Euler Theorem

If a and m are integers and (a, m) = 1 then $a^{\varphi(m)} \equiv 1 \bmod m$.

----- φ (m) is called as phi (phi value).

Calculation of φ(m).

Its count of GCD (i, m) = 1 where i is between 1< i <n

For example:

φ(m). -> φ(5).

GCD(1, 5)=1
GCD (2,5)=1
GCD (3,5)=1
GCD(4,5)=1
GCD (5, 5)=0 The total number of 1's =4 φ(5)=4

From φ(1) to φ(100)

$\pi\ 1 = 0$	$\pi\ 21 = 12$	$\pi\ 41 = 40$	$\pi\ 61 = 60$	$\pi\ 81 = 54$
$\pi\ 2 = 1$	$\pi\ 22 = 10$	$\pi\ 42 = 12$	$\pi\ 62 = 30$	$\pi\ 82 = 40$
$\pi\ 3 = 2$	$\pi\ 23 = 22$	$\pi\ 43 = 42$	$\pi\ 63 = 36$	$\pi\ 83 = 82$
$\pi\ 4 = 2$	$\pi\ 24 = 8$	$\pi\ 44 = 20$	$\pi\ 64 = 32$	$\pi\ 84 = 24$
$\pi\ 5 = 4$	$\pi\ 25 = 20$	$\pi\ 45 = 24$	$\pi\ 65 = 48$	$\pi\ 85 = 64$
$\pi\ 6 = 2$	$\pi\ 26 = 12$	$\pi\ 46 = 22$	$\pi\ 66 = 20$	$\pi\ 86 = 42$
$\pi\ 7 = 6$	$\pi\ 27 = 18$	$\pi\ 47 = 46$	$\pi\ 67 = 66$	$\pi\ 87 = 56$
$\pi\ 8 = 4$	$\pi\ 28 = 12$	$\pi\ 48 = 16$	$\pi\ 68 = 32$	$\pi\ 88 = 40$
$\pi\ 9 = 6$	$\pi\ 29 = 28$	$\pi\ 49 = 42$	$\pi\ 69 = 44$	$\pi\ 89 = 88$
$\pi\ 10 = 4$	$\pi\ 30 = 8$	$\pi\ 50 = 20$	$\pi\ 70 = 24$	$\pi\ 90 = 24$
$\pi\ 11 = 10$	$\pi\ 31 = 30$	$\pi\ 51 = 32$	$\pi\ 71 = 70$	$\pi\ 91 = 72$
$\pi\ 12 = 4$	$\pi\ 32 = 16$	$\pi\ 52 = 24$	$\pi\ 72 = 24$	$\pi\ 92 = 44$
$\pi\ 13 = 12$	$\pi\ 33 = 20$	$\pi\ 53 = 52$	$\pi\ 73 = 72$	$\pi\ 93 = 60$
$\pi\ 14 = 6$	$\pi\ 34 = 16$	$\pi\ 54 = 18$	$\pi\ 74 = 36$	$\pi\ 94 = 46$
$\pi\ 15 = 8$	$\pi\ 35 = 24$	$\pi\ 55 = 40$	$\pi\ 75 = 40$	$\pi\ 95 = 72$
$\pi\ 16 = 8$	$\pi\ 36 = 12$	$\pi\ 56 = 24$	$\pi\ 76 = 36$	$\pi\ 96 = 32$
$\pi\ 17 = 16$	$\pi\ 37 = 36$	$\pi\ 57 = 36$	$\pi\ 77 = 60$	$\pi\ 97 = 96$
$\pi\ 18 = 6$	$\pi\ 38 = 18$	$\pi\ 58 = 28$	$\pi\ 78 = 24$	$\pi\ 98 = 42$
$\pi\ 19 = 18$	$\pi\ 39 = 24$	$\pi\ 59 = 58$	$\pi\ 79 = 78$	$\pi\ 99 = 60$
$\pi\ 20 = 8$	$\pi\ 40 = 16$	$\pi\ 60 = 16$	$\pi\ 80 = 32$	$\pi\ 100 = 40$

Case i) In φ(m) if m =prime , then φ(m)=(m-1)

