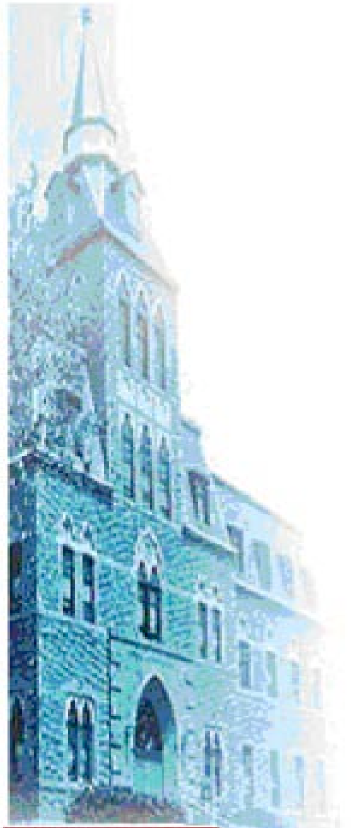


STEVENS
Institute of Technology

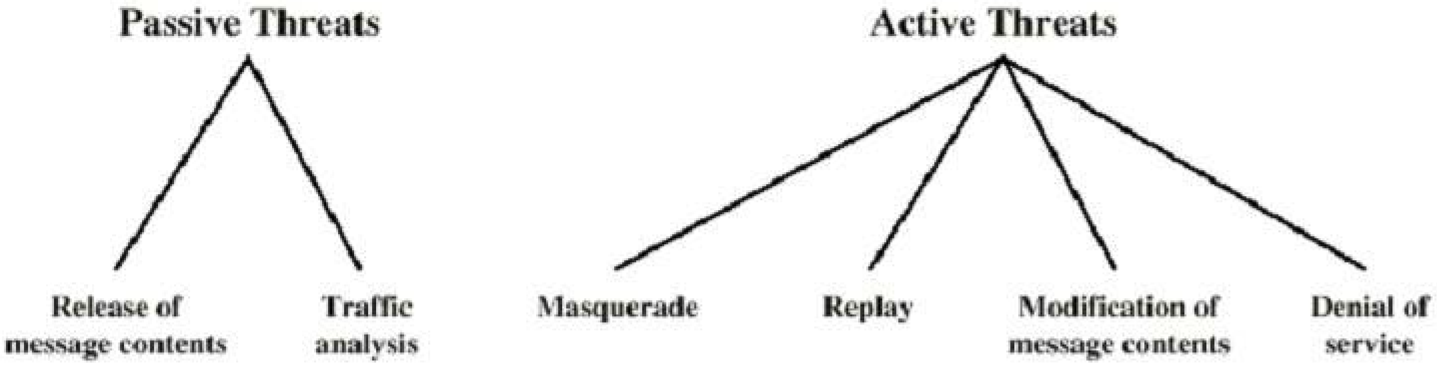
Network Security

Security Requirements And Attacks

- Computer and network security address three requirements:
- Confidentiality: Requires that data only be accessible for reading by authorized parties.
- Integrity: Requires that data can be modified only by authorized parties.
- Availability: Requires that data are available to authorized parties.

