Secure Home Automation

Chukpozohn Toe*
Department of Computer Science
University of Massachusetts Lowell
ctoe@cs.uml.edu

***Abstract*—Home Automation has become increasingly popular in recent years. Home automation is a way to make smart homes. Many companies have taken it upon themselves to create entire systems of home automation for their users. There are also open source home automation projects that enable developers to create their own home automation, but many have not focused on the security of these IoT devices involved in these systems of home automation. Many also have neglected to focus on the security of home automation itself. In this paper, I propose a secure form of home automation. I introduce a method to secure the communication between devices involved in the home automation such as a raspberry pi, a database, and a smart phone. In the future, I plan to introduce EEG sensors into my home automation to enable users to control devices in their homes. Here I focus on these main areas.**

***Index Terms*—Zigbee, zigpy, bellows, Home Automation, Android, IoT, Security**

I. Introduction

Home automation, or domotics, is building automation for a home, called a smart home or smart house. These home automation systems' abilities range from monitoring devices to controlling devices such as lights and appliances. There are many different home automation devices out there. Some of these devices come with their own system of operating them such as an app, and those are those that are open-source. One of these is Home Assistant which is a free and open-source home automation software designed to be the central control system in a smart home or smart house. I took it upon myself to start to create my own home automation system that focuses on security to address the widespread vulnerability of IoT devices; and also to enable users to control devices via their mind using an EEG in the future. In my home automation system, I'm using five main devices: 1) A Raspberry Pi 3, 2) A Zigbee Shield and 3) Innr Zigbee smart plugs 4) An android phone 5) and EEG sensor. My reasoning for using these five devices is that I am able to write my own code to create my home automation system using them. Many of the smart devices do not allow the user to manipulate it by writing their own code for it. Most of the smart home devices are prepackaged which means they are meant to be used right out the box.

II. RELATED WORKS

There's an entire community of people out there creating their own home automation using the same hardware I am using or very similar ones that work for the same purposes. These people, including myself, are using a python library which is still under development, zigpy/bellows. There's a github page where we all post questions about the issues we are having in order to get help from others including the developers of the libraries. One user Daniel built an application using the libraries that allows devices to join a network. He controlled these devices via a HTTP API. This will be very useful as it was one of the very few projects that that actually showed how to interface with the libraries. I modeled my implementing very closely to his.

III. Overview

My secure home automation system consists of three main devices: (a) an Elelabs Zigbee Raspberry Pi Shield (b) an Innr smart plug (c) a Raspberry Pi 3. This is the hardware that runs the system.

A. Elelabs Zigbee Raspberry Pi Shield: The Elelabs Zigbee Raspberry Pi Shield is designed specifically for Raspberry Pi (1,2,3). It is based on EFR32MG1 SiLabs chip, which is a 2.4-GHZ, IEEE 802.15.4/Zigbee microcontroller. It is preprogrammed with Network CoProcessor firmware and provides the UART interface to Raspberry Pi to form and manage the Zigbee network, as well as communicate with Zigbee devices easily.

B. Innr Smart Plug: This smart plug uses Zigbee communication protocol. These smart plugs can be used by connecting it to "SmartThings" which is a home automation app that enables you to control your smart devices such as smart plugs.

C. Raspberry Pi 3 Model B: The Raspberry Pi 3 Model B is a single-board computer with wireless LAN and Bluetooth connectivity. It has Quad core 1.2GHz Broadcom BCM2837 64bit CPU, 16GB RAM, 40-pin extended GPIO, and 4 USB 2 ports. This small and powerful computer is where most of the code for the system is written.

The secure home automation use primarily two external software; (a) zigpy (b) bellows and (x) Android Studio.

A. Zigpy: zigpy is Zigbee protocol stack integration project to implement the Zigbee Home Automation standard as a Python 3 library.

B. Bellows: bellows is a Python3 library implementation for the zigpy project to add Zigbee radio support for Silicon Labs EM35x("Ember") and EFR32 ("Might Gecko") based Zigbee coordinator devices using the EZSP (EmberZNet Serial Protocol) interface.

C. Android App: The Android app I'm developing is the software that gives us easy access to turn on and off devices connected to the smart plug.

IV. The layout of the devices in the home automation

At the heart of the hardware layout is the database which store all the information of the system. The Raspberry Pi connects to the database. The zigbee microcontroller is connected to the Raspberry Pi by means of the GPIO poins and it's powered by the GPIO pins too. On the other side of the system is the android app which connects to the database and the EEG sensor will be connected to the android app.

V. struct of the home automation

The heart of the home automation starts with the program ezsc that is an interface for zigpy and bellows libraries. It is a well documented version of the application that Daniel wrote. The application scans for zigbee devices on the network. Using zigpy, it stores the devices information in a sqlite database. Now comes in the main program. It contains the functions and the calls to functions that carries out specific routines for the system. It imports the database connector file which is the interface between my system and the MySQL database I set up in AWS. The purpose of the database is that I can store information about the devices. There is one table in the database consisting of four attributes: 1) the unique IEEE number of the devices, 2) the name of the device, 3) the action to be performed by the device such as on/off and 4) the status of the device which denotes if a specific action was successfully carried out or not. On one end of the database is the Raspberry Pi which is responsible for inserting the IEEE number it obtained from the device and also the status after it has carried out an action. On the other end is the android app which is responsible for the name of the device and also the action that is to be carried out. All of these work and will work in such a way create a very easy to use system. The last thing that will be implemented will be the use of the EEG sensor which will enable user to control the devices with their mind.

VI. Conclusion

This work has the potential to develop a more secure home automation system. With the help of my mentor who has experience is this field (Prof. Mohammad Arif UI Alam), we could implement a safer home automation system that allows for reliably safe communication between devices. Furthermore we can implement an EEG sensor such that it enables quadriplegic or otherwise disabled individuals to have more control over their home. This will be done by enabling them to directly communicate with the smart devices on the system by sending commands gathered by the EEG sensor they are wearing.

I have provided documentation of the discussions between the developers of zigpy and bellows. During the process of these discussions, I was able to set up the devices on the system and learn how to use the library. Please check the documentation.

References