UNIT-II

Introduction to Wireless Security Protocols and Cryptography

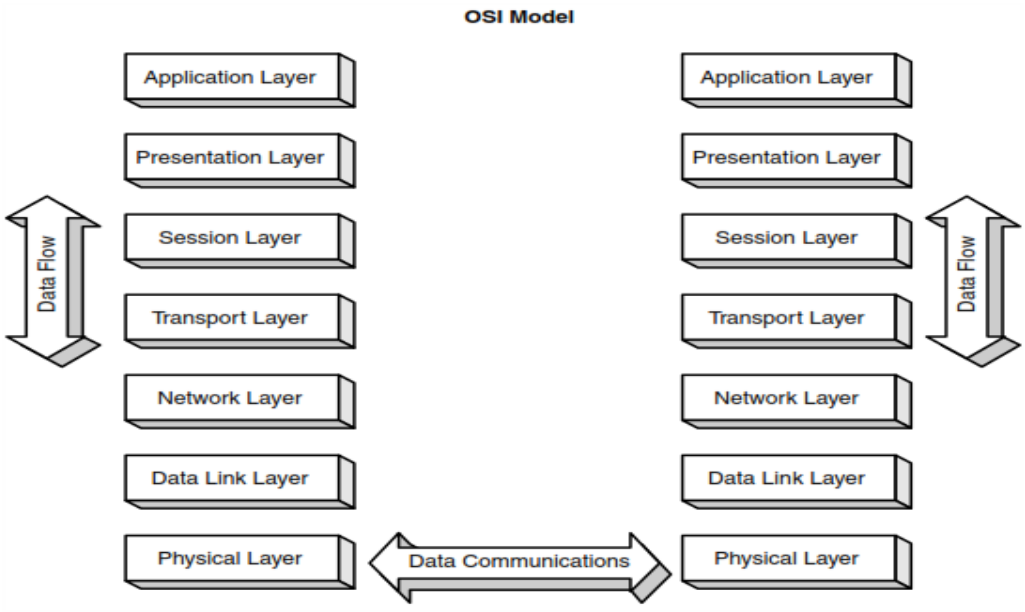
Removing the FUD

- FUD means Fear, Uncertainty and Doubt.
- With the commercial Internet reaching a decade of age, information security professionals and academics have devoted large amounts of time and resources tackling these problems.
- All we need to do is clearly identify the ways to mitigate threats, and this can be done by applying technology and applications that are already in use for other applications on the Internet and in the office.

OSI Model

- OSI stands for Open System Interconnection.
- OSI model is a set of protocols and rules by which communication between two network devices is made possible.
- The network device can be either of mobile device, tablet, laptop, PC, workstation or any other network device.
- OSI model was developed by ISO (International Standard organization).

Layers of OSI model



Application Layer

- The software applications send and receive data over the network.
- The application layer is the user's interface to network communications.
- Examples of application software are Chrome, Firefox, WhatsApp, Office365, Microsoft Edge etc.
- The application layer work on different protocols e.g., File transfer protocol (FTP), Hypertext transfer protocol (HTTP), Simple mail transfer protocol (SMTP), Post office protocol (POL), and Domain name system (DNS)

Presentation layer

- The data move from the application layer to the presentation layer.
- This layer negotiates syntax, so the applications communicating will be able to understand each other.
- The presentation layer encrypts the data so that the size of the data becomes small.
- The data is compressed and encoded in the presentation layer. On the receiver end, the presentation layer then decrypts, uncompressed and decode the data.

Session layer

- In the session layer, the sessions are created. All the data goes through checkpoints.
- This layer is responsible for coordinating communications between applications as well as tracking what data belongs to what data connection.
- Suppose the data link is disconnected then after reconnection the data is again sent through the session so that the previous session is restored and only remaining data is transferred.

Transport layer

- In the transport layer, the data received from the session layer are segmented and then transferred to the network layer.
- Portions of data in this layer are commonly called segments.
- The transport layer must match the connection speed of the sender and receiver.
- Suppose the computer receiving the data has slow connection speed so the transport layer also slows down the data transfer speed of sender.

