UNIT-II

INTRODUCTION TO WIRELESS SECURITY PROTOCOLS AND CRYPTOGRAPHY

→ **Removing the FUD**

→ The Abbreviation of FUD is fear, Uncertainity and doubt in wireless security solutions.

→ The threats that like eavesdropping, Jamming, routing attacks, IP Address spoofing etc are not unique to wireless.

→ The security professionals and academics have devoted large amounts of time and resources, tackling these problems.

→ We reinvent to do clearly identify the ways to mitigate threats and this can be done by applying technology and applications that are already used for applications in Internet.

→ The OSI (open System Interconnection) model can identify at what layer common security technologies can be used to secure a wireless network.

OSI Model

→ This standard developed in the mid 1970's that defines a frame work for developing networking protocols that are seven layers.

→ Not all protocols are based on the OSI model and in many cases a single application will perform the functions of many layers of the OSI-Model.

Application Layer: It is the Interface to network Communication programs such as browsers, e-mail, and file transfer s/w are on this layer.

Presentation layer: This layer negotiates Syntax, so the applicat Communicating will be able to Understand each other.

Session Layer: This layer is responsible for Coordinating communications between applications as well as tracking what data belongs to what data Connection.

Transport Layer: This layer primarly provides the Organization for network communications. Reliability and ordering are primare functions.
→ Portions of data are Commonly called Segments.

Network Layer: The routing and logical addressing are handled. The portions of data are commonly called packets

Data Link Layer: The physical addressing such as. Media Access Control (MAC) address are part of this. The portions of data are commonly called. frames.

Physical Layer: It is responsible for the actual communication, changing the zeros and ones into voltages for wires or radio signals for the air.

OSI Simplifier

→ In many large enterprises, different groups handle different networking functions.
→ For example. a large financial institution from the perspective the Customer service application.
→ The Telecom group handles network Cabling.
→ The desk top / Server group is responsible for the NIC cards. in the end users pc's and sever's as well as hubs and switches.
→ The NOG (Network Operations group) is responsible. for the routers in the group, connections, assigning IP addressing, operations of DNS of the network.
→ The ADG (Application Development Group) handles the Customer account program that runs over the network.
→ The Customer Service representatives use the application and are responsible for inputting Customer data.
→ It maps to the OSI model rather well use.
→ The Organizations seem overly complicated trouble shooting of applications easier.
→ pulling wires through the drop ceiling and debugging code. are two very different applications.

Application	Customer Service
presentation	Application development
Session	Application development
Transport	Network operations
Network	Network operations
Data Link	Desktop / Server
physical	Telco

Internet Model

→ For many developers, the OSI model is too complex for practical use with regard to implementation.
→ This Internet model sometimes called as TCP/IP model, simplification of OSI model.
→ It is used more accurately reflects how Internet applications are built.

Wireless Local Area Network (LAN) Security Protocols

→ Wireless Ethernet was designed to be a drop-in replacement for wired Ethernet.
→ The entire protocol exists on the physical and data link layers of OSI model.
→ As a result, any specific security protocol could be directly implemented in the physical or data link layers.
→ Many manufacturers and standards bodies are working feverishly to improve 802.11 security mechanisms.
→ The different layers between OSI and Internet model are

OSI model	Internet model
Application Layer, Presentation Layer, Session Layer	→ Application Layer
Transport Layer	→ Transport Layer
Network Layer	→ Internet Layer
Data Link Layer, physical Layer	→ Network Interface Layer

Cryptography

→ Cryptography is commonly defined as the process or skill of communicating or deciphering secret writings or ciphers.

→ One famous historical example of cryptography is the Caesar Cipher, which was used by Julius Caesar.

→ It was based on substitution of each letter in the encoded message with another letter in the alphabets.

→ In fact, much of the cryptography that is used today is based on research that was first done to keep govt. information safe during times of war.

→ Due to the value of the treasure, you decide to spend a significant amount of money protecting it.

→ Therefore, the storage of keys and the methods used to lock the valuables are equally as important as the protection scheme.

→ The cryptography is to help to solve some security problems, but the overall security will be impacted by choosing the correct process for encrypting ad & algorithms and by choosing the best protection for our keys.

→ We deal some of the most common cryptographic methods that can be easily used with wireless technology to solve security problems.

There are Three primary areas where cryptography used.

(a) Authentication: This is used to reliability determine some one or something Identity.
→ This is to prevent some one from impersonating a legitimate user.

(b) Encryption: → This supposed to keep data safe from an intended listeners.
→ There are two types (a) Symmetric (b) Asymmetric

(c) Integrity: This guarantees that data has not been modified. We need to make sure that the message that was received is the message that was sent.

