M.Sc (Computer Science)

II year – III Semester

COMPUTER NETWORK SECURITY AND CRYPTOGRAPHY

Handled by

Dr.K.Shanmugavadivu

COMPUTER NETWORK SECURITY AND CRYPTOGRAPHY

UNIT-I

Types of Physical Medium-Topologies-Wireless Networking: Wireless Protocols. Data Link Layer: Layered Data Link Protocols-SLIP and PPP-MAC and ARP. Network Layer: Routing Risks-Addressing-Fragmentation-Security.

UNIT-II

Internet Protocol: IP Addressing-ICMP-Security options. Transport Layer: Common Protocols-Transport Layer Functions-Gateways. TCP: Connection Oriented Protocols-TCP Connections-UDP. Session Layer: Session State Machine-Session and Stacks. SSL: SSL Functionality-Certificates. SSH: SSH and Security-SSH Protocols. STMP: Email Goals-Common servers. HTTP: HTTP Goals-URL.

UNIT-III

Security: Importance-Threat Models-Concepts-Common Mitigation Methods. Network theory: Standards Bodies-Network Stacks-Multiple Stacks-Layers and Protocols-Common Tools. Cryptography: Securing Information-Necessary Elements-Authentication and Keys-Cryptography and Randomness-Hashes-Ciphers-Encryption-Steganography.

UNIT-IV

Data Encryption Techniques-Data Encryption Standards-Symmetric ciphers. Public key Cryptosystems-Key Management.

UNIT-V

Authentication-Digital Signatures-E-Mail Security-Web Security-Intrusion-Firewall.

TEXT BOOKS:

1. Neal Krawetz, Introduction Network Security, India Edition, Thomson Delmar Learning. 2007 (Unit-I:5.1,5.4,7.2,8.3,9,10,11.2,11.3,11.5,11.9,Unit-II: 12.1,12.2,12.4,14.1,14.2,14.3,15.1,15.2,15.7,16.2,16.3,19.2,19.3,20.1,20.2,22.2,2223.1,23.2,Unit-III:1.1,1.2,1.3,1.4,3.1,3.2,3.3,3.4,3.5,4.1,4.2,4.3,4.4,4.5,4.6,4.7,4.8)
2. V.K.Pachghare, Cryptography and Information Security, PHI Learning Private Limited 2009, (Unit-IV: 2,3,5,7,8, Unit-V: 9,10,11,13,14,16)

REFERENCE BOOK:

1. William Stallings, Cryptography and Network Security, Prentice –Hall of India, 2008

PHYSICAL LAYER:-

Introduction :-

The OSI model begins with the physical layer. This incorporates the physical network mediums, network interface cards (NIC), and operating system drivers for controlling the NIC. The type of physicalmedium and network layout (topology) determines the physical security of the network.

The physical medium does not need to be corporeal. The OSI physical layer has one purpose to directly communicate with the physical medium over a physical link. This communication includes establishing the physical link, transmitting data over the link, and receiving data from the link.

Depending on the type of medium, the physical link may also require activation and deactivation. The transmission and reception of data on the physical layer follows a five-step cycle:-

1. A program generates data and sends it to the physical device driver.
2. The physical device driver uses the NIC to transmit the data over the physical link.
3. The NIC on the recipient system receives the data.
4. The data is passed to the recipient's physical device driver.
5. The physical device driver passes the data to higher OSI layers for processing.

The physical layer operates independent of the data sent or received—it only ensures that data is transmitted and received properly, not that the data itself is proper. The physical layer ensures that the transmitted data is not corrupted, but it does not validate the content of the transmitted information

TYPES OF PHYSICAL MEDIUMS

A physical medium is transmit and receive data. The protocols that are commonly used include wired protocols, fiber optics, high-volume trunk lines, dynamic connections (e.g., dialup), and wireless networks.

***Wired Network Protocols**

Wired networks comprise some of the most common physical layer protocols. These wired networks connect end-user computers to servers and branching subnetworks from high-bandwidth trunk lines in buildings and small offices.

Coax cable was commonly used for wired networks.

The 10Base-2 standard,also known as thinnet or Ethernet, used a 50-ohm coaxial cable (RG58) to transmit amplitude modulated RF signals.

The designation "10Base-2" denotes a maximum throughput of 10 Mbps over two wires (coaxial cable). The maximum cable length was 185 meters. The 10Base-5 (thicknet)—also used RG58 but had a maximum cable length of 500 meters. 10Base-T and 100Base-T use twisted-pair wire such as category 3 (Cat3), Cat5, or Cat5e cable with an RJ45 connector. These standards use a low-voltage alternating current to transmit data at 10 Mbps and 100 Mbps, respectively.

*** Fiber-Optic Networks**

Fiber-optic cables carry pulses of light. This medium is commonly used with the Fiber Distributed Data Interface (FDDI) protocol. FDDI is an OSI layer 2 protocol and operates as a high-speed token ring, achieving 100 Mbps and faster. High-speed networks, such as 10-Gb Ethernet, also commonly use fiber-optic cables. Fiber-optic networks are generally more expensive than wired networks but provide much higher bandwidths.

*** Trunk Lines**

Trunk lines connect major network hubs with other hubs, providing very large bandwidths. Some trunk lines use copper wire, and others use fiber-optic cable. As an example, T-1, T-3, and FT-1 are trunk phone line connections, and the number indicates the type. A T-1 is a "trunk level 1" link. It contains 24 channels, with each channel supporting a data rate of 64 Kbps. A T-3 is a "trunk level 3" link, consisting of three T-1 links, or 672 separate channels.

A fractional T-1 (FT-1) consists of a subset of channels from a T-1 connection and is usually used for leased lines. Other types of trunk lines include OC-1, OC-3, OC-12, and OC-48.

