IBM Subversive Project

Team name: Yellow

Harry Chapman : up839653@myport.ac.uk
Matthew Shore : up879148@myport.ac.uk
Ricky Claven : up864163@myport.ac.uk

Contents Page

1.0 Introduction

What do we aim to achieve?

Our goals in undertaking this project are to identify and then present the cyber security risks which exist within a commercial airport. Our presentation is aimed at ordinary people who would use an airport and whom would not have significant amounts of technical knowledge. Ultimately we seek to raise awareness for these cyber security risks and propose solutions to help mitigate the risk that is posed by them.

What system are we looking at?

We are looking at an airport.

Chosen case-studies:

Gibraltar International Airport has a main road that cuts directly through the runway. This requires lots of attention from the tower crew as they have to ensure both parties are safe when either taking off/landing and crossing these roads.

This also means that any hacks or interferences to security could cause fatalities, but usually hackers are after data.

Ukrainian banks and **Boryspil airport** systems went down after an attack from an unknown source. The attack affected the flight schedule and all the computers were down. The hacker team deployed ransomware, demanding a payment of $300 in Bitcoin to allow their files to be decrypted.

Aircraft missing from radar systems increase fear of cyber attacks. The direction, speed, altitude and position were not showing. This could be very potentially dangerous as if the aircraft's position isn't known then the airport has to hold off on any departures or landings as aircraft could collide.

SATCOM / EICAS
A security professional named Chris Roberts hacked the entertainment service on a commercial aircraft. He was able to send EICAS (Engine-indicating and crew-alerting system) messages. This means he was able to communicate false information about the planes status if he wanted. If this would've unfolded then it could have caused panic and delays. Lots of vital members of staff would have had to divert their attention onto this incident only to find out it was someone wasting time.

Why have we chosen these?

There are a plethora of options when deciding the environment to be displayed and tested; It can't be too niche.

When visiting IBM Hursley Labs, we were invited to a design workshop which helped to narrow the scope of interest. Firstly, we were organized into our groups and were told to brainstorm environments in a given time frame. After the minute or so, we came up with a considerable list of choices;

- Nuclear power station
- Airport
- School / University
- Supermarket
- Bank
- Police station
- Shopping mall
- City junction
- Dockyard
- Train Station
- Hospital

Out of all these we chose to use an airport environment for our project because the cyber security risks at an Airport are extremely high as well far more numerous than at other high-risk places such as a nuclear power plant where the risks are more deadly but less likely to happen as well as less numerous.

In addition to this the cyber security risks at an airport will be much more relevant to market to people because significant amounts of people use an airport where as a nuclear power stations internal cyber security is very closed off to the public.

What do we anticipate could be an issue?

- Cyber attacks on publicly accessible wireless hotspots : https://timesofindia.indiatimes.com/india/airport-railway-wi-fis-hotspots-for-cyber-attacks-warns-govt-agency/articleshow/61147090.cms
- VASI (Visual Approach Slope Indicator) : http://bayareapilot.com/vasiPAPI.htm

- Runway lighting : https://www.thebalance.com/airport-runway-lighting-explained-282727
- SATCOM / EICAS : https://arstechnica.com/information-technology/2015/04/researcher-who-joked-about-hacking-a-jet-plane-barred-from-united-flight/
- Baggage system & unattended computers/servers: *http://www.airport-business.com/2014/06/need-talk-cyber-security/*

We will be assessing these risks in 5 categories:

- Risk (Likelihood of it happening)(This will be between 0 - 10 with 0 meaning no chance and 10 meaning frequently)
- Danger (How dangerous is it)
- Feasibility (Is it too hard for us to physically represent)
- Recovery (How easy will it be to recover from it)
- Impact (Will it be expensive for the airport)

Cyber attack on runway lights

Risk
2/10 - very unlikely to happen.

Danger

Airplanes wouldn't be able to see where to land or take off from which could cause air traffic, panic and delays.
Very dangerous, planes could potentially crash.

Feasibility

This would be easy for us to represent physically as we could implement an LED lighting system.

Impact

- The airport could turn the lights back on using backup power.

Cost

- This would cost the airport a minimal amount only if the lights are destroyed.

Security check failure due to untrained staff

Risk

3/10 - pretty low chances of this happening.

Danger

Very potentially dangerous as someone could board a plane with contraband.

Feasibility

We could have 3D printed x-ray machines and metal detectors and show system failure through a LED either being green for okay or red for bad.

