무인이동체의 취약점을 통해 본 IoT 보안 위협과 대응 방안

㈜테르텐 부사장 김대근

배경

Drone의 취약점을 연구하게 된 배경

- ㈜테르텐은 사이버 보안 컨설팅을 수행하는 업체로 다양한 종류의 IoT 보안 컨설팅을 수행



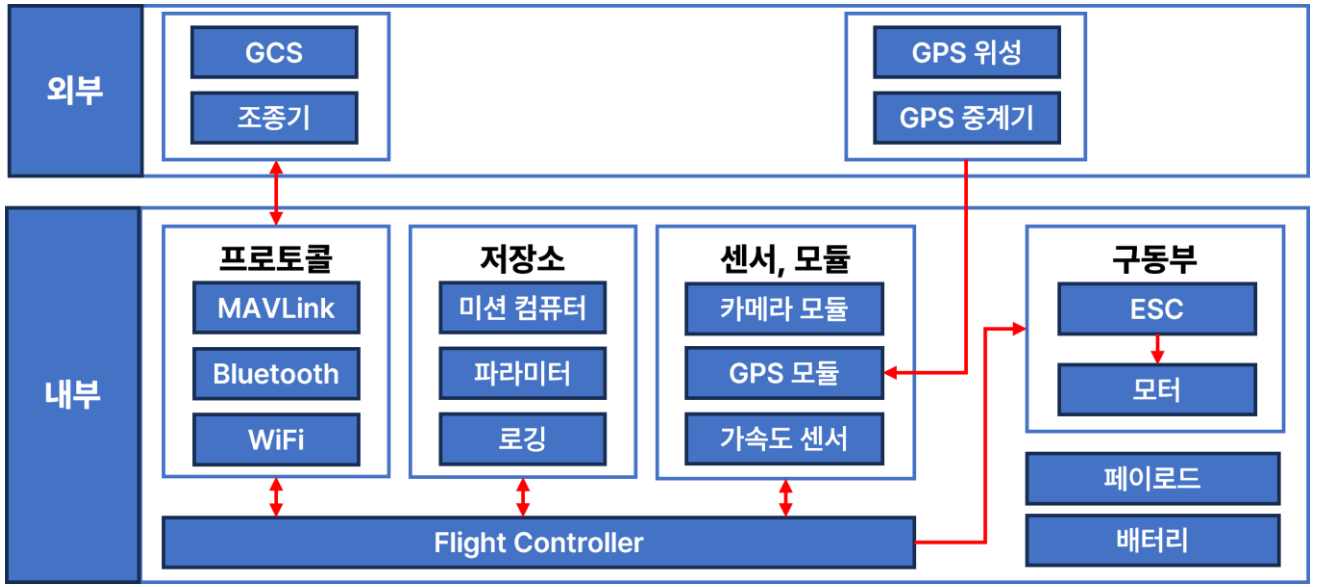
• • •

- 군 무인이동체 특성 및 운용 환경을 고려한 사이버보안 프레임워크 및 실내·외 상시 시험환경 개발 R&D 사업('23~'25년 – 3년) 수행

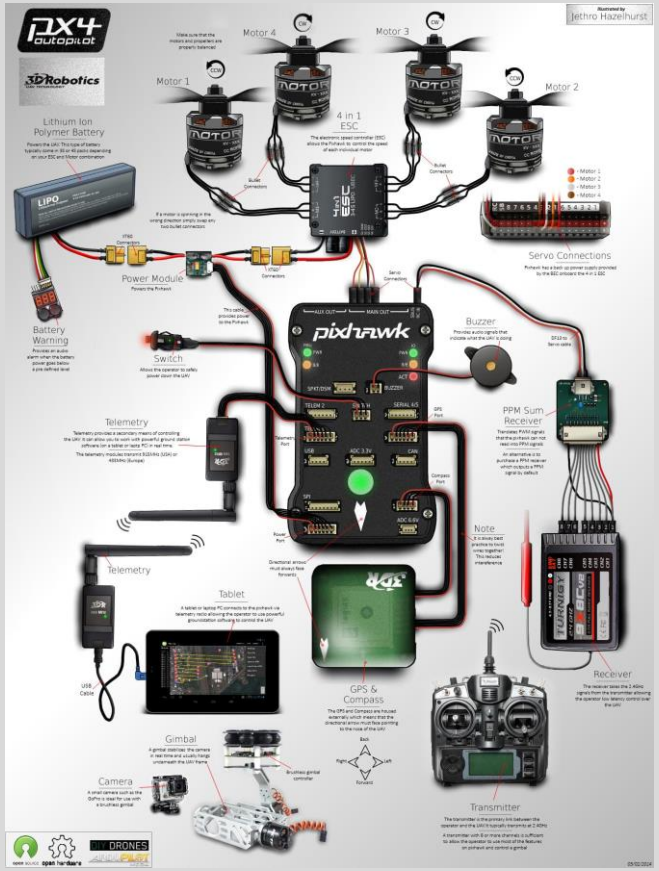
드론의 구조

Drone의 구조

- 드론은 기존 전자제품에, 비행하기 위해 필요한 모터, 로터가 장착된 기기
- 통신 방식에 따라 MAVLink, Bluetooth, ZigBee, WiFi, LTE, 5G 등의 통신 장비 장착
- 임무 기능에 따라 별도의 미션컴퓨터의 SD Card, Flash 등에 다양한 Data 저장용
