
INTERNET OF THINGS, VOICE CONTROL, AI, & OFFICE AUTOMATION
BUILDING YOUR VERY OWN
J.A.R.V.I.S.
BY ED SKOUDIS
2016 SECURE DELAWARE WORKSHOP
Barranquilla, Colombia
Date 3/29/13 1:00 PM
32°C
Partly Cloudy
Chance of Rain: 10%
Visibility: 10.0 km
Wind Direction: 29 km/h (NE)
Sunrise: 5:58 AM
Sunset: 6:10 PM
Tomorrow
Mar, 30
33° / 26°
Partly Cloudy
Sunday
Mar, 31
33° / 27°
Partly Cloudy
Monday
Apr, 1
32° / 27°
Partly Cloudy
Tuesday
Apr, 2
33° / 26°
Partly Cloudy
Wednesday
Apr, 3
33° / 26°
Partly Cloudy
Thursday
Apr, 4
32° / 27°
Partly Cloudy
Friday
Apr, 5
32° / 26°
Partly Cloudy
Friday
March
29
Total: 82 G
Avaliable: 3 G
Total: 153 G
Avaliable: 3 G
22 Waste Status
56.5 MB
System
Uptime: 0d 3h 32 min
Email empty
Graphic Apps:
3d's Max
Control Panel
mem: 80%
cpu: 53%
0:00
Winamp Circles
190.255.231.233

$ whoami

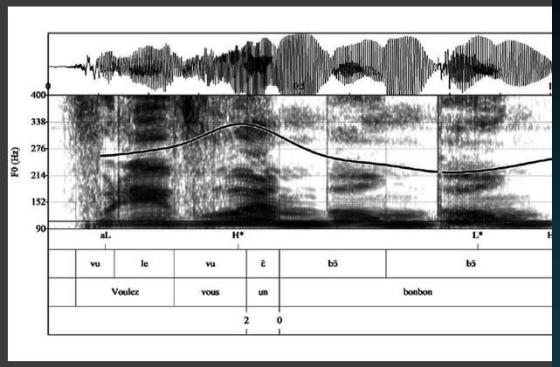

TWEETS
9,876
FOLLOWING
165
Tweets
Tweets &
edskoudis
@edskoudis
Computer security geek. Pen Tests & Incident Handling. Father.
NJ USA
counterhack.com
Joined August 2008
895 Photos and videos
edskoudis @edsk
Yes! I show in m
other voice stuf

You Remember J.A.R.V.I.S., Right?

Wouldn't It Be Cool...

- To have a voice-activated digital assistant that controls stuff throughout your office?
  - No… not just music or data like Siri, Alexa, Cortana, or OK Google, but something that controls *physical* devices?

- Many practical uses
  - Good morning – turn on lights, music, etc.
  - Good night



- Lotsa fun stuff too
  - Scenes with integrated light show and music
  - A development platform to experiment with new technologies

Start with Some IoT Equipment

- Philips Hue bulbs and light strips
  - Colors, Hub, Scenes, Groups, etc.
  - Control device → Wifi → Philips Hub → Zigbee → Bulbs
  - Easily controllable via a Python library
  - But no switchable outlet product available!
- WeMo
  - Switchable outlets!
  - Wifi only
  - Easily controllable thru… uh… An unauthenticated HTTP request
  - Sketchy security… more on that later

Deploy the Equipment

- Let's revive some old stuff
- I want my office to feel like it's alive and friendly

