IoT

Martin Hron
researcher

What is Internet Of Things

The **Internet of things** (**IoT**) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data.

Wikipedia

Basic facts

~4 billion

personal computers and smart phones in the world

in 2014

Basic facts

~15 billion

smart devices connected in the world

now

Basic facts

~75 billion

devices will be connected to the Internet Of Things

by 2025

Basic facts

Typical Long time support (TLS) lifespan in IT industry

is in average

5 years

Except…

Basic facts

Typical lifespan of a fridge is

14-17 years

Basic facts

Roughly every fourth device is vulnerable to some type of attack

Product placement ☺

At least until beginning of this week.

Possible outcome

That'll give us ~20B unmonitored, unsupervised, inter-connected vulnerable devices

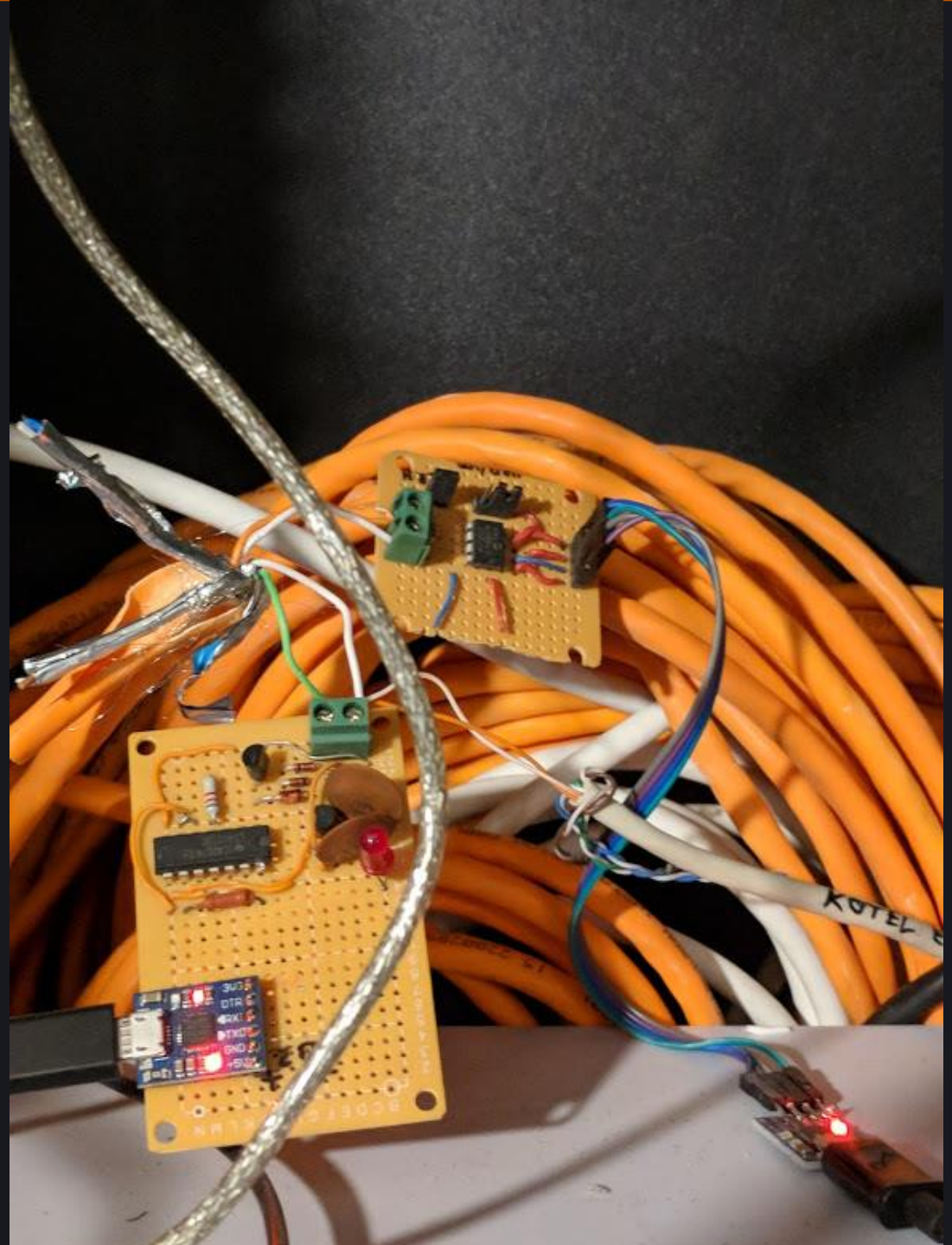
with hardly any support

Do you still want to buy a smart fridge?

Or smart personal scale?

