Welcome Home!

Internet Open Telemetry

Martin Hron
security researcher

HITCON 2018

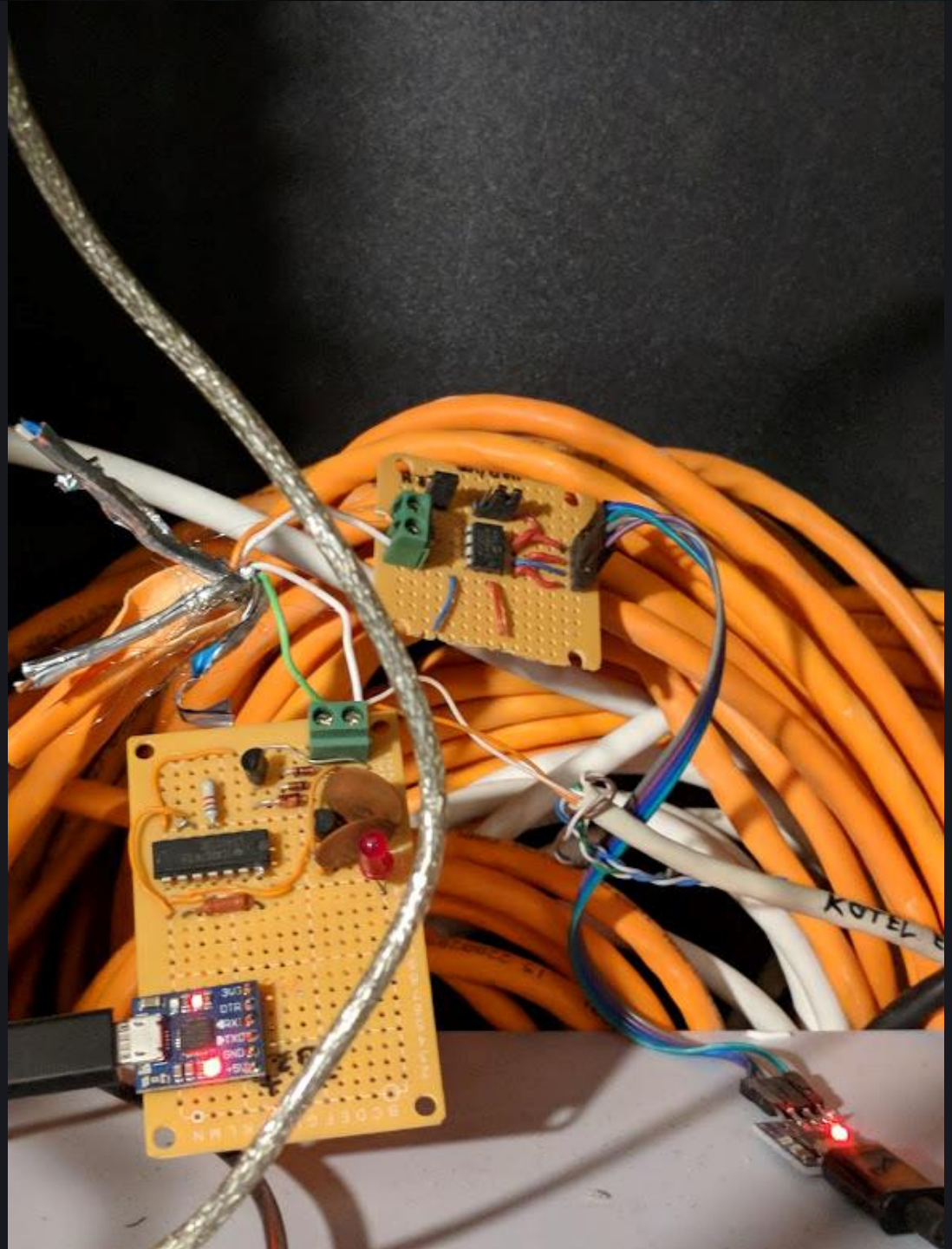
avast

Buzzword

A word or phrase which has become fashionable or popular, or sounds technical or important and is used to impress people


So let’s talk about IoT

What is IoT?


