers -- one of the oldest wireless devices in common use by consumers; usually operates at radio frequencies.
- Two-way radios -- this includes Amateur and Citizens Radio Service, as well as business, marine, and military communications.
- Baby monitors -- these devices are simplified radio transmitter/receiver units with limited range.
- Satellite television -- allows viewers in almost any location to select from hundreds of channels.
- Wireless LANs or local area networks -- provide flexibility and reliability for business computer users.
- Mobile telephones (cellular phone) with more than 5 billion mobile cellular subscriptions worldwide. 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.

2.6 WIRELESS DEVICES-HEALTH ISSUES

Communication devices such as cell phones, global positioning systems, and computers all use wireless technology. It is estimated that over one million

people worldwide use cell phones and that over three quarters of the earth is considered under the blanket of wireless technology. This means that most of the planet is subject to radio waves apart from natural radio and electromagnetic wave fields. Scientists and other community health working groups regularly address radiation exposure to provide information so people can make informed decisions regarding wireless technology.

Cell phones use wireless technology created by radio waves, which are on the lowest level of the electromagnetic wave spectrum. While most waves are propelled forward by molecular action, electromagnetic waves create energy by moving electric and magnetic fields back and forth. It has long been disputed whether large doses of these waves and the fields creating them are safe to humans.

Cell phones, cell towers, wi-fi, smart meters, DECT phones, cordless phones, baby monitors and other wireless devices all emit non ionizing radio frequencies, which the World Health Organization (WHO) has classified

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What is a wireless device?

.....

.....

.....

.....

2) List two advantages and disadvantages of Wireless technology.

.....

.....

.....

.....

3) Define Bluetooth.

.....

.....

.....

.....

4) How do you find out if the Mac has Bluetooth?

.....

.....

.....

.....

5) Mention some Wireless Applications.

.....

.....

.....

.....

2.7 LET US SUM UP

Wireless devices continue to change rapidly. While no one is quite sure what the ultimate wireless device(s) will be, there is definitely a need to ensure that devices can function with one another. There is also the need for a truly global wireless communication infrastructure with sufficiently high bandwidth to satisfy the needs of wireless applications. The establishment of a wireless infrastructure costs a great deal, and there will be many difficulties ahead for the companies paving the way for new technologies, but the long-term prospects look good for the companies that survive.

2.8 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) A wireless device is one that has connectivity to the Internet without being physically plugged into a network with a wire.

   The most common examples of these are the Internet-enabled cell phone such as a WAP Phone or i-Mode phone, personal digital assistant (PDA) such as Palm VII, Pocket PC such as Wireless iPaq, and pager.

2) A wireless technology offers advantages and disadvantages compared to a wired network.

   Advantages of wireless include: mobility and elimination of unsightly cables. Disadvantages of wireless include: the potential for radio interference due to weather, other wireless devices, or obstructions like walls.

3) Bluetooth is a technology that makes short-range wireless connections between devices (such as your Mac and your mouse or keyboard) at distances up to 10 meters (33 feet).

   The Bluetooth-enabled iPhone can act as a modem for your Mac through the wireless service provider.

4) Most Mac computers come with Bluetooth technology built-in. To determine whether the computer supports Bluetooth do one of the following:

   - Look for the Bluetooth Icon  in the menu bar. If the Bluetooth icon is present, the computer has Bluetooth.
   - Choose **System Preferences** from the **Apple** (🍎) menu and **Bluetooth** from the **View** menu. If the Bluetooth preference lists options for enabling Bluetooth and making your device discoverable, Bluetooth is installed.
   - From the **Apple** (🍎) menu choose **About this Mac**, then click More Info. Select Bluetooth from the Hardware section. If the Hardware Setting section populated with information, your system has Bluetooth installed.

5) Wireless is quickly emerging into many new applications:

   - networking computers
   - allowing remote monitoring and data acquisition
   - providing access control and security

   Wireless ideally accommodates environments where wires are impossible, such as vehicles and hand-held devices. Most wireless products can be categorized by application, some of which include the following:
   Voice and Messaging:

      - Cordless phones
      - Cellular phones
      - Beepers, pagers, and messaging systems
      - Wireless e-mail systems
      - CB Radio
      - Commercial two-way business radios
      - Intercom systems

Computer Networking:

- Wireless Local Area Networks (WLANs)
- Infrared (IR) ports on computers, printers, and other devices
- Radio modems

Remote Data Acquisition:

- Personal Digital Assistants (PDA's)
- Radio Frequency (RF) modems

Commercial Home Products:

- Security and access control
- 900 MHz stereo distribution
- Temperature control systems
- Remote control
  - Keyless entry systems
  - Garage door openers
  - Remote Controlled toys
  - TV remotes

Global Positioning Systems (GPS)

- Aviation navigation
- Nautical navigation
- Roadway navigation

Radio Frequency Identification technology (RFID)

- Tags and readers - Inventory Control, Animal migration/tracking
- Smart cards - Access control, Identification, Debit cards
- Merchant RF security tags

Many other applications exist. In fact, many companies take existing products, cluttered with wires, and make them wireless.

2.9 SUGGESTED READINGS

- Quinn, C. (2006). Qualcomm, *Inc. In Metcalf, D. mLearning: Mobile Learning and Performance in the Palm of Your Hand.*
- Quinn, C. (2007). *Don't dream it, do it: m-Learning by design. In S. Wexler (Ed.) Guild Research 360° Report on Mobile Learning.*
- Rappaport, T S. (2002).*Wireless Communications: Principles and Practice,* 2nd Ed. Prentice Hall.
- Stallings, W. (2005). *Wireless Communications and Networks*,2nd Ed., Prentice Hall

UNIT 3 SECURING WIRELESS NETWORK

Structure

3.0 INTRODUCTION

Today's global workforce is extremely mobile. This mobile global environment has put a great deal of strain on both wired and wireless networks. The rise in the demand of smart-phones and laptops has also increased the strain on already exhausted wireless networks (Lin, 2006) Corporations and individuals demand high speed, mobile networks that support high bandwidth applications to perform their everyday activities (Agarwal, 2006). The advent of wireless networking has raised some very compelling issues. Most important are security issues. Other issues can be legal and social. Since their emergence in the 1970s, wireless networks have become increasingly popular in the computing industry. This is particularly true within the past decade which has seen wireless networks being adapted to enable mobility. Wireless networks are emerging fast as latest technology to allow users to access information and services via electronic media, without taking geographic position in account. Mobile hosts and wireless networking hardware are becoming widely available, and extensive work has been done recently in integrating these elements into traditional networks such as the internet. Wireless networks have taken the world by storm. Enterprises and people using computer at home are avoiding the expenses and delays associated with installing wired networks. High speed internet facility is enjoyed by travellers all over the places worldwide. Along with increases in throughput, wireless networks remain unlicensed and affordable. This has further helped their exponential growth in businesses, homes, communities and open spaces. Wireless networks are not robust enough to support all this demand, and there is a tradeoff between network speed and security due to the shared medium in unlicensed frequency channels (Agarwal, 2006). Wireless networks are not as secure as wired networks because it is easier to access radio channels than to access wired lines. If security is the top priority for a wireless network, then bandwidth is comprised and error rates increase. Wireless networks are not meant to replace wired arrangements hence the challenge faced by IT professionals to develop the adequate wireless infrastructure to support high bandwidth needs (Haleem, 2007) (Sun, 2007). Many other security risks exist that organizations have to account for. But the recent surge in demand for data services on wireless networks highlights the importance of protecting wireless networks in this mobile business environment. And because the wireless revolution is at its infancy stage, the research on providing adequate wireless security is also at its infancy stage (Issac, 2007). Furthermore, the research and analysis on the extent system performance is altered by different security procedures, in

multiple mobility scenarios, different applications, and heterogeneous networks is limited (Agarwal, 2006). The wireless revolution began in the late 1990s when different wireless standards were produced (known as 802.11 standards). In wireless arrangements, devices such as computers and routers are connected through radio waves or infrared technologies. The two wireless setups currently constructed are peer-to-peer or access point (Vakil, 2005). In the peer-to-peer environment, computers communicate with other wireless enabled computers via network interface cards. While in the access point environment, computers communicate with other computers through an access point such as a router. Access points are a critical part of wired and wireless infrastructures. An access point, also known as a node, is a stationary base posting that connects wired and wireless networks together. Cyber criminals continuously seek vulnerable access points to initiate security threats (Issac, 2007) (Teo, 2007).

There are currently two variations of mobile wireless networks. The first is known as infrastructure networks, i.e., those networks with fixed and wired gateways. The bridges for these networks are known as base stations. A mobile unit within these networks connects to, and communicates with, the nearest base station that is within its communication radius. Typical applications of this type of network include office wireless local area networks (WLANs). The second type of mobile wireless network is the infrastructure less mobile network, commonly known as an ad-hoc network. A 'mobile adhoc network' is an autonomous system of mobile hosts which are free to move around randomly and organise themselves arbitrarily.

3.1 OBJECTIVES

After going through this Unit, you should be able to:

- describe the need of security;
- explain security issues related to wireless network;
- identify Modes of unauthorized access;
- explain Wireless intrusion prevention concepts;
- describe wireless intrusion prevention system;
- describe Wireless security best practices; and
- enumerate Additional steps taken to secure the wireless network.

3.2 NEED OF SECURITY

Over a decade or so there have been tremendous changes in the way people communicate. Description of computing device has changed from PC to communication systems, PDAs, smart phones and so on. Moreover there are

over one billion subscribers using mobile phone technology as opposed to the number of PCs installed. The new computing devices have the capacity to transmit data in its varying forms, not only to similar devices, but also to different devices across a network. Mobile internet and mobile network are reality now.

The convergence of technologies has made the devices and the network upon which they operate, more interchangeable than ever before with their overlapping applications. The market is also using latest technology as in E-Commerce which uses B2B (Business to Business), B2C (Business to Consumer), G2G (Government to Government) and G2C (Government to Citizen) all requiring data exchanges. Also some private communication systems like VPN (virtual private network) and VPA (virtual private access) uses a lot of communication between two networks.

According to IDC sources, Global internet commerce is expected to hit US$ 1 trillion by the end of 2004. With so much abundance of networking, it is becoming more and more needful to have a secured transmission and so security has become a major element in both hardware and the application software. It is being argued that, though a high degree of transmission is already in process, the number would be much greater if data security could be guaranteed. To ensure future growth of markets and their applications, a high degree of security is required, due to potentially high commercial value of both the business and private data is being submitted. The need for security arises due to:

- Growth of mobile internet access and applications,
- Individual user requirements and Corporations (business or governmental) who both require internal and external
- Contact and data transfer through remote places

3.3 SECURITY ISSUES

Security is an important issue for wireless networks, especially for those security sensitive applications. Many users of data transmission devices (such as laptops, PDAs, PCs, phones, etc.) demand for Protecting data residing within devices, protecting the transmission network, protecting transfer of data, and ensuring proper transfer. One of the goals of current wireless standard was to provide security and privacy that was 'Wired equivalent' and to meet this goal, several security mechanisms were provided for confidentiality, authentication, and access control. Unfortunately all of these can be easily broken. Points to consider as security parameters are:

(a) **Identity:** An essential element in any security system is reliable, robust non-malleable identity.

(b) **Access control:** Access control is the constraint that limits those who can utilize system resources. Two approaches are used, one is called 'access control list (ACL)' and other as 'closed network'.

(c) **Authentication:** It ensures that communication from one node to other is genuine. Only legitimate users can access the system and services. Two used systems are 'open system' and 'shared key'.

(d) **Availability:** Availability ensures the service offered by node will be available to its users when expected, in spite of attacks. Also only legitimate users can access data anytime.

(e) **Integrity:** It protects nodes from maliciously altered messages. The receiver wants to be sure that the source is genuine. It assures the data, system or platform has not been tampered with.