Attacks

- Passive attacks
- Active attacks



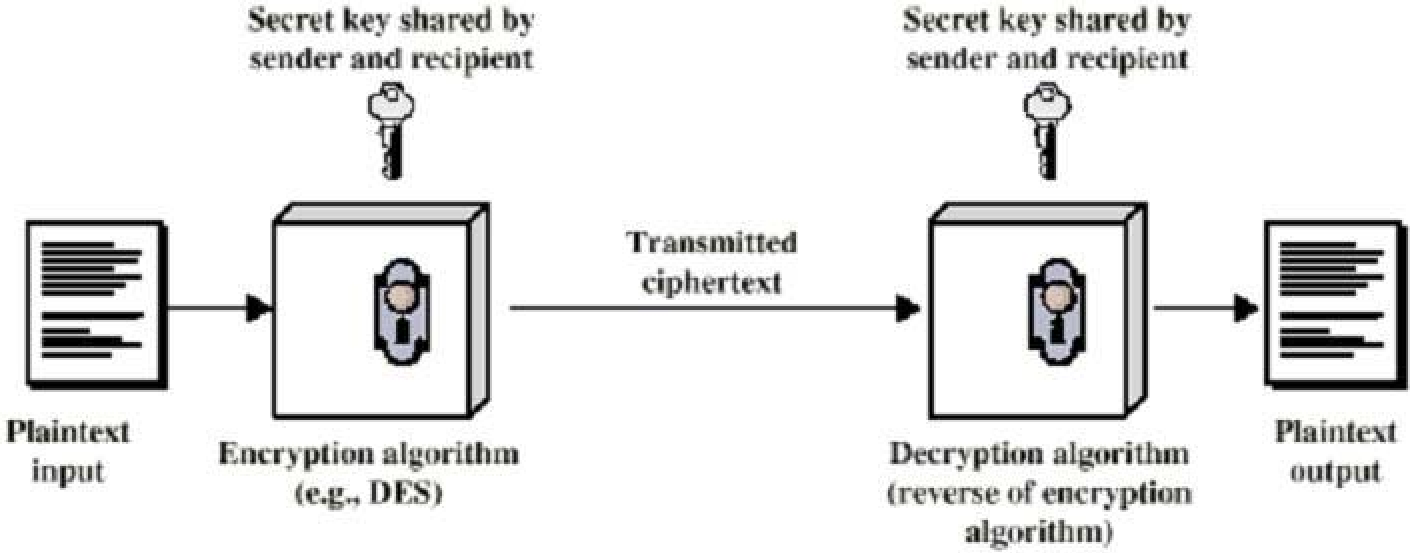
Passive Attacks:

- The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.
- A second passive attack, traffic analysis, is more subtle. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication.

Active Attacks:

- A masquerade takes place place when one entity pretends to be a different entity.
- Replay involves the passive capture of the data unit and its subsequent retransmission to produce an unauthorized effect.
- Modification of messages simply means that some portion of a legitimate message is alternate, or that messages are delayed or reordered, to produce an unauthorized effect.
- A denial of service attack prevents or inhibits the normal use or management of communications facilities.

Confidentiality with Conventional Encryption


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Conventional Encryption:

- A conventional encryption scheme has five ingredients:
  - Plaintext: This is the original message or data that is fed into the algorithm as input.
  - Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.
  - Secret key: The secret key is also input to the encryption algorithm. The exact sustitutions and transformations performed by the algorithm depend on the key.
  - Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
  - Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Two Requirements for Secure Use of Conventional Encryption

- We need a strong encryption algorithm. The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number or ciphertexts together with the plaintext that produced each ciphertext.
- Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

Cryptanalytic Attacks

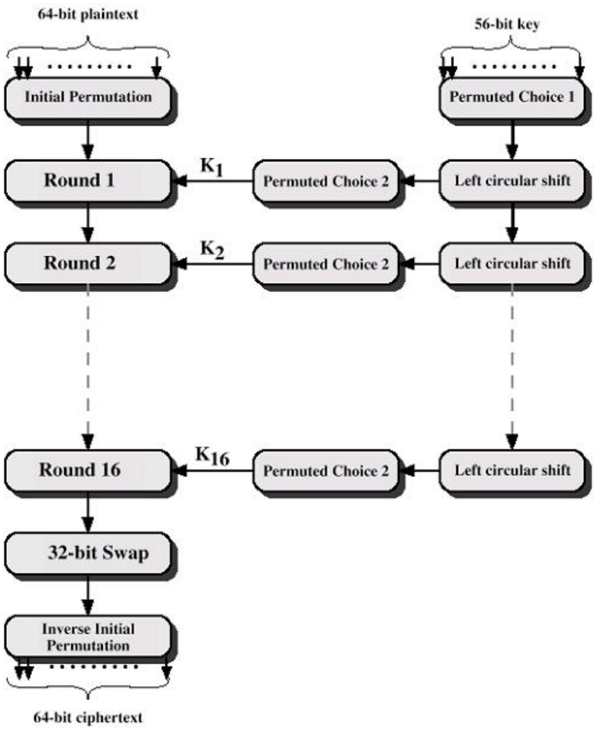
- Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs.