*** Dynamic Networks**

Not every network medium is static and always connected. Dynamic networks provide a large portion of home and small office network connections and are used when static networks are not required. Dynamic networks generally consist of a modem (MOdulator and DEModulator) for connecting to an Internet service provider (ISP). A standard modem sends a data signal over a voice phone line.

Dynamic networks are generally less expensive for end consumers, but they do not provide the same high bandwidth as wired, fiber-optic, or trunk network connections.

These networks have one significant security benefit: they are not always connected. When the modem disconnects from the ISP, the network is no longer vulnerable to remote network attacks.

*** Wireless**

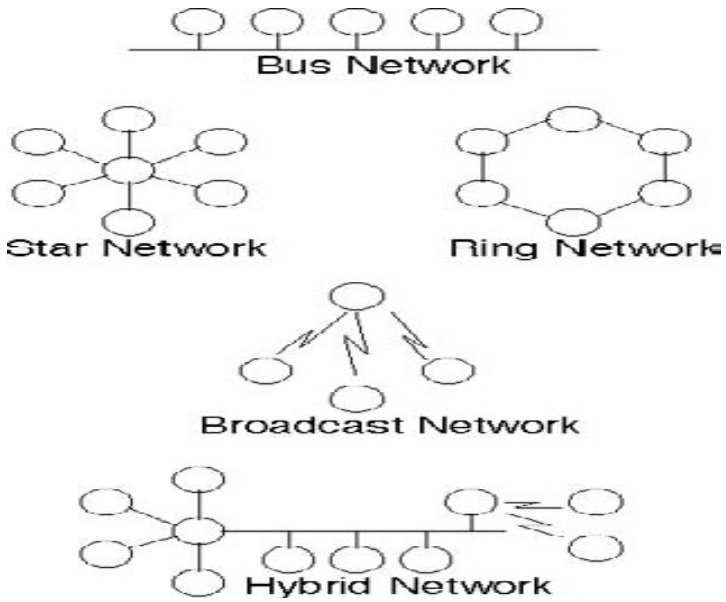
Wireless networks are frequently used in places where traditional wired, fiber-optic, and trunk lines are unavailable, too costly, or too difficult to install. Rather thanwiring an entire home for using a network, wireless networks permit the computer to be anywhere as long as it can access the wireless hub's radio signal.

IEEE 802.11, also called wireless fidelity (WiFi), defines a suite of protocols commonly used for wireless networking.

Wireless networks can be very inexpensive to deploy because they require only a network access point (AP, or "hotspot") and a wireless network interface (SP, or subscriber point). Wireless networks do not require any physical medium installation such as cables.

TOPOLOGIES

. The four commonly used network topologies are bus, star, ring, and broadcast. Small networks may use single topology architectures, but large networks generally appear as a hybrid where connectors join different topologies.



*** Bus Networks**

A *bus network* consists of a single link that includes all nodes. In a bus architecture, any transmission on the network is received by every node on the network. Nodes can be readily added and removed without significantly impacting the network. Network collisions, when two nodes transmit data at the same time, are common and can lower overall network performance.

*** Star Networks**

A *star network* topology relies on a central hub for communicating with nodes.For example in a twisted-pair network every RJ45 connector links a node (computer) to acentral hub –this is physically a star network. But if the hub acts as a bridge or switch (OSI layer 2), then it can interpret the network data and direct it to the correct branches of the star network.

Hubs can provide a centralized point for authenticating new network nodes.star networks have one significant limitation: the hub acts as a central point of failure. If the hub becomes inaccessible for any reason, then the network collapses.

*** Ring Networks**

The *ring network* topology moves the hub from the center of the network to each node. Each node in a ring network contains two connections that lead to two neighboring nodes. Data is passed through the neighboring nodes until it reaches the destination. Ring networks typically maintain two paths between each node: clockwise and counter-clockwise around the ring.

From a security perspective, ring networks are midway between a bus and star network. A single node on the ring can only eavesdrop on the traffic that it receives. Because half of the traffic likely takes a route that does not include the node, the node cannot eavesdrop on all the traffic.In addition the impact from DoS is limited to the response by the adjacent nodes; if the neighbors do not propagate the DoS, then the DoS has little impact.

Every device has access to the token and the opportunity to transmit.It does not require network server to manage the connectivity between the computers.

*** Broadcast Networks**

Broadcast networks are used when data is transmitted over radio frequencies rather than over a point-to-point wire. These networks are very desirable due to their low cost and simple setup—a network only needs a hub (access point, or AP) and a network card containing a transmitter (subscriber point, or SP); they do not require cables linking every node. The only requirement is for the radio signal to be strong enough between the AP and SP.

Broadcast and wireless networks extend on the limitations from the bus network.For example in a bus network, every node can receive all transmitted data, In a wireless network, anyone with a radio receiver can receive all transmitted data.

*** Hybrid Networks**

A *hybrid network* connects multiple network architectures to permit a combination of benefits. For example, a company may use a star architecture for connecting departments but a bus architecture within each department. The benefits for this example include cost, speed, and security.A hybrid network can be more cost effective than a star network because a single hub is less expensive than supplying a hub for everyone in a department.

Hybrid topologies reduce security risks from homogenous networks. A risk impacting one department is compartmentalized to that department. For example, an eavesdropper in the human resources department cannot spy on data from the finance department. Similarly, a hub that becomes disabled may not impact an entire corporation..

Wireless Networking

WIRELESS PROTOCOLS

The, 802.11 defines how a wireless network subscriber point (SP) identifies the correct wireless network access point (AP). These include a service set identifier (SSID) and wired equivalent privacy (WEP).

SSID

The service set identifier (SSID) is a 32-character text string used to identify an AP and distinguish it from other APs. For example, 802.11b defines a frequency range 2.4 GHz) and 11 channels within that range. An AP may be placed on any single channel, but many APs may share the same channel. The SSID is used to distinguish APs that share a channel.

