Boston University
Electrical & Computer Engineering
EC464 Capstone Senior Design Project

User's Manual
VETCON BADGE ASSEMBLY AND OPERATION

Submitted to:

VETCON
(910) 551-6746

Mike Jones
jonesmlr@gmail.com

BY:

Team 32

VETCON Badge

Team Members

Ryan Sullivan ryanbs@bu.edu
Derek Barbosa dbarbosa@bu.edu
John Kircher kircherj@bu.edu
Carlos Ortiz cartex10@bu.edu
Julian Padgett jpadgett@bu.edu

Submitted: 03/25/22

Table of Contents

Executive Summary

We, Team 32, are working closely with our client (VETCON) – a group of information security professionals who have served in the armed forces of the United States or close allies– to provide a detailed blueprint for an identification “badge” to be used by VETCON in the upcoming DEFCON conference that sticks with a Cybersecurity theme.

In other words, VETCON wants a unique, functional, and production-ready badge for DEFCON 30. This DEFCON badge will provide customizable identification for VETCON attendees and as a collection of interactive minigames on a consistent hardware “platform.”

1 Introduction

Every year, DEFCON, the largest underground hacking conference, employs unique badges that feature complex puzzles, electronics, and artistically designed circuit boards that allow different “villages” (DEFCON groups) to interact with each other beyond hacking competitions and research conferences.

This year, our client, VETCON (a group of information security professionals who have served in the United States armed forces and its close allies, and one of the villages present at DEFCON each year) wants to create a cost-friendly but unique badge that DEFCON attendees can purchase to interact with others. However, developing a badge takes time. Badge developers need to consider many components: not only do they need to order parts, but they also need to create a badge production process that does not exceed a given budget. Moreover, VETCON wants to create a badge that stands out. The badge should be visually sophisticated and aesthetically pleasing so that attendees see it and immediately want to purchase one.

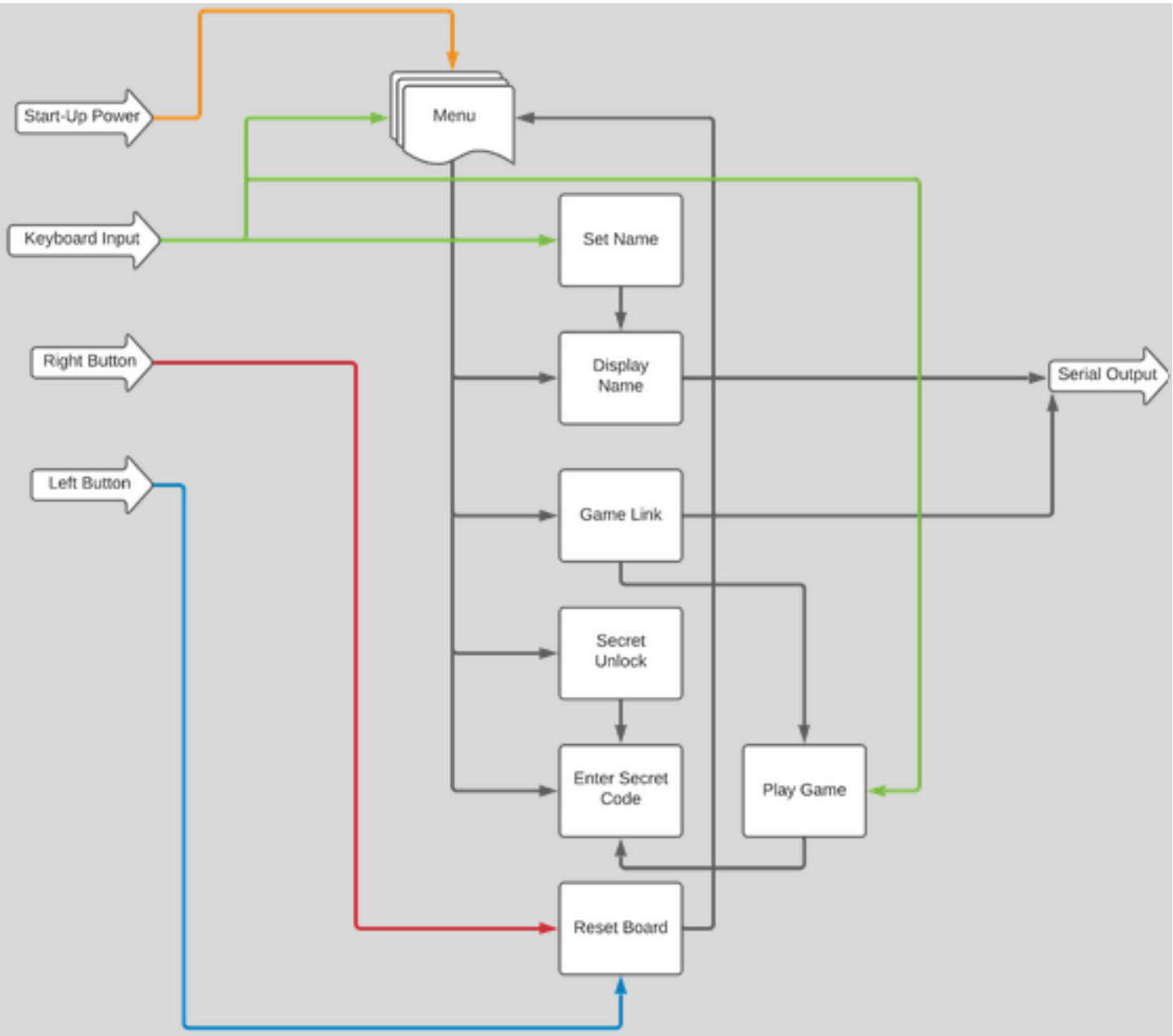
The badge we have designed for VETCON to distribute at DefCon is powered by Texas Instruments' MSP430FR2433 microcontroller (MCU). A big reason for this choice is that the controller is part of the lowest-cost family of MCUs for sensing and measurement applications. The architecture, FRAM, and integrated peripherals, combined with extensive low-power modes, are optimized to achieve extended battery life in portable and battery-powered sensing applications. The onboard software is written in a stripped down version of C++ that is compiled with an open source framework toolchain called Wired, which is automatically deployed through a compilation of scripts and toolkits through PlatformIO – this enables us to interface and flash the MCU.

