Authentication and Remote Access

Chapter 11

Introduction

- **Remote access -** Enables users outside a network to have network access and privileges as if they were inside the network.
  - The user must establish a connection remotely, by
    - dialing in,
    - connecting using the Internet,
    - or connecting through a wireless connection.
  - Connectivity depends upon security requirements as well as hardware and software employed.

- **Requires two things:**
  1. A temporary network connection
  2. A series of protocols to negotiate privileges and commands

Establishing Proper Privileges

- To establish proper privileges, three steps are used (AAA):
  - Authentication
    - Matches user-supplied credentials to stored credentials – usually done with an account name and a password.
  - Authorization
    - Grants specific permissions based on the privileges held by the account.
  - Accounting
    - Keep detailed security logs to maintain an audit trail of tasks being performed.

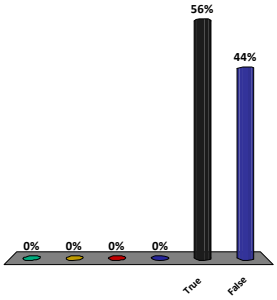
Authentication and Authorization are often confused with each other, **but they are different**

Identification

- Identification
  - The process of ascribing a computer ID to a specific user, computer, or network device.
  - Usually takes the form of a unique logon ID or userid.
    - Links the logon ID or user ID to previously assigned credentials.
  - User IDs should not be shared or descriptive of job function.
  - User identification enables **authentication and authorization** – the basis for **accountability.**
    - Accountability traces activities to individual users or computer processes.
      - **establishes responsibility for actions**.

Authentication grants specific permissions based on the privileges held by the account.

1.
2.
3.
4.
5. True
6. False



Authentication

- Deals with verifying the identity of a subject.
- Used to admit only valid users.

- To verify their identity, users can provide:
  - Something they know (password)
  - Something they have. (tokens/key cards)
  - Something about them (biometrics)

  - An additional category-
    - What users do (dynamic biometric)

Authentication

- Implementation Approaches
  - Kerberos
  - Certificates
  - Multifactor
  - Mutual authentication

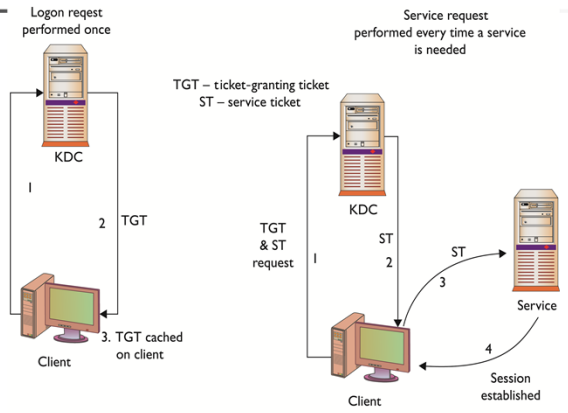
Authentication- Kerberos

- A network authentication protocol **designed for a client/server environment.**
- Uses strong encryption so that clients can prove their identity to a server and the server can in turn authenticate itself to the clients.
- Communicates via "tickets" that serve to prove the identity of users
- Built around the idea of **a trusted third party**, termed a **key distribution center (KDC),**
- **Key distribution center (KDC)** consists of two logically separate parts
  1. An **authentication server (AS)**
     - It is an entity trusted by both the client and the server the client wishes to access.
  2. A **ticket-granting server (TGS).**

Kerbosis- Tickets

- The basis for authentication in a Kerberos environment is a **ticket.**
- It eliminates the inherently insecure transmission of items such as a password that can be intercepted on the network.
- <u>The Kerberos server</u>
  - contains user IDs and hashed passwords for all users that will have authorizations to realm services.
  - also has shared secret keys with every server to which it will grant access tickets.
- <u>Tickets are used in a two-step process with the client.</u>
  - The first ticket is a *ticket-granting ticket (TGT)* issued by the AS to a requesting client.
  - The client can then present this ticket to the Kerberos server with a request for a ticket to access a specific server.
  - This *client-to-server ticket* (also called a *service ticket)* is used to gain access to a server's service in the realm.
  - **Tickets are time-stamped, and cannot be reused.**

Kerberos Operations



Client Authentication

1. The client sends a cleartext message to the AS requesting services on behalf of the user.
2. The AS checks to see if the client is in its database. If it is, the AS sends back ticket-granting ticket.
3. Once the client receives messages, it decrypts them to obtain the client/TGS session key.

