ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

DIPLOMA IN CYBER SECURITY

DCS-05 NETWORK CYBER SECURITY

BLOCK

3 WIRELESS NETWORK SECURITY

UNIT-1	WIRELESS NETWORK SECURITY
UNIT-2	SECURITY ISSUES IN WIRELESS NETWORKS
UNIT-3	SECURING A WIRELESS NETWORK
UNIT-4	MOBILE DEVICE SECURITY

EXPERT COMMITTEE

DIPLOMA IN CYBER SECURITY

Course Writers

Chandrakant Mallick
Odisha State Open University, Sambalpur, Odisha
Bijay Kumar Paikaray
Centurion University of Technology and Management, Odisha

ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

DIPLOMA IN CYBER SECURITY

DCS-05 NETWORK CYBER SECURITY

BLOCK

2 WIRELESS NETWORK SECURITY

UNIT-1	WIRELESS NETWORK SECURITY
UNIT-2	SECURITY ISSUES IN WIRELESS NETWORKS
UNIT-3	SECURING A WIRELESS NETWORK
UNIT-4	MOBILE DEVICE SECURITY

EXPERT COMMITTEE

Dr. P.K Behera (Chairman)
Reader in Computer Science
Utkal University
Bhubaneswar, Odisha

Dr.J.R Mohanty(Member)
Professor and HOD
KIIT University
Bhubaneswar, Odisha

Sri Pabitrananda Pattnaik(Member)
Scientist-E, NIC
Bhubaneswar, Odisha

Sri Malaya Kumar Das (Member)
Scientist-E, NIC
Bhubaneswar, Odisha

Dr. Bhagirathi Nayak(Member)
Professor and Head (IT & System)
Sri Sri University
Bhubaneswar,Odisha

Dr.Manoranjan Pradhan(Member)
Professor and Head (IT & System)
G.I.T.A
Bhubaneswar, Odisha

Sri Chandrakant Mallick(Convener)
Consultant (Academic)
School of Computer and Information Science
Odisha State Open University
Sambalpur, Odisha

DIPLOMA IN CYBER SECURITY

Course Writers

Chandrakant Mallick
Odisha State Open University, Sambalpur, Odisha
Bijay Kumar Paikaray
Centurion University of Technology and Management, Odisha

UNIT – 1 WIRELESS NETWORK SECURITY

Unit Structure

1.1 Introduction
1.2 Learning Objectives
1.3 Wireless Network
1.3.1 WLAN
1.3.1.1 Major issues with WLAN
1.3.1.2 Secure WLAN
1.4 Wireless Network Components
    1.4.1 Firewall
    1.4.2 Wireless Access Point
    1.4.3 Modem
    1.4.4 Server
    1.4.5 Switch
    1.4.6 USB Network Adapter
    1.4.7 Hub
    1.4.8 Routers: Wired or Wireless
    1.4.9 Station (STA)
    1.4.10 Access Point (AP)
    1.4.11 Ad Hoc Mode
    1.4.12 Infrastructure Mode
1.5Wireless Security
    1.5.1 Use of Wi-Fi
    1.5.2 Service Set Identification (SSID)
1.6 Types of Wireless Security
1.7 WPA Security problems
    1.7.1 Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2)
    1.7.2 Difference between WPA & WPA2
1.8 Wireless Security Policy
1.9 Let us Sum up
1.10 Self assessment Questions
1.11 Model Questions
1.12 References &Suggested Readings

1.1 Introduction

In this unit we will explain the important factor in the growth of a country that is a good communication infrastructure and will sees how wireless networks have an important role to play in the development of a country like India. 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 phones and tablets also great benefits. However, wireless networking has many security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. So there should have proper Management of Operational and Technical issues and recommendations for the secure deployment of wireless network security**.**

In this unit will introduce the benefits, components and security issues in wireless networks**.**

1.2 Learning Objectives

After going through this unit you should be able to

- Define a wireless network.
- Identify the components of wireless networks
- Explain the security issues in wireless networks

1.3 Wireless Network

Wireless networks are computer networks that are not connected by cables of any kind. The use of a wireless network enables enterprises to avoid the expensive process of introducing cables into buildings or as a connection between different equipment locations. The basis of wireless systems is radio waves, an implementation that takes place at the physical level of network structure.

Wireless networks use radio waves to connect devices such as laptops to the Internet, the business network and applications. When laptops are connected to Wi-Fi hot spots in public places, the connection is established to that business's wireless network.

There are four main types of wireless networks:

- Wireless Local Area Network (LAN): Links two or more devices using a wireless distribution method, providing a connection through access points to the wider Internet.
- Wireless Metropolitan Area Networks (MAN): Connects several wireless LANs.
- Wireless Wide Area Network (WAN): Covers large areas such as neighboring towns and cities.
- Wireless Personal Area Network (PAN): Interconnects devices in a short span, generally within a person's reach.

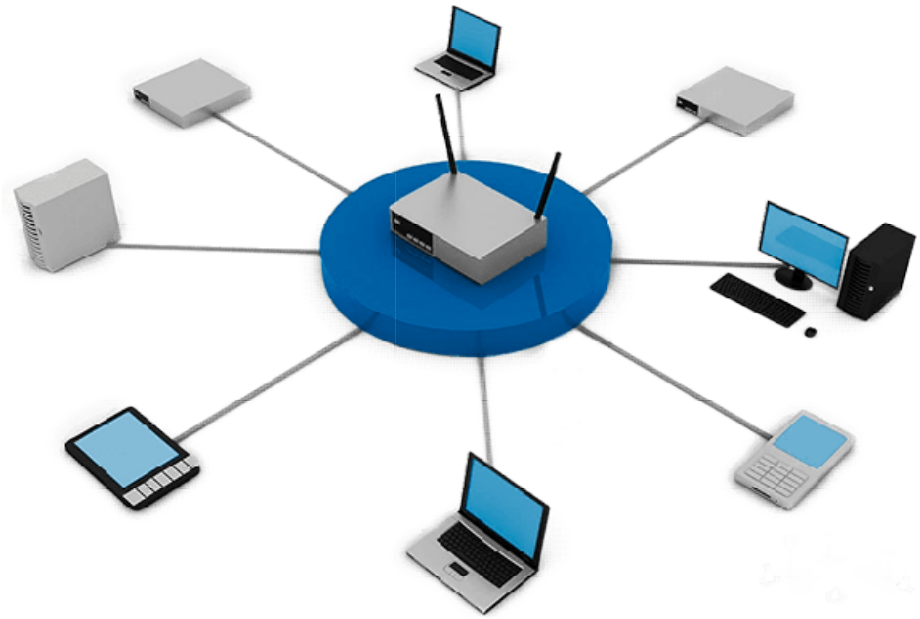
Table: Comparison of Wireless Network Types

Type	Coverage	Performance	Standards	Applications
Wireless PAN	Within reach of a person	Moderate	Wireless PAN Within reach of a person Moderate Bluetooth, IEEE 802.15, and IrDa Cable replacement for peripherals	Cable replacement for peripherals
Wireless LAN	Within a building or campus	High	IEEE 802.11, Wi-Fi, and HiperLAN	Mobile extension of wired networks
Wireless MAN	Within a city	High	Proprietary, IEEE 802.16, and WIMAX	Fixed wireless between homes and businesses and the Internet
Wireless WAN	Worldwide	Low	CDPD and Cellular 2G, 2.5G, and 3G,4G	Mobile access to the Internet from outdoor areas

1.3.1 WLAN

A wireless local area network (WLAN) is a wireless computer network that links two or more devices using a wireless distribution method (often

spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and still be connected to the network, and can provide a connection to the wider Internet. Most modern WLANs are based on IEEE 802.11 standards.



The other factors why WLANs are becoming more acceptable are:

1. No need to be connected physically with each other through any medium such as cables. You can roam around freely in office premises, home or around.
2. WLANs are cost effective. Cabling all the way in the offices, hotels etc. are not needed. So it's cheap and provides same quality of service.
3. Unreachable spots where a cable is hardly accessible, WLAN signals can reach out such as big installations like airports. Also surfing outdoors is also convenient. Just install the device called Access Points (AP) and you are done.
4. Less interruption and easy trouble shooting in case of failures as compared to cabled networks.
5. More secure as most of APs support best encryption methods which protect them from sniffing and other attacks.

1.3.1.1 Major issues with WLAN

Having said that, WLAN are also as prone to various attacks as their counterpart wired LNAs are. Actually WLANs are easier to hack as compared to wired LANs, if not properly configured, due to its easy accessibility around the installation. No need to be in contact of physical wires to hack can be done from anywhere. Its convenience can turn into serious risk to the organization if not configured properly. Major attacks include such as, Sniffing, Key cracking, DoS (Denial of Service), De-authentication attacks, War driving etc. This chapter is not focused on attacks, we shall mainly concentrate on best practices- how to install and use WLAN securely which can thwart a number of above mentioned attacks.

1.3.1.2 Secure WLAN

Wireless Security mainly depends on these 3 factors:

- How much is your wireless network secured in terms of encryption being used?
- Monitoring for suspicious and unusual activities.
- User awareness and education.

These are the combination of various approaches ranging from corporate to home networks. These are also for users how to remain safe while surfing.

Wi-Fi at home

Wi-Fi at home is not a luxury anymore it has become a necessity. However, when the question of security comes into the scene, the first thought that would arise in my mind is how you can protect something which you cannot see, neither can you feel it?

Protecting a home wireless network is altogether a different side of the coin as compared to wired networks. Most of wireless network device vendor's and Internet Service provider do not provide any security settings by default and leave the customer to find for herself. So make sure, your network is secured from being maliciously used. There is no silver bullet that will protect your wireless network infrastructure. These are, however, some countermeasures listed below that should be used in conjunction with each other to secure your wireless network to the highest level:

1. Use most secure possible encryption: The first and most necessary step- use industry standard encryptions. The old (however generally used) WEP-Wired Equivalent Privacy, has been known to be broken. Even you use complex passwords it can be broken and decrypted within minutes or hours. WEP uses 40 bit or 128 bits RC4 ciphers to encrypt the channel.

Instead use secure protocols such as WPA 2 – Wi-Fi Protected Access -2, which uses strong 128 bits AES ciphers and is typically considered more robust encryption strategy available.

2. Use Firewall: All the wireless routers come with built-in firewalls. Enable them with all the security features. You should block any anonymous ping requests and place restrictions on website browsing, if required. Define additional security policies and apply them.

3. Have a monitoring system in place: There's a saying- prevention is better than a cure. If you are able to detect some suspicious activities before it penetrates your network, you can block them or take precautionary measures. Deploy WIPS/WIDS for monitoring suspicious activities.

4. Don't use default credentials: Every wireless router comes with a set of default username/password. Sometimes, people don't change them and keep using them for long time. Username and passwords are used by computers or other devices to connect to wireless router. If any hacker is able to guess them, he can connect to your network easily. Studies show that majority of users use the same combination of username/passwords as set by manufacturers. Some default username combinations are: admin/admin, admin/password or admin/ " ".

5. Disable Auto-connect feature: Some devices or the computers/laptops have 'Let this tool manage your wireless networks' or 'Connect automatically to available network'. Such users having this auto-connect feature enabled are prone to Phishing attack or Rogue AP attack. Attackers keep their APs alive and kicking for such kind of unsuspecting users. They also use luring names as 'HotSpot', 'SecureConnect', 'Govt Networks' etc. The user will never suspect them and keep surfing the wireless network happily. Also if you have not changed the default password of your router, the attacker will try to use this feature on their machine and automatically connect using the easily guessable default passwords.

6. Don't use public Wi-Fi spots to surf sensitive websites: Free and open wireless networks available on airports, cafes, railway stations are not very secure by nature. They do not use any encryption to secure the channel between your laptop to the router. So any information which is not by default going on HTTPS from your laptop/smart phone is susceptible to sniffing and even more your session could be hijacked because the unencrypted channel may leak the active session ID used by your website. All the attacker needs to do is to just install this tool in Firefox and start sniffing the communications on a public unencrypted Wi-Fi. Some applications like Facebook encrypts the login page [HTTPS] but internal pages are served on unencrypted [HTTP] channel so your session ID can be leaked

7. Change the default SSID: Although this will not prevent hackers breaking into a network, using a default SSID acts as an indication that the user is careless. So he may be an obvious target to explore further to see if he still uses the default passwords as well?

8. Restrict access by assigning static IP addresses and MAC filtering: Disable automatic IP assigning feature and use private static IPs to the legitimate devices you 115 want to connect. This will help you in blocking unwanted devices from being connected to your network. Also, enable MAC filtering- router remembers MAC of each and every device connected to it and saves it as list. You can use this facility to restrict access. Only a set of trusted devices can be allowed to connect. However MAC spoofing is still possible but it raises an extra bar for your wireless network.

9. Turn off your router when not in use: Last but not least, a little obvious, but it will save your network from all the attacks for that time period.

1.4 Wireless Network Components

A wireless **network** is "**unsecured**" if you can access the Internet using the **network** without entering a password or **network** key. For example, a "hotspot" is a wireless **network** that is open and available for the public to use.

Depending on network budget or customers, instead of using wired network cards, it can use wireless ones. Most laptops already have a wireless card built-in so it may not have to acquire one. Many new desktop computers now have built-in wireless capability. A wireless NIC appears as its wired counterpart.

1.4.1 Firewall

A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Fig: Firewall

1.4.2 Wireless Access Point

In computer networking, a **wireless access point** (WAP) is a networking hardware device that allows a Wi-Fi compliant device to connect to a wired network. The WAP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself. This is an area in which you can access the wireless network. An example of this device would be a wireless router.

Fig: Wireless Access Point

1.4.3 Modem

A modem (modulator-demodulator) is a network hardware device that modulates one or more carrier wave signals to encode digital information for transmission and demodulates signals to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used with any means of transmitting analog signals, from light emitting diodes to radio. A common type of modem is one that

turns the digital data of a computer into modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

Fig: Modem

1.4.4 Server

In information technology, a server is a computer program that provides services to other computer programs (and their users) in the same or other computers.

The computer that a server program runs in is also frequently referred to as a server (though it may be used for other purposes as well).
In the client/server programming model, a server is a program that awaits and fulfills requests from client programs in the same or other computers. A given application in a computer may function as a client with requests for services from other programs and also as a *server* of requests from other programs.
Specific to the Web, a Web server is the computer program (housed in a computer) that serves requested HTML pages or files. A Web *client* is the requesting program associated with the user. The Web browser in your computer is a client that requests HTML files from Web servers.
This is your connection to the internet. A server is also considered the main computer of a network as it runs the rest of the computers in the network.

