<부록1. 보안목표명세서>

# CHAOS ver1.0
# 보안목표명세서 ver1.0

## - 고등급 보안 마이크로커널 개발 -

# <목 차>

# <표 목차>



# <그림 목차>

# 1. 보안목표명세서 소개

본 장에서는 보안목표명세서 및 TOE 참조, TOE 개요, 그리고 TOE 설명에 대해 기술한다. 보안목표명세서 및 TOE 참조에서는 보안목표명세서와 TOE의 식별 자료를 제공하고, TOE 개요에서는 TOE에 대해 간략하게 기술하고, TOE 설명 부분에서는 TOE를 좀 더 상세하게 기술함으로써 본 보안목표명세서가 설명하고자 하는 TOE에 대해 단계적으로 알 수 있도록 한다.

## 1.1. 보안목표명세서 참조

본 절에서는 보안목표명세서의 제목, 버전, 작성자, 작성일 등을 통해 보안목표명세서를 유일하게 식별하는 정보를 제공한다.

- 제목: CHAOS(ChibiOS-based High-Assurance Operating System) ver1.0 보안목표명세서 ver1.0
- 보안목표명세서 버전: ver1.0
- 작성자: 고신뢰 보안 운영체제 연구센터
- 최초 작성일: 2018.11.27.
- 마지막 수정일: 2020.11.25.

## 1.2. TOE 참조

보안목표명세서를 준수하는 TOE는 다음과 같이 식별된다.

- TOE명: CHAOS(ChibiOS-based High-Assurance Operating System) ver1.0
- 개발자: CHAOS
- TOE 식별
  - CHAOS : ChibiOS-based High-Assurance Operating System ver1.0

## 1.3. TOE 개요

본 절에서는 임베디드 디바이스 상에서 보안 기능을 수행하는 마이크로커널의 용도와 주요 보안 특성에 대해 서술한다. TOE(CHAOS)는 하드웨어 및 소프트웨어의 설치, 제거, 관리, 실행 기능을 수행한다.

### 1.3.1. TOE 사용 용도 및 주요 보안 특성

TOE는 임베디드 디바이스 상에 설치되어 디바이스의 기능을 관리하는 마이크로커널로서, 디바이스의 보안성 및 안전성을 높이기 위해 운영체제의 핵심 기능만을 갖추고 이외의 기능은 모두 사용자 모드에서 실시하는 시스템을 말한다. TOE의 용도 및 주요 보안 특성을 열거하면 다음과 같다.

- 접근 제어

TOE는 모든 자원(객체)과 모든 사용자 어플리케이션 스레드(주체)에 대해 Capability Model을 통하여 접근을 통제한다. Capability는 주체가 접근하고자 하는 객체에 대한 접근 권한의 수준을 판별할 수 있도록 하는 정보를 의미한다. 주체가 특정 객체에 접근하고자 할 때, TOE는 주체의 Capability를 열람하여 해당 접근을 인가하거나 비인가 하는 것으로 접근을 통제한다.

■ 잔여 데이터 보호

TOE는 사용자 어플리케이션(주체)이 종료하기 전에 메모리에 저장되어 있는 데이터를 완전히 소거한 후 종료한다. TOE는 물리적 메모리에 남겨진 잔여 정보를 통하여 보안성이 위협받는 상황을 배제하기 위하여 해당 주체에게 할당되었던 물리 메모리 영역의 값을 0으로 덮어씀으로써 관련된 데이터를 소거한다.

TOE는 TOE 자체가 종료되기 전에도 물리 메모리에 저장되어 있는 데이터를 완전히 소거한 후에 종료한다. 소거 방식은 물리 메모리 영역의 데이터 중 디스크에 반영할 사항을 저장한 후 모든 메모리 영역을 0으로 바꾸는 것이다.

■ 감사 기능

TOE는 실행 도중 발생하는 특정 이벤트에 대하여 감사 기록을 생성한 후, 사전에 할당된 메모리 영역 내에 증적한다. 증적된 감사 기록들을 바탕으로 TOE는 보안 기능과 관련된 모든 이벤트에 대해, 책임 소재를 구분하는 것이 가능하다.

TOE는 감사 기능의 시작 및 종료 시 감사 기록을 생성하며, 기본 감사 수준에 따라 보안기능이 사용되는 모든 시도와 보안속성이 변경되는 주체가 발생하는 경우에 대하여 모두 기록한다. 이 때, TOE의 감사 기록은 이벤트 일시, 이벤트 유형, 주체의 신원, 이벤트 결과에 대하여 저장한다.

### 1.3.2. 비-TOE 하드웨어/소프트웨어

TOE가 설치되어 동작하는데 있어 필요한 부가적인 하드웨어, 소프트웨어, 운영체제가 식별된다.

| 구분 | | 설명 |
|---|---|---|
| 하드웨어 | CPU | 180 MHz |
| | DDRMemory | 256 KiB 이상 |
| | FlashMemory | 2MiB 이상 |

[표 1] TOE 하드웨어/소프트웨어/운영체제

## 1.4. TOE 설명

본 절에서는 TOE가 사용될 수 있는 응용 환경을 서술하기 위해 TOE의 구성 범위, 물리적 범위, 그리고 논리적 범위에 대해 서술한다.

### 1.4.1. 물리적 범위

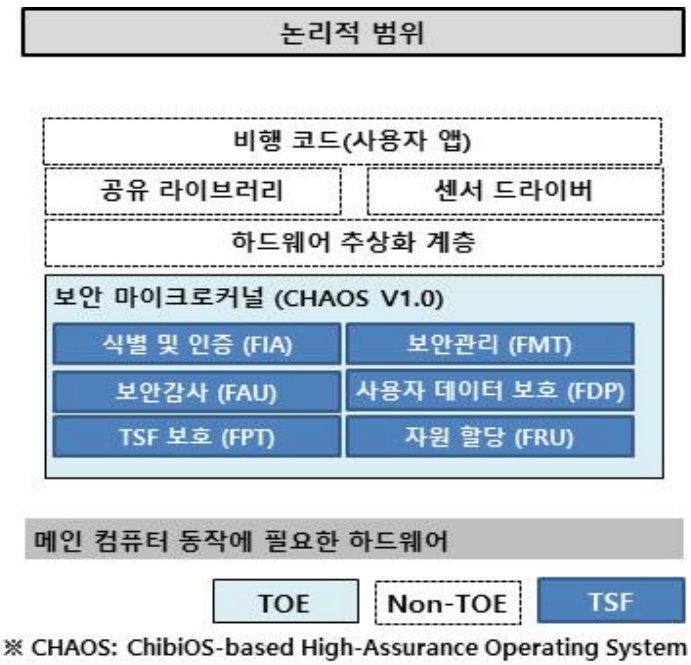
공통평가기준에서 TOE의 형태는 크게 하드웨어, 소프트웨어, 펌웨어로 구분된다. TOE는 그중에서 드론의 동작을 제어하기 위해 드론 메인 컴퓨터에 탑재되는 소프트웨어이다. 따라서 TOE는 드론의 동작을 제어하기 위해 아래 그림 1과 같이 다양한 물리적 구성 요소들과 연결된다.

TOE와 연결되는 물리적 구성 요소는 드론 메인 컴퓨터, 해당 컴퓨터와 유선으로 연결되어 센서로부터 수집되는 외부 입력값을 처리하는 컴패니언 보드, 그 외 외부로부터 비행 또는 임무 수행에 필요한 데이터를 수집하는 다양한 센서(예: 카메라, GPS, Gyro 센서 등)와 비행에 필요한 동력원이 되는 모터와 해당 모터를 제어하기 위한 , ESC(Electronic Speed Control) 모듈이 존재한다. 그 외에도 드론과 무선 통신할 수 있는 지상 관제 시스템(예: 원격 조종기 등)이 존재한다.


