LECTURE NOTES ON COMPUTER AND DATA SECURITY

By
Dr. Samaher Hussein Ali

College of Information Technology, University of Babylon, Iraq
Samaher_hussein@yahoo.com
Basic Concepts

Computer

an electronic device which is capable of receiving information (data) in a particular form and of performing a sequence of operations in accordance with a predetermined but variable set of procedural instructions (program) to produce a result in the form of information or signals.

Computer is derived from the word compute which means compute or calculating in right manner. It can access, store, and retrieved the large amount of data without intervention of human.

Data

- Collection of data objects and their attributes
- An attribute is a property or characteristic of an object
  
  Examples: eye color of a person, temperature, etc.
- A collection of attributes describe an object.
  
  Object is also known as record, point, case, sample, entity, or instance

Information

Collection of organization data or preparing data to take the decision, where

Data + Processing = Information

Example: book is data while my book is information.
Security

Refer to the communication (information) security

**Source of information**

<table>
<thead>
<tr>
<th>sender part</th>
<th>receiver part</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Person (text, speech)</td>
<td>Person</td>
</tr>
<tr>
<td>2. Video</td>
<td>TV</td>
</tr>
<tr>
<td>3. Sensor</td>
<td>Controller</td>
</tr>
<tr>
<td>4. Image</td>
<td>Computer storage of image</td>
</tr>
</tbody>
</table>

**Processor 1**

Adaptation of the source information into the communication channel by one of the three methods “modulation, coding, ciphering “
Basic Concepts

Processor 2

receive the information from the communication channel and treatment by one of the three methods “demodulation, decoding, deciphering “

In general:

Processor 1  processor 2
1. Modulation  ======>  Demodulation
2. coding  ======>  Decoding
3. Ciphering  ======>  Deciphering

Computer Security

Refer to the security of computers against intruders (e.g., hackers) and malicious software (e.g., viruses). Typically, the computer to be secured is attached to a network and the bulk of the threats arise from the network.

Data Security

Refer to the term Cryptography is one of the mathematical application that is useful in transforming that data through an insecure communication network, which is the worst case.

As a result: security have two parts:

1. Cryptography
2. Physical pretiction
Basic Concepts

cryptography
is the study of secret (crypto-) writing (-graphy)

cryptography
the art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form

plaintext
the original intelligible message

ciphertext
the transformed message

cipher
an algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods

key
some critical information used by the cipher, known only to the sender & receiver

encipher
the process of converting plaintext to ciphertext using a cipher and a key

decipher
the process of converting ciphertext back into plaintext using a cipher and a key

cryptanalysis
the study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key.
cryptology
both cryptography and cryptanalysis