

LICHTSTEUERUNGSAUTOMATISIERUNG

Projekt: DV-Anwendungen in der Technik

Schuller, Thiemann, Wildt

Betreuer: Prof. Dr. Franz Josef Schmitt

January 20, 2016

Hochschule Rosenheim

GRUNDLAGEN

INTERNET *of* THINGS

- Alltägliche Geräte
- Zugang zu IP-Netz
- Unterstützung des Menschen

*Das Ziel des **Internets der Dinge** ist es, die Informationslücke zwischen der realen und virtuellen Welt zu minimieren.*

– Mattern, F. (2005), Das Internet der Dinge



Seasonally Affected

@sadserver

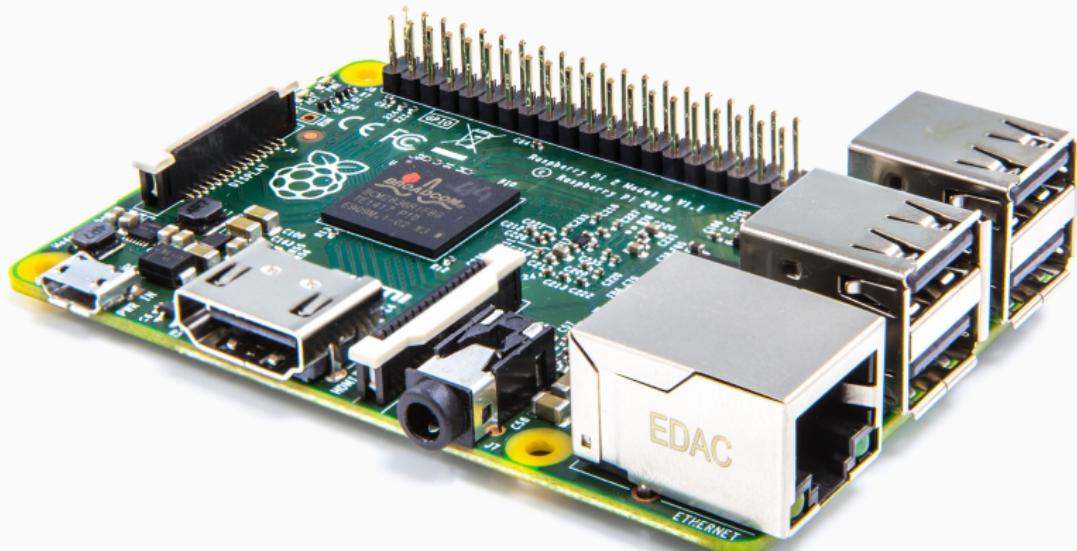
Internet of Things?

SPOILER ALERT

That's what the internet is.

HARDWARE

HARDWARE - RASPBERRY PI 2



- Universell einsetzbar
- Sehr gutes Preis/Leistungs-Verhältnis
- Umfangreicher Support durch Community
- Große Basis unterstützter Software
- Einfach in der Handhabung

HARDWARE - RASPBERRY PI 2 - SPEZIFIKATIONEN

CPU	ARM Cortex-A7
CPU-Kerne	4
CPU-Takt	900 MHz
RAM	1 GB
Stromverbrauch	max. 4 W
Preis	~40€

HARDWARE - RASPBEETM



- Sehr gute Unterstützung für RPIs
- Komplette Verwaltungssoftware
- Gute Verfügbarkeit
- Weit verbreitet

