



# Security in IoT Ecosystem

## Module 7

### Smart Socket Pentest Part I

Prof.: Joaquín Recas

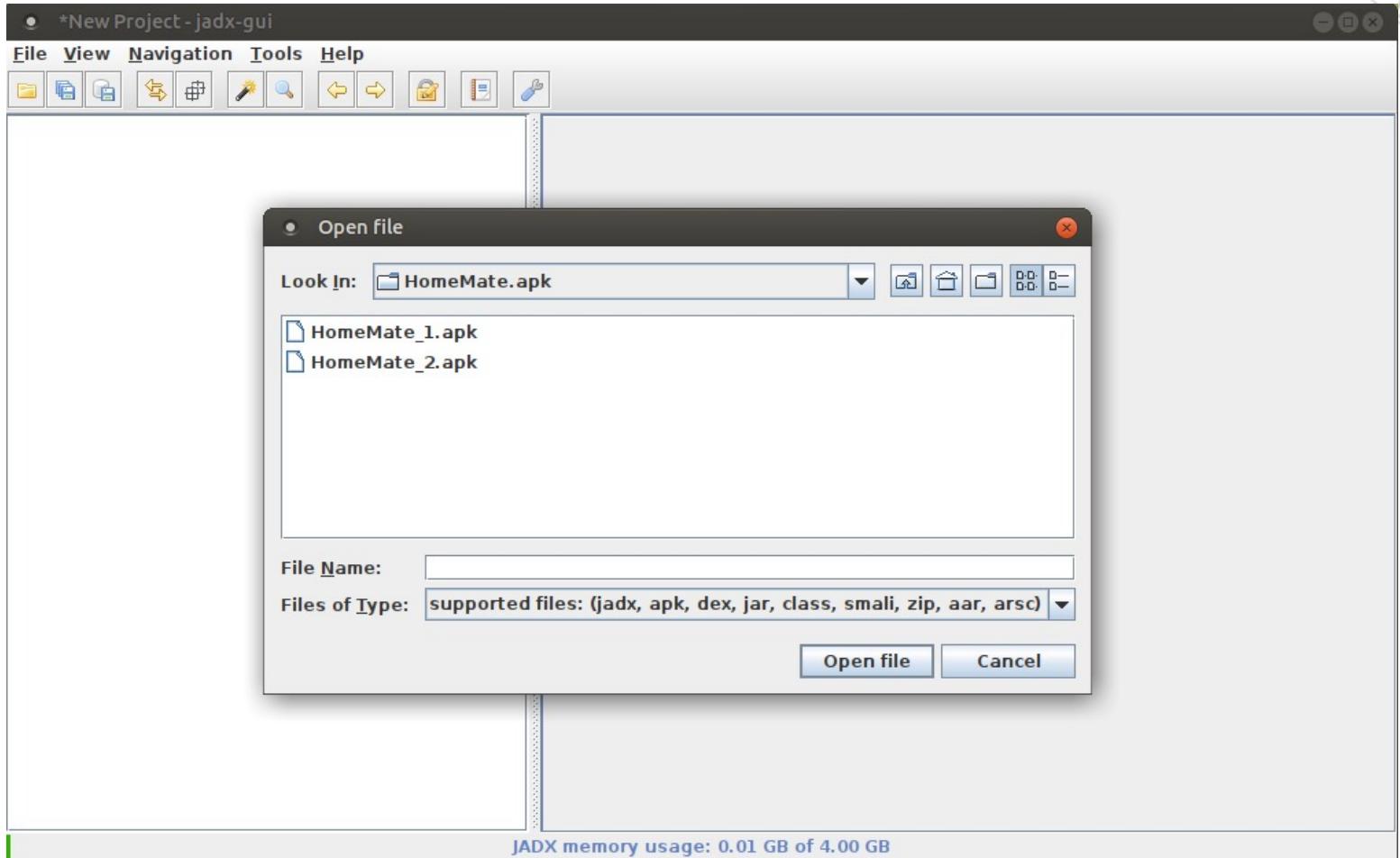
# Initial Setup: Linux VM

## 1. Prepare the Linux Virtual Machine

- Wireshark (already installed)
- JADX Dex to Java decompiler:
  - [github project homepage](#)
  - Download releases from [github](#)
- Binary Ninja homepage [link](#)
  - Demo version [link](#)



# JADX Dex to Java decompiler





# Binary Ninja homepage

A screenshot of the Binary Ninja application window. The title bar says "Binary Ninja". The menu bar includes File, Edit, View, Tools, Window, and Help. A toolbar below the menu has "New Tab" and other icons. The main content area features the Binary Ninja logo (a red circle with a white mask-like face) and the text "BINARNINJA". Below this is a message: "Thank you for trying Binary Ninja. This demo version supports disassembly of x86, x64 and ARMv7 binaries for a variety of platforms. Additional architectures are available in the full release. See the [list of features](#) for more information." It also notes a 25-minute session limit and links to FAQ and Slack. A "Purchase Binary Ninja to unlock all features." button is present. At the bottom, there's a "Recently opened files:" section showing a single file path, and a "File" menu with options like Open..., Options..., New, and Triage...

Binary Ninja homepage

File Edit View Tools Window Help

New Tab

BINARNINJA

Thank you for trying Binary Ninja.

This demo version supports disassembly of x86, x64 and ARMv7 binaries for a variety of platforms. Additional architectures are available in the full release. See the [list of features](#) for more information.

Note that the demo is limited to 25 minutes of analysis before the session ends.

Questions about Binary Ninja? First check the [frequently asked questions](#) page. You can also join our [Slack](#) to interact with us and our community. See the [user documentation](#) to learn more about how to use Binary Ninja.

**Purchase Binary Ninja to unlock all features.** Product comparisons are available on the purchase page.

Recently opened files:

1: /media/sf\_PX-OKLOK/PY-Bulb/Hao Deng\_v1.2.8\_apkpure.com.apk\_FILES/lib/armeabi/libTelinkCrypto.so

Open... Open an existing file.

Options... Open an existing file with custom options.

New Create a new binary file.

Triage... Open file(s) for quick analysis in the Triage Summary view.

