



Why hack the vacuum cleaner?

tCSC on Security, Split 2022, Björn Leder



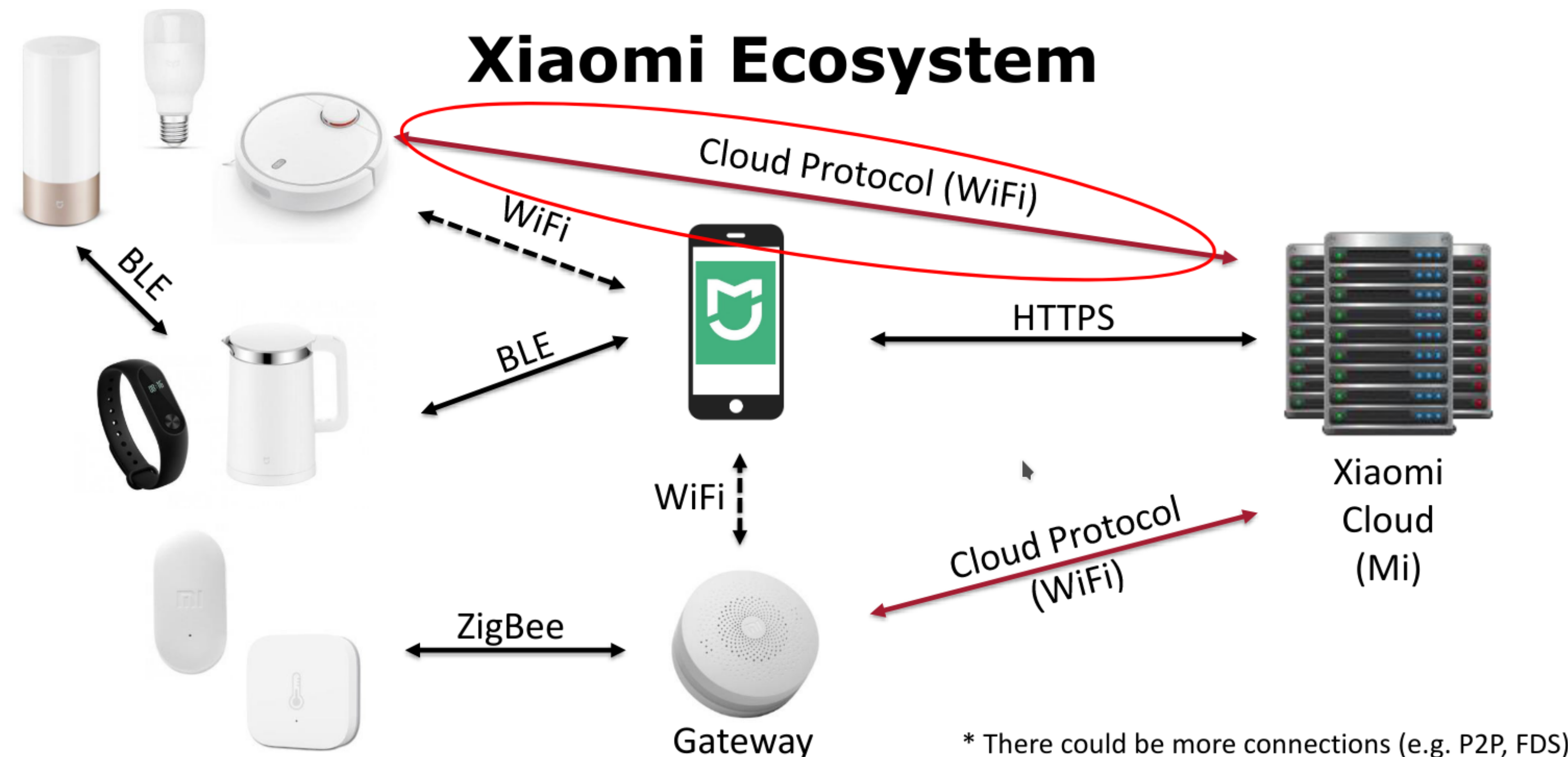
