# Computer Lab 03

## Sharing Files and Analyzing Encryption Key Management Approaches

Networked Information Systems (COMP2410/ COMP6340), 2022 Semester 1

A/Prof Hanna Suominen, Dr Zakir Hossain, and Dr Okki Lee

Research School of Computer Science,

College of Engineering and Computer Science (CECS)

The Australian National University

Canberra ACT 2601 Australia

www.anu.edu.au

CRICOS Provider No. 00120C

# Contents

# VPN and Encryption Key Management Software

## Summary

A virtual private network (VPN) masks internet protocol (IP) address to ensure security from a public internet connection by creating a private network. It is established by using tunneling protocols or dedicated circuits over existing networks. It allows users to access resources remotely and securely.

Kleopatra is a security encryption key manager, helping to create both public and private keys with RSA algorithm. It supports managing X.509 and OpenPGP certificates in the GpgSM keybox and retrieving certificates from LDAP servers. In this lab, we will learn to compare and contrast available approaches for encryption key management. In addition, we will also learn how to share folders/files in Linux.

You should complete the encryption lab of the textbook (i.e., the Hands-on Activity 11C, pp. 336-339). The purpose of this lab is to practice encrypting and decrypting email messages using a standard called PGP (Pretty Good Privacy) that is implemented in an open-source software Gnu Privacy Guard. You will need to download and install the Kleopatra software on your computer from this website: https://www.symantec.com/connect/downloads/symantec-pgp-desktop-peer-review-source-code . For Mac OS X users, please visit this website: http://macgpg.sourceforge.net. Alternatively, if installing the software is not possible for you (e.g., restricted network bandwidth), you may wish to complete the activity by analysing the screen captures of the textbook (i.e., Figures 11-21–11-23) instead.

## Learning Objectives

After completing this lab, students should

- be able to share folders/files in Linux, and
- be able to analyse available approaches (e.g., Kleopatra) for encryption key management

# Folders/files sharing in Linux

## Requirements

i. Ubuntu Host 16.04 / Mac or Windows with a virtual box installed

ii. Ubuntu VM on VirtualBox - Ubuntu 16.04 guest

   a. Download it from here if you don't have it already https://cloudstor.aarnet.edu.au/plus/s/FEhtnfbpufo7MJq.Username: vagrant, Password: vagrant.

   b. Note: Feel free to use your own Ubuntu VM if you want.

   c. Attach two network adopters with the guest. NAT (for internet access) and Host-only (to communicate with the host)

iii. Ubuntu Host can ping Ubuntu guest (should work if you attached host-only adopter correctly)

iv. Username: vagrant password: vagrant ***on Ubuntu guest***

## Procedures

***On Ubuntu guest***

**1. Install samba**

vagrant@vagrant16:~$ sudo apt-get install samba

**2. Configure samba on Ubuntu guest**

vagrant@vagrant16:~$ sudo nano /etc/samba/smb.conf

nano is an editor. refer (https://www.hostinger.com/tutorials/how-to-install-and-use-nano-text-editor) for more information.

Once smb.conf opens up, add the following lines to define a samba user [sharedusr] and give path of the directory that will be shared with the host (we will make this folder later on). Make sure you save changes.

```
[sambashare]
comment = Samba directory
path = /home/sharedusr/samba
public = yes
read only = no
browsable = yes
```

Your file should look something like this.

```
arslan@arslan-VirtualBox:~$ cat /etc/samba/smb.conf
[sambashare]
comment = Samba directory
path = /home/sharedusr/samba
public = yes
read only = no
browsable = yes

#
# Sample configuration file for the Samba suite for Debian GNU/Linux.
#
#
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
```

3. **Create a Linux user (sharedusr)**

   vagrant@vagrant16:~$ sudo adduser sharedusr

   Enter new UNIX password: samba

   Retype new UNIX password: samba

4. **Create a samba user**

   vagrant@vagrant16:~$ sudo smbpasswd -a sharedusr

   New SMB password: samba

   Retype new SMB password: samba

   Added user sharedusr.

