INTRODUCTION TO CYBER SECURITY

EMAIL SECURITY

- Email (short for electronic mail) is a digital method by using it we exchange messages between people over the internet or other computer networks.
- **Email security** refers to the steps where we protect the email messages and the information that they contain from unauthorized access, and damage.
- It involves ensuring the confidentiality, integrity, and availability of email messages, as well as safeguarding against phishing attacks, spam, viruses, and another form of malware.
- It can be achieved through a combination of technical and non-technical measures.
- Some standard technical measures include the encryption of email messages to protect their contents, the use of digital signatures to verify the authenticity of the sender, and email filtering systems to block unwanted emails and malware, and the non-technical measures may include training employees on how to recognize and respond to phishing attacks and other email security threats, establishing policies and procedures for email use and management, and conducting regular security audits to identify and address vulnerabilities.

TYPES OF EMAIL ATTACKS

1. PHISHING

- Phishing is a form of fraud. Cybercriminals use email, instant messaging, or other social media to try to gather information such as login credentials by masquerading as a reputable person.
- **Phishing** occurs when a malicious party sends a fraudulent email disguised as being from an authorized, trusted source.
- The message's intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information.
- **Spear phishing** is a highly targeted phishing attack.
- While phishing and spear-phishing both use emails to reach the victims, spear-phishing sends customized emails to a specific person.
- Phishing attacks involve sending emails that appear to come from a trusted source, such as a bank or an online retailer, to trick users into revealing sensitive information, such as passwords or credit card numbers.
- One advantage of this attack is that it can be easily carried out using basic social engineering techniques, without the need for sophisticated tools or technical skills.

Disadvantages:

- It can be easily detected if users know the legitimate source of the email and are cautious about clicking on links or downloading attachments.

2. SPYWARE

- Spyware is software that enables a criminal to obtain information about a user's computer activities.
- Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings.
- Spyware often bundles itself with legitimate software or with Trojan horses. Many shareware websites are full of spyware.

3. **ADWARE**

- Adware typically displays annoying pop-ups to generate revenue for its authors.
- The malware may analyze user interests by tracking the websites visited.
- It can then send pop-up advertising relevant to those sites. Some versions of software automatically install Adware.

4. **PHARMING**

- Pharming is the impersonation of an authorized website in an effort to deceive users into entering their credentials.
- Pharming misdirects users to a fake website that appears to be official. Victims then enter their personal information thinking that they are connected to a legitimate site.

5. **SPAM**

- Spam (also known as junk mail) is an unsolicited email.
- In most cases, spam is a method of advertising. However, spam can send harmful links, malware, or deceptive content.
- The end goal is to obtain sensitive information such as a social security number or bank account information.
- Most spam comes from multiple computers on networks infected by a virus or worm.
- These compromised computers send out as many bulk email as possible.

6. **RANSOMWARE**

- Picture your files locked up in a digital vault. The villain malicious software holds them hostage until you pay a ransom.
- It's like a cyber kidnapper

7. **MALWARE**

- Sneaky software that infiltrates your computer without asking permission

8. **SPOOFING**

- Imagine someone wearing a disguise at a masquerade ball.
- Attackers forge email headers, making messages look legit even when they're not. Trust no masked stranger

9. **MAN-IN-THE-MIDDLE ATTACK**

- Visualize a sneaky eavesdropper intercepting your messages.
- They can read, alter, or inject new content.

10. **DENIAL OF SERVICE**
11. **IDENTITY THEFT**

STEPS SHOULD BE TAKEN TO SECURE EMAIL

- **Choose a secure password:** Password must be at least 12 characters long, and contains uppercase and lowercase letters, digits, and special characters.
- **Two-factor authentication:** Activate the two-factor authentication, which adds an additional layer of security to your email account by requiring a code in addition to your password.
- **Use encryption:** It encrypts your email messages so that only the intended receiver can decipher them. Email encryption can be done by using the programs like PGP or S/MIME.
- **Choose a trustworthy email service provider:** Search for a service provider that protects your data using encryption and other security measures.
- **Use a VPN:** Using a VPN can help protect our email by encrypting our internet connection and disguising our IP address, making it more difficult for hackers to intercept our emails.

KEY FEATURES OF EMAIL SECURITY SERVICES

Email is one of the greatest sources of cyber risk to an organization, and an email security solution is a vital component of a corporate security strategy. Some key features of email security services include:

- **Anti-Phishing Protection :** Phishing is a leading cyber threat and can result in malware infections and the loss of credentials and other sensitive data. Email security services should be able to identify and block emails with malicious links and attachments before they reach the intended recipient.
- **Data Loss Prevention (DLP) :** Email is a common medium for information to both enter and leave an organization. Email security solutions should incorporate DLP functionality to identify and respond to the attempted transmission of intellectual property (IP) and other sensitive data to unauthorized parties.
- **Malware Blocking :** Phishing emails are a common means of distributing malware to target systems within an organization. Email security solutions should analyze attachments in a sandboxed environment to identify malware attached to an email.
- **Content Disarm and Reconstruction (CDR) :** Bad actors often embed malicious code in Microsoft Office and PDF documents. An email security solution with CDR support can deconstruct a file, excise malicious code from it, and rebuild the sanitized file for transmission to the receiving party.
- **Account Takeover Prevention :** Email accounts contain sensitive information and often control access to other corporate accounts. Email security solutions should help to protect against account takeover attacks by cyber threat actors attempting to exploit weak or compromised user credentials.

ESTABLISH KEY PRIVACY IN EMAIL SECURITY:

- **Use public and private keys**

  Public-key cryptography uses a public key that can be widely distributed and a private key that is known only to the user. The sender uses the recipient's public key to encrypt the message, which can only be decrypted by the recipient's private key. This method ensures that only the intended recipient can access the information.

- **Use PGP encryption**

  PGP (Pretty Good Privacy) is a public-key cryptography software that encrypts data to make email communication more private. PGP can be used to encrypt and decrypt emails, text messages, and files. You can generate PGP keys using PGP encryption software or some email platforms.

- **Use TLS/SSL connections**
  To establish a secure connection, use the START TLS command to instruct your email server to switch to a secure connection via TLS or SSL.

AUTHENTICATION OF THE SOURCE OF AN EMAIL

- Email authentication is critical as it protects an organization's brand, customers, employees, and partners from spoofing.
- With email authentication, an organization can prove that every email using its domain actually came from a legitimate sender.

- **Use email authentication protocols**

  Use protocols like Domain Keys Identified Mail (DKIM), Sender Policy Framework (SPF), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) to authenticate emails.

- **Use a secure email provider**

  Choose a secure email service provider that uses advanced security measures.

- **Use email filters**

  Use email filters to detect and block suspicious emails.

- **Use S/MIME**

  S/MIME, or Secure Multipurpose Internet Mail Extension, is an encryption protocol that digitally signs and encrypts emails.

- **Use Pretty Good Privacy (PGP)**
  PGP is a security program that uses digital signatures and file encryption to authenticate email messages

MESSAGE INTEGRITY – EMAIL

- Message integrity is the process of verifying that a received email message is the same as the one that was sent, and has not been altered in any way.
- This is important because it ensures that the message has not been tampered with, such as by changing content, adding or removing fragments, or transposing content.
- To verify the integrity of an email message, the receiver can use a cryptographic hash function to run the message again and compare the new digest with the previous one.
- If the two digests are the same, the receiver can be sure that the original message has not been changed.

- To **provide authentication and confidentiality in e-mail** we use two methods :
  - **Pretty Good Privacy**
  - **S/MIME**

PRETTY GOOD PRIVACY (PGP)

- PGP stands for Pretty Good Privacy which is invented by Phil Zimmermann
- PGP is an open-source, freely available software package for e-mail security.
- PGP was designed **to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation** in the sending of email.
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation.
- PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
- **PGP provides authentication through the use of Digital Signature**.
- **It provides confidentiality through the use of symmetric block encryption.**
- **It provides compression by using the ZIP algorithm, and email compatibility** using the radix-64 encoding scheme.

