오픈 소스 기반 드론에 대한 취약점 분석 및 방어 기술 개발

부산대학교 전기컴퓨터공학부 정보컴퓨터공학전공

팀명: Joy security

팀원: 201924523 이경민

201624587 조수현

목차

1. 과제 배경 및 목표
   1.1. 과제 배경
   1.2. 목표

2. 시스템 주요 구조
   2.1. 시스템 주요 구조

3. 연구 방향
   3.1. PX4 스터디
   3.2. 개발 환경 구축
   3.3. PX4 취약점 분석
   3.4. 방어 기법 최적화

4. 개발 일정 및 역할 분담
   4.1. 개발 일정
   4.2. 역할 분담

1. 과제 배경 및 목표

1.1. 과제 배경

최근 드론, 즉 UAV(Unmaned Aerial Vehicle) 기술의 발전에 따라 UAV가 군사, 건설, 농업, 영상 촬영 등 다양한 분야에서 활용되고 있으며, 시장 또한 빠르게 성장하고 있다. 또한, 향후 물류 수송, 교통 관제, 통신 등 새로운 서비스/산업 분야로 그 영역을 확대하는 등 새로운 성장동력으로 주목받고 있다.

미래 항공 산업의 핵심 기술로 드론이 부각되면서 미국, EU, 중국, 일본 등 세계 각국에서 무인 항공기의 단계별 발전 로드맵을 발표하여, 드론 산업 육성과 시장 활성화에 노력을 기울이고 있다. 국내에서도 드론 산업 발전 기본 계획으로 네거티브 방식의 규제 최소화를 통한 드론 산업 실용화를 위해 법제도적 지원을 하고 있다.

하지만 이러한 급격한 UAV 시장의 성장은 UAV의 취약점을 악용한 다양한 공격의 급증을 유발하고 있다. UAV는 원거리에서 무선으로 원격 조정하거나 입력된 프로그램에 따라 비행하고, 센서를 통해 데이터를 전송한다. 이처럼 드론과 지상 제어 장치가 네트워크로 연결되어 있기 때문에, 드론이 탈취당하거나 서비스 장애가 발생할 수 있다.

드론 서비스에서 발생될 수 있는 사이버 보안 위협을 조금 더 자세히 살펴보면, 드론, 지상 제어 장치, 정보 제공 장치와 같은 자산 요소에서 발생될 수 있는 보안 위협이 존재한다.

먼저, 드론 환경에서는 GPS Spoofing과 GPS Jamming, 제어신호 전파 방해 및 무력화, 센서 교란, 임베디드 시스템의 펌웨어 변조를 통한 시스템 권한 탈취 등이 발생될 수 있다. 다음으로, 지상 제어 장치에서는 기밀 정보 유출, 암호키 노출 및 취약한 암호 알고리즘으로 인한 제어권 탈취, 잘못된 설계 및 구성으로 인한 소프트웨어 오류 등이 발생될 수 있다. 또한, 정보 제공 장치 상에서는 세션 하이재킹, 재전송 공격, 중간자 공격과 같은 메시지 위변조 공격, 데이터 위변조 등이 발생될 수 있다.

또한, 드론 개발에 오픈 소스 코드를 이용하면서 발생할 수 있는 문제가 존재한다. 최근의 드론 개발자들은 드론 비행 제어 소스 코드의 크기가 커지고 기능들이 많아짐에 따라 오픈소스를 가져와 활용하는 것에 익숙해지고 있으며 별도의 보안 취약점에 대한 점검없이 활용하고 있다. 이러한 오픈소스는 공격자가 접근 가능하기 때문에 다양한 취약점에 노출될 수밖에 없다.

드론 사이버 공격의 실제 사례를 살펴보면, 2011년 2월 이란 핵시설을 정찰 중이던 미국 드론을 대상으로 GPS Spoofing 기술을 사용하여 드론을 탈취하는 사건이 발생했고, 2014년 11월에는 드론 시스템의 취약점을 활용하여 해킹, 촬영 영상 복원, 드론을 복제하는 사건이 발생하였다.

