

DC423 March 25th 2019

#STAYTHEFSKHOME



TREND  
MICRO™



TREND  
MICRO™



TREND  
MICRO™



TREND  
MICRO™



TREND  
MICRO™



TREND  
MICRO™

# Agenda

- @tothehilt - STUFF
- @maggs - Blockchain Applications for ML AI in Substations Over PTP  
Distributed Herd Immunity For SpaceX Martian Power Systems
- @gladiola - August Locks
- @bigun - back up fun with video



# COVID-19



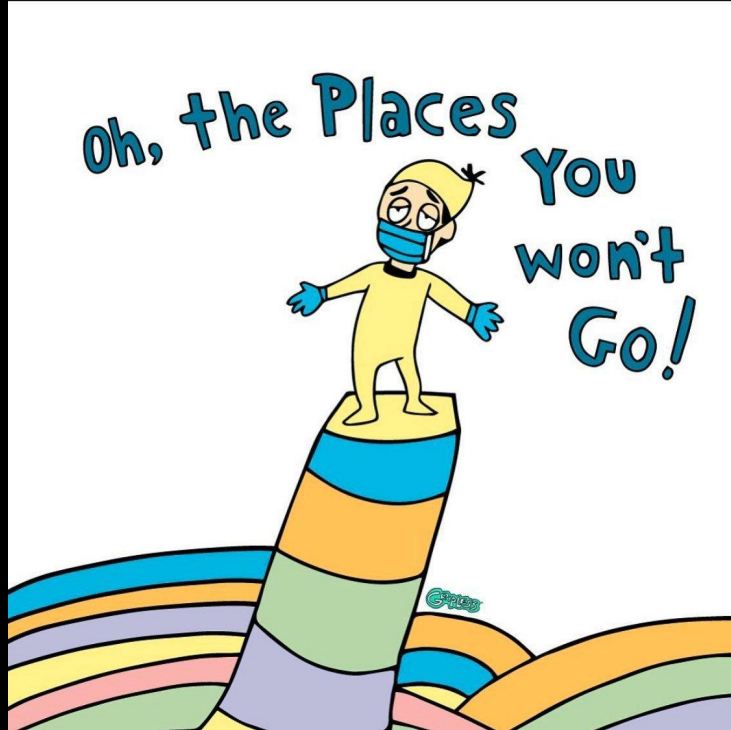
# STOP HOARDING



# STAY HOME



gripless



@maggs

Title: Blockchain Applications for ML AI in Substations Over PTP Distributed Herd Immunity For SpaceX Martian Power Systems



@gladiola

- Title: August Locks





# August Locks

gladiola January 2020



# Operational Fundamentals

- Replaces thumbturn on deadbolt
- Round housing used manually to lock or unlock
- Does not override existing mechanical keys
- Bluetooth and WiFi connectivity
- Battery powered lock assembly
- Smartphone apps





**“I’m surprised  
you’re gonna do this.”**

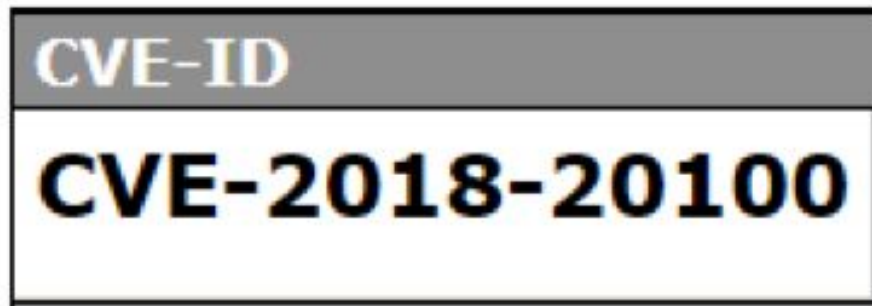
**– Mrs. OKO**

- August Locks website, c. 2016
- AirBnB August lock success
- Fondren Lock, OK.

# Case Studies in Risk and Denial

- My threat model:
  - People inside the home will screw up
  - Am I really running a secured facility?
- Their risk controls:
  - Failures at every step in the communications process
  - QA and Testing feedback at DEFCON Live Demos

# Due Diligence: Initially, Not So Diligent




**Severity**

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 NIST: NVD

Base Score: **9.8 CRITICAL**

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An issue was discovered on August Connect devices. Insecure data transfer between the August app and August Connect during configuration allows attackers to discover home Wi-Fi credentials. This data transfer uses an **unencrypted access point** for these credentials, and passes them in an HTTP POST, using the AugustWifiDevice class, with data encrypted with a **fixed key found obfuscated in the app**

<https://nvd.nist.gov/vuln/detail/CVE-2018-20100>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20100>

<https://www.cnet.com/news/august-smart-lock-hacked/>



# Patches, Hacks and Chains of Vulns

Demo at DEFCON 24.