KOTEL

Flashback: How it has started

- Many smart devices or devices that can be made smart ☺


T5A H250V


WOLF


TP-LINK


RAIL-09
19:12:46
OEZ
LTE
B16

Babylon of “standards”

- You can go two ways:
  - use one vendor and one solution, one cloud
  - you have many devices from different vendors or even dumb devices which need to be made smart

Babylon of “standards”

- Physical layer / data link
  - Bluetooth
  - RS232, RS485, CAN, eBUS
  - WiFi, Ethernet
  - ZigBee
  - 433, 866 MHz
  - and many others

Babylon of “standards”

- Transport / application layer
  - Textual data
  - JSON
  - HTTP
  - XML
  - Binary oriented protocols
  - Proprietary protocols


MQTT.ORG

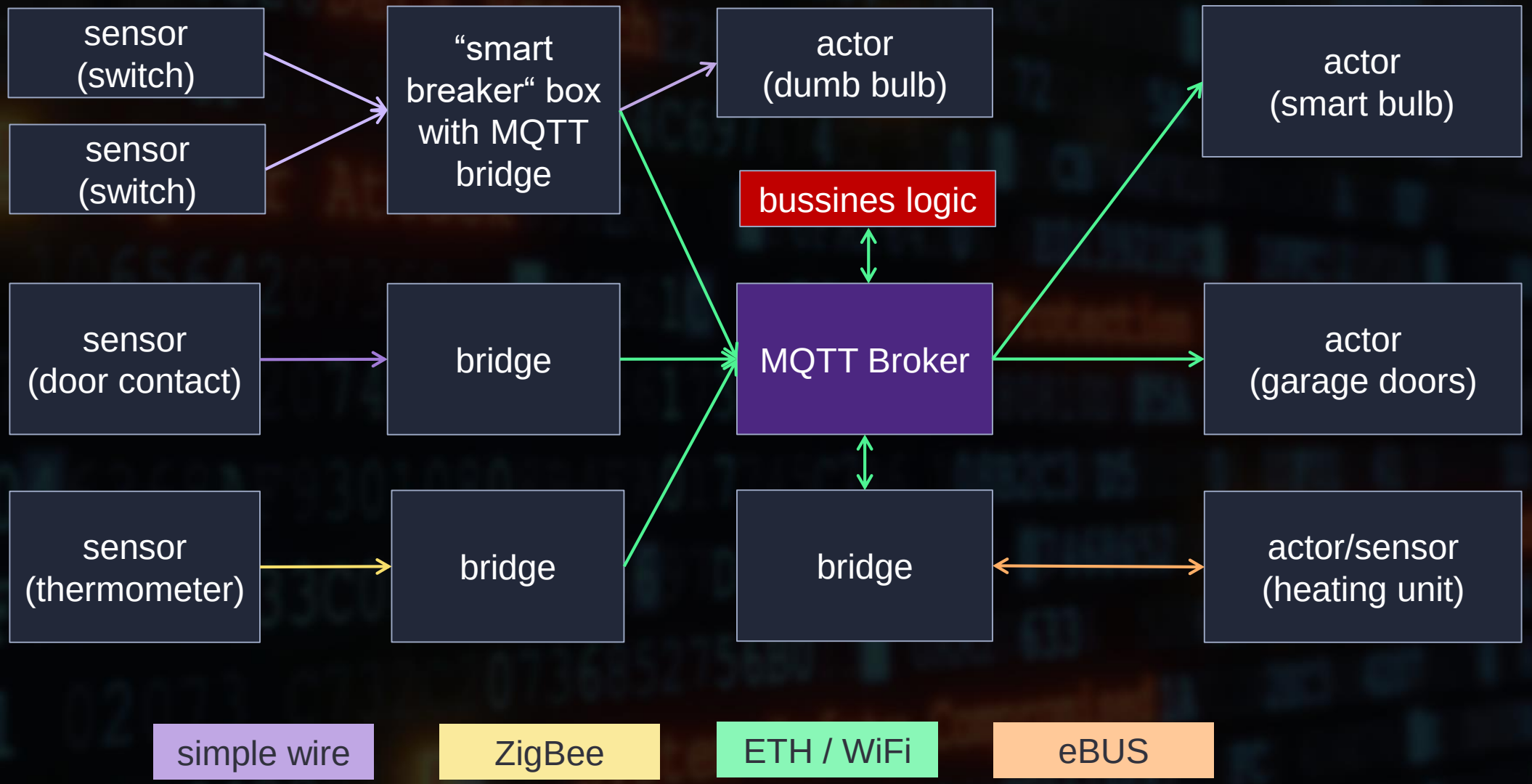
Message Queue Telemetry Transport - MQTT

