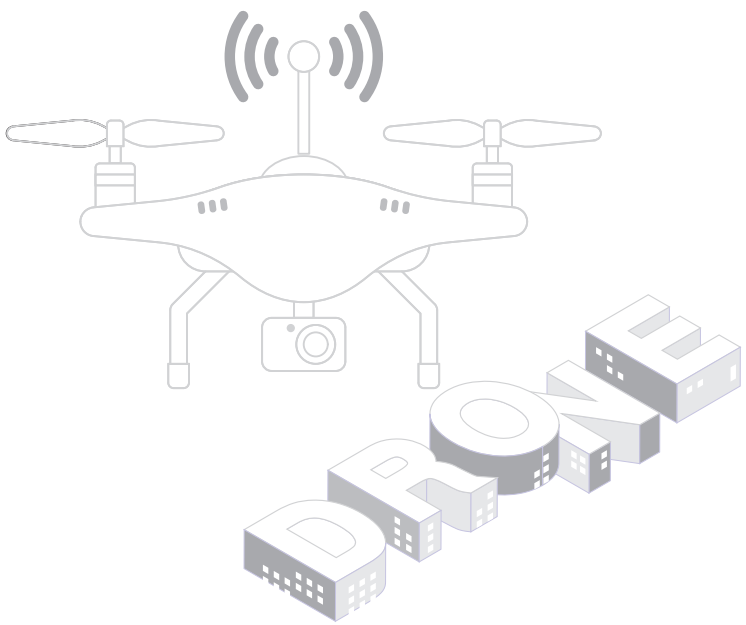
Cyber Security Guide for **Drone**

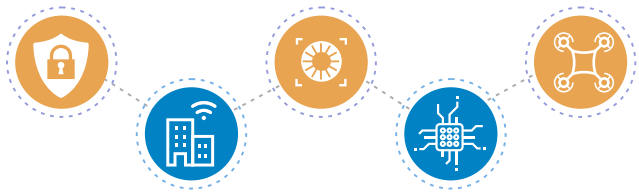
드론 분야 ICT 융합 제품·서비스의
보안 내재화를 위한

드론 사이버보안 가이드

2020.12.

KISA 한국인터넷진흥원


DRONE



CONTENTS

PART 01

개 요

제1절 배경 및 목적
제2절 적용 범위
제3절 용어 및 약어 정의

PART 1

개 요

제1절 배경 및 목적

국내에서는 드론(Drone)은 조종사가 직접 탑승하지 않고 원거리에서 무선으로 원격 조정을 하거나 입력된 프로그램에 따라 비행이 가능한 비행체로 정의하고 있다.[1] 드론의 개발 초기에는 군사 목적으로 개발, 활용되었으나, 최근 정보통신기술(ICT, Information & Communication Technology)과 융합되어 배송, 안전관리, 환경 관리, 재난 상황 감시 등의 다양한 산업 서비스에 활용되고 있다.

국토교통부에 따르면 전 세계 드론 시장규모는 2016년 7조2000억 원에서 2022년 43조2000억 원, 2026년 90조3000억 원의 규모로 성장할 것이라고 예상하고 있다. 또한, M&M(Marketsandmarkets)에 따르면 드론 서비스의 글로벌 시장 규모는 2016년 7억530만 달러에서 연평균 71.62% 고성장을 지속하여 2022년 180억2,270만 달러의 규모로 확대될 것이라고 예상하고 있다. 드론 기반의 서비스는 ICT 기술과 다양한 서비스, 콘텐츠가 융합되어 단순 비행체가 아닌 새로운 비즈니스 모델이 창출되고 있기 때문이다.

그러나 드론, 드론 서비스에 사이버 위협이 발생할 경우 서비스 마비뿐만 아니라 인명피해와 같은 치명적인 위협이 발생할 수 있기 때문에 전세계의 다양한 연구기관에서 드론과 관련된 보안정책과 요구사항들을 제시하고 있다.

드론의 사이버 보안에 관한 국제적 활동에 비해 국내 드론 산업계의 보안의식 수준이 낮고, 드론 서비스의 분류와 지침이 부족한 형편이다. 따라서 본 가이드는 현재 활용 및 운용 중인 드론 기반 서비스에 필요한 기본적인 보안항목과 대응방안을 제시함으로써 드론과 관련된 서비스를 설계·제조하는 IT업체와 운용업체 및 이용자를 대상으로 하여 보안인식 제고와 보안 내재화를 촉진하는데 목적이 있다.

1) 출처 : 한국정보통신기술협회(TTA) 정보통신 용어 사전 및 정보통신단체표준(TTAK.KO-10.0789-Part14 ICT DIY 제14부: 창작 활동 안전 지침) 용어 정의

제2절 적용 범위

드론은 크기, 비행고도, 비행반경, 이착륙방식 등 종류를 분류하는 방법이 다양하다. 국내 항공안전법에서는 드론을 이륙중량 및 위험도에 따라 분류하고 있으며, 미국의 연방항공청은 드론의 무게에 따라 등록 및 사용 규정을 다르게 적용하고 있다.

분류	구분	기체신고	조종자격	비행승인
완구용 모형비행장치	최대 이륙중량 250g 이하	신고 불필요	자격 불필요	관제권(9.3km) 비행금지구역 내 교육목적 비행가능
저위험 모형비행장치	최대 이륙중량 250g 초과 ~ 7kg이하	신고 불필요	250g 초과 ~ 2kg 이하 (온라인교육)	
		소유자 신고	2kg 초과 ~ 7kg 이하 (필기+비행경력 6시간)	
중위험 모형비행장치	최대 이륙중량 7kg 초과 ~ 25kg이하	소유자 신고	7kg 초과 ~ 25kg 및 1,400J 초과 필기+비행경력 10시간+실기(약식)	*비행승인 필요
고위험 모형비행장치	최대 이륙중량 25kg 초과	소유자 신고	25kg 초과 ~ 14,000J 초과 필기+비행경력 20시간+실기	*비행승인 필요

출처 국토부 (2020.2.19, 항공안전법)

본 가이드의 대상이 되는 드론은 소유자가 신고를 해야 하는 저위험 모형비행장치 이상의 드론이 대상이다. 신고가 불필요한 개인이 레저를 위해 구입한 드론은 대상에서 제외되며, 드론을 이용하여 서비스 운용에 사용되는 드론을 대상으로 한다.

본 가이드 1장에서는 드론 산업에서의 안전한 서비스를 위한 가이드의 배경 및 목적과 적용 범위를 설명하고 사용되는 핵심 용어들을 정의한다.

2장에서는 드론 서비스 분석 및 드론 서비스 구성에 대해 설명한다. 또한 드론 서비스에서 발생할 수 있는 보안위협 및 위협 시나리오를 분석한다.

3장에서는 드론 서비스에서 필요한 기본적인 보안항목 및 대응방안을 제시하고 세부 보안 요구사항을 설명한다.

제3절 용어 및 약어 정의

가용성 (Availability)

인가를 받은 사용자가 정보나 서비스를 요구할 경우, 정보시스템에 대한 사용 가능 여부에 대한 권고사항

감사 로그 (Audit Log)

모든 작업의 활동 및 실행에 대한 기록

개인정보 (Privacy)

살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 식별할 수 있는 정보를 의미

기밀성 (Confidentiality)

중요 정보가 인가되지 않은 상대방에게 노출되지 않음을 보장해 주는 성질

드론 시스템 (UAS, Unmanned Aircraft System)

실제 조종사가 직접 탑승하지 않고, 지상에서 사전 프로그램된 경로에 따라 자동 또는 반자동으로 비행하는 드론, 지상제어장치, 정보제공장치와 통신링크(데이터 링크) 등의 드론 운용 시스템을 통칭

드론 서비스 (Drone Service)

배송, 안전 관리, 환경 관리, 재난 상황 감시 등 서비스의 드론을 활용한 서비스를 의미하며, 구성으로 드론 시스템과 드론 서비스 제공자 및 서비스 요청자를 포함함

멀티콥터 (multi-copter)

기체(회전익항공기)에 로터(회전날개 또는 프로펠러)를 2개 이상 이용해 이착륙, 추진 그리고 회전하는 항공기를 의미
프로펠러의 숫자에 따라 바이콥터(2개), 트리콥터(3개), 쿼드콥터(4개), 헥사콥터(6개), 옥토콥터(8개)로 분류

무결성 (Integrity)

네트워크를 통해 송·수신되거나 정보시스템에 보관되어 있는 정보가 불법적으로 변경되거나 삭제되지 않도록 보장하는 성질. 데이터 및 네트워크 보안에 있어서 정보가 인가된 사람에 의해서만 접근 또는 변경이 가능하다는 확실성

부인방지 (Non-Repudiation)

메시지의 송·수신이나 교환 후, 또는 통신이나 처리가 실행된 후에 그 사실을 사후에 증명함으로써 사실 부인을 방지하는 보안기술

스푸핑 (Spoofing)

외부의 악의적인 네트워크 공격자가 구성요소 간의 트래픽을 공격자의 컴퓨터로 우회시켜 정보를 탈취하는 기법

인증 (Authentication)

인증은 사용자가 허가된 사용자인지 확인하거나 전송된 메시지 위·변조 여부를 확인하는 성질

지상제어장치 (GCS, Ground Control Station)

드론에게 명령을 전달하거나 직접 드론을 원격으로 제어하는 장치로, 드론에게 실질적인 임무를 부여하는 명령을 전달하는 조종장치(조종기), 지상통제소 등을 의미

텔레메트리 (Telemetry)

자동화된 감지, 데이터 측정 및 원격 장치의 제어를 가리키는 것으로 디바이스에서 중앙 제어 지점으로의 데이터 전송을 말하며, 디바이스로 구성 및 제어 정보를 송신하는 것을 포함

호버링 (Hovering)

드론이 공중에서 비행 시 정지 상태를 일정기간 유지하는 능력으로 호버링 능력의 주요 요소는 모터의 추력(Thrust)임

C2 링크

드론에 Command and Control 명령을 전달하기 위한 Radio System

DoS (Denial of Service)

시스템 또는 네트워크 자원에 대해 합법적으로 접근하는 사용자를 접근하지 못하도록 하는 시도로써, 주로 대량의 서비스 요구 데이터 패킷을 보내어 시스템을 과부하를 발생시켜 사용자에게 서비스를 제공하지 못하도록 하는 공격

FPV (First Person View)

운영자가 UAV의 관점에서 UAV를 비행할 수 있게 하는 기술

GNSS (Global Navigation Satellite System)

인공위성을 이용하여 지상물의 위치·고도·속도 등에 관한 정보를 제공하는 시스템

GPS (Global Positioning System

드론의 정확한 위치를 파악하기 위한 핵심 장치로 드론 운행에 꼭 필요함. GPS는 인공위성으로부터 수신되는 전파를 분석하여 현재 드론의 위치를 파악하도록 함. 정확한 위치 파악을 위해 보통 3개 이상의 위성이 제공하는 정보를 분석하여 위치를 파악함

JTAG (Joint Test Action Group)

임베디드 시스템 개발 시에 사용하는 디버깅 장비로 개발 시 통합한 회로로 사용되는 IEEE 1149.1의 일반적인 이름

PART 02

드론 서비스 구성 및 보안위협

제1절 드론 서비스 구성
제2절 드론 서비스 보안위협
제3절 위협 시나리오

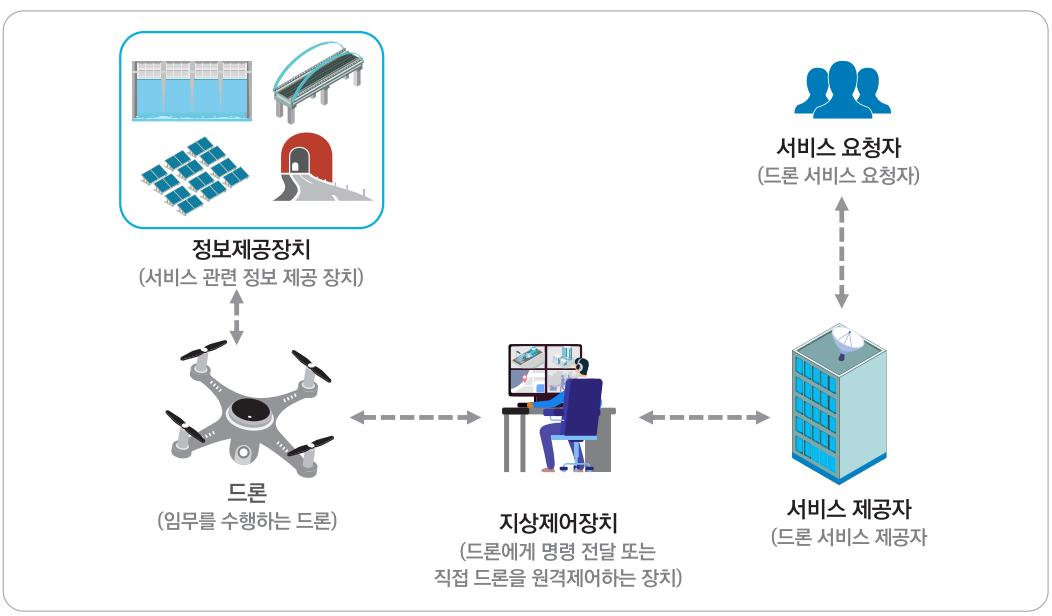
PART 2

드론 서비스 구성 및 보안위협

제1절 드론 서비스 구성

드론(Drone) 서비스는 드론의 무인비행 특성을 기반으로 ICT 기술을 결합한 신산업 서비스이다. 드론은 조종사가 직접 탑승하지 않고 무선으로 원격 조정할 수 있으며, 입력된 프로그램에 따라 역할 수행이 가능하기 때문에 개인, 상업 및 공공 분야에서 다양한 서비스를 제공하고 있다. 최근에는 드론을 이용하여 우편·택배 서비스, 스마트 도시 안심 서비스, 도시 환경 관리 서비스, 재난 상황 감시 서비스 등 다양한 서비스로 확대되고 있다.

이에 따라 본 가이드에서는 드론 기반의 대표적인 서비스를 분석하고 일반적인 구성요소를 분류, 분석한다.



드론 서비스 구성

드론 서비스의 구성은 크게 ‘드론’, ‘지상제어장치’, ‘정보제공장치’, ‘서비스 제공자, ‘서비스 요청자’로 구성된다. 이를 분석하기에 앞서 국내에서 운영 및 개발 중인 드론 기반 서비스를 분석하고 구성요소별 설명 및 발전동향과 서비스에 적용되는 사례를 설명한다.

1. 드론 서비스 분석

(1) 물품 배송 서비스

드론 기반 물품 배송 서비스

우체국에서 드론을 기반으로 물품을 배송하기 위한 시범사업을 운영하는 서비스이다. 도서(전라남도 고흥) 및 산간(강원도 영월) 지역에 테스트베드를 구축하여 의약품, 구호품 등의 긴급 물품을 대상으로 시범 운영하고 있다.

우체국의 드론 배송 서비스는 단계별로 서비스를 운영하고 있으며, 21년까지 도서·산간 지역을 중심으로 실증사업을 추진하고 이후 전국 우체국 현장에 적용할 계획이다.

(2) 도시 안심 서비스

드론 서비스 구성

도시 안심 서비스는 제주도의 스마트 친환경 드론 기반 도시행정 혁신 사업으로 수행되는 서비스 중 하나이다. 인적이 드물고 CCTV 설치가 어려운 곳에 순찰 드론을 활용하여 안전하게 귀가할 수 있도록 돕는 서비스로 '제주도 올레길'에 시범 도입할 예정이다.

위험에 처한 이용자가 스마트기기 앱으로 위험 신호를 보내면 드론이 현장으로 바로 출동한 후, 이용자의 스마트기기 위치 신호를 감지하여 이용자를 따라 가면서 영상을 촬영하고 목적지까지 안전하게 에스코트하는 서비스이다.

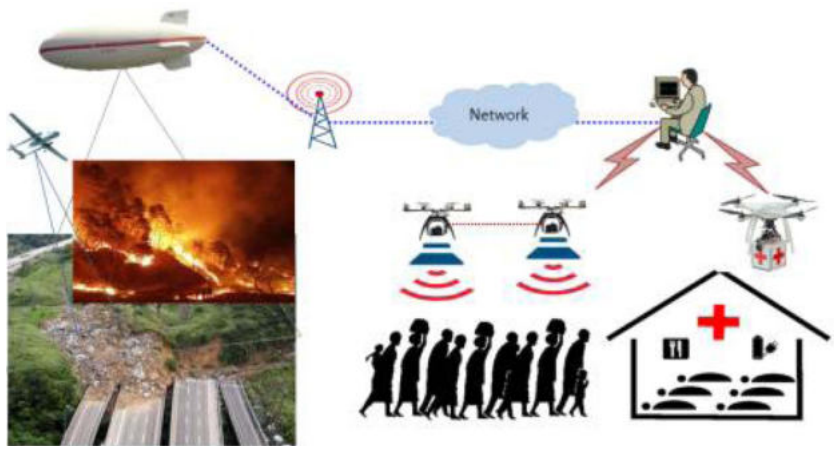
(3) 도시 환경 관리 서비스

출처 https://play.google.com/store/apps/details?id=kr.co.threessolution.droneintegrationsystem&hl=km

도심 환경 관리 서비스

도심 환경 관리 서비스는 부산시 드론 실증도시 서비스로 도심의 대기오염을 측정하기 위해 측정 센서(기상계측, 가스, 미세먼지, 오존, 자외선, 악취 센서 등)를 장착한 드론이 도심을 비행하면서 각 지점마다 대기질 상태를 측정한다. 드론은 위치정보와 측정 데이터를 지상제어장치로 송신한다.