Service Request

1. Using its TGT, client requests a service ticket (ST).
2. Client gets ST.
3. Client submits ST to service provider with request.
4. The server provides the requested services to the client.

Authentication- Certificates

- Digital certificates
  - A digital file that is sent as an attachment to a message and is used to verify that the message did indeed come from the entity it claims to have come from.
- Digital signature
  - An encrypted hash of an item that enables the recipient, using the public key, to verify that the original contents are not changed.

Authentication- Tokens

- A *token* is a hardware device that can be used in a challenge/response authentication process.
  - A hardware device that counts as both something-you-have and something-you-know.
- In this way, it functions as both a something-you-have and something-you-know authentication mechanism.
- A number is displayed on the screen that is used in conjunction with a user ID.
- The number changes at a constant interval.
- Even if someone finds the token, they won't know the corresponding user ID.

One-Time Password Generator Token

Authentication- Multifactor

- A term that describes the use of more than one authentication mechanism at the same time.
- Examples:
  - Biometric scanners and a PIN
  - Hardware tokens
  - ATM card and a PIN
  - Multifactor authentication increases the level of security.
    - It requires more than one mechanism to be spoofed for an unauthorized individual to gain access to a computer system or network.

Authentication- Single Sign-On

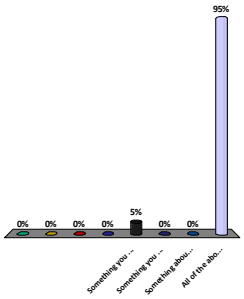
- As more and more systems are combined in daily use, users are forced to have multiple sets of credentials.
- A user may have to log into three, four, five, or even more systems every day just to do her job.
- A form of authentication that involves the transferring of credentials between systems.
- Single sign-on allows a user to transfer her credentials, so that logging into one system acts to log her into all of them.
- **Advantage-** Reduces login hassles:
  - Fewer usernames and passwords to remember
- **Disadvantage-** Inherently less secure:
  - If a login is compromised for one system, all systems the user can access are also compromised

Mutual Authentication

- A process in which each side of an electronic communication verifies the authenticity of the other.
- A common method involves using a secure connection, such as Secure Sockets Layer (SSL), to the server and a one-time password generator that then authenticates the client.

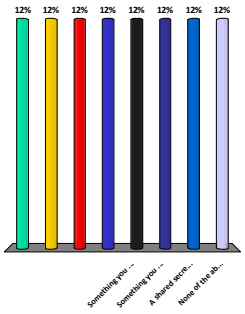
Authentication is typically based upon

1.
2.
3.
4.
5. Something you know
6. Something you have.
7. Something about you
8. All of the above



Passwords are an example of

1.
2.
3.
4.
5. Something you know
6. Something you have.
7. A shared secret
8. None of the above



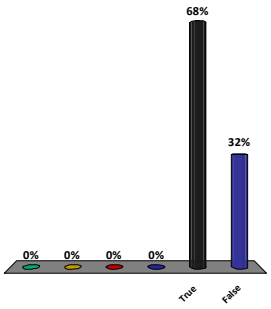
Authorization

Authorization

- The process of permitting or denying access to a specific resource
  - Determine whether a user has permissions for a particular object or resource.
- Once identity is confirmed via authentication, specific actions can be authorized or denied
  - Used to ensure that an authenticated user has permission to access the requested resources
- The separation of tasks, from identification to authentication to authorization, has several advantages.
  - Many methods can be used to perform each task, and on many systems several methods are concurrently present for each task.
  - Separation of these tasks into individual elements allows combinations of implementations to work together.
    - Any system or resource, be it hardware (router or workstation) or a software component (database system), that requires authorization can use its own authorization method once authentication is done

Authorization is the matching of user-supplied credentials to previously stored credentials on a host machine, and usually involves a username and password.

1.
2.
3.
4.
5. True
6. False



Access Control

- Access is the ability of a subject to interact with an object.
- Access controls define **what actions a user can perform** or **what objects a user can have access to**, because these controls assume that the identity of the user has been verified.
- An **access control matrix** shows **what can be accessed by whom**.