DEMO VERSION Version 1.2.1921 demo, Build ID 4ca675f1

Copyright © 2015-2019 Vector 35 Inc

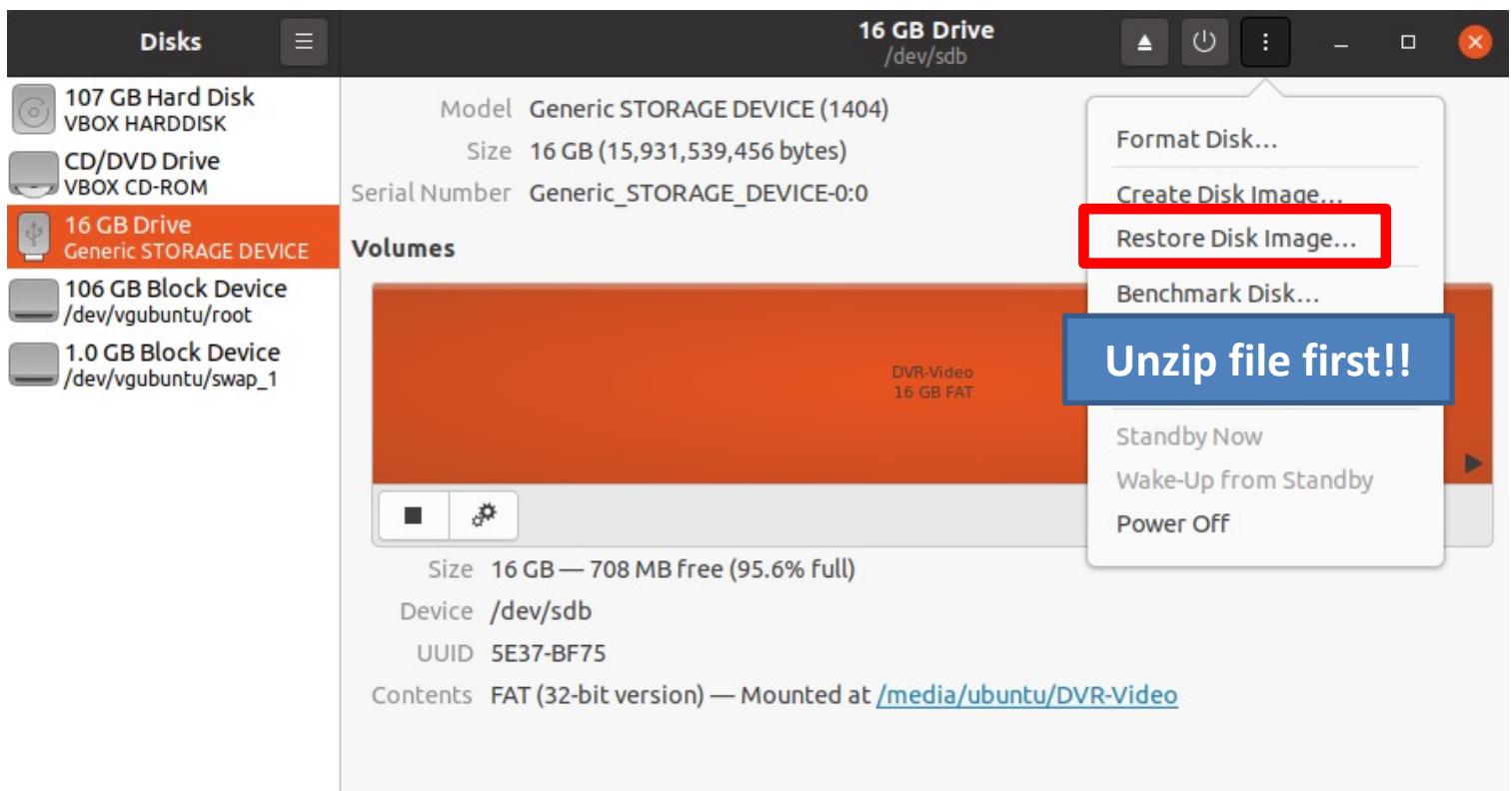
# Initial Setup: raspberry Pi 4

## 2. Prepare the Raspberry Pi:

- Download Raspi-IoT-DA.`img.zip` image
  - Link available in your email
- Flash the image into the SD cart using:
  - Option 1: Use the Linux Virtual Machine or
  - Option 2: Raspberry Pi Imager: [link](#) or
  - Option 3: balenaEtcher: [link](#)