WEP

IEEE 802.11 defines the wired equivalent privacy (WEP) protocol, providing a degree of security to wireless networks. In a wired network, Privacy is limited to physical access—if an attacker cannot gain physical access to the network, then the physical network is likely secure. In contrast, wireless networks broadcast a radio signal. Anyone who can receive the signal immediately gains physical access to the medium. WEP defines a cryptographic authentication system that deters unauthenticated SP access. The WEP cryptography includes keys and encryption.

WEP Keys

WEP supports two types of encryption: 64 bit and 128 bit. These correspond with 40-bit and 104-bit length secret keys, respectively. These keys are used to authenticate network access.

There are two ways to create the secret key. The first method simply allows the user to enter in the 8- or 16-character hexadecimal number that represents the key;, many AP configurations permit the use of a text-based password for generating the secret keys. A text password is hashed into a 40-bit (or 104-bit) encryption key. Regardless of the generation method, the AP and SP must have the same key.

WEP 40-Bit Password Hash

The algorithm used to convert a text string into a secret key differs based the encryption strength. The CD-ROM contains source code for WEP-password—a program that generates WEP keys based on text strings.

WEP 104-Bit Password Hash

Unlike the 40-bit hash function, the 104-bit key generation uses the MD5 cryptographic hash algorithm. The text password must consist of 64 characters. When the user specifies a shorter password, the phrase is repeated until 64 characters are present.For example, the password "Simplistic" becomes "SimplisticSimplisticSimplisticSimplisticSimplisticSimplisticSimp."

Longer passwords are truncated at 64 characters.

WEP Encryption

WEP encryption uses the RC4 stream cipher encryption algorithm. For each packet being transmitted, an initial vector (IV) is generated. For 64-bit WEP, the IV is 14 bits long; the IV for 128-bit encryption is 24 bits long. The IV is combined with the secret key to seed the RC4 encryption. RC4 then encrypts the data.

When the AP or SP receives data, the encryption process is reversed. The RC4 algorithm combines the secret key with the unencoded IV that was transmitted with the packet. This combination is used to decode the encrypted data. The final CRC is checked to validate the decoded data.

WEP Cracking

For attackers to crack the WEP encryption, they only need to determine the secret key. There are two main approaches for cracking WEP: brute-force password guessing and data analysis.

Brute-Force WEP Cracking

WEP and 802.11 define no method for deterring dictionary attacks—an attacker can try thousands of keys without ever being denied access and without ever having the AP generate a log entry concerning a possible attack. From the AP's viewpoint, there is no distinction between a corrupt packet due to a CRC error (e.g., poor radio signal) and a corrupt packet due to a decryption problem (bruteforce key attack).

Many APs are configured using weak passwords. These may include people's names, addresses, or manufacturer brands.

Data Analysis WEP Cracking

For 64-bit encryption, there are only 4,096 (212) different IV values. If the IV does not change between packets, then a duplicate is immediately available. But if the IV changes between each packet, then a duplicate IV will be observed after no more than 4097 packets. When an attacker captures two packets with a duplicate IV, it is just a matter of trying different key sequences to find the ones that result in an RC4 decryption with the correct CRC checksum. By assuming weak passwords for creating the secret key, the search process can be sped up. Given two packets with the same IV, the entire 64-bit WEP analysis can take a few minutes. 128-bit encryption may take a few hours, depending on the computer's speed.

DATA LINK LAYER

LAYERED DATA LINK PROTOCOLS

The data link layer usually contains multiple protocols that, together, provide the full data link functionality. The lower protocols manage the physical layer communications. The middle layer protocols manage routing and addressing, and upper layer protocols control network discovery.

1 Low-Level Protocols

The lower level data link protocols are directly associated with the physical layer. Examples include the following:

FDDI: This layer 2 protocol acts as a high-speed Token Ring over fiber-optic networks.

LAPF: The standard ITU Q.921 defines the Link Access Protocol for Frame Mode Services. This frame relay protocol is commonly used on ISDN, F-T1, and faster networks.

PPP: The Point-to-Point Protocol commonly connects dynamic connections, such as modem or ISDN.

Carrier Sense Multiple Access/Collision Detection: CSMA/CD is part of the IEEE 802.3 standard and is used for most end-user Ethernet traffic. This protocol determines when data may be transmitted and detects when collisions occur. The physical layer is commonly twisted pair (10Base-T or 100Base-T), or coax such as 10Base-2 or 10Base-5.

2 Middle-Level Protocols

The middle protocols within the data link layer manage addressing. These are closely associated with specific lower-level layer 2 protocols. For example, IEEE 802.2 defines two data link sublayers: MAC and LLC. The MAC defines a unique address on a particular network. The logical link control (LLC) is the higher portion that provides a consistent interface regardless of the MAC format.

3 High-Level Protocols

The high-level data link layer protocols manage address discovery. For example, when using MAC addressing, the ARP is used to identify the MAC address of a particularhost. Other higher-level protocols include the AppleTalk Address Resolution Protocol (AARP) and the multilink protocol (MP) for X.25 networks.

SLIP AND PPP

1 SIMPLIFIED DATA LINK SERVICES

This includes simpler framing methods, flow control, and address support. \

1.1 Simplified Flow Control

The physical layer ensures that the data received matches the data transmitted, but it does not address transmission collisions. When two nodes transmit at the same time, data becomes overwritten and corrupted.

This is required functionality on a multinode network because any node may transmit at any time.

The most common types of point-to-pointnetworks use simplex, half-duplex, or full-duplex connections.

1.1 Simplex

A *simplex* channel means that all data flows in one direction; there is never a reply from a simplex channel. For networking, there are two simplex channels, with one in each direction. The flow control is simplified: there is no data link layer flow control because it is always safe to transmit. Examples of simplex networks include ATM, FDDI, satellite networks, and cable modems.

1.2 Half-Duplex

Half-duplex channels are bidirectional, but only one node may transmit at a time. Either a node is transmitting, or it is listening. Each node must periodically check to see if the other node wants to transmit. Examples of half-duplex networks include some dialup, serial cable, and wireless network configurations.