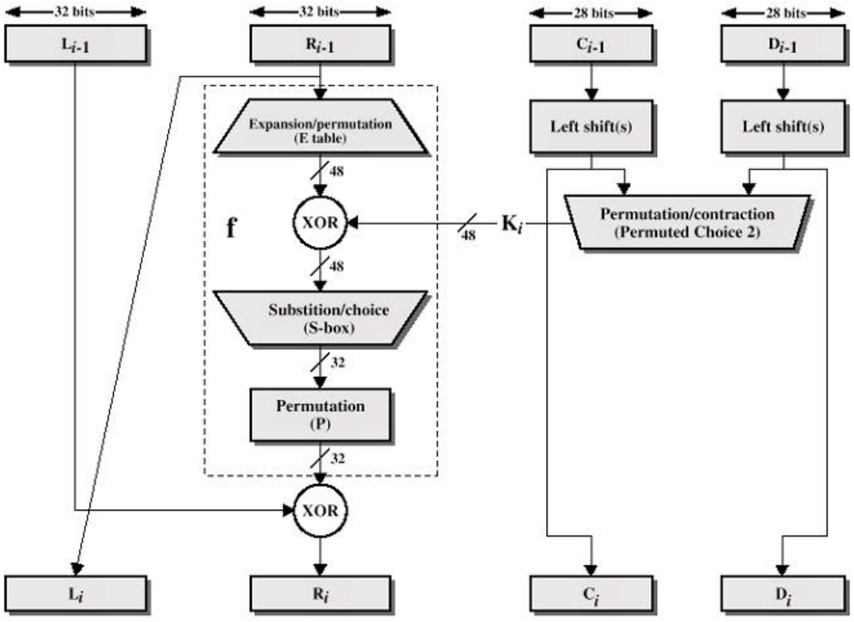
- The second method, known as the brute-force attack, is to try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

Key Size (bits)	Number of alternative Keys	Time Required at 1 Encryption/s	Time Required at 10^6 Encryptions/s
32	$2^{32} = 4.3 * 10^9$	2^{31}s = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 * 10^{16}$	2^{55}s = 1142 years	10.01 hours
128	$2^{128} = 3.4 * 10^{38}$	2^{127}s = 5.4 * 10^{24}years	5.4 * 10^{18} years
168	$2^{168} = 3.7 * 10^{50}$	2^{167}s = 5.9 * 10^{36}years	5.9 * 10^{30} years

Encryption Algorithms:

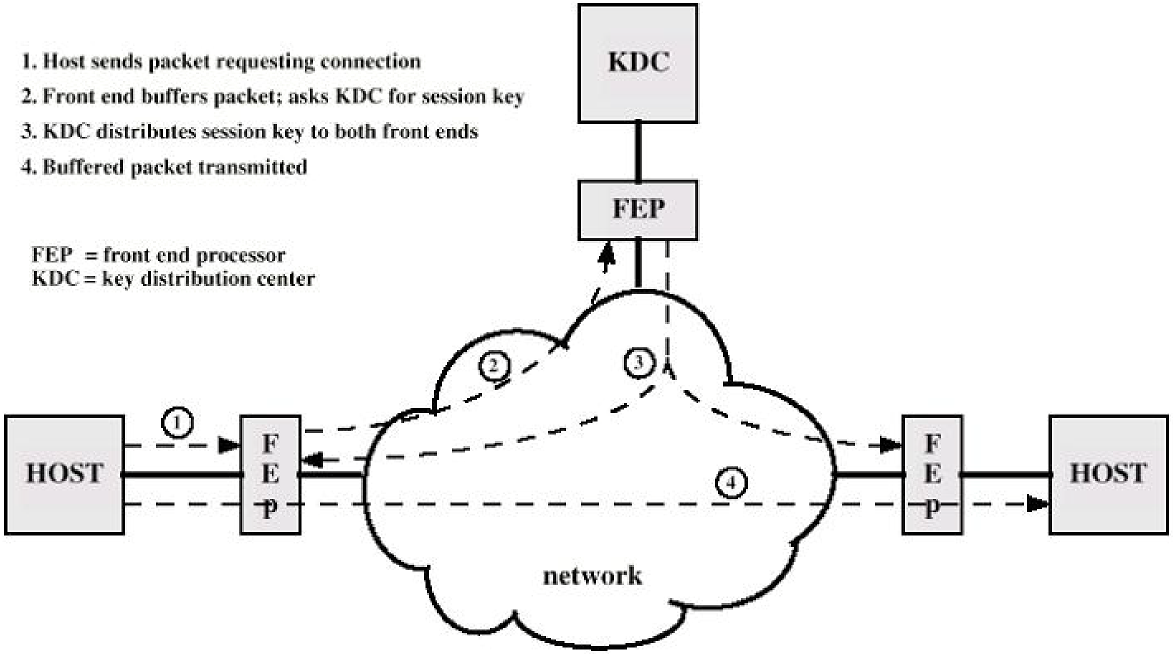
- The most commonly used conventional encryption algorithms are block ciphers. A block cipher processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block. The two most important conventional algorithms, both of which are block ciphers, are DES and TDEA.