- publisher - subscriber model
- payload agnostic
- topics can be organized in tree like structure
- when subscribing wildcards can be used
- usually operates through TCP on port 1883
- supports “last will” and persistent topics

MQTT topics

- Examples of topics:
  /house/attic/light
  /house/basement/door
  /house/basement/light
- Tree like organized structure. When subscribing, you can use wildcards. # for all levels from here down the tree or + for any single level.
- Subscription to /house/+/light delivers all light topics in any room
- Subscription to only # delivers every topic published by anyone to this MQTT server/broker.

MQTT Broker use case in “smart home”



Typical implementation

- Various smart and dumb devices bridged to MQTT
- One namespace of topics spans whole building
- MQTT broker, Mosquitto is commonly used one
- Business logic usually provided by some server software which connects to MQTT
- It usually provides some dashboard and frontend
  Domoticz, openHAB, Home Assistant, MQTT dash, Node-Red and many others

Welcome home!

Welcome home!

```
unifi_user: [redacted]
unifi_password: [redacted]

unifi_ssh_user: [redacted]
unifi_ssh_password: 12345678

spotify_[redacted]_client_id: [redacted]
spotify_[redacted]_client_secret: [redacted]

spotify_[redacted]_client_id: [redacted]
spotify_[redacted]_client_secret: [redacted]

zap2it_pass: [redacted]
```

Welcome home!

- Many dashboards have no password set
- There are ~45K MQTT servers available to connect
- There are ~26K MQTT servers opened without any password set
- Remember? You can subscribe to #
- If there is password you can still get there……

Rules of the house

no exploits

use what is available

cause no harm

even if you are tempted to do so ;)