1.3 Full-Duplex

In a *full-duplex* network, one channel is bidirectional, but both nodes can transmit at the same time. Examples include many fiber-optic systems, where the transmitted light pulses do not interfere with the received light pulses. Some FDDI, optical cable networks, and telephone modem protocols use full-duplex channels.

9.1.2 Simplified Message Framing

Message framing ensures that the transmitted data is received in its entirety. The physical layer ensures that the data received matches the data transmitted, simultaneous transmissions can corrupt the data. In point-to-point networks, the message frame only needs to indicate when it is clear for the other side to transmit.

9.1.3 Simplified Address Support

In a multinode network, the message frame must be addressed to the appropriate node. In a point-to-point network, however, all transmitted data are only intended for the other node on the network.

For example, a user with a dialup modem may have the data link layer assign a random MAC address to the connection. After the connection terminates, the next connection may have a different MAC address. In many implementations, the data link layer's MAC address may appear to be the system's assigned IP address; an assigned dialup IP address of 1.2.3.4 may generate the MAC address 00:00:01:02:03:04. The next time the user dials into the service provider, the system may be assigned a new IP address and generate a new MAC address.

9.2 POINT-TO-POINT PROTOCOLS

Two common point-to-point protocols are SLIP and PPP.

SLIP

The *Serial Line Internet Protocol* (SLIP) is defined by RFC1055. This simple protocol was originally designed for serial connection. SLIP provides no initial headers and only offers a few defined bytes:

END: The byte 0xC0 denotes the end of a frame.

ESC: The byte 0xDB denotes an escape character.

Encoded END: If the data stream contains the END byte (0xC0), then SLIP reencodes the character as 0xDB 0xDC.

Encoded ESC: If the data stream contains the ESC byte (0xDB), then SLIP reencodes the character as 0xDB 0xDD.

When the OSI network layer has data to transmit, SLIP immediately begins transmitting the data. At the end of the transmission, an END byte is sent.

Error Detection

SLIP contains no mechanism for error detection, such as a framing checksum.

Maximum Transmission Units

The *maximum transmission unit* (MTU) defines the largest size message frame that is permitted. The SLIP message frame has MTU restrictions. The receiving system must be able to handle arbitrarily large SLIP message frames. most SLIP drivers restrict frames to 1006 bytes (not including the END character). SLIP also permits transmitting an END END sequence, resulting in a zero-length datagram transmission.

No Network Service

Many multinode data link protocols include support for multiple network layer protocols. SLIP contains no header information and no network service identifier. As such, SLIP is generally used with TCP/IP only.

Parameter Negotiations

A SLIP connection requires a number of parameters. Because it relies on a TCP/IP network layer, both nodes need IP addresses. The MTU should be consistent between both ends of the network, and the network should authenticate users to prevent unauthorized connections. Authentication for SLIP connections generally occurs at the physical layer. SLIP does not support other options, such as encryption and compression.

PPP (Point-to-Point Protocol)

The *Point-to-Point Protocol* (PPP) provides all data link functionality.

Many RFCs cover different aspects of PPP: RFC 1332, 1333, 1334, 1377, 1378, 1549, 1551, 1638, 1762, 1763, and 1764. The main standard for PPP is defined in RFC1661. The PPP message frame includes a header that specifies the size of data within the frame and type of network service that should receive the frame.

PPP does not provide a means to protect authentication credentials, detect transmission errors, or deter replay attacks.

Authentication

For authentication, PPP supports both PAP and CHAP, but only one should be used. CHAP and PAP both provide a means to transmit authentication creden-tials, neither provides encryption; the authentication is vulnerable to eavesdropping and replay attacks at the physical layer.

For PAP and CHAP, the login credentials must be stored on the PPP server. If they are stored in plaintext, then anyone with access to the server may compromise the PAP/CHAP authentication. Even if the file is stored encrypted, the method for decrypting the file must be located on the PPP server.

Transmission Error Detection

PPP includes a frame header and tail, it does not include a checksum for frame validation. PPP assumes that error detection will occur at a higher OSI layer.

Replay Attack Transmission

PPP's message frame header contains packet and protocol information but not sequence identification. Because PPP was designed for a point-to-point network, it assumes that packets cannot be received out of order.

Nonsequential, missing, and duplicate packets are not identified by PPP. If the physical layer permits nonsequential transmissions, then PPP may generate transmission problems. Examples include using PPP with asynchronous transfer mode (ATM) or grid networks.

In these examples, data may take any number of paths, may not be received sequentially, and in some situations may generate duplicate transmissions. An attacker with physical access to the network may insert or duplicate PPP traffic without difficulty. This opens the network to insertion and replay attacks.

Other Attacks

As with SLIP, PPP provides no encryption. An attacker on the network can readily observe, corrupt, modify, or insert PPP message frames transmissions.

Tunneling

VPNs are commonly supported using PPP (and less common with SLIP). A true network connection is established between two nodes, and then PPP is initiated over the connection, establishing the virtual point-to- point network. Common tunneling systems include PPP over SSH and PPP over Ethernet (PPPoE).

PPP over SSH

Secure Shell is an OSI layer 6 port forwarding protocol that employs strong authentication and encryption. SSH creates a single network connection that is authenticated, validated, and encrypted. Any TCP (OSI layer 4) connection can be tunneled over the SSH connection, but SSH only tunnels TCP ports.

By using an SSH tunneled port as a virtual physical medium, PPP can establish a point-to-point network connection. The result is an encrypted, authenticated, and validated PPP tunnel between hosts. This tunnel can forward packets from one network to the other—even over the Internet—with little threat from eavesdropping, replay, or insertion attacks

PPPoE

PPP over Ethernet (PPPoE), defined in RFC2516, extends PPP to tunnel over IEEE 802.3 networks. Many cable and DSL connections use PPPoE because PPP provides a mechanism for negotiating authentication, IP address, connection options, and connection management.