Secure Sockets Layer / Transport Layer Security (SSL/TLS)

→ SSL was originally designed to solve the security problems with web browsers.
→ At that time the Internet boom was a great Commercial opportunity, but the security concerns of sending personal and credit card Info.
→ Netscape was the first browser to offer SSL and the web safe for Commercial transactions.
→ It is transparent, which means that the data arrives at the destination Uncharged by encryption / Decryption process. It will be used for many applications.
→ In 1994 SSL/TLS is implemented for Transport layer Security for security protocols on the Internet was developed.
→ This is the basis for other security protocols including Microsoft Private Communication Technology (PCT), Secure Transport Layer Protocol (STLP) and WTLS (Wireless Transport layer Security) were developed.
→ The SSL was Originally a Netscape defacto standard, but was adopted by IETF (Internet Engineering Task Force) as TLS.
→ The primary application for web traffic on the is HTTP.
→ Then The TCP Connection is made, a request is sent for a document, and sent it.
→ With an SSL/TLS HTTP Connection was established. then HTTP Connection proceeds over this Connection and and does not change the HTTP Communication.
→ SSL/TLS is used to authenticate and encrypt a Connection
→ The Authentication is accomplished by Using public key Cryptography and referred to as handshake.
→ The most Common implementations are based on known TCP Communication such as e-mail, news, telnet and FTP

Secure Shell (SSH)

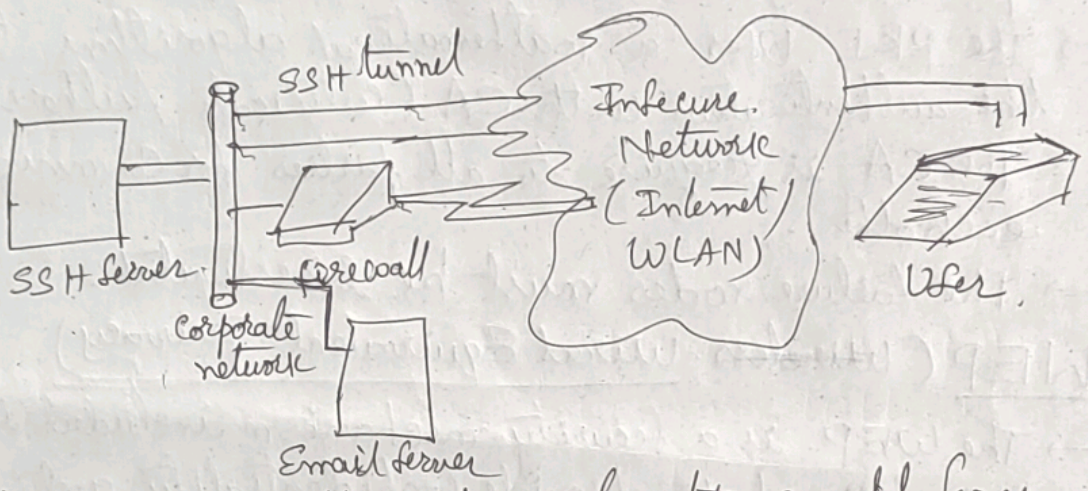
→ Like SSL/TLS the SSH was created out of necessity for secure communication when only protocols being used were unsecured protocols.
→ SSH was developed in 1995 by Tatu Ylonen after his University network fell victim to a password sniffing attack earlier that year.
→ It was originally developed to replace some UNIX programs such as telnet, FTP, remote login (rlogin), rshell (remote shell) and remote copy (rcp).
→ Due to the flexibility and ease of use, SSH is a highly used security protocol and comes with the standard installation with many OS.
→ It also uses a ~~public~~ public-key exchange to secure the intial connection and negotiates symmetric key for data transfer.
→ It also configured to authenticate both server and client.
→ The SSH protocol is the UNIX SSh program.
→ Some of these programs are Open Source and some are distributed for free.

Terminal Access and File Transfer

→ The common use of SSH is for replacing telnet.
→ The telnet application to manage network hosts.
→ The telnet sessions can be easily sniffed, hijacked and data can be injected and to be executed.
→ Telnet is replace it with SSH immediately.
→ Most FTP, the Trivial FTP and Common Internet File System (CIFS) are very insecure.
→ SSH includes the capability to transfer files over an encrypted authenticated System.

Port Forwarding

→ Some manufacturers are not supporting SSH as a telnet or FTP replacement.
→ The SSH can be used to secure otherwise insecure applications such as. telnet, FTP, the POP (post office Protocol) & HTTP.
→ This can be accomplished by using the port forwarding feature of SSH.
→ The firewall is configured to only allow traffic from the insecure network to the SSH server.