Ex:- φ(7) =(7-1)=6

Case ii) In φ(m), can be expressed as $= \varphi(x) * \varphi(y)$ (if x and y are not same) calculate φ(x) and φ(y)

Ex :- $\varphi(35) = \varphi(5) * \varphi(7) = 4*6=24$

Case iii) In φ(m), can be expressed as $= \varphi(x) * \varphi(x) \ldots = x^n - x^{n-1}$

Ex $\varphi(49) = \varphi(7) * \varphi(7) = 7^2 = 7^2 - 7^{(2-1)} = 49-7=42$

Ex: φ(240) which large then Take LCM

2	**240**
2	**120**
2	**60**
2	**30**
3	**15**
5	**5**
	1

Can be written as : $\varphi(2^4) * \varphi(3) * \varphi(5) = (2^4 - 2^{4-1}) * 2 * 4$

$= 8 * 2 * 4$

$= 64$

Fermat's "Little" Theorem

Let 'p' be prime and 'a' be an integer which is not a multiple of p. Then $a^{(p-1)} \equiv 1 \pmod{p}$.

i) Example. 97 is prime and 2 is not a multiple of 97, so $2^{96} \equiv 1 \pmod{97}$.

ii) $4^{16} \bmod 17 = ?$,

(p-1)= 17-1 Prime(p)

Since 17 is prime , (17-1) = 16 , So $4^{16} \bmod 17 = 1$,

iii): $2^{602} \bmod 11 = 2^{10*60+2} \bmod 11$

$= 2^{(10**60)} * 2^2 \bmod 11$ (since $2^{10} \bmod 11 = 1$, by Fermat)

$= 1 * 4 \bmod 11$

$= 4$

iv). 97 is prime and 2 is not a multiple of 97, so 296 ≡ 1 (mod 97).

<u>Primality test:</u> <u>(Miller-Rabin-Test)</u>

To find given number is prime or Not

```
Miller-Rabin-Test (n, a) // n is the number; a is the base{
Find m and k such that n − 1 = m x 2^k
T ← a^m mod n
If (T = ±1)return "a prime"
for (i ← 1 to k − 1) // k − 1 is the maximum number of steps{
T ← T^2 mod n
if (T = ±1) return "a composite"
if (T = −1) return "a prime"
}
return "a composite"}
```

Example 1) : Apply Miller-Rabin Algorithm using base 2 to test whether the number 341 is composite or not.

Solution: Using Miller-Rabin Algorithm, we can test the number 341 as follows −

Step1: $341 - 1 = 2^2 \times 85$. Thus p = 341, k = 2 and q = 85

Step2: x = 2 (given)

Step3: $S = x^q \bmod p$

$= 2^{85} \bmod 341 = (2^{10}) \times 2^5 \bmod 341$ 8

$= 2^{10} \bmod 341 \times 2^{13} \bmod 341$

$= 1 \times 8192 \bmod 341 = 8192 \bmod 341$

$= 8$

Step4: As $8 \neq 1$, we move to the next step.

Step5: For j = 1, $S = x^{2q} \bmod p$

$= 2^{170} \bmod 341 = (2^{20})^8 \times 2^{10} \bmod 341$

$= 2^{20} \bmod 341 \times 2^8 \bmod 341 \times 2^{10} \bmod 341$

$= 1 \times 256 \times 1 = 256$

Now, $= 256 \neq 1$

and result is inconclusive

So, 341 is not a composite number.

Example ii) n=97

Step 1 : (n-1) = 2^K *d

96 = 2^5 * 3

Step 2 : x=2, S = x^q mod p

= 2^3 mod 97

=8 mod 97

KEY POINTS

- The **Open Systems Interconnection** (OSI) security architecture provides a systematic framework for defining security attacks, mechanisms, and services.
- **Security attacks** are classified as either passive attacks, which include unauthorized reading of a message of file and traffic analysis or active attacks, such as modification of messages or files, and denial of service.
- A **security mechanism** is any process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. Examples of mechanisms are encryption algorithms, digital signatures, and authentication protocols.
- **Security services** include authentication, access control, data confidentiality, data integrity, nonrepudiation, and availability.