이러한 문제들을 해결하기 위해 드론 시스템의 취약점을 파악하고, 취약점을 보완할 수 있는 방안을 탐색하는 것이 중요하다. 이는 드론 시스템의 기밀성, 무결성, 가용성의 보장으로 이어지므로, UAV 운영의 안전성과 신뢰성을 확보할 수 있다. 또한, 드론 기술이 더욱 다양한 산업 분야에서 안정적으로 활용될 수 있는 기반이 될 것이다.

1.2. 목표

대표적인 오픈소스 UAV 플랫폼인 PX4 autopilot과 MAVLink 프로토콜을 대상으로 알려진 취약점을 확인하고 분석하여, 취약점에 대한 방어 기법을 보완하고 최적화한다.

2. 시스템 주요 구조

2.1. 시스템 주요 구조

PX4 시스템 아키텍처의 구조도는 다음과 같다.

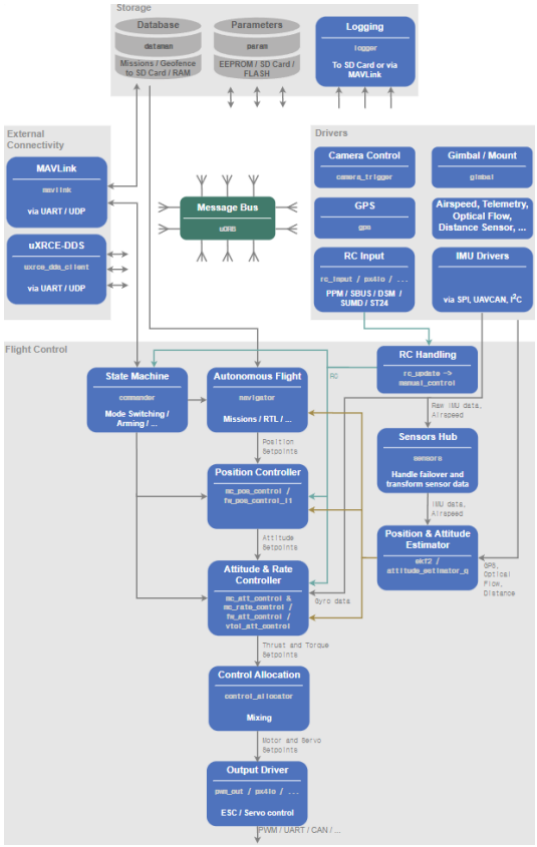


그림 1. PX4 아키텍처 주요 구조

PX4의 시스템 아키텍처는 Storage 모듈, Drivers 모듈, Flight Control 모듈, External Connectivity 모듈로 이루어져 있으며 각각의 데이터들은 uORB라고 불리는 메시지 버스에 의해 각각의 모듈들이 통신하게 되고, 통신 프로토콜로 MAVLink를 사용한다.

Storage 모듈은 dataman, param, logger 모듈로 나뉜다. 먼저, dataman 모듈은 MAVLink로부터 전달받은 비행 미션에 관련된 데이터를 SD card에 저장한다. 다음으로, param 모듈은 PX4 Autopilot 관련 파라미터를 EEPROM, SD card, Flash 메모리에 저장한다. 마지막으로, logger 모듈은 GPS, 기압계 등 센서로부터 들어오는 입력이나, Controller, Estimator에서 처리된 데이터를 미들웨어인 uORB의 API

를 통해 SD card에 저장한다.

Driver 모듈에서는 camera_trigger, gps, fmu, px4io 등의 프로그램에 의해 카메라 제어, GPS 시그널 송/수신, 모터 제어 등의 동작을 담당하고, External Connectivity 모듈에서는 MAVLink 프로토콜을 통해 PX4와 지상통제소 사이의 통신을 담당한다.

Flight Control 모듈에서는 commander, navigator, mc_pos_control, mc_att_control 등의 어플리케이션에 의해 비행 제어를 담당한다. Navigator 어플리케이션은 자동 비행을 담당하는 프로그램으로 미션을 주입하면 그에 따른 비행을 수행하게 하고 미션이 종료될 때 RTL을 수행하여 홈 좌표로 돌아오게 하는 기능을 가지고 있다.