SHODAN

DEMO TIME

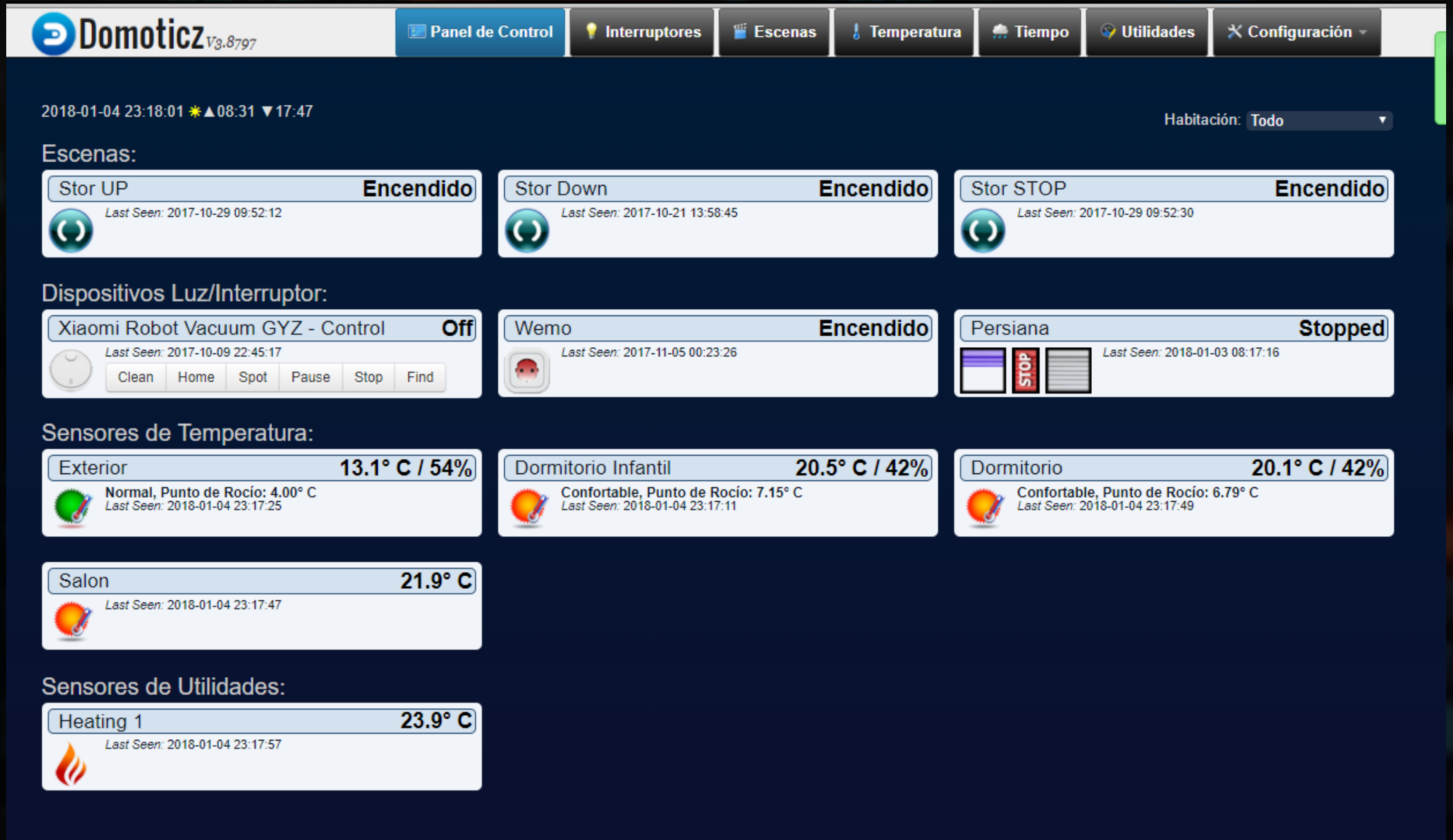
Domoticz

Home Assistant

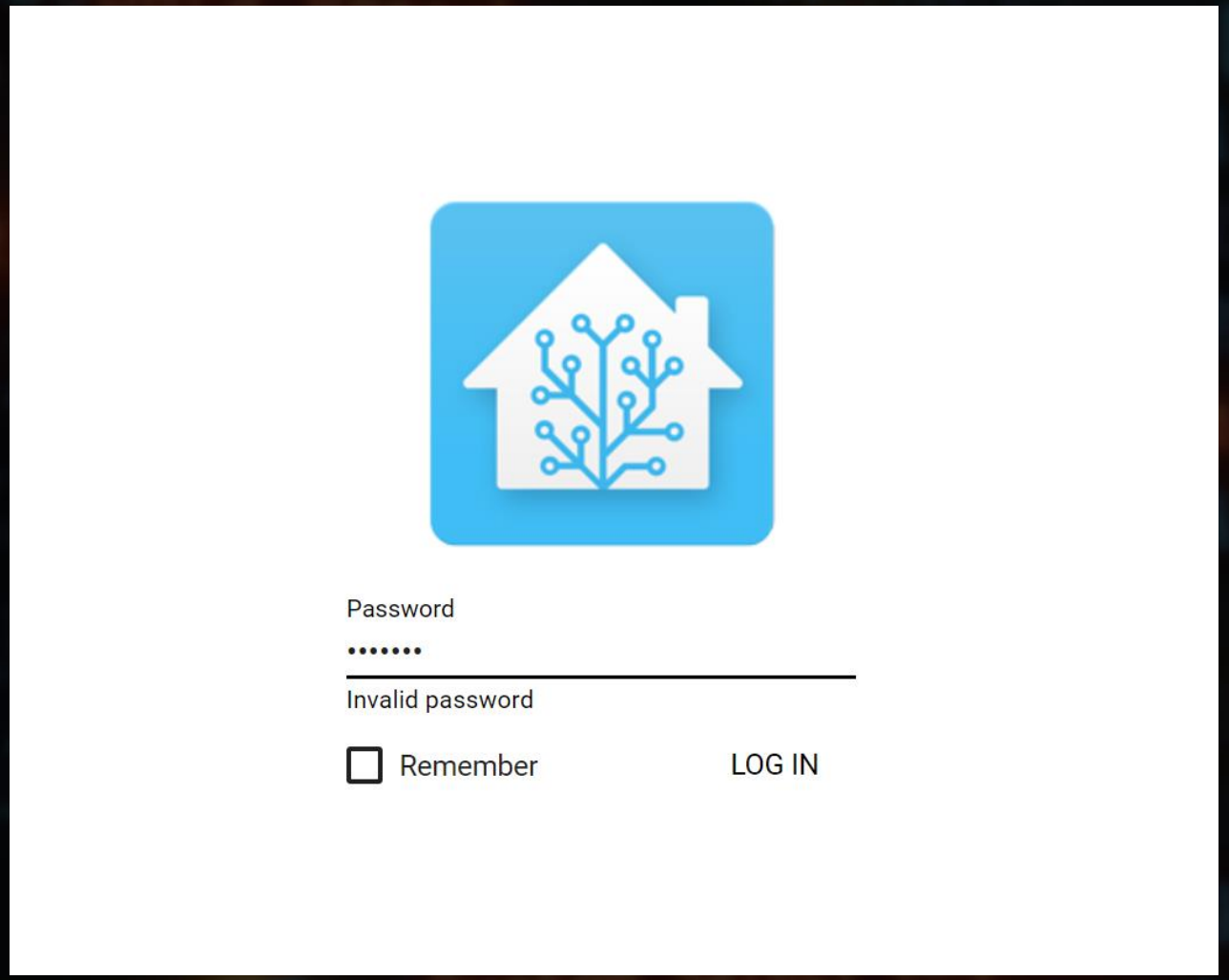
Home automation systems

- Similar concept
- Provide business logic
- Provide frontend / dashboard
- Usually Integrate with MQTT

Domoticz


Domoticz V3.8797
Panel de Control
Interruptores
Escenas
Temperatura
Tiempo
Utilidades
Configuración
2018-01-04 23:18:01 ☀▲08:31 ▼17:47
Habitación: Todo
Escenas:
Stor UP Encendido
Last Seen: 2017-10-29 09:52:12
Stor Down Encendido
Last Seen: 2017-10-21 13:58:45
Stor STOP Encendido
Last Seen: 2017-10-29 09:52:30
Dispositivos Luz/Interruptor:
Xiaomi Robot Vacuum GYZ - Control Off
Last Seen: 2017-10-09 22:45:17
Clean Home Spot Pause Stop Find
Wemo Encendido
Last Seen: 2017-11-05 00:23:26
Persiana Stopped
STOP
Last Seen: 2018-01-03 08:17:16
Sensores de Temperatura:
Exterior 13.1° C / 54%
Normal, Punto de Rocío: 4.00° C
Last Seen: 2018-01-04 23:17:25
Dormitorio Infantil 20.5° C / 42%
Confortable, Punto de Rocío: 7.15° C
Last Seen: 2018-01-04 23:17:11
Dormitorio 20.1° C / 42%
Confortable, Punto de Rocío: 6.79° C
Last Seen: 2018-01-04 23:17:49
Salon 21.9° C
Last Seen: 2018-01-04 23:17:47
Sensores de Utilidades:
Heating 1 23.9° C
Last Seen: 2018-01-04 23:17:57