Impact

The staff could be trained and hopefully the airport on the other end of the flight could pick up the contraband but the risk on the airplane cannot be avoided.

Cost

It could be potentially quite expensive as the machines might have to be replaced

Cyber attack on air traffic control systems

Risk

2/10 unlikely to happen.

Danger

Potentially, very dangerous. Pilots mainly need to communicate with the ATC in order to avoid traffic collisions during both landing, takeoff and emergencies.

Feasibility

Die hard 2: guy takes over ATC and makes plane crash.

Impact

- Use different frequency (radio comms).
- Backup generators if power goes out.
- Communicate to nearby air traffic control towers to relay information?

Cost

Varies by type of attack carried out.
Could be damaging to the airports reputation and therefore might lose out on profits. Could cause damage to aircraft and lives which is very expensive.

Scene setting (this or these vulnerabilities have been found in similar systems)

2.0 Introduction to the Team

Who are the members?

Matt Shore

Harry Chapman

Ricky Claven

What experience they have?

Matt Shore:

- Prior to undertaking this project I had little experience when it came to DIY. I had only created projects at school during KS3 and had done nothing beyond this. Cyber Security has always been a big interest of mine. In the past I have met with Cyber Security professionals from companies such as BT. My main interest is with Cyber Security on the web such as on websites.

Harry Chapman:

- I have a background in DIY and model building so those are the aspects of the project that will be easiest for me. I don't have much prior knowledge in terms of cybersecurity, I've only discovered the area whilst starting my degree this academic year. However, I am finding it incredibly interesting to learn about.

Ricky Claven:

- My main strengths are electronics and programming. I've had a bit of practice programming on a PICAXE microcontroller and also on an Atmega from an arduino uno.

Why are they here?

We are all here because we all share the view that this project has been a great boost to our understanding of creating a project and presenting it to a specific audience. As well as a boost to our knowledge of Cyber Security in generally and the impacts that it can have. Prior to this project we all had an interest in Cyber Security however, this project has given us more incentive to do further independent study into this area.

3.0 The Story

Personas

Jeff, 47 → Head of Security: Jeff is the head of airport security. He manages all the airports security systems and has access to a large amount of sensitive information. His office is usually locked and his computer secured. However, this time he has left his computer on with the door open. This leads to a potential unauthorized person accessing the sensitive information on the airport network and potentially causing damage.

Stephanie, 36 → Air-Traffic Control Manager: Stephanie is the person responsible for managing the airports Air-Traffic Control tower. Her job involves managing all the systems there. However, this time there has been a cyber DDOS attack on the control tower's systems and they have been temporarily disabled. This means there is a pileup of planes as none of them are permitted to land or take off.

Bob, 23 → Untrained Staff: Bob is new to his job working in the airport. His job involves working in the bagging area. He is responsible for using the latest technology to scan baggage that is coming through the airport. However, due to his lack of experience with the technology he lets many potential risks get through the system. The airport need to train Bob with the technology more to mitigate the risks posed by the lack of staff training.

John, 52 → Trained Staff: John is experienced at his job working in the airport. His job involves working in the bagging area. He is responsible for using the latest technology to scan baggage that is coming through the airport. Due to his years of experience with the technology he does not let many potential risks get through the system. The airport can utilise Johns' expertise to help train other members of staff.

Detail how the vulnerability(ies) are manifested and displayed/described

ATC - If the air traffic control tower was hacked it would cause delays and possibles crashes for aircraft. We will display this on our model by adding LEDs on the inside of the ATC model. They will flash red when the ATC has been compromised.

Runway lights - If the runway lights were turned off or a hacker increased the voltage so much that they overloaded and broke then the aircraft's VASI wouldn't work as effectively and there could be some crashes and delays, especially in bad weather conditions. We will be representing this with LEDs on one side of the runway as we don't need to show both sides.

Untrained staff- Untrained staff could let contraband through the baggage system which is the scenario we've given them. This is very risky as contraband cover a vast amount of usually illegal items that could prove to be highly dangerous such as bombs or guns. We will be displaying this by having two baggage checkers set up; one with trained staff and the other with untrained. We will use LEDs to indicate when something is going wrong on the untrained baggage checker.

