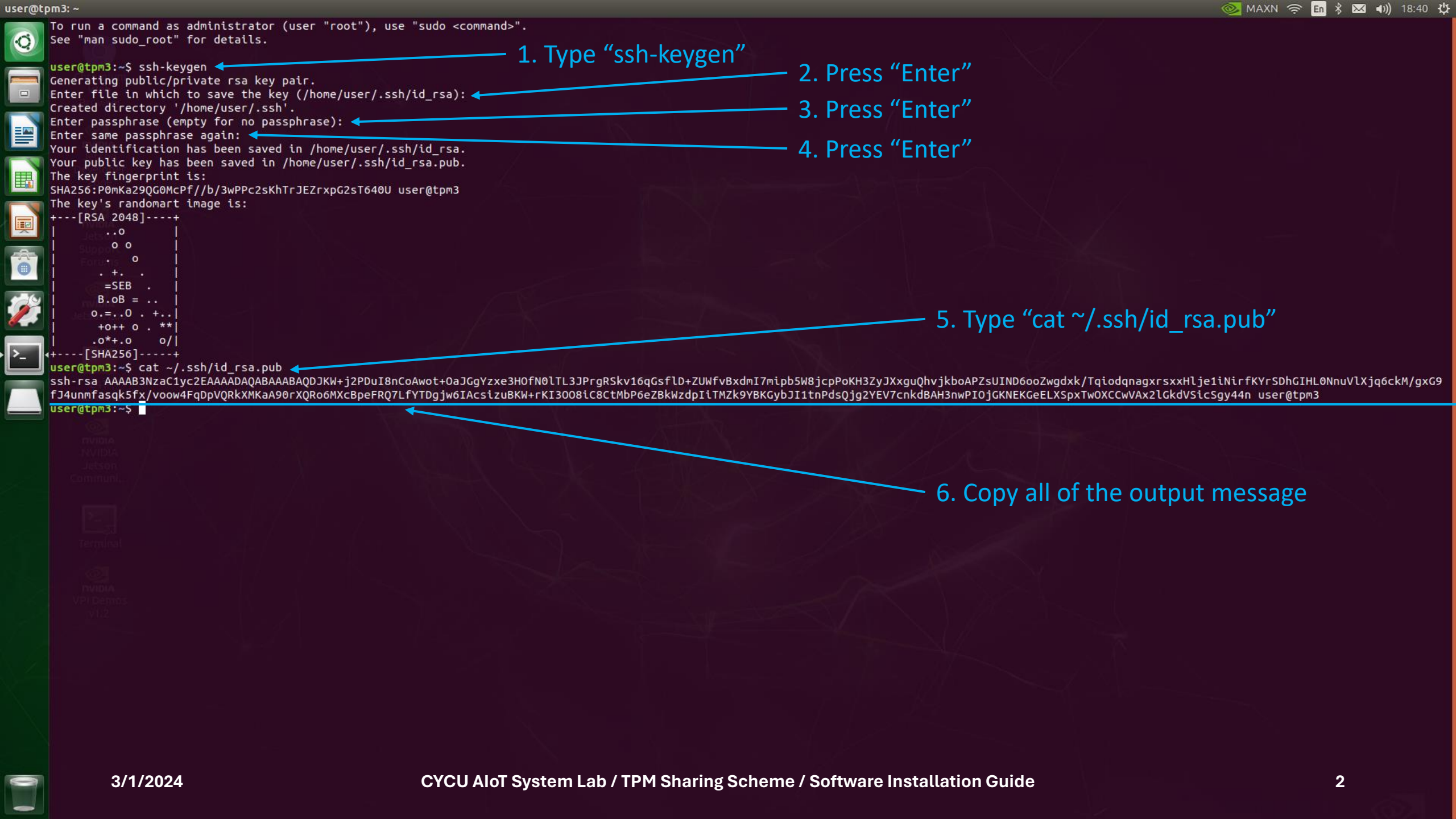
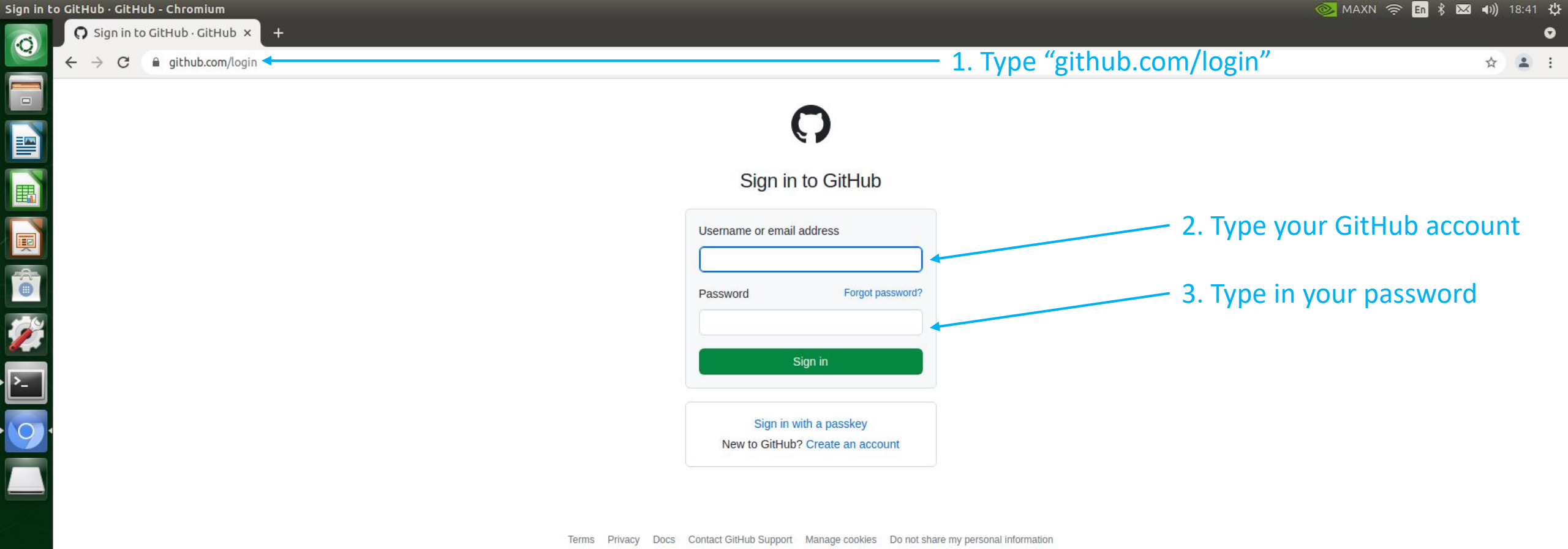
TPM Sharing Scheme Installation Guide

Common Utilities + TPM2TSS

by CYCUEE Da-Chuan Chen


user@tpm3: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
user@tpm3:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_rsa.
Your public key has been saved in /home/user/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:P0mKa29QG0McPf//b/3wPPc2sKhTrJEZrxpG2sT640U user@tpm3
The key's randomart image is:
+---[RSA 2048]----+
| ..o |
| o o |
| .   o |
| . +. . |
| =SEB . |
| B.oB = .. |
| o.=..O . +..|
| +o++ o . **|
| .o*+.o   o/|
+----[SHA256]-----+
user@tpm3:~$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJKW+j2PDuI8nCoAwot+OaJGgYzxe3HOfN0lTL3JPrgRSkv16qGsflD+ZUWfvBxdmI7mipb5W8jcpPoKH3ZyJXxguQhvjkboAPZsUIND6ooZwgdxk/Tqiodqnagxrsxx
fJ4unmfasqk5fx/voow4FqDpVQRkXMKaA90rXQRo6MXcBpeFRQ7LfYTDgjw6IAcsizuBKW+rKI3OO8iC8CtMbP6eZBkWzdpIiTMZk9YBKGybJI1tnPdsQjg2YEV7cnkdBAH3nwPIOjGKNEKGeELXSpxTwOXCCwVAx2lGkdVSicSgy44n user@tpm3
user@tpm3:~$
1. Type “ssh-keygen”
2. Press “Enter”
3. Press “Enter”
4. Press “Enter”
5. Type “cat ~/.ssh/id_rsa.pub”
6. Copy all of the output message



Note: Your account need to be a member of CYCU AIoT System Lab

CYCU-AIoT-System-Lab/TPM_Sharing_Scheme - Chromium

1. Type “github.com/CYCU-AIoT-System-Lab/TPM_Sharing_Scheme”

github.com/CYCU-AIoT-System-Lab/TPM_Sharing_Scheme

CYCU-AIoT-System-Lab / **TPM_Sharing_Scheme**

Code | Issues | Pull requests | Actions | Projects | Security | Insights | Settings

TPM_Sharing_Scheme

Private

Edit Pins | Watch 0 | Fork 0 | Starred 1

main | 1 Branch | 0 Tags | Go to file | Add file | Code

belongtothenight Add steps to Jetson Nano setup — 978d12b · 5 minutes ago — 1,013 Commits

common	Update readme.md	2 days ago
doc	Add steps to Jetson Nano setup	5 minutes ago
install_log	Pipe not just STDOUT but also STDERR to tee	last month
setup_environment	Update documentation after branches merged	2 months ago
setup_ibmtpm	Update config_RA_server.ini	2 days ago
setup_optiga	Update readme.md	last week
socket_com	Update server.c	2 months ago
.gitattributes	Initial commit	5 months ago
.gitignore	update	2 months ago
README.md	Update repo readme and move os_setup.md to doc	last month

README

TPM_Sharing_Scheme

2. Click “./common”

Refer to `./common` for overall installation script.

Repo Structure

1. common: Common utilities accross different subprojects

About

No description, website, or topics provided.