Home Assistant: case study



Home Assistant: at the same IP

445
tcp
smb

Samba Version: 4.5.12-Debian

```
SMB Status
Authentication: disabled
SMB Version: 1
Capabilities: raw-mode,unicode,large-files,nt-smb,rpc-remote-api,nt-status,lev
el2-oplocks,lock-and-read,nt-find,dfs,infolevel-passthru,large-readx,large-wri
tex,unix,extended-security

Shares
Name                    Type       Comments
---------------------------------------------------------------------
print$                  Disk       Printer Drivers
homeassistant           Disk
IPC$                    IPC        IPC Service (Samba 4.5.12-Debian)
```

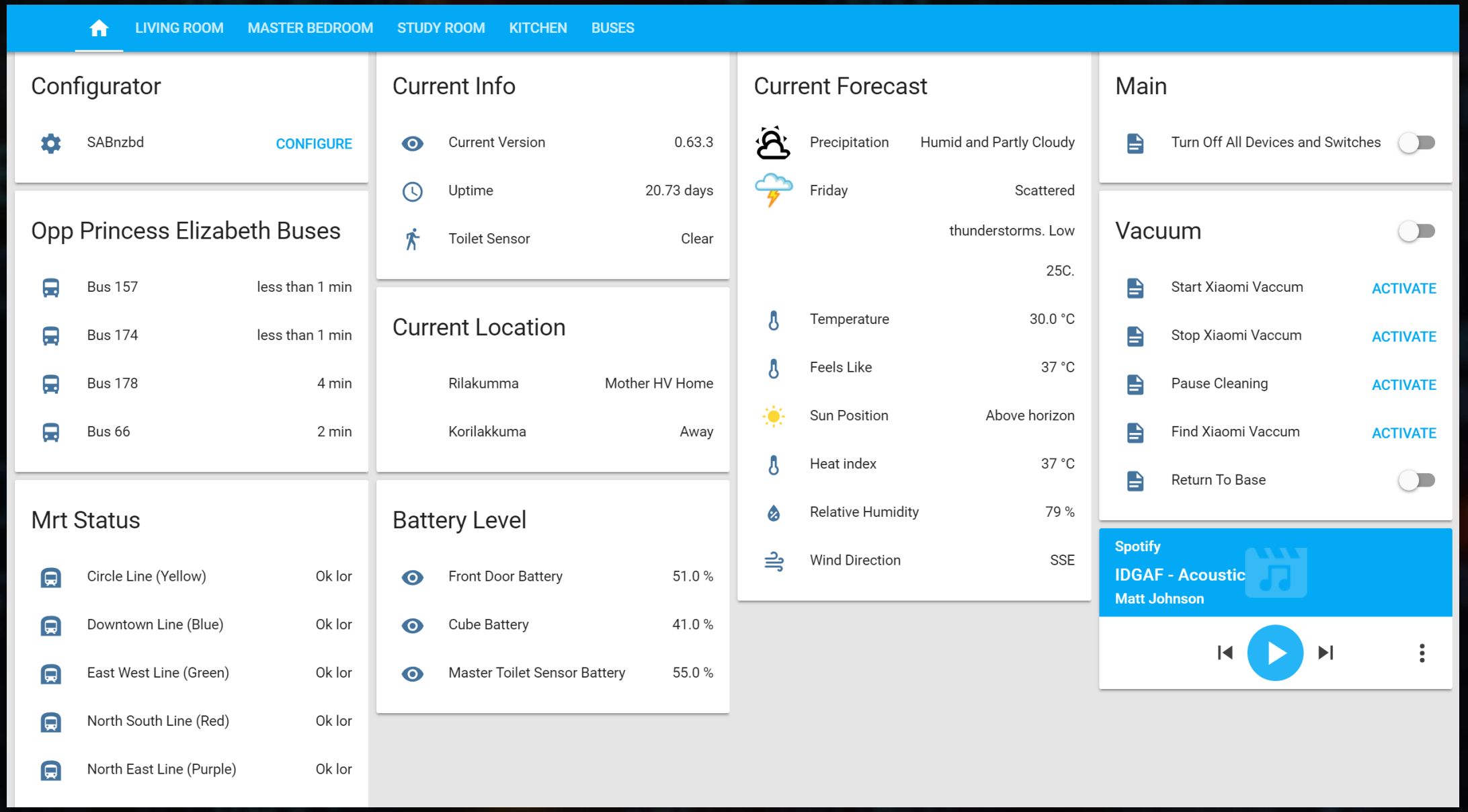
Home Assistant: at the same IP

Name	Date modified	Type	Siz
home-assistant_v2	6/22/2018 10:27 A	Data Base File	
html5_push_registrations.conf	6/10/2018 4:43 PM	CONF File	
input_select.yaml	11/7/2017 4:53 PM	YAML File	
known_devices.yaml	3/25/2018 5:29 AM	YAML File	
lights.yaml	2/23/2018 5:03 PM	YAML File	
notify.yaml	5/1/2018 2:18 AM	YAML File	
scripts.yaml	6/10/2018 4:43 PM	YAML File	
secrets.yaml	5/5/2018 3:17 AM	YAML File	
sensors.yaml	5/5/2018 2:44 PM	YAML File	
switches.yaml	5/31/2018 6:50 PM	YAML File	
zones.yaml	5/5/2018 3:36 AM	YAML File	

Home Assistant: give me your secrets

```
# Use this file to store secrets like usernames and passwords.
# Learn more at https://home-assistant.io/docs/configuration/secrets/
http_password: [redacted]
ssl_certificate: [redacted]
ssl_key: [redacted]
xiaomi_gateway_mac: [redacted]
xiaomi_gateway_key: [redacted]
ifttt: [redacted]
google_assistant_projectid: [redacted]
google_assistant_clientid: [redacted]
google_assistant_accesstoken: [redacted]
broadlink_host: 192.168.1.76
broadlink_mac: [redacted]
broadlink_host2: 192.168.1.77
broadlink_mac2: [redacted]
mqtt_username: [redacted]
```