Our badge also includes unique peripherals that allow for an engaging user experience whether it be communication, customization, or the unique challenges on the badge. These include: 1) the HC-05 wireless bluetooth module which has been programmed for users to have simple communication with other badge holders. 2) A 16x2 alphanumeric liquid crystal display allowing users to display a name of their choice and other customizable glyphs. 3) An array of LEDs to display user progress for the challenges provided. 4) Push buttons that allow badge reset capabilities. The badge also includes 3 games/puzzles which can be accessed in a progessive manner (you can’t access the next puzzle without solving the previous one). Each game/puzzle includes unique ciphers and codes that vary in difficulty and can even penalize the user and restart their progress if the ciphers are not decrypted correctly.

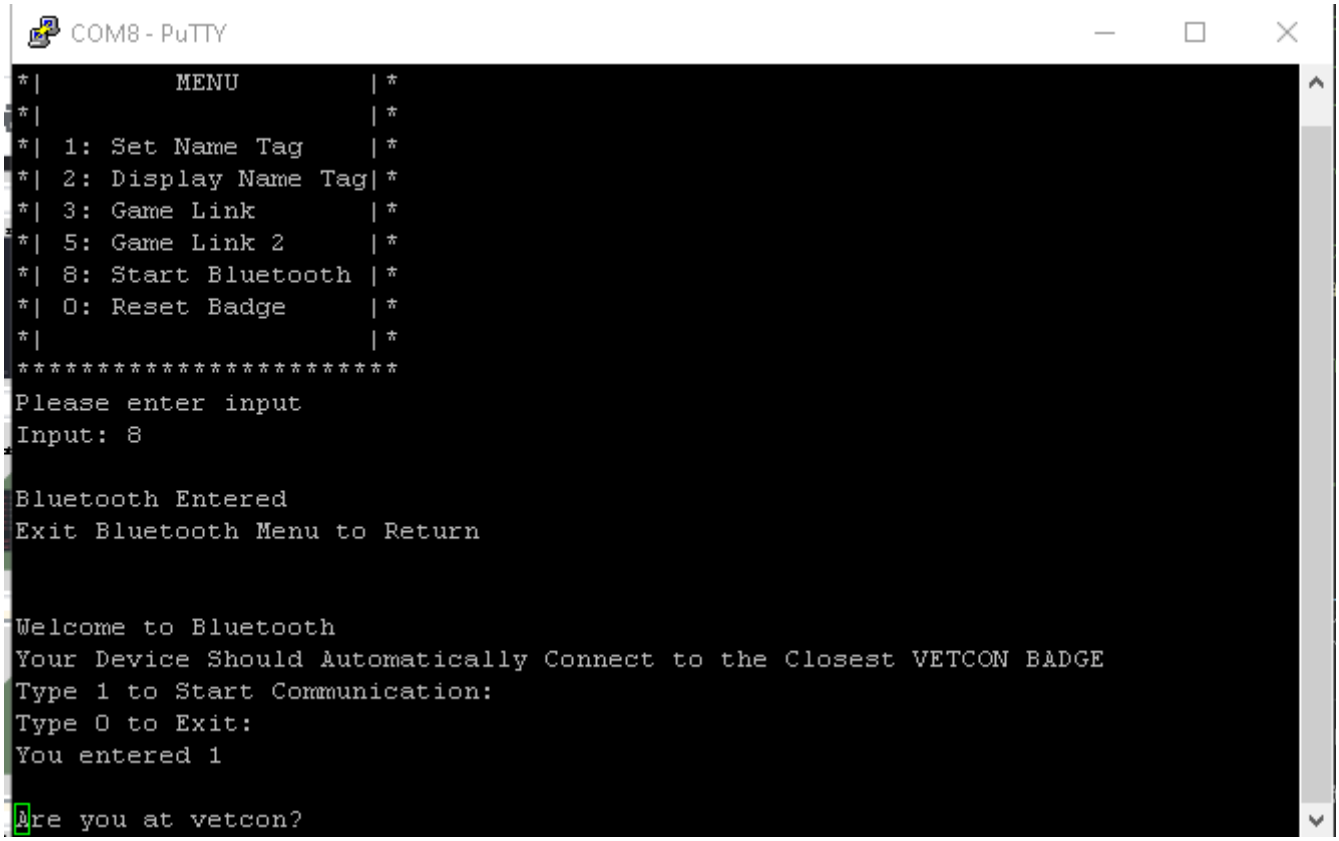
Ultimately, the badge we have produced for VETCON is unique, functional, and fun. The remaining sections of this document will dive into a more technical overview of the badge as well as its general operation and a breakdown of the user interface and setup.