Morse Code Key
1861

Burns Speaker
1925

Atwater-Kent Model 80 Radio
1932

Westinghouse Fan
1938

Model Train Engine
2012

Mesmer Tube
2015

Philips Hue Bulbs
2016

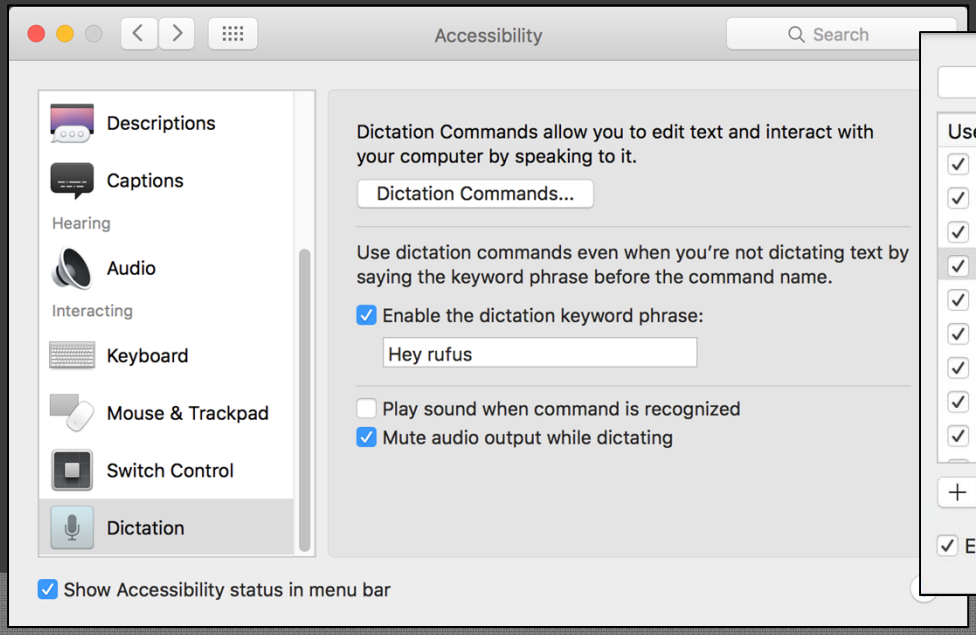
Lutron Caseta Shades
2016

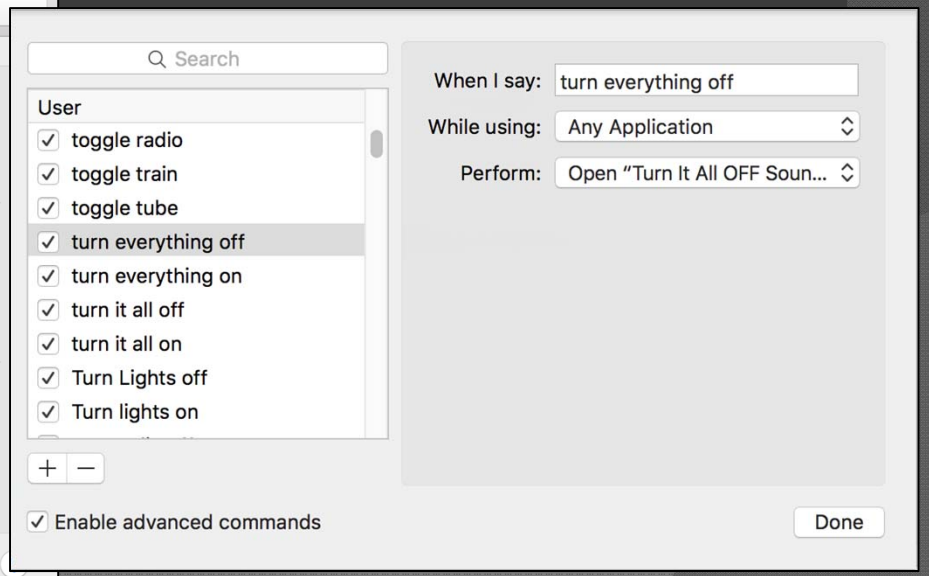
Round 1: Point and Click

- Control everything from my Mac using AppleScript → bash / Python → device, all with point and click
  - Looks nice
  - Easy to use
  - But I have to be sitting at the Mac to use it
  - My dock got a little busy… Here is 1/3 of it:

Round 2: Voice Control & R.U.F.U.S.

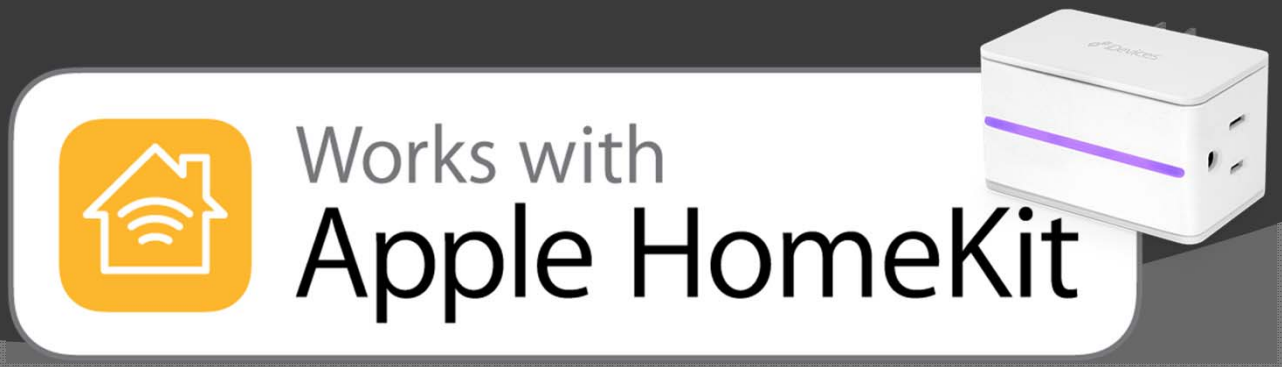
- Using Mac OS X voice control to launch my dock items… I built R.U.F.U.S.
- Invoked with “Hey RUFUS”
  - It worked... But R.U.F.U.S. was not very smart
  - My wife: “You should just build your own Siri!”
  - Me: “Ummmm... Not so much.”





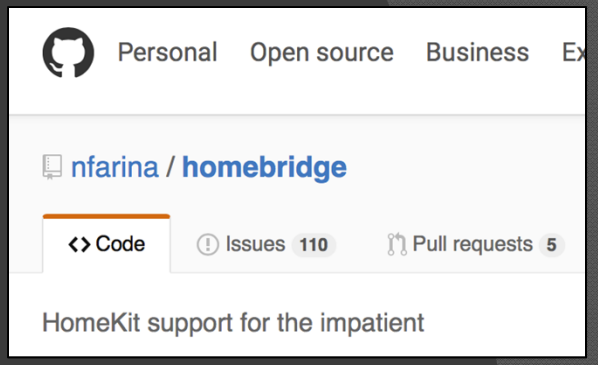
Round 3: HomeKit & Siri

- Late 2015: Apple finally releases HomeKit
  - Offers the promise of Siri integration
    - But officially only works with Apple-certified products
  - Great for Hue (with new bridge)… but no WeMo?
  - iDevices switched outlets available (but I bought WeMo)
  - No HomeKit GUI – Device vendor provides UI
  - I start using HomeKit & Siri for my Hue lights... And still control WeMo from my Dock and R.U.F.U.S. – Yuck!



Round 4: Homebridge FTW!

- Free, open-source tool that provides integration of… pretty much any IoT device with HomeKit (& Siri)
  - Written in node.js by Nick Farina
  - Configuration is a little weird
  - Not HomeKit-certified by Apple, but works well