File ("object")

Process ("subject")

Table 11.1 An Access Control Matrix

	Process 1	Process 2	File 1	File 2	Printer
Process 1	Read, write, execute		Read, write	Read	Write
Process 2	Execute	Read, write, execute	Read, write	Read, write	Write

Each matrix entry is the access rights that subject has for that object

Models of Access Control

- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control (RBAC)
- Rule-based access control (RBAC)

Discretionary Access Control (DAC)

- **Discretionary Access Control (DAC)**
  - Restrict access to objects based on the identity of subjects and/or groups to which they belong.
  - In systems that employ discretionary access controls, the owner of an object can decide which other subjects may have access to the object and what specific access they may have.
    - Subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
  - Often use **access control lists**

- **Access Control List**
  - Contains the subjects with access rights to a particular object.
  - Identifies not only the subject but also the specific access the subject has for the object.
  - Types of access include read, write, and execute.

Mandatory Access Controls (MAC)

"A means of restricting access to objects based on
  - **the sensitivity** (as represented by a label) of the information contained in the objects and
  - **the formal authorization** (i.e., clearance) of subjects to access information of such sensitivity."

- The label attached to every subject and object identifies the level of classification for that object and the level that the subject is entitled.
  - For example, a subject with a "secret" label cannot access an object with a "top-secret" label.
- The security mechanism controls access to all objects, and individual subjects cannot change that access
  - The operating system decides whether access is to be granted to another subject.
  - The owner or the subject **cannot** determine whether access is to be granted to another subject.

Role-Based Access Control

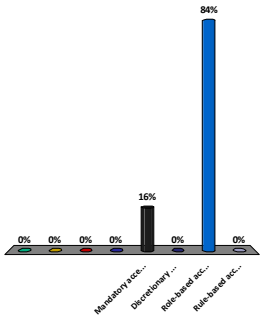
- Role-Based Access Control:
  - Instead of each user being assigned specific access permissions for the objects associated with the computer system or network, that **user is assigned a set of roles that the user may perform.**
  - **The roles are assigned the access permissions needed to perform tasks associated with the role.**
  - Users are granted permissions to objects in terms of the specific duties required—not of a security classification associated with individual objects.
- Simplifies access control:
  - People who need the same level of access are assigned to the same role, instead of having to give them all permission individually.

Rule-Based Access Control

- Rule-based access control (RBAC) again uses objects such as ACLs to help determine whether or not access should be granted,
- As compared to **Discretionary Access Control,** in this case, a series of rules is contained in the ACL and the determination of whether to grant access is made based on these rules.
  - An example: a rule that states that no employee may have access to the payroll file after hours or on weekends
- Can be used in addition to other access control methods or as a stand-alone method.

Which type of access control would be used to grant permissions based on the duties that must be performed?

1.
2.
3.
4.
5. Mandatory access control
6. Discretionary access control
7. Role-based access control
8. Rule-based access control



Remote Access Protocols

- IEEE 802.1X
- RADIUS
- Diameter
- TACACS+

IEEE 802.1x

- Describes methods used to authenticate a user **prior to granting access to network and the authentication server, such as a RADIUS server.**
- Once a client successfully authenticates itself to the 802.1X device, the switch opens ports for normal traffic.
  - At this point, the client can communicate with the system's AAA method, such as a RADIUS server, and authenticate itself to the network.
- 802.1X acts through an intermediate device, such as an edge switch, enabling ports to carry normal traffic if the connection is properly authenticated.
- This prevents unauthorized clients from accessing the publicly available ports on a switch, keeping unauthorized users out of a LAN.

IEEE 802.1x

- **Steps:**
  - A user requests access to an access point (known as the *authenticator*).
  - The access point forces the user into an unauthorized state that allows the client to send only an EAP (Extensible Authentication Protocol) start message.
  - The access point returns an EAP message requesting the user's identity.
  - The client returns the identity, which is then forwarded by the access point to the *authentication server*, which uses an algorithm to authenticate the user and then returns an accept or reject message back to the access point.
  - Assuming an accept was received, the access point changes the client's state to authorized and normal traffic can now take place.

