

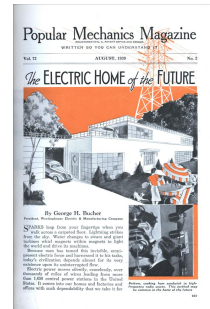
# Theoretischer Ablauf von IoT Hacking am Beispiel einer WLAN Steckdose

Thomas Höfert

18. September 2019

## Die Entwicklung hin zum Smart-Home

- 1939 die ersten Ideen zum automatischen Haus [Quelle 1]
- 1960 beginn der Störmeldesysteme
- 1973 SPS Speicherprogrammierbare Steuerung über Zentralrechner
- 1987 Entstehung des European Home System über die Stromleitung
- 1991 Gründung des EIB/KNX-Bus Standard
- 2005 Ursprung des Smart Home [Quelle 2]
- 2008 Haus V
- 2015 Smart Home für Generationen
- 2018 Wechsel in Individualsteuerungen



## Drahtgebunden ( über separate Leitung)

- KNX/EIB
- LON
- DALI
- PROFIBUS
- SPS-gesteuerte Systeme
- viele weitere . . .

## Aufmoduliert auf die Stromleitung

- KNX-PN (Powernet)
- Powerline
- digitalSTROM

### ISM-Band (Industrial, Scientific and Medical Band)

Frequenz	Bussystem
433 MHz	Proprietäre Systeme
868 MHz	EnOcean, Z-Wave, ZigBee, Homatic

### Dect (ULE)

Frequenz	Bussystem
1800 Mhz	Funktelefon, AVM, HAN FUN

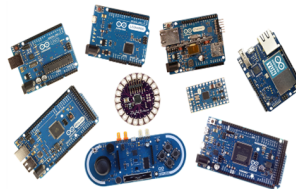
### Bluetooth

Frequenz	Bussystem
2,4GHz	Bluetooth, Bluetooth Low Energy

### W-LAN

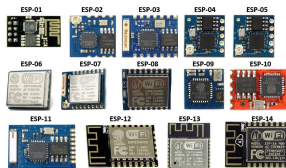
Frequenz	Bussystem
2,4 GHz	WLAN
5 GHz	WLAN
60 GHz	WirelessHD, Wireless HDMI

- Microchip (ehemals Atmel)  
Atmega (Arduino)  
Cortex-A



[Quelle 10]

- Espressif  
ESP01 (ESP8266)  
ESP12F (ESP8266)  
ESP 32



[Quelle 9]

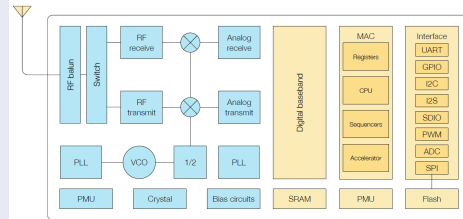
## Aufbau und Leistung des ESP8266

32-bit RISC 80MHz

512kb bis 4MB Flashspeicher

16 GPIO Pins

Unterstützt das SDK von Espressif, LUA,  
Python, JavaScript, Basic, C und viele  
weitere



- Hersteller wollen / müssen immer smarter werden
- Generationsübergreifendes wohnen soll leichter werden
- Selbstständige Installationen werden immer einfacher
- Komponenten werden günstiger

## Physische Sicherheitsmöglichkeiten

- Sicherheit durch erschwerten Zugang zum Gerät
- Schutz vor unbefugtem öffnen
- Versiegeln / Unkenntlich machen der Programmierschnittstelle

## Logische Sicherheitsmöglichkeiten

- Nutzen von proprietärer Software
- Einsetzen von Verschlüsselungen
- Kapseln des Systems

- Schutz vor unbefugtem öffnen  
Y- Triwing Schraubendreher



[Quelle 8]

- Verschlüsselung  
Vorrangig MD5 **?! [Quelle 6]**

- Kapseln des Systems



- Schutz vor unbefugtem öffnen  
Y- Triwing Schraubendreher



[Quelle 8]

- Verschlüsselung  
Vorrangig Wi-Fi [Quelle 6]