- 카메라, GPS 등 별도의 기능을 수행하기 위한 장치 등 부착

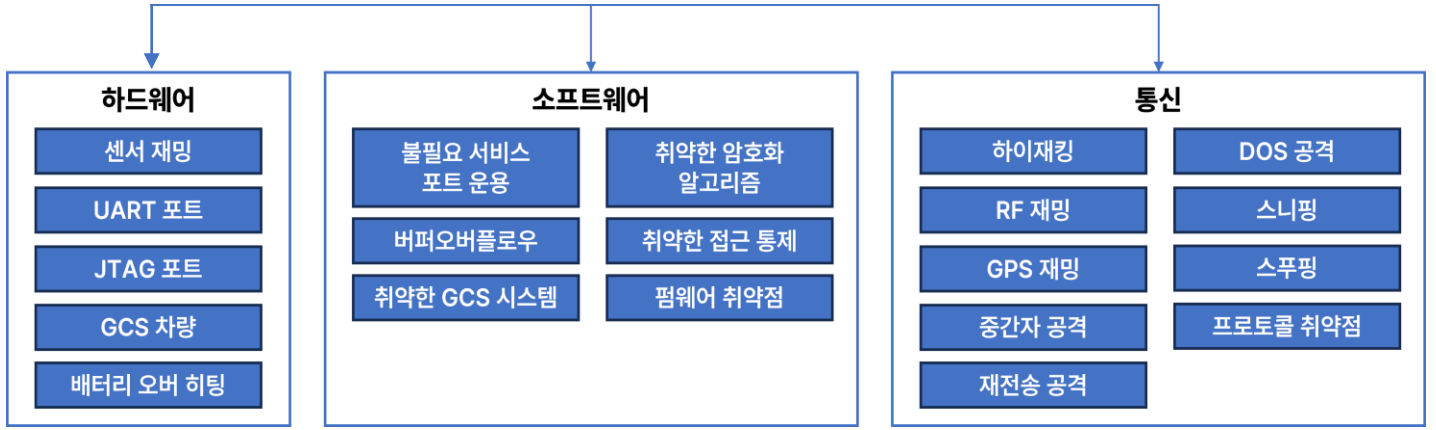


취약점



Drone Attack Surface

- 모든 기능, 서비스 및 잠재적인 진입 지점을 식별
- 취약점에 접근을 용이 하기 위해 하드웨어, 소프트웨어, 통신 분야 등으로 구분



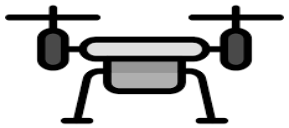
취약점 진단 목적

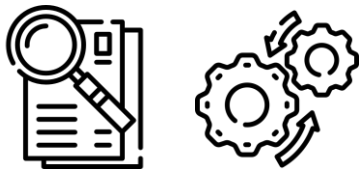
- 드론의 무력화, 제어권 탈취, 자료 유출 등으로 부터 드론을 안전하게 보호

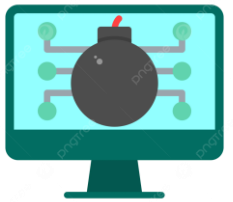
취약점 진단 방법

진단프로세스

탐색 → 분류(공격 벡터 식별) → 발견(취약점 진단) → 공격(적대적 공격)