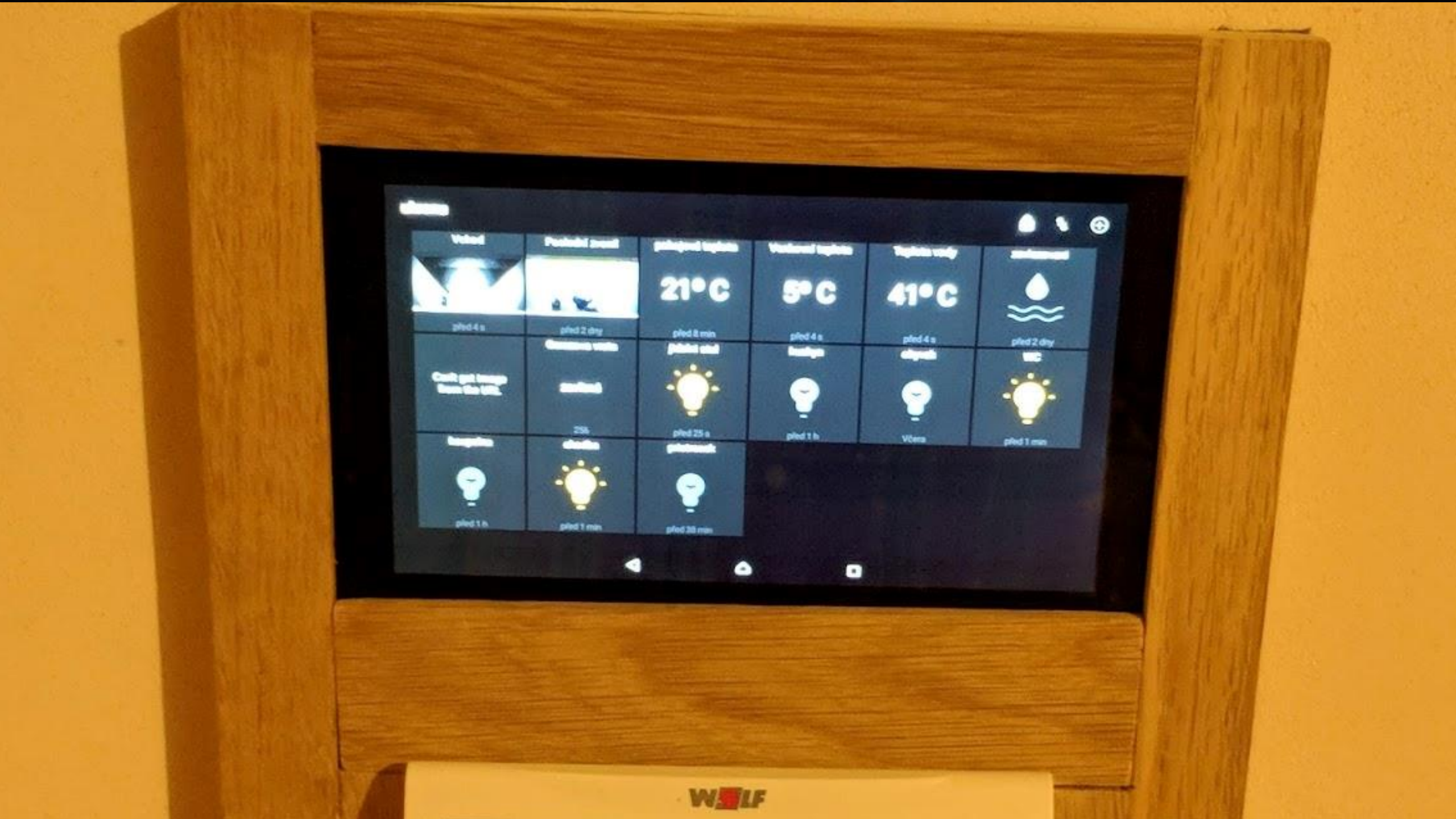
Home Assistant: Welcome Home!



MQTT DASH

MQTT Dash

- Simple Android/IOS app
- MQTT centric, simple UI that directly reflects state or controls devices through MQTT topics
- Interesting concept of storing/loading whole configuration by publishing it to the “persistent” topic


21°C
5°C
41°C
WOLF

DEMO TIME

OWNTRACKS

Your “personal” GPS tracker

- Basically Android and IOS application for creating GPS tracking log
- Supports MQTT
- Forget about unsecured cameras, this is even worse.

DEMO TIME

Conclusion

- Real world example how bad the situation is
- Educate people more about security
- Let’s stick to security as an opt-out choice everywhere it is possible
- Please, pretty please
- I beg you
- DON’T STORE PASSWORDS IN PLAINTEXT

THERE SAVING IOT SECURITY!

MQTT can be also used for automation of your garden

But the risks can sometimes be “high”

Go ahead and ask!

Thank You!

Martin Hron


@thinkcz


hron@avast.com


www.avast.com