Network layer

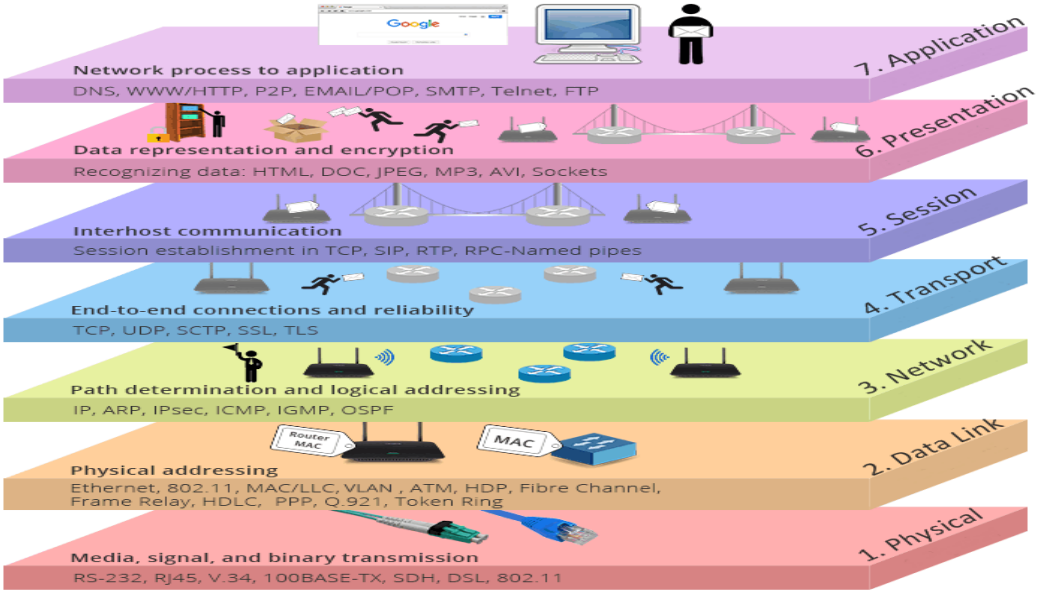
- In the network layer, the segments received from the transport layer are further divided into packets and then transferred to the data link layer.
- On this layer, routing and logical addressing are handled. Portions of data in this layer are commonly called packets.
- The shortest network path is also calculated in the network layer.
- The network layer also identifies the IP addresses of the receiver and sender to transfer data.

Data link layer

- The data link layer further divides the packets received from the network layer into frames.
- This layer also stores the MAC addresses of the sender and receiver.
- The mac addresses are used to identify the sender and receiver devices.
- The error checking of data and synchronization of data frames is also done in this layer.

Physical layer

- The physical layer is responsible for transferring data through physical devices such as wireless devices, cables and network connectors.
- The data frames received from the data link layer are further divided into 0 and 1 form i.e. in bits form then transferred to the physical layer of the receiver.
- The receiver device gets data through the physical layer and goes from the data link layer and all the layers up to the application layer.



OSI Simplified

- In many large enterprises, different groups handle different networking functions.
- For example, let us examine the organization of a large financial institution from the perspective of the customer service application.
- There is a telco group that handles network cabling.
- The desktop/server group is responsible for the network interface cards (NICs) in the end users' PCs and servers, as well as the hubs and switches.
- The network operations group is responsible for the routers in the network, assigning IP addressing, and operating the Domain Name System (DNS) on the network.
- The 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.
- This particular organization maps to the OSI model rather well.

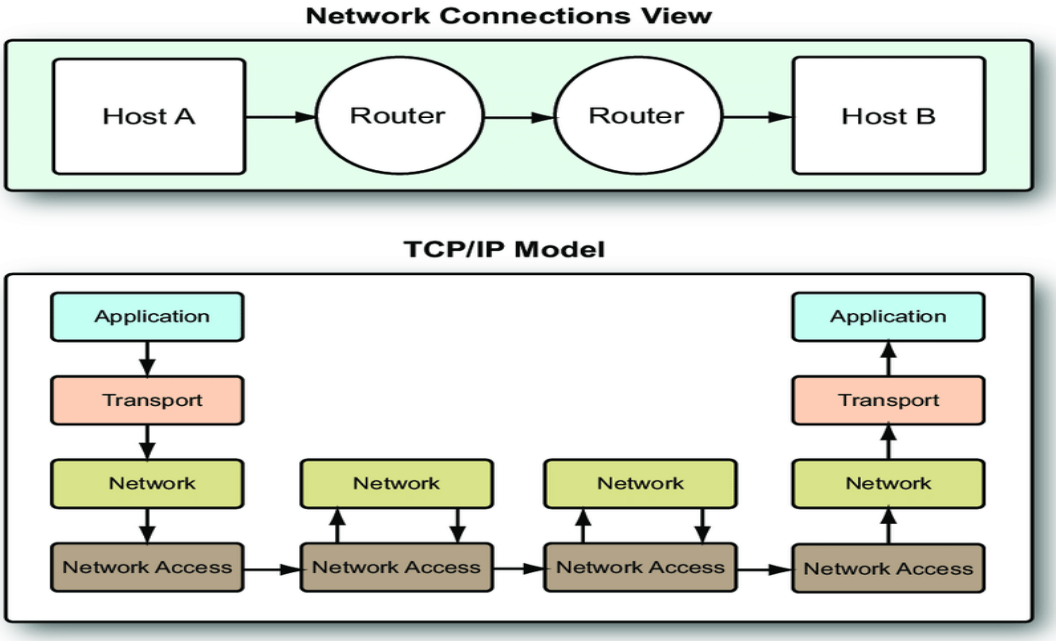
Mapping to the OSI Model

Application	Customer Service
Presentation	Application development
Session	Application development
Transport	Network operations
Network	Network operations
Data link	Desktop/server
Physical	Telco