(4) 재난 상황 감시 서비스

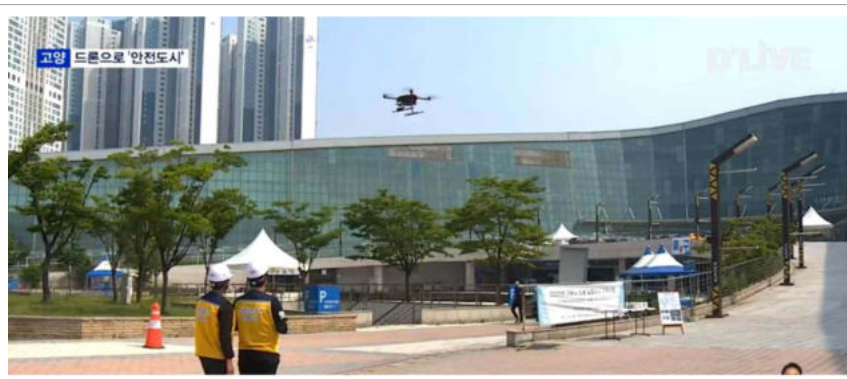


출처 시설 관리 및 재난 대응을 위한 드론 통신 및 보안 기술 동향, IITP, 2019.10.

드론 기반 재난 상황 감시 서비스

지진, 홍수, 산사태, 화재, 해일과 같은 재난 상황이 발생하기 전에 이를 조기에 감지하여 주변의 주민들이 대피하도록 알림으로써, 인명 피해를 줄이고 피해 상황을 신속하고 정확하게 파악하기 위한 서비스이다. 특히, 재난 상황 발생 시 드론 단독으로 임무를 수행하는 것보다는 감시 센서들을 조사 지역에 배치하여 조사 데이터를 수집하고 드론이 각 지역에서 수집된 데이터를 비행하면서 데이터를 모을 수 있도록 하여 더 효율적으로 재난 상황을 분석하므로 재난에 대비할 수 있도록 할 수 있다.

(5) 노후 인프라 안전점검 서비스



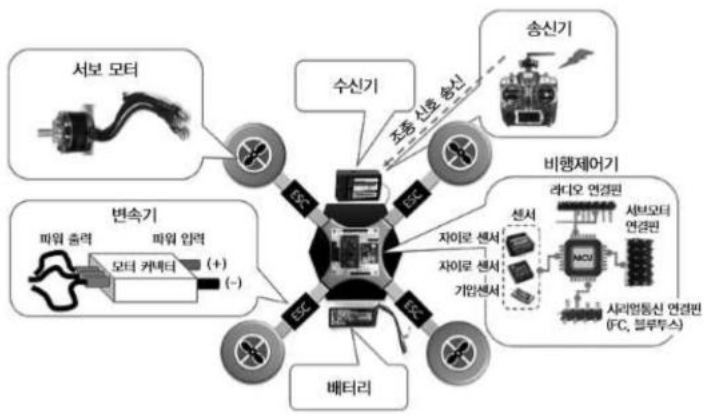
출처 https://www.youtube.com/watch?v=xj40YLJg5Ls

노후 인프라 안전점검 서비스 예시

고양시의 드론 실증도시 구축 사업인 노후 인프라 안전점검 서비스는 사람이 육안으로 확인하기 어려운 도로나 건물의 외벽 파손 등에 대하여 드론으로 상세 상태를 촬영하고 촬영한 영상을 3D모델링하여 향후에 발생할 수 있는 위험요소를 제거하기 위한 서비스이다.

2. 드론 서비스 구성

2.1. 드론



출처 드론의 구성, http://www.sigmapress.co.kr/shop/shop_image/g47841_1550542236.pdf

드론 HW 구성

드론은 조종사가 탑승하지 않고 원거리에서 무선으로 원격 조정 또는 입력된 프로그램에 따라 비행이 가능한 비행체를 말한다.

드론 내부 구성은 각각의 특징에 따라 구분될 수 있으며, 일반적으로 구동부, 제어부, 페이로드, 통신부로 구분된다. 따라서 본 가이드에서는 드론의 기본적인 기능에 따라 드론을 4가지 구성으로 분류하여 설명한다.

출처 드론의 구성, http://www.sigmapress.co.kr/shop/shop_image/g47841_1550542236.pdf

드론 구성도

2.1.1. 구성

드론 내부 구성은 각각의 특징에 따라 구분될 수 있으며, 일반적으로 구동부, 제어부, 페이로드, 통신부로 구분된다. 따라서 본 가이드에서는 드론의 기본적인 기능에 따라 드론을 4가지 구성으로 분류하여 설명한다.

〈드론 구성 및 기능〉

분류	기능
구동부	모터, 프로펠러, 전자변속기, 배터리 등을 포함하며, 드론의 비행을 구동하는 기능을 수행
제어부	가속도센서, 자이로센서, GPS 센서, 지자기센서 등을 포함하며, 드론의 비행을 제어하는 기능을 수행
페이로드	비디오 카메라, 적외선 카메라, 라이다, 가스 분석기, 농약 살포기, 초음파 센서 등이 포함될 수 있으며, 사용목적에 따라 탑재되어 각 기능을 수행
통신부	RC 수신기, 비디오 송신기, 텔레메트리 송신기, LTE, Wifi 등이 포함될 수 있으며, 데이터 송·수신 및 명령어 수신 등의 기능을 수행

가. 구동부

드론의 비행을 구동하는 기능을 수행하며 구동부의 구성과 발전 동향은 다음과 같다.

- **구　　성** : 모터, 프로펠러, 전자변속기, 배터리 등으로 구성된다.

- **발전동향** : 지상제어장치로부터 신호를 받은 전자 변속기는 모터를 구성시키고 프로펠러를 회전시켜 비행과 호버링을 가능하게 한다. 모터는 별도의 전자변속기로 구동되며 드론의 배터리는 대부분 리튬 폴리머(Li-Po) 배터리를 사용하는데, 이는 리튬 이온 배터리에 비해 안정성이 뛰어나며, 다양한 크기와 모양으로 제조가 가능하고 에너지 효율이 좋은 장점이 있다.

나. 제어부

드론의 비행을 제어하는 기능을 수행하며 제어부의 구성과 발전 동향은 다음과 같다.

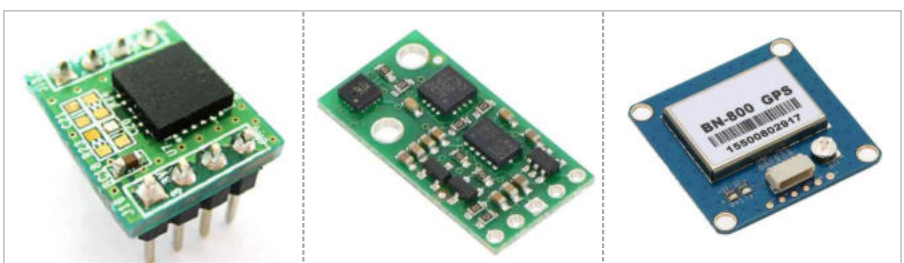
- **구　　성** : 비행제어기(Flight Controller)와 가속도센서, 자이로센서, GPS 센서, 지자기 센서 등으로 구성된다.

- **발전동향** : 드론의 안정적인 비행을 위해 각종 센서가 드론에 장착되어야 한다. 다양한 센서를 이용하여 비행상태를 측정한다. 드론의 비행상태는 회전운동상태와 병진운동상태로 정의되며, 회전운동상태는 요*(Yaw, z축회전), 피치**(Pitch, y축회전), 롤***(Roll, x축회전)을 의미하고 병진운동상태는 경도, 위도, 고도, 속도를 의미한다.

* Yaw : 또는 Rudder, 드론의 수평을 유지한 상태에서 동체를 회전시킴
** Pitch : 또는 Elevator, 드론 기수를 상하로 움직여 전진하거나 후진
***Roll : 또는 Aileron, 동체를 좌우로 기울임에 따라 드론이 좌우로 이동

회전운동상태를 측정하기 위해서는 자이로센서*, 가속도센서**, 지자기센서***가 장착되어야 하며, 병진운동상태를 측정하기 위해서는 GPS 수신기****와 기압센서가 장착되어야 한다. 비행제어기는 수신기로부터 전달받은 원격 비행명령어를 센서 융합기에서 보내온 상태 추정치와 비교하여 그 차이 값을 이용하여 구동부에 전달한다. 또한, 경유지 통과, 자동회귀, 충돌회피 등의 다양한 기능이 추가됨에 따라 빠른 연산을 위해 MCU(Micro Controller Unit)가 요구되고 있다.

* 중력에 대한 위치와 움직임을 측정하여 드론의 수평 유지를 돕는 센서
** X축, Y축, Z축의 세축 방향으로 기체의 속도, 위치, 기술기 방향전환 등을 감지
*** 지구의 자기를 측정하는 센서로, 지구 자기장의 방향과 세기를 파악함, 일종의 전자 나침반
**** GPS 센서로 표현되기도 하며, 인공위성의 신호를 사용하여 드론의 위치 자표와 고도를 측정



지자기센서 | 가속도 센서/자이로센서 | GPS 센서

출처 https://www.anadronestarting.com/%EC%84%BC%EC%84%9C/

다. 페이로드

드론의 사용목적에 따라 탑재될 수 있는 장비로 구성되며 발전 동향은 다음과 같다.

- **구 성** : 비디오 카메라, 적외선 카메라, 라이다, 가스 분석기, 농약 살포기, 초음파 센서 등으로 구성된다.

- **발전동향** : 드론의 사용목적에 따라 다양한 센서들이 장착되고 있으며, 다양한 센서에서 측정한 측정값 및 데이터는 통신부를 통해 지상제어장치로 송신하여, 사용자가 실시간으로 데이터를 수신 및 확인이 가능하다.

라. 통신부

데이터 송·수신 및 명령어 수신 등의 기능을 수행하며 통신부의 구성과 발전 동향은 다음과 같다.

- **구　　성** : RC 수신기, 비디오 송신기, 텔레메트리 송신기, LTE, Wifi 등으로 구성된다.

- **발전동향** : 통신부는 지상의 조종기로부터 비행명령어를 수신하는 RC 수신기, 촬영한 이미지나 동영상을 송신하는 비디오 송신기, 위치/속도/배터리 잔량 등 비행정보를 지상으로 송신하는 텔레메트리 송신기로 구성된다. 최근에는 WiFi 또는 LTE 송수신기를 탑재하여 원격 조정 명령어 및 비디오 데이터를 송수신하는 드론도 출시되었다.

2.1.2. 서비스 적용 사례

드론이 본 가이드의 제2장 제1절에서 설명한 서비스에 적용되는 사례는 다음과 같다.

(1) 물품 배송 서비스

도미노 피자 영국지사는 2012년 '도미콥터'라고 이름 붙은 에어로사이트사의 옥타콥터를 이용하여 피자는 배달해주는 시연을 성공하였다. '도미콥터'는 페퍼로니 피자 라지 사이즈 2판을 6.5km 거리의 주문자에게 10분 만에 배달해주었으며, 해당 드론은 위성항법장치와 카메라가 장착되어 배달과정을 촬영하고 영상 송신이 가능하다.

출처 https://youtu.be/on4DRTUvst0

도미콥터 소개 영상 캡처

(2) 도시 안심 서비스

출처 https://brunch.co.kr/@jejucenter/211

도시 안심 서비스 활용 드론

제주도에서 운영하고 있는 도시 안심 서비스에 순찰 드론 등 다양한 드론이 사용되고 있다. 순찰 드론은 이용자의 스마트기기의 위치신호를 감지하고 출동하여 이용자를 따라 가면서 영상을 촬영한다.

(3) 도시 환경 관리 서비스

출처 https://play.google.com/store/apps/details?id=kr.co.threessolution.droneintegrationsystem&hl=km

대기오염 측정 드론

대기오염 측정 드론은 대기환경 관측, 대기질 측정으로 나눠져 임무를 수행하며, 자동이륙, 자동비행, 자동착륙 기능이 내장되어 기상 및 대기오염 관측 임무가 자동화 가능하다.

(4) 재난 상황 감시 서비스

출처 https://www.donga.com/news/Economy/article/all/20191031/98163205/1

재난 치안용 드론

소방청, 해경청, 경찰청에 활용 가능한 재난 상황 감시 드론은 재난상황 발생 시 재난 현장 감시를 통하여 수집한 재난 영상정보를 전송하고, 조난자 발견 시 구명장비를 투하하는 등의 임무를 수행한다. 이를 위한 드론은 기존 상용 드론이 감당하기 어려운 재난 환경(붕괴 위험, 화재, 유해화학물질 유출, 해양 환경 등)에 대응할 수 있도록 현장 대응능력을 향상시킨 방수, 내열, 내풍, 내염 등의 극한 환경에서도 운용 가능한 드론을 선보이고 있다.

(5) 노후 인프라 안전점검 서비스

출처 http://www.asoa.co.kr/

시설물 점검 및 측량/관측 드론

시설물 점검 및 측량/관측용 장비를 장착한 드론이 자동경로 비행을 통하여 시설물 영상을 수집한다. 충돌 방지를 위한 라이다 센서 등을 탑재하여 임무에 특화되었다.

2.2. 지상제어장치

지상제어장치(GCS : Ground Control Station)는 드론에게 명령을 전달하고 원격 제어하는 장치로 C2 링크를 통해 드론에게 실질적인 임무 및 명령어를 전달하는 조종장치(조종기), 지상통제소 등이 포함된다.

2.2.1. 구성

가. 조종장치

조종장치는 수동으로 드론 조종을 가능하게 하는 휴대 제어장치로 다양한 방식으로 드론을 조종하는 장치이다.

조종기 | 스마트폰을 탑재한 조종기

- **구　　성** : 송신기, 수신기, 서보(Servo) 등으로 구성된다.

분류	기능
송신기	전파를 발사하여 동작에 대한 명령을 내리는 기능을 수행
수신기	송신기에서 발생한 전파를 수신하는 기능을 수행
서보	수신기의 명령에 따라 전파의 신호를 기계적인 움직임으로 바꾸는 기능을 수행

- **발전동향** : 기존의 전파를 발사하여 동작의 명령을 송수신하는 조종장치 뿐만 아니라 스마트폰의 보급과 발전으로 스마트폰, 스마트태블릿 등의 스마트 기기와 연결하여 앱을 통해 드론을 제어할 수 있다.

나. 지상통제소

지상통제소는 드론의 형태, 비행고도, 비행반경 등 임무의 형태에 따라 다양한 방식으로 드론을 지상에서 조종하는 장치, 시스템 등이다.

휴대형 지상통제장치

차량 지상통제시스템

2인 지상통제센터

- **구 성** : 휴대형 지상통제장치, 차량 지상통제시스템 등으로 구성된다.

- **발전동향** : 다수의 드론을 임무에 투입할 경우, 효율적인 임무수행 및 관리를 위해 다중 드론의 운영관리시스템(OMS : Operation Management System)이 운영되기도 한다. 운영관리시스템은 드론의 조종기와 드론 간의 통신이 항상 운영관리시스템을 통해 이뤄지게 함으로써 드론을 중앙 집중적으로 통제 및 관리할 수 있다.

2.2.2. 서비스 적용 사례

지상제어장치가 본 가이드의 제2장 제1절에서 설명한 서비스에 적용되는 사례는 다음과 같다.

(1) 물품 배송 서비스

드론 물품 배송의 운영제어시스템은 물품 배송을 위한 임무계획 수립, 택배 드론에 대한 조종 명령 및 통제, 영상 및 데이터의 수신 및 분석, 가시권·비가시권·야간 비행 제어 등 핵심적인 역할을 수행한다. 주요 기능은 택배드론 자원 관리, 실시간 지도 데이터 처리, 영상 및 텔레메트리 정보 분석 기능을 제공하고 자동비행, 고장 예측, 트래픽 관리 등과 연계하여 조종 명령 지시하고 드론의 상태정보에 따라 적절한 조종 명령을 수행한다.

