An undertaking of Bhaktapur Municipality
Khwopa College of Engineering
Affiliated to Tribhuvan Univeristy
Libali, Bhaktapur, Nepal

A
Note
on
Computer Network

Compiled By

Er. Dinesh Ghemosu

Table of Contents

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have our position unassailable.

- The Art of War, Sun Tzu.

8

Network Security

8.1 Background

- *Information security* was provided, before digital age, in an organization by physical and administrative means e.g. Filing cabinet with locking system, personnel screening at the time of recruitment etc.
- With the introduction of computers, and development of shared systems, public telephone networks, data networks and the internet, the term *Computer securit*y was defined as "A collection of tools designed to protect data and to thwart hackers."
- Distributed systems and the use of network and communications facilities give rise to the need of security measures to protect data during their transmission, and hence the term *Network securit*y was introduced.
- Nowadays, most organizations interconnect their data processing equipment's with inter-connected networks (i.e. internet). So, the term *internet security* is used.

8.2 Security Violation

Scenario 1:
User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure. User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission

Scenario 2:
A network manager, D, transmits a message to a computer, E, under its management. The message instructs computer E to update an authorization file to include the identities of a number of new users who are to be given access to that computer. User F intercepts the message, alters its contents to add or delete entries, and then forwards the message to E, which accepts the message as coming from manager D and updates its authorization file accordingly.

Scenario 3:
Rather than intercept a message, user F constructs its own message with the desired entries and transmits that message to E as if it had come from manager D. Computer E accepts the message as coming from manager D and updates its authorization file accordingly.

Scenario 4:
An employee is fired without warning. The personnel manager sends a message to a server system to invalidate the employee's account. When the invalidation is accomplished, the server is to post a notice to the employee's file as confirmation of the action. The employee is able to intercept the message and delay it long enough to make a final access to the server to retrieve sensitive information. The message is then forwarded, the action taken, and the confirmation posted. The employee's action may go unnoticed for some considerable time.

Scenario 5:
A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.

8.3 Computer Security

- The NIST (National Institute of Standards and Technology) Computer Security Handbook[NIST95] defines the term computer security as:

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources includes hardware, software, firmware, information/data, and telecommunications).

- This definition includes three key objectives that are at the heart of computer security.

- Confidentiality
- Integrity
- Availability

- These three concepts form what is often referred to as ***CIA triad***.

8.3.1 The CIA Triad: Confidentiality

Confidentiality: This term covers two related concepts:
- *Data confidentiality*: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

- *Privacy*: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

8.3.2 The CIA Triad: Integrity

Integrity: This term covers two related concepts:
- *Data integrity*: Assures that information and programs are changed only in a specified and authorized manner.

- *System integrity*: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

8.3.3 The CIA Triad: Availability

- **Availability**: Assures that systems work promptly and service is not denied to authorized users. - Assures that systems work promptly and service is not denied to authorized users.

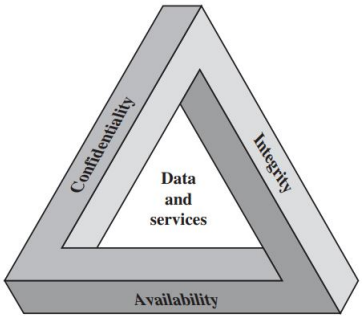


Figure 8.1: The CIA traid.

8.3.4 The CIA Triad: Security Characteristics

- FIPS 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Additional concepts for complete picture:
Authenticity
- The property of being genuine and being able to be verified and trusted.

Accountability
- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

8.4 The OSI Security Architecture

The ITU-T (International Telecommunication Union Telecommunication Standardization Sector) Recommendation X.800, Security Architecture for OSI, gives structured definition of security attacks, security mechanism and security services.

Security attack: Any action that compromises the security of information owned by an organization.

Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. Examples: encipherment, digital signature, access control etc.

Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. It includes authentication, access control, data confidentiality, data integrity and non-repudiation.

According to RFC 4949:

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack
An intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

8.5 Security Threat

- A *threat* is a potential violation of security which might or might not occur.
- The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for).
-Those actions are called *attacks*.
- Those who execute such actions, or cause them to be executed, are called *attackers*.

Class of Security Threat:
Security Threats divided into four broad classes:

- **Disclosure**, an unauthorized access to information.

- **Deception**, an acceptance of false data.
- **Disruption**, an interruption of prevention of correct information.
- **Usurpation**, an unauthorized control to some part of a system.

8.6 Security Attacks

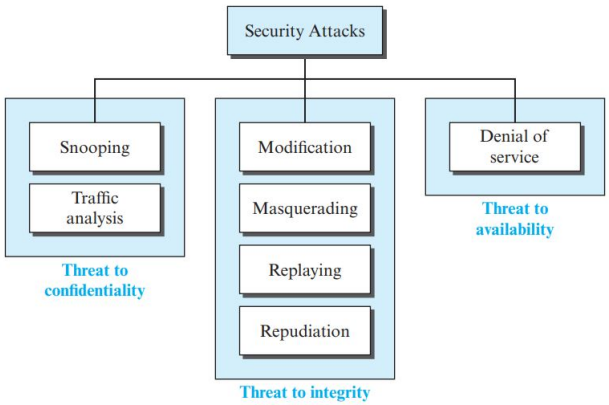


Figure 8.2: The CIA traid.

Security attacks are classified as:
1. Passive Attacks
2. Active Attacks

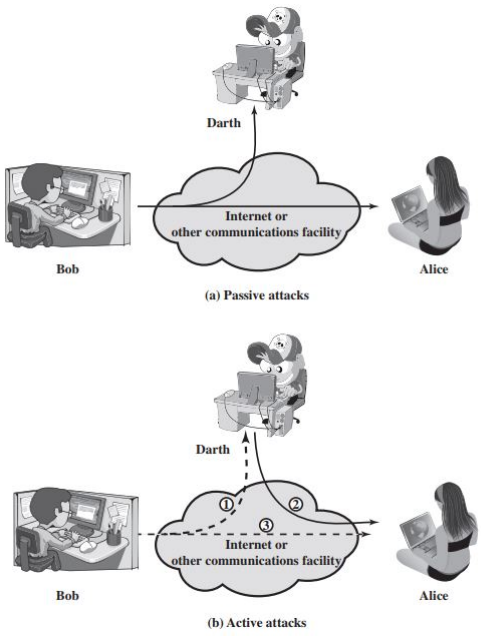


Figure 8.3: Security attacks.

8.6.1 Passive Attacks

- Passive attack attempts to learn or make use of information from the system but does not affect system resources.
- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
- Two types:

i. The release of message
ii. Traffic analysis

- Passive attacks are very difficult to detect, because they do not involve any alternation of the data.
- But it is feasible to prevent by means of encryption.

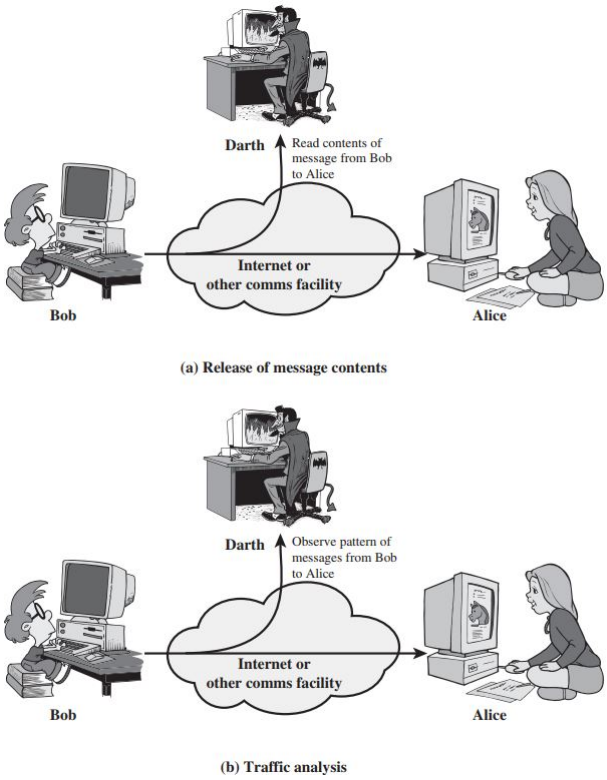


Figure 8.4: Passive network security attacks.

8.6.2 Active Attacks

- Active attacks attempt to alter system resources or affect their position.
- It involves some modification of the data stream or the creating of a false stream.
- Active attacks are quite difficult to be absolutely prevented because of the wide variety of potential physical, software, and network vulnerabilities.
- Examples of active attacks are:

  – Masquerade

  – Replay

  – Modification of messages,

  – Denial of service, etc.

Snooping:
- Snooping refers to unauthorized access to or interception of data.
- For example, a file transferred through the Internet may contain confidential information. An unauthorized entity may intercept the transmission and use the contents for her own benefit.

Traffic Analysis:
- Unauthorized access to information by observing the monitoring online traffic.
- For example: observing and collecting the email address, nature of transactions etc.

Modification:
- Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
- For example, a message meaning “Allow John Smith to read confidential file accounts” is modified to mean “Allow Fred Brown to read confidential file accounts.”

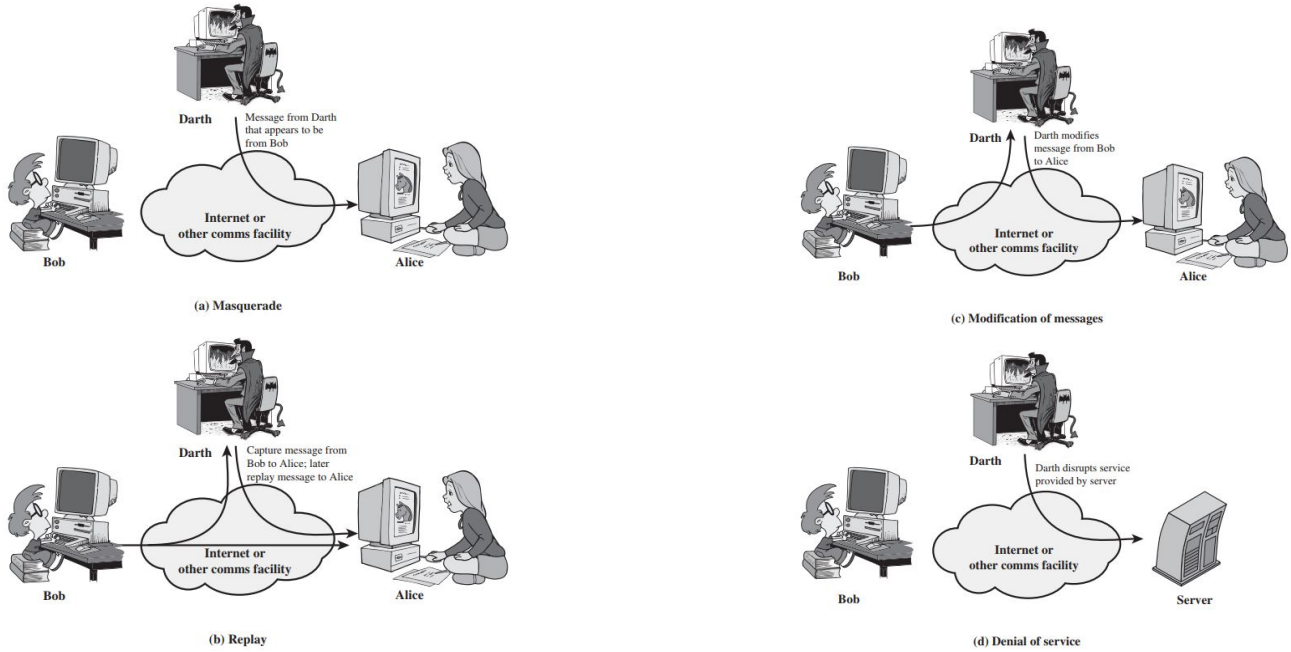


Figure 8.5: Active passives.

Masquerade:
- Masquerade takes place when the attacker impersonate somebody else.
- If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.
- For example: gaining access to the account of a legitimate user either by stealing the victim's account ID and password.

Replay:
- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Repudiation:
- This type of attack is different from others because it is performed by one of the two parties in the communication: the sender or the receiver.
- The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

Denial of Service:
- The denial of service prevents or inhibits the normal use or management of communications facilities.
- This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service).
- Another form of service denial is the disruption of an entire network—either by disabling the network or by overloading it with messages so as to degrade performance.

8.7 Network Security Model

- A message is to be transferred from one party to another (called principals) across some sort of Internet service (through a logical information channel) by the cooperation of a communication protocol (e.g. TCP/IP).
- It is necessary to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity etc.

Techniques for providing security have two components:
1. A security-related transformation on the information to be sent e.g.
   - Include the encryption of a message so as to make in unreadable by the opponent,

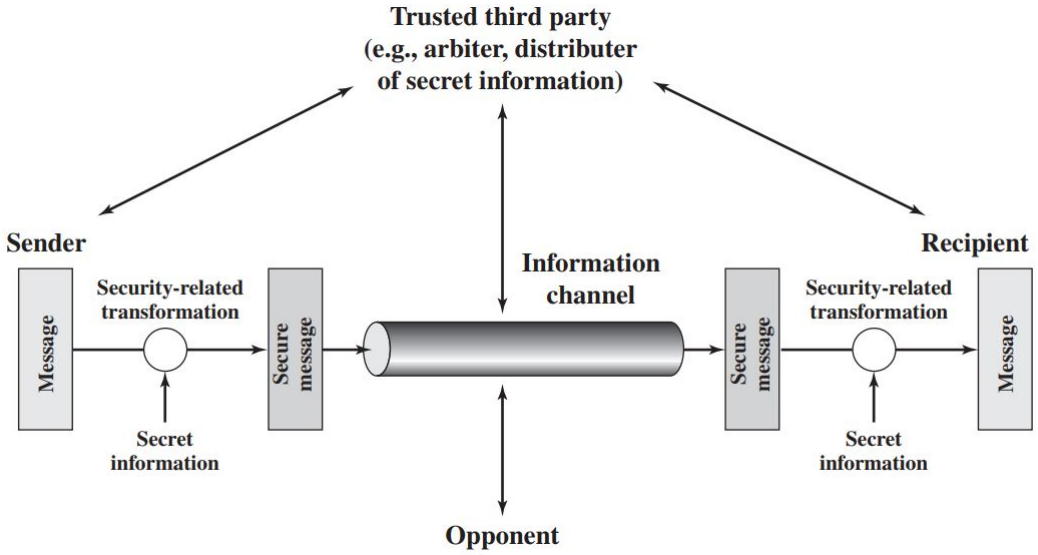


Figure 8.6: Network Security Model.

- Addition of code based on the contents to verify the identity of the sender.

2. Some secret information shared by two principals only. E.g.
   - an encryption key to scramble and unscramble the message.

A trusted third party may be needed to achieve secure transmission. For example
- distributing the secret information to the two principals while keeping it away from its opponent.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm

Properties of Secure Communication:

- Confidentiality
- Authentication
- Message integrity
- Authorization
- Non-repudiation
- Availability

8.8 Cryptography

- *Cryptography*, a word with Greek origins, means “secret writing.” and is the art and science of concealing meaning.
- The Concise Oxford English Dictionary (9th ed.) defines cryptography as “the art of writing or solving codes." This is historically accurate, but does not capture the current breadth of the field or its modern scientific foundations. The definition focuses solely on the codes that have been used for centuries to enable secret communication.
- But cryptography nowadays encompasses much more than this: it deals with mechanisms for ensuring integrity, techniques for exchanging secret keys, protocols for authenticating users, electronic voting, cryptocurrency, and more.
- Modern cryptography involves the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks.
- It involves three distinct mechanisms: symmetric-key encipherment, asymmetric-key encipherment, and hashing.

- It is the techniques of converting ordinary plain text into unintelligible text and vice-versa.
- It is the practice and study of techniques for secure communication in the presence of third parties.
- Techniques used for deciphering message without any knowledge of the enciphering details fall into the area of cryptanalysis. *Cryptanalysis* is what the layperson calls "breaking the code".
- The area of cryptography and cryptanalysis together are called *cryptology*.

- Before message is sent by the sender to the network , the message the user entered (plain-text) will be encrypted (converting plain-text to cipher-text) and after receiving the cipher-text will be decrypted (converting cipher-text to plain-text) and used by receiver.
- Encryption and decryption algorithms are referred as *ciphers*.

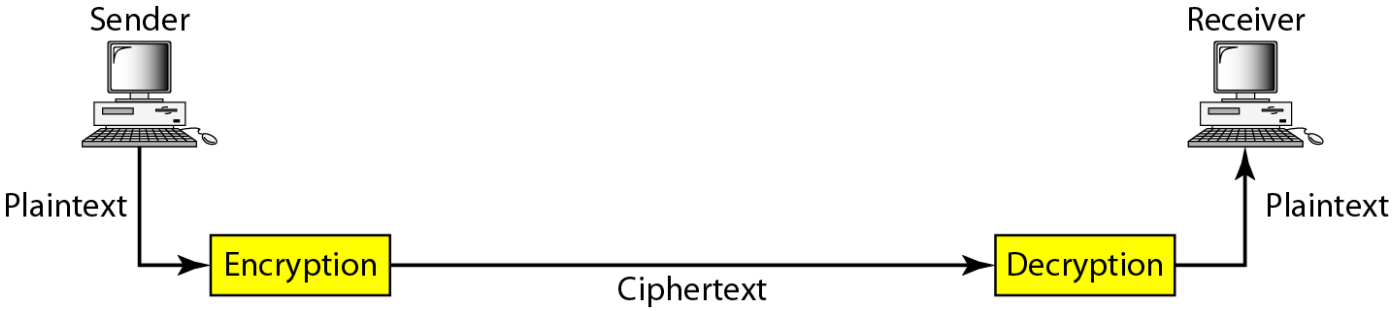


Figure 8.7: Encryption and decryption.

Cryptography Basic Terminology:

- **Plain text**: Original message fed to encryption algorithm; readable.
- **Encryption algorithm**: changes plain text to coded ciphertext by various substitution and transformation methods. The process of converting plaintext to ciphertext is called enciphering or encryption.
- **key**: input to the encryption algorithm. Known to sender and receiver only.
- **Ciphertext**: coded/scrambled output message by the algorithm. Different secret key applied on plain text produces different ciphertext.
- **Decryption Algorithm**: the encryption algorithm that run in reverse i.e. takes ciphertext and key to produce the original transmitted plain text. The process is known as deciphering or decryption

Encryption and Decryption:

Encryption

- Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized Cannot.
- Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor.