The PPPoE server is called the *access concentrator* (AC) because it provides access for all PPPoE clients. PPPoE does have a few specified limitations:

MTU: The largest MTU value can be no greater than 1,492 octets. The MTU for Ethernet is defined as 1,500 octets, but PPPoE uses 6 octets and PPP uses 2.

Broadcast: PPPoE uses a broadcast address to identify the PPPoE server.

AC DoS: The AC can undergo a DoS if there are too many requests for connection allocations**9.2.3.3 CSLIP and CPPP**

When tunneling PPP or SLIP over another protocol, the overhead from repeated packet headers can significantly impact performance. For example, TCP surrounds data with at least 20 bytes of header. IP adds another 20 bytes. So IP(TCP(data)) increases the transmitted size by at least 40 bytes more than the data size.

Transmit Size: When tunneling, there are 80 additional bytes of data per packet. More headers mean more data to transmit and slower throughput.

Message Frames: Many data link protocols have well-defined MTUs. Ethernet, for example, has an MTU of 1,500 bytes. Without tunneling, TCP/IP and MAC headers are at least 54 bytes, or about 4 percent of the MTU. With tunneling, the TCP/IP and PPP headers add an additional 3 percent plus the overhead from SSH.

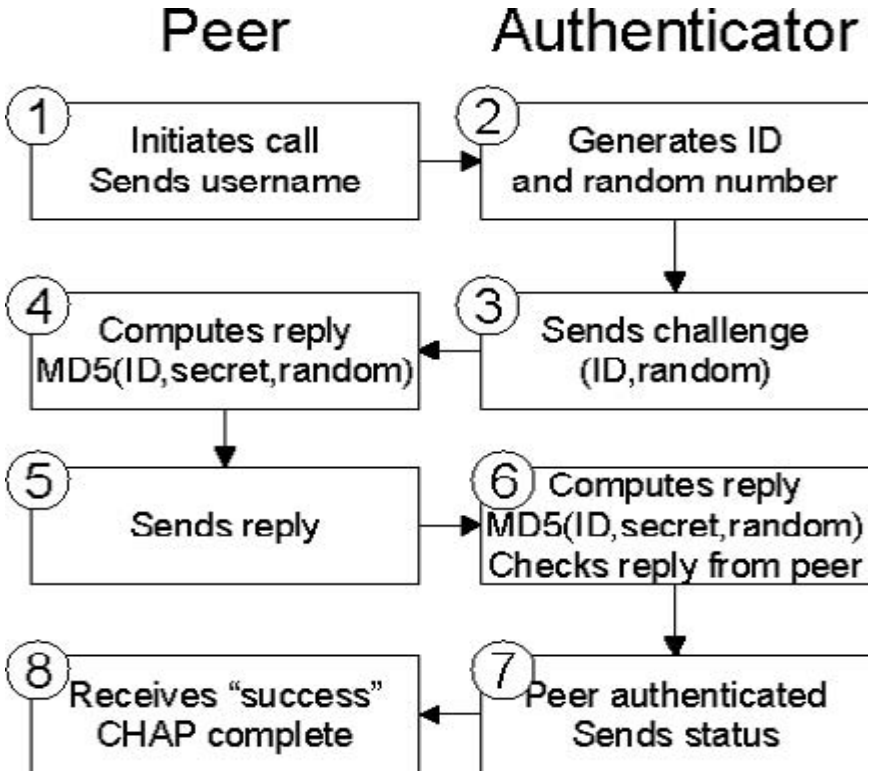
Stack Processing: When transmitting and receiving, twice as many layers must process each byte of data.

COMMON RISKS

The largest risks from PPP and SLIP concern authentication, bidirectional communication, and user education.

Authentication

SLIP provides no authentication mechanism. PPP supports both PAP and CHAP for authentication [RFC1334]. PAP uses a simple credential system containing a username and password; the username and password are sent to the server unencrypted and then validated against the known credentials. CHAP uses a more complicated system based on a key exchange and a shared secret key



(, CHAP transmits a username from the client (*peer*) to the server (*authenticator*). The server replies with an 8-bit ID and a variable-length random number. The ID is used to match challenges with responses—it maintains the CHAP session. The client returns an MD5 hash of the ID, shared secret (account password), and random number. The server computes its own hash and compares it with the client's hash. A match indicates the same shared secret.;

CHAP has two limitations.

First, it only authenticates the initial connection. After authentication, PPP provides no additional security—someone with eavesdropping capabilities can hijack the connection after the authentication. Second, if an eavesdropper captures two CHAP negotiations with small-length random numbers, then the hash may be vulnerable to a brute-force cracking attack

Bidirectional Communication

PPP and SLIP provide full-data link support in that the node may communicate with a remote network, and the remote network may communicate with the node.

PPP and SLIP provide full bidirectional communication support. As such, any network service operating on the remote client is accessible by the entire network.

User Education

. Most dialup, DSL, and cable modem users may not be consciously aware that their connections are bidirectional. Moreover, home firewalls can interfere with some online games and conferencing software such as Microsoft NetMeeting.

LLC

LLC resides in the upper portion of the data link layer. It provides four functions: link management , SAP management, connection management, and sequence man

Link Management

LLC provides the control mechanisms for protocols that require flow control. Many quality-of-service protocols, use LLC link management to compute the quality. Spanning Tree is used by bridges and ensures that routing loops do not form. Each bridge sends out a Spanning Tree message frame with an identifier.

SAP Management

Service Access Points (SAPs) are ports to network layer protocols. Each network layer protocol uses a different 16-bit identifier to identify the network protocol. The *Sub Network Access*

Protocol (SNAP) extends the number of DSAP/SSAP values. SNAP defines a 3-byte Organizationally Unique ID (OUI) and a 2-byte protocol type.