Location of Encryption Devices

- In using encryption , we need to decide what to encrypt and wehre the encryption gear should be located. As the following figure indicates, there are two fundamental alternatives: link encryption and end-to-end encryption.


1. Host sends packet requesting connection
2. Front end buffers packet; asks KDC for session key
3. KDC distributes session key to both front ends
4. Buffered packet transmitted
FEP = front end processor
KDC = key distribution center
KDC
FEP
HOST
FEP
FEP
HOST
1
2
3
4
network

Location of Encryption Devices Cont’d

- With link encryption, each vulnerable communications link is equipped on both ends with an encryption device. Thus, all traffic over all communications links is secured. One disadvantage of this approach is that the message must be decrypted each time it enters a packet switch; this is necessary because the switch must read the address (virtual circuit number) in the packet header to route the packet. Thus, the message is vulnerable at each switch.

- With the end-to-end encryption, the encryption process is carried out at the two end systems. The source host or terminal encrypts the data. The destination shares a key with the source and so is able to decrypt the data. This approach would seem to secure the transmission against attacks on the network links or switches.

Location of Encryption Devices Cont’d

- Data are transmitted over such a network in the form of packets, consisting of a header and some user data. Suppose that the host encrypts the entire packet, including the header. The packet-switching node will receive an encrypted packet and be unable to read the header. Therefore, it will not be able to route the packet. Thus, with end-to-end encryption, the user data are secure.

- However, the traffic pattern is not, because packet headers are transmitted in the clear. When both forms are employed, the host encrypts the user data portion of a packet using an end-to-end encryption key. The entire packet is then encrypted using a link encryption key. As the packet traverses the network, each switch decrypts the packet using a link encryption key to read the header. Now the entire packet is secure except for the time that the packet is actually in the memory of a packet switch, at which time the packet header is in the clear.

Key Distribution

- For conventional encryption to work, the two parties to a secure exchange must have the same key, and that key must be protected from access by others. The strength of any cryptographic system rests with the key distribution technique, a term that refers to the means of delivering a key to two parties that wish to exchange data, without allowing others to see the key. Key distribution can be achieved in a number of ways. For two parties A and B:
- A key could be selected by And physically delievered to B
- A third party could select the key and physically deliver it to A and B
- If A and B have previously and recently used a key, one party could transmit the new key to the other, encrypted using the old key
- If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B.

Key Distribution Cont'd

- Session Key: When two end systems (hosts, terminals) wish to communicate, they establish a logical connection (eg: virtual circuit). For the duration of that logical connection, all user data are encrypted with a one-time session key. At the conclusion of the session, or connection, the session key is destroyed.

- Permanent Key: A permanent key is a key used between entities for the purpose of distributing session keys.

- Key Distribution Center: The key distribution center determines which systems are allowed to communicate with each other. When permission is granted for two systems to establish a connection, the key distribution center provides a one-time session key for that connection.

- Front-end processor: The front end processor performs end-to-end encryption and obtains session keys on behalf of its host terminal.

Traffic Padding

- It is still possible in those circumstances for an attacker to assess the amount of traffic on a network and to observe the amount of traffic entering and leaving each end system. An effective countermeasure to this attack is traffic padding.

- Traffic padding is a function that produces ciphertext output continuously even in the absence of plaintext. When input plaintext is not present, the random data are encrypted and transmitted.

Message Authentication And Hash Functions

- Encryption protects against passive attack (eavesdropping). A different requirement is to protect against active attack. Protection against such attacks is known as message authentication.
- Approaches to Message Authentication
- Authentication Using Conventional Encryption:
- If we assume that only the sender and receiver share a key (which is as it should be), then only the genuine sender and receiver would be able successfully to encrypt a message for the other participant.