5. **Create a shared folder and Restart samba server**

   Give sharedusr the sudo access

   vagrant@vagrant16:~$ sudo usermod -aG sudo sharedusr

   Start working as sharedusr (notice name change from vagrant to sharedusr)

   vagrant@vagrant16:~$ sudo su sharedusr

   Go to root directory where we will make a shared folder samba, this is the same path which we defined in smb.conf file. Use pwd command to verify this as well.

   sharedusr@vagrant16:/home/vagrant$ cd ~

   Make folder named samba

```
sharedusr@vagrant16:~$ mkdir samba
```

Restart samba services

```
vagrant@vagrant16:~$ sudo service smbd restart
```

6. **Find out the IP address of samba server**

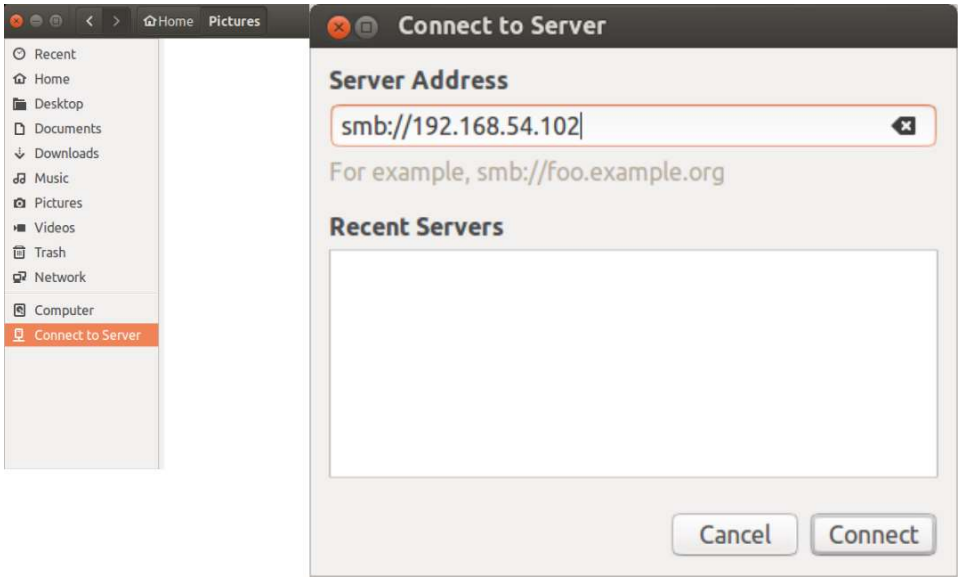
```
vagrant@vagrant16:~$ ifconfig
…
enp0s8 Link encap:Ethernet HWaddr 08:00:27:2a:d5:c8
inet addr:192.168.54.102 Bcast:192.168.54.255 Mask:255.255.255.0
```

You will see two ip addresses. You need the one from host-only adaptor and not the NAT adapter. NOTE: you necessarily won't see exactly the same IP address as shown in this handout and pictures.