- Kapseln des Systems

## ■ Entwenden von Geräten

W-Lan Steckdose

Leuchtmittel

Thermostate

Erwerb von IoT Geräten

## ■ Zugang zur Verkabelung [Quelle 14] ,

Einbinden eigener manipulierter Module in den Bus

Einbinden von Scannern zum Mitschneiden von Kommunikation

- W-Lan Sniffing  
Mitschneiden des W-Lan Datenverkehrs
- Man-in-the-Middle-Angriff  
Auslesen und verändern der Netzwerkkommunikation
- Simulation eines IoT-Herstellers  
Erstellen eines eigenen Cloudservice Accounts
- DNS-Spoofing  
Senden von gefälschten DNS-Antworten
- Scan über Sicherheitslücken [Quelle 6]

## Physischer Zugriff

- 1 Kauf einer WLAN Steckdose
  - Über den Onlinehandel
  - Über den lokalen Baumarkt
- 2 Flashen einer eigenen Firmware
  - Z.B. mit der Arduino IDE
- 3 Zurücksenden an den Lieferant
  - Online gilt innerhalb von 14 Tagen nach §§312g Abs. 1, 355 BGB
  - Lokal im Baumarkt nur auf Kulanz










## Aktivierung des kompromittierten Gerätes

- 1 Kunde richtet das manipulierte Gerät ein
- 2 Es wird eine Verbindung zum Fake-Server hergestellt
- 3 Aufbau eines reverse Proxyserver

## Persönliche Maßnahmen um die Sicherheit zu verbessern

- Ein separates WLAN nur für die Automation erstellen  
Kapseln des Netzwerkes vom Produktivnetz
- Möglichst Kabelgebundene Systeme nutzen  
Verringerung der Angriffsfläche durch Medienreduzierung
- Nur aus vertrauenswürdigen Quellen kaufen  
Keine Bestellungen aus Fernost  
Nur bei namhaften Shops bestellen oder vom Fachmarkt
- Günstige Geräte für den Eigenbedarf anpassen  
Flashen von eigener Firmware z.B.  
ESPEasy<sup>[Quelle 11]</sup>, Tasmota<sup>[Quelle 12]</sup>, ESPurna<sup>[Quelle 13]</sup>,
- Nutzen einer Firewall

## Quellen

-  <https://bit.ly/2PDmPgF> , The Electric Home of the Future (Aug, 1939) , *Modern Mechanix* , Online; Stand 15. Mai 2008
-  <http://bit.ly/2lYQIZL> , Die Historie des Smart Home (Nov, 2016) , *Modern Mechanix* , Online; Stand November 2016
-  <http://bit.ly/2keFobp> , Smart Home - Smart Hack (Dez, 2018) , *Michael Steigerwald* , Online; Stand Dezember 2018
-  <http://bit.ly/2kLaAiQ> , GLÄSERNER KUNDE (Jul, 2019) *Katharina Nocun* , Online; Stand Juli 2019
-  <http://bit.ly/2kKlrJR> , Tuya Inc. (Sep, 2019), Online; Stand September 2019
-  <http://bit.ly/2lVpF1k> , Shodan (Sep, 2019), Online; Stand September 2019
-  <http://bit.ly/2mluaTr> , InfoSec Handlers Diary Blog (Dez, 2008), Online; Stand 30. Dezember 2008
-  <http://bit.ly/2lYePHT> , wikipedia.org (Sep, 2019), Online; Stand September 2019
-  <http://bit.ly/2lTF6r7> , MicroControllerLab (Mai, 2019), Online; Stand Mai 2019
-  <http://bit.ly/2meKrsZ> , elprocus (Sep, 2019), Online; Stand September 2019

# Quellen



<http://bit.ly/2lZFGmX> , letscontrolit.com (Sep, 2019), Online; Stand September 2019



<http://bit.ly/2kNNLLq> , Sonoff-Tasmota (Sep, 2019), Online; Stand September 2019



<http://bit.ly/2kgn0im> , EPurna (Sep, 2019), Online; Stand September 2019



<http://bit.ly/2klTpnM> , Antago GmbH (Sep, 2019), Online; Stand September 2019