SERVICES OFFERED BY PGP:

1. Authentication

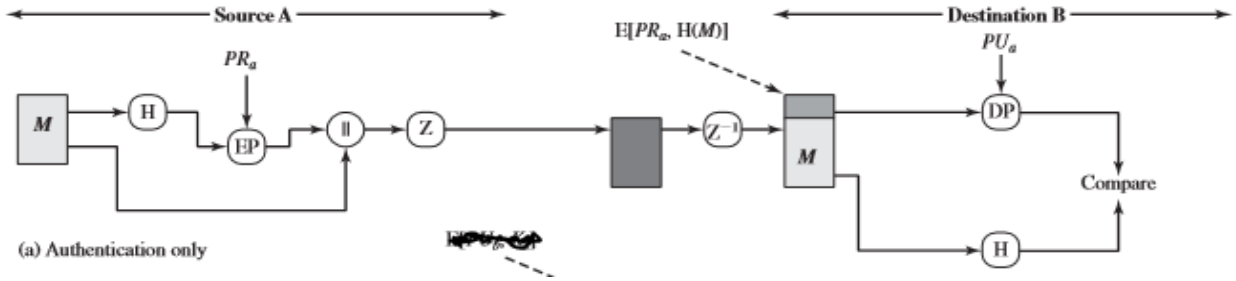
2. Confidentiality

3. Email Compatibility

4. Segmentation

AUTHENTICATION IN PGP

- Authentication basically means something that is used to validate something as true or real. To login into some sites sometimes we give our account name and password, that is an authentication verification procedure.
- In the email world, checking the authenticity of an email is nothing but to check whether it actually came from the person it says.
- In emails, authentication has to be checked as there are some people who spoof the emails or some spams and sometimes it can cause a lot of inconvenience.
- The Authentication service in PGP is provided as follows:



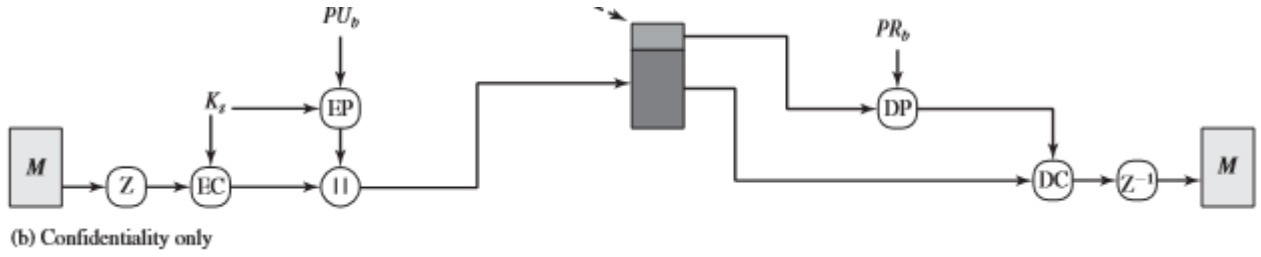
As shown in the above figure, the Hash Function (H) calculates the Hash Value of the message.

- For the hashing purpose, **SHA-1** is used and it produces a **160 bit** output hash value.
- Then, using the sender's private key (PRa), it is encrypted and it's called as **Digital Signature**.
- The Message is then appended to the signature. All the process happened till now, is sometimes described as signing the message .
- Then the message is compressed to reduce the transmission overhead and is sent over to the receiver.
- At the receiver's end, the data is decompressed and the message, signature are obtained.
- The signature is then decrypted using the sender's public key(PUa) and the hash value is obtained.
- The message is again passed to hash function and it's hash value is calculated and obtained.
- Both the values, one from signature and another from the recent output of hash function are compared and if both are same, it means that the email is actually sent from a known one and is legit, else it means that it's not a legit one.

CONFIDENTIALITY IN PGP

- In the email service, only the sender and the receiver should be able to read the message, that means the contents have to be kept secret from every other person, except for those two.

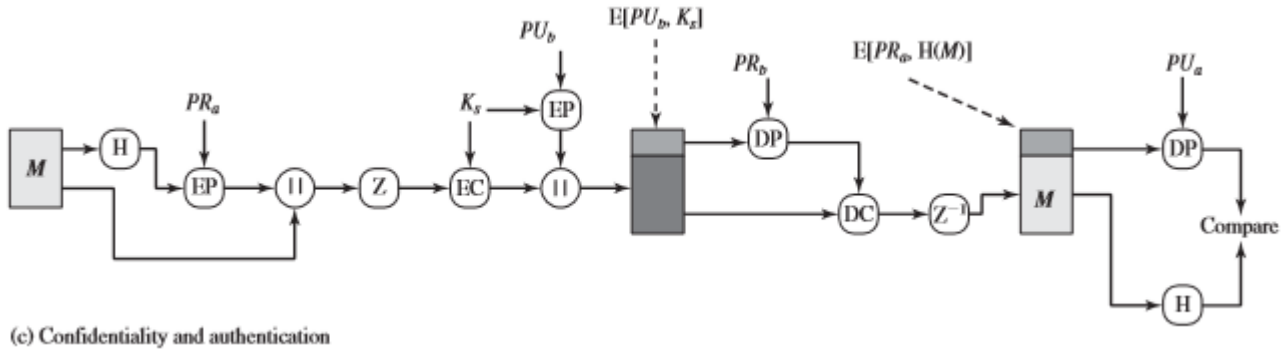
PGP provides that Confidentiality service in the following manner:



(b) Confidentiality only

- Then, the session key (Ks) itself gets encrypted through public key encryption (EP) using receiver's public key(PUb) .
- Both the encrypted entities are now concatenated and sent to the receiver.
- The original message was compressed and then encrypted initially and hence even if any one could get hold of the traffic, he cannot read the contents as they are not in readable form and they can only read them if they had the session key (Ks). Even though session key is transmitted to the receiver and hence, is in the traffic, it is in encrypted form and only the receiver's private key can be used to decrypt that and thus our message would be completely safe.
- At the receiver's end, the encrypted key is decrypted using PRb and the message is decrypted with the obtained session key. Then, the message is decompressed to obtain the M.
- RSA algorithm is used for the public-key encryption and for the symmetric key encryption.

AUTHENTICATION AND CONFIDENTIALITY SERVICES ARE PROVIDED IN PARALLEL



(c) Confidentiality and authentication

- Authentication and confidentiality play pivotal roles in Pretty Good Privacy (PGP), ensuring the security and integrity of virtual verbal exchange.
- Authentication, carried out through virtual signatures, verifies the identity of the sender and safeguards towards spoofing and impersonation. By signing messages with their personal key, senders offer recipients with a means to verify the authenticity of the verbal exchange. This authentication mechanism not simplest fosters agree with among parties but additionally guarantees message integrity, as virtual signatures verify that the message has not been tampered with at some stage in transmission.
- On the opposite hand, confidentiality, facilitated via encryption, protects the content material of messages from unauthorized access. Through encryption algorithms, PGP scrambles the message, rendering it unreadable to everybody without the decryption key. This ensures that touchy facts stays private and inaccessible to eavesdroppers and unauthorized parties.
- Together, authentication and confidentiality in PGP set up a stable framework for relied on conversation, allowing individuals and corporations to change information confidentially and securely while keeping privacy and integrity.

EMAIL COMPATIBILITY

- Email Compatibility in Pretty Good Privacy (PGP) is important because the sender and recipient must use compatible versions of PGP to read encrypted messages.
- If the versions are not compatible, the recipient cannot decrypt the message.
- PGP's email compatibility function works by converting a raw 8-bit binary stream into a stream of printable ASCII characters.
- This is done using radix-64 conversion, which maps each group of three octets of binary data into four ASCII characters. This format also adds a CRC to detect transmission errors.
- As PGP evolves, newer versions can create encrypted messages that older versions cannot decrypt. To avoid this, PGP communication partners should understand each other's capabilities or agree on PGP settings.
- PGP can also be used for email verification. A recipient can use a digital signature to verify the identity of the sender.

COMPRESSION

- PGP compresses the message after applying the signature but before encryption. This has the benefit of saving space both for e-mail transmission and for file storage.
- The placement of the compression algorithm, indicated by Z for compression and Z-1 for decompression is critical: The signature is generated before compression for two reasons:
- It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification. If one signed a compressed document, then it would be necessary either to store a compressed version of the message for later verification or to recompress the message when verification is required.
- Even if one were willing to generate dynamically a recompressed message for verification, PGP‟s compression algorithm presents a difficulty
- . Applying the hash function and signature after compression would constrain all PGP implementations to the same version of the compression algorithm.

SEGMENTATION

- Segmentation in Pretty Good Privacy (PGP) is the process of breaking up a message into smaller segments and mailing them separately when the message is too large to fit the maximum message length of an email facility
- E-mail facilities are restricted to a maximum message length.
- For instance, some facilities accessible throughout the internet set a maximum length of 50,000 octets. Some message higher than that should be broken up into smaller segments, each of which is mailed independently.