IoT

Insecure open Telemetry


KOTEL

Flashback: How it has started

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


T5A H250V


TP-LINK


RAIL-09
19:12:49
OEZ
LTE
B16


WOLF

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 you need to make 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
- originally developed in 1999
- payload agnostic
- publisher publishes payload on topics
- subscriber registers for topics
- topics can be structured in directory like tree
- 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

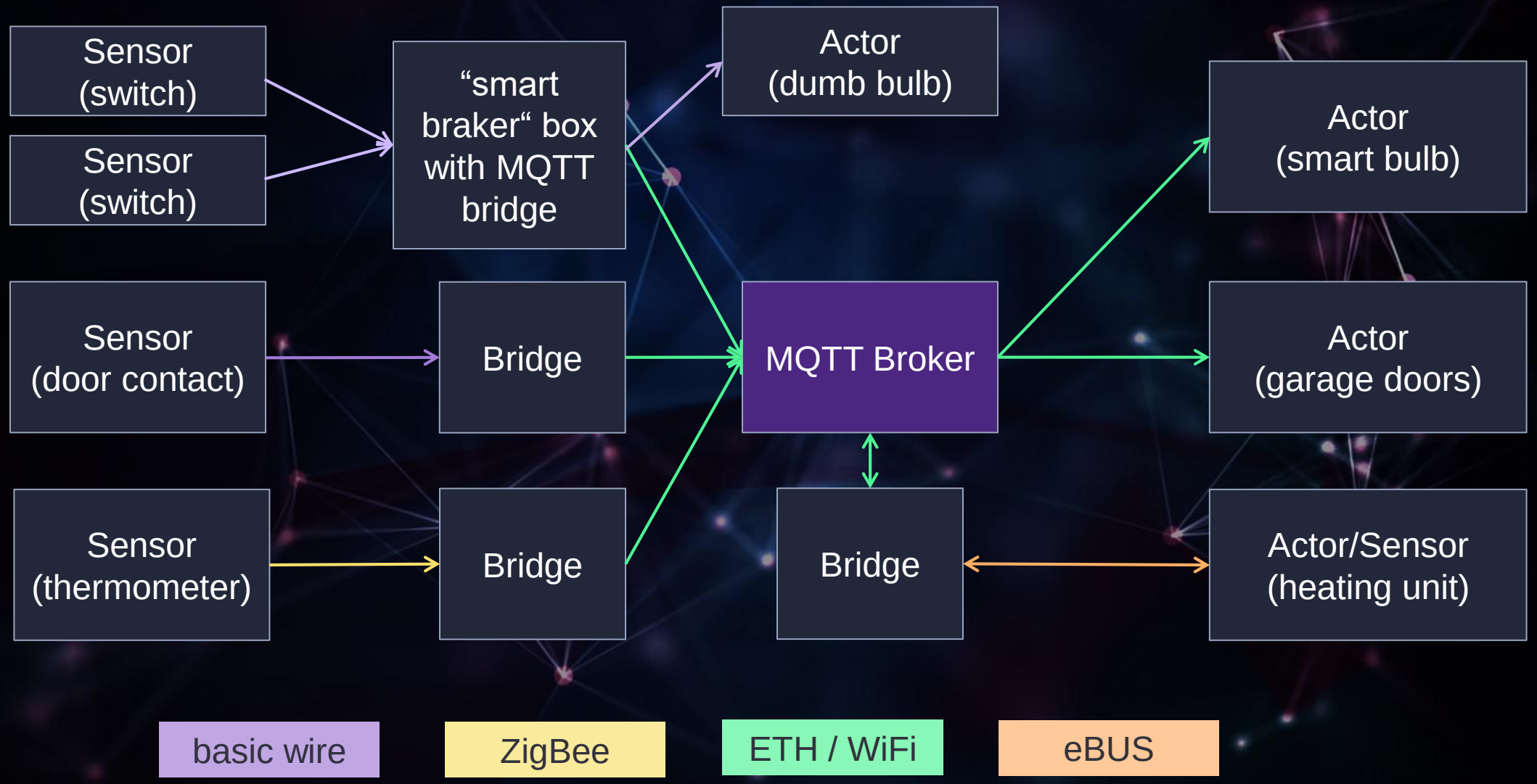
/house/basement/light

Tree like organized structure, client either publishes to the topic or subscribes. When subscribing, it 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
- MQTT namespace of topics is very convenient way of integration different devices altogether and not only devices (you can find social networks, image feeds, RSS,weather forecast and other internet services bridged to MQTT)

MQTT: 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
- Remember? You can subscribe to #
- Lazy hacker is a happy hacker ;)

Domoticz

openHAB

empowering the smart home

Home automation systems

- Similar concepts
- Provide business logic
- Provide frontend
- Work by connecting to MQTT broker and subscribing/publish to topics of devices, also work as MQTT bridge for various protocols and standards of IoT devices.