Fig: Server

1.4.5 Switch

In a telecommunications network, a switch is a device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. In the traditional circuit-switched telephone network, one or more switches are used to set up a dedicated though temporary connection or circuit for an exchange between two or more parties. On an Ethernet local area network (LAN), a switch determines from the physical device (Media Access Control or MAC) address in each incoming message frame which output port to forward it to and out of. In a wide area packet-switched network such as the Internet, a switch determines from the IP address in each packet which output port to use for the next part of its trip to the intended destination.

Fig: Switch

1.4.6 USB Network Adapter

Besides the wireless network cards that can be installed inside the computer, it can use external cards. These are installed using a USB port.

Fig: USB Network Adapter

1.4.7 Hub

A hub is rectangular box that is used as the central object on which computers and other devices are connected. To make this possible, a hub is equipped with small holes called ports. It can be equipped with 4, 8, 12, 16, 32 ports.

Fig: HUB

1.4.8 Routers: Wired or Wireless

Like a hub, a router is another type of device that acts as the central point among computers and other devices that are part of a network Security.

1.4.9 Station (STA): A STA is a wireless endpoint device, also called a client device. STAs enable end users to gain access and utilize resources provided by wireless networks. Examples include laptop computers, personal digital assistants, mobile phones and other consumer electronic devices with IEEE 802.11 capabilities.

1.4.10 Access Point (AP): An AP logically connects STAs with a distribution system (DS), which is typically an organization's wired network. APs can also logically connect wireless STA with each other without accessing a distribution system. Wireless APs provide users with a mobile capability by allowing users to freely move within a APs coverage area while maintaining connectivity between the user's client device and the AP. APs can also be linked together using wired infrastructure to allow users to "roam" between APs within a building or campus.

The IEEE 802.11 standard also defines the following two WLAN design structures or configurations, as follows:

1.4.11 Ad Hoc Mode: The ad hoc mode does not use APs. Ad hoc mode is sometimes referred to as infra structure less because only peer-to-peer STAs are involved in the communications. This mode of operation is possible when two or more STAs are able to communicate directly to one another. Examples are laptops, mobile phones, PDAs, printers and scanners being able to communicate with each other without an AP. One of the key advantages of ad hoc WLANs is that theoretically they can be formed anytime and anywhere, allowing multiple users to create wireless connections cheaply, quickly, and easily with minimal hardware and user maintenance. However, an ad hoc WLAN cannot communicate with external networks. A further complication is that an ad hoc network can interfere with the operation of an AP-based infrastructure mode network that exists within the same wireless space.

1.4.12 Infrastructure Mode: In infrastructure mode, an AP logically connects STAs to each other or to a distribution system (DS), which is typically an organization's wired network. The DS is the means by which STAs can communicate with the organization's wired LANs and external

networks such as the Internet. Infrastructure mode is the most commonly used mode for WLANs.

1.5 Wireless Security

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users at home. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables.

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. WEP is an old IEEE 802.11 standard from 1999, which was out dated in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP.

Wireless devices communicate through radio transmissions, without physical connections and without network or peripheral cabling. Wireless systems include local area networks, personal networks, cell phones, and devices such as wireless headphones, microphones, and other devices that do not process or store information. Other wireless devices being widely used include infrared (IR) devices such as remote controls, cordless computer keyboards, mouse devices, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver.

Authentication: Only clients who know a shared secret may connect to the network.WEP was the first cryptographic protocol developed for Wi-Fi to enable privacy and authentication. WEP, however, was not secure after all. To rectify the security issues with WEP, the Wi-Fi Alliance pushed a new cryptographic protocol, WPA. Since then, a common practice of securing a WPA enabled network with passwords has been discovered to be vulnerable to an offline dictionary-attack. Even though WPA itself is

thought to be secure, apart from the dictionary-attack, it was a quick fix to the problems in WEP.

1.5.1 Use of Wi-Fi

Wireless technologies have become inexpensive, user- friendly and available to a large number of people and companies. In dense urban areas, access points belonging to different individuals are so closely spaced that their coverage areas overlap. With its popularity and the availability to anyone within range, many individuals detect Wi-Fi networks as a hobby. War drivers bring their laptops and Wi-Fi gear1With WEP, anyone participating in the network can eavesdrop on other conversations in the network in their cars. With the aid of a Global Positioning System (GPS) receiver and an antenna, they explore areas and map the locations and coverage areas of access points. Some do it for the fun, and some with the intent to exploit vulnerable Wi-Fi networks. War bikers and war walkers do the same by other means of transportation.

1.5.2 Service Set Identification (SSID)

Service set identification (SSID) a series of 0 to 32 octets. It is used as a unique identifier for a wireless LAN. Since this identifier must often be entered into devices manually by a human user, it is often a human-readable string and thus commonly called the "network name". An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. A network administrator often uses a public SSID that is set on the access point and broadcast to all wireless devices in range. Some newer wireless access points disable the automatic SSID broadcast feature in an attempt to improve network security.

1.6 Types of Wireless Security

Wireless security is of two types: WEP and WPA.

WEP: WEP stands for Wired Equivalent Privacy. WEP was designed to provide the same level of security as wired networks. When you enable WEP, you set up a network security key. This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

When using WEP, all clients and APs on a wireless network use the same key to encrypt and decrypt data. The key resides in the client computer and

in each AP on the network. Since the 802.11 standard does not specify a key management protocol.15

The shared key can be used for client authentication. This requires a four step process between the AP and the client. This process is as follows:

1. The client makes an authentication request to the AP.
2. The AP returns a challenge phrase to the client.
3. The client encrypts the challenge phrase using the shared symmetric key and transmits it to the AP.
4. The AP then compares the client's response with its phrase; if there is a match, the client is authorized otherwise the client is rejected.

Security problems with WEP include the following:

1. **The use of static WEP keys:** Many users in a wireless network potentially sharing the identical key for long periods of time, is well-known security vulnerability. This is in part due to the lack of any key management provisions in the WEP protocol. If a computer such as a laptop were to be lost or stolen, the key could become compromised along with all the other computers sharing that key.
2. **Caffe Latte attack**: The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.16
3. **WEP provides no cryptographic integrity protection.** However, the 802.11 MAC protocol uses a no cryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledge packets with the correct checksum. The combination of no cryptographic checksums with stream ciphers is dangerous and often introduces vulnerabilities, as is the case for WEP. There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet and CRC sending it to the AP and noting whether the packet is acknowledged. These kinds of attacks are often subtle, and it is now considered risky to design encryption protocols that do not include cryptographic integrity protection, because of the possibility of interactions with other protocol levels that can give away information about cipher text.12

4. **Authentication is not enabled; only simple SSID identification occurs.** Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easily intercepted.
5. **Device authentication is simple shared-key challenge-response.** One-way challenge-response authentication is subject to ―man-in the-middle‖ attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

1.7 WPA Security problems

WPA also implements something called the Extensible Authentication Protocol (EAP) for authorizing users. Instead of authorizing computers based solely on their MAC address, WPA can use several other methods to verify each computer's identity. This makes it more difficult for unauthorized systems to gain access to the wireless network. Security problems with WPA include the following:

1. **Weak Password:** Pre-shared key WPA and WPA2 remain vulnerable to password cracking attacks if users rely on a weak password or passphrase. To protect against a brute force attack, a truly random passphrase of 20 characters (selected from the set of 95 permitted characters) is probably sufficient. Brute forcing of simple passwords can be attempted using the Air crack Suite starting from the four-way authentication handshake exchanged during association or periodic re-authentication.
2. **WPS PIN recovery:** Most recent models have this feature and enable it by default. Many consumer Wi-Fi device manufacturers had taken steps to eliminate the potential of weak passphrase choices by promoting alternative methods of automatically generating and distributing strong keys when users add a new wireless adapter or appliance to a network. These methods include pushing buttons on the devices or entering an 8-digit PIN. The Wi-Fi Alliance standardized these methods as Wi-Fi Protected Setup; however the PIN feature as widely implemented introduced a major new security flaw. The flaw allows a remote attacker to recover the WPS PIN and, with it, the router's WPA/WPA2 password in a few hours.

1.7.1 Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2)

Wi-Fi Protected Access (WPA) is a security standard that improves on older security standards by authenticating network users and providing more advanced encryption techniques. Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two most common security protocol and security certification programs developed by the Wi-Fi Alliance to secure wireless computer network. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP.

1.7.2 Difference between WPA & WPA2

WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA2 became available in 2004 and is common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

1.8 Wireless Security Policy

- **Secure communications:** Encrypt data that travels on the network, and authenticate users to be sure you know who is using the WLAN. Cisco supports all industry-standard encryption and authentication methods for the broadest client device compatibility.
- **Use strong encryption:** As soon as you install your network, set up the strongest wireless encryption you can. Wired Equivalent Privacy (WEP) encryption is adequate, but WPA and WPA2 give you stronger options.
- **Change the default network name:** When you set up your network equipment, change the default name to make it more difficult for hackers to find. Do not choose your company name, company phone number, or other information about your company that is easy to guess or find on the Internet. Use VLANs or MAC address control lists combined with encryption to restrict user access.

- Implement Cisco secure guest access features to allow visitors to connect to the network or Internet while keeping your business network and resources separate and secure.

- Be sure that management ports are secured.
- Physically hide or secure access points to prevent tampering. In many buildings, Cisco access points can be installed in the plenum space above the ceiling, providing optimal coverage in a secure location.
- Use video surveillance cameras to monitor your office building and site for suspicious activity.

1.9 Let us Sum up

In this unit we have discussed about the importance of a wireless network, its components and explained the security issues in different wireless networks. We have compared the performances of different network types. We have also discussed wireless security concepts and types of wireless security. Finally we have outlined the wireless security policies.

1.10 Self assessment Questions

1. What are different wireless components?

……
……
……
……
……
……..

2. Discuss different design structures or configurations of WLAN according to IEEE 802.11 standard?

……
……
……
……
……
……
……
……
……
……

3. What do you mean by Wireless security? What are common types of Wireless security?

……
……
……
……
……
……..

4. What is the security problems associated with WPA?

……
……
……
……
……
……..

5. Discuss the policies on maintaining Wireless Security.

……
……
……
……
……
…….

1.11 Model Questions

1. What is the security problems associated with WEP?
2. What is firewall?
3. Explain about the Wireless Security Policy.
4. Write the Wi-Fi protect process.

1.12 References &Suggested Readings

1. N. Poorinma, S.Gowri, r. Abinaya, "Issues and the Advantages of Wireless Network", 2015 IJEDR, NC3N 2015, ISSN: 2321-9939.
2. https://en.wikibooks.org/wiki/Introduction_to_Computer_Information_Systems/Security
3. Post-Graduate Diploma in Cyber Security Practical Handbook of Internet Security for Beginners (PGDCS-04)
4. Certificate in e-Governance and Cyber Security Cyber Security Techniques (PGDCS-02)

UNIT–2 SECURITY ISSUES IN WIRELESS NETWORKS

Unit Structure

2.1 Introduction
2.2 Learning Objectives
2.3 Wireless Vulnerabilities, Threats and Countermeasures
2.4 Security Concerns for Wireless Networks in Businesses
2.4.1 Public Wireless Security Issues
2.4.2 Security Concerns with Wireless Networks
2.5 About Wireless Attacks Issues
2.5.1 War Driving
2.5.2 Cracking Attacks
2.5.3 Denial of Service
2.5.4 Karma Attacks
2.6 Wireless Security Tips
2.6.1 Wireless Myth Busting
2.6.2 Wireless Encryption
2.7 Wireless Network Attacks
2.7.1 Accidental association
2.7.2 Malicious association
2.7.3 Ad-hoc networks
2.7.4 Non-traditional networks
2.7.5 Identity theft (MAC spoofing)
2.7.6 Man-in-the-middle attacks
2.7.7 Denial of service
2.7.8 Network injection
2.7.9 Caffe Latte attack
2.8 Wireless Attacks Detection Techniques
2.9 Network Auditing
2.9.1 Safety First
2.9.2 Policy
2.9.3 Taking Stock
2.9.4 WLAN Meets LAN
2.9.5 802.11 Security
2.9.6 802.1X
2.9.7Alternative WLAN Network Topologies
2.9.8 Wireless Protected Access
2.9.9 VPNs
2.9.10 WLANs Present Their Own Set of VPN Issues
2.9.11. The Many Facets of Wireless
2.9.12. Portals and 'Mobile VPNs'
2.9.13. Hot Spots Give Security Managers the Chills
2.10 Let us Sum up

2.1 Introduction

The need for security on any network is apparent: the prevention of eavesdropping and the desire for authentication has been the main focus of many network administrators. However, the problems that already exist are added to when you add wireless networking to the equation. As wireless networking becomes more popular, the flawed security of most of those networks becomes more apparent. Several organizations have devised ways to secure their wireless networks from intruders. However, there is currently no wireless security implementation that everyone agrees is always suitable, regardless of what network it is to be used on. Some implementations are satisfactory for some environments, and there is work underway to create future solutions. Meanwhile, some wireless users make the situation more difficult as they advertise existing vulnerable networks.
In this unit we will cover the Vulnerabilities, Threats and Attacks in Wireless Networks, Security issues in wireless networks and the process of Securing Wireless Transmissions, Securing Wireless Access Points, and Securing Wireless Client Devices etc.

2.2 Learning Objectives

After going through this unit you should be able to

- Identify the Vulnerabilities, Threats and Attacks in Wireless Networks
- Know about the different type of wireless security issues.
- Note the Wireless Security Tips.
- Know the Wireless Attacks Detection Techniques.

2.3 Wireless Vulnerabilities, Threats and Countermeasures

The wireless networks consist of four basic components: The transmission of data using radio frequencies; Access points that provide a connection to the organizational network and/or the Client devices (laptops, PDAs, etc.); and users. Each of these components provides an avenue for attack that can result in the compromise of one or more of the three fundamental security objectives of confidentiality, integrity, and availability.

2.4 Security Concerns for Wireless Networks in Businesses

Working in reverse, in using customer networks, you are giving up security in two regards: you're connecting to a network that may or may not require a password that anyone can obtain. You have no way to ascertain the security of the network or even verify and validate that it is truly the network and not an "Evil Twin". You have no way to make sure no one can intercept and read and/or modify your data. Furthermore, while not dangerous yet still annoying, the stores can also monitor your connections and dependent upon the fine print you click "OK" in order to connect, they could query your device and get data about you. This data could be the apps you have installed, location data, and others. The same also applies for applications you install (Walmart Savings Catcher, Macy's App, etc.). These stores also have NO legal obligation or responsibility to protect your device or data on their network. Moral obligations and responsibilities are a different story.

