Chris Littlebury

HOME ALONe

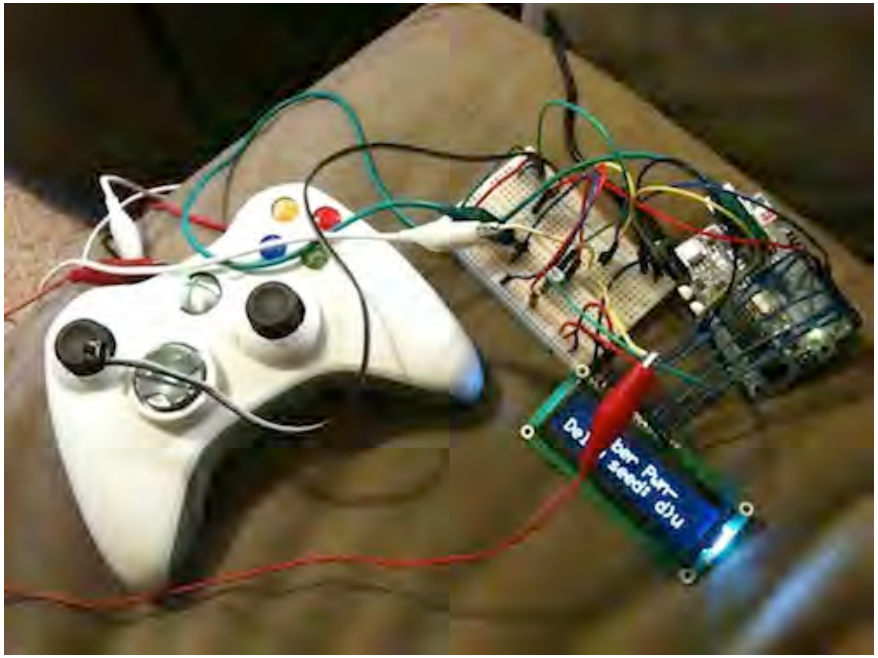
with localhost

AUTOMATING HOME DEFENSE

About me

Chris Littlebury
Senior Penetration Tester with Knowledge Consulting Group
Chris.Littlebury@KnowledgeCG.com

I like building stuff.



-DISCLAIMER-

I am:

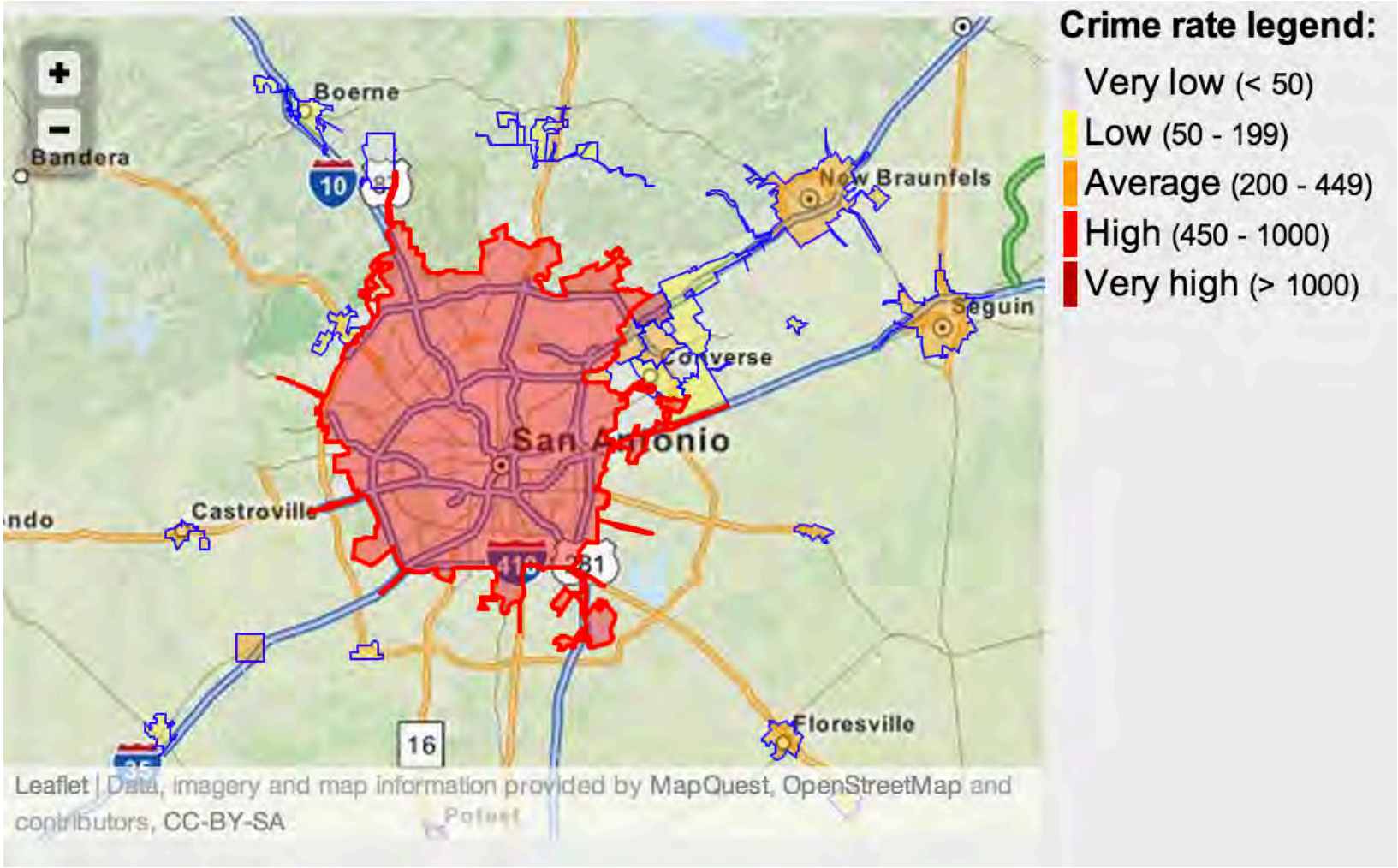
- Providing ideas, examples, and code of what's worked for me.
- Open to questions afterward and suggestions.