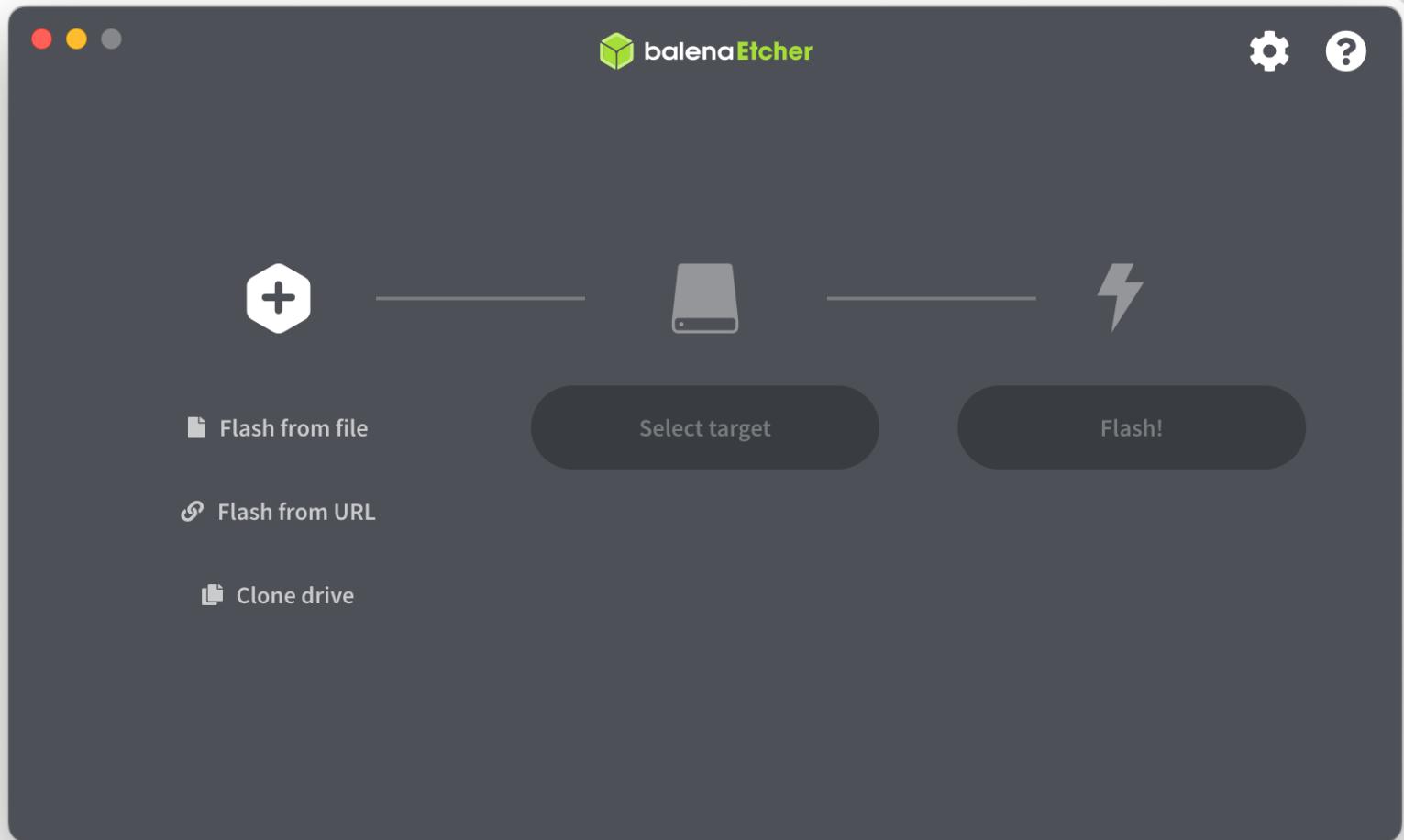


# Flash the image: Virtual machine



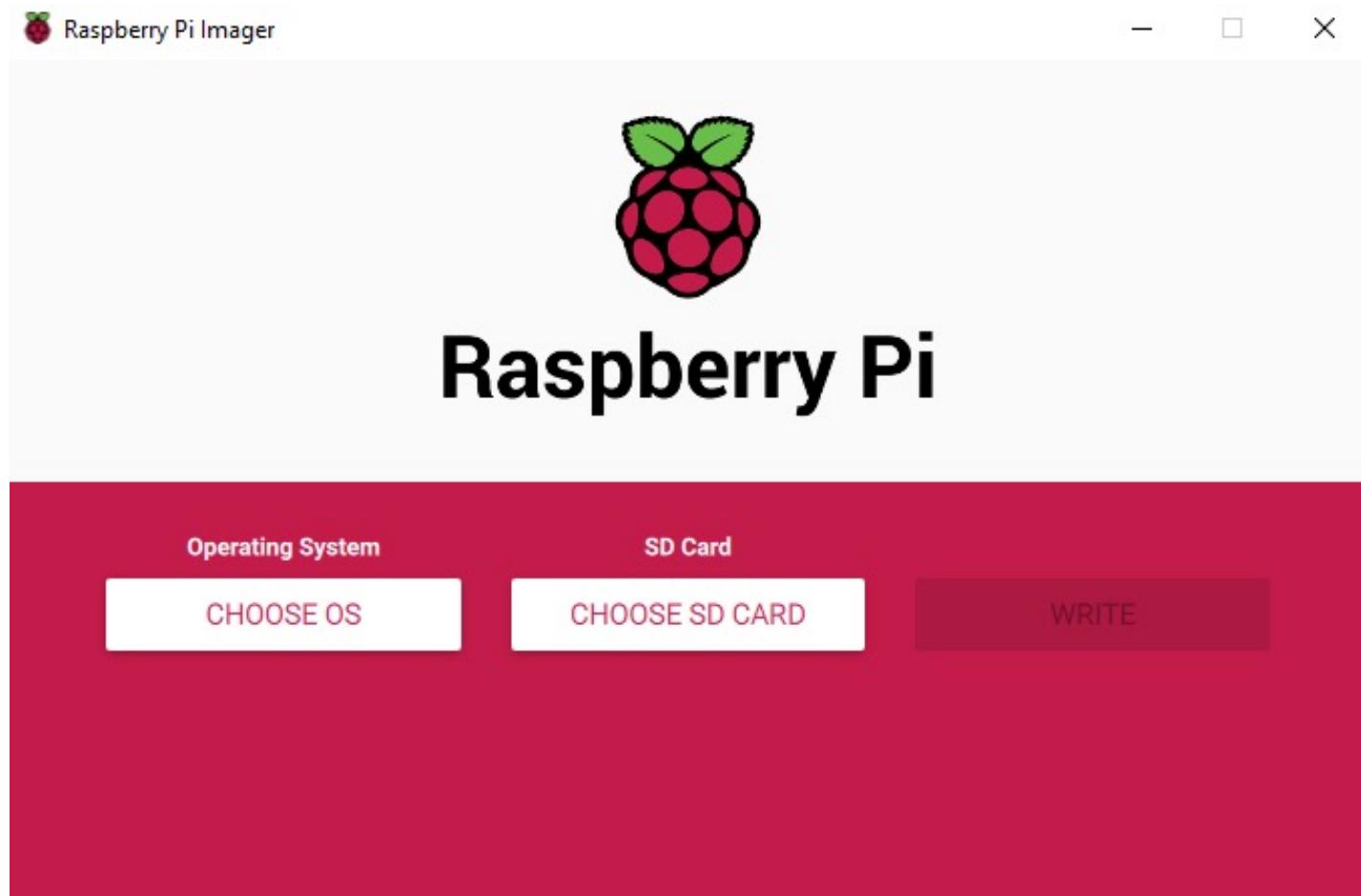


# Flash the image: balenaEtcher





# Flash the image: Raspberry Pi Imager



# Initial Setup: raspberry Pi 4

## 2. Prepare the Raspberry Pi:

- Download Raspi-IoT-DA.img.zip image
- Flash the image into the SD cart using:
- Plug the SD card in the Raspberry Pi 4
  - Connect the ethernet cable (**access to the Internet**)
  - Optional: connect a mouse, keyboard, HDMI monitor
  - Connect the power supply and wait for 3min
    - User 'iot', password 'IoT-DA'
  - Obtain IP address:
    - ping -c 4 raspy-iot-da
    - Access your router: <http://192.168.1.1>
    - nmap -sn 192.168.1.0/24

# Obtain Raspberry Pi IP address



```
iot@raspy-iot-da: ~
vpn-216-178:iot-da.github.io jrecas$ ping -c 4 raspy-iot-da
PING raspy-iot-da.home (192.168.1.211): 56 data bytes
64 bytes from 192.168.1.211: icmp_seq=0 ttl=64 time=0.642 ms
64 bytes from 192.168.1.211: icmp_seq=1 ttl=64 time=0.668 ms
64 bytes from 192.168.1.211: icmp_seq=2 ttl=64 time=0.664 ms
64 bytes from 192.168.1.211: icmp_seq=3 ttl=64 time=0.808 ms

--- raspy-iot-da.home ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.642/0.696/0.808/0.066 ms
vpn-216-178:iot-da.github.io jrecas$
```