RADIUS

- Remote Authentication Dial-In User Service (RADIUS)
  - A connectionless AAA protocol
  - Uses User Datagram Protocol (UDP) as its transport level protocol.
  - A Client Server Protocol
    - **The RADIUS client is a Network Access Server (NAS).**
      - Network access servers act as intermediaries, authenticating clients before allowing them access to a network.
    - **The RADIUS server is a process or daemon running on a UNIX or Windows NT machine.**
    - Communications between a RADIUS client and RADIUS server are encrypted.
    - Hence, communications between a RADIUS client (typically a NAS) and a RADIUS server are secure, but the communications between a user (typically a PC) and the RADIUS client are subject to compromise.

AAA - authentication, authorization and accounting

RADIUS Authentication

- A RADIUS user login authentication consists of a query (Access-Request) from the client and a corresponding response (Access- Accept or Access-Reject) from the server.
- The Access-Request message contains the username, encrypted password, NAS IP address, port, and contains information concerning the type of session the user wishes to initiate.
- Once the RADIUS server receives this information, it searches its database for a match on the username.
  - If a match is not found, either a default profile is loaded or an Access-Reject reply is sent.
  - If the entry is found, or the default profile is used, the next phase involves authorization, for in RADIUS, these steps are performed in sequence.

- RADIUS servers can allow for multiple methods of authentication. These include:
  - Point-to-Point Protocol (PPP)
  - Password Authentication Protocol (PAP)
  - Challenge-Handshake Authentication Protocol (CHAP)
  - UNIX login

RADIUS Authorization

- Performed in conjunction with authentication in response to a single Access-Request message
- Determines what parameters are returned to the client
- Parameters include:
  - Service type allowed
  - Protocols allowed
  - IP address to assign to the user
- These parameters are defined in the configuration information on the RADIUS client and server during setup.
  - Using this information, the RADIUS server returns an Access-Accept message with these parameters to the RADIUS client.

RADIUS Accounting

- RADIUS accounting functions are performed independently of authentication and authorization.
  - The accounting functions allow data to be transmitted at the beginning and the end of a session.
- It can indicate resource utilization, such as time and bandwidth.
- The accounting function uses a separate UDP port, 1813.
- Established to support ISPs in their user accounting
  - Time billing
  - Security logging

DIAMETER

- DIAMETER
  - Is TCP-based
  - Operates in the same way as the RADIUS client/server configuration.
  - Improves upon RADIUS, resolving interoperability issues
  - Has an improved method of encrypting message exchanges to prohibit replay and man-in-the-middle attacks.
  - Has more extensive capabilities in authentication, authorization, and accounting.

Authentication Protocols

Authentication Protocols

- Numerous authentication protocols exist. Some of them include:
  - L2TP (layer 2 tunneling protocol) and PPTP (Point to point tunneling protocol)
  - PPP
  - EAP
  - CHAP
  - SSH

L2TP and PPTP

- Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP) are both OSI Layer 2 tunneling protocols.
- Tunneling is the encapsulation of one packet within another:
  - This allows you to hide the original packet from view
  - Provides greater security

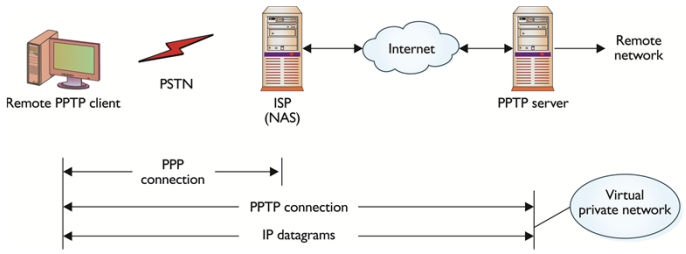
PPP (Point-to-Point Protocol)

- Point-to-Point Protocol (PPP) is an OSI Layer 2 protocol used to connect devices.
- These protocols are used to authenticate the peer device, not a user of the system
- Used for establishing dial-in connections over serial lines or Integrated Services Digital Network (ISDN) services.
- Has several authentication mechanisms:
  - PAP- Password Authentication Protocol
  - CHAP- Challenge handshake Authentication Protocol
  - EAP.- Extensible Authentication Protocol

PPTP (Point to point Tunneling Protocol)

- An extension of PPP that enables the creation of virtual private networks (VPNs)
- Enables the secure transfer of data from a remote PC to a server by creating a VPN across a TCP/IP network
- Involves three computers:
  - The PPTP client
  - The NAS (usually an ISP)
  - The PPTP server