Connection Management

LLC determines whether the data link layer should use a connection-oriented or connection-less communication flow. The type of connection is independent of higher layer protocols. For example, UDP is an OSI layer 4 connection-less protocol, and TCP is an OSI layer 4 connection-oriented protocol.

Sequence Management

LLC includes a sequence number and uses a sliding window system. The sequence numbers ensure that each message frame is received in the correct order. The sliding window reduces communication overhead by only requiring occasional acknowledgements

MAC

The *media access control* (MAC) sublayer provides two key functions: transmission control and network addressing.

Transmission Control

CSMA/CD determines when it is safe to transmit. When a node has data to transmit, CSMA specifies that the node first listen to the network. If nobody else is transmitting, then the data is transmitted; Collision Detection (CD) monitors the network for additional voltage. Upon detecting a collision, the node immediately stops transmitting, waits a few microseconds, and then repeats the process.

Network Addressing

Every node on the network requires a unique address. This hardware address allows unicast and multicast packets to be processed by the recipient node.

. Ethernet network cards use a preset 6-byte code to specify the MAC address. These are usually written in a colon-delimitated format: 00:11:22:33:44:55. The first three octets are the *Organizationally Unique Identifier* (OUI). The remaining three octets are vendor specific—they may indicate the particular make and model of the network card or a third-party vendor.

Attackers may target the MAC address through hardware profiling reconnaissance, impersonation, and load attacks.

Acquiring Hardware Addresses

Each physical layer interface is associated with a unique identifier (name) and MAC address.

LLC provides hardware addresses are only needed for multinode networks, point-to-point networks.

MAC Vulnerabilities

Although the MAC provides the means to communicate information between hosts on a network, it also introduces potential attack vectors.

1. Hardware Profiling Attacks

The first step in attacking a system is reconnaissance. An attacker blindly attempt to attack an unknown system will rarely be successful. The OUI provides hardware and operating system information to an attacker. Hardware profiling is a viable information reconnaissance technique.. In environments where it is desirable to obscure the hardware profile, most network drivers permit changing the MAC address. The method to change the MAC address differs by operating system

Windows 2000: The advanced configuration for most network adapters permits setting the hardware address

RedHat Linux: The root user can use the ifconfig command to change the adapter's hardware address.

2 Impersonation Attacks

An attacker may intentionally change the address to duplicate another node on the network. If both nodes can coexist on the same network with the same hardware address,use different network layer,they may operate without interference. This type of impersonation may bypass some IDSs, Finally, the impersonation attack may be used to bypass MAC filtering.

3 Load Attacks

In the OUI, the first octet contains addressing flags. The least significant bit of the first octet indicates a multicast packet. Every odd value for the first octet is a multicast. Attackers can quickly initiate a load attack because they can change their MAC address to be a broadcast or multicast address.

ARP AND RARP

The *Address Resolution Protocol* (ARP) is an example of a service access protocol, assists the network layer by converting IP addresses to hardware addresses. The *Reverse Address Resolution Protocol* (RARP) converts a hardware address to an IP address.

ARP packets include a function code such as ARP request, ARP reply, RARP request, and RARP reply. ARP and RARP requests are broadcast packets that include the query information. For

example, an ARP request contains an IP address. All nodes will receive the broadcast, but only one node will claimthe IP address. The node that identifies the IP address will transmit an ARP reply back to the querying host. The ARP table lists all nodes on the local network that have responded to ARP requests.

ARP Poisoning

Mapping IP addresses to hardware addresses (and vice versa) can add a delay to network connections. *ARP tables* contain a temporary cache . ARP packets are only required when a new IP address (or MAC address) lookup needs to be performed. these cached entries open the system to ARP poisoning,

ARP Poisoning Impact

The result from an ARP poisoning can range from a resource attack

Resource Attack

The amount of cache in ARP table is limited, sometimes ARP tables can be filled up with false entries. At that time there are only two options: ignore additional ARP entries or throw out old entries. If the system ignores additional entries, new nodes cannot be contacted and if the system throws the old entries , there will be a slower network performance due to constant ARP queries for each packet that the system wants to transmit.

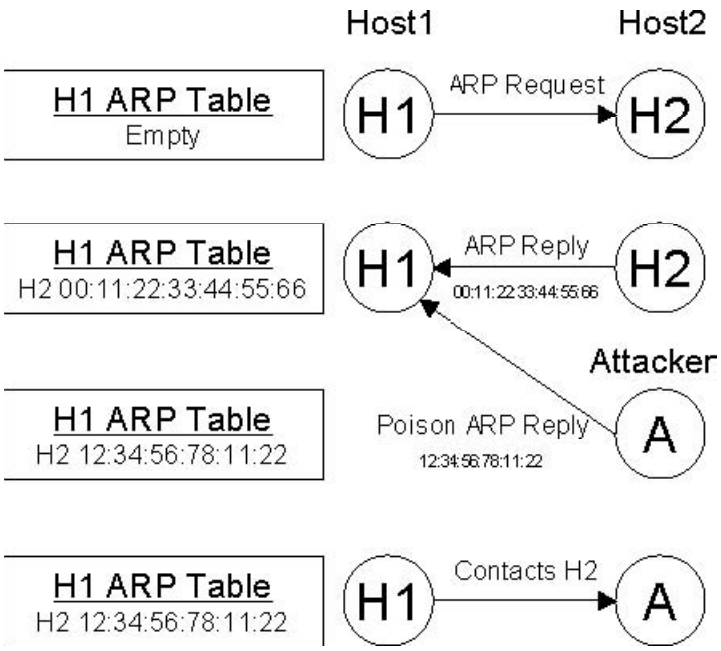
Denial of Service (DoS)

Newer ARP replies overwrite older ARP replies in the ARP table. If an entry in the ARP table is overwritten with a bad MAC address, then future connections to the overwritten node's IP address will fail.

Man-in-the-Middle (MitM)

The MitM attack routes all traffic through a hostile node. Similar to the DoS attack, the ARP table entry is overwritten with a different machine's MAC address. In this situation, the new node will receive all traffic intended for the old node. By poisoning both nodes the hostile node can establish a successful MitM.