# Obtain Raspberry Pi IP address



```
$ sudo apt-get install nmap
```

```
ubuntu@ubuntu2004:~$ nmap -sn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-05 07:55 EDT
Nmap scan report for liveboxplus (192.168.1.1)
Host is up (0.00012s latency).
Nmap scan report for 192.168.1.2
Host is up (0.0039s latency).
Nmap scan report for JRecas-MacBook.home (192.168.1.76)
Host is up (0.0061s latency).
Nmap scan report for raspy-syl.home (192.168.1.211)
Host is up (0.027s latency).
Nmap done: 256 IP addresses (9 hosts up) scanned in 2.33 seconds
ubuntu@ubuntu2004:~$
```

# Initial Setup: raspberry Pi 4

## 2. Prepare the Raspberry Pi:

- Download Raspi-IoT-DA.img.zip image
- Flash the image into the SD cart using:
- Plug the SD card in the Raspberry Pi 4
- Log in:
  - Option 1: Mouse, keyboard, HDMI monitor
  - Option 2: remote ssh access
  - Option 3: use VNC viewer



# VNC Server

```
iot@raspy-iot-da: ~
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
JRecas-MacBook:~ jrecas$ clear
JRecas-MacBook:~ jrecas$ ssh iot@raspy-iot-da
iot@raspy-iot-da's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-1059-raspi aarch64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

154 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

*** System restart required ***
Last login: Thu May  5 14:08:07 2022 from 192.168.1.76
iot@raspy-iot-da:~$ vncserver

New 'X' desktop is raspy-iot-da:1

Starting applications specified in /home/iot/.vnc/xstartup
Log file is /home/iot/.vnc/raspy-iot-da:1.log
iot@raspy-iot-da:~$
```

```
$ vncserver -kill :1
```



# VNC Viewer

A screenshot of the VNC Viewer application window. At the top, there are three colored circles (red, yellow, green) and the title "VNC Viewer". Below that is the "vnc connect by RealVNC" logo and a search bar containing the placeholder "Enter a VNC Server address or search". To the right of the search bar is a user profile icon with a checkmark and the name "J Recas". On the left side of the main area, there are two items: "Address book" with a grid icon and "J's Team (Home)" with a people icon. On the right side, there is a thumbnail preview of a green polygonal desktop screen with a small white window in the center. Below this preview is the text "IoT-DA".

VNC Viewer

vnc connect by RealVNC Enter a VNC Server address or search J Recas

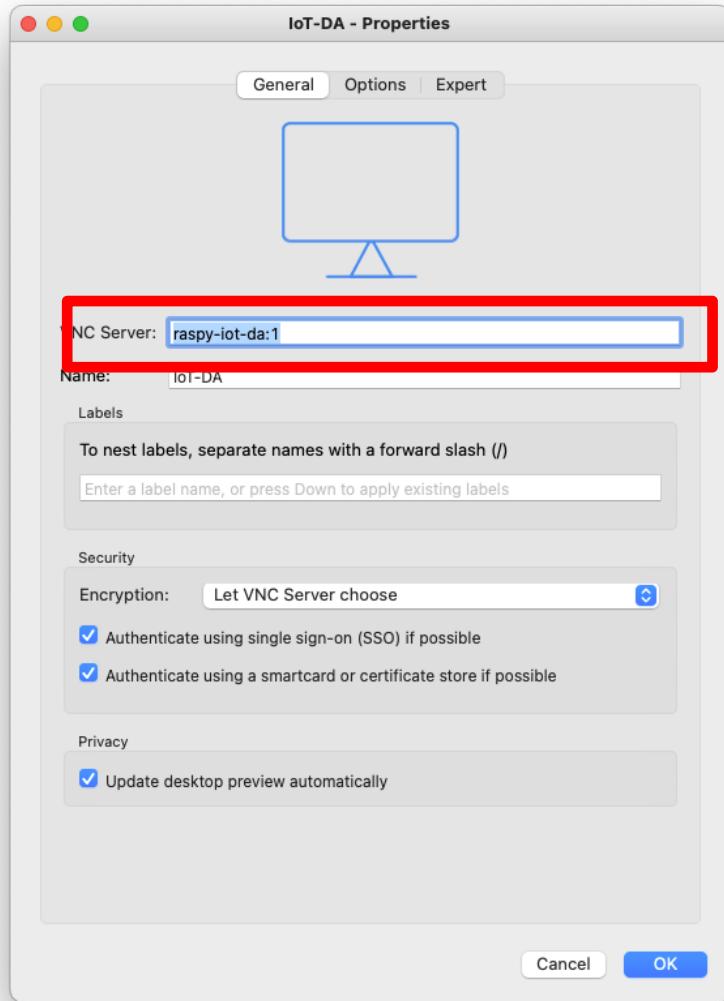
Address book

J's Team (Home)

