

INDEX

과제 1. C-ITS STRIDE 수행	1
1. F2 ~ F8에 대한 STRIDE를 수행하라	1
2. F2 ~ F8에 해당하는 위협을 선정한 이유를 설명하라	2
3. Module 2-3 학습 내용을 활용하여 방어 기법에 대해 간단히 논하라	3
 과제 2. STRIDE 설명	 5
1. STRIDE의 정의를 정리하라	5
2. STRIDE가 의미하는 위협의 실제 사례를 찾아 보고서를 작성하라	5
 과제 3. 위협 모델링 실습	 7
1. 서비스 대상 선정 및 설명	7
2. DFD 그리기	8
3. 위협 식별하기	10
4. 식별된 위협을 STRIDE에 매칭 시키기	13

과제 1. C-ITS STRIDE 수행

1. F2 ~ F8에 대한 STRIDE를 수행하라

Data Flow	위협	STRIDE	보안 기법
F2 도로교통/센서 정보	A3. 정보 전송 행위의 부인	R (Repudiation)	전자서명, 감사로그
	A4. 다른 노변기기로 위장	S (Spoofing)	인증, 전자서명
	A5. 도로 교통 정보 변경	T (Tampering)	해시, 전자서명
	A8. 센서 정보 변경	T (Tampering)	해시, 전자서명
F3 차량주행 정보	A1. 다른 차량으로 위장	S (Spoofing)	인증, 전자서명
	A2. 차량 주행 정보 변경	T (Tampering)	해시, 전자서명
	A3. 정보 전송 행위의 부인	R (Repudiation)	전자서명, 감사로그
F4 차량주행 정보	A2. 차량 주행 정보 변경	T (Tampering)	해시, 전자서명
	A3. 정보 전송 행위의 부인	R (Repudiation)	전자서명, 감사로그
	A4. 다른 노변기기로 위장	S (Spoofing)	인증, 전자서명
F5 도로교통 정보	A3. 정보 전송 행위의 부인	R (Repudiation)	전자서명, 감사로그
	A5. 도로 교통 정보 변경	T (Tampering)	해시, 전자서명
	A6. 다른 교통관리센터로 위장	S (Spoofing)	인증, 전자서명
F6 수집된 센서 정보	A3. 정보 전송 행위의 부인	R (Repudiation)	전자서명, 감사로그
	A7. 다른 지원 시스템으로 위장	S (Spoofing)	인증, 전자서명
	A8. 센서 정보 변경	T (Tampering)	해시, 전자서명
F7 수집된 센서 정보	A3. 정보 전송 행위의 부인	R (Repudiation)	전자서명, 감사로그
	A7. 다른 지원 시스템으로 위장	S (Spoofing)	인증, 전자서명
	A8. 센서 정보 변경	T (Tampering)	해시, 전자서명
F8 도로교통 정보 공유	A3. 정보 전송 행위의 부인	R (Repudiation)	전자서명, 감사로그
	A5. 도로 교통 정보 변경	T (Tampering)	해시, 전자서명
	A6. 다른 교통관리센터로 위장	S (Spoofing)	인증, 전자서명