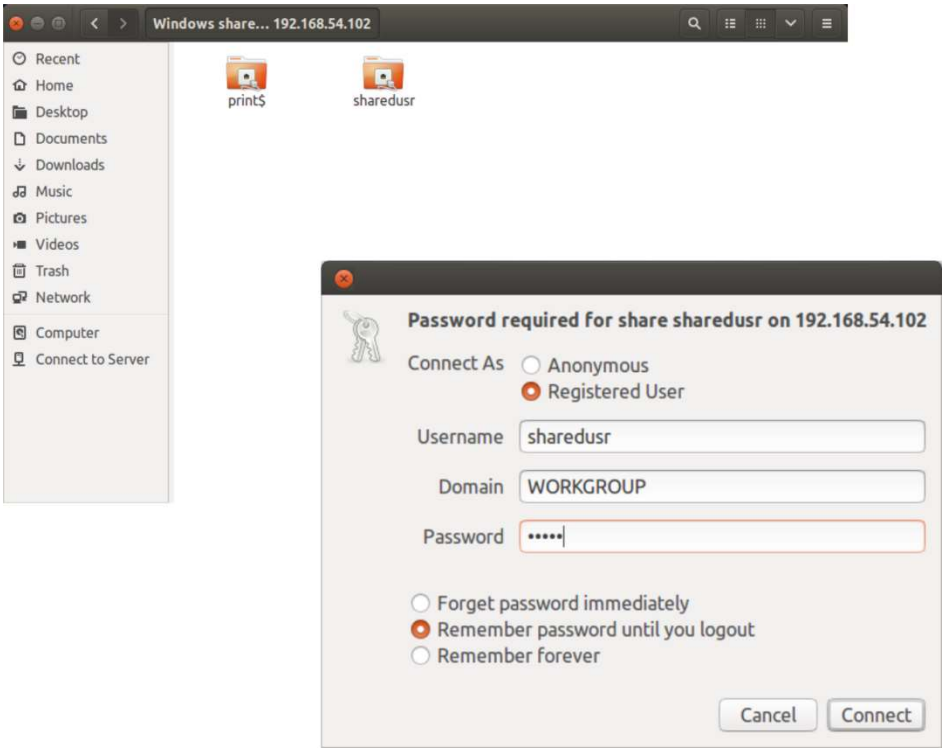
***On Ubuntu host***

If your personal host is windows or mac then things might be a little different. Video tutorial will cover mac. Once you know the basic concept it should be fairly easy to do it on windows as well. If you get stuck, shoot a query on the Wattle forum. We are happy to help :)

1. **Start File System Navigator**



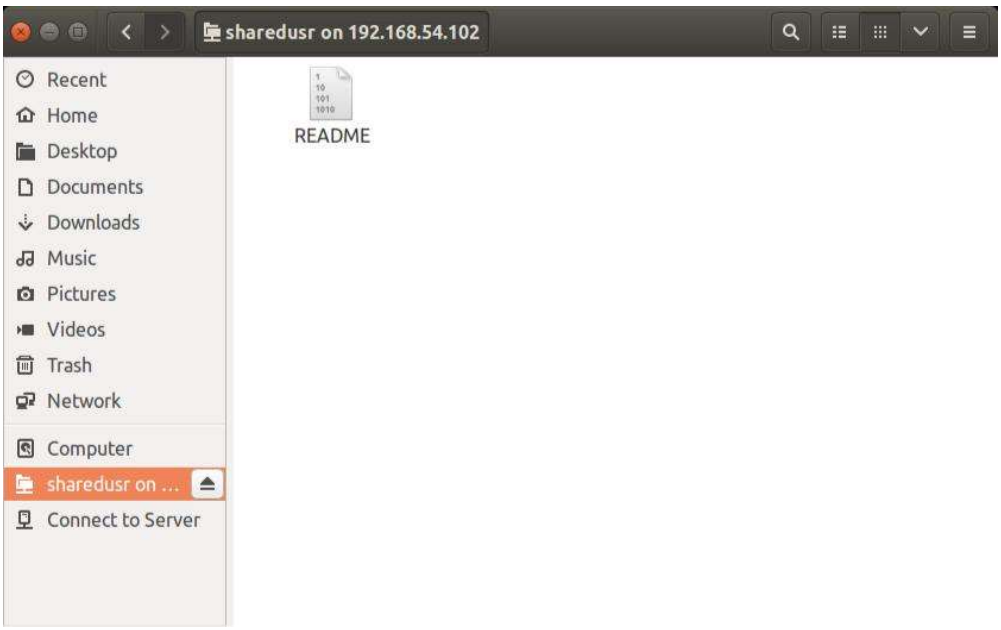
## 2. Enter the samba user name/password




## 3. Sharing a folder/file

➢ Create a file on VirtualBox **guest**, README

➢ Browse the file on Ubuntu **Host**



# TASK 2: Installing Kleopatra in Ubuntu or Analysing Textbook Figures 11-21–11-23

If you are continuing on the same guest machine. It is a good idea to login as vagrant again by typing su vagrant.