FIGURE ARP poisoning as a MitM attack.



Mitigating ARP Poisoning

The few options for limiting the impact of ARP attacks include hard-coding ARP tables, expiring ARP entries, filtering ARP replies, and locking ARP tables.

Hard-Coding ARP Tables:

ARP tables can be populated statically using the operating system's arp command. This command statically sets a MAC address and IP address pair into the ARP table and prevents future modification.

Expiring ARP Entries

Cached entries in an ARP table may timeout. Expired entries, where the same MAC and IP address can be removed from the ARP table.

Filtering ARP Replies

ARP reply filtering does prevent unsolicited entries, it does not prevent new replies from overwriting existing entries.

Locking ARP Tables

ARP tables can be temporarily locked. In this situation, an established connection (such as an IP connection) locks the ARP table entry for a short duration. During this time, new ARP replies

cannot overwrite the locked table entry—ensuring that an established connection cannot be changed while it is established and mitigating MitM attacks.

NETWORK ROUTING

Network devices such as switches and bridges commonly use ARP packets. These systems are susceptible to ARP attacks such as switch poisoning and switch flooding.

Switches

switches are "smart" network devices. Switches maintain their own internal ARP table and associate each ARP reply with a physical port on the switch. As each packet is received, the switch identifies the destination MAC address and routes the packet to the specific port rather than sending it to every port. Switches only retransmit the packet to every port when the destination MAC address is unknown.A switch can identify MAC addresses in three ways:

ARP Requests

ARP Replies

Frame Headers

Bridges

Bridges link two networks that use the same data link protocol.

Switch Attacks

In any network node, switches and bridges are vulnerable to poisoning and flooding attacks.

Switch Poisoning Attacks

Switches maintain an ARP table to route traffic. ARP poisoning attack can corrupt the ARP table. The poisoning ARP reply can associate another node's MAC address with a different port. This effectively cuts off the victim node from the network and sends all traffic intended for the victim through the attacker's port. This attack allows connection hijacking.

Switch Flooding Attacks

Switches and bridges normally ensure that nodes only receive traffic intended for the local physical network. An attacker, using ARP poisoning, can flood a switch's ARP table. Because switches cannot afford to drop packets, In this state, all nodes receive all traffic; promiscuous mode can begin receiving all network .

ROUTING RISK:-

In the OSI model, network routers are the only option for communicating with distant networks. Router-based attacks appear in many forms: direct attacks, table poisoning, table flooding, metric attacks, and router looping attacks.

Direct Router Attacks

A *direct router attack* takes the form of a DoS or system compromise. A DoS prevents the router from performing the basic routing function, which effectively disables network connectivity. Historically, these attacks have been load based: if the network volume on a particular interface is too high, then the router will be unable to manage the traffic, including traffic from other network interfaces.

The router can be reconfigured to forward traffic to a different host, block traffic from specific hosts, or arbitrarily allocate new, covert subnets.

Router Table Poisoning

As with the data link layer's ARP table, the network layer's routing table is vulnerable to poisoning attacks. Few network protocols authenticate the network's traffic. Forged or compromised network traffic can overwrite, insert, or remove routing table entries.

Network layer protocols support dynamic routing tables, where the table is automatically generated and updated based on the observed network traffic. These protocols are more vulnerable because (1) a new node may generate poisoning data, and (2) few dynamic nodes are verifiable. Critical routers should use static routing tables to deter poisoning.

11.2.3 Router Table Flooding

Routers generally do not have large hard drives or RAM for storing routing tables. The routing table size is usually limited. Devices that do not use static routes must manage route expiration and table filling.

An attacker can generate fake data that the router will use to populate the routing table. When routing tables fill, the router has three options: ignore, discard oldest, or discard worst routes:

Ignore New Routes: Routers may choose to ignore new routes. An attacker will be unable to dislodge established table entries but can prevent new, valid entries from being inserted into the table.

Discard Oldest Routes: As with ARP tables, routing tables may discard routes that are not used. A large flooding attack can dislodge established table entries.

Discard Worst Routes: The router may consider routing table metrics. Less desirable paths can be replaced with more desirable routes. For a router table flooding attack to be successful, the attacker must know how the router responds to a full routing table. Most dynamic routing tables also support static entries. Critical routes should be configured as static entries.

Routing Metric Attacks

A *routing metric attack* poisons the dynamic metrics within a routing table. This attack can make a preferred path appear less desirable

Router Looping Attacks

Many network protocols attempt to detect and prevent network *loops*, where data forwarded though one interface is routed to a different interface on the same router. Network loops cause excessive bandwidth consumption and can result in feedback that consumes all available network bandwidth.

When a network router identifies a network loop, the path is removed from the routing table. A looping attack generates a false reply to a loop check, making the router falsely identify a network loop. The result is a desirable network path that is disabled.

. An attacker must control two systems—one on each router interface being attacked. As the loop-check query is observed by one system, a message is sent to the second system with the reply information.

The second system creates the false loop reply and sends it to the router. Many network protocols assign a *time-to-live* (TTL) value to packets. The TTL is decremented by each network relay. If the TTL reaches zero, then the packet is assumed to be undeliverable

ADDRESSING

. The two approaches for providing address information are numeric and name routing.

Numeric Addressing

Numeric addressing uses a sequence of numbers to identify a particular node on a specific network. This is analogous to contacting someone with a telephone number. The phone number routes the call

to a particular location.. Examples of numerical routing protocols include IP, IPv6, VINES, IPX, and X..25

.**X.25 -**The X.25 network layer protocol applies the concept of telephone network address routing to data connections.

IPX-*IPX* is a network protocol commonly associated with Novell NetWare. IPX uses a simplified addressing scheme..

VINES-Banyan *Virtual Integrated Network Service* (VINES) use an

addressing scheme similar to IPX but does not use a centralized router.

