CEN 4010 Principles of Software Engineering, Spring 2018
Milestone 1 Project Proposal and High-Level Description
Team: Pogchamps 13
Project: IoT Equipment Access Control
Members: Erin Knapp, Henry Herzfeld, David Patch, Jerad Branscum, Mike Bures,
Romael Simmonds
February 9th, 2018

Revision History

Initial Draft	2/9/18
Second Draft	2/17/18

Executive Summary

The Equipment Access Control product will be a secure and user-friendly app/web interface for controlling access to any amount of equipment. This project will be highly scalable for both small and large networks. The Sonoff wifi wireless switch works in conjunction with the app/web interface to remotely control when equipment should be turned on or off.

A sleek interface allows end users to easily and securely sign on to the network, select the equipment they wish to use and the time they need. When equipment is not in use it will remain off to protect the equipment from power failures or hacking attempts.

Administrators are able to provide and deny access to any equipment for any user based on the company's requirements for user access. Administrators can allow permanent or temporary access to a specific user for specific equipment. Temporary access is granted for an allotted time of the administrator's choosing.

This product is ideal for small businesses, college labs, private labs, large businesses and even home use. Small business owners and large businesses can delegate which employees can use any expensive or dangerous equipment to protect employees as well as the equipment. College and private labs can manage which users are allowed equipment access based on training level. Parents can select how long their children can use the Xbox or protect children from using dangerous equipment in the garage such as power saws and woodworking equipment. Anyone with a network who wishes to protect people and equipment can use this product with ease.

Competitive Analysis

Competitive Products	**Our Product**
Network security	Network Security
Expensive	Inexpensive
Access controlled doors with card readers	Wide range of appliances
Interfaces with door controllers	Interfaces with Wi-Fi electronic switches
Used by facility managers/administrators	Used by students and administrators

Currently, there are several apps on the market offering remote security access. These secure apps connect to home or business security systems or special doors. Ours offers a middle ground with the ability to securely turn electronic on or off without needing to be connected to a full security system.

Data definition

IoT/Internet of Things: is defined as the interconnection of Internet enabled devices and everyday objects allowing the transfer of data
Benches: is defined as a workbench with electronic equipment
Equipment: any device that needs to be access controlled
Soldering Iron: a tool that melts solder which joins metals. In this context, soldering irons are used to join electronic components
User: any person requiring access to equipment
Admin: any person controlling access to equipment
Front-End: the user and admin view of the equipment access program as viewed from a mobile device or computer
Back-End: portion of the equipment access program hidden from users and admins. This is how the program works
Sonoff: Wi-Fi enabled product that allows for devices to be switch on and off remotely
Git/GitHub: Version control system for project. This allows the developers to track changes to the program during development and maintenance of the program.

Overview, scenario, use cases

In a college or private lab, faculty, managers and staff may need to control students' or employees' access to certain pieces of equipment. For example, some equipment may be expensive or dangerous and therefore only students or employees' who have demonstrated ability to properly use it should be granted access. In other situations, students may only need access to equipment for certain classes or projects or employees may need to access equipment for certain projects.

Their professors or managers should be able to grant or deny access for the duration of a class or project. Lastly, students working on independent projects who have demonstrated knowledge of how to use equipment should be able to request access for a given period of time. In all of these situations, faculty, managers and staff need to be able to control which students use which equipment and for how long.

In a small or large business, administrators or management may also want to restrict access to equipment to certain employees for certain reasons such as the user's skill level, user's need, and for certain lengths of time. This may be because equipment is expensive, dangerous, or difficult to use properly. An access control system would help employers save time, money, and liability in the event of an employee injury from equipment.

Lastly, in a home setting, parents may need to restrict a child's access to equipment such as TVs, video game consoles, or dangerous power tools. Such a program would allow the parents to ensure their children are not spending all day playing video games and watching TV or accidentally injuring themselves on power tools.

Initial list of high level function requirements

1. Remotely control access to engineering laboratory equipment.
2. Allow administrators (faculty/staff/admins) to deny/permit access to equipment
3. Allow students to request access to equipment
4. Wifi-encryption to prevent hacking
5. Website and mobile app interface

List of non-functional requirements

1. Must be easy to use by students and faculty/staff
2. Accessibility for users with or without mobile devices
3. System should always be working
4. Must be secure and on accessible according to university standards
5. The expected load is 1 - 60 users at any given moment.

High-level system architecture

We will be using PHP with Laravel for our project. Laravel front-end uses Bootstrap and Vue frameworks installed using NPM. Laravel Mix is an API provided for webpack and asset compilation. Any preprocessor can be used with Laravel framework. Laravel commonly uses the Vue Javascript framework but any other framework can be used instead or in conjunction with Vue.

NodeJS will also be applied because it is lightweight and easily scalable for all network applications. Laravel also has built in security features for authentication, encryption, hashing and password reset.GitHub will be our code repository and version control system.

Supported browsers: Chrome, Firefox, Internet Explorer, Microsoft Edge, Safari, Opera. For a more detailed look at how much support each browser lends to HTML5 and CSS3, we will consult the HTML5 and CSS3 Readiness website.

Licenses

- Laravel: open-sourced software licensed under the MIT license.
- PHP: PHP 4, PHP 5 and PHP 7 are distributed under the PHP License v3.01, copyright(c) the PHP Group. This is an Open Source license, certified by the Open Source Initiative. The PHP license is a BSD-style license which does not have the "copyleft" restrictions associated with GPL.
- Bootstrap: Code and documentation copyright 2011-2018 the Bootstrap Authors and Twitter, Inc. Code released under the MIT License. Docs released under Creative Commons.
- Vue: open-sourced software licensed under MIT license.
- NPM: open-sourced
- NodeJS: open-sourced and free to use under this license.
- GitHub: Licensed under CC0-1.0.

Team

- Erin Knapp: GitHub Master
- Henry Herzfeld: Back-End Team Lead
- Jared Branscum - Scrum Master
- Mike Bures - Front and back end developer
- David Patch - Product Owner
- Romael Simmonds - Front-End Team Lead

Checklist

- Team decided on basic means of communications: DONE
- Team found time slow to meet outside of the class: DONE
- Front and back end team leads chosen: ON TRACK
- Github master chosen: DONE
- Team ready and able to use the chosen back and front-end frameworks: ON TRACK
- Skills of each team member defined and known to all: ON TRACK