→ No traffic will be allowed to or from the email server to the insecure network.
→ In addition to using SSH for terminal access to the SSH server, port forwarding can be used to tunnel email traffic over the insecure network to the SSH server.
→ Then SSH server forwards the packets to the email server.
→ The SSH server and packets would be returned to the SSH server to Tunneling back to the user.
→ Due to the flexibility and ubiquitous access that SSH enables, great care must be taken when implement SSH.
→ This may be used by legitimate users or by malicious attackers.
→ The SSH servers and clients are adequately secured.

Man-in-the Middle (MITM) of SSL/TLS and SSH

→ The SSL/TLS and SSH may also be vulnerable to MITM attacks.
→ It uses public key algorithm for establishing Symmetric keys for data transfer.
→ The malicious attacker could intercept the handshake and replace the public keys exchanged with Counterfeit keys. It is able to attack on SSL/SSH based
→ To prevent this type of attack PKI (public key Infrastructure) is used.
→ The PKI uses a mathematical algorithms to verify the authentication with CA (Certificate Authority) given
→ The CA is require to all parties for Communicate to each other.
→ The failure modes must be investigated.

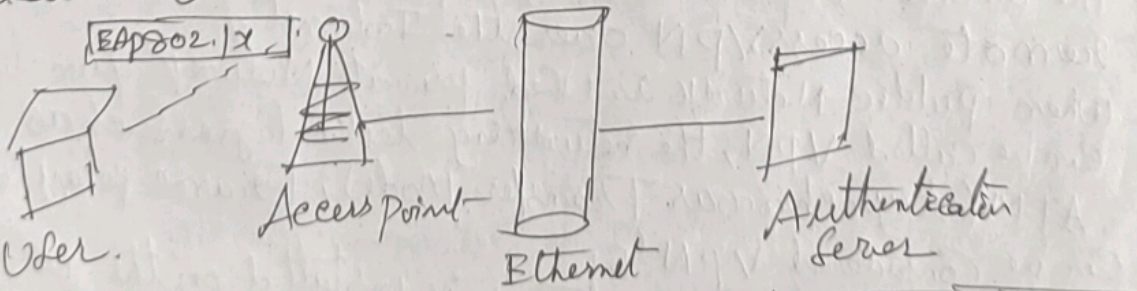
WEP (Wired Equivalent Privacy)

→ The WEP is a security mechanism included in 802.11 to is designed to provide Confidentiality and authentication services.
→ It is based on RC4 algorithm, which is referred to as a stream Cipher.
→ The Packets are encrypted by generating RC4 Stream with the Combination of 24-bit IV (Initialization Vector) and a shared key different for different transactions.
→ The data is then XORed with generated stream and transmitted in a WEP frame with IV in the header.
→ The receiver can also generate the same RC4 Stream to XORed for decryption.
→ But It faces some problems about security.
→ A typical wireless network the WEP key can be Compromised using S/W on the Internet for a few hours.
→ Also it is very difficult to protect the key. WEP keys would need to be changed very frequently.

→ It is often bundled in 802.1x functional Upgrades, negotiate a WEP key at the time of intial authentication.
→ Advanced implementations also rekey during the Session without awarness of the end Users.