IP-The *Internet Protocol* (IP) uses four bytes to provide address information. The bytes are usually written in a dotted-decimal format

Name-Based Addressing

, Name-based network addressing provides more flexibility. Rather than allocating networks and subnets based on numerical addresses, *name-based addressing* uses text strings to identify each node. Longer strings permit more complicated networks. Two examples of name-based protocols for addressing

.1. AX.25 2. NBRP.

1.AX.25

AX.25 modifies X.25 networking to support name-based routing. Amateur radio packet networks commonly use this protocol.

2.NBRP

The *Name-Based Routing Protocol* (NBRP) is far more flexible than IP or IPv6 because any number of nodes and subnets can be derived from a parent subnet.

NBRP does not have address space limitations beyond the maximum length of a node's address.

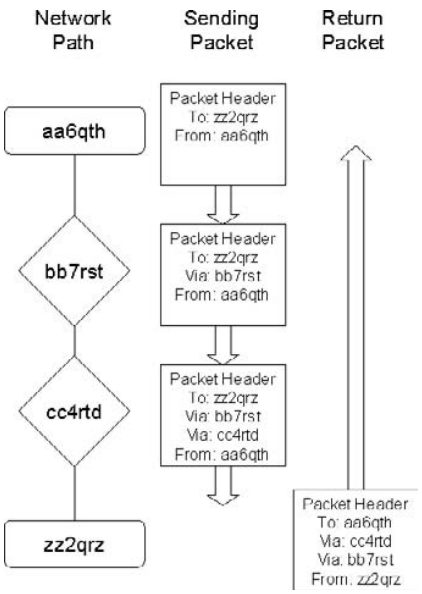


FIGURE - AX.25 address routing

FRAGMENTATION

Each network protocol has limitations concerning maximum packet size, and these may vary based on the physical network infrastructure. For example, most IP implementations use a default *maximum transmission unit* (MTU) of 1,500 bytes.

The network layer is responsible for fragmenting data from higher OSI layers into network packets and then reassembling the fragments upon receipt. Fragments may be managed using a sequence number or offset value.

Fragments and Sequence Numbers

The data link layer may not preserve the order of transmission, and alternate routes may shuffle the order that the packets are received. One method to ensure proper reassembly is to label each fragment with a sequence number. As each fragment is received, they are reassembled in order.

IPX is an example of a network protocol that uses sequence numbers for fragmentation tracking.

Fragments and Offsets

When using fragments with offsets, each packet contains an identification field, length, and memory offset value. The identification field identifies fragments from the same data block. Instead of including a sequence number, an offset is provided that identifies which part of the original

sequence appears in the packet. Finally, the length of the fragment packet is known. Each packet in the sequence contains a flag that identifies it as being part of a fragment; the last packet uses a flag identifying the end of the series

LISTING Sample Packet Fragmentation

Original data size: 3000 bytes.

Fragmented IP packets using offsets and an MTU of 1200 bytes:

Packet #1: length 1200, flag=fragment, offset=0

Packet #2: length 1200, flag=fragment, offset=1200

Packet #3: length 600, flag=last_fragment, offset=2400

Fragmented IPX packets using sequences and an MTU of 1200 bytes:

Packet #1: length 1200, sequence = 1 of 3

Packet #2: length 1200, sequence = 2 of 3

Packet #3: length 600, sequence = 3 of 3

SECURITY

The network layer offers many services for ensuring successful internetwork data transfers, but it does not describe methods for securing the network transfer. Most network layer protocols do not implement features for authenticating, validating, or otherwise protecting network data. The general risks that face the network layer include eavesdropping, impersonation, and insertion attacks.

Secure Protocols

The most common protocols, such as IP, IPX, and VINES, do not provide any security precautions beyond simple checksums. Checksums can detect data errors, they are trivial for an attacker to compute. For example, RFC1071 describes the checksum used within IP packets, including source code written in C and assembly language.

IPv6 and IPsec are the two best-known examples. IPsec is a combination of security-oriented additions to IP. For example, RFC2401, 2402, 2406, and 2409 describe authentication headers, data encapsulation, and key exchange methods applied to IP.

IPv6 also includes supports authentication and data encapsulation via encryption.

Network Incompatibility

The OSI stack is designed as a framework for combining independent protocols. One network protocol can replace another without modifying the higher OSI layer protocols. For example, the transport layer protocol UDP is network-protocol independent. UDP can use IPv6, IPX, VINES, or any other network layer protocol for internetwork support.

Most network applications include code for managing the transport and/or network layer protocols. Switching from IP to IPX can break the network implementation for Web browsers, email clients, and other network-oriented tools.

IPv6 supports data encryption for confidentiality, many higher-layer protocols and applications may not support IPv6.

Architecture

Reducing access to the physical layer lessens the risk from eavesdropping, intercept, and replay attacks. Data link layer is secured with an authenticated or encrypted tunnel, such as CHAP or a VPN, this only protects the data link connection. Hostile network layer traffic that can enter the data link tunnel is just as allowed and protected as regular network layer traffic.

Server Filtering

Filters operating on IP addresses can mitigate some authentication issues. For example, network servers (OSI layer 7) that rely on applications such as iptables or tcpwrapper can restrict access based on the client's IP address. It acts as a level of security-byobscurity, an attacker must know the acceptable network addresses to access the servers.

Firewalls and Egress Filtering

Routers normally pass traffic from one network interface to another. Firewalls can be implemented within routers and restrict access based on IP address. Although remote attackers may impersonate different IP addresses, they cannot receive the reply unless they are on the route between the target host and the impersonated network.

Filtering inbound traffic can reduce the success of an impersonation attack, but it does not prevent the network from originating an impersonation. *Outbound* (*egress*) *filtering* restricts packet relaying based on network addressing.The egress filter blocks obviously incorrect packets (due to misconfiguration or forgery) from being routed between networks.