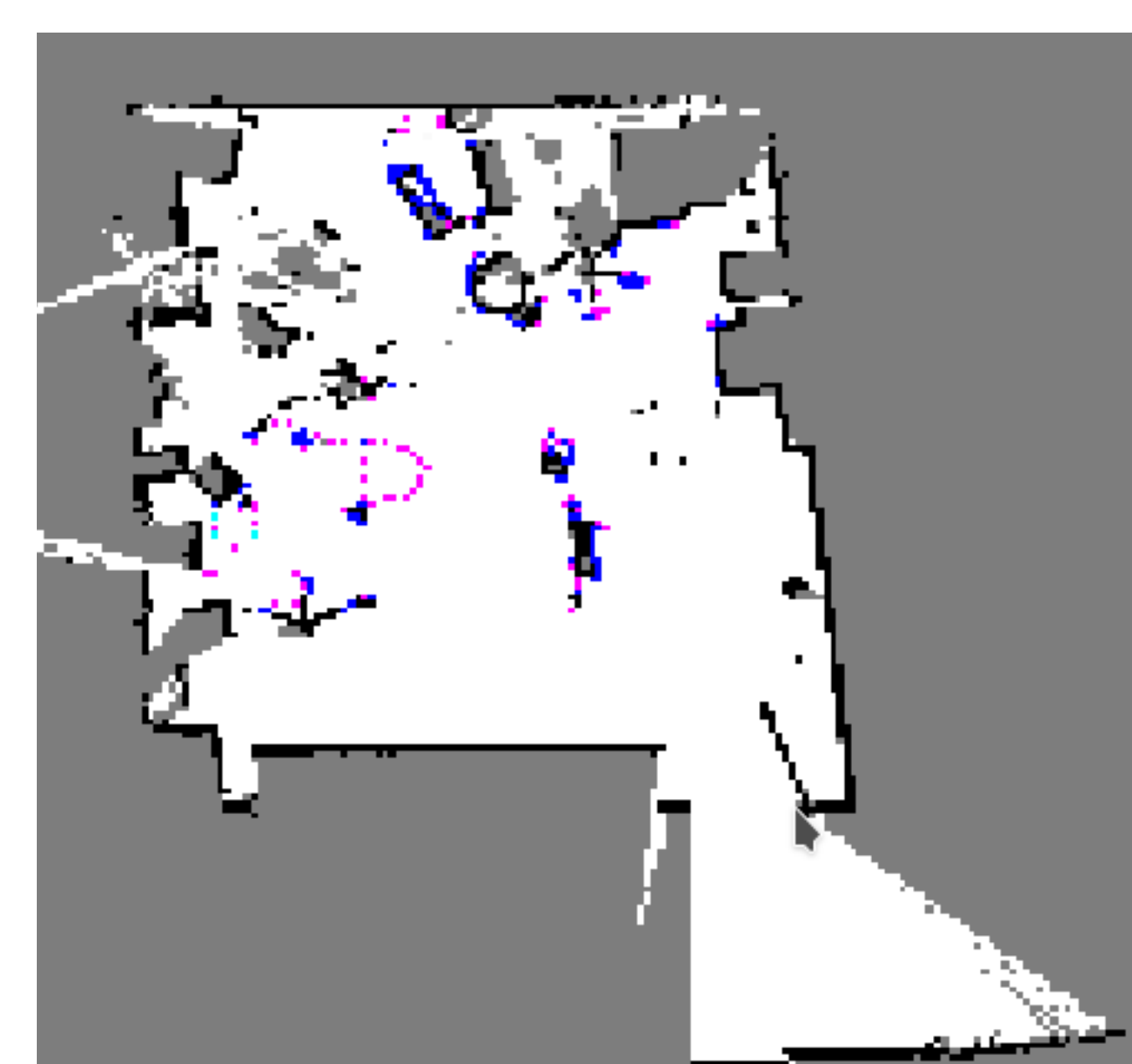
Smart Home

Consumer:  
Convenience!