PPTP Communication Diagram

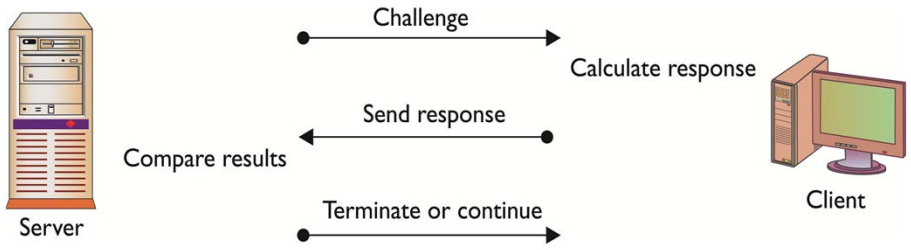


1. First the client makes a PPP connection to a NAS, typically an ISP.
2. Once the PPP connection is established, a second connection is made over the PPP connection to the PPTP server.
3. This second connection creates the VPN connection between the remote client and the PPTP server.
4. This connection acts as a tunnel for future data transfers.

CHAP (Challenge handshake Authentication Protocol)

- CHAP provides authentication periodically through the use of a challenge/response system – a three-way handshake.
  - The initial challenge (a randomly generated number) is sent to the client.
  - The client uses a one-way hashing function to calculate the response and then sends this back.
  - The server compares the response with the response calculated by it.
  - If it matches, the communication continues.
  - If the two values do not match, the connection is terminated.
  - This mechanism relies on a shared secret between the two entities so that the correct values can be calculated.

CHAP Challenge/Response Sequence



NTLM

- **NT LAN Manager** is an authentication protocol designed by Microsoft for use with the Server Message Block (SMB) protocol.
  - SMB is an application-level network protocol primarily used for sharing of files and printers in Windows-based networks
- Is used when:
  - Authenticating to a server using an IP address
  - Authenticating to a server that belongs to a different Active Directory forest
  - Authenticating to a server that doesn't belong to a domain
  - No Active Directory domain exists

L2TP (*Layer 2 Tunneling Protocol*)

- Designed for use across all kinds of networks, including ATM and Frame Relay
- Can be implemented by both hardware and software
- Designed to work with established AAA services such as RADIUS

Telnet

- Allows users to log in remotely and access resources as if they had a local terminal connection
- Offers little security, as usernames, passwords, and all data are passed in clear text over the TCP/IP connection
- Access control to Telnet on machines and routers should be implemented when they are first set up
- Uses TCP port 23

Secure Shell (SSH)

- Secure Shell is a protocol series designed to facilitate secure network functions across an insecure network.
- SSH was designed as a replacement for the insecure telnet.
- SSH opens a secure transport channel between machines by using an SSH daemon on each end.
  - These daemons initiate contact over TCP port 22 and then communicate over higher ports in a secure mode.
- The SSH protocol has facilities to encrypt data automatically, provide authentication, and compress data in transit.
- It can support strong encryption, cryptographic host authentication, and integrity protection.

VPNs

- A virtual private network is a secure network built on top of a physical network.
- Security of VPN lies in the encryption of packet contents between the endpoints that define the VPN
  - The packet contents between the VPN are encrypted, to an outside observer on the public network, the communication is secure.
- It's not a protocol in and of itself, but rather a method of using protocols to achieve secure communications.
- It is typically used to access a corporate data network from a home PC across the Internet.

Ipsec (Internet Protocol Security)

- Internet Protocol Security (IPsec)
  - A set of protocols developed to securely exchange packets at the network layer (Layer 3) of the OSI model
  - Content protection
    - The transport method encrypts only the data portion of a packet, thus enabling an outsider to see source and destination IP addresses.
    - Protection of the data portion of a packet is referred to as content protection
  - Context protection
    - Tunneling provides encryption of source and destination IP addresses, as well as of the data itself.
    - It provides the greatest security, but can be done only between IPsec servers (or routers) because the final destination needs to be known for delivery.
    - Protection of the header information is known as context protection