2 System Overview and Installation

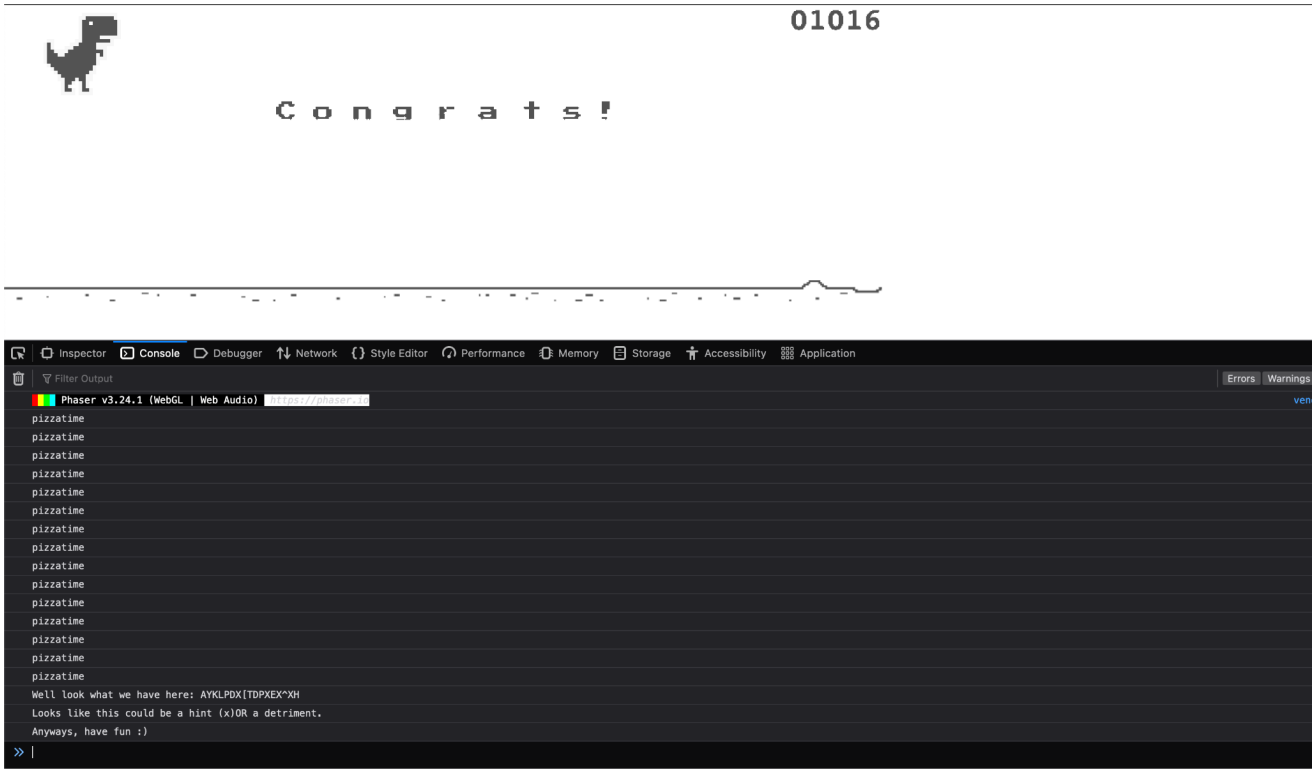
2.1 Overview block diagram



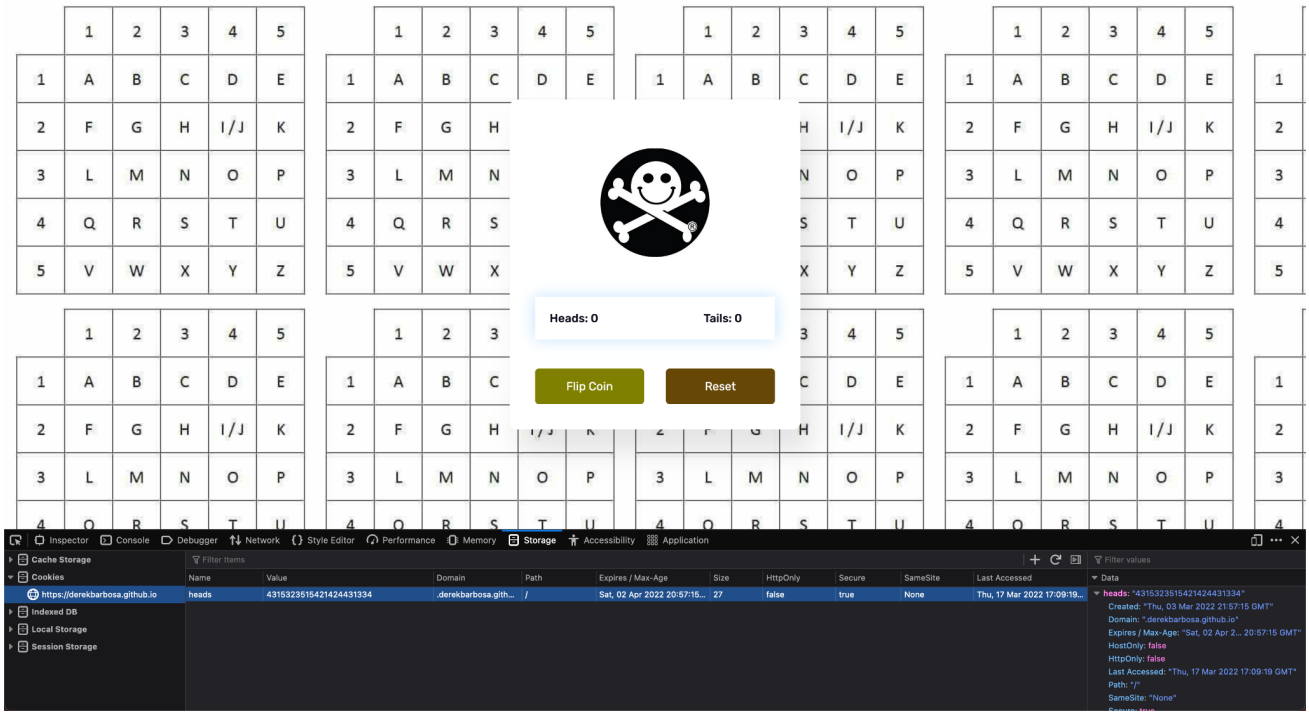