- This organization may seem overly complicated and you may think that troubleshooting the application can be difficult, but this organization actually makes troubleshooting easier.
- Pulling wires through a drop ceiling and debugging code are two very different disciplines.
- The separation of duties enables each group to become domain experts in their area of responsibility.
- Therefore, when groups are well coordinated, the specialized experienced groups solve problems faster.

Internet Model

- Internet model is also referred to as the Transmission Control Protocol/Internet Protocol (TCP/IP) model.
- The TCP/IP model is a conceptual framework for how data is transmitted over computer networks.
- Internet Model or TCP/IP Model consists of four layers:
    - Application layer
    - Transport layer
    - Internet layer
    - Network Access layer
- Each layer plays a specific role in the transmission process.



Application Layer

- The application layer is a combination of the application, presentation, and session layers.
- This layer is responsible for interaction between the user and the application.
- Here, data is formatted, converted, encrypted, decrypted, and set to the user.
- Protocols used by the application layer are: HTTP, SMTP, FTP, DNS, TELNET.

- HTTP->Hypertext transfer protocol allows the users to interact with the World Wide Web through browser applications.
- SMTP->Simple mail transfer protocol is used to send mails.
- FTP->File transfer protocol is used for transmitting files from one system to another.
- DNS->Domain name system is the phonebook of the internet.
- TELNET->Teletype network acts as a client-server protocol. It is used to provide bidirectional connection.

Transport Layer

- The transport layer is responsible for end-to-end communication and provides error-free delivery of data.
- This layer can transport the data through a connection-oriented or connectionless layer.
- The two protocols used in the transport layer are user datagram protocol (UDP) and TCP.

UDP

- This protocol provides connectionless service and end-to-end delivery of transmission.
- It is considered an unstable protocol because it discovers the errors but does not specify them.

TCP

- It provides all transport services to the application layer.
- TCP is a dependable protocol for error detection and retransmission.
- It assures that all segments must be received and recognized before completing the transmission and discarding the virtual circuit.

Network Layer

- The network layer provides host addressing and chooses the best path to the destination network.
- This layer maintains the quality of service and offers connectionless end-to-end networking.
- The protocols in the network layer are: IPV4, ICMPV4, IGMP
- IPV4-> Internet protocol version 4 is employed for packetizing, forwarding, and delivery of packets. IP is an unreliable datagram protocol.
- ICMPV4->Interrupt control message protocol controls all errors. These mistakes are handled by ICMP protocol during the delivery of the message to target problems.
- IGMP->Internet group management protocol helps in multicasting

Network Access layer

- This layer is responsible for transmitting data over physical networks.
- It includes protocols like Ethernet, Wi-Fi, and Bluetooth, which define how data is transmitted over physical media.
- This layer interacts directly with the physical network hardware, such as network interface cards (NICs) and switches.

Equivalent Layers in the OSI and Internet Models

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

Wireless LAN Security Protocols

- Wireless Local Area Network (LAN) security protocols are essential to ensure the confidentiality, integrity, and availability of data transmitted over wireless networks.
- These protocols help protect against unauthorized access, data interception, and other security threats.
- Here are some commonly used wireless LAN security protocols: WEP, WPA, WPA2, WPA3.

WEP (Wired Equivalent Privacy)

- WEP was one of the earliest wireless LAN security protocols but is now considered highly insecure.
- It uses a static encryption key for data protection.
- However, due to vulnerabilities in its encryption algorithm and weak key management, WEP can be easily cracked, allowing attackers to gain unauthorized access.

WPA (Wi-Fi Protected Access)

- WPA was introduced as a replacement for WEP to address its security flaws.
- WPA employs stronger encryption mechanisms and key management than WEP.
- There are two versions of WPA: WPA-Personal (WPA-PSK) and WPA-Enterprise.
- WPA-PSK uses a pre-shared key (password) for authentication, while WPA-Enterprise employs a centralized authentication server, such as RADIUS.