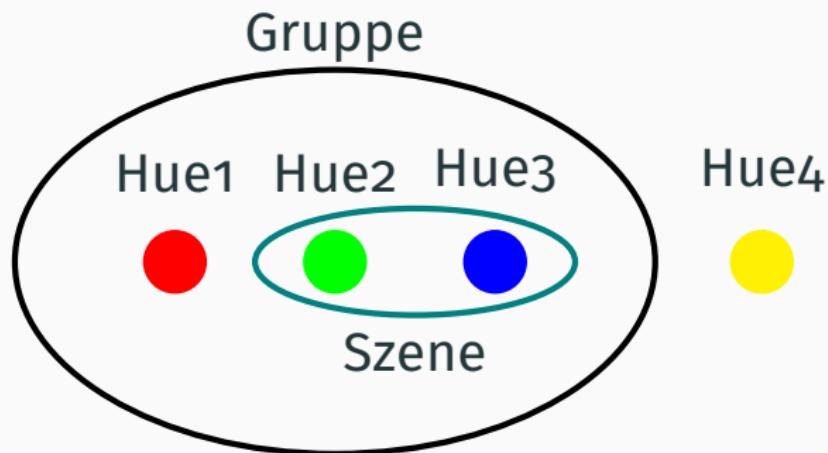
HARDWARE - HUE



- Weite Verbreitung
- Gute Erfahrungen
- Gute Qualität

HARDWARE - HUE - HUE - HUE - HUE

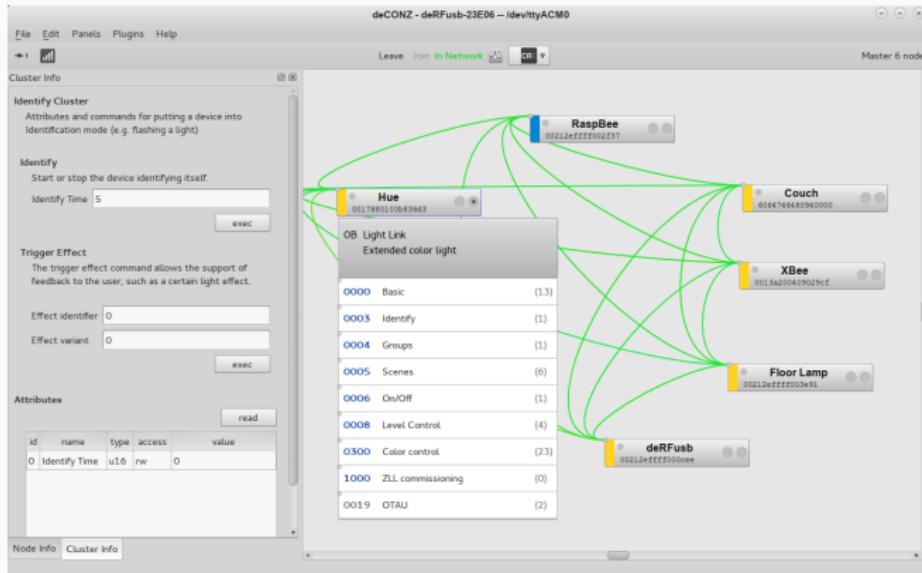
HARDWARE - HUE - ORGANISATION



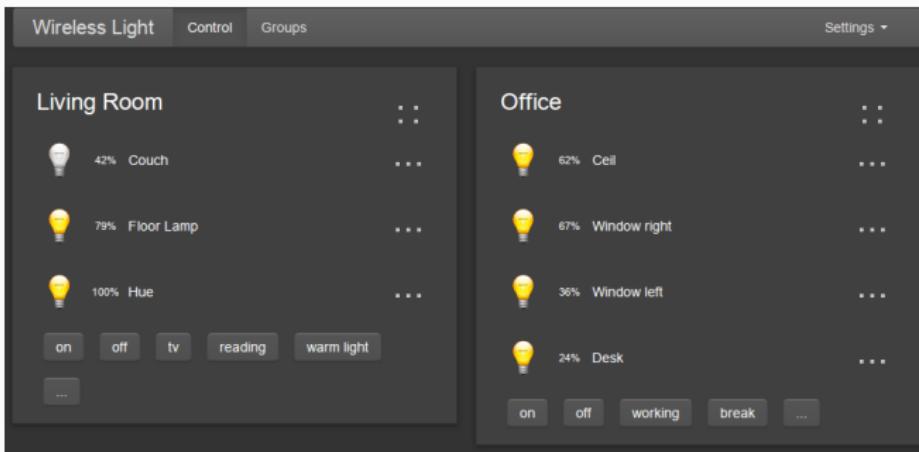
SOFTWARE

- GCFFlasher
 - Firmware-Tool für RaspBee
 - Flashen und Reset des Moduls
 - Von uns nicht verwendet
- deCONZ
 - Desktop Applikation
 - Web Applikation
 - REST API