[그림 1] TOE 물리적 범위

### 1.4.2. 논리적 범위

TOE의 논리적 범위는 아래 그림 2와 같다. TOE는 물리적 범위에서 식별된 드론 메인 컴퓨터에 탑재되는 보안 마이크로커널로 1) 식별 및 인증, 2) 보안 기능관리, 3) 보안감사, 4) 사용자 데이터 보호, 5) TSF 보호, 6) 자원 할당의 총 6가지 TSF를 포함한다. 외부와의 통신으로 입력되는 데이터는 그 유형에 따라 상기에서 나열된 6가지 TSF 중 최소 하나의 TSF에 의해 처리된다.




[그림 2] TOE 논리적 범위

상기에서 설명된 6가지의 TSF에 대한 상세한 설명은 다음과 같다.

**보안감사(FAU)**

TOE는 시스템에 대한 보안위협 발생 시 해당 위협에 대한 원인을 추적하기 위해 보안감사 기능을 제공한다. 이러한 보안감사 기능은 이벤트에 대한 주체, 해당 이벤트의 발생 시각, 이벤트의 내용을 담은 메시지를 감사 기록으로 저장한다. 또한, 감사 기록의 손실을 방지하기 위해 잔여 감사 기록 저장 공간을 주기적으로 확인하고 경고 메시지를 출력함으로써 의도치 않게 감사 기록이 손실되는 상황에 대응한다.

**사용자 데이터 보호(FDP)**

TOE는 신뢰되지 않은 외부 객체로부터 TSF 데이터를 보호하기 위해 접근 통제 모델을 적용한다. 또한, TOE는 스레드가 종료된 후, 사용자가 활용한 데이터가 외부에 유출되는 것을 방지하기 위해, 종료 직전에 메모리에 저장되어 있는 스레드 관련 데이터를 모두 소거한다.

**보안관리(FMT)**

TOE는 인가된 관리자에 한하여 보안기능을 관리 및 조정할 수 있도록 관리자 인터페이스를 지원한다. 이 때, TOE는 관리자 인터페이스에 접근하고자 하는 주체가 인가된 관리자인지 확인하기 위해 관리자에게 식별 정보를 요청한다.

**TSF 보호(FPT)**

TOE의 모든 보안기능은 커널 영역에서 동작하며, 주기적으로 자체 검사를 수행한다. 자체 검사 결과 문제가 발생하지 않을 경우, TOE는 현재 상태를 안전 상태로 정의한 후 커널 영역에 해당 값을 저장한다.

만약 TSF 기능에 대해 수행한 자체 검사 결과 문제가 발생하는 경우 TOE는 자가 복구 메커니즘을 통해 이전의 안전 상태로 복구된다. 따라서 일시적으로 TSF 기능에 문제가 발생하더라도 자체 검사를 통해 이전의 안전 상태로 자가 복구되어 시스템 전체로 문제가 확대되지 않아 보안기능에 영향을 끼치지 않는다.

**자원 할당(FRU)**

TOE는 TSF 및 사용자 애플리케이션의 기능이 과도한 자원을 할당받지 않도록 방지하여 서비스 거부와 같은 공격을 방지한다.

## 1.5. 작성 규칙

본 보안목표명세서는 일부 약어 표기 및 명확한 의미 전달을 위해 영어를 혼용한다. 사용된 표기법, 형태, 작성규칙은 공통평가기준을 따른다.

공통평가기준은 보안기능요구사항에서 수행될 수 있는 선택, 할당, 반복, 정교화 오퍼레이션을 허용한다. 이 오퍼레이션은 본 보안목표명세서에서도 사용된다.

**반복**

다양한 오퍼레이션과 같은 컴포넌트가 반복될 경우 사용된다. 반복 오퍼레이션의 결과는 컴포넌트 식별자 뒤에 괄호 안의 반복 번호, 즉 (반복 번호)로 표시된다.

**선택**

요구사항 서술 시 정보보호시스템 공통평가기준에서 제공되는 선택사항 중 하나 이상을 선택하는데 사용된다. 선택 오퍼레이션의 결과는 *밑줄 그은 이탤릭체*로 표시된다.

**정교화**

요구사항에 상세사항을 추가함으로써 요구사항을 더욱 제한하는데 사용된다. 정교화 오퍼레이션의

결과는 **굵은 글씨**로 표시된다.

**할당**

명세되지 않은 매개변수에 특정 값을 할당하는데 사용된다. 할당 오퍼레이션의 결과는 대괄호, 즉 [할당_값]으로 표시된다.

**보안목표명세서 작성자**

속성의 최종 결정이 보안목표명세서 작성자에 의해 이루어짐을 나타내는데 사용된다. 보안목표명세서 작성자 오퍼레이션의 결과는 중괄호 안의 {보안목표명세서 작성자에 의해 결정}으로 표시된다. 또한, 보호프로파일에서 완벽하게 수행되지 않은 보안기능요구사항의 오퍼레이션은 보안목표명세서 작성자에 의해서 완벽하게 수행되어야 한다.

**응용 시 주의사항**

요구사항의 의미를 명확히 하고, 구현 시 선택사항에 대한 정보를 제공하며, 요구사항에 대한 '적합/부적합' 기준을 정의하기 위해 응용 시 주의사항이 제공된다. 응용 시 주의사항은 필요한 경우 해당 요구사항과 함께 제공된다.

## 1.6. 용어 정의

본 보안목표명세서에 사용된 용어 중 공통평가기준 및 보호프로파일에 사용된 용어와 동일한 것은 공통평가기준을 따르며 본 보안목표명세서에는 추가로 기술하지 않는다.

**인가된 관리자**

보안기능 요구사항에 따라서 TOE를 안전하게 운영 및 관리하는 인가된 사용자이다. TOE의 설정값 및 운영절차를 변경할 수 있는 권한을 보유하고 있으며, 이를 위해 충분한 교육을 받은 관리자를 지칭한다. 또한, 인가된 관리자는 의도적으로 TOE의 보안 기능을 우회하거나 정지시키지 않으며, 의도치 않은 사고가 발생하지 않게끔 운영할 수 있도록 교육받는다.

**인가된 일반 사용자**

TOE를 정상적으로 이용하고자 하는 일반 사용자이다.

**주체**

주체는 TOE 상에서 구동되는 스레드와 TOE에 접근하고자 하는 외부 객체를 총칭한다. 주체는 공통적으로 Capability 보안속성을 소유하며, 스레드의 경우 추가적으로 우선순위 보안속성을 소유한다. 이러한 주체는 TSF에 의해 관리되고 있는 보안속성에 기반하여 TOE에 접근할 수 있다.

**우선순위**

우선순위는 TOE 상에서 구동되는 스레드가 스케줄러에 의해 CPU를 점유할 수 있는 순위이다. 해당 속성은 오직 인가된 관리자에 의해서만 변경될 수 있다. 해당 속성을 통해 모든 사용자 스레드보다 TSF 스레드가 일반 사용자 스레드 보다 우선적으로 CPU를 할당받을 수 있다.

**객체**

주체가 TOE 상에서 수행하고자 하는 오퍼레이션(Operation)의 대상으로, 데이터를 포함하는 수동적인 실체이다.

# 2. 준수 선언

준수 선언은 본 보안목표명세서가 준수하는 공통평가기준, 보호프로파일, 패키지에 대한 선언과 본 보안목표명세서에서 보호프로파일 준수를 선언하는 방법을 서술한다.

## 2.1. 공통평가기준 준수 선언

본 보안목표명세서는 다음의 공통평가기준을 준수한다.

■ 공통평가기준 식별

- 정보보호시스템 공통평가기준, 1부: 소개 및 일반 모델, 버전 3.1r5, 2017. 4, CCMB-2017-04-001
- 정보보호시스템 공통평가기준, 2부: 보안기능컴포넌트, 버전 3.1r5, 2017. 4, CCMB-2017-04-002
- 정보보호시스템 공통평가기준, 3부: 보증컴포넌트, 버전 3.1r5, 2017. 4, CCMB-2017-04-003

■ 공통평가기준 준수여부

- 정보보호시스템 공통평가기준 2부 준수
- 정보보호시스템 공통평가기준 3부 준수

## 2.2. 보호프로파일, 패키지 준수 선언

본 보안목표명세서는 다음의 보호프로파일, 패키지를 준수한다.