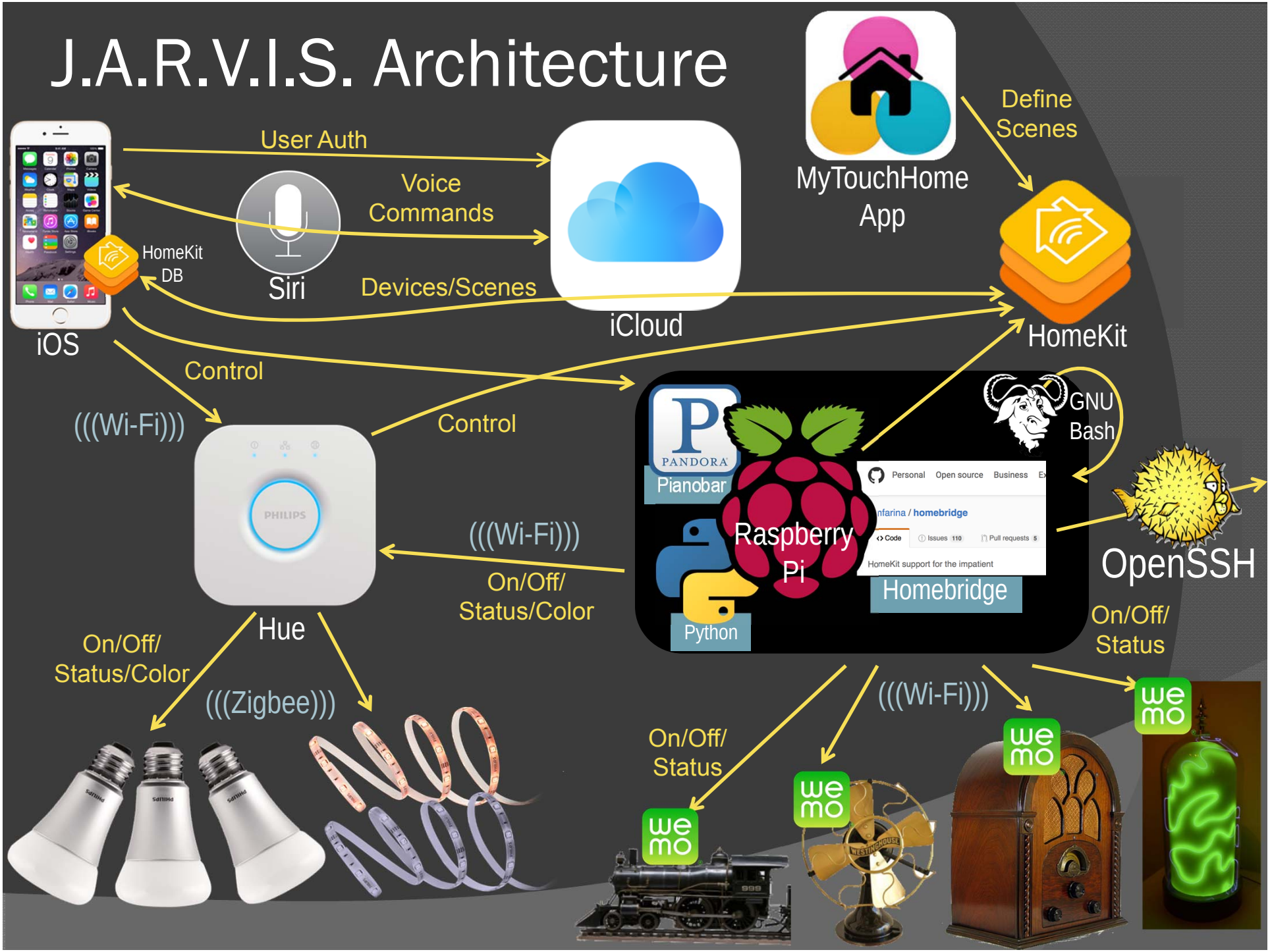
- I installed it on a Raspberry Pi… and was shocked at how much you can do with it
  - Plug-in to control WeMo
  - Over 50 plug-ins to control most every other IoT device
  - AND.... Run an arbitrary command in Linux, even ssh
- I wonder if Apple realized how much it opened up Siri by releasing HomeKit

Additional Notes on Homebridge

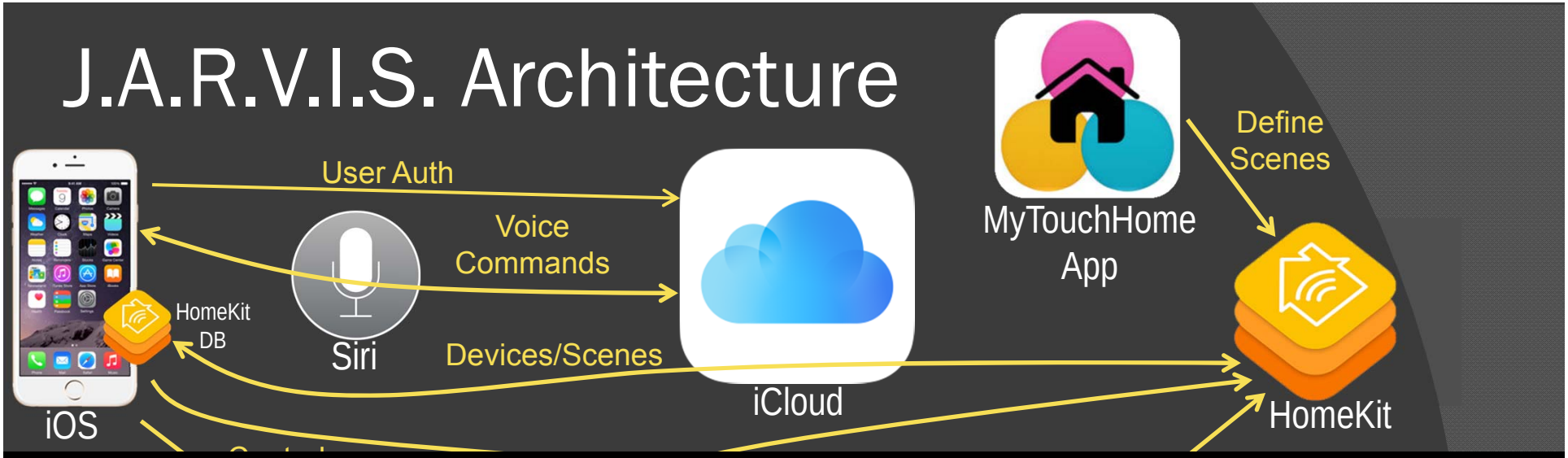
- I've outsourced my AI to Apple via Siri
  - Its understanding gets better and better over time…
  - ...As I train it (and as it trains me)
  - Siri has become one of my closest friends
  - Apple must be wondering what the heck that weirdo in Central Jersey is doing, talking to Siri all day long, saying all kinds of weird IoT stuff
- The integration and control of all IoT via Siri is really exciting
  - Even when Apple hasn't officially certified a device for its ecosystem
- An alternative approach is to use OpenHAB (Java, super flexible, visualizations)