Hardwarenahe Steuerung von ZigBee-Nodes



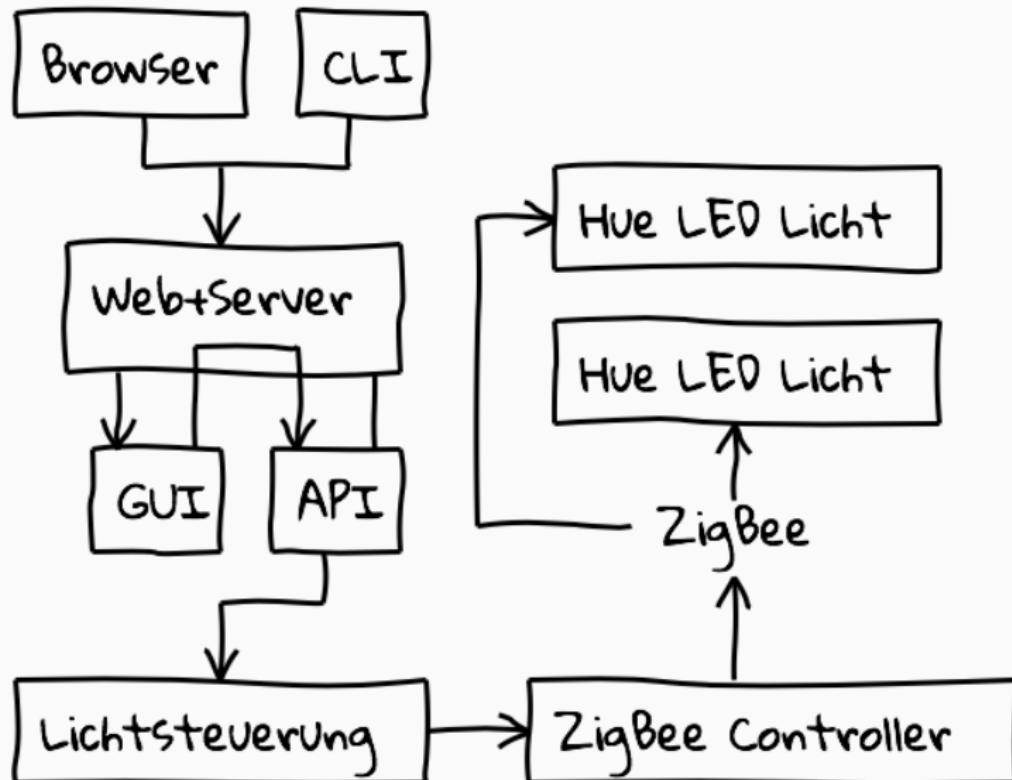
Steuerung der Beleuchtung über den Browser