Decryption

- Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand (original form).
- It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

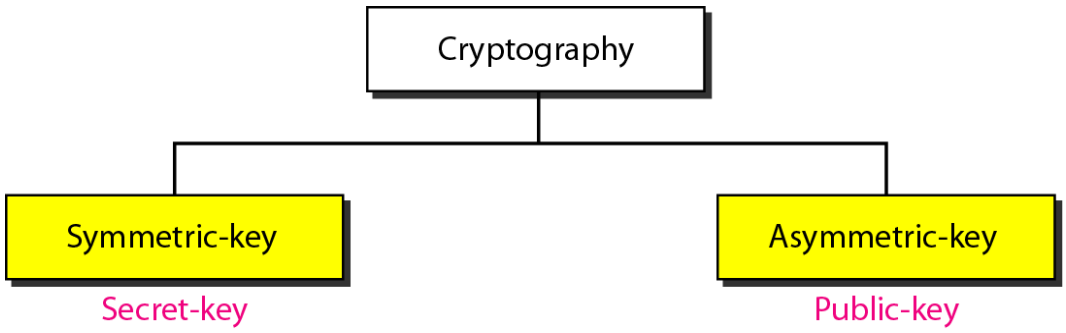


Figure 8.8: Types of cryptography.

8.9 Symmetric Key Cryptography

- Symmetric encryption (also called *classical cryptosystems*), also referred to as *conventional encryption*, *secret-key*, or *single-key encryption*, was the only type of encryption in use prior to the development of public-key encryption in the late 1970s.
- Same key is shared by sender (for encryption) and receiver (for decryption). - Ciphertext is generated either by substitution or transformation method by encryption algorithm.
- A symmetric encryption has five ingredients:

  – Plaintext
  – Encryption algorithm
  – Secret key
  – Ciphertext
  – Decryption algorithm

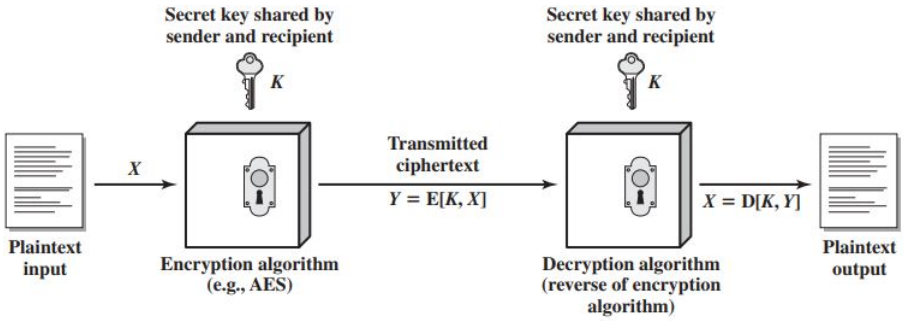


Figure 8.9: Simplified Model of Symmetric Encryption.

There are two requirements for secure use of symmetric encryption:

1. We need a strong algorithm.
   - At minimum, an operator who knows the algorithm and has access to one or more ciphertext would be unable to decipher the ciphertext.
2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

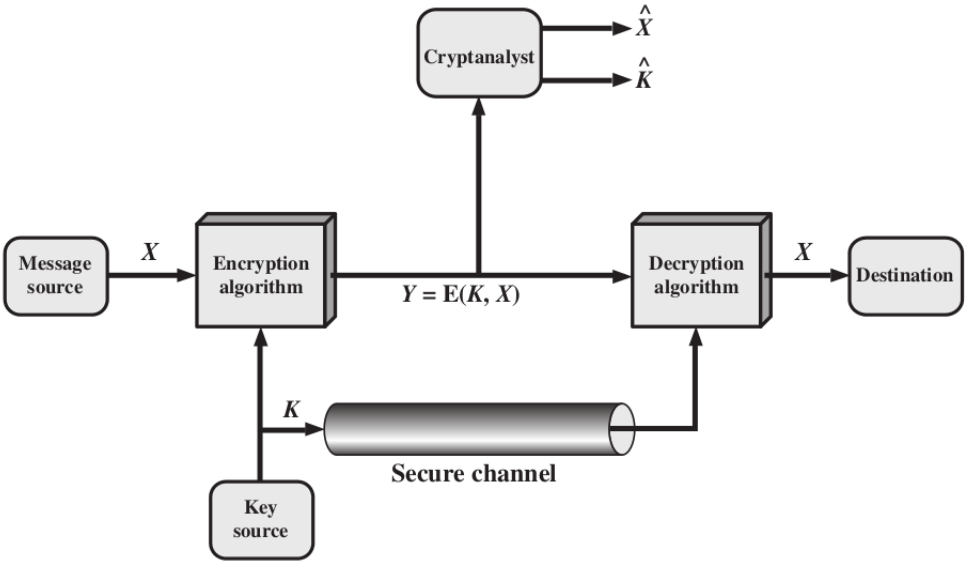


Figure 8.10: Model of symmetric key cryptography.

There are two basic types of classical ciphers:
i. Transposition ciphers, and
ii. Substitution ciphers

8.9.1 Transposition Ciphers

- A transposition cipher does not substitute one symbol for another; instead it changes the location of the symbols.
- A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext.
- A symbol in the eighth position in the plaintext may appear in the first position of the ciphertext.
- In other words, a transposition cipher reorders (transposes) the symbols.

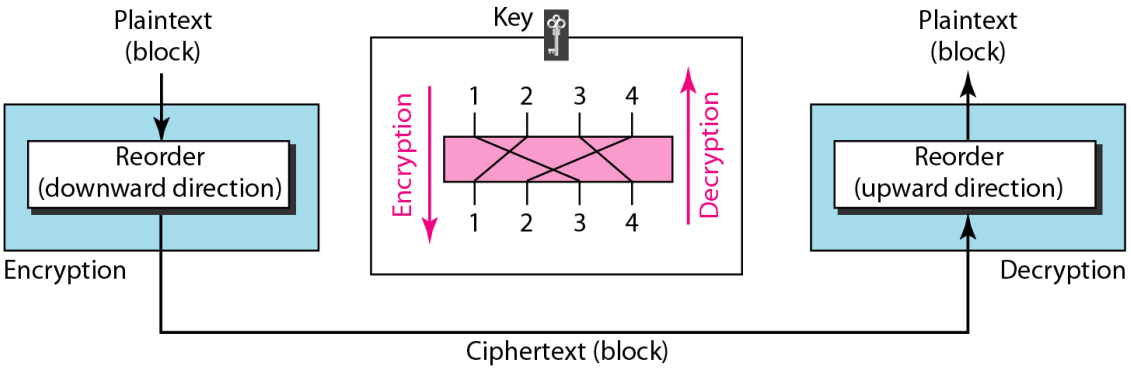


Figure 8.11: Transposition cipher.

For example:
Suppose Alice wants to secretly send the message "Enemy attacks tonight" to Bob. The encryption and decryption is shown in Figure. Note that we added an extra character (z) to the end of the message to make the number of characters a multiple of 5.

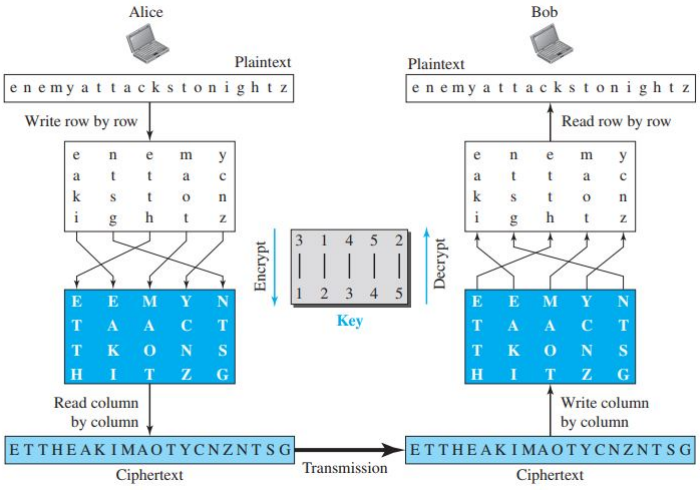


Figure 8.12: An example of substitution cipher.

8.9.2 Subsitution Cipher

- A substitution cipher changes characters in the plaintext to produce the ciphertext.
- For example: Caesar cipher, Vigenere Cipher, One-time pad are example of substitution cipher.

Caesar Cipher

- Substitution cipher
- Shift cipher
- Earliest known and simplest substitution scheme developed by Julis Ceasar.
- Replaces each letter of the alphabet with the letter standing three places further down the alphabet.
  plain: meet me after the toga party
  cipher: PHHW PH DIWHU WKH WRJD SDUWB
- A Caesar cipher is susceptible to a statistical ciphertext-only attack.

8.10 Data Encryption Standard (DES)

- The Data Encryption Standard (DES) works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key.
- It is a symmetric key cryptography.
- Symmetric key algorithm in which data are encrypted in 64-bit blocks using a 56-bit key.

- Originally designed by researchers at IBM in the early 1970s, DES was adopted by the U.S. government as an official Federal Information Processing Standard (FIPS) in 1977 for the encryption of commercial and sensitive yet unclassified government computer data.
- It was the first encryption algorithm approved by the U.S. government for public disclosure.

- The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time.
- To encrypt a plaintext message, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit ciphertext by means transposition and substitution.

DES Encrpytion:

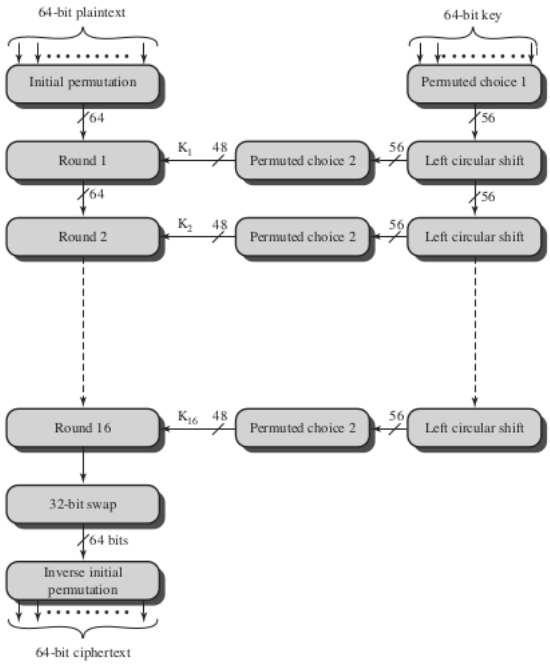


Figure 8.13: General Depiction of DES Encryption Algorithm.

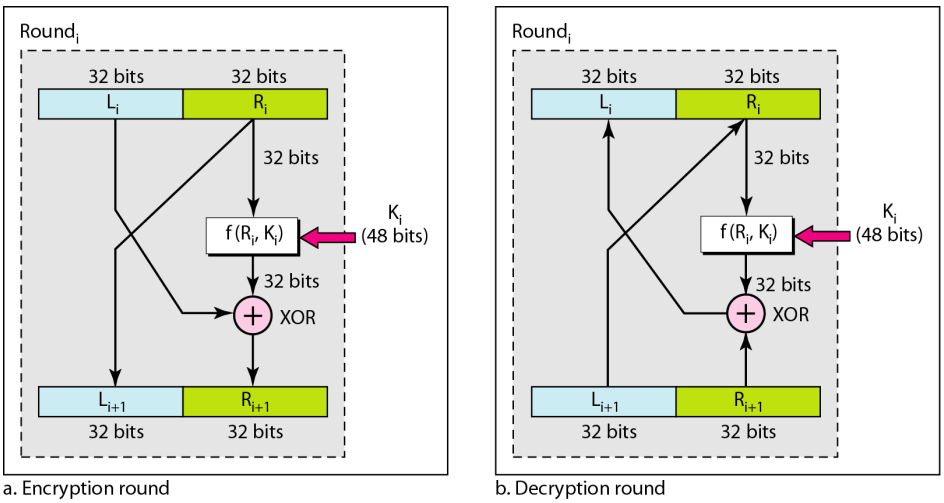


Figure 8.14: One round in DES.

- The process involves 16 rounds and encrypting blocks individually or making each cipher block is dependent

on all the previous blocks.
- DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).
- The check bits or parity bits are used to check if the key was indeed correctly retrieved.

- The rounds are executed sequentially, the input of one round being the output of the previous round.
- The right half of the input, and the round key, are run through a function f that produces 32 bits of output; that output is then XOR'ed into the left half, and the resulting left and right halves are swapped.

- The keys for each round is separate which is just the result of left circular shift operation of the original key.
- The round key generator is the component which is responsible to generate 16 sub keys for 16 rounds.
- The round operation is nothing but the XOR operation between the plain text and the key. The final key to the cipher text is the resulting key at the end of 16 rounds.

- Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied.
- It would take maximum of 2^{56} or 72,057,594,037,927,936 attempts to find the correct key.
- For any cipher, the most basic method of attack is brute force, which involves trying each key until you find the right one.

- Even though few messages encrypted using DES encryption are likely to be subjected to this kind of code-breaking effort, many security experts felt the 56-bit key length was inadequate even before DES was adopted as a standard.
- Thus, DES is upgraded to more secure Advanced Encryption Standard (AES).

8.11 Public Key Cryptography

- Also known as Public Key Cryptography.
- Used two keys: *public-key* and *private key*.

Public key:
- Shared with the public who wants to communicate with the receiver.
- Used for enciphering the sender's plaintext into cipher text.

Private key
- Is kept secret by the receiver.
- Used to deciphering ciphertext into plaintext by the receiver.
- Proposed by Diffie and Hellman in 1976
- RSA uses public-key cryptosyst

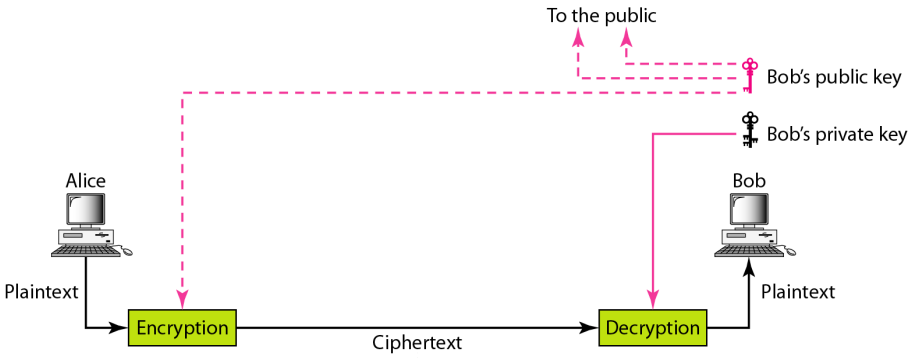


Figure 8.15: Asymmetric key cryptography.

The essential steps:

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register or other accessible file.
3. This is the public key. The companion key is kept private. As Figure suggests, each user maintains a collection of public keys obtained from others.

4. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
5. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

Because one key is public, and its complementary key must remain secret, a public key cryptosystem must meet the following three conditions:

1. It must be computationally easy to encipher and decipher a message given the appropriate key.
2. It must be computationally infeasible to derive the private key from the public key.
3. It must be computationally infeasible the private key from a chosen plaintext attack.

8.12 RSA Algorithm

- Developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978.
- Most widely used asymmetric key encryption.
- Used in security protocol such as IPSEC, SSH, TLS etc.
- The RSA scheme is a cipher in which the plaintext and ciphertext are integers between 0 and $n-1$ for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 2^{1024} .

- RSA uses two exponents, e and d, where e is public and d is private. Suppose P is the plaintext and C is the ciphertext. Alice uses $C = P^e \bmod n$ to create ciphertext C from plaintext P; Bob uses $P = C^d \bmod n$ to retrieve the plaintext sent by Alice. The modulus n, a very large number, is created during the key generation process.

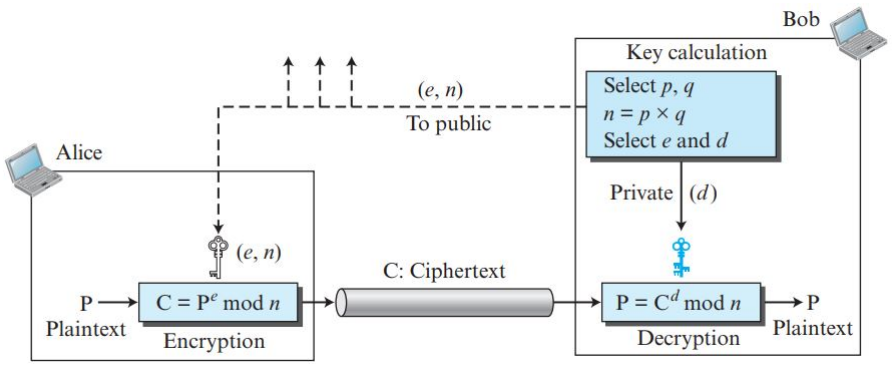


Figure 8.16: Encryption, decryption and key generation used in RSA.

- A user of RSA creates and then published a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret.
The RSA algorithm involves four steps:

- Key generation
- Key distribution
- Encryption
- Decryption

RSA: Key Generation
The keys for RSA algorithm are generated in the following way:

1. Generate two large random prime numbers, p and q. (p and $q \geq 2^{512}$).
2. Compute $n = p \times q$, n is called modulus.
3. Compute the totient $\phi(n) = (p-1)(q-1)$.
4. Choose e such that $1 < e < \phi(n)$, where e and $\phi(n)$ do share factors other than one i.e. $gcd(e, \phi(n)) = 1$).
5. Computer d such that $d \times e = 1 \bmod \phi(n)$ (i.e.$de\{mod\phi(n)\} = 1$
6. Publish e and n as the public key (Sender's public key) for encryption.
7. Keep d and n as private key (Receiver's private key) for decryption.

RSA:Key Generation
- The totient $\phi(n)$ of positive integer n is the numbers less than n with no factors in common with n (i.e. they share no factors except 1).

- *For example*:
Let n = 10. The numbers that are less than 10 and are relatively prime to (have no factors in common with) n are 1,3,7, and 9. Hence,$\phi(n)$ = 4. Similarly, if n =21, the numbers that are relatively prime to n are 1,2,4,5,8,10, 11, 12, 13,16,19, and 20. So $\phi(n)$=12.

RSA: Key Distribution
- Suppose that Bob wants to send information to Alice. IF they decide to use RSA, Bob must know Alice's public key to encrypt the message and Alice must use her private key to decrypt the message.
- To enable Bob to send his encrypted messages, Alice transmit her public key (e ,n) to Bob via a reliable,but not necessarily secret, route. Alice' private key (d, n) is never distributed.

RSA : encryption and decryption
Given public key (e ,n) and private key (d, n) are computed

- To encrypt bit pattern, P, compute cipher text C as:
$C = P^e \bmod n$

- To decrypt bit pattern, C, compute
$P = C^d \bmod n$

RSA Example:
Pick two prime numbers: p=3, q = 5.
$n = p \times q = 3 \times 5 = 15$
$\phi(n) = (p-1)(q-1) = (3-1)(5-1) = 2 \times 4 = 8$.
Choose e satisfying $1 < e < \phi(n)$.
Let us choose e=3,which do not share any common factors with 8 rather than 1.
Compute d satisfying de mod $\phi(n)$=1
So $d \times 3 \bmod 8 = 1$
Let us choose d =11 which satisfy the relation.

- So public key (e,n) is (3,15) which is released publicly and the persons that want to send the message use this key to encrypt the message and send it to the receiver.
- Private key(d,n) is (11,15) which is kept secret by the receiver.