다음으로, 통신 프로토콜인 MAVLink는 드론 통신을 위한 경량화 메시지 프로토콜이다. 드론과 지상 제어 스테이션(Ground Control Station) 간의 통신, 또는 드론 내부 컴포넌트 간 통신에 이용된다.

3. 연구 방향

3.1. PX4 기초 지식 스터디

먼저, 드론이라는 특수한 분야에서의 개발이므로, 드론 자체에 대한 이해가 필요하다. 또한, PX4는 UAV를 제어하기 위해 특별히 설계된 소프트웨어로, 시스템에 대한 충분한 이해를 바탕으로 개발을 진행해야 한다.

따라서, 드론의 구성 요소와 비행 제어 시스템에 대한 스터디를 진행할 것이다. 이후 PX4의 공식 문서를 참고하면서 PX4 아키텍처를 이해하고, 이해한 내용을 바탕으로 소스 코드를 분석할 것이다.

3.2. 환경 구축

필요한 도구와 라이브러리를 Ubuntu 등의 환경에 설치하고, PX4와 호환되는 시뮬레이터인 Gazebo를 사용하여 테스트 환경을 구축할 예정이다. 해당 시뮬레이터에서 사용자 지정 이륙 위치 설정, 시뮬레이션 속도 변경, 풍속 변경, 거리 센서 성능 조절, GPS 노이즈 시뮬레이션 등의 다양한 기능을 이용할 수 있다.

그림 2. Gazebo 실행 화면

3.3. PX4 취약점 분석

Gazebo 시뮬레이터를 이용하여 GPS 스푸핑, 잘못된 센서 데이터 입력 등 다양한 악의적인 입력을 통해 시스템의 반응을 테스트하고, 데이터 전송 중 발생할 수 있는 위협 (중간자 공격, 재전송 공격 등)을 테스트한다. 또한, 보안 이벤트를 모니터링하고, 로그를 분석하여 보안 위협을 발견한다. 이후, 취약점의 심각도와 영향 범위 등을 분석하여, 보안 강화 방안 탐색의 기반이 될 수 있도록 한다.

Wireshark를 통해 MAVLink 메시지를 분석하여 메시지의 무결성을 확인한다. MAVLink는 기본적으로 암호화를 제공하지 않기 때문에 스니핑 등을 통해 암호화 되지 않은 메시지에 대해 일어날 수 있는 공격 방안을 예측하고 예방할 수 있는 방법 또한 설계할 수 있도록 한다.