unter Nutzung der REST-API

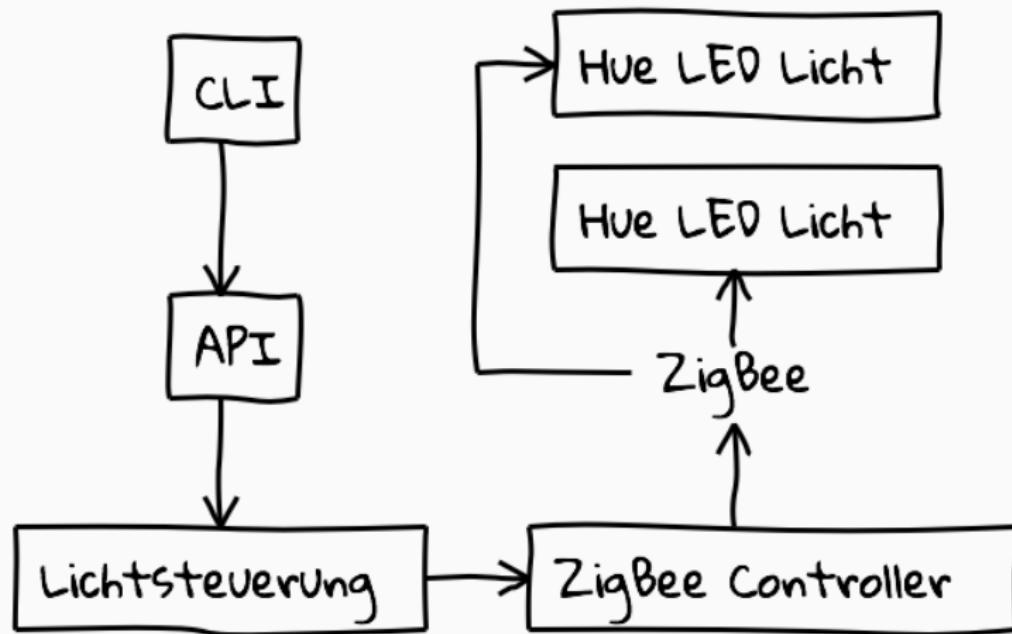
WAS WIR MACHEN WOLLTEN

PROJEKT - IDEE



WAS WIR DANN GEMACHT HABEN

PROJEKT - REALITÄT



GET-Requests: Informationsbeschaffung

<url>/<apikey>

Lichter /lights

Gruppen /groups

Szenen ↳ /<id>/scenes

für alle Lichter, Gruppen und Szenen.

GET-Requests: Informationsbeschaffung

<url>/<apikey>

Lichter /lights/<id>

Gruppen /groups/<id>

Szenen ↳ /scenes/<id>

für einzelne Lichter, Gruppen und Szenen

PUT-Requests: Datenaktualisierung

<url>/<apikey>

Lichter

/lights/<id>/state

Gruppen

/groups/<id>

Szenen

↳ /scenes/<id>

für einzelne Lichter, Gruppen und Szenen

POST-Requests: Erstellung

<url>/<apikey>

Gruppen /groups

Szenen ↫ /<id>/scenes

von Gruppen und Szenen

DELETE-Requests: Löschung

<url>/<apikey>

Gruppen /groups

Szenen ↫ /<id>/scenes

von Gruppen und Szenen

* Welcome to CityPower Grid Rerouting *

Authorised Users only!

New users MUST notify Sys/Ops.

login:

```
80/tcp      open   http          host<2>.nc
81/tcp      open
10@tcp     open
11@nmap -v -SS -O 10.2.2.2
12 Starting nmap 0. 2.54DETA25
13 Insufficient responses for TCP sequencing (3), OS detection
14 inaccurate
15 Interesting ports on 10.2.2.2:
16 (The 1539 ports scanned but not shown below are in state: c
17 Port      State    Service
18 22/tcp    open     ssh
19 No exact OS matches for host
20 Nmap run completed -- 1 IP address (1 host up) scanned
21 @ sshnuke 10.2.2.2 -rootpw="Z10H0101"
22 Connecting to 10.2.2.2:ssh... successful.
23 Attempting to exploit SSHv1 ... successful.
24 IP Resetting root password to "Z10H0101".
25 System open: Access Level <9>
26 @ ssh 10.2.2.2 -l root
27 Root@10.2.2.2's password: ■
```

EDIT11

rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
shrd ebx, adv, CL
[mobile]

[mobile]

Starting nmap 0. 2.54DETA25

Insufficient responses for TCP sequencing (3), OS detection

accurate

The 1539 ports scanned but not shown below are in state: c

Port State Service

22/tcp open ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanned

@ sshnuke 10.2.2.2 -rootpw="Z10H0101"

Connecting to 10.2.2.2:ssh... successful.

Attempting to exploit SSHv1 ... successful.

IP Resetting root password to "Z10H0101".

System open: Access Level <9>

@ ssh 10.2.2.2 -l root

Root@10.2.2.2's password: ■

RIF CONTROL

ACCESS GRANTED

48

1:50I

28

- Command-Line-Interface
- Ruby
- clamp
- rest-client
- nutzt deCONZ Rest-API

DEMO TIME!