Let us consider the message be 2.
So, at encryption process, the sender uses the public key to encrypt the message. Resulting cipher text will be:
$C = m^e$ (mod n) = 2^3 (mod 15) = 8.
At decryption process, the private key is used to decrypt the cipher text. Plain text is obtained as:
$P = c^d$ (mod n) = 8^{11} (mod 15) = 2.
Hence the original message 2 is obtained at receiver end after decryption.

8.13 Digital Signature
- Digital signature is the most important work on public-key cryptography.
- Digital signature is an electronic analogue of a written signature.
- It can be used to provide assurance that the claimed signatory signed the information.
- It may be used to detect whether or not the information was modified after it was signed.

- For a given message, **M**, a digital signature, **S**, is appended to the message.
- The signature is realized as a function with the message M and the private key as input.
- The public key and the message M are the inputs to the verification function.

- The digital signature must have the following properties:

i. It must verify the author and the date and time of the signature.
ii. It must authenticate the contents at the time of the signature.
iii. It must be verifiable by third parties, to resolve disputes.

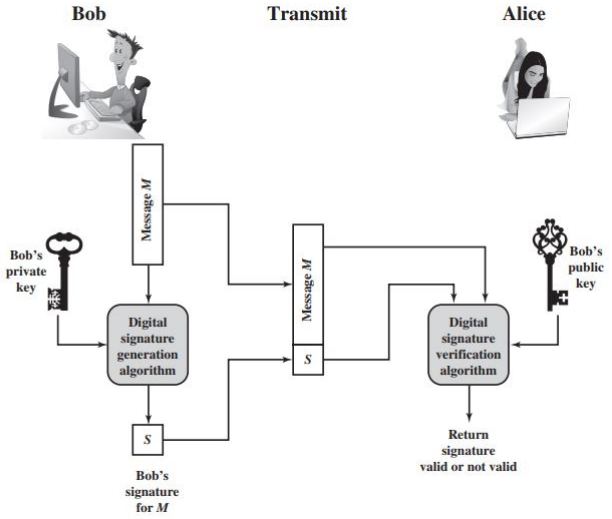


Figure 8.17: Generic model of digital signature.

- Thus, the digital signatures function includes the authentication function.

- To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed.
- The private key is then used to encrypt the hash. The encrypted hash is the digital signature.
- The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter.
- This saves time since hashing is much faster.

- The value of the hash is unique to the hashed data.
- Any change in the data, even changing or deleting a single character, results in a different value.
- This attributes enables others to validate the integrity of the data by using the signer's public key to decrypt the hash.
- If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed.
- Of the two hashes don't match, the data has either been tempered with in some way (integrity) or the signature was created with a private key that doesn't correspond to the public key presented by the signer (authentication).

Types:
i. Direct Digital Signature
ii. Arbitrated Digital Signature

8.14 PGP: Pretty Good Privacy

- PGP is an open-source, freely available software package for e-mail security. It provides authentication through the use of digital signature, confidentiality through the use of symmetric block encryption, compression using the ZIP algorithm, and e-mail compatibility using the radix-64 encoding scheme.
- PGP incorporates tools for developing a public-key trust model and public-key certificate management. - PGP has grown explosively and is now widely used. A number of reasons can be cited for this growth.

- Independent of operating system; can run of different platforms such as unix, windows, mac etc.
- Use widely used cryptographic algorithms; includes RSA, DSS, and Diffie-Hellman for public-key encryption; CAST-128, IDEA, and 3DES for symmetric encryption; and SHA-1 for hash coding.
- Open source: documentation, source code and packages freely available
- Used in wide range of applications.
- PGP is now on an Internet standards track (RFC: 3156)

8.14.1 PGP Services

- The PGP operation provides four services: authentication, confidentiality, compression, and e-mail compatibility.

Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed for storage or transmission using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

Figure 8.18: PGP services.

Notation Uses:
K_s = session key used in symmetric encrpytion scheme.
PR_a = private key of user A, used in public-key encryption scheme.
PU_a = public key of user A, used in public-key encryption scheme.
EP = public-key encrpytion.
DP = public-key decrpytion.
EC = symmetric encryption.
DC = symmetric decryption.
H = hash function.
$||$ = concatenation.

8.14.1.1 PGP Operation: Authentication

1. The sender creates a message.
2. SHA-1 is used to generate a 160-bit hash code of the message.
3. The hash code is encrypted with RSA using the sender's private key, and the result is prepended to the message.
4. The receiver uses RSA with the sender's public key to decrypt and recover the hash code.
5. The receiver generates a new hash code for the message and compares it with the received hash. If they both matched, the message is accepted otherwise rejected.

8.14.1.2 PGP Operation: Confidentiality

1. The sender generates a message and a random 128-bit number to be used as a session key for this message only.
2. The message is encrypted using CAST-128 (or IDEA or 3DES) with the session key.
3. The session key is encrypted with RSA using the recipient's public key and is prepended to the message.
4. The receiver uses RSA with its private key to decrypt and recover the session key.

8.14.1.3 PGP Operation: Confidentiality and Authetication

1. Can use both services on the same message
   - Create signature and attach to the message.
   - Encrypt both message and signature using CAST-128 (or IDEA or 3DES)
   - Attach RSA/EIGamal

8.14.1.4 PGP Operation: Compression

- By default PGP compress message after signing but before encryption, so can store uncompressed message and signature for later verification.
- Uses ZIP compression algorithm

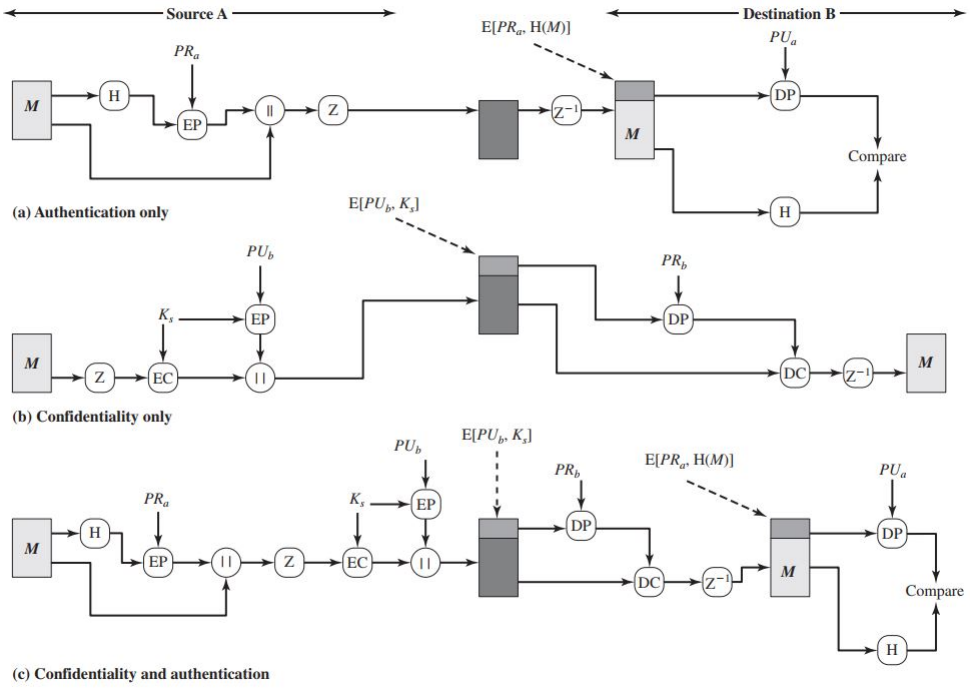


Figure 8.19: PGP cryptographic functions.

8.15 Transport Layer Security: SSL

- SSL stands for *Secure Socket Layer*.
- SSL originally developed by NetScape in 1994.
- SSL v3, designed with public input, became Internet standard known as **Transport Layer Security (TLS)**.
- SSL is a general purpose service implemented as a set of protocols that rely on TCP. - It provide security at transport layer.
- SSL/TSL provides confidentiality using symmetric encryption, data integrity and message authentication between server and client.

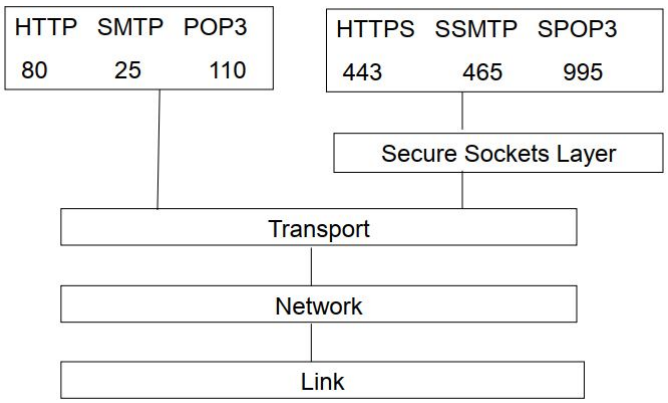


Figure 8.20: SSL uses.

8.15.1 SSL Architecture

- SSL has two layer of protocols which are implemented above the TCP layer.
- The SSL Record Protocol provides basic security services to various higher layer protocols e.g. HTTP.
- Three higher-layer protocols are defined as part of SSL:

i. Handshake protocol
ii. Change cipher Spec Protocol
iii. Alert Protocol

Two important concepts of SSL:

i. **SSL connection**:

- A transient peer-to-peer communication link that provides a suitable type of service. - Every connection is

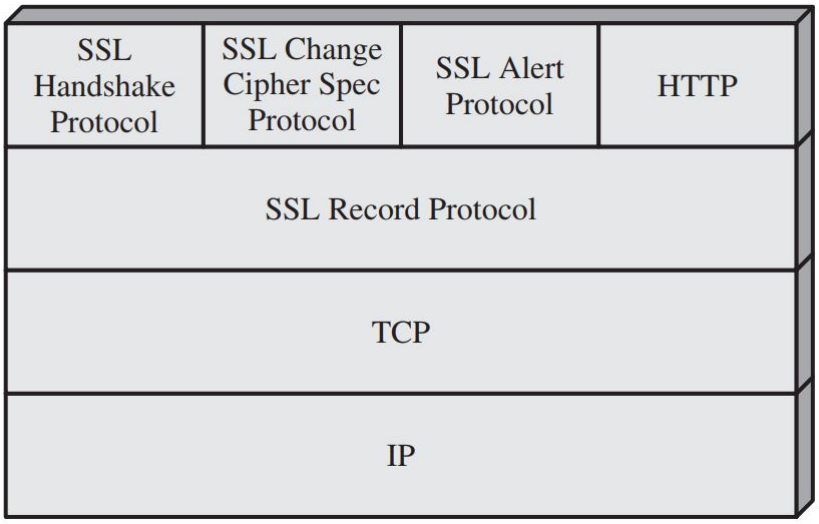


Figure 8.21: SSL protocol stack.

associated with one session.

ii. **SSL session**:
- An SSL session is an association between a client and a server.
- Created by handshake protocol.

SSL Record Protocol
- 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)

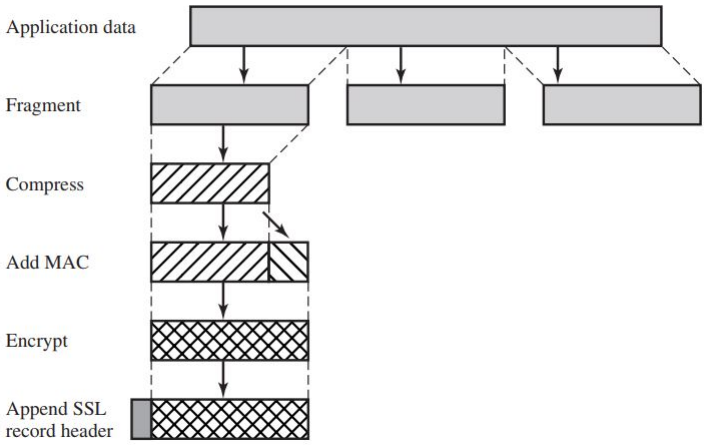


Figure 8.22: SSL protocol operation.

SSH Handshake Protocol:
- Allows server and client to:
  • Authenticate each other
  • To negotiate encryption and MAC (Message Authentication Code) algorithms
  • To negotiate cryptographic keys to be used

Comprises a series of messages exchanged in phases
  • Establish security capabilities
  • Server authentication and key exchange
  • Client authentication and key exchange
  • finish

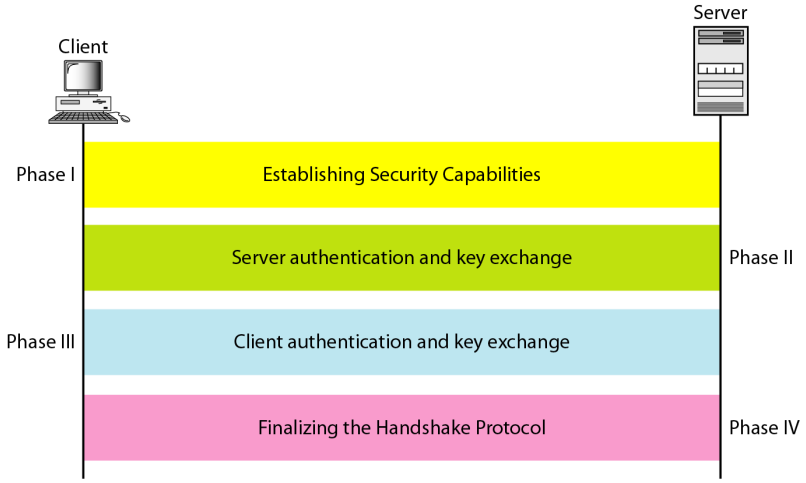


Figure 8.23: SSL handshake protocol.

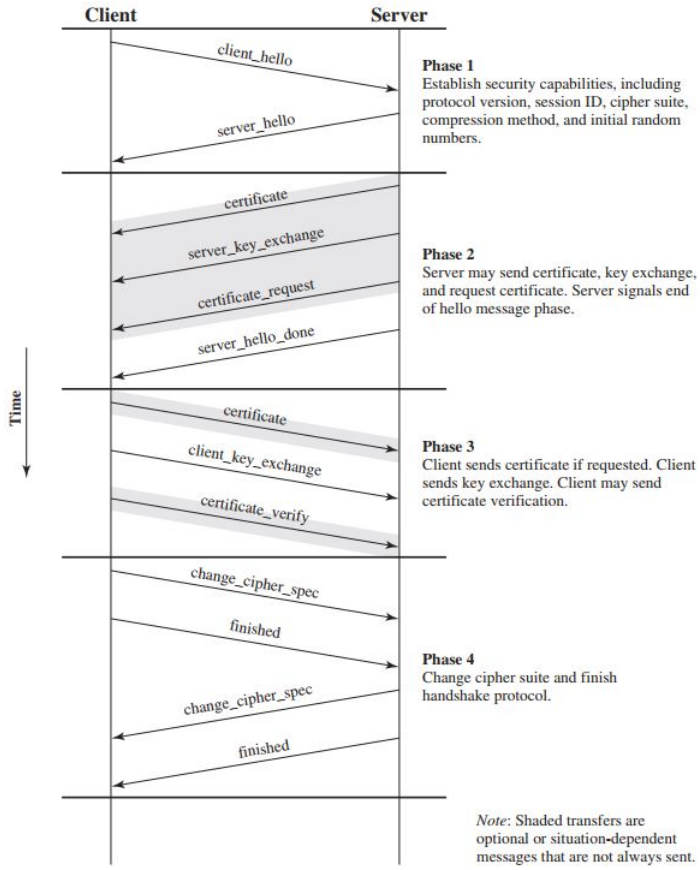


Figure 8.24: SSL handshake protocol action.

SSL Change Cipher Spec Protocol:
- One of 3 SSL specific protocols which use the SSL Record protocol.
- A single message with the value of 1.
- Causes pending state to become current, hence updating the cipher suit in use.

SSL Alert Protocol:
- Used to convey SSL-related alerts to the peer entity.
- SSL alerts are compressed and encrypted like all SSL data.
- Each message in this protocol consists of two bytes. The first byte takes the value warning (1) and fatal (2) to convey the severity of the message. If the level is fatal, SSL immediately terminates the connection.
- Specific alert: Unexpected message, decompression failure, handshake failure, illegal parameters.

8.16 Network Layer Security: IPSec and VPN

8.16.1 IPSec

- IPSec stands for Internet Protocol Security.
- It is a collection of protocols to provide security for a packet at the network layer.
- IPSec is a standard framework for ensuring private communication over public network.
- It has become the most common network layer security control, typically used to create a VPN.
- A VPN is a virtual network built on top of existing physical networks that can provide a secure communication for data transfer.
- VPNs are used most often to protect communication carried over public networks such as the Internet.
- A VPN can provide several types of data protection:
  - Confidentiality
  - Integrity
  - Data origin authentication

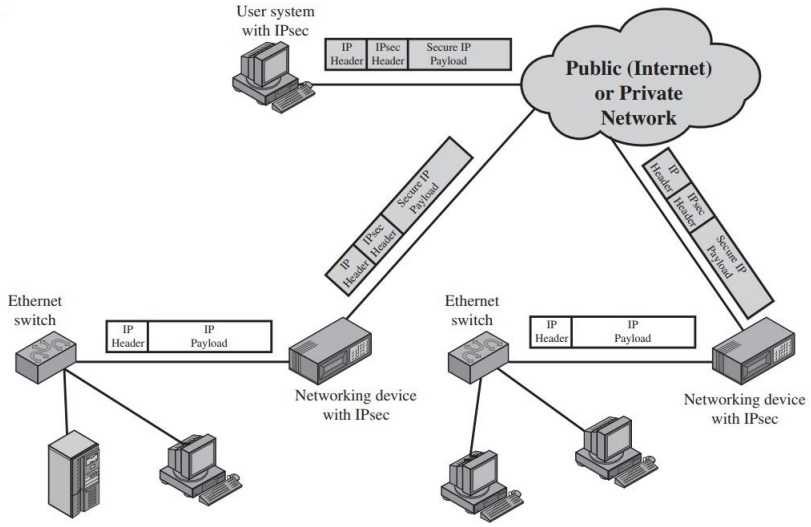


Figure 8.25: An IPSec scenario.

8.16.1.1 Modes of IPSec

IPSec operates in one of two different mode: *transport mode* and t*unnel mode*. **Transport Mode**

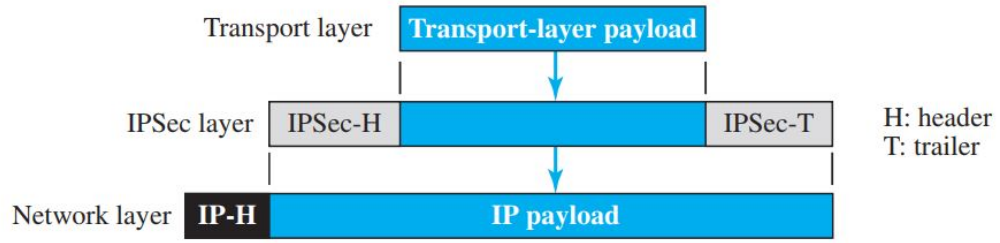
- Transport mode protects the payload to be encapsulated in the network layer i.e. it protects what is delivered from the transport layer to the network layer.
- It does not protect the whole IP header or in other words, it does not protect the whole IP packet.