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
Stor Down	Encendido
Stor STOP	Encendido

Last Seen: 2017-10-29 09:52:12

Last Seen: 2017-10-21 13:58:45

Last Seen: 2017-10-29 09:52:30

Dispositivos Luz/Interruptor:

Xiaomi Robot Vacuum GYZ - Control	Off
Wemo	Encendido
Persiana	Stopped

Last Seen: 2017-10-09 22:45:17

Clean | Home | Spot | Pause | Stop | Find

Last Seen: 2017-11-05 00:23:26

STOP

Last Seen: 2018-01-03 08:17:16

Sensores de Temperatura:

Exterior	13.1° C / 54%
Dormitorio Infantil	20.5° C / 42%
Dormitorio	20.1° C / 42%

Normal, Punto de Rocío: 4.00° C
Last Seen: 2018-01-04 23:17:25

Confortable, Punto de Rocío: 7.15° C
Last Seen: 2018-01-04 23:17:11

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

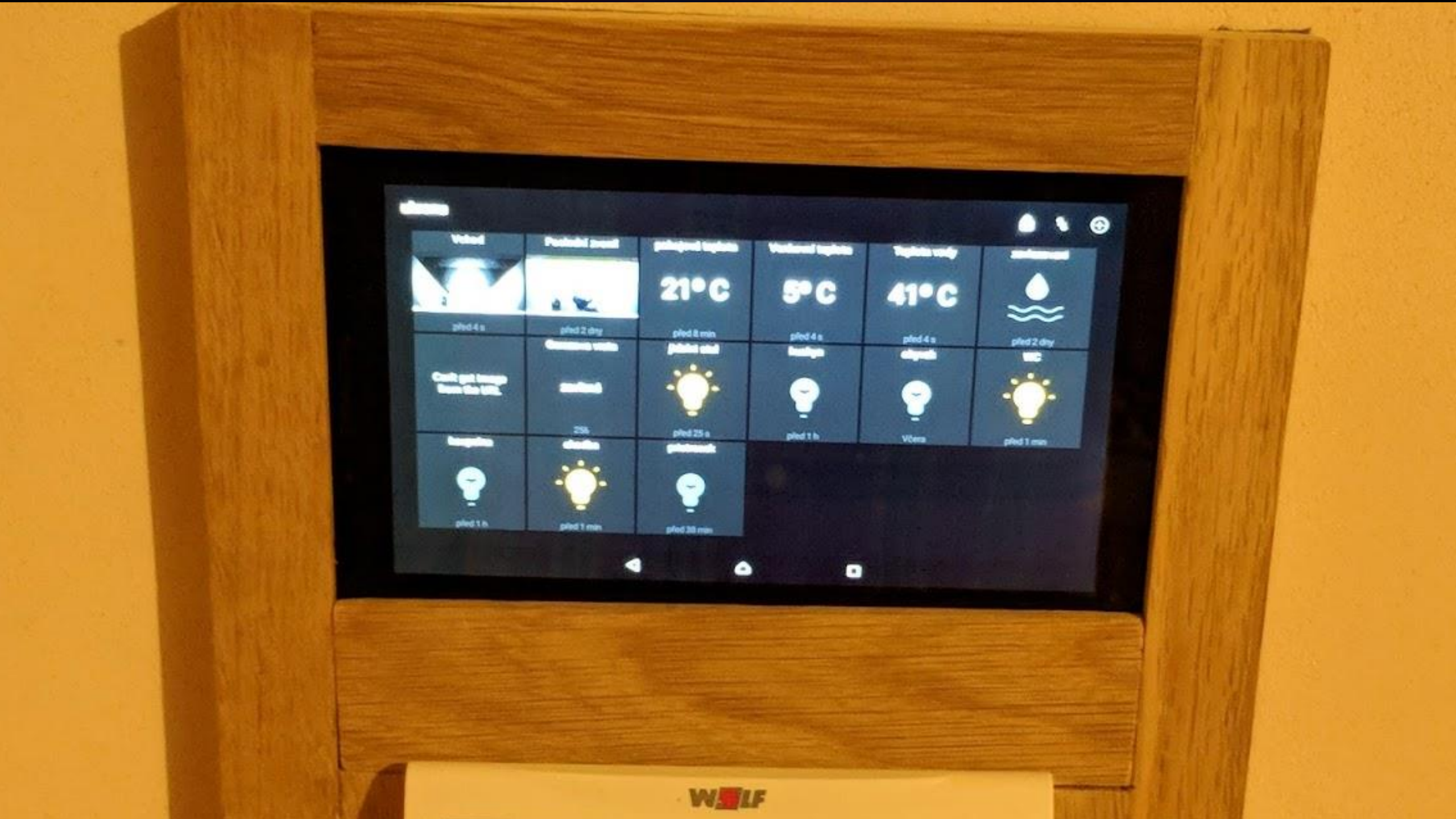
Last Seen: 2018-01-04 23:17:57

DEMO TIME

MQTT DASH

MQTT Dash

- Simple Android/IOS app
- MQTT centric, simple UI that directly reflects 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