IoT-DA

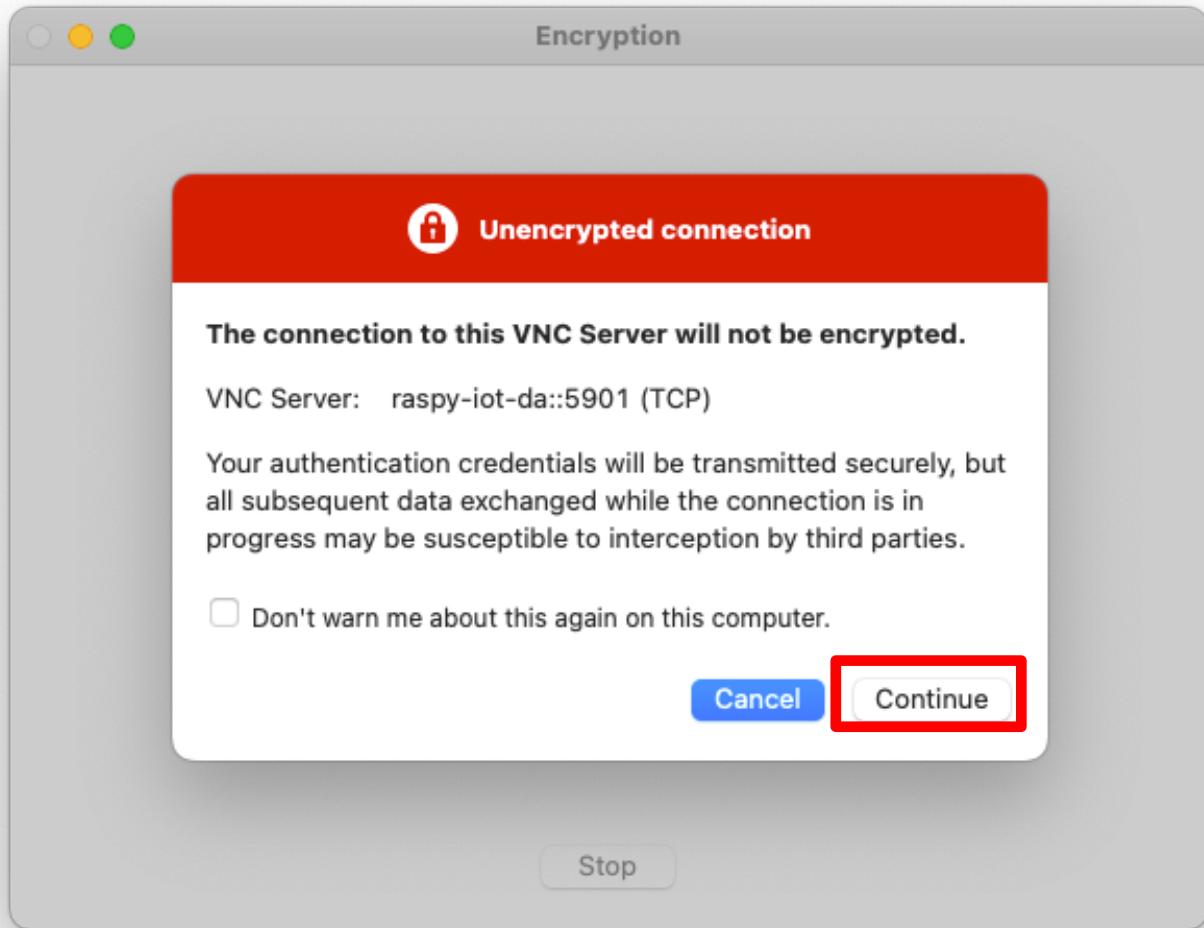
Real VNC Viewer

# VNC Viewer

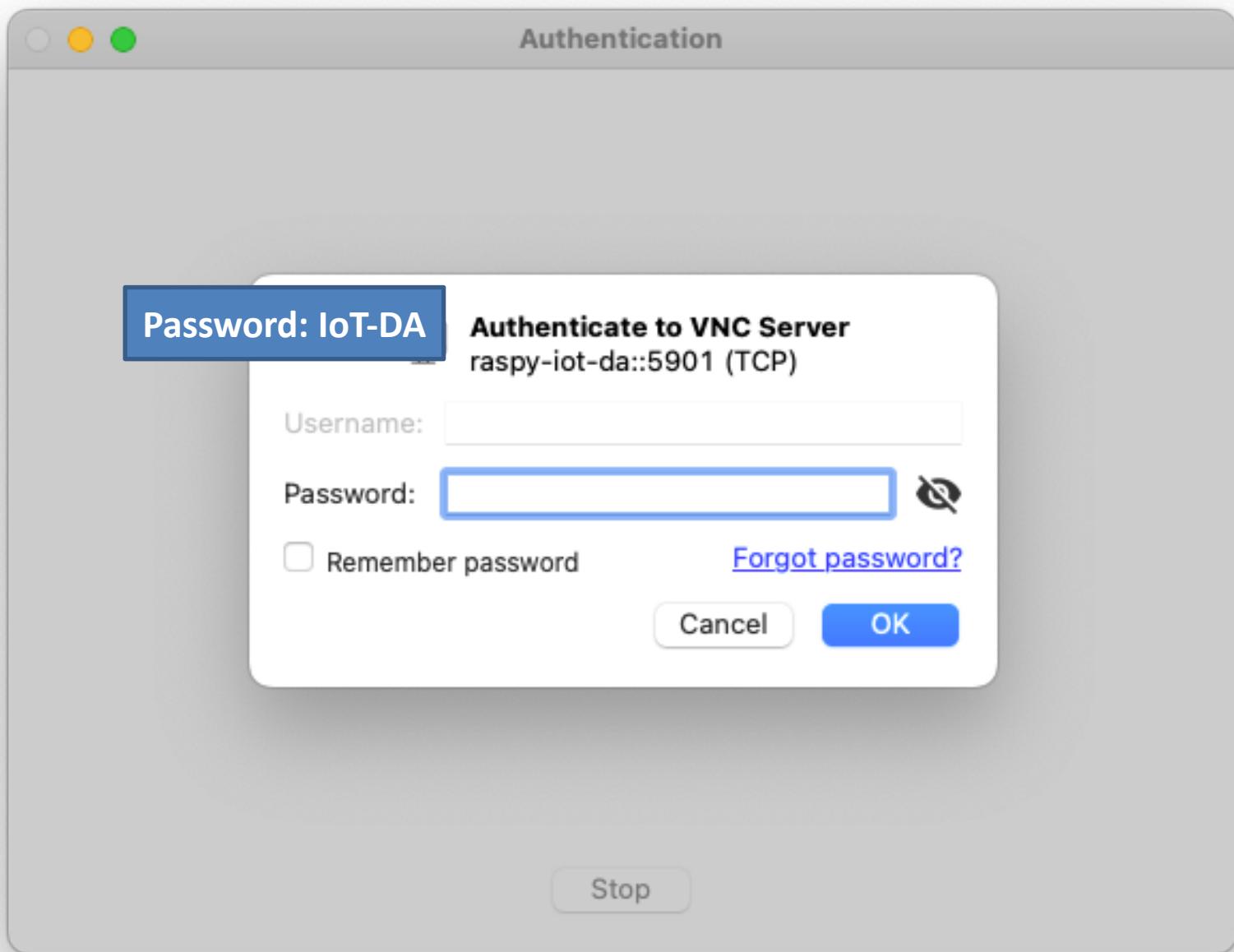




# VNC Viewer



Stop



# Initial Setup: raspberry Pi 4

## 2. Prepare the Raspberry Pi:

- Download Raspi-IoT-DA.img.zip image
- Flash the image into the SD cart using:
- Plug the SD card in the Raspberry Pi 4
- Log in
- By default the Raspi creates a WiFi Access Point
  - SSID: MasterIoT
  - Password: MasterIoT
- Connect to the AP and check internet access

# Initial Setup: Smart Socket

## 3. Pair the Smart Socket

- Download the android App ([HomeMate.apk](#))
- Install it in your Android device
  - If you do not have an Android device contact me
- Register into the App by creating a new user