Message Authentication And Hash Functions Cont’d

- Message Authentication without Message Encryption
  - There are a number of applications in which the same message is broadcast to a number of destinations (for example, notification to users that the network is now unavailable or an alarm signal in a control center). It is cheaper and more reliable to have only one destination responsible for monitoring authenticity. Thus, the message must be broadcast in plaintext with an associated message authentication tag. The responsible system performs authentication. If a violation occurs, the other destination systems are alerted by a general alarm.
  - Another possible scenario is an exchange in which one side has a heavy load and cannot afford the time to decrypt all incoming messages. Authentication is carried out on a selective basis, with messages chosen at random for checking.
  - Authentication of a computer program in plaintext is an attractive service. The computer program can be executed without having to decrypt it every time, which would be wasteful of processor resources. However, if a message authentication tag were attached to the program, it could be checked whenever assurance is required of the integrity of the program.

Message Authentication Code

- This technique assumes that two communicating parties, say A and B, share a common secret key KAB. When A has a message to send to B, it calculates the message authentication code as a function of the message and the key:

MACM = F(KAB, M).

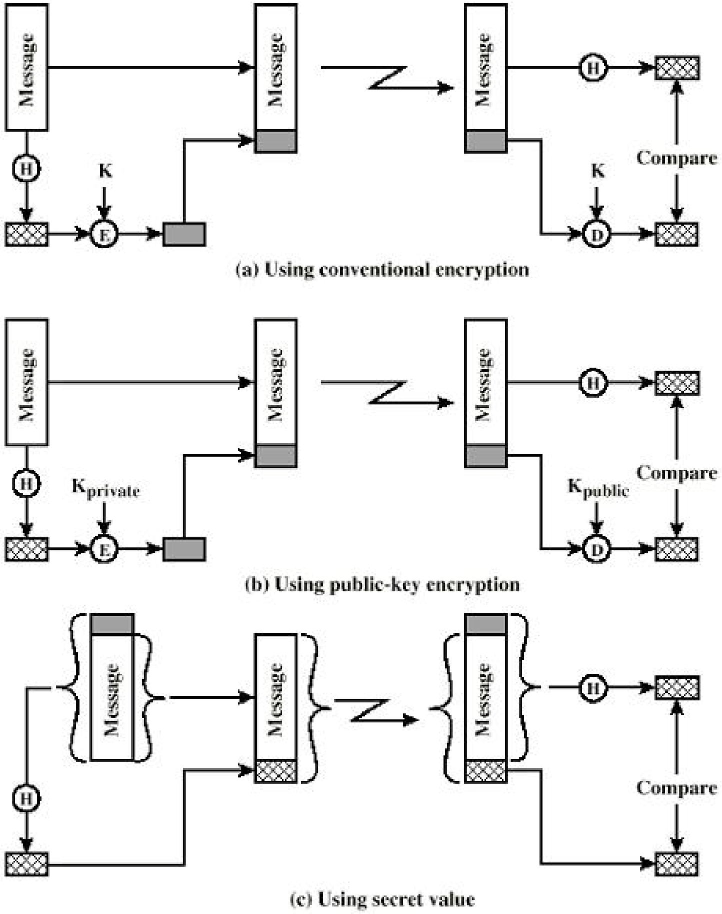
- The message plus code are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new message authentication code. The received code is compared to the calculated code.

One Way Hash Function:

- A variation on the message authentication code that has received much attention recently is the one-way hash function.

- As with the message authentication code, a hash function accepts variable-size message M as input and produces a fixed-size message digest H(M), as output. Unlike the MAC, a hash function does not also take a secret key as input.

- To authentication a message, the message digest is sent with the message in such a way that the message digest is authentic. The following figure illustrates three ways in which the message can be authenticated.