I am *not*:

- Getting paid to endorse any products.
- Promising an end to burglaries.
- Advocating setting up booby traps in your home.
- Challenging anyone to "test" my home. Please, please do not.

Once Upon a Time in South Texas

Once Upon a Time in South Texas



Once Upon a Time in South Texas

San Antonio Crime Data

Crime Data FAQ

CRIME INDEX

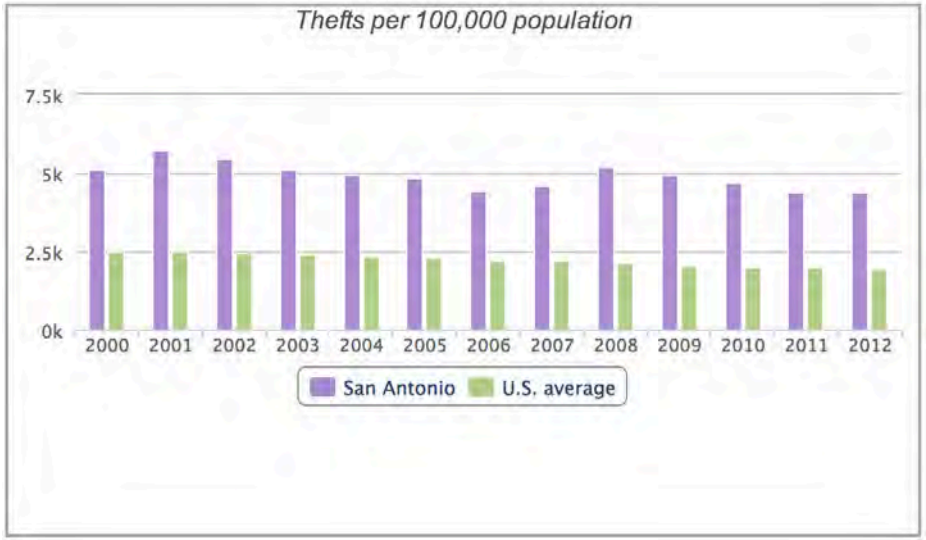
3

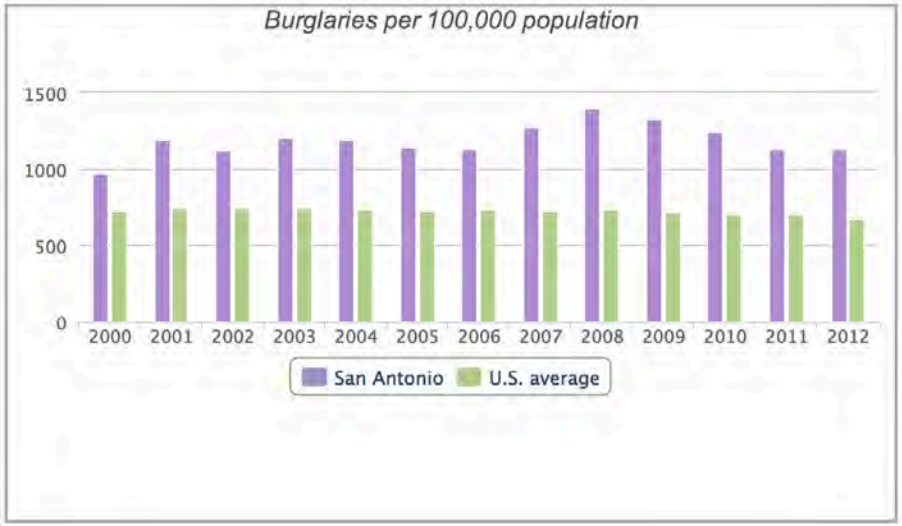
(100 is safest)

Safer than 3% of the cities in the US.

