Exercise 04

Feb 20, 2023

# Overview

This exercise provides hands-on experience with Cryptography to perform secure exchange of Keys between two parties using Diffie Hellman Key Exchange algorithm.

# Learning Objectives

* Understand basics of Diffie Hellman Key Exchange.
* Understand basic of Discrete algorithm.
* Ability to implement the algorithm and communicate message across TCP/IP network
* Ability to work together in a small team.

# Reading Material

1. Chapter 21, Principles of Computer Security, 4th ed, Stallings and Brown, Pearson.
2. Using netcat to transfer data.

# Prerequisites and environment familiarity

Familiarity with Linux and command line terminal usage.

Familiarity with network communication between two systems connected via a network. This could be either using socket programming or using netcat (nc) to communicate across the network between two hosts.

Familiarity with tcpdump (or wireshark) to capture and analyze the packets.

As a team of two you have access to 2 systems connected via a network. If you would like, you can work independently as well though it would be preferred to have a team. If you are not able to find your team mate, get in touch with TA and he will (randomly) assign the team mate to you.

# Description

This exercise is done with the same team as in Exercise 3, involves exchanging a secure key using DH Key exchange algorithm. Thus, it involves a bit of programming (in your preferred prog. language). You need to write a program to implement DH Key Exchange algorithm, and after key is exchanged, send and receive the message using this secret shared key.

## Assignment details

1. Use one of the two given prime numbers P as given in appendix A. Each student is given a prime number and thus team gets two prime numbrs.
2. Compute α as one of the primitive root.
3. User1 (First member of the team) chooses Xa (at least of 4 digits), and computes Ya=αXa,
4. User2 (Second member of the team) chooses Xb (at least of 4 digits) and computes Yb=αXb.
5. Assuming two machines are vm1 and vm2.
6. User1 communicates Ya to user2, and user2 computes key K=YaXb.
7. User2 communicates Yb to user1 and user1 computes Key K=YbXa.
8. Consider that message m as m=”Hello, it is a nice sunny day and we should enjoy the weather” and reply r as r=”Busy with assignment right now.”.
9. On vm1, implement RC4 using the key K (integer value converted to text) as computed above and send the message m to vm2.
10. Follow the instructions/guidelines in Exercise 03 on communicating between two systems especially for those who aren’t aware of socket programming.
11. Do a tcpdump capture on both vm1 and vm2 to ensure that encrypted message is being transmitted.

## Explanation and Hints

1. Revise your network programming concepts. If you haven’t done network programming, get familiar with using netcat (nc).
2. Refresh/revise your wireshark/tcpdump skills. In case you haven’t used wireshark before, install the same and become familiar with it.
3. First just output the key from RC4 sender and manually encrypt the data being sent character by character by XORing it with pseudorandom number key k.
4. Verify that same encrypted value is being transmitted over the network.

# Assessment and Rubric

Please do submit the following

1. Readme.txt file which will contain the following information
   1. Team information i.e. names of both team mates with their university id.
   2. Values of prime number P, primitive root α, Xa, Xb and key K.
   3. Commands invoked on both the vms for invoking the program.
   4. Challenges faced and how did you address these.
   5. Summary of your overall learning.
   6. References. Any website/resource that you used to took help.
2. The programs on vm1 and vm2 along with their respective tcpdump/wireshark capture. This time the program would involve using DH Key exchange implementation as well as RC4 based stream cipher communication. So, this will be enhancement over exercise 03.

**Rubric for assessment (20 marks)**

* 1. 4 marks for a Readme.txt file containing all the required information
  2. 8 marks DH key exchange implementation
  3. 4 marks for using key as agreed upon using DH Key exchange.
  4. 4 marks for tcpdump/wireshark captures.

# Appendix: Prime Number[[1]](#footnote-1)

|  |  |  |
| --- | --- | --- |
| Student Name | usernames | Prime Number |
| Abir | abir | 1003001 |
| Ben | Ben | 1008001 |
| Bhargavi | Bhargavi | 1022201 |
| Cyriac | Cyriac | 1028201 |
| Darshan | Darshan | 1035301 |
| Deepak | Deepak | 1043401 |
| Divya | Divya | 1055501 |
| Ekta | Ekta | 1062601 |
| Faisal | Faisal | 1065601 |
| Funiba | Funiba | 1074701 |
| Joseph | Joseph | 1082801 |
| Kathleen | Kathleen | 1085801 |
| Kyle | Kyle | 1092901 |
| Lakshmipriyanka | Lakshmipriyanka | 1093901 |
| Mounika | Mounika | 1114111 |
| Mythri | Mythri | 1117111 |
| Namratha | Namratha | 1120211 |
| Sairam | Sairam | 1123211 |
| Shrenik | Shrenik | 1126211 |
| Smit | Smit | 1129211 |
| Tejish | Tejish | 1134311 |
| Varun | Varun | 1145411 |
| Vishnu | Vishnu | 1150511 |

# Note

Any plagiarism activity will result in penalties of being awarded 0 marks. If you are using the sample program as shown in the class, please attribute the same.

<end of Exercise 03>

1. The prime number values are taken from https://www.rsok.com/~jrm/7\_digit\_palindromic\_primes.html [↑](#footnote-ref-1)