

Smart Home

A Secure Design and Implementation

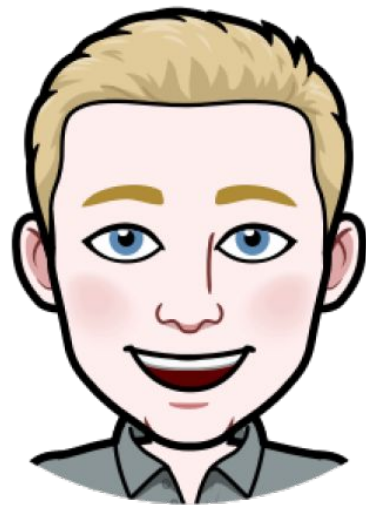
Owen Parkins

Contents

- Who am I?
- Why build a smart home?
- Different designs
- Building your own smart home

whoami

- Graduate student
 - New Mexico Institute of Mining and Technology
 - CyberCorp Scholarship for Service Recipient
 - Computer Science with “focus” in Cybersecurity
 - Graduate May 2020
- Current projects
 - Smart home (@themattvirus)
 - UHF RFID Spoofer
 - Ansible Ignition Scripts (@_johnhammond)
 - github.com/oparkins



Why Would You Build a Smart Home

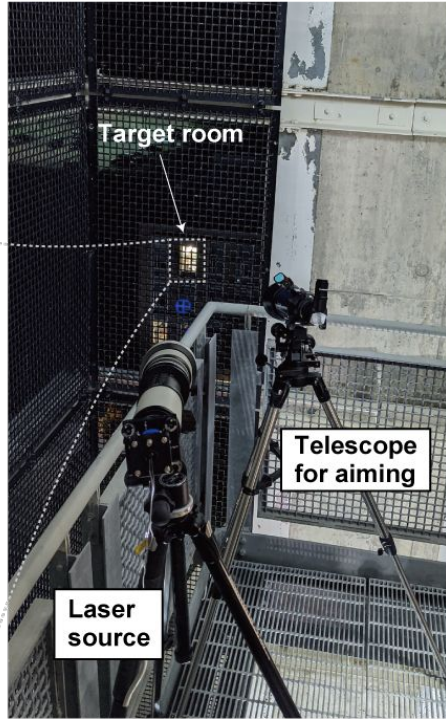
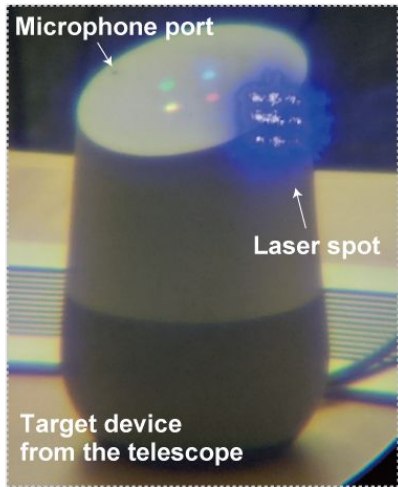
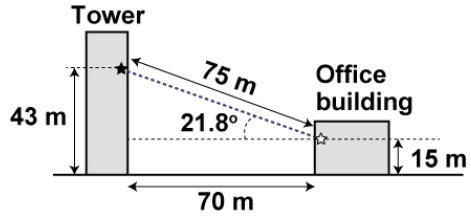
- Because you like
 - Experimenting with technology
 - Convenience
 - Automation
 - Save energy
 - Living dangerously
 - Unauthorized charges on credit cards
 - Guests controlling your house
 - Having people spy on you
 - Amazon/Apple/Google using human transcribers

The Typical Smart Home Design

- Buy within a brand
 - Nest/Google
 - Amazon Echo
 - Samsung SmartThings
- No security
 - Devices are just on the wireless network
 - Possible security through obscurity
- Dependent on Internet
 - Connects to the mothership
- Voice commands are encouraged
 - Identification is poor, no authentication
 - Light Commands

Down the Rabbit Hole - Light Commands

- “modulating the amplitude of laser light to produce an acoustic pressure wave”
 - MEMS microphone devices
 - Micro-electromechanical systems
 - Amazon Echo, Apple’s Siri, Google Home, and more
 - Identification/Authentication is useless
- Able to be applied from various distances
 - Some devices are vulnerable from 110+ meters
- lightcommands.com
- Keep your devices away from the windows



A Smarter Smart Home Design

- Custom Firmware
 - Tasmota
 - Designed for ESP8266 chips
 - Open Source
 - Most likely not calling to China
 - Allows control via MQTT, HTTP, Serial and KNX
 - github.com/arendst/Tasmota
- Use personal, on-site servers
 - Home Assistant (Hass)
 - MQTT service
- Not the “smartest”, just “smarter”
 - Still increasing attack surface from a dumb house
 - No audit completed on Tasmota
 - No hardware audits