2.4.1 Public Wireless Security Issues

Public Wireless networks (for this, those with a Pre-Shared Key) are not much safer, if at all. While they may not have the same intentions as retail stores, there is no level of assurance or legal obligation for them to secure your device or data. Again, you have no way to make sure no one can intercept and read and/or modify your data. You should question why this network exists, especially if the connection is free. You are probably the "product" via data mining (like retail stores above) or via advertising.

2.4.2 Security Concerns with Wireless Networks

Open Wireless networks are bastions for malicious intent. While some people genuinely want to share and others are ignorant as to the possible outcomes or the ability to secure the networks, others blatantly leave the networks open. Again, you have no way to make sure no one can intercept and read and/or modify your data. If you are connecting to a network that is named after an establishment, you should check to verify they even have a Wireless network before connecting. Many attackers will name their networks after establishments to get people to connect so they can steal their data.

2.5 About Wireless Attacks Issues

2.5.1 War Driving

This is the act of driving around neighborhoods and areas to enumerate what wireless networks exist, what type of encryption (if any) is used, password (if known), and any other pertinent information. This information may chalk or painted to the street or sides walk or posted to various websites. Some websites, like SkyHook ask their users for this. Be cautious when you see various cars sitting outside your house for long periods of time (unless you live near a Pokemon Gym or a Pokestop).

2.5.2 Cracking Attacks

Just like anything else using Passwords, there are desires and ways to crack those passwords to gain access. Without password attacks, there would be no Have I Been Pwned and other similar sites. Very much like other password attacks, there are the simplistic attacks (brute force) and the complex attacks. While brute force will eventually work, there are methods to minimize the impact if compromised. These mitigating factors are mentioned below in the Wireless Security Tips. One tool, or rather a suite of tools, used to crack Wireless (WEP, WPA1, and WPA2) passwords is Aircrack-ng. It is the replacement for Airsnort. You will also need the airmon-ng, airodump-ng, and aireplay-ng tools (hence the suite) as well as a wireless card set to to "Monitor Mode" (like promiscuous mode) to steal the handshake file and replay handshake to get the file to crack. Once you have the file, you can use your favorite password list (mine is a custom list with rockyou.txt as a base) to attempt to crack the key. Note: The key MUST be in the dictionary for this attack to work. See mypasswords blog post for guidance on how to make a complex and difficult password.

2.5.3 Denial of Service

A Denial of Service (DoS) attack is more of a nuisance than a true technical attack. Think of it as an extreme brute force attack that overwhelms something, in this case, a Wireless network or assets/nodes on it. My broad over generalization of it being a nuisance vice technical is an exaggeration; sometimes the vectors of attack for DoS are very technical. Many technologies, namely web servers and websites, have DoS protective measures, as the internet can connect to them if they are public facing.

2.5.4 Karma Attacks (as seen on S2.E6 of Mr. Robot)

The NANO and TETRA Pineapple Wireless Auditing Platforms

Karma was a tool that was used to sniff, probe, and attack Wireless networks using Man-in-the-Middle (MITM) methods. It has since fell from support as Karma but now exists as several other products. For the scope of this blog post, I will be focusing on the current incarnation known as Karmetasploit a portmanteau of Karma and Metasploit. Once the run control file is obtained and everything properly configured, the attacker will use airmon-ng and airbase-ng (relative of all the other airX-ng tools) to establish itself as a wireless access point (AP). This is what perpetrates the Wireless version of the Evil Twin attack. Note: A femtocell was used to do the same thing on Mr. Robot S2.E6. Femtocells target cellular communications vice Wireless and are carrier specific in addition to being specific for 3G, 4G, or LTE as well as GSM or CDMA/WCDMA. In perpetrating the actual attack, the attacker will open metasploit and input the Karma run control file then wait for users to connect. Once they connect, the attacker has visibility into what the victim is doing and browsing as well as the capability to interrogate the victim machine and extract cookies, passwords, and hashes.

2.6 Wireless Security Tips

Now that you're (hopefully) going to avoid using unsecure Wireless, I would like to present to you ways to be secure and maintain your confidentiality, integrity, and availability. We'll discuss a few myths as well as a couple steps to both protect your wireless network as well as protect you on other wireless networks. Keep in mind that there is not and will never be a 100% solution (aside from the obvious of never connecting).

2.6.1 Wireless Myth Busting

The biggest myth I hear is that by not broadcasting your Wireless network name or Service Set Identifier (SSID) attackers will not see your network and thus will not attack it. The SSID is sent in every single packet transmitted wirelessly. Below is the output of a program called inSSIDer that enumerates these networks and their SSIDs, encryption types, and channels. Below is a screen shot of an inSSIDer capture that shows my test network and all types of encryption? You can also see which channel(s) a network is operating on. Note: I edited the SSIDs and MACs out of extreme caution and respect for my neighbors.

The second myth I hear is that MAC filtering works for preventing unauthorized access to wireless networks. This works under a single condition: the attacker does not know and cannot ascertain the MAC address of a client on the network. This is less effective now due to Karma attacks. 802.1x deals with this and is commonly called "Port Security" or Port-based Network Access Control (PBNAC). It also works on wired networks.

2.6.2 Wireless Encryption

In the early days of Wireless, it was more challenging to encrypt the wireless transmission than it was the wired. This led to the creation of WEP, Wired Equivalent Privacy. WEP was great for its time, but with the evolution of computers and the reduced cost of processing power, it was quickly defeated. Below is a summary of wireless encryption protocols:

- Wired Equivalent Privacy (WEP): Deprecated; 64 bit key - 40 bit key and 24 bit Initialization Vector (IV); used Rivest Cipher 4 (RC4); although not as common, also had 128, 152, and 256 bit versions as well;
- Wireless Protected Access (WPA): Deprecated; began implementation of 802.1i standard; used Temporal Key Integrity Protocol (TKIP; which changes the encryption key per packet) vice Cyclic Redundancy Checking (CRC); also use a fixed encryption key for all users' authentication
- Wireless Protected Access Version 2 (WPA-3): Current Standard; implementation of 802.1i standard; eliminated TKIP in favor of CCMP (CCM Protocol; CCM is a mouthful) which enables the use of the Advanced Encryption Standard also use a fixed encryption key for all users' authentication

Both WPA and WPA2 have the following characteristics:

- PSK (Personal)
- Enterprise
- Wireless Protected Setup
- EAP

Using an encrypted network is awesome with this caveat: it depends on how the encryption is implemented. If it is enterprise, then you are more protected because it has multiple keys and does not share them with multiple hosts. Personal (PSK) encryption is better than nothing, but anyone with access can decrypt packets.

2.7 Wireless Network Attacks

Wireless forensics is a sub-discipline of network forensics. The main goal of wireless forensics is to provide the methodology and tools required to collect and analyze (wireless) network traffic that can be presented as valid digital evidence in a court of law. The evidence collected can correspond to plain data or, with the broad usage of Voice-over-IP (VoIP) technologies, especially over wireless, can include voice conversations. Analysis of wireless network traffic is similar to that on wired networks; however there may be the added consideration of wireless security measures. Wireless networks have entered in a paramount way in the day to day life of people as well as enterprises. The wireless have added convenience of mobility and thus introduced risks on the traditional networks.

2.7.1 Accidental association

Unauthorized access to company wireless and wired networks 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.

2.7.2 Malicious association

“Malicious associations” are when wireless devices can be actively made by crackers 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 cracker runs some software that makes his/her wireless network card look like a legitimate access point. Once the cracker 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 cracker is just trying to take over the client at the Layer 2 level.

2.7.3 Ad-hoc networks

Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-topeer 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.

2.7.4 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 nontraditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.

2.7.5 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.

2.7.6 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 AirJack, 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.

2.7.7 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).

2.7.8 Network injection

In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as "Spanning Tree" (802.1D), OSPF, RIP, and HSRP. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.

2.7.9 Caffe Latte attack

The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.

2.8 Wireless Attacks Detection Techniques

Now that we have a good idea of various attacks in a wireless system, we should now look into certain ways that can be employed to detect certain attacks. These detection techniques can be categorized in following three basic forms:

a) Wireless Access point monitoring
b) Wireless client/node monitoring
c) Wireless traffic monitoring

Wireless Access Point Monitoring

In this the wireless network keeps a list of authorized access points and hardware using the net with information like respective SSID, MAC address and other channel information recorded earlier. The monitoring agent/component would continuously listen to wireless frames like beacons, frame probes; responses and authentications etc. sent out by every Access Points and compare these with the previously recorded information. The monitoring device must listen to every possible channel and record all packets for this technique to be effective. To detect Man-in-the-middle attack, such a monitoring component needs to detect that whether there is a sudden introduction of an AP on another channel previously not present. Though the SSID, MAC address might be spoofed (see previous section) by the attacker in the process of setting up the rouge AP, the channel information in which the genuine AP was operating from has been changed which provides an alert on a possible MitM attack.

Wireless Client/Node Monitoring

The access point monitoring is much simpler, in the wireless client monitoring a list of allowed clients' needs to be maintained. This adds up to lot of administrative overheads, however, some of the clients aspects can be recorded and monitored. Like, list of blacklisted clients can be maintained and any movements from these nodes can generate alerts for analysis. Also, all wireless clients with an unauthorized MAC address (MAC address ranges 143 which have not been allocated out yet) are automatically denied access and an alert send off. Also, clients sending probes with typical nicknames can also be recorded and alert generated. One more area where monitoring might be applied is WEP (encrypted) traffic is being used to send/receive, no station should be reusing the same WEP Initialization Vector (used to generate keys) over and over again within a very short period of time (WepWedgie and other cracking tools use this).

For wireless clients that are legitimate, there is a sequence number field within the IEEE 802.11 header which can be tracked for abrupt changes. Certain times when impersonation attacks are being carried out, the attacker will be able to read the MAC / IP address of the victim, but it will not be able to continue with the sequence number used previously by the victim, thus by monitoring the sequence number in these client generated packets impersonation attacks can be easily detected.

General Wireless Traffic Monitoring

To detect DoS attacks, Wireless traffic can be monitored for attempts to flood the network using de-authentication, de-association, authentication, association, erroneous authentication. Frequency and Signal-To-Noise

Ratio monitoring could help signal an oncoming RF based DOS attack on your wireless network. Failures in authentication as well as association can also be monitored and reported.

2.9 Network Auditing

Wireless network auditing is an important part of WLAN security policy. The network needs to be regularly audited for rouge hardware. In this method the network is scanned and mapped for all access points and WLAN nodes. Then this is compared with previous network map. Commonly available network mapping tools like nets tumbler and wavelan-tool can be used to do this. Specialized tools such as Air snort can be used for WEP cracking and auditing the network for weak keys, key reuse and WEP security settings. These methods include the same tests as those carried out by hackers for breaking into the network.

2.9.1 Safety First

The unprotected WLANs are many. Wireless traffic is easily recorded. Passive eavesdroppers can gather proprietary information, logins, passwords, intranet server addresses, and valid network and station addresses. Intruders can steal Internet bandwidth, transmit spam, or use your network as a springboard to attack others. They can capture and modify traffic to masquerade as you, with financial or legal consequences. Even a low-tech attacker can disrupt your business by launching wireless packet floods against your APs, nearby servers, next-hop wired network or Internet uplink.

Fortunately, these risks are not yet heavily exploited. Jupiter Media Research recently reported that 26 percent of surveyed businesses had experienced at least one type of WLAN attack in the past year. However, most of these incidents were problems waiting to happen: rogue APs, stations associating with the wrong AP and war driving. Serious security breaches--like wired network intrusion, theft of confidential data and forgery--were far less common, according to the survey.

In short, early adopters have been lucky. The cost of downtime and cleanup can be an order of magnitude greater than the cost of prevention. Now is the time to start playing catch-up with WLAN security.

2.9.2 Policy

If you don't know what you're defending and why, your security measures are just shots in the dark. It's critical to identify business assets that must be protected and the impact of damage, theft or loss.

For wireless, as with dial-up and DSL, your policy should define access requirements. Who needs access to what and when? If your company already has a remote access policy for travelers and telecommuters, expand it to incorporate wireless. If you have no such policy, create one. Remember to include scenarios that are unique to wireless, like employees at public hot spots (see "Hot Spots Give Security Managers the Chills") or office visitors.

Consider how wireless changes the rules for office visitors. Few companies offer Ethernet access to visiting customers or business partners. Jacks in public areas are typically disabled or latched to known addresses. But wireless laptops and PDAs can easily associate with nearby APs or other wireless stations. This is both a threat and an opportunity. Security policies should define rules for "walled garden" guest access. For example, you may prohibit peer-to-peer networking while permitting logged guest sessions through specific APs with limited destinations, protocols, duration and bandwidth. If guest access is banned, your policy must state this so that steps can be taken to prevent visitor intrusion.

2.9.3 Taking Stock

Before you plot out access point deployment, conduct a site survey using a WLAN discovery tool such as NetStumbler. What you learn might surprise you. According to a recent Gartner report, at least one in five companies find APs deployed without IT department permission. Commodity pricing, retail distribution and setup wizards have made it trivial for employees to install rogue APs, which can expose corporate assets to outsiders and interfere with WLAN performance. Find and eliminate rogue APs from the start--or safely incorporate them into your wireless network design.

You may find nearby APs and stations that don't belong to you. Survey public areas (parking lots, hallways, lobbies) just beyond the physical boundaries of your facility, including upstairs and downstairs. Neighboring MAC addresses should be recorded, along with network name (SSID) and channel. This list will be used to avoid cross-channel interference and eliminate false-positive intrusion alerts.

2.9.4 WLAN Meets LAN

Consider how new WLAN segments will be integrated with and reuse components of your wired infrastructure. Your network topology, device placement and current security measures all have direct impact on wireless LAN security.

Restrict AP placement in your network topology. Wireless applications require protected access to the intranet and/or Internet, affecting routers,

firewall rules and VPN policies. Wireless APs are untrusted entities and should always sit outside the firewall or within a DMZ--never inside the firewall.

Think in terms of a three-interface firewall--intranet on the inside, APs (and other public servers) on the DMZ, and Internet on the outside interface. Circumstances dictate whether your APs should sit on the DMZ or outside.

A DMZ can protect the WLAN from Internet threats while protecting the wired intranet from WLAN threats. However, for example, if your firewall doesn't let VPN tunnels originate in the DMZ, you may need to place your AP on the outside interface instead.

However, WLANs require more bandwidth per user than v.90 or even residential broadband. Smart APs can offload VPN processing, placing fewer demands on the firewall.