802.1x

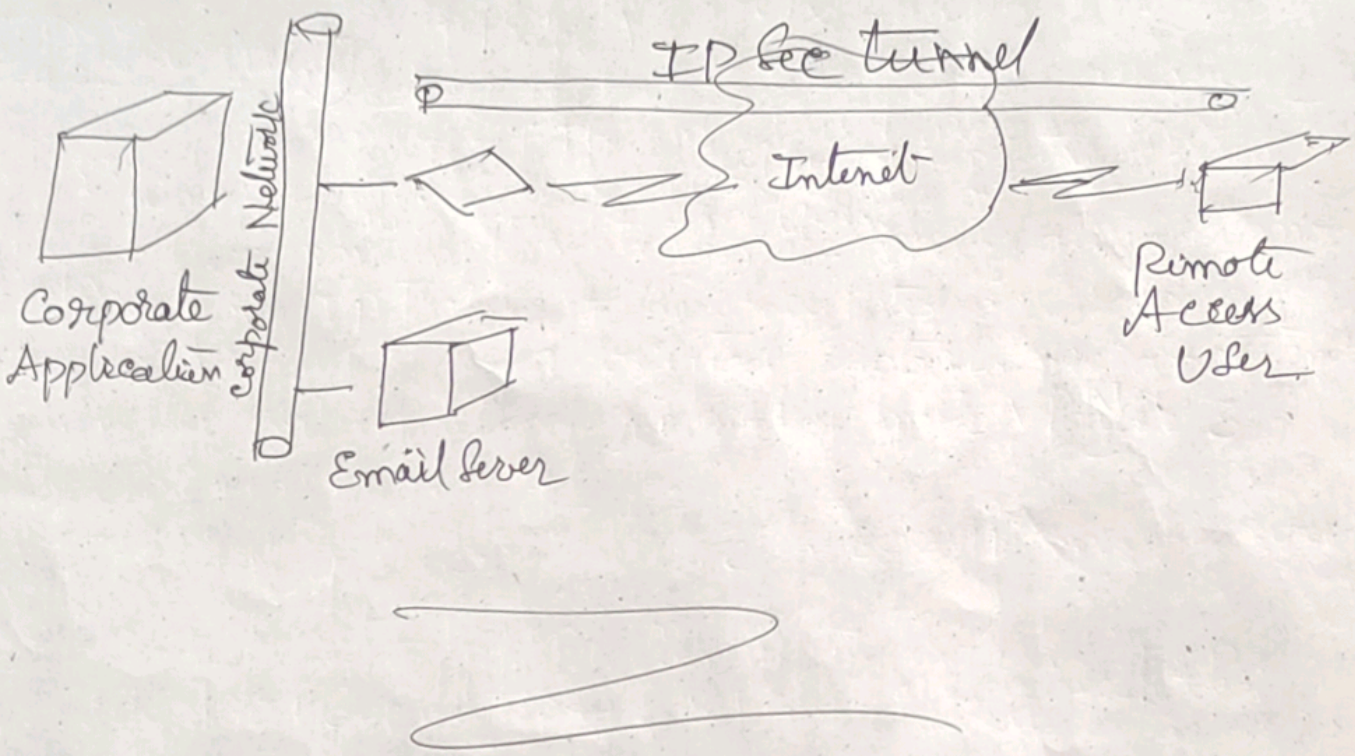
→ The 802.1x and its associated protocols are an attempt to increase the Security of networks befor layer 3 protocols (IP layer) are Setup.
→ This technology is not specifice to 802.11 and can be Used on Ethernet, Token ring and so on.
→ The 802.1x is a layer 2 protocol that can be Used for a no. of. Operations.
→ The basic purpose of 802.1x is to authenticate Users Can optionally be Used to establish encryption keys.
→ when Connection is established only 802.1x traffic is allowed to pass.
→ The protocols Suchas DHCP (Dynamic Host Configuration Protocol), IP are not permitted.
→ The EAP (Extensible Authentication Protocol) Used for authentication. It was Originally designed to solve Some of. authentication issues in PPP (point-to-Point)
→ The EAP packets are Sent to the access point with Users login Information.
→ The access point Can authenticate the User by means of Vendor choose to Support.
→ It will be identified also by Remote Authentication Dial in User Service (RADIUS).



Authentication protocols of RADIUS

IP Security (IPSec)

→ It was developed by IETF and it is lower in the protocols stack than SSL/WTLS, SSH & WTLS.
→ The most common Implementations are using a tunnel mode that enables IP traffic to be encrypted and optionally authenticated.
→ It is the enabling technology behind most VPN used on the Internet today.
→ Because of its flexibility to application support for securing their wireless applications are used.
→ It can be used to provide encryption by using ESP (Encapsulated Security payload) and Authentication by AH (Authentication Header).
→ AH is used without ESP to provide Confidentiality against sniffing, to prevent tampering of data, damaging in Transp
→ The ESP used without AH to provide Confidentiality and basic authentication services of data, but many administrator choose to implement both.
→ It has different Cryptographic algorithms can be used in both ~~such as~~ AH & ESP such as DES, Triple DES and AES..
→ This IP Sec Standards that implemented at all.
→ The most commonly authenticated algorithms such as MD5 and SHA.
→ There are two modes are used. Transport mode and tunnelmod
→ Transport mode only encrypts the data of IP packet without header information, whereas in tunnel mode both header and IP packet are Encrypted. It is a best mode for many enterprizes utilize private Networks.
→ The another implementation of IP Sec is Communication for remote access VPN over the Internet.
→ When public Network is used private Network functions, it can be called VPN, the networking technologies such as ATM (Asynchronous Transfer Mode), Frame Relay and X.25 can be considered VPN's.
→ In this applications, a gateway is installed on the perimeter of the Corporate Network.


IPsec tunnel
Internet
Corporate Application
Corporate Network
Email Server
Remote Access User