Where are the CVEs for all these hacks?

Patched in August 2016



**Jmaxxz** @jmaxxz · Aug 19, 2016



Replying to @jmaxxz

They still need to patch a couple more things, but this is a big deal.



**David Wang**

@planetbeing

Have they stopped leaking the firmware key?



4:38 PM · Aug 20, 2016



... and it connects to other vulnerable devices.



**Jmaxxz**

@jmaxxz

How to be a dick with ZWave. Step 1, buy a ZWave controller. Step 2, write a script to keep it in exclusion mode. Step 3, wait for your neighbor to use their ZWave switches.

3:23 PM · Dec 8, 2019 · [Twitter Web App](#)

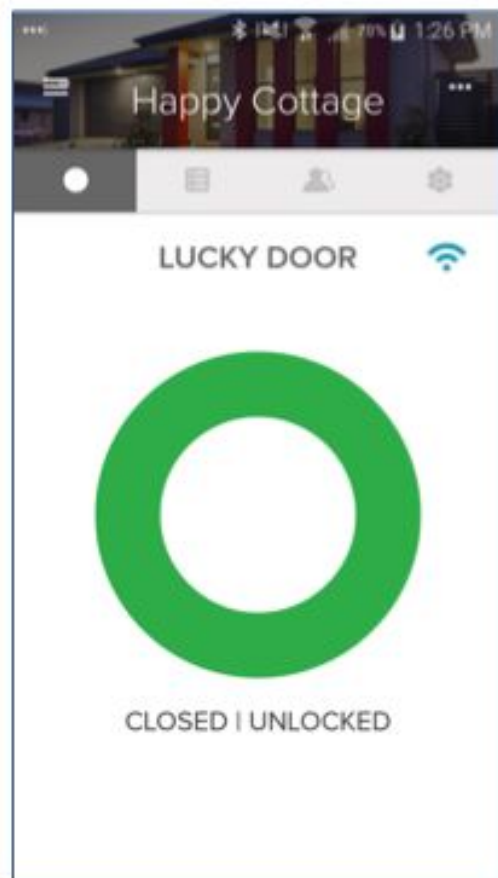
REF: <https://jmaxxz.com/blog/?p=550#more-550>

REF:

<https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEF%20CON%2024%20-%20Jmaxxz-Backdooring-the-Frontdoor.pdf>

# Questions My Wife Asked

- Color of the item?
- Will it show? Does it look like people should try to hack this lock from outside our house?
- What if daughter loses her phone?
- Can we know if someone left the door open?



# Sales Ecosystem



Apple HomeKit (Siri)



The Google Assistant

amazon

Amazon Alexa

nest

IFTTT

Honeywell

SimpliSafe

logitech

Yonomi

wink

xfinity

stringify

zwave

brilliant

LEVITON

SmartThings

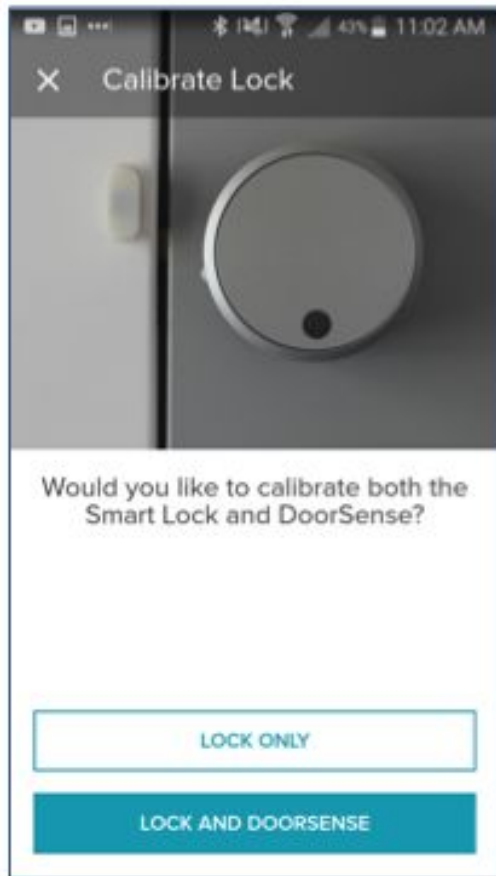
Control4





# Installation: Easy

- No printed directions
- In-App tutorials
- Config/Signal confirmation
- Fittings for most forms of locks
- Some UI stubs and misleads
  - Configure lock first
  - No generation info on box
  - Confidential data printed on box label