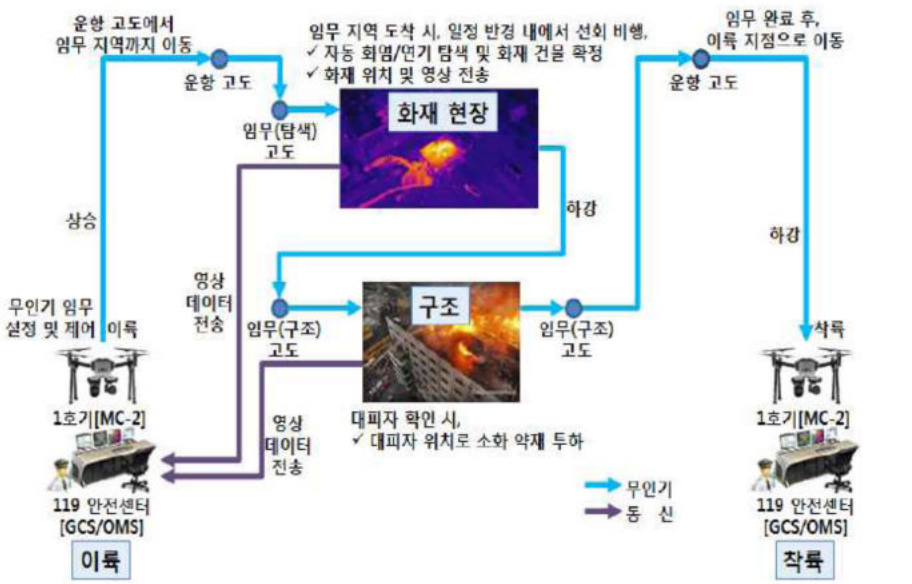
(2) 도시 안심 서비스

스마트기기 앱을 통하여 위험 상황에 처한 이용자가 신고하면 스마트도시 안심 모니터링 시스템은 앱을 통하여 신고자의 위치 정보를 파악한 후 드론을 출동시킨다. 안전한 상황이 확인되면 드론을 복귀시키도록 하며, 평시에는 위험지역을 정하여 주야간 일정하게 순찰하면서 모니터링한다.

(3) 도시 환경 관리 서비스

드론으로부터 측정된 대기오염 측정 정보를 수집하고 분석한 후 각 도심의 위치별 측정정보를 시민들이 실시간으로 확인할 수 있게 대형 전광판으로 전송한다.

(4) 재난 상황 감시 서비스



출처 재난치안용 드론 떴다, 산업통산자원부 보도자료, 2019.10.31.

아파트 화재 현장 출동

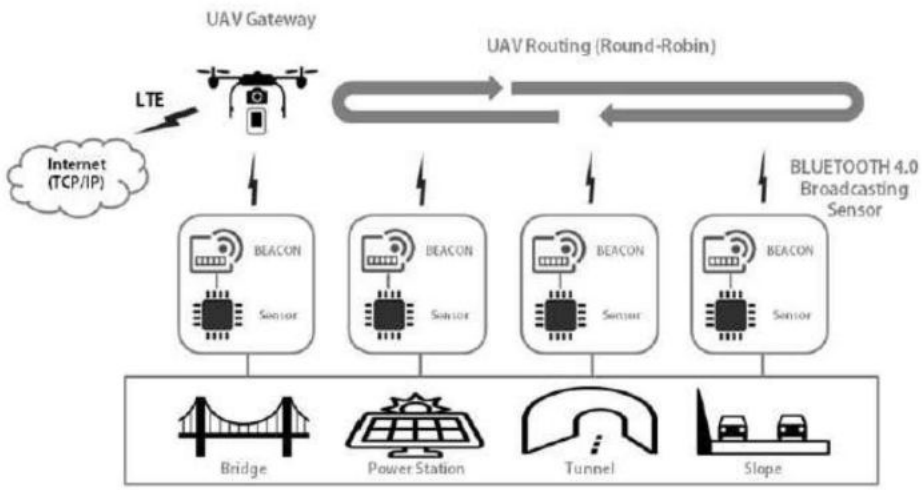
드론은 화재 현장 상황 영상 데이터를 수집하고 이를 운영관리시스템(119 안전센터)과 지상제어장치(지원 차량)로 송신한다. 또한 드론은 소화 약재 사출(투하)이 필요한 경우 운영관리시스템(119 안전센터) 또는 지상제어장치(지원 차량)의 명령에 따라 화재 발생 건물로 접근하여 드론에 탑재했던 소화 약재를 사출한다.

(5) 노후 인프라 안전점검 서비스

드론으로부터 수집된 영상 데이터와 측정 데이터를 기반으로 노후 인프라에 대한 전반적인 상태를 점검한다.

2.3. 정보제공장치

드론 서비스와 관련된 정보를 제공하는 장치를 말하며, 임무의 특성에 따라 다양한 센서, 감지기 등 센서를 통해 수집한 정보를 드론에 전달하여 임무를 완료할 수 있도록 하는 장치이다.



출처 SOC 시설물의 스마트 통합 유지 관리를 위한 드론 기반 3D 엔진 및 무선 제어 계측 플랫폼 기반 기술 개발 최종보고서, 국토교통부, 2019.01.

정보제공장치를 통한 데이터 수집

사람이 직접 접근할 수 없는 시설물 관리나 재난 상황 발생 확인, 해양 환경 측정, 방사능 측정 등과 같은 환경에서 정보제공장치 내 센서를 이용하여 데이터를 수집하고 드론에게 송신한다.

2.3.1. 구성

광학, 음파, 방향 탐지, 압력, 무게, 영상(가시광선/적외선 등), 레이다(Radar), 방사능(가이거) 등과 같은 센서와 탐지된 정보를 드론에 전달하는 통신링크 부분으로 구성될 수 있다.

- **구　　성** : 센서와 통신링크 등으로 구성된다.

분류	기능
센서	광학, 음파, 방향 탐지, 압력, 무게, 영상(가시광선/적외선 등), 레이다(Radar), 방사능(가이거 센서) 등의 센서
통신링크	센서를 통해 탐지된 정보를 드론에 전달하는 기능

- **발전동향** : 드론에 활용분야의 센서를 직접 탑재하여 활용하는 서비스가 대부분이며, 센서 기반의 실시간 모니터링 기능을 수행하는 정보제공장치는 원격에서 시설물 등을 점검할 수 있는 실험적인 연구가 계속 진행되고 있다.

2.3.2. 서비스 적용 사례

정보제공장치가 본 가이드의 제2장 제1절에서 설명한 서비스에 적용되는 사례는 다음과 같다.

(1) 물품 배송 서비스

디지털 택배함처럼 물품이 배달되는 지점에 위치하여 드론에 의해 배달된 물품의 배송 완료 여부를 확인한다. 서비스 제공자가 관리하여 고객에게 물품 수령을 알려준다.

(2) 도시 안심 서비스

감시 영역 내에 있는 센서들이 정보제공장치의 역할을 수행한다. 센싱한 정보는 드론이 감시 영역 내에 들어왔을 때 드론에게 전달하고, 감시 서비스 관련 사항을 확인시켜 주는 기능을 수행한다.

2.4. 서비스 제공자 및 서비스 요청자

드론 기반의 서비스를 제공하는 기관은 서비스 제공자 또는 사업자로 구분할 수 있으며, 드론 서비스를 요청하는 서비스 요청자 또는 사용자로 구분할 수 있다. 사용자는 드론 서비스를 이용하기 위해 서비스(임무)를 요청하고 서비스 제공자의 애플리케이션, 웹사이트, 개발 프로그램 등을 통해 제공된다.

2.4.1. 구성

- **구 성** : 서비스 제공자(드론 서비스를 제공하는 기관, 사업자 등), 서비스 요청자(드론 서비스를 요청하는 요청자, 사용자 등)로 구분되며 애플리케이션 등을 통해 서비스를 제공한다.

분류	기능
애플리케이션	웹 애플리케이션 또는 스마트기기 애플리케이션으로 요청자(고객)가 서비스를 이용하기 위해 접속하는 프로그램

- **발전동향** : 현재까지 일반 고객(요청자)을 대상으로 드론 기반 서비스를 제공한 사례는 없다고 할 수 있다. 아마존, 구글, DHL, 월마트 등의 민간 기업이 배송·물류 분야에서 드론을 활용하기 위해 지속적으로 추진하고 있으나 아직은 상용화 단계에 도달하지는 못한 실정이며, 이는 규제에 따른 제한 때문으로 파악된다. 현재 정부는 물품수송, 산림보호 감시, 해안선 관리, 국토 조사 순찰, 시설물 안전 진단, 통신망 활용, 촬영·레저, 농업지원 8대 분야를 2020년까지 상용화하는 것을 목표로 하고 있다.

2.4.2. 서비스 적용 사례

서비스 제공자 및 서비스 요청자가 본 가이드의 제2장 제1절에서 설명한 서비스에 적용되는 사례는 다음과 같다.

(1) 물품 배송 서비스

서비스 요청자는 물품 배송을 위해 PC 또는 스마트폰을 통하여 물품에 대한 드론 배송을 신청하고 물품 비용 및 배송 비용을 결제한다. 서비스 제공자는 고객(서비스 요청자)의 물품 배송 정보를 확인하고 해당 물품 정보를 배달부서 또는 배달 전문기관의 지상제어장치에게 전달하여 드론을 배정하고 드론 비행 일정 확정한다. 확정된 비행 정보를 서비스 제공자에 전달하여 드론 비행 정보에 따라 배송을 진행하고 서비스 요청자가 지정한 장소에 물품을 배송 완료한다.

(2) 도시 안심 서비스

서비스 제공자인 스마트폰 애플리케이션을 통하여 도시 안심 서비스를 신청한 사용자는 스마트폰 앱을 이용하여 '순찰 드론'을 신청하고, 최종 목적지를 입력한다. 사용자는 위험 지역을 벗어나 목적지에 도착할 때까지 드론의 에스코트를 받을 수 있다.

(3) 재난 상황 감시 서비스

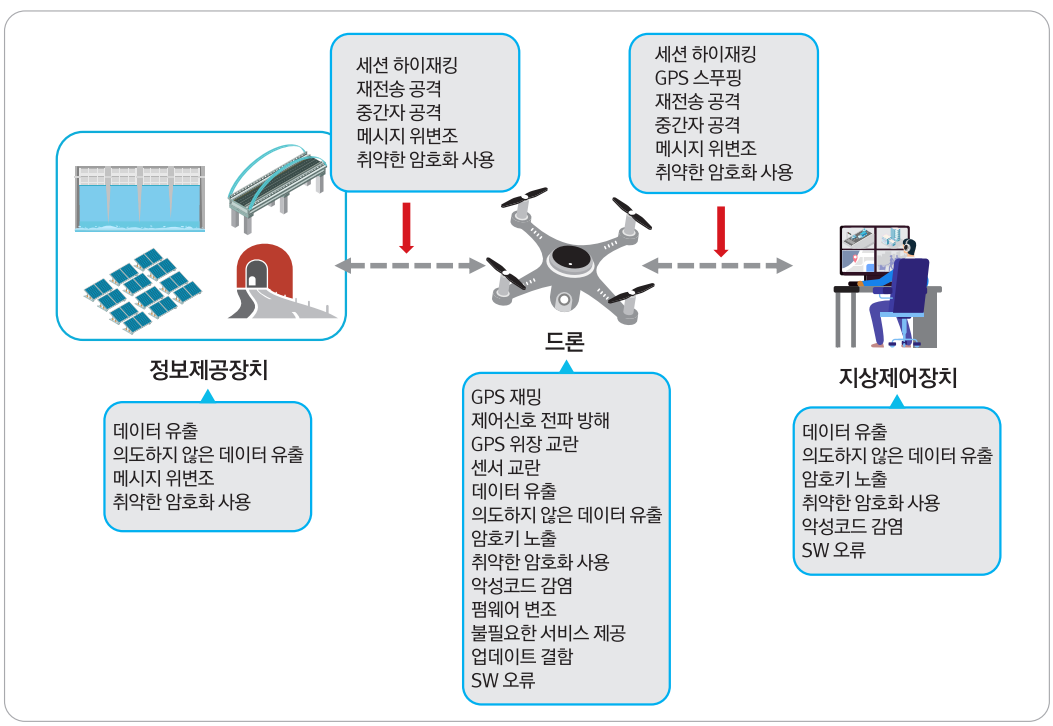
2015년 8월 태풍 고니에의한 방파제, 제방 등의 손상 피해를 태풍 전후로 촬영하여 비교하였다. 대상 지역의 3차원 공간정보를 이용하여 토양 유실 및 해안 고도 변화를 정량적으로 파악하여 요청자에게 피해복구를 위한 토공량 산정에 활용할 수 있는 정보를 제공하였다.

제2절 드론 서비스 보안위협

드론은 지상제어장치와의 네트워크를 통해 사용자가 원하는 서비스 환경에 적용되어 배송, 안전 등의 다양한 서비스를 제공하고 있다. 드론은 네트워크로 연결됨에 따라 드론, 지상제어장치 뿐만 아니라 정보제공장치에 보안위협이 노출될 경우 드론 탈취, 서비스 장애 등의 위협이 발생할 수 있다. 이에 따라 드론 서비스에서 발생 가능한 보안위협을 파악하고 이에 대한 공격 방식을 파악하는 것이 중요하다.

본 가이드에서 분석한 드론 서비스 구성요소와 구성요소 간의 발생 가능한 주요 보안위협은 아래와 같다.

단, 서비스 제공자 및 서비스 요청자의 보안위협은 일반 ICT의 보안위협과 동일하므로 본 가이드에서 포함되지 않는다.



드론 시스템 주요 보안위협

드론 서비스 분석 내용을 기반으로 보안위협에 영향을 미치는 드론 서비스 피해 자산을 아래와 같이 드론, 지상제어장치, 정보제공장치로 구분하였다.

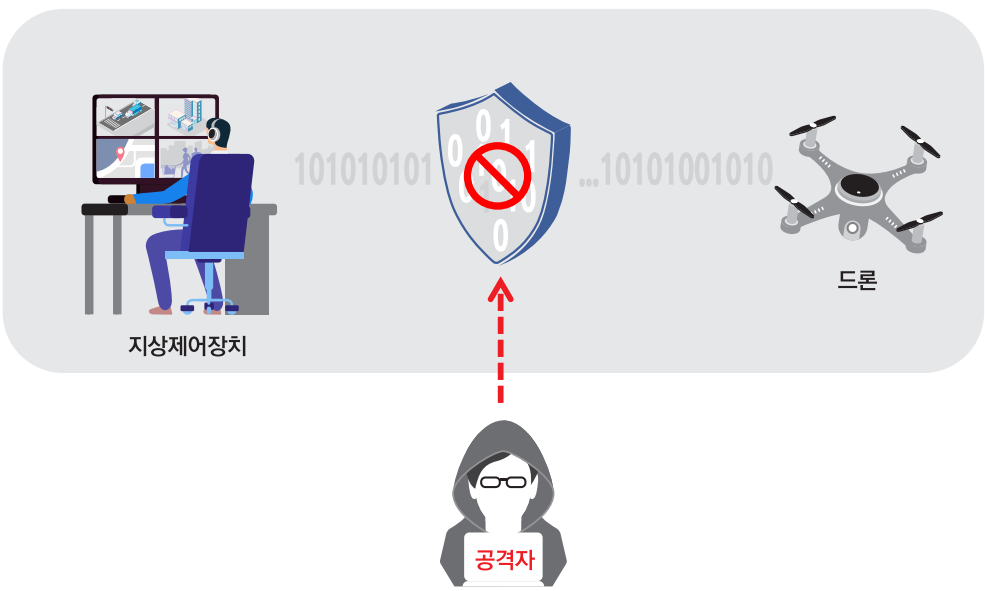
구분	보안위협	피해 자산		
		드론	지상 제어 장치	정보 제공 장치
중간자 공격	세션 하이재킹	○	○	○
	재전송 공격	○	○	○
	중간자 공격	○	○	○
가용성 방해	GPS 재밍	○		
	제어신호 전파 방해	○		
	GPS 위장 교란	○		
	센서 교란	○		
데이터 손실	데이터 유출	○	○	○
	의도하지 않은 데이터 유출	○	○	○
	메시지 위·변조	○	○	○
부적절한 암호사용	암호키 노출	○	○	○
	취약한 암호화 사용	○	○	○
악의적인 프로그램 실행	악성코드 감염	○	○	
	펌웨어 변조	○	○	
잘못된 설계 및 구현	불필요한 서비스 제공	○		
	업데이트 결함	○		
	SW 오류	○	○	

제3절 위협 시나리오

2절에서 분석한 주요 보안위협과 드론 서비스의 실제 위협 사례를 바탕으로 위협 시나리오와 피해 자산을 도출하였다.