Gate changing LEDs - The gates will be changed over on each screen and constantly change between multiple gates. This will cause panic which in an area filled with people is not ideal. It will also waste time. We will display this on the model by using two LCD screens which will show gate numbers. These numbers when triggered by us will switch or change to random numbers. This means that people will have to move to the new gate location. We will constantly change the gates which will annoy passengers and cause panic. Their movements and anger levels will be displayed on an LED matrix. Over time the colours will change to red when fully aggravated. Also we will move them across the matrix to show their footstep movements.

Office door left open - If the office door is left open it means that anyone who notices it can get in and potentially access information about the systems of the airport. If the person finds information on the systems useful then they could take over potentially the entire airport. This will be displayed on our model by a door simply being left ajar.

Interaction Script

Our script for presenting this project is:

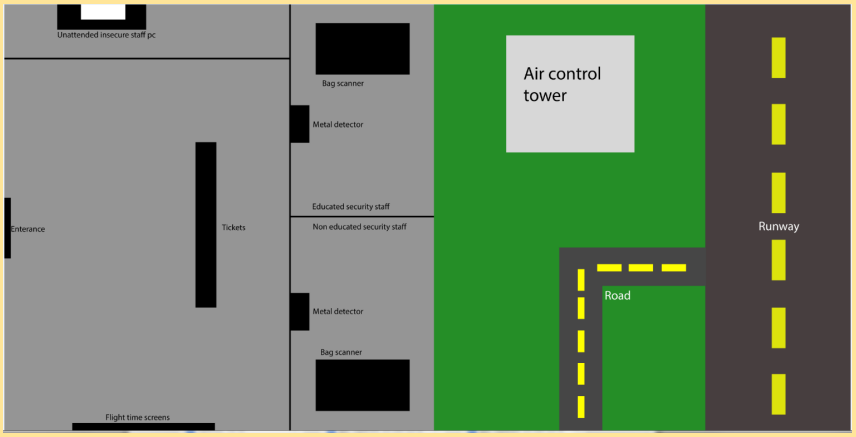
1. Introduction to our model. We will set the scene.
2. We will then proceed to explain why we choose an airport over other things.
3. We will start the presentation inside the airport. First we will discuss Jeff (Head of Security).
4. Secondly, we will discuss the untrained vs trained staff issues with Bob and John.

5. Thirdly, we will discuss the electronics within the airport. The LED lighting on the floor and the display screens we have installed.
6. Finally we will explain outside of the airport. We will discuss the Control Tower and the implications with it.
7. After we have presented all of the model we will finally give a summary and will leave it open to questions.

