ARM PSA 기반의 드론 보안 시스템 설계

김성수°, 박현우, 조진성
경희대학교 컴퓨터공학과
korkeep@khu.ac.kr, purepdu1109@gmail.com, chojs@khu.ac.kr

A Drone Security System Design based on ARM PSA

Sungsu Kim°, HyeonWoo Park, Jinsung Cho
Department of Computer Science and Engineering, KyungHee University

요 약

드론은 빅데이터, 사물인터넷, 인공지능, 클라우드 등 첨단기술과 융합하여 고도화되고 있다. 드론과 서비스의 연결은 사용자에게 편리함을 제공하는 동시에 드론 시스템의 보안 취약점을 노출시킬 수 있다. 오늘날 드론의 보안 취약점을 악용한 해킹 시도가 지속적으로 증가하고 있으며, 이에 따라 보안 기능이 강화된 드론 시스템이 요구되는 상황이다. 본 논문에서는 ARM PSA(Platform Security Architecture) 기능을 활용하여 개인키, 사용자 데이터, 보안 기능 등 드론 시스템의 주요 자산을 보호할 수 있는 아키텍처를 제안한다.

1. 서 론

드론은 빅데이터, 사물인터넷, 인공지능, 클라우드 등 첨단기술을 적용, 검증할 수 있는 테스트베드(Testbed)로 활용 가능하다. 이에 따라 정부는 혁신성장 8대 사업으로 드론을 선정하여 드론 산업의 시장규모를 2026년까지 4조 4000억 원으로 키우는 것을 목표하고 있다.[1]

오늘날 드론은 4차 산업혁명의 핵심 기술과 융합하여 군사, 촬영, 감시, 측량, 수송 등 다방면에서 특수한 임무를 수행하고 있다. 드론과 서비스의 연결은 사용자에게 편리함을 제공하는 반면, 해커가 드론 시스템에 접근할 수 있는 취약점으로도 작용한다.

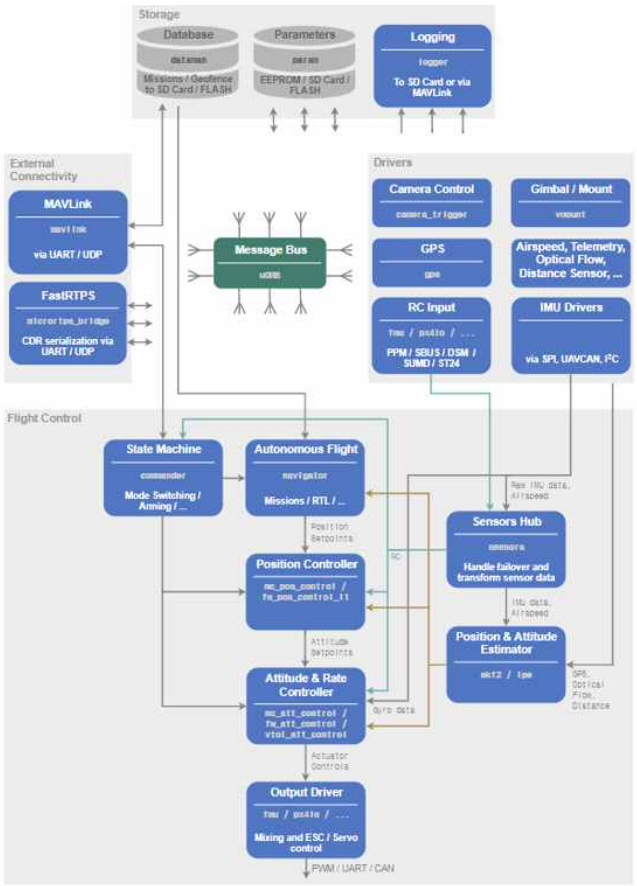
최근 드론 취약점에 대한 연구가 활발하게 이루어짐에 따라 이를 악용한 사례가 나오고 있다. Parrot AR 드론의 경우, nmap 포트 스캐닝 기법을 활용하여 FTP와 Telnet 포트가 열린 것을 확인한 후, shell에 접근하여 데이터 전송 및 강제 종료 명령을 내릴 수 있었다.[2] 이외에도 드론을 표적으로 한 해킹 기법이 지속적으로 밝혀지고 있으며, 드론의 보안성 강화가 요구되는 상황이다.