openHAB
empowering the smart home

J.A.R.V.I.S. Architecture

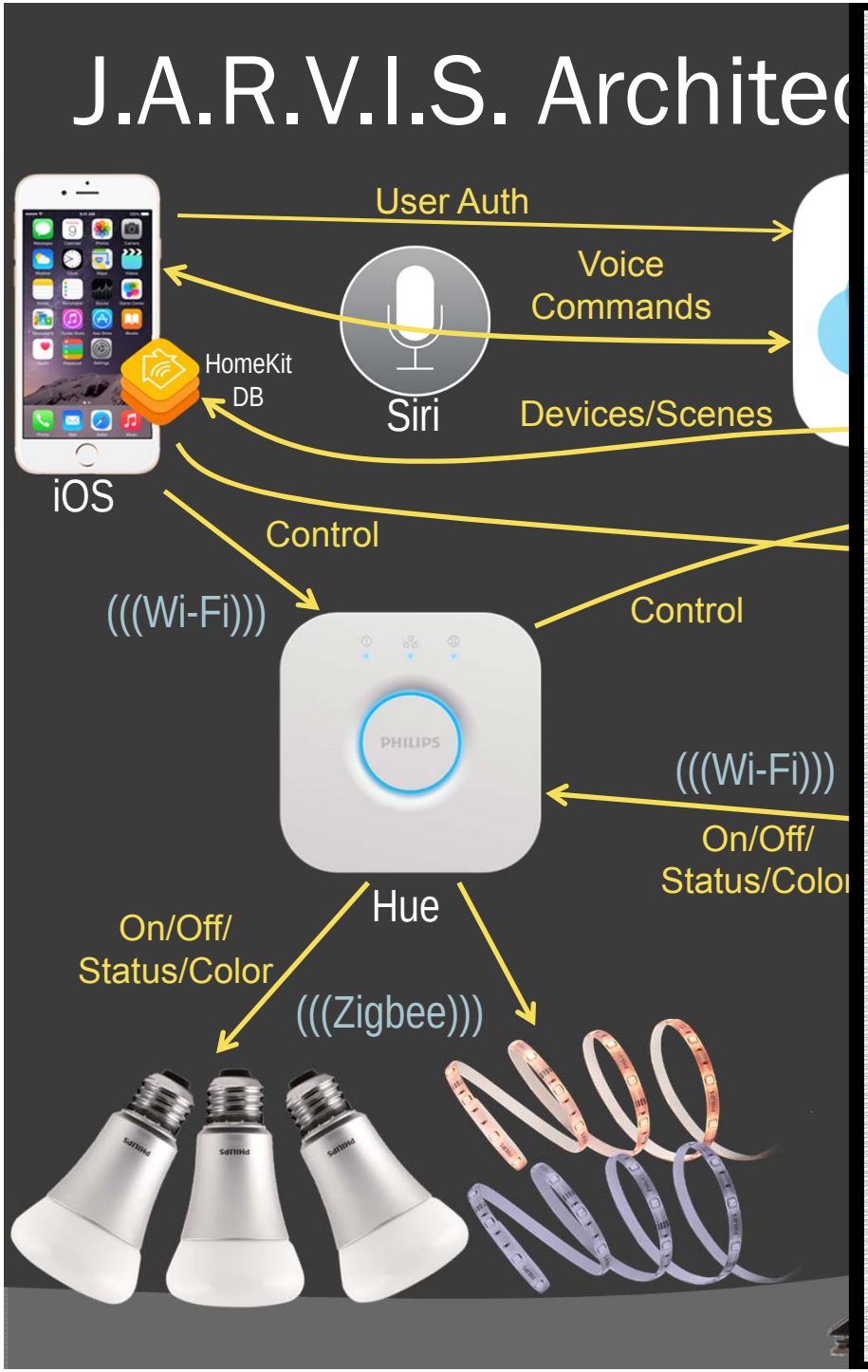


J.A.R.V.I.S. Architecture



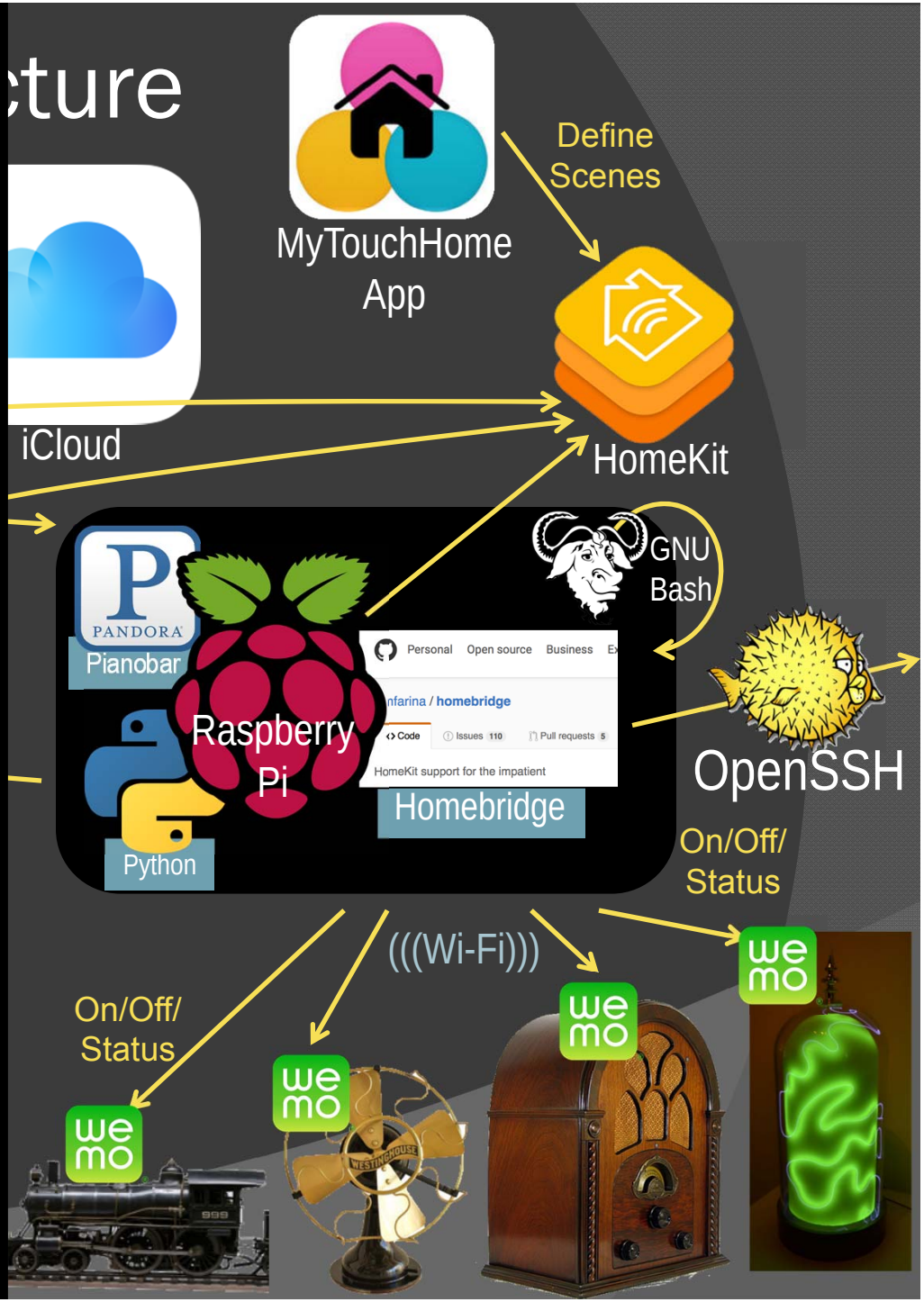
- Everything above this box is Apple
- It can be replaced with:
  - Amazon Echo with Alexa
  - Microsoft Cortana
  - OK Google & Cloud Speech API
  - Other options

J.A.R.V.I.S. Architec



- Everything to the left of this box is kinda pricey
- It's also kinda closed
- But the build quality is good
- You can replace it with stuff on previous slides and WeMo/other bulbs