WPA2 (Wi-Fi Protected Access II)

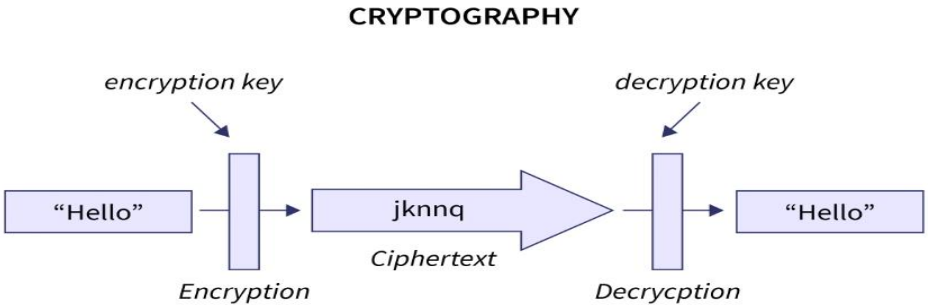
- WPA2 is an improved version of WPA and is widely used for securing wireless networks.
- It provides stronger encryption and security mechanisms, using the Advanced Encryption Standard (AES) for data encryption.
- WPA2-PSK and WPA2-Enterprise are the two main variants, similar to their WPA counterparts.

WPA3 (Wi-Fi Protected Access III)

- WPA3 is the latest iteration of Wi-Fi security, introduced to address vulnerabilities found in WPA2.
- It offers enhanced security features, including protection against brute-force attacks on weak passwords.
- WPA3 also improves security for open networks and introduces a more secure way of connecting Internet of Things (IoT) devices.
- When choosing a wireless LAN security protocol, it's crucial to select the most up-to-date and secure option available.
- WPA3 and WPA2-Enterprise are currently recommended due to their improved security mechanisms.
- Additionally, strong password practices and regular updates to network equipment are important for maintaining the security of your wireless LAN.

Cryptography

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.



Modern cryptography concerns itself with the following four objectives

- Authentication
- Confidentiality
- Non-repudiation
- Integrity

Authentication

The sender and receiver can confirm each other's identity and the origin/destination of the information.

Confidentiality

The information cannot be understood by anyone for whom it was unintended.

Non-repudiation

The creator/sender of the information cannot deny at a later stage their intentions in the creation or transmission of the information.

Integrity

The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

Types of Cryptography

There are three types of cryptography

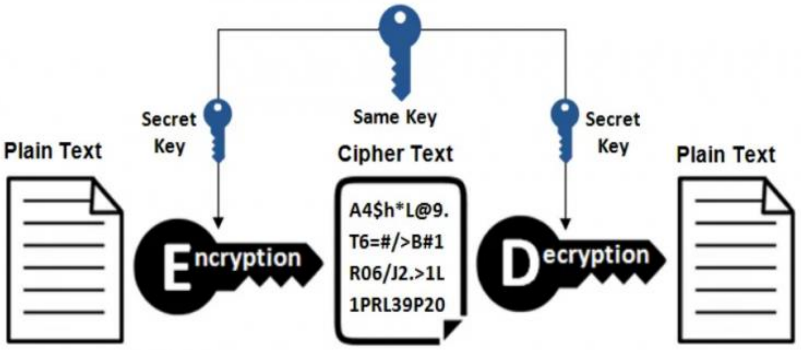
- Symmetric key cryptography
- Asymmetric key cryptography
- Hash Function

Symmetric key cryptography

- It is also known as secret-key cryptography, and in this type of cryptography, you can use only a single key.
- The sender and the receiver can use that single key to encrypt and decrypt a message.
- Advanced Encryption Standard (AES), Data Encryption Standard (DES) and DES3 are the examples of symmetric key cryptography

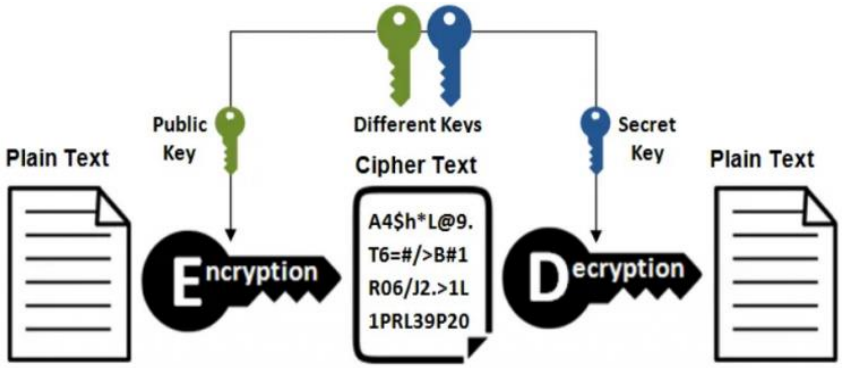
Disadvantage

The two parties must exchange the key in a secure manner.