Tunnel Model

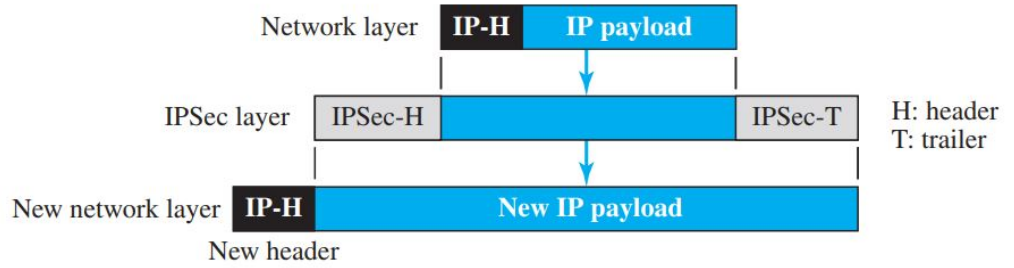
- In tunnel mode, IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header

8.16.1.2 IPSec Components

- Two security protocols :
  - **Authentication Header (AH)**: AH is an extension header to provide message authentication. Because message authentication is provided by ESP, the use of AH is deprecated.
  - **Encapsulating Security Payload (ESP)**: ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication and integrity protection
- Internet Key Exchange (IKE) protocol
  - IPSec uses IKE to negotiate IPSec connection settings.
  - Authenticate endpoints to each other.
  - Define the security parameters of IPSec-protected connections
  - Negotiate secret keys and



(a) An IPSec in transport mode.



(b) Am IPSec in tunnel model.

Figure 8.26: An IPSec model

– Manage, update, and delect IPSec-protected communication channels.

- **IP Payload Compression Protocol (IPComp)**
  - Optionally, Ipsec can use Ipcomp to compress packet payloads before encrypting them.

8.16.1.3 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. Traffic within a company or workgroup does not incur the overhead of security-related processing.
- 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

8.16.1.4 IPSec Applications

- Secure branch office connectivity over the Internet.
- Secure remote access over the internet.
- Establishing extranet and intranet connectivity with partners.

8.16.2 VPN: Vitual Private Network

- One of the applications of IPSec is in virtual private networks.
- VPN creates a network that is private but virtual. It is private because it guarantees privacy inside the organization. It is virtual because it does not use real private WANs; the network is physically public but virtually private.
- It is build on top of existing physical networks and provides a secure communications mechanisms for data and IP information transmitted between networks.
- VPN technology uses the ESP protocol of IPSec in the tunnel mode. Moreover, firewalls, - - VPNs, and IPsec with ESP in tunnel mode are a natural combination and widely used in practice .

- VPSs can use both symmetric and asymmetric forms of cryptography.

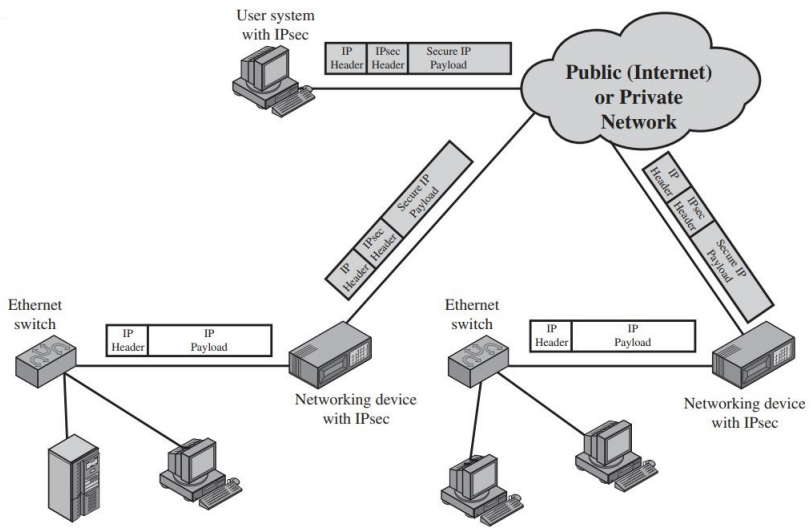


Figure 8.27: An IPSec scenario.

Three primary models for VPN architecture:

1. **Gateway-to-Gateway**
   - Protects communications between two specific networks.
   - Eg. An organization's main office network and a branch office network, or two business partners networks.
2. **Host-to-gateway**
   - Protects communications between one or more individual hosts and a specific network belonging to an organization.
   - Eg. Tranveling employees to gain access to internal organizational services, such as the organization's e-mail and Web servers.
3. **Host-to-Host**
   - Protects communcations between two specific computers.
   - Eg. Small number of users need to use or administer a remote system.

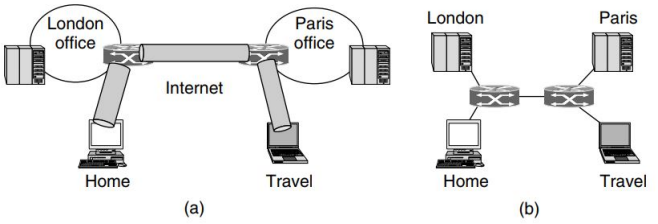


Figure 8.28: a) A VPN b) Topology as seen from the inside.

8.17 Securint Wireless LANs

- IEEE 802.11 is a standard for wireless LAN. (Wi-fi).
- IEEE 802.11i specifies security standard for IEEE 802.11 LANs.

- Wireless networks more vulnerable • No inherent physical protection: sending/receiving message do not need physical access to network infrastructure.

- As a consequence
  - •Eavesdropping is easy.
  - •Injecting bogus message is easy.
  - •Replaying previously recorded message is easy.

•Illegitimate access to network and services is easy.
• of service is easy (jamming).

8.18 WEP: Wireless Equivalent Privacy

- It is the original (first generation) wireless security protocol for the 802.11 standard.
- The stated goal of WEP is to make wireless LAN as secure as a wired LAN.
◇Protocol goals:
•Confidentiality: prevent eavesdropping
•Access control: prevent unauthorized access
•Data integrity: prevent tampering of messages
◇ Failure: none of the security goal is attained.
- It uses RC4 stream cipher, using 64-bit key.

8.18.1 WEP Encryption

Weak Security
- Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5,000 packets.

- Software to crack WEP passwords within a minute is now freely available and the use of WEP is very strongly discouraged.

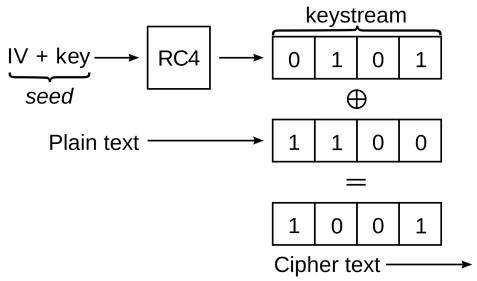


Figure 8.29: XORing operation.

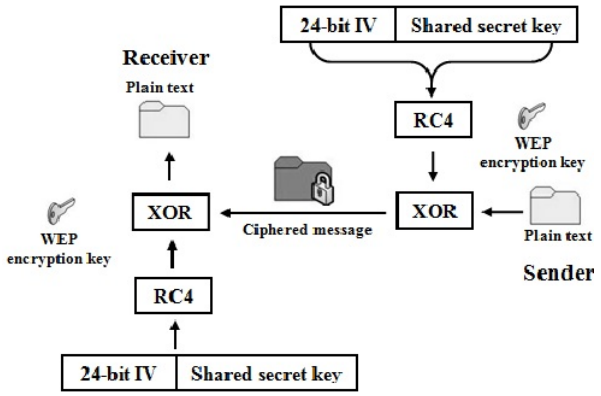


Figure 8.30: Wep encryption.

8.19 WPA: Wifi-Protected Access

- WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard.
- IEEE 802.11i addresses three main security areas: authentication, key management, and data transfer privacy.
- Use Authentication server (AS) for authentication process as well as for key distribution to AP, which in turn manages and distributes keys to stations. Extensible Authentication Protocol (EAU) and Remote Authentication Dial-In User Service (RADIUS) are popular authentication protocol.

8.20 Firewall

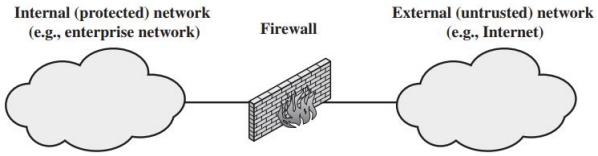


Figure 8.31: A general model of firewall.

- Firewall is a device (usually a router or computers) installed between the internal network of an organization and the rest of the Internet.
- A firewall is a network security system designed to prevent unauthorized access to or from a private network. A firewall security policy dictates which traffic is authorized to pass in each direction.
- A firewall may be designed to operate as a filter at the level of IP packets, or may operate at a higher protocol layer.
- A firewall provides a location for monitoring security-related events as a single-choke point.
- Auditing and controlling access can implement alarms for abnormal behavior.

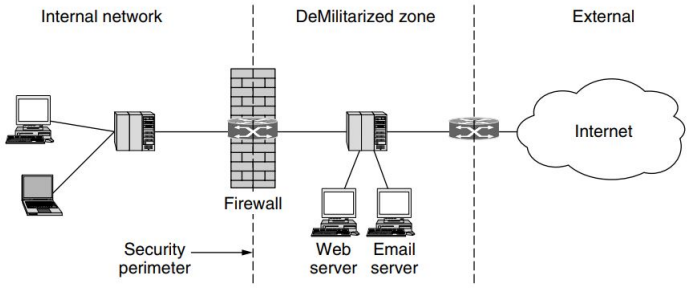


Figure 8.32: A firewall protecting an internal network.

8.20.1 Firewall Design Goals

i. All traffic from inside to outside, and vice-versa, must pass through the firewall. This is achieved by physical blocking all access to the local network except via the firewall.
ii. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.
iii. The firewall itself is immune to penetration; trusted system with a secured OS used to host a firewall.

8.20.2 Firewall Contral Access Methods

Service Control

- Filter traffic on the basis of IP address, protocol or TCP port address.
- Example: block port 80, allow port 23.

Directional Control

- Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

User control

- Controls access to a service according to which user is attempting to access it.
- This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users.

Behaviour control

- Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only.

8.20.3 Scope of Firewall

- The following capabilities are within the scope of a firewall:

i. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.
ii. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
iii. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.
iv. A firewall can serve as the platform for IPsec. Using the tunnel mode capability the firewall can be used to implement virtual private.

8.20.4 Types of Firewalls

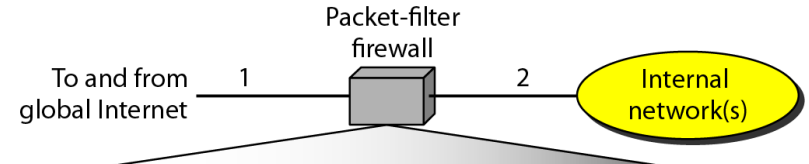
- Packet-Filter Firewall
- Proxy Firewall

8.20.4.1 Packet Filter Firewall

- Packet-Filter Firewall applies a set of rules to each incoming and outgoing IP packet and then forwards of discard the packet.
- Packet filter is based on

- source IP address,
- destination IP address,
- source port address,
- destination port address,
- IP protocol,
- Interface

- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP.



Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Figure 8.33: An example of packet filter firewall.

According to the figure 8.33, the following packets are filtered:

i. Incoming packets from network 131.34.0.0 are blocked (security precaution). Note that the $*$ (asterisk) means "any."
ii. Incoming packets destined for any internal TELNET server (port 23) are blocked.
iii. Incoming packets destined for internal host 194.78.20.8 are blocked. The organization wants this host for internal use only.
iv. Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browse the Internet.

8.20.4.2 Application Gateway Firewall

- Also called application proxy firewall or simply proxy firewall.
- Acts as a relay of application-level traffic.
- It inspect the message of application.

Example:

-As an example, assume that an organization wants to implement the following policies regarding its web pages: only those Internet users who have previously established business relations with the company can have access; access to other users must be blocked. In this case, a packet-filter firewall is not feasible because it cannot distinguish between different packets arriving at TCP port 80 (HTTP). Testing must be done at the application level (using URLs).

• The user contacts the gateway using a TCP/IP application, such as HTTP or FTP, and the gateway asks the user for the name of the remote host to be accessed.

• When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints

8.20.5 Limitation of Firewalls

- IP Snooging:
  • routers can't know if data '"really" comes from claimed source.
  • an intruder can transmit packets from the outside with source IP address field containing an address of an internal host.
- The firewall does not protect against internal threats,
  • Such as a dishonest employee
  • or an employee who unwittingly cooperates with an external attacker.
- The firewall cannot protect against the transfer of virus-infected programs or files.

8.21 Intrusion Detection System

Background

- A significant security problem for networked systems is hostile, or at least unwanted, trespass by users or software.
- User trespass can take the form of unauthorized logon to a machine or, in the case of an authorized user, acquisition of privileges or performance of actions beyond those that have been authorized.
- Software trespass can take the form of a virus, worm, or Trojan horse.

Intrusion:

- One of the key threats to security is the use of some form of hacking by an *intruder*, often referred to as a *hacker* or *cracker*, or *interceptor*.
- *Intrusion* is a phenomenon that performs an activity that compromises a computer system by breaking the security or causing it to enter into an insecure state by an intruder.
- A set of attempts to compromise a computer or a computer network resource security is regarded as an intrusion.

8.21.1 Types of Intruders

Anderson identified three classes of intruders:

- **Masquerader**: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account. The masquerader is likely to be an outsider.
- **Misfeasor**: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges . The misfeasor generally is an insider.
- **Clandestine user**: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection. The clandestine user can be either an outsider or an insider.

8.21.2 Intruder Attacks/Examples of intrusion

Intruder attacks range from the benign to the serious. The following are some examples of intrusions:
- Performing a remote root compromise of an e-mail server.
- Defacing a Web server.
- Guessing and cracking passwords.
- Copying a database containing credit card numbers.
Viewing sensitive data, including payroll records and medical information, without authorization.
- Running a packet sniffer on a workstation to capture usernames and passwords.
- Using a permission error on an anonymous FTP server to distribute pirated software and music files.
- Dialing into an unsecured modem and gaining internal network access.
- Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password.
- Using an unattended, logged-in workstation without permission.

8.21.3 Intrusion Detection

- **Security Intrusion**: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.
- **Intrusion Detection**: A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.
- Intrusion detection is *based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified*.

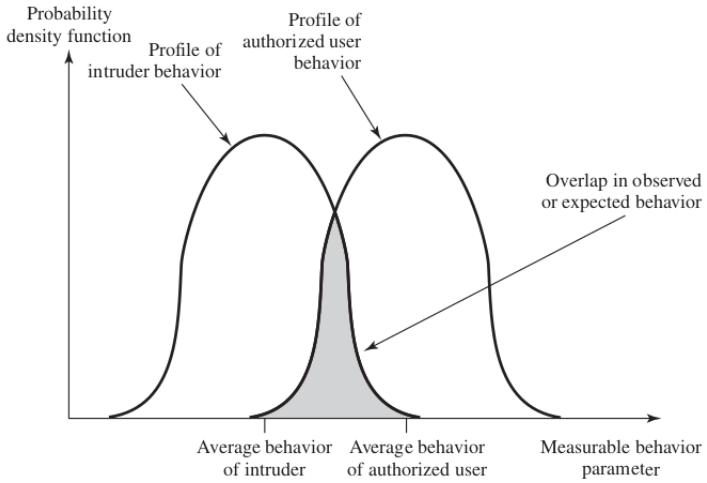


Figure 8.34: Profiles of Behavior of Intruders and Authorized Users.

8.21.3.1 Goals of Intrustion Detection

Detect a wide variety of intrusions.
- Intrusions from within the site, as well as those from outside the site, are of interest.

Detect intrusions in a timely fashion.
- "Timely" here need not be in real time. Often, it suffices to discover an intrusion within a short period of time.

Present the analysis in a simple, easy-to-understand format.

Be accurate.
- A *false positive* occurs when an intrusion detection system reports an attack, but no attack is underway. False positives reduce confidence in the correctness of the results as well as increase the amount of work involved. However, *false negatives* (occurring when an intrusion detection system fails to report an ongoing attack) are worse, because the purpose of an intrusion detection system is to report attacks.

8.21.3.2 Approaches to Intrustion Detection

1. **Statistical anomaly detection**: Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.
   • *Threshold detection*: This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
   • *Profile based*: A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

2. **Rule-based detection**: Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.
   • *Anomaly detection*: Rules are developed to detect deviation from previous usage patterns.
   • *Penetration identification*: An expert system approach that searches for suspicious

8.21.4 IDS: Instrustion Detection System

- Unauthorized intrusion into a computer system or network is one of the most serious threats to computer security.
- ntrusion are the activities that violate the security policy of system: Integrity, confidentiality, or availability, of a computing and networking resource.
- Intrusion detection systems have been developed to provide early warning of an intrusion so that defensive action can be taken to prevent or minimize damage.
- Intrusion detection involves detecting unusual patterns of activity or patterns of activity that are known to correlate with intrusions.

8.21.4.1 Types of IDS

i. Host-based IDS
ii. Network-based IDS
iii. Anomaly detection
iv. Signature based

Host Based IDS

- Various software tools such as Metasploit, Sqlmap, Nmap, Browser Exploitation provide the necessary framework to examine and gather information form target system vulnerabilities. Malicious attackers use such information to launch attacks to various application like FTP servers, web server, SSH server etc.

- A HIDS operates at host-level by analyzing and monitoring all traffic activities on the system application files, system calls and operating system. These types of traffic activities are called typically called as audit trails.
- A host based intrusion detection system monitors the security event logs or checks the changes to the system, for example unauthorized login attempts and aberrant (departing from normal access) file accesses, on the actual target machine.

Network Based IDS

- A system that monitors network traffic and packets, and attempts to discover if a hacker/cracker is attempting to break into a system (or cause a denial of service attack).

Anomaly Detection

- Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly.
- This detection method uses machine learning to create a defined model of trustworthy activity, and then compare new behaviour against this trust model.

Signature Based IDS

- Signature-based IDS detects possible threats by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. - This terminology originates from antivirus software, which refers to these detected patterns as signatures.

- Although signature-based IDS can easily detect known attacks, it is impossible to detect new attacks, for which no pattern is available.

Most signature analysis systems are based on simple pattern matching algorithms.

- The question of what information is relevant to an IDS depends upon what it is trying to detect.
- In most cases, the IDS simply looks for a sub string within a stream of data carried by network packets.
  - When it finds this sub string (for example, the "phf" in "GET /cgi-bin/phf?"), it identifies those network packets as vehicles of an attack.

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have our position unassailable.

- The Art of War, Sun Tzu.