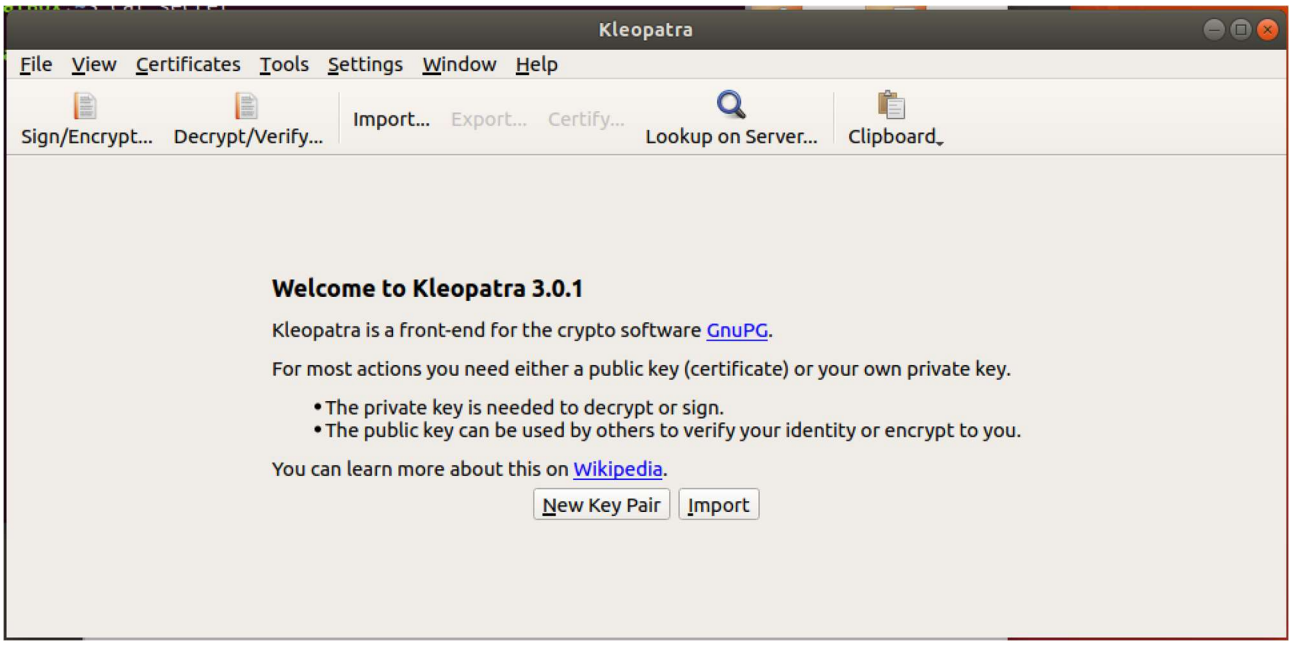
sharedusr@vagrant16:~$ sudo su vagrant

1. Certificate Manager for installing Kleopatra

   $ sudo apt-get update

   $ sudo apt-get install kleopatra

2. **Run kleopatra** (Click on ***Cancel*** if Message box pops up) and create a new Key Pair




   $ kleopatra

3. Once kleopatra is running. (Online PGP Encryption: https://youritmate.us/pgp)
   a. Create a new Key Pair.
   b. Encrypt any message using your public key
   c. Decrypt this message using your private key
4. Give it a go and if you get stuck we have shown how to do these steps in the video tutorial.

# Completing the Hands-on Activity 11C of the Textbook

Please complete the encryption lab of the textbook (i.e., the Hands-on Activity 11C, pp. 336-339). The purpose of this lab is to practice encrypting and decrypting email messages using a standard called PGP (Pretty Good Privacy) that is implemented in an open-source software Gnu Privacy Guard. You could use Kleopatra for this. Alternatively, if installing the software is not for you now, you may wish to complete the activity by analyzing the screen captures of the textbook (i.e., Figures 11-21–11-23) instead.

# Reflective Questions

a) Why do you think we need to learn sharing folders/files in Linux?
    a. How can you access your home drive from every computer in ANU?

b) What are the benefits of setting up a VPN?
    a. How is it different from sharing a folder using samba?
    b. Remember FTP protocol that we saw in previous lab? What's the difference?
    c. Have you ever used a VPN? Who needs a VPN?

c) Why do we need Kleopatra or other software for encryption key management?
    a. Kleopatra is a GUI of which program?
    b. Can you encrypt messages, emails, folders using these tools?
    c. What are the different encryption methods (hint: look at the advance settings when creating a new key)?
    d. Can you break encryption using brute force? How long will it take?

d) What are the benefits of using Kleopatra? What other options are available?

e) How could we determine what is the best option to use? What kind of criteria should we be using to compare and contrast our options? What are the pros and cons of 2-5 options out there?