Asymmetric Key Cryptography

- It is also known as public-key cryptography, and it employs the use of two keys.
- This cryptography differs from and is more secure than symmetric key cryptography.
- In this system, each user encrypts and decrypts using two keys or a pair of keys (private key and public key).
- Each user keeps the private key secret and the public key is distributed across the network so that anyone can use those public keys to send a message to any other user.
- You can use any of those keys to encrypt the message and can use the remaining key for decryption.
- An RSA algorithm, Digital Signature Algorithm (DSA) and Diffie-Hellman key exchange are the examples of asymmetric key cryptography.



Hash Function

- This algorithm makes no use of any keys.
- A hash value with a fixed length is calculated based on the plain text, making it impossible to recover the plain text's contents.
- Many operating systems encrypt passwords using hash functions.

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

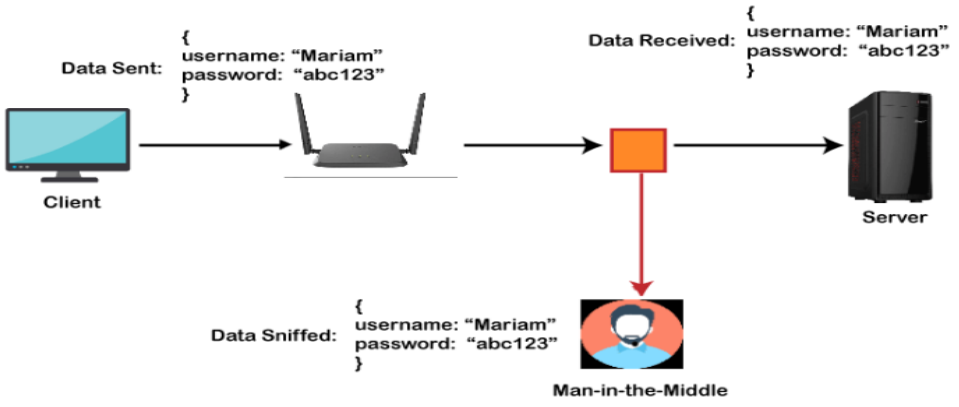
- Secure Sockets Layer (SSL) was originally designed to solve the security problems with web browsers.
- Netscape was the first browser to offer SSL and made the Web safe for commercial transactions and a secure channel could be provided for transmission of data.
- SSL is transparent, which means that the data arrives at the destination unchanged by the encryption/decryption process. Therefore, SSL can be used for many applications.
- SSL and its successor, Transport Layer Security (TLS), are the most widely implemented security protocols on the Internet.
- Originally implemented by Netscape in 1994, SSL/TLS is implemented in nearly every browser and most e-mail clients.
- SSL/TLS has been the basis for other security protocols including Microsoft's Private Communications Technology (PCT), Secure Transport Layer Protocol (STLP), and Wireless Transport Layer Security (WTLS).
- SSL/TLS's primary application is for web traffic or the Hypertext
- Transfer Protocol (HTTP). The process is very basic.
- In normal HTTP communications, a TCP connection is made, a request is sent for a document, and the document is sent.
- With an SSL/TLS HTTP connection, the TCP connection is established, an SSL/TLS connection is established, and then the HTTP connection proceeds over the SSL/TLS connection.
- Two things to note —SSL/TLS relies on TCP for the connection and the addition of the SSL/TLS connection does not change the HTTP communication.
- To prevent confusing standard HTTP servers, HTTP over SSL/TLS is typically implemented over a different TCP port (443) than standard HTTP (80).
- Many of the applications that use SSL/TLS use different ports than the non-SSL/TLS standard protocol.
- SSL/TLS is used to authenticate and encrypt a connection. This is accomplished by using a combination of different technologies that are based on **symmetric and asymmetric algorithms.**
- SSL/TLS has the capability to authenticate the server and client, but in most cases, only server authentication is actually performed.
- The authentication is accomplished by using public-key cryptography and is referred to as a handshake.
- The actual communications using SSL/TLS use a symmetrical encryption algorithm.
- SSL/TLS can be used to secure many varieties of network communications.
- The most common implementations are based on known TCP communication, such as e-mail, news, telnet, and the File Transfer Protocol (FTP). In many cases, different TCP ports are used for the SSL/TLS secured communications.