8

Network Security

8.1 Background

- *Information security* was provided, before digital age, in an organization by physical and administrative means e.g. Filing cabinet with locking system, personnel screening at the time of recruitment etc.
- With the introduction of computers, and development of shared systems, public telephone networks, data networks and the internet, the term *Computer securit*y was defined as "A collection of tools designed to protect data and to thwart hackers."
- Distributed systems and the use of network and communications facilities give rise to the need of security measures to protect data during their transmission, and hence the term *Network securit*y was introduced.
- Nowadays, most organizations interconnect their data processing equipment's with inter-connected networks (i.e. internet). So, the term *internet security* is used.

8.2 Security Violation

Scenario 1:
User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure. User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission

Scenario 2:
A network manager, D, transmits a message to a computer, E, under its management. The message instructs computer E to update an authorization file to include the identities of a number of new users who are to be given access to that computer. User F intercepts the message, alters its contents to add or delete entries, and then forwards the message to E, which accepts the message as coming from manager D and updates its authorization file accordingly.

Scenario 3:
Rather than intercept a message, user F constructs its own message with the desired entries and transmits that message to E as if it had come from manager D. Computer E accepts the message as coming from manager D and updates its authorization file accordingly.

Scenario 4:
An employee is fired without warning. The personnel manager sends a message to a server system to invalidate the employee's account. When the invalidation is accomplished, the server is to post a notice to the employee's file as confirmation of the action. The employee is able to intercept the message and delay it long enough to make a final access to the server to retrieve sensitive information. The message is then forwarded, the action taken, and the confirmation posted. The employee's action may go unnoticed for some considerable time.

Scenario 5:
A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.

8.3 Computer Security

- The NIST (National Institute of Standards and Technology) Computer Security Handbook[NIST95] defines the term computer security as:

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources includes hardware, software, firmware, information/data, and telecommunications).

- This definition includes three key objectives that are at the heart of computer security.

- Confidentiality
- Integrity
- Availability

- These three concepts form what is often referred to as ***CIA triad***.

8.3.1 The CIA Triad: Confidentiality

Confidentiality: This term covers two related concepts:
- *Data confidentiality*: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

- *Privacy*: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

8.3.2 The CIA Triad: Integrity

Integrity: This term covers two related concepts:
- *Data integrity*: Assures that information and programs are changed only in a specified and authorized manner.

- *System integrity*: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

8.3.3 The CIA Triad: Availability

- **Availability**: Assures that systems work promptly and service is not denied to authorized users. - Assures that systems work promptly and service is not denied to authorized users.

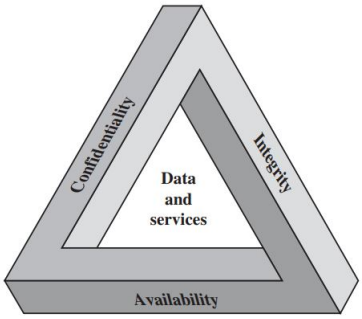


Figure 8.1: The CIA traid.

8.3.4 The CIA Triad: Security Characteristics

- FIPS 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Additional concepts for complete picture:
Authenticity
- The property of being genuine and being able to be verified and trusted.

Accountability
- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

8.4 The OSI Security Architecture

The ITU-T (International Telecommunication Union Telecommunication Standardization Sector) Recommendation X.800, Security Architecture for OSI, gives structured definition of security attacks, security mechanism and security services.

Security attack: Any action that compromises the security of information owned by an organization.

Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. Examples: encipherment, digital signature, access control etc.

Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. It includes authentication, access control, data confidentiality, data integrity and non-repudiation.

According to RFC 4949:

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack
An intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

8.5 Security Threat

- A *threat* is a potential violation of security which might or might not occur.
- The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for).
-Those actions are called *attacks*.
- Those who execute such actions, or cause them to be executed, are called *attackers*.

Class of Security Threat:
Security Threats divided into four broad classes:

- **Disclosure**, an unauthorized access to information.

- **Deception**, an acceptance of false data.
- **Disruption**, an interruption of prevention of correct information.
- **Usurpation**, an unauthorized control to some part of a system.

8.6 Security Attacks

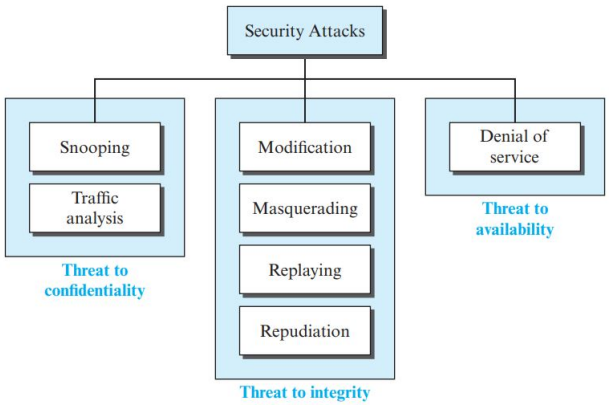


Figure 8.2: The CIA traid.

Security attacks are classified as:
1. Passive Attacks
2. Active Attacks

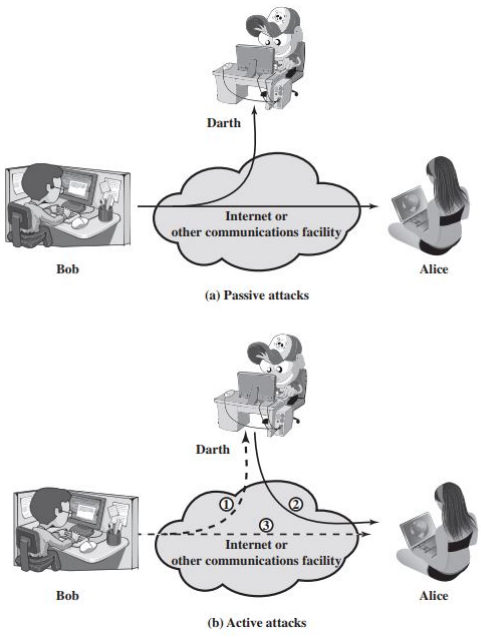


Figure 8.3: Security attacks.

8.6.1 Passive Attacks

- Passive attack attempts to learn or make use of information from the system but does not affect system resources.
- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
- Two types:

i. The release of message
ii. Traffic analysis

- Passive attacks are very difficult to detect, because they do not involve any alternation of the data.
- But it is feasible to prevent by means of encryption.

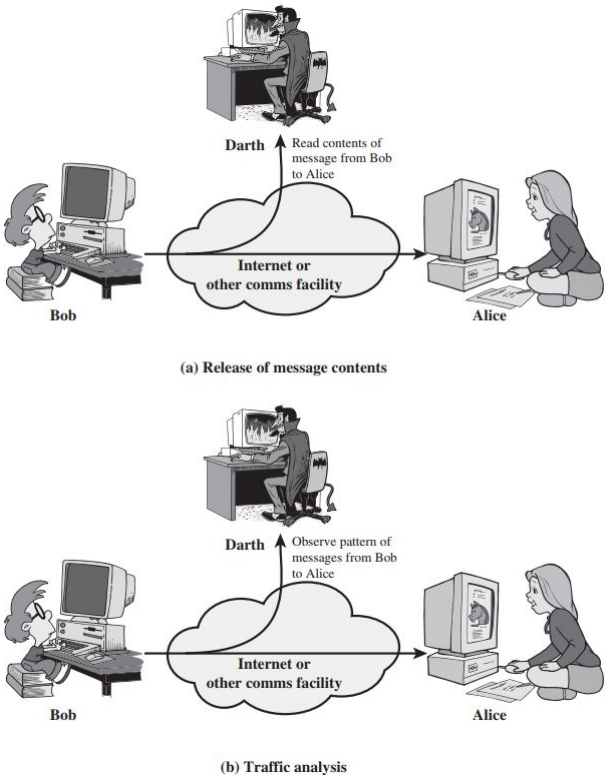


Figure 8.4: Passive network security attacks.

8.6.2 Active Attacks

- Active attacks attempt to alter system resources or affect their position.
- It involves some modification of the data stream or the creating of a false stream.
- Active attacks are quite difficult to be absolutely prevented because of the wide variety of potential physical, software, and network vulnerabilities.
- Examples of active attacks are:

  – Masquerade
  – Replay
  – Modification of messages,
  – Denial of service, etc.

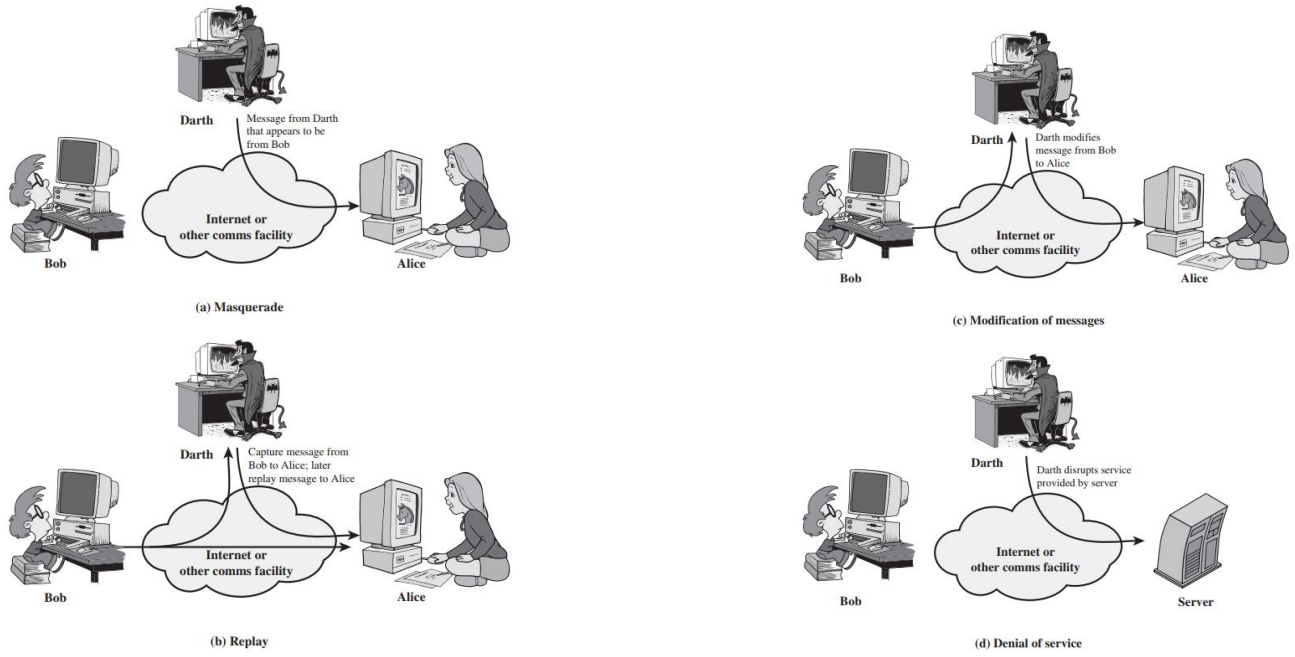


Figure 8.5: Active passives.

Snooping:
- Snooping refers to unauthorized access to or interception of data.
- For example, a file transferred through the Internet may contain confidential information. An unauthorized entity may intercept the transmission and use the contents for her own benefit.

Traffic Analysis:
- Unauthorized access to information by observing the monitoring online traffic.
- For example: observing and collecting the email address, nature of transactions etc.

Modification:
- Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
- For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."

Masquerade:
- Masquerade takes place when the attacker impersonate somebody else.
- If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.
- For example: gaining access to the account of a legitimate user either by stealing the victim's account ID and password.

Replay:
- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Repudiation:
- This type of attack is different from others because it is performed by one of the two parties in the communication: the sender or the receiver.
- The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

Denial of Service:
- The denial of service prevents or inhibits the normal use or management of communications facilities.
- This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service).
- Another form of service denial is the disruption of an entire network—either by disabling the network or by overloading it with messages so as to degrade performance.

8.7 Network Security Model

- A message is to be transferred from one party to another (called principals) across some sort of Internet service (through a logical information channel) by the cooperation of a communication protocol (e.g. TCP/IP).
- It is necessary to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity etc.

Techniques for providing security have two components:
1. A security-related transformation on the information to be sent e.g.
   - Include the encryption of a message so as to make in unreadable by the opponent,
   - Addition of code based on the contents to verify the identity of the sender.
2. Some secret information shared by two principals only. E.g.
   - an encryption key to scramble and unscramble the message.

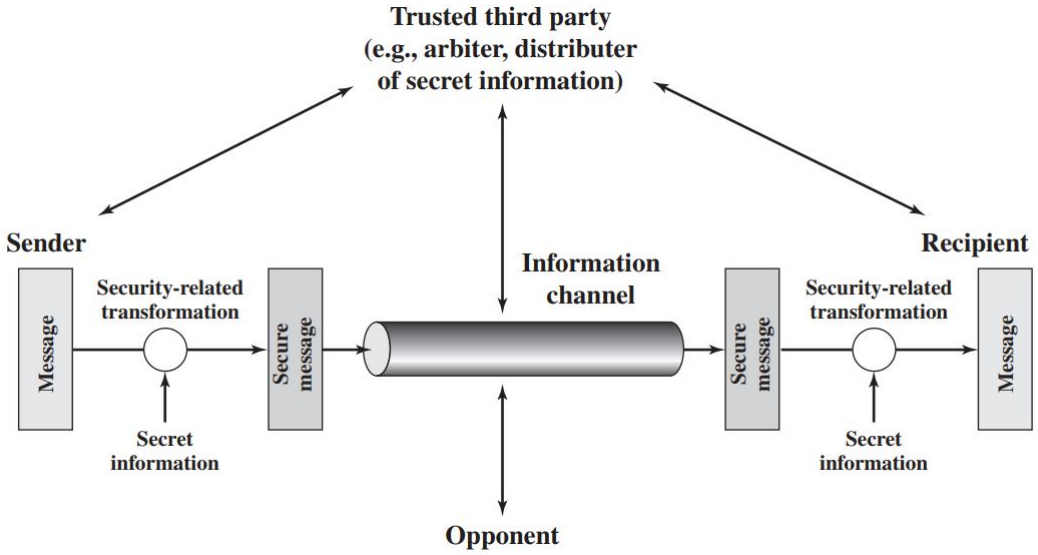


Figure 8.6: Network Security Model.

A trusted third party may be needed to achieve secure transmission. For example
- distributing the secret information to the two principals while keeping it away from its opponent.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm

Properties of Secure Communication:

- Confidentiality
- Authentication
- Message integrity
- Authorization
- Non-repudiation
- Availability

8.8 Cryptography

- *Cryptography*, a word with Greek origins, means “secret writing.” and is the art and science of concealing meaning.
- The Concise Oxford English Dictionary (9th ed.) defines cryptography as “the art of writing or solving codes." This is historically accurate, but does not capture the current breadth of the field or its modern scientific foundations. The definition focuses solely on the codes that have been used for centuries to enable secret communication.
- But cryptography nowadays encompasses much more than this: it deals with mechanisms for ensuring integrity, techniques for exchanging secret keys, protocols for authenticating users, electronic voting, cryptocurrency, and more.
- Modern cryptography involves the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks.
- It involves three distinct mechanisms: symmetric-key encipherment, asymmetric-key encipherment, and hashing.

- It is the techniques of converting ordinary plain text into unintelligible text and vice-versa.
- It is the practice and study of techniques for secure communication in the presence of third parties.
- Techniques used for deciphering message without any knowledge of the enciphering details fall into the area

of cryptanalysis. *Cryptanalysis* is what the layperson calls "breaking the code".
- The area of cryptography and cryptanalysis together are called *cryptology*.

- Before message is sent by the sender to the network , the message the user entered (plain-text) will be encrypted (converting plain-text to cipher-text) and after receiving the cipher-text will be decrypted (converting cipher-text to plain-text) and used by receiver.
- Encryption and decryption algorithms are referred as *ciphers*.

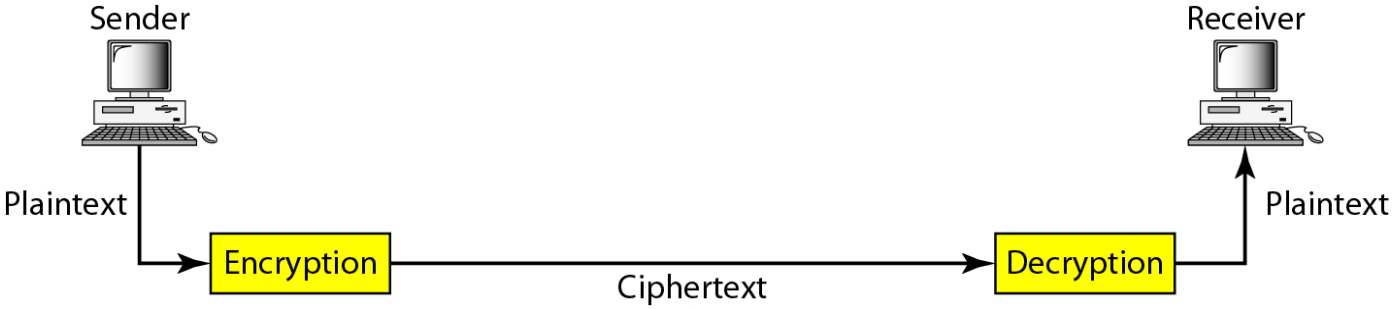


Figure 8.7: Encryption and decryption.

Cryptography Basic Terminology:

- **Plain text**: Original message fed to encryption algorithm; readable.
- **Encryption algorithm**: changes plain text to coded ciphertext by various substitution and transformation methods. The process of converting plaintext to ciphertext is called enciphering or encryption.
- **key**: input to the encryption algorithm. Known to sender and receiver only.
- **Ciphertext**: coded/scrambled output message by the algorithm. Different secret key applied on plain text produces different ciphertext.
- **Decryption Algorithm**: the encryption algorithm that run in reverse i.e. takes ciphertext and key to produce the original transmitted plain text. The process is known as deciphering or decryption

Encryption and Decryption:
Encryption
- Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized Cannot.
- Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor.

Decryption
- Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand (original form).
- It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

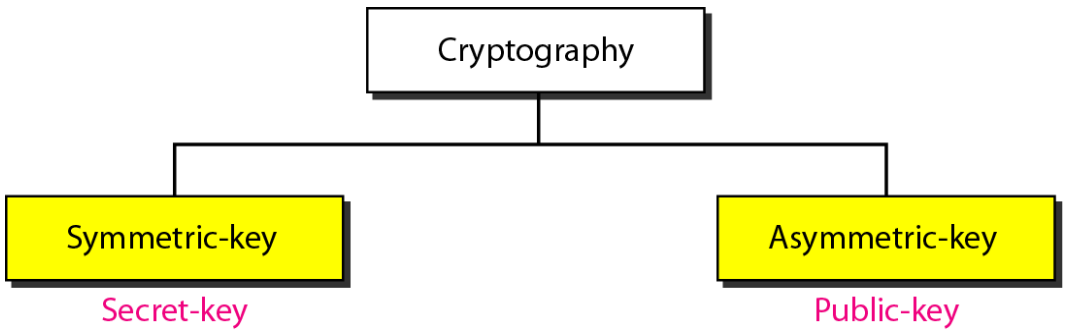


Figure 8.8: Types of cryptography.