본 논문에서는 개인키, 사용자 데이터, 보안 기능 등 드론 시스템의 주요 자산을 보호할 수 있는 아키텍처를 제안한다. ARMv8-M 프로세서를 기반으로 신뢰 환경의 보장, 안전한 키 저장, 안전한 펌웨어 업데이트, 암호화 가속기 등 ARM PSA의 보안 기능을 제공하는 SoC(System on Chip) 드론 아키텍처를 설계했다.

본 논문은 ETRI부설연구소의 위탁연구과제[2021-076]로 수행하였고, 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학지원사업[2017-0-00093]의 연구결과로 수행되었음

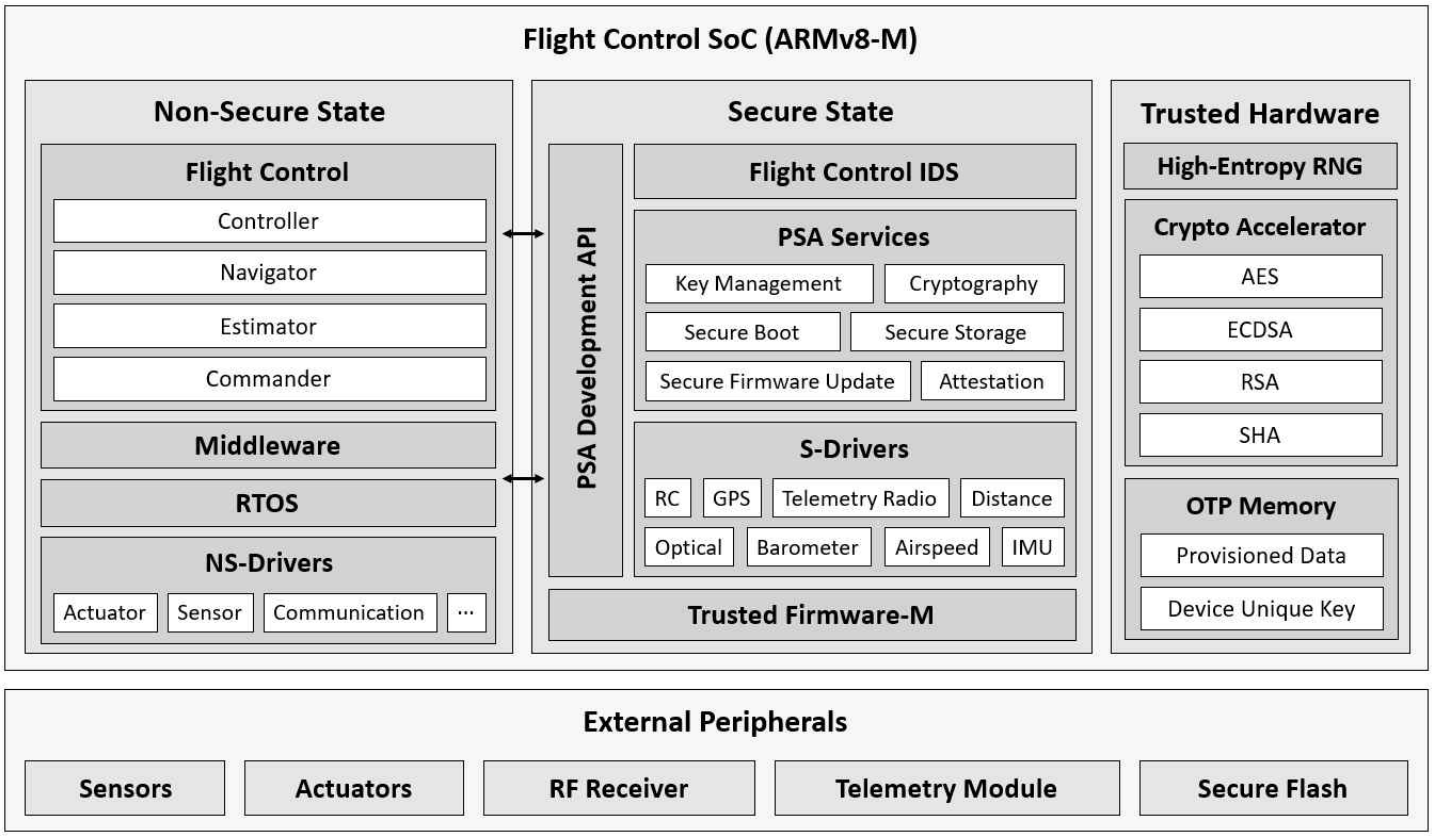
2. 관련 연구

2.1 PX4



[그림 1] PX4 소프트웨어 아키텍처

PX4 프로젝트는 오픈소스 기반의 드론 SDK이다. PX4는 드론 시스템의 표준을 제공함으로써 PX4 Ecosystem이 유지될 수 있도록 확장성을 보장한다.[3] [그림 2]의 드론 시스템 구조는 [그림 1]을 참고하여 설계했다.