2.9.5 802.11 Security

You have an increasing choice of options for authentication and encryption, from several emerging technologies to VPNs. Depending on the size of your enterprise and the level of risk WLAN opens up, you may want to start with the security 802.11 offers out of the box.

Basic 802.11 securities deter accidental association or casual eavesdropping. In most WLAN products, however, these security features are disabled by default. Disabled means the WLAN operates in "open system" mode--any station can join because they know the network's Service Set Identifier (SSID) or by capturing beacon frames broadcast by APs.

2.9.6 802.1X

Many APs can be configured with a list of MAC addresses to allow or block. But MAC addresses can be forged. To address this, IEEE 802.1X provides a standard, multivendor framework for combining port-level access control with some type of authentication.

2.9.7Alternative WLAN Network Topologies

802.1X applies the Extensible Authentication Protocol (EAP) to LANs--wired and wireless--defining messages to be exchanged between LAN stations (supplicants), APs (authenticators) and backend authentication servers. Think of 802.1X as an on/off switch that blocks everything but EAP until the authentication server accepts the supplicant's access request.

Encryption keys are supplied dynamically to authorized stations on a per-session basis.

2.9.8 Wireless Protected Access

Wireless is the brand given to 802.11 products certified by the Wireless Alliance, a consortium organized to promote 802.11 products and interoperability among them. Wireless Protected Access (WPA) is a security enhancement for current-generation WLAN hardware. WPA incorporates just the stable parts of the 802.11i advanced security standard, which is still a work in progress. WPA products can interoperate with the older WEP products.

2.9.9 VPNs

If your company already has a remote access VPN, consider using it for WLAN security. Reuse makes the most sense when security policy is consistent for WAN and LAN access--the same credentials can be used for authentication; the same encryption algorithms can be used for confidentiality.

2.9.10 WLANs Present Their Own Set of VPN Issues

There is more data to encrypt on a high-speed WLAN. Additional gateways may be needed to support wireless encryption, particularly when using 802.11a/g at link speeds up to 54 Mbps.

Tunnels are bound to IP addresses. WLAN stations roam between APs, changing IP address. Broken tunnels can be reestablished, but service disruption is often noticeable. In smaller WLANs, several APs can share the same DHCP scope. VLANs can help, up to a point. In larger WLANs, wireless gateways can provide tunnel persistence when stations roam.

Client deployment can be costly and difficult to mandate. Reusing deployed clients is one thing, adding new clients and policies quite another.

VPN tunnels, WEP/TKIP and 802.1X address different problems. Consider a business partner using a guest WLAN. A tunnel controls access to the visitor's own network; 802.1X controls access to the guest WLAN. A tunnel prevents eavesdropping from end to end; WEP/TKIP prevents eavesdropping on the air link only.

2.9.11. The Many Facets of Wireless

When considering wireless, it's important to realize that there are many kinds of wireless technologies, aimed at different devices and usage environments:
Wireless Personal Area Networks (WPANs) use very short-range wireless technology to replace cables connecting PCs with peripherals, phones with headsets, etc. The most popular WPAN is Bluetooth (IEEE 802.15), which reaches about 30 feet, at speeds up to 780 Kbps.

2.9.12. Portals and 'Mobile VPNs'

Portals frequently control access to public hot spots and guest networks (wired or wireless). Outbound HTTP requests are redirected to a login page, where the user authenticates via SSL before access is granted to the network.

2.9.13. Hot Spots Give Security Managers the Chills

For several years, road warriors have used Internet cafés to check e-mail. Wireless hot spots make this more convenient. Workers use hot spots to make productive use of time spent waiting in airports and hotel lobbies.
Hot spots are found in 1.67 million access locations across the United States. With cellular carriers buying their way into the hot spot market, things are likely to change. By 2007, Analysis Re-search predicts 21 million people in the U.S. will use hot spots. Cometa Networks-an AT&T, IBM Global Services and Intel partnership-wants to make wireless connectivity ubiquitous by building a national hot spot network, are placing APs within a five-minute walk in cities and a five-minute drive elsewhere.

2.10 Let us Sum up

In this unit we have provided an overview of the security problems in wireless networks and focusing on security issues of wireless network. We have describe about how to securing wireless transmission and how to protect it confidentiality. Wireless networks have entered in a paramount way in the day to day life of people as well as enterprises. The wireless networks have added convenience of mobility and thus introduced risks on the traditional networks.

2.11 Self assessment Questions

1. What is malicious association?

……
……
……
……
……
……
……

2. What is network auditing?

……
……
……
……
……
……
……

3. Write about wireless network attacks.

……
……
……
……
……
……
……

4. How to secure wireless client devices?

……
……
……
……
……
……

5. Discuss about different type of wireless attack issues.

……
……

……
……
……
……

2.12 Model Questions

1. Discuss about the tips to Wireless Network Security.
2. Write the sort notes about Wireless Encryption.
3. What are the different types of Wireless Network Attacks?
4. What are the public wireless security issues?

2.13 References &Suggested Readings

1. Wireless Networks: Security Problems and Solutions, SANS Institute 2002
2. Jie Gao, Department of Computer Science, Stony Brook University, Stony Brook, NY 11794, USA, jgao@cs.sunysb.edu, April 24, 2007
3. R. Rathika, D. Sowmyadevi, Wireless Sensor Network Security: Vulnerabilities, Threats and Countermeasures, IJARCSSE, Volume 6, Issue 1, January 2016 ISSN: 2277 128X.
4. Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, Wireless Network Security: Vulnerabilities, Threats and Countermeasures, International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008.
5. Post-Graduate Diploma in Cyber Security Cyber Attacks and Counter Measures: User Perspective (PGDCS-03).

UNIT – 3 SECURING A WIRELESS NETWORK

Unit Structure

3.1 Introduction
3.2 Learning Objectives
3.3 Securing Wireless Signal Transmissions
3.3.1 Protecting the Wireless Transmissions
3.3.2 Preventing Alteration of Intercepted Communications
3.3.3 Reduce the Risk of Denial-of-Service Attacks
3.4 Securing Wireless Access Points
3.4.1 Countermeasures to Secure Wireless Access Points
3.5 Securing the Wireless Client
3.6 Securing Wireless Communications
3.7 Securing Wireless Client Devices
3.8 Vulnerabilities of wireless networks, devices, and protocols.
3.8.1 Insertion attacks
3.8.2. Interception and Monitoring of Wireless Traffic
3.8.3. Jamming
3.8.4. Client-to-Client Attacks
3.8.5. Brute Force Attacks against Access Point Passwords
3.8.6. Attacks against Encryption
3.9. Misconfiguration
3.10 Securing Wireless Networks
3.10.1 Use of Encryption
3.10.2 Use anti-virus, anti-spyware software, and a firewall
3.10.3 Turn off identifier broadcasting
3.10.4 Change the identifier on your router from the default
3.10.5 Change your router's pre-set password for administration
3.10.6 Allow only specific computers to access your wireless network
3.10.7 Turn off your wireless network when you know you won't use it
3.10.8 Don't assume that public "hot spots" are secure
3.11 Wireless Network Security protocols
3.12 Authentication of Wireless Network
3.12.1 Use of Wi-Fi
3.12.2 Security problems with WEP include the following
3.13 Let us Sum up

3.1 Introduction

Wireless Networking (Wireless) has made it so easy for anyone to use Internet on your computer, mobile phones, tablets and other wireless devices anywhere in the house without the clutter of cables.
With traditional wired networks, it is extremely difficult for someone to steal your bandwidth but the big problem with wireless signals is that others can access the Internet using your broadband connection even while they are in a neighboring building or sitting in a car that's parked outside your apartment.

3.2 Learning Objective

After going through this unit you should be able to

- Know the security risks posed by wireless computer networks.
- To provide guidance for establishing secure wireless networks.
- To know the suggested management, operational and technical countermeasures to help mitigate security risks specific to wireless computing technologies.
- Authentication of secure wireless networks with attacks.

3.3 Securing Wireless Signal Transmissions

The nature of wireless communications creates three basic threats: Interception, Alteration and Disruption.

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

3.3.1 Protecting the Wireless Transmissions

Two types of countermeasures exist for reducing the risk of eavesdropping on wireless transmissions. The first involves methods for making it more difficult to locate and intercept the wireless signals. The second involves the use of encryption to preserve confidentiality even if the wireless signal is intercepted.

Signal-Hiding Techniques

In order to intercept wireless transmissions, attackers first need to identify and locate wireless networks. There are, however, a number of steps that organizations can take to make it more difficult to locate their wireless access points. The easiest and least costly include the following: Turning off the service set identifier (SSID) broadcasting by wireless access points, Assign cryptic names to SSIDs, Reducing signal strength to the lowest level that still provides requisite coverage or Locating wireless access points in the interior of the building, away from windows and exterior walls. More effective, but also more costly methods for reducing or hiding signals include: Using directional antennas to constrain signal emanations within desired areas of coverage or Using of signal emanation-shielding techniques, sometimes referred to as TEMPEST, 1 to block emanation of wireless signals.

Encryption

The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic. This is especially important for organizations subject to regulations.

3.3.2 Preventing Alteration of Intercepted Communications

Interception and alteration of wireless transmissions represents a form of "man-in the middle" attack. Two types of countermeasures can significantly reduce the risk of such attacks: strong encryption and strong authentication of both devices and users.

3.3.3 Reduce the Risk of Denial-of-Service Attacks

Wireless communications are also vulnerable to denial-of-service (DoS) attacks. Organizations can take several steps to reduce the risk of such unintentional DoS attacks. Careful site surveys can identify locations where signals from other devices exist; the results of such surveys should be used when deciding where to locate wireless access points. Regular periodic audits of wireless networking activity and performance can identify

problem areas; appropriate remedial actions may include removal of the offending devices or measures to increase signal strength and coverage within the problem area.

3.4 Securing Wireless Access Points

Insecure, poorly configured wireless access points can compromise confidentiality by allowing unauthorized access to the network.

3.4.1 Countermeasures to Secure Wireless Access Points

Organizations can reduce the risk of unauthorized access to wireless networks by taking these three steps:

1. Eliminating rogue access points;
2. Properly configuring all authorized access points; and
3. Using 802.1 xs to authenticate all devices.

1 Eliminate Rogue Access Points

The best method for dealing with the threat of rogue access points is to use 802.1 xs on the wired network to authenticate all devices that are plugged into the network. Using 802.1x will prevent any unauthorized devices from connecting to the network.

2 Secure Configurations of Authorized Access Points

Organizations also need to ensure that all authorized wireless access points are securely configured. It is especially important to change all default settings because they are well known and can be exploited by attackers.

3 Use 802.1 xs to authenticate all devices

Strong authentication of all devices attempting to connect to the network can prevent rogue access points and other unauthorized devices from becoming insecure backdoors. The 802.1x protocol discussed earlier provides a means for strongly authenticating devices prior to assigning them IP addresses.

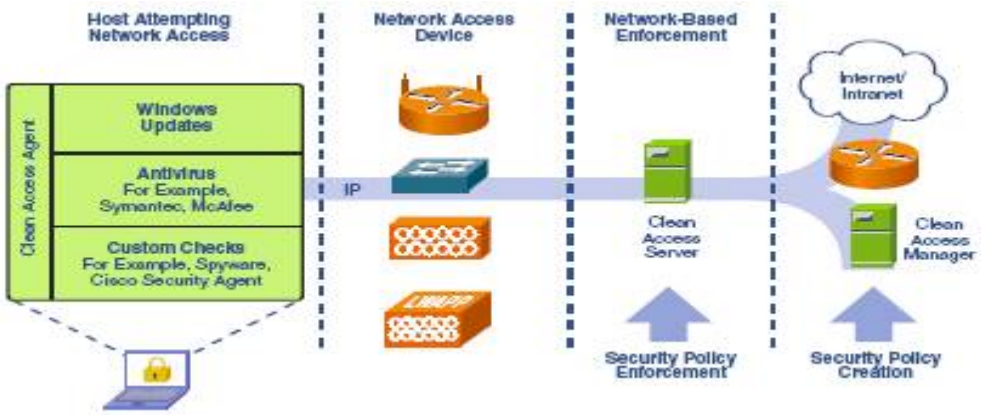
3.5 Securing the Wireless Client

An essential step in wireless security is locking down the client device used to access the wireless network. If a laptop or other endpoint is compromised, then the device can be used to gain entry into the network, regardless of other wireless security measures that may be in place. By the way, this is true whether a client is used to access the network over wireless or wired. Mobile clients, like laptops, are inherently used in some unfriendly places outside the corporate network, and can become infected with malicious software.

One way hackers have gained access to corporate wireless networks is to hack the laptop of an employee while they are sitting in an airport or coffee shop. There are a couple of well known attacks that can be launched at a wireless NIC, which can result in learning the corporate wireless security key.

Whether accessing a wired or wireless network, it is a best practice to implement host-based security on clients, including anti-virus and host intrusion protection such as Cisco Security Agent (CSA). With CSA, attempts to install software or execute harmful calls in the operating system can be intercepted and prevented.

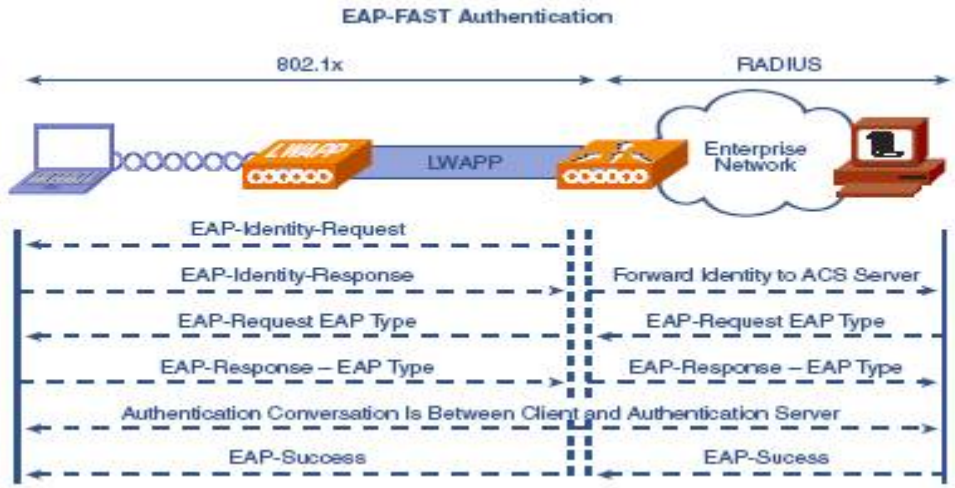
Another important measure is to insure that clients accessing the network are "healthy," meaning that they have not been compromised, have the correct anti-virus software running, and are otherwise compliant with the company's security policy. Enforcement of all these measures can be difficult, but with Cisco Clean Access (CCA) solution, the wireless network can challenge endpoints to prove compliance and "health" before being permitted on the network.