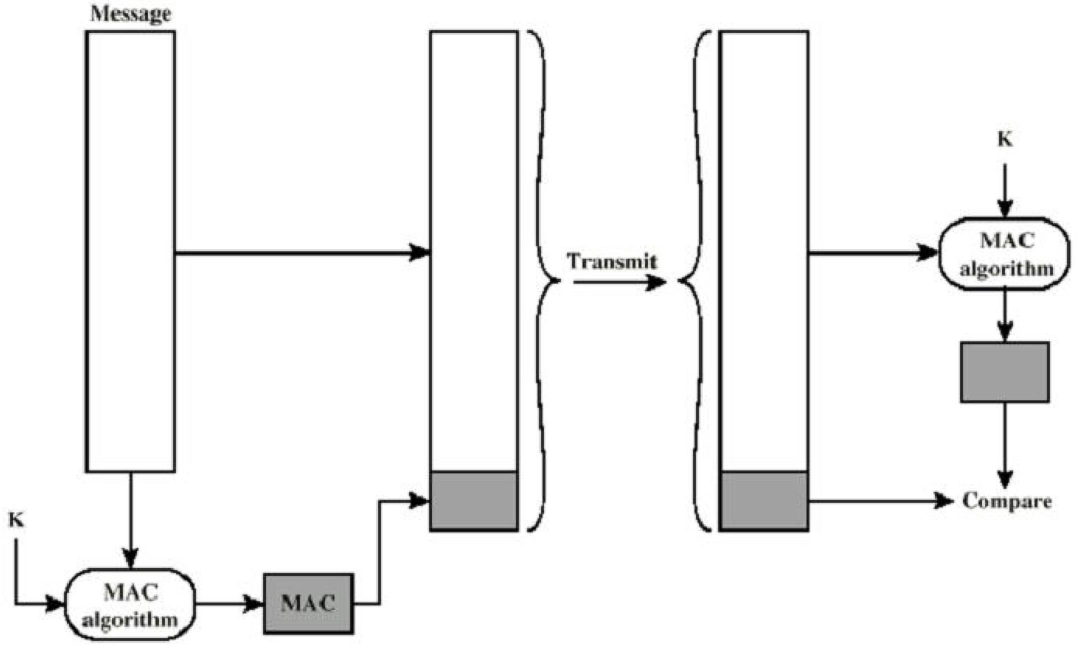
(a) Using conventional encryption

(b) Using public-key encryption

(c) Using secret value

Message Authentication Code Cont’d

- A number of algorithms could be used to generate the code. The National Bureau of Standards, in its publication DES Modes of Operation, recommends the use of DEA. A 16- or 32-bit code is typical. The process just described is similar to encryption. One difference is that the authentication algorithm need not be reversible as it must be for decryption.



Secure Hash Functions

- Hash function requirements
- To be useful for message authentication, a hash function H must have the following properties:
  - H can be applied to a block of data of any size.
  - H produces a fixed-length output.
  - H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
  - For any given code h, it is computationally infeasible to find x such that H(x) = h.
  - For any given block x, it is computationally infeasible to find y not equal to x with H(y) = H(x).
  - It is computationally infeasible to find any pair (x,y) such that H(x) = H(y).
- The first three properties are requirements for the practical application of a hash function to message authentication. A hash function that satisfies the first five properties in the preceding list is referred to as a weak has function. If the sixth property is also satisfied, then it is referred to as a strong hash function. The sixth property protects against a sophisticated class of attack known as the birthday attack.

IPv4 AND IPv6 SECURITY

- IPSec provides the capability to secure communications across a LAN, across private and public WAN's, and across the Internet. Examples of its use include the following:

- Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.

- Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.

- Establishing extranet and intranet connectivity with partners: IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

- Enhancing electronic commerce security: Even though some Web and electronic commerce applications have built-in security protocols, the use of IPSec enhances that security.

- The principal feature of IPSec that enables it to support these varied applications is that it can encrypt and/or authenticate all traffic at the IP level. Thus, all distributed applications, including remote logon, client/server, email, file transfer, Web access, and so on, can be secured.

The Scope of IPSec

- IPSec provides three main facilities: an authentication-only function referred to as Authentication Header (AH), a combined authentication/encryption function called Encapsulating Security Payload (ESP), and a key exchange function.

- For virtual private networks, both authentication and encryption are generally desired, because it is important both to
  - (1)assure that unauthorized users do not penetrate the virtual private network and
  - (2) assure that eavesdroppers on teh Internet cannot read messages sent over the virtual private network.

- Because both features are generally desirable, most implementations are likely to use ESP rather than AH. The key exchange function allows for manual exchange of keys as well as an automated scheme.

