

# Welcome Home!

Internet Open Telemetry

**BSIDES**  
MANCHESTER

2018

**Martin Hron**  
security researcher

**Welcome to the age of speed and security!**

“A computer lets you make more mistakes faster than any invention in human history - with the possible exceptions of handguns and tequila.”

*Mitch Ratliff*

So let's talk about the IoT

## Personal story

**P A R E N T A L**  
**ADVISORY**  
**EXPLICIT CONTENT**

Following part of the presentation contains best practices violation, domestic violence on devices, broken security and self-confidence.





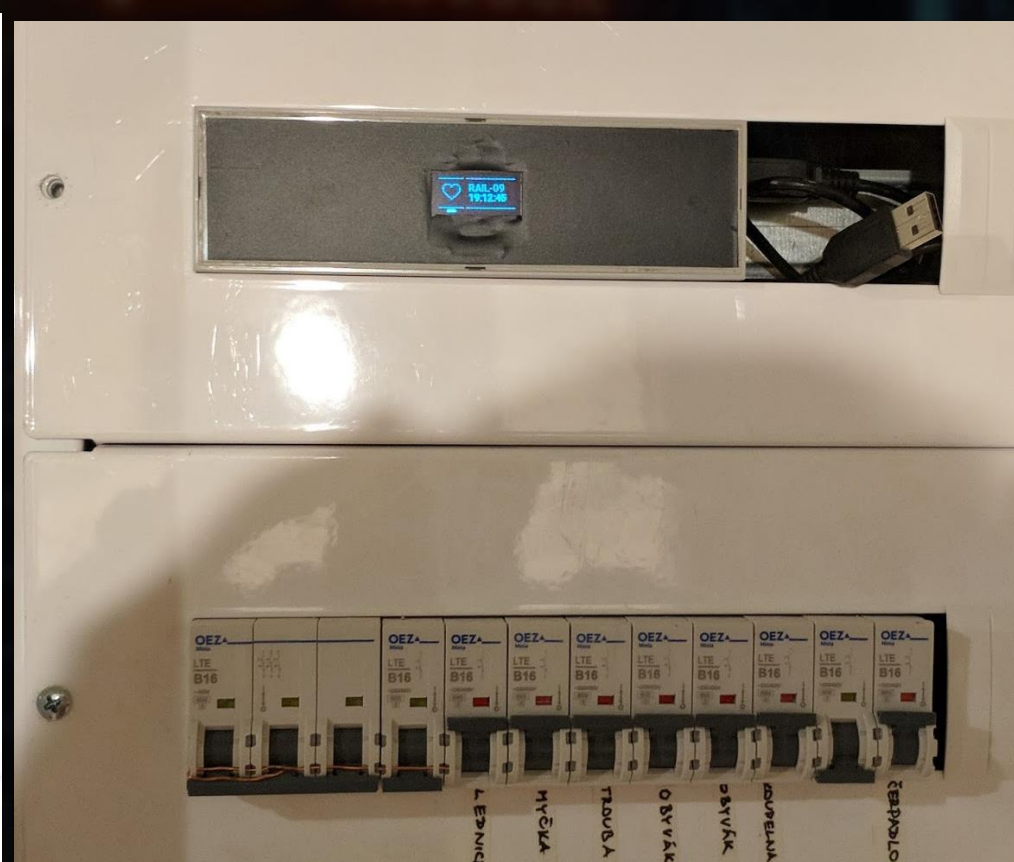
## Personal story : options

use one vendor and one  
solution, one cloud

You've got a bunch of devices  
from different vendors or even  
dumb devices







# Personal story

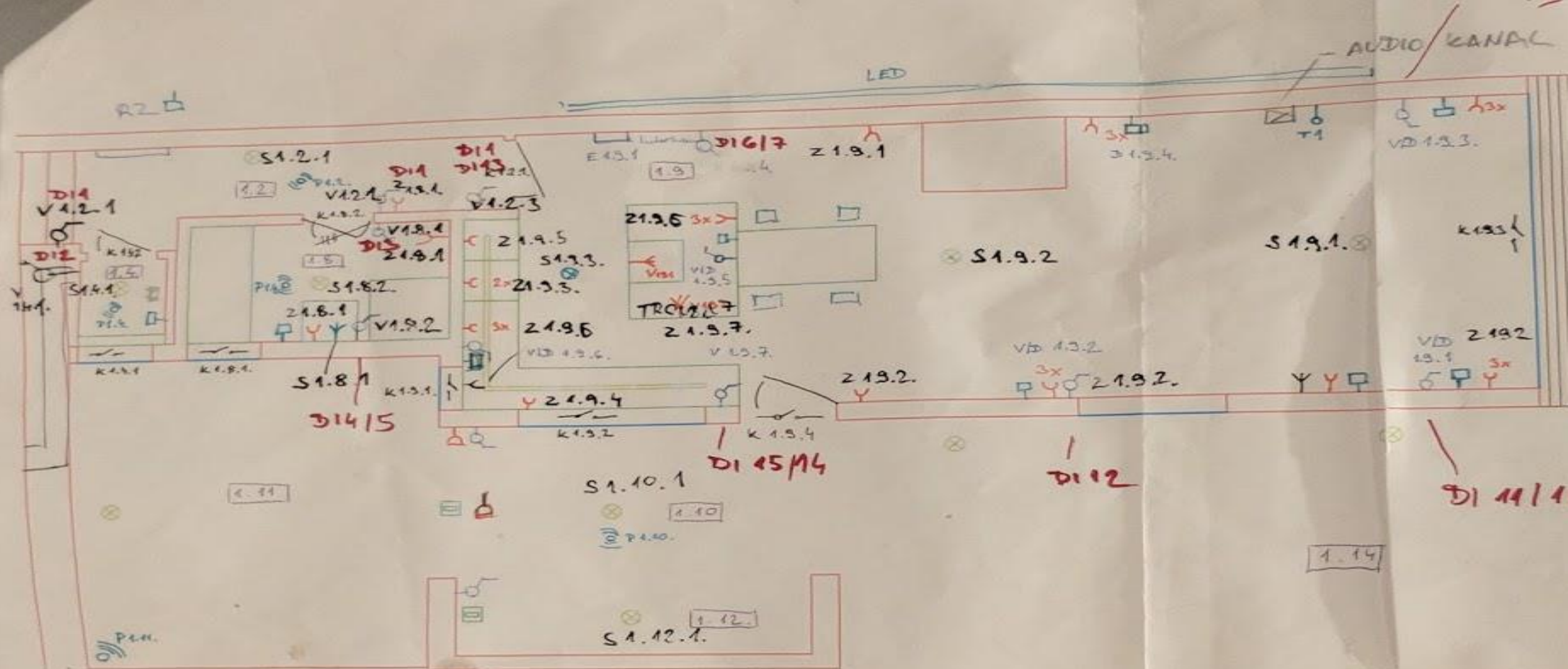
Some devices might be exotic.