2.2 User interface.



Initial Menu at Startup (upon connection).



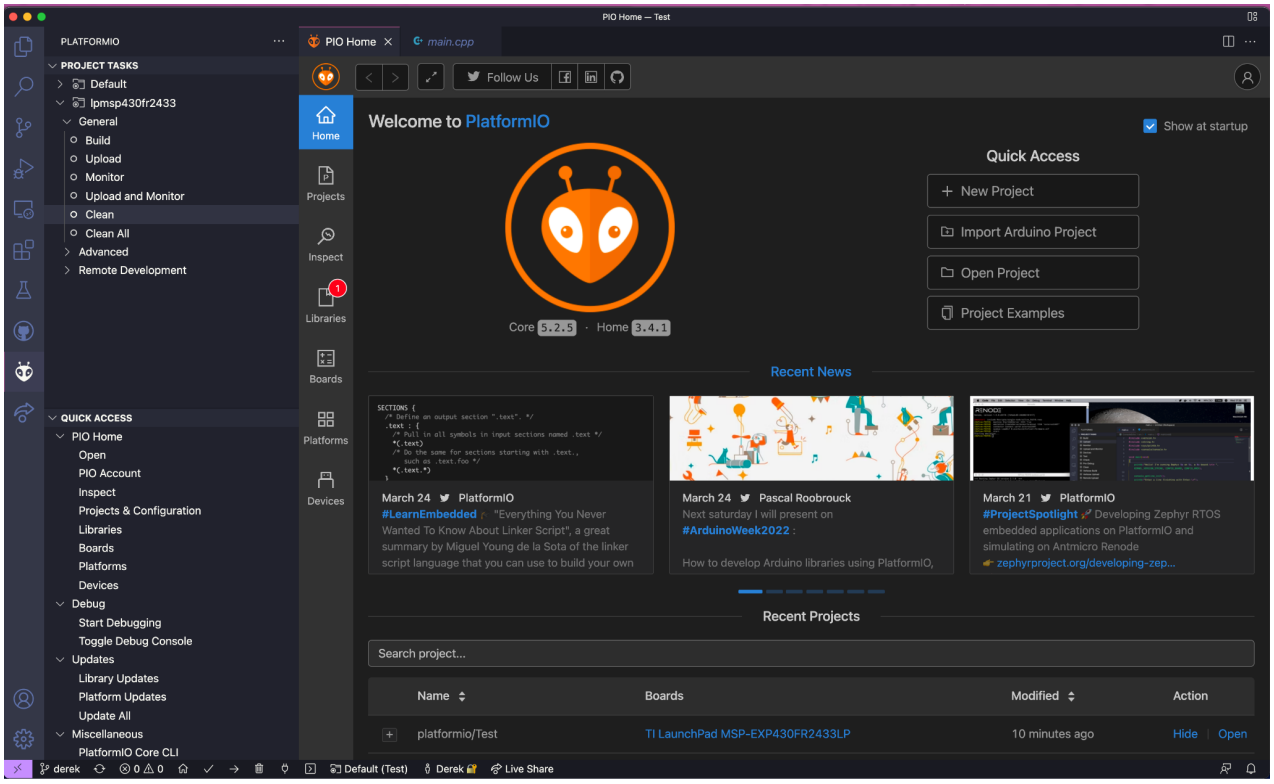
Minigame #1 and subsequent “secrets”