Advantages of PGP

- The primary benefit of PGP encryption lies in its unbreakable algorithm.
- It is regarded as a top technique for improving cloud security and is frequently utilised by users who need to encrypt their private conversations.
- This is due to PGP’s ability to prevent hackers, governments, and nation-states from accessing files or emails that are encrypted with PGP.

Disadvantage of PGP

- The main drawback of PGP encryption is that it is usually not intuitive to use. PGP requires time and effort to fully encrypt data and files, which might make messaging more difficult for users. If an organisation is thinking about deploying PGP, it has to train its employees.

- It is imperative that users comprehend the intricacies of the PGP system to prevent unintentionally weakening their security measures. This may occur from using PGP incorrectly or from losing or corrupting keys, endangering other users in situations where security is at an extreme.

- Absence of anonymity: PGP encrypts user messages but does not provide users with any anonymity. This makes it possible to identify the source and recipient of emails sent using a PGP solution.

S/MIME

- **Secure/Multipurpose Internet Mail Extension is an e-mail security standard.**
- PGP is used for personal e-mail security and S/MIME is for commercial purpose.
- S/MIME is an upgrade of MIME(Multipurpose Internet Mail Extensions).
- Due to the limitations of MIME, S/MIME came into play.
- S/MIME is based on asymmetric cryptography which means that communications can be encrypted or decrypted using a pair of related keys namely public and private keys.
- S/MIME can do both symmetric encryption and digital signatures, which are two very important functions for securing emails in the best possible way.
- Symmetric encryption guarantees that only the addressee will be able to read your email, and digital signatures identify who it came from and show that it wasn't changed on its way to your inbox.
- With S/MIME, you will be able to protect your communication against unwanted readers and establish trust with those receiving your emails.

How S/MIME Works?

- S/MIME enables non-ASCII data to be sent using Secure Mail Transfer Protocol (SMTP) via email.
- Moreover, many data files are sent, including music, video, and image files.
- This data is securely sent using the encryption method.
- The data which is encrypted using a public key is then decrypted using a private key which is only present with the receiver of the E-mail.
- The receiver then decrypts the message and then the message is used.
- In this way, data is shared using e-mails providing an end-to-end security service using the cryptography method.

S/MIME Functionality:

- S/MIME provides the following functions :-
- **Enveloped data**: This consists of encrypted content of any type and encrypted content encryption keys for one or more recipients.

- **Signed data**: A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base64 encoding. A recipient can only view a signed data message with S/MIME capability.

- **Clear-signed data**: As with signed data, a digital signature of the content is formed. However, only the digital signature is encoded using base64. As a result, recipients without S/MIME capability can view the message Content, although they cannot verify the signature.

- **Signed and enveloped data**: Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

CRYPTOGRAPHIC ALGORITHMS USED IN S/MIME.

- S/MIME incorporates three public-key algorithms
- The Digital Signature Standard (DSS) is the preferred algorithm for digital signature.
- S/MIME lists Diffie-Hellman as the preferred algorithm for encrypting session keys; in fact, S/MIME uses a variant of Diffie-Hellman that does provide encryption/decryption, known as ElGamal

Table 18.6 Cryptographic Algorithms Used in S/MIME

Function	Requirement
Create a message digest to be used in forming a digital signature.	MUST support SHA-1. Receiver SHOULD support MD5 for backward compatibility.
Encrypt message digest to form a digital signature.	Sending and receiving agents MUST support DSS. Sending agents SHOULD support RSA encryption. Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits.
Encrypt session key for transmission with a message.	Sending and receiving agents SHOULD support Diffie-Hellman. Sending and receiving agents MUST support RSA encryption with key sizes 512 bits to 1024 bits.
Encrypt message for transmission with a one-time session key.	Sending and receiving agents MUST support encryption with tripleDES. Sending agents SHOULD support encryption with AES. Sending agents SHOULD support encryption with RC2/40.
Create a message authentication code.	Receiving agents MUST support HMAC with SHA-1. Sending agents SHOULD support HMAC with SHA-1.

S/MIME Messages

- S/MIME secures a MIME entity with a signature, encryption, or both.
- A MIME entity may be an entire message or if the MIME content type is multipart, then a MIME entity is one or more of the subparts of the message
- Then the MIME entity plus some security-related data, such as algorithm identifiers and certificates, are processed by S/MIME to produce what is known as a PKCS (Public Key Cryptographic Standards) object
- A PKCS object is then treated as message content and wrapped in MIME (provided with appropriate MIME headers).

Advantages of S/MIME

1. It offers verification.
2. It offers integrity to the message.
3. By the use of digital signatures, it facilitates non-repudiation of origin.
4. It offers seclusion.
5. Data security is ensured by the utilization of encryption.
6. Transfer of data files like images, audio, videos, documents, etc. in a secure manner.

What is S/MIME used for?

- S/MIME offer's two services :
    - Digital signatures provide non-repudiation and authentication.
    - Message encryption provides Data Integrity and Confidentiality.

Difference Between PGP and S/MIME

S.NO	PGP	S/MIME
1.	It is designed for processing plain texts	While it is designed to process email as well as many multimedia files.
2.	PGP is less costly as compared to S/MIME.	While S/MIME is comparatively expensive.
3.	PGP is good for personal as well as office use.	While it is good for industrial use.
4.	PGP is less efficient than S/MIME.	While it is more efficient than PGP.
5.	It depends on user key exchange.	Whereas it relies on a hierarchically valid certificate for key exchange.
6.	PGP is comparatively less convenient.	While it is more convenient than PGP due to the secure transformation of all the applications.
7.	PGP contains 4096 public keys.	While it contains only 1024 public keys.
8.	PGP is the standard for strong encryption.	While it is also the standard for strong encryption but has some drawbacks.
9.	PGP is also be used in VPNs.	While it is not used in VPNs, it is only used in email services.
10.	PGP uses **Diffie hellman digital signature**.	While it uses **Elgamal digital signature**.
11.	In PGP Trust is established using Web of Trust.	In S/MIME Trust is established using Public Key Infrastructure.
12.	PGP is used for Securing text messages only.	S/MIME is used for Securing Messages and attachments.
13.	Their is less use of PGP in industry .	While S/MIME is widely used in industry.
14.	Convenience of PGP is low.	Convenience of S/MIME is High.
15.	Administrative overhead of PGP is high.	Administrative overhead of S/MIME is low.

IP SECURITY

OVERVIEW OF IPSEC :

- IP security (IPsec) is a capability that can be added to either current version of the Internet Protocol (IPv4 or IPv6) by means of additional headers.
- **IPsec encompasses three functional areas: authentication, confidentiality, and key management.**
- Authentication makes use of the HMAC message authentication code. Authentication can be applied to the entire original IP packet (tunnel mode) or to all of the packet except for the IP header (transport mode).
- Confidentiality is provided by an encryption format known as encapsulating security payload. Both tunnel and transport modes can be accommodated.
- IKE defines a number of techniques for key management.

APPLICATIONS OF IPSEC

- IPsec provides the capability to secure communications across a LAN,across private and public WANs,and across the Internet.
    - **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. IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated ,adding an additional layer of security to whatever is provided at the application layer.

- 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, e-mail, file transfer, Web access, and so on) can be secured.

BENEFITS OF IPSEC

• When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.

• IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.

• IPsec is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPsec is implemented in the firewall or router. Even if IPsec is implemented in end systems, upper-layer software, including applications, is not affected.

• IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.

• IPsec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

IPSEC DOCUMENTS

- IPsec encompasses three functional areas: authentication, confidentiality, and key management.
- The totality of the IPsec specification is scattered across dozens of documents
- The documents can be categorized into the following groups.
- **Architecture:** Covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology
- **Authentication Header (AH):** AH is an extension header to provide message authentication
- **Encapsulating Security Payload (ESP):** ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication.
- **Internet Key Exchange (IKE):** This is a collection of documents describing the key management schemes for use with IPsec
- **Cryptographic algorithms:** This category encompasses a large set of documents that define and describe cryptographic algorithms for encryption, message authentication, pseudorandom functions (PRFs), and cryptographic key exchange.