(f) **Non repudiation:** It ensures that the origin of the message cannot deny having sent the message.

(g) **Confidentiality:** It ensures that certain information is never disclosed to unauthorized entities. Personal or sensitive data is protected.

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. Without properly setting up, a user sets themselves up for certain risks that could be prevented or at least halted. Using even the most basic form of protection is better than nothing.

Most common types of wireless security are:-

1. Wired Equivalent Privacy (WEP) and
2. Wi-Fi Protected Access (WPA)

WEP is one of the least secure forms of security. A network that is secured with WEP has been cracked in 3 minutes by the FBI. WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or Wi-Fi Protected Access. WPA was a quick alternative for those wishing to get away from the problematic WEP security. There are some pieces of hardware that cannot support WPA2 without being replaced or having the firmware upgraded. WPA2 uses a encryption device which encrypts the network with a 256 bit key. This adds a multitude of security more than WEP does to the wireless network.

Many laptop computers have **wireless cards** pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues.

Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. As a result, it's very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources.

Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies. The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Crackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. However, there are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge.

Some organizations that have no **wireless access points** installed do not feel that they need to address wireless security concerns.

Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A cracker could sit out in the parking lot and gather info from it through laptops and/or other devices as handhelds, or even break in through this wireless card-equipped laptop and gain access to the wired network.

Anyone within the geographical network range of an open, unencrypted wireless network can **'sniff'** or capture or record the **traffic**, gain unauthorized access to internal network resources as well as to the internet, and then possibly send spam or do other illegal actions using the wireless network's **IP address**, all of which are rare for home routers but may be significant concerns for office networks.

If router security is not activated or if the owner deactivates it for convenience, it creates a free **hotspot**. Since most 21st century laptop PCs have wireless networking built in, they don't need a third-party adapter such as a **PCM CIA Card** or **USB dongle**. Built in wireless networking might be enabled by default, without the owner realizing it, thus broadcasting the laptop's accessibility to any computer nearby.

Modern operating systems such as Linux, Mac OS, or Microsoft Windows make it fairly easy to set up a PC as a wireless LAN 'base station' using Internet Connection Sharing, thus allowing all the PCs in the home to access the Internet via the 'base' PC. However, lack of knowledge about the security issues in setting up such systems often means that someone nearby

may also use the connection. Such piggybacking is usually achieved without the wireless network operators knowledge; it may even be without the knowledge of the intruding user if their computer automatically selects a nearby unsecured wireless network to use as an access point.

3.4 THREATS

Wireless security is an aspect of computer security. All organizations with any number of members or employees are particularly vulnerable to security breaches caused by rogue access points. If an employee (trusted entity) in a location brings in an easily available **wireless router**, the entire network can be exposed to anyone within range of the signals. If an employee adds a wireless interface to a networked computer via an open USB port, the very same risk may be spread for the respective network. However, for any of these entities concepts are available to protect the computer and the network. Such protection must be applied to all levels of communication, to all entities networked and to all functions used and data processed. Information Technology security threats to organizations have increased dramatically as technology has developed. The Internet provides tremendous opportunities for corporations to reach customers and partner organizations efficiently and creatively. But with this opportunity, there are increased threats from outside and inside domains. Employees of an organization can harm Local area networks intentionally or unintentionally. Cyber criminals are constantly seeking to destroy and reap benefits from weak network infrastructures.

3.5 THE MOBILITY ADVANTAGES

Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. As a result, it's very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

3.5.1 The Air Interface and Link Corruption Risk

There were relatively few dangers when wireless technology was first introduced, as the effort to maintain the communication was high and the effort to intrude is always higher. The variety of risks to users of wireless technology have increased as the service has become more popular and the technology

more commonly available. Today there are a great number of security risks associated with the current wireless protocols and encryption methods, as carelessness and ignorance exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless.

3.6 MODES OF UNAUTHORIZED ACCESS

The modes of unauthorised access to links, to functions and to data are as variable as the respective entities make use of program code. There does not exist a full scope model of such threat. To some extent the prevention relies on known modes and methods of attack and relevant methods for suppression of the applied methods. However, each new mode of operation will create new options of threatening. Hence prevention requires a steady thrive for improvement. The described modes of attack are just a snapshot of typical methods and scenarios where to apply.

3.6.1 Accidental Association

Violation of security perimeter of corporate network can come from a number of different methods and intents. One of these methods is referred to as "accidental association". When a user turns on a computer and it latches on to a wireless access point from a neighboring company's overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network.

Accidental association is a case of wireless vulnerability called as mis-association. It can be accidental, deliberate (for example, done to bypass corporate firewall) or it can result from deliberate attempts on wireless clients to lure them into connecting to attacker's APs.

3.6.2 Malicious Association

Malicious associations are when wireless devices can be actively made by attackers to connect to a company network through their cracking laptop instead of a company access point (AP). These types of laptops are known as "soft APs" and are created when a cyber criminal runs some software that makes his/her wireless network card look like a legitimate access point.

Once the thief has gained access, he/she can steal passwords, launch attacks on the wired network, or plant trojans. Since wireless networks operate at the Layer 2 level, Layer 3 protections such as network authentication and virtual private networks (VPNs) offer no barrier. Wireless 802.1x authentications do help with protection but are still vulnerable to cracking. The idea behind this

type of attack may not be to break into a VPN or other security measures. Most likely the criminal is just trying to take over the client at the Layer 2 level.

3.6.3 Ad-hoc Networks

Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

The security hole provided by Ad-hoc networking is not the Ad-hoc network itself but the bridge it provides into other networks, usually in the corporate environment, and the unfortunate default settings in most versions of Microsoft Windows to have this feature turned on unless explicitly disabled. Thus the user may not even know they have an unsecured Ad-hoc network in operation on their computer. If they are also using a wired or wireless infrastructure network at the same time, they are providing a bridge to the secured organizational network through the unsecured Ad-hoc connection.

Bridging is in two forms

- A direct bridge, which requires the user actually configure a bridge between the two connections and is thus unlikely to be initiated unless explicitly desired, and
- An indirect bridge which is the shared resources on the user computer. The indirect bridge provides two security hazards:
  - The first is that critical organizational data obtained via the secured network may be on the user's end node computer drive and thus exposed to discovery via the unsecured Ad-hoc network.
  - The second is that a computer virus or otherwise undesirable code may be placed on the user's computer via the unsecured Ad-hoc connection and thus has a route to the organizational secured network. In this case, the person placing the malicious code need not "crack" the passwords to the organizational network; the legitimate user has provided access via a normal and routine log-in. The malfactor needs to place the malicious code on the unsuspecting user's end node system via the open (unsecured) Ad-hoc networks.

3.6.4 Non-traditional Networks

Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured.

These non-traditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.

3.6.5 Identity Theft (MAC spoofing)

Identity theft (or MAC spoofing) occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to only allow authorized computers with specific MAC IDs to gain access and utilize the network. However, a number of programs exist that have network "sniffing" capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires, and the cracker can easily get around that hurdle.

MAC filtering is only effective for small residential (SOHO) networks, since it only provides protection when the wireless device is "off the air". Any 802.11 device "on the air" freely transmits its unencrypted MAC address in its 802.11 headers, and it requires no special equipment or software to detect it. Anyone with an 802.11 receiver (laptop and wireless adapter) and a freeware wireless packet analyzer can obtain the MAC address of any transmitting 802.11 within range. In an organizational environment, where most wireless devices are "on the air" throughout the active working shift, MAC filtering only provides a false sense of security since it only prevents "casual" or unintended connections to the organizational infrastructure and does nothing to prevent a directed attack.

3.6.6 Man-in-the-Middle Attacks

A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a "de-authentication attack". This attack forces AP-connected computers to drop their connections and reconnect with the cracker's soft AP. Man-in-the-middle attacks are enhanced by software such as LAN jack and Air Jack, which automate multiple steps of the process. What once required some skill can now be done by script kiddies. Hotspots are particularly vulnerable to any attack since there is little to no security on these networks.

3.6.7 Denial of Service

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network

and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

The DoS attack in itself does little to expose organizational data to a malicious attacker, since the interruption of the network prevents the flow of data and actually indirectly protects data by preventing it from being transmitted. The usual reason for performing a DoS attack is to observe the recovery of the wireless network, during which all of the initial handshake codes are re-transmitted by all devices, providing an opportunity for the malicious attacker to record these codes and use various "cracking" tools to analyze security weaknesses and exploit them to gain unauthorized access to the system. This works best on weakly encrypted systems such as WEP, where there are a number of tools available which can launch a dictionary style attack of "possibly accepted" security keys based on the "model" security key captured during the network recovery.

3.7 WIRELESS INTRUSION PREVENTION CONCEPTS

There are three principal ways to secure a wireless network

- **Closed networks** (like home users and organizations)

  The most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address. Another option is to disable ESSID broadcasting, making the access point difficult for outsiders to detect. Wireless Intrusion Prevention Systems can be used to provide wireless LAN security in this network model.

- **Commercial providers** (hotspots and large organizations)

  The preferred solution is often to have an open and unencrypted, but completely isolated wireless network. The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN.

- **Wireless networks**

  They are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it's also often possible for remote intruders to gain access to the network through backdoors. One

general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public.

There is no ready designed system to prevent from fraudulent usage of wireless communication or to protect data and functions with wirelessly communicating computers and other entities. However there is a system of qualifying the taken measures as a whole according to a common understanding that shall be seen as state of the art.

3.7.1 Wireless Intrusion Prevention System

A Wireless Intrusion Prevention System (WIPS) is a concept for the most robust way to counteract wireless security risks. However such WIPS does not exist as a ready designed solution to implement as a software package. A WIPS is typically implemented as an overlay to an existing Wireless LAN infrastructure, although it may be deployed standalone to enforce no-wireless policies within an organization. WIPS is considered so important to wireless security; the Payment Card Industry Security Standards Council published wireless guidelines for PCI DSS recommending the use of WIPS to automate wireless scanning and protection for large organizations.

3.8 WIRELESS SECURITY BEST PRACTICES

3.8.1 MAC ID Filtering

One of the simplest techniques is to only allow access from known, approved MAC addresses. However, this approach gives no security against sniffing, and client devices can easily spoof MAC addresses, leading to the need for more advanced security measures. Most wireless access points contain some type of MAC ID filtering that allows the administrator to only permit access to computers that have wireless functionalities that contain certain MAC IDs.

Some access points can also support "AP isolation" which isolates all wireless clients and wireless devices on the network from each other. Wireless devices will be able to communicate with the gateway but not with each other in the network.

Unlike IP addresses, MAC addresses are unique to specific network adapters, so by turning on MAC filtering we can limit network access to only our systems. In order to use MAC filtering we need to find (and enter into the router or AP) the 12-character MAC address of every system that will connect to the network, so it can be inconvenient to set up, especially if we have a lot of wireless clients or if our clients change a lot. MAC addresses can be "spoofed" (imitated) by a knowledgeable person, so while it's not a guarantee of security, it does add another hurdle for potential intruders to jump.

Every NIC has its own unique MAC address, and wireless access points can be configured to block all but a handful of specified NICs. The problem with filtering by MAC address, however, is that these addresses are easily faked and readily detected by anyone using appropriate monitoring software. In addition, this approach requires a great deal of overhead in corporate environments, and even for a large home network with multiple machines and gadgets (consoles, phones, and consumer electronics) it quickly becomes untenable.

Filtering MAC addresses is the only one with even a minimal level of value. MAC address filtering can keep obnoxious and non-tech-savvy neighbors from easily freeloading on our wireless network, but it won't do much else. To keep more determined intruders off of our network, we'll have to use encryption. A wireless network can broadcast far outside our building. With a powerful antenna and some widely available hacking software, anyone sitting near our installation—or even driving by—can passively (without alerting the target) scan all the data flowing in our network.