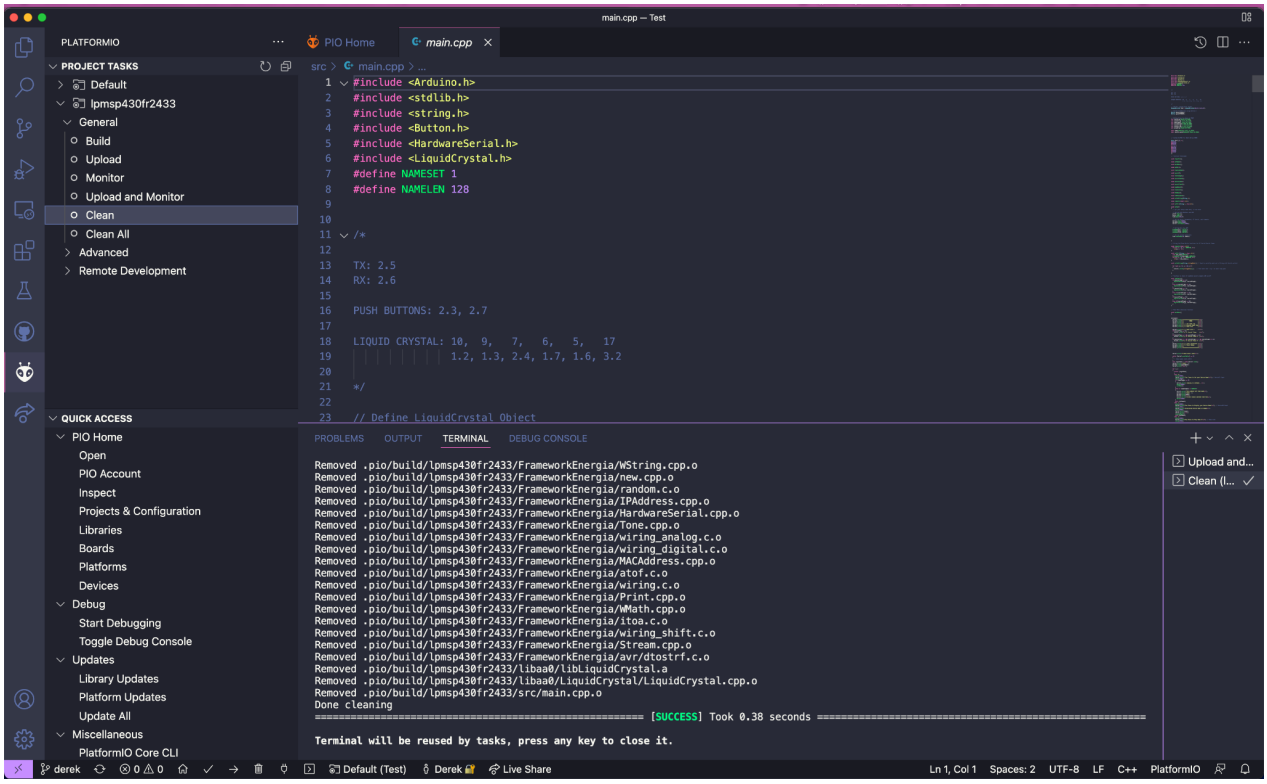


Minigame 2 and subsequent “secrets”

```
A seasoned veteran!
Loading day: 45

These are your current stats
Grades: 110      Health: 170     Social: 140     Money: 100
You're thinking of attending the next DEFCON. You're deciding to bring.

[1] Bring your laptop and phone so you can play all the games and make some friends :)  [2] Bring nothing.

2
You have a good time.
Loading day: 46

These are your current stats
Grades: 110      Health: 170     Social: 140     Money: 100
You're running low on cash, you see a poster advertising firms that will buy your plasma for a hefty amount of cash.

[1] Do it. You could use the extra few hundred bucks.   [2] Turn it down, you have standards.

1
Payday is good! And you got some cranberry juice out of it too :)
Loading day: 47

These are your current stats
Grades: 110      Health: 170     Social: 140     Money: 130
A fellow student created a new Crypto Token called Terrier Coin, he attempts to convince you to throw a few bucks into it.

[1] You agree, begrudgingly.    [2] Refuse, you're not a crypto person.

1
The coin explodes overnight, with a 1000% gain. Your few dollars turned into a couple hundred fast.
Loading day: 48

These are your current stats
Grades: 110      Health: 170     Social: 140     Money: 160
You're late on an assignment. You're almost finished but the deadline is five minutes away

[1] Accept defeat, finish the assignment, and move on.  [2] Send a fork bomb to the submission portal

1
Your homework average takes a hit, but you can pull through in the class
Loading day: 49

These are your current stats
Grades: 90       Health: 170     Social: 140     Money: 160
You're considering a semester abroad

[1] Apply for it        [2] Eh another semester

2
You miss out on a great time but your friends are glad you stayed and you can really focus on your grades.
Loading day: 50

These are your current stats
Grades: 120      Health: 170     Social: 150     Money: 160
What's that noise?

[1] Investigate.        [2] Ignore it.

1
I'M IN YOUR WALLS I'M IN YOUR WALLS I'M IN YOUR WALLS I'M IN YOUR WALLS I'M IN YOUR WALLS I'M IN YOUR WALLS I'M IN YOUR WALLS

 Congratulations, you win. I hope you're happy with yourself. Take a look at the clock, how much time did you waste?
Well, here's your 'secret surprise' you wanted this whole time. I guess i'll just be here... alone.... forever.
SECRET UNLOCKED         SECRET UNLOCKED         SECRET UNLOCKED         SECRET UNLOCKED         SECRET UNLOCKED         SECRET UNLOCKED         SECRET UNLOCKED         SECRET UNLOCKED         SECRET UNLOCKED         SECRET UNLOCKED         SECRET UNLOCKED         SECRET UNLOCK
D         SECRET UNLOCKED         SECRET UNLOCKED         SECRET UNLOCKED
696c6f7665576574636f6e
```