1. COMPUTER SECURITY CONCEPTS

- COMPUTER SECURITY: 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 introduces three key objectives that are at the heart of computer security:
- **Confidentiality**
- **Integrity**
- **Availability**

- **Confidentiality:** Data confidentiality, Privacy
- **Integrity:** Data integrity, System integrity
- **Availability**.

CIA triad (Figure 1.1)

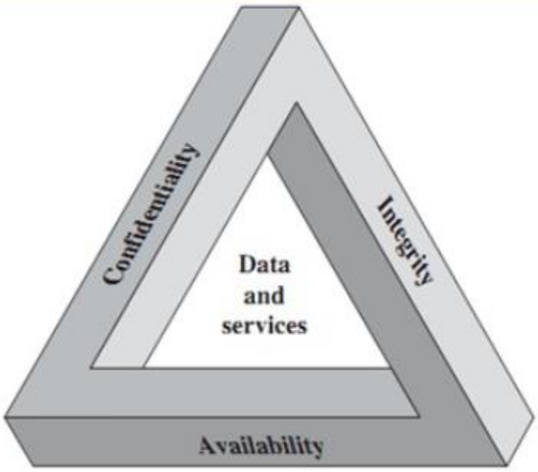


Figure 1.1 The Security Requirements Triad

- Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:
- **Authenticity**: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source

2. THE OSI SECURITY ARCHITECTURE

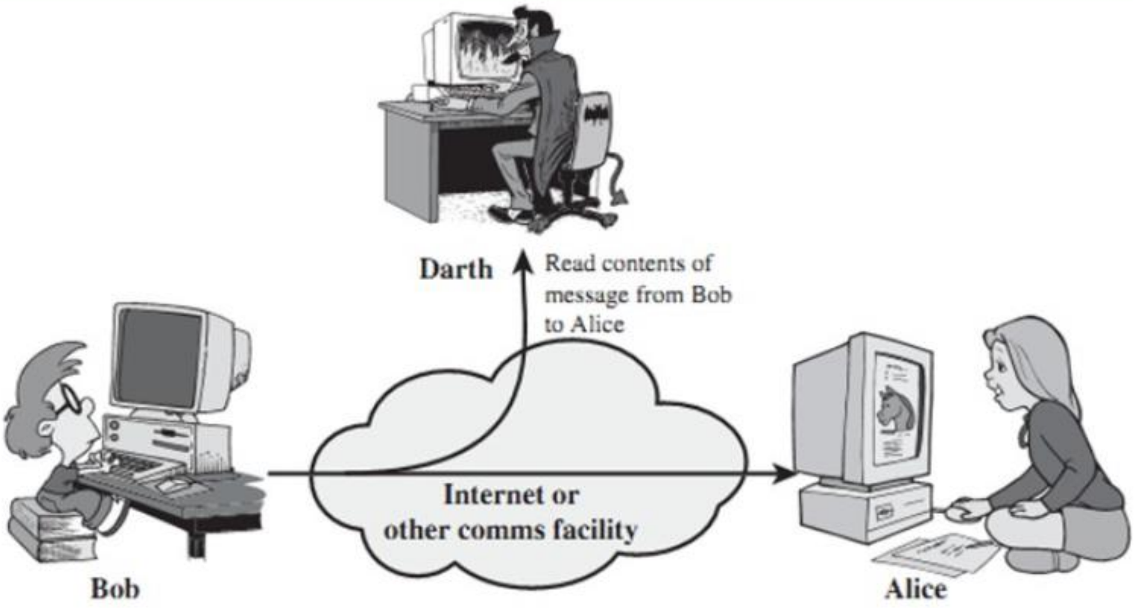
- **Threats and Attacks (RFC 2828)**
- **Threat:** A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
- **Attack:** An assault on system security that derives from an intelligent threat; that is, 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.