Security Associations

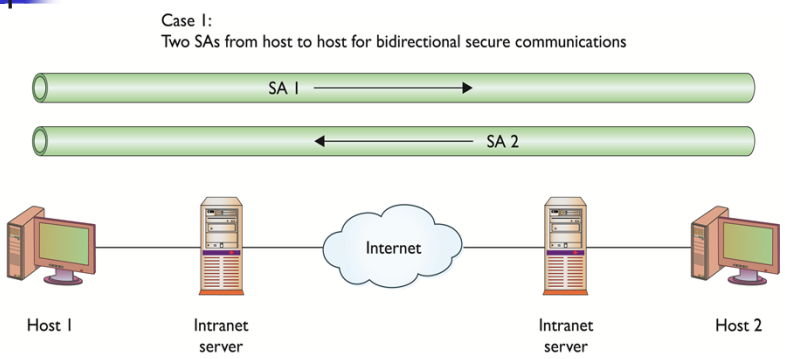
- Security Associations
  - A formal manner of describing the necessary and sufficient portions of the IPsec protocol series to achieve a specific level of protection.
  - Because many options exist, communicating parties must agree on the use of the protocols that are available, and this agreement is referred to as a security association
  - SAs exist both for integrity-protecting systems and confidentiality-protecting systems.
  - In each IPsec implementation, a security association database (SAD) defines parameters associated with each SA.
  - The SA is a one-way (simplex) association, and if two-way communication security is desired, two SAs are used—one for each direction.

IPsec Configurations

- Four basic configurations can be applied to machine-to-machine connections.

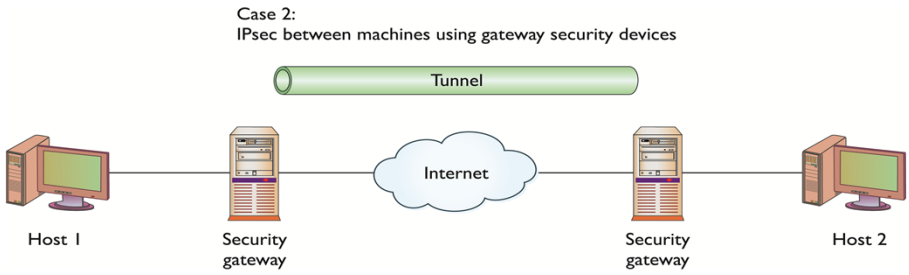
  1. Host-to-host connection, wherein the Internet is not part of the SA between the machines.
  2. Two security devices in the stream secure the network between them.
  3. A combination of the first two configurations.
  4. User establishes an SA with the security gateway and then a separate SA with the desired server.

A Host-to-Host Connection Between Two Machines



•The simplest is a host-to-host connection between two machines.
•In this case, the Internet is not a part of the SA between the machines.
•If bidirectional security is desired, two Sas are used. The SAs are effective from host to host.

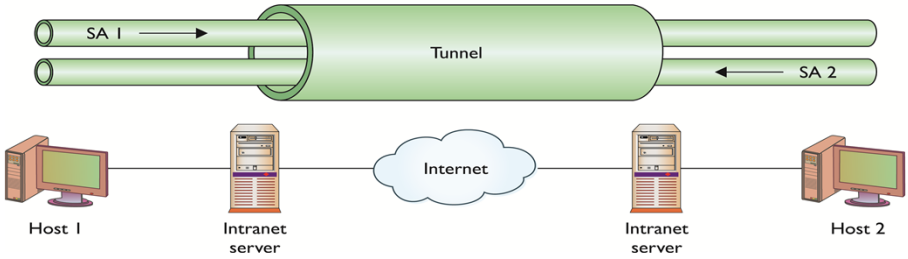
Two Security Gateways with a Tunnel Across the Internet



- The second case places two security devices in the stream, relieving the hosts of the calculation and encapsulation duties.
- These two gateways have an SA between them.
- The network is assumed to be secure from each machine to its gateway, and no IPsec is performed across these hops.

A Tunnel Inside a Tunnel

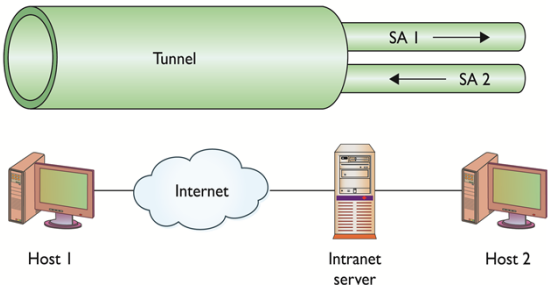
Case 3:
Separate IPsec tunnels, host to host and gateway to gateway



- The third case combines the first two.
- A separate SA exists between the gateway devices, but an SA also exists between hosts.
- This could be considered a tunnel inside a tunnel.