IPSEC SERVICES

- IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm
- Two protocols are used to provide security:
    - an authentication protocol designated by the header of the protocol,
    - a combined encryption/ authentication protocol designated by the format of the packet for that protocol

Lists the following Services:

• Access control

• Connectionless integrity

• Data origin authentication

• Rejection of replayed packets

• Confidentiality

• Limited traffic flow confidentiality

Advantages of IPSec

- Flexibility
- Integrity & Authentication
- Wide Compatability & Scalability
- Strong Security
- Improve network efficiency

Disadvantages of IPSec

- Configuration Complexity
- Performance impact on network due to overhead of encryption and decryption of IP packets
- Limited Protection : DNS, routing protocols still vulnerable to attacks.

TRANSPORT AND TUNNEL MODES

- Both AH and ESP support two modes of use: transport and tunnel mode.
- Functionalities are:

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

IPV4 and IPV6

- IPv4 and IPv6 are connectionless protocols that use multi-packet routing to break data into smaller blocks to send across the internet.
- IPv4 and IPv6 determine the path each of these packets take, meaning packets from the same piece of data may take different internet traffic routes across the internet.

What is IPv4?

- IPv4 addresses consist of two things: the network address and the host address.
- It stands for **Internet Protocol version four.**

IPv4 Address Format

- IPv4 Address Format is a 32-bit Address that comprises binary digits separated by a dot (.).

Drawback of IPv4

- **Limited Address Space** : IPv4 has a limited number of addresses, which is not enough for the growing number of devices connecting to the internet.
- **Complex Configuration** : IPv4 often requires manual configuration or DHCP to assign addresses, which can be time-consuming and prone to errors.
- **Less Efficient Routing** : The IPv4 header is more complex, which can slow down data processing and routing.
- **Security Issues** : IPv4 does not have built-in security features, making it more vulnerable to attacks unless extra security measures are added.

- **Limited Support for Quality of Service (QoS)** : IPv4 has limited capabilities for prioritizing certain types of data, which can affect the performance of real-time applications like video streaming and VoIP.
- **Fragmentation** : IPv4 allows routers to fragment packets, which can lead to inefficiencies and increased chances of data being lost or corrupted.
- **Broadcasting Overhead** : IPv4 uses broadcasting to communicate with multiple devices on a network, which can create unnecessary network traffic and reduce performance.

What is IPv6?

- IPv6 is based on IPv4 and stands for Internet Protocol version 6
- IP version 6 is the new version of Internet Protocol, **which is way better than IP version 4 in terms of complexity and efficiency.**

IPv6 Address Format

- IPv6 Address Format is a 128-bit IP Address, which is written in a group of 8 hexadecimal numbers separated by colon (:).
- To switch from IPv4 to IPv6, there are several strategies:
    - **Dual Stacking** : Devices can use both IPv4 and IPv6 at the same time. This way, they can talk to networks and devices using either version.
    - **Tunneling** : This method allows IPv6 users to send data through an IPv4 network to reach other IPv6 users. Think of it as creating a "tunnel" for IPv6 traffic through the older IPv4 system.
    - **Network Address Translation (NAT)** : NAT helps devices using different versions of IP addresses (IPv4 and IPv6) to communicate with each other by translating the addresses so they understand each other.

Benefits of IPv6 over IPv4

The recent Version of IP IPv6 has a greater advantage over IPv4. Here are some of the mentioned benefits:

- **Larger Address Space:** IPv6 has a greater address space than IPv4, which is required for expanding the IP Connected Devices. IPv6 has 128 bit IP Address rather and IPv4 has a 32-bit Address.
- **Improved Security:** IPv6 has some improved security which is built in with it. IPv6 offers security like Data Authentication, Data Encryption, etc. Here, an Internet Connection is more Secure.
- **Simplified Header Format:** As compared to IPv4, IPv6 has a simpler and more effective header Structure, which is more cost-effective and also increases the speed of Internet Connection.
- **Prioritize:** IPv6 contains stronger and more reliable support for QoS features, which helps in increasing traffic over websites and increases audio and video quality on pages.
- **Improved Support for Mobile Devices:** IPv6 has increased and better support for Mobile Devices. It helps in making quick connections over other Mobile Devices and in a safer way than IPv4.

DIFFERENCE BETWEEN IPV4 & IPV6

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end-to-end, connection integrity is Achievable
The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available
It has a broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has a header of 40 bytes fixed
IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
IPv4 consists of 4 fields which are separated by addresses dot (.)	IPv6 consists of 8 fields, which are separated by a colon (:)

ENCAPSULALTION SECURITY PAYLOAD (ESP) PROTOCOL

- ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity),and (limited) traffic flow confidentiality.
- The set of services provided depends on options selected at the time of Security Association (SA) establishment.
- ESP can work with a variety of encryption and authentication algorithms, including authenticated encryption algorithms
- ESP is an individual protocol in IPSec.
- ESP is responsible for CIA triad:
    - Confidentiality
    - Integrity
    - Availability

- Securing all payload or packets or content in IPV4 and IPV6 is responsibility of ESP.
- It involves encapsulation of content or payload , encrypts it to suitable form and then a security check takes place for payload
- Encryption is performed by an authenticated user
- Similarly, decryption is performed only when receiver is verified

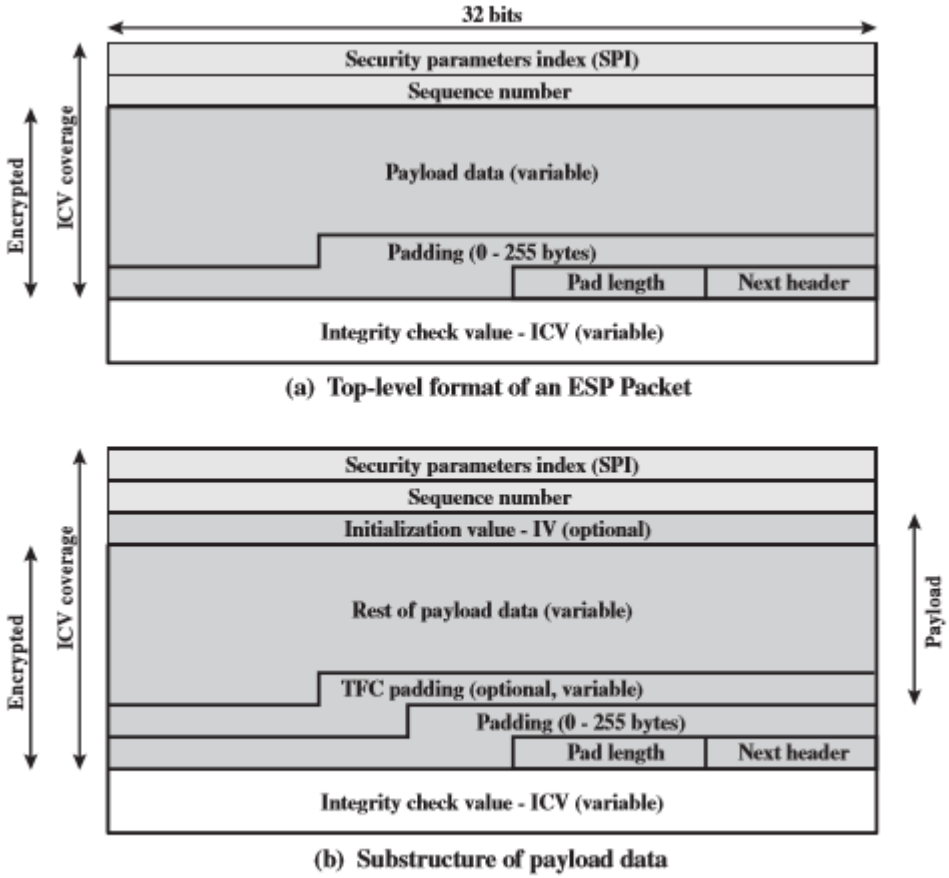


Figure 19.5 ESP Packet Format

- **Security Parameters Index** (32 bits): Identifies a security association.
- **Sequence Number** (32 bits) : A monotonically increasing counter value; this provides an anti-replay function,as discussed for AH.
- **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): The purpose of this field is discussed later.
- **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
- **Integrity Check Value** (variable): A variable-length field that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field.