3.6 Securing Wireless Communications

The next step to securing the wireless network (which is where most people start and often stop) is securing the actual wireless communications over the air between the client device and the wireless access point. There are two best practices to follow: authentication and encryption.

Authentication of wireless clients by the network insures that only authorized devices are allowed to join the wireless network. The best practice for authentication is to implement Extensible Authentication Protocol (EAP) and Flexible Authentication via Secure Tunnel (FAST). Using a set of credentials on the client device, the wireless network can authenticate the endpoint against the credentials stored in the corporate identity database. If a match is not achieved, access to the wireless network is denied. (Wired networks are implementing an equivalent technique via 802.1x.)



Just as important as the network authenticating a wireless client is for the wireless client to authenticate the network to which it is connecting. "Imposter" access points can be setup posing as legitimate corporate wireless network access points. If only the SSID is used to determine the network authenticity, this is trivial to imitate. The wireless client needs to use additional factors and credentials to authenticate that the access point it is trying to connect to be really a corporate network access point. This mutual authentication is also part of the EAP-FAST authentication process.

3.7 Securing Wireless Client Devices

Two major threats to wireless client devices are
(1) Loss or Theft
(2) Compromise.
Loss or theft of laptops and PDAs is a serious problem. Laptops and PDAs often store confidential and proprietary information. Consequently, loss or theft of the devices may cause the organization to be in violation of privacy regulations involving the disclosure of personal identifying information it has collected from third parties. Another threat to wireless client devices is that they can be compromised so that an attacker can access sensitive information stored on the device or use it to obtain unauthorized access to other system resources.

3.8 Vulnerabilities of wireless networks, devices, and protocols.

There are a number of vulnerabilities in the security protocols listed above. We describe some of these vulnerabilities in the following sections.

3.8.1 Insertion attacks

Insertion attacks are based on deploying unauthorized devices or creating new wireless networks without going through security process and review.

- **Unauthorized Clients –** An attacker tries to connect a wireless client, typically a laptop or PDA, to an access point without authorization. Access points can be configured to require a password for client access. If there is no password, an intruder can connect to the internal network simply by enabling a wireless client to communicate with the access point.
- **Unauthorized or Renegade Access Points –** An organization may not be aware that internal employees have deployed wireless capabilities on their network in the form of an unauthorized access point, attached to the wired network.. This lack of awareness could lead to the previously described attack, with unauthorized clients gaining access to corporate resources through the rogue access point.

3.8.2. Interception and Monitoring of Wireless Traffic

As in wired networks, it is possible to intercept and monitor network traffic across a wireless LAN. The attacker needs to be within range of an access point (approximately 300 feet for 802.11b) for this attack to work, whereas a wired attacker can be anywhere there is a functioning network connection. The advantage for a wireless interception is that a wired attack requires the placement of a monitoring agent on a compromised system. All a wireless intruder needs is access to the network data stream traveling over public air waves.

There are two important considerations to keep in mind with the range of 802.11b access points. First, directional antennae can dramatically extend either the transmission or reception ranges of 802.11b devices. Therefore, the 300 foot maximum range attributed to 802.11b only applies to normal, as-designed installations. Enhanced equipment also enhances the risk. Second, access points transmit their signals in a circular pattern, which means that the 802.11b signal almost always extends beyond the physical boundaries of the work area it is intended to cover. This signal can be intercepted outside buildings, or even through floors in multistory buildings. Some of the monitoring techniques:

- **Wireless Packet Analysis –** Attacker captures wireless traffic using techniques similar to those employed on wired networks. Many of these tools capture the first part of the connection session, where the data would typically include the username and password. An intruder can then masquerade as a legitimate user by using this captured information to hijack the user session and issue unauthorized commands.
- **Broadcast Monitoring –** If an access point is connected to a hub rather than a switch, any network traffic across that hub can be potentially broadcast out over the wireless network. Because the Ethernet hub broadcasts all data packets to all connected devices including the wireless access point, an attacker can monitor sensitive data on the wireless network, not even intended for any wireless clients.
- **Access Point Clone (Evil Twin) Traffic Interception –** The availability of WiFi in coffee shops, airports and other high-traffic areas led to the evolution of the Evil Twin Network. The Evil Twin is essentially a wireless version of a phishing scam users think they're connecting to a genuine hot spot but are actually connecting to a rogue access point set up by a phisher. Once connected, the

attacker serves up pages mimicking actual websites. Banking, EBay or PayPal sites are the websites of choice. All the attacker needs is the hardware for an access point (with a higher signal strength than the target network) and off-the-shelf software tools like Karma 10 which is a set of wireless sniffing tools to discover clients and their preferred/trusted networks by passively listening for 802.11 Probe Request frames.

3.8.3. Jamming

Denial of service attacks are also easily applied to wireless networks, where legitimate traffic cannot reach clients or the access point because illegitimate traffic overwhelms the frequencies. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency (or the other frequencies in which WiFi operates), corrupting the signal until the wireless network ceases to function. In addition, cordless phones, baby monitors and other devices that operate on the 2.4 GHz band can disrupt a wireless network using this frequency. These denials of service attacks can originate from outside the work area serviced by the access point, or can inadvertently arrive from other WiFi devices installed in other work areas that degrade the overall signal.

3.8.4. Client-to-Client Attacks

Two wireless clients can talk directly to each other, bypassing the access point. Users therefore need to defend clients not just against an external threat but also against each other.

- File Sharing and Other TCP/IP Service Attacks – Wireless clients running TCP/IP services such as a Web server or file sharing are open to the same exploits and Misconfiguration as any user on a wired network.
- DOS (Denial of Service) – A wireless device floods another wireless client with bogus packets, creating a denial of service attack. In addition, duplicate IP or MAC addresses, both intentional and accidental, can cause disruption on the network.

3.8.5. Brute Force Attacks against Access Point Passwords

Most access points use a single key or password that is shared with all connecting wireless clients. Brute force dictionary attacks attempt to compromise this key by methodically testing every possible password. The intruder gains access to the access point once the password is guessed. In addition, passwords can be compromised through less aggressive means. A compromised client can expose the access point. Not changing the keys on

a frequent basis or when employees leave the organization also opens the access point to attack. Managing a large number of access points and clients only complicates this issue, encouraging lax security practices.

3.8.6. Attacks against Encryption

The 802.11, Wired Equivalent Privacy (WEP) standard, described above, was intended to make a WLAN as secure as an unsecured wired network. Not long after WEP was developed, a series of independent research studies began to expose its cryptographic weaknesses. The first practical attack on WEP was identified by researchers11 Scott Fluhrer, Itsik Mantin and Adi Shamir who found that, even with WEP enabled, third parties with a moderate amount of technical expertise and resources could breach WLAN security.

Three key difficulties were identified:

- WEP uses a single, static shared key. It remains the same unless a network administrator manually changes it on all devices in the WLAN, a task that becomes ever more daunting as the size of the WLAN increases.
- At the time of its introduction, WEP employed a necessarily short 40-bit encryption scheme. The scheme was the maximum allowed by US export standards at that time. In 1997, the US government deemed the export of data cryptography to be as threatening to national security as the export of weapons of mass destruction. By necessity, WiFi security had to be weak if the specification was to be adopted as an international standard and if products were to be freely exported.
- Other technical problems contributed to its vulnerability, including attacks that could lead to the recovery of the WEP key itself. Attacks based on Fluhrer, Mantin and Shamir's paper have come to be known as "FMS Attacks". Shortly after the FMS paper was released, the following tools to automate WEP cracking were developed:
- WEPCrack
- AirSnort

In response to the weaknesses in WEP new security mechanisms were developed.

- Cisco developed the Lightweight Extensible Authentication Protocol (LEAP)
- WiFi protected access (WPA) was developed to replace WEP. It had 2 sub-parts-
- WPA-PSK (Pre-Shared key)

- WPA-Radius

In March 2003, Joshua Wright12 disclosed that LEAP was vulnerable to dictionary attack. A short time later Wright released ASLEAP, a tool to automate attacks against LEAP. Cisco released EAP-FAST as a replacement for LEAP about a year after Wright's initial disclosure to them. In November 2003 Robert Moskowitz of ISCA Labs detailed potential problems with WPA when deployed using a Pre-Shared Key in his paper "Weakness in Passphrase Choice in WPA Interface".

In November 2004 Joshua Wright released CoWPAtty which could perform an automated dictionary attack process against WPA-PSK networks.

Attacks against WEP

Even with chopping attacks, a large number of packets still need to be captured by an attacker. The easiest way to do this is by re-injecting packets back into the network to generate unique initialization vectors.

Attacks against WPA

WPA Pre shared keys with pass-phrases shorter than 21 characters is vulnerable to dictionary attacks. This is an offline attack and not as easy to identify in real time as attacks against WEP.

3.9. Misconfiguration

Many access points ship in an unsecured configuration in order to emphasize ease of use and rapid deployment. Unless administrators understand wireless security risks and properly configure each unit prior to deployment, these access points will remain at a high risk for attack or misuse. The following section examines three leading access points, one each from Cisco, Lucent and 3Com. Although each vendor has its own implementation of 802.11b, the underlying issues should be broadly applicable to products from other vendors.

- **Server Set ID (SSID) –** SSID is a configurable identification that allows clients to communicate with an appropriate access point. With proper configuration, only clients with the correct SSID can communicate with access points. In effect, SSID acts as a single shared password between access points and clients. Access points come with default SSIDs. If not changed, these units are easily compromised. Here are common default SSID's:

Manufacturer	Default SSID
Cisco	tsunami
3Com	101
Lucent/Cabletron	Roam About Default Network Name
Addtron	WLAN
Intel	intel
Linksys	linksys

SSIDs go over the air as clear text if WEP is disabled, allowing the SSID to be captured by monitoring the network's traffic. Another common vulnerability regarding the SSID is setting it to something meaningful such as the AP's location or department, or setting them to something easily guessable.

By default, the Access Point broadcasts the SSID every few seconds in what are known as 'Beacon Frames'. While this makes it easy for authorized users to find the correct network, it also makes it easy for unauthorized users to find the network name. This feature is what allows most wireless network detection software to find networks without having the SSID upfront.

- **Wired Equivalent Privacy (WEP) –** WEP can be typically configured as follows:
  - No encryption
  - 40 bit encryption
  - 128 bit encryption

Most access point's ship with WEP turned off. Although 128 bit encryption is more effective than 40 bit encryption, both key strengths are subject to WEP's known flaws.

- **SNMP Community Passwords** – Many wireless access points run SNMP agents. If the community word is not properly configured, an intruder can read and potentially write sensitive data on the access point. If SNMP agents are enabled on the wireless clients, the same risk applies to them as well.

By default, many access points are read accessible by using the community word, "public". 3Com access points allow write access by using the community word, "comcomcom". Cisco and Lucent/Cabletron require the write community word to be configured by the user or administrator before the agent is enabled.

- **Client Side Security Risk –** Clients connected to access point store sensitive information for authenticating and communicating to the access point. This information can be compromised if the client is not properly configured. Cisco client software stores the SSID in the Windows registry, and the WEP key in the firmware, where it is more difficult to access. Lucent/Cabletron client software stores the SSID in the Windows registry. The WEP key is stored in the Windows registry, but it is encrypted using an undocumented algorithm. 3Com client software stores the SSID in the Windows registry. The WEP key is stored in the Windows registry with no encryption.
- **Installation –** By default, all three access points are optimized to help build a useful network as quickly and as easily as possible. As a result, the default configurations minimize security.

3.10 Securing Wireless Networks

3.10.1 Use of Encryption

The most effective way to secure your wireless network from intruders is to encrypt, or scramble, communications over the network. Most wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router doesn't have an encryption feature, consider getting one that does. Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on.

3.10.2 Use anti-virus, anti-spyware software, and a firewall

Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

3.10.3 Turn off identifier broadcasting

Most wireless routers have a mechanism called identifier broadcasting. It sends out a signal to any device in the vicinity announcing its presence. You don't need to broadcast this information if the person using the network already knows it is there. Hackers can use identifier broadcasting to home in on vulnerable wireless networks. Disable the identifier broadcasting mechanism if your wireless router allows it.

3.10.4 Change the identifier on your router from the default

The identifier for your router is likely to be a standard, default ID assigned by the manufacturer to all hardware of that model. Even if your router is

not broadcasting its identifier to the world, hackers know the default IDs and can use them to try to access your network. Change your identifier to something only you know, and remember to configure the same unique ID into your wireless router and your computer so they can communicate. Use a password that's at least 10 characters long: The longer your password, the harder it is for hackers to break.

3.10.5 Change your router's pre-set password for administration

The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router. Hackers know these default passwords, so change it to something only you know. The longer the password, the tougher it is to crack.

3.10.6 Allow only specific computers to access your wireless network

Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

3.10.7 Turn off your wireless network when you know you won't use it

Hackers cannot access a wireless router when it is shut down. If you turn the router off when you're not using it, you limit the amount of time that it is susceptible to a hack.

3.10.8 Don't assume that public "hot spots" are secure

Many cafés, hotels, airports, and other public establishments offer wireless networks for their customers' use.

3.11 Wireless Network Security protocols

One of the biggest concerns for wireless users is making sure their router and wireless network are secure. I think we all know by now that, when it comes to technology, there is no such thing as being 100 percent secure. Once you send data over a wireless signal, you've already potentially exposed your data to hackers, and once you've set up a router, Wireless signal leeches are always a possibility.

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users at home. Wireless technologies, in the simplest sense, enable one or more devices to

communicate without physical connections—without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables.

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wireless Protected Access (WPA). WEP is a notoriously weak security standard. WEP is an old IEEE 802.11 standard from 1999, which was out dated in 2003 by WPA, or Wireless Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP.

Wireless devices communicate through radio transmissions, without physical connections and without network or peripheral cabling. Wireless systems include local area networks, personal networks, cell phones, and devices such as wireless headphones, microphones, and other devices that do not process or store information. Other wireless devices being widely used include infrared (IR) devices such as remote controls, cordless computer keyboards, mouse devices, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver.