San Antonio Annual Crimes

VIOLENT	PROPERTY	TOTAL
7,047	83,762	90,809
annual crimes per 1,000 residents		
5.11	60.69	65.80





My $1500 Thief Magnet

Most Stolen Cars – United States

According to the National Insurance Crime Bureau (NICB), in 2009 the most stolen cars in the U.S. were:

1. 1994 Honda Accord
2. 1995 Honda Civic
3. 1991 Toyota Camry
4. 1997 Ford F-150 Pickup
5. 2004 Dodge Ram Pickup
6. 2000 Dodge Caravan
7. 1994 Chevrolet Pickup (Full Size)
8. 1994 Acura Integra
9. 2002 Ford Explorer
10. 2009 Toyota Corolla

*http://learningcenter.statefarm.com/auto/safety/most-stolen-cars-of-2009/

I Had an Idea

- Remove the main fuel relay at night
- Install two-way alarm system with only paging functionality.

Success!

(Depending on how you look at it)

My Awesome Apartment Complex

/u/TheDovahkiinsDad (Not me or my pic)

http://www.reddit.com/r/WTF/comments/2784oo/my_buddies_jeep_was_set_on_fire_by_some_crazy_ass/

Movin’ on Up

Tips From Cops

- Make your home look occupied, and make it difficult to break in.
- Leave lights on when you go out. If you are going to be away for a length of time, connect some lamps to automatic timers to turn them on in the evening and off during the day.
- Lock all outside doors and windows before you leave the house or go to bed. Even if it is for a short time, lock your doors.
- Keep your garage door closed and locked.
- Don't allow daily deliveries of mail, newspapers or flyers build up while you are away. Arrange with the Post Office to hold your mail, or arrange for a friend or neighbor to take them regularly.

http://www.sjpd.org/bfo/community/Crimeprev/PreventionTips/Prevent_Burglary.html

X10 Protocol

-Created in the late 1970s.

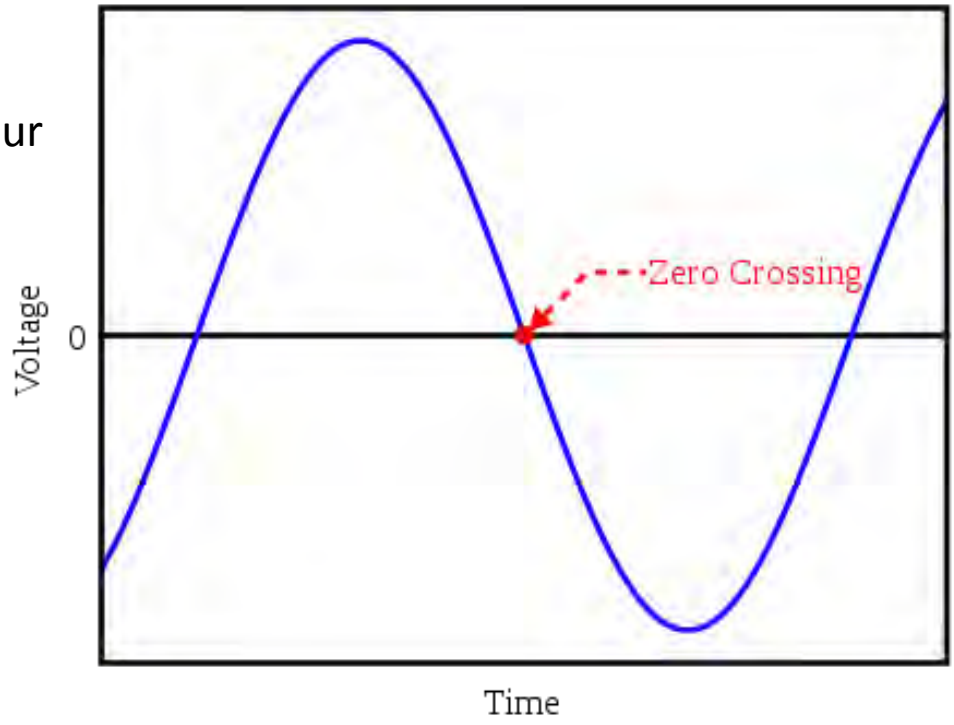
-Data is encoded onto a 120khz carrier which is transmitted as bursts during the zero crossings of the 60hz AC waveform. One bit is transmitted at each zero crossing.

-Four bit house code, four bit unit code, and four bit command.

