**Tracking Ownership:**

The Philips Hue IoT White Light Bulb offers a unique approach to home lighting. The bulb allows users to design unique arrangements that take advantage of the bulb's built-in wifi connectivity, where the bulb can connect to Apple's HomeKit and be controlled by an iOS device. Its press material boasts that it "lets you control your lights from your bedroom or your backyard" even when you're not at home, and helps capture "the right ambiance for any moment" with a variety of digital settings that adjust color, set timers, and more.

But beneath the surface, the lighting system doesn't appear all that secure. Each bulb connects to the Philips Hue Bridge, which pulls data about its on/off status, as well as color and brightness variables from the web, applying such setting to each bulb. It also pushes new data to each bulb through similar means. Bulb connect to the Bridge system through an [open-standards protocol](https://www.developers.meethue.com/documentation/how-hue-works) called [ZigBee Light Link](http://www.zigbee.org/), which creates a mesh network that connects each light together, allowing them to pass signals between one another without the risk of a dropped connection. Last year, students at Dalhousie University in Halifax, Canada hacked this ZigBee system, infecting a single bulb with bugged software that allowed them to connect to the mesh network and catastrophically spread the bug to all the lights in the system, allowing the hackers to manipulate lights throughout the unit, which in some cases can be as big as an entire city. In a [paper](https://pdfs.semanticscholar.org/b457/e4b95a70f8d1726ba70885ee10c13e43330b.pdf) published by the students, they note that the bug could spread to a critical mass the size of Paris given that enough bulbs are present within the 105 square kilometers of the city. But even on a small scale, this mesh system poses obvious risks.

The system also can also sync with Apple's HomeKit system, allowing the lights to be controlled from within Apple's native iOS operating system. HomeKit is linked to user's iCloud account which, though encrypted, still places a heavy security risk on a single account. Apple's AppleID system has been [notoriously](http://www.businessinsider.com/apple-id-protect-password-from-turkish-crime-family-hack-2017-3) the victim of hacks in the past, and even it's heightened security features like two-factor authentication can be [laughably insecure](https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess) since it largely relies on text message and email authenticators, both of which have their own vulnerabilities.

**Replicate and Replace:**

In response to this problem, I've built a simple IoT LED lighting system that allows smartphone users a similar series of options without the security risks. Using the Blynk application for Apple's iOS operating system, I made a simple button that toggles the LED light between on and off, allowing users to turn their lights off through a similar wifi-based remote connection. This required me to write a program in Arduino that lets users toggle the light switch within the Blynk application.

Our Photon RedBoard communicates with Particle.io for its wifi connectivity, which itself is built on [Heroku](https://www.heroku.com/) and hosted by [Amazon Web Services](https://aws.amazon.com/) and its cloud-computing network. Though Amazon tends to be a pretty transparently monopolistic force on the internet these days, its web services are largely secure and continue to power some of the internet's biggest sites. While it's safest to host the data on your own servers, web services like Amazon and others offer cheap alternatives that can be secure in the right hands.