2. F2 ~ F8에 해당하는 위협을 선정한 이유를 설명하라

Data Flow	위협 선정 이유
F2 도로교통/센서 정보	(A3) 노변기기의 위협원이 자신이 보낸 정보에 대해 부인하는 보안 문제가 발생할 수 있다고 보았다.
	(A4) 정보 송신해야 하는 노변기기가 아닌 다른 노변기기가 위장하여 정보를 전송하는 보안 문제가 발생할 수 있다고 보았다.
	(A5) 노변기기에서 차량으로 전송하는 도로교통 정보가 변경되는 보안 문제가 발생할 수 있다고 보았다.
	(A8) 노변기기에서 송신하는 센서 정보가 변경되는 보안 문제가 발생할 수 있다고 보았다.
F3 차량주행 정보	(A1) 정보 송신해야 하는 차량이 아닌 다른 차량이 위장하여 정보를 전송하는 보안 문제가 발생할 수 있다고 보았다.
	(A2) 차량 간 주행 정보를 주고받는 과정에서 전송되는 데이터의 변경에 대한 보안 문제가 발생할 수 있다고 보았다.
	(A3) 차량의 위협원이 자신이 보낸 정보에 대해 부인하는 보안 문제가 발생할 수 있다고 보았다.
F4 차량주행 정보	(A2) 정보 송신 측의 노변기기에서 송신하는 데이터가 변경되는 보안 문제가 발생할 수 있다고 보았다.
	(A3) 노변기기의 위협원이 자신이 보낸 정보에 대해 부인하는 보안 문제가 발생할 수 있다고 보았다.
	(A4) 정보 송신해야 하는 노변기기가 아닌 다른 노변기기가 위장하여 정보를 전송하는 보안 문제가 발생할 수 있다고 보았다.
F5 도로교통 정보	(A3) 교통관리센터의 위협원이 자신이 보낸 정보에 대해 부인하는 보안 문제가 발생할 수 있다고 보았다.
	(A5) 교통관리센터에서 노변기기로 전송하는 도로교통 정보가 변경되는 보안 문제가 발생할 수 있다고 보았다.
	(A6) 정보 송신해야 하는 교통관리센터가 아닌 다른 교통관리센터가 위장하여 정보를 전송하는 보안 문제가 발생할 수 있다고 보았다.
F6 수집된 센서 정보	(A3) 지원시스템의 위협원이 자신이 보낸 정보에 대해 부인하는 보안 문제가 발생할 수 있다고 보았다.
	(A7) 정보 송신해야 하는 지원시스템이 아닌 다른 지원시스템이 위장하여 정보를 전송하는 보안 문제가 발생할 수 있다고 보았다.
	(A8) 지원시스템에서 송신하는 센서 정보가 변경되는 보안 문제가 발생할 수 있다고 보았다.
F7 수집된 센서 정보	(A3) 지원시스템의 위협원이 자신이 보낸 정보에 대해 부인하는 보안 문제가 발생할 수 있다고 보았다.
	(A7) 정보 송신해야 하는 지원시스템이 아닌 다른 지원시스템이 위장하여 정보를 전송하는 보안 문제가 발생할 수 있다고 보았다.
	(A8) 지원시스템에서 송신하는 센서 정보가 변경되는 보안 문제가 발생할 수 있다고 보았다.
F8 도로교통 정보 공유	(A3) 하나의 교통관리시스템의 위협원이 자신이 보낸 정보에 대해 부인하는 보안 문제가 발생할 수 있다고 보았다.
	(A5) 교통관리센터 간 주행 정보를 주고받는 과정에서 전송되는 데이터의 변경에 대한 보안 문제가 발생할 수 있다고 보았다.
	(A6) 정보 송신해야 하는 교통관리센터가 아닌 다른 교통관리센터가 위장하여 정보를 전송하는 보안 문제가 발생할 수 있다고 보았다.

3. Module 2-3 학습 내용을 활용하여 방어 기법에 대해 간단히 논하라

▶ 암호화

1) 대칭키

- 대칭키의 특징

- ① 암호화와 복호화에 사용하는 키가 동일
- ② 송신자와 수신자 모두 동일한 키 공유
- ③ 비밀키는 송신자와 수신자 이외에는 알지 못하도록 함
- ④ 대규모 데이터의 빠른 암호화에 사용이 있음

- 대칭키의 장단점

(장점)

- ① 연산이 매우 효율적임
- ② 키 생성 과정이 비교적 간단함
- ③ 키 길이가 비교적 짧음
- ④ 알고리즘의 표준화가 잘 되어 있고 특허가 없음
- ⑤ 표준화된 대칭키 암호 알고리즘들은 매우 안전함

(단점)

- ① N명의 사람이 서로 통신하기를 원할 경우, $n(n-1)/2$ 개의 대칭 키가 필요
→ 대규모 네트워크에 적용하기 어려움
- ② N명의 그룹에서 각 사람은 $n-1$ 개의 키를 가지고 있으며, 그룹 내의 다른 사람에 대한 $n-1$ 개의 키를 기억해야 함 → 비효율적
- ③ 안전한 키의 공유와 분배가 가능해야 함

2) 공개키

① 공개키(Public Key)

누구나 이용할 수 있는 공개된 값, 메시지 암호화에 사용

송신자는 수신자의 공개키를 이용하여 전달하고자 하는 메시지를 암호화 한다.

② 개인키(Private Key)

개인이 소장하고 있는 비밀 값, 메시지 복호화에 사용

수신자는 개인키를 이용하여 송신자가 보낸 암호문을 복호화 한다.