Security Associations

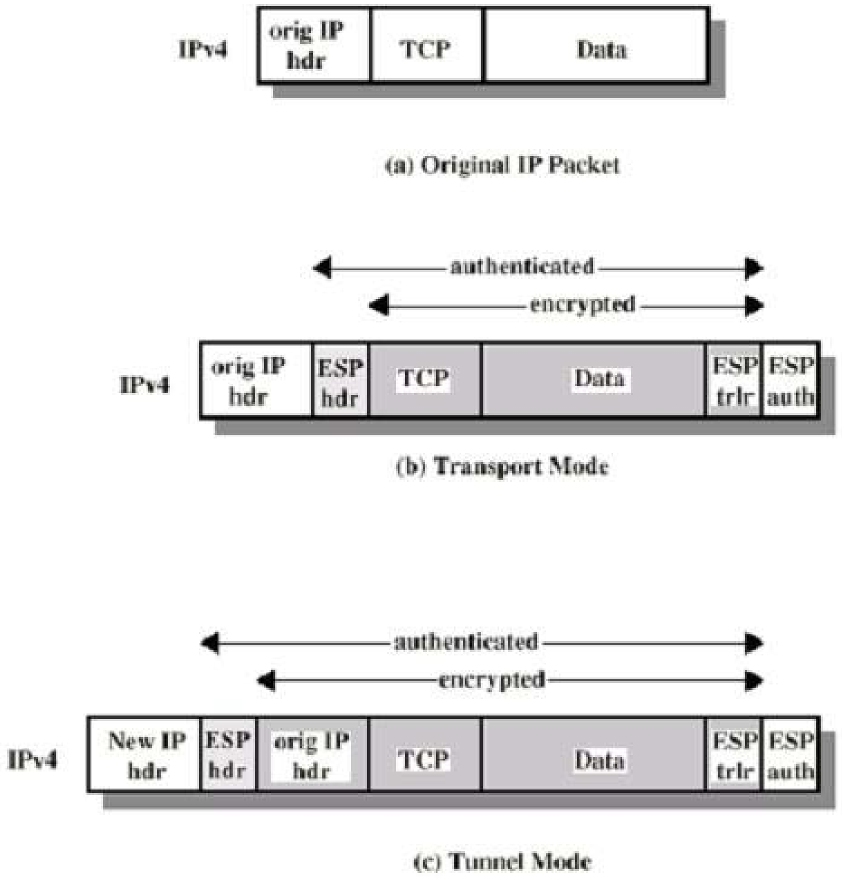
- A key concept that appears in both the authentication and confidentiality mechanisms for IP is the security association (SA). An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it. If a peer relationship is needed, for two-way secure exchange, then two security associations are required. Security services are afforded to the SA for the use of AH or ESP, but not both.
- A security association is uniquely identified by 3 parameters:
- Security parameters index (SPI): A bit string assigned to this SA and having local significance only. The SPI carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
- IP destination address: Currently, only unicast addresses are allowed; this is the address of the destination endpoint of the SA, which may be an end user system or a network system such as a firewall or router.

Security Associations Cont’d

- Security protocol identifier: This indicates whether the association is an AH or ESP security association.
- Hence, in any IP packet, the security association is uniquely identified by the Destination Address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP). An IPSec implementation includes a security association data base that defines the parameters associated with each SA. A security association is defined by the following parameters:
- Sequence number counter: A 32-bit value used to generate the sequence number field in the AH or ESP headers.
- Sequence counter overflow: A flag indicating whether overflow of the sequence number counter should generate an auditable event and prevent further transmission of packets on the SA.
- Anti-replay window: Used to determine whether an inbound AH or ESP packet is replay, by defining a sliding window within which the sequence number must fall.
- AH information: Authentication algorithm, keys, key lifetimes, and related parameters being used with AH.
- ESP information: Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP.

Security Associations Cont’d

- Lifetime of this security association: A time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated, plus an indication of which of these actions should occur.
  - IPSec protocol mode: Tunnel, transport, or wildcard (required to all implementations).
  - Path MTU: Any observed path maximum transmission unit (maximum size of a packet that can be transmitted without fragmentation) and aging variables (required for all implementations).
- Transport and Tunnel Modes:
  - Both AH and ESP support two modes of use: transport and tunnel mode.



(a) Original IP Packet

(b) Transport Mode

(c) Tunnel Mode

Transport Mode

- Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet. Examples include a TCP or UDP segment, or an ICMP packet, all of which operate directly above IP in a host protocol stack.
- Typically, transport mode is used for end-to-end communication between two hosts (e.g. a client and a server, or two workstations). ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header. AH in transport mode authenticates the IP payload and selected portions of the IP header.