[그림 2] ARM PSA 기반의 드론 보안 시스템 아키텍처

2.2 ARM PSA

ARM PSA는 개인키, 사용자 데이터, 보안 기능 등 시스템의 주요 자산을 인가되지 않은 외부의 접근으로부터 보호하기 위해 도입되었다. PSA는 메모리, 주변장치, 기능을 Secure 영역과 Non-Secure 영역으로 나눔으로써 하드웨어적으로 실행 환경의 분리를 보장하는 메커니즘이다. ARMv8-M은 ARM Cortex-M 프로세서를 기반으로 PSA 기능을 활용할 수 있는 모델이다. ARMv8-M 시리즈는 대표적으로 M23, M33, M35P, M55가 있으며 해당 프로세서에서는 신뢰 환경의 보장, 안전한 키 저장, 안전한 펌웨어 업데이트, 암호화 가속기 등 PSA 기반의 보안 기능이 제공된다.[4]

ARMv8-M 프로세서는 Non-Secure에서 Secure 영역으로의 접근을 막는 방법으로 각 도메인마다 Exception Level 이라는 권한을 설정함으로써 인가되지 않은 외부의 접근을 하드웨어적으로 보호하고 있다. 만약 Non-Secure 영역에서 Secure 영역으로의 접근이 필요하다면, NSC (Non-Secure Callable) 함수를 통해 프로세서의 상태를 Secure State로 전환하여 Secure 영역의 자산에 접근 가능하다. Secure 영역의 함수 동작이 완료되면, 프로세서는 BXNS 명령어를 호출해 Non-Secure State로 전환된다. 반면 Secure 영역에서 Non-Secure 영역으로 접근하는 경우, 프로세서는 BLXNS 명령어를 호출해 Secure State에서 Non-Secure State로 전환된다. Non-Secure 영역의 함수 동작이 완료되면, BLXNS 명령에서 설정된 FUNC_RETURN 주소로 분기되면서 Secure State로 전환된다.[5][6]

3. 드론 보안 시스템 설계

3장에서는 ARMv8-M 프로세서 기반 SoC(System on Chip) 드론 보안 시스템에 대해 소개한다. [그림 2]에서 설계한 아키텍처를 모듈별로 구분하여 각 구성요소의 역할이 무엇인지 설명한다.

3.1 Flight Control SoC

3.1.1 Secure State

Secure State는 ARM PSA를 활용해 인가되지 않은 외부의 접근으로부터 보호할 수 있는 안전한 실행 환경이다. Secure State의 구성요소로 Trusted Firmware, S-Driver, Flight Control IDS, PSA Services, PSA Development API가 있다.

- **Trsuted Firmware**: Trusted Firmware는 안전한 실행 환경을 구축할 수 있는 소프트웨어 패키지를 제공하며, PSA 기능을 활용할 수 있는 기반이 된다.
- **S-Drivers**: 드론 시스템 구동에 핵심적인 역할을 수행하며, 안전한 실행 환경에서 작동하는 드라이버다.

• **PSA Services**: 드론 시스템에 적용할 수 있는 보안 기능이다. PSA Services에서 제공하는 기능으로는 Key Management, Cryptography, Secure Boot, Secure Storage, Secure Firmware Update, Attestation이 있다.

• **Flight Control IDS**: 드론에서 기록되는 로그를 모니터링하여 일반적인 경우와 다른 로그가 발생한다면, 사용자에게 알림을 주는 것으로 침입을 탐지한다.

• **PSA Development API**: Non-Secure 영역의 애플리케이션에서 Secure 영역의 자산에 접근할 수 있는 PSA Development API를 제공한다.

3.1.2 Non-Secure State

Non-Secure State는 드론 애플리케이션, 미들웨어, 운영체제, 드라이버가 작동하는 일반적인 실행 환경이다. Non-Secure State의 구성요소로는 NS-Driver, RTOS, Middleware, Flight Control이 있다.

• **NS-Drivers**: 드론 시스템 구동에 부수적인 역할을 수행하며, 일반 실행 환경에서 작동하는 드라이버다.