3.8.2 Static IP Addressing

Disabling at least the IP Address assignment function of the network's DHCP server, with the IP addresses of the various network devices then set by hand; will also make it more difficult for a casual or unsophisticated intruder to log onto the network. This is especially effective if the subnet size is also reduced from a standard default setting to what is absolutely necessary and if permitted but unused IP addresses are blocked by the access point's firewall. In this case, where no unused IP addresses are available, a new user can log on without detection using TCP/IP only if he or she stages a successful man in the Middle Attack using appropriate software.

3.8.3 WLANs 802.11 Security

3.8.3.1 Regular WEP

The Wired Equivalent Privacy (WEP) encryption standard was the original encryption standard for wireless. As its name implies, this standard was intended to make wireless networks as secure as wired networks. Unfortunately, this never happened as flaws were quickly discovered and exploited. There are several open source utilities like air cracking, weplab, WEPCrack, or airsnort that can be used by crackers to break in by examining packets and looking for patterns in the encryption. WEP comes in different key sizes. The common key lengths are currently 128- and 256-bit. The longer the better as it will increase the difficulty for crackers. However, this type of encryption is now being considered outdated and seriously flawed.

In 2005 a group from the FBI held a demonstration where they used publicly available tools to break a WEP encrypted network in three minutes. WEP protection is better than nothing, though generally not as secure as the more

sophisticated WPA-PSK encryption. A big problem is that if a cracker can receive packets on a network, it is only a matter of time until the WEP encryption is cracked.

WEP has some serious issues. First, it does not deal with the issue of key management at all. Either the keys have to be manually given to end users, or they have to be distributed in some other authentication method. Since WEP is a shared key system, the AP uses the same key as all the clients and the clients also share the same key with each other. A cracker would only have to compromise the key from a single user, and he would then know the key for all users.

3.8.3.2 WPAv1

The Wi-Fi Protected Access (WPA and WPA2) security protocols were later created to address the problems with WEP. If a weak password, such as a dictionary word or short character string is used, WPA and WPA2 can be cracked. Using a long enough random password (e.g. 14 random letters) or passphrase (e.g. 5 randomly chosen words) makes pre-shared key WPA virtually untraceable. The second generation of the WPA security protocol (WPA2) is based on the final IEEE 802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance. With all those encryption schemes, any client in the network that knows the keys can read all the traffic.

Wi-Fi Protected Access (WPA) is a software/firmware improvement over WEP. All regular WLAN-equipment that worked with WEP are able to be simply upgraded and no new equipment needs to be bought. WPA is a trimmed-down version of the 802.11i security standard that was developed by the IEEE 802.11 to replace WEP. The TKIP encryption algorithm was developed for WPA to provide improvements to WEP that could be fielded as firmware upgrades to existing 802.11 devices. The WPA profile also provides optional support for the AES-CCMP algorithm that is the preferred algorithm in 802.11i and WPA2.

WPA Enterprise provides RADIUS based authentication using 802.1x. WPA Personal uses a pre-shared Shared Key (PSK) to establish the security using an 8 to 63 character passphrase. The PSK may also be entered as a 64 character hexadecimal string. Weak PSK passphrases can be broken using off-line dictionary attacks by capturing the messages in the four-way exchange when the client reconnects after being de authenticated. Wireless suites such as air cracking can crack a weak passphrase in less than a minute. Other WEP/WPA crackers are Air Snort and Auditor Security Collection. Still, WPA Personal is secure when used with 'good' passphrases or a full 64-character hexadecimal key.

3.8.3.3 Additions to WPAv1

In addition to WPAv1, TKIP, WIDS and EAP may be added alongside. Also, VPN-networks (non-continuous secure network connections) may be set up under the 802.11-standard. VPN implementations include PPTP, L2TP, IPSec and SSH. However, this extra layer of security may also be cracked with tools such as Anger, Deceit and Ettercap for PPTP; and IKEProbe, ipsectrace, and IKEcrack for IPSec-connections.

3.8.3.3.1 TKIP

This stands for Temporal Key Integrity Protocol and the acronym is pronounced as tee-kip. This is part of the IEEE 802.11i standard. TKIP implements per-packet key mixing with a re-keying system and also provides a message integrity check. These avoid the problems of WEP.

3.8.3.3.2 EAP

The WPA-improvement over the IEEE 802.1X standard already improved the authentication and authorization for access of wireless and wired LANs. In addition to this, extra measures such as the Extensible Authentication Protocol (EAP) have initiated an even greater amount of security. This, as EAP uses a central authentication server. Unfortunately, during 2002 a Maryland professor discovered some shortcomings Over the next few years these shortcomings were addressed with the use of TLS and other enhancements. This new version of EAP is now called Extended EAP and is available in several versions; these include: EAP-MD5, PEAPv0, PEAPv1, EAP-MSCHAPv2, LEAP, EAP-FAST, EAP-TLS, EAP-TTLS, MSCHAv2, EAP-SIM.

3.8.3.3.2.1 EAP-versions

EAP-versions include LEAP, PEAP and other EAP's

LEAP

This stands for the Lightweight Extensible Authentication Protocol. This protocol is based on 802.1X and helps minimize the original security flaws by using WEP and a sophisticated key management system. This EAP-version is safer than EAP-MD5. This also uses MAC address authentication. LEAP is not safe against crackers. THC-Leap Cracker can be used to break Cisco's version of LEAP and be used against computers connected to an access point in the form of a dictionary attack. Anwrap and asleap finally are other crackers capable of breaking LEAP.

PEAP

This stands for Protected Extensible Authentication Protocol. This protocol allows for a secure transport of data, passwords, and encryption keys without the need of a certificate server. This was developed by Cisco, Microsoft, and RSA Security.

Other EAPs

There are other types of Extensible Authentication Protocol implementations that are based on the EAP framework. The framework that was established supports existing EAP types as well as future authentication methods. EAP-TLS offers very good protection because of its mutual authentication. Both the client and the network are authenticated using certificates and per-session WEP keys. EAP-FAST also offers good protection. EAP-TTLS is another alternative made by Certicom and Funk Software. It is more convenient as one does not need to distribute certificates to users, yet offers slightly less protection than EAP-TLS.

3.8.4 Restricted Access Networks

Solutions include a newer system for authentication, IEEE 802.1x, that promises to enhance security on both wired and wireless networks. Wireless access points that incorporate technologies like these often also have routers built in, thus becoming wireless gateways.

3.8.5 End-to-End Encryption

Both layer 2 and layer 3 encryption methods are not good enough for protecting valuable data like passwords and personal emails. Those technologies add encryption only to parts of the communication path, still allowing people to spy on the traffic if they have gained access to the wired network somehow. The solution may be encryption and authorization in the application layer, using technologies like SSL, SSH, GnuPG, PGP and similar.

The disadvantage with the end to end method is, it may fail to cover all traffic. With encryption on the router level or VPN, a single switch encrypts all traffic, even UDP and DNS lookups. With end-to-end encryption on the other hand, each service to be secured must have its encryption "turned on," and often every connection must also be "turned on" separately. For sending emails, every recipient must support the encryption method, and must exchange keys correctly. For Web, not all web sites offer https, and even if they do, the browser sends out IP addresses in clear text.

An office LAN owner seeking to restrict such access will face the non trivial enforcement task of having each user authenticate him for the router.

3.8.6 802.11i Security

The newest and most rigorous security to implement into WLAN's today is the 802.11i RSN-standard. This full-fledged 802.11i standard (which uses WPAv2) however does require the newest hardware (unlike WPAv1), thus potentially requiring the purchase of new equipment. This new hardware required may be either AES-WRAP (an early version of 802.11i) or the newer and better AES-CCMP-equipment. One should make sure one needs WRAP or CCMP-equipment, as the 2 hardware standards are not compatible.

3.8.6.1 WPAv2

WPA2 is a WiFi Alliance branded version of the final 802.11i standard. The primary enhancement over WPA is the inclusion of the AES-CCMP algorithm as a mandatory feature. Both WPA and WPA2 support EAP authentication methods using RADIUS servers and pre shared key (PSK).

Most of the world has switched their WAP from WEP to WPA2, since WEP has been proved too unsecured to be used. It is important to note there is a possible security flaw to the WPA protocol. It is referred to as Hole196. It is a hole in the protocol that exposes the user to insider attacks.

3.8.6.2 Additions to WPAv2

Unlike 802.1X, 802.11i already has additional security-services such as TKIP. Just as with WPAv1, WPAv2 may work in cooperation with EAP and a WIDS.

3.8.7 Smart Cards, USB Tokens and Software Tokens

This is a very strong form of security. When combined with some server software, the hardware or software card or token will use its internal identity code combined with a user entered PIN to create a powerful algorithm that will very frequently generate a new encryption code. The server will be time synced to the card or token. This is a very secure way to conduct wireless transmissions. Companies in this area make USB tokens, software tokens, and smart cards. They even make hardware versions that double as an employee picture badge. Currently the safest security measures are the smart cards / USB tokens. However, these are expensive. The next safest methods are WPA2 or WPA with a RADIUS server.

Any one of the three will provide a good base foundation for security.

The third item is to educate both employees and contractors on security risks and personal preventive measures. It is also IT's task to keep the company workers' knowledge base up-to-date on any new dangers that they should be cautious about. If the employees are educated, there will be a much lower chance that anyone will accidentally cause a breach in security by not locking down their laptop or bring in a wide open home access point to extend their

mobile range. Employees need to be made aware that company laptop security extends to outside of their site walls as well. This includes places such as coffee houses where workers can be at their most vulnerable. The last item deals with 24/7 active defense measures to ensure that the company network is secure and compliant.

This can take the form of regularly looking at access point, server, and firewall logs to try to detect any unusual activity. For instance, if any large files went through an access point in the early hours of the morning, a serious investigation into the incident would be called for. There are a number of software and hardware devices that can be used to supplement the usual logs and usual other safety measures.

3.8.8 RF Shielding

It's practical in some cases to apply specialized wall paint and window film to a room or building to significantly attenuate wireless signals, which keeps the signals from propagating outside a facility. This can significantly improve wireless security because it's difficult for hackers to receive the signals beyond the controlled area of an enterprise, such as within parking lots.

Despite security measures as encryption, hackers may still be able to crack them. This is done using several techniques and tools. An overview of them can be found at the Network encryption cracking article, to understand what we are dealing with. Understanding the mindset/techniques of the hacker allows one to better protect their system.

For closed networks (like home users and organizations) the most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address.

Another option is to disable ESSID broadcasting, making the access point difficult for outsiders to detect. Wireless Intrusion Prevention Systems can be used to provide wireless LAN security in this network model. For commercial providers, hotspots, and large organizations, the preferred solution is often to have an open and unencrypted, but completely isolated wireless network.

The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN. Wireless networks are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it's also often possible for remote intruders to gain access to the network through backdoors. One general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public.

3.9 MOBILE DEVICES

With increasing number of mobile devices with 802.1x interfaces, security of such mobile devices becomes a concern. While open standards such as Kismet are targeted towards securing laptops, access points solutions should extend towards covering mobile devices also. Host based solutions for mobile handsets and PDA's with 802.1x interface.

Security within mobile devices fall under three categories:

1. Protecting against ad-hoc networks
2. Connecting to rogue access points
3. Mutual authentication schemes such as WPA2

Wireless IPS solutions now offer wireless security for mobile devices. Mobile monitoring devices are becoming an integral part of any industry and these devices will eventually become the method of choice for accessing and implementing various issues for people located in remote areas.

3.10 IMPLEMENTING NETWORK ENCRYPTION

In order to implement 802.11i, one must first make sure both that the router/access point(s), as well as all client devices are indeed equipped to support the network encryption. If this is done, a server such as RADIUS, ADS, NDS, or LDAP needs to be integrated. This server can be a computer on the local network, an access point / router with integrated authentication server, or a remote server. AP's/routers with integrated authentication servers are often very expensive and specifically an option for commercial usage likes hot spots. Hosted 802.1X servers via the Internet require a monthly fee; running a private server is free yet has the disadvantage that one must set it up and that the server needs to be on continuously.