# Initial Setup: S20C/S30C devices

- WIFI Smart Socket  
ORVIBO-S20C/S30C
- Wifi 2,4 GHz b/g/n
  - WEP/WPA-PSK/WPA2-PSK
  - Power cons.:  $\leq 0.3 \text{ W}$
- Input/output:
  - 100-240V ~, 50 H, 8A





# ORVIBO Home

HomeMate 365 Co., Ltd. House & Home

★★★★★ 1,968

E Everyone

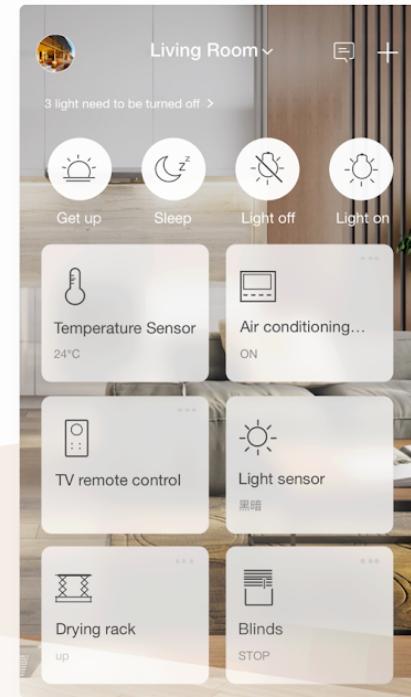
This app is available for some of your devices

You can share this with your family. [Learn more about Family Library](#)

Add to Wishlist

## More Convenient

All of times, care about your home and family



- With smart home platform ORVIBO Home, you can many controls as follow:
  - Control and manage all kinds of devices like curtains, air conditioners, TV, lights, switches, sockets and etc in one APP.
  - Create different scenes to control multiple devices.
  - Make 'If this then that' synchronizations scenario.



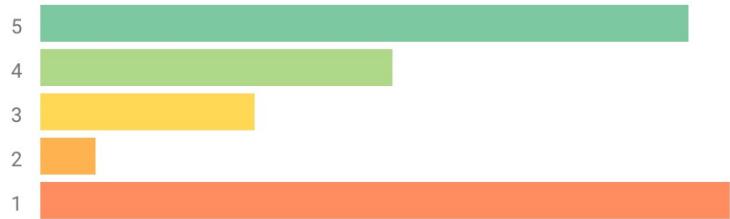
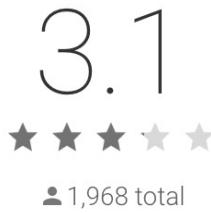
# ORVIBO Home

## ADDITIONAL INFORMATION

Updated	Size	Installs
April 29, 2022	150M	100,000+
Current Version	Requires Android	Content Rating
5.0.6.304	4.4 and up	Everyone
		<a href="#">Learn more</a>
Permissions	Report	Offered By
<a href="#">View details</a>	<a href="#">Flag as inappropriate</a>	HomeMate 365 Co., Ltd.

## REVIEWS

[Review policy and info](#)





# ORVIBO Home has access to:



## Device & app history

- retrieve running apps
- read your Web bookmarks and history



## Identity

- find accounts on the device



## Contacts

- modify your contacts
- read your contacts



## Location

- approximate location (network-based)
- precise location (GPS and network-based)



## Phone

- read phone status and identity



## Photos/Media/Files

- read the contents of your USB storage
- modify or delete the contents of your USB storage



## Microphone

- record audio



## Storage

- read the contents of your USB storage
- modify or delete the contents of your USB storage