1. 중간자 공격

가. 위협 시나리오



① 공격자는 드론과 지상제어장치 간, 드론과 정보제공장치 간 통신세션에 접근
② 세션을 가로채어 제어권 탈취 및 데이터 위·변조

▶ 드론 제어권 획득, 데이터 유출 및 위·변조 등의 위협 발생

공격자가 드론-지상제어장치 간, 드론-정보제공장치 간의 통신세션에 접근하여 세션 가로채기를 통해 드론의 제어권 탈취와 데이터의 유출과 위·변조가 가능하다. 취약한 프로토콜이나 취약한 암호 알고리즘을 사용할 경우 위협에 노출될 수 있다.

나. 주요 보안위협

구분	보안위협	피해 자산		
		드론	지상 제어 장치	정보 제공 장치
중간자 공격	세션 하이재킹	○	○	○
	재전송 공격	○	○	○
	중간자 공격	○	○	○

(1) 세션 하이재킹

드론-지상제어장치 간, 드론-정보제공장치 간 세션관련 정보를 가로채어 네트워크 상으로 전송되는 데이터를 불법적으로 노출, 변조하는 방법이다. 네트워크 트래픽을 통한 내부 정보 유출이 가능하고, 공격자는 인가되지 않은 트래픽을 유입시켜 내부망 침해가 가능하다.

(2) 재전송 공격

조종신호를 별도의 RF 채널(전용 프로토콜)로 활용하는 경우, 제어용 무선신호를 저장 및 재전송하여 드론의 제어권 탈취할 수 있다.

(3) 중간자 공격

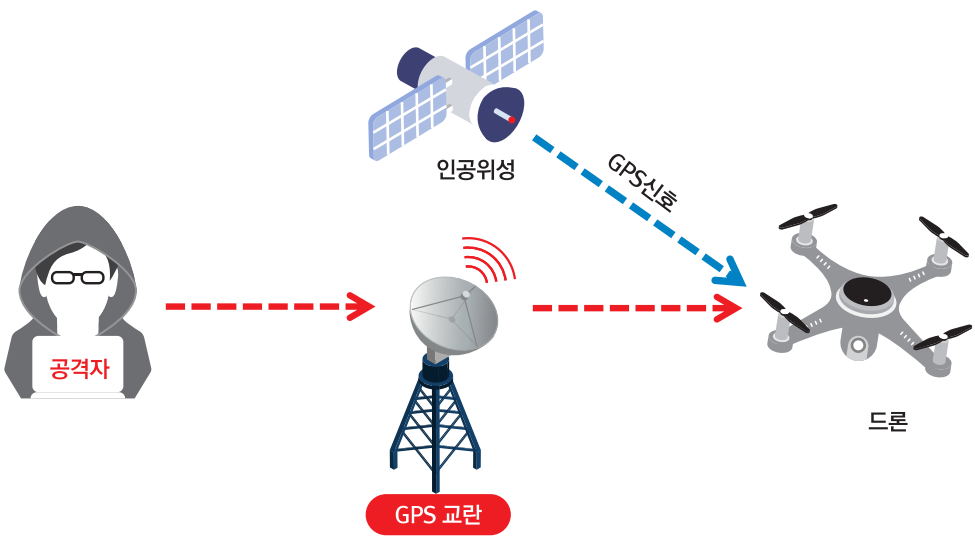
드론-지상제어장치 간, 드론-정보제공장치 간 인증기능이 없을 시 드론 또는 지상제어장치로 위장하여 서로에게 변조된 정보를 보내, 공격자가 원하는 대로 제어할 수 있다.

다. 사례

- 이라크 반군은 미국 드론이 촬영한 이라크의 상공 영상을 실시간으로 가로채기함, 2008.12.
- 이란은 GPS, 신호와 제어신호의 위·변조 공격으로 미국의 드론을 탈취하였으며, 이로 인해 무인기에 저장된 군사정보가 유출됨, 2011.12.
- 이슬람 지하드 해커 Oydeh는 이스라엘 기지 상공의 무인기를 해킹하여 비디오 스트림을 도청함, 2012~2016

2. 가용성 방해

가. 위협 시나리오

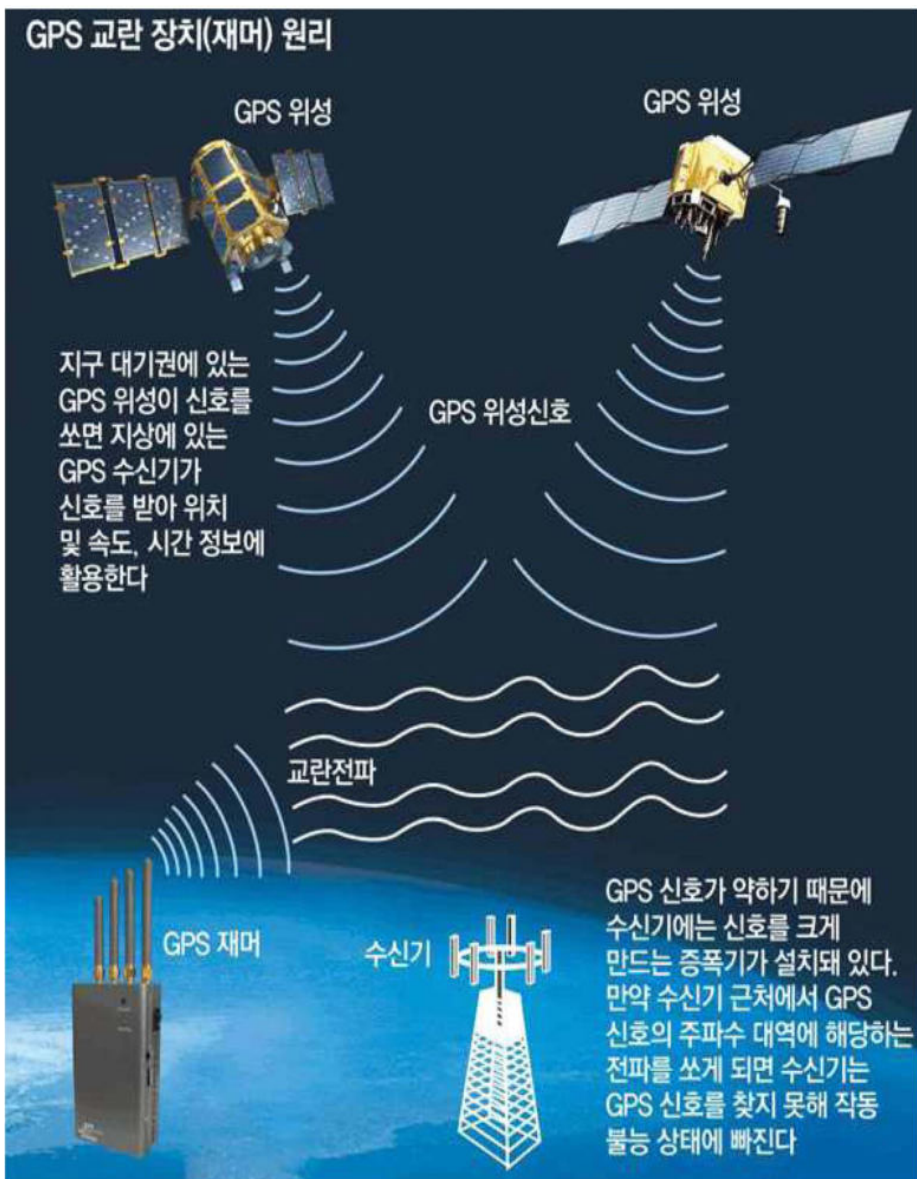


① 공격자는 GPS Jammer를 이용하여 조작된 GPS 신호를 송신
② GPS 수신기 및 센서를 장착한 드론은 정상 GPS 신호를 받지 못하고 조작된 GPS 신호를 계속 수신
③ 조작된 GPS 신호를 정상 GPS 신호로 수신하여 정상 비행 경로 이탈

▶ 드론 탈취, 무력화, 서비스 장애 등의 위협 발생

공격자가 GPS Jammer를 이용하여 드론에게 조작된 GPS 신호를 송신할 경우 드론이 정상 비행 경로를 이탈하거나 서비스 장애 등의 위협이 발생할 수 있다.

위성통신을 이용하는 드론은 GPS에서 보내주는 신호를 분석하여 드론의 현재 위치를 파악하고 앞으로 비행해야 할 거리를 알 수 있게 해준다. 그러나 GPS 신호는 20,000km 상공에 있는 위성으로부터 발사되기 때문에 지상에 도달할 때면 신호가 매우 약하다. 이러한 이유로 GPS 교란신호에 의해 교란이 발생하기 쉽다.



출처 https://www.donga.com/news/It/article/all/20110601/37686475/1

GPS 재밍 원리

GPS 재밍 공격을 받은 드론은 제어 통신 뿐 아니라 GPS 신호도 받을 수 없는 상태가 된다. 이때 출발 위치로 돌아가거나(리턴투홈) 그 자리에서 추락하게 된다.

출처 https://www.anadronestarting.com/%ED%95%B4%ED%82%B9/

나. 주요 보안위협

구분	보안위협	피해 자산		
		드론	지상 제어 장치	정보 제공 장치
가용성 방해	GPS 재밍	○		
	제어신호 전파 방해	○		
	GPS 위장 교란	○		
	센서 교란	○		

(1) GPS 재밍

강한 GPS 신호를 발생시켜 정상 GPS 신호 감지를 불능 상태로 만드는 공격 방법이다.

(2) 제어신호 전파 방해

(2-1) 특정 주파수 대역의 제어신호를 무작위하게 보내어 드론의 정상비행을 방해하고 비행 및 조종을 무력화 할 수 있다.

(2-2) 정상적인 방법으로 서비스를 제공할 수 없도록 무가치한 신호를 전송한다.

(3) GPS 위장 교란

조작된 GPS 신호를 전송하여, 신호를 받은 드론이 정상 비행 경로를 이탈하여 드론을 탈취하거나 추락시키는 공격이다.

(4) 센서 교란

(4-1) 드론의 자이로센서*를 활용하는 드론이 주파수 소음이 발생하는 지역에 들어갈 경우 드론 비행 오류 및 제어력 등의 오류가 발생한다. 따라서 주파수 재밍 공격으로 드론의 정상비행을 방해하고 비행 및 조종을 무력화 할 수 있다.

*물체 회전 각도를 감지하여 드론을 제어하는 센서

ex) 자이로센서 재밍

드론의 방향을 측정하고 유지 제어를 위해 자이로센서를 탑재하고 있는데, 센서 주변에 공진주파수(Resonant Frequency)를 보내어 정상적인 주행을 막는 공격방법이다. 실제로 ST마이크로의 MEMS 자이로스코프를 탑재한 드론에 8200Hz의 공진주파수 전파를 받아 드론이 추락하기도 하였다.

출처 http://www.boan24.com/news/articleView.html?idxno=2505

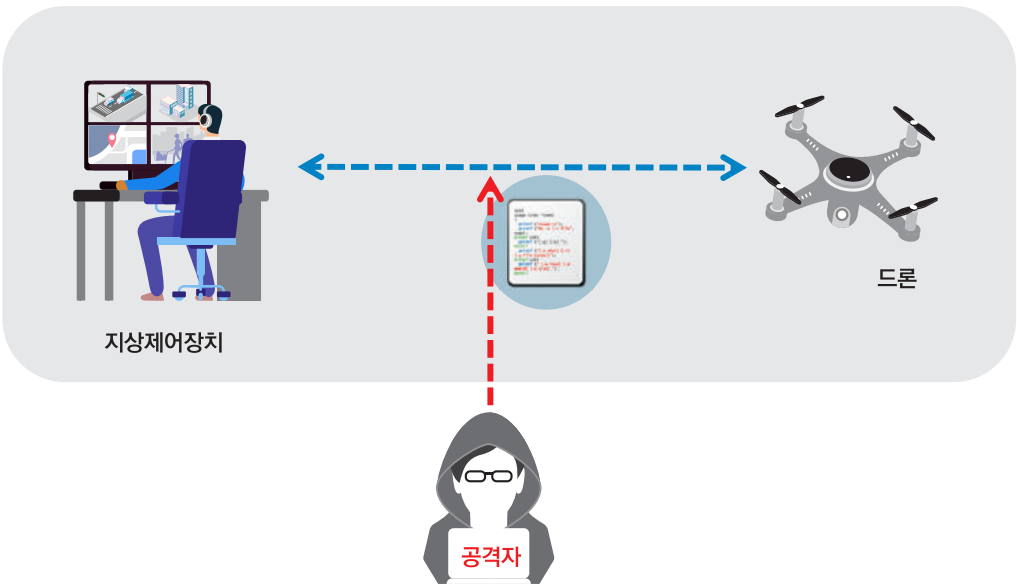
(4-2) 드론에 탑재된 적외선 센서에 레이저 포인터를 조사하여 센서 교란을 일으킬 경우, 드론의 제어권이 무력화되어 드론이 추락할 수 있다.

다. 사례

- 멕시코의 마약 조직이 마약 밀매와 밀입국 목적으로 미국-멕시코 국경 수비대 드론을 GPS 재밍, 스푸핑 공격을 통해 무력화 시킴, 2016.1.

3. 데이터 손실

가. 위협 시나리오



① 공격자는 드론-지상제어장치 간, 드론-정보제공장치 간의 통신 세션에 접근
② 세션을 가로채어 송·수신 메시지를 분석하고 위·변조
③ 위·변조된 메시지를 지상제어장치, 정보제공장치에 전송

▶ 데이터 유출, 허위 정보 제공, 서비스 장애 등의 위협 발생

공격자가 드론-지상제어장치 간, 드론-정보제공장치 간의 통신 세션을 가로채어 송·수신 메시지를 분석할 경우, 데이터의 위·변조가 가능하다. 데이터가 위·변조될 경우 개인정보를 포함한 중요정보 데이터 유출, 허위 정보 제공뿐만 아니라 드론 서비스 장애 등의 위협이 가능하다.

나. 주요 보안위협

구분	보안위협	피해 자산		
		드론	지상 제어 장치	정보 제공 장치
데이터 손실	데이터 유출	○	○	○
	의도하지 않은 데이터 유출	○	○	○
	메시지 위·변조	○	○	○

(1) 데이터 유출

드론이 탈취될 경우, 드론이 수집한 데이터(사진, 영상, 위치, 센싱 데이터 등)와 인증정보 및 민감정보 등의 중요정보가 유출될 수 있다.

(2) 의도하지 않은 데이터 유출

의도하지 않은 드론 분실, 정보제공장치 등에 의도하지 않은 데이터 공유로 인해 데이터가 유출될 수 있다.

(3) 메시지 위·변조

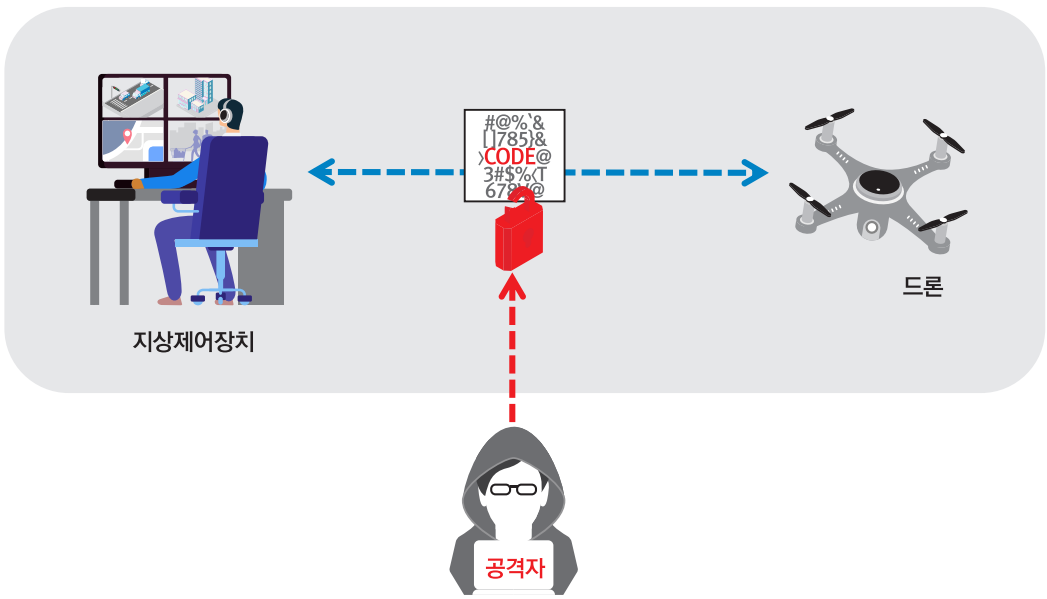
드론-지상제어장치 간, 드론-정보제공장치 간 세션에 접근하여 송·수신 메시지를 위·변조하여 오작동 유발, 메시지 송·수신 부인 및 서비스 장애 등을 발생시킬 수 있다.

다. 사례

- Blackhat Asia에서 비행 중인 드론을 무선 인터넷망으로 둔갑하여 주변 스마트폰을 연결을 허용하고 스마트폰의 통신 내용을 확인하여 약 150여개의 정보를 탈취, 2014.3.