-Stupid cheap

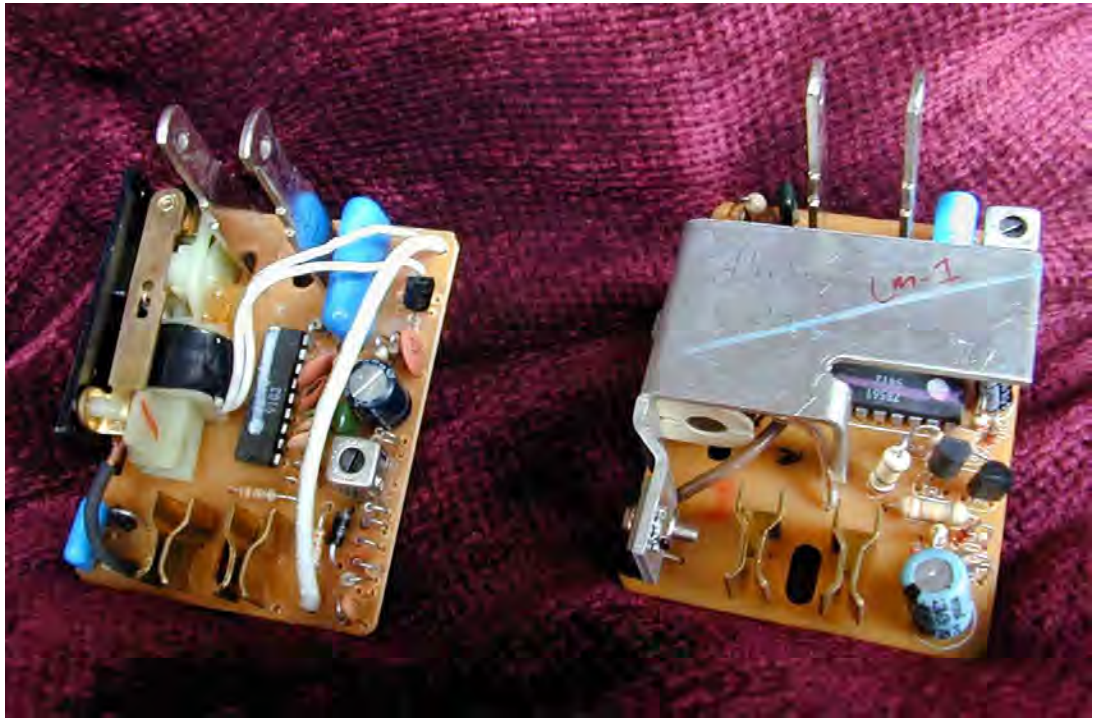
-Prone to interference

-Each command set sent three times



X10 Hardware

Again, stupid cheap



X10 Setup

- Light timers that operated by day of the week and time
- Security timing feature
- Remote control (RF)
- Not awesome, but worked

X10 – Adding Exterior Lighting

So Long South Texas

Time to Do it Right*

*I do not advocate creating laser booby traps in your home.

Wish list

- Efficient lighting
- Granular control over timing events
- Integration into existing security system
- Adaptive timing
- Conditional decision system
- In-house geo-fencing
- Defense against wireless home automation attacks
- Create tangible house reactions to external stimuli (active defenses)

New Programmable Light Tech: LIFX

Funded! This project was successfully funded on Nov 14, 2012.