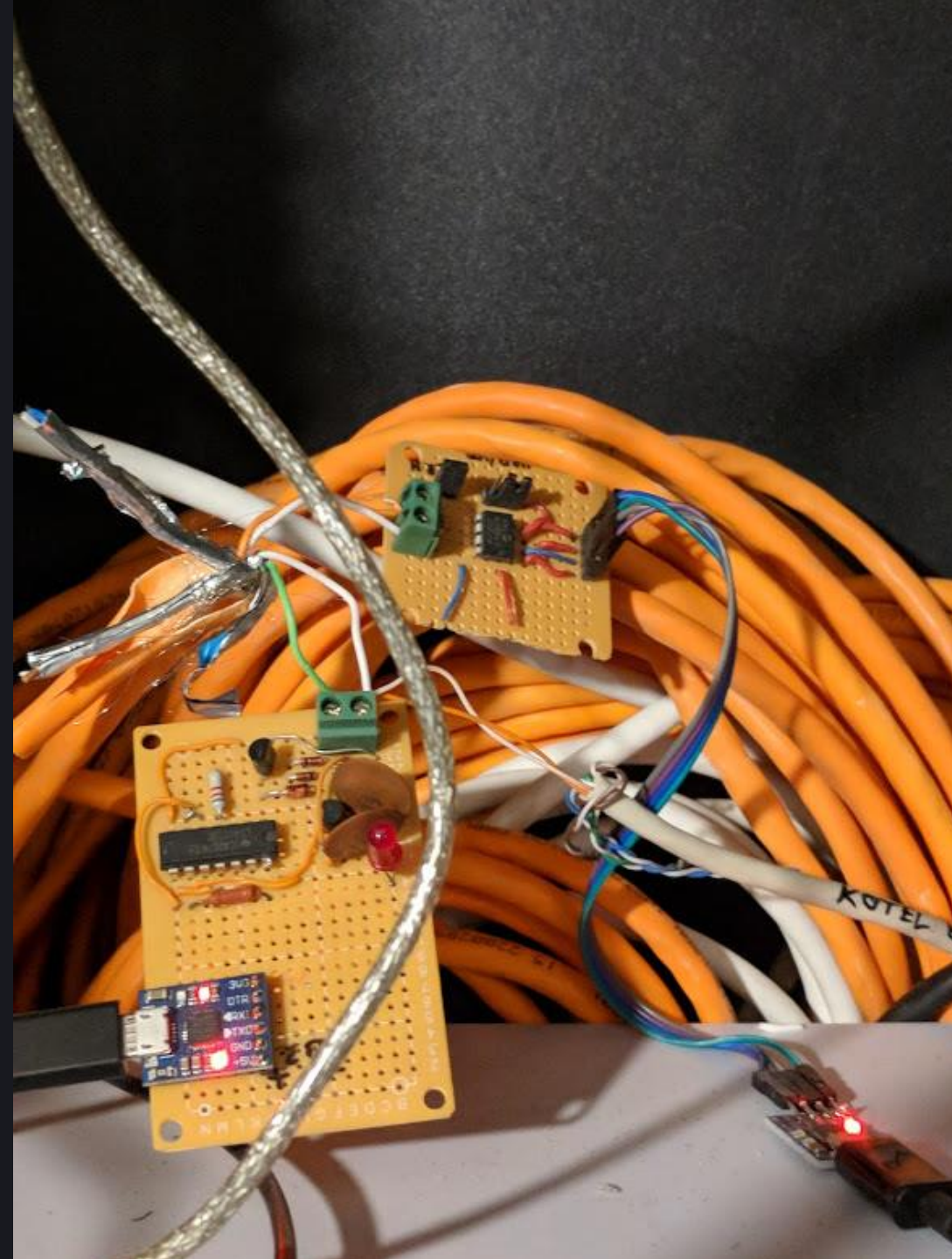


## Personal story

- I had mixture of devices and a was dreaming of nice rig for my “smart hub” and all the equipment. Dreaming about a house where everything just happens.