### 2.2.1. 보호프로파일 준수

본 보안목표명세서가 수용하는 보호프로파일은 없다.

### 2.2.2. 패키지 준수

본 보안목표명세서는 보증요구사항 패키지 EAL6를 준수한다.

## 2.3. 준수 선언의 이론적 근거

본 보안목표명세서는 다른 보호프로파일에 대한 준수를 선언하지 않았으므로, 준수 선언의 이론적 근거 기술은 필요치 않다.

# 3. 보안문제정의

보안문제정의는 TOE 및 TOE 운영환경에서의 위협, 조직의 보안정책 및 가정사항을 정의한다. 이때 TOE에 대한 자산, 위협은 위협모델링 기법 중 STRIDE를 통해 체계적으로 식별된다. STRIDE는 소프트웨어에 대한 보안위협을 6가지(Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege)로 분류한 후 체계적으로 위협을 식별하기 때문에, 위협을 완화하기 위한 보안기능 요구사항 도출 시 충분성을 입증하는 근거로 활용될 수 있다. 먼저 위협모델링 기법에 따라 체계적으로 위협을 도출하기 위해 자산을 식별한 후 TOE 내부 동작을 파악하기 위한 DFD를 작성한다. 이때 DFD 작성 과정에서 식별된 TOE의 구성요소에 대해 알려진 취약점을 수집하여 공격라이브러리를 구성한다. 이후 TOE에서 발생할 수 있는 위협을 STRIDE 기법에 따라 도출한 후, 도출된 위협 목록을 바탕으로 실제 발생할 수 있는 공격 시나리오를 공격 트리로 도식화한다. 공격 트리는 TOE에 대해 발생할 수 있는 실제 위협 목록으로 본 연구팀은 해당 위협의 발생 조건(공격 트리 내 리프노드)를 제거할 수 있는 보안기능 요구사항을 선정하였다.

## 3.1. 자산

본 절에서는 STRIDE 기법에 따라 TOE에 대한 첫 번째로 수행되는 데이터흐름도(DFD, Data Flow Diagram)와 자산 간의 관계를 식별한다. DFD와 구성요소에 대한 정의는 <부록A>를 참고한다. <부록A>를 기반으로 TOE 영역 내 자산은 아래와 같이 식별되며, 자산과 DFD 구성요소는 아래와 같이 매핑된다.

| 자산 | 상세 설명 | 관련된 부록 A 내 DFD 요소 |
|---|---|---|
| AS.TSF 데이터 | TOE에 저장되는 TSF 데이터 | DS1 |
| AS.TSF | TOE에 탑재되는 TSF | P1, P4 |
| AS.Non-TSF | TOE에 탑재되는 Non-TSF | P2, P3, P5 ~ P11 |

[표 2] 자산 목록

## 3.2. 위협

다음 절에서는 TOE에 대한 위협원과 그로 인해 발생할 수 있는 위협에 대해 서술한다. 위협원은 일반적으로 전송중인 자산의 비밀성 및 무결성을 훼손하려 하거나 TOE에 대해 불법적인 접근을 시도하고 비정상적인 방법으로 TOE에 위해를 가하는 IT 실체를 말한다.

위협원은 높은 수준의 전문지식, 자원, 동기를 가지며, 위협원이 악용 가능한 취약성을 발견할 가능성이 높다고 가정한다. 즉, 위협원은 명백한 취약성 정보를 이용하여 악용 가능한 취약성 정보 및 공격도구를 인터넷을 통하여 쉽게 획득하여 목표하는 컴퓨터 자원을 훼손하거나 불법적으로 정보를 획득할 수 있다. TOE는 이러한 명백한 취약성에 대한 위협으로부터 자산을 보호하기 위해 STRIDE 기법을 활용하여 체계적으로 위협을 도출해야 한다. 하지만 STRIDE 기법만을 통해 도출된 위협은 추상적이기 때문에 구체화되어야 한다. 이를 위해 CVE, CWE와 같은 대형 취약점 데이터베이스나 취약점 연구 논문 등을 수집하여 공격라이브러리를 구축한 후, 기존에 도출된 위협과 매핑함으로써 위협을 구체화시킬 수 있다. 그에 대한 상세 정보는 <부록B. 공격라이브러리>, <부록C. 도출된 위협 목록>을 참고한다. 도출된 위협을 바탕으로 실제 드론에 대해 발생할 수 있는 공격을 시각적으로 표현한 공격 시나리오는 <부록D. 공격 트리>와 같다. 부록 C와 D를 통해 매핑된 위협을 공통평가기준에 맞게 구분할 경우, 아래와 같은 위협이 구분되며 도출된 위협과 공격트리는 아래와 같이 매핑된다.

| 위협 | 상세 설명 | 부록 2 내 도출된 위협 목록 간 매핑 | 부록 3 내 도출된 공격트리 간 매핑 |
|---|---|---|---|
| T.TSF 데이터 유출 | TSF가 실행되기 위해 필요한 TSF 데이터 (시스템 설정 값, 스레드 큐, 스레드 실행 시간, 스레드 포인터 등)의 정보가 비인가된 방식으로 유출할 수 있음 | T4, T10, T16, T22, T28, T29, T35, T41, T47, T54, T60, T66, T71, T105, T139, T184, T200, T201, T202, T218, T219, T230 | AT1, 2, 3 |
| T.TSF 데이터 훼손 | TSF 데이터가 인가되지 않은 접근 방식으로 변조될 수 있음 | T2, T8, T14, T20, T26, T27, T33, T39, T45, T52, T58, T64, T69, T103, T137, T203, T226 | AT1, 3 |
| T.TSF 우회 | TSF 데이터가 변조되어 TSF가 우회될 수 있음 | T6, T50, T56, T62, T138, T221, T239, T241 | AT 3 |
| T.안전하지 않은 상태 | 잘못된 설정 값이 탑재되어 TOE가 불안전한 상태에 빠짐 | T2, T6, T12, T14, T20, T26, T27, T31, T62, T72, T111 | AT 1 |
| T.서비스 거부 | TSF 데이터 변조 또는 TOE에 대한 무분별한 작업 요청으로 인해 TOE 객체에 접근할 수 없음 | T19, T23, T30, T31, T185, T211 | AT 4 |
| T.인가되지 않은 접근 | 인가되지 않은 접근을 통해 신뢰하지 않은 주체나 외부 개체가 TOE에 접근하는 것이 가능함 | T160, T164, T168, T170, T172, T180, T190, T191, T199, T207, T208, T212 | AT1, 3 |

[표 3] 위협과 공격트리 간의 매핑

## 3.3. 조직의 보안정책

다음 절에서는 TOE 및 TOE 운영환경에서 고려해야 하는 조직의 보안정책에 대해 서술한다.

**P.신뢰된 관리자**

TOE를 관리하는 인가된 관리자는 의도적으로 TSF를 우회하거나 TSF 데이터를 유출 혹은 훼손하지 않는다. 또한, 인가된 관리자는 TOE와 관련된 다양한 교육과 관리자 지침을 바탕으로 TOE를 안전하게 관리한다.

**P.신뢰된 애플리케이션**

TOE와 통신하는 애플리케이션은 악성코드를 포함하지 않아, TSF나 Non-TSF를 우회하거나 영향을 끼칠 수 없다.

**P. 암호화**

TOE는 외부 개체와 통신할 때 NSA(National Security Agency), KISA(Korea Internet & Security Agency) 등과 같은 전문기관에서 권고하는 암호화 알고리즘을 활용하여 데이터를 전송한다.

## 3.4. 가정사항

다음 절에서는 보안 기능성을 제공하기 위해 운영환경에 요구되는 가정사항들에 대해 서술한다.

**A.물리적 접근 제한**

TOE가 설치되는 프로세서는 TOE를 설치하기 이전에 제3자에 의한 접근 및 변조 없이 안전하게 제공된다. 사용자 애플리케이션에서 활용하며, TOE가 중간자 역할로 조정하는 외부 센서와 액츄에이터는 TOE가 설치된 프로세서에 연결하기 이전에 제3자에 의한 접근 및 변조 없이 안전하게 제공된다.