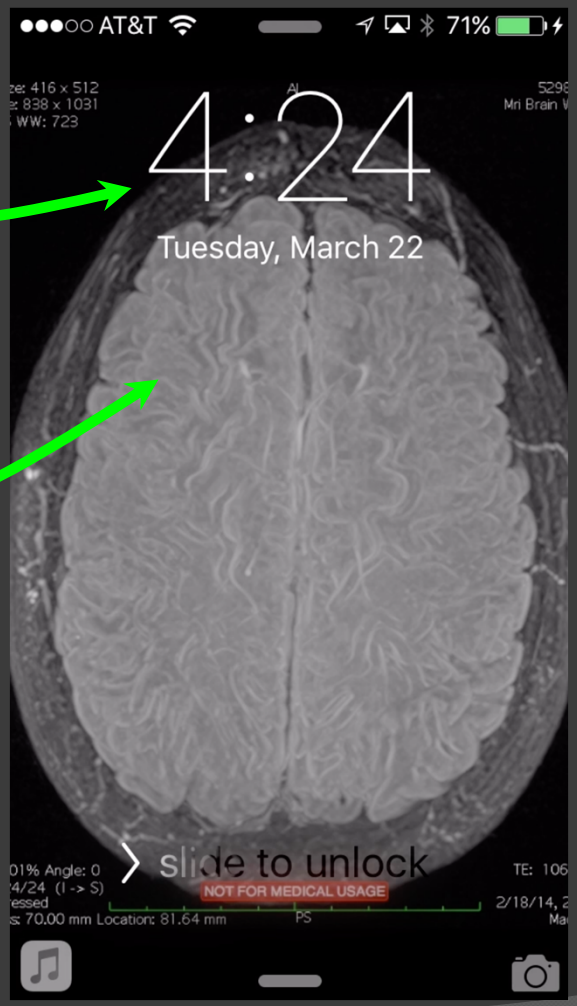
- Everything to the right of this box is free or cheap
- It's also really open
- You can make it do almost anything
- Python, bash, and/or ssh on a Raspberry Pi!



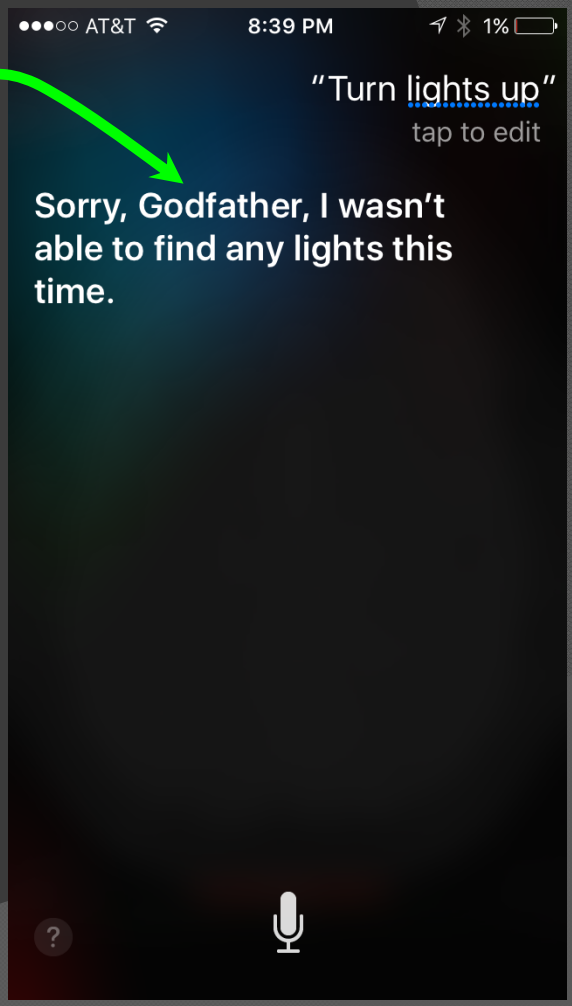
A Little Context about My Phone & Siri

That's my phone

That's my brain (an MRI… don't ask)



My phone insists on calling me "Godfather." Please don't judge. ☺



My Own Personal J.A.R.V.I.S. In Action

What It Can Do... and Limitations

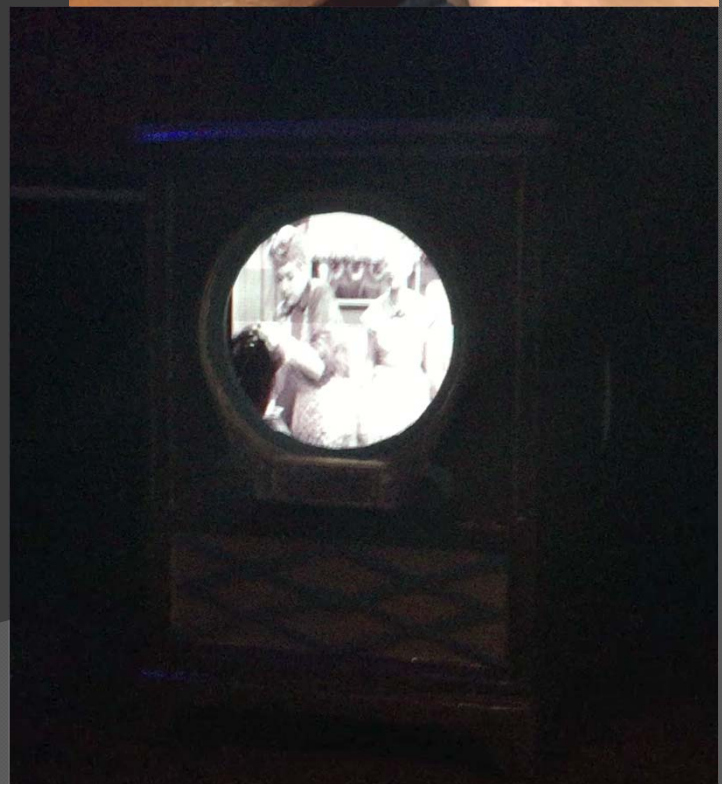
- By creating a scene name, I can take any words that don't collide with Siri's existing functionality and use them to launch arbitrary actions
  - No: "Run", "Launch", "Play", Existing App Names
  - Yes: "Volume Up", "Good Morning", "Activate", "Brian Setzer" (note collision of Good Morning, but it's ok)
- I can't take arguments on my input ☹
- I can't control spoken output, exactly
  - Although, it occurs to me that I can play an audio file with whatever output I want via the 1932 speaker
  - My 1932 Radio is the default speaker for audio output… it works surprisingly well given that it is 84 years old

Coming Soon...