3.12 Authentication of Wireless Network

Only clients who know a shared secret may connect to the network.WEP was the first cryptographic protocol developed for Wireless to enable privacy and authentication. WEP, however, was not secure after all. To rectify the security issues with WEP, the Wireless Alliance pushed a new cryptographic protocol, WPA. Since then, a common practice of securing a WPA enabled network with passwords has been discovered to be vulnerable to an offline dictionary-attack. Even though WPA itself is thought to be secure, apart from the dictionary-attack, it was a quick fix to the problems in WEP.

3.12.1 Use of Wi-Fi

Wireless technologies have become inexpensive, user- friendly and available to a large number of people and companies. In dense urban areas,

access points belonging to different individuals are so closely spaced that their coverage areas overlap. With its popularity and the availability to anyone within range, many individuals detect Wi-Fi networks as a hobby. War drivers bring their laptops and Wi-Fi gear1With WEP, anyone participating in the network can eavesdrop on other conversations in the network in their cars. With the aid of a Global Positioning System (GPS) receiver and an antenna, they explore areas and map the locations and coverage areas of access points. Some do it for the fun, and some with the intent to exploit vulnerable Wi-Fi networks. War bikers and war walkers do the same by other means of transportation.

3.12.2 Security problems with WEP include the following

1. The use of static WEP keys: Many users in a wireless network potentially sharing the identical key for long periods of time, is well-known security vulnerability. This is in part due to the lack of any key management provisions in the WEP protocol. If a computer such as a laptop were to be lost or stolen, the key could become compromised along with all the other computers sharing that key.

2. Caffe Latte attack: The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.

3. WEP: WEP provides no cryptographic integrity protection. However, the 802.11 MAC protocol uses a no cryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledge packets with the correct checksum. The combination of no cryptographic checksums with stream ciphers is dangerous and often introduces vulnerabilities, as is the case for WEP. There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet and CRC sending it to the AP and noting whether the packet is acknowledged.

4. Authentication is not enabled: only simple SSID identification occurs. Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easily intercepted.

5. Device authentication is simple shared-key challenge-response. One-way challenge-response authentication is subject to ―man-in the-middle‖

attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

3.13 Let us Sum up

Although Wi-Fi technologies have significantly improved their security capabilities, many of the features and abilities are available only in newer equipment for IT-managed infrastructure. Meanwhile, cellular data networks rely on a completely separate security architecture that emphasizes protection of the radio link and does not provide end-to-end encryption. By using an SSL VPN, you can secure all forms of wireless communication, both externally and internally. Moreover, this approach accommodates a wide range of user equipment. Nevertheless, it's too soon to tell whether WNS encryption problems will turn out to be a tempest in a teapot or seriously exploited vulnerabilities.

3.14 Self assessment Questions

1. Describe about securing wireless signal transmission.

……
……
……
……
……
……
……

2. What is an insertion attack?

……
……
……
……
……
……
……

3. Write about the Use of Wi-Fi in network.

……
……
……
……

……
……
……
4. Explain about Jamming signal.
……
……
……
……
……
……
……
5. Write about Authentication of Wireless Network.
……
……
……
……
……
……
……

3.15 Model Questions

1. What are the methods for securing wireless transmissions?
2. What are the processes for securing wireless networks?
3. Write about Client-to-Client Attacks.
4. What is Misconfiguration
5. How to secure wireless client devices?

3.16 References &Suggested Readings

1. Using Wireless Technology Securely, Produced 2006 by US-CERT, a government organization. Updated 2008.
2. Jeff Bilger, Holly Cosand, Noor-E-Gagan Singh, Joe Xavier, "Security and Legal Implications of Wireless Networks, Protocols, and Devices".
3. Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks" June 30, 2012.
4. http://www.cisco.com/web/services/news/ts_newsletter/tech/chalktalk/archives/200802.html

UNIT-4 MOBILE DEVICE SECURITY

Unit Structure

4.1 Introduction
4.2 Learning Objective
4.3 Mobile Device Security
    4.3.1 Security Threats
4.4 Mobile Device Security Strategy
4.5 Mobile Security Process
    4.5.1 Theft protection
    4.5.2 Lock
    4.5.3 Locate
    4.5.4 SIM Protection
    4.5.5 Malware protection
    4.5.6 Windows products
    4.5.7 Battery usage
4.6 Protection against Android malware
4.7 Encryption for mobile devices
4.8 Authentication and authorization for mobile devices
4.9 Remote wipe for mobile device security
4.10 Mobile device management
4.11 Let us Sum up

4.1 Introduction

Smartphone's are the future of modern communications. According to a survey carried out by IDC there are over 1.6 billion smart phones running Android in current use. Classic telephone functions are becoming less relevant. For example, the inclusion of high-quality cameras means that smart phones are being used more and more to take photos. Additionally, users are employing services like Facebook, WhatsApp and Email to run their lives from their smart phones. This means that smart phones are being targeted by criminals, who try to infect devices and/or steal sensitive data, e.g. by phishing attacks. As modern smart phones are often expensive to buy, they are also an attractive target for thieves. As it is not possible to physically prevent them from being stolen, they must be made less attractive to thieves. Consequently, many of today's security products contain not only malware protection, but also highly developed theft-protection

functions, such as anti theft software, which make the device less attractive to thieves (e.g. by locking the device), and help the owner to find it again.

4.2 Learning Objective

After going through this unit you should be able to

- Know the use of security software on MOBILE.
- Develop a sense of responsibility to store personal data, private photos, Internet banking information or even company data.
- Know how to protect smart phones which are know a days are more costly.

4.3 Mobile Device Security

Prior to the widespread use of smart phones, the dominant paradigm for computer and network security in organizations was as follows. Corporate IT was tightly controlled. User devices were typically limited to Windows PCs. Business applications were controlled by IT and either run locally on endpoints or on physical servers in data centers. Network security was based upon clearly defined perimeters that separated trusted internal networks from the un-trusted Internet. Today, there have been massive changes in each of these assumptions. An organization's networks must accommodate the following.

Growing use of new devices: Organizations are experiencing significant growth in employee use of mobile devices. In many cases, employees are allowed to use a combination of endpoint devices as part of their day-to-day activities.

Cloud-based applications: Applications no longer run solely on physical servers in corporate data centers. Quite the opposite, applications can run anywhere on traditional physical servers, on mobile virtual servers, or in the cloud. Additionally, end users can now take advantage of a wide variety of cloud-based applications and IT services for personal and professional use. Facebook can be used for an employee's personal profiles or as a component of a corporate marketing campaign. Employees depend upon Skype to speak with friends abroad or for legitimate business video conferencing. Drop box and Box can be used to distribute documents between corporate and personal devices for mobility and user productivity.

De-parameterization: Given new device proliferation, application mobility and cloud-based consumer and corporate services, the notion of a static network perimeter is all but gone. Now there are a multitude of network perimeters around devices, applications, users, and data. These perimeters have also become quite dynamic as they must adapt to various environmental conditions such as user role, device type, server virtualization mobility, network location and time-of-day.

External business requirements: The enterprise must also provide guests, third-party contractors, and business partners network access using various devices from a multitude of locations.

The central element in all of these changes is the mobile computing device. Mobile devices have become an essential element for organizations as part of the overall network infrastructure. Mobile devices such as smart phones, tablets, and memory sticks provide increased convenience for individuals as well as the potential for increased productivity in the workplace. Because of their widespread use and unique characteristics, security for mobile devices is a pressing and complex issue. In essence, an organization needs to implement a security policy through a combination of security features built into the mobile devices and additional security controls provided by network components that regulate the use of the mobile devices.

4.3.1 Security Threats

Mobile devices need additional, specialized protection measures beyond those implemented for other client devices, such as desktop and laptop devices that are used only within the organization's facilities and on the organization's networks.

Major security concerns for mobile devices:

Lack of Physical Security Controls: Mobile devices are typically under the complete control of the user, and are used and kept in a variety of locations outside the organization's control, including off premises. Even if a device is required to remain on premises, the user may move the device within the organization between secure and no secured locations. Thus, theft and tampering are realistic threats.

The security policy for mobile devices must be based on the assumption that any mobile device may be stolen or at least accessed by a malicious party. The threat is twofold: A malicious party may attempt to recover sensitive data from the device itself, or may use the device to gain access to the organization's resources.

Use of Untrusted Mobile Devices In addition to company-issued and company controlled mobile devices; virtually all employees will have personal smart phones and/or tablets. The organization must assume that these devices are not trust worthy. That is, the devices may not employ encryption and either the user or a third party may have installed a bypass to the built-in restrictions on security, operating system use, and so on.
Use of Un-trusted Networks If a mobile device is used on premises; it can connect to organization resources over the organization's own in-house wireless networks. However, for off-premises use, the user will typically access organizational resources via Wi-Fi or cellular access to the Internet and from the Internet to the organization. Thus, traffic that includes an off-premises segment is potentially susceptible to eavesdropping or man-in-the-middle types of attacks. Thus, the security policy must be based on the assumption that the networks between the mobile device and the organization are not trustworthy.

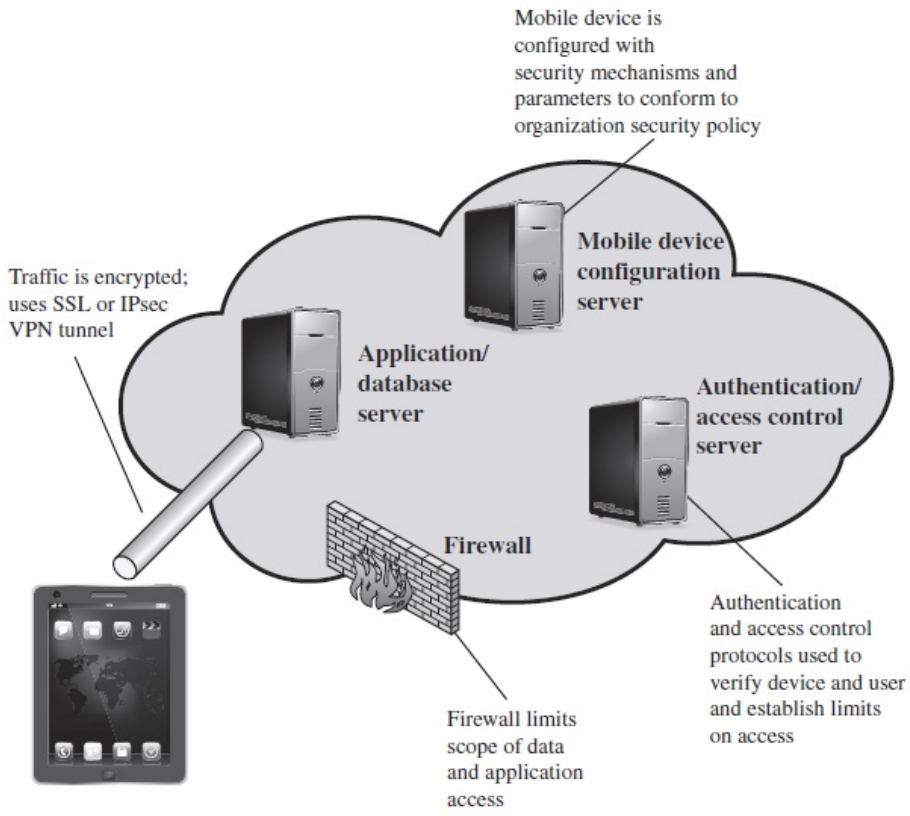
Use of Applications Created by Unknown Parties: By design, it is easy to find and install third-party applications on mobile devices. This poses the obvious risk of installing malicious software. An organization has several options for dealing with this threat, as described subsequently.
Interaction with Other Systems a common feature found on smart phones and tablets is the ability to automatically synchronize data, apps, contacts, photos, and so on with other computing devices and with cloud-based storage. Unless an organization has control of all the devices involved in synchronization, there is considerable risk of the organization's data being stored in an unsecured location, plus the risk of the introduction of malware.

Use of Un-trusted Content: Mobile devices may access and use content that other computing devices do not encounter. An example is the Quick Response (QR) code, which is a two-dimensional barcode. QR codes are designed to be captured by a mobile device camera and used by the mobile device. The QR code translates to a URL, so that a malicious QR code could direct the mobile device to malicious Web sites.

Use of Location Services: the GPS capability on mobile devices can be used to maintain knowledge of the physical location of the device. While this feature might be useful to an organization as part of a presence service, it creates security risks. An attacker can use the location information to determine where the device and user is located, which may be of use to the attacker.

4.4 Mobile Device Security Strategy

With the threats listed in the preceding discussion in mind, we outline the principal elements of a mobile device security strategy. They fall into three categories: device security, client/server traffic security, and barrier security



Mobile Device Security Elements

Device Security: A number of organizations will supply mobile devices for employee use and pre configure those devices to conform to the enterprise security policy. However, many organizations will find it convenient or even necessary to adopt a bring your- own-device (BYOD) policy that allows the personal mobile devices of employees to have access to corporate resources. IT managers should be able to inspect each device before allowing network access. IT will want to establish configuration guidelines for operating systems and applications. For example, "rooted" or "jail-broken" devices are not permitted on the network, and mobile devices

cannot store corporate contacts on local storage. Whether a device is owned by the organization or BYOD, the organization should configure the device with security controls, including the following:

- Enable auto-lock, which causes the device to lock if it has not been used for a given amount of time, requiring the user to re-enter a four-digit PIN or a password to re-activate the device.
- Enable password or PIN protection. The PIN or password is needed to unlock the device. In addition, it can be configured so that e-mail and other data on the device are encrypted using the PIN or password and can only be retrieved with the PIN or password.
- Avoid using auto-complete features that remember user names or passwords.
- Enable remote wipe.
- Ensure that SSL protection is enabled, if available.
- Make sure that software, including operating systems and applications, is up to date.
- Install antivirus software as it becomes available.
- Either sensitive data should be prohibited from storage on the mobile device or it should be encrypted.
- IT staff should also have the ability to remotely access devices, wipe the device of all data, and then disable the device in the event of loss or theft.
- The organization may prohibit all installation of third-party applications,
- Implement white listing to prohibit installation of all unapproved applications, or implement a secure sandbox that isolates the organization's data and applications from all other data and applications on the mobile device. Any application that is on an approved list should be accompanied by a digital signature and a public-key certificate from an approved authority.
- The organization can implement and enforce restrictions on what devices can synchronize and on the use of cloud-based storage.
- To deal with the threat of untrusted content, security responses can include training of personnel on the risks inherent in untrusted content and disabling camera use on corporate mobile devices.
- To counter the threat of malicious use of location services, the security policy can dictate that such service is disabled on all mobile devices.