8.9 Symmetric Key Cryptography

- Symmetric encryption (also called *classical cryptosystems*), also referred to as *conventional encryption*, *secret-key*, or *single-key encryption*, was the only type of encryption in use prior to the development of public-key

encryption in the late 1970s.
- Same key is shared by sender (for encryption) and receiver (for decryption). - Ciphertext is generated either by substitution or transformation method by encryption algorithm.
- A symmetric encryption has five ingredients:

- Plaintext
- Encryption algorithm
- Secret key
- Ciphertext
- Decryption algorithm

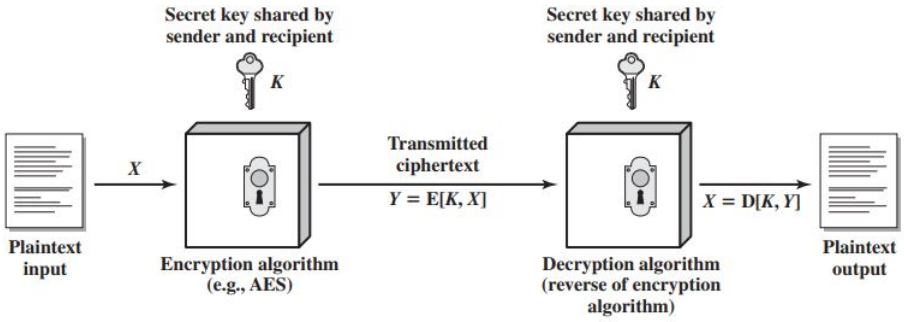


Figure 8.9: Simplified Model of Symmetric Encryption.

There are two requirements for secure use of symmetric encryption:

1. We need a strong algorithm.
   - At minimum, an operator who knows the algorithm and has access to one or more ciphertext would be unable to decipher the ciphertext.
2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

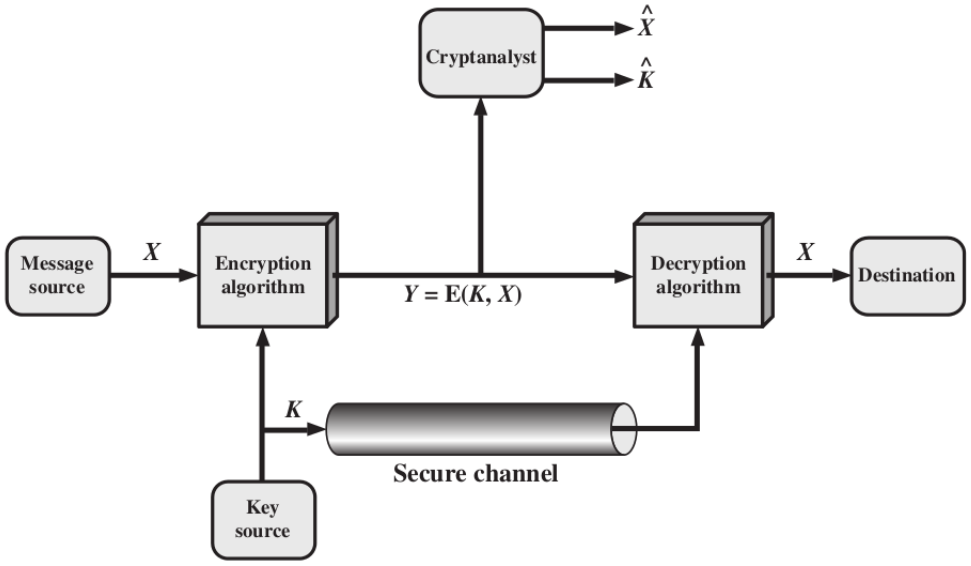


Figure 8.10: Model of symmetric key cryptography.

There are two basic types of classical ciphers:
i. Transposition ciphers, and
ii. Substitution ciphers

8.9.1 Transposition Ciphers

- A transposition cipher does not substitute one symbol for another; instead it changes the location of the symbols.
- A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext.
- A symbol in the eighth position in the plaintext may appear in the first position of the ciphertext.

- In other words, a transposition cipher reorders (transposes) the symbols.

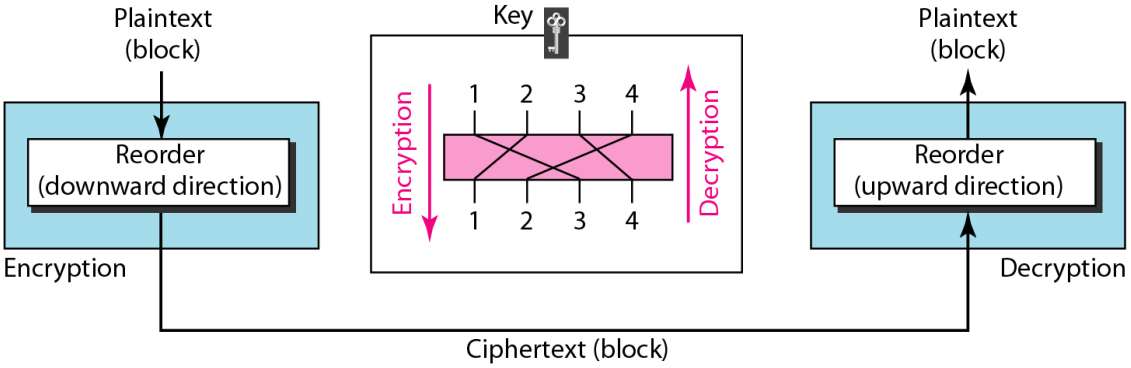


Figure 8.11: Transposition cipher.

For example:
Suppose Alice wants to secretly send the message "Enemy attacks tonight" to Bob. The encryption and decryption is shown in Figure. Note that we added an extra character (z) to the end of the message to make the number of characters a multiple of 5.

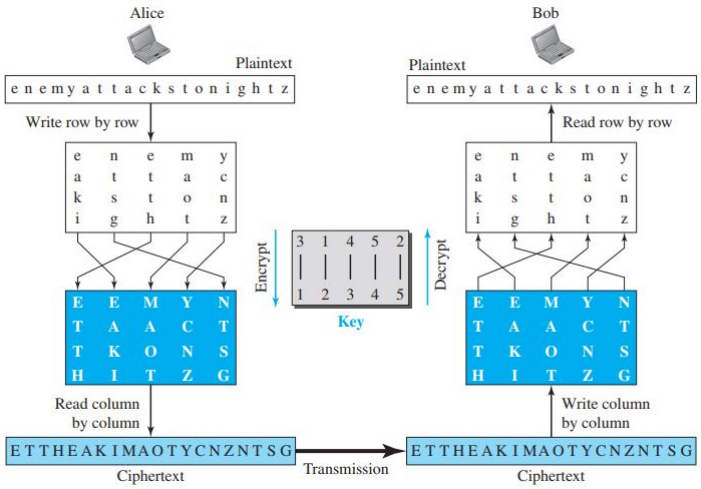


Figure 8.12: An example of substitution cipher.

8.9.2 Subsitution Cipher

- A substitution cipher changes characters in the plaintext to produce the ciphertext.
- For example: Caesar cipher, Vigenere Cipher, One-time pad are example of substitution cipher.

Caesar Cipher

- Substitution cipher
- Shift cipher
- Earliest known and simplest substitution scheme developed by Julis Ceasar.
- Replaces each letter of the alphabet with the letter standing three places further down the alphabet.
  plain: meet me after the toga party
  cipher: PHHW PH DIWHU WKH WRJD SDUWB
- A Caesar cipher is susceptible to a statistical ciphertext-only attack.

8.10 Data Encryption Standard (DES)

- The Data Encryption Standard (DES) works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key.
- It is a symmetric key cryptography.
- Symmetric key algorithm in which data are encrypted in 64-bit blocks using a 56-bit key.

- Originally designed by researchers at IBM in the early 1970s, DES was adopted by the U.S. government as an official Federal Information Processing Standard (FIPS) in 1977 for the encryption of commercial and sensitive yet unclassified government computer data.
- It was the first encryption algorithm approved by the U.S. government for public disclosure.

- The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time.
- To encrypt a plaintext message, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit ciphertext by means transposition and substitution.

DES Encrpytion:

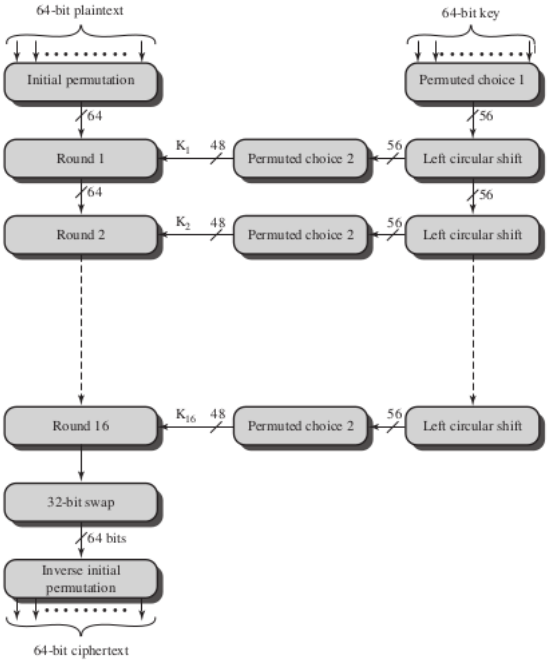


Figure 8.13: General Depiction of DES Encryption Algorithm.

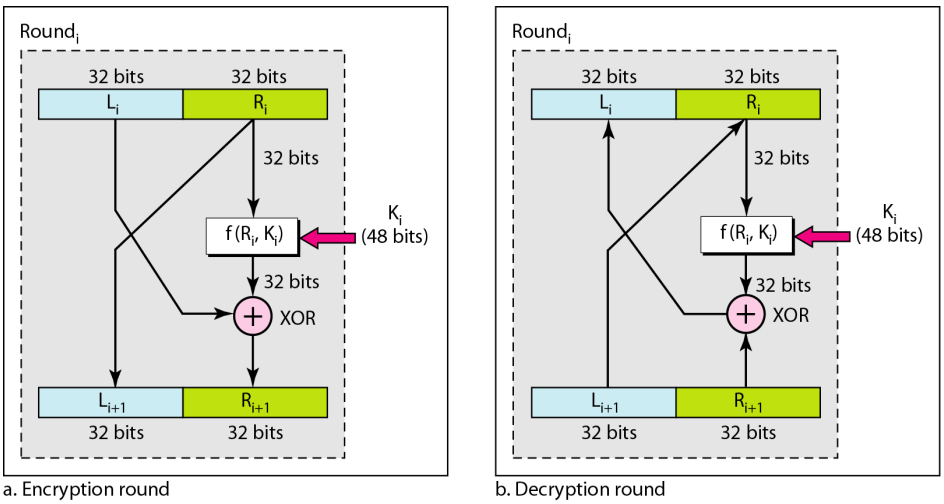


Figure 8.14: One round in DES.

- The process involves 16 rounds and encrypting blocks individually or making each cipher block is dependent on all the previous blocks.
- DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).
- The check bits or parity bits are used to check if the key was indeed correctly retrieved.

- The rounds are executed sequentially, the input of one round being the output of the previous round.

- The right half of the input, and the round key, are run through a function f that produces 32 bits of output; that output is then XOR'ed into the left half, and the resulting left and right halves are swapped.

- The keys for each round is separate which is just the result of left circular shift operation of the original key.
- The round key generator is the component which is responsible to generate 16 sub keys for 16 rounds.
- The round operation is nothing but the XOR operation between the plain text and the key. The final key to the cipher text is the resulting key at the end of 16 rounds.

- Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied.
- It would take maximum of 2^{56} or 72,057,594,037,927,936 attempts to find the correct key.
- For any cipher, the most basic method of attack is brute force, which involves trying each key until you find the right one.

- Even though few messages encrypted using DES encryption are likely to be subjected to this kind of code-breaking effort, many security experts felt the 56-bit key length was inadequate even before DES was adopted as a standard.
- Thus, DES is upgraded to more secure Advanced Encryption Standard (AES).

8.11 Public Key Cryptography

- Also known as Public Key Cryptography.
- Used two keys: *public-key* and *private key*.

Public key:
- Shared with the public who wants to communicate with the receiver.
- Used for enciphering the sender's plaintext into cipher text.

Private key
- Is kept secret by the receiver.
- Used to deciphering ciphertext into plaintext by the receiver.
- Proposed by Diffie and Hellman in 1976
- RSA uses public-key cryptosyst

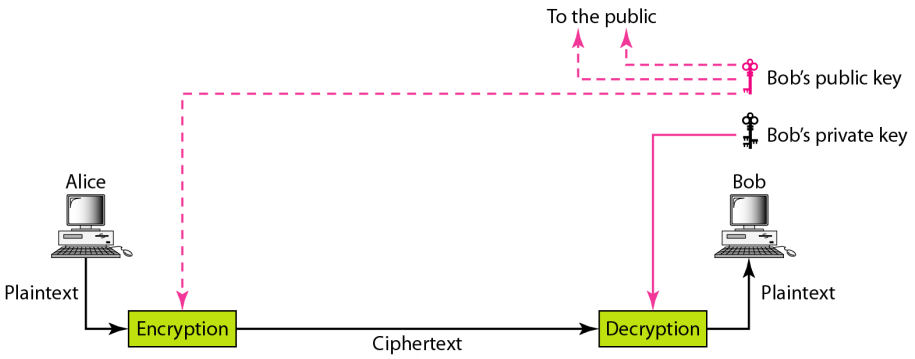


Figure 8.15: Asymmetric key cryptography.

The essential steps:

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register or other accessible file.
3. This is the public key. The companion key is kept private. As Figure suggests, each user maintains a collection of public keys obtained from others.
4. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
5. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

Because one key is public, and its complementary key must remain secret, a public key cryptosystem must meet the following three conditions:

1. It must be computationally easy to encipher and decipher a message given the appropriate key.
2. It must be computationally infeasible to derive the private key from the public key.
3. It must be computationally infeasible the private key from a chosen plaintext attack.

8.12 RSA Algorithm

- Developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978.
- Most widely used asymmetric key encryption.
- Used in security protocol such as IPSEC, SSH, TLS etc.
- The RSA scheme is a cipher in which the plaintext and ciphertext are integers between 0 and $n-1$ for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 2^{1024} .

- RSA uses two exponents, e and d, where e is public and d is private. Suppose P is the plaintext and C is the ciphertext. Alice uses $C = P^e \bmod n$ to create ciphertext C from plaintext P; Bob uses $P = C^d \bmod n$ to retrieve the plaintext sent by Alice. The modulus n, a very large number, is created during the key generation process.

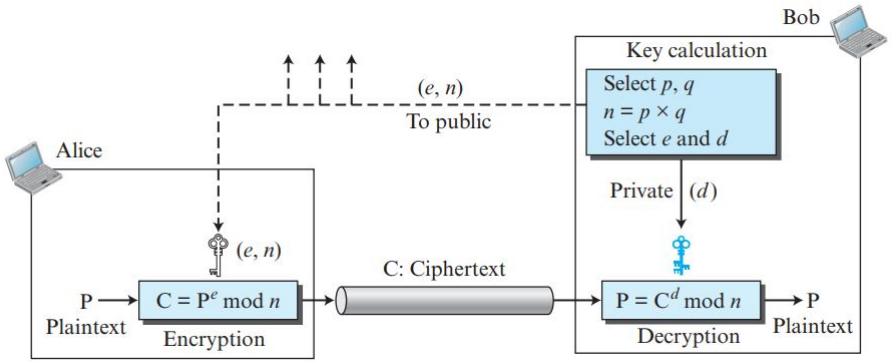


Figure 8.16: Encryption, decryption and key generation used in RSA.

- A user of RSA creates and then published a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret.
The RSA algorithm involves four steps:

- Key generation
- Key distribution
- Encryption
- Decryption

RSA: Key Generation
The keys for RSA algorithm are generated in the following way:

1. Generate two large random prime numbers, p and q. (p and $q \geq 2^{512}$).
2. Compute $n = p \times q$, n is called modulus.
3. Compute the totient $\phi(n) = (p-1)(q-1)$.
4. Choose e such that $1 < e < \phi(n)$, where e and $\phi(n)$ do share factors other than one i.e. $gcd(e, \phi(n)) = 1$).
5. Computer d such that $d \times e = 1 \bmod \phi(n)$ (i.e.$de\{mod\phi(n)\} = 1$
6. Publish e and n as the public key (Sender's public key) for encryption.
7. Keep d and n as private key (Receiver's private key) for decryption.

RSA:Key Generation
- The totient $\phi(n)$ of positive integer n is the numbers less than n with no factors in common with n (i.e. they share no factors except 1).
- *For example*:
Let n = 10. The numbers that are less than 10 and are relatively prime to (have no factors in common with) n are 1,3,7, and 9. Hence,$\phi(n)$ = 4. Similarly, if n =21, the numbers that are relatively prime to n are 1,2,4,5,8,10, 11, 12, 13,16,19, and 20. So $\phi(n)$=12.

RSA: Key Distribution

- Suppose that Bob wants to send information to Alice. IF they decide to use RSA, Bob must know Alice's public key to encrypt the message and Alice must use her private key to decrypt the message.
- To enable Bob to send his encrypted messages, Alice transmit her public key (e ,n) to Bob via a reliable,but not necessarily secret, route. Alice' private key (d, n) is never distributed.

RSA : encryption and decryption

Given public key (e ,n) and private key (d, n) are computed

- To encrypt bit pattern, P, compute cipher text C as:
  $C = P^e \bmod n$

- To decrypt bit pattern, C, compute
  $P = C^d \bmod n$

RSA Example:

Pick two prime numbers: p=3, q = 5.
$n = p \times q = 3 \times 5 = 15$
$\phi(n) = (p-1)(q-1) = (3-1)(5-1) = 2 \times 4 = 8.$
Choose e satisfying $1 < e < \phi(n)$.
Let us choose e=3,which do not share any common factors with 8 rather than 1.
Compute d satisfying de mod $\phi(n)$=1
So $d \times 3$ mod 8 = 1
Let us choose d =11 which satisfy the relation.

- So public key (e,n) is (3,15) which is released publicly and the persons that want to send the message use this key to encrypt the message and send it to the receiver.
- Private key(d,n) is (11,15) which is kept secret by the receiver.

Let us consider the message be 2.
So, at encryption process, the sender uses the public key to encrypt the message. Resulting cipher text will be:
  $C = m^e$ (mod n) = 2^3 (mod 15) = 8.
At decryption process, the private key is used to decrypt the cipher text. Plain text is obtained as:
  $P = c^d$ (mod n) = 8^{11} (mod 15) = 2.
Hence the original message 2 is obtained at receiver end after decryption.

8.13 Digital Signature

- Digital signature is the most important work on public-key cryptography.
- Digital signature is an electronic analogue of a written signature.
- It can be used to provide assurance that the claimed signatory signed the information.
- It may be used to detect whether or not the information was modified after it was signed.

- For a given message, **M**, a digital signature, **S**, is appended to the message.
- The signature is realized as a function with the message M and the private key as input.
- The public key and the message M are the inputs to the verification function.