Readme
Activity
Custom properties
1 star
0 watching
0 forks

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Languages

Shell 90.1% C 7.9% CMake 1.3% PowerShell 0.7%

Suggested workflows

Based on your tech stack

C/C++ with Make — Configure

Build and test a C/C++ project using

Name	Last commit message	Last commit date
..		
config.ini	Add wget flag to prevent unwanted weird fail	3 days ago
copy_VM.ps1	Update readme information to latest	last month
download_repo.sh	Rename setup_repo to download_repo for better autocomplete experience	2 days ago
function_common.sh	Separate libssl settings to config file	5 days ago
functions.sh	Replace apt-get with apt	5 days ago
readme.md	Update readme.md	2 days ago
remove.sh	Update remove.sh	5 days ago
setup.sh	Update setup.sh	3 days ago

readme.md

Common Utilities

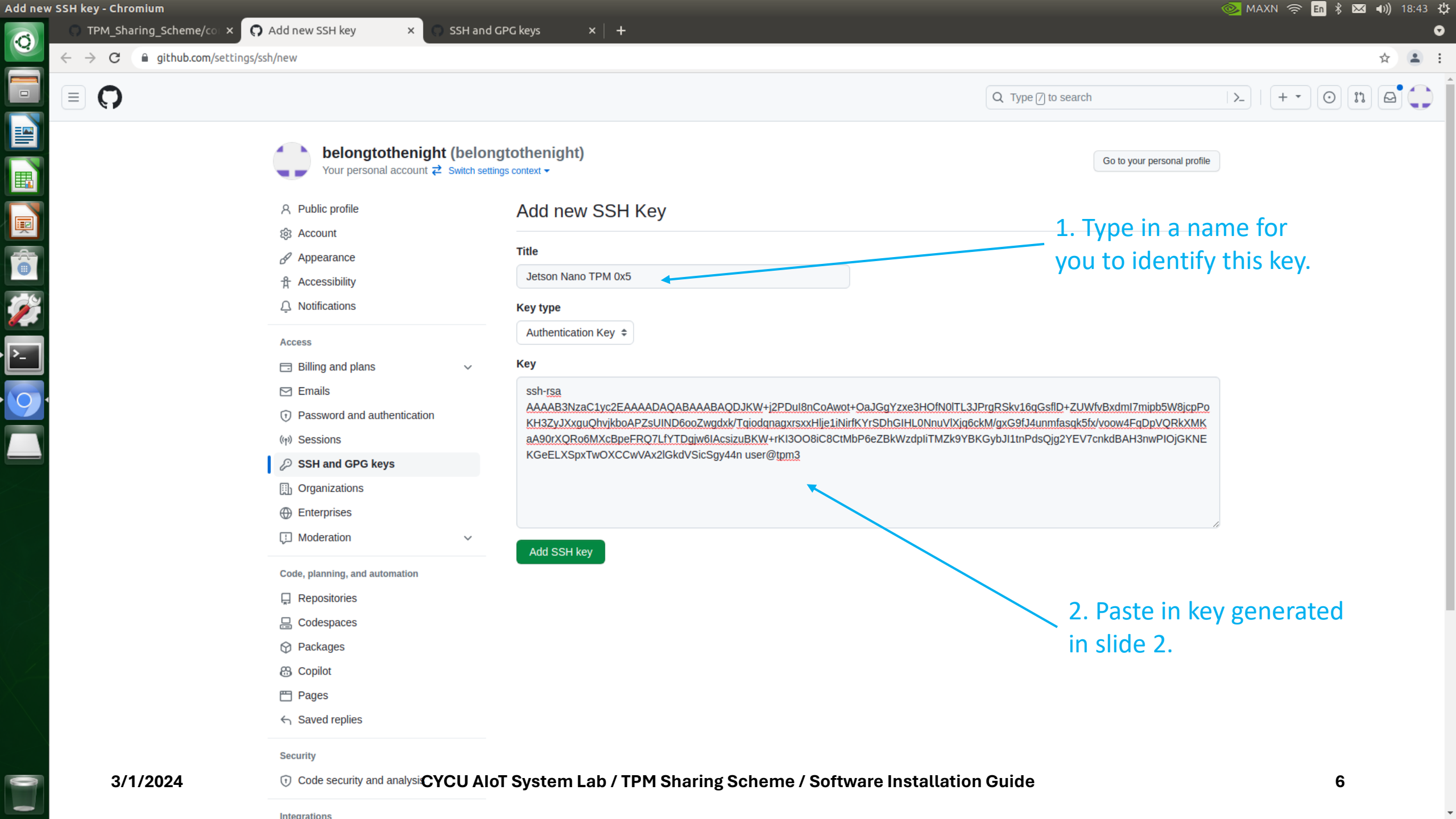
This directory holdes common utilities for this project.

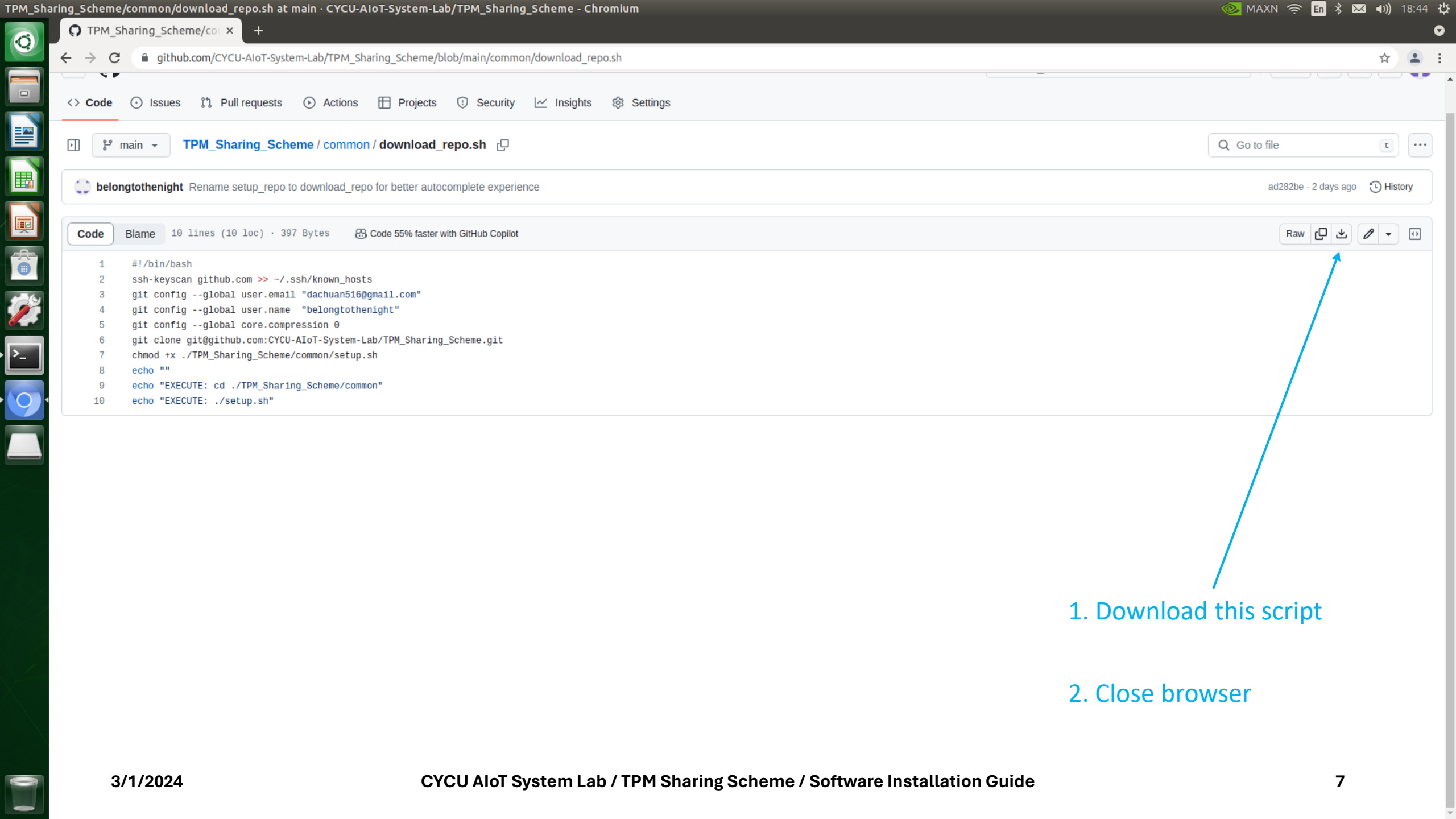
Install Steps

0. Setup OS, refer to ../doc/technology/os_setup.md.
1. In terminal, type `ssh-keygen`, keep pressing `enter` till command is finished.
2. In terminal, type `cat ~/.ssh/id_rsa.pub`, copy all of the output string.
3. In browser, go to https://github.com/settings/ssh/new, type the name of this key in title, and paste copied RSA public key in.
4. In terminal, copy the code in ./download_repo.sh into a local bash file and execute it without privilege.
5. After the script is finished, set ./config.ini item `install_platform` to your platform.
6. Execute ./setup.sh.
7. After the script is finished, and showed "Reboot", reboot.
8. Edit `/common/config.ini` to disable `setup_optiga` and enable other components you want to install, and execute `/common/setup.sh` again.