- Two additional fields may be present in the payload
- An initialization value (IV),or nonce, is present if this is required by the encryption or authenticated encryption algorithm used for ESP.
- If tunnel mode is being used,then the IPsec implementation may add traffic flow confidentiality (TFC) padding after the Payload Data and before the Padding field
- The Payload Data, Padding, Pad Length, and Next Header fields are encrypted by the ESP service.
- If the algorithm used to encrypt the payload requires cryptographic synchronization data, such as an initialization vector (IV),then these data may be carried explicitly at the beginning of the Payload Data field
- The ICV field is optional.
- It is present only if the integrity service is selected and is provided by either a separate integrity algorithm or a combined mode algorithm that uses an ICV.
- The ICV is computed after the encryption is performed

The Scope of ESP for the Tunnel Mode & Transport Mode

The considerations are somewhat different for IPv4 and IPv6:

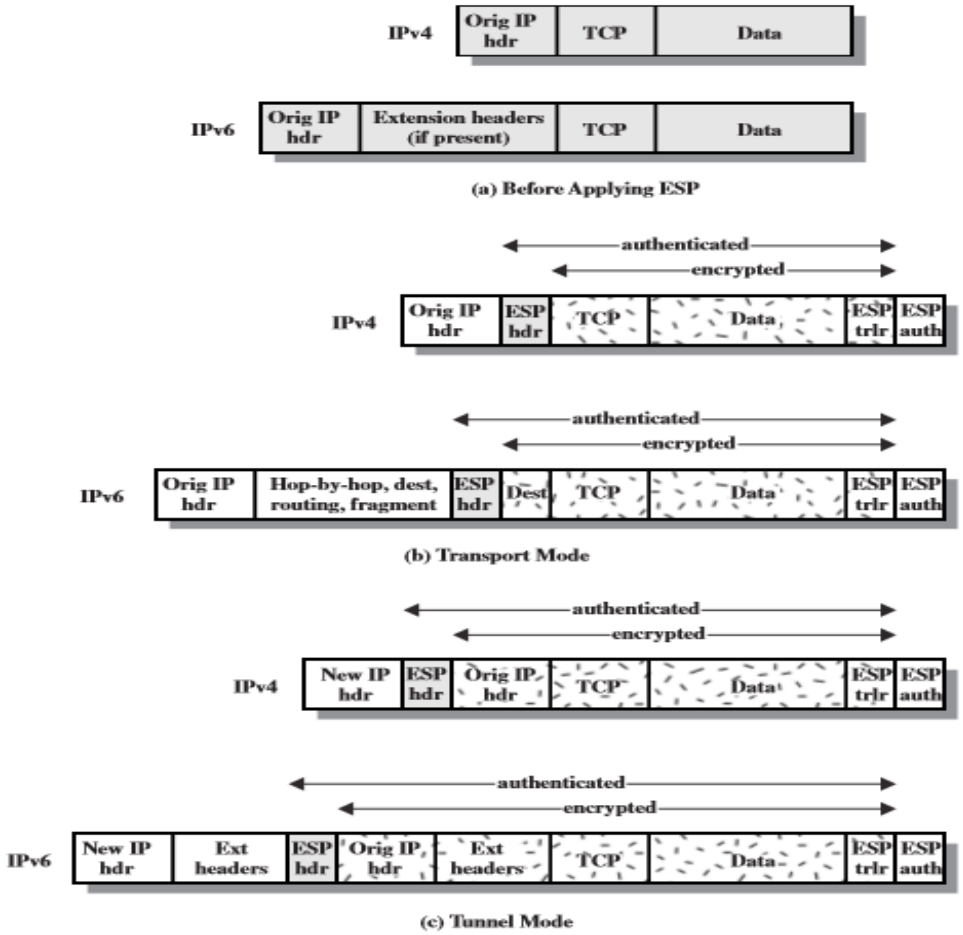


Figure 19.8 Scope of ESP Encryption and Authentication

For this **mode using IPv4**,the ESP header is inserted into the IP packet immediately prior to the transport-layer header (e.g., TCP, UDP, ICMP), and an ESP trailer (Padding, Pad Length, and Next Header fields) is placed after the IP packet. If authentication is selected, the ESP Authentication Data field is added after the ESP trailer. The entire transport-level segment plus the ESP trailer are encrypted. Authentication covers all of the ciphertext plus the ESP header.

In the context of IPv6, ESP is viewed as an end-to-end payload .Therefore, the ESP header appears after the IPv6 base header and the hop-by-hop, routing, and fragment extension headers. The destination options extension header could appear before or after the ESP header, depending on the semantics desired. For IPv6, encryption covers the entire transport-level segment plus the ESP trailer plus the destination options extension header if it occurs after the ESP header.

Transport mode operation of ESP

1. At the source, the block of data consisting of the ESP trailer plus the entire transport-layer segment is encrypted and the plaintext of this block is replaced with its ciphertext to form the IP packet for transmission. Authentication is added if this option is selected.

2. The packet is then routed to the destination. Each intermediate router needs to examine and process the IP header plus any plaintext IP extension headers but does not need to examine the ciphertext.

3. The destination node examines and processes the IP header plus any plaintext IP extension headers. Then, on the basis of the SPI in the ESP header, the destination node decrypts the remainder of the packet to recover the plaintext transport-layer segment.

- **Transport mode operation provides confidentiality** for any application that uses it, thus avoiding the need to implement confidentiality in every individual application.
- **One drawback** to this mode **is that it is possible to do traffic analysis on the transmitted packets.**

Tunnel Mode ESP

- Tunnel mode ESP is used to encrypt an entire IP packet
- For this mode, the ESP header is prefixed to the packet and then the packet plus the ESP trailer is encrypted

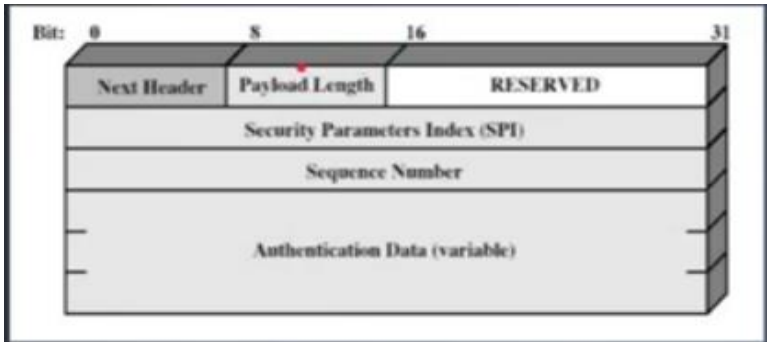
1. The source prepares an inner IP packet with a destination address of the target internal host. This packet is prefixed by an ESP header; then the packet and ESP trailer are encrypted and Authentication Data may be added. The resulting block is encapsulated with a new IP header (base header plus optional extensions such as routing and hop-by-hop options for IPv6) whose destination address is the firewall; this forms the outer IP packet.
2. The outer packet is routed to the destination firewall. Each intermediate router needs to examine and process the outer IP header plus any outer IP extension headers but does not need to examine the ciphertext.
3. The destination firewall examines and processes the outer IP header plus any outer IP extension headers. Then, on the basis of the SPI in the ESP header, the destination node decrypts the remainder of the packet to recover the plaintext inner IP packet. This packet is then transmitted in the internal network.
4. The inner packet is routed through zero or more routers in the internal network to the destination host

Advantages of ESP Protocol

- Encrypting data provide security
- Providing needed data integrity
- Maintaining data confidentiality
- Maintaining a secure gateway for data or message transmission

AUTHENTICATION HEADER (AH) PROTOCOL

- Provides support for data integrity and authentication of IP packets
- Data integrity feature ensures that undetected modification to a packets content in transit is not possible.
- Authentication feature enables an end system to authenticate the user and filter the traffic accordingly.
- It also prevents the address spoofing attacks.
- AH also guards against replay attacks
- Authentication is based on the use of a message authentication code (MAC)



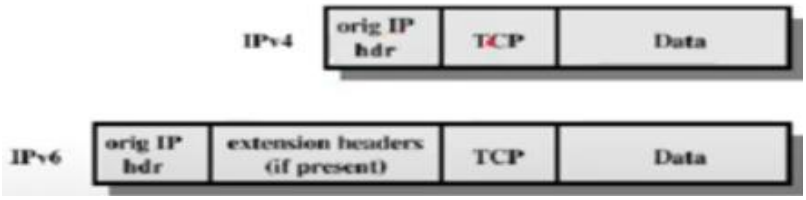
- **Next Header (8 bits)** : Identifies the type of header immediately following this header
- **Payload Len (8 bits)** : Length of this authentication header in 32 bit words, minus 2
- **Reserved (16 bits)** : Reserved for future use (all zeros until then)
- **Security Parameters Index (32 bits)** : Identifies a security association
- **Sequence Number (32 bits)** : A monotonic strictly increasing counter value (incremented by 1 for every packet sent) to prevent replay attacks
- **Authentication Data (variable)** : Variable length field that contains the integrity check value or MAC for this Packet