To set up a server, server and client software must be installed. Server software required is a enterprise authentication server such as RADIUS, ADS, NDS, or LDAP. The required software can be picked from various suppliers as Microsoft, Cisco, Funk Software, Meetinghouse Data, and from some open-source projects. Software includes:

- Cisco Secure Access Control Software
- Microsoft Internet Authentication Service
- Meetinghouse Data EAGIS
- Funk Software Steel Belted RADIUS (Odyssey)

- free RADIUS (open-source)
- Sky Friendz (free cloud solution based on free RADIUS)

Client software comes built-in with Windows XP and may be integrated into other OS's using any of following software:

- Intel PROSet/Wireless Software
- Cisco ACU-client
- Odyssey client
- AEGIS-client

3.10.1 RADIUS

This stands for Remote Authentication Dial in User Service. This is an AAA (authentication, authorization and accounting) protocol used for remote network access. This service provides an excellent weapon against crackers. RADIUS was originally proprietary but was later published under ISOC documents RFC 2138 and RFC 2139. The idea is to have an inside server act as a gatekeeper through the use of verifying identities through a username and password that is already pre-determined by the user. A RADIUS server can also be configured to enforce user policies and restrictions as well as recording accounting information such as time connected for billing purposes.

3.11 OPEN ACCESS POINTS

Today, there is almost full wireless network coverage in many urban areas - the infrastructure for the wireless community network (which some consider to be the future of the internet) is already in place. One could roam around and always be connected to Internet if the nodes were open to the public, but due to security concerns, most nodes are encrypted and the users don't know how to disable encryption. Many people consider it proper etiquette to leave access points open to the public, allowing free access to Internet. Others think the default encryption provides substantial protection at small inconvenience, against dangers of open access that they fear may be substantial even on a home DSL router.

The density of access points can even be a problem - there are a limited number of channels available, and they partly overlap. Each channel can handle multiple networks, but places with many private wireless networks (for example, apartment complexes), the limited number of Wi-Fi radio channels might cause slowness and other problems.

According to the advocates of Open Access Points, it shouldn't involve any significant risks to open up wireless networks for the public:

- The wireless network is after all confined to a small geographical area. A computer connected to the Internet and having improper configurations or other security problems can be exploited by anyone from anywhere in the world, while only clients in a small geographical range can exploit an open wireless access point. Thus the exposure is low with an open wireless access point, and the risks with having an open wireless network are small. However, one should be aware that an open wireless router will give access to the local network, often including access to file shares and printers.

- The only way to keep communication truly secure is to use end-to-end encryption. For example, when accessing an internet bank, one would almost always use strong encryption from the web browser and all the way to the bank - thus it shouldn't be risky to do banking over an unencrypted wireless network. The argument is that anyone can sniff the traffic applies to wired networks too, where system administrators and possible crackers have access to the links and can read the traffic. Also, anyone knowing the keys for an encrypted wireless network can gain access to the data being transferred over the network.

- If services like file shares, access to printers etc. are available on the local net, it is advisable to have authentication (i.e. by password) for accessing it (one should never assume that the private network is not accessible from the outside). Correctly set up, it should be safe to allow access to the local network to outsiders.

- With the most popular encryption algorithms today, a sniffer will usually be able to compute the network key in a few minutes. It is very common to pay a fixed monthly fee for the Internet connection and not for the traffic - thus extra traffic will not hurt. Where Internet connections are plentiful and cheap, freeloaders will seldom be a prominent nuisance.

3.12 ADDITIONAL STEPS TAKEN TO SECURE THE WIRELESS NETWORK

Certain wireless security best practices are recommended for every Wireless LAN deployment. Certain practices may not be possible due to deployment constraints.

Hiding the SSID

The SSID (Service Set Identifier) is an identification code (typically a simple name) broadcast by a wireless router. If a wireless device detects multiple SSIDs from multiple access points (APs), it will typically ask the end-user which one it should connect to. Telling a router not to broadcast its SSID may prevent basic wireless access software from displaying the network in question as a connection option, but it does nothing to actually secure the network. Any

time a user connects to a router, the SSID is broadcast in plaintext, regardless of whether or not encryption is enabled. SSID information can also be picked up by anyone listening to the network in passive mode.

Changing the SSID

This is sometimes touted as a security measure. Changing our access point's SSID will change the identification code the router is broadcasting, but it won't change anything else. It doesn't prevent the router from being detected, snooped, or hacked in any way. Devices come with a default system ID called the SSID (Service Set Identifier) or ESSID (Extended Service Set Identifier). It is easy for a hacker to find out what the default identifier is for each manufacturer of wireless equipment so you need to change this to something else. Use something unique- not your name or something easily guessed.

Use SSIDS wisely

Change the default Service Set Identifiers (SSIDs) for our APs, and don't use anything obvious like our address or company name. For corporate setups, buy APs that let us disable broadcast SSID. Intruders can use programs such as Kismet (www.kismetwireless.net) to sniff out SSIDs anyway (by observing 802.11x management frames when users associate with APs), but again, every bit of inconvenience helps.

Don't broadcast SSID

The access points and routers automatically (and continually) broadcast the network's name, or SSID (Service Set Identifier). This makes setting up wireless clients extremely convenient since we can locate a WLAN without having to know what it's called, but it will also make our WLAN visible to any wireless systems within range of it. Turning off SSID broadcast for our network makes it invisible to our neighbors and passers-by.

Disable identifier broadcasting

Announcing that you have a wireless connection to the world is an invitation for hackers. You already know you have one so you don't need to broadcast it. Check the manual for your hardware and figure out how to disable broadcasting.

Disable DHCP

Switching DHCP off and using static IP addressing is no defense against hacking. Anyone snooping the network can usually figure out the pattern that has been used to assign the IP addresses in question and then make a specific request accordingly.

Enable encryption

WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) encrypt your data so that only the intended recipient is supposed to be able to read it. WEP has many holes and is easily cracked. 128-bit keys impact performance slightly without a significant increase in security so 40-bit (or 64-bit on some equipment) encryption is just as well. As with all security measures there are ways around it, but by using encryption you will keep the casual hackers out of your systems. If possible, you should use WPA encryption (older equipment can be upgraded to be WPA compatible). WPA fixes the security flaws in WEP but it is still subject to DOS (denial-of-service) attacks.

Restrict unnecessary traffic

Many wired and wireless routers have built-in firewalls. They are not the most technically advanced firewalls, but they help create one more line of defense. Read the manual for your hardware and learn how to configure your router to only allow incoming or outgoing traffic that you have approved.

Change the default administrator password

This is just good practice for all hardware and software. The default passwords are easily obtained and because so many people don't bother to take the simple step of changing them they are usually what hackers try first. Make sure you change the default password on your wireless router / access point to something that is not easily guessed like your last name.

Patch and protect our PC's

As a last line of defense you should have personal firewall software such as Zone Alarm Pro and anti-virus software installed on your computer. As important as installing the anti-virus software, you must keep it up to date. New viruses are discovered daily and anti-virus software vendors generally release updates at least once a week. You also must keep up to date with patches for known security vulnerabilities. For Microsoft operating systems you can use Windows Update to try and help keep you current with patches.

Setting a password for the router

To secure any wireless network is to change the default router password. Most manufacturers set the default password to something along the lines of "admin," "password," or "change name," and the router IP address is almost always a simple variation on 192.168.x.1, where x = 0, 1, or 15. A nonstandard, strong password is no substitute for actual encryption, but it's a step in the right direction. The next step should be to check for a firmware update for your router, particularly if it's an older model. Many routers that didn't support more advanced security settings (i.e., WPA) had such support added via later firmware updates.

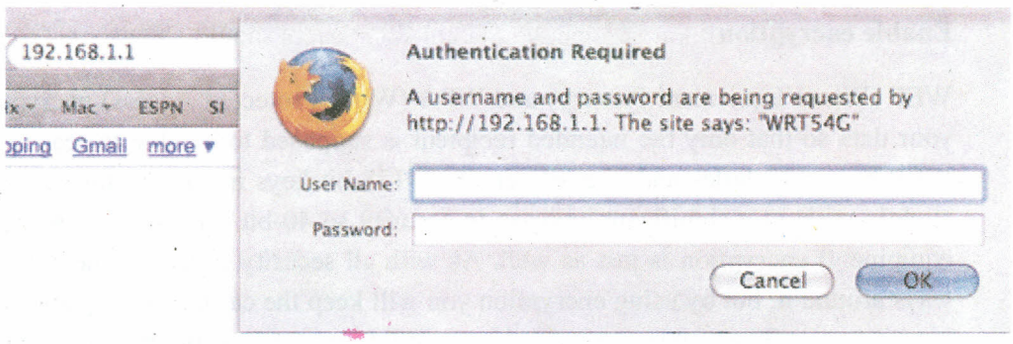


Fig 1: Authentication Requirement

Control broadcast area

Many wireless APs (access points) adjust the signal strength; some adjust signal direction. Begin by placing our APs as far away from exterior walls and windows as possible, then play around with signal strength so we can just barely get connections near exterior walls. Sensitive snooping equipment can pick up wireless signals from an AP at distances of several hundred feet or more. So even with optimal AP placement, the signal may leak.

Lock each AP

Changing the defaults on their APs, and maintaining the default administrator password (like admin for Linksys products) makes our system a good target. Use a strong password to protect each AP. For tips on creating substantial passwords, go towww.pcmag.com/passwords and click on Password Dos and Don'ts.

Enable WPA encryption instead of WEP

802.11's WEP (Wired Equivalency Privacy) encryption has well-known weaknesses that make it relatively easy for a determined user with the right equipment to crack the encryption and access the wireless network. A better way to protect our WLAN is with WPA (Wi-Fi Protected Access). WPA provides much better protection and is also easier to use, since the password characters aren't limited to 0-9 and A-F as they are with WEP. WPA support is built into Windows XP (with the latest Service Pack) and virtually all modern wireless hardware and operating systems. A more recent version, WPA2, is found in newer hardware and provides even stronger encryption.

WEP is better

Some of the wireless devices only support WEP encryption (this is often the case with non-PC devices like media players, PDAs, and DVRs), avoid the temptation to skip encryption entirely because in spite of it's flaws, using WEP is still far superior to having no encryption at all. If using WEP, don't use an encryption key that's easy to guess like a string of the same or consecutive

numbers. Also, although it can be a pain, WEP users should change encryption keys often-- preferably every week.

Limit access rights

Chances are, not everyone in our building needs a wireless card. Once we determine who should take to the airwaves, set our APs to allow access by wireless cards with authorized MAC addresses only.

Limit the number of user addresses

If we don't have too many users, consider limiting the maximum number of DHCP addresses the network can assign, allowing just enough to cover the users we have. Then if everyone in the group tries to connect but some can't, we know there are unauthorized log-ons.

Authenticate users

Install a firewall that supports VPN connectivity, and require users to log on as if they were dialing in remotely. The Linksys BEFSX41 router is a great choice for this. Tweak the settings to allow only the types of permissions that wireless users need. VPNs help prevent users from being fooled by malicious association attacks. In this type of assault, the perpetrator sets up a machine that pretends to be an authorized AP, in the hope that someone will be tricked into logging on.

Securing the Router and Wireless Network Connection

Go to 'Network Connections' and search for Wireless Networks in range. This should get with all available wireless networks in the area.