SICHERHEITSASPEKTE

SICHERHEITSLÜCKEN IN DER LOGIK

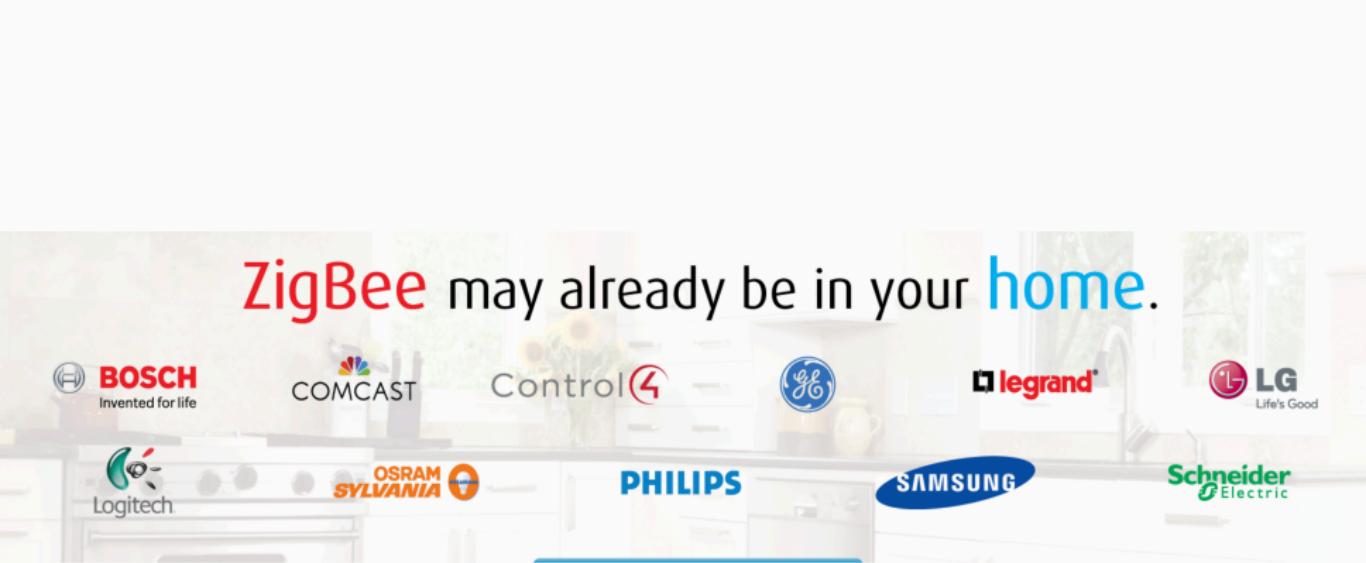
*By causing a failure condition in the 2.4 GHz radio frequency band, the security system **does not fail closed** with an assumption that an attack is underway. Instead, **the system fails open**, and the security system continues to report that "All sensors are in-tact and all doors are closed. No motion is detected."*

– Rapid7 (05.01.2016), R7-2015-23

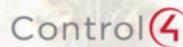
Verschlüsselung als Satire

... alle Geräte ein und dasselbe Schlüsselpaar (Fallback Key) kennen und akzeptieren müssen – und dieses asymmetrische Schlüsselpaar ist öffentlich bekannt.

– heise (21.11.2015), <http://heise.de/-3010287>



ZigBee may already be in your **home**.



<http://www.zigbee.org>



Fragen?

The \LaTeX theme *mtheme* is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.



- Internet of Things (Folie 3):
<http://brillency.com/tag/internet-of-things/>
- SPOILER ALERT (Folie 5):
<https://twitter.com/sadserver/status/621382996323536896>
- RPI2 (Folie 7):
<https://www.raspberrypi.org/blog/raspberry-pi-2-on-sale/>
- RaspBee (Folie 10):
<https://www.conrad.de/de/raspbee-1369408.html>
- Philips Hue LED Leuchte (Folie 12):
<http://www.homewizard.co.uk/phillips-hue-led-lamp-single-pack.html>
- Disaster Girl (Folie 36):
<http://knowyourmeme.com/memes/disaster-girl>