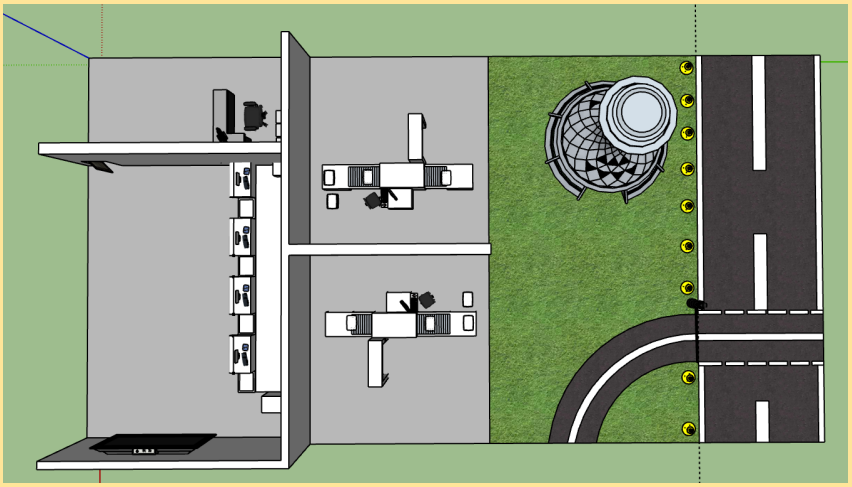
4.0 Ideas prototyping/build

Pictures

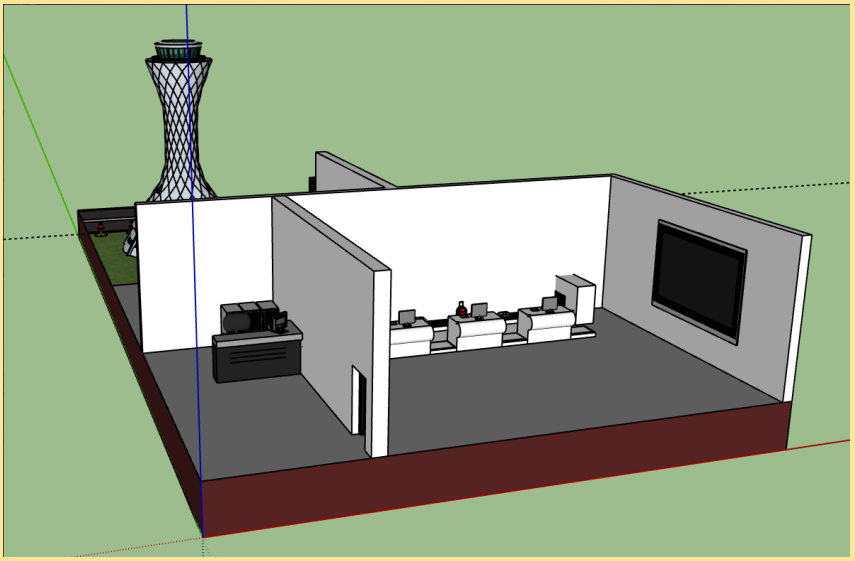
4.1 - 2D Birds Eye View



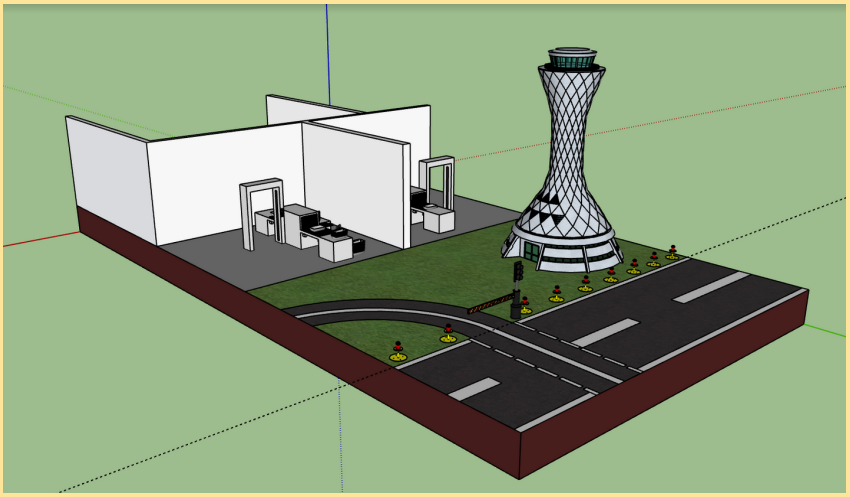
4.2 - 3D Birds Eye View



4.3 - Airport Interior



4.4 - Airport Runway & Control Tower



5.0 Project Construction

Introduction:

To create the base for our project we purchased MDF boards which were initially 80x40cm. These were then cut to be 67x37cm in size as to allow 3cm tolerance between the required size of 70x40cm.

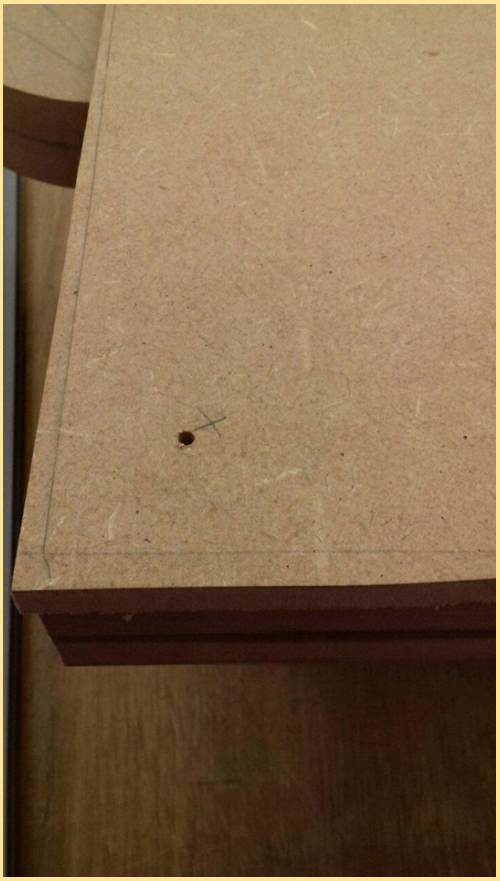
5.1

Cutting the frame out of MDF - the circuits will go in here.