4. 부적절한 암호 사용

가. 위협 시나리오



① 공격자는 드론-지상제어장치 간, 드론-정보제공장치 간의 통신 세션에 접근
② 암호를 해제하고 중요한 정보를 추출

▶ 데이터 유출, 서비스 장애 등의 위협 발생

드론-지상제어장치 간 통신 시 암호화된 채널을 이용하더라도 취약한 암호 프로토콜을 사용한다든지 안전하지 않은 암호 알고리즘을 사용하는 경우, 암호키가 노출되거나 암호화 채널을 복호화하여 평문 전송데이터를 확인할 수 있는 취약점이 존재한다.

나. 주요 보안위협

구분	보안위협	피해 자산		
		드론	지상 제어 장치	정보 제공 장치
부적절한 암호사용	암호키 노출	○	○	○
	취약한 암호화 사용	○	○	○

(1) 암호키 노출

드론에서 암호화키 노출로 인해 키 관련 정보가 유출될 수 있으며 암호키의 부적절한 관리로 중요정보가 노출될 수 있다.

(2) 취약한 암호화 사용

취약한 무선 통신 암호를 사용할 경우, 드론-지상제어장치 간과 드론-정보제공장치 간의 사용되는 암호키, 전송 이미지, 제어신호, 영상정보 등이 노출될 수 있다.

또한 취약한 암호 알고리즘을 사용하여 데이터를 암호화할 경우, 암호문을 수집·분석하여 암호키를 유추할 수 있다.

민간 드론에서 널리 사용되는 MAVLink(Micro Air Vehicle Link)는 경량화에 중점을 두어 개발된 프로토콜로 보안 메커니즘이나 암호화 알고리즘을 채택하지 않고 개발되었다. 이에 MAVLink 프로토콜을 사용하는 경우, 스푸핑, 메시지 위조 및 서비스 거부 등 여러 공격에 취약하고, 비밀성 및 무결성이 지원되지 않는 문제가 있다.

출처 드론 보안에 적용된 암호 기술 현황, 정보보호학회지, 2020.4

* MAVLink의 보안문제를 해결하기 위해, 2013년도에 Station-to-Station 키교환 프로토콜과 AES-GCM 대칭키 암호알고리즘을 적용한 sMAVLink(Secure MAVLink)가 제안되었으나, 패킷구조 변경 및 이식성 문제 등으로 상업 드론에 적용이 미미한 상태임

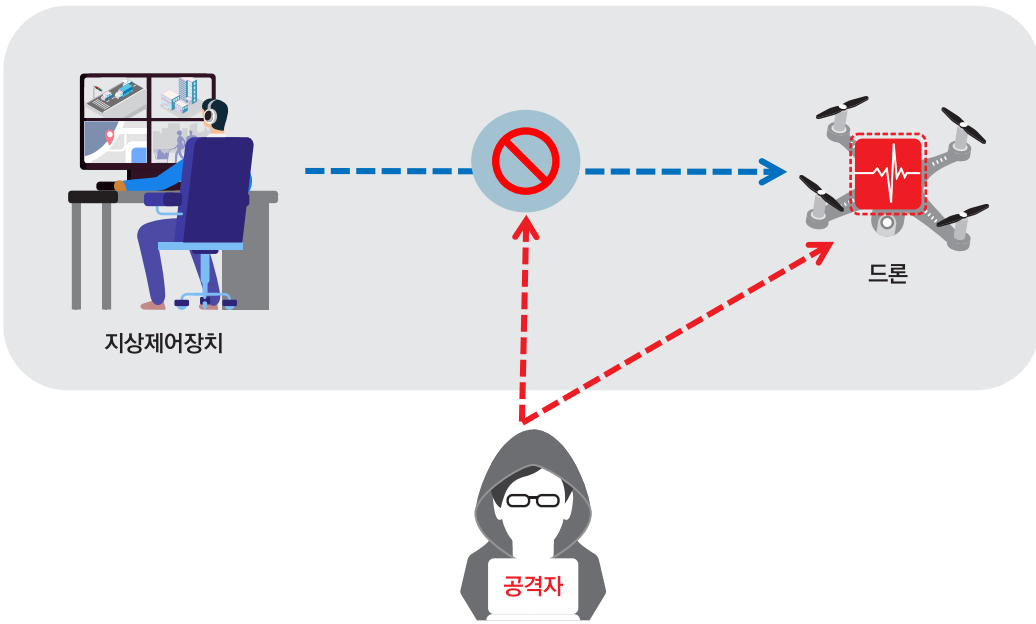
다. 사례

- RSA2016 컨퍼런스에서 닐스 로데이 보안연구원은 드론-지상제어장치(태블릿)-텔레메트리 박스 간의 취약한 통신 방식을 발견하여 주파수 조작, 세션 가로채기 등의 해킹 시연을 발표, 2016.3.

- 2016PacSec 컨퍼런스에서 트렌드마이크로리서치 그룹의 요나탄 안데르손 매니저는 드론 해킹 시스템 이카루스를 이용하여, DSMx(Digital Spectrum Modulation) 프로토콜(2.4GHz 사용)을 사용하는 드론의 제어권 탈취 시연을 발표, 2016.10.

5. 악의적인 프로그램 실행

가. 위협 시나리오



① 공격자는 드론의 펌웨어 구조와 프로토콜을 분석하여 펌웨어 변조 및 악성코드를 삽입
② 펌웨어 변조를 통한 조작된 명령어 전송 및 제어권 탈취

▶ 드론 탈취, 제어권 탈취, 중요정보 유출, 서비스 장애 등의 위협 발생

악성코드 감염에 의해 드론의 비행정보 조작으로 목적지 변경, 공격자에게 수집정보 전달 등 사이버/물리 공격 가능하다. 드론의 펌웨어 구조와 프로토콜을 분석하여 펌웨어 변조 및 악성코드를 삽입할 경우 조작된 명령어 전송이 가능하고 제어권 탈취가 가능하여 드론을 탈취할 수 있다. 특히, GPS 수신기에 GPS 악성코드를 내장하여 수신된 위성 신호로부터 계산된 위치와 다른 위치를 생성하는 GPS 스푸핑 악성코드를 이용하는 방법도 있다.

드론의 API를 이용하거나 드론에 근접 접근하여 악성코드를 주입하는 방법으로 수행하며 드론에 공격자가 제작한 펌웨어를 주입 시, 공격자의 의도대로 실행되어, 드론 서비스에서의 드론 및 정보제공장치가 역할 수행이 불가하다.

나. 주요 보안위협

구분	보안위협	피해 자산		
		드론	지상 제어 장치	정보 제공 장치
악의적인 프로그램 실행	악성코드 감염	○	○	
	펌웨어 변조	○	○	

(1) 악성코드 감염

악의적인 용도로 개발된 악성코드가 드론 및 지상제어장치 시스템에 실행되는 경우, 중요 정보(키, 비밀번호 등)이 노출되거나 악의적인 명령을 내려 드론을 악용할 수 있다.

(2) 펌웨어 변조

공격자는 드론의 펌웨어 구조와 프로토콜을 분석하여 펌웨어를 변조할 경우, 악성코드를 실행시켜 중요 정보를 노출 시키거나 명령을 내릴 수 있다. 또한 백도어를 설치하여 공격자는 시스템의 권한을 탈취할 수 있다.

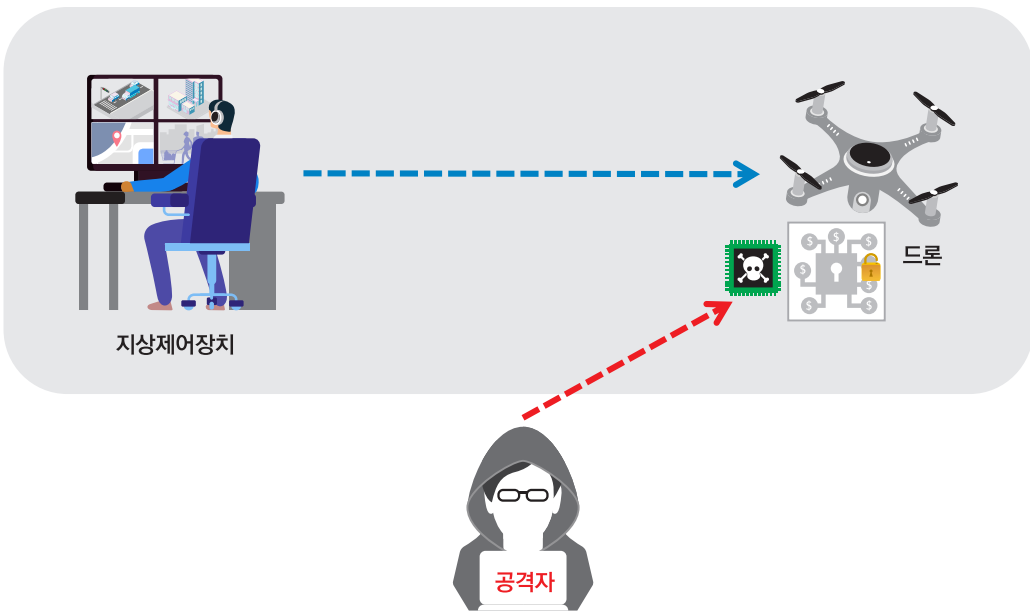
다. 사례

- 인도의 보안전문가 라홀 사시는 드론용 백도어 악성코드 몰드드론(Maldrone)을 통해 드론 무력화 및 제어권 탈취가 가능하다고 밝힘, 2015.02.

- 미국의 군용 드론 프레데터와 리퍼 조종실이 악성코드에 감염되어 조종사가 입력한 정보가 유출되었으며 조종의 오작동을 유발시킴, 2017.10.

6. 잘못된 설계 및 구현

가. 위협 시나리오



① 공격자는 드론, 지상제어장치, 정보제공장치에 물리적으로 접근
② 드론, 지상제어장치, 정보제공장치에 악성 메시지 전송 및 펌웨어 변조

▶ 드론 탈취, 제어권 탈취, 중요정보 유출, 서비스 장애 등의 위협 발생

드론의 HW 및 SW 기술은 80% 이상 거의 알려진 오픈소스(Open Source)에 의하여 구현될 수 있으므로 약간의 기술만 가지면 드론의 제작도 매우 용이하다. 드론의 원격 무선 조종 주파수 또한 일정한 대역에 있으므로 타 드론에 대한 해킹도 매우 용이하다.

보안을 고려하지 않은 드론의 설계 및 구현으로 안전하지 않은 부트로더, 펌웨어 등에 대한 공격이 일어날 수 있고, 인가되지 않은 펌웨어 업데이트 시 드론 플랫폼을 완전히 제어하고 임무를 방해할 수 있다. 그리고 SW 오류를 일으켜 악성코드에 감염되어 데이터가 유출될 수 있다.

나. 주요 보안위협

구분	보안위협	피해 자산		
		드론	지상 제어 장치	정보 제공 장치
잘못된 설계 및 구현	불필요한 서비스 제공	○		
	업데이트 결함	○		
	SW 오류	○	○	

(1) 불필요한 서비스 제공

개발에 사용한 인터페이스(ex. 디버그 포트, JTAG 포트 등)의 불필요한 접근을 허용할 경우 물리적인 접근을 통해 펌웨어 변조, 데이터 유출 등의 위협이 발생할 수 있다.

(2) 업데이트 결함

드론의 펌웨어 업데이트 및 SW 업데이트 자체에 포함된 취약점으로 인한 기기 오작동 및 데이터 유출 등의 위협이 발생할 수 있다.

(3) SW 오류

최신 버전의 SW 업데이트 보안 패치가 되지 않거나 안전한 업데이트를 수행하지 않을 경우 악성 코드에 감염될 수 있다.

다. 사례

- D 社의 드론에서 FTP(File Transfer Protocol) 서비스를 사용자가 접근할 수 있도록 설계되어 드론 내의 이미지, 비디오 파일을 비롯한 중요 파일에 접근할 수 있는 취약점이 공개, 2017

- D 社 드론은 안전과 보안을 위해 제한지역 접근 통제와 속도 및 고도에 제한을 두었지만, 일부 해커들이 편의성을 위해 펌웨어를 조작하여 무력화시키는 탈옥툴을 개발, 2017.7.

- Defcon2015 컨퍼런스에서 보안업체 플랫닛주다는 드론의 실시간 운영체제인 비지박스(busyBox)를 임의로 조작하여 드론을 무력화시키는 과정을 시연, 2015.8.

PART 03

드론 서비스 보안 대응방안

제1절 위협 시나리오별 대응방안
제2절 보안항목 및 대응방안

PART 3

드론 서비스 보안 대응방안

제1절 위협 시나리오별 대응방안

위협 시나리오	주요 보안항목
중간자 공격	• 인증 • 안전한 통신 • 암호 • 중요 데이터 보호
가용성 방해	• HW 및 SW의 안전성 • 인증 • 안전한 통신 • 안전한 비행
데이터 손실	• HW 및 SW의 안전성 • 인증 • 중요 데이터 보호 • 보안 감사
부적절한 암호사용	• HW 및 SW의 안전성 • 안전한 통신 • 암호 • 중요 데이터 보호
악의적인 프로그램 실행	• HW 및 SW의 안전성 • 인증 • 암호 • 중요 데이터 보호
잘못된 설계 및 구현	• HW 및 SW의 안전성 • 안전한 통신 • 안전한 비행 • 중요 데이터 보호 • 보안감사

제2절 보안항목 및 대응방안

보안항목	대응방안
HW 및 SW의 안전성	안전한 업데이트
	변조 대응
	악성코드 대응
	안전한 3rd Party 라이브러리
	시큐어코딩
인증	드론 식별
	사용자 인증
	상호 인증
안전한 통신	무선신호 보호 기능
	통신 채널 확보/재밍 대응
	전송 데이터 보호
	메시지 감지
안전한 비행	자율비행
	위치추적 대체수단 제공
	특정지역 접근 방지
	자동충돌 회피
	자동 회귀
암호	안전한 암호키 관리
	안전한 암호 알고리즘 사용
	안전한 난수 생성
	안전한 암호모듈 사용
중요 데이터 보호	저장 데이터 보호
	운영 데이터 보호
	접근통제
	개인정보 보호
보안감사	감사기록
	모니터링

1. HW 및 SW 안전성

가. 개요

드론의 안전한 비행과 임무를 위한 비행제어는 고신뢰성과 안전성을 보장할 수 있는 HW 및 SW로 구성되어야 하며, System-on-Chip으로 소형화 및 고성능화 추세에 있다. HW 및 SW의 통합에 따라, 모듈 부품 뿐 아니라 공통부품, 운영체계 및 SW 아키텍처까지 드론 시스템의 통합에 따른 설계 기술 및 시험, 분석 기술이 필요하다. 이렇게 통합된 기기의 경우, 기기 출시이후 기능 변경, HW 오류나 SW 오류 및 취약점을 개선하기 위해서는 기기 개발 이후에 더 많은 비용과 노력이 든다.

이에 따라, 개발 당시부터 드론 위협에 대응할 수 있는 기능이 포함된 보안이 고려된 드론 시스템 개발이 요구된다.

요약

HW 및 SW 안전성의 주요 대응방안은 아래와 같다.

- 안전한 업데이트
- 변조 대응
- 악성코드 대응
- 안전한 3rd party 라이브러리
- 시큐어코딩

나. 보안대책

드론 시스템 및 서비스에 따라 다음 대응방안을 선별하여 적용할 수 있다.

① 안전한 업데이트

- 드론 및 지상제어장치의 펌웨어 또는 SW를 업데이트 하는 경우 인가된 사용자 또는 관리자에 의해 인증 후 업데이트를 안전하게 수행하여야 한다.

- 드론의 운영체제를 오픈소스 운영체제를 사용하는 경우에는 보안기능이 적용된 운영체제를 선택해야 한다.

  ※ 드론 해킹방지용 시큐어 임베디드 4(seL4) 마이크로 커널 등과 같은 운영체제를 사용할 수 있다.