- I've added another Raspberry Pi to control a 1951 Zenith Porthole TV
- A deluxe 19" widescreen circle!
  - The King of Televisions
- "Honeymooners" "I Love Lucy" "Buck Rogers" and more
- New Pi and all integration done… awaiting TV repair shop!

Already Here! Mini-TV

- Phil Smith, US Army, 3D printed a miniature version of the Zenith TV
  - Put a Raspberry Pi Zero inside, with a specialized screen and audio
  - Controlled via a web page and JSON
  - I integrated it with the office!



Once the Base Infrastructure Is Done... You Can Have Fun

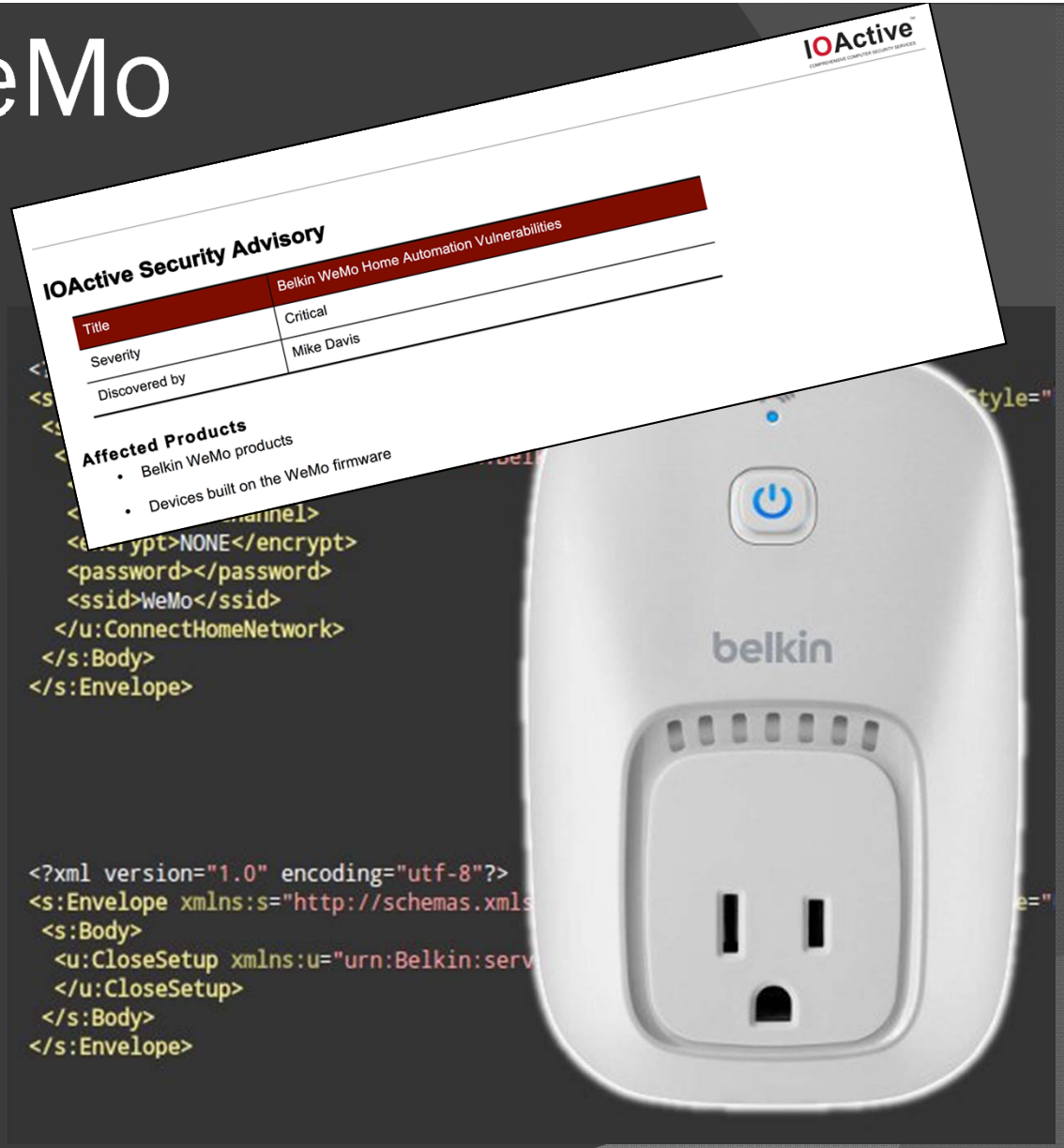
- Say what kind of music you want and the appropriate Pandora station automatically plays
- “Volume Up” / “Volume Down” with BING effect
- “It’s Friday Friday!”, “Chase Lights”, “Candles”
- “Activate Red Alert”, “Happy Birthday”
- “Sports Info”, “Weather Info”, and more!
- Westminster Chimes every hour with Bong sound
- Controlled via Python and/or bash, running on a Pi, with sound through a 1932 radio
- If you have more ideas for fun stuff, please let me know!

Psychologically Speaking

- There are 10 kinds of people in this world:
  - Those who really like voice control
  - Those who don't like voice control
- The thrill of building things and moving fast make it ***REALLY*** tempting to skip security
  - "I'll work on that later… I'm having FUN now!"
  - Seductive... But Must. Be. Resisted.

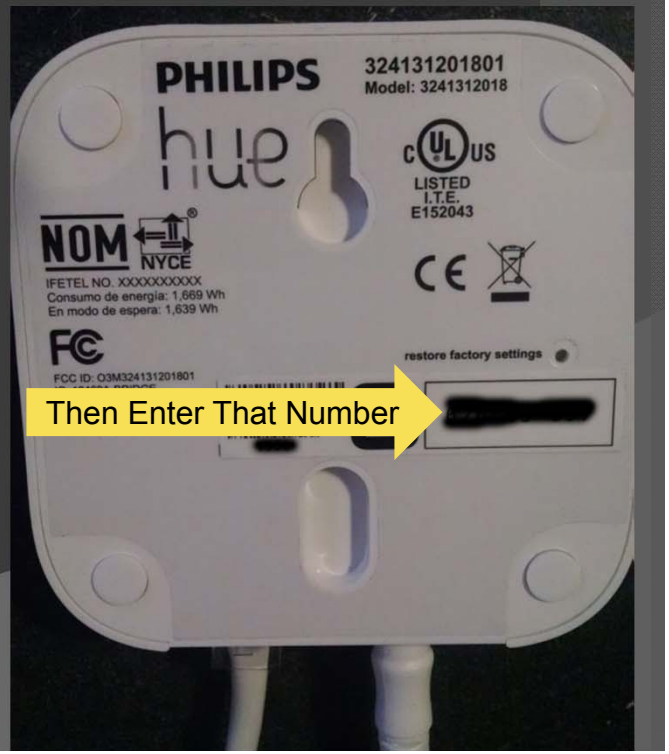
Security - WeMo

- Some great work done here back in Feb 2014 by Mike Davis at IOActive… WeMo fixed lots of that stuff
- But still, if you are on my LAN, you can turn on / off any WeMo device via simple HTTP request
  - CURL for the WIN!
- Solution: deploy separate wireless LAN with crazy-hard WPA2 pre-shared key