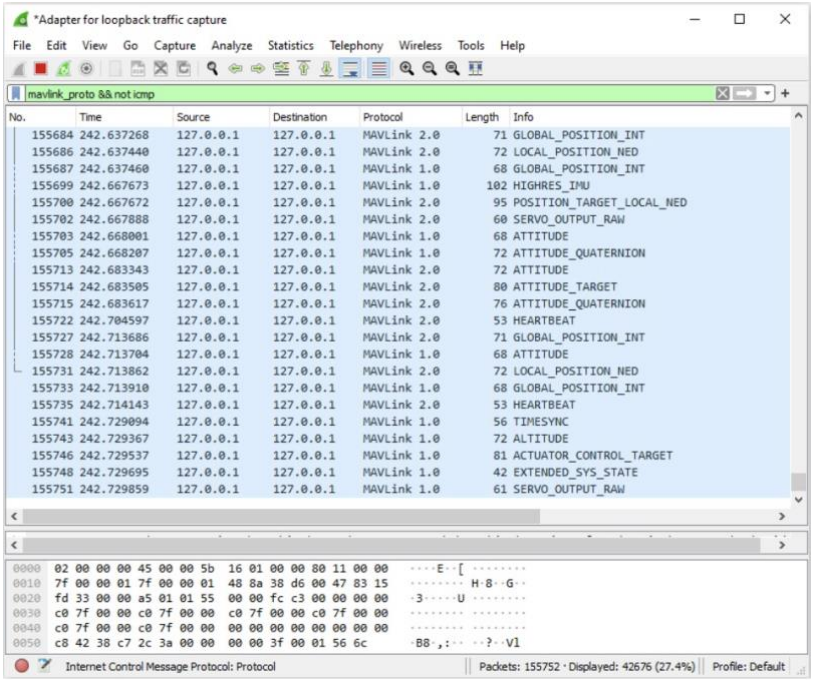


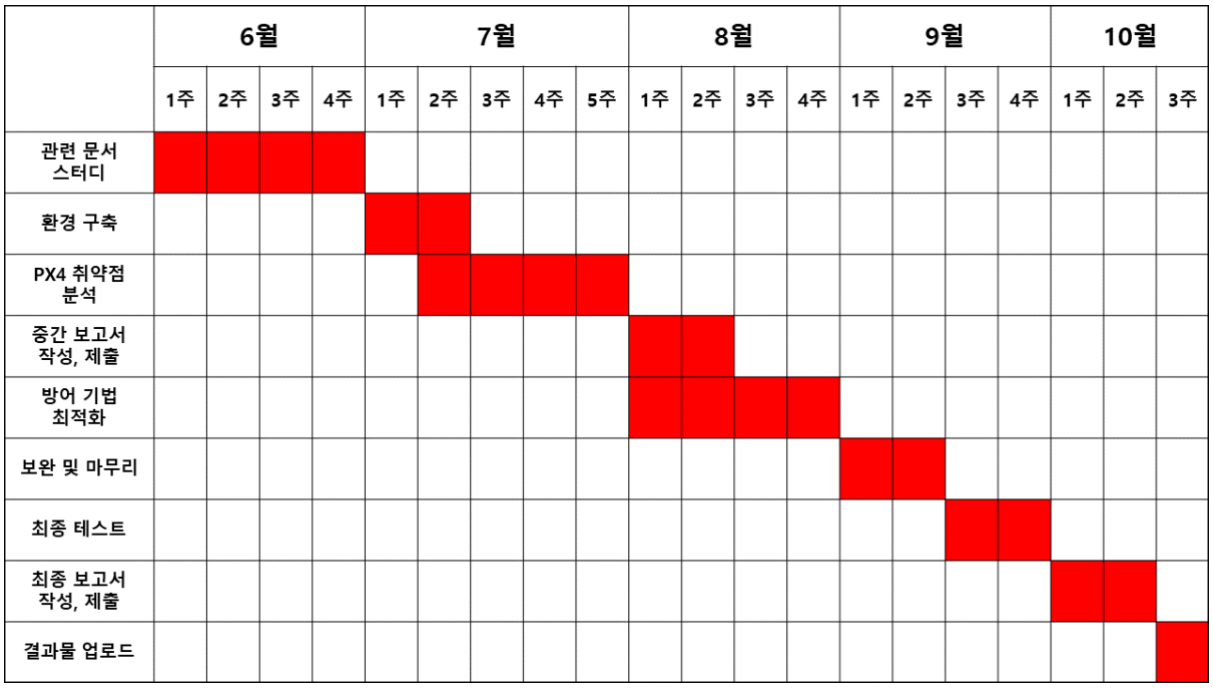
그림 3. Wireshark를 통한 패킷 분석

3.4. 방어 기법 최적화

PX4 Autopilot과 MAVLink에 대해 알려진 취약점을 분석하고, 기존 방어 기법에 최적화 및 경량화를 적용한다.

4. 개발 일정 및 역할 분담

4.1. 개발 일정



4.2. 역할 분담

이름	역할
공통	PX4 스터디, 보고서 작성, 취약점 분석, 오픈 소스 코드 분석, 방어 기법 최적화, 발표 및 시연 준비
이경민	PX4 Autopilot 시스템 구조 분석, 비행 및 통신에 대한 코드 분석, 취약점에서 발생하는 보안 공격에 대한 방어 기법 연구
조수현	MAVLink 메시지 분석, 시뮬레이션을 통한 비행 및 통신 데이터 분석, 취약점에 대한 공격 시나리오 연구