② 변조 대응

- 드론 및 지상제어장치에서 구동되는 프로그램의 무결성을 보장해야 한다.
  - 펌웨어, 업데이트 소스 및 패치 관리 기능에 대한 해시값을 통해 무결성을 보장

- 업데이트를 진행할 경우 파일의 해시값에 전자서명을 적용하여 업데이트 파일 변조 및 무결성을 보장

〈보안강도에 따른 메시지인증/키유도/난수생성용 해시함수 분류〉

보안강도	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내
112 비트 이상	SHA-1[1)] SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512	SHA-256 SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512 SHA3-shake128 SHA3-shake256 Whirlpool-512 BLAKE-224 BLAKE-256 BLAKE-384 BLAKE-512	HAS-160[2)] SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512 LSH-224 LSH-256 LSH-384 LSH-512 LSH-512-224 LSH-512-256
128 비트 이상	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512	SHA-256 SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512 SHA3-shake128 SHA3-shake256 Whirlpool-512 BLAKE-224 BLAKE-256 BLAKE-384 BLAKE-512	HAS-160 SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512 LSH-224 LSH-256 LSH-384 LSH-512 LSH-512-224 LSH-512-256

보안강도	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내
192 비트 이상	SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512	SHA-256 SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512 SHA3-shake128 SHA3-shake256 Whirlpool-512 BLAKE-224 BLAKE-256 BLAKE-384 BLAKE-512	SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512 LSH-224 LSH-256 LSH-384 LSH-512 LSH-512-224 LSH-512-256
256 비트 이상	SHA-256 SHA-384 SHA-512 SHA-512/256 SHA3-256 SHA3-384 SHA3-512	SHA-256 SHA-384 SHA-512	SHA-256 SHA-384 SHA-512 SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHA3-shake128 SHA3-shake256 Whirlpool-512 BLAKE-256 BLAKE-384 BLAKE-512	SHA-256 SHA-384 SHA-512 SHA-512/256 SHA3-256 SHA3-384 SHA3-512 LSH-256 LSH-384 LSH-512 LSH-512-256

출처 암호 알고리즘 및 키 길이 이용 안내서, 과학기술정보통신부, 2018.12

※ 세부적인 사항은 과학기술정보통신부의 '암호 알고리즘 및 키 길이 이용 안내서' 등을 참고한다.

- 온보드 펌웨어 SW가 변조되지 않도록 보호해야 한다.

- 온보드 HW가 변조되지 않도록 보호해야 한다.
  - 드론 내부의 부품 간의 데이터 주입 공격을 방지하기 위한 경량 SW 도입이 필요

- 무선 모듈, GPS, 비행 컨트롤러와 같은 중요한 HW를 교체하는 메커니즘을 적용해야 한다.
  - 물리 보안 대응 기술(Hardware Tamper Proof) : 공격 발생 시 침투된 증거가 표시되거나(FIP 140-2 Level 2), 중요 HW 내부 정보에 대한 접근 시 공격을 탐지하고 중요정보를 파기함(FIPS 140-2 Level 3이상)

- 비행 매개변수를 변경하기 위한 인증 절차가 있어야 한다.

③ 악성코드 대응

- 악의적인 메시지 및 행위를 탐지 및 차단해야 한다.

- 불량 시스템 변경, 악성 애플리케이션 또는 업데이트, 3rd party의 손상된 플러그인에 대한 드론 관련 시스템의 동작 상황에 대하여 모니터링해야 한다.

④ 안전한 3rd party 라이브러리

- 드론 및 지상제어장치에 설치되는 3rd party 코드는 사전에 검토되어야 한다.

⑤ 시큐어코딩

- 드론 및 지상제어장치의 SW 개발 시 보안 취약점을 최소하기 위해 SW 개발 생명주기(SDLC)의 단계별 보안을 고려하여 안전하게 구현해야 한다.

〈소프트웨어 개발 단계별 보안 고려사항〉

요구사항 분석	설계	구현	테스트	유지보수
- 요구사항 중 보안항목 식별 - 요구사항 명세서	- 위협원 도출을 위한 위협모델링 - 보안설계 검토 및 보안설계서 작성 - 보안 통제 수립	- 표준 코딩 정의서 및 SW개발 보안가이드를 준수해 개발 - 소스코드 보안약점 진단 및 개선	- 모의침투 테스트 또는 동적 분석을 통한 보안취약점 진단 및 개선	- 지속적인 개선 - 보안 패치

출처 소프트웨어 개발보안 가이드, 한국인터넷진흥원, 2019

※ 세부적인 사항은 한국인터넷진흥원의 "소프트웨어 개발보안 가이드" 등을 참고한다.

다. 적용 범위

보안항목	대응방안	적용 자산		
		드론	지상 제어 장치	정보 제공 장치
HW 및 SW 안전성	안전한 업데이트	○	○	
	변조 대응	○	○	
	악성코드 대응	○	○	
	안전한 3rd Party 라이브러리	○	○	
	시큐어코딩	○	○	

2. 인증

가. 개요

드론은 안전한 비행이 첫 번째 목표이므로 악의적인 사용자나 관리자의 접근을 차단해야 하며, 허가된 사용자 및 관리자에 의해 안전하게 운영되어야 최소한의 안전한 비행을 보장할 수 있다.

요약

인증의 주요 대응방안은 아래와 같다.

· 드론 식별
· 사용자 인증
· 상호 인증

나. 보안대책

드론 시스템 및 서비스에 따라 다음 대응방안을 선별하여 적용할 수 있다.

① 드론 식별

- 드론 시스템은 유추 불가능한 고유하고 변경할 수 없는 고유 식별번호를 보유해야 한다.

※ 드론 및 지상제어장치 등의 드론 시스템은 식별할 수 있는 기능을 제공해야 한다.

② 사용자 인증

- 관리 서비스 및 개인정보와 같은 민감 정보에 접근할 경우 사용자 인증을 수행해야 한다.
  - ID/PW 기반의 사용자 및 관리자 인증 수행
  - 중요 데이터는 스마트폰을 통해 SMS, NFC 등과 같은 2차 인증을 수행

※ 인증이 실패할 경우 계정 비활성화 및 관리자 확인을 통한 잠금 해제 수행

- 잘못된 인증정보를 통한 반복된 인증 시도를 허용할 경우 무차별 대입 공격(Brute Force Attack)에 취약할 수 있으므로, 드론 시스템은 잘못된 인증정보를 통한 지속적인 인증 시도에 대해 이를 적절하게 대응하는 기능을 제공해야 한다.
  - 인증 시도 횟수를 제한하여 정해진 인증 시도 횟수 초과 시 계정 잠금 혹은 일정 시간 인증 기능을 비활성화 (인증 시도 횟수는 5회 이하, 인증 기능 비활성화 시간은 5분 이상으로 구현하도록 권고)
  - 정해진 인증 시도 횟수 초과 시 허가되지 않은 네트워크 트래픽으로 판단하여 자동 차단 목록에 추가(인증 시도 횟수는 5회 이하로 구현하도록 권고)

- 초기 인증정보를 사용하는 드론 시스템의 경우, 제품별로 서로 다른 초기 인증정보를 가지고 있어야 한다.
  - 초기 인증정보 : 사용자가 처음으로 드론 시스템에 접근을 시도할 때 입력하는 정보(ex, ID/PW 등)로, 초기 인증번호 입력 후 새로운 인증정보(ex, ID/PW 등) 입력을 요청

- 제조사는 불필요한 계정(ex, guest 등)을 생성하여 배포하지 않아야 한다.

- 관리서비스에 동일한 관리자 계정을 이용하여 동시 접속 시 이를 제한해야 하며, 이전 접속에 대한 연결을 끊거나 새로운 접속에 대해 제한하는 기능을 제공해야 한다.

- 드론 시스템은 사용자가 비밀번호 설정할 때 아래와 같이 길이, 주기, 복잡성을 고려하여 안전한 비밀번호로 설정되도록 기능을 제공해야 한다.

고려사항	세부
길이	기본 9자리 이상을 권고
주기	비밀번호의 변경 주기는 6개월 이내를 권고 * 비밀번호 변경 주기가 지났을 때 사용자에게 이를 알려 위험을 인지시키고 변경하도록 유도하는 편이 좋으나, 변경의 강제성은 개발자의 선택사항임
복잡성	영문자(대·소) / 숫자 / 특수문자 중 3가지 이상의 규칙을 혼합한 구성으로 비밀번호가 설정되도록 권고

- 비인가자의 접근 통제를 위한 물리적/논리적 접근 시 사용자 인증 기능이 필요하다. 경우에 따라서는 다중 인증 기능을 수행하여 드론 뿐 아니라 드론 시스템의 안전성을 확보하여야 한다.
  - PUF(Physical Unclonable Funtion) 기반 인증으로 칩, 보드 및 RFID 태그, 스마트 카드 및 원격 센서와 같은 시스템 구성 요소의 신원 및 진위를 확인하는 프로세스를 수행

③ 상호 인증

- 드론 시스템 구성요소 간, 중요 정보 전송 시 혹은 서비스 접근 시 상호 인증을 선행하도록 해야 하며 인증 방식의 예는 아래와 같다.
  - 고유한 식별번호는 보안속성값, UID, Key 등이 될 수 있고 이를 이용하여 인증하는 방식 사용
  - 공개키 암호 방식의 개인키를 이용한 상호인증 수행
  - 인증코드(Token, OTP)를 발급받아 인증하는 방식 사용
  - 보안칩 기반의 상호 인증 수행

다. 적용 범위

보안항목	대응방안	적용 자산		
		드론	지상 제어 장치	정보 제공 장치
인증	드론 식별	○	○	○
	사용자 인증	○	○	
	상호 인증	○	○	○

3. 안전한 통신

가. 개요

드론 서비스에서의 통신은 드론에게 비행 관련 명령어를 송·수신하는 제어 데이터와 드론이 임무를 수행하며 수집하는 임무데이터로 나눌 수 있다. 제어 데이터와 임무데이터를 송·수신 안전성 확보가 필요하다.

요약

안전한 통신의 주요 대응방안은 아래와 같다.

- 무선신호 보호 기능
- 통신 채널 확보/재밍 대응
- 전송 데이터 보호
- 메시지 감지

나. 보안대책

드론 시스템 및 서비스에 따라 다음 대응방안을 선별하여 적용할 수 있다.

① 무선신호 보호 기능

- 드론-지상제어장치 간, 드론-정보제공장치 간 사용되는 무선신호(RF, Wi-Fi, 무선통신 등)에 대해 보호 기능을 적용해야 한다.
  - RF 통신 보호 기능 : RF 송수신기를 이용하면 통신에 사용되는 주파수를 쉽게 분석 가능하여 재전송 공격에 취약하기 때문에, 신호 값 내에 Nounce와 타임스탬프 값 등을 함께 전송하여 이를 검증

② 통신 채널 확보/재밍 대응

- 무선통신 방해 재밍 신호를 탐지하고 우회 통신 채널 확보할 수 있어야 한다.
- 드론이 운용되는 지역에 설치된 시스템 및 드론 자체적으로 재밍 신호 모니터링할 수 있어야 한다.
- 백업 주파수나 통신 장비, 비상 백업 경로 등과 같은 추가 장비가 필요하다.

③ 전송 데이터 보호

- 드론 시스템 간 중요정보, 암호키가 전송되는 경우, 중요한 정보가 노출되지 않도록 국제표준 암호 알고리즘을 통해 데이터 암호화하여 전송해야 한다.
- 중요정보 암호화 전송 시 신로된 프로토콜을 사용해야 한다.
- 데이터 전송 시, 평문이 아닌 최소한의 인코딩 변환을 거쳐 전송해야 한다.

④ 메시지 감지

- 배터리 소모를 야기하는 비정상 메시지를 감지하고 대응할 수 있어야 한다.
- 드론-지상제어장치 간, 드론-정보제공장치 간 비인가 메시지를 감지할 수 있어야 한다.
  - 변경 감지 코드(MDC, Modification Detection Code) : 데이터 변조 및 조작, 오류에 대하여 대처할 수 있는 방법으로 변경 감지 코드를 전송 데이터에 붙여 전송
  - 메시지 인증 코드(MAC, Message Authentication Code) : 메시지에 대한 인증이 필요한 경우 메시지 인증 코드를 추가

다. 적용 범위

보안항목	대응방안	적용 자산		
		드론	지상 제어 장치	정보 제공 장치
안전한 통신	무선신호 보호 기능	○		
	통신 채널 확보/재밍 대응	○	○	
	전송 데이터 보호	○	○	○
	메시지 감지	○	○	○

4. 안전한 비행

가. 개요

드론 기반 서비스의 임무 완료를 위해서는 먼저 정상적인 비행이 가능해야 한다. 그러나 예상치 못한 비상상황이나 악의적인 이유로 정상적인 비행이 불가능한 경우, 서비스 완료하는 것보다는 인적 또는 물리적인 손상 및 손해를 끼치지 않는 것이 우선시 되어야 한다.

이를 위해서 드론 기반 서비스가 구현해야 하는 기능은 다음과 같다.

요약

안전한 비행의 주요 대응방안은 아래와 같다.

- 자율비행
- 위치추적 대체수단 제공
- 특정지역 접근방지 기능
- 자동충돌 회피
- 자동 회귀(Return To Home)

나. 보안대책

- 드론 시스템 및 서비스에 따라 다음 대응방안을 선별하여 적용할 수 있다.

① 자율비행

위치 정보에 의한 자율비행 기능과 인증된 지상제어장치의 명령을 수신할 경우 명령에 따른 임무 수행 기능이 수행되어야 한다.

② 위치추적 대체수단 제공

- GPS 위성에 접근할 수 없을 때 대응하는 대체 절차가 구현되어야 한다.

- 위치 추적에 일반적으로 사용되는 GPS 및 GLONASS와 같은 신호는 안전하지 않으므로, 셀룰러 네트워크(ex, 모바일 타워 ID), WIFI 신호 데이터베이스, 지리 정보 시스템(GIS, Geographic Information Systems), RFID 등과 같은 대체 위치추적 수단을 적용해야 한다.

GPS 스푸핑 공격 탐지 기법

2005년에 L1 신호(1575.42 MHz) 신호를 조작하는 스푸핑 공격에 착안하여 L1 대역 신호와 L2 대역 신호(1227.60 MHz) 신호의 세기 차이를 활용하여 스푸핑을 탐지하는 기법이 제안되었으며 2012년도에는 스푸핑 신호가 일반신호보다 크고 심한 변동을 가지는 특성을 이용하여 통계적 분석을 기반으로 하는 스푸핑 탐지 기법이 제안되었다.

2014년도에는 수신된 GPS 신호의 비정상적인 도플러 주파수(Doppler frequency)로 스푸핑 공격을 탐지하는 기법도 제안되었다.

브로드캐스트 신호를 암호화하거나 전자서명하는 암호학적 스푸핑 탐지 기법도 제안되었으며, 대표적인 방법으로 GNSS(위성측위시스템, Global Navigation Satellite System) 위성이 생성하는 내비게이션 메시지에 메시지 인증 개념을 적용한 NMA(Navigation Message Authentication)가 있으며, 초기 NMA는 일부 신호인증 리플레이 스푸핑 공격에 취약점이 발견되었으나 안전한 GPS 신호인증으로 재제안되었다.

출처 드론 보안에 적용된 암호 기술 현황, 정보보호학회지, 2020.4

관성항법장치 활용 기술

GPS 전파 공격에 대한 대응 방법 중 하나로, 관성항법장치는 잠수함, 항공기, 미사일 등 자기의 위치를 감지하여 목적지까지 유도하기 위한 장치이다. 자이로스코프와 가속도계를 이용하여 이동 변위를 구한 다음 처음 위치를 입력하면 현재위치와 속도를 항상 계산하여 파악할 수 있다. 이 방법은 악천후나 GPS 전파 방해에 가장 효과적인 방법이나 고가의 관성항법장치를 드론에 적용하기 쉽지 않고 누적되는 오차의 문제가 있다.

GPS 신호에 사용자 인증을 중복 적용

GPS 스푸핑 공격은 GPS 신호위조기(스푸퍼)를 이용하여 위조된 위치 및 시각 정보를 제공하여 정해진 경로를 이탈하거나 정해진 시간에 도달하지 못하도록 하는 공격으로, 이에 대한 대응방법으로 GPS 신호에 사용자 인증을 추가하여 인증 불일치 시 자동으로 신호를 제거하므로 독자적인 항법체계를 유지하거나, 드론의 GPS 수신에서 정상 GPS 신호와 스푸프된(기만) 신호를 비교하여 스푸프된 신호를 제거하는 항재밍 배열안테나 기법도 사용될 수 있다.

출처 군보안상 드론위협과 대응방안, 2018

- 드론이 추락하는 경우, 드론에 물리적 손상이 발생하지 않도록 하는 기술적인 방안도 고려되어야 한다. 가능한 방법은 낙하산, 에어쿠션, 프로펠러의 자동분리 등이 있을 수 있으며 낙하산이 가장 일반적이다.

③ 특정지역 접근방지 기능

- 위치 정보에 기반으로 비행 금지구역 및 접근불가 지역 등으로의 접근방지 기능이 필요하다.

  – GPS와 지도 데이터를 이용하여 가상의 울타리라고 할 수 있는 Geo-Fencing 기술을 적용하여 허가된 운행 경로를 설정

④ 자동충돌 회피

- 조종자에 의한 드론 제어와 무관하게 장애물이나 비행 중인 다른 비행체 등 위험요소를 탐지하고 자동으로 충돌을 회피하는 기능 및 자동 착륙기능 적용해야 한다.