1. Open this in new tab

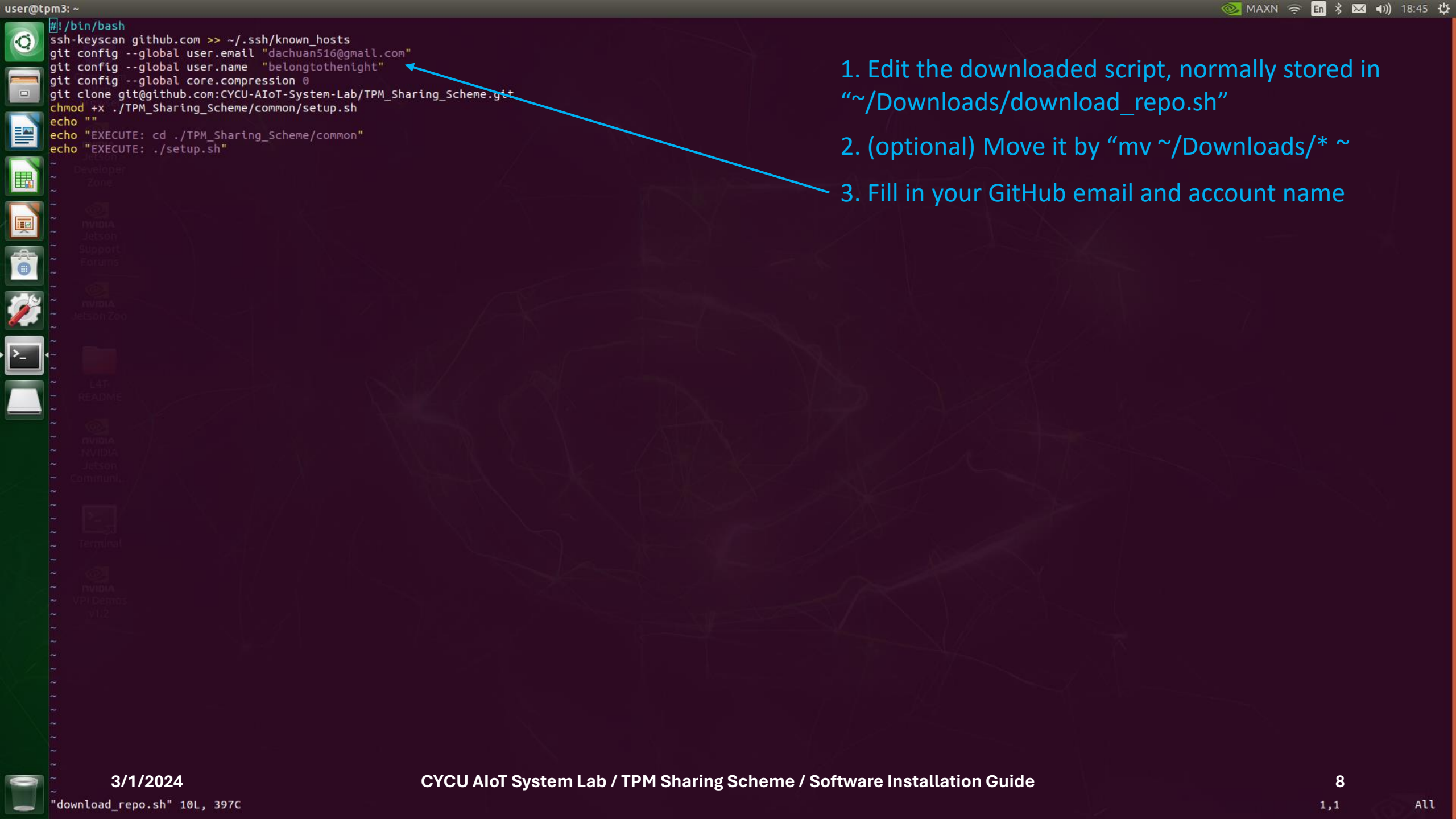
2. Open this in new tab

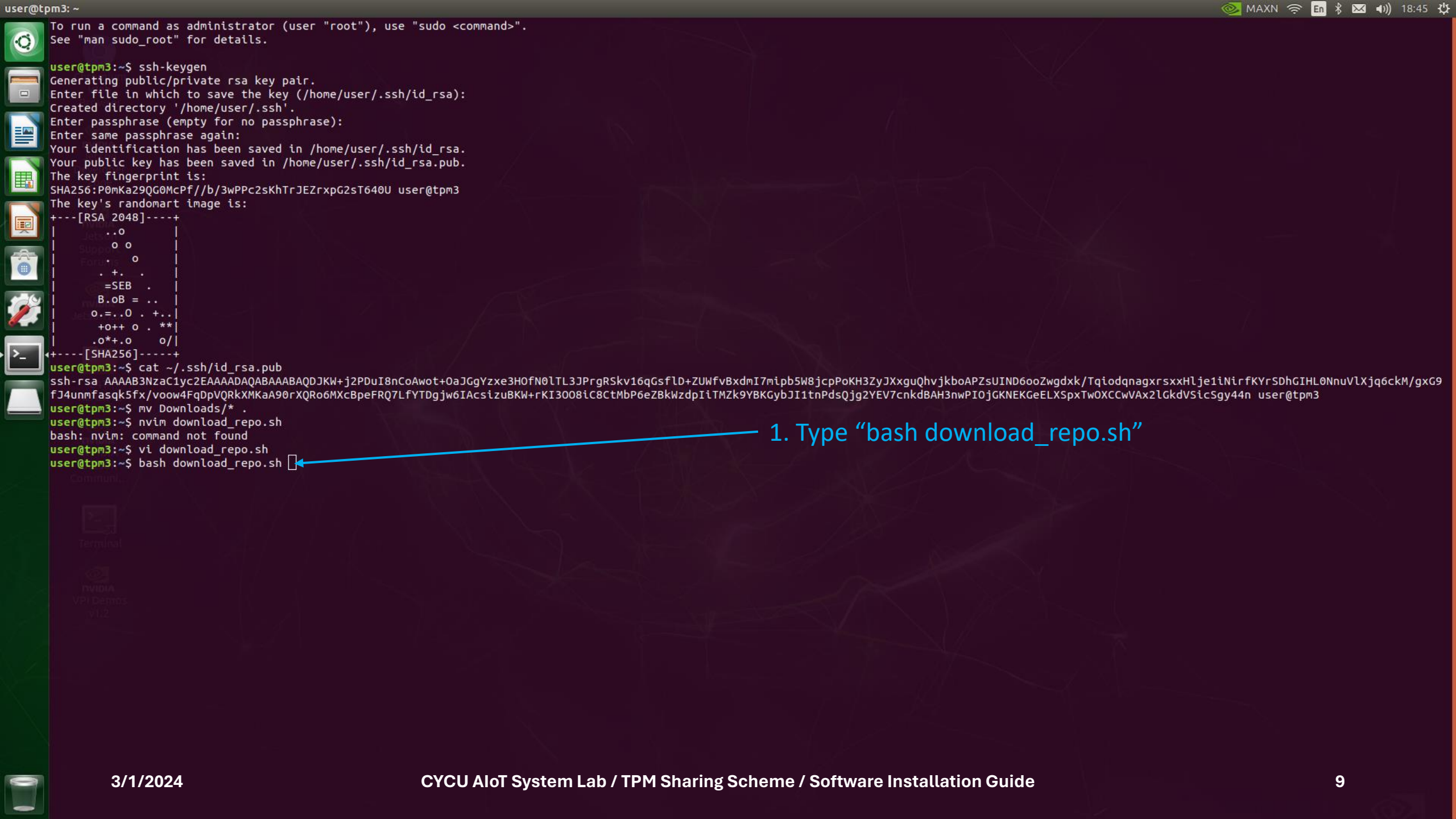

Add new SSH key - Chromium
TPM_Sharing_Scheme/co
Add new SSH key
SSH and GPG keys
github.com/settings/ssh/new
Type / to search
belongtothenight (belongtothenight)
Your personal account
Switch settings context
Go to your personal profile
Public profile
Account
Appearance
Accessibility
Notifications
Access
Billing and plans
Emails
Password and authentication
Sessions
SSH and GPG keys
Organizations
Enterprises
Moderation
Code, planning, and automation
Repositories
Codespaces
Packages
Copilot
Pages
Saved replies
Security
Code security and analysis
Integrations
Add new SSH Key
Title
Jetson Nano TPM 0x5
Key type
Authentication Key
Key
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJKW+j2PDuI8nCoAwot+OaJGgYzxe3HOfN0lTL3JPrgRSkv16qGsflD+ZUWfvBxdmI7mipb5W8jcpPo
KH3ZyJXxguQhvjkboAPZsUIND6ooZwgdxk/TqiodqnagxrsxxHlje1iNirfKYrSDhGIHL0NnuVlXjq6ckM/gxG9fJ4unmfasqk5fx/voow4FqDpVQRkXMK
aA90rXQRo6MXcBpeFRQ7LfYTDgjw6IAcsizuBKW+rKI3OO8iC8CtMbP6eZBkWzdpIiTMZk9YBKGybJI1tnPdsQjg2YEV7cnkdBAH3nwPIOjGKNE
KGeELXSpxTwOXCCwVAx2lGkdVSicSgy44n user@tpm3
Add SSH key
1. Type in a name for you to identify this key.
2. Paste in key generated in slide 2.