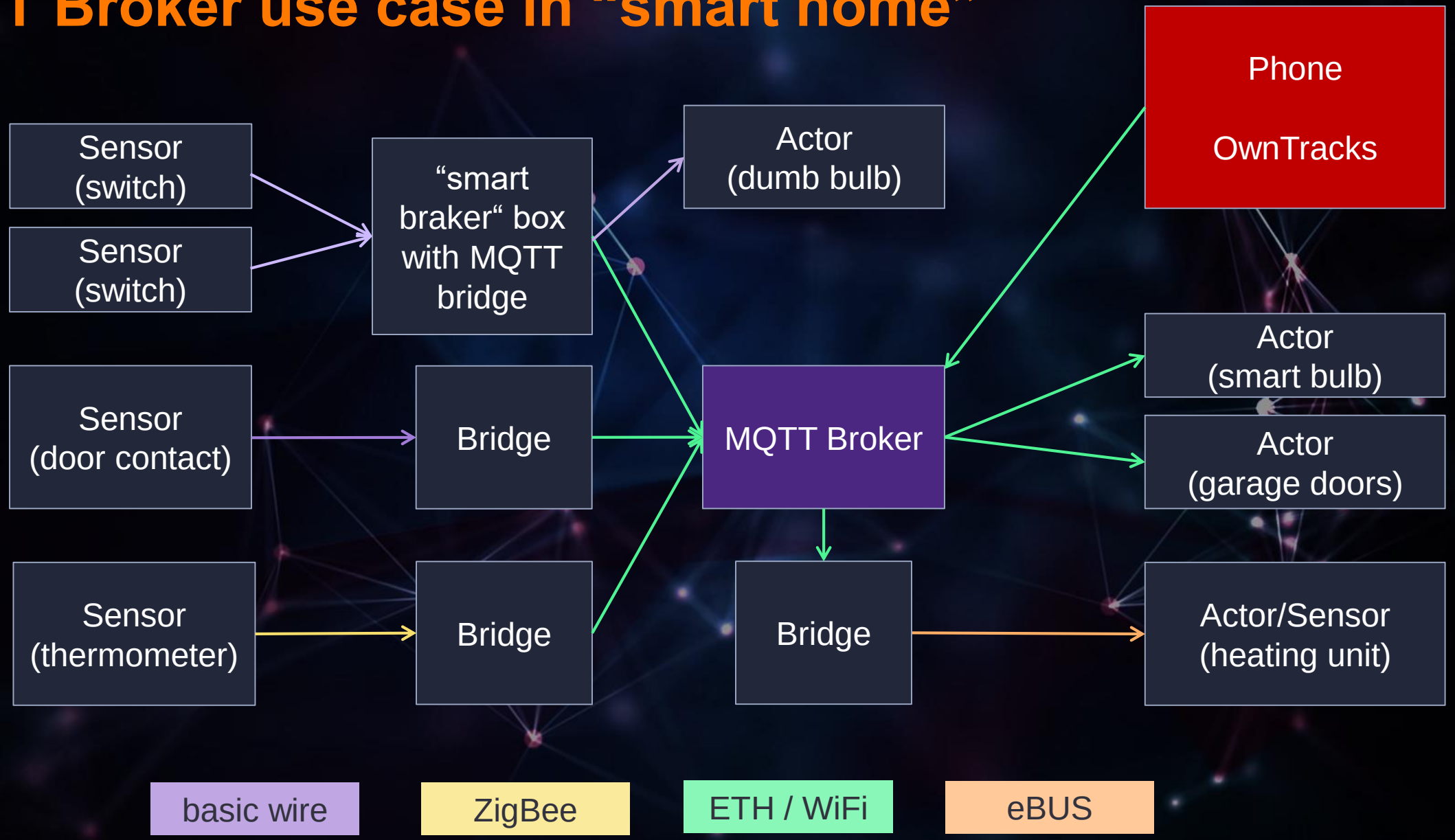
DEMO TIME

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.**

MQTT Broker use case in “smart home”



DEMO TIME

Conclusion

- Real world example how bad the situation is
- No single and simple solution
- Educate people more about security
- Let’s stick to security as an opt-out choice everywhere it is possible
- Better and faster patch adoption
- Change the way how we support devices and SW today

- These were not rocket science hacks, more to come……

Go ahead and ask!

- and I'll try to make up some answers

"Hello, could I have five minutes of your time?"

Thank You!

Martin Hron

@thinkcz

hron@avast.com

www.avast.com