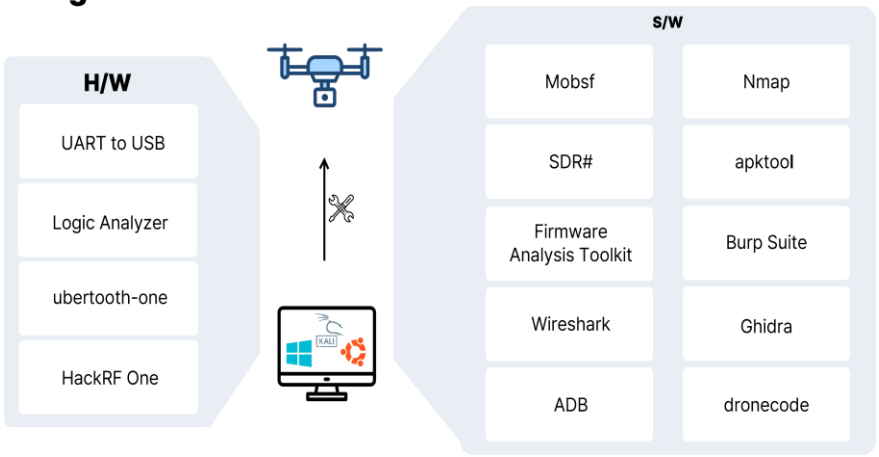


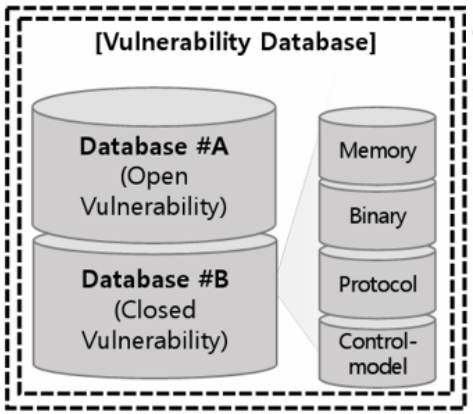




공격 벡터 식별 후 진단에 필요한 도구 선별

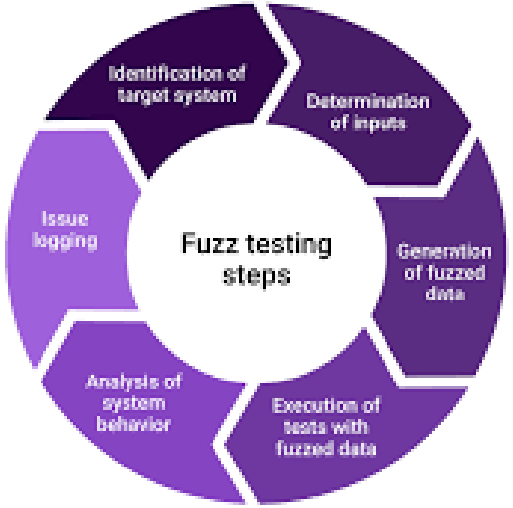
Testing tools





Bugs & Vulnerabilities

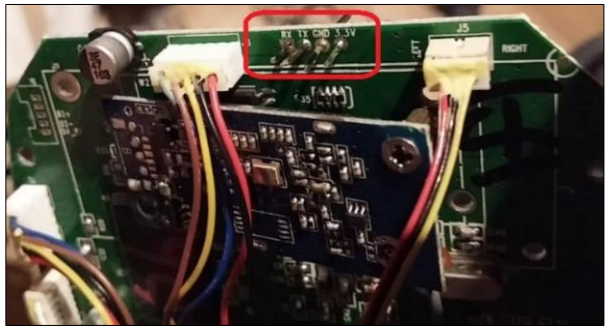
위협분석
1-Day 취약점 진단



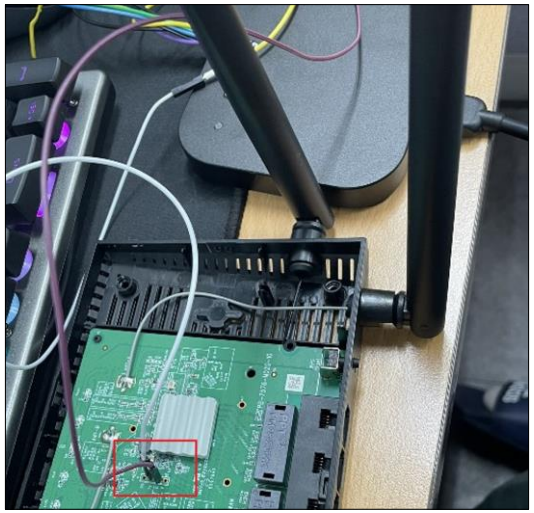
취약점 진단 과정 (1/3)

