

Secure Communications Protocol For Drones Based On A Flying Ad Hoc Network

Software Requirements Specification

R. Wishal Dhiraj Samaranayake

20200903/ w1838836

Supervised by

Mr Geethapriya Liyanage

Key Words - Secure communications protocol, drone technology, quantum-resistant cryptography, flying ad hoc networks

Table of Contents

[1. Chapter Overview 3](#_Toc151979158)

[2. Rich Picture Diagram 4](#_Toc151979159)

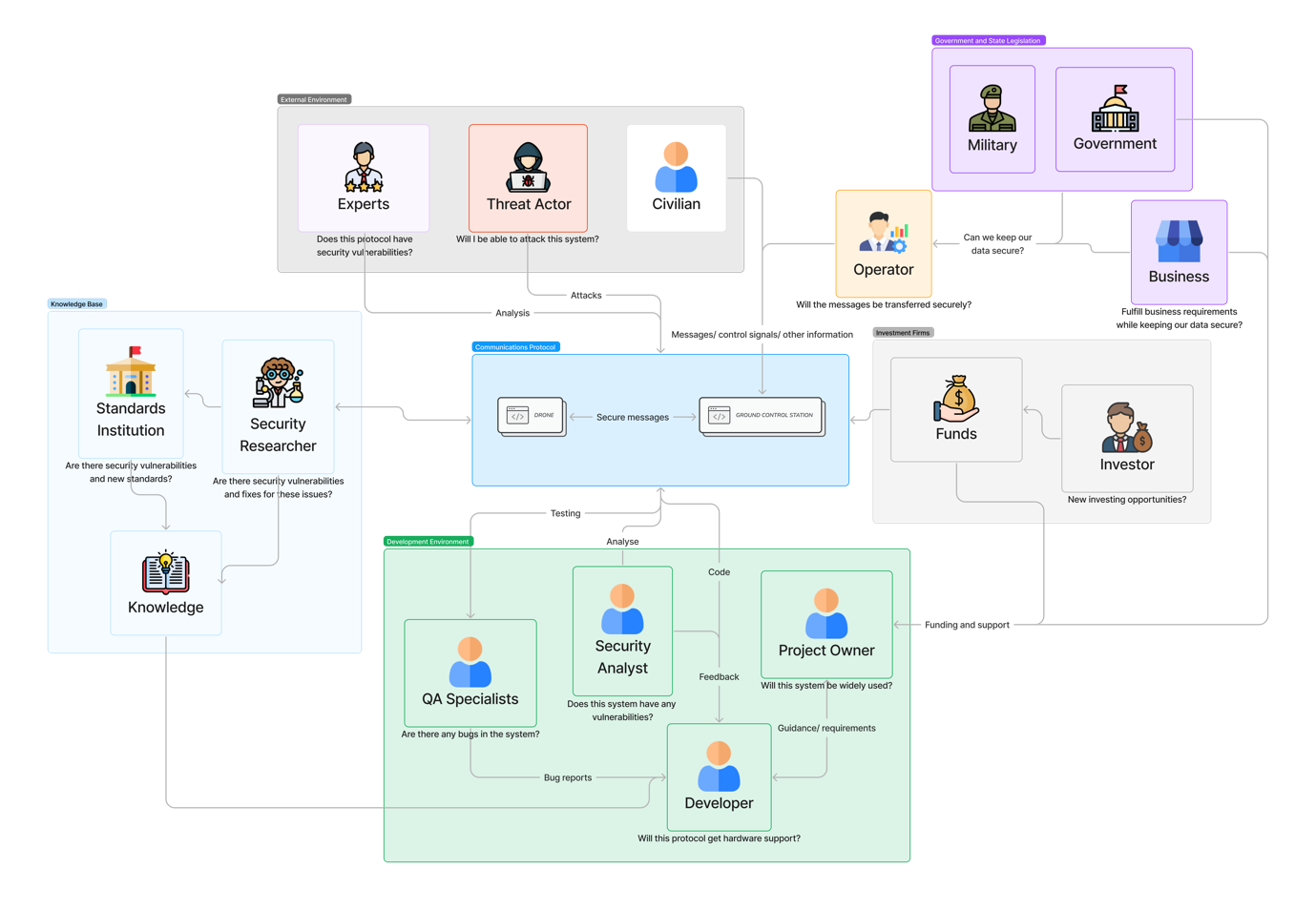
[3. Stakeholder Analysis 5](#_Toc151979160)

[3.1. Stakeholder Onion Model 5](#_Toc151979161)

# Chapter Overview

This document contains an overview of the software requirements, the goals of this project and all the associated stakeholders of this project.

# Rich Picture Diagram



*Figure n: Rich picture diagram.*

# Stakeholder Analysis

|  |  |  |
| --- | --- | --- |
| 1. **Stakeholder** | **Stakeholder Type** | **Description** |
| Developer | Developer | The development team developing the system. |
| QA Team | Check if the system works as intended and give feedback to the developer regarding any bugs. |
| Project Manager | Manages the project and coordinates development. |
| Security Analysts | Check if the system has any security vulnerabilities and inform the developers. |
| Operational Support | Operational | Provide support to the system users. |
| Project Owner | Owner | The owner of the product. |
| Domain Expert (security specialist) | Consultant | Check if the system has any issues and it complies to standards.  Also checks if the system is viable in different scenarios (i.e., legal). |
| Government/ Law Enforcement | Wider Environment | The governing body of a geographical location which authorizes the usage of the protocol. |
| Military | User | The military which can use this system for military activities (i.e., intelligence gathering, surveillance, reconnaissance, communications, etc.).  They can also use this system for disaster management. |
| Businesses | Businesses can use this system for various business applications (i.e., surveillance). |
| Civilians | Civilians can use this system for secure communications and other civilian uses. |
| Operator | Operators that operate the system and provide services to third parties (i.e., businesses, government entities, etc.). |
| Threat Actors | Negative Stakeholder | Threat actors that attack the system and attempt to get sensitive information that are transmitted. This could be normal and sponsored hackers, and militaries from other countries. |
| Sponsors | Financial Support | People who give financial support to build the system. This may include individual people, governments, businesses and other parties. |

# Stakeholder Onion Model

# Things to do next.

# Questionnaire

|  |  |  |
| --- | --- | --- |
| **Questions** | **Relevancy (Reason)** | **Research question** |
| Are sensitive and mission critical information shared through drones or from a ground control station to drones? | If sensitive and mission critical information passed through the drones and how much security matters. |  |
|  |  |  |

* Areas that are covered through this protocol:
  + Recon missions.
  + Disaster management.
  + Network relays.
* Talk to the supervisor after showing it to the supervisor.
* Afterwards talk to domain experts about it and validate them.
* Put it in to a form and identify target audience. Pick 10 – 15 people (from that list) that we know of and send it to them to review the questions. Have a 1:1 session to figure out if they understood the questions.
* Add a 3 min video explaining the project so the user can have a better understanding of the questionnaire.

Closed ended questions: Using data.

Open ended questions: Thematic analysis.