Authentication Data Field holds a value referred to as the **Integrity Check Value (ICV)**

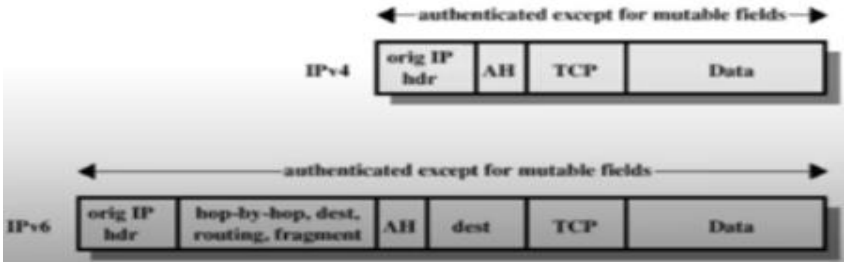
- **ICV** is a message authentication code or a truncated version of a code produced by a MAC algorithm
- The MAC is calculated over
    - IP header fields that either do not change in transit or that are predictable in value upon arrival at the endpoint for the AH SA.
    - Fields that may change in transit and whose value on arrival are unpredictable are set to zero for purposes of calculation at both source and destination

  AH header other than the Authentication Data Field . The ADF is set to zero for purposes of calculation at both source and destination

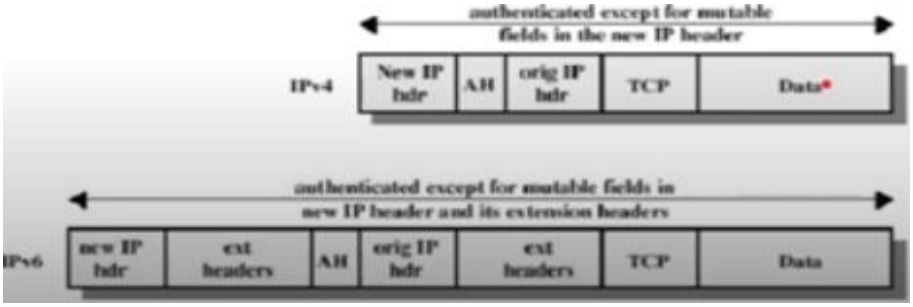
  Entire upper level protocol data , which is assumed to be immutable in transit



Before applying AH



After applying AH – Transport Mode



After applying AH – Tunnel Mode

Advantages of Authentication Header Protocol

- It **provide connectionless integrity** and data origin authentication for IP datagrams
- **Source Authentication**: The AH allows certification that the source of the IPv6 packet is indeed the source from which the data is expected.
- **Replay Protection**: Protection against replay attacks is provided using a sequence number field.
- Ensures that no one changes the data during transit.

INTERNET KEY EXCHANGE (IKE)

- The key management portion of IPsec involves the determination and distribution of secret keys.
- A typical requirement is four keys for communication between two applications: transmit and receive pairs for both integrity and confidentiality.
- 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.

The default automated key management protocol for IPsec is referred to as ISAKMP/Oakley and consists of the following elements:

- **Oakley Key Determination Protocol:** Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security. Oakley is generic in that it does not dictate specific formats.
- **Internet Security Association and Key Management Protocol (ISAKMP):** ISAKMP provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes.

1. **Key Determination Protocol**
   - IKE key determination is a refinement of the Diffie-Hellman key exchange algorithm.
   - The Diffie-Hellman algorithm has **two attractive features**:
     - Secret keys are created only when needed. There is no need to store secret keys for a long period of time, exposing them to increased vulnerability.
     - The exchange requires no pre-existing infrastructure other than an agreement on the global parameters.

   There are **a number of weaknesses** to Diffie-Hellman

     - It does not provide any information about the identities of the parties.
     - It is subject to a man-in-the-middle attack
2. **IKE key determination supports the use of different groups** for the DiffieHellman key exchange.

   Each group includes the definition of the two global parameters and the identity of the algorithm
3. **IKE key determination employs nonces** to ensure against replay attacks.
   Each nonce is a locally generated pseudorandom number.
   Nonces appear in responses and are encrypted during certain portions of the exchange to secure their use.

Three different authentication methods can be used with IKE key determination:

- **Digital signatures**: The exchange is authenticated by signing a mutually obtainable hash;each party encrypts the hash with its private key. The hash is generated over important parameters, such as user IDs and nonces.
- **Public-key encryption**: The exchange is authenticated by encrypting parameters such as IDs and nonces with the sender's private key.
- **Symmetric-key encryption**: A key derived by some out-of-band mechanism can be used to authenticate the exchange by symmetric encryption of exchange parameters.

IKE Header and Payload Formats

- IKE defines procedures and packet formats to establish, negotiate, modify, and delete security associations.
- As part of SA establishment, IKE defines payloads for exchanging key generation and authentication data.
- These payload formats provide a consistent framework independent of the specific key exchange protocol, encryption algorithm,and authentication mechanism.

IKE Header Format :

- An IKE message consists of an IKE header followed by one or more payloads.
- All of this is carried in a transport protocol.
- The specification dictates that implementations must support the use of UDP for the transport protocol.

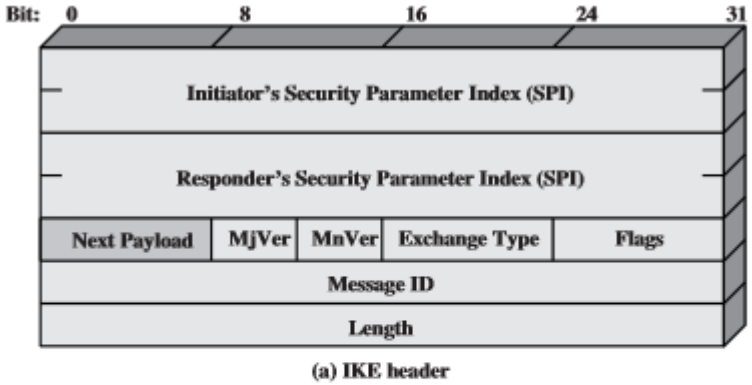


Figure 19.12 IKE Formats

- **Initiator SPI (64 bits):** A value chosen by the initiator to identify a unique IKE security association (SA).
- **Responder SPI (64 bits**): A value chosen by the responder to identify a unique IKE SA.
- **Next Payload (8 bits**): Indicates the type of the first payload in the message
- **Major Version (4 bits):** Indicates major version of IKE in use.
- **Minor Version (4 bits**): Indicates minor version in use.
- **Exchange Type (8 bits):** Indicates the type of exchange; these are discussed later in this section.
- **Flags (8 bits**) : Indicates specific options set for this IKE exchange.
  Three bits are defined :
  The **initiator bit** indicates whether this packet is sent by the SA initiator.
  The **version bit** indicates whether the transmitter is capable of using a higher major version number than the one currently indicated.
  The **response bit** indicates whether this is a response to a message containing the same message ID.
- **Message ID (32 bits):** Used to control retransmission of lost packets and matching of requests and responses.
- **Length (32 bits):** Length of total message (header plus all payloads) in octets.

TRANSPORT LEVEL SECURITY

SSL/TLS BASIC PROTOCOL

- Secure Socket Layer (SSL) provides security services between TCP and applications that use TCP.
- The Internet standard version is called Transport Layer Service (TLS).
- SSL/TLS provides confidentiality using symmetric encryption and message integrity using a message authentication code.
- SSL/TLS includes protocol mechanisms to enable two TCP users to determine the security mechanisms and services they will use.

SSL Architecture

- SSL is designed to make use of TCP to provide a reliable end-to-end secure service.
- SSL is not a single protocol but rather two layers of protocols
- The SSL Record Protocol provides basic security services to various higher layer protocols.
- Three higher-layer protocols are defined as part of SSL:
  - Handshake Protocol
  - Change Cipher Spec Protocol
  - Alert Protocol.
- These SSL-specific protocols are used in the management of SSL exchanges and are examined later in this section.

