Secure and Remote 3D Printing {

01 Team

Tiffanie Petersen, Isaiah Thomas, Carl Mann, & Nick Cottrell

02 Faculty Advisor

Dr. Sid Bhattacharyya

03 Client

Mike C Newton
(Director - Strategic Technology - Sciperio)

}

Our goal is to provide users with a secure method of remote 3D printing

1. Develop a website which allows users to register and submit gcode files to be remotely printed by an Ender 3. Requests will be handled as a queue and processed by selected administrators. Only approved accounts will be allowed to submit requests. Various security checks will be done on submitted files to ensure their authenticity.
2. Communication between the website, octoprint, and the printer is facilitated over a raspberry pi. Octoprint has a pre-existing api that will allow the website to communicate with the printer in real time and display relevant information to users. Some relevant information may include time until completion and potential errors. All applications will be deployed using docker.
3. Ensuring each print job is completed as expected we must prevent tampering during the execution. One way in which we will attempt to prevent tampering will be to install the GreatFET in order to listen to commands currently being executed by the printer and cross reference this with the expected commands in the given gcode file.

1
2
3
4
5
6
7
8
9
10
11
12
13
14

Octoprint's api is fairly extensive
and to utilize it to its full
potential will require a lot of
research as well as trial and
error.

1
2
3
4
5
6
7
8
9
10
11
12
13
14

Using the GreatFET is new to the team so there will be a lot of trial and error as well as research into how the tool works. We want to ensure that we know how to use it otherwise something could break.

1

2

3

4

5

6

7

8

9

10

11
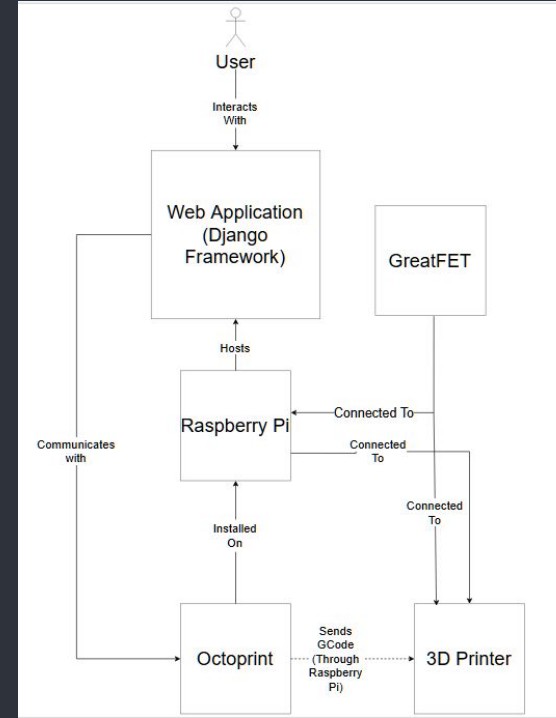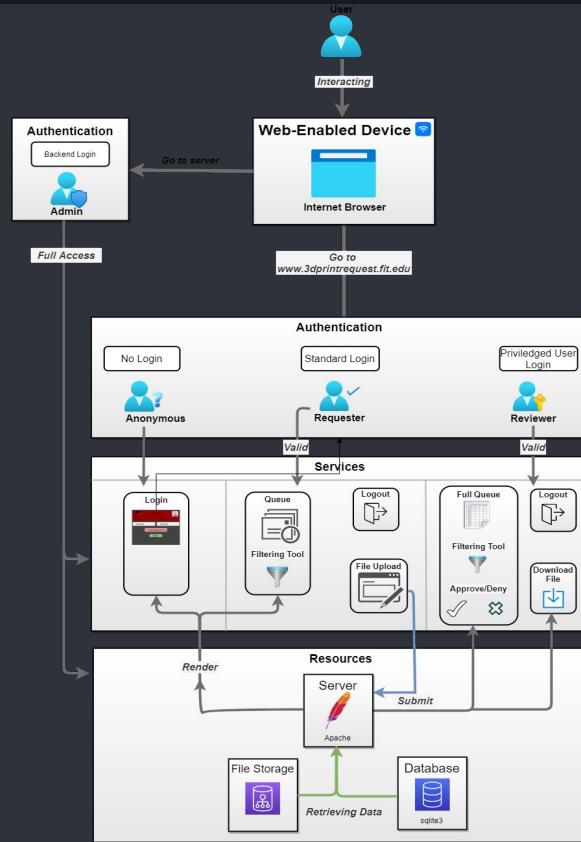
12