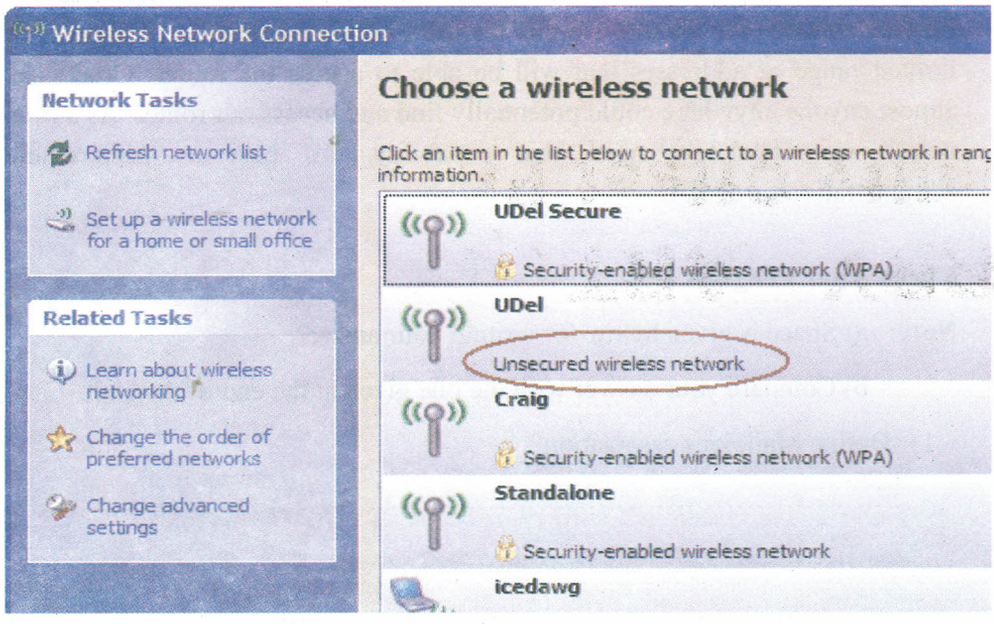


Fig. 2: Selection of Wireless Network

One should be able to see whether the wireless network that user is "Connected" to is secure or not. If it's secure, the only thing that needs to do is check if it is using WPA or WEP encryption method. Right click on the network, select 'Properties' and then Look for 'Encryption Type'.

Secure wireless router or access point administration interface

Almost all routers and access points have an administrator password that's needed to log into the device and modify any configuration settings. Most devices use a weak default password like "password" or the manufacturer's name, and some don't have a default password at all.

As soon as we set up a new WLAN router or access point, our first step should be to change the default password to something else. We may not use this password very often, so be sure to write it down in a safe place so we can refer to it if needed. Without it, the only way to access the router or access point may be to reset it to factory default settings which will wipe away any configuration changes.

Reduce WLAN transmitter power

To lower the power of our WLAN transmitter and thus reduce the range of the signal, Although it's usually impossible to fine-tune a signal so precisely that it won't leak outside our home or business, with some trial-and-error we can often limit how far outside our premises the signal reaches, minimizing the opportunity for outsiders to access our WLAN.

Disable remote administration

Most WLAN routers have the ability to be remotely administered via the Internet. Ideally, we should use this feature to define a specific IP address or limited range of addresses that will be able to access the router. Otherwise, almost anyone anywhere could potentially find and access our router. As a rule, unless we absolutely need this capability, it's best to keep remote administration turned off.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Define Malicious association?

.....

.....

.....

.....

2) What are three principal ways to secure a wireless network?

.....

.....

.....

.....

3) Describe EAP-versions

.....

.....

.....

.....

4) Why does the need for security arise?

.....

.....

.....

.....

5) Name two types of wireless securities.

.....

.....

.....

.....

6) Define Ad-hoc Network.

.....

.....

.....

.....

7) What is the prevention of unauthorized access or damage to computers using wireless networks?

.....

.....

.....

.....

8) What does EAP stand for?

.....

.....

.....

.....

9) Define RADIUS.

.....

.....

.....

.....

3.13 LET US SUM UP

Organizations and individuals benefit when wireless networks and devices are protected. After assessing the risks associated with wireless technologies, organizations can reduce the risks by applying countermeasures to address specific threats and vulnerabilities. These countermeasures include management, operational, and technical controls. While these countermeasures will not prevent all penetrations and adverse events, they can be effective in reducing many of the common risks associated with wireless technology.Organizations and individuals demand high-speed networks to increase efficiencies. The trade-off between high bandwidth and secure networks has to be taken into consideration when designing network infrastructures. Cyber criminals can slow down a network significantly, or they can capture important information. There are many methods cyber criminals can use to affect networks. IT professionals are struggling to design high-speed networks that will protect organizations and individuals from cyber crimes. As emerging technologies compete to solve the security and bandwidth dilemma, one or a few technologies will surface as winners and there will be many losers. Unified standards should also be developed to increase coordination of security applications.

3.14 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Malicious associations are when wireless devices can be actively made by attackers to connect to a company network through their cracking laptop instead of a company access point (AP). These types of laptops are known

as "soft APs" and are created when a cybercriminal runs some software that makes his/her wireless network card look like a legitimate access point.

Once the thief has gained access, he/she can steal passwords, launch attacks on the wired network, or plant trojans. Since wireless networks operate at the Layer 2 level, Layer 3 protections such as network authentication and virtual private networks (VPNs) offer no barrier. Wireless 802.1x authentications do help with protection but are still vulnerable to cracking. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the criminal is just trying to take over the client at the Layer 2 level.

2) **There are three principal ways to secure a wireless network**

- **Closed networks** (like home users and organizations)

  The most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address. Another option is to disable ESSID broadcasting, making the access point difficult for outsiders to detect. Wireless Intrusion Prevention Systems can be used to provide wireless LAN security in this network model.

- **Commercial providers**, hotspots, and large organizations

  The preferred solution is often to have an open and unencrypted, but completely isolated wireless network. The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN.

- **Wireless networks**

  They are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it's also often possible for remote intruders to gain access to the network through backdoors. One general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public.

3) EAP-versions include LEAP, PEAP and other EAP's

LEAP

This stands for the Lightweight Extensible Authentication Protocol. This protocol is based on 802.1X and helps minimize the original security flaws by using WEP and a sophisticated key management system. This EAP-

version is safer than EAP-MD5. This also uses MAC address authentication. LEAP is not safe against crackers. THC-Leap Cracker can be used to break Cisco's version of LEAP and be used against computers connected to an access point in the form of a dictionary attack. Anwrap and asleap finally are other crackers capable of breaking LEAP.

PEAP

This stands for Protected Extensible Authentication Protocol. This protocol allows for a secure transport of data, passwords, and encryption keys without the need of a certificate server. This was developed by Cisco, Microsoft, and RSA Security.

Other EAPs

There are other types of Extensible Authentication Protocol implementations that are based on the EAP framework. The framework that was established supports existing EAP types as well as future authentication methods. EAP-TLS offers very good protection because of its mutual authentication. Both the client and the network are authenticated using certificates and per-session WEP keys. EAP-FAST also offers good protection. EAP-TTLS is another alternative made by Certicom and Funk Software. It is more convenient as one does not need to distribute certificates to users, yet offers slightly less protection than EAP-TLS.

4) The need for security arises due to:

   - Growth of mobile internet access and applications,
   - Individual user requirements and Corporations (business or governmental) who both require internal and external
   - Contact and data transfer through remote places

5) Two types of wireless security are:-

   1. Wired Equivalent Privacy (WEP) and
   2. Wi-Fi Protected Access (WPA)

6) Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

7) Wireless security

8) Extensible Authentication Protocol

9) This stands for Remote Authentication Dial in User Service. This is an AAA (authentication, authorization and accounting) protocol used for remote network access. This service provides an excellent weapon against crackers. RADIUS was originally proprietary but was later published under ISOC documents RFC 2138 and RFC 2139. The idea is to have an inside server act as a gatekeeper through the use of verifying identities through a username and password that is already pre-determined by the user. A RADIUS server can also be configured to enforce user policies and restrictions as well as recording accounting information such as time connected for billing purposes.

3.15 SUGGESTED READINGS

- Agarwal, A. K., and Wang, W. (2007). *On the Impact of Quality of Protection in Wireless Local Area Networks with IP Mobility. Mobile Networks and Applications,* 12. 93-100.
- Andrew Tan (September 2006). "Gunning for "N" - Linksys WRT300N Wireless Router and WPC300N Wireless PCMCIA Adapter". Hardware Mag. pp. 47.
- Design and Implementation of WLAN Authentication and Security(2010) - ISBN 978-3838372266
- "Extensible Authentication Protocol Overview". *Microsoft TechNet.*
- "Fitting the WLAN Security pieces together". pcworld.com.
- Haleem, M., Mathur, C., Chandramouli, R., & Subbalakshmi, K. (2007). Opportunistic Encryption: *The Trade-Off between Security and Throughput in Wireless Networks. Washington: IEEE Transactions on Dependable and Secure Computing,* 4. 1-12.
- Joshua Bardwell; Devin Akin (2005). *CWNA Official Study Guide*(Third ed.). McGraw-Hill. p. 435. ISBN 0072255382.
- Kevin Beaver, Peter T. Davis, Devin K. Akin. "Hacking Wireless Networks for Dummies".
- Lin, P. P. (2006). *System Security Threats and Controls. New York: The CPA Journal,* 76. 58-65.
- Nate Anderson (2009). "One-minute WiFi crack puts further pressure on WPA". *Ars Technica.*
- "Network Security Tips". *Cisco.*

- Robert McMillan. "Once thought safe, WPA Wi-Fi encryption is cracked". *IDG.*
- Real 802.11 Security: Wi-Fi Protected Access and 802.11i (2003) - ISBN 978-0321136206
- Soppera, A., & Burbridge, T. (2005). *Wireless Identification – Privacy and Security. BT Technology Journal,* 23. 54-65.
- Sun, Y., Belding-Royer, E. M., Gao, X., & Kempf, J. (2007). *Real-time Traffic Support in Heterogeneous Mobile Networks. Wireless Networks*, 13. 431-445.
- "The Hidden Downside of Wireless Networking".
- "Top reasons why corporate WiFi clients connect to unauthorized networks". Info Security.
- Wi-Foo: The Secrets of Wireless Hacking (2004) - ISBN 978-0321202178
- Wireless Security Primer (Part II). Window security.com.

UNIT 4 ETHICAL HACKING-WIRELESS SECURITY

Structure

4.0 INTRODUCTION

With the growth of the Internet, computer security has become a major concern for businesses and governments. They want to be able to take advantage of the Internet for electronic commerce, advertising, information distribution and access, and other pursuits, but they are worried about the possibility of being "hacked." At the same time, the potential customers of these services are worried about maintaining control of personal information that varies from credit card numbers to social security numbers and home addresses. In their search for a way to approach the problem, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems. This is similar to having independent auditors come into an organization to verify its bookkeeping records. In the case of computer security, these "tiger teams" or "ethical hackers" would employ the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information. Instead, they would evaluate the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them.

4.1 OBJECTIVES

After going through this Unit, you should be able to:

- describe the need of Ethical Hackers;
- explain Ethical Hackers and their duties;
- identify Modes of Ethical Hacking ;
- explain the things which needs to practice to Become an Ethical Hacker;
- describe Five Stages of Ethical Hacking;
- describe Ethical Hacking Process;
- describe Cyber Law of India;

- explain Ethical Hacking: Wireless Security; and
- describe Test Phases of Security Assessments.

4.2 THE RATIONALE FOR THE ETHICAL HACKER

Virtually everyday, one either reads in the newspaper or sees on the Internet some reference to a company or an organization suffering from the brunt of an overt attack against their networks. Hacking or cracking as it is known in some circles, has become synonymous with this new breed of criminal activity, hence to be labeled a "hacker" is understood in today's society as being a derisive term.

