# Department of Computing

**CS-381: Network Security**

**Class: Group-1**

# Lab 01: Attributes of a Secure Network

**Date: September 11, 2017**

**Time: 0900 to 1200**

# Instructor: Dr. Shahzad Saleem

# Hadaiq Ahmad

# 112807

# Group-1

# 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 can a required security attribute for a network. You are required to list down such attributes. You are also required to study about each attribute and give some description (one paragraph) for each attribute with an example to help us understand its cornerstones.

Ans:

1. **Integrity:**

Information security plays a very important role in maintaining the security in different types of drastic conditions such as the errors of the integrity. As we know that information, security is used to provide the protection to the documentation or different types information present on the network or in the system. So, there are many viruses that can infect the computer, slows down the working and also break the integrity of the system. Therefore, information security provides the valuable and easy steps to prevent the different types of errors created due to integrity.

1. **Confidentiality:-**

It is uses to protect the information on network to keep your information safe.  For example, different types of thieves use different types of methods to steel the confidential information on the internet without the knowledge of the person, such as credit card number and steel all the money

#### **Availability**

Availability is a requirement intended to ensure that systems work promptly and service is not denied to authorized users it represents the ability to protect against and recover from a damaging event

1. Accuracy

Information has accuracy when it is free from mistakes or errors and it has the value that the end user expects. for example, a checking account. You assume that the information contained in your checking account is an accurate representation of your finances. Incorrect information in your checking account can result from external or internal errors

1. Authenticity

Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred.

1. Utility

The utility of information is the quality or state of having value for some purpose or end. Information has value when it can serve a purpose. If information is available, but is not in a format meaningful to the end user, it is not useful

1. Possession

The possession of information is the quality or state of ownership or control. Information is said to be in one’s possession if one obtains it, independent of format or other characteristics.

References

<http://wifinotes.com/security/what-is-information-security.html>

<http://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf>

<https://www.nap.edu/read/1581/chapter/4#60>

**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 encrypted 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.

Ans-

package nslab1;

/\*\*

\*

\* @author test1

\*/

import java.util.Scanner;

public class NsLab1

{

public static final String ALPHABET = "abcdefghijklmnopqrstuvwxyz";

public static String encrypt(String plainText, int shiftKey)

{

plainText = plainText.toLowerCase();

String cipherText = "";

for (int i = 0; i < plainText.length(); i++)

{

int charPosition = ALPHABET.indexOf(plainText.charAt(i));

int keyVal = (shiftKey + charPosition) % 26;

char replaceVal = ALPHABET.charAt(keyVal);

cipherText += replaceVal;

}

return cipherText;

}

public static String decrypt(String cipherText, int shiftKey)

{

cipherText = cipherText.toLowerCase();

String plainText = "";

for (int i = 0; i < cipherText.length(); i++)

{

int charPosition = ALPHABET.indexOf(cipherText.charAt(i));

int keyVal = (charPosition - shiftKey) % 26;

if (keyVal < 0)

{

keyVal = ALPHABET.length() + keyVal;

}

char replaceVal = ALPHABET.charAt(keyVal);

plainText += replaceVal;

}

return plainText;

}

public static void main(String[] args)

{

Scanner sc = new Scanner(System.in);

System.out.println("Enter the String for Encryption: ");

String message = new String();

message = sc.next();

System.out.println(encrypt(message, 3));

System.out.println(decrypt(encrypt(message, 3), 3));

sc.close();

}

}

Part -2

TCP\_sender

#key = 'abcdefghijklmnopqrstuvwxyz'

#def encrypt(n, plaintext):

#result = raw\_input('Encrypt the string and return the ciphertext:')

def encrypt(data):

cypher = 1

ALPHABET ='abcdefghijklmnopqrstuvwxyz .'

modifiedsen = [ALPHABET[ALPHABET.index(x)+cypher] for x in data]

return ''.join(modifiedsen)

#for l in plaintext.lower():

#try:

#i = (key.index(l) + n) % 26

#result += key[i]

#except ValueError:

#result += l

#print result

#clientSocket.send(result)

#return result.lower()

from socket import \*

serverIP = '10.99.39.138'

serverPort = 12000

clientSocket = socket(AF\_INET, SOCK\_STREAM)

result = raw\_input('Encrypt the string')

result=str(result)

print 'crypted:',encrypt(result)

clientSocket.connect((serverIP,serverPort))

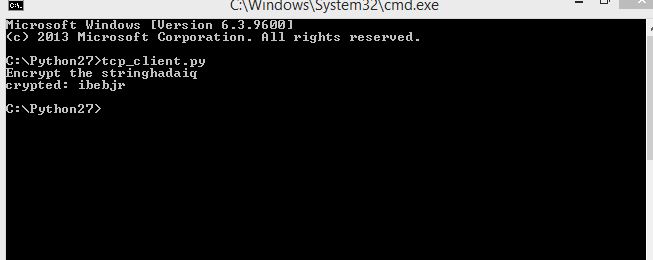
clientSocket.send(encrypt(result))

clientSocket.close()

#modifiedSentence = clientSocket.recv(1024)

#print 'From Server:', modifiedSentence

#clientSocket.close()



Tcp\_reciever

#def decrypt(n, ciphertext):

#result = ''

#for l in ciphertext:

#try:

#i = (key.index(l) - n) % 26

#result += key[i]

#except ValueError:

#result += l

#return result

def decrypt(data):

cypher = 1

alphabet ='abcdefghijklmnopqrstuvwxyz .'

newsen = [alphabet[alphabet.index(x)-cypher] for x in data]

return ''.join(newsen)

#key = 'abcdefghijklmnopqrstuvwxyz'

#def encrypt(n, plaintext):

#result = raw\_input('Encrypt the string and return the ciphertext:')

#for l in plaintext.lower():

#try:

#i = (key.index(l) + n) % 26

#result += key[i]

#except ValueError:

#result += l

#print result

#return result.lower()

from socket import \*

serverPort = 12000

serverSocket = socket(AF\_INET,SOCK\_STREAM)

serverSocket.bind(('',serverPort))

serverSocket.listen(1)

print 'The server is ready to receive'

while 1:

connectionSocket, addr = serverSocket.accept()

sentence = connectionSocket.recv(1024)

print 'encrypted message from client:',sentence

print "decrypted message: ",'',decrypt(sentence)

connectionSocket.close()

#def show\_result(plaintext, n):

#'Generate a resulting cipher with elements shown'

#encrypted = encrypt(n, plaintext)

#decrypted = decrypt(n, encrypted)

#print 'Rotation: %s' % n

#print 'Plaintext: %s' % plaintext

#print 'Encrytped: %s' % encrypted

#print 'Decrytped: %s' % decrypted



**Deliverable:**

Students are required to upload the complete report on LMS before the deadline.