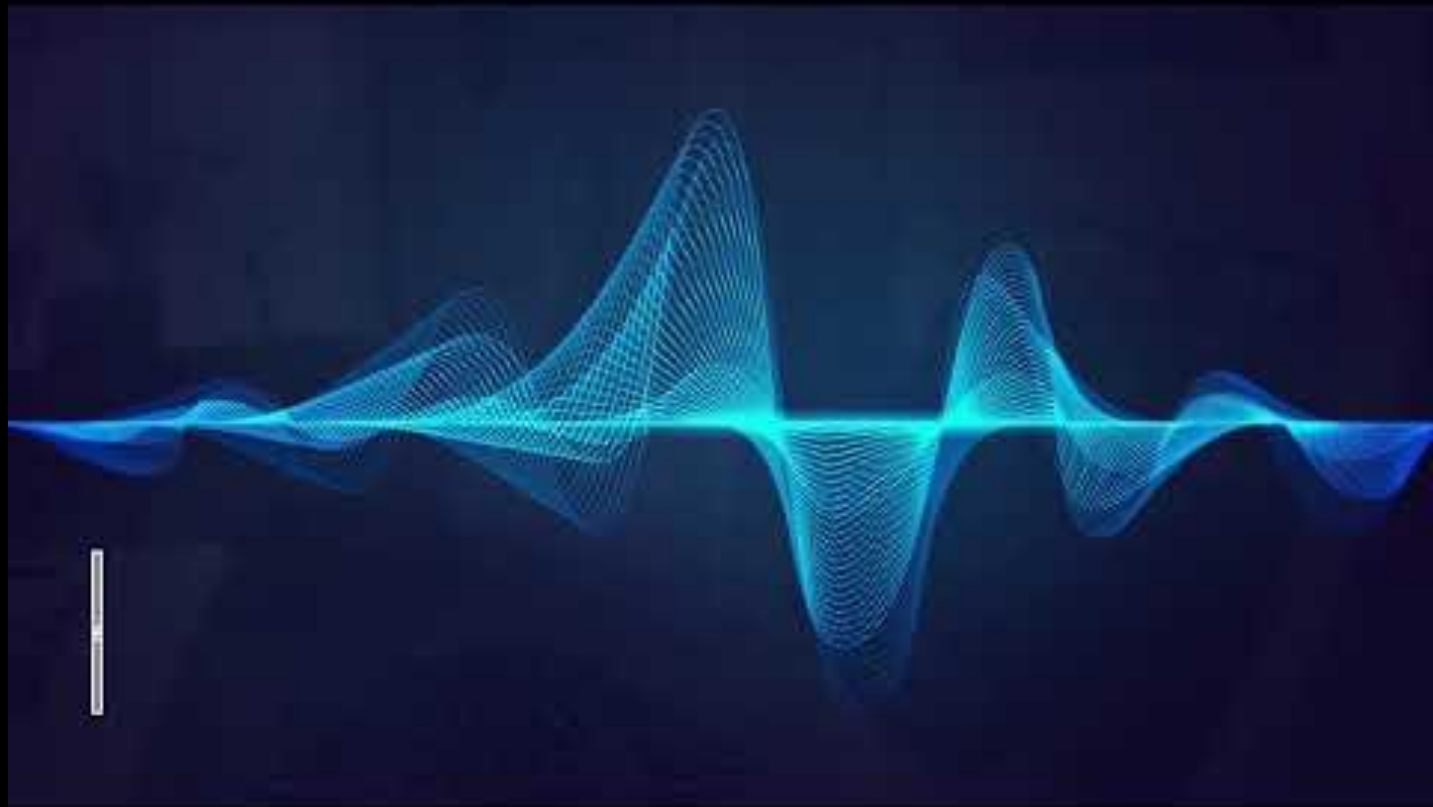
# Conclusions

They're horrible, but you'll love it.

# August Locks

gladiola January 2020





@bigun

- Title: Backup Fun With Video