However; this was not always the case, as it originally was understood to be a "badge of honor" bestowed to one who exhibited a high-level of expertise in knowledge about various computer-based subjects. Unfortunately, adverse media publicity skewed this view and blurred the distinction between one who was merely an intellectual seeker of computer knowledge and one who utilized this knowledge for criminal or selfish gains. Because of the explosive growth of the Internet and networks, there is a shortage of information technology security specialists. Now, a new breed of network defenders has arrived, known as **"Ethical Hackers",** and these individuals are viewed almost as an enigma. The marriage of the term ethical with hacking is understood as being an oxymoron, analogous to calling someone an "honest criminal." Nevertheless, it would appear as though Ethical Hackers may have found a place in our arsenal of defenses of network assets and that they are here to stay. Today, the stakes are much higher and the playing field encompasses every aspect of our society, business and industry, national security, educational enterprises and public/private organizations. The realm of the ethical hacker will expand into all these arenas and the insight derived from their expertise will have to be included in the body of statistical and empirical knowledge used to properly defend informational assets.

Business and industry face increasing scrutiny from regulatory constraints and from debacles like the Enron scandal. Corporations are forced to confront many factors that they have not had to face in the past. It is no longer acceptable to have a laissez-faire attitude towards protecting one's informational assets. As Gary Baker and Simon Tang of the Chartered Accountants of Canada Information Technology Committee indicate: successful businesses are challenged with pressures from a whole range of representatives including management, board of directors, customers and shareholders, in order to give an account for the information which they have been entrusted and how they are attempting to protect it. These additional factors have contributed to the heightened sensitivity to maintaining the

confidentiality, integrity and availability of network and financial resources. Business is not the only entity that is a target in network attacks.

As computers became increasingly available at universities, user communities began to extend beyond researchers in engineering or computer science to other individuals who viewed the computer as a curiously flexible tool. Whether they programmed the computers to play games, draw pictures, or to help them with the more mundane aspects of their daily work, once computers were available for use, there was never a lack of individuals wanting to use them.

Because of this increasing popularity of computers and their continued high cost, access to them was usually restricted. When refused access to the computers, some users would challenge the access controls that had been put in place. They would steal passwords or account numbers by looking over someone's shoulder, explore the system for bugs that might get them past the rules, or even take control of the whole system. They would do these things in order to be able to run the programs of their choice, or just to change the limitations under which their programs were running. Initially these computer intrusions were fairly benign, with the most damage being the theft of computer time. Other times, these recreations would take the form of practical jokes. However, these intrusions did not stay benign for long. Occasionally the less talented, or less careful, intruders would accidentally bring down a system or damage its files, and the system administrators would have to restart it or make repairs. Other times, when these intruders were again denied access once their activities were discovered, they would react with purposefully destructive actions. When the number of these destructive computer intrusions became noticeable, due to the visibility of the system or the extent of the damage inflicted, it became "news" and the news media picked up on the story. Instead of using the more accurate term of "computer criminal," the media began using the term hacker" to describe individuals who break into computers for fun, revenge, or profit. Since calling someone a "hacker" was originally meant as a compliment, computer security professionals prefer to use the term "cracker" or "intruder" for those hackers who turn to the dark side of hacking.

Hacker is a word that has two meanings

Traditionally, a hacker is someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically or one who programs enthusiastically or who enjoys programming rather than just theorizing about programming.

Recently, hacker has taken on a new meaning — someone who maliciously breaks into systems for personal gain.

Technically, these criminals are crackers (criminal hackers). Crackers break into (crack) systems with malicious intent. They are out for personal gain:

fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable. The good-guy (white-hat) hackers don't like being in the same category as the bad-guy (black-hat) hackers.

Hackers (or bad guys) try to compromise computers.

Ethical hackers (or good guys) protect computers against illicit entry.

Hackers go for almost any system they think they can compromise. Some prefer prestigious, well-protected systems, but hacking into anyone's system increases their status in hacker circles.

4.3 NEED FOR ETHICAL HACKERS

In order to protect the computers from malicious intrusions, we need Security Professionals. Polices protect us from thieves. Ethical hackers protect us from Hackers.

4.3.1 Authorized to Hack

In the world of technology, breaking things, or at least attempting to do so, is also an integral part of getting them to work. One of the first examples of ethical hackers at work was in the 1970s, when the United States government used groups of experts called red teams to hack its own computer systems. According to Ed Skoudis, Vice President of Security Strategy for Predictive Systems' Global Integrity consulting practice, ethical hacking has continued to grow in an otherwise lackluster IT industry, and is becoming increasingly common outside the government and technology sectors where it began. Many large companies, such as IBM, maintain employee teams of ethical hackers. Many contracts IBM inks with large clients require a security audit, involving an authorized visit to the firm by a team of hackers using agreed-upon "rules of engagement."

In the last few years, the surge in use of wireless computer networks has been a particular focus for IBM. Traditional wired local area networks, of the kind probably used in your office, are essentially limited to the computers hooked up to the network. Local wireless networks revolve around access points computers can detect on their own. But since wireless network capabilities are now frequently built into computers, even machines sitting in offices may seek out access points. They will often take access points -- which can be bought in stores -- and set up shop in the parking lot outside a client's headquarters to see how quickly they can penetrate a company's information system.

Employees who telecommute or use a laptop computer at a public wireless access point -- in an airport, coffee shop or another location -- can also put

valuable company information at risk. Given the existence of an access point, skilled hackers can monitor the flow of packets of information being sent over wireless networks, and, if a computer is not using encryption technology, potentially view the actual data being sent as well.

4.4 ETHICAL HACKING

An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. To test a security system, ethical hackers use the same methods as their less principled counterparts. Ethical hacking is also known as penetration testing, intrusion testing and red teaming.

Ethical hacking — also known as white-hat hacking — involves the same tools, tricks, and techniques that hackers use, but with one major difference: Ethical hacking is legal. Ethical hacking is performed with the target's permission. It can also ensure that vendors' claims about the security of their products are legitimate.The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. It is part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

Ethical hackers are technically skilled IT professionals. They process the penetration testing and find the vulnerability of the system. They perform the same activities a hacker would but without malicious intent. They must work closely with the host organization to understand what the organization is trying to protect, who they are trying to protect these assets from, and how much money and resources the organization is willing to expend to protect the assets.

4.5 ETHICAL HACKERS AND THEIR DUTIES

Ethical hackers need hands-on security skills. Although you do not have to be an expert in everything, you should have an area of expertise. Security tests are typically performed by teams of individuals, where each individual typically has a core area of expertise. These skills include:

Knowledge of Routers

Knowledge of routers, routing protocols, and access control lists (ACLs). Certifications such a Cisco Certified Network Associate (CCNA) or Cisco Certified Internetworking Expert (CCIE) can be helpful.

Microsoft Certified

These can run the gamut from Windows NT to Windows 2003. These individuals might be Microsoft Certified Administrator (MCSA) or Microsoft Certified Security Engineer (MCSE) certified.

Linux Certified

This includes security setting, configuration, and services such as Apache. These individuals may be Red Hat, or Linux+ certified.

Firewall configuration

Knowledge of firewall configuration and the operation of intrusion detection systems (IDS) and intrusion prevention systems (IPS) can be helpful when performing a security test. Individuals with these skills may be certified in Cisco Certified Security Professional (CCSP) or Checkpoint Certified Security Administrator (CCSA).

Mainframes skill set

Although mainframes do not hold the position of dominance they once had in business, they still are widely used. If the organization being assessed has mainframes, the security teams would benefit from having someone with that skill set on the team.

Knowledge of Network protocols

Most modern networks are Transmission Control Protocol/ Internet Protocol (TCP/IP), although you might still find the occasional network that uses Novell or Apple routing information. Someone with good knowledge of networking protocols, as well as how these protocols function and can be manipulated, can play a key role in the team. These individuals may possess certifications in other OSes, hardware, or even possess a Network+ or Security+ certification.

Project management skills

Someone will have to lead the security test team, and if you are chosen to be that person, you will need a variety of the skills and knowledge types listed previously. It can also be helpful to have good project management skills. After all, you will be leading, planning, organizing, and controlling the penetration test team. Individuals in this role may benefit from having Project Management Professional (PMP) certification.

4.6 MODES OF ETHICAL HACKING

Security testing is the primary job of ethical hackers. These tests might be configured in such way that the ethical hackers have no knowledge, full knowledge, or partial knowledge of the target of evaluation (TOE).

Insider attack

This ethical hack simulates the types of attacks and activities that could be carried out by an authorized individual with a legitimate connection to the organization's network.

Outsider attack

This ethical hack seeks to simulate the types of attacks that could be launched across the Internet. It could target Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), Structured Query Language (SQL), or any other available service.

Stolen equipment attack

This simulation is closely related to a physical attack as it targets the organization's equipment. It could seek to target the CEO's laptop or the organization's backup tapes. No matter what the target, the goal is the same extract critical information, usernames, and passwords.

Physical entry

This simulation seeks to test the organization's physical controls. Systems such as doors, gates, locks, guards, closed circuit television (CCTV), and alarms are tested to see whether they can be bypassed.

Bypassed authentication attack

This simulation is tasked with looking for wireless access points (WAP) and modems. The goal is to see whether these systems are secure and offer sufficient authentication controls. If the controls can be bypassed, the ethical hacker might probe to see what level of system control can be obtained.

Social engineering attack

This simulation does not target technical systems or physical access. Social engineering attacks target the organization's employees and seek to manipulate them to gain privileged information. Proper controls, policies, and procedures can go a long way in defeating this form of attack.

Rules of Engagement

Every ethical hacker must abide by a few simple rules when performing the tests described previously. If not, bad things can happen to you, which might include loss of job, civil penalty, or even jail time.

Never exceed the limits of your authorization

Every assignment will have rules of engagement. These not only include what you are authorized to target, but also the extent that you are authorized to

control such system. If you are only authorized to obtain a prompt on the target system, downloading passwords and starting a crack on these passwords would be in excess of what you have been authorized to do.

4.7 TO BECOME AN ETHICAL HACKER- THINGS WHICH NEEDS TO PRACTICE

Personal Interest: The interest is the main key to become an ethical hacker. If you have more interest, you can learn new things.

Learning: Read computer related books and blogs. Learn how the computers and Operating system works.

Know how the hackers hack: You cannot solve the problem until you know what is behind the problem. So you have to learn how hackers hacks the computer, learn hacking (read for knowledge, don't become one of them).

Programming: You have to learn programming languages. Then only you can determine the flows and malicious codes. Learn the basic programming languages like: C, Java, perl, PHP. Buy best programming books and learn it. There are plenty of website is teaching you the Programming, you can learn in Internet also.

UNIX/Linux: Learn to work with UNIX/LINUX operating systems. These two are the most secure operating system.

Back Track Linux Distribution: Backtrack Linux is the famous linux distribution for Security Professionals. This backtrack is funded by Offensive Security. Backtrack has almost all penetration testing tools. One can run the backtrack OS from pen drive itself.

Get Certification for Ethical Hackers: There are plenty of institutions which teach ethical hacking and provide the Certification. Require to take the online training from Offensive Security. The offensive security will make as Penetration tester.

Break the Security: Break The Security provides tutorial for Ethical hacking. One can learn Ethical hacking for free. If one likes to become penetration tester, Break the Security will help. If anybody require certification, write Certification exams.

Buy Books: Buy any security /Ethical Hacking/ Penetration testing related books and read.

Forums: Participate in any Security or Hacking related forums.

4.8 THE FIVE STAGES OF ETHICAL HACKING

Phases of hacking

Phase1— Passive and Active Reconnaissance

Phase 2—Scanning

Phase 3—Gaining Access

Phase 4—Maintaining Access

Phase 5—Covering Tracks

Phase 1: Passive and Active Reconnaissance

Passive reconnaissance involves gathering information regarding a potential target without the targeted individual's or company's knowledge. Passive reconnaissance can be as simple as watching a building to identify what time employees enter the building and when they leave. However, it's usually done using Internet searches or through Google search an individual or company can gain information. This process is generally called information gathering. Social engineering and dumpster diving are also considered passive information-gathering methods.

