Honey, Please Don’t Burn Down Your Office:

Further Adventures in Smart Office Automation

Ed Skoudis

SANS Pen Test HackFest
November 13, 2017
Previously...

- In 2009, I built a steam punk office for Counter Hack imperial Headquarters (CHC iHQ)
- I always wanted my office to feel alive… like Tony Stark’s J.A.R.V.I.S
- In 2016, I started with a handful of IoT devices
- It grew into an IoT testbed, a development platform, a weekend dance club, and a way for me to keep my skills sharp
Some Office Artifacts (Deployed pre-2017)

- Morse Code Key 1861
- Atwater-Kent Model 80 Radio 1932
- Atwater-Kent Model 10 Radio 1924
- Burns Speaker 1925
- Westinghouse Fan 1938
- Model Train Engine 2012
- Mesmer Tube 2015
- Philips Hue Bulbs 2016
- Lutron Caseta Shades 2016
New Office Stuff
(in Past 12 Months)

- Mini 3D Printed TV
  - 2016

- Zenith Porthole TV
  - 1951
  - 2016

- Flashing Fedora
  - 2014
  - 2017

- Nest Thermostat
  - 2017

- Tesla Raygun
  - 2017

- Birthday Bear
  - 2017

- Monster
  - 2009
  - 2017

- CHiP
  - 2017

- Geissler Tubes
  - 1911
  - 2017
Me

Amazon Cloud

Turn Good Morning on
Me

Amazon Cloud

Turn Good Morning on

(((BLE)))

(((ZigBee)))

(((Wi-Fi)))

(((Wi-Fi)))

(((Wi-Fi)))

(((Wi-Fi)))

(((Wi-Fi)))
Office Architecture 2016

- **iOS**: Siri, iCloud, HomeKit DB, Control
- **Philips Hue**: On/Off/Status/Color, ((ZigBee))
- **Lutron Caseta**: Control, Open/Close Blinds, ((ZigBee))
- **MyTouchHome App**: Define Scenes, Control
- **OpenSSH**
- **GNU Bash**: Control
- **ZigBee**
- **Wi-Fi**: On/Off/Status/Color
- **Wemo**: Open/Close Blinds, On/Off/Status
- **Pandora**: Control
• Siri was stealing my words!
  – “Speaker” → “Atwater”
  – “Volume,” “Frankie Valli,” “Motown,” “Vitamin String Quartet”… and then…
  – “FRANK SINATRA”

• We needed a change… Amazon’s Echo and Alexa seemed very interesting and developer friendly

• Skills require that you have a web service on the Internet that controls things… that scared me

• Then, I discovered Project Fauxmo
Alexa Skills versus Alexa Wemo

- **My Office**
  - **Echo**
  - **Amazon Cloud**
  - **Internet-Accessible Web Server**
    - *My own, IoT Provider’s, or Amazon Lamda*

- **Me**
  - **Turn lights on**

- **Amazon Cloud**

- **Alexa Wemo**
  - **Echo**
  - **Amazon Cloud**
  - **Turn Tesla Raygun on**

- **Me**

*Image of a smart plug with 'belkin' on it connected to a Tesla Raygun.*
Fauxmo

- Fauxmo is simply a software implementation of the Wemo protocol
- “Turn X on/off” runs a command on a Pi or NUC
- The HTTPS call to activate something goes from Echo to NUC, all in my office
- Feels a lot safer to me
Simplifying Alexification

• I had a Pi with a bunch of code that I wrote in Python and Bash, which Siri could call
  - It occurred to me that I didn’t need to re-write all my code for Alexa!
    - I wrote an HTTPS/PHP/Apache wrapper around all my Siri-related code, so that Fauxmo could call it
    - It’s like having two different GUIs with the same back-end
• Alexa is MUCH better at voice recognition than Siri
  - I am limited, though, with Fauxmo’s On/Off syntax
NUC vs. Pi

- Both are solid, small, low-cost platforms
- NUC is best for performance-oriented things
  - Constantly running services
  - Cron jobs
- Pi is best for GPIO-initiated tasks
  - Often kicked off by NUC
  - ssh for the win!
- The two work together remarkably well
Tesla Raygun

- Christmas present from my wife
- Strattman Design
- Controlled via Wemo
- Looks really cool!
- Sounds pretty neat too!
- I wemo’ed it, naturally
Animatronics

- Birthday Bear – For my birthday at SANSFIRE 2017, my wife and kids sent me this furry friend
- Monster – my family bought it for me in 2009
- Simple relay hooked up to GPIO of Pi... it essentially makes a connection for the wires in the bear or monster’s foot
- They are fun and make the office feel more alive
CHiP, Our Robot Dog

- In 2009, I looked at getting a Sony AIBO robot dog
  - But… $2k and limited features
  - I waited…