취약점 진단 과정이 쉽지 않다

- 정보체계 취약점 진단과 같이 LAN 선 하나 연결 후 작업을 수행 하는 것처럼 쉽게 취약점을 식별하고 도출해 낼 수 없다(접근이 용이하지 않다)
- 드론의 종류에 따라 다수의 수작업과 드론과 분석장비를 연결하기 위한 보조 장비들이 필요
- 비행중인 드론을 원격에서 취약점 진단하는 것은 Jamming, Spoofing 등 전용 장비로 무선신호를 공격하는 것 외에 곤란



Uart 핀 식별



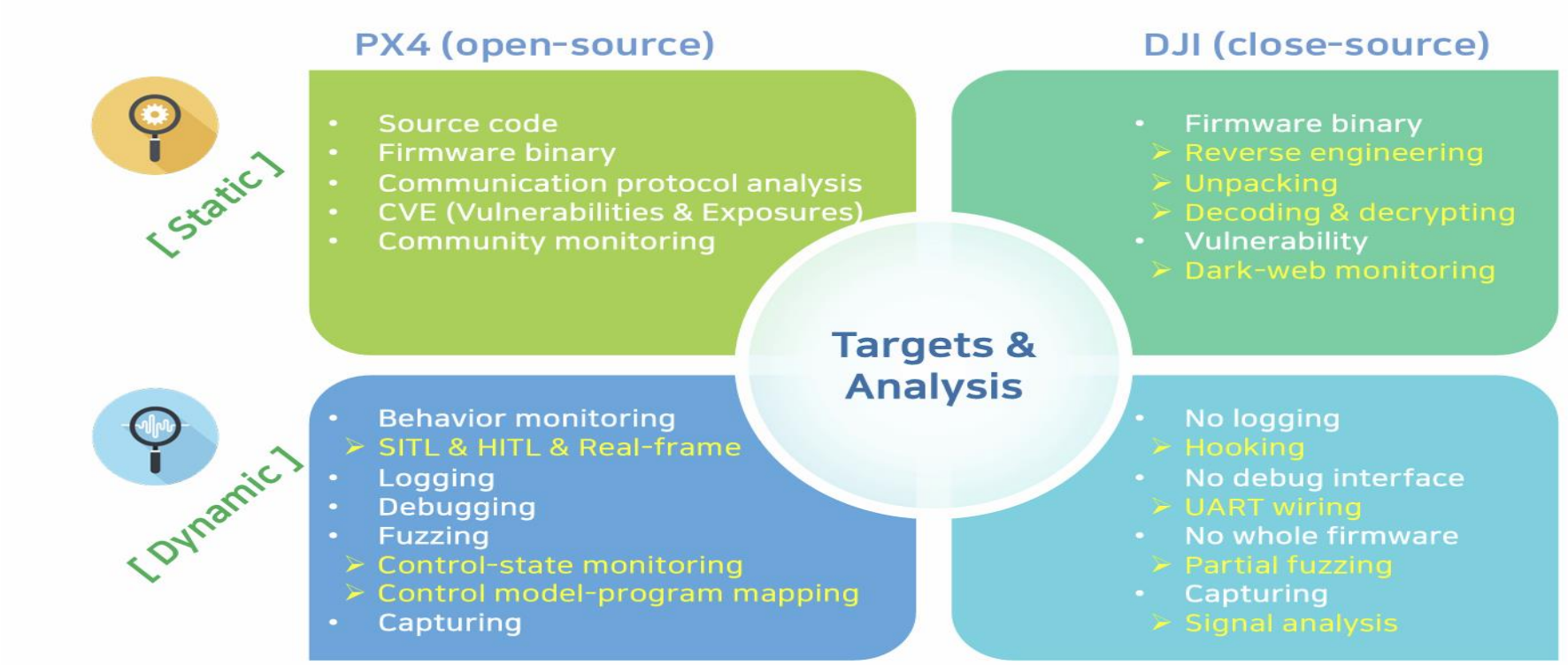
Log Analyzer로 Uart 핀 구분

USB to Uart를 이용, PC에 연결

취약점 진단 과정 (2/3)