5.2

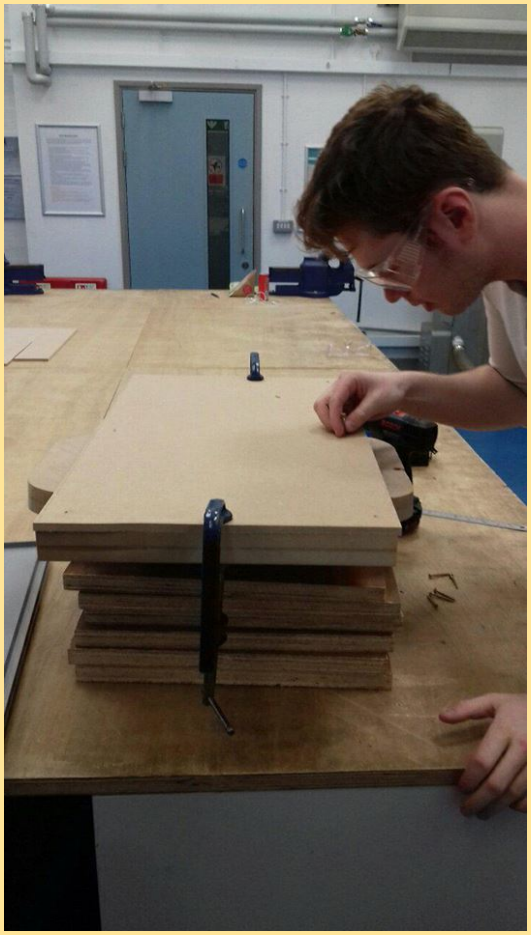
The board of MDF which will go on top of the frame.
Our models will go on this.

5.3



Screwing the frame onto the top.

5.4



Countersinking for a flush head of the screw.

5.5

Picture of a countersink.

5.6

The frame + top together upside down.

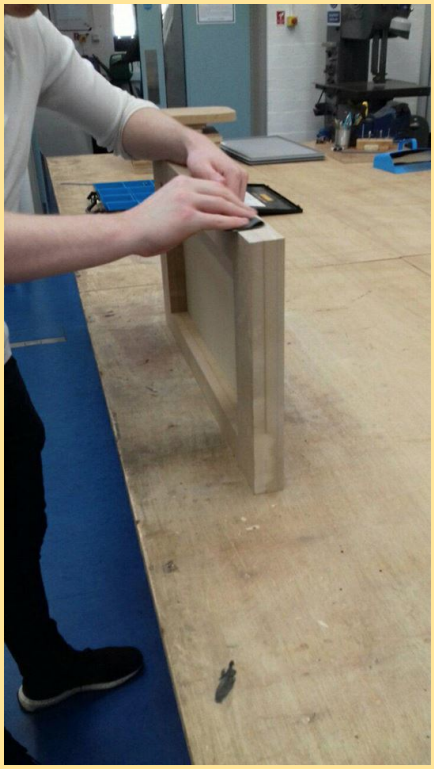
5.7

The frame + top together.

5.8

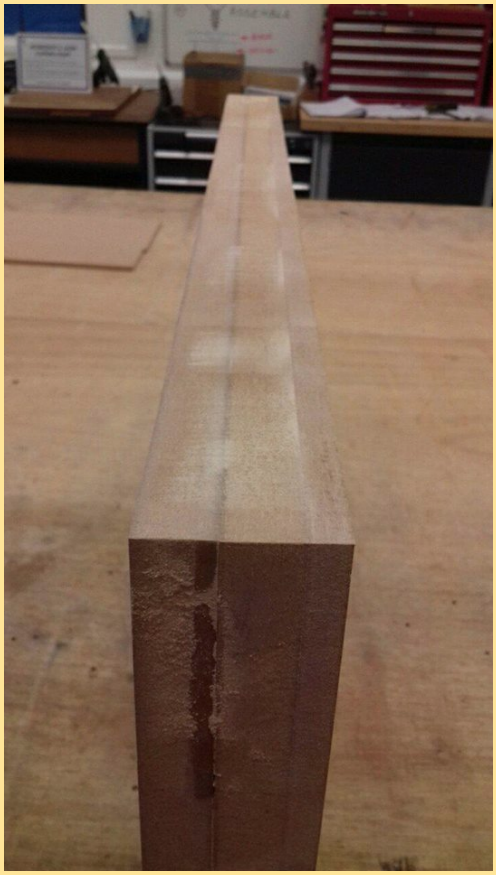
Screws to hold it together.
Neatly flushed due to countersinking.