Tunnel from Host to Gateway

Case 4:
Tunnel from host to gateway
Optional: Two SAs for bidirectional secure communications



- Remote users commonly connect through the Internet to an organization's network.
- The network has a security gateway through which it secures traffic to and from its servers and authorized users.
- In the last case, the user establishes an SA with the security gateway and then a separate SA with the desired server, if required.

IPsec Security

- Uses two protocols to provide traffic security:
  - Authentication Header (AH)
    - A header added to a packet for the purpose of integrity checking
    - IPsec AH protects integrity, but it does not provide privacy.
  - Encapsulating Security Payload (ESP)
    - A method of encrypting the data portion of a datagram to provide confidentiality.
    - IPsec ESP provides confidentiality, but it does not protect integrity of the packet.
  - To cover both privacy and integrity, both headers can be used at the same time.

IPsec Security

- Uses three protocols: for key management and exchange
  - Internet Security Association and Key Management Protocol (ISAKMP)
  - Oakley
  - Secure Key Exchange Mechanism for Internet (SKEMI)

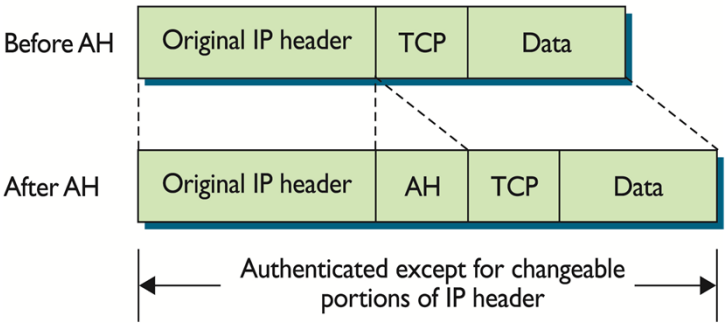
- These key management protocols can be collectively referred to as Internet **Key Management Protocol (IKMP) or Internet Key Exchange (IKE).**

IPsec Security

- IPsec does not define specific security algorithms, nor does it require specific methods of implementation.
- IPsec is an open framework that allows vendors to implement existing industry-standard algorithms suited for specific tasks.
  - This flexibility is key in IPsec's ability to offer a wide range of security functions.
  - IPsec allows several security technologies to be combined into a comprehensive solution for network-based confidentiality, integrity, and authentication.

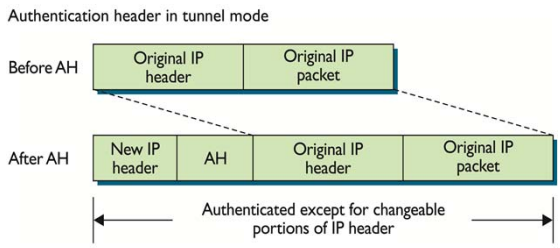
AH (Authentication Header) in Transport Mode

Authentication header in transport mode



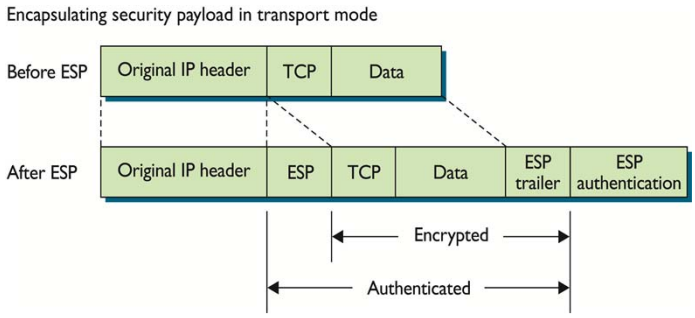
When AH is in transport mode, the original IP header is exposed, but its contents are protected via the AH block in the packet.