Cooperation:  
Data!

# Xiaomi Roborock (2018) Robotic Vacuum Cleaner

- three processors, Ubuntu OS
- log files, maps, geo location uploaded to cloud
- OTA updates, but firmware not signed
- https, but no verification
- good: can be modified by user
- bad: attacker as well
- credit: Dennis Giese, <https://github.com/dgiese/dustcloud>



# Lets root remotely



unprovisioned state

← „Get Token“



→

← „miIO.ota“



←

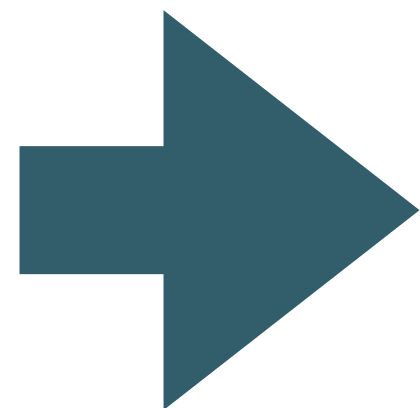


custom firmware



Webserver

```
root@rockrobo: ~  
login as: root  
Authenticating with public key "rsa-key-gami" from agent  
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.4.39 armv7l)  
  
* Documentation: https://help.ubuntu.com/  
Last login: Thu Dec 14 01:43:59 2017 from 192.168.8.67  
root@rockrobo:~# █
```



use with private cloud  
or with no cloud at all

# Plug-in Solar Power Plant



## selfPV Balkonpaket (Runde Stäbe) 370Wp - Bosswerk / Canadian

selfPV Komplettanlage inkl. Canadian 370Wp Solarmodul, Anschlusskabel und Bosswerk Modulwechselrichter MI301. Komplett mit Montagepaket zur Installation am Balkongeländer (mit **runden** Stäben).