• **RTOS**: 실시간 애플리케이션 관리에 초점이 맞춰진 운영체제다. PX4에서는 NuttX가 이 역할을 수행한다.

• **Middleware**: RTOS와 Flight Control 사이에서 데이터 중개 역할을 하는 소프트웨어다. PX4에서는 uORB가 이 역할을 수행한다.

• **Flight Control**: 드론 제어에 필요한 모듈과 드론 시스템에서 데이터가 처리되는 흐름을 나타낸 것이다. 먼저 Commander에서 사용자 명령을 받아와 Estimator, Navigator, Controller 순으로 데이터가 전달된다.

3.1.3 Trusted Hardware

Trusted Hardware는 Secure State에서 제공하는 보안 기능을 활용하기 위해 필요한 하드웨어 모듈이다. Trusted Hardware의 구성요소로는 High-Entropy RNG, Crypto Accelerator, OTP Memory가 있다.

• **High-Entropy RNG**: 높은 엔트로피를 가지는 난수를 하드웨어적으로 생성한다. 난수는 암호화 과정에 사용되며, PRNG(Pseudo RNG)보다 높은 신뢰성을 가진다.

• **Crypto Accelerator**: 키 생성, 암호화, 복호화를 수행하는 하드웨어로 AES, ECDSA, RSA, SHA 등 다양한 암호화 알고리즘을 지원한다. Crypto Accelerator는 Secure Flash에 데이터를 암호화하여 저장한다.

• **OTP(One-Time Programmable) Memory**: OTP Memory는 비휘발성이고 재기록이 불가능하다는 특징을 가진다. SoC 장치를 제작할 때 기본적으로 제공되는 Provisioned Data와, 암호화 과정에 사용되는 Device Unique Key가 존재한다.

3.2 External Peripherals

3.2.1 Sensors

드론 시스템을 구동하기 위해 필요한 센서이다. 대표적으로 GPS, IMU, Optical Flow, Distance, Camera, Barometer, Airspeed 센서를 통해 데이터를 수집한다.

3.2.2 Actuators

센서에서 수집된 데이터를 Flight Control SoC에서 처리하고, 드론은 처리된 데이터와 액추에이터를 이용해 비행한다. Servo Motor가 이 역할을 수행한다.

3.2.3 RF Receiver

Radio Controller를 통해 드론에 전달되는 전파 신호를 탐지하기 위한 장치이다.

3.2.4 Telemetry Module

사용자가 GCS(Ground Control Station)를 이용해 드론에게 전달하는 명령을 탐지하기 위한 장치이다. 대표적으로 WLAN 기반의 ESP-8266, SDR(Software Defined Radio)를 이용하는 SiK Radio가 있다.

3.2.5 Secure Flash

Secure Flash는 Crypto Accelerator에 의해 암호화된 데이터가 저장되는 공간이다. 드론이 공격자에 의해 포획되더라도 데이터가 암호화되어 있기 때문에 공격자는 Secure Flash에 저장된 데이터를 확인할 수 없다.

4. 결론 및 향후 계획

본 논문에서는 ARM PSA 기능을 활용해 SoC 기반 드론 시스템에서 주요 자산을 보호할 수 있는 아키텍처를 설계했다. 향후 ARM PSA 기능을 지원하는 STM32 개발 보드에 [그림 2]에서 제안하는 아키텍처를 적용하여, PSA Service, Flight Control IDS, S-Drivers 등 보안 기능이 강화된 드론 시스템을 구축할 계획이다.

참고문헌

[1] 국토교통부「드론산업 발전 기본계획」1-6 (2017)
[2] Ignacio Astaburuaga, Amee Lombardi, Brian La Torre, Carolyn Hughes, Shamik Sengupta「Vulnerability Analysis of AR.Drone 2.0, an Embedded Linux System」IEEE Computing and Communication Conference (2019)
[3] PX4 Development Guide「PX4 Architecture overview」https://dev.px4.io/master/en/ (2019)
[4] ARM「Arm Platform Security Architecture Trusted Base System Architecture for Armv6-M, Armv7-M and Armv8-M 1.0」Architecture & Tech. Group, 12-15 (2019)
[5] ARM「Secure software guideline for ARMv8-M version 2.0」9-12 (2020)
[6] 정준영, 조진성「KHU-TEE: ARM PSA 기반 IoT 보안 플랫폼」KIISE Transactions on Computing Practices, Vol. 26, No. 5, 244-249, (2020)