Sniffing the network is another means of passive reconnaissance and can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. Sniffing network traffic is similar to building monitoring: A hacker watches the flow of data to see what time certain transactions take place and where the traffic is going.

Active reconnaissance involves probing the network to discover individual hosts, IP addresses and services on the network. This usually involves more risk of detection than passive reconnaissance and is sometimes called rattling the doorknobs. Active reconnaissance can give a hacker an indication of security measures in place (is the front door locked), but the process also increases the chance of being caught or at least raising suspicion.

Phase 2: Scanning

Scanning involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase can include dialers, port scanners, network mappers, sweepers, and vulnerability scanners. Hackers are seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts.

Phase 3: Gaining Access

This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the hacker uses for an exploit can be a local area network (LAN, either wired or wireless), local access to a PC, the Internet, or offline. Examples include stack-based buffer overflows, denial of service (DoS), and session hijacking. Gaining access is known in the hacker world as owning the system.

Phase 4: Maintaining Access

Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system.

Phase 5: Covering Tracks

Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms. Examples of activities during this phase of the attack include the use of tunnelling protocols, and altering log files.

4.9 THE ETHICAL HACKING PROCESS

Like practically any IT or security project, ethical hacking needs to be planned in advance. Strategic and tactical issues in the ethical hacking process should be determined and agreed upon. Planning is important for any amount of testing — from a simple password-cracking test to an all-out penetration test on a Web application.

4.9.1 Formulating the Plan

Approval for ethical hacking is essential. Make what you're doing known and visible — at least to the decision makers. Obtaining *sponsorship* of the project is the first step. This could be the manager, an executive, a customer, or even yourself if you're the boss. You need someone to back you up and sign off on your plan. Otherwise, your testing may be called off unexpectedly if someone claims they never authorized you to perform the tests.

If you're testing for a customer, have a signed contract in place, stating the customer's support and authorization. Get written approval on this sponsorship as soon as possible to ensure that none of your time or effort is wasted.

A well-defined scope includes the following information:

- **Specific systems to be tested:** When selecting systems to test, start with the most critical systems and processes or the ones you suspect to be the most vulnerable. For instance, you can test computer passwords, an Internet-facing Web application, or attempt social engineering attacks before drilling down into all your systems.

- **Risks involved:** It pays to have a contingency plan for your ethical hacking process in case something goes awry. What if you're assessing your firewall or Web application and you take it down? This can cause system unavailability, which can reduce system performance or employee productivity. Even worse, it could cause loss of data integrity, loss of data itself, and even bad publicity. It'll most certainly tick off a person or two and make you look bad.

  Handle social engineering and DoS attacks carefully. Determine how they can affect the systems you're testing and your entire organization.

- **When the tests will be performed and your overall timeline:** Determining when the tests are performed is something that you must think long and hard about. Do you perform tests during normal business hours? How about late at night or early in the morning so that production systems aren't affected? Involve others to make sure they approve of your timing.

  The best approach is an unlimited attack, wherein any type of test is possible at any time of day. The bad guys aren't breaking into your systems within a limited scope, so why should you. Some exceptions to this approach are performing DoS attacks, social engineering, and physical security tests.

- **How much knowledge of the systems you have before you start testing:** You don't need extensive knowledge of the systems you're testing — just a basic understanding. This basic understanding helps protect you and the tested systems.

- **What action will be taken when a major vulnerability is discovered:** Don't stop after you find one security hole. This can lead to a false sense of security. Keep going to see what else you can discover. You don't have to keep hacking until the end of time or until you crash all your systems; simply pursue the path you're going down until you can't hack it.

any longer (pun intended). If you haven't found any vulnerabilities, you haven't looked hard enough.

- **The specific deliverables:** This includes security assessment reports and a higher-level report outlining the general vulnerabilities to be addressed, along with countermeasures that should be implemented.

  One of the goal may be to perform the tests without being detected. For example, you may be performing your tests on remote systems or on a remote office and you don't want the users to be aware of what you're doing. Otherwise, the users may catch on to you and be on their best behavior — instead of their normal behavior.

4.9.2 Selecting Tools

As with any project, if you don't have the right tools for ethical hacking, accomplishing the task effectively is difficult. Having said that, just because you use the right tools doesn't mean that you will discover all vulnerabilities.

Know the personal and technical limitations. Many security-assessment tools generate false positives and negatives (incorrectly identifying vulnerabilities). Others may miss vulnerabilities. If you're performing tests such as social engineering or physical-security assessments, you may miss weaknesses. Many tools focus on specific tests, but no one tool can test for everything. Like one shouldn't use a word processor to scan the network for open ports. This is why you need a set of specific tools that you can call on for the task at hand. The more tools you have, the easier your ethical hacking efforts are.

To crack passwords, you need a cracking tool such as LC4, John the Ripper, or pwdump. A general port scanner, such as SuperScan, may not crack passwords. For an in-depth analysis of a Web application, a Web-application assessment tool (such as Whisker or WebInspect) is more appropriate than a network analyzer (such as Ethereal).

When selecting the right security tool for the task, ask around. Get advice from your colleagues and from other people online. A simple Groups search on Google (www.google.com) or perusal of security portals, such as SecurityFocus.com, SearchSecurity.com, and ITsecurity.com, often produces great feedback from other security experts. Lots of tools can be used for ethical hacking — from the own words and actions to software-based vulnerability-assessment programs to hardware-based network analyzers.

The following list runs downsome of my favorite commercial, freeware, and open-source security tools:

- Nmap
- EtherPeek

- SuperScan
- QualysGuard
- WebInspect
- LC4 (formerly called L0phtcrack)
- LANguard Network Security Scanner
- Network Stumbler
- ToneLoc

Here are some other popular tools:

- Internet Scanner
- Ethereal
- Nessus
- Nikto
- Kismet
- THC-Scan

The capabilities of many security and hacking tools are often misunderstood. This misunderstanding has shed negative light on some excellent tools, such as SATAN (Security Administrator Tool for Analyzing Networks) and Nmap (Network Mapper). Some of these tools are complex. The tools which you use, familiarize with them before you start using them.

Ways to do that:

- Read the readme and/or online help files for tools.
- Study the user's guide for commercial tools.
- Consider formal classroom training from the security-tool vendor or another third-party training provider, if available.

Look for Characteristics in tools for Ethical Hacking

- Adequate documentation.
- Detailed reports on the discovered vulnerabilities, including how they may be exploited and fixed.
- Updates and support when needed.
- High-level reports that can be presented to managers or nontechie types.

These features can save time and effort when one is writing the report.

4.9.3 Executing the Plan

Ethical hacking can take persistence. Time and patience are important. Be careful when you're performing your ethical hacking tests. A hacker in your network or a seemingly benign employee looking over your shoulder may watch what's going on. This person could use this information against you. It's not practical to make sure that no hackers are on your systems before you start. Just make sure you keep everything as quiet and private as possible. This is especially critical when transmitting and storing your test results. If possible, encrypt these e-mails and files using Pretty Good Privacy (PGP) or something similar. At a minimum, password-protect them.

You're now on a reconnaissance mission. Harness as much information as possible about the organization and systems, which is what malicious hackers do. Start with a broad view and narrow down the focus:

1. **Search the Internet for the organization's name, computer and network system name, and IP addresses**

Google is a great place to start for this.

2. **Narrow the scope, targeting the specific systems you're testing**

Whether physical-security structures or Web applications, a casual assessment can turn up much information about the systems.

3. **Further narrow the focus with a more critical eye, perform actual scans and other detailed tests on the systems.**

4. **Perform the attacks, if that's what you choose to do.**

4.9.4 Evaluating Results

Assess the results to see what one uncovered, assuming that the vulnerabilities haven't been made obvious before now. This is where knowledge counts. Evaluating the results and correlating the specific vulnerabilities discovered is a skill that gets better with experience. You'll end up knowing your systems as well as anyone else. This makes the evaluation process much simpler moving forward.

Submit a formal report to upper management or to your customer, outlining your results. Keep these other parties in the loop to show that the efforts and their money are well spent.

4.9.5 Moving On

When one is finished with ethical hacking tests, you still need to implement your analysis and recommendations to make sure your systems are secure. New

security vulnerabilities continually appear. Information systems constantly change and become more complex. New hacker exploits and security vulnerabilities are regularly uncovered. You may discover new ones! Security tests are a snapshot of the security posture of your systems. At any time, everything can change, especially after software upgrades, adding computer systems, or applying patches. Plan to test regularly (for example, once a week or once a month).

4.10 CYBER LAW OF INDIA

In Simple way we can say that cyber-crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber-crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

Categorize Cyber-crimes in two ways-

The Computer as a Target:-using a computer to attack other computers.

E.g. Hacking, Virus/Worm attacks, DOS attack etc.

The computer as a weapon:-using a computer to commit real world crimes.

E.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

4.10.1 Technical Aspects

Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies such as

4.10.2 Unauthorized Access and Hacking

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to

stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

By hacking web server taking control on another person's website called as **web hijacking.**

4.10.3 Trojan Attack

The program that act like something useful but do the things that are quiet damping and are called as Trojans. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the trojan.

TCP/IP protocol is the usual protocol type used for communications, but some functions of the trojans use the UDP protocol as well.

4.10.4 Virus and Worm Attack

A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus.

Programs that multiply like viruses but spread from computer to computer are called as worms.

4.10.5 E-Mail and IRC Related Crimes

4.10.5.1 E-mail Spoofing

E-mail spoofing refers to e-mail that appears to have been originated from one source when it was actually sent from another source.

4.10.5.2 E-mail Spamming

E-mail spamming refers to sending e-mail to thousands and thousands of users - similar to a chain letter.

4.10.5.3 Sending Malicious Codes through E-mail

E-mails are used to send viruses, Trojans etc through e-mails as an attachment or by sending a link of website which on visiting downloads malicious code.

4.10.5.4 E-mail Bombing

E-mail bombing is characterized by abusers repeatedly sending an identical e-mail message to a particular address.

4.10.5.5 Sending Threatening E-mails

Mails sent for harassing purpose.

4.10.5.6 Defamatory E-mails

Sending false, derogatory statement(s) in private or public mails about a person's business practices, character, financial status, morals or reputation.

4.10.5.7 E-mail Frauds

E-mail fraud is the intentional deception made for personal gain.

4.10.5.8 IRC Related

Three main ways to attack IRC are: verbal attacks, clone attacks and flood attacks.

4.10.6 Denial of Service Attacks

Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users.

Examples include

- attempts to flood a network, thereby preventing legitimate network traffic
- attempts to disrupt connections between two machines, thereby preventing access to a service
- attempts to prevent a particular individual from accessing a service
- attempts to disrupt service to a specific system or person.

4.11 ETHICAL HACKING-WIRELESS SECURITY

Wireless Security services measure the security of wireless infrastructure and provide with a roadmap to ensure the integrity and availability of information and resources.

This assessment is complete in three phases. Each phase provides the ethical hacking team with information.

During the first phase

Map and Identify Active Wireless Networks, the ethical hacking team will determine network's vulnerability to an attacker with radio access to the wireless network space. The ethical hacking team will attempt detect the 802.11 wireless networks in place (including any ad-hoc networks identified), determine the locations and ranges of the wireless networks, evaluate the range

of the wireless access area, determine network configuration information, and probe points of entry for identifying system information or access parameters.

In the second phase of the engagement

Assess Wireless Implementation for Vulnerabilities, pose as someone with normal user access and evaluate the security measures taken to secure infrastructure, including the following ESSID, the use and strength of WEP encryption, network segmentation, and access control devices.