# 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







# Message Queue Telemetry Transport - MQTT

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

# MQTT topics

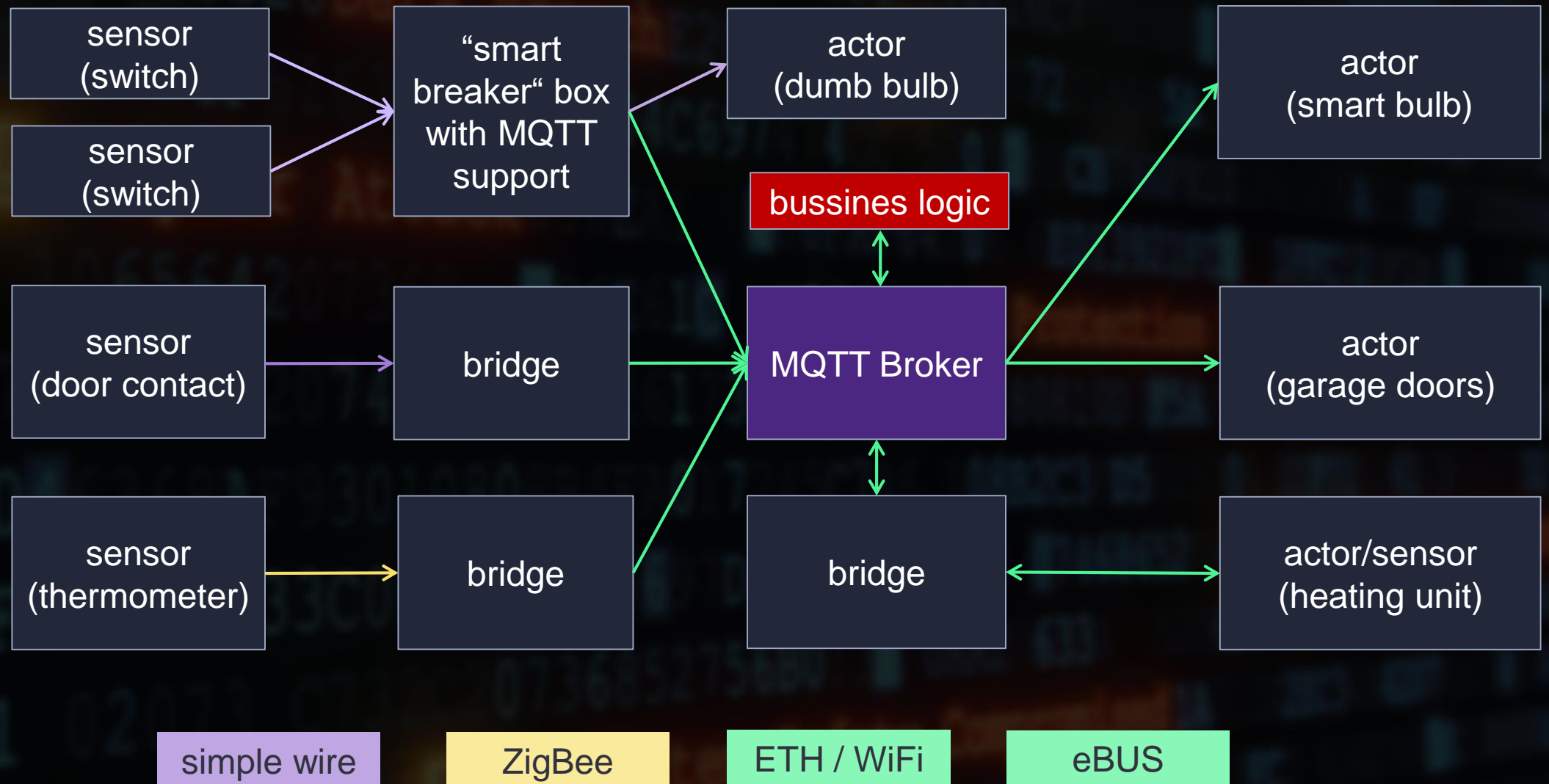
- Examples of the topics:
  - `/house/attic/light`
  - `/house/basement/door`
  - `/house/basement/light`
- Tree like organized structure. When subscribing, you can use wildcards. `#` for the all levels from here down the tree or `+` for any single level.
- Subscription to `/house/+/light` delivers all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



# Typical implementation

- Mixture of devices
- One namespace
- MQTT broker
- Business logic
- Usually, this also provides some dashboard and a frontend (Domoticz, openHAB, Home Assistant, MQTT dash, Node-Red and many others)

# MQTT Broker typical setup of “smart home”







Welcome home!



# Welcome home!

unifi\_user: `haxida`

unifi\_password: `haxidax`

unifi\_ssh\_user: `jay`

unifi\_ssh\_password: `12345678`



spotify\_`jay`\_client\_id: `haxida`

spotify\_`jay`\_client\_secret: `haxida`

spotify\_`haxidax`\_client\_id: `haxida`

spotify\_`haxidax`\_client\_secret: `haxida`

zap2it\_pass: `haxida`

# Welcome home!

- Many dashboards have no password set
- There are ~49K MQTT servers available to connect
- There are ~32K MQTT servers opened without any password set
- Remember? You can subscribe to #



## Rules of the house

no real exploits

use what is available

cause no harm

even if you are tempted to do so ;)



SHODAN

DEMO TIME





**Domoticz**



**Home Assistant**



**openHAB**  
empowering the smart home

# Home automation software “smart hubs”

- Similar concept
- Provide business logic
- Provide frontend / dashboard
- Usually integrate with MQTT and cloud services

# 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

 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

29



DEMO TIME

# Home Assistant: case study



Password

.....