Security - Hue

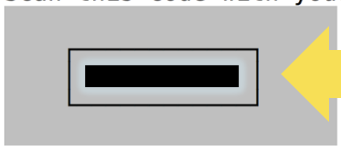
- If you are on my LAN, you've got to push my button to pair with Hue
- I like that local physicality
  - You could lock it up in a Secret Secret Room inside a Secret Room, for example
- You also need to know my device ID
  - 8 digit number printed on Hue bridge
- You enter that device ID into your app
  - Such as the Hue control app
- Then, you add Siri support in the Hue app
- The Hue bridge reaches out to Apple iCloud and tells it about devices
- …so it depends on my iCloud account



Security - Homebridge

- Security is all based on a “username” (MAC address), device ID (an 8-digit number)...
  - Completely controllable by me
- You enter device ID into HomeKit application
- If you know my device ID (and have access to my iCloud account), you can join and control stuff
- Solution: Make a device ID that no one could ever guess... And....

```
ed — pi@raspberrypi: ~ — ssh pi@10.1.1.9 — 95×43
Loaded plugin: homebridge-cmd
Registering accessory 'homebridge-cmd.CMD'
---
Loaded plugin: homebridge-ssh
Registering accessory 'homebridge-ssh.SSH'
---
Loaded plugin: homebridge-wemo
Registering accessory 'homebridge-wemo.WeMo'
---
Loaded config.json with 17 accessories and 0 platforms.
---
Loading 17 accessories...
[Fan] Initializing WeMo accessory...
[Fan] Searching for WeMo device with exact name 'Fan'...
[train] Initializing WeMo accessory...
[train] Searching for WeMo device with exact name 'Choo Choo'...
[Mesmer Tube] Initializing WeMo accessory...
[Mesmer Tube] Searching for WeMo device with exact name 'Mesmer Tube'...
[Speaker] Initializing WeMo accessory...
[Speaker] Searching for WeMo device with exact name 'Radio Power'...
[Piano] Initializing CMD accessory...
[Volume] Initializing CMD accessory...
[Red Alert] Initializing CMD accessory...
[Friday Friday] Initializing CMD accessory...
[forties] Initializing CMD accessory...
[parov] Initializing CMD accessory...
[post modern] Initializing CMD accessory...
[vitamin] Initializing CMD accessory...
[setzer] Initializing CMD accessory...
[bluegrass] Initializing CMD accessory...
[honey] Initializing SSH accessory...
[buck] Initializing SSH accessory...
[lucy] Initializing SSH accessory...
Scan this code with your HomeKit App on your iOS device to pair with Homebr
```

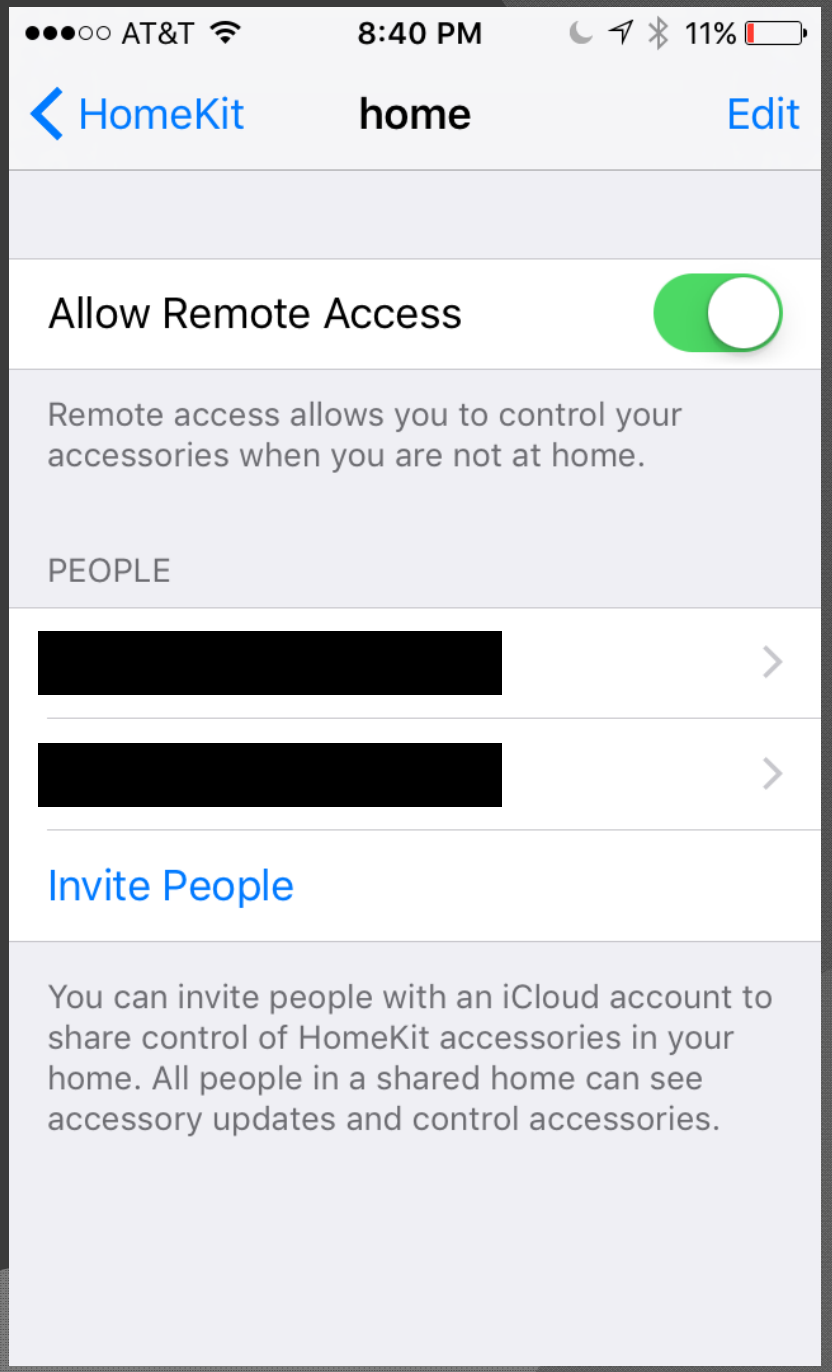


No Hue button for Homebridge… just the number

```
Homebridge is running on port 51826.
[Fan] Found 'Fan' device at 10.1.1.16
[Mesmer Tube] Found 'Mesmer Tube' device at 10.1.1.13
[Speaker] Found 'Radio Power' device at 10.1.1.14
```

