# Department of Computing

**CS-381: Network Security**

**Class: BESE 5**

# Lab 01: Attributes of a Secure Network

**Date: September 14, 2017**

**Time: 2pm to 5 pm**

**Maryam Hashmi**

**11254**

# Lab 01: Attributes of a Secure Network

**Introduction**

The security attack is an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or makes unauthorized use of an asset. It is mainly classified into two main categories: (i) Passive Attacks, (ii) Active Attacks. The passive attacks, monitors unencrypted traffic; looks for clear-text passwords and sensitive information that can be used to launch other type of attacks. While, in active attacks, the attacker tries to bypass or break into the secure systems with the help of stealth, viruses, worms, or Trojan horses.

The purpose of this lab is to let the students become familiar with the attributes of a secure network that can resist both active and passive attacks. For this lab the students are required to perform two tasks (i) to surf the internet and list the attributes that a network must have to become a secure network and (ii) implement confidentiality service and exchange a message securely to another computer over the internet without using a secure socket.

**Objectives**

The main objective of this lab is:

* To understand the attributes that a secure network should have.
* To understand confidentiality services and how to switch them on.
* To implement a basic cipher, encrypt the message and then send it over an insecure medium.

**Tools/Software Requirements**

Java (or any other language of choice), Socket Programming

**Description**

**Task 1:**

You are required to search and list down the attributes of a secure network e.g. confidentiality is a required security attribute for a network. You are also required to study about each attribute and give some description (2-3 lines) for each attribute in the form of an example to help understand its cornerstones.

Major attributes of a secure network are:

**Confidentiality:**

Ability to hide information from those unauthorized to view it.

Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question.

**Integrity:**

Ability to ensure that data is an accurate and unchanged representation of the original secure information. It involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality).

There can be two kinds of integrity; data integrity an system integrity.

**Availability:**

The information is visible to authorized user at all times. Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It’s also important to keep current with all necessary system upgrades.

**Task 2:**

After studying the attributes in Task 1, you will be able to understand the meanings of confidentiality i.e. to process data in such a manner that only the intended recipient can understand the meanings.

Confidentiality can be achieved by using various ciphers, one of the basic one is called “Caesar Cipher”. You are required to study it and then make a class called “CaesarCipher” that should have the following functions:

1. public String encrypt(String plainMessage)
2. public String decrypt(String cipherText)

“encrypt” function will encrypt the plaintext and return the cipher text while decrypt will do the reverse of it.

You are required to implement two more classes called:

1. Sender.java: It will encrypt the user messages and then send them by using normal sockets. See manual of Socket class in Java. Your implementation will be evaluated by entering a text string e.g. “HelloWorld”. This string should be first encrypted to something like “JgnnqYqtnf” and then sent to the receiver program.
2. Receiver.java: It will receive the messages, decrypt them and then show the plaintext as an output.

**The files are attached.**