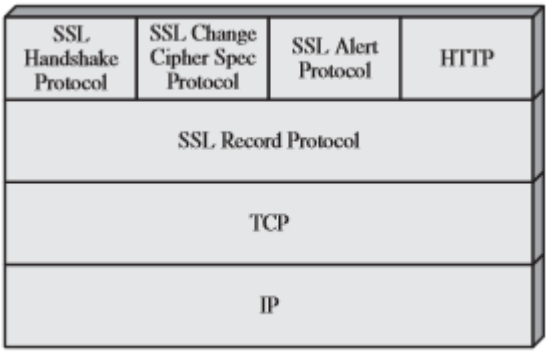


Figure 16.2 SSL Protocol Stack

- Two important SSL concepts are the **SSL session and the SSL connection**
  - **Connection**: A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session.
  - **Session**: An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection

A session state is defined by the following parameters.

- **Session identifier:** An arbitrary byte sequence chosen by the server to identify an active or resumable session state.
- **Peer certificate** : An X509.v3 certificate of the peer. This element of the state may be null.
- **Compression method** : The algorithm used to compress data prior to encryption.
- **Cipher spec** : Specifies the bulk data encryption algorithm and a hash algorithm) used for MAC calculation. It also defines cryptographic attributes such as the hash_size.

- **Master secret** : 48-byte secret shared between the client and server.
- **Is resumable** : A flag indicating whether the session can be used to initiate new connections.

A connection state is defined by the following parameters.

- **Server and client random** : Byte sequences that are chosen by the server and client for each connection.
- **Server write MAC secret** : The secret key used in MAC operations on data sent by the server.
- **Client write MAC secret** : The secret key used in MAC operations on data sent by the client.
- **Server write key** : The secret encryption key for data encrypted by the server and decrypted by the client.
- **Client write key** : The symmetric encryption key for data encrypted by the client and decrypted by the server.
- **Initialization vectors :** When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL Handshake Protocol. Thereafter, the final ciphertext block from each record is preserved for use as the IV with the following record.
- **Sequence numbers**: Each party maintains separate sequence numbers for transmitted and received messages for each connection

SSL Record Protocol

- The SSL Record Protocol provides two services for SSL connections:
  - Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
  - Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

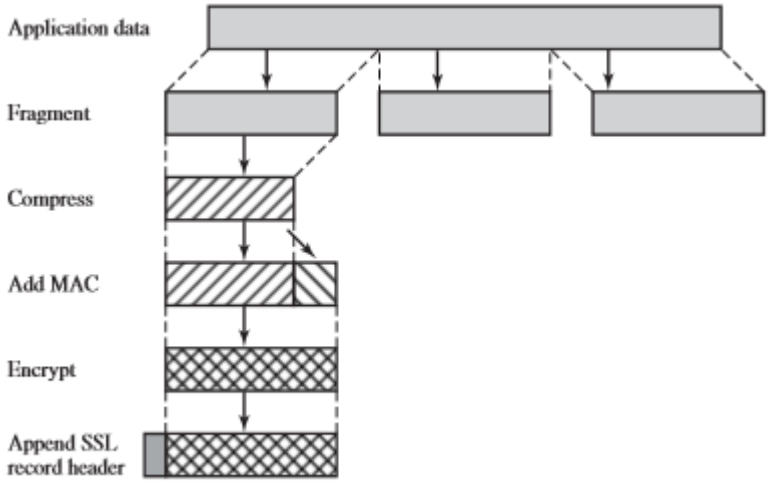


Figure 16.3 SSL Record Protocol Operation

- The Record Protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment.
- Received data are decrypted, verified, decompressed, and reassembled before being delivered to higher-level users.
- The first step is fragmentation. Each upper-layer message is fragmented into blocks of 214 bytes or less.
- Next, compression is optionally applied. Compression must be lossless and may not increase the content length by more than 1024 bytes

- The next step in processing is to compute a message authentication code over the compressed data.For this purpose, a shared secret key is used
- Next, the compressed message plus the MAC are encrypted using symmetric encryption.
- The final step of SSL Record Protocol processing is to prepare a header consisting of the following fields:

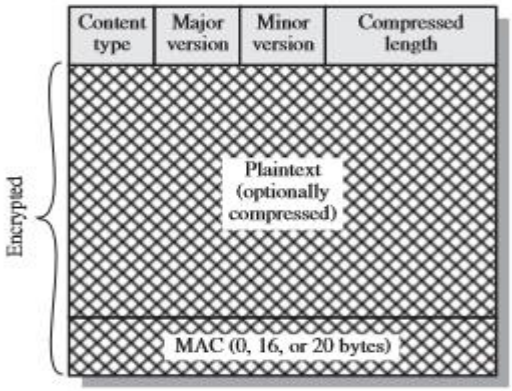


Figure 16.4 SSL Record Format

  - **Content Type** (8 bits): The higher-layer protocol used to process the enclosed fragment.
  - **Major Version** (8 bits): Indicates major version of SSL in use. For SSLv3,the value is 3.
  - **Minor Version** (8 bits): Indicates minor version in use. For SSLv3,the value is 0.
  - **Compressed Length** (16 bits): The length in bytes of the plaintext fragment

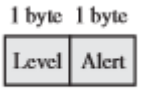
Change Cipher Spec Protocol

- The Change Cipher Spec Protocol is one of the three SSL-specific protocols that use the SSL Record Protocol, and it is the simplest.
- This protocol consists of a single message , which consists of a single byte with the value 1.
- The sole purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.

(a) Change Cipher Spec Protocol

Alert Protocol

- The Alert Protocol is used to convey SSL-related alerts to the peer entity.
- As with other applications that use SSL, alert messages are compressed and encrypted, as specified by the current state. Each message in this protocol consists of two bytes
- The first byte takes the value warning (1) or fatal (2) to convey the severity of the message.
- If the level is fatal, SSL immediately terminates the connection.
- Other connections on the same session may continue, but no new connections on this session may be established. The second byte contains a code that indicates the specific alert.



(b) Alert Protocol

Handshake Protocol

- The most complex part of SSL is the Handshake Protocol.
- This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record.
- The Handshake Protocol is used before any application data is transmitted.
- The Handshake Protocol consists of a series of messages exchanged by client and server.

(c) Handshake Protocol

- Each message has three fields:
  - **Type** (1 byte): Indicates one of 10 messages.
  - **Length** (3 bytes): The length of the message in bytes.
  - **Content** (bytes): The parameters associated with this message

The initial exchange needed to **establish a logical connection between client and server**. The exchange can be viewed as having **four phases**.