펌웨어 분석이 어렵다

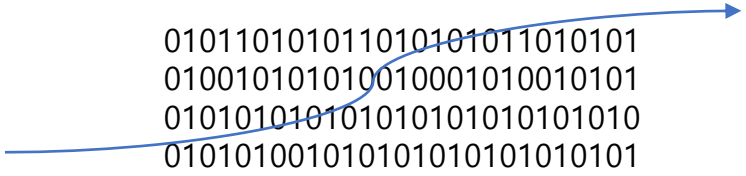
- 펌웨어의 내부 정보(예,라이브러리,설정,구조 등) 부족, Px4 같은 경우 Source Code가 공개되어 있어 다소 양호하나 DJI 같은 경우 온전히 Binary 분석(Reverse Engineering, Unpacking, Decode 등)에 의존
- 온전한 펌웨어 추출 난해, 특히 분석 방지 및 보안 기능 등을 사용할 경우 더욱 곤란



취약점 진단 과정 (3/3)

종류도 많고 취약점 진단 환경도 제한된다

- 드론 비행제어기는 운행에 필요한 필수 프로그램만 운용할 수 있도록 경량, 취약점 발견 희박
- 또한, 드론 종류가 많고 기능도 다변화되어 있어 동일 취약점을 각 기기에 적용 곤란, 취약점에 접근이 제한됨
- 취약점을 운행중인 드론에 적용하여 검증하는 것도 매우 어려움

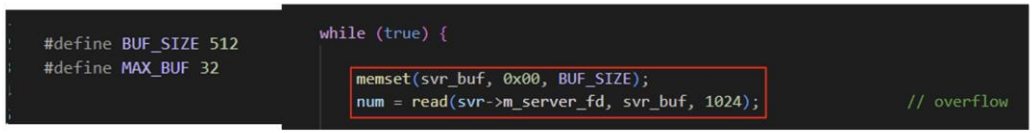


취약점 진단 결과(보안 위협)

비행제어기 보다 임무기능 컴퓨터에 취약점이 많음

- 암호장비, 영상수집기, 비행 분석기 등 드론에 부착되는 임무 기능 수행 장비 취약점 수집 용이

  * 디폴트 패스워드 등 취약한 계정정보 노출, BOF 등 응용 프로그램 취약점 등

취약한 비밀번호 사용	Buffer Overflow 취약점
	

접근이 용이할수록 위험에 노출

- 보안에 취약한 근거리 무선 통신(Bluetooth, Wifi 등) 등을 사용할 경우 제어권 탈취 등 공격 용이
- 범용 OS를 사용하는 GCS 컨트롤러를 해킹 시 백도어 등 악성코드 삽입 공격 가능

무선신호를 이용한 공격(Jamming, GNSS Spoofing 등)에 무방비

드론은 고급 해킹 기술과 상당히 오랜 기간동안 장비와 시간을 투자하여 공격해야 가능,

의도적 공격이 경우 국가적 큰 위협,미국이 국가수권법으로 중국산 드론을 통제하는 이유

대응 방안

드론 등 IoT 장비들은 해킹 시 신체적·물리적 위해 가능, 사전 예방 활동 중요

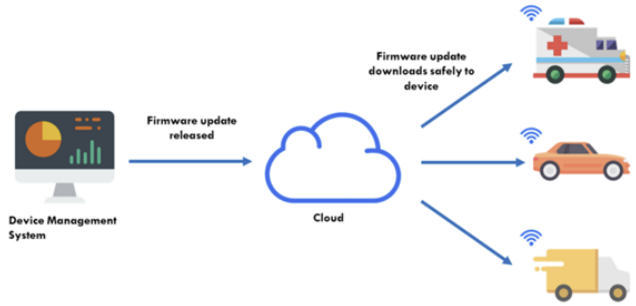
- 기존의 정보체계 해킹은 자기 과시 · 금전적 이득 · 정보획득 등이 목적이 반면, 드론 등 IoT 장비는 전복 · 파괴 등에 따른 물리적 손상 뿐 아니라 신체적 위해 가능
- 따라서, 제품 출시 前 **보안컨설팅 등을 통한 사전 예방 활동** 매우 중요

인터넷, WiFi 등에 노출될 경우 초보자에게도 해킹 당할 수 있는 위험 내재, 기본 보안에 충실 필요

- 초기 인증 비밀번호 사용 금지, 특수기호 포함 9자리 이상 비밀번호 설정 등 **계정 설정 강화** 필요
- 중요 내용을 담고 있는 자료는 유출 방지를 위해 반드시 **비도가 보장된 암호화** 저장