비밀키를 초기 생성할 때에 사용하는 난수를 생성하는 난수 발생기가 있다. 난수를 생성할 때는 두 가지 방법을 예로 들 수 있는데 랜덤한 소스를 입력으로 사용하여 난수를 생성하는 TRNG와 고정 값 seed를 입력 받아 난수를 생성하는 PRNG가 있다.

TRNG의 경우 랜덤한 소스를 입력으로 사용하기 때문에 PRNG에 비해 보안성이 더 높지만 랜덤한 소스를 받아오는데 걸리는 시간이 오래 걸려 난수를 생성하는 시간이 비교적 오래 걸린다. 반대로 PRNG의 경우 고정된 seed를 사용하기 때문에 난수를 생성하는 시간은 비교적 짧지만 정해진 값을 사용하는 만큼 보안성이 떨어진다고 할 수 있다.

이러한 이유로 Hybrid pseudo random number generator 기법을 많이 사용하는데 이 기법은 TRNG를 사용해 짧은 길이의 value를 가져와 seed로 사용하여 필요한 길이의 pseudo random number를 생성하기 때문에 TRNG와 PRNG 각각의 단점을 보완한 기법이라고 할 수 있다.

▶ 전자서명

전자서명은 인감도장의 역할을 하는 ‘생성’과 인감증명의 역할을 하는 ‘검증’등 한 쌍의 전자서명키로 구성되는데 생성키는 서명자만 보관해서 사용하고 전자서명검증키는 정보통신망을 통해 누구나 알 수 있도록 공개된다. 이처럼 전자서명은 공개키 기반 구조로 전자문서의 Hash값을 서명자의 개인키로 암호화한 것으로서 RSA사에서 만든 표준이 널리 사용된다.

▶ Hash

Hash 함수는 데이터를 압축할 때 사용하며 다른 길이의 입력이 들어가더라도 고정된 길이의 Hash value가 생성된다. 이러한 Hash 함수를 사용할 때에는 필요조건이 존재하는데 이 조건을 암호학적 Hash 함수의 필요조건이라 한다. 이러한 필요조건에는 충돌 저항성(Collision resistance), 역상 저항성(Preimage resistance), 제 2 역상 저항성(Second preimage resistance)가 존재한다.

또한 이러한 Hash 함수 중 독특한 특징을 가진 일 방향 Hash 함수라는 것이 존재한다. 이 함수는 password를 저장할 때 사용하는 데 단순한 암호화에 비해 복잡한 복호화 과정을 갖는 것이 특징이다.

▶ 감사로그

감사 로그는 컴퓨터의 사용자를 추적할 수 있도록 컴퓨터의 모든 활동을 시간별로 자동 기록해 놓은 것이다. 즉 특정 작업, 절차, 이벤트에 영향을 미치는 일련의 활동 증거를 제공하는 레코드의 출처와 도착지, 레코드의 집합, 시간 순 보안 관련 기록이다. 감사용 기록은 일반적으로 금융 거래, 과학 연구, 의료 데이터 트랜잭션, 개인, 시스템, 계정, 기타 실제 간 커뮤니케이션 등의 활동에서 비롯되는 것이 보통이다. 따라서 감사 로그를 활용하여 데이터 전송 행위의 부인과 같은 문제를 해결할 수 있다.

▶ 메시지 인증

메시지 인증은 데이터 무결성 보장을 위한 메시지 인증 코드 생성에 사용된다. 송신자가 수신자에게 보내는 메시지에 대해 공격자가 위조, 변조, 삭제 등의 공격을 대비하기 위하여 메시지 인증 코드(MAC: Message Authentication Code)를 사용한다. 메시지 인증을 위해서는 키가 사용되는데 이때 대칭키를 사용하여 송신자와 수신자의 MAC 값을 비교하여 메시지의 상태를 확인할 수 있다.

과제 2. STRIDE 설명

1. STRIDE의 정의를 정리하라

STRIDE(Spoofing identify, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege)는 Microsoft사에서 1999년에 개발한 보안 위협 모델링 방법이다.

STRIDE는 인증, 무결성, 부인 방지, 기밀성, 가용성, 권한 부여와 같은 보안 속성을 고려하고, DFD(Data Flow Diagram)의 개체, 프로세스 등에 존재하는 위협을 식별한다.

예를 들어, 사용자란 개체에 Spoofing identify 키워드를 적용할 때, 해커가 사용자로 위장하여, 시스템 접근 권한을 획득한다와 같은 위협 을 식별할 수 있다.