1. Download this script

2. Close browser


user@tpm3: ~
MAXN
En
18:45
#!/bin/bash
ssh-keyscan github.com >> ~/.ssh/known_hosts
git config --global user.email "dachuan516@gmail.com"
git config --global user.name "belongtothenight"
git config --global core.compression 0
git clone git@github.com:CYCU-AIoT-System-Lab/TPM_Sharing_Scheme.git
chmod +x ./TPM_Sharing_Scheme/common/setup.sh
echo ""
echo "EXECUTE: cd ./TPM_Sharing_Scheme/common"
echo "EXECUTE: ./setup.sh"
"download_repo.sh" 10L, 397C
1,1
All
1. Edit the downloaded script, normally stored in "~/Downloads/download_repo.sh"
2. (optional) Move it by "mv ~/Downloads/* ~
3. Fill in your GitHub email and account name


user@tpm3: ~
MAXN
En
18:45
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
user@tpm3:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_rsa.
Your public key has been saved in /home/user/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:P0mKa29QG0McPf//b/3wPPc2sKhTrJEZrxpG2sT640U user@tpm3
The key's randomart image is:
+---[RSA 2048]----+
| ..o |
| o o |
| .   o |
| . +. . |
| =SEB . |
| B.oB = .. |
| o.=..O . +..|
| +o++ o . **|
| .o*+.o   o/|
+----[SHA256]-----+
user@tpm3:~$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJKW+j2PDuI8nCoAwot+OaJGgYzxe3HOfN0lTL3JPrgRSkv16qGsflD+ZUWfvBxdmI7mipb5W8jcpPoKH3ZyJXxguQhvjkboAPZsUIND6ooZwgdxk/Tqiodqnagxrsxx
fJ4unmfasqk5fx/voow4FqDpVQRkXMKaA90rXQRo6MXcBpeFRQ7LfYTDgjw6IAcsizuBKW+rKI3OO8iC8CtMbP6eZBkWzdpIiTMZk9YBKGybJI1tnPdsQjg2YEV7cnkdBAH3nwPIOjGKNEKGeELXSpxTwOXCCwVAx2lGkdVSicSgy44n user@tpm3
user@tpm3:~$ mv Downloads/* .
user@tpm3:~$ nvim download_repo.sh
bash: nvim: command not found
user@tpm3:~$ vi download_repo.sh
user@tpm3:~$ bash download_repo.sh
1. Type “bash download_repo.sh”

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

user@tpm3:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_rsa.
Your public key has been saved in /home/user/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:P0mKa29QG0McPf//b/3wPPc2sKhTrJEZrxpG2sT640U user@tpm3
The key's randomart image is:
+---[RSA 2048]----+
|       ..o       |
|        o o      |
|       .   o     |
|      . +.  .    |
|       =SEB  .   |
|      B.oB = ..  |
|     o.=..O . +..|
|      +o++ o . **|
|     .o*+.o    o/|
+----[SHA256]-----+
user@tpm3:~$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJKW+j2PDuI8nCoAwot+OaJGgYzxe3HOfN0lTL3JPrgRSkv16qGsflD+ZUWfvBxdmI7mipb5W8jcpPoKH3ZyJXxguQhvjkboAPZsUIND6ooZwgdxk/Tqiodqnagxrsxxhlje1iNirfKYrSDhGIHL0NnuVlXjq6ckM/gxG9
fJ4unmfasqk5fx/voow4FqDpVQRkXMKaA90rXQRo6MXcBpeFRQ7LfYTDgjw6IAcsizuBKW+rKI3OO8iC8CtMbP6eZBkWzdpIiTMZk9YBKGybJI1tnPdsQjg2YEV7cnkdBAH3nwPIOjGKNEKGeELXSpxTwOXCCwVAx2lGkdVSicSgy44n user@tpm3
user@tpm3:~$ mv Downloads/* .
user@tpm3:~$ nvim download_repo.sh
bash: nvim: command not found
user@tpm3:~$ vi download_repo.sh
user@tpm3:~$ bash download_repo.sh
# github.com:22 SSH-2.0-babeld-8405f9f3
# github.com:22 SSH-2.0-babeld-8405f9f3
# github.com:22 SSH-2.0-babeld-8405f9f3
Cloning into 'TPM_Sharing_Scheme'...
Warning: Permanently added the ECDSA host key for IP address '20.27.177.113' to the list of known hosts.
remote: Enumerating objects: 4551, done.
remote: Counting objects: 100% (1009/1009), done.
remote: Compressing objects: 100% (323/323), done.
remote: Total 4551 (delta 761), reused 915 (delta 686), pack-reused 3542
Receiving objects: 100% (4551/4551), 4.80 MiB | 429.00 KiB/s, done.
Resolving deltas: 100% (3109/3109), done.

EXECUTE: cd ./TPM_Sharing_Scheme/common
EXECUTE: ./setup.sh
user@tpm3:~$
```

1. Check cloning is finished with no error

```
# This file is used to set up the environment variables for the common setup.sh script
# Param Format: <param_name> = <param_value>

[ Param - PLATFORM ]

# Installing Platform
# 1: Ubuntu 18.04 VM
# 2: Raspbian Bullseye 2022-07-01 5.1 Kernel Debian i386 VM
# 3: Raspbian Bullseye 2023-05-03 6.x Kernal Debian arm64 on Raspberry Pi 4
# 4: Ubuntu 22.04.3 on Raspberry Pi 4 B
# 5: Jetson Nano
# Default: 1
install_platform      = 3

[ Param - VERSION ]

# CMAKE version
# Default: 3.18
cmake_ver             = 3.18

# CMAKE build
# Default: 4
cmake_build           = 4

# VALGRIND version
# Default: 3.22.0
valgrind_ver          = 3.22.0

# LIBSSL version
# Default: 1.1.1w
libssl_ver            = 1.1.1w

[ Param - URL ]

# Neovim configuration url
# Default: https://raw.githubusercontent.com/belongtothenight/config-files/main/ubuntu_init.vim
nvim_config_url       = https://raw.githubusercontent.com/belongtothenight/config-files/main/ubuntu_init.vim

[ Param - PATH ]
# "${HOME}" will be interpreted and modified as the user's home directory

# Neovim configuration path
# Default: ${HOME}/.config/nvim
nvim_dir              = ${HOME}/.config/nvim

# Apport configuration path
# Default: ${HOME}/.config/apport
apport_dir            = ${HOME}/.config/apport

# CMAKE install path
# Default: /opt/cmake
cmake_dir             = /opt/cmake

# VALGRIND install path
# Default: /opt/valgrind
valgrind_dir          = /opt/valgrind
```

1. Edit configuration file in "~/TPM_Sharing_Scheme/common/config.ini"

Note: Location dependes on where you ran "download_repo.sh"

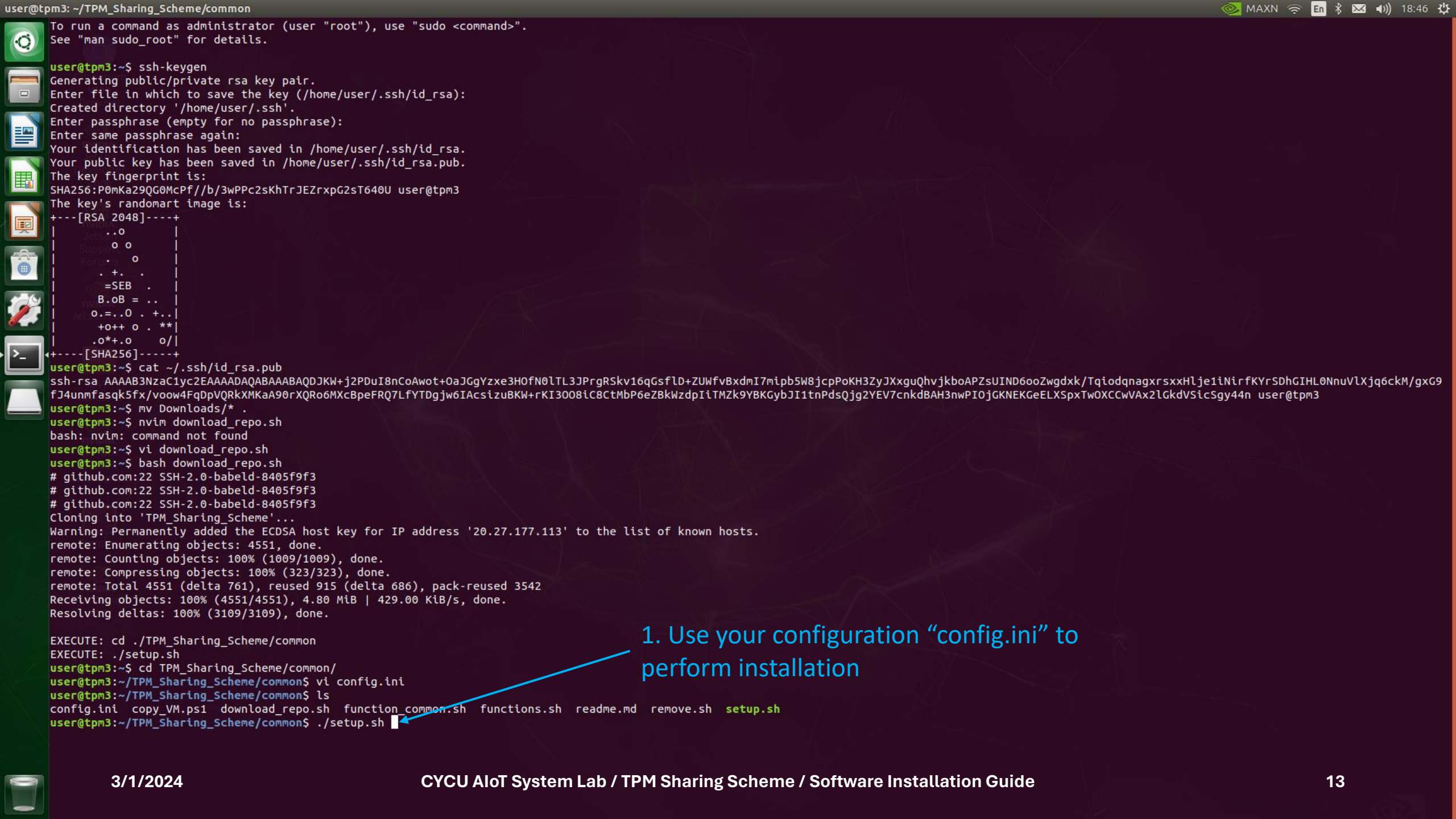
2. Adjust "install_platform" setting to your current machine

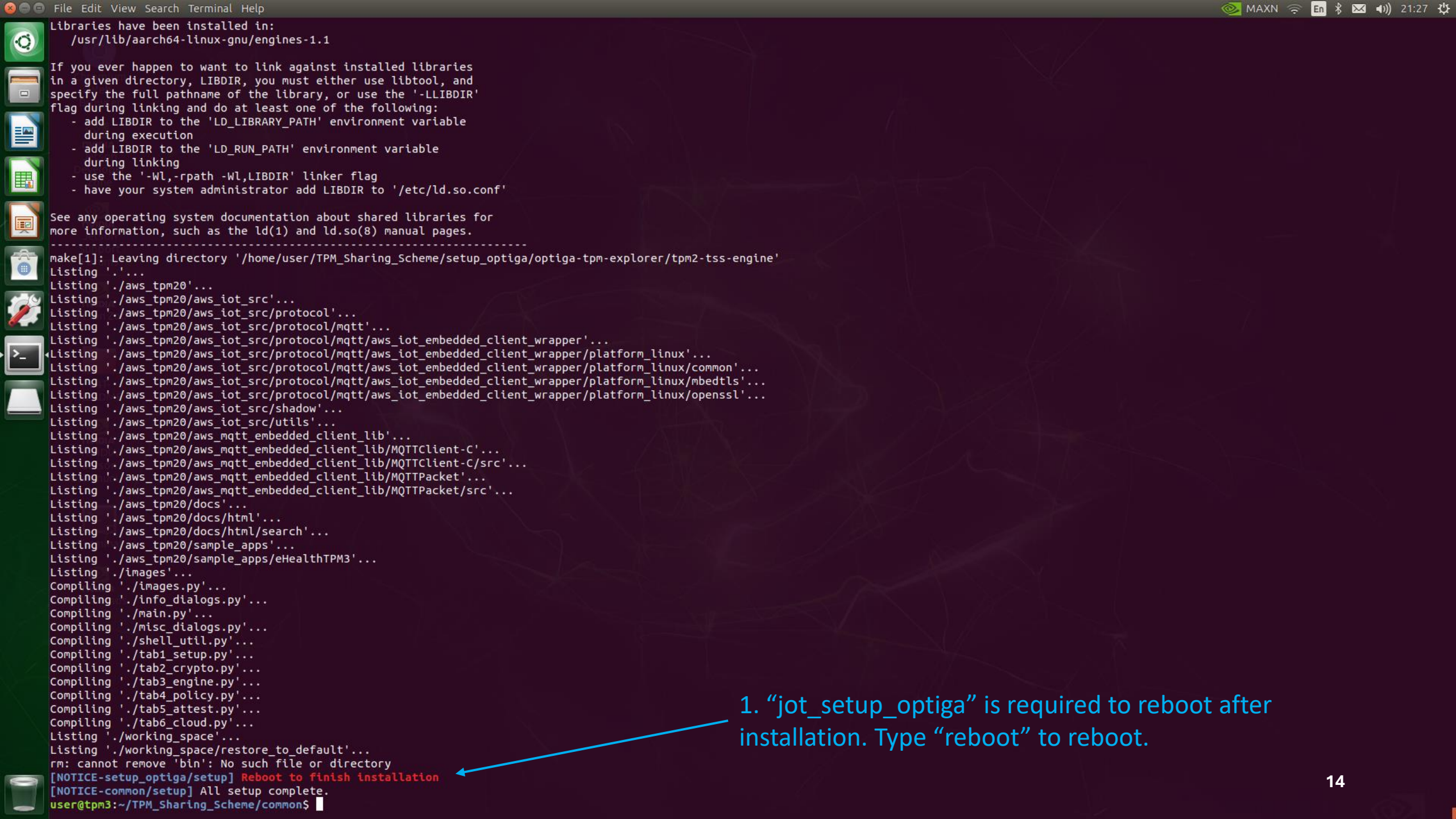
```
job_compile_req         = 1