The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as

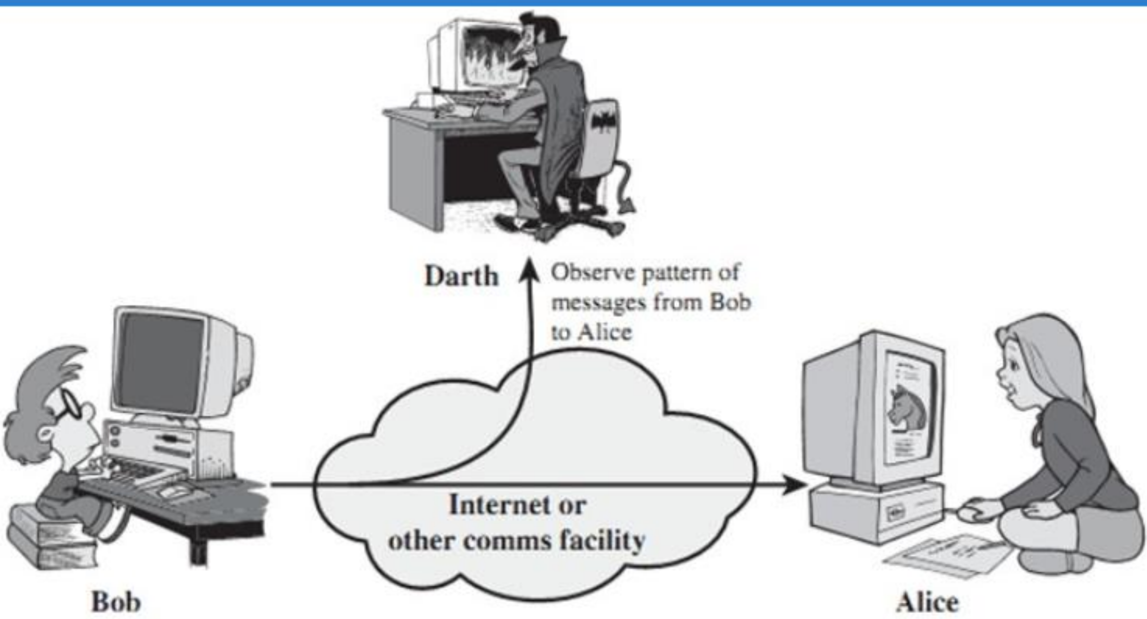
- **Security attack**: Any action that compromises the security of information owned by an organization.
- **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service**: A processing or communication 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.

3. SECURITY ATTACKS

- **Passive Attacks**: Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are **the release of message contents** and **traffic analysis.**