## Camera

- take pictures and videos



## Wi-Fi connection information

- view Wi-Fi connections



## Device ID & call information

- read phone status and identity



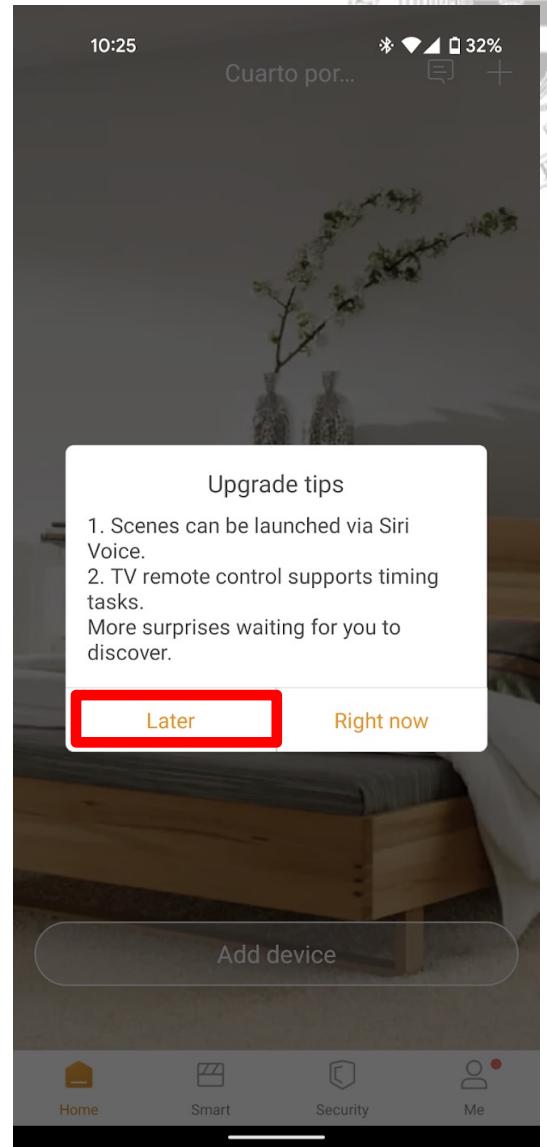
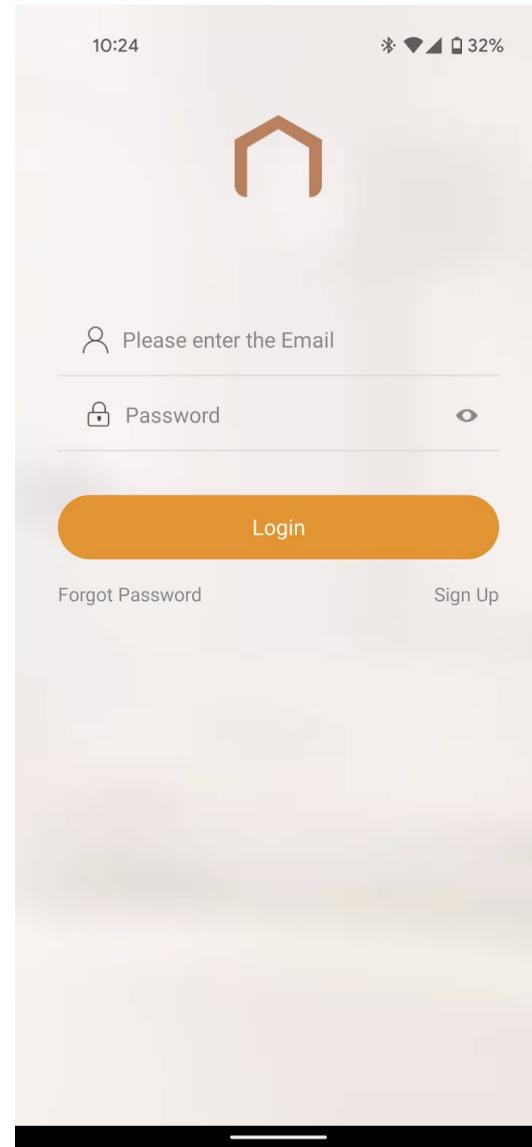
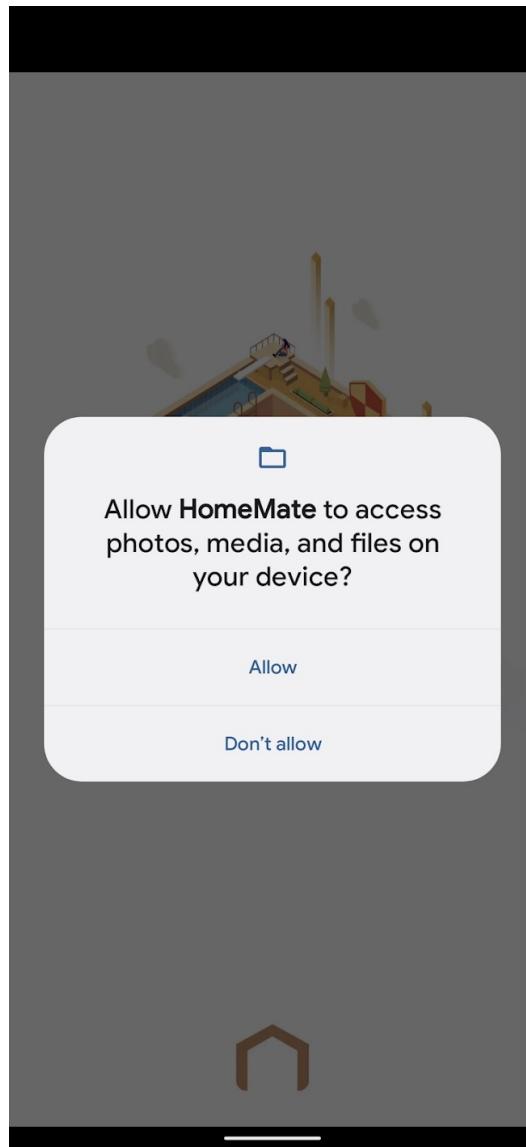
## Other

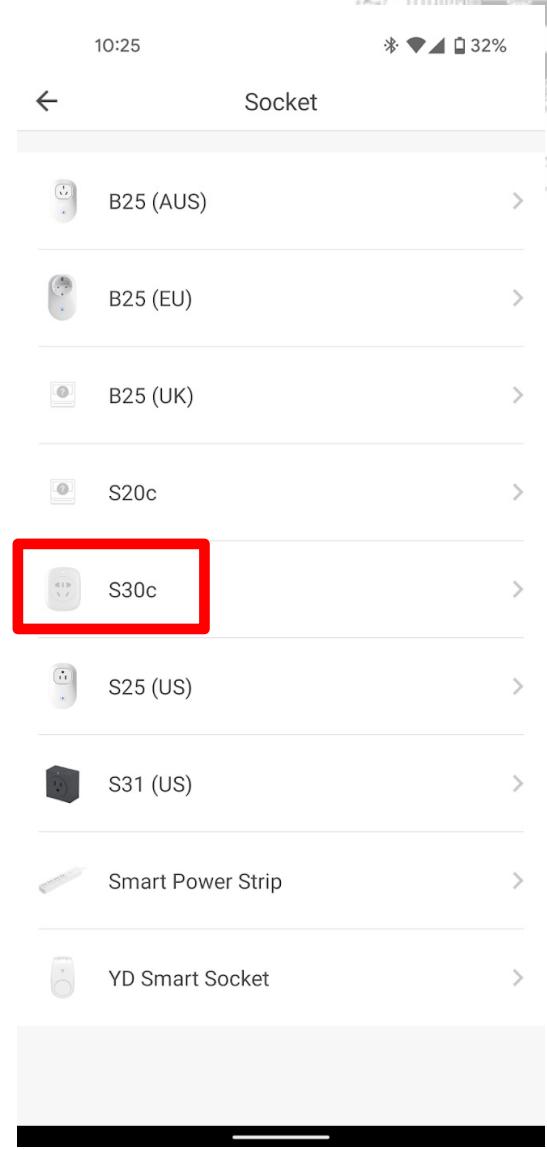
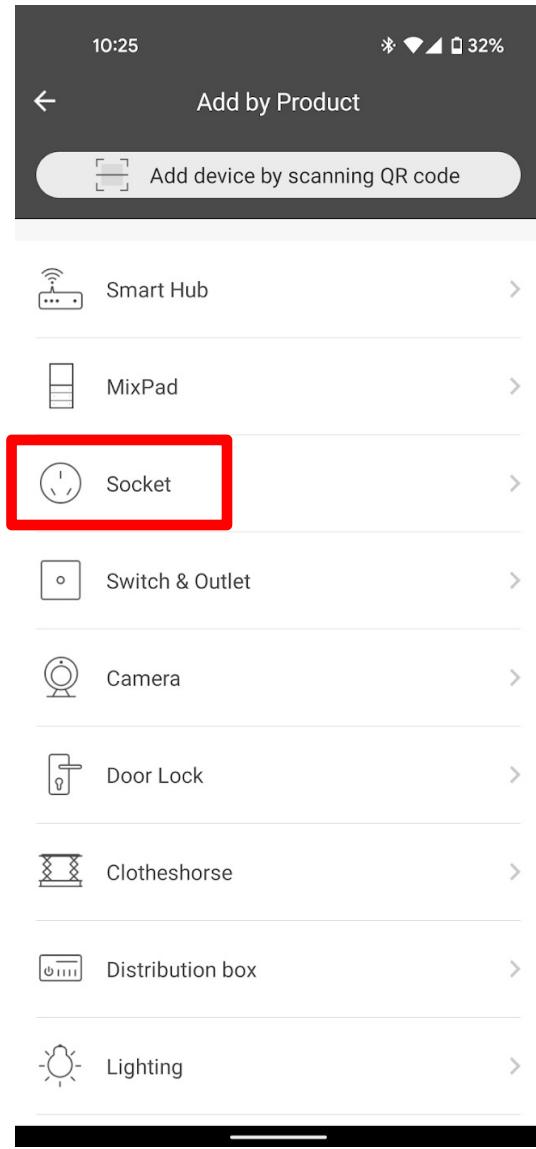
- download files without notification
- view network connections
- pair with Bluetooth devices
- access Bluetooth settings
- connect and disconnect from Wi-Fi
- full network access
- control Near Field Communication
- control vibration
- prevent device from sleeping