> * 이동통신망을 이용한 드론 관제 인프라 시스템 활용 : 운행 드론들이 밀집된 지역에서 운영되는 경우, 충돌 위험 가능성이 높아짐에 따라 이동통신 인프라 시스템을 이용한 관제 시스템 구축도 가능하다. 이 방법의 장점은 SIM 카드를 장착한 드론이 이동전화 기지국과 연동하여 저비용으로 짧은 시간 내에 전국적인 드론 관리 인프라를 구축할 수 있을 뿐 아니라 국제간 로밍에 의한 드론 관제가 가능하고 모바일 단말기와 같이 드론에 대한 정보가 관리되어 드론의 비행허가, 운행 경로 추적 등이 가능하고 셀내의 드론 수를 제한하여 운행 중 드론의 밀집을 해소할 수 있다는 것이다.

출처 드론의 비즈니스 활성화를 위한 안전, 보안 그리고 인프라, 2016.12

⑤ 자동 회귀(Return To Home)

- 드론이 제어권을 벗어나거나 제어통제권 상실 시, 지정된 지점으로 자동 회귀하는 기능이 필요하다.

- 조종사와 드론 사이의 링크가 오프라인이 되어 통신이 끊길 경우 드론이 안전하게 집으로 돌아오는 데 필요한 정보를 제공해야 한다.

다. 적용 범위

보안항목	대응방안	적용 자산		
		드론	지상 제어 장치	정보 제공 장치
안전한 비행	자율비행	○		
	위치추적 대체수단 제공	○	○	
	특정지역 접근 방지	○		
	자동충돌 회피	○		
	자동 회귀	○		

5. 암호

가. 개요

드론의 비행정보, 임무정보 등과 같은 중요정보 저장 및 전송 시 데이터 유출, 위변조 등의 방지를 위해 중요정보에 대해 암호화를 수행해야 한다.

요약

암호의 주요 대응방안은 아래와 같다.

- 안전한 암호키 관리
- 안전한 암호 알고리즘 사용
- 안전한 난수 생성
- 안전한 암호모듈 사용

나. 보안대책

드론 시스템 및 서비스에 따라 다음 대응방안을 선별하여 적용할 수 있다.

① 안전한 암호키 관리

- 안전성이 검증된 방법을 이용하여 암호키를 생성해야 한다.
- 암호키 전송·저장 시 기밀성을 보장해야 한다.
- 암호키 사용 기간을 제한해야 한다.
- 암호키 재전송 방지를 위해 타임스탬프 기능을 제공해야 한다.
- 통신 개체들은 데이터 암호화/복호화 동작을 수행하되, 암호화/복호화 키가 공격자에게 노출되지 않아야 한다.
- 드론이 탈취되더라도 암호화/복호화 키와 관련된 어떠한 정보도 노출되지 않아야 한다.
- 인증과 관련된 비밀키/개인키를 안전하게 저장해야 한다.

② 안전한 암호 알고리즘 사용

- 통신 구간에 적합한 암호화 알고리즘을 사용해야 한다.

〈국내외 권고 암호 알고리즘〉

분류		NIST(미국) (2015)	CRYPTREC(일본) (2013)	ECRYPT(유럽) (2018)	국내[1] (2018)
대칭키 암호 알고리즘 (블록암호)		AES 3TDEA[2]	AES Camellia	AES Camellia Serpent	SEED HIGHT ARIA LEA
해시함수		SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512	SHA-256 SHA-384 SHA-512	SHA-256 SHA-384 SHA-512 SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHA3-shake128[3] SHA3-shake256[3] Whirlpool-512 BLAKE-256 BLAKE-384 BLAKE-512	SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512 LSH-224 LSH-256 LSH-384 LSH-512 LSH-512-224 LSH-512-256
공개키 암호 알고리즘	키 공유용	DH ECDH MQV ECMQV	DH ECDH	ECIES-KEM PSEC-KEM RSA-KEM	DH ECDH
	암 · 복호화용	RSA	RSA - OAEP	RSA-OAEP	RSAES
	전자 서명용	RSA DSA ECDSA	RSA-PSS RSASSA-PKCS1(v1.5) DSA ECDSA	RSA-PSS ISO-9796-2 RSA-DS2 PV Signatures Schnorr ECSchnorr KDSA[4] ECKDSA[4] XMSS	RSA-PSS KCDSA ECDSA EC-KCDSA

출처 암호 알고리즘 및 키 길이 이용 안내서, 과학기술정보통신부, 2018.12

※ 세부적인 사항은 과학기술정보통신부의 '암호 알고리즘 및 키 길이 이용 안내서' 등을 참고한다.

일회성 패드(One-Time Pad) 기반 암호 통신

2017년에 드론과 지상제어장치간의 안전한 데이터 전송을 위해 제안되었으며, 속도가 빠르고 단순한 구현이 가능하다.

출처 드론 보안에 적용된 암호 기술 현황, 정보보호학회지, 2020.4

③ 안전한 난수 생성

- 드론에 사용하는 안전한 암호키를 생성하고 보호하기 위해서 안전한 난수 생성기를 이용해야 한다.

드론 전용 난수생성기(DroneRNG)

기존 난수생성기가 PC의 마우스, 키보드 등과 같은 주변장치, 인터럽트 요청 시간 등에서 Seed을 추출하여 난수를 생성 하므로 난수성이 떨어지는 문제가 존재하였음, 드론 전용 난수생성기는 정지 상태일 때와 비행 중일 때 각각의 센서값의 특성을 분석하고, 그 특징을 활용하여 각각의 상황에 따라 다르게 후처리 하므로 생성되는 난수가 난수성이 좋은 특징을 갖는다.

출처 드론 보안에 적용된 암호 기술 현황, 정보보호학회지, 2020.4

④ 안전한 암호모듈 사용

- 안전성이 검증된 KCMVP(한국 암호모듈 검증제도, Korea Cryptographic Module Validation Program) 검증필 암호모듈 사용을 권고한다.

다. 적용 범위

구분	보안위협	피해 자산		
		드론	지상 제어 장치	정보 제공 장치
암호	안전한 암호키 관리	○	○	○
	안전한 암호 알고리즘 사용	○	○	○
	안전한 난수 생성	○	○	
	안전한 암호모듈 사용	○	○	

6. 중요 데이터 보호

가. 개요

드론과 지상제어장치에서 저장 및 수집한 임무 데이터, 비행 데이터 등의 중요정보는 안전하게 보호되어야 한다. 또한 드론은 다양한 방법으로 녹음 및 녹화 기능을 제공하고 있기 때문에 수집된 정보는 개인정보 침해 문제를 발생시킬 수 있다. 이러한 우려로 일부 사용자는 드론이 사용되는 드론 기반 서비스까지 거부할 수 있으며, 드론 기반 서비스를 제공하는 서비스 제공자 및 드론 개발자는 이를 고려한 책임감 있고 윤리적인 적용이 필요하다.

요약

안전한 통신의 주요 대응방안은 아래와 같다.

- 저장 데이터 보호
- 운영 데이터 보호
- 접근통제
- 개인정보 보호

나. 보안대책

드론 시스템 및 서비스에 따라 다음 대응방안을 선별하여 적용할 수 있다.

① 저장 데이터 보호

- 드론이 수집하고 저장하는 데이터에 대해 기밀성과 무결성을 보장해야 한다.
  - -임무 데이터, 비행 데이터 등의 중요정보가 드론(ex, SDCard 등)에 저장될 수 있는 경우, 데이터 암호화를 수행

    ex) 지상제어장치와 비대칭 암호화 알고리즘을 사용하여 데이터 암호화 수행
- 개인정보와 중요정보 등에 대한 보안을 위해 AES, RSA 등과 같은 국제표준 암호 알고리즘을 통해 데이터 암호화를 수행해야 한다.

② 운영 데이터 보호

- 드론의 경로 이탈을 방지하기 위해 내비게이션 데이터베이스의 무결성을 보장해야 한다. (ex, 경로 계획, 지오펜스 지침, 비행 금지 구역, 비상 경로)

③ 접근통제

- 저장된 데이터에 접근 시 접근권한에 대한 인증이 이루어져야 한다.
- 허가되지 않은 네트워크 트래픽을 차단하는 기능을 제공해야 한다.

화이트박스 암호(WBC, White-Box Cryptography)

탈취된 드론의 경우, 공격자가 드론의 암호 알고리즘을 분석하여 볼 수 있는 화이트박스 공격이 가능하고, 암호화키가 드론 내에 저장되어 있는 경우, 암호키를 획득하여 암호화 저장된 데이터까지 획득할 수 있는 취약점이 존재한다.

화이트박스 공격으로부터 데이터와 암호키를 보호하기 위해 화이트박스 암호를 사용하는 보안프레임워크가 제안되었다.(2019년)

출처 드론 보안에 적용된 암호 기술 현황, 정보보호학회지, 2020.4

④ 개인정보 보호

- 드론 사용을 안내하고 개인정보 수집 시, 동의를 받아야 한다.
  - 드론의 사용이 예상되는 시간이나 지역(영역)에 대해 드론 서비스 요청자에게 사전에 통지한다.
  - 개인정보 수집 시 개인정보 항목, 처리목적, 보유기간, 미동의의 불이익 내용이 포함된 법적 고지사항을 사용자에게 구체적으로 안내하고 동의를 받아야 한다.

    ※ 세부적 사항은 개인정보보호법 제15조, 개인정보보호법 제22조 등을 참고한다.
  - 소유자의 동의 없이 사유재산을 침해하지 않는다.

- 드론에 의해 수집되는 데이터의 수집 목적
- 수집 대상이 되는 데이터의 종류
- 데이터 보존 및 삭제에 대한 정보
- 데이터를 공유할 기업의 유형
- 개인정보 보호 및 보안 불만사항 등에 대한 제출 방법
- 법 집행기관 요청에 대응하는 사례를 설명하는 정보

- 개인정보가 포함된 데이터 수집 시 주의사항을 숙지해야 한다.

- 개인정보처리방침에 수집된 개인정보의 이용 및 제3자 제공에 대한 방침을 명시하고 수집·이용 목적 범위 내에서 처리해야 한다.
- 개인정보가 포함된 데이터를 동의 없이 수집·저장하지 않는다.
- 개인정보가 포함된 데이터의 지속적인 수집을 목적으로 드론을 사용하지 않는다.
- 개인정보와 관련된 정보는 암호화하여 저장 및 관리해야함
- 개인정보가 포함된 데이터 수집 시 비식별 조치하여 안전하게 관리해야 한다.

〈개인정보 비식별 조치 방법 예시〉

처리기법	예시	세부기술
가명처리	홍길동, 35세, 한국대 재학 ▶ 임꺽정, 30대, 국제대 재학	휴리스틱 가명화 암호화 교환방법
총계처리	임꺽정 180cm, 홍길동 170cm ▶ 한국학과 직원 키 합 : 350cm, 평균키 : 175cm	총계처리 부분총계 라운딩 재배열
데이터 삭제	주민등록번호 901206-1234567 ▶ 90년대 생, 남자	식별자 삭제 식별자 부분삭제 레코드 삭제 식별요소 전부삭제
데이터 범주화	홍길동, 35세 ▶ 홍씨, 30~40세	감추기 랜덤 라운딩 범위방법 제어 라운딩
데이터 마스킹	홍길동, 35세, 한국대 재학 ▶ 홍○○, 35세, ○○대학 재학	임의 잡음 추가 공백과 대체

출처 개인정보 비식별 조치 가이드라인, 관계부처합동, 2016

- 개인정보가 포함된 데이터에 대한 사용 및 공유를 제한해야 한다.
  - 명시적으로 허용된 경우를 제외하고 개인정보가 포함된 데이터를 사용하지 않는다.
  - 개인정보가 포함된 수집 데이터를 사용 목적 외에 사용하거나 공유하지 않아야 한다.
  - 드론 서비스를 수행하기 위해 개인정보가 포함된 데이터를 공개하지 않아야 하며, 공개하는 경우 비식별화 조치(가명 처리, 익명 처리 등)를 수행해야 한다.
  - 동의 없이 마케팅 목적을 사용하거나 공유하지 않아야 한다.

- 수집된 데이터에 대한 보안 조치를 수행해야 한다.
  - 개인정보 보유기간 경과 및 처리목적이 완료될 경우 개인정보 처리정치, 정정, 파기 등의 절차를 진행해야 한다.
  - 드론에 의해 수집된 개인정보가 포함된 데이터에 대하여 데이터 보호를 위한 보안위험 관리 조치를 취한다.
  - 개인정보가 포함된 데이터 수집, 사용, 저장, 배포에 대한 보안정책을 수립한다.
  - 드론 서비스 시스템에 대한 정기적인 모니터링을 수행한다.
  - 개인정보가 포함된 데이터에 접근할 수 있는 직원에 대한 보안교육을 실시한다.
  - 개인정보처리자의 접속기록, 처리한 정보주체 정보, 수행업무 등을 최소 1년 이상 보관·관리해야 한다.

〈접속기록 항목 예시〉

- 계정 : A0001(개인정보취급자 계정)
- 접속일시 : 2019-02-25, 17:00:00
- 접속지 정보 : 192.168.100.1(접속한 자의 IP주소)
- 처리한 정보주체 정보 : CLI060719(정보주체를 특정하여 처리한 경우 정보주체의 식별정보)
- 수행업무 : 회원목록 조회, 수정, 삭제 다운로드 등

※ 위 정보는 반드시 기록해야 하며 개인정보처리자의 업무환경에 따라 책임추적성 확보에 필요한 항목은 기록해야 한다.

출처 개인정보의 안전성 확보조치 기준 해설서, 행정안전부, 2019

  - 개인정보에 대한 접근권한을 부여하여 개인정보에 대한 접근을 통제해야 한다.
  - 드론에 전송 데이터 암복호화용 세션키를 저장하지 않는 보안 채널을 제공한다.

- 정부의 법 및 규정 등에 대한 모니터링하고 준수해야 한다.

다. 적용 범위

구분	보안위협	피해 자산		
		드론	지상 제어 장치	정보 제공 장치
중요 데이터 보호	저장 데이터 보호	○	○	○
	운영 데이터 보호	○	○	○
	접근통제	○	○	○
	개인정보 보호	○	○	○

7. 보안감사

가. 개요

블랙박스 등을 활용하여 드론의 운항 동작, 수집 데이트 등에 대한 감사기록을 유지해야 향후 드론 사고 및 고장 등의 원인을 파악할 수 있다. 또한 비행 전에 비행을 위한 기능의 동작상태 등을 확인해야 한다.

요약

보안감사의 주요 대응방안은 아래와 같다.

· 감사기록
· 모니터링

나. 보안대책

- 드론 시스템 및 서비스에 따라 다음 대응방안을 선별하여 적용할 수 있다.

① 감사기록

- 감사기록 생성 기능을 구현해야 하며, 드론 시스템의 이상행위를 탐지 및 추적할 수 있어야 한다.

- 감사기록은 사건발생 일시, 유형, 사건을 발생시킨 주체의 신원, 작업내역 및 결과(성공/실패) 등을 고려하도록 권고한다.
  - 감사기록 대상 : 사용자 로그인 성공/실패, 설정 변경 내역, 기능 수행내역(보안기능 포함) 등 - 감사기록 제외 대상 : 비밀번호, 암호키 등 민감한 정보 등
  - 사건발생 일시는 신뢰할 수 있는 타임스탬프가 사용되어야 하며, 시간 동기화가 필요하다.

- 인가된 사용자(관리자)가 해석 할 수 있도록 감사기록을 생성하고, 검토할 수 있는 기능을 제공해야 한다

② 모니터링

- 시스템 설계의 잠재적 취약점을 식별하기 위해 사전 점검이 필요하다.

- 드론 플랫폼의 구성 변경 및 드론 임무 변경 등을 확인한다.

- 드론 시스템에서 사용자 계정 추가/삭제를 확인한다.

- 드론 시스템 내 계정과 관련된 권한 변경 여부를 확인한다.

다. 적용 범위

구분	보안위협	피해 자산		
		드론	지상 제어 장치	정보 제공 장치
보안감사	감사기록	○	○	
	모니터링	○	○	○

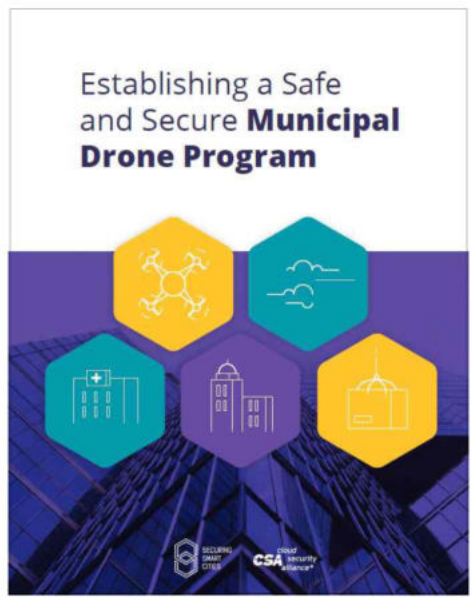
PART

부록

A. 국외 드론 보안 관련 가이드
B. 참고 문헌

부록 A. 국외 드론 보안 관련 가이드

1. CSA, Establishing a Safe and Secure Municipal Dron Program



클라우드 보안 협회 (CSA, Cloud Security alliance)는 도시에서 운영되는 드론에서 야기될 수 있는 문제점(개인정보 유출 방지 및 중요시스템에 대한 비인가 접근을 막기 위한 보호방법, 센서 및 카메라 데이터의 신뢰를 위한 데이터 무결성 보호방법, 규정 준수 등)에 대한 가이드를 제시하기 위해 아래와 같이 요구사항을 정의하여 안내한다.