During the last phase of the assessment

Exploit Vulnerabilities and Access Other Networks, the team will try to use the previously discovered vulnerabilities to obtain access to other network segments. If the team is successful, they will test different methods to exploit that access. This phase will determine which network segments and systems the wireless network infrastructure can access, the security controls that separate the wireless network from other network segments and if the wireless network can be used as a launching point to attack other systems.

Developing the boundaries for actions and events that can perform during the vulnerability assessment. Any High-Risk vulnerabilities/risks identified during the assessment will be immediately communicated.

After the testing has been completed, provide an organization with a formal report that:

- Lists all identified weaknesses and vulnerabilities
- Explains the risks associated with the current network configuration
- Presents recommendations to increase the security of wireless infrastructure

4.11.1 Maintain Confidentiality

During security evaluations, one will likely be exposed to many types of confidential information. We have both a legal and moral standard to treat this information with the utmost privacy. This information should not be shared with third parties and should not be used by you for any unapproved purposes. There is an obligation to protect the information sent between the tester and the client. This has to be specified in the agreement.

4.11.2 Do No Harm

It's of utmost importance that you do no harm to the systems you test. Again, a major difference between a hacker and an ethical hacker is that you should do no harm. Misused, security tools can lock out critical accounts, cause denial of service (DoS), and crash critical servers or applications. Care should be taken to prevent these events unless that is the goal of the test.

4.11.3 Test Plans — Keeping It Legal

Make plans before we take a job. In Ethical hacking any details need to be worked out before a single test is performed. If you or your boss is tasked with managing the project, some basic questions need to be answered, such as what's the scope of the assessment, what are the driving events, what are the goals of the assessment, what will it take to get approval, and what's needed in the final report. Before an ethical hack test can begin, the scope of the engagement must be determined.

Defining the scope of the assessment is one of the most important parts of the ethical hacking process. At some point, you will be meeting with management to start the discussions of the how and why of the ethical hack. Before this meeting ever begins, you will probably have some idea what management expects this security test to accomplish. Companies that decide to perform ethical hacking activities don't do so in a vacuum. You need to understand the business reasons behind this event. Companies can decide to perform these tests for various reasons.

Some of the most common reasons are listed as follows:

A breach in security - One or more events has occurred that has highlighted a lapse in security. It could be that an insider was able to access data that should have been unavailable to him, or it could be that an outsider was able to hack the organization's web server.

Compliance with state, federal, regulatory, or other law or mandate — Compliance with state or federal laws is another event that might be driving the assessment. Companies can face huge fines and potential jail time if they fail to comply with state and federal laws.

4.12 TEST PHASES OF SECURITY ASSESSMENTS

Security assessments in which ethical hacking activities will take place are composed of three phases:

These include the scoping of the assessment in which goals and guidelines are established, performing the assessment, and performing post assessment activities. The post assessment activities are when the report and remediation activities would occur.

This shows the three phases of the assessment and their typical times.

4.12.1 Establishing Goals

The need to establish goals is also critical. Although you might be ready to jump in and begin hacking, a good plan will detail the goals and objectives of

the test. Some common goals include system certification and accreditation, verification of policy compliance, and proof that the IT infrastructure has the capability to defend against technical attacks.

Are the goals to certify and accredit the systems being tested?

Certification is a technical evaluation of the system that can be carried out by independent security teams or by the existing staff. Its goal is to uncover any vulnerabilities or weaknesses in the implementation. Your goal will be to test these systems to make sure that they are configured and operating as expected, that they are connected to and communicate with other systems in a secure and controlled manner, and that they handle data in a secure and approved manner.

If the goals of the penetration test are to determine whether current policies are being followed, the test methods and goals might be somewhat different. The security team will be looking at the controls implemented to protect information being stored, being transmitted, or being processed. This type of security test might not have as much hands-on hacking, but might use more social engineering techniques and testing of physical controls. You might even direct one of the team members to perform a little dumpster diving.

The goal of a technical attack might be to see what an insider or outsider can access. Your goal might be to gather information as an outsider and then use that data to launch an attack against a web server or externally accessible system.

Regardless of what type of test you are asked to perform, there are some basic questions you can ask to help establish the goals and objectives of the tests.

These include the following:

- What is the organization's mission?
- What specific outcomes does the organization expect?
- What is the budget?
- When will tests be performed — during work hours, after hours, or weekends?
- How much time will the organization commit to completing the security evaluation?
- Will insiders be notified?
- Will customers be notified?
- How far will the test proceed? Root the box, gain a prompt, or attempt to retrieve another prize, such as the CEO's password.
- Who do you contact should something go wrong?
- What are the deliverables?

- What outcome is management seeking from these tests?

4.12.2 Getting Approval

Getting approval is a critical event in the testing process. Before any testing actually begins, you need to make sure that you have a plan that has been approved in writing. If this is not done, you and your team might face unpleasant consequences, which might include being fired or even criminal charges.

Written approval is the most critical step of the testing process. You should never perform any tests without written approval. If you are an independent consultant, you might also get insurance before starting any type of test. Umbrella policies and those that cover errors and omissions are commonly used. These types of liability policies can help protect you should anything go wrong. To help make sure that the approval process goes smoothly, you should make sure that someone is the champion of this project. This champion or project sponsor is the lead contact to upper management and your contact person. Project sponsors can be instrumental in helping you gain permission to begin testing and also to provide you with the funding and materials needed to make this a success.

4.12.3 Ethical Hacking Report

4.12.3.1 Describe Test Deliverables

One should not actually begun testing; but need to start thinking about the final report. Throughout the entire process, one should be in close contact with management to keep them abreast of the findings.

If you have found some problems, it should be discussed with management before the report is written and submitted. The goal is to keep them in the loop and advised of the status of the assessment. If you find items that present a critical vulnerability, you should stop all tests and immediately inform management. Your priority should always be the health and welfare of the organization.

The report itself should detail the results of what was found. Vulnerabilities should be discussed as should the potential risk they pose. Although people aren't fired for being poor report writers, don't expect to be promoted or praised for your technical findings if the report doesn't communicate your findings clearly. The report should present the results of the assessment in an easy, understandable, and fully traceable way. The report should be comprehensive and self-contained.

Most reports contain the following sections:

- Introduction

- Statement of work performed
- Results and conclusions
- Recommendations

Since most companies are not made of money and cannot secure everything, you should rank your recommendations so that the ones with the highest risk/highest probability is at the top of the list. The report needs to be adequately secured while in electronic storage. Encryption should be used. The printed copy of the report should be marked "Confidential" and while in its printed form, care should be taken to protect the report from unauthorized individuals. You have an ongoing responsibility to ensure the safety of the report and all information gathered. Most consultants destroy reports and all test information after a contractually obligated period of time.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What are the modes of Ethical Hacking?

.....

.....

.....

.....

2) What are the characteristics for Ethical Hacking?

.....

.....

.....

.....

3) Define Passive and Active Reconnaissance in Hacking.

.....

.....

.....

.....

4) Define Trojan Attack.

.....

.....

.....

.....

5) Define Ethical Hacking.

.....

.....

.....

.....

4.13 LET US SUM UP

The demands of modern business have made wireless technology a necessity. The mobile workforce has spurred the development of technologies that make it possible for the employees to instantly access data and network infrastructure from nearly any place in the world. With that access, however, comes significant risk. Ethical Hacking is a tool, which if properly utilized, can prove useful for understanding the weaknesses of a network and how they might be exploited. Ethical Hacking is not a panacea for all network security problems, but it is a fascinating craft that can be used to bolster the defense system. In conclusion, it must be reiterated that the ethical hacker is an educator who seeks to enlighten not only the customer, but also the security industry as a whole. By thinking like the enemy, the ethical hacker is able to ferret out issues in security which others may not even be aware of. Corporations and other entities are faced with the unenviable task of trying to defend their networks against various types of intrusive attacks. Although traditional methods of deterrence, (i.e. firewalls, intrusion detection devices, etc.) have their place in this battle, there has arisen the need to utilize specialists who are adept at exploiting both known and unknown vulnerabilities in networks in order to determine the security posture of an organization. These "Ethical Hackers" have created a niche for themselves in the "defense in-depth" spectrum.

4.14 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Security testing is the primary job of ethical hackers. These tests might be configured in such way that the ethical hackers have no knowledge, full knowledge, or partial knowledge of the target of evaluation (TOE).

   Insider attack

   This ethical hack simulates the types of attacks and activities that could be carried out by an authorized individual with a legitimate connection to the organization's network.

Outsider attack

This ethical hack seeks to simulate the types of attacks that could be launched across the Internet. It could target Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), Structured Query Language (SQL), or any other available service.

Stolen equipment attack

This simulation is closely related to a physical attack as it targets the organization's equipment. It could seek to target the CEO's laptop or the organization's backup tapes. No matter what the target, the goal is the same extract critical information, usernames, and passwords.

Physical entry

This simulation seeks to test the organization's physical controls. Systems such as doors, gates, locks, guards, closed circuit television (CCTV), and alarms are tested to see whether they can be bypassed.

Bypassed authentication attack

This simulation is tasked with looking for wireless access points (WAP) and modems. The goal is to see whether these systems are secure and offer sufficient authentication controls. If the controls can be bypassed, the ethical hacker might probe to see what level of system control can be obtained.

Social engineering attack

This simulation does not target technical systems or physical access. Social engineering attacks target the organization's employees and seek to manipulate them to gain privileged information. Proper controls, policies, and procedures can go a long way in defeating this form of attack.

Rules of Engagement

Every ethical hacker must abide by a few simple rules when performing the tests described previously. If not, bad things can happen to you, which might include loss of job, civil penalty, or even jail time.

Never exceed the limits of your authorization

Every assignment will have rules of engagement. These not only include what you are authorized to target, but also the extent that you are authorized to control such system. If you are only authorized to obtain a prompt on the target system, downloading passwords and starting a crack on these passwords would be in excess of what you have been authorized to do.

2) Adequate documentation.

- Detailed reports on the discovered vulnerabilities, including how they may be exploited and fixed.
- Updates and support when needed.
- High-level reports that can be presented to managers or nontechie types.

3) Passive reconnaissance involves gathering information regarding a potential target without the targeted individual's or company's knowledge. Passive reconnaissance can be as simple as watching a building to identify what time employees enter the building and when they leave.

However, it's usually done using Internet searches or through Google search an individual or company can gain information. This process is generally called information gathering. Social engineering and dumpster diving are also considered passive information-gathering methods.

Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. This usually involves more risk of detection than passive reconnaissance and is sometimes called rattling the doorknobs. Active reconnaissance can give a hacker an indication of security measures in place (is the front door locked), but the process also increases the chance of being caught or at least raising suspicion.

4) **Trojan Attack**

The program that acts like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans. The name **Trojan horse** is popular.

Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the trojan.

TCP/IP protocol is the usual protocol type used for communications, but some functions of the trojans use the UDP protocol as well.

5) An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. To test a security system, ethical hackers use the same methods as their less principled counterparts. Ethical hacking is also known as ***penetration testing***, ***intrusion testing*** **and** ***red teaming.***

Ethical hacking — also known as white-hat hacking — involves the same tools, tricks, and techniques that hackers use, but with one major

difference: Ethical hacking is legal. Ethical hacking is performed with the target's permission. It can also ensure that vendors' claims about the security of their products are legitimate.The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. It is part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

4.15 · SUGGESTED READINGS

- Goheen, S. M. and Fiske, R. S. (October 16, 1972). OS/360 *Computer Security Penetration Exercise*, WP-4467, The MITRE Corporation, Bedford, MA.
- Karger, P. A. and Schell, R. R. (June 1974). *Multics Security Evaluation: Vulnerability Analysis,* ESD-TR-74-193, Vol. II, Headquarters Electronic Systems Division, Hanscom Air Force Base, MA.
- Raymond, E. S. (1991). *The New Hacker's Dictionary*, MIT Press, Cambridge, MA.

MPDD-IGNOU/P.O.1T/Feb,2012

ISBN-978-81-266-5925-8