# 4. 보안목적

본 보안목표명세서에는 보안목적을 TOE 및 운영환경에 대한 보안목적이 정의되어 있다. TOE에 대한 보안목적은 TOE에 의해 직접적으로 다루어지는 보안목적이고, 운영환경에 대한 보안목적은 TOE가 보안기능을 정확히 제공할 수 있도록 운영환경에서 지원하는 기술적/절차적 수단에 의해 다루어지는 보안목적이다.

## 4.1. TOE에 대한 보안목적

다음은 TOE에 의해 직접적으로 다루어지는 보안목적이다.

**O.감사기록**

TOE는 보안과 관련된 행동의 책임추적이 가능하도록 보안관련 사건을 기록하고 유지해야한다.

**O.암호지원**

TOE가 외부 개체와 통신하는 경우 안전한 암호화 및 복호화 알고리즘을 활용해야 한다.

**O.정보흐름통제**

TOE는 외부에서 내부로 또는 내부에서 외부로의 인가되지 않은 정보의 흐름을 통제해야 한다. 또한, 인가되지 않은 사용자에게 TSF 간 전송되는 정보가 유출되는 것을 방지해야 한다.

**O.잔여정보보호**

TOE는 TSF나 사용자 애플리케이션이 종료되면 해당 기능이 점유한 메모리에 남아있는 정보들을 모두 삭제함으로써 다른 사용자에게 주요 정보가 노출되는 것을 방지해야 한다.

**O.식별및인증**

TOE는 접근하는 사용자의 인가 여부 및 권한을 판별하여 보안 역할에 대한 TSF 접근 권한을 부여할 수 있어야 한다.

**O.가용성**

TOE는 TSF 기능 혹은 non-TSF 기능이 사용자의 요청에 대해 항상 응답할 수 있도록 보장하기 위해 CPU 기아현상 및 과도한 자원할당을 방지하여 가용성을 보장해야 한다.

**O.복구**

TOE는 이상 상황 혹은 고장 상황에서 안전한 상태를 유지하고 정상인 상태로 복구할 수 있는 기능을 지원해야 한다.

**O.무결성**

TOE는 TSF 및 TSF 데이터의 무결성을 검증하고 보장하기 위하여 자체 검사 기능을 지원해야 한다.

**O.기능관리**

TOE의 보안기능은 인가된 관리자에 의해서만 열람 및 운용될 수 있어야 한다.

## 4.2. 운영환경에 대한 보안목적

다음은 TOE가 보안 기능을 정확히 제공할 수 있도록 운영환경에서 지원하는 비기술적/절차적 수단에 의해 다루어지는 보안목적이다.

**OE.신뢰된 관리자**

TOE를 관리하는 인가된 관리자는 의도적으로 TOE 보안 기능을 우회하거나 데이터를 유출 혹은 훼손하지 않음을 입증하기 위해 보안 서약서나 동의서 등을 제출해야 한다.

**OE.신뢰된 애플리케이션**

TOE와 통신하는 사용자 어플리케이션은 악의적으로 개발되지 않아 커널 내 보안 기능을 우회하거나 영향을 끼칠 수 없다.

**OE.물리적 접근 제한**

TOE가 설치된 시스템은 관리자의 보안정책에 따라 제3자로부터 물리적 접근을 제한하여 기밀정보를 안전하게 보호한다. 또한 TOE가 설치되는 프로세서가 활용되기 이전에 제3자에 의한 접근이 없음을 입증하기 위한 홀로그램 스티커 혹은 물리적 조치가 필요하다.

## 4.3. 보안목적에 대한 이론적 근거

보안목적의 이론적 근거는 명세된 보안목적이 적합하고, 보안 문제를 다루기에 충분하며, 과도하지 않고 반드시 필요한 것임을 입증한다. 보안목적의 이론적 근거는 다음을 입증한다.

- 각 위협, 조직의 보안정책, 가정사항이 최소한 하나의 보안목적에 의해 다루어진다.
- 각 보안목적은 최소한 하나의 위협, 조직의 보안정책, 가정사항을 다룬다.

| 위협 | TOE 보안목적 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | O.<br>감사<br>기록 | O.<br>암호<br>지원 | O.<br>정보<br>흐름<br>통제 | O.<br>잔여<br>정보<br>보호 | O.<br>식별<br>및<br>인증 | O.<br>가용<br>성 | O.<br>복구 | O.<br>무결<br>성 | O.<br>기능<br>관리 |
| T.TSF 데이터 유출 | | | X | X | X | | | | X |
| T.TSF 데이터 훼손 | X | | X | | X | X | X | X | X |
| T.TSF 우회 | | | X | | X | X | | X | X |
| T.안전하지 않은 상태 | X | | | | | | X | X | X |
| T.서비스 거부 | X | | | | | X | | | X |
| P.암호화 | | X | | | | | | | |

[표 4] 보안문제정의와 보안목적 대응 (1)

| 위협 | 운영환경에 대한 보안목적 | | |
|---|---|---|---|
| | OE.신뢰된 관리자 | OE.신뢰된 애플리케이션 | OE.물리적 접근 제한 |
| T.TSF 데이터 유출 | | | X |
| T.인가되지 않은 접근 | | | X |
| P.신뢰된 관리자 | X | | |
| P.신뢰된 애플리케이션 | | X | |
| A.물리적 접근 제한 | | | X |

[표 5] 보안문제정의와 보안목적 대응 (2)

### 4.3.1. TOE 보안목적의 이론적 근거

| 위협 | TOE 보안목적 | 근거 |
|---|---|---|
| **T.TSF 데이터 유출**<br>TSF가 실행되기 위해 필요한 TSF 데이터 (시스템 설정 값, 스레드 큐, 스레드 실행 시간, 스레드 포인터 등)의 정보가 비인가된 방식으로 유출할 수 있음 | **O.정보흐름통제**<br>TOE는 외부에서 내부로 또는 내부에서 외부로의 인가되지 않은 정보의 유입을 통제해야 한다. 또한, 인가되지 않은 사용자에게 TSF 간 정보가 전송되는 것을 방지해야 한다. | TOE는 인가된 사용자 계정에만 정보의 유입이 허용된다. 이는 인가되지 않은 사용자에게 TOE 간 데이터가 유출되는 것을 방지한다. |
| | **O.잔여정보보호**<br>TOE는 TSF나 사용자 애플리케이션이 종료되면 해당 기능이 점유하고 메모리상의 정보를 모두 삭제하여 다른 사용자에게 노출되는 것을 방지해야 한다. | TOE는 애플리케이션 종료 시 메모리상의 정보를 모두 삭제한다. 이는 다른 사용자에게 TOE 데이터가 유출되는 것을 방지한다. |
| | **O.식별및인증**<br>TOE는 접근하는 사용자의 인가 여부 및 권한을 판별하여 보안 역할에 대한 TSF 접근 권한을 부여할 수 있어야 한다. | TOE는 사용자의 인가 여부 및 권한을 판별하여 접근 권한을 부여한다. 이는 정보가 비인가된 방식으로 유출되는 것을 방지한다. |
| | **O.기능관리**<br>TOE의 보안기능은 인가된 관리자에 의해서만 열람 및 운용되어야 한다. | TOE는 인가된 관리자에 의해서만 열람 및 운용된다. 이는 인가되지 않은 사용자에게 TOE 데이터가 유출되는 것을 방지한다. |
| **T.TSF 데이터 훼손**<br>TSF 데이터가 인가되지 않은 접근 방식으로 변조될 수 있음 | **O.감사기록**<br>TOE는 보안과 관련된 행동의 책임 추적이 가능하도록 보안관련 사건을 기록 및 유지해야한다. | TOE는 보안관련 사건을 기록 및 유지해야한다. 이는 공격자와 공격 방법 대한 정보를 기록하여, 다음 공격을 방지할 수 있다. |