Traffic Security: Traffic security is based on the usual mechanisms for

encryption and authentication. All traffic should be encrypted and travel by secure means, such as SSL or IPv6. Virtual private networks (VPNs) can be configured so that all traffic between the mobile device and the organization's network is via a VPN.
A strong authentication protocol should be used to limit the access from the device to the resources of the organization. Often, a mobile device has a single device-specific authenticator, because it is assumed that the device has only one
User. A preferable strategy is to have a two-layer authentication mechanism, which involves authenticating the device and then authenticating the user of the device.

Barrier Security: The organization should have security mechanisms to protect the network from unauthorized access. The security strategy can also include firewall policies specific to mobile device traffic. Firewall policies can limit the scope of data and application access for all mobile devices. Similarly, intrusion detection and intrusion prevention systems can be configured to have tighter rules for mobile device traffic.

4.5 Mobile Device Security Process

Mobile devices face a number of threats that pose a significant risk to corporate data. Like desktops, smart phones and tablet PCs are susceptible to digital attacks, but they are also highly vulnerable to physical attacks given their portability. Here is an overview of the various mobile device security threats and the risks they pose to corporate assets.

Eavesdropping – Carrier-based wireless networks have good link-level security but lack end-to-end upper-layer security. Data sent from the client to an enterprise server is often unencrypted, allowing intruders to eavesdrop on users' sensitive communications.

Unauthorized access – Users often store login credentials for applications on their mobile devices, making access to corporate resources only a click or tap away. In this manner unauthorized users can easily access corporate email accounts and applications, social media networks and more.

Theft and loss – Couple mobile devices' small form factor with PC-grade processing power and storage, and you have a high risk for data loss. Users store a significant amount of sensitive corporate data–such as business

email, customer databases, corporate presentations and business plans–on their mobile devices. It only takes one hurried user to leave their iPhone in a taxicab for a significant data loss incident to occur.

Unlicensed and unmanaged applications – Unlicensed applications can cost your company in legal costs. But whether or not applications are licensed, they must be updated regularly to fix vulnerabilities that could be exploited to gain unauthorized access or steal data. Without visibility into end users' mobile devices, there is no guarantee that they are being updated.

4.5.1Theft protection

Along with malware protection, theft protection is one of the most important security features for an Android security product. It allows the user to run commands remotely on a lost or stolen phone. These principally concern protection of the user's private data and the recovery of the device. The commands are sent via web interface or text message.

4.5.2 Lock

The lock function prevents unauthorized access by locking the device. There should be no means of bypassing the lock screen. Some manufacturers use the same PIN for the lock screen as for the text- message commands. This can be a problem, if text messages are displayed on the lock screen (which is the default Android setting). A thief could thus easily see the PIN and so unlock the device. We feel that manufacturers who use such a mechanism should urgently find and offer an alternative.

Another problem noted with some products is the ability to open the Android notification bar. This enables a thief not only to activate aero plane mode, thus rendering commands from the product's web interface useless, but also to switch to the guest account. Even if functions such as making phone calls are disabled in this mode, it is still possible to use the phone for some other functions. Google's own recommendation to allow only trusted people to use the phone in guest mode makes this point clear. In our evaluation, we also considered the opportunity to use a customizable lock screen. This could be employed e.g. to display the user's contact details when the device is locked, which might be used by an honest finder to contact the owner and arrange to return the phone. We also feel it is important that it should always be possible to use the phone to make emergency calls (e.g. fire brigade, police, and ambulance). Just a few products provide the option to take pictures with the front-facing camera

when the phone is locked. This makes it possible to photograph and thus identify a thief. In our tests, we discovered that not all features of all products work in a satisfactory fashion. In some cases, we were able to unlock the device by reading the text message with the PIN on the lock screen. Other products allowed the notification bar to be opened, thus giving access to the guest account. In some apps, it was not possible to make an emergency call. On the other hand, we have to praise all manufacturers for their respective products' behavior when the device is restarted.

4.5.3 Locate

A Locate function allows the position of the phone to be determined when it has been lost or stolen. This could be valuable if the owner has simply forgotten where he/she left the phone. Some manufacturers of mobile security software warn explicitly against trying to track down a thief oneself, and recommend contacting the police instead. Differences between the locate functions of different products are usually quite small. All allow a single location to be determined.
Android version and its text-message app Hangouts. Browser history and bookmarks were not removed by some products. We have stressed the importance of deleting the Google Account details, so that access to mails, calendar, call history and contacts is prevented. It is also important to remove the user's files.

4.5.4 SIM Protection

A SIM Protection feature saves metadata to the user's SIM card. This makes it possible to recognize if a thief has swapped the SIM card, in order to use the phone to make calls. Most products will lock the device as soon as the SIM-card change is registered. The user does not need to send a command; the function works automatically. Some security apps inform a trusted person, whose details were entered during product setup, that the SIM card has been changed. This might help the owner to identify or contact the thief.

4.5.5 Malware protection

This component scans the mobile phone for malicious software, which it deletes or quarantines. For this function to work effectively, it has to be kept up-to-date. When travelling abroad, users need to be careful that automatic updates and cloud scans do not incur high roaming costs from the mobile service provider.

4.5.6 Windows products

The perfect mobile-security product does not yet exist. As with Windows products, we recommend drawing up a short list after reading about the advantages and disadvantages of each product in our review. A free trial version of each candidate product can then be installed and tested for a few days; this should make the decision easier. Especially with Android security products, new versions with improvements and new functions are constantly being released. By participating in this test, the manufacturers have shown their commitment to providing customers with quality security software. As this report shows, we have found some degree of malfunction in many of the tested products. The manufacturers of the affected products have taken these problems very seriously and are already working on solutions. As the core functions of all the products we tested reached a very good level, we are happy to present our "Approved Award" to all participating manufacturers. We have noticed a significant improvement in the overall standard of the products since last year's test.

4.5.7 Battery usage

Testing the battery usage of a device might appear at first glance to be very straightforward. If one goes into more detail, the difficulties become apparent. Particularly with mobile phones, the usage patterns of different users are very varied. Some use the multimedia functions extensively, others view a lot of documents, while some use only the telephone functions. We need to differentiate between power users, who take advantage of all of the possible functions in the device, and traditional users who merely make and receive phone calls.

4.6 Protection Against Android Malware

Methods of attacking mobile devices are getting more and more sophisticated. Fraudulent applications attempt to steal users' data or money. To reduce the risk of this happening, follow the advice given here. Only download apps from Google Play or reputable app makers own stores. Avoid third-party stores and side loading. Another indication of untrustworthy apps is irrelevant access rights. For example, an app that measures the speed at which you are travelling has no need to access your phone book or call log. Of course, even if an app does this, it is not a clear-cut indication that it is malicious, but it makes sense to consider whether it is genuine and should be used. A look at the reviews in the app store is also a guide; avoid apps with bad or dubious reviews. If you Root your smart

phone, you will have more functionality on the phone, but equally the opportunity for malicious apps to take control will also increase. Another point to consider is the warranty. It is not legally clear-cut whether the warranty is still valid if the phone is rooted. In many cases, the warranty will be considered null and void.

Android Security

Android Security is the range of security features built into the Android operating system, and thus preinstalled on every Android device. It includes theft-protection functionality, and the ability to verify apps online.

Locate

This function locates a lost or stolen device and displays its position using Google Maps. This is done automatically when the user logs on to the web interface. Only a single location is provided each time, continuous tracking is not possible.

Installation

Installation is not necessary, as the features are already built into the operating system. On our test device, the functions were activated by default. Users can see the status of the Android security features and enable/disable them by going to Google Settings\Security.

Theft Protection

Android includes theft protection with the most important functions. They are controlled by web interface: This requires a Google Account, which is of course a requirement for many Android features. Text-message commands are not provided.

Ring

This function plays a melody at full volume for 5 minutes. It can be used to locate a mislaid mobile phone at home, for instance. The command does not lock the device. The on/off button on the phone can be used to stop the phone ringing.

Lock

The Lock function uses the Android lock screen to lock the phone. This makes it inaccessible to unauthorized persons. The unlock password for the lock screen can be set in the web interface. We liked the fact that it is possible to define a message in the web interface, which will be displayed on the lock screen. This would allow the owner to provide an honest finder with contact details. Additionally, a phone number can be entered.

Wipe

This function deletes the user's personal data from the smart phone. When the command has been received, the phone is reset to factory settings.

Verify Apps

Android includes several settings to prevent malicious attacks. Prior to installing an application downloaded outside of the Play store, Google's Safe Browsing feature will scan the app and warn of any potential threats.

Android Security allows the user to check installed apps regularly, whereby it will warn of any potentially malicious ones found.

Updates

We could not find any information relating to updates for malware signatures.

Help

No significant help functions are provided.

De-Installation

The Android Device Manager, which includes Android Security, cannot be uninstalled, only disabled.

License

The protection features are already installed with the operating system and can be used free of charge without restriction.

Summary

Android Security provides the user with basic theft-protection and malware-protection functionality. In our test, these features impressed us as stable and well thought-out, and they represent a usable, simple alternative to external security products.

Ahn Lab V3 Mobile Security

Ahn Lab V3 Mobile Security is a comprehensive security product. Even the Free version provides the most important functions. The Premium version includes additional functions such as app lock and URL scan.

URL Scan

The URL scan protects the user while surfing the Internet. It has to be activated before it can be used. In a well-designed dialog box, the user is taken through the configuration. AhnLab has to be made the default program for surfing the Internet (although it is not itself a browser). Any browser of the user's choice can be used.

Privacy Advisor

Privacy Advisor alerts the user to apps that demand specific permissions. The apps are shown in pre-defined categories, such as "Access to Contacts". All apps with this permission will be listed.

Installation

We installed Ahn Lab V3 Mobile Security from the Google Play Store. Once the license agreement has been accepted, the scope of malware scans can be configured. As well as installed apps, the user can also scan all files. Detection of PUAs (potentially unwanted programs) can additionally be enabled at this stage. After this, updates can be set to run only via Wi-Fi, or additionally via a mobile data connection. A scan is then started, and the installation is complete.

Malware Scan

This function allows the device to be checked for malicious software. In addition to real- time protection, on-demand scans can be run. The malware signatures are updated before each scan. Tapping an app in the list will display all its current permissions.

Privacy Cleaner

Privacy Cleaner deletes files that potentially contain personal data. Browser logs and the cache can be removed by the feature.

Application Lock

Application Lock allows installed apps to be protected with a PIN, which has to be entered before an app can be run. This might be useful e.g. if a child is going to use the phone.

Lock Device

Text-message command: #lock <PIN> This function locks the device by sending a text message with the PIN. AhnLab have overlooked an important point here. In the Android version used for the test, text messages are shown on the lock screen by default, meaning that a thief would be able to see the PIN and so unlock the phone. This would not be a major problem if it were possible to use a different PIN or lock pattern for the lock screen.

Hidden Gallery

The Hidden Gallery can be used to hide specific photos and videos on the

device. These are moved into a hidden folder, and can then only be viewed if the PIN is entered.

Call Block

This component can reject calls from unwanted callers. This involves creating a blacklist of unwanted numbers. We liked the fact that it is possible to block numbers according to a pattern (e.g. a particular dialing code).

Track Location

Text-message command: #locates <PIN>. This command determines the smart phone's location. The sender's phone will receive in reply the device's current co-ordinates and a direct link to Google Maps. These two pieces of information are sent as two separate text messages.

Anti-Theft

A wizard is again provided to configure the feature. AhnLab needs to be registered as a device administrator. Next, a trusted phone number has to be entered, which will be used to contact the owner in the event that the SIM card is exchanged. In the final step, a personalized message can be entered, which will be displayed on the lock screen.

4.7 Encryption for mobile devices

Encrypting data at rest and in motion helps prevent data loss and successful eavesdropping attempts on mobile devices. Carrier networks have good encryption of the airlink, but the rest of the value chain between the client and enterprise server remains open unless explicitly managed. Contemporary tablet PCs and smartphones can secure Web and email with SSL/TLS, Wi-Fi with WPA2 and corporate data with mobile VPN clients. The primary challenge facing IT organizations is ensuring proper configuration and enforcement, as well as protecting credentials and configurations to prevent reuse on unauthorized devices.

Data at rest can be protected with self-protecting applications that store email messages, contacts and calendars inside encrypted containers. These containers separate business data from personal data, making it easier to wipe business data should the device become lost or stolen.

4.8 Authentication and authorization for mobile devices

Authentication and authorization controls help protect unauthorized access to mobile devices and the data on them. Ideally, Craig Mathias, principal with advisory firm Farpoint Group, says IT organizations should implement two-factor authentication on mobile devices, which requires users to prove their identity using something they know–like a password–and something they have–like a fingerprint. In addition to providing robust authentication and authorization, Mathias says two-factor authentication can also be used to drive a good encryption implementation. Unfortunately, two-factor authentication technology is not yet widely available in mobile devices. Until then, IT organizations should require users to use native device-level authentication (PIN, password).

4.9 Remote wipe for mobile device security

Authentication and encryption help prevent data loss in the case of mobile device theft or loss, but physical security can be further fortified with remote wipe and "phone home" capabilities. Native remote lock, find and wipe capabilities can be used to either recover a lost mobile device or permanently delete the data on them. Be careful, however, if you choose to use these functionalities. Experts recommend defining policies for these technologies and asking users to sign a consent form. Remote wipe could put the user's personal data at risk and "phone home" or "find me" services can raise privacy concerns.

4.10 Mobile device management

When experts and IT professionals talk about securing mobile devices, the conversation often turns to mobile device management systems, and for good reason. Most mobile device management products include basic security functionality. They also enable centralized visibility, policy configuration, application provisioning and compliance reporting for any mobile device that accesses network resources – regardless of who owns it. These functions are key security controls and their centralized management makes them practical. For example, most mobile device management systems feature Exchange ActiveSync policies, which allow you to deny corporate mail access by unencrypted devices. Others offer more extensive

and transparent control to enable IT organizations to enroll and secure iPads, for example, without relying on iTunes or Exchange.

4.11 Let us Sum up

Today's mobile devices are a mixed bag when it comes to security. On the one hand, these platforms have been designed from the ground up to be more secure—they raise the bar by leveraging techniques such as application isolation, provenance, encryption, and permission-based access control. On the other hand, these devices were designed for consumers, and as such, they have traded off their security to ensure usability to varying degrees. These tradeoffs have contributed to the massive popularity of these platforms, but they also increase the risk of using these devices in the enterprise.

While mobile devices promise to greatly improve productivity, they also introduce a number of new risks that must be managed by enterprises. We hope that by explaining the security models that undergird each platform, and the environment these devices participate in, we have discussed, you will be able to more effectively derive value from these devices and also more effectively manage this risks they introduce.