Tunnel Mode

- Tunnel mode provides protection to the entire IP packet. To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as the payload of new "outer" IP packet with a new outer IP header.

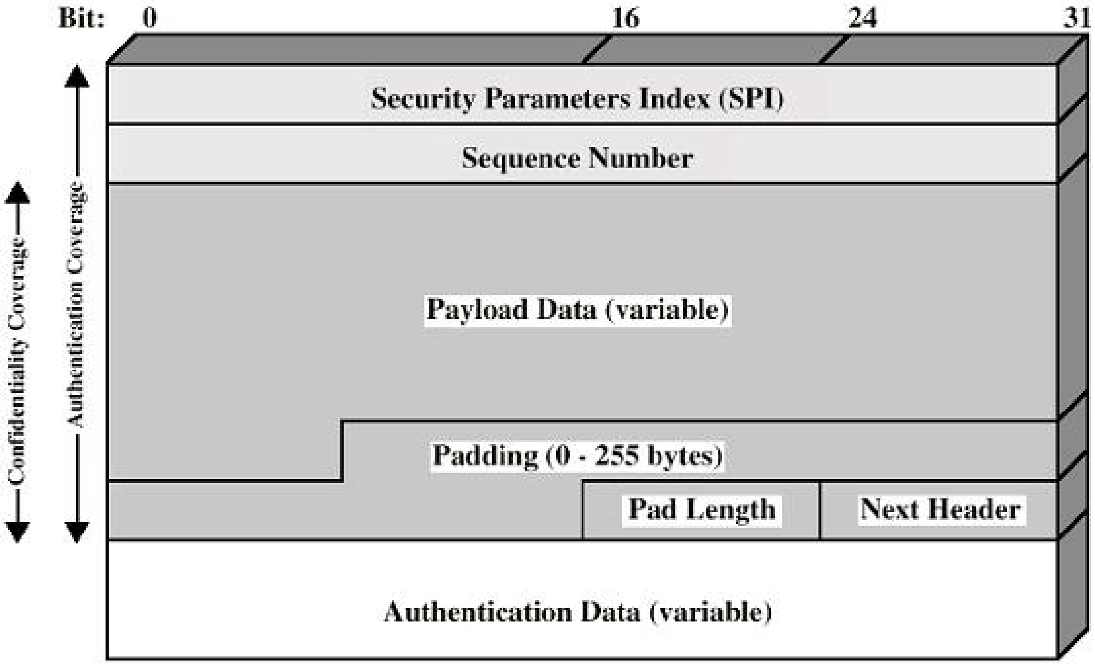
- The entire original, or inner, packet travels through a "tunnel" from one point of an IP network to another; no routers along the way are able to examine the inner IP header. Because the original packet is encapsulated, the new, larger packet may have totally different source and destination addresses, adding to the security.

- Tunnel mode is used when one or both ends of an SA is a security gateway, such as a firewall or router that implements IPSec.

- With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing IPSec.

Encapsulating Security Payload

- The encapsulating security payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality.
- As an optional feature, ESP can also provide the same authentication services as AH. The following figure shows the format of an ESP packet. It contains the following fields:



Encapsulating Security Payload cont’d

- Security Parameters Index (32 bits): Identifies a security association.
- Sequence Number (32 bits): A monotonically increasing counter value.
- Payload Data (variable): This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
- Padding (0-255 bytes): May be required if the encryption algorithm requires the plaintext to be a multiple of some number of octects.
- Pad Length (8 bits): Indicates the number of pad bytes immediately preceding this field.
- Next Header (8 bits): Identifies the type of data contained in the payload data field by identifying the first header in that payload (for example, an extension header in IPv6, or an upper-layer protocol such as TCP).
- Authentication Data (variable): A variable-length field (must be an integral number of 32-bit words) that contains the integrity check value computed over the ESP packet minus the Authentication Data field.

Key Management

- The key management portion of IPSec involves the determination and distribution of secret keys. The IPSec Architecture document mandates support for two types of key management:

- Manual: A system administrator manually configures each system with its own keys and with the keys of other communicating systems. This is practical for small, relatively static environments.

- Automated: An automated system enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration. An automated system is the most flexible but requires more effort to configure and requires more software, so smaller installations are likely to opt for manual key management.

- The default automated key management protocol for IPSec is referred to as ISAKMP/Oakley.