Home Assistant (Hass)

- Open source
- Local home automation
- Interfaces with many devices
- All available without internet connection

Home

Updater Owen Parkins AWAY ophone HOME OPhone Sun

Living Room

- Living Room Lights


Outdoors

- Garage Front Light
- Outdoor Front Lights






Automation

- Outdoor Lights Mirror
- Ghost Mode (Lights On)
- Outside Lights Auto Off
- Proximity Lights On
- Ghost Mode (Lights Off)
- Proximity Lights Off

Partly cloudy Home

 **57.6°F**

Air pressure: 1019.2 inHg
Humidity: 24 %
Wind speed: 4.7 mi/h (S)

Sun 12 PM	Mon 12 PM	Tue 12 PM	Wed 12 PM	Thu 12 PM
 64.8 °F	 54.7 °F			

OP



MQTT Protocol

- MQ Telemetry Transport
- Simple protocol
 - Useful for IoT devices
 - Publish/subscribe model
- Supports authentication
- Does not support encryption
 - But can be used with TLS
- Different implementations
 - Eclipse Mosquitto
 - Emitter
 - HiveMQ
 - RabbitMQ (with plugin)



Network Setup

- Docker containers
 - macvlan
 - Assigns MAC address to each container
 - Allows for more auditability for network traffic
 - Does not allow for host <-> container communication
 - Host network
 - Simple
 - Possible port collisions
 - docker-compose
 - Maintains the containers
 - Allows for easy multiple network setup
 - macvlan
 - Internal host network
 - Updates are easier
 - Setup and transfer of containers to another system

Network Setup Continued

- External services provided
 - Port forwarding Hass
 - LetsEncrypt with nginx reverse proxy
 - Allows for managing the home remotely
 - Be sure to use SplitDNS

Smart Home Features

- All available without internet
- Able to add custom automations
 - Ghost mode
 - Semi-randomly turn on/off indoor lights at night
 - Location detection
 - Turn on outdoor lights when I arrive after dark
 - Outdoor Lights are mirrored
 - Door and Garage lights will turn on/off at same time
- Secure for my current threat statement
 - HTTP Basic Auth for Tasmota
 - No TLS for internal devices
 - Not low hanging fruit for malicious actors



Smart switches installed inside the home.



Using a smart relay to control garage light.



Sketchy wiring was already there.



Using a smart relay to control garage light.



The separation between the front door and the garage. Using the switch and relay together allows the front yard to be illuminated more evenly.



The ~~guest~~ server room current status after a boot issue fix.

Planned Network Setup

- Separated networks
 - WPA2-Enterprise for people
 - WPA2 for IoT
 - No internet access or only internet access
- More devices
 - Light switches
 - Door sensors
 - Cameras with Zoneminder
- Snips
 - Voice Processing
 - “Private by Design” ~ snips.ai
 - All on device processing
 - Interact with Hass

Problems with the Smart Home

- When internet goes out, the devices all broadcast something
 - All Google Home devices create a network
 - Don't exactly know what the Tasmota devices do
 - Doesn't create network
- MQTT devices do not reconnect
 - When Mosquitto gets reset
- Location detection
 - Either battery drains quickly or location doesn't update enough

Smart Home Future Work

- Z-Wave/Zigbee Mesh Networks
 - Z-Wave
 - Less interference due to lower frequencies
 - Maximum of 232 devices
 - Zigbee
 - Higher frequencies (Wifi/Microwave/etc interference)
 - Maximum of 2,500 devices
- Compile custom firmware
 - Add builtin SSL verification
- Use Google Location Services
 - They already have the information, why shouldn't I use it?
- Project Connected Home over IP
 - [Connectedhomeip.com](https://connectedhomeip.com)
 - Announced Dec. 18, 2019

A Present For You!

- Want a starting place?
 - Ansible Scripts
 - github.com/oparkins/smarthome
- Very basic at the moment
 - But will be filled out when I move
 - Pull requests welcome

Resources

- Zigbee/Z-Wave Intro
 - <https://www.pcmag.com/article/327457/what-is-a-smart-home-hub-and-do-you-need-one>
- Siri/Human Transcribers
 - <https://nakedsecurity.sophos.com/2019/08/30/apple-apologizes-for-humans-listening-to-siri-clips-changes-policy/>
- Light Commands
 - <https://thehackernews.com/2019/11/hacking-voice-assistant-laser.html>
 - <https://lightcommands.com>
- MQTT Protocol
 - <https://mqtt.org>
- Tasmota
 - <https://github.com/arendst/Tasmota/>
- Home Assistant (Hass)
 - <https://www.home-assistant.io/>
- Kernelcon Hardware Hacking (@themattvirus)
 - <http://hackspace.io/projects/projects-smartplugs/>