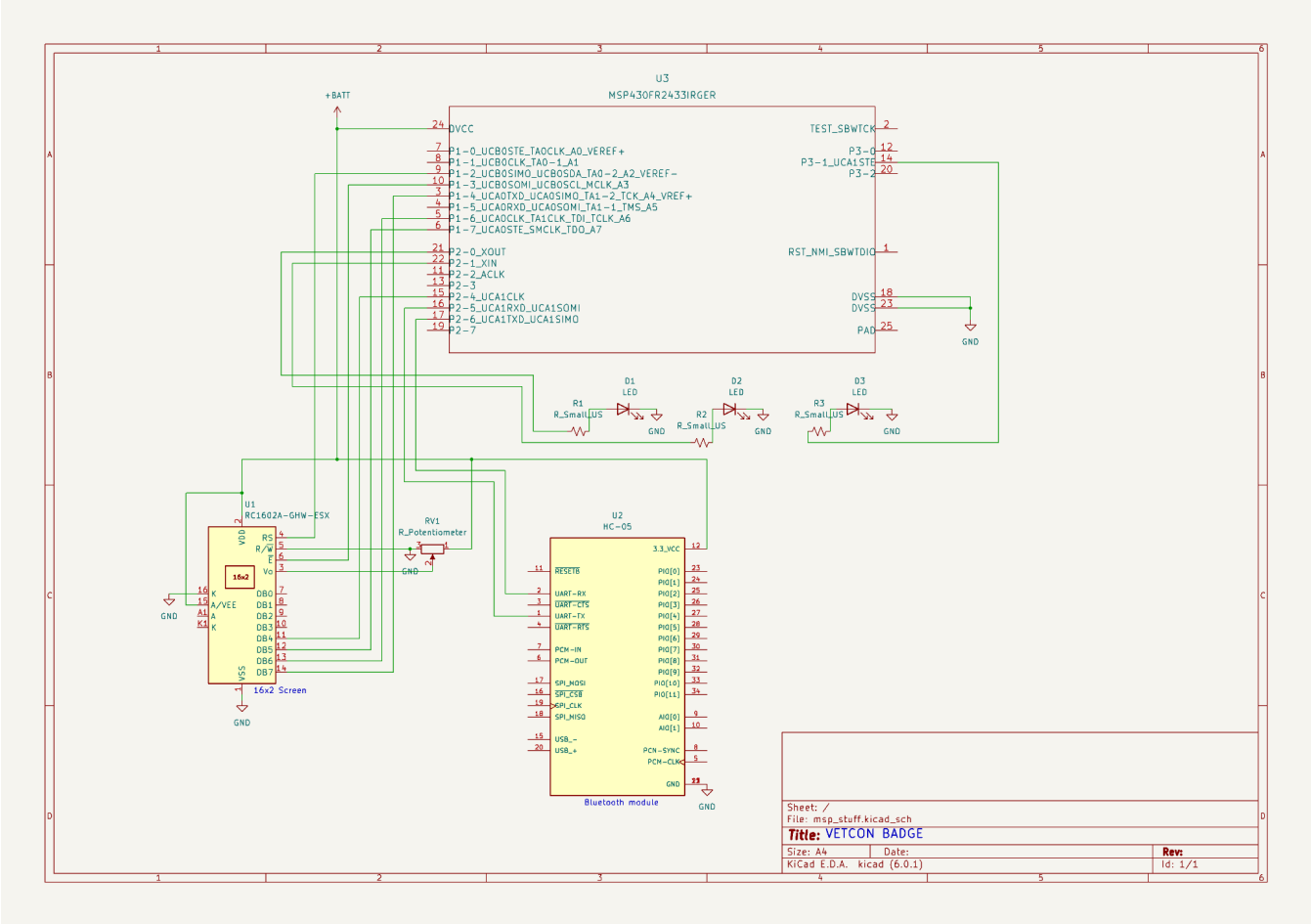
Minigame 3 and subsequent “secrets”



