Aaron
Vs
The Power Switch

by Aaron Grothe
www.grothe.us
August 17th, 2022

Disclaimer

We are going to be talking about devices that will be working with mains power 110/220v at a US house.

So please as always be careful.

Also any opinions expressed here are mine and mine alone. They don't necessarily represent the opinions of anyone else.

Introduction

If you have questions/comments please feel free to ask them anytime. You don't have to hold them until the end of the talk.

If there are other resources similar to these that you think might be useful to people please let the group know.

Hopefully this will be an interactive and productive session.

The slides for this are at the NEbraskaCERT website https://www.nebraskacert.org/csf and on my home page https://www.grothe.us in the presentations section

A Power Switch???

Why a Power Switch?

Lots of people are buying smart power switches, light bulbs, bluetooth speakers, vacuum cleaners and so on.

A cheap power switch seemed like a worthwhile thing to try

A Power Switch??? (Cont'd)

My initial plan for this talk was pretty simple.

- Try out the plug
- See if it was vulnerable to tcpdump/tcpreplay attacks
- Grab the apk for the smart app from pureapk
- Use jadx and ghidra to rip apart the executable find the key and how it is generated
- Be able to turn the switch off and on from my computer

Instead I got a Tuya and took the red pill :-)

WTH is Tuya?

Tuya is a company that allows anyone to create branded versions of their products. They have over 18,000 partners and something like 60,000 products.

They are rebranded under many different names. Smart Home, Phillips, Scheinder Electric, etc.

We'll hit https://www.tuya.com to take a quick peek at things

Tuya uses industry standard parts/technologies

- Tuya uses ESP8266 (wifi) and ESP32 (wifi/bluetooth) chips in their devices
  - These can be treated as regular arduinos and use the arduino toolchain, or you could put micro python/circuit python on them.
  - Regular tools such as esptool can be used to dump the firmwares from the devices
- In terms of software it uses MQTT and other standard technologies for communicating
  - ATOM IDE, and Arduino studio are typically used for developing software

Wakeup Call

One of the more interesting things I discovered when I plugged in my powerswitch to my wall and did discover devices. I had two powerstrips that were also trying to pair with the app.

I have owned these powerstrips for over a year and wasn't even aware they were wifi enabled.

Home Lab Setup

Used the following for this

- Router with customizable firmware
  - Archer C7 supports both openwrt/ddwrt
  - Went with OpenWRT
    - Ability to install tcpdump with opkg easier than grabbing executables putting on a stick and so on
- Old Android phone to put Tuya app on
  - Moto G5 Plus works for this
  - Was a fine phone in its day and still works pretty well

Home Lab Setup (Continued)

Used the following for this

- Laptop able to work with Archer C7 router
  - This actually was difficult as my usual elitebook would not work with it over wifi
  - Broke down and used my Ryzen 5 windows laptop with a Spiral Linux distribution on it
- Finally the device
  - The Mini Smart Socket from Aliexpress

How did you find out you had a Tuya?

The switch didn't come with any instructions :-(

Had to google the product name Model XS-SSA01 to be able to find out what app to install.

There were two apps mentioned.

Tuya Smart App and Smart Life App

Bit of Github research on Tuya

Doing a search of Tuya on Github.com - gives you the result of 2094 repositories

Needless to say we'll just pick a few of them that look interesting

- TinyTua - python script to allow you to control tuya devices
- Tuya-convert - convert tuya to alternative firmwares :-)
- Tuya-local - locally control your tuya devices
- Tasmota - alternative firmware for Tuya devices
- WThermostatBeca

TinyTuya - python control of devices

TinyTuya - https://github.com/jasonacox/tinytuya

Python library to allow you to control a tuya device on your network

You have to get several pieces of information to be able to control a device

- IP - ip address of device
- Device ID - ID for the device (supposedly unique)
- Local_Key - Local key for control, need to register for IoT account to get this

TinyTuya - status.py

```
#!/usr/bin/python3
import tinytuya

DEVICE_ID="00200441600194467c4a"
IP_ADDRESS="192.168.1.107"
LOCAL_KEY="bf22cefc1e031b38"

d = tinytuya.OutletDevice(DEVICE_ID, IP_ADDRESS,
LOCAL_KEY)
d.set_version(3.1)
data = d.status()
print('Device status: %r' % data)
```

TinyTuya - on.py

```
#!/usr/bin/python3
import tinytuya

DEVICE_ID="00200441600194467c4a"
IP_ADDRESS="192.168.1.107"
LOCAL_KEY="bf22cefc1e031b38"

d = tinytuya.OutletDevice(DEVICE_ID, IP_ADDRESS,
LOCAL_KEY)
d.set_version(3.1)
d.turn_on()
data = d.status()
print('Device status: %r' % data)
```

TinyTuya - off.py

```
#!/usr/bin/python3
import tinytuya

DEVICE_ID="00200441600194467c4a"
IP_ADDRESS="192.168.1.107"
LOCAL_KEY="bf22cefc1e031b38"

d = tinytuya.OutletDevice(DEVICE_ID, IP_ADDRESS,
LOCAL_KEY)
d.set_version(3.1)
d.turn_off()
data = d.status()
print('Device status: %r' % data)
```

TinyTuya - Demo

We'll give it a shot and see if we can turn the powerswitch on/off and so on. Hopefully it'll all work tonight.