가. 보안을 위한 구현 및 테스트 지침

지침	설명
인증 및 권한 부여 절차	• 공격자가 드론의 조종권을 탈취할 수 없도록 각 인터페이스에 대해 인증절차를 구현해야한다. 인증과 관련된 비밀키/개인키를 안전하게 저장해야한다.
정책 관리	• 드론시스템의 특징 상 많은 관리자가 접근이 필요하기 때문에 접근 제어를 위해 유연한 정책관리 기능이 필요하다.
안전한 통신	• 조종기와 드론 사이의 연결이 끊어질 시 및 GPS위성에 접근이 불가할 시 대응 솔루션에 대한 구현 필요함. 드론 시스템의 모든 인터페이스에 대해 암호화가 필요함

지침	설명
드론에 대한 데이터베이스 구축	• 드론시스템에 대한 제어를 위해 국가데이터베이스 구축하여 일련번호, 하드웨어 모델, 주파수 채널, 활동 등에 대한 기록을 해야함. 사이버 공격 및 펌웨어 조작으로 인한 오작동을 감지하는데 사용될 수 있음.
데이터 보안	• 드론이 탈취되는 경우 드론에 저장된 운영데이터 및 수집데이터가 유출될 수 있어 암호화가 필요함
보안 기능 테스트	• 전송구간 암호화 및 메시지 인증 등 드론시스템에 대해 계획된 보안기능요구사항에 대해 정기적으로 테스트를 수행하여 드론시스템의 보안 제어의 정상 작동여부를 확인해야함
제3자 소스코드 검토	• 드론 시스템에 설치될 수 있는 타사모듈에 대해 설치 전 소스코드에 대해 테스트 및 보안평가를 수행해야한다. 타사 모듈이 도입될 시 새로운 위협과 취약점이 발생될 수 있으므로, 정기적으로 보안위협을 추적해야한다.
가용성 보장	• 드론이 제공하는 서비스의 품질을 유지할 수 있도록 가용성이 보장되어야한다.
위치 추적 보증	• 위치추적에 사용되는 GPS 등의 신호는 쉽게 스푸핑되므로, 위치추적에 대한 대안 기술이 병렬로 실행되어야한다. 셀룰러 네트워크 또는 GIS, RFID 등 각 지역에 분산된 위치정보시스템을 연계하는 솔루션이 있을 수 있다.
통신 채널 중단 / 재밍 방지	• 방해신호로 인해 드론시스템의 서비스 중단 및 서비스가 거부될 수 있다. 방해신호의 감지를 위해 드론이 서비스되는 지역에 미리 관련 시스템을 설치하여 방해신호를 모니터링 할 수 있고, 백업 주파수나 비상 백업 경로 등을 마련하는 대응 방법이 필요하다.
무결성 검사 및 악성코드 방지	• 드론 시스템 운영의 품질과 지속 가능성을 위해 무결성 검사가 필요함. 데이터베이스 및 악성코드, 업데이트, 타사 코드 등에 대해 무결성 보호가 필요함
업데이트 관리	• 소프트웨어·펌웨어·패치관리 등의 기능에도 무결성 검사기능을 제공하여 드론시스템이 안전하고 신뢰될 수 있도록 운영되어야한다.
모니터링	• 시스템 설계의 잠재적인 약점을 식별하기 위해 드론시스템의 전자적·물리적 정찰 수행이 필요함 • 비행 관리 소프트웨어 내의 구성 변경에 대한 모니터링 필요함 • 드론 플랫폼 구성 변경에 대한 모니터링 필요함 • 드론 시스템에서 사용자 계정 추가·삭제 및 권한 변경에 대한 모니터링 필요함 • 드론 및 임무 계획 시스템에 대한 접근(로그인)등에 대한 모니터링 필요
취약성 점검	• 드론 배치 전 침투테스트를 통해 보안제어와 절차 및 교육등에 대한 약점을 식별할 수 있다. 배치 후에는 최소 매년 침투테스트가 필요하다.
사고 대응	• 사이버 보안 문제를 모니터링 해야함. 드론시스템에 대한 사고는 크게 인프라에 대한 사이버공격과 드론 기체의 손상이 있음. 사고는 장치관리솔루션(접근성, 무결성 검사 등) 및 오작동에 대한 신고자에 의해 발견될 수 있다. 사고 대응을 위해 백업 경로를 미리 설정하고, 복구를 위한 체계를 갖춰야한다.

나. 사이버 보안 구축

많은 수의 장치를 수동으로 모니터링 할 수 없으므로 자동화가 필요하다. 안전한 드론시스템이 구축되면, 사이버 보안 문제 및 사고대응에 대한 이점이 있다. 드론 시스템 운영 시 아래와 같은 문제가 발생될 수 있다.

위장 시스템

- 무선네트워크 트래픽의 스니핑을 위해 설치되는 시스템

위장 드론

- 드론으로 위장하여 드론시스템의 손상 및 서비스 중단이 유발될 수 있다.

재밍 시스템

- 무선 신호를 방해할 목적으로 사용되는 전파방해 신호로, 서비스 거부 등 장애가 일어 날 수 있음.

취약한 시스템

- 잘못 구성되거나 패치가 적용되지 않은 시스템은 스니핑 및 비인가된 접근 등의 보안에 취약할 수 있다.

2. NTIA, Voluntary best practices for UAS(unmanned aircraft systems) privacy transparency and accountability

미국 NTIA(National Telecommunications and Information Administration)는 무인항공기에 사용 대한 지침으로, 개인정보보호와 투명성 및 책임성을 위한 모범사례를 안내한다. UAS는 작은 크기로 녹음 및 영상촬영 등을 할 수 있어 다양한 분야에 사용이 가능하지만 개인정보에 대한 우려를 불러일으킬 수 있다.

UAS 사업자의 개인 및 상업적 사용에 대한 프라이버시, 투명성 및 책임성을 향상시키기 위해 취할 수 있는 자발적인 모범 사례를 개략적으로 설명하는 가이드이다.

가. UAS 운영자를 위한 가이드 "주변 드론을 위한 운영 가이드"

- 헌법상 보장된 자유를 감소시키거나 제한할 수 없다.
- 지방법, 주법, 연방법규를 우선시한다.
- UAS 사업자와 계약을 하고자 하는 기업은, 계약 의무 등 UAS 사업자가 우선시 되도록 해야 한다. UAS 사업자는 계약 시 모범사례를 고려하여 계약조건을 설정해야한다.
- UAS의 안전한 비행을 방해할 수 없다.

나. 자발적 모범 사례

- UAS 운영자는 모든 해당 법률 및 규정을 준수해야 한다. 이러한 모범 사례는 법적 준수를 보완하는 긍정적인 행동을 장려하기 위한 것이다.
- UAS 사용을 알린다.
  - UAS가 데이터를 수집할 것으로 예상할 수 있는 시간을 사전에 통지하기 위한 노력을 기울여야함
  - 수집한 데이터에 개인정보보호 정책을 제공해야하며, 데이터를 수집하는 목적, 데이터의 종류, 보존 및 삭제 정보, 데이터가 공유되는 기업, 개인정보보호 에 대한 불만사항을 제출하는 방법, 법 집행기관의 요청에 대한 대응 등이 공개되어야함.
- UAS 작동 및 데이터 저장 시 주의사항 표시
  - 데이터주체의 동의가 없거나 불필요한 경우 의도적으로 데이터를 수집하는 것을 피해야한다.

- 재산 소유자의 동의가 없거나 적절한 법적 권한이 없는 경우 사유 재산에 대한 UAS 운영을 최소화하여야 한다.

수집한 데이터의 사용 및 공유 제한

- 데이터 주체가 사용 또는 공개에 대한 동의를 제공하지 않는 한 커버된 데이터를 마케팅 목적으로 사용하거나 공유하지 않도록 합리적인 노력을 기울여야 한다.
- 개인 정보 보호 정책에 포함되지 않은 목적을 위해 커버된 데이터를 사용하거나 공유하지 않도록 합리적인 노력을 기울여야 한다.

보안이 보장된 데이터

- UAS 운영자는 데이터 수집 및 사용, 저장, 배포에 대한 서명 보안정책을 수립한다.
- 데이터 보안 위험에 대해 정기적인 모니터링을 수행해야함
- 데이터 접근권한이 있는 직원에 대한 보안교육을 수행해야함
- 인가된 직원만 데이터에 접근할 수 있도록 정책을 수립해야함.

법률 준수

- UAS 운영자는 해당 법률 및 규정과 개인 정보 보호 및 보안 정책 준수를 보장해야 한다.

3. SDC, Drone Security Guide

일본 Secure Drone Consortium에서 작성한 'Drone security guide'는 드론의 보안 위협 분석 및 특성을 설명하고, 드론을 안전하게 비행하기 위해 무인 항공기 관리자 인증에 대한 설명 등을 다루고 있다.

가. 드론 보안 위험 분석

드론 고유의 취약성

- 드론은 다목적으로 사용되기 때문에 플랫폼과 네트워크 구성이 다양함
- 도난 및 분실 시 물리적 공격에 대한 위험이 있음

드론 운영 시스템의 자산 구분

- 개인정보, 기밀정보 등을 구분하고, 자산 관리에 대한 책임자를 지정하는 등 자산에 대한 보호 프로세스가 필요함

위험 사전 검증

- 조직 내 보안취약점 여부를 항상 점검하고 대응해야함.
- 보안 책임자를 지정하고 취약점 발견 시 신속한 처리가 가능하도록 프로세스를 규정해야함

위험 분석 및 평가

- 사전 검증된 위험이 실제 발생 시 초래되는 결과를 분석한다.

드론의 사이버 공격

- 조종권이 탈취 된 드론은 비행금지 구역에 침입하거나 촬영금지구역에서 촬영을 할 수 있고, 운반드론에 대해 운반되는 물품을 탈취할 수 있다.
- 드론이 수집한 데이터가 탈취되는 경우 수집한 데이터를 기반으로하는 서비스(교통량 및 기후 등)가 동작되지 않아 연계서비스에 큰 피해를 입힐 수 있다.
- 드론의 각 프로토콜에 대해 접근을 시도하고 오류 및 접근 제어 등에 대한 결함을 확인한다.
- 인증메커니즘과 암호정책을 조사한다.
- 통신 시 암호화여부를 확인하고 중간자 공격에 대한 대응여부를 확인한다.
- 클라우드 서비스가 지원되는 경우 백엔드 서버에 대해서도 취약점 진단을 실시해야한다.
- 진단을 통해 발견된 취약점에 대해서 보수를 실시한다.
- 새로운 취약점이 발견될 수 있으므로 정기적으로 진단을 실시한다.

나. 조종권 인증

- 인가된 사용자만이 조종을 할 수 있도록 시스템이 구현되어야한다.
- 드론과 조종기와의 연결 시 생체인식 및 전자 인증서등을 통한 인증이 필요하다.

다. 데이터 보안

- 드론이 수집한 데이터를 드론에 탑재된 SD카드등에 저장하는 경우 저장매체 관리 및 보관에 주의를 기울여야하며, 클라우드 서비스에 업로드를 하는 경우 인증 절차통해 접근되어야한다.
- 보안을 위해 드론이 LTE·5G를 이용하여 직접 업로드할 수 있도록 구현되는 방법이 있을 수 있다.

라. 비행을 위한 점검 및 조종사 훈련

- 비행 전 및 주기적으로 기체에 대해 외관 및 소음 등을 확인하여 점검
- 드론 조종사들에 대한 훈련 및 조종 시 준수사항 등 안전 보장을 위한 체제가 필요함

부록 B. 참고문헌

[1] 드론 신규 수요 발굴 및 기술 격차 극본을 통한 산업 활성화 필요, NICE평가정보(주), 2019.8.1.

[2] 드론 제품·서비스 현황, 영진전문대학교, 2019.05.

[3] 드론택배 서비스 실현 방안분석, ETRI, 2018.08.01.

[4] 시설 관리 및 재난 대응을 위한 드론 통신 및 보안 기술 동향, IITP, 2019.10.

[5] TTAK.KO-12.0317, 드론 기반 서비스를 위한 보안 요구 사항

[6] SOC 시설물의 스마트 통합 유지 관리를 위한 드론 기반 3D 엔진 및 무선 제어 계측 플랫폼 기반 기술 개발 최종보고서, 2019.01.

[7] 드론을 이용한 물류서비스 추진 방향, 2015

[8] "재난치안용 드론 떴다", 산업통산자원부 보도자료, 2019.10.

[9] 재난치안용 멀티콥터 무인기 운용 개념 - 임무 시나리오를 중심으로, 한국항공우주연구원

[10] 재난치안용 드론 초도비행, 국토교통부

[11] 스마트 하천관리를 위한 하천조사 최적화 드론시스템(River Drone) 개발 기획

[12] 드론 보안에 적용된 암호 기술 현황, 정보보호학회지, 2020.4

[13] 군보안상 드론위협과 대응방안, 2018

[14] 드론의 비즈니스 활성화를 위한 안전, 보안 그리고 인프라, 한경호

[15] 드론 보안에 적용된 암호 기술 현황, 정보보호학회지, 2020.4

[16] 산업테마보고서 드론, NICE평가정보(주), 2019

[17] 국내외 드론산업 동향 분석을 통한 공공분야에서의 드론 활용방안에 대한 연구, 한국IT서비스학회, 2016

[18] 드론의 구성, http://www.sigmapress.co.kr/shop/shop_image/g47841_1550542236.pdf

[19] 열린친구, https://www.openmakerlab.co.kr/

[20] 드론으로 밀수 잡다!, http://www.korea.kr/news/reporterView.do?newsId=148866065

[21] 드론, 부산항의 경쟁을 거들고 나서다, 아나드론, https://www.anadronestarting.com/%eb%b6%80%ec%82%b0%ed%95%ad%ec%9d%98/

[22] 국토교통부 보도자료, http://www.motie.go.kr

[23] 고양시, 드론실증도시 구축 사업 본격 시작, https://www.boannews.com/media/view.asp?idx=88996&kind=2
[24] 고양시 드론으로 안전도시 만든다(서울경기케이블TV뉴스), https://www.youtube.com/watch?v=xj40YLJg5Ls,
[25] IBM Knowledge Center
[26] https://www.anadronestarting.com/%EC%84%BC%EC%84%9C/
[27] https://www.anadronestarting.com/%ED%95%B4%ED%82%B9
[28] http://www.asoa.co.kr/
[29] https://brunch.co.kr/@jejucenter/211
[30] http://www.boan24.com/news/articleView.html?idxno=2505
[31] https://www.donga.com/news/It/article/all/20110601/37686475/1
[32] https://www.etnews.com/20200619000223
[33] https://www.mk.co.kr/news/society/view/2017/10/703361/
[34] https://play.google.com/store/apps/details?id=kr.co.threessolution.droneintegrationsystem&hl=km
[35] http://www.polinews.co.kr/news/article.html?no=178386
[36] https://sharehobby.tistory.com/entry/XFile-26
[37] https://youtu.be/on4DRTUvst0
[38] 개인정보 비식별 조치 가이드라인, 관계부처합동, 2016.6
[39] 개인정보의 안전성 확보조치 기준 해설서, 행정안전부, 2019.6
[40] 개인정보의 기술적·관리적 보호조치 기준 해설서, 방송통신위원회, 2017.12
[41] IoT 공통 보안 가이드, 한국인터넷진흥원, 2015.09
홈·가전 IoT 보안 가이드, 한국인터넷진흥원, 2017.7
[42] 스마트교통 사이버보안 가이드, 한국인터넷진흥원, 2019.12
[43] 스마트의료 사이버보안 가이드, 한국인터넷진흥원, 2018.5
[44] 소프트웨어 개발보안 가이드, 한국인터넷진흥원, 2019.11
[45] 암호 알고리즘 및 키 길이 이용 안내서, 과학기술정보통신부, 2018.12
[46] 사물인터넷(IoT) 환경에서의 암호·인증기술 이용 안내서, 과학기술정보통신부, 2017.12

드론 분야 ICT 융합 제품·서비스의
보안 내재화를 위한

드론 사이버보안 가이드

인 쇄 2020. 12월
발 행 2020. 12월

발행처 **한국인터넷진흥원**
(58324) 전라남도 나주시 진흥길 9
(한국인터넷진흥원)
TEL. 1544-5118 **FAX.** 405-5119
www.kisa.or.kr

드론 분야 ICT 융합 제품·서비스의
보안 내재화를 위한

드론 사이버보안 가이드

Cyber Security Guide for **Drone**

KISA 한국인터넷진흥원