4.12 Self assessment Questions

1. Discuss about mobile device security.

……
……
……
……
……
……
……

2. What are the Mobile device security threats?

……
……
……
……
……
……
……

3. Explain about the Mobile device policies.

……
……
……
……
……
……
……

4. How to do the Mobile device management

……
……
……
……
……
……
……

5. Discuss about android malware.

……
……
……
……
……
……
……

4.13 Model Questions

1. What are the steps for SIM protection?
2. Write about the malware protection in mobile.
3. Discuss about Security Threats in mobile security.
4. What are the theft protections for mobile phones?

4.14 References &Suggested Readings

1. https://www.av-comparatives.org/wp-content/uploads/2015/09/avc_mob_2015_en.pdf
2. https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile.aspx
3. Babu B., S., & Venkataram, P. Wireless and Mobile Security 1st Edition. Mcgraw Hill Education.

ANSWER TO SELF ASSESSMENT QUESTIONS (UNIT-1)

1. What are different wireless components?

Firewall, Wireless Access Point, Server, Switch/Hub, Modem, USB Network Adapter, Wireless Routers, Station (STA), Access Point (AP) and Smart Phones and other wireless computing devices etc.

2. Discuss different design structures or configurations of WLAN according to IEEE 802.11 standard?

The IEEE 802.11 standard also defines two WLAN design structures or configurations. They are:

(i) Ad Hoc Mode:
(ii) Infrastructure Mode

(i) Ad Hoc Mode: The ad hoc mode does not use APs. Ad hoc mode is sometimes referred to as infra structure less because only peer-to-peer STAs are involved in the communications. This mode of operation is possible when two or more STAs are able to communicate directly to one another.

Examples are laptops, mobile phones, PDAs, printers and scanners being able to communicate with each other without an AP.

Advantages

They can be formed anytime and anywhere, allowing multiple users to create wireless connections cheaply, quickly, and easily with minimal hardware and user maintenance.

Disadvantages

Ad hoc WLAN cannot communicate with external networks.

Ad hoc network can interfere with the operation of an AP-based infrastructure mode network that exists within the same wireless space.

(ii) Infrastructure Mode: In infrastructure mode, an AP logically connects STAs to each other or to a distribution system (DS), which is typically an organization's wired network. The DS is the means by which STAs can communicate with the organization's wired LANs and external networks

such as the Internet. Infrastructure mode is the most commonly used mode for WLANs.

3. What do you mean by Wireless security? What are common types of Wireless security?

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

WEP is a weak security standard. WEP is an old IEEE 802.11 standard from 1999, which was out dated in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP.

4. What are the Security problems associated with WPA?

Security problems with WPA include the following:

(i) **Weak Password:** Pre-shared key WPA and WPA2 remain vulnerable to password cracking attacks if users rely on a weak password or passphrase.
To protect against a brute force attack, a truly random passphrase of 20 characters (selected from the set of 95 permitted characters) is probably sufficient. Brute forcing of simple passwords can be attempted using the Air crack Suite starting from the four-way authentication handshake exchanged during association or periodic re-authentication.

(ii) **WPS PIN recovery:** Most recent models have this feature and enable it by default. Many consumer Wi-Fi device manufacturers had taken steps to eliminate the potential of weak passphrase choices by promoting alternative methods of automatically generating and distributing strong keys when users add a new wireless adapter or appliance to a network. These methods include pushing buttons on the devices or entering an 8-digit PIN. The Wi-Fi Alliance standardized these methods as Wi-Fi Protected Setup; however the PIN feature as widely implemented introduced a major new security flaw. The flaw allows a remote attacker to recover the WPS PIN and, with it, the router's WPA/WPA2 password in a few hours.

5. Discuss the policies on maintaining Wireless Security

- **Secure communications:** Encrypt data that travels on the network, and authenticate users to be sure you know who is using the WLAN. Cisco supports all industry-standard encryption and authentication methods for the broadest client device compatibility.
- **Use strong encryption:** As soon as you install your network, set up the strongest wireless encryption you can. Wired Equivalent Privacy (WEP) encryption is adequate, but WPA and WPA2 give you stronger options.
- **Change the default network name:** When you set up your network equipment, change the default name to make it more difficult for hackers to find. Do not choose your company name, company phone number, or other information about your company that is easy to guess or find on the Internet. Use VLANs or MAC address control lists combined with encryption to restrict user access.
- Implement Cisco secure guest access features to allow visitors to connect to the network or Internet while keeping your business network and resources separate and secure.
- Be sure that management ports are secured.
- Physically hide or secure access points to prevent tampering. In many buildings, Cisco access points can be installed in the plenum space above the ceiling, providing optimal coverage in a secure location.
- Use video surveillance cameras to monitor your office building and site for suspicious activity.

ANSWER TO SELF ASSESSMENT QUESTIONS (UNIT-2)

1. What is malicious association?

Malicious associations" are when wireless devices can be actively made by crackers 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 cracker runs some software that makes his/her wireless network card look like a legitimate access point.

2. What is network auditing?

Network auditing is the collective measures done to analyze, study and gather data about a network with the purpose of ascertaining its health in accordance with the network/organization requirements.
Network auditing primarily provides insight into how effective network control and practices are, i.e. its compliance to internal and external network policies and regulations.

3. Write about wireless network attacks.

Our modern networks are increasingly moving towards wireless technologies. As convenient as they are, wireless connections have one major drawback – security. As compared to their wired counterparts, securing wireless technologies poses a bit of an extra challenges.
My main focus for this article will be security over Wi-Fi access, but I'll address 3G/4G and Bluetooth as well. Read on to learn about the methods that hackers use to steal data and what you can do to keep them out.

4. How to secure wireless client devices?

An essential step in wireless security is locking down the client device used to access the wireless network. If a laptop or other endpoint is compromised, then the device can be used to gain entry into the network, regardless of other wireless security measures that may be in place. By the way, this is true whether a client is used to access the network over wireless or wired. Mobile clients, like laptops, are inherently used in some unfriendly places outside the corporate network, and can become infected with malicious software.

5. Discuss about different types of wireless attack issues.

Type of Attack	Description	Methods and Tools
War Driving	Discovering wireless LANs by listening to beacons or sending probe requests, thereby providing launch point for further attacks.	Airmon-ng, DStumbler, KisMAC, MacStumbler, NetStumbler, Wellenreiter, WiFiFoFum

Rogue Access Points	Installing an unsecured AP inside firewall, creating open backdoor into trusted network.	Any hardware or software AP
Ad Hoc Associations	Connecting directly to an unsecured station to circumvent AP security or to attack station.	Any wireless card or USB adapter
MAC Spoofing	Reconfiguring an attacker's MAC address to pose as an authorized AP or station.	MacChanger, SirMACsAlot, SMAC, Wellenreiter, wicontrol
802.1X RADIUS Cracking	Recovering RADIUS secret by brute force from 802.1X access request, for use by evil twin AP.	Packet capture tool on LAN or network path between AP and RADIUS server

Answer to Self Assessment questions (Unit3)

1. Describe about securing wireless signal transmission.

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

- **Radio Transmission**

Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike. Radio waves can have wavelength from 1 mm – 100,000 km and have frequency ranging from 3 Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency). Radio frequencies are sub-divided into six bands.

- **Microwave Transmission**

Electromagnetic waves above 100 MHz tend to travel in a straight line and signals over them can be sent by beaming those waves towards one particular station. Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line-of-sight.

- **Infrared Transmission**

Infrared wave lies in between visible light spectrum and microwaves. It has wavelength of 700-nm to 1-mm and frequency ranges from 300-GHz to 430-THz.

Infrared wave is used for very short range communication purposes such as television and it's remote. Infrared travels in a straight line hence it is directional by nature. Because of high frequency range, Infrared cannot cross wall-like obstacles.

- **Light Transmission**

Highest most electromagnetic spectrum which can be used for data transmission is light or optical signaling. This is achieved by means of LASER.

Because of frequency light uses, it tends to travel strictly in straight line. Hence the sender and receiver must be in the line-of-sight. Because laser transmission is unidirectional, at both ends of communication the laser and the photo-detector need to be installed. Laser beam is generally 1mm wide hence it is a work of precision to align two far receptors each pointing to lasers source.

2. What is an insertion attack?

Insertion attacks are based on deploying unauthorized devices or creating new wireless networks without going through security process and review.

Unauthorized Clients – An attacker tries to connect a wireless client, typically a laptop or PDA, to an access point without authorization. Access points can be configured to require a password for client access. If there is no password, an intruder can connect to the internal network simply by enabling a wireless client to communicate with the access point.

Unauthorized or Renegade Access Points – An organization may not be aware that internal employees have deployed wireless capabilities on their network in the form of an unauthorized access point, attached to the wired network.. This lack of awareness could lead to the previously described attack, with unauthorized clients gaining access to corporate resources through the rogue access point.

3. Write about the Use of Wi-Fi in network.

Turn Your Smartphone into a Remote Control

If all the computers in your house are connected to a Wi-Fi network, you can easily connect your smart phone to the same network and control them.

Send Documents to Your Printer from Any Computer or Smartphone

There's no reason to have five different printers in your house just so you can print in any room. Instead of constantly plugging and unplugging the printer from your laptop, you can print wirelessly from any computer.

Forward Notifications from Your Smartphone to Your PC

If you're rocking an Android phone (and most of you are), you can send call, SMS, and battery notifications straight to your Windows, Mac with Growl, or Linux PC over Wi-Fi with Android notifier.

Tether Your Smartphone to Your Computer for Internet Anywhere

Okay, so we kind of cheated on this one—it does involve connecting to the internet, but it's definitely not in the traditional way people use Wi-Fi (especially because you often need a hacked or rooted device to do it).

Stream Movies to Any TV in the House

Instead of having a giant collection of DVDs or ripping your movies to every XBMC box you have in your house, you can build yourself an affordable home media server and stream video over Wi-Fi to any other HTPC (or Xbox or Playstation)-enabled TV in the house.

Share Files with Nearby Computers

If you're sharing something other than video between PCs, you have a bunch of options for transferring them. While it isn't the absolute fastest method, sharing files over the same Wi-Fi network (or an ad-hoc network if you're out and about) is certainly one of the easiest ways to get files from one computer to another.

Stream Audio to Any Speakers in the House

While you need extra PCs or game systems lying around to stream video, streaming audio is a cinch with something like Apple's AirPort Express router. Even if you're not streaming from iTunes, Apple's AirPort Express will get any music to any speakers you want in the house.

4. Explain about Jamming signal.

A signal that intentionally introduces interference into a communication channel, either to intentionally prevent error-free reception or as a means of advising stations of some event is called as a jamming signal.

For example, in local area networks (LANs), employing the carrier sense multiple access with collision detection (CSMA/CD) protocol, a station that detects a signal collision sends a jamming signal over a subcarrier frequency to advise all stations of that fact.

5. Write about Authentication of Wireless Network.

a. **The use of static WEP keys:** Many users in a wireless network potentially sharing the identical key for long periods of time, is well-known security vulnerability. This is in part due to the lack of any key management provisions in the WEP protocol. If a computer such as a laptop were to be lost or stolen, the key could become compromised along with all the other computers sharing that key.
b. **Caffe Latte attack:** The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11
c. **WEP:** WEP provides no cryptographic integrity protection. However, the 802.11 MAC protocol uses a no cryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledge packets with the correct checksum.
d. **Authentication is not enabled:** only simple SSID identification occurs. Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easily intercepted.
e. **Device authentication is simple shared-key challenge-response.** One-way challenge-response authentication is subject to ―man-in the-middle attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

Answer to Self Assessment questions (Unit-4)

1. Discuss about mobile device security.

Mobile devices allow employees to access information resources wherever they are, whenever they need. The small form factor, constant internet access, and powerful mobile applications are already improving workforce productivity. Yet mobile devices may be lost or stolen. A compromised mobile device may allow remote access to sensitive on premise organizational data, or any other data that the user has entrusted to the device.

2. What are the Mobile device security threats?

Mobile devices face a number of threats that pose a significant risk to corporate data. Like desktops, smart phones and tablet PCs are susceptible to digital attacks, but they are also highly vulnerable to physical attacks given their portability. Here is an overview of the various mobile device security threats and the risks they pose to corporate assets.

Mobile malware – Smartphone's and tablets are susceptible to worms, viruses, Trojans and spyware similarly to desktops. Mobile malware can steal sensitive data, rack up long distance phone charges and collect user data. High-profile mobile malware infections are few, but that is likely to change. In addition, attackers can use mobile malware to carry out targeted attacks against mobile device users.

Eavesdropping – Carrier-based wireless networks have good link-level security but lack end-to-end upper-layer security. Data sent from the client to an enterprise server is often unencrypted, allowing intruders to eavesdrop on users' sensitive communications.

Unauthorized access – Users often store login credentials for applications on their mobile devices, making access to corporate resources only a click or tap away. In this manner unauthorized users can easily access corporate email accounts and applications, social media networks and more.

Theft and loss – Couple mobile devices' small form factor with PC-grade processing power and storage, and you have a high risk for data loss. Users store a significant amount of sensitive corporate data–such as business email, customer databases, corporate presentations and business plans–on their mobile devices. It only takes one hurried user to leave their iPhone in a taxicab for a significant data loss incident to occur.

3. Explain about the Mobile device policies.

A mobile device policy is a written document that outlines the organization's strategy for allowing tablet PCs and smart phones to connect to the corporate network. A mobile device policy covers who gets a mobile device, who pays for it, what constitutes acceptable use, user responsibilities, penalties for non-compliance, and the range of devices and operating systems the IT organization supports. In order to make these decisions, it is important that management understands what data is sensitive, whether data is regulated and the impact mobile devices will have on that data.

4. How to do the Mobile device management

When experts and IT professionals talk about securing mobile devices, the conversation often turns to mobile device management systems, and for good reason. Most mobile device management products include basic security functionality. They also enable centralized visibility, policy configuration, application provisioning and compliance reporting for any mobile device that accesses network resources – regardless of who owns it. These functions are key security controls and their centralized management makes them practical. For example, most mobile device management systems feature Exchange ActiveSync policies, which allow you to deny corporate mail access by unencrypted devices. Others offer more extensive and transparent control to enable IT organizations to enroll and secure iPads, for example, without relying on iTunes or Exchange.

5. Discuss about android malware.

Mobile malware is malicious software that targets mobile phones or wireless-enabled Personal digital assistants (PDA), by causing the collapse of the system and loss or leakage of confidential information. As wireless phones and PDA networks have become more and more common and have grown in complexity, it has become increasingly difficult to ensure their safety and security against electronic attacks in the form of viruses or other malware.