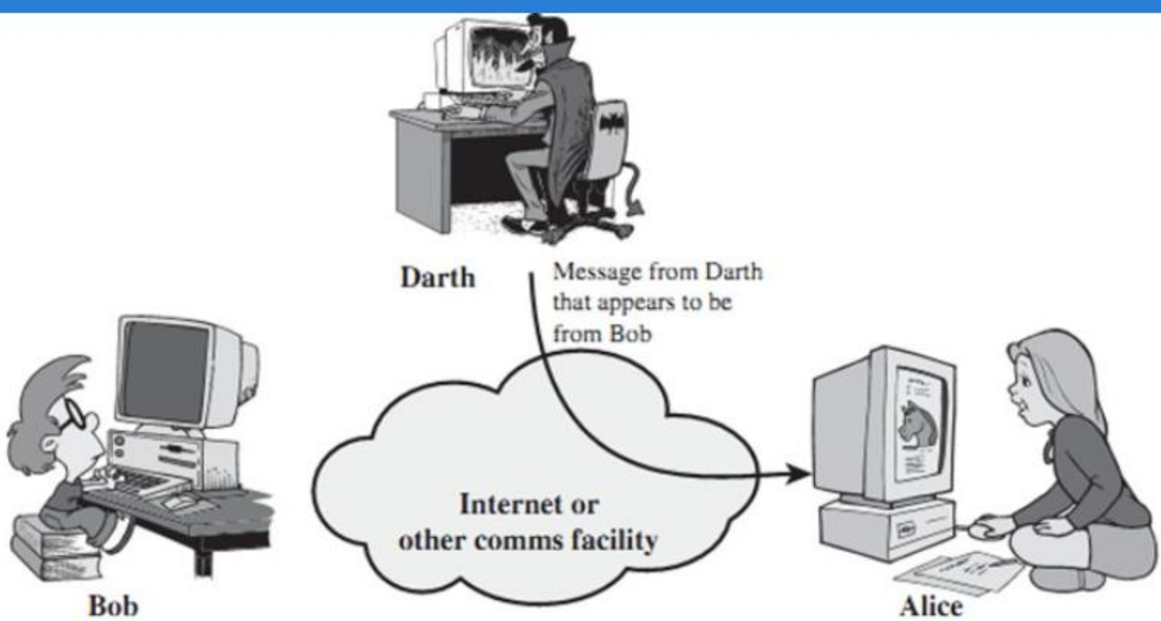
(a) Release of message contents



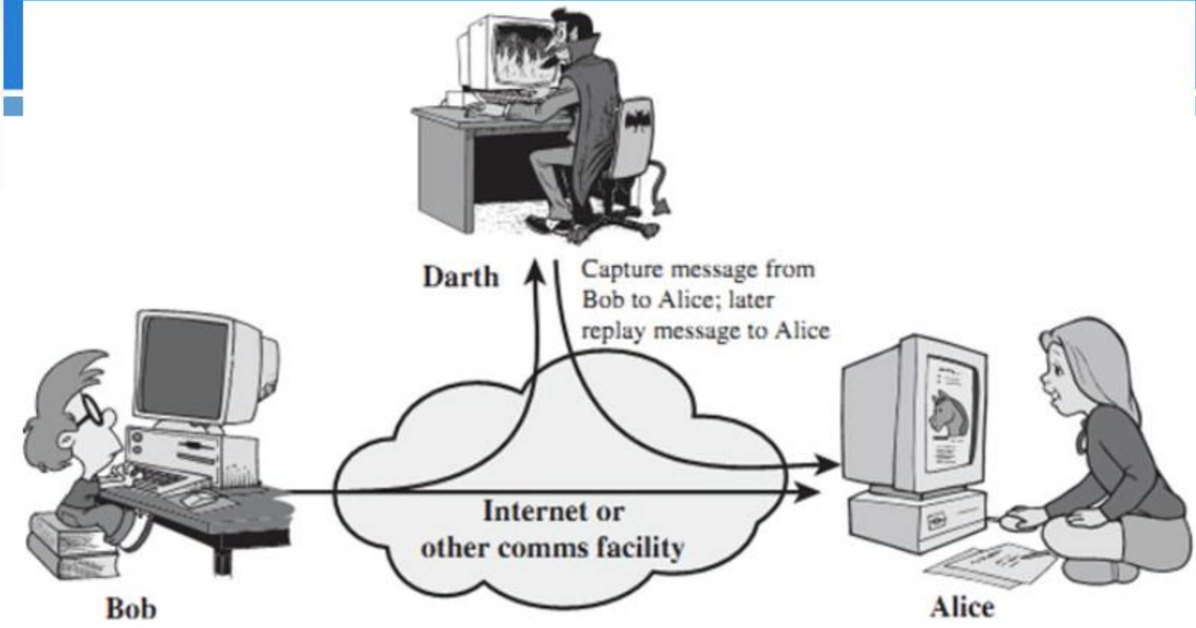
(b) Traffic analysis

Active Attacks

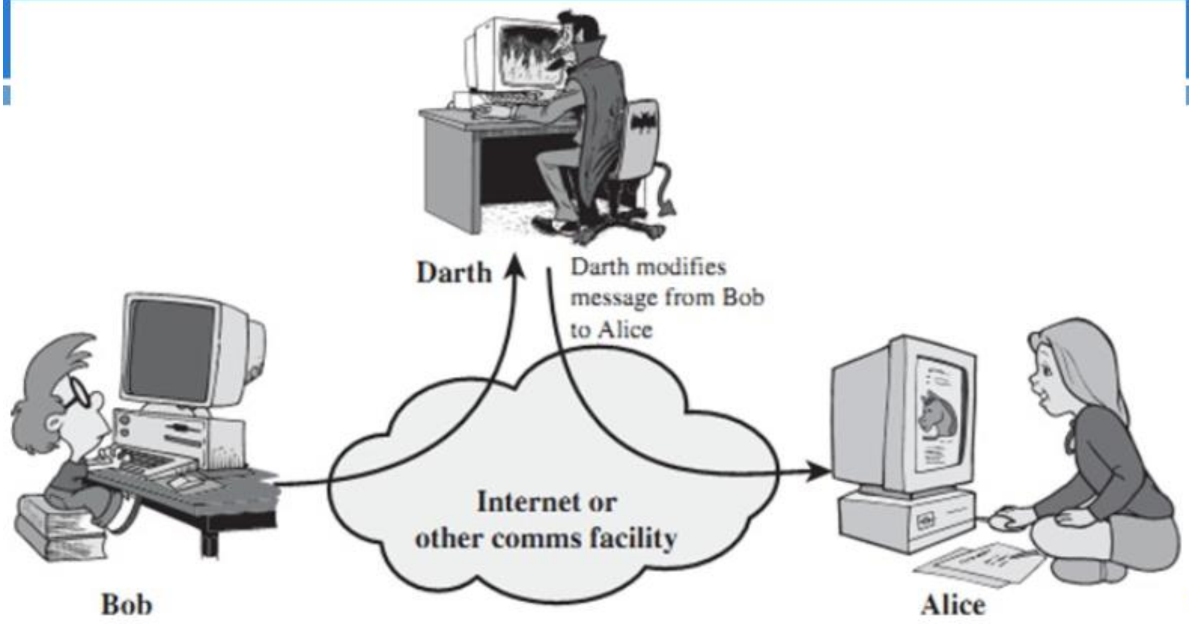
- Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: **masquerade, replay, modification of messages,** and **denial of service**.
- Masquerade (Figure 1.3a)
- Replay (Figure 1.3b)
- Modification of messages (Figure 1.3c)
- Denial of service (Figure 1.3d)