[출처: 사이버 보안 표준 및 위협 분석 기법 동향 | 작성자 상명대학교 특임교수 도성룡]

위협 유형	설명
위장 (Spoofing identity)	false identity를 이용해 시스템 접근 권한을 획득하는 경우
데이터 변조 (Tampering with data)	데이터가 전송될 때 공격자가 데이터를 수정하는 경우
부인 (Repudiation)	공격자 자신이 수행한 특정 행동이나 트랜잭션을 부인하는 경우
정보 유출 (Information disclosure)	개인정보 혹은 잠재적으로 유해한 데이터가 유출되는 경우
서비스 거부 (DoS, Denial of Service)	시스템 또는 어플리케이션의 가용성을 떨어뜨리는 경우
권한 상승 (Elevation of privilege)	권한이 있는 사용자의 권한을 습득하는 경우

2. STRIDE가 의미하는 위협의 실제 사례를 찾아 보고서를 작성하라

▶ 네이트 개인정보 유출 사건

[출처: wikipedia]

https://ko.wikipedia.org/wiki/%EB%84%A4%EC%9D%B4%ED%8A%B8_%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4_%EC%9C%A0%EC%B6%9C_%EC%82%AC%EA%B1%B4]

네이트 개인정보 유출 사건은 해킹으로 인해 2011년 7월 26일에 네이트의 데이터베이스에 저장된 가입자 3500만 명의 아이디, 비밀번호, 이름, 주민등록번호, 연락처 등의 개인정보가 유출된 사건이다.

전문가들은 IP 주소로 미뤄보아 중국발 해킹으로 추정되며, 돈을 노린 해커가 SK커뮤니케이션즈 내부 개발자 PC를 해킹해 벌어진 사고라고 관측하고 있다. 네이트를 운영하는 SK커뮤니케이션즈 측에서는 사고 발생 이틀만에야 해킹 사실을 파악하였다.

※ 해당 해킹 사건은 돈을 노린 해커가 기업 내부 개발자의 PC를 해킹하여 개인정보가 유출된 사건으로 STRIDE 중 I에 해당한다. 또한 내부 개발자의 PC를 해킹하는 과정에서 PC에 대하여 위장과 정보 유출(S, I) 공격이 이뤄졌음을 짐작해 볼 수 있다.

▶ 7·7 DDoS 공격

[출처: wikipedia]

https://ko.wikipedia.org/wiki/7%C2%B77_DDoS_%EA%B3%B5%EA%B2%A9]

7·7 디도스 공격 또는 777 디도스 공격은 2009년 7월 7일을 기점으로 대한민국과 미국의 주요 정부기관, 포털 사이트, 은행 사이트 등이 분산 서비스 거부 공격(DDoS, 디도스)을 당하여 서비스가 일시적으로 마비된 사건이다.

2009년 7월 9일 국가정보원에서는 발생의 진원지가 조선민주주의인민공화국의 110호 연구소로 추정된다는 발표를 하였고, 보안 업체에서는 미국과 대한민국을 포함한 여러국가의 IP에서 발생이 시작된 것이라고 추정하였다.

10월 말, 국정원에서는 진원지가 조선민주주의인민공화국의 체신청이라는 공식 조사결과를 발표했다. 11월 17일 미국의 보안업체 맥아피는 조선민주주의인민공화국이 만약 디도스 공격을 감행했다면 주한미군과 본토 지휘부 사이의 커뮤니케이션을 마비시키기 위한 전략에 따른 것일 수 있다고 보고했고, CNN 등 언론이 이를 인용하여 보도했다.

※ 해당 해킹 사건은 서비스가 DDoS 공격을 당하여 서비스가 마비되어 정상적으로 수행되지 못하도록 한 사건으로 STRIDE 중 D에 해당한다. 또한 DDoS 공격 과정에서 위장과 권한 상승(S, E) 공격이 이뤄졌음을 짐작해 볼 수 있다.