9,236
backers

$1,314,542
pledged of $100,000 goal

0
seconds to go

Share Tweet Embed

Project by
Phil Bosua
San Francisco, CA
Contact me

3 created · 5 backed

Phil Bosua 194 friends

Website: lifx.co

See full bio

LIFX is a WiFi enabled, multi-color, energy efficient LED light

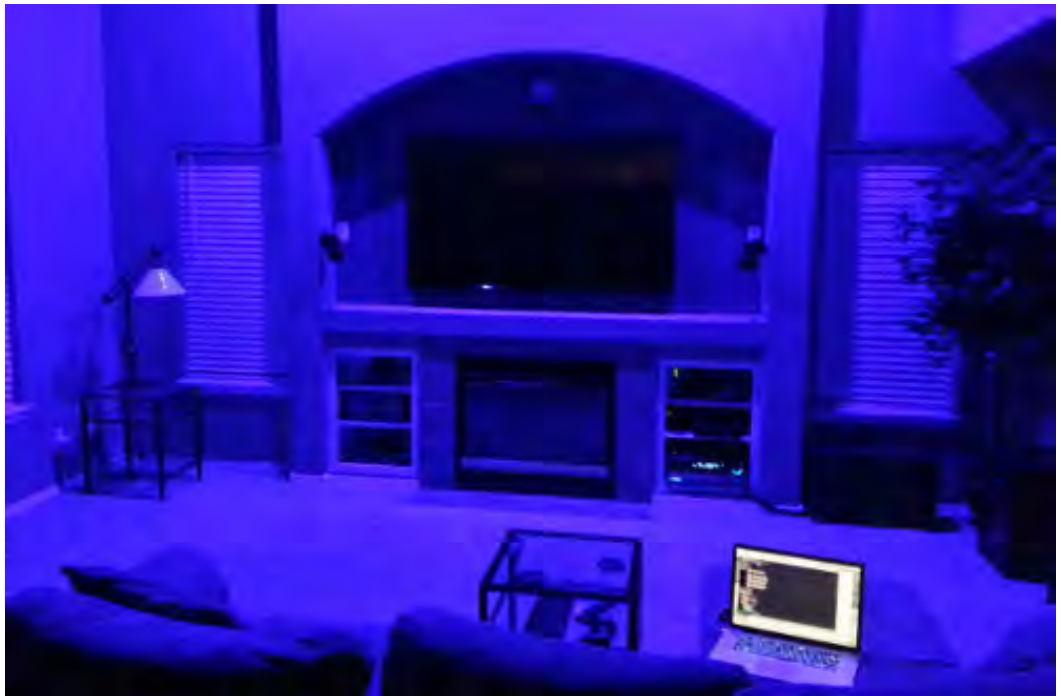
LIFX Pros/Cons

Pros:

- Excellent color reproduction
- 802.11 built-in (no hub needed)
- White output of over 1000 lumens
- Low power consumption (17 watts at full brightness)

Cons:

- Bulbs are physically large (limits fixture selection)
- Relatively heavy (again, limits fixture selection)



Philips Hue Pros/Cons

Pros:

- Small bulb size (fits in regular fixtures)
- Low power consumption (8.5 watts at full brightness)
- Slightly cheaper

Cons:

- Lower light output
- Limited color reproduction

Combine the Two

WeMo Devices

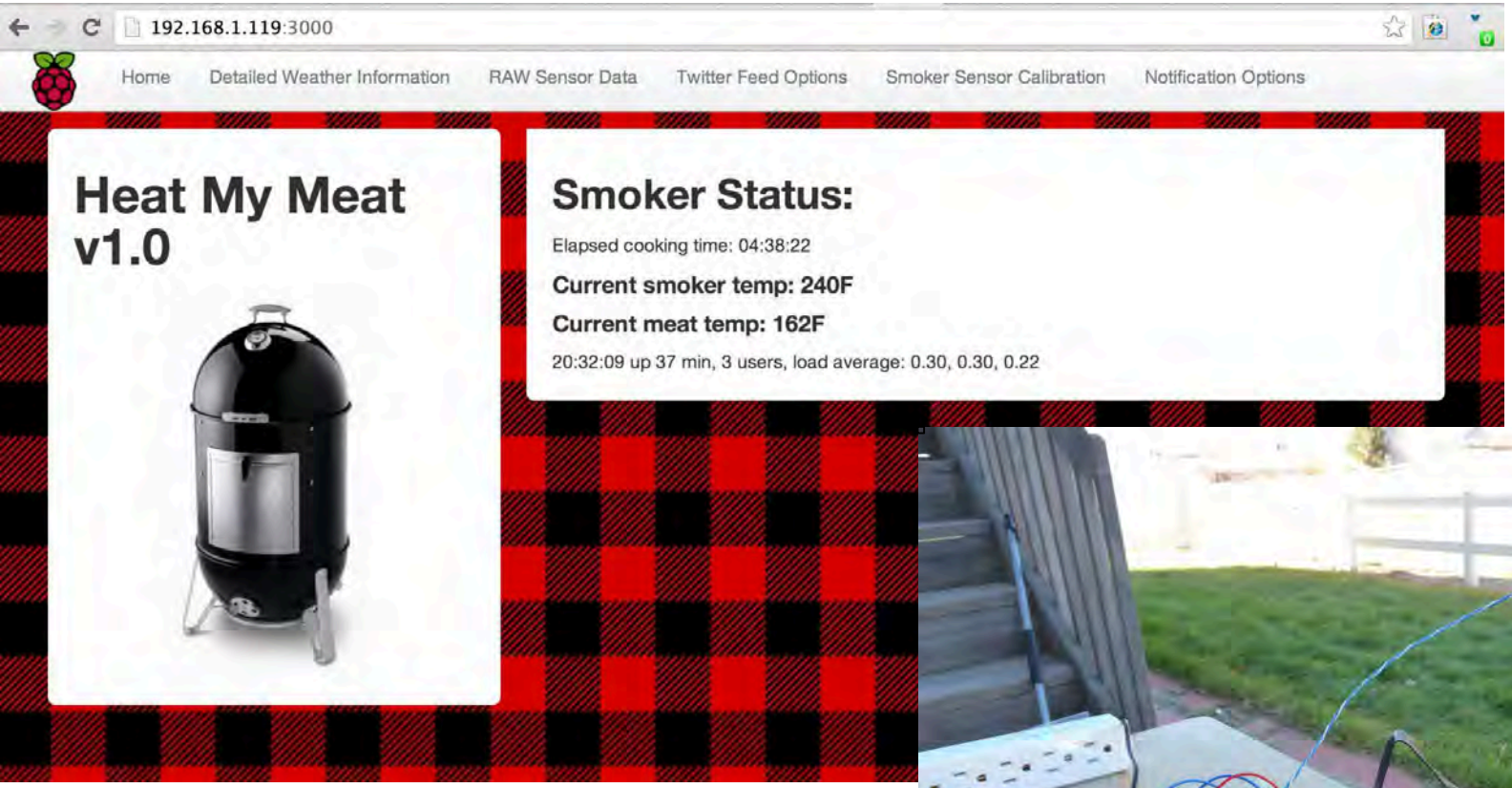
- WLAN to Zigbee bridge like LIFX devices
- Uses UPnP and SOAP
- Control outlets and wall switches
- Semi-cheap
- Terrible App support
- Scheduling rules that sometimes work
- Integration with IFTTT that works 20% of the time
- Terrible security