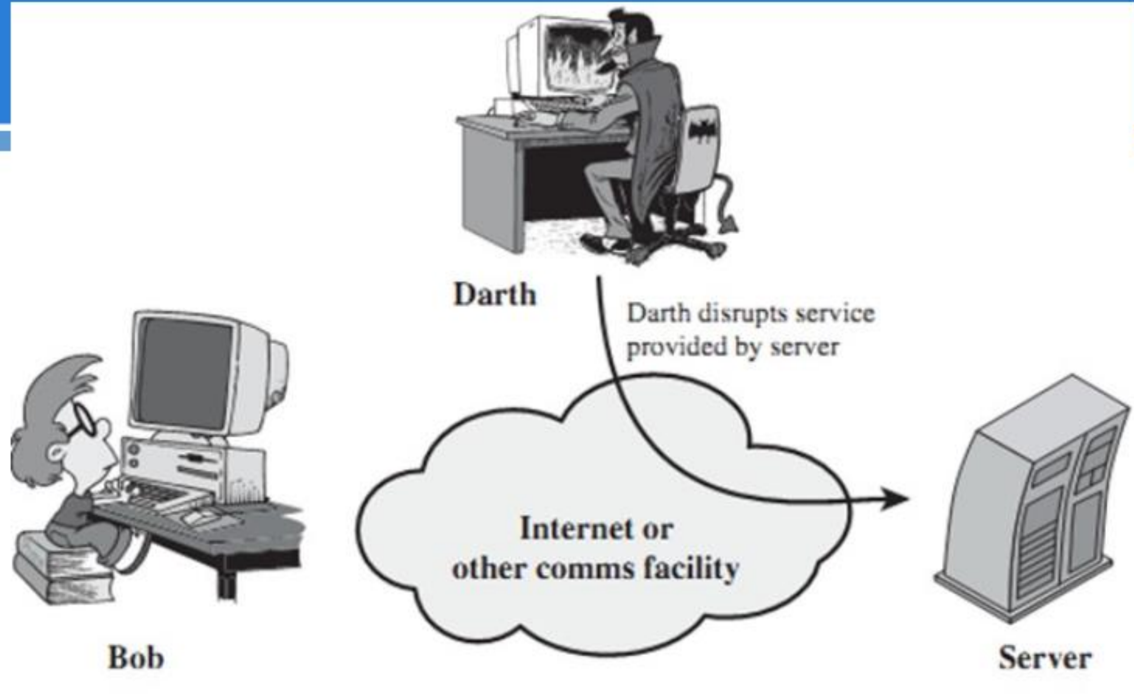
(a) Masquerade



(b) Replay



(c) Modification of messages



(d) Denial of service

4. SECURITY SERVICES

Table 1.2 Security Services (X.800)

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

5. SECURITY MECHANISMS

Table 1.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment
The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Digital Signature
Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

Access Control
A variety of mechanisms that enforce access rights to resources.