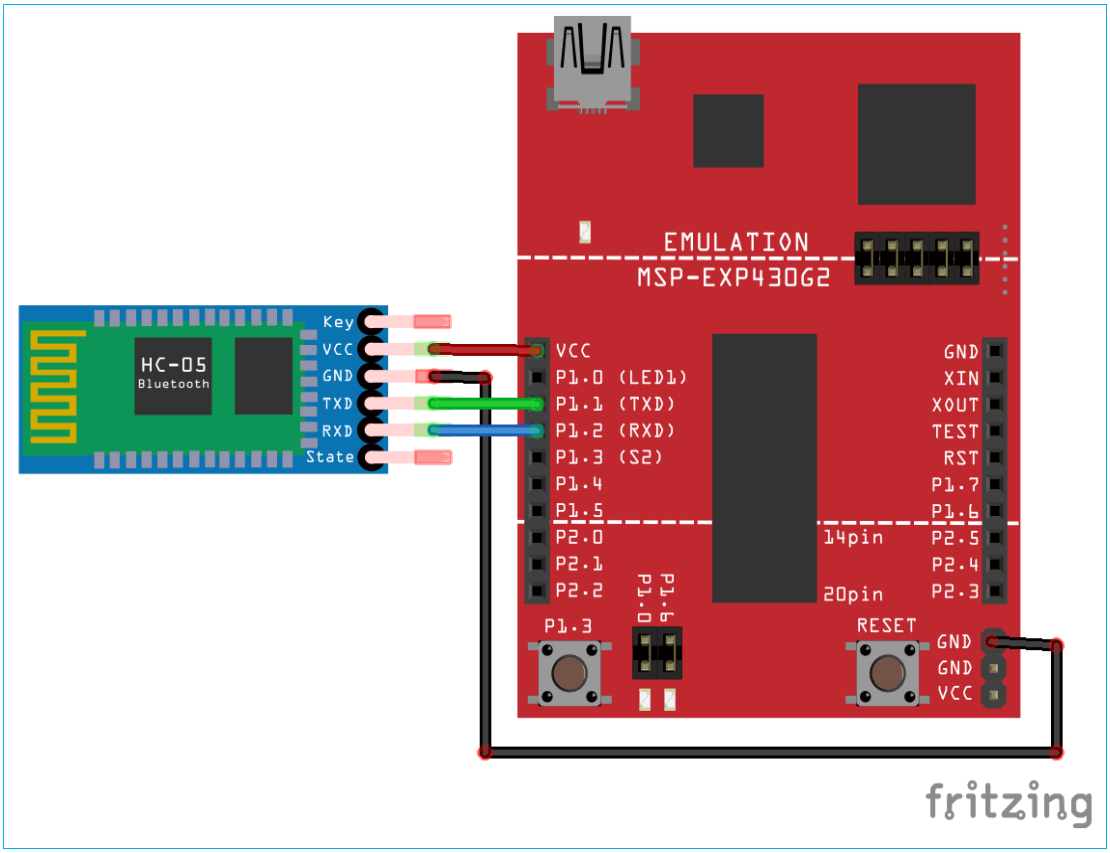


PlatformIO Flashing/Build Process

2.3 Physical description.



Schematic for complete prototype circuit



Colored representation of Bluetooth Module hookup.

2.4 Installation, setup, and support

Services Needed:

1. PlatformIO (Arduino Framework, C++)
    a. PlatformIO will be used for flashing our software to the board
2. Visual Studio Code
    a. Used in tandem with PlatformIO
3. Software (Available with invite to our private repo)

Setup:

To flash software:

1) Plug in MSP430FR2433 via USB-C to laptop with PlatformIO
2) Open Visual Studio Code
3) Open downloaded software project via PlatformIO
4) Select PlatformIO with VSCode
5) Click upload.

Once the flashing process has been completed, the badge is ready for use and can be distributed to users. Please see support below for specific badge operations.

Support

1) Power
    a) Switch the power button on/off to activate/deactivate the badge. i) / ii) show badge is running properly.
        i) LCD will initialize with “Welcome to VETCON 30”.
        ii) Bluetooth module status LED will flash rapidly.
2) Serial Communication
    a) USB-C cable serial communication will be initiated once plugged into a user's computer. COM port will look like MSP - UART in a device manager.
        i) Serial Preferences (widely accepted default serial settings):
            (1) Baud Rate: 9600
            (2) Data Bits: 8
            (3) Parity: None
            (4) Terminal / Logging: Implicit CR in every LF (Highly recommended)
3) LCD / Potentiometer
    a) LCD includes a backlight switch to turn on/off the backlight for the display
    b) Potentiometer controls voltage received by the LCD to make the backlight brighter or dimmer
4) Bluetooth
    a) Command mode (enable switch on)
        i) In command more the LED should slowly blink, roughly once every 2 seconds
    b) Communication mode (enable switch off)
        i) Scanning
            (1) LED blinks rapidly every half second
        ii) Connected
            (1) LED blinks twice every other second
        iii) Off
            (1) LED stays off. Turn the badge off and back on to reset.

3 Project Operation

3.1 Operating Mode 1: Normal Operation

The device has two main modes of operation. The first is the functionality provided by the device on its own: the user can interface with the buttons on the device and see output on the connected screen. The second mode of operation can only be accessed when the user connects the device to their laptop using the device's USB-C port and initiates a TTY connection. This mode of operation provides the user with much more functionality, as not only does this operational mode give the user the ability to control the device using their keyboard, but the connection will also provide the user with a visual interface to control the device.