Security - HomeKit

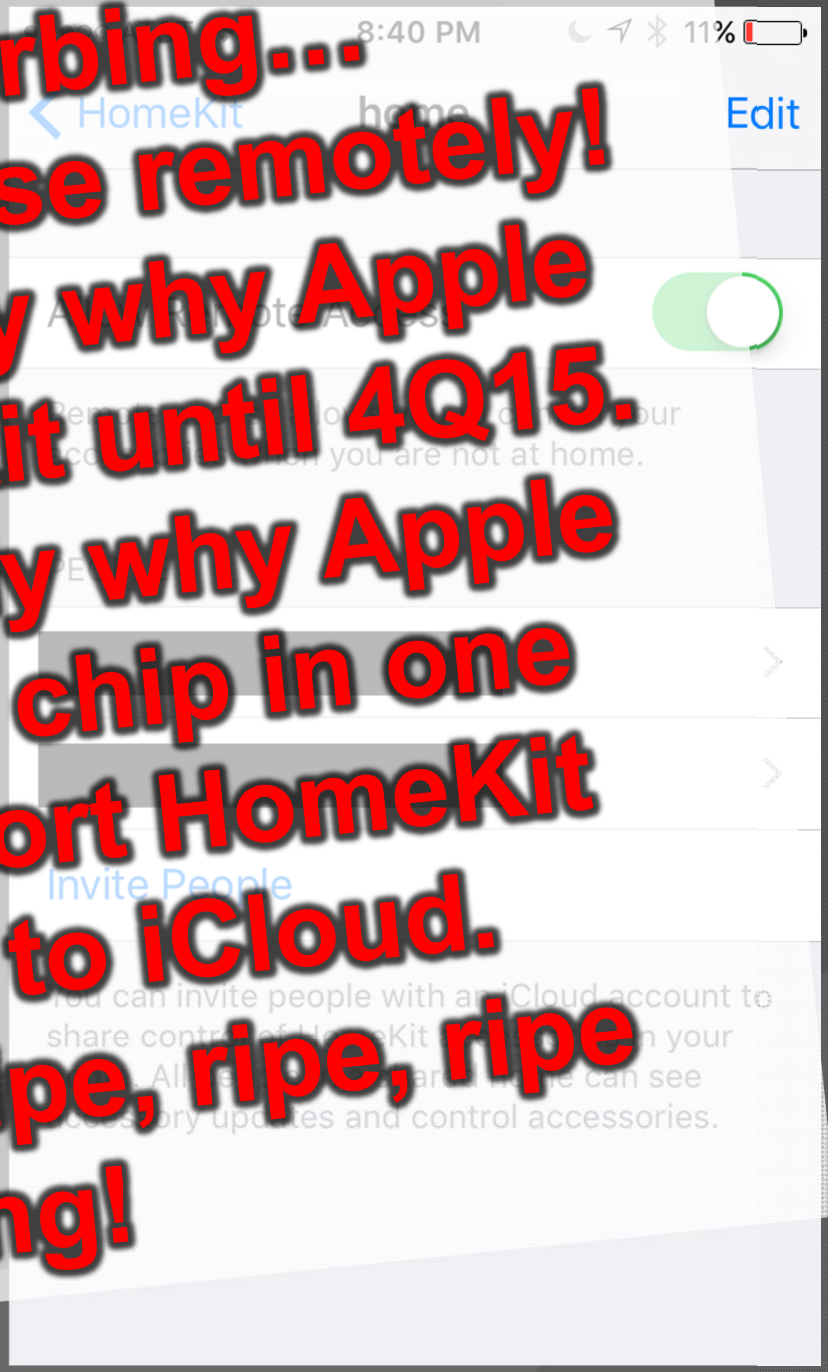
- HomeKit Security is based on… my Apple ID (a.k.a., my iCloud/iTunes account) and my keychain
- I can invite other people via their iCloud accounts, and they can activate assets and scenes
  - But they can't edit anything
  - I can revoke at any time
- I have the option of disallowing "remote access"
  - Internet versus just LAN control
- Remote access requires you to have at least one "Certified by Apple" Mfi device in the home



Security – HomeKit

- All security is based on my AppleID (a.k.a., my iCloud/iTunes account) and its encryption
- I can invite other people into their iCloud accounts, and they can activate as "trusted devices"
  - But they can't edit anything
  - I can revoke anytime
- I have the option of disallowing "remote access"
  - Internet control
- Remote access requires you to have at least one "Certified by Apple" Mfi device
  - Hue Hub, AppleTV, etc.

- Yes, this is disturbing…
- Yes, it's fun to use remotely!
- Yes, this is likely why Apple delayed HomeKit until 4Q15.
- Yes, this is likely why Apple requires an Mfi chip in one device to support HomeKit authentication to iCloud.
- Yes, this is a ripe, ripe, ripe area for hacking!



A Call To Action: Start Working With and Hacking This Stuff

- It's tremendously fun
- It can be done on a shoestring budget
- A Raspberry Pi with WeMo can get you rolling
  - Add voice via Siri (with Homebridge), Alexa, Cortana, or OK Google
  - Or, if you want a lot of pre-developed code (in Java :/), consider using the OpenHAB project
- And grow as you see fit
- Have fun!

Going Forward

- I predict IoT will soon be thought of as a passing fad, widely derided as just plain silly
  - Like cyber, cyber, cyber; big data; APT; etc.
  - But IoT will be one of those fads that seems clichéd and passing, then gradually just infiltrates the mainstream when no one looks and turns up everywhere

Conclusions

- The Internet of Things is in its infancy
  - Rolling this stuff out makes you feel like a mad scientist or wizard, especially with voice control
  - Industry focus is turning from devices to frameworks and APIs for managing those devices
  - From a security perspective, lots of vulns… It's like the 1990s all over again
    - Crazy architectures, unauthenticated access, hard-coded passwords, RFI, XSS, and more
  - Let's get hacking!!!
  - Got any ideas???