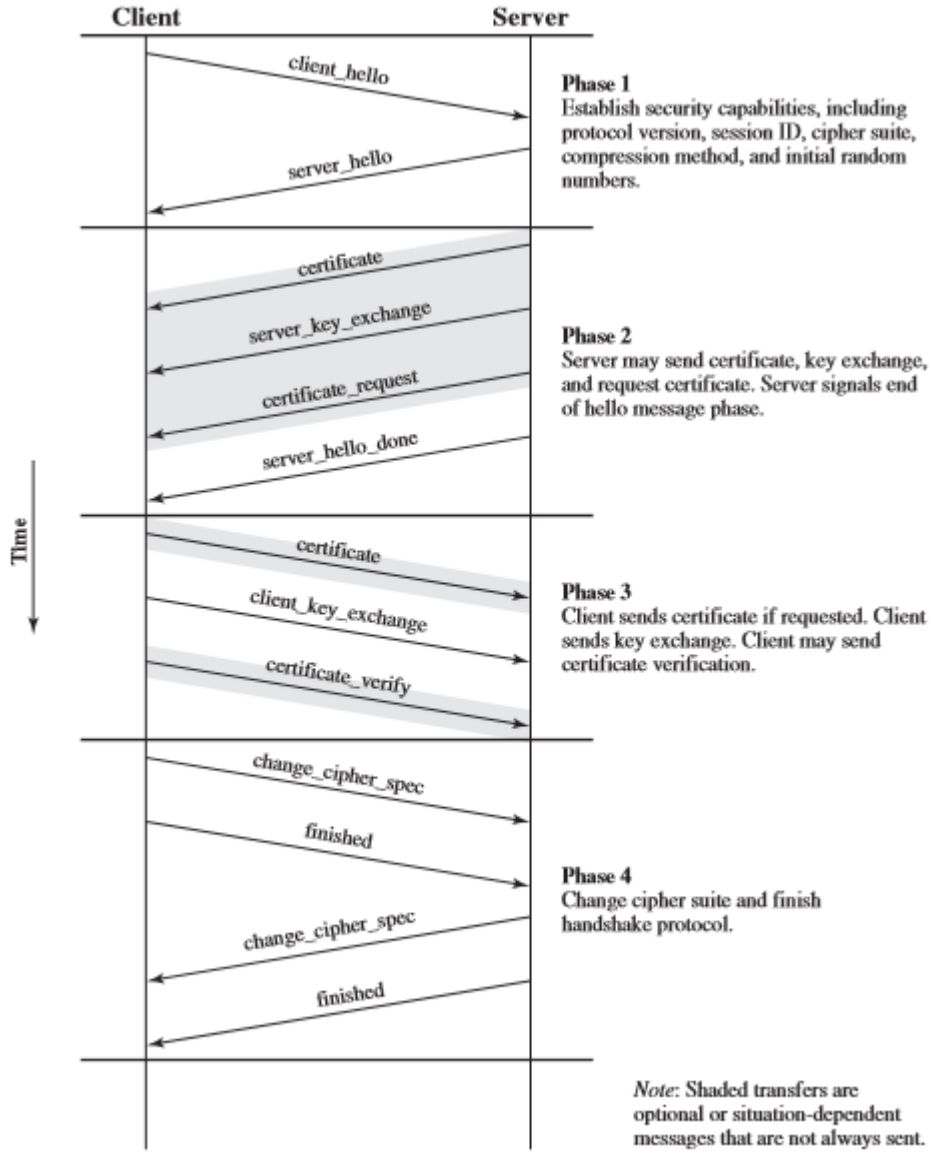


Figure 16.6 Handshake Protocol Action

TLS

- TLS – Transport Layer Security
- It is an internet standard approach
- The TLS Record Format is the same as that of the SSL Record Format and the fields in the header have the same meanings.
- The one difference is in version values.
- For the current version of TLS, the major version is 3 and the minor version is 3.
- TLS makes use of the ***HMAC algorithm***
- TLS makes use of a ***pseudorandom function*** to expand secrets into blocks of data for purposes of key generation or validation.
- The objective is to make use of a relatively small shared secret value but to generate longer blocks of data in a way that is secure from the kinds of attacks made on hash functions and MACs.
- TLS ***supports all of the alert codes, with the exception of no_certificate.***
- ***Cipher Suites*** available under TLS
    - Key Exchange: TLS supports all of the key exchange techniques
    - Symmetric Encryption Algorithms: TLS includes all of the symmetric encryption algorithms

- TLS protocol accomplishes :
    - Encryption
    - Authentication
    - Integrity

APPLICATION LEVEL SECURITY :

SECURE ELECTRONIC TRANSACTION

- Secure Electronic Transaction or SET is a security protocol designed to ensure the security and integrity of electronic transactions conducted using credit cards.
- Unlike a payment system, SET operates as a security protocol applied to those payments.
- It uses different encryption and hashing techniques to secure payments over the internet done through credit cards.
- It is not itself a payment system
- It is a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network, such as the internet, in a secure fashion

1. **SET provides three services**
    - It provides a secure communications channels among all parties involved in a transaction
    - Provides trust by the use of digital certificates
    - Ensures privacy because the information is only available to parties in a transaction when and where necessary.

2. **Requirements in SET**

- The SET protocol has some requirements to meet, some of the important requirements are:

    - It has to ***provide mutual authentication***
      i.e., customer (or cardholder) authentication by confirming if the customer is an intended user or not, and merchant authentication.

- It has to keep the PI (Payment Information) and OI (Order Information) ***confidential by appropriate encryptions.***

- ***Ensure the integrity of all transmitted data by using digital signatures***
  It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.

- SET also needs to ***provide interoperability*** and make use of the best security mechanisms.

- Ensure use of best security practices and system design techniques

- Create a protocol that neither depends on transport securities (SSL/TLS)

3. Participants in SET

In the general scenario of online transactions, SET includes similar participants:

- **Cardholder –** customer or authorized holder of a payment card that has been issued by an issuer

- **Issuer –** customer financial institution , such as bank , that provides the cardholder with the payment card

- **Merchant –** A person or an organization that has goods and services to sell to the cardholder

- **Acquirer –** Merchant financial or financial institution that establishes an account with a merchant and processes payment card authorizations and payments

- **Certificate authority –** Authority that follows certain standards and issues certificates (like X.509V3) to all other participants.

- **Payment Gateway** – Function operated by the acquirer or a designated third party that processes merchant payment messages

4. SET functionalities

- **Provide Authentication**

- **Merchant Authentication**

  To prevent theft, SET allows customers to check previous relationships between merchants and financial institutions. Standard X.509V3 certificates are used for this verification.

- **Customer / Cardholder Authentication**

  SET checks if the use of a credit card is done by an authorized user or not using X.509V3 certificates.

- **Provide Message Confidentiality**

  Confidentiality refers to preventing unintended people from reading the message being transferred.

  SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purposes.

- **Provide Message Integrity**

  SET doesn't allow message modification with the help of signatures.

  Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1

- **Dual Signature**

  The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers :

  Order Information (OI) for merchant &
  Payment Information (PI) for bank

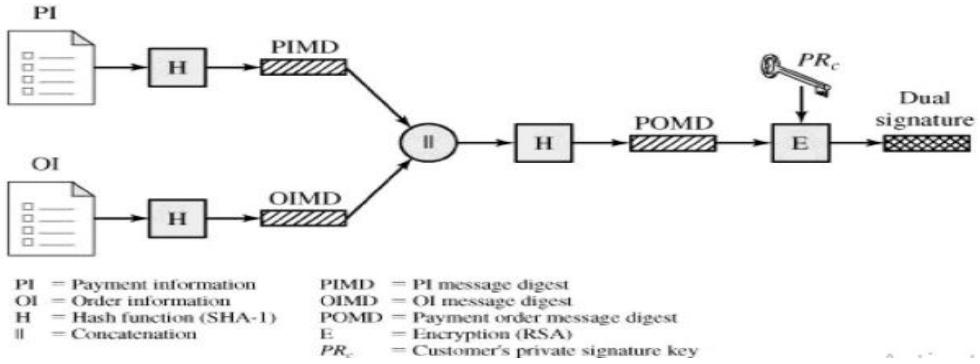
5. SET Transaction Steps

1. The customer opens an account
2. The customer receives the certificate
3. Merchants have their own certificates
4. The customer places an order
5. The merchant is verified
6. The order and payments are sent
7. The merchant requests payment authorization
8. The merchant confirms the order
9. The merchant provides the goods or services
10. The merchant request payment

DUAL SIGNATURE

- The purpose of the dual signature is to link two messages that are intended for two different recipients.
- In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank.
- The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order.
- The customer is afforded extra protection in terms of privacy by keeping these two items separate.
- However, the two items must be linked in a way that can be used to resolve disputes if necessary.
- The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods or service.
- To the need for the link, suppose that the customers send the merchant two messages: a signed OI and a signed PI, and the merchant passes the PI on to the bank.
- If the merchant can capture another OI from this customer, the merchant could claim that this OI goes with the PI rather than the original OI.
- The linkage prevents this.

Figure below shows the use of a dual signature to meet the requirement :



- The customer takes the hash (using SHA-1) of the PI and the hash of the OI.
- These two hashes are then concatenated and the hash of the result is taken.
- Finally, the customer encrypts the final hash with his or her private signature key, creating the dual signature. The operation can be summarized as

$$DS = E(PRc, [H(H(PI) || H(OI)])$$

where PRc is the customer's private signature key.

- Now suppose that the merchant is in possession of the dual signature (DS), the OI, and the message digest for the PI (PIMD).
- The merchant also has the public key of the customer, taken from the customer's certificate.
- Then the merchant can compute the quantities

$$H(PIMS || H[OI]) ; D(PUc, DS)$$

where PUc is the customer's public signature key.

- If these two quantities are equal, then the merchant has verified the signature.
- Similarly, if the bank is in possession of DS, PI, the message digest for OI (OIMD), and the customer's public key, then the bank can compute

$$H(H[OI]||OIMD); D(PUc, DS)$$

- Again, if these two quantities are equal, then the bank has verified the signature.
- In summary,
    1. The merchant has received OI and verified the signature.
    2. The bank has received PI and verified the signature.
    3. The customer has linked the OI and PI and can prove the linkage.

Advantages & Disadvantages of SET

- The security properties of SET are better than SSL and the more current TLS,
- The **greatest downside of SET is its intricacy.**

Ie, SET requires the two clients and traders to introduce extraordinary programming .SSL and TLS don't have such issues.

- The above associated with PKI and the instatement and enlistment processes additionally slowed down the far reaching reception of SET.
- **Interoperability among SET items**