# Configure Neovim
# Default: 1
job_config_nvim         = 1

# Update code source to latest
# Default: 1
job_update_src          = 1

# Adjust all bash script permission
# Default: 1
job_change_all_sh_mod   = 1

# Configure apport to generate core dump
# Default: 1
job_config_apport       = 0

# Enable SSH
# Default: 0
job_enable_ssh          = 1

# Enable SPI
# Default: 0
# Supported Platform: 3
job_enable_pi_spi       = 1

# Reload terminal session
# Default: 1
job_reload_term         = 1

[ Param - COMPONENT ]
# For setup.sh + remove.sh
# 1: Enable

# Launch setup.sh in setup_environment (deprecated)
# Default: 1
# Supported Platform: N/A
job_setup_environment   = 0

# Launch setup.sh in setup_ibmtpm
# 1: setup_sudo.sh
# 2: setup.sh (deprecated, bugged)
# Default: 1
# Supported Platform: 1 (4,5 under development)
job_setup_ibmtpm        = 0

# Launch setup.sh in socket_com (developing)
# Default: 1
# Supported Platform: 1 (2,3,4,5 under development)
job_socket_com          = 0

# Launch setup.sh in setup_optiga (developing)
# Only enable if you have optiga installed
# Default: 1
# Supported Platform: 3 (4 under development)
job_setup_optiga        = 1
```

1. If you do not want to have outdated libssl, cmake, valgrind to compile from source, set “job_compile_req” to not 1.

2. Make sure “job_update_src” is not 1. So that your configuration won’t be overwritten with default value.

3. Enable “job_setup_optiga”. This is recommended to ensure all TPM2TSS functionalities are installed.


user@tpm3: ~/TPM_Sharing_Scheme/common
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
user@tpm3:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_rsa.
Your public key has been saved in /home/user/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:P0mKa29QG0McPf//b/3wPPc2sKhTrJEZrxpG2sT640U user@tpm3
The key's randomart image is:
+---[RSA 2048]----+
| ..o |
| o o |
| .   o |
| . +. . |
| =SEB . |
| B.oB = .. |
| o.=..O . +..|
| +o++ o . **|
| .o*+.o   o/|
+----[SHA256]-----+
user@tpm3:~$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJKW+j2PDuI8nCoAwot+OaJGgYzxe3HOfN0lTL3JPrgRSkv16qGsflD+ZUWfvBxdmI7mipb5W8jcpPoKH3ZyJXxguQhvjkboAPZsUIND6ooZwgdxk/Tqiodqnagxrsxx
fJ4unmfasqk5fx/voow4FqDpVQRkXMKaA90rXQRo6MXcBpeFRQ7LfYTDgjw6IAcsizuBKW+rKI3OO8iC8CtMbP6eZBkWzdpIiTMZk9YBKGybJI1tnPdsQjg2YEV7cnkdBAH3nwPIOjGKNEKGeELXSpxTwOXCCwVAx2lGkdVSicSgy44n user@tpm3
user@tpm3:~$ mv Downloads/* .
user@tpm3:~$ nvim download_repo.sh
bash: nvim: command not found
user@tpm3:~$ vi download_repo.sh
user@tpm3:~$ bash download_repo.sh
github.com:22 SSH-2.0-babeld-8405f9f3
github.com:22 SSH-2.0-babeld-8405f9f3
github.com:22 SSH-2.0-babeld-8405f9f3
Cloning into 'TPM_Sharing_Scheme'...
Warning: Permanently added the ECDSA host key for IP address '20.27.177.113' to the list of known hosts.
remote: Enumerating objects: 4551, done.
remote: Counting objects: 100% (1009/1009), done.
remote: Compressing objects: 100% (323/323), done.
remote: Total 4551 (delta 761), reused 915 (delta 686), pack-reused 3542
Receiving objects: 100% (4551/4551), 4.80 MiB | 429.00 KiB/s, done.
Resolving deltas: 100% (3109/3109), done.
EXECUTE: cd ./TPM_Sharing_Scheme/common
EXECUTE: ./setup.sh
user@tpm3:~$ cd TPM_Sharing_Scheme/common/
user@tpm3:~/TPM_Sharing_Scheme/common$ vi config.ini
user@tpm3:~/TPM_Sharing_Scheme/common$ ls
config.ini copy_VM.ps1 download_repo.sh function_common.sh functions.sh readme.md remove.sh setup.sh
user@tpm3:~/TPM_Sharing_Scheme/common$ ./setup.sh
1. Use your configuration “config.ini” to perform installation



1. “jot_setup_optiga” is required to reboot after installation. Type “reboot” to reboot.

TPM Sharing Scheme Installation Guide

IBMTSS + IBMTPM + IBMACS

by CYCUEE Da-Chuan Chen


user@tpm3: ~/TPM_Sharing_Scheme/common
MAXN
21:29
user@tpm3:~$ cd TPM_Sharing_Scheme/common/
user@tpm3:~/TPM_Sharing_Scheme/common$ ls
config.ini copy_VM.ps1 download_repo.sh function_common.sh functions.sh readme.md remove.sh setup.sh
user@tpm3:~/TPM_Sharing_Scheme/common$ nvim config.ini
1. Edit “config.ini” for installing other components

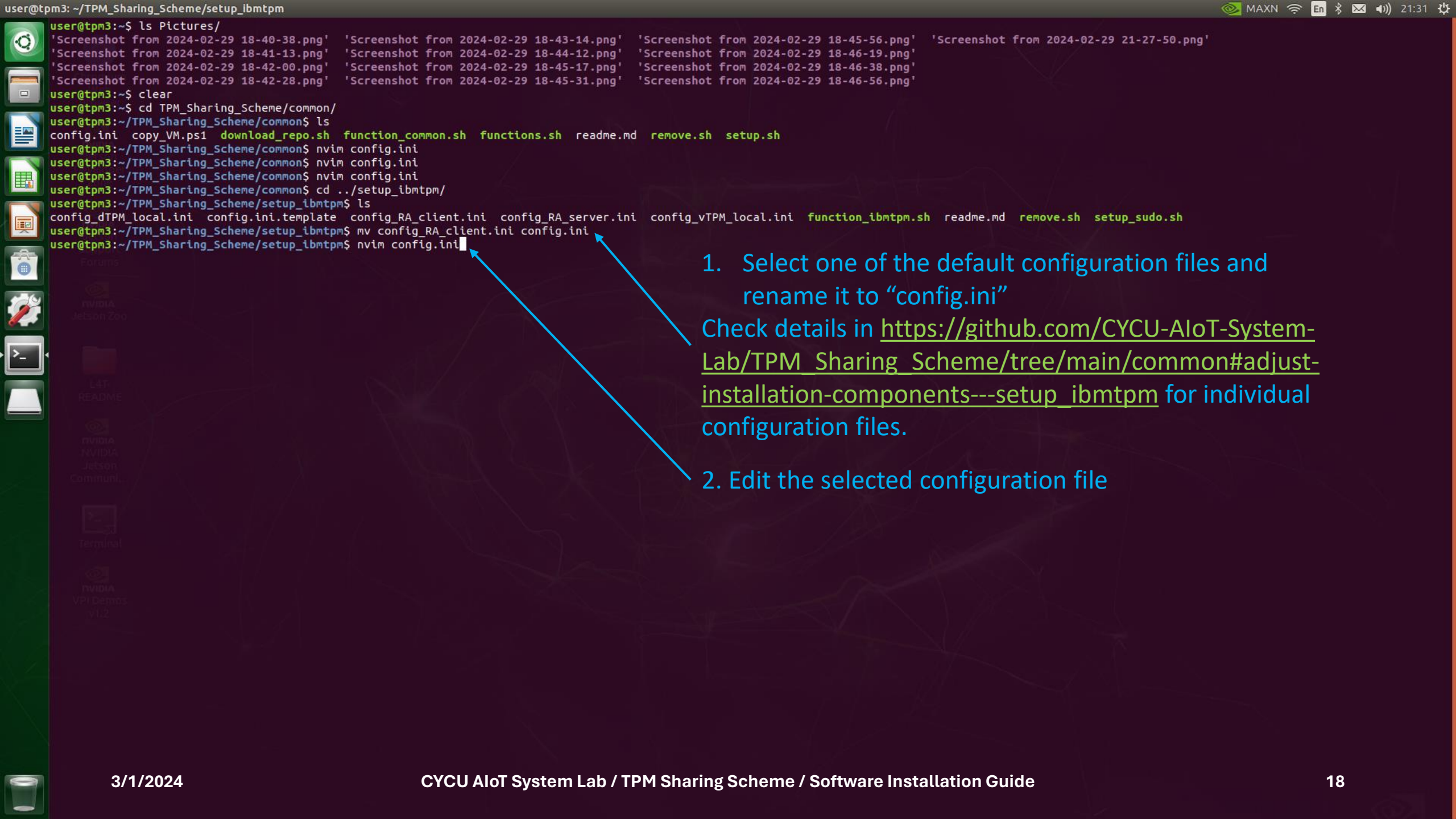
```
[ Param - JOB ]
# For setup.sh
# 1: Enable