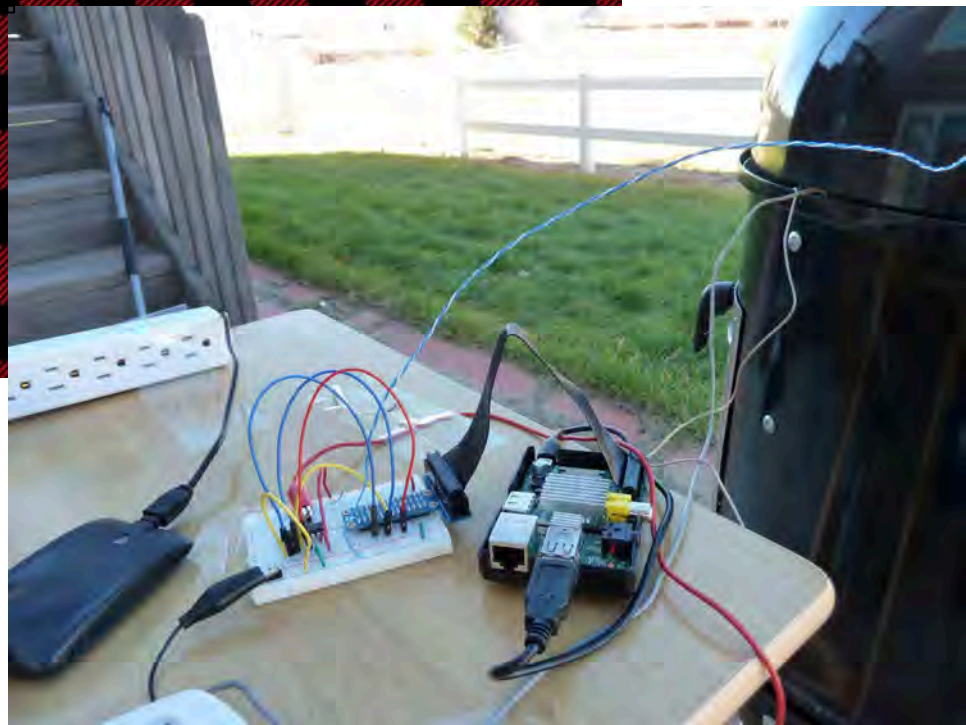
http://bit.ly/1e6Vsvt

Creating a Home Defense Server

- Needs to be available 24/7
- Low power consumption would be nice (UPS)
- Integration of analog/digital sensors and components
- Output for integration into traditional home security system
- Raspberry Pi was the obvious choice

Previous Experience with Pis





Open Source to the Rescue!

Magicmonkey – lifxjs: https://github.com/magicmonkey/lifxjs
- -Reversed the LIFX protocol
- -Paved the way

Sharph – lifx-python: https://github.com/sharph/lifx-python
- -Based on Magicmonkey's protocol dissection and js library
- -Written in glorious Python
- -Awesome API that bridges WLAN to LIFX's Zigbee (802.15 915mhz) protocol

LIFX Official API: https://github.com/LIFX/lifx-gem
- -Written in Ruby
- -Support for addressing multiple bulbs at once

iancmcc's ouimeaux: https://github.com/iancmcc/ouimeaux
- - Extensive Python API for WeMo devices
- - Application written on top of the official API

Creating a Front End and Services

- Choose a lightweight framework like Flask (Python) or Sinatra (Ruby)
- Create services for each tech (LIFX, Hue, WeMo)
- Individual services prevent system-wide failures and segregate code
- Choose a lightweight database like Redis and host it on a separate Pi
- Create monitoring services with alerts