One tip: Only one app can be talking to a Tuya device at a time, so if you've got the app open and are trying to use tinytua at the same time, you're going to have some issues.

LocalKey???

WTH - is a local key?

A local key is something you generate by signing up for an account at https://iot.tuya.com

Go to cloud services and take a look around a bit

By registering with this I was able to get to this.

Tuya-Convert

Tuya-convert - https://github.com/ct-Open-Source/tuya-convert

Is a project to make it possible to flash alternative firmwares onto your device without having to open the device up

The webpage also has a lot of great information about Tuya devices as well.

Tuya-Convert

Has a reference to vtrust.de - who did a really good job at analyzing the security of tuya from 2018:

https://media.ccc.de/v/35c3-9723-smart_home_-_smart_hack

Unfortunately it is in German and my german is pretty limited.

Tuya-Local

Tuya-Local - https://github.com/make-all/tuya-local

System to allow you to locally control all your Tuya devices

What I find cool about it is that it gives a list of some of the devices that it supports

Humidifiers, Air Purifiers, Vacuums, Power Switches, Kettles, Sirens

Tasmota

Tasmota - https://github.com/arendst/Tasmota

Alternative firmware for Tuya devices - full source/full control

Has one of the best pieces of advice you will find. "Unless your Tasmota powered device exhibits a problem or lacks a feature that you need, leave your device alone - it works so don't make unnecessary changes!"

WThermostatBeca

WThermostatBeca - https://github.com/klausahrenberg/WThermostatBeca

Alternative firmware for Tuya Thermostats - full source/full control

Nice project that talks about the standard infrastructure and how you can insert yourself into it. If you have one of the thermostats offers a lot of options.

ESPtool

ESPtool - https://github.com/espressif/esptool

Is a tool to dump the current firmware in an esp8266 device. It provides this in a dump format.

./esptool.py -h

Have to hook up to the pins on the device

It is an Arduino!!!

I know I mentioned this several times, but it bears repeating. Their IoT devices are Arduino compatible.

This means there are a whole group of people who know how to program these devices. The barrier to entry is very low.

For example the next slide is a wifi-scanner from https://techtutorialsx.com/2017/02/25/esp8266-scanning-wifi-networks/ to give you an idea how easy it is

It is an Arduino!!!

```
#include "ESP8266WiFi.h"

void setup() {
  Serial.begin(115200);
  int numberOfNetworks = WiFi.scanNetworks();
  for(int i =0; i<numberOfNetworks; i++){
      Serial.print("Network name: ");
      Serial.println(WiFi.SSID(i));
      Serial.print("Signal strength: ");
      Serial.println(WiFi.RSSI(i));
      Serial.println("-----------------------");
  }
}
```

It is an Arduino!!!

So how hard would it be to add additional functionality to the firmware of one of these devices?

IoT Tuya Site

Time to go back to the Tuya IoT site https://iot.tuya.com and take a deeper look at it

I was playing around with creating an RGB mouse pad. That might make a nice "giveaway" to certain targets.

You can upload custom firmware, use their firmware, etc. The options are truly unlimited.

Firmware Update options

There are options to flash new firmware onto the device after it has been deployed. These request the user allow it from the Tuya app.

Also Tuya is a Chinese company. Theoretically that means they might be forced to do things legally in terms of backdoors if there was a "sensitive" target.

Need to mention rumors of "special" itunes/google chrome and other tools.

Tuya IoT SIM options

Tuya has begun to offer devices with SIM options, this means 4g lte/5g data network access is coming. This opens up a whole new world of possibilities.

While it might be harder to slip a SIM into a power plug, a powerstrip is another option, or a humidifier, etc.

How many companies have all of their IoT devices separated onto a different network or extensive access control rules to restrict access?

Companies Go out of Business

Tuya has over 8,400 customers. Some of those are going to go out of business. What is to prevent a bad actor from buying the assets of one of those companies and using their ability to update firmware in the devices to do something less good?

That is even assuming all of their 8,400 customers are operating in good faith.

Free USB Sticks 2.0???

One of the tests that security firms would do was to drop some usb sticks in the parking lot of a company and see who would actually try and put them into their computer.

Now we are talking about the possibility of getting nicely designed products built that you could arrange for people to get.

Even better - who wouldn't want a cool RGB mouse pad you can control from your phone. If you work from home, it might even be your kid who sets it up.

Summary

- I started going down one path initially and ended up going down a totally different path
- Tuya is both amazing and scary at the same time. I might actually see how much it would cost to get a custom RGB mouse pad from them and have it have a custom firmware on it. To get one of the devices built is probably relatively expensive, but am curious.

Q & A

Any Questions?

Thanks for listening.