# Install Mutual Requirement
# Default: 1
job_install_req         = 0

# Compile Mutual Requirement from Source
# Default: 1
job_compile_req         = 0

# Configure Neovim
# Default: 1
job_config_nvim         = 0

# Update code source to latest
# Default: 1
job_update_src          = 0

# Adjust all bash script permission
# Default: 1
job_change_all_sh_mod   = 1

# Configure apport to generate core dump
# Default: 1
job_config_apport       = 0

# Enable SSH
# Default: 0
job_enable_ssh          = 0

# Enable SPI
# Default: 0
# Supported Platform: 3
job_enable_pi_spi       = 0

# Reload terminal session
# Default: 1
job_reload_term         = 1

[ Param - COMPONENT ]
# For setup.sh + remove.sh
# 1: Enable

# Launch setup.sh in setup_environment (deprecated)
# Default: 1
# Supported Platform: N/A
job_setup_environment   = 0

# Launch setup.sh in setup_ibmtpm
# 1: setup_sudo.sh
# 2: setup.sh (deprecated, bugged)
# Default: 1
# Supported Platform: 1 (4,5 under development)
job_setup_ibmtpm        = 1

# Launch setup.sh in socket_com (developing)
# Default: 1
# Supported Platform: 1 (2,3,4,5 under development)
job_socket_com          = 0