[PDF](#) Datenblatt: Bosswerk Mikrowechselrichter MI301

[PDF](#) Datenblatt: CanadianSolar HiKu CS3L-370 370Wp

[PDF](#) selfPV Anschlussanleitung

Art.Nr.: BPVR370.BW.CSA



versandfertig in 5-8 Werktagen

~~589,- €~~

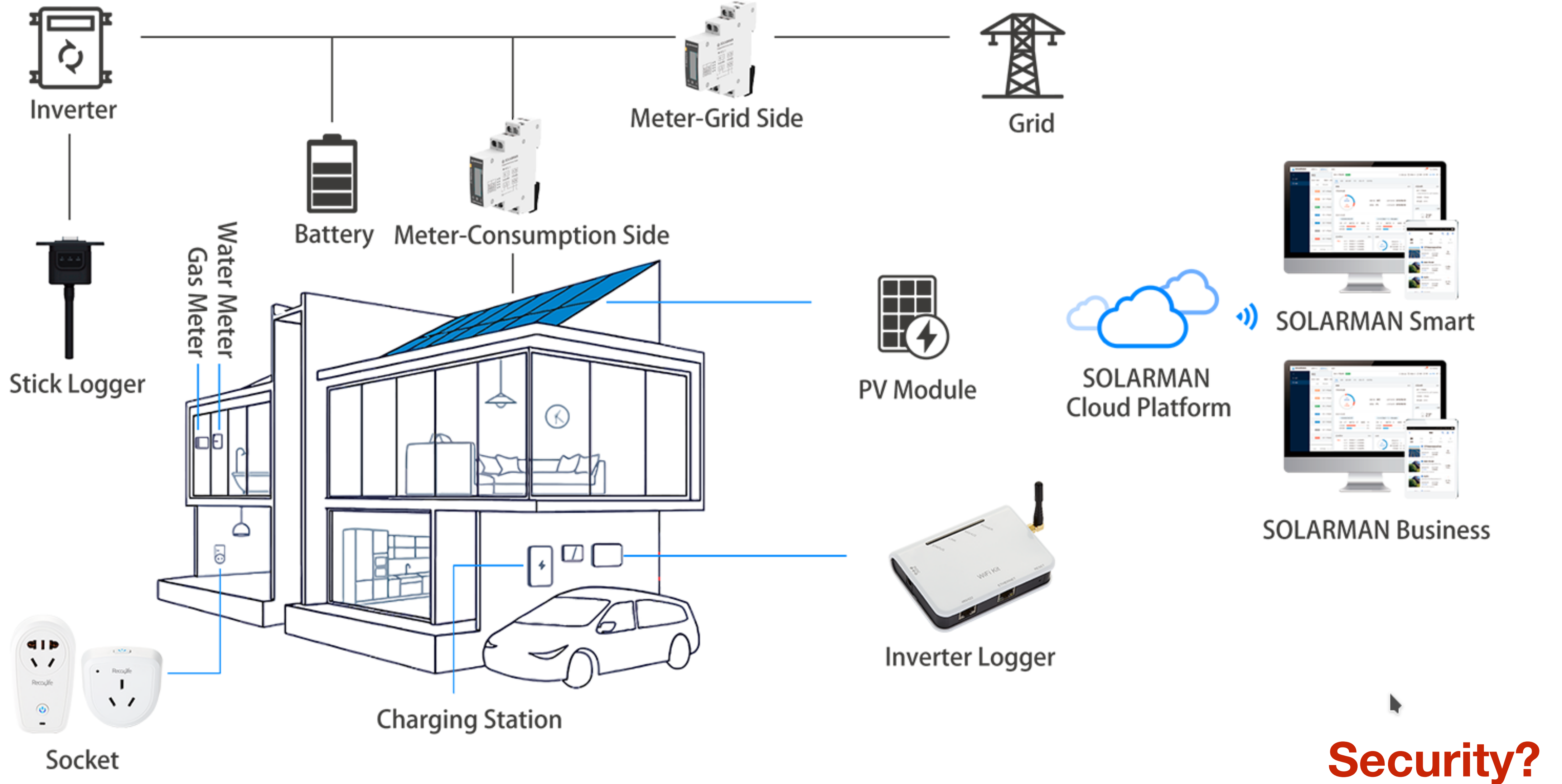
**Aktionspreis**

**531,- €**

inkl. 19 % MwSt. zzgl. **Versand**  
Paketversand 26,0 kg

- micro inverter: invert power from DC to AC (<1kWp)
- use power locally or feed in to grid
- cloud used for monitoring
- access point for setup, password is 12345678

# Solution for Household Owner



Status

Wizard

Quick Set

Advanced

Remote server

Access point

Upgrade

Restart

Reset

### Access point setting

Network mode	11bgn
Network name(SSID)	AP_4111631112
Module MAC address	2C:9C:6E:25:5D:10
Select channel	Auto-select

Save

### Security setting

#### Change the user name and password for Web server

Current user name	admin
New user name (Max.15 characters)	<input type="text"/>
Re-enter user name	<input type="text"/>
New password (Max.15 characters)	<input type="text"/>
Re-enter password	<input type="text"/>

Save

#### Change the encryption mode for AP

Encryption mode	WPA2-PSK
WPA encryption Encryption algorithm	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP/AES
Password (8 to 63 characters)	12345678

Save

### Help

In this page, you can configure the parameters of the device when it works under the access point mode.

It is recommended to change the encryption mode for AP to enhance the system security. Please remember your password. If password is forgotten, you need to Reset the device to default setting.

★Note: After changing the settings, the device must be restarted.

After restart, you will need to re-login the configuration interface. It is recommended to restart after completing all configurations.