AH (Authentication Header) in Tunnel Mode



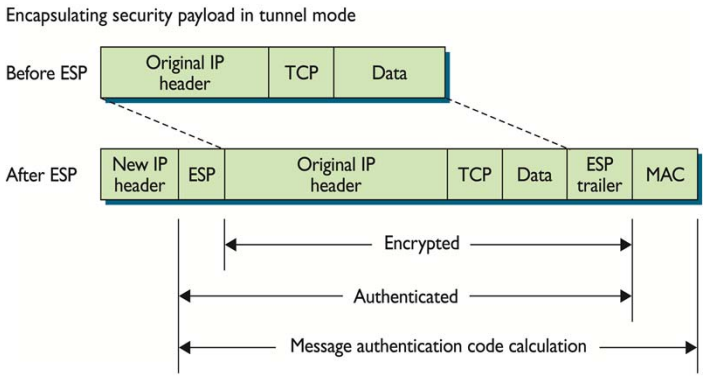
- Tunneling is a means of encapsulating packets inside a protocol that is understood only at the entry and exit points of the tunnel.
  - Provides security during transport in the tunnel, because outside observers cannot decipher packet contents or even the identities of the communicating parties.
- When AH is employed in tunnel mode, portions of the outer IP header are given the same header protection that occurs in transport mode, with the entire inner packet receiving protection.
- The true source and destination information is contained in the inner IP header, which is encrypted in the tunnel.
- The outer IP header contains the addresses of the endpoints of the tunnel.

ESP (Encapsulating Security Payload) in Transport Mode

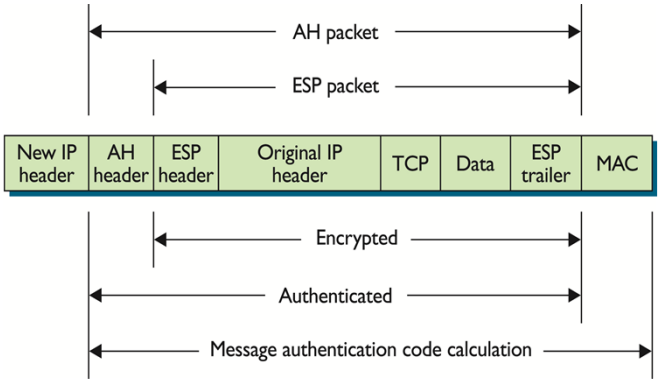


- ESP provides a means of encrypting the packet's contents.
- In this case, in transport mode, the datagram contents are encrypted and authenticated via the ESP header and footer/trailer that are inserted into the datagram.

ESP (Encapsulating Security Payload) in Tunnel Mode



- ESP affords the same encryption protection to the contents of the tunneled packet, which is the entire packet from the initial sender.



Together, in tunnel mode, AH and ESP can provide complete protection across the packet.
The specific combination of AH and ESP is referred to as a *security association* in IPsec.

Vulnerabilities

- The primary vulnerability associated with methods of remote access is the passing of critical data.
  - Plaintext passing of passwords provides no security if the password is sniffed, and sniffers are easy to use on a network.
  - Even plaintext passing of usernames gives away data that can be correlated and possibly used.
  - This is one of the flaws with RADIUS and TACACS+, as they have a segment unprotected.
- The strength of the encryption algorithm is also a concern.
  - Should a specific algorithm or method prove to be vulnerable (such as WEP), services that rely solely on it are also vulnerable.
  - To get around this dependency, many of the protocols allow numerous encryption methods, so that should if one protocol is vulnerable, another protocol can be used to restore security

Vulnerabilities

- The primary vulnerability associated with many of these methods of remote access is the passing of critical data in clear text.
  - Plaintext passing of passwords provides no security if the password is sniffed, and sniffers are easy to use on a network.
  - Even plaintext passing of user IDs gives away information that can be correlated and possibly used by an attacker.
  - Plaintext credential passing is one of the fundamental flaws with Telnet and is why SSH was developed.
- The strength of the encryption algorithm is also a concern.
  - Should a specific algorithm or method prove to be vulnerable, services that rely solely on it are also vulnerable.
  - To get around this dependency, many of the protocols allow numerous encryption methods, so that should one prove vulnerable, a shift to another restores security.

Vulnerabilities

- As with any software implementation, there always exists the possibility that a bug opens the system to attack clients, servers and more.
  - Bugs can open the system to attack
  - Vendor responsiveness to fixing the bugs once they are discovered