| | | |
|---|---|---|
| | | |
| | **O.정보흐름통제**<br>TOE는 외부에서 내부로 또는 내부에서 외부로의 인가되지 않은 정보의 유입을 통제해야 한다. 또한, 인가되지 않은 사용자에게 TSF 간 정보가 전송되는 것을 방지해야 한다 | TOE는 인가된 사용자 계정에만 정보의 유입이 허용된다. 이는 인가되지 않은 사용자가 TOE에 접근하여 데이터를 훼손되는 것을 방지한다. |
| | **O.식별및인증**<br>TOE는 접근하는 사용자의 인가 여부 및 권한을 판별하여 보안 역할에 대한 TSF 접근 권한을 부여할 수 있어야 한다. | TOE는 사용자의 인가 여부 및 권한을 판별하여 접근 권한을 부여한다. 이는 인가되지 않은 사용자가 TOE에 접근하여 데이터를 훼손하는 것을 방지한다. |
| | **O.가용성**<br>TOE는 TSF 기능 혹은 non-TSF 기능이 사용자의 요청에 대해 항상 응답할 수 있도록 보장하기 위해 CPU 기아현상 및 과도한 자원할당을 방지하여 가용성을 보장해야 한다. | TOE는 과도한 자원할당을 방지하기 위해 자원 할당 이전에 해당 자원의 잔여량을 점검하는 기능을 지원한다. 이는 인가되지 않은 사용자에게 TSF가 우회되더라도 가용성을 확보할 수 있다. |
| | **O.복구**<br>TOE는 이상 상황 혹은 고장 상황에서 안전한 상태를 유지하고 정상인 상태로 복구할 수 있는 기능을 지원해야 한다. | TOE는 이상 상황 혹은 고장 상황에서 정상인 상태로 복구할 수 있는 기능을 지원한다. 이는 인가되지 않은 사용자에게 TOE 데이터가 변조되더라도 정상인 상태로 복구할 수 있다. |
| | **O.무결성**<br>TOE는 TSF 및 TSF 데이터의 무결성을 검증 및 보장하기 위해 자체 검사 기능을 지원한다. | TOE는 데이터의 무결성을 검증 및 보장하기 위해 자체 검사 기능을 지원한다. 이는 인가되지 않은 사용자에 의해 TOE 데이터가 변조되더라도 무결성 검사를 통해 변조된 데이터를 확인할 수 있다. |
| | **O.기능관리**<br>TOE의 보안기능은 인가된 관리자에 의해서만 열람 및 운용되어야 한다. | TOE는 인가된 관리자에 의해서만 열람 및 운용된다. 이는 인가되지 않은 사용자에게 TOE 데이터가 노출되어 변조되는 것을 방지한다. |
| **T.TSF 우회**<br>TSF 데이터가 변조되어 TSF가 우회될 수 있음 | **O.정보흐름통제**<br>TOE는 외부에서 내부로 또는 내부에서 외부로의 인가되지 않은 정보의 유입을 통제해야 한다. 또한, 인 | TOE는 인가된 사용자 계정에만 정보의 유입이 허용된다. 이는 TOE 데이터가 변조되어 TOE가 우회되는 것을 방지한다. |

| | | |
|---|---|---|
| | 가되지 않은 사용자에게 TSF 간 정보가 전송되는 것을 방지해야 한다. | |
| | **O.식별및인증**<br>TOE는 접근하는 사용자의 인가 여부 및 권한을 판별하여 보안 역할에 대한 TSF 접근 권한을 부여할 수 있어야 한다. | TOE는 사용자의 인가 여부 및 권한을 판별하여 접근 권한을 부여한다. 이는 TOE 데이터가 변조되어 TOE가 우회되는 것을 방지한다. |
| | **O.가용성**<br>TOE는 TSF 기능 혹은 non-TSF 기능이 사용자의 요청에 대해 항상 응답할 수 있도록 보장하기 위해 CPU 기아현상 및 과도한 자원할당을 방지하여 가용성을 보장해야 한다. | TOE는 과도한 자원할당을 방지하기 위해 자원 할당 이전에 해당 자원의 잔여량을 점검하는 기능을 지원한다. 이는 인가되지 않은 사용자에게 TSF가 우회되더라도 가용성을 확보할 수 있다. |
| | **O.무결성**<br>TOE는 TSF 및 TSF 데이터의 무결성을 검증 및 보장하기 위해 자체 검사 기능을 지원한다. | TOE는 데이터의 무결성을 검증 및 보장하기 위해 자체 검사 기능을 지원한다. 이는 인가되지 않은 사용자에 의해 TOE 데이터가 변조되더라도 무결성 검사를 통해 변조된 데이터를 확인하여 TOE가 우회되는 것을 방지한다. |
| | **O.기능관리**<br>TOE의 보안기능은 인가된 관리자에 의해서만 열람 및 운용되어야 한다. | TOE는 인가된 관리자에 의해서만 열람 및 운용된다. 이는 인가되지 않은 사용자에게 TOE 데이터가 변조되어 TOE가 우회되는 것을 방지한다. |
| **T.안전하지 않은 상태**<br>잘못된 설정 값이 탑재되어 TOE가 불안전한 상태에 빠짐 | **O.감사기록**<br>TOE는 보안과 관련된 행동의 책임 추적이 가능하도록 보안관련 사건을 기록 및 유지해야한다. | TOE는 보안관련 사건을 기록 및 유지해야한다. 이는 공격자와 공격 방법 대한 정보를 기록하여, 다음 공격을 방지할 수 있다. |
| | **O.복구**<br>TOE는 이상 상황 혹은 고장 상황에서 안전한 상태를 유지하고 정상인 상태로 복구할 수 있는 기능을 지원해야 한다. | TOE는 이상 상황 혹은 고장 상황에서 정상인 상태로 복구할 수 있는 기능을 지원한다. 이는 잘못된 설정 값이 탑재되어 TOE가 불안전한 상태에 빠지더라도 정상인 상태로 복구할 수 있다. |
| | **O.무결성**<br>TOE는 TSF 및 TSF 데이터의 무결성을 검증 및 보장하기 위해 자체 검사 기능을 지원한다. | TOE는 데이터의 무결성을 검증 및 보장하기 위해 자체 검사 기능을 지원한다. 이는 TOE 데이터에 잘못된 설정 값이 탑재되더라도 무결성 검사를 통해 잘못된 설정 값을 확 |

| | | |
|---|---|---|
| | | 인하여 TOE가 불안전한 상태에 빠지는 것을 방지한다. |
| | **O.기능관리**<br>TOE의 보안기능은 인가된 관리자에 의해서만 열람 및 운용되어야 한다. | TOE는 인가된 관리자에 의해서만 열람 및 운용된다. 이는 인가되지 않은 사용자가 잘못된 설정 값을 탑재하여 TOE가 불안전한 상태에 빠지는 것을 방지한다. |
| **T.서비스 거부**<br>TSF 데이터 변조 또는 TOE에 대한 무분별한 작업 요청으로 인해 TOE 객체에 접근할 수 없음 | **O.감사기록**<br>TOE는 보안과 관련된 행동의 책임 추적이 가능하도록 보안관련 사건을 기록 및 유지해야한다. | TOE는 보안관련 사건을 기록 및 유지해야한다. 이는 공격자와 공격 방법 대한 정보를 기록하여, 다음 공격을 방지할 수 있다. |
| | **O.가용성**<br>TOE는 TSF 기능 혹은 non-TSF 기능이 사용자의 요청에 대해 항상 응답할 수 있도록 보장하기 위해 CPU 기아현상 및 과도한 자원할당을 방지하여 가용성을 보장해야 한다. | TOE는 CPU 기아현상 및 과도한 자원할당을 방지하여 TSF 기능 혹은 non-TSF 기능이 사용자의 요청에 대해 항상 응답할 수 있도록 보장해야한다. 이는 TOE 데이터 변조 또는 TOE에 대한 무분별한 작업 요청으로 인해 TOE 객체에 접근 불가한 상황을 방지한다. |
| | **O.기능관리**<br>TOE의 보안기능은 인가된 관리자에 의해서만 열람 및 운용되어야 한다. | TOE는 인가된 관리자에 의해서만 열람 및 운용된다. 이는 인가되지 않은 사용자가 TOE 데이터 변조 또는 TOE에 대한 무분별한 작업 요청으로 인해 TOE 객체에 접근 불가한 상황을 방지한다. |
| **P.암호화**<br>TOE는 외부 개체와 통신할 때 NSA(National Security Agency), KISA(Korea Internet & Security Agency) 등과 같은 전문기관에서 권고하는 암호화 알고리즘을 활용하여 데이터를 전송한다. | **O.암호지원**<br>TOE는 외부 개체와 통신하는 경우 안전한 암호화 및 복호화 알고리즘을 활용해야 한다. | TOE는 외부 개체와 통신하는 경우 안전한 암호화 및 복호화 알고리즘을 활용해야 한다. 이는 인가되지 않은 사용자가 TOE에 접근하는 것을 방지한다. |

[표 6] 보안문제정의와 보안목적 대응 (1)

# 5. 확장 컴포넌트 정의

본 보안목표명세서에는 공통평가기준 2부 또는 3부에서 확장한 컴포넌트가 존재하지 않는다.