2.897,0 MiB Memory free  
0,14 Load (15m)  
28. M... Last boot  
9,4 % Disk use (percent) /config  
Sun  
Björn

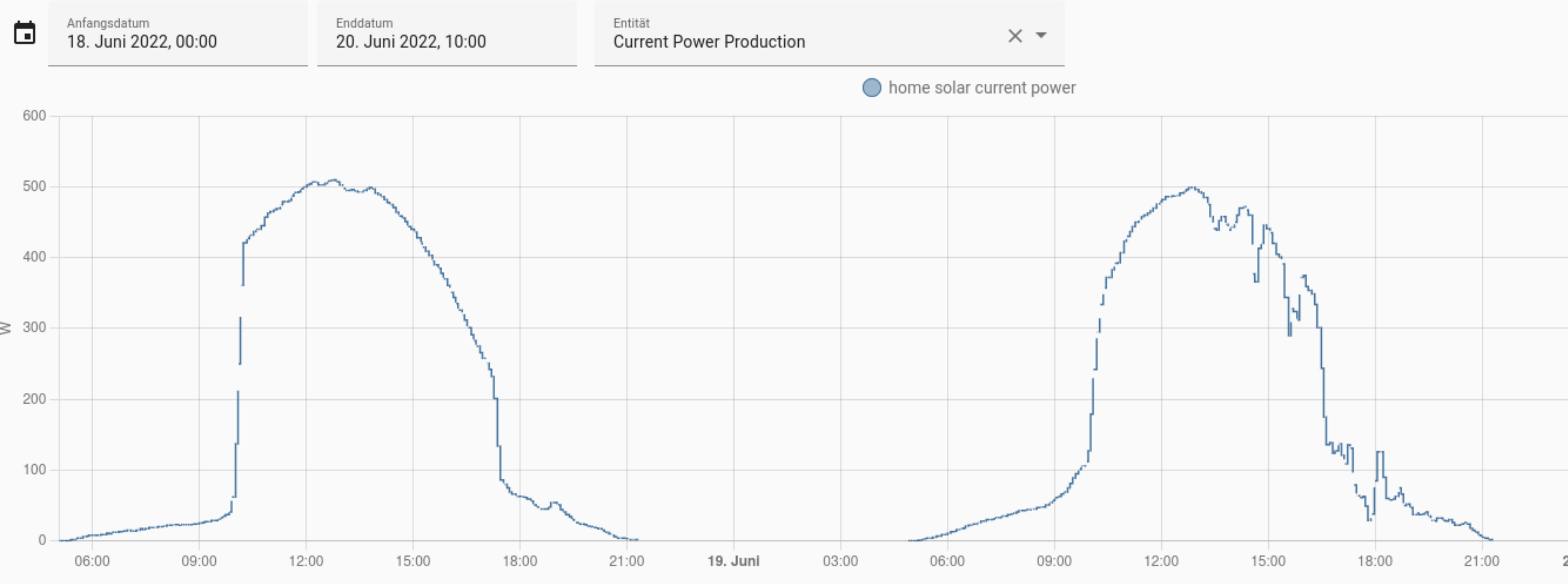
### Schalter

- Ventilator Tabea
- Schlafzimmer
- Medientechnik Wohnzimmer
- Heizung Tabea
- Beamer Wohnzimmer
- Bewässerung Eingang
- Outdoor switch
- Heizung Schlafzimmer
- Licht Decke Küche UG

### kamera



Medientechnik Wohnzimmer Aktueller Verbrauch  
Heizung Tabea Aktueller Verbrauch



# My Home Server

- Home Assistant
- MQTT
- Nextcloud, Bitwarden
- ...
- IoT devices not connected to the internet

But I don't want to run a private cloud!  
What can I do?

---

Or hack my  
fridge!

- Don't use smart devices.
- Don't use cloud, i.e. do without some functionality / convenience.
- Choose a vendor which you trust: transparency, cloud in your country, ...

Problem: what if devices can't be used w/o cloud and no alternatives?