과제 3. 위협 모델링 실습

1. 서비스 대상 선정 및 설명

< 드론 배송시스템 >



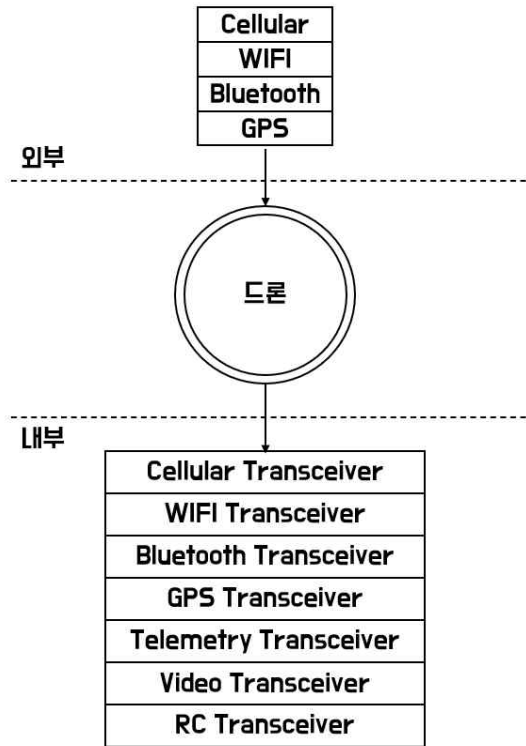
드론 배송이란 드론의 기체에 전용박스 등 배송 물품을 장착한 후 공로로 배송 하는 것이다. 물류 분야에서 드론은 배송거리, 배송시간, 비용 면에서 장점을 가지고 있는데 특히 농촌 지역 및 산간지역과 같은 외진지역으로의 배송뿐만 아니라 의약품이나 수혈용 혈액 등 긴급배송에서도 최고의 선택 중 하나로 간주되고 있다.

물류창고에서 일반가정이나 사무실로의 배송은 배송거리는 짧으나 도로배송으로 비교적 긴 시간과 많은 노력이 소요 되어 “라스트 원 마일(last one mile)”이라고 불리는 물류말단의 효율성 제고가 물류업계의 큰 과제이다. 따라서 드론을 이용한 배송이 세계 각국의 주목을 받으며 활발히 연구가 진행되고 있는데 미국이 기술개발부분에서 선구적이며, 최근에는 유럽 각국과 중국에서도 활발하게 연구가 진행 중이다. 특히 2013년 아마존이 ‘프라임에어’라는 배송서비스를 시행한 후, 다른 대형 유통업계에서도 드론을 이용한 배송에 큰 관심을 보이며 시범사업을 추진하여 성공하고 있다.

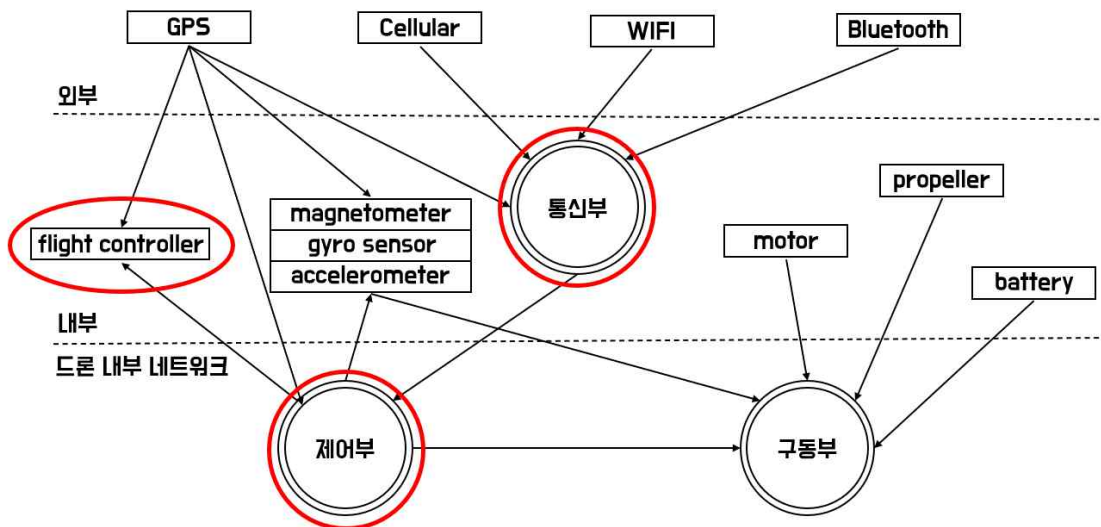
[출처: 물류분야의 드론 응용 동향 | 작성자 한국교통연구원]