# Launch setup.sh in setup_optiga (developing)
# Only enable if you have optiga installed
# Default: 1
# Supported Platform: 3 (4 under development)
job_setup_optiga        = 0
```

1. Disable all jobs performed before and only leave ones you still want to execute.

2. Set corresponding jobs to 1 to enable other components for installation.

3. Disable previously finished job.

config.ini 86,26 Bot
"config.ini" 146L, 3310C written


user@tpm3: ~/TPM_Sharing_Scheme/setup_ibmtpm
MAXN
21:31
user@tpm3:~$ ls Pictures/
'Screenshot from 2024-02-29 18-40-38.png' 'Screenshot from 2024-02-29 18-43-14.png' 'Screenshot from 2024-02-29 18-45-56.png' 'Screenshot from 2024-02-29 21-27-50.png'
'Screenshot from 2024-02-29 18-41-13.png' 'Screenshot from 2024-02-29 18-44-12.png' 'Screenshot from 2024-02-29 18-46-19.png'
'Screenshot from 2024-02-29 18-42-00.png' 'Screenshot from 2024-02-29 18-45-17.png' 'Screenshot from 2024-02-29 18-46-38.png'
'Screenshot from 2024-02-29 18-42-28.png' 'Screenshot from 2024-02-29 18-45-31.png' 'Screenshot from 2024-02-29 18-46-56.png'
user@tpm3:~$ clear
user@tpm3:~$ cd TPM_Sharing_Scheme/common/
user@tpm3:~/TPM_Sharing_Scheme/common$ ls
config.ini copy_VM.ps1 download_repo.sh function_common.sh functions.sh readme.md remove.sh setup.sh
user@tpm3:~/TPM_Sharing_Scheme/common$ nvim config.ini
user@tpm3:~/TPM_Sharing_Scheme/common$ nvim config.ini
user@tpm3:~/TPM_Sharing_Scheme/common$ nvim config.ini
user@tpm3:~/TPM_Sharing_Scheme/common$ cd ../setup_ibmtpm/
user@tpm3:~/TPM_Sharing_Scheme/setup_ibmtpm$ ls
config_dTPM_local.ini config.ini.template config_RA_client.ini config_RA_server.ini config_vTPM_local.ini function_ibmtpm.sh readme.md remove.sh setup_sudo.sh
user@tpm3:~/TPM_Sharing_Scheme/setup_ibmtpm$ mv config_RA_client.ini config.ini
user@tpm3:~/TPM_Sharing_Scheme/setup_ibmtpm$ nvim config.ini
1. Select one of the default configuration files and rename it to “config.ini”
Check details in https://github.com/CYCU-AIoT-System-Lab/TPM_Sharing_Scheme/tree/main/common#adjust-installation-components---setup_ibmtpm for individual configuration files.
2. Edit the selected configuration file

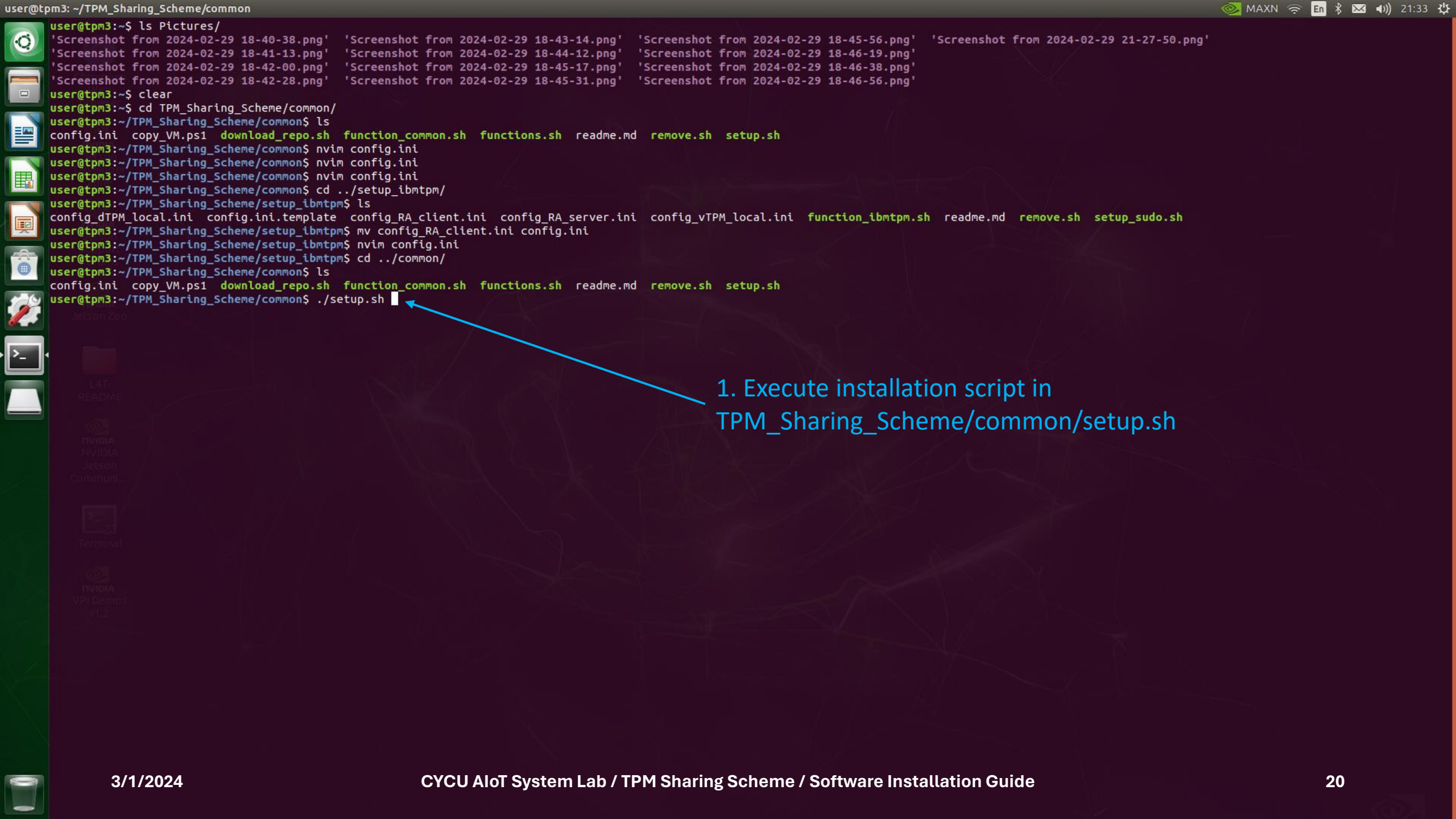
Note: Only follow this page if using “config_RA_client.ini”

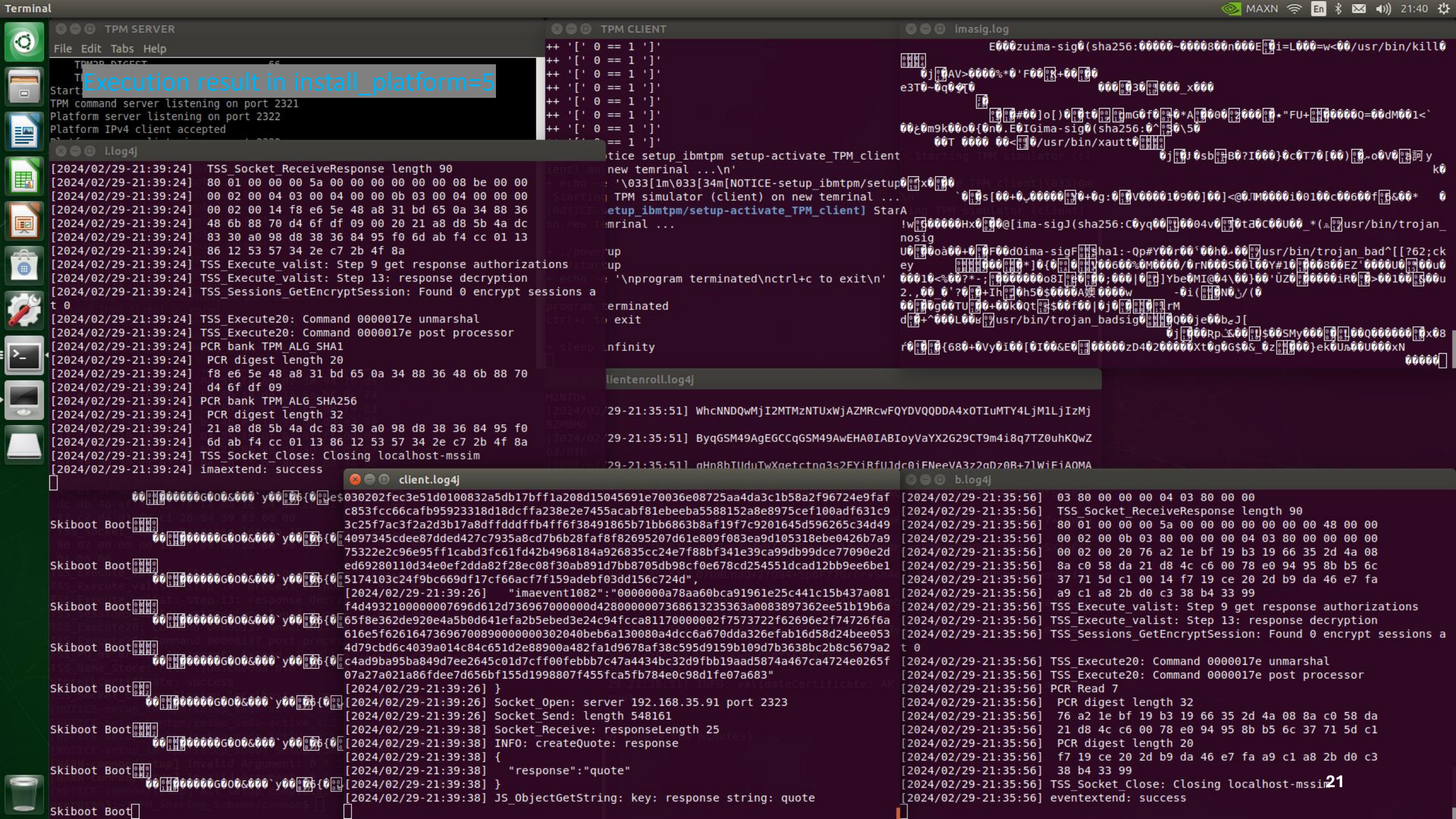
```
# Default: 1
SCmachineMode          = 2

# ACS SQL setting, edit into PHP code
# 0: Not edit setting into code
# 1: Edit setting into code
# Default: 1
force_acs_sql_setting  = 1

[Param - MySQL]

# MySQL DB username
mysql_user             = tpm2ACS

# MySQL DB password
mysql_password         = 123456

# MySQL DB name
mysql_database         = tpm2

[Param - URL]

# GitHub webpage to display
# Default: https://github.com/CYCU-AIoT-System-Lab/TPM_Sharing_Scheme/tree/main/setup_ibmtpm
repo_url               = https://github.com/CYCU-AIoT-System-Lab/TPM_Sharing_Scheme/tree/main/setup_ibmtpm

# ACS demo server ipv4 address
# Default: ipv4 address of the server machine
acs_demo_server_ip     = 192.168.35.91

# ACS demo webpage port
# Default: 8000
acs_demo_server_port   = 80

# ACS demo client ipv4 address
# Default: ipv4 address of the current machine
acs_demo_client_ip     = 192.168.35.232

# IBM TSS port
# Default: 2321
tpm_command_port       = 2321

# IBM ACS port
# Default: 2323
acs_port               = 2323

[Param - FORMAT]