- The digital signature must have the following properties:

  i. It must verify the author and the date and time of the signature.
  ii. It must authenticate the contents at the time of the signature.
  iii. It must be verifiable by third parties, to resolve disputes.

- Thus, the digital signatures function includes the authentication function.

- To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed.
- The private key is then used to encrypt the hash. The encrypted hash is the digital signature.
- The reason for encrypting the hash instead of the entire message or document is that a hash function can convert

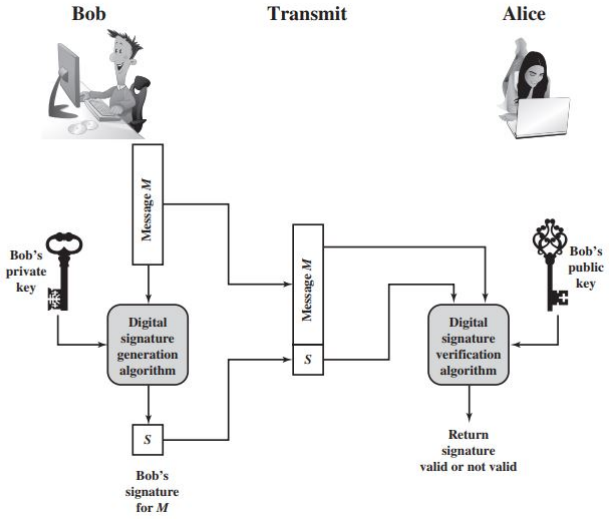


Figure 8.17: Generic model of digital signature.

an arbitrary input into a fixed length value, which is usually much shorter.
- This saves time since hashing is much faster.

- The value of the hash is unique to the hashed data.
- Any change in the data, even changing or deleting a single character, results in a different value.
- This attributes enables others to validate the integrity of the data by using the signer's public key to decrypt the hash.
- If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed.
- Of the two hashes don't match, the data has either been tempered with in some way (integrity) or the signature was created with a private key that doesn't correspond to the public key presented by the signer (authentication).

Types:
i. Direct Digital Signature
ii. Arbitrated Digital Signature

8.14 PGP: Pretty Good Privacy

- PGP is an open-source, freely available software package for e-mail security. It provides authentication through the use of digital signature, confidentiality through the use of symmetric block encryption, compression using the ZIP algorithm, and e-mail compatibility using the radix-64 encoding scheme.
- PGP incorporates tools for developing a public-key trust model and public-key certificate management. - PGP has grown explosively and is now widely used. A number of reasons can be cited for this growth.

- Independent of operating system; can run of different platforms such as unix, windows, mac etc.
- Use widely used cryptographic algorithms; includes RSA, DSS, and Diffie-Hellman for public-key encryption; CAST-128, IDEA, and 3DES for symmetric encryption; and SHA-1 for hash coding.
- Open source: documentation, source code and packages freely available
- Used in wide range of applications.
- PGP is now on an Internet standards track (RFC: 3156)

8.14.1 PGP Services

- The PGP operation provides four services: authentication, confidentiality, compression, and e-mail compatibility.

Notation Uses:
K_s = session key used in symmetric encrpytion scheme.
PR_a = private key of user A, used in public-key encryption scheme.
PU_a = public key of user A, used in public-key encryption scheme.

Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed for storage or transmission using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

Figure 8.18: PGP services.

EP = public-key encrpytion.
DP = public-key decrpytion.
EC = symmetric encryption.
DC = symmetric decryption.
H = hash function.
|| = concatenation.

8.14.1.1 PGP Operation: Authentication

1. The sender creates a message.
2. SHA-1 is used to generate a 160-bit hash code of the message.
3. The hash code is encrypted with RSA using the sender's private key, and the result is prepended to the message.
4. The receiver uses RSA with the sender's public key to decrypt and recover the hash code.
5. The receiver generates a new hash code for the message and compares it with the received hash. If they both matched, the message is accepted otherwise rejected.

8.14.1.2 PGP Operation: Confidentiality

1. The sender generates a message and a random 128-bit number to be used as a session key for this message only.
2. The message is encrypted using CAST-128 (or IDEA or 3DES) with the session key.
3. The session key is encrypted with RSA using the recipient's public key and is prepended to the message.
4. The receiver uses RSA with its private key to decrypt and recover the session key.

8.14.1.3 PGP Operation: Confidentiality and Authetication

1. Can use both services on the same message
    - Create signature and attach to the message.
    - Encrypt both message and signature using CAST-128 (or IDEA or 3DES)
    - Attach RSA/EIGamal

8.14.1.4 PGP Operation: Compression

- By default PGP compress message after signing but before encryption, so can store uncompressed message and signature for later verification.
- Uses ZIP compression algorithm

8.15 Transport Layer Security: SSL

- SSL stands for *Secure Socket Layer*.
- SSL originally developed by NetScape in 1994.
- SSL v3, designed with public input, became Internet standard known as **Transport Layer Security (TLS)**.
- SSL is a general purpose service implemented as a set of protocols that rely on TCP. - It provide security at transport layer.

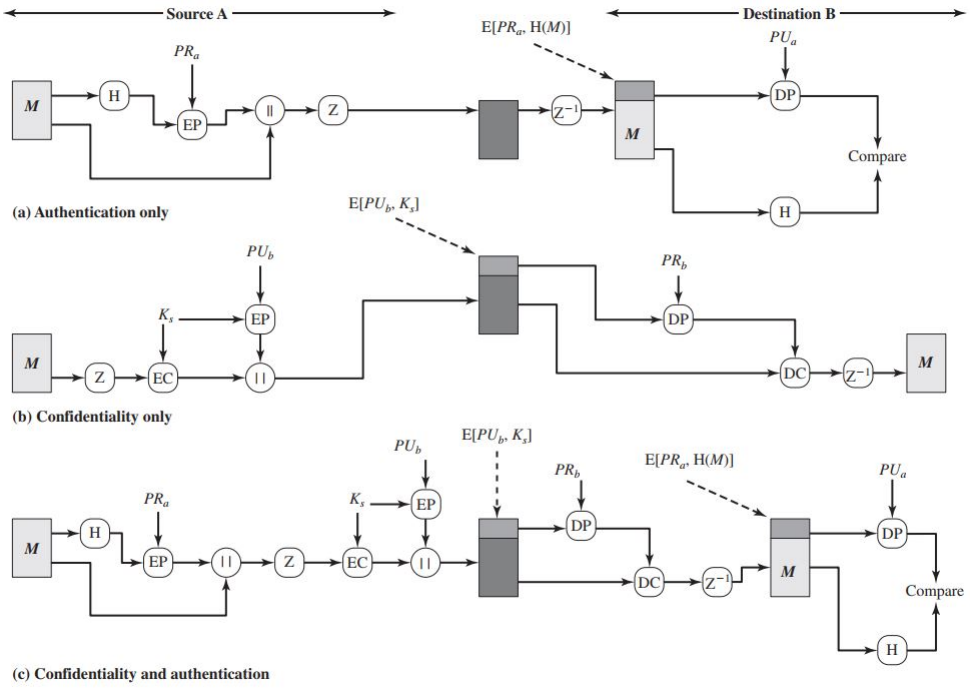


Figure 8.19: PGP cryptographic functions.

- SSL/TSL provides confidentiality using symmetric encryption, data integrity and message authentication between server and client.

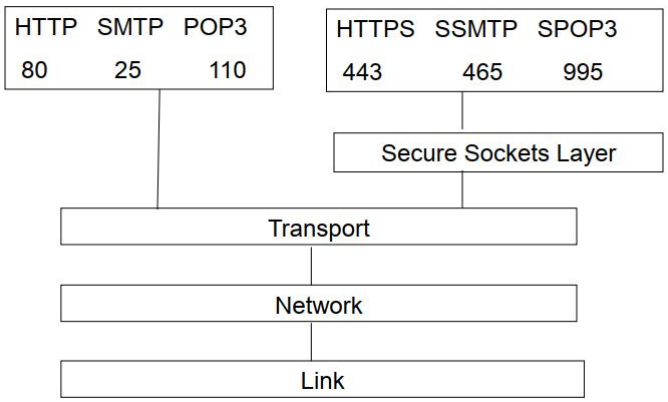


Figure 8.20: SSL uses.

8.15.1 SSL Architecture

- SSL has two layer of protocols which are implemented above the TCP layer.
- The SSL Record Protocol provides basic security services to various higher layer protocols e.g. HTTP.
- Three higher-layer protocols are defined as part of SSL:
i. Handshake protocol
ii. Change cipher Spec Protocol
iii. Alert Protocol

Two important concepts of SSL:
i. **SSL connection**:
- A transient peer-to-peer communication link that provides a suitable type of service. - Every connection is associated with one session.

ii. **SSL session**:
- An SSL session is an association between a client and a server.
- Created by handshake protocol.

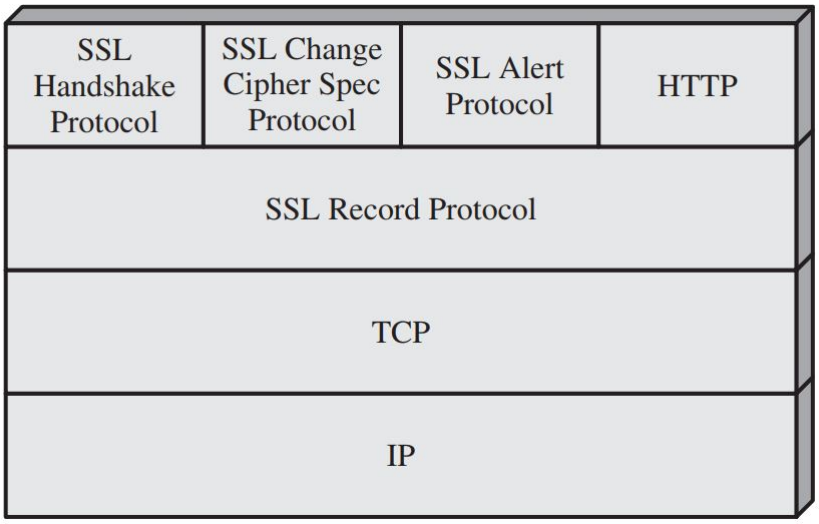


Figure 8.21: SSL protocol stack.

SSL Record Protocol

- 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)

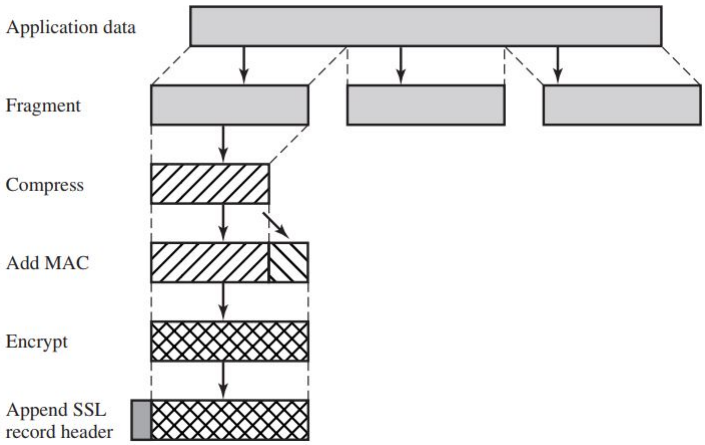


Figure 8.22: SSL protocol operation.

SSH Handshake Protocol:

- Allows server and client to:
  - Authenticate each other
  - To negotiate encryption and MAC (Message Authentication Code) algorithms
  - To negotiate cryptographic keys to be used

Comprises a series of messages exchanged in phases

- Establish security capabilities
- Server authentication and key exchange
- Client authentication and key exchange
- finish

SSL Change Cipher Spec Protocol:

- One of 3 SSL specific protocols which use the SSL Record protocol.
- A single message with the value of 1.
- Causes pending state to become current, hence updating the cipher suit in use.

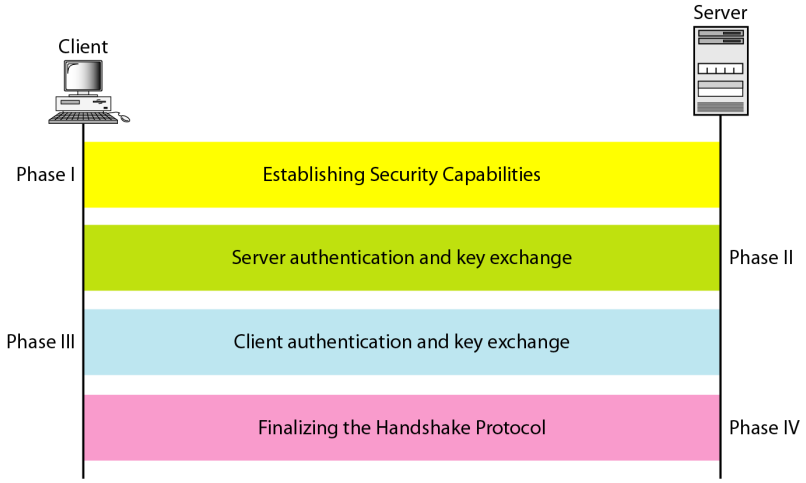


Figure 8.23: SSL handshake protocol.

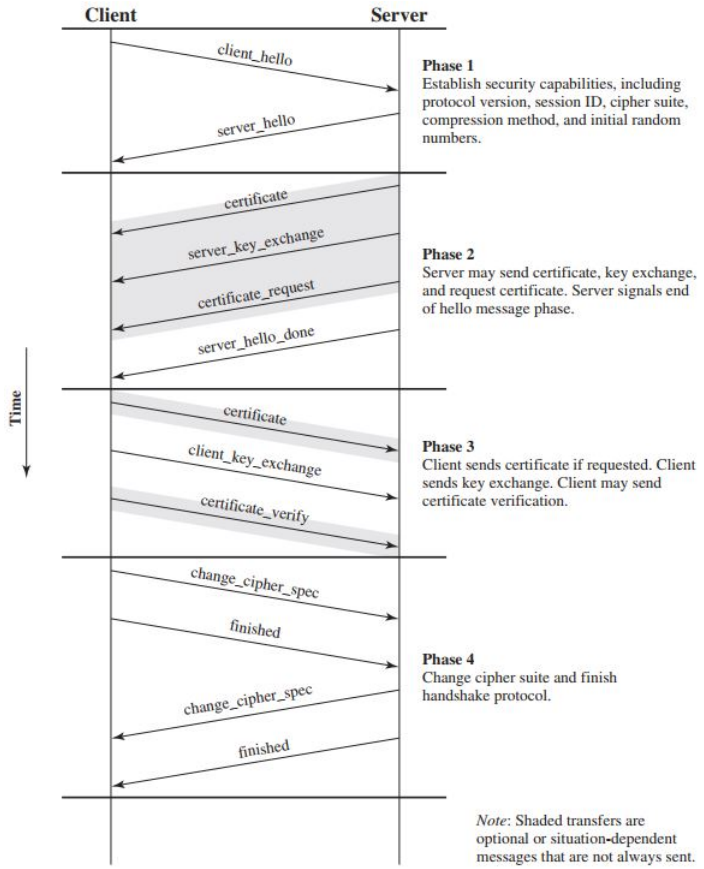


Figure 8.24: SSL handshake protocol action.

SSL Alert Protocol:
- Used to convey SSL-related alerts to the peer entity.
- SSL alerts are compressed and encrypted like all SSL data.
- Each message in this protocol consists of two bytes. The first byte takes the value warning (1) and fatal (2) to convey the severity of the message. If the level is fatal, SSL immediately terminates the connection.
- Specific alert: Unexpected message, decompression failure, handshake failure, illegal parameters.

8.16 Network Layer Security: IPSec and VPN

8.16.1 IPSec

- IPSec stands for Internet Protocol Security.
- It is a collection of protocols to provide security for a packet at the network layer.
- IPSec is a standard framework for ensuring private communication over public network.

- It has become the most common network layer security control, typically used to create a VPN.
- A VPN is a virtual network built on top of existing physical networks that can provide a secure communication for data transfer.
- VPNs are used most often to protect communication carried over public networks such as the Internet.
- A VPN can provide several types of data protection:
  - Confidentiality
  - Integrity
  - Data origin authentication

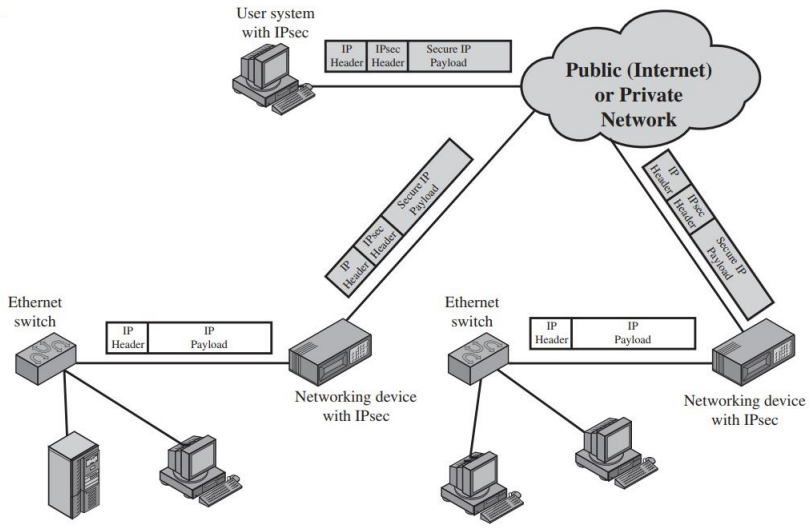


Figure 8.25: An IPSec scenario.

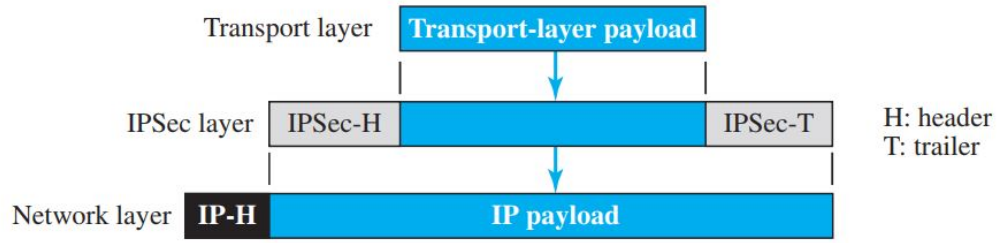
8.16.1.1 Modes of IPSec

IPSec operates in one of two different mode: *transport mode* and t*unnel mode*. **Transport Mode**
- Transport mode protects the payload to be encapsulated in the network layer i.e. it protects what is delivered from the transport layer to the network layer.
- It does not protect the whole IP header or in other words, it does not protect the whole IP packet.