Secure Shell

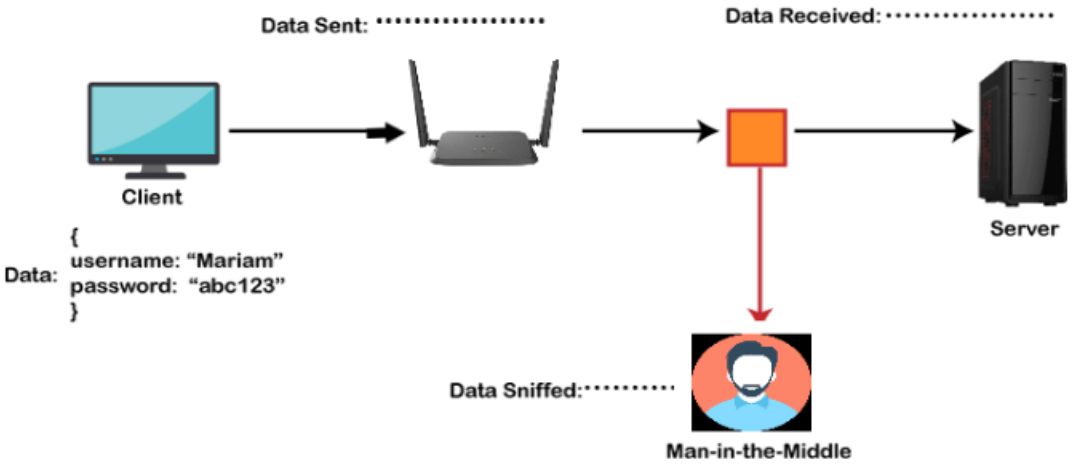
- SSH stands for Secure Shell or Secure Socket Shell.
- SSH was created out of a necessity for secure communication when the only protocols being used were unsecured protocols.
- SSH was originally designed to replace some Unix programs such as telnet, FTP, remote login (rlogin), rshell remote shell (rshell), and remote copy (rcp).
- Besides replacing these programs, SSH can be used to secure otherwise insecure programs over a network.
- Due to its flexibility and ease of use, SSH is a highly used security protocol and comes with the standard installation of many operating systems.
- SSH uses a public-key exchange to secure the initial connection and negotiates a symmetric key for the data transfer during the session.
- SSH can also easily be configured to authenticate both the server as well as the client.

Secure Shell Protocol

- The SSH protocol was developed by SSH communication security Ltd to safely communicate with the remote machine.
- Secure communication provides a strong password authentication and encrypted communication with a public key over an insecure channel.
- The most common implementation of the SSH protocol is the Unix ssh program.
- There are multiple SSH programs available: commercial ssh, Open SSH, putty for Windows platforms, and F-Secure ssh.
- Each of these programs is interoperable with each other, but have their own unique features and configuration options.
- Some of these programs are open source and some are distributed for free.
- You will need to examine the features and support options to determine which program will be appropriate for your application.
- It is used to replace unprotected remote login protocols such as Telnet, rlogin, rsh, etc., and insecure file transfer protocol FTP.
- Its security features are widely used by network administrators for managing systems and applications remotely.
- The SSH protocol protects the network from various attacks such as DNS spoofing, IP source routing, and IP spoofing.



Before SSH



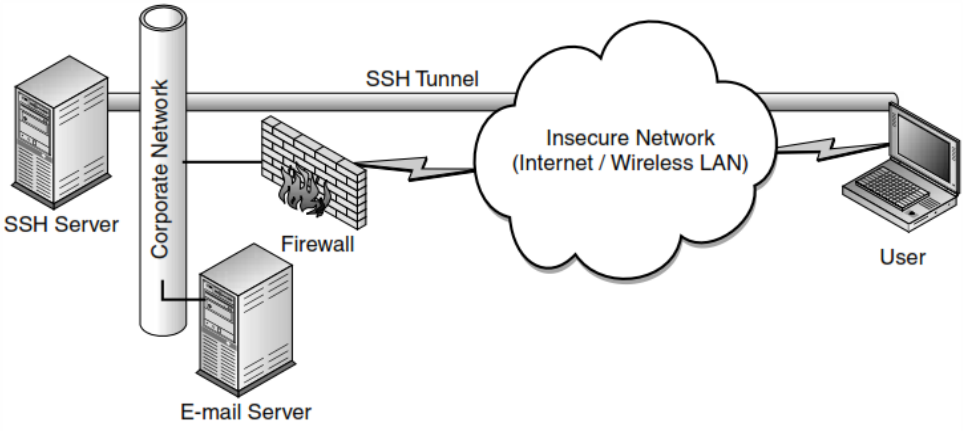
After SSH

Terminal Access and File Transfer

- The most common use of SSH is for replacing telnet. Telnet is a common application used to manage network hosts.
- Telnet sessions can be easily sniffed (revealing sensitive data), hijacked, or data can be injected.
- If properly implemented, SSH eliminates these security concerns. If you are still using telnet for anything, please replace it with SSH immediately.

Port Forwarding

- Some manufacturers are not supporting SSH as a telnet or FTP replacement.
- In these situations SSH can be used to secure otherwise insecure applications such as telnet, FTP, the Post Office Protocol (POP), or even HTTP.
- This can be accomplished by using the port-forwarding feature of SSH.
- Many device and operating manufacturers are starting to include support for SSH.
- Most file transfer protocols such as FTP, the Trivial File Transfer Protocol (TFTP), and the Common Internet File System (CIFS) are very insecure. These protocols suffer from the same sniffing, injection, and hijacking attacks.
- SSH includes the capability to transfer files over an encrypted authenticated session.



