49 오픈 소스 드론에 대한 취약점 분석 및 방어 기술 개발

소속 정보컴퓨터공학부 분과 D 팀명 Joy Security 참여학생 이경민, 조수현 지도교수 손준영

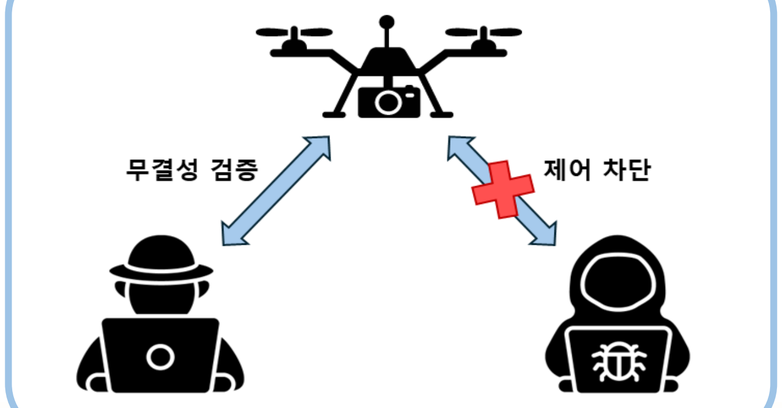
과제 소개

MAVLink 프로토콜 통신에 대한 무결성 및 보안성 강화

기존의 PX4 시스템에서는 MAVLink의 CRC만을 이용하여 메시지의 오류를 탐지한다.

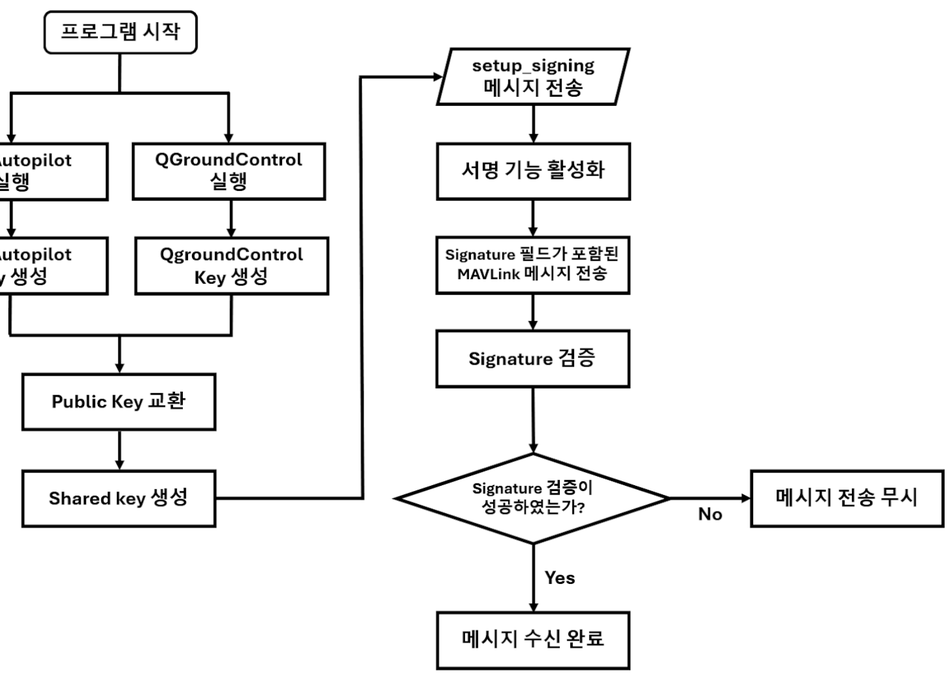
☞ CRC는 고의적인 데이터 변조에 취약하기 때문에 무결성을 보장하지 못한다.

서명 기반의 메시지 인증 기능을 통해 무결성을 보완하고 최적화하는 방법을 모색한다.
또한, 인증되지 않은 메시지를 수신하지 않음으로써 보안성을 강화한다.