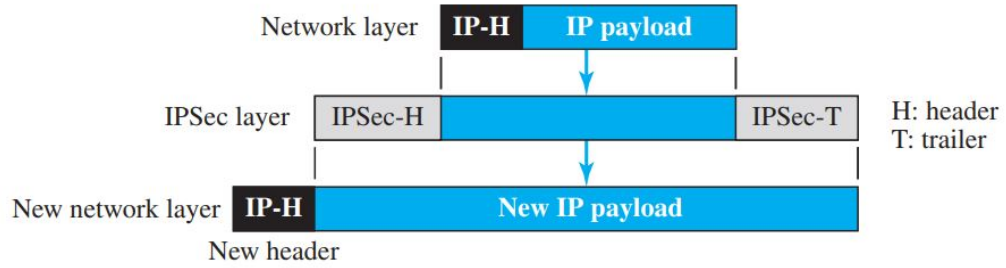
Tunnel Model
- In tunnel mode, IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header

8.16.1.2 IPSec Components

- Two security protocols :
  - **Authentication Header (AH)**: AH is an extension header to provide message authentication. Because message authentication is provided by ESP, the use of AH is deprecated.
  - **Encapsulating Security Payload (ESP)**: ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication and integrity protection
- Internet Key Exchange (IKE) protocol
  - IPSec uses IKE to negotiate IPSec connection settings.
  - Authenticate endpoints to each other.
  - Define the security parameters of IPSec-protected connections
  - Negotiate secret keys and
  - Manage, update, and delect IPSec-protected communication channels.
- **IP Payload Compression Protocol (IPComp)**
  - Optionally, Ipsec can use Ipcomp to compress packet payloads before encrypting them.



(a) An IPSec in transport mode.



(b) Am IPSec in tunnel model.

Figure 8.26: An IPSec model

8.16.1.3 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. Traffic within a company or workgroup does not incur the overhead of security-related processing.
- 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

8.16.1.4 IPSec Applications

- Secure branch office connectivity over the Internet.
- Secure remote access over the internet.
- Establishing extranet and intranet connectivity with partners.

8.16.2 VPN: Vitual Private Network

- One of the applications of IPSec is in virtual private networks.
- VPN creates a network that is private but virtual. It is private because it guarantees privacy inside the organization. It is virtual because it does not use real private WANs; the network is physically public but virtually private.
- It is build on top of existing physical networks and provides a secure communications mechanisms for data and IP information transmitted between networks.
- VPN technology uses the ESP protocol of IPSec in the tunnel mode. Moreover, firewalls, - - VPNs, and IPsec with ESP in tunnel mode are a natural combination and widely used in practice .
- VPSs can use both symmetric and asymmetric forms of cryptography.

Three primary models for VPN architecture:

1. **Gateway-to-Gateway**

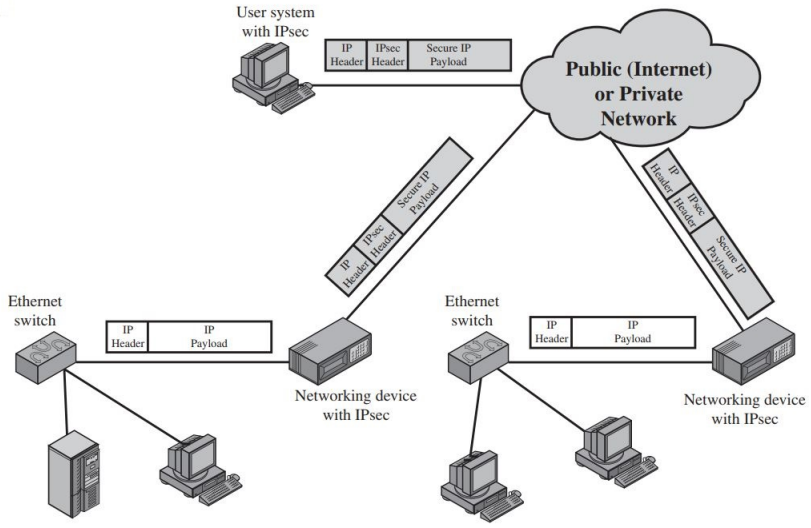


Figure 8.27: An IPSec scenario.

- Protects communications between two specific networks.
- Eg. An organization's main office network and a branch office network, or two business partners networks.

2. **Host-to-gateway**
   - Protects communications between one or more individual hosts and a specific network belonging to an organization.
   - Eg. Tranveling employees to gain access to internal organizational services, such as the organization's e-mail and Web servers.
3. **Host-to-Host**
   - Protects communcations between two specific computers.
   - Eg. Small number of users need to use or administer a remote system.

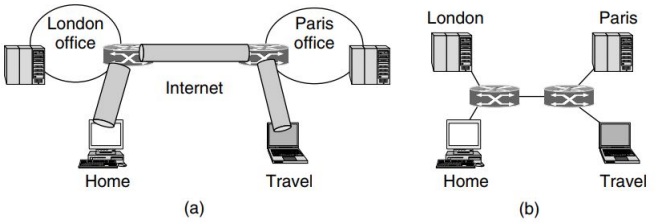


Figure 8.28: a) A VPN b) Topology as seen from the inside.

8.17 Securint Wireless LANs

- IEEE 802.11 is a standard for wireless LAN. (Wi-fi).
- IEEE 802.11i specifies security standard for IEEE 802.11 LANs.

- Wireless networks more vulnerable • No inherent physical protection: sending/receiving message do not need physical access to network infrastructure.

- As a consequence
  - •Eavesdropping is easy.
  - •Injecting bogus message is easy.
  - •Replaying previously recorded message is easy.
  - •Illegitimate access to network and services is easy.
  - • of service is easy (jamming).

8.18 WEP: Wireless Equivalent Privacy

- It is the original (first generation) wireless security protocol for the 802.11 standard.
- The stated goal of WEP is to make wireless LAN as secure as a wired LAN.
  - ◇Protocol goals:
    - •Confidentiality: prevent eavesdropping
    - •Access control: prevent unauthorized access
    - •Data integrity: prevent tampering of messages
  - ◇ Failure: none of the security goal is attained.
- It uses RC4 stream cipher, using 64-bit key.

8.18.1 WEP Encryption

Weak Security

- Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5,000 packets.

- Software to crack WEP passwords within a minute is now freely available and the use of WEP is very strongly discouraged.

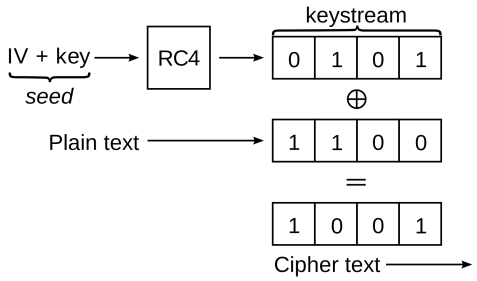


Figure 8.29: XORing operation.

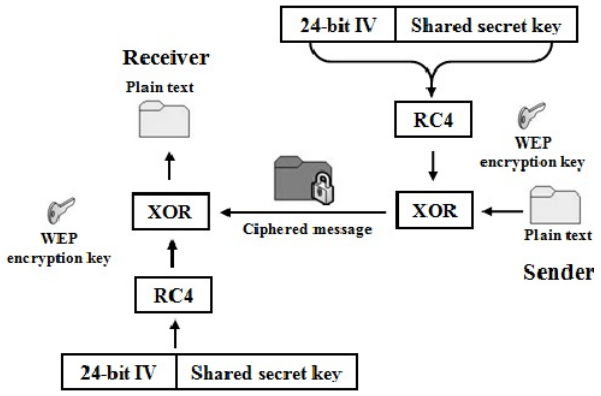


Figure 8.30: Wep encryption.

8.19 WPA: Wifi-Protected Access

- WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard.
- IEEE 802.11i addresses three main security areas: authentication, key management, and data transfer privacy.
- Use Authentication server (AS) for authentication process as well as for key distribution to AP, which in turn manages and distributes keys to stations. Extensible Authentication Protocol (EAU) and Remote Authentication Dial-In User Service (RADIUS) are popular authentication protocol.

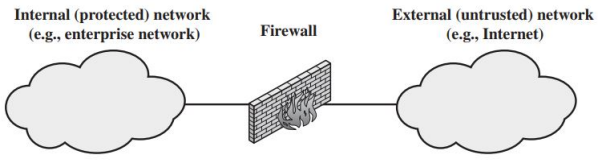


Figure 8.31: A general model of firewall.

8.20 Firewall

- Firewall is a device (usually a router or computers) installed between the internal network of an organization and the rest of the Internet.
- A firewall is a network security system designed to prevent unauthorized access to or from a private network. A firewall security policy dictates which traffic is authorized to pass in each direction.
- A firewall may be designed to operate as a filter at the level of IP packets, or may operate at a higher protocol layer.
- A firewall provides a location for monitoring security-related events as a single-choke point.
- Auditing and controlling access can implement alarms for abnormal behavior.

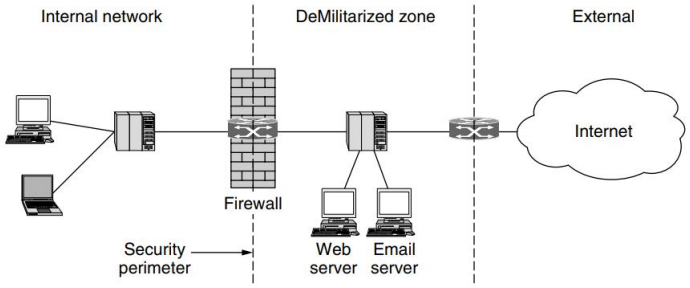


Figure 8.32: A firewall protecting an internal network.

8.20.1 Firewall Design Goals

i. All traffic from inside to outside, and vice-versa, must pass through the firewall. This is achieved by physical blocking all access to the local network except via the firewall.
ii. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.
iii. The firewall itself is immune to penetration; trusted system with a secured OS used to host a firewall.

8.20.2 Firewall Contral Access Methods

Service Control

- Filter traffic on the basis of IP address, protocol or TCP port address.
- Example: block port 80, allow port 23.

Directional Control

- Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

User control

- Controls access to a service according to which user is attempting to access it.
- This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users.

Behaviour control

- Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only.

8.20.3 Scope of Firewall

- The following capabilities are within the scope of a firewall:

i. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.
ii. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
iii. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.
iv. A firewall can serve as the platform for IPsec. Using the tunnel mode capability the firewall can be used to implement virtual private.

8.20.4 Types of Firewalls

- Packet-Filter Firewall
- Proxy Firewall

8.20.4.1 Packet Filter Firewall

- Packet-Filter Firewall applies a set of rules to each incoming and outgoing IP packet and then forwards of discard the packet.
- Packet filter is based on

- source IP address,
- destination IP address,
- source port address,
- destination port address,
- IP protocol,
- Interface

- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP.

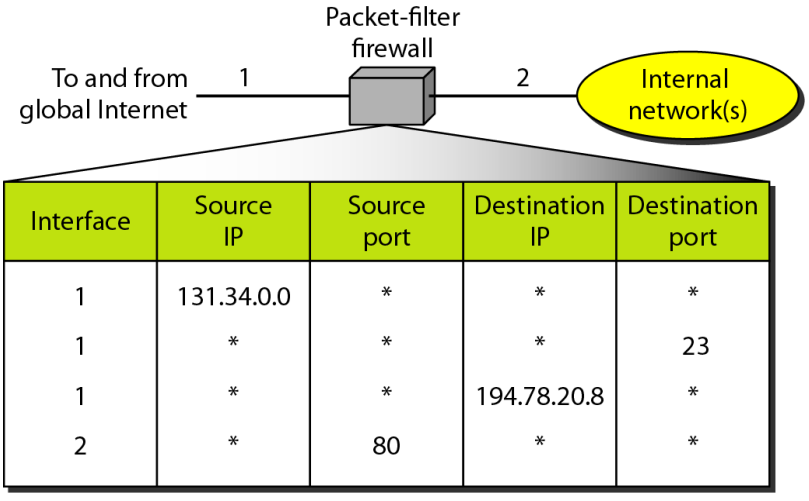


Figure 8.33: An example of packet filter firewall.

According to the figure 8.33, the following packets are filtered:

i. Incoming packets from network 131.34.0.0 are blocked (security precaution). Note that the $*$ (asterisk) means "any."
ii. Incoming packets destined for any internal TELNET server (port 23) are blocked.
iii. Incoming packets destined for internal host 194.78.20.8 are blocked. The organization wants this host for internal use only.

iv. Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browse the Internet.

8.20.4.2 Application Gateway Firewall

- Also called application proxy firewall or simply proxy firewall.
- Acts as a relay of application-level traffic.
- It inspect the message of application.

Example:

-As an example, assume that an organization wants to implement the following policies regarding its web pages: only those Internet users who have previously established business relations with the company can have access; access to other users must be blocked. In this case, a packet-filter firewall is not feasible because it cannot distinguish between different packets arriving at TCP port 80 (HTTP). Testing must be done at the application level (using URLs).

• The user contacts the gateway using a TCP/IP application, such as HTTP or FTP, and the gateway asks the user for the name of the remote host to be accessed.

• When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints

8.20.5 Limitation of Firewalls

- IP Snooging:
  • routers can't know if data '"really" comes from claimed source.
  • an intruder can transmit packets from the outside with source IP address field containing an address of an internal host.
- The firewall does not protect against internal threats,
  • Such as a dishonest employee
  • or an employee who unwittingly cooperates with an external attacker.
- The firewall cannot protect against the transfer of virus-infected programs or files.

8.21 Intrusion Detection System

Background

- A significant security problem for networked systems is hostile, or at least unwanted, trespass by users or software.
- User trespass can take the form of unauthorized logon to a machine or, in the case of an authorized user, acquisition of privileges or performance of actions beyond those that have been authorized.
- Software trespass can take the form of a virus, worm, or Trojan horse.

Intrusion:

- One of the key threats to security is the use of some form of hacking by an *intruder*, often referred to as a *hacker* or *cracker*, or *interceptor*.
- *Intrusion* is a phenomenon that performs an activity that compromises a computer system by breaking the security or causing it to enter into an insecure state by an intruder.
- A set of attempts to compromise a computer or a computer network resource security is regarded as an intrusion.

8.21.1 Types of Intruders

Anderson identified three classes of intruders:

- **Masquerader**: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account. The masquerader is likely to be an outsider.
- **Misfeasor**: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges . The misfeasor generally is an insider.
- **Clandestine user**: An individual who seizes supervisory control of the system and uses this control to

evade auditing and access controls or to suppress audit collection. The clandestine user can be either an outsider or an insider.

8.21.2 Intruder Attacks/Examples of intrusion

Intruder attacks range from the benign to the serious. The following are some examples of intrusions:
- Performing a remote root compromise of an e-mail server.
- Defacing a Web server.
- Guessing and cracking passwords.
- Copying a database containing credit card numbers.

Viewing sensitive data, including payroll records and medical information, without authorization.
- Running a packet sniffer on a workstation to capture usernames and passwords.
- Using a permission error on an anonymous FTP server to distribute pirated software and music files.
- Dialing into an unsecured modem and gaining internal network access.
- Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password.
- Using an unattended, logged-in workstation without permission.

8.21.3 Intrusion Detection

- **Security Intrusion**: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.
- **Intrusion Detection**: A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.
- Intrusion detection is *based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified*.

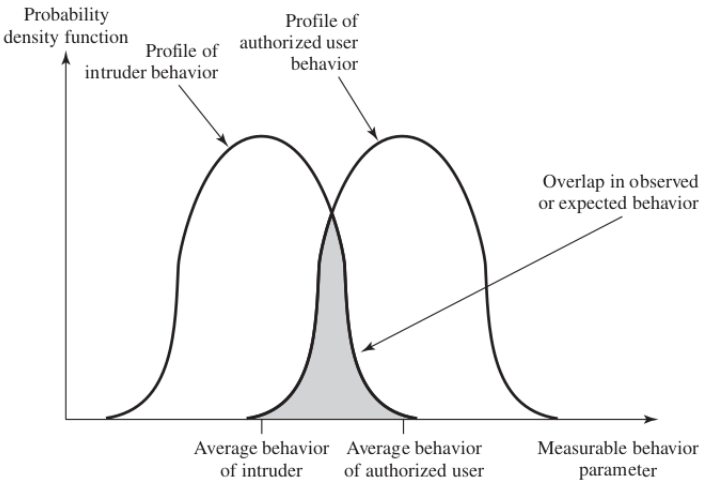


Figure 8.34: Profiles of Behavior of Intruders and Authorized Users.

8.21.3.1 Goals of Intrustion Detection

Detect a wide variety of intrusions.
- Intrusions from within the site, as well as those from outside the site, are of interest.

Detect intrusions in a timely fashion.
- "Timely" here need not be in real time. Often, it suffices to discover an intrusion within a short period of time.

Present the analysis in a simple, easy-to-understand format.

Be accurate.
- A *false positive* occurs when an intrusion detection system reports an attack, but no attack is underway. False positives reduce confidence in the correctness of the results as well as increase the amount of work involved.

However, *false negatives* (occurring when an intrusion detection system fails to report an ongoing attack) are worse, because the purpose of an intrusion detection system is to report attacks.

8.21.3.2 Approaches to Intrustion Detection

1. **Statistical anomaly detection**: Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.
   • *Threshold detection*: This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
   • *Profile based*: A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

2. **Rule-based detection**: Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.
   • *Anomaly detection*: Rules are developed to detect deviation from previous usage patterns.
   • *Penetration identification*: An expert system approach that searches for suspicious

8.21.4 IDS: Instrustion Detection System

- Unauthorized intrusion into a computer system or network is one of the most serious threats to computer security.
- ntrusion are the activities that violate the security policy of system: Integrity, confidentiality, or availability, of a computing and networking resource.
- Intrusion detection systems have been developed to provide early warning of an intrusion so that defensive action can be taken to prevent or minimize damage.
- Intrusion detection involves detecting unusual patterns of activity or patterns of activity that are known to correlate with intrusions.

8.21.4.1 Types of IDS

i. Host-based IDS
ii. Network-based IDS
iii. Anomaly detection
iv. Signature based

Host Based IDS

- Various software tools such as Metasploit, Sqlmap, Nmap, Browser Exploitation provide the necessary framework to examine and gather information form target system vulnerabilities. Malicious attackers use such information to launch attacks to various application like FTP servers, web server, SSH server etc.

- A HIDS operates at host-level by analyzing and monitoring all traffic activities on the system application files, system calls and operating system. These types of traffic activities are called typically called as audit trails.
- A host based intrusion detection system monitors the security event logs or checks the changes to the system, for example unauthorized login attempts and aberrant (departing from normal access) file accesses, on the actual target machine.

Network Based IDS

- A system that monitors network traffic and packets, and attempts to discover if a hacker/cracker is attempting to break into a system (or cause a denial of service attack).

Anomaly Detection

- Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly.
- This detection method uses machine learning to create a defined model of trustworthy activity, and then compare new behaviour against this trust model.

Signature Based IDS

- Signature-based IDS detects possible threats by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. - This terminology originates from antivirus software, which refers to these detected patterns as signatures.
- Although signature-based IDS can easily detect known attacks, it is impossible to detect new attacks, for which no pattern is available.

Most signature analysis systems are based on simple pattern matching algorithms.
- The question of what information is relevant to an IDS depends upon what it is trying to detect.
- In most cases, the IDS simply looks for a sub string within a stream of data carried by network packets.

• When it finds this sub string (for example, the “phf” in “GET /cgi-bin/phf?”), it identifies those network packets as vehicles of an attack.