# 6. 보안요구사항

이 장은 TOE의 보안기능요구사항 및 보증요구사항을 서술한다. 보안기능 요구사항은 부록4에서 제시하는 각 세부 공격 리프노드를 통한 공격 성공 가능성을 제거함으로써 완화해야 한다. 해당 부분에 대한 상세 내용은 <부록E. 보안기능 요구사항 도출>을 참고한다.

## 6.1. 보안기능요구사항

본 보안목표명세서에서 정의된 보안기능요구사항은 앞장에서 식별한 보안목적을 만족시키기 위하여 공통평가기준 2부로부터 관련 기능 컴포넌트를 선정하여 표현하였다. 다음의 표는 본 보안목표명세서에서 사용하는 보안기능컴포넌트를 요약하여 보여준다.

| 번호 | 보안기능 클래스 | 보안기능컴포넌트 |
|---|---|---|
| 1 | 보안감사 (FAU) | FAU_GEN.1 감사 데이터 생성 |
| 2 | | FAU_STG.1 감사 증적 저장소 보호 |
| 3 | | FAU_STG.3 감사 데이터 손실 예측 시 대응 행동 |
| 4 | | FAU_STG.4 감사 데이터의 손실 방지 |
| 5 | 사용자데이터 보호 (FDP) | FDP_IFC.1 부분적인 정보흐름통제 |
| 6 | | FDP_IFF.1 단일 계층 보안속성 |
| 7 | | FDP_RIP.1 부분적인 잔여정보 보호 |
| 8 | 식별 및 인증(FIA) | FIA_UAU.1 인증 |
| 9 | | FIA_UID.1 식별 |
| 10 | 보안관리 (FMT) | FMT_MOF.1 TSF 기능 관리 |
| 11 | | FMT_MSA.1 보안속성 관리 |
| 12 | | FMT_MSA.3 정적 속성 초기화 |
| 13 | | FMT_MTD.1 TSF 데이터 관리 |
| 14 | | FMT_SMF.1 관리기능명세 |
| 15 | | FMT_SMR.1 보안 역할 |
| 16 | TSF 보호 (FPT) | FPT_FLS.1 안전한 상태 유지 |
| 17 | | FPT_RCV.1 수동 복구 |
| 18 | | FPT_TST.1 TSF 자체 시험 |
| 19 | 자원 활용(FRU) | FRU_PRS.1 자원사용 우선순위 : 부분적용 |
| 20 | | FRU_RSA.1 최대 할당치 |

[표 7] 보안기능 요구사항

### 6.1.1. 보안감사(FAU)

**FAU_GEN.1 감사 데이터 생성**

계층관계 : 없음

종속관계 : FPT_STM.1 신뢰할 수 있는 타임스탬프

FAU_GEN.1.1 TSF는 다음과 같은 감사대상 사건들의 감사 레코드를 생성할 수 있어야 한다.

a) 감사 기능의 시동(start-up)과 종료(shut-down)

b) 지정되지 않음 감사수준에 따른 모든 감사대상 사건

c) [ 표 6 감사대상 사건 참조 ]

FAU_GEN.1.2 TSF는 최소한 다음 정보를 각 감사 레코드 내에 기록해야 한다.

a) 사건 일시, 사건 유형, 주체의 신원(가능한 경우), 사건 결과 (성공 또는 실패)

b) 각 감사 사건 유형에 대하여, 보호프로파일/보안목표명세서에 포함된 기능 컴포넌트의 감사대상 사건 정의에 기반한 [표 6 감사대상 사건 참조, 기타 감사 관련 정보]

| 번호 | 컴포넌트 | 감사대상사건 | 추가적인 감사기록내용 |
|---|---|---|---|
| 1 | FAU_GEN.1 | - | - |
| 2 | FAU_STG.1 | - | - |
| 3 | FAU_STG.3 | - | - |
| 4 | FAU_STG.4 | - | - |
| 5 | FDP_IFC.1 | 없음 | - |
| 6 | FDP_IFF.1 | 오퍼레이션 거부 | 객체 및 주체 Capability |
| 7 | FDP_RIP.1 | 없음 | - |
| 8 | FIA_UAU.1 | | |
| 9 | FIA_UID.1 | | |
| 10 | FMT_MOF.1 | TSF 기능에 대한 모든 변경 | - |
| 11 | FMT_MSA.1 | TSF 기능에 대한 모든 변경 | - |
| 12 | FMT_MSA.3 | TSF 기능에 대한 모든 변경 | - |
| 13 | FMT_MTD.1 | TSF 기능에 대한 모든 변경 | - |
| 14 | FMT_SMF.1 | TSF 기능에 대한 모든 변경 | - |
| 15 | FMT_SMR.1 | TSF 기능에 대한 모든 변경 | - |
| 16 | FPT_FLS.1 | 안전한 상태로 유지하기 위한 기능의 원인 | 기능 작동 원인 |
| 17 | FPT_RCV.1 | 관리 모드 전환 시 | - |
| 18 | FPT_TST.1 | TSF 데이터 무결성 검사 이상 시 | 이상 데이터 해시 값 |
| 19 | FRU_PRS.1 | 우선순위 미준수 주체 혹은 TSF | 미준수 주체 혹은 TSF 정보 |
| 20 | FRU_RSA.1 | 지정한 메모리 한도 이상 점유 시<br>지정한 CPU 점유 시간 초과 시 | - |

[표 8] 감사대상 사건

**FAU_STG.1 감사 증적 저장소 보호**

계층관계 : 없음

종속관계 : FAU_GEN.1 감사 데이터 생성

FAU_STG.1.1 TSF는 인가되지 않은 삭제로부터 감사 증적 내에 저장된 감사 레코드를 보호해야 한다.

FAU_STG.1.2 TSF는 감사 증적 내에 저장된 감사 레코드에 대한 비인가된 변경을 방지해야 한다.

**FAU_STG.3 감사 데이터 손실 예측 시 대응 행동**

계층관계 : 없음

종속관계 : FAU_STG.1 감사 증적 저장소 보호

FAU_STG.3.1 TSF는 감사 증적이 [ 감사 레코드 용량의 85% ]를 초과할 경우 [ 가장 오래된 감사 레코드 덮어쓰기 ]를 취해야 한다.

**FAU_STG.4 감사 데이터의 손실 방지**

계층관계 : FAU_STG.3 감사 데이터 손실 예측 시 대응 행동

종속관계 : FAU_STG.1 감사 증적 저장소 보호

FAU_STG.4.1 TSF는 감사 증적이 포화인 경우, TSF는 가장 오래된 감사 레코드 덮어쓰기 및 [ 없음 ]을 수행해야 한다.