2. DFD 그리기

< Level 0 >

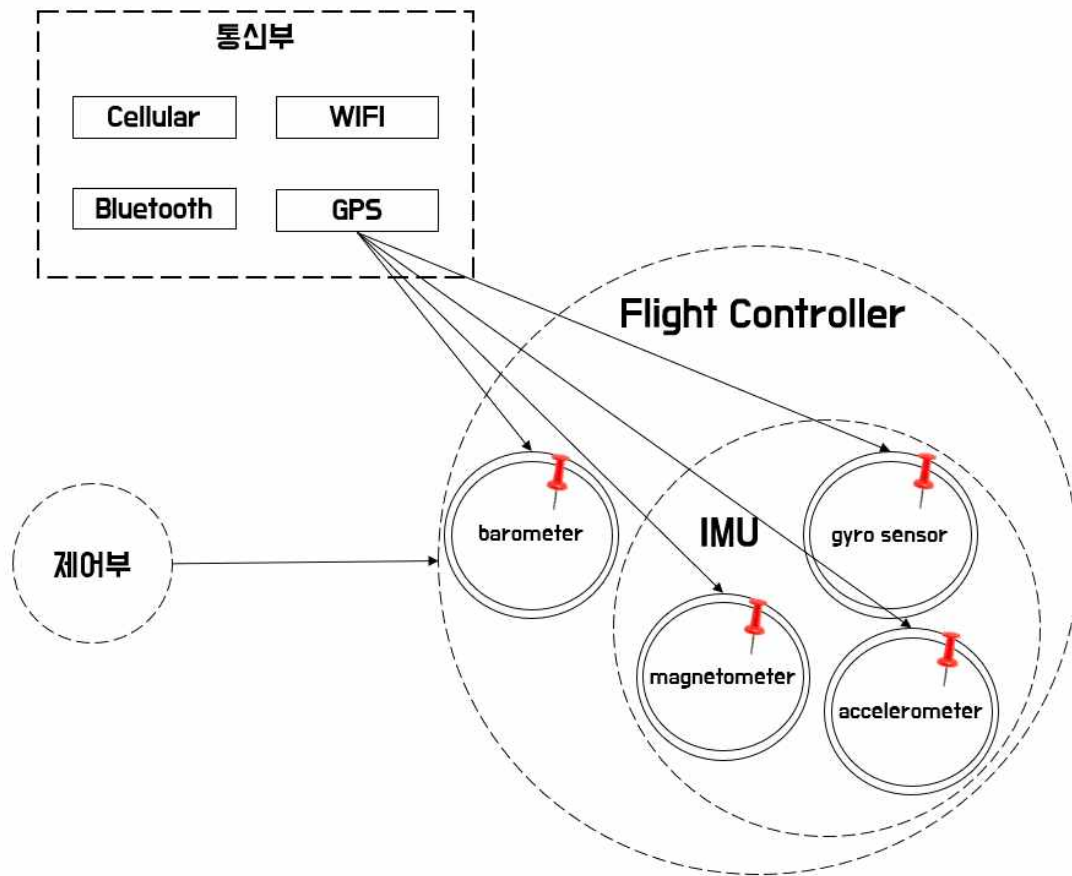


< Level 1 >



※ 드론에서 flight controller는 드론의 뇌와 같은 역할을 하는 비행제어장치로써 무선 조종기에서 송출되는 조종 명령(주파수)에 따라 변속기에 모터를 제어하는 신호를 보내는 역할을 한다. 이에 flight controller와 직접적 연관이 있는 통신부, 제어부를 중심으로 Level 2를 전개해 보았다.

< Level 2 >



barometer	대기압을 측정하여 무인기의 고도를 측정
gyro sensor	드론이 수평을 유지할 수 있도록 도와주며 세 축 방향의 각가속도를 측정하여 드론의 기울기 정보 제공
accelerometer	센서에 가해지는 가속도를 측정하며 중력에 대한 상대적인 위치와 움직임 측정(3축: x축, y축, z축)
magnetometer	나침반 기능을 하며 자북을 측정하여 드론의 방향 정보를 드론의 CPU로 전송

※ flight controller가 드론에서 핵심적인 역할을 하는 만큼 GPS와 제어부에서 송신하는 정보에 문제가 발생하면 드론에 치명적이라고 판단하였다.