# Output time format for log4j
# Default: "%Y/%m/%d-%H:%M:%S"
log4j_time_format      = %Y/%m/%d-%H:%M:%S

# Output log line number at startup for log4j
# Default: 100
log4j_line_number      = 10000
```

1. Type in server IPv4 address (“hostname –I”)

2. Type in client IPv4 address (“hostname –I”)

config.ini [+] 88,0-1 32%


user@tpm3: ~/TPM_Sharing_Scheme/common
MAXN
En
21:33
user@tpm3:~$ ls Pictures/
'Screenshot from 2024-02-29 18-40-38.png' 'Screenshot from 2024-02-29 18-43-14.png' 'Screenshot from 2024-02-29 18-45-56.png' 'Screenshot from 2024-02-29 21-27-50.png'
'Screenshot from 2024-02-29 18-41-13.png' 'Screenshot from 2024-02-29 18-44-12.png' 'Screenshot from 2024-02-29 18-46-19.png'
'Screenshot from 2024-02-29 18-42-00.png' 'Screenshot from 2024-02-29 18-45-17.png' 'Screenshot from 2024-02-29 18-46-38.png'
'Screenshot from 2024-02-29 18-42-28.png' 'Screenshot from 2024-02-29 18-45-31.png' 'Screenshot from 2024-02-29 18-46-56.png'
user@tpm3:~$ clear
user@tpm3:~$ cd TPM_Sharing_Scheme/common/
user@tpm3:~/TPM_Sharing_Scheme/common$ ls
config.ini copy_VM.ps1 download_repo.sh function_common.sh functions.sh readme.md remove.sh setup.sh
user@tpm3:~/TPM_Sharing_Scheme/common$ nvim config.ini
user@tpm3:~/TPM_Sharing_Scheme/common$ nvim config.ini
user@tpm3:~/TPM_Sharing_Scheme/common$ nvim config.ini
user@tpm3:~/TPM_Sharing_Scheme/common$ cd ../setup_ibmtpm/
user@tpm3:~/TPM_Sharing_Scheme/setup_ibmtpm$ ls
config_dTPM_local.ini config.ini.template config_RA_client.ini config_RA_server.ini config_vTPM_local.ini function_ibmtpm.sh readme.md remove.sh setup_sudo.sh
user@tpm3:~/TPM_Sharing_Scheme/setup_ibmtpm$ mv config_RA_client.ini config.ini
user@tpm3:~/TPM_Sharing_Scheme/setup_ibmtpm$ nvim config.ini
user@tpm3:~/TPM_Sharing_Scheme/setup_ibmtpm$ cd ../common/
user@tpm3:~/TPM_Sharing_Scheme/common$ ls
config.ini copy_VM.ps1 download_repo.sh function_common.sh functions.sh readme.md remove.sh setup.sh
user@tpm3:~/TPM_Sharing_Scheme/common$ ./setup.sh
1. Execute installation script in
TPM_Sharing_Scheme/common/setup.sh


Terminal
TPM SERVER
File Edit Tabs Help
Execution result in install_platform=5
TPM command server listening on port 2321
Platform server listening on port 2322
Platform IPv4 client accepted
TPM CLIENT
imasig.log
i.log4j
[2024/02/29-21:39:24] TSS_Socket_ReceiveResponse length 90
[2024/02/29-21:39:24] 80 01 00 00 00 5a 00 00 00 00 00 00 08 be 00 00
[2024/02/29-21:39:24] 00 02 00 04 03 00 04 00 00 0b 03 00 04 00 00 00
[2024/02/29-21:39:24] 00 02 00 14 f8 e6 5e 48 a8 31 bd 65 0a 34 88 36
[2024/02/29-21:39:24] 48 6b 88 70 d4 6f df 09 00 20 21 a8 d8 5b 4a dc
[2024/02/29-21:39:24] 83 30 a0 98 d8 38 36 84 95 f0 6d ab f4 cc 01 13
[2024/02/29-21:39:24] 86 12 53 57 34 2e c7 2b 4f 8a
[2024/02/29-21:39:24] TSS_Execute_valist: Step 9 get response authorizations
[2024/02/29-21:39:24] TSS_Execute_valist: Step 13: response decryption
[2024/02/29-21:39:24] TSS_Sessions_GetEncryptSession: Found 0 encrypt sessions a
t 0
[2024/02/29-21:39:24] TSS_Execute20: Command 0000017e unmarshal
[2024/02/29-21:39:24] TSS_Execute20: Command 0000017e post processor
[2024/02/29-21:39:24] PCR bank TPM_ALG_SHA1
[2024/02/29-21:39:24] PCR digest length 20
[2024/02/29-21:39:24] f8 e6 5e 48 a8 31 bd 65 0a 34 88 36 48 6b 88 70
[2024/02/29-21:39:24] d4 6f df 09
[2024/02/29-21:39:24] PCR bank TPM_ALG_SHA256
[2024/02/29-21:39:24] PCR digest length 32
[2024/02/29-21:39:24] 21 a8 d8 5b 4a dc 83 30 a0 98 d8 38 36 84 95 f0
[2024/02/29-21:39:24] 6d ab f4 cc 01 13 86 12 53 57 34 2e c7 2b 4f 8a
[2024/02/29-21:39:24] TSS_Socket_Close: Closing localhost-mssim
[2024/02/29-21:39:24] imaextend: success
client.log4j
Skiboot Boot
[2024/02/29-21:39:26] "imaevent1082":"0000000a78aa60bca91961e25c441c15b437a081
[2024/02/29-21:39:26] }
[2024/02/29-21:39:26] Socket_Open: server 192.168.35.91 port 2323
[2024/02/29-21:39:26] Socket_Send: length 548161
[2024/02/29-21:39:38] Socket_Receive: responseLength 25
[2024/02/29-21:39:38] INFO: createQuote: response
[2024/02/29-21:39:38] {
[2024/02/29-21:39:38] "response":"quote"
[2024/02/29-21:39:38] }
[2024/02/29-21:39:38] JS_ObjectGetString: key: response string: quote
b.log4j
[2024/02/29-21:35:56] 03 80 00 00 00 04 03 80 00 00
[2024/02/29-21:35:56] TSS_Socket_ReceiveResponse length 90
[2024/02/29-21:35:56] 80 01 00 00 00 5a 00 00 00 00 00 00 00 48 00 00
[2024/02/29-21:35:56] 00 02 00 0b 03 80 00 00 00 04 03 80 00 00 00 00
[2024/02/29-21:35:56] 00 02 00 20 76 a2 1e bf 19 b3 19 66 35 2d 4a 08
[2024/02/29-21:35:56] 8a c0 58 da 21 d8 4c c6 00 78 e0 94 95 8b b5 6c
[2024/02/29-21:35:56] 37 71 5d c1 00 14 f7 19 ce 20 2d b9 da 46 e7 fa
[2024/02/29-21:35:56] a9 c1 a8 2b d0 c3 38 b4 33 99
[2024/02/29-21:35:56] TSS_Execute_valist: Step 9 get response authorizations
[2024/02/29-21:35:56] TSS_Execute_valist: Step 13: response decryption
[2024/02/29-21:35:56] TSS_Sessions_GetEncryptSession: Found 0 encrypt sessions a
t 0
[2024/02/29-21:35:56] TSS_Execute20: Command 0000017e unmarshal
[2024/02/29-21:35:56] TSS_Execute20: Command 0000017e post processor
[2024/02/29-21:35:56] PCR Read 7
[2024/02/29-21:35:56] PCR digest length 32
[2024/02/29-21:35:56] 76 a2 1e bf 19 b3 19 66 35 2d 4a 08 8a c0 58 da
[2024/02/29-21:35:56] 21 d8 4c c6 00 78 e0 94 95 8b b5 6c 37 71 5d c1
[2024/02/29-21:35:56] PCR digest length 20
[2024/02/29-21:35:56] f7 19 ce 20 2d b9 da 46 e7 fa a9 c1 a8 2b d0 c3
[2024/02/29-21:35:56] 38 b4 33 99
[2024/02/29-21:35:56] TSS_Socket_Close: Closing localhost-mssim
[2024/02/29-21:35:56] eventextend: success
21

```
TSS_Execute_valist: Step 6 calculate HMACs
TSS_HmacSession_SetHMAC: Step 6 session 40000009
TSS_Execute_valist: Step 7 set command authorizations
TSS_Execute_valist: Step 8: process the command
TSS_AuthExecute: Executing TPM2_NV_Write
TSS_Socket_SendCommand: TPM2_NV_Write
 TSS_Socket_SendCommand length 476
 80 02 00 00 01 dc 00 00 01 37 40 00 00 0c 01 c0
 00 0a 00 00 00 09 40 00 00 09 00 00 00 00 00 01
 b9 30 82 01 b5 30 82 01 5b a0 03 02 01 02 02 15
 00 e2 70 d5 a7 44 8c b6 cf 7d 46 a5 07 af de 7e
 d2 a5 3c 2e 3b 30 0a 06 08 2a 86 48 ce 3d 04 03
 02 30 4e 31 0b 30 09 06 03 55 04 06 13 02 55 53
 31 0b 30 09 06 03 55 04 08 0c 02 4e 59 31 11 30
 0f 06 03 55 04 07 0c 08 59 6f 72 6b 74 6f 77 6e
 31 0c 30 0a 06 03 55 04 0a 0c 03 49 42 4d 31 11
 30 0f 06 03 55 04 03 0c 08 45 4b 20 45 43 20 43
 41 30 1e 17 0d 32 34 30 32 32 39 31 33 33 35 34
 39 5a 17 0d 34 34 30 32 32 36 31 33 33 35 34 39
 5a 30 52 31 0b 30 09 06 03 55 04 06 13 02 55 53
 31 0b 30 09 06 03 55 04 08 0c 02 4e 59 31 11 30
 0f 06 03 55 04 07 0c 08 59 6f 72 6b 74 6f 77 6e
 31 0c 30 0a 06 03 55 04 0a 0c 03 49 42 4d 31 15
 30 13 06 03 55 04 03 0c 0c 49 42 4d 27 73 20 53
 57 20 54 50 4d 30 59 30 13 06 07 2a 86 48 ce 3d
 02 01 06 08 2a 86 48 ce 3d 03 01 07 03 42 00 04
 f6 3d 7d 93 4b a0 5b 8d 3f fe 68 07 38 94 7b d5
 82 e2 fa 60 10 4d d9 55 8b 18 de 13 5a bf 0c 74
 f5 40 17 26 dd f4 df c1 56 b4 a0 1d c6 8e f9 c3
 6d 2d 8f 33 c0 ec 89 b2 4b e3 1a 98 0b 0d e3 88
 a3 12 30 10 30 0e 06 03 55 1d 0f 01 01 ff 04 04
 03 02 03 08 30 0a 06 08 2a 86 48 ce 3d 04 03 02
 03 48 00 30 45 02 20 0a 20 31 bb 80 ef bd 4a bc
 39 0c c0 87 e2 18 d2 29 07 e7 79 2e 59 4f 95 cc
 4f d1 52 0d c3 11 f3 02 21 00 f5 26 86 e3 a0 41
 dc 4b 46 ef e7 e3 78 fa da 1e 84 52 28 e1 85 bf
 12 c2 d4 d1 fd c1 26 94 39 83 00 00
 TSS_Socket_ReceiveResponse length 19
 80 02 00 00 00 13 00 00 00 00 00 00 00 00 00 00
 01 00 00
TSS_Execute_valist: Step 9 get response authorizations
TSS_Execute_valist: Step 10: process response authorization 40000009
TSS_Execute_valist: Step 13: response decryption
TSS_Sessions_GetEncryptSession: Found 0 encrypt sessions at 0
TSS_Execute20: Command 00000137 unmarshal
TSS_Execute20: Command 00000137 post processor
TSS_PO_NV_Write, Increment, Extend, SetBits:
TSS_Name_Store: File ./h01c0000a.bin
storeEkCertificate: success
TSS_Socket_Close: Closing localhost-mssim
[NOTICE-setup_ibmtpm/setup_sudo-active_ACS_Demo_Client] Activating ACS Demo on remote machine ...
[NOTICE-setup_ibmtpm/setup_sudo-active_ACS_Demo_verify] Checking TPM2BIOS.LOG ...
[NOTICE-setup_ibmtpm/setup_sudo-active_ACS_Demo_verify] Checking IMASIG.LOG (it can take a few minutes) ...
[NOTICE-setup_ibmtpm/setup_sudo] Setup complete
[WARN-common/setup] Invalid Argument: 0 ! Skipping setup_socket_com...
[WARN-common/setup] Invalid Argument: 0 ! Skipping setup_optiga...
[NOTICE-common/setup] All setup complete.
user@tpm3:~/TPM_Sharing_Scheme/common$
```

"setup_ibmtpm" execution complete.