Invalid password

☐

Remember

LOG IN

# 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,level2-oplocks,lock-and-read,nt-find,dfs,infolevel-passthru,large-readx,large-writex,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]  
matt username: [REDACTED]
```

# Home Assistant: Welcome Home!

LIVING ROOMMASTER BEDROOMSTUDY ROOMKITCHENBUSES

Configurator

SABnzbdCONFIGURE

Opp Princess Elizabeth Buses

Bus 157less than 1 min

Bus 174less than 1 min

Bus 1784 min

Bus 662 min

Mrt Status

Circle Line (Yellow)Ok lor

Downtown Line (Blue)Ok lor

East West Line (Green)Ok lor

North South Line (Red)Ok lor

North East Line (Purple)Ok lor

Current Info

Current Version0.63.3

Uptime20.73 days

Toilet SensorClear

Current Location

RilakummaMother HV Home

KorilakkumaAway

Battery Level

Front Door Battery51.0 %

Cube Battery41.0 %

Master Toilet Sensor Battery55.0 %

Current Forecast

PrecipitationHumid and Partly Cloudy

FridayScattered thunderstorms. Low  
25C.

Temperature30.0 °C

Feels Like37 °C

Sun PositionAbove horizon

Heat index37 °C

Relative Humidity79 %

Wind DirectionSSE

Main

Turn Off All Devices and Switches

Vacuum

Start Xiaomi VaccumACTIVATE

Stop Xiaomi VaccumACTIVATE

Pause CleaningACTIVATE

Find Xiaomi VaccumACTIVATE

Return To Base

Spotify

IDGAF - Acoustic  
Matt Johnson

⏮️▶️⏭️⋮



# Home Assistant: I'm not the only one

```
# Use this file to store secrets like usernames and passwords.  
# Learn more at https://home-assistant.io/docs/configuration/secrets/
```

```
# sorry mate  
#you have been hacked  
# dont get depress , didnt change anything  
  
#keep it as a lesson and change all passwords
```

```
http_password: [REDACTED]
```

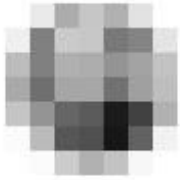
```
icloud_user: [REDACTED]
```

```
icloud_password: bXh[REDACTED]PC7
```

```
ring_user: [REDACTED]
```

```
ring_password: CKr[REDACTED]nP
```

# Home Assistant: I've been hacked



so i got this text file in my home assistant root this morning.

Your system is very inscure.

Your shares are available from web.

Delete your samba shares from web !

I can edit and delete all your HA files without password.

If you dont know how to do, have a look at here: <https://community.home-assistant.io/>

Proof:

New Password: HaCKeD!

# Home Assistant: I've been hacked

- Flash the downloaded image to an SD card using [Etcher](#).
- Optional - Setup the WiFi or static IP: On a USB stick, create the `network/my-network` file and follow the [HassOS howto](#).
- Insert the SD card (and optional USB stick) into the Raspberry Pi and turn it on. On first boot, it downloads the latest version of Home Assistant which takes ~20 minutes (slower/faster depending on the platform).
- You will be able to reach your installation at <http://hassio.local:8123>.
- Enable either the [Samba add-on](#) or the [SSH add-on](#) to manage your configuration in `/config/` (From the UI choose **Hass.io** which is located in the sidebar).





# Home Assistant: I've been hacked

This addon allows you to set up a [Samba](#) server to access hass.io folders using Windows network shares.