All code available post-conference at: https://github.com/lowercase-b

Device Proximity Monitoring

- Original plan was to use Bluetooth ranging
  - Linux's rfcomm/hcitool/l2ping
  - Inconsistent results
  - Required constant packet transmission for RSSI values
  - Would brick the device if too aggressive
  - Demo: http://www.youtube.com/watch?v=DSMaUdPEJMM

```
#!/bin/bash

while :
do
    l2ping -c 3 <BT MAC ADDR> &
    sleep 2
    hcitool rssi <BT MAC ADDR> status
    sleep 5
done
```

Device Proximity Monitoring

Utilize WLAN Frames

- Much more reliable
- Doesn't brick the device
- Allows for monitoring of additional devices (guests)
- Requires airmon-ng suite

Specific device's Received Signal Strength Indicator (RSSI):

```
tshark -i mon0 -f "wlan src host <WLAN MAC>" -l -T fields –e radiotap.dbm_antsignal
```

All devices visible and their RSSI:

```
tshark -i mon0 -l -T fields -e radiotap.dbm_antsignal -e wlan.sa
```

All fields available for a specific device:

```
tshark -i mon0 -f "wlan src host <WLAN MAC>" -l -T pdml
```

Device Proximity Monitoring

- Created a service that looks for pre-defined list of mobile phone MACs (flat file)
- Looks for WLAN beacon frames and calculates signal strength
- Records last known signal strength and last time seen in Redis db
- Capability for historical recording of locational data
- Separate service monitors timestamps and determines if devices are present
- Updates database flags which affect decision making in other services

Adaptive Scheduling System

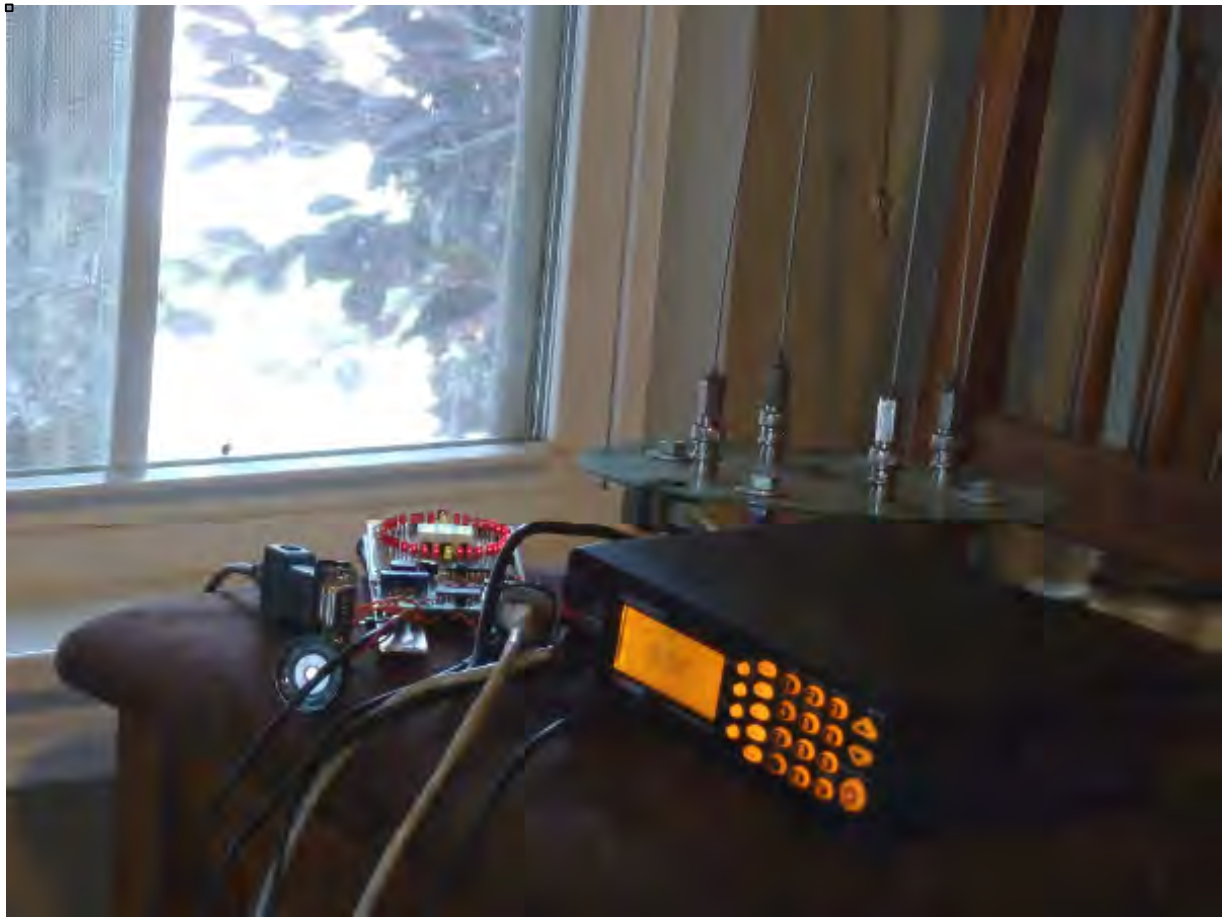
- "SmartCron" system
- Schedules all lighting events
- Pulls sunrise/sunset data from Weather Underground's API (free)
- Creates randomized, variable windows for events centered around sunrise, sunset, etc
- Events are conditional on other event flags in the main database
- Monitors local weather to advance evening lighting in cases of severe weather