연구 내용

전체 흐름도



MAVROS를 통한 커스텀 메시지 전송

√ 일정 주기의 커스텀 메시지 전송을 수신하면 공개키 확인

√ 즉, 공개키 값을 모니터링할 수 있도록 하는 역할

ECDH를 이용한 키 교환

√ 통신 채널에는 공개키만 노출

√ 타원 곡선 상의 연산을 통해 공유된 비밀키 생성

√ 키가 노출되는 상황 고려하여 키 값 갱신 기능 추가

SHA256을 통한 서명 검증

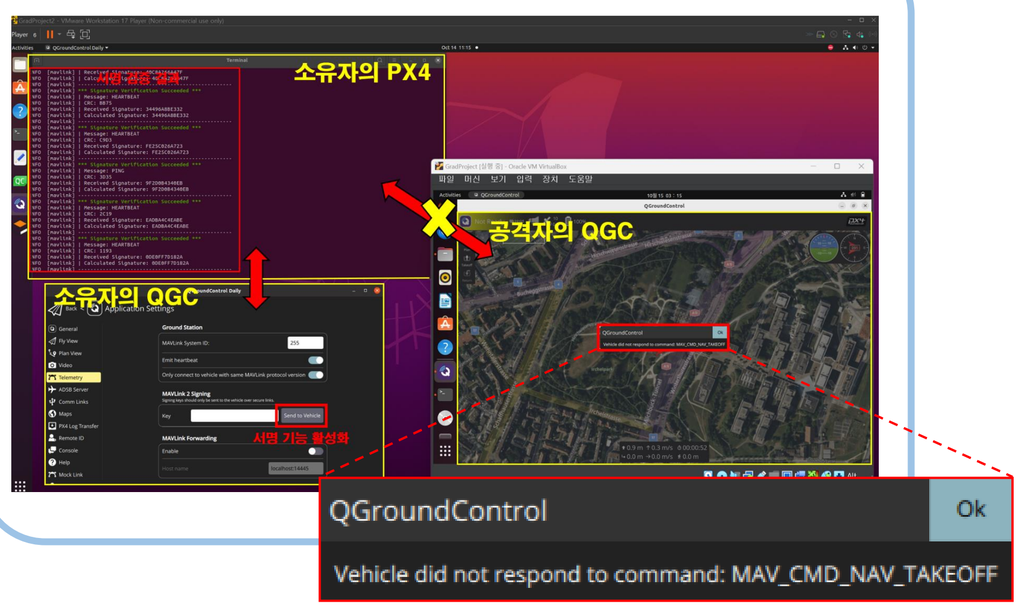
√ 전송받은 데이터에 해시 함수 적용하여 서명과 비교

√ 동일한 경우, 메시지에 대한 처리 함수 호출

√ 동일하지 않은 경우, 메시지 거부

연구 결과

인증되지 않은 메시지 무시

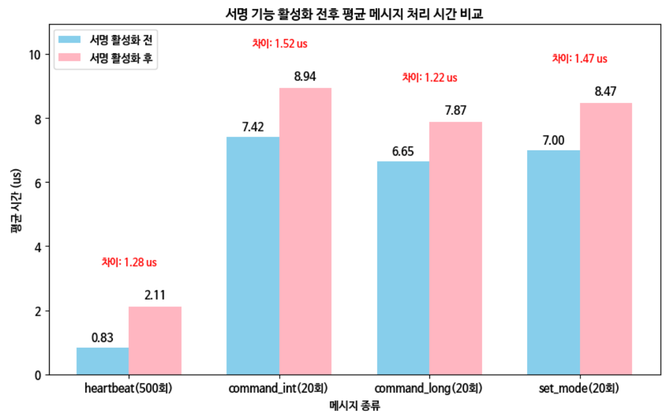


공격 상황 가정

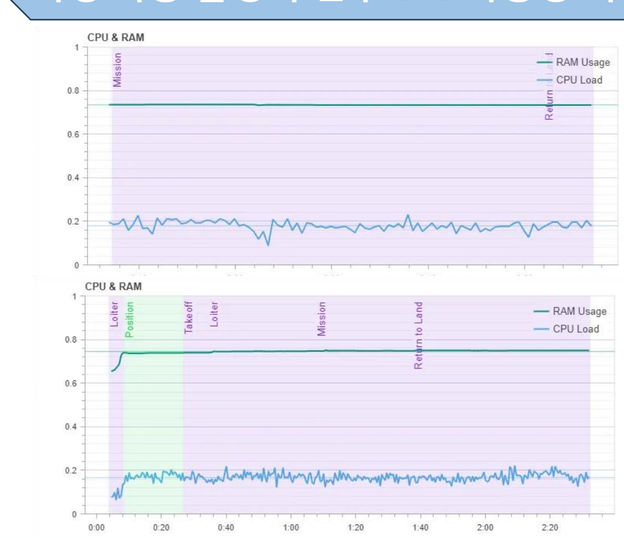
√ 공격자가 PX4의 UDP port로 접속을 하여 연결에 성공하였지만, 공격자의 QGC는 메시지에 올바른 서명이 포함되지 않았기 때문에 공격자의 드론 제어 명령이 무시되는 모습이다.

√ 가령, 키 값이 노출되어 서명을 생성하여도, Signing Stream은 하나의 GCS의 접근만을 허용하도록 하였기 때문에 서명 검증에 실패하게 된다.

서명 기능 활성화 전후 처리 시간



서명 기능 활성화 전후 CPU 사용량 비교



성능 측정

√ 서명 인증 기능 활성화 전후로 메시지 처리에 대한 시간 측정

√ 활성화 전의 평균 시간과 후의 평균 시간을 측정하여 차이를 구한 결과 약 1.2 μs ~ 1.5 μs 차이 발생 (해당 시간은 서명 검증에 필요한 시간)

√ CPU와 RAM에 대한 사용량 분석

√ 위 – 서명 활성화 이전
아래 – 서명 활성화 이후

√ RAM 사용량에 있어 대략 1% 차이만을 보이고, CPU 사용량 또한 대략 1% 내외의 차이를 보여준다.