SSH Tunnel

- 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 e-mail server to the insecure network.
- In addition to using SSH for terminal access to the SSH server, port forwarding can be used to tunnel e-mail traffic over the insecure network to the SSH server.
- Then the SSH server forwards the packets to the e-mail server.
- From the e-mail server's perspective, the traffic would be coming from the SSH server and packets would be returned to the SSH server for tunneling back to the user.
- E-mail is just one example of the many TCP protocols that can be tunneled over SSH.
- Other common applications for SSH include securing file transfers (Network File System [NFS], FTP and CIFS), web applications (HTTP), and thin client applications (MS Terminal Server and XWindows).

A Word of Caution

- Due to the flexibility and ubiquitous access that SSH enables, great care must be taken when implementing SSH.
- SSH is a tool that is commonly used by attackers.
- In our port forwarding example, we explained how SSH can be used to bypass firewall rules for accessing e-mail or other applications.
- This may be used by legitimate users or by malicious attackers.
- Therefore, make sure that SSH servers and clients are adequately secured and do not forget to secure applications behind the firewall.

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

- Some implementations of SSL/TLS and SSH may also be vulnerable to man-in-the-middle (MITM) attacks.
- Both SSL/TLS and SSH use a public key algorithm for establishing symmetric keys for the data transfer.
- A malicious attacker could intercept the handshake and replace the public keys exchanged with counterfeit keys. The attacker would then be able to attack the SSL/TLS or SSH session.
- Implementing a Public Key Infrastructure (PKI) or holding key-signing parties are ways to prevent this type of attack.
- PKI uses complex mathematical algorithms to verify the authenticity of a key by checking it against information from a certificate authority (CA).
- Key-signing parties eliminate the need for a CA, but require all parties that would communicate to meet together and personally exchange keys.
- The error messages in many applications displayed during an SSL/TLS or SSH MITM attack may go unnoticed by users.

WTLS(Wireless Transport Layer Security)

- WTLS is based on SSL/TLS. WTLS is used by Wireless Application Protocol (WAP) devices such as mobile phone handsets and personal digital assistants (PDAs).
- The primary difference between SSL and WTLS is the transport layer. SSL relies on TCP for reliability functions, such as the retransmission of lost packets and out-of-order packets.

- The WAP devices using WTLS cannot use TCP for these functions because WAP devices only use the User Datagram Protocol (UDP).
- UDP is not a connection oriented protocol, so these functions have been included in WTLS.

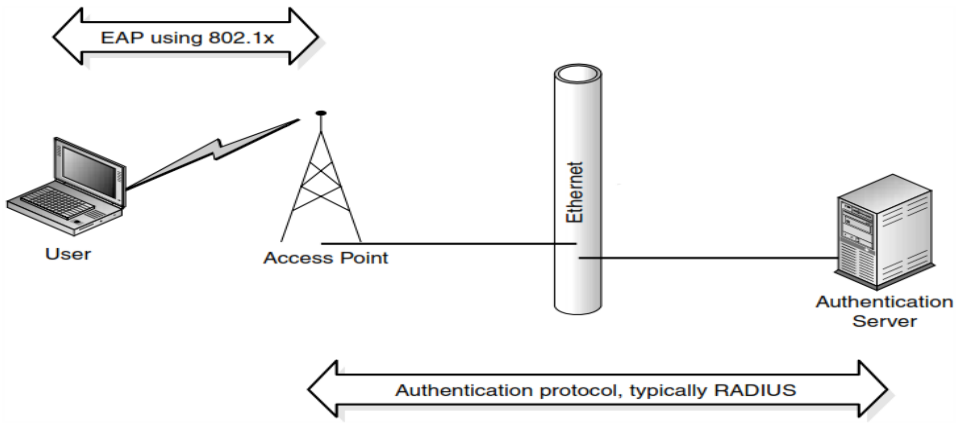
  Three classes can be negotiated during the handshake process
  - WTLS class 1 No certificates
  - WTLS class 2 Server certificate only
  - WTLS class 3 Client and server certificates
- In class 1, no authentication takes place and the protocol is simply used to set up an encrypted channel.
- In class 2, the client (typically a handset) authenticates the server, in most cases, the certificates are included in the firmware of the handset.
- In class 3, both the client and server are authenticated. This normally involves the implementation of a PKI.
- WTLS is similar to SSL/TLS in that it can be used to secure other protocols, such as Wireless Markup Language (WML).
- WML is much like Hypertext Markup Language (HTML), but it is specifically designed for WAP devices, such as mobile phones and PDAs.