Again, all code available post-conference at: https://github.com/lowercase-b

wunderground.com®

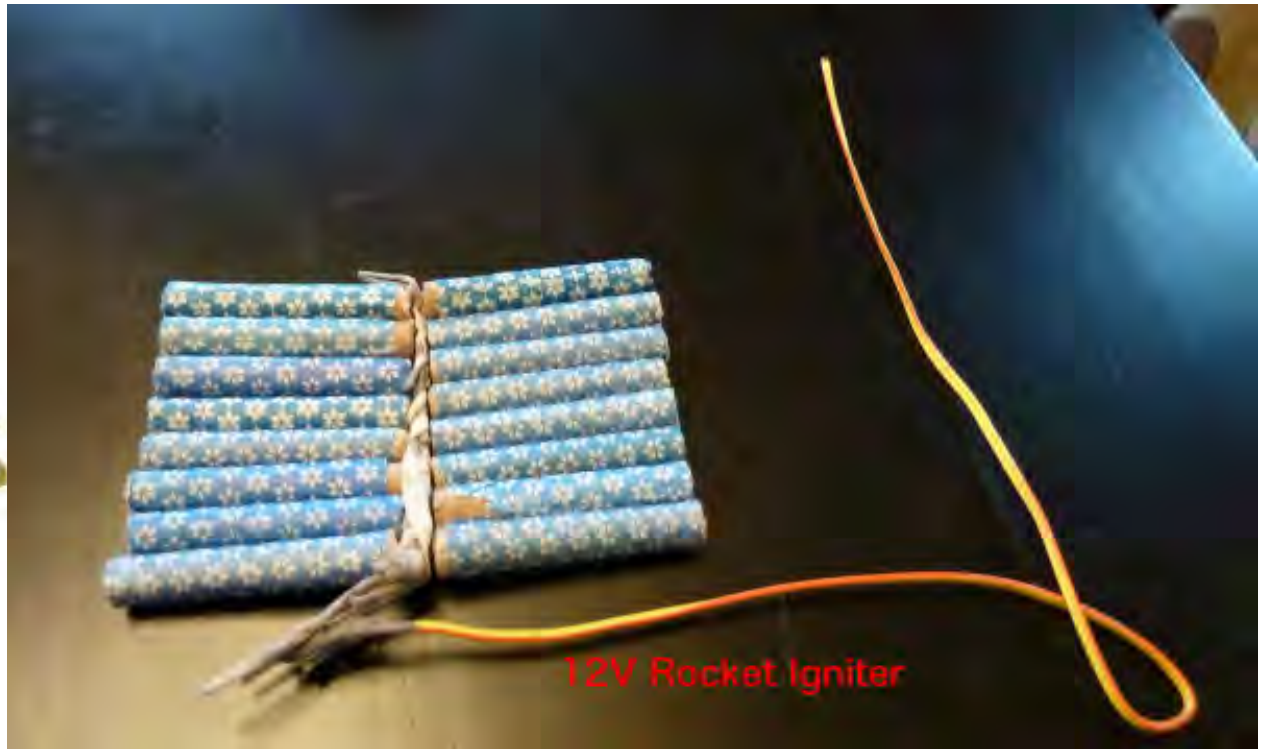
Defenses Against Wireless-Based Attacks

- Utilizes pico-dopp doppler system for real-time direction finding
- Detects persistent wireless attacks outside the perimeter of the house (jamming)
- See http://www.silcom.com/~pelican2/PicoDopp/PICODOPP.htm for parts/equipement
- Works against 345 mhz sensor attacks and Zwave
- Requires Ethernet to ensure alerting isn't jammed



Keep the Change you Filthy Animal: Active Defenses

- Intruders desire anonymity
- Anything that can be electronically activated and produce a loud, audible response
- Flash all house lights in red
- Rocket igniters and firecrackers
- 12V solenoids to knock over heavy objects (scuba tanks)
- DO NOT CREATE ANYTHING THAT CAN HARM!



Roadmap

- Buy Z-Wave devices and integrate them
- Integrate SDR scanning and data sniffing
- Hear ideas from DEFCON folks

Questions?

If you have any questions, please come find me or email me at Chris.Littlebury@knowledgecg.com