3. 위협 식별하기

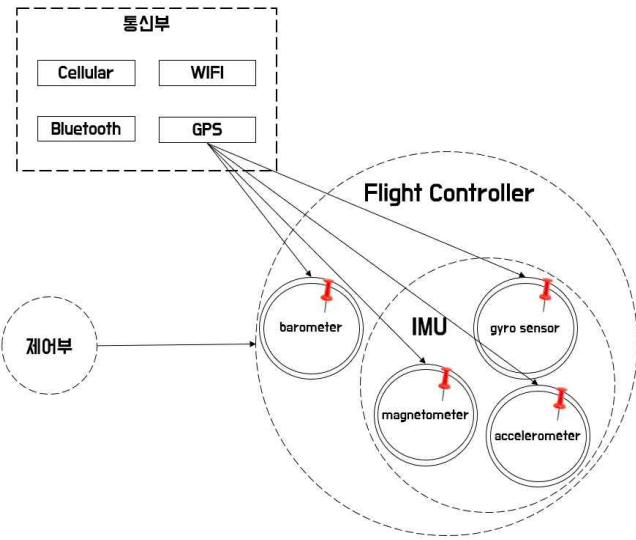
< Level 0 >

DFD	위협 식별
	<p>- 외부</p> <p>전송 데이터 탈취 전송 데이터 변경 데이터 전송 행위의 부인</p> <p>- 드론</p> <p>드론 제어 권한 탈취 드론 시동 시스템 셧 다운 드론 도난 드론 추적 드론 내 악성 프로그램 설치</p> <p>- 내부</p> <p>전송 데이터 탈취 전송 데이터 변경 데이터 전송 행위의 부인</p>

< Level 1 >

DFD			
위협 식별	<p>- WIFI</p> <p>네트워크 통신 데이터 탈취 네트워크 통신 데이터 변경 데이터 전송 행위의 부인 드론 위치 추적</p>	<p>- Cellular</p> <p>네트워크 통신 데이터 탈취 네트워크 통신 데이터 변경 데이터 전송 행위의 부인 드론 위치 추적</p>	<p>- GPS</p> <p>GPS 통신 데이터 탈취 GPS 통신 데이터 변경 데이터 전송 행위의 부인</p>

< Level 2 >

DFD	위협 식별
	<p>– accelerometer</p> <p>가속도 데이터 탈취 가속도 데이터 변경 데이터 전송 행위의 부인 악성 SW 업로드</p>
	<p>– gyro sensor</p> <p>기울기정보 탈취 기울기정보 변경 데이터 전송 행위의 부인 악성 SW 업로드</p>
	<p>– magnetometer</p> <p>방향정보 탈취 방향정보 변경 데이터 전송 행위의 부인 악성 SW 업로드</p>
	<p>– barometer</p> <p>고도정보 탈취 고도정보 변경 데이터 전송 행위의 부인 악성 SW 업로드</p>

4. 식별된 위협을 STRIDE에 매칭 시키기

LEVEL	위협 발생 위치	위협	STRIDE
Level 0	외부	전송 데이터 탈취	I
		전송 데이터 변경	T
		데이터 전송 행위의 부인	R
	드론	드론 제어 권한 탈취	S, E
		드론 시동 시스템 셧 다운	D
		드론 도난	D
		드론 추적	I
		드론 내 악성 프로그램 설치	D
	내부	전송 데이터 탈취	I
		전송 데이터 변경	T
		데이터 전송 행위의 부인	R
Level 1	WIFI	네트워크 통신 데이터 탈취	I
		네트워크 통신 데이터 변경	T
		데이터 전송 행위의 부인	R
		드론 위치 추적	I
	Cellular	네트워크 통신 데이터 탈취	I
		네트워크 통신 데이터 변경	T
		데이터 전송 행위의 부인	R
		드론 위치 추적	I
	GPS	GPS 통신 데이터 탈취	I
		GPS 통신 데이터 변경	T
		데이터 전송 행위의 부인	R
Level 2	accelerometer	가속도 데이터 탈취	I
		가속도 데이터 변경	T
		데이터 전송 행위의 부인	R
		악성 SW 업로드	D
	gyro sensor	기울기정보 탈취	I
		기울기정보 변경	T
		데이터 전송 행위의 부인	R
		악성 SW 업로드	D
	magnetometer	방향정보 탈취	I
		방향정보 변경	T
		데이터 전송 행위의 부인	R
		악성 SW 업로드	D
	barometer	고도정보 탈취	I
		고도정보 변경	T
		데이터 전송 행위의 부인	R
		악성 SW 업로드	D