5.9



Sanding the sides down to make them smoother.

5.10



Smoothed out sides.

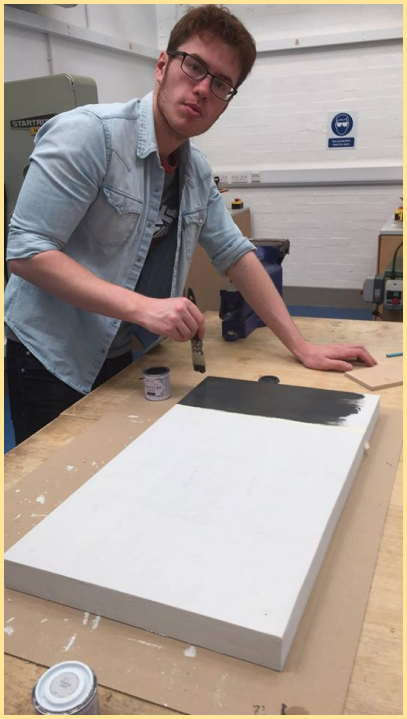
5.11

Painting the base.

5.12

Fake grass for airport.

5.13

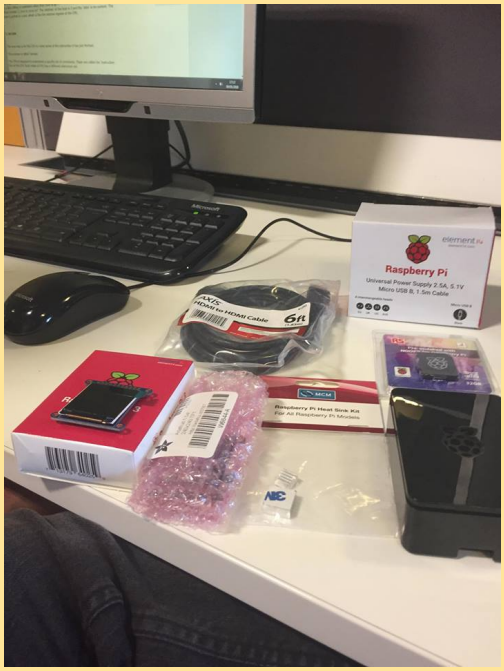


Painting the runway.

5.14

Runway painted on the base.
Used masking tape to get a fine line for the edges.

5.15



Raspberry Pi electronics kit.

6.0 Future Demonstration/Work

We did not have enough time to include the continuation of the creation of our model in this document. Here we will explain what we did next to finish the project.

- We added walls to the airport as seen in the 2D/3D models. These walls will be painted white and will have a graphite coloured top to make them more easily visible from above.
- We added models for the interior of the airport such as tables, computers, lego characters to populate the airport.
- We got a couple of plane models and added them to the runway to represent the issues posed there.
- We added the air-traffic control tower to our model.
- We added circuits and LED lighting to the underside of our base. The LEDs are used to map footsteps in the airport to show which areas have higher amounts of traffic under different circumstances. As well as this LED lighting will also be used in the airport to show errors. This can include the air-traffic control tower and also the baggage search area.

7.0 Individual Reflections

What has each team member learnt or gained from the project?

Matt Shore:

- From this project I have gained valuable knowledge and experience in the creation of models and woodwork. Creating this project with MDF in a workshop was very enjoyable. This project made me much more aware of the possible cyber security risks posed at an airport and also in other places such as a hospital. I would definitely consider a career in Cyber Security once I leave University.

Harry Chapman:

- Personally I have enjoyed this project, it's been a fun extracurricular activity for me. I will take away a lot in terms of learning from mistakes and overcoming challenges that have presented themselves whilst designing and building the model. I feel equal amongst my team members in the effort we have all spent to make this project work. Cyber security has been an interesting field to me for a short time now and it's a career I could myself ending up in so this project has shown me how fun it can be.

Ricky Claven:

- From this project I have discovered how powerful the raspberry pi is, compared to the what was available decades ago, and how easy it is to control electronics with python code and using the GPIO pins available on the board. Programming in python was easy because of previous experience and also the limitless documentation available however getting the electronics working was very satisfying and has taught me a lot. This project has also taught me how important it is to have strong cyber security within an airport.