WEP(Wired Equivalent Privacy)

- Wired Equivalent Privacy (WEP) is the security mechanism included in the 802.11 standard and is designed to provide confidentiality and authentication services.
- WEP is based on the RC4 algorithm, which is referred to as a stream cipher.
- Packets are encrypted by generating an RC4 stream with a combination of a 24-bit initialization vector (IV) and a shared key.
- The IV is used to make the RC4 stream generated with the shared key different for many of the data transmissions.
- The data is then XORed with the generated stream and transmitted in a WEP frame with the IV in the header so the receiver can generate the same RC4 stream to XOR the packet for decryption.
- There are problems with the implementation of WEP. WEP can be used as a first line of defense, but cannot be relied on for security because weaknesses have been proven that can compromise the WEP key.
- WEP also presents a number of key management problems. A common WEP key is normally used for all users on a given wireless network, which makes it very difficult to protect the key.
- WEP keys would need to be changed very frequently. Employees are constantly leaving the company or are losing wireless equipment such as laptops.
- Some of the latest implementations of WEP, often bundled in 802.1x functionality upgrades negotiate a WEP key at the time of initial authentication.

802.1x

- 802.1x and its associated protocols are an attempt to increase the security of networks before layer 3 protocols (such as IP) are set up.
- The technology is not specific to 802.11 and can be used on Ethernet, Token Ring, and so on.
- 802.1x is a layer 2 protocol that can be used for a number of operations.
- The basic purpose of 802.1x is to authenticate users and can optionally be used to establish encryption keys.
- When a connection is established, only 802.1x traffic is allowed to pass.
- This means the other protocols such as the Dynamic Host Configuration Protocol (DHCP), IP, and so on are not permitted.
- Extensible Authentication Protocol (EAP) (RFC 2284) is used to authenticate the users.
- EAP was originally designed to solve some of the authentication issues with the Point-to-Point Protocol (PPP), but its main use will probably be solving wireless issues.
- EAP authentication packets are sent to the access point with user login information, in most cases, this will be a username and password.
- The access point can authenticate the user by any means the vendor chooses to support.
- In most cases, this will be via Remote Authentication Dial-in User Service (RADIUS).
- Once the user is authenticated and optional encryption is established, communication will be enabled and protocols such as DHCP will be allowed to pass.



802.1x overview

IP Security (IPSec)

- IP Security (IPSec) was developed by the Internet Engineering Task Force (IETF) working group and continues to evolve.
- The IPSec protocol is lower in the protocol stack than SSL/WTLS, SSH, or WTLS.
- The security is implemented on the IP layer in the Internet model.
- The most common implementations of IPSec are using a tunnel mode that enables all IP traffic to be encrypted and optionally authenticated inside a single session.

- IPSec is the enabling technology behind most virtual private networks (VPNs) used on the Internet today.Due to the flexibility of IPSec and its broad range of application support, many choose to use it for securing their wireless applications.
- IPSec has multiple implementation options that should be used based on the application.
- IPSec can be used to provide encryption by using Encapsulated Security Payload (ESP) or authentication by using Authentication Header(AH).
- AH may be implemented without ESP. This would not provide confidentiality against sniffing, but would prevent tampering with the data and damaging the data in transport, and positively identify the sender.
- ESP can be implemented without AH to provide confidentiality and basic authentication services of data, but many administrators choose to implement both AH and ESP.
- IPSec has many different cryptographic algorithms that can be used for AH and ESP.
- The most commonly used encryption algorithms for ESP are the Data Encryption Standard (DES), Triple DES (TDES), and Advanced Encryption Standard (AES).
- AES is the replacement for DES and TDES, and the IPSec standard mandates that it be implemented in all IPSec implementations.
- The most commonly used authentication algorithms used for AH are Message Digest 5 (MD5) and Secure Hash Algorithm (SHA).
- Two modes can be used by IPSec for encapsulating data.
- Transport mode is normally used when using IPSec to communicate between two hosts. Transport mode only encrypts the data of the IP packet and all the header information remains unencrypted.
- Tunnel mode encrypts the entire IP packet including the headers. Tunnel mode is more flexible for Internet applications because many enterprises utilize private network addressing, as described in RFC 1918.
- The most common implementation of IPSec for secure communications is for remote-access VPNs over the Internet.
- Whenever a public network is used for private networking functions, it can be called a VPN.
- Using this definition, networking technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and X.25 can be considered VPNs, but most people exclusively use the term to refer to encrypted tunnels over the Internet.
- In this application, a gateway is installed on the perimeter of the corporate network.
- Remote-access users will establish an IPSec tunnel to the gateway using tunnel mode with ESP and AH.