The user has many options from this menu, such as selecting a display name if they input "1". Inputting this will allow the user to change the name displayed on the device's screen. Depending on the user's name, certain images may appear alongside it. If the user wishes to display their name tag from the TTY connection window, they can select "2" to print it. If the user selects option "3", the device will print a link to a game, which the user can play as long as they are connected to the internet. The user can initiate a bluetooth connection with another device by selecting option "8". The badge will then ask the user if they wish to search for other devices, and the device will be able to connect to another after successfully finding a valid connection. If the user wishes to restore the badge to factory defaults, they can do so by selecting option "0" and following the instructions presented onscreen. The options shown in the menu initially are not all of the options a user can select. Menu options are revealed to the user over time through experimentation and puzzle-solving.

3.2 Operating Mode 2: Abnormal Operations

Doing any of the following will prompt misinput and would be considered “Abnormal Operation,” that is, outside the scope of defined operation:

- If a user selects either an invalid or hidden option, the badge will warn them and return to option selection with no consequences to the user.
- If the user selects an option and then regrets their selection and wishes to cancel, most options will allow the user to cancel input and return to the menu.
- If the user hits “enter” to confirm any typed text (rather than waiting 1-2 seconds for the serial timeout functionality), it will send an additional “newline” character that will lead to incorrect parsing of their input string. Errors may occur in between menus or when confirming selected options.

3.3 Safety Issues

Our badge has very few, if any, safety issues. The device operates at a relatively low voltage and should not be able to physically harm users. In terms of data security, this badge should have no issues at all. Attendees who purchase a VETCON badge are *supposed* to attempt to hack the device.

4 Technical Background

PlatformIO:

PlatformIO acts as our main way of flashing and interacting with MSP430 EXP-FR2433 and all the connected hardware. PlatformIO also allows us to more easily create and test code for the microcontroller as it abstracts the standard C used by CCStudio into the more palatable Arduino coding standard.

Badge:

Hardware:

Our badge is based on TI's MSP430 EXP-FR2433 microcontroller. This is the platform for our software and allows utilization of peripheral devices. Such as, our HC-O5 bluetooth modules and our LCD alphanumeric display.

Software:

We coded the entirety of the codebase in C++. An infinite loop handles the menu functions with a series of flags being set and unset for inputs that the user makes through serial communication. Our bluetooth is also interfaced through a hardware serial communication port, and follows the same coding paradigm as the main menu code.

5 Relevant Engineering Standards

Our badge operates under the ANSI-C++ Standard for all board/badge programming. Furthermore we are using GNU Make and GNU GCC/G++ library headers and dynamically linked libraries. Finally, we are operating according to typical DEFCON procedures.

6 Cost Breakdown

Project Costs for Production of Beta Version (Next Unit after Prototype)				
Item	Quantity	Description	Unit Cost	Extended Cost
TI-MSP430 EXP FR2433	1	Microcontroller to Micro-ly control things	9.99	9.99
HC-05 BT MODULE	1	Bluetooth module to connect to other badges	1.93	1.93
16x2 AlphaNumeric Display	1	Alphanumeric Display to display non serial messages	1.71	1.71
Multicolored LEDs (Assorted)	3	Light Emitting Diodes to be used as progress indicators	0.01	0.03
D1 Mini Charge/Boost Module (LIPO)	1	Charge Controller/Regulator for Lithium Polymer Batteries.	1.93	1.93
3.7v, 3000mAH 18650 Battery	1	Lithium Ion Battery to provide 20 hours of continuous use.	4.25	4.25
			Beta Version-Total Cost	19.84

7 Appendices

7.1 Appendix A - Specifications

ALL EMPIRICAL REQUIREMENTS ARE WITHIN ± 10% TOLERANCE

Battery Life	21 Hours of Continuous Operation
Dimensions	4” x 4” x 1”
Weight	150 Grams
Attachments	Secure Lanyard Attachment Point
Branding	Visible VETCON branding or Military Decor
Interfaces	On/Off Switch; USB-C Interface;
Networking/Communication	Physical P2P (Serial) ; Bluetooth
Interactivity	Liquid Crystal Display; On-board and Web-based minigames

7.2 Appendix B – Team Information

John Kircher – Cybersecurity Research and Development Team at Raytheon
Worked primarily on ciphers for games 1,2,3 – software development – bluetooth research and development – circuit design.

Derek Barbosa – Working on the RHEL Real-Time Linux Kernel Team at Red Hat
Worked primarily on research for all phases, Microcontroller Software, Game 1 deployment, Game 2 Development, Game 3 Development (engine and frontend), LCD Interfacing, Circuit Design.

Ryan Sullivan – Working on the Research Kernel Team at Red Hat
Worked primarily on main menu code development, general debugging of code in all phases, Game 3 development and troubleshooting.

Carlos Ortiz – Searching for work
Worked primarily on game 1 development – LCD interfacing – PCB design – Circuit diagram

Julian Padgett – Software Engineer at Northrop Grumman
Worked on bluetooth research, LCD research, Game 3 concept and content, 3D printed enclosure.