### 6.1.2. 사용자데이터보호(FDP)

**FDP_IFC.1 부분적인 정보흐름통제**

계층관계 : 없음

종속관계 : FDP_IFF.1 단일 계층 보안속성

FDP_IFC.1.1 TSF는 [ 다음의 주체, 정보, 오퍼레이션 목록 ]에 대하여 [ CHAOS Information Flow Control Policy ]를 강제해야 한다.

a) 주체 : TSF Process, User Process

b) 정보 : TSF 설정 데이터, 메모리 주소, 인터럽트 플래그

c) 오퍼레이션

- User Process의 메모리 요청
- User Process의 인터럽트 요청
- TSF Process의 TSF 데이터 변경, 열람, 삭제 요청 및 그 응답

**FDP_IFF.1 단일 계층 보안속성**

계층관계 : 없음

종속관계 : FDP_IFC.1 부분적인 정보흐름통제 FMT_MSA.3 정적 속성 초기화

FDP_IFF.1.1 TSF는 적어도 [ 다음의 SFP에서 통제되는 주체와 정보의 목록, 주체와 정보 각각에 대한 보안속성 ]과 같은 주체 보안속성 및 정보 보안속성 유형에 기반하여 [ CHAOS Information Flow Control Policy ]를 강제해야 한다.

a) 주체 보안속성 : Process Priority, Capability Level

b) 정보 보안속성 : Endpoint, Notification, Page, Capability Level

FDP_IFF.1.2 TSF는 다음과 같은 규칙이 유지되면 통제된 오퍼레이션을 통하여 통제된 주체와 통제된 정보 간의 정보흐름을 허용해야 한다 : [다음 각 오퍼레이션에 대하여 주체와 정보 보안속성 간에서 유지되어야 하는 보안속성에 기반한 관계]

[

a) 주체(Thread)가 특정 메모리 주소에 접근하고자 요청하여 정보를 전송할 시에 주체의 보안속성(Capability)과 인가된 관리자가 정의한 정보흐름통제 보안정책의 속성(Capability)을 비교하여, 그 정보흐름에 대한 처리 방법이 '허용'으로 지정되어 있으면 요청된 정보흐름을 허용해야 한다.

b) 한 주체가 접근하고 있는 메모리에 다른 주체가 접근하고자 할 때, 두 주체의 보안속성(Priority)를 비교하여 상대적으로 우위에 있는 주체와의 정보흐름을 우선시해야 한다.

c) b)에서 정보흐름을 교체해야 하는 경우에 인가된 관리자가 정의한 정보흐름(인터럽트 플래그)을 발생시켜서 정보흐름의 교체를 허용해야 한다.

]

FDP_IFF.1.3 TSF는 [ 없음 ]을 강제해야 한다.

FDP_IFF.1.4 TSF는 [ 없음 ]에 기반하여 정보흐름을 명시적으로 인가해야 한다.

FDP_IFF.1.5 TSF는 [ 없음 ]에 기반하여 정보흐름을 명시적으로 거부해야 한다.

**FDP_RIP.1 부분적인 잔여정보 보호**

계층관계 : 없음

종속관계 : 없음

FDP_RIP.1.1 TSF는 다음의 객체 [인가된 일반 사용자가 사용하는 사용자 애플리케이션]으로부터 자원을 회수하는 경우에 자원의 모든 이전 정보 내용이 가용하지 않음을 보장해야 한다.

### 6.1.3. 식별 및 인증(FIA)

**FIA_UAU.1 인증**

계층관계 : 없음

종속관계 : FIA_UID.1 식별

FIA_UAU.1.1 TSF는 사용자가 인증되기 전에 사용자를 대신하여 수행될 [ 식별 및 인증 절차 ]을 허용해야 한다.

FIA_UAU.1.2 TSF는 FIA_UAU.1.1에서 명시된 행동 이외의 사용자를 대신하여 TSF가 중재하는 다른 모든 행동을 허용하기 전에 사용자를 성공적으로 인증해야 한다.

**FIA_UID.1 식별**

계층관계 : 없음

종속관계 : 없음

FIA_UID.1.1 TSF는 사용자를 식별하기 전에 사용자를 대신하여 수행될 [식별 및 인증 절차]을 허용해야 한다.

FIA_UID.1.2 TSF는 FIA_UID.1.1에서 명시된 행동 이외의 사용자를 대신하여 TSF가 중재하는 다른

모든 행동을 허용하기 전에 각 사용자를 성공적으로 식별해야 한다.

### 6.1.4. 보안관리(FMT)

**FMT_MOF.1 보안기능 관리**

계층관계 : 없음

종속관계 : FMT_SMF.1 관리기능명세 FMT_SMR.1 보안 역할

FMT_MOF.1.1 TSF는 [다음 표 7의 보안기능 목록]의 기능에 대해 행동을결정, 중지, 개시, 행동을 변경하는 능력을 [인가된 관리자]로 제한해야 한다.

| 보안 기능 | 능력 | | | |
|---|---|---|---|---|
| | 행동을 결정 | 중지 | 개시 | 행동을 변경 |
| 감사데이터 생성 / 저장 | O | O | O | O |
| 정보흐름통제 정책(기능) | O | - | O | O |
| 잔여 정보보호 | - | - | O | - |
| 식별 및 인증 | O | - | O | O |
| 보안기능 설정 | O | O | O | O |
| 보안기능 데이터 관리 | O | - | O | O |
| TOE 복구 | - | - | O | - |
| TOE 재기동 | - | - | O | - |
| 무결성 검사 | - | - | O | - |
| 자원 할당 | - | - | O | - |

범례: - 미지원, O 지원

[표 9] 보안기능 목록

**FMT_MSA.1 보안속성 관리**

계층관계 : 없음

종속관계 : [FDP_ACC.1 부분적인 접근통제 또는 FDP_IFC.1 부분적인 정보흐름통제]
FMT_SMF.1 관리기능명세 FMT_SMR.1 보안 역할

FMT_MSA.1.1 TSF는 [다음 표 0 보안속성 관리 능력]의 보안속성을 디폴트값변경, 질의, 변경, 삭제하는 능력을 [인가된 관리자]로 제한하도록 [ CHAOS Information Flow Control Policy ]를 강제해야 한다.

| 보안속성 | | 능력 | | | |
|---|---|---|---|---|---|
| | | 디폴트값 변경 | 질의 | 변경 | 삭제 |
| 주체 | Priority | O | O | O | - |
| | Capability Level | O | O | O | O |
| 정보 | Endpoint | - | O | - | - |
| | Notification | - | O | - | - |
| | Page | O | O | O | O |
| | Capability Level | O | O | O | O |

범례: - 미지원, O 지원

[표 10] 보안 속성 관리 능력

**FMT_MSA.3 정적 속성 초기화**

계층관계 : 없음

종속관계 : FMT_MSA.1 보안속성 관리 FMT_SMR.1 보안 역할

FMT_MSA.3.1 TSF는 SFP를 강제하기 위하여 사용되는 보안속성의 제한적인 디폴트값을 제공하도록 [ CHAOS Information Flow Control Policy ]를 강제해야 한다.

FMT_MSA.3.2 TSF는 객체나 정보 생성 시 디폴트값을 대체하기 위하여 [ 인가된 관리자 ]가 선택적인 초기값을 명세하도록 허용해야 한다.

**FMT_MTD.1 TSF 데이터 관리**

계층관계 : 없음

종속관계 : FMT_SMF.1 관리기능명세 FMT_SMR.1 보안 역할

FMT_MTD.1.1 TSF는 [다음 표 8 TSF 데이터 목록 및 관리 능력]을 디폴트값변경, 질의, 변경, 삭제, [추가]하는 능력을 [ 인가된 관리자 ]로 제한해야 한다.

| TSF 데이터 | 능력 | | | |
|---|---|---|---|---|
| | 디폴트값 변경 | 질의 | 변경 | 삭제 |
| 감사 데이터 | - | - | - | - |
| 무결성 점검 데이터 | - | O | O | - |
| 환경 설정 : 시간 | - | O | O | - |
| 관리 대상 TOE 정보 | - | O | - | - |
| 암호화 설정값 | O | O | O | O |
| 자원 할당 최대치 | O | O | O | - |
| 사용자 인증 데이터 | - | O | O | O |

범례: - 미지원, O 지원

[표 11] TSF 데이터 목록 및 관리 능력

**FMT_SMF.1 관리기능명세**

계층관계 : 없음

종속관계 : 없음

FMT_SMF.1.1 TSF는 다음의 관리 기능을 수행할 수 있어야 한다: [FMT_MOF.1의 보안기능 목록, FMT_MSA.1의 보안속성 목록, FMT_MSA.3의 정적 속성 초기화 목록, FMT_MTD.1의 TSF 데이터 목록 및 관리 능력]

**FMT_SMR.1 보안 역할**

계층관계 : 없음

종속관계 : FIA_UID.1 식별

FMT_SMR.1.1 TSF는 [다음 표 12의 사용자 보안 역할] 역할을 유지해야 한다.