```
{
  "name": "hassio",
  "workgroup": "WORKGROUP",
  "guest": true,
  "map": {
    "config": true,
    "addons": true,
    "share": true,
    "backup": true,
    "ssl": false
  },
  "username": "",
  "password": "",
  "interface": "eth0"
}
```

# Home Assistant: I've been hacked

- **username** (*Optional*): Username for logging in if guest login is not used.
- **password** (*Optional*): Password for . An empty password is not supported.



# Home Assistant: I've been hacked

- **name** (*Optional*): Set netbios name of Hass.io device. Default is `hassio`.
- **workgroup** (*Optional*): Set network workgroup name. Default is `WORKGROUP`.
- **guest** (*Optional*): Allow login without a username or password. Default is `true`.







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





MQTT Dash

sample1

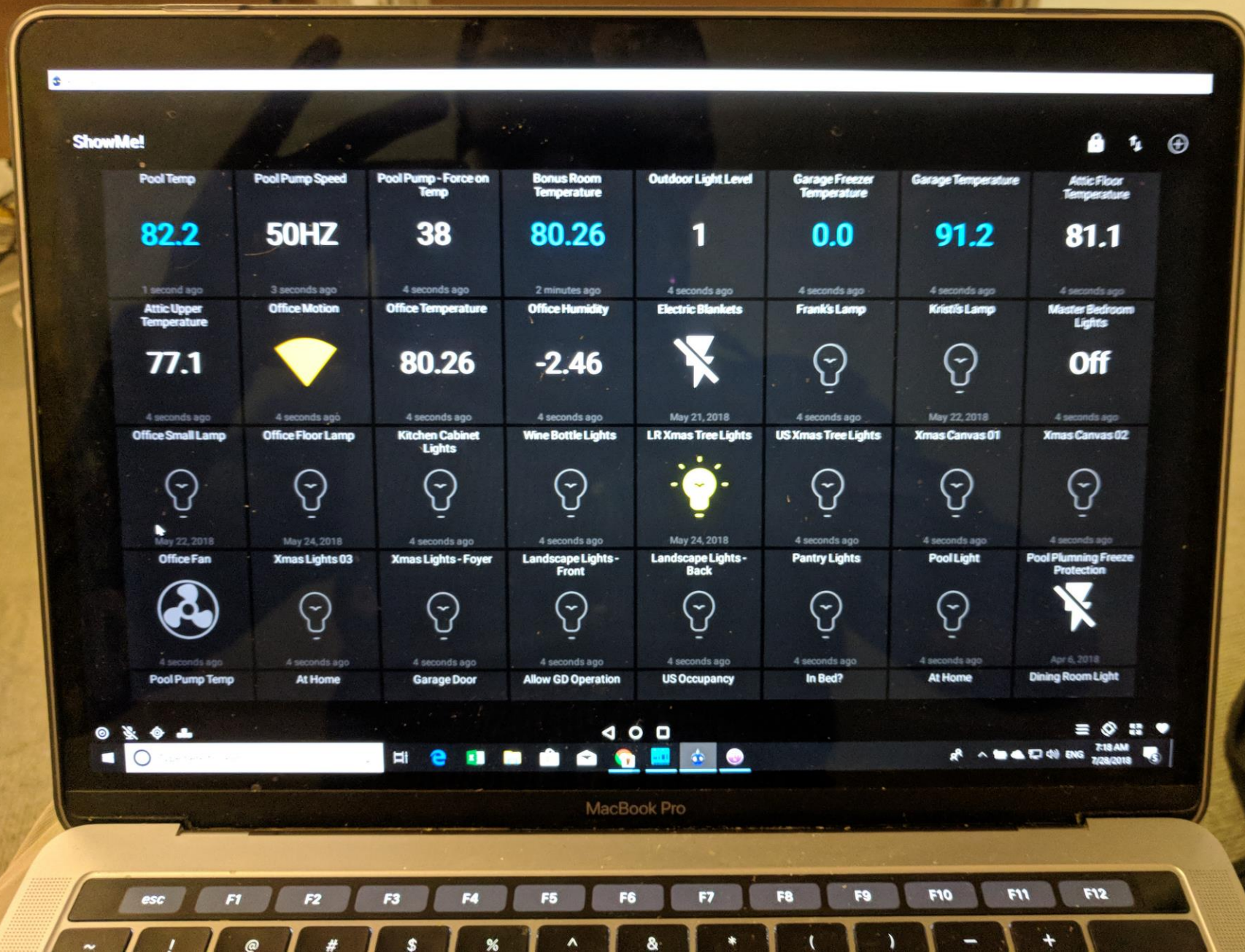
Test

Sample2

62.75.148.146

Anonymous

ShouldNot







OWNTRACKS



## Your “personal” GPS tracker

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

DEMO TIME

# Conclusion

- Real world examples how bad the situation is
- Educate people more about security
- Educate vendors and developers
- Let's stick to the security as an opt-out choice.
- **DON'T STORE PASSWORDS IN PLAINTEXT**
- **NEVER**
- **EVER**



THEY'RE SAYING IT'S ONLY SECURITY!

**MQTT can be also used for automation of your garden**

**But the risks could be “high”**





# Thank You!

Martin Hron



@thinkcz



hron@avast.com



www.avast.com