독립적으로 운용되는 외부 非 노출시스템의 경우, 공급망 보안 통제 강화 필요

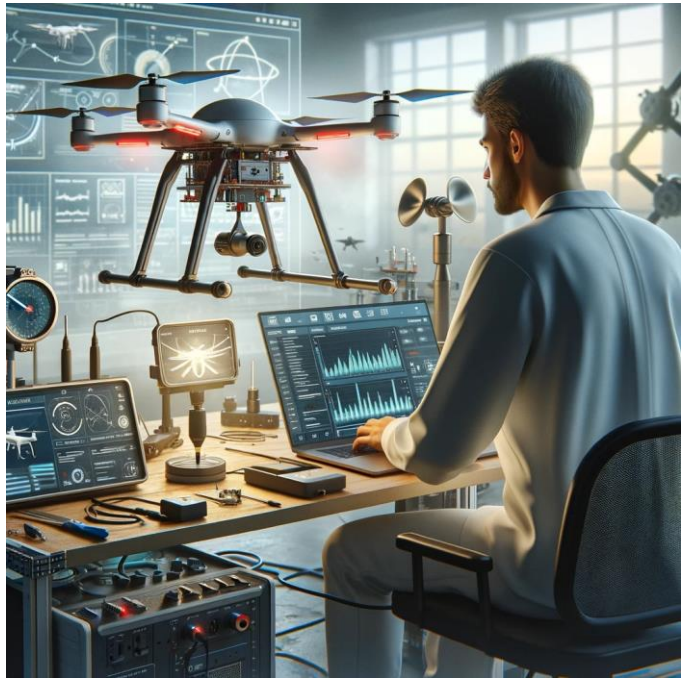
- USB, OTA 등 펌웨어 업그레이드 등 **성능 개선을 위한 Update 시 보안통제 강화**
- 유지보수 업체 직원 방문 조치 및 제품 개선을 위해 제조사에 품질 개선을 요구 시 **공급망 보안 규정 준수**

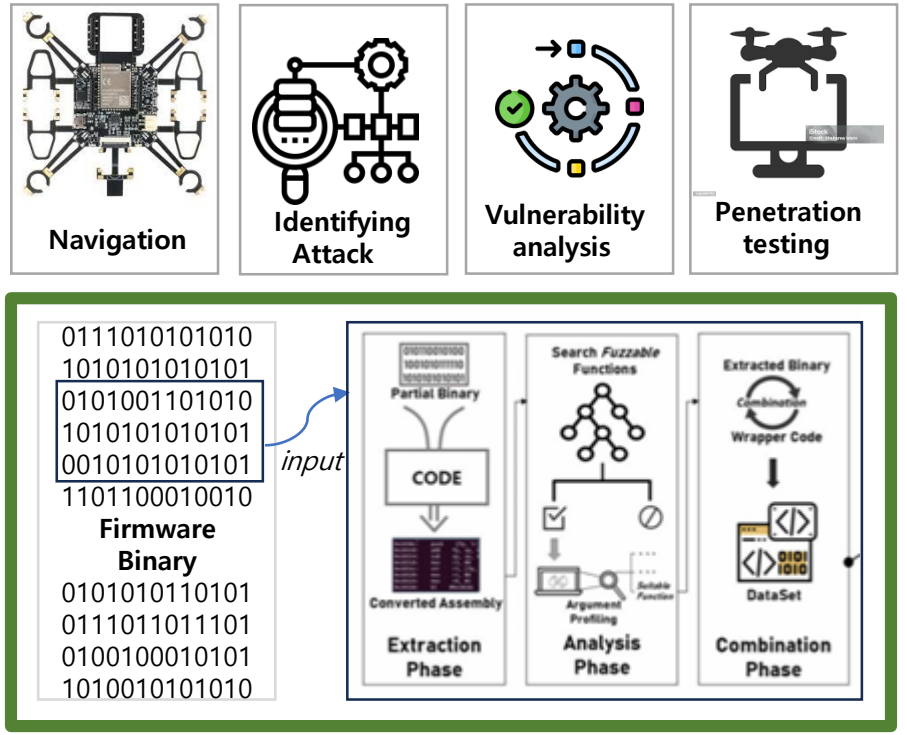


결론

드론, 자동차, AI 장비 등 첨단 컴퓨터가 장착된 IoT 기기들은

보안컨설팅 등 사전 사이버 보안 활동을 통해 보호하는 것이 피해를 최소화 하는 것입니다.





(주)테르텐은 IoT 기기에 대한 사이버보안 진단, 시험, 위협 평가 등 사이버보안 활동을 수행하기 위한 다양한 장비와 전문 기술 인력을 갖추고 있습니다.

감사합니다