Assignment 6

INFT3075

Pod 7 – Courtney Hagen, Jessey Harlow, Zach Slaunwhite

Table of Contents

[Introduction 2](#_Toc38180490)

[Security Recommendation Plan 2](#_Toc38180491)

[Technology Description 2](#_Toc38180492)

[Security Issues 2](#_Toc38180493)

[Recommendations 2](#_Toc38180494)

[Responsibilities/Requirements 2](#_Toc38180495)

[Enforcement 2](#_Toc38180496)

[Appendix A 2](#_Toc38180497)

[References 4](#_Toc38180498)

Assignment 6

# Introduction

The purpose of this document is to highlight potential security issues and recommendations for our Emergency Management Drone implementation on our final project.

# Security Recommendation Plan

## Technology Description

The technology chosen is Emergency Management Drones. These drones have a multitude of features that help with emergency events such as fires and lockdown situations. Some of these features include:

* Face/people detection
* Location awareness/GPS
* Autonomous control
* Extreme temperature detection
* Data capture, collection, and transfer
* Noxious gasses detection
* Connection to sprinkler system
* Phone monitoring access

## Security Issues

For our technology to send information to emergency personnel, wherever the camera feed goes to with the control room for human takeover, its database, it needs to connect to a few different networks. This comes with an unavoidable risk because all data isn’t on one private network, and need to traverse different networks, where a man in the middle attack could occur. So, one of the risks with this technology is that data needs to be moved, and if the data is changed along the way, it could be disastrous. A situation I can think of is if drones human tagging system is changed in the event of an attacker, where the tagged attacker is changed to a student. Not only will the attacker no longer be seen as a threat by it, or emergency personnel, a police officer could end up shooting a student.

Another security concern is the control room, where the cameras feed and information get sent to. I see two risks present there. The first is the person controlling the technology in the case of human takeover, because of this I think the person controlling should have an extensive background in either the police force, or the military. I believe they both do a good enough at weeding out the kind of people you wouldn’t want to hold someone else’s life in their hands. Of course we likely need a psychological testing contractor to get involved anyways.

The other risk with the control room is someone getting access to the control room that shouldn’t. I believe this can’t be a normal building on the side of the street in a city. I think a special building with strong security measures should be built specifically for this situation to begin with, rented from a company that specially builds secure environments for this reason, or it should be placed in a safe government building somewhere.

## Recommendations

Restricting access and control. This can be done by only granting control to a very select few individuals or operate and have full authority over the drones. This will be delegated through a user system where authorized personnel can login with a username and password, as well as require a physical OTP (one-time password) device. The less people that have access, the more trusting the drones will be. Securing access to the room inside the building is also crucial. Access to the control room should be only accessible through swipe card for very few individuals, as well as video surveillance of people going to and from the room.

Securing tunnels. The access to these drones is top priority, which will require a secure connection to the drones. When connecting to the drone system, all traffic will be encrypted on an internal network, and information such as video live feed to phone devices and image/file transfers will be a separate network.

Executing any commands will only be enabled on certain IP addresses, to limit the risk of malicious hackers from being able to use the drones in an unintended way.

It is recommended that policies be created for every scenario imaginable, focusing primarily on the use of the drones, and retention of personal information and images acquired by the drones. Having a clear outline of how the drones should be used is crucial.

Securing video and images in secure locations and servers. The server the database or storage resides requires just as much security as the drones, and will be maintained, including backups and redundancies

Using any features of the drone that involve crowd control or could potentially injure a student, including any features added to the drones in the future, will require authorization of law enforcement, either verbal or written.

## Responsibilities/Requirements

There will be a designated team responsible for the oversight of the emergency management drone devices. They will also be the ones who oversee them when introducing them to the drills and active events. They will be responsible for overseeing the configuration of the security measures to the devices. However, all who interact with the emergency management devices will be required to not interfere with the security of the devices.

## Enforcement

If any staff, student, or passerby interferes with the security of these devices, due to the nature of managing emergencies and potential safety impacts, there may be criminal consequences of these actions. Members of the team responsible for the emergency management drones will also be responsible for monitoring, documenting, and reporting any breeches detected for any relevant security teams to decide on an action.

# Appendix A

Individual Work Logs

Courtney Hagen

|  |  |
| --- | --- |
| **Total time spent:** | **3 Hours** |
| **Details of work completed:** | Completed technology description, introduction, responsibilities/requirements, and enforcement section. Created document |

Zach Slaunwhite

|  |  |
| --- | --- |
| **Total time spent:** | **2 Hours** |
| **Details of work completed:** | Recommended section |

Jessey Harlow

|  |  |
| --- | --- |
| **Total time spent:** | **2 Hours** |
| **Details of work completed:** | I did the security issues section |

Marking Rubric

Courtney Hagen

|  |  |  |  |
| --- | --- | --- | --- |
| Criteria | Courtney | Zach | Jessey |
| Attendance | 1 | 1 | 1 |
| Submission Deadline | 1 | 1 | 1 |
| Quality of Work | 1 | 1 | 1 |
| Communication | 1 | 1 | 1 |
| Participation | 1 | 1 | 1 |

Zach Slaunwhite

|  |  |  |  |
| --- | --- | --- | --- |
| Criteria | Courtney | Zach | Jessey |
| Attendance | 1 | 1 | 1 |
| Submission Deadline | 1 | 1 | 1 |
| Quality of Work | 1 | 1 | 1 |
| Communication | 1 | 1 | 1 |
| Participation | 1 | 1 | 1 |

Jessey Harlow

|  |  |  |  |
| --- | --- | --- | --- |
| Criteria | Courtney | Zach | Jessey |
| Attendance | 1 | 1 | 1 |
| Submission Deadline | 1 | 1 | 1 |
| Quality of Work | 1 | 1 | 1 |
| Communication | 1 | 1 | 1 |
| Participation | 1 | 1 | 1 |

# References

Beware of the drone! Privacy and security issues with drones. (2019, April 22). Retrieved April 29, 2020, from <https://resources.infosecinstitute.com/privacy-and-security-issues-with-drones/#gref>

Pritchard, S., & Pritchard, S. (n.d.). Drones are Quickly Becoming a Cybersecurity Nightmare. Retrieved April 30, 2020, from <https://threatpost.com/drones-breach-cyberdefenses/143075/>

Where do drones fit in with security? (2020, February 16). Retrieved April 29, 2020, from <https://resources.genetec.com/blog/where-do-drones-fit-in-with-security>

Pitchford, M. (2013, July 31). What's needed to ensure safety and security in UAV software. Retrieved April 30, 2020, from <http://mil-embedded.com/articles/whats-needed-ensure-safety-security-uav-software/>

McNabb, M. (2019, October 17). Drones and Cybersecurity: An Expert Opinion on Protecting Industry Against Drone and Data Attacks. Retrieved April 30, 2020, from https://dronelife.com/2019/10/17/drones-and-cybersecurity-an-expert-opinion-on-protecting-industry-against-drone-and-data-attacks/