- In 2016, Wowwee released CHiP
  - And there’s now a Chocolate CHiP
  - I’m in…
  - But no SDK or Python library…YET!
  - So I wrote a Python script to replay all commands from previous toy (MiP) until I found one that worked
Geissler Tubes

• High-voltage gas tubes, invented in 1857 by Heinrich Geissler
• Fancy glass, pretty colors, 3kV
• I have 22 tubes, from 1910 to 1911
• I’ve always wanted to have a set that was always ready to power on SAFELY
• Switching 3kV was impractical, so I got 4 power supplies
Mr. Tesla's High-Voltage A/C Circuit in Use

DANGER

Kindly Do Not Touch
GoodMorning.sh

- Blinds Up
- Lights On
- Little musical prelude – sounds like NPR or BBC
- Small light color show
- Sense who is in office and say “Good Morning” followed by names (random order, with “and” between last two), followed by cheery randomly selected greeting
- Today’s Date (Dynamically send recorded voice to Alexa and get response)
- Today’s Weather
- Today in History
- Close with an encouraging or silly saying, randomly selected
Amazon Voice Service

- High-quality free cloud voice synthesis
  - You don’t need an Echo -- Just sign up as a developer
  - Use bash to build JSON and then send via cURL
- The magic of “Simon Says”
  - Use Audacity to record my voice in 16kHz .mp3
  - I send to AVS and get back a 44kHz .wav file
- I wrote audio converter code to do it en masse
- Ask for the date, weather, history…

```bash
metadata.json
{
  "messageHeader": {},
  "messageBody": {
    "profile": "alexa-close-talk",
    "locale": "en-us",
    "format": "audio/L16; rate=16000; channels=1"
  }
}
```

```bash
request.sh

TOKEN="Atza:IQEBljAsAhR...

curl -i \n-H "Authorization: Bearer ${{TOKEN}}" \n-F "metadata=<metadata.json;type=application/json; charset=UTF-8" \n-F "audio=<hello.wav;type=audio/L16; rate=16000; channels=1" \n-o response.txt \nhttps://access-alexa-na.amazon.com/v1/avs/speechrecognizer/recognize
```

https://miguelmota.com/blog/alexa-voice-service-with-curl/
Sensing Who’s In The Office

• I’ve always wanted the office to have a sense of who is in it, but without being creepy
• I came up with a really simple way to do it
• Tcpdump running for 600 seconds sniffing Wi-Fi, writing into alternating files
• Then grep for phone MAC addresses, choosing voice files with names in random order
Strange Little Hacks

• Synchronizing the blinds
• Dealing with Fauxmo 90-ish device limit
• Phue library requiring contiguous device numbers
• Amazon Voice Remote – Limit of One???
• The mess of Raspberry Pi audio drivers
Staying Sharp

• Code (pretty much) every day
  – “But I don’t know how to code”
  – If you code every day, that problem kinda goes away

• Pick a project that will interest you – FUN!

• Do Python… it’s very portable and has so many useful modules and tutorials
  – http://www.diveintopython3.net - FREE!

• I code between 5 min and 14 hours per day, every day
  – Even two all-nighters in the past 18 months
  – It’s been immensely helpful for my understanding and career
Be Purposeful

- Schedule time with yourself at least weekly to work on technical stuff, deep and hands-on
  - 2 hours per week, on a Saturday or Sunday, perhaps
  - Put on your favorite music
  - DJ Sk0d0 and his side-kick Snoop CHiPpy CHiP absolutely rock Club Counter Hack
- Brainstorm with friends for projects
- CtFs at: www.amanhardikar.com/mindmaps/Practice.html
Secure It As You Build It

• It is SUPER tempting to say “I’ll just make it work now… I’ll secure it later…”
• There is NO LATER
• You never will get back to it
• No matter how disciplined you are, make it work now and secure it NOW

Green Jelly’s Three Little Pigs: For Security, Be the Third Pig!
Your Ideas?

• I’d love to hear your suggestions
• I’ve got some things I still want to tackle
  – CHiP’s BLE interface
  – CHiP’s RF interface
  – Laser show… with DMX control from Python! Sounds fun
• Any ideas?
Conclusions

• Build a lab… have fun!
• The IoT space is in its infancy and gosh, it’s fun
• Building your skills with these technologies is exciting and fun
• Web, cloud, networking, embedded, wireless, crypto, host security, coding, packets, and more! It’s all there, folks!
• Let’s get hacking!!!
• We have been granted unprecedented, behind-the-scenes access to the history and peoples of the North Pole
• An epic battle to save the North Pole itself from destruction
• Thank you, Santa, for sharing this with us so we can share it with the info security community!
• Launches approximately December 10, 2017
• COMPLETELY FREE
• www.holidayhackchallenge.com