13

14
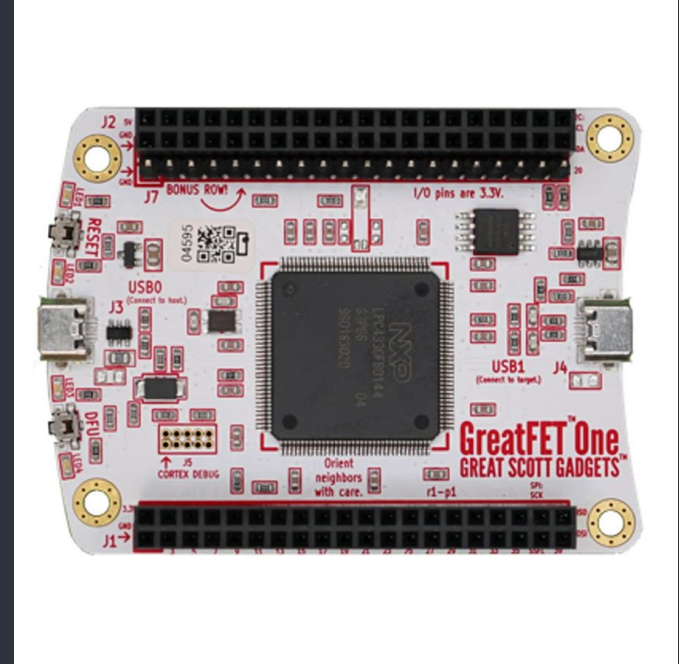
3D printers can fail at any point during the printing process, we need to figure out how to handle a failed print and have the queue not skip over a "completed" print. We also need to note that the printer has failed, but octoprint does not have a check for that so we need to implement how to determine if it has failed.

Design

1
2
3
4
5
6
7
8
9
10
11
12
13
14

Module feature	Completion	To Do
GUI	50%	Allowing drop down menus, mouse-over help messages...
Docker Container	50%	Upload to the new raspberry pi
Networking on Raspberry pie	25%	Setup website communication with octoprint's api
Pen Testing Tools (GreatFET)	25%	Install the new software onto the raspberry pi and begin testing

1
2   Measuring success:
3
4   *   Speed
5   ○   How fast does the printer move through the queue?
6   ○   How long does it take to infiltrate the system?
7   *   Accuracy (e.g. how accurate is the system?)
8   ○   Does the 3D printer misprint?
9
10   ○   Does the 3D printer waste filament?
11   *   Reliability
12   ○   How often does the 3D printer fail a print from the queue?
13   *   User survey
14   ○   Rating of how easy the website is to navigate.

1 Task 1: Implement, test & demo use of the raspberry pie to print
2   ➢   The web application needs to be on the raspberry pi as well as octoprint
3   ➢   The admin should be able to tell the printer to select the first option from the
4   queue and begin printing
5 Task 2: Implement, test & demo the website interfacing with octoprint's api
6   ➢   The interface, while printing the web app should work with octoprint to display
7   a completion time for the user
8   ➢   Display print failures at any point and notify the user
9 Task 3: Utilize the GreatFET to intercept and inject traffic
10   ➢   Place GreatFET in between the printer and the Raspberry and set it to listen to
11   & forward traffic between the endpoints
12   ➢   Design functionality for the GreatFET to select and modify packet fields being
               transmitted as a man-in-the-middle attack.
13
14   ➢   Connect GreatFET as an endpoint to the Ender 3 printer and configure it to
               operate as a fuzzer.

Task 4: Investigate potential vectors for attack in the Ender 3 firmware

➢ Given that the Ender 3 is open source, it will make it easier to look through the firmware for vulnerabilities. These vulnerabilities would give insight to see the best possible path to exploit the printer

➢ Analyze the fuzzing traffic from Task 3 to determine any attack vectors

➢ Utilize automated analysis tools such as centrifuge

Task 5: Update the Dockerfile to include Octoprint & Web application

➢ Including all three software applications into the dockerfile will allow the team to easily pull changes together and stay up to date

➢ This is the most efficient way to keep all of our tools together which will allow us to monitor what is installed on the raspberry pi

1
2
3
4
5   Tasks:
6
7   *   Implement, test, and demo which features/modules
8   *   Evaluation results
9   *   Create poster for Senior Design Showcase
10
11
12
13
14

```
1
2
3
4    Tasks:
5
6    *    Implement, test, and demo which features/modules
7    *    Test/demo of the entire system
8    *    Evaluation results
9    *    Create user/developer manual
10   *    Create demo video
11
12
13
14
```

Task Matrix

Task	Tiffanie	Carl	Isaiah	Nick
1. Implement, test & demo use of the raspberry pie to print	100%	0%	0%	0%
2. Implement, test & demo the website interfacing with octoprint's api	0%	100%	0%	0%
3. Utilize the GreatFET to intercept and inject traffic	0%	50%	0%	50%
4. Investigate potential vectors for attack in the Ender 3 firmware	0%	0%	100%	0%
5. Update the Dockerfile to include Octoprint & Web application	0%	0%	0%	100%