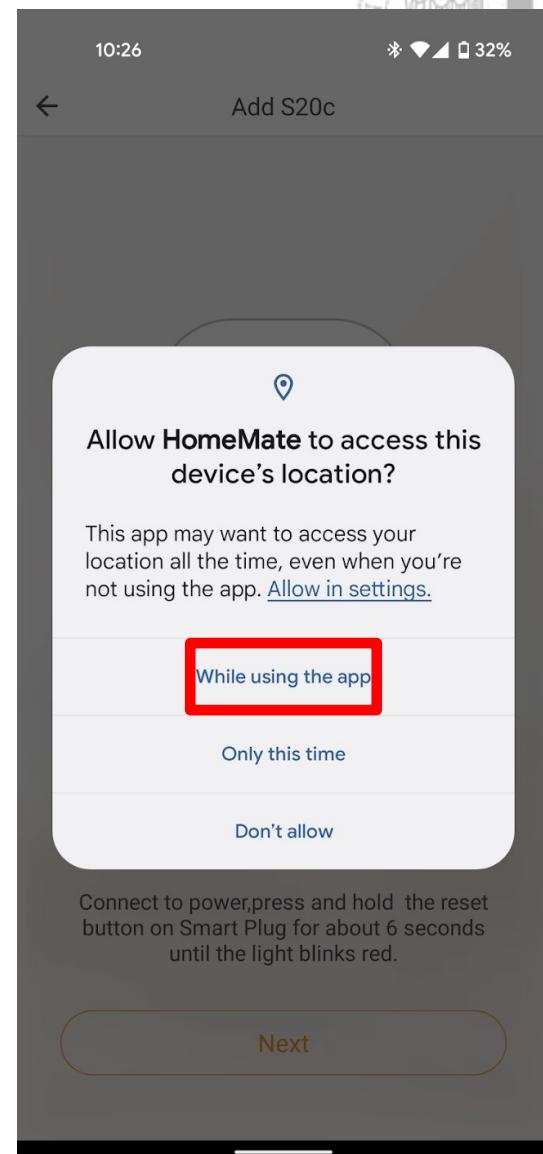
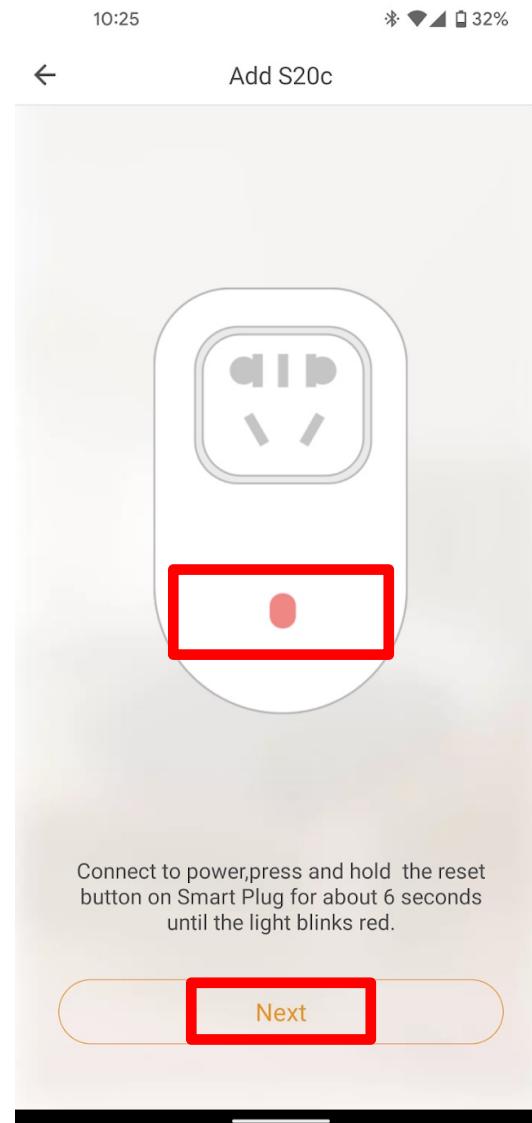
# Initial Setup: Smart Socket

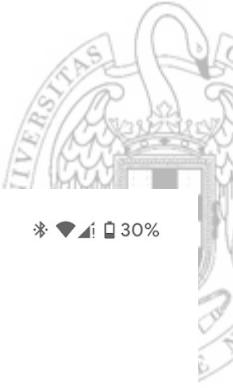
## 3. Pair the Smart Socket

- Download the android App ([HomeMate.apk](#))
- Install it in your Android device
  - If you do not have an Android device contact me
- Register into the App by creating a new user
- Pair the socket









The image consists of three screenshots from a mobile application interface, likely for setting up a Raspberry Pi device.

**Screenshot 1: Scanning the device**  
10:26 | 32%  
Scanning the device  
Scanning the device...  
Please ensure that the device has been in a status to be configured and is near the mobile phone.

**Screenshot 2: Device Network Configuration**  
10:26 | 32%  
Cancel figure Device Network  
5G WiFi not supported  
MasterloT  
MasterloT  
Make your mobile phone, device and router close to each other as much as possible.  
Next  
**Raspberry Pi running!!**

**Screenshot 3: Success Confirmation**  
10:33 | 30%  
Successfully added  
Device Name S20c Plug  
Room Cuarto por defecto  
Done

# Setup completed!!!



- ✓ The Smart Plug is paired to our App
- ✓ The Smartphone and the Smart Socket are connected to the Raspberry Pi Access Point
- ✓ We can turn on/off the Smart Socket using the App