Data Integrity
A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange
A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding
The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control
Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization
The use of a trusted third party to assure certain properties of a data exchange.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality
That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label
The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection
Detection of security-relevant events.

Security Audit Trail
Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

Security Recovery
Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

6. A MODEL FOR NETWORK SECURITY

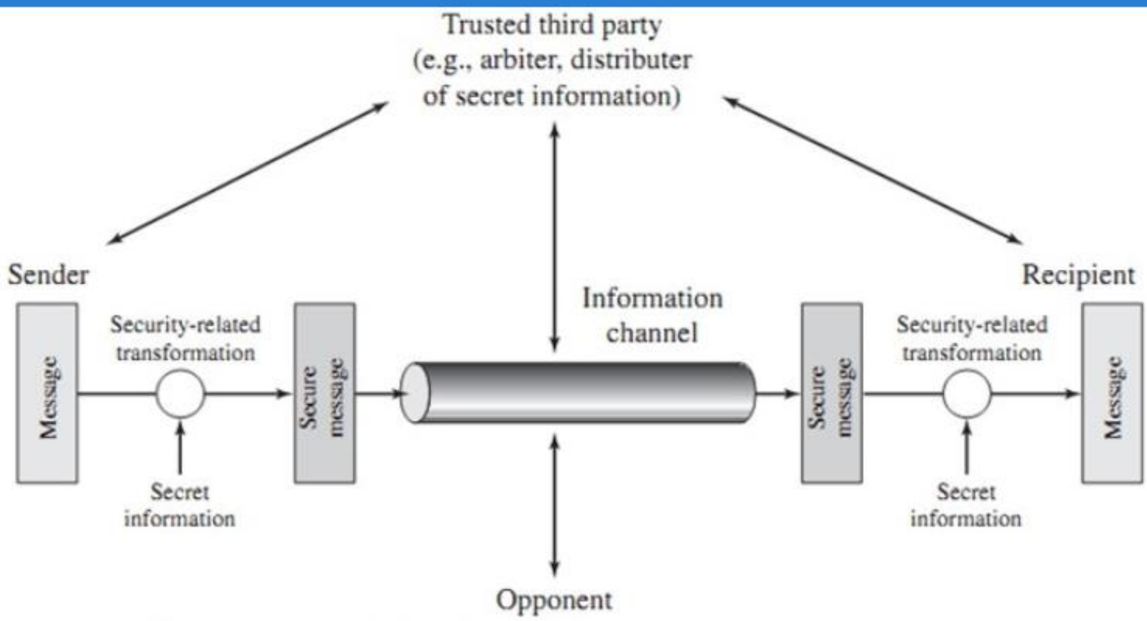


Figure 1.4 Model for Network Security

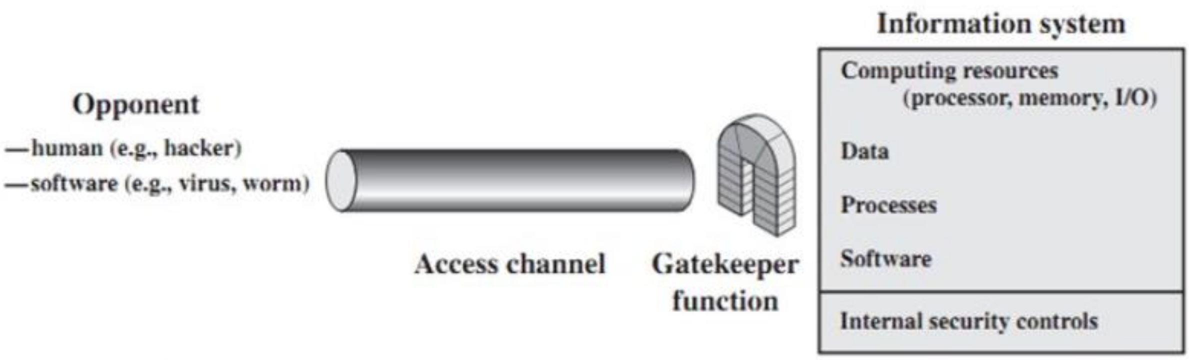


Figure 1.5 Network Access Security Model