FMT_SMR.1.2 TSF는 사용자와 역할을 연관 지을 수 있어야 한다.

| 역할 | 설명 |
|---|---|
| 인가된 관리자 | 모든 보안 기능의 설정값, 기능 관리 권한 및 감사기록에 대한 접근 권한을 가진 관리자 |
| 인가된 일반 사용자 | 보안 기능에 대한 설정은 제한되고 오직 TOE를 이용하여 사용자 애플리케이션을 실행할 수 있는 일반 사용자 |

[표 12] 사용자 보안 역할

### 6.1.5. TSF 보호(FPT)

**FPT_FLS.1 장애 시 안전한 상태 유지**

계층관계 : 없음

종속관계 : 없음

FPT_FLS.1.1 TSF는 다음과 같은 유형의 장애가 발생한 경우 안전한 상태를 유지해야 한다 :

**FPT_RCV.1 수동 복구**

계층관계 : 없음

종속관계 : AGD_OPE.1 사용자 운영 설명서

FPT_RCV.1.1 [할당 : 장애/서비스 불연속 목록] 이후, TSF는 TOE를 안전한 상태로 돌아가게 하는 기능이 제공되는 관리 모드가 되어야 한다.

**FPT_TST.1 TSF 자체 시험**

계층관계 : 없음

종속관계 : 없음

FPT_TST.1.1 TSF는 TSF의 정확한 운영을 입증하기 위하여 시동시, 정규 운영 동안 주기적으로, 인가된 사용자 요구 시, [관리자의 보안기능 수정 후]조건시 자체 시험을 실행해야 한다.
FPT_TST.1.2 TSF는 인가된 사용자에게 TSF 데이터의 무결성을 검증하는 기능을 제공해야 한다.
FPT_TST.1.3 TSF는 인가된 사용자에게 TSF의 무결성을 검증하는 기능을 제공해야 한다.

### 6.1.6. 자원 활용(FRU)

**FRU_PRS.1 자원사용 우선순위 : 부분적용**

계층관계 : 없음

종속관계 : 없음

FRU_PRS.1.1 TSF는 TSF 내의 각 주체에게 우선순위를 할당해야 한다.
FRU_PRS.1.2 TSF는 [주체가 접근하는 메모리의 범위, 객체가 점유하는 메모리 용량, 주체의 CPU 점유 시간]에 대한 각 접근이 주체에 할당된 우선순위에 기반하여 중재되어야 함을 보장해야 한다.

**FRU_RSA.1 최대 할당치**

계층관계 : 없음

종속관계 : 없음

FRU_RSA.1.1 TSF는 주체가 명세된기간동안 사용할 수 있는 다음의 자원 [주체가 접근하는 메모리의 범위, 객체가 점유하는 메모리 용량, 주체의 CPU 점유 시간]의 최대 할당치를 강제해야 한다.

## 6.2. 보증요구사항

본 보안목표명세서의 보증요구사항은 공통평가기준 3부의 보증 컴포넌트로 구성되었고, 평가보증등급은 EAL6이다. 다음 표는 보증 컴포넌트를 요약하여 보여준다.

| 보증 클래스 | 보증 컴포넌트 |
|---|---|
| 개발 | ADV_ARC.1 보안 구조 설명 |
| | ADV_FSP.5 추가적인 오류 정보를 제공하는 준정형화된 완전한 기능명세 |
| | ADV_IMP.2 완전히 대응되는 TSF에 대한 구현의 표현 |
| | ADV_INT.3 최소화된 복잡도를 갖는 TSF 내부 |
| | ADV_SPM.1 정형화된 TOE 보안정책모델 |
| | ADV_TDS.5 완전한 준정형화된 모듈화 설계 |
| 설명서 | AGD_OPE.1 사용자 운영 설명서 |
| | AGD_PRE.1 준비 절차 |
| 생명주기 지원 | ALC_CMC.5 고급 지원 |
| | ALC_CMS.5 개발도구 형상관리 범위 |
| | ALC_DEL.1 배포 절차 |
| | ALC_DVS.2 보안정책의 충분함 |
| | ALC_LCD.1 개발자가 정의한 생명주기 모델 |
| | ALC_TAT.3 모든 부분에서 적용된 구현표준 |
| 보안목표명세서 | ASE_CCL.1 준수 선언 |
| | ASE_ECD.1 확장 컴포넌트 정의 |
| | ASE_INT.1 보안목표명세서 소개 |
| | ASE_OBJ.2 보안목적 |
| | ASE_REQ.2 도출된 보안요구사항 |
| | ASE_SPD.1 보안문제정의 |
| | ASE_TSS.1 TOE 요약명세 |
| 시험 | ATE_COV.3 시험범위의 엄밀한 분석 |
| | ATE_DPT.3 모듈 설계 시험 |
| | ATE_FUN.2 순서화된 기능 시험 |
| | ATE_IND.2 독립적인 시험 : 표본 시험 |
| 취약성 평가 | AVA_VAN.5 고도의 체계적인 취약성 분석 |

[표 13] 보증요구사항

### 6.2.1. 보안목표명세서

**ASE_CCL.1 준수 선언**

종속관계: ASE_INT.1 보안목표명세서 소개
ASE_ECD.1 확장 컴포넌트 정의
ASE_REQ.1 명시된 보안요구사항

개발자 요구사항

ASE_CCL.1.1D 개발자는 준수 선언을 제공해야 한다.

ASE_CCL.1.2D 개발자는 준수 선언의 이론적 근거를 제공해야 한다.

증거 요구사항

ASE_CCL.1.1C 준수 선언은 보안목표명세서 및 TOE가 준수하는 공통평가기준의 버전을 식별하기 위해 공통평가기준 준수 선언을 포함해야 한다.

ASE_CCL.1.2C 공통평가기준 준수 선언은 보안목표명세서의 공통평가기준 2부에 대한 준수 선언을 '2부 준수' 또는 '2부 확장'으로 서술해야 한다.

ASE_CCL.1.3C 공통평가기준 준수 선언은 보안목표명세서의 공통평가기준 3부에 대한 준수 선언을 '3부 준수' 또는 '3부 확장'으로 서술해야 한다.

ASE_CCL.1.4C 공통평가기준 준수 선언은 확장 컴포넌트 정의와 일관성이 있어야 한다.

ASE_CCL.1.5C 준수 선언은 보안목표명세서가 준수하는 모든 보호프로파일 및 보안요구사항 패키지를 식별해야 한다.

ASE_CCL.1.6C 준수 선언은 보안목표명세서의 패키지에 대한 준수 선언을 '패키지 준수' 또는 '패키지 추가'로 서술해야 한다.

ASE_CCL.1.7C 준수 선언의 이론적 근거는 보안목표명세서의 TOE 유형이 그 보안목표명세서가 준수하는 보호프로파일의 TOE 유형과 일관성이 있음을 입증해야 한다.

ASE_CCL.1.8C 준수 선언의 이론적 근거는 보안목표명세서의 보안문제정의에 대한 설명이 그 보안목표명세서가 준수하는 보호프로파일의 보안문제정의 설명과 일관성이 있음을 입증해야 한다.

ASE_CCL.1.9C 준수 선언의 이론적 근거는 보안목표명세서의 보안목적에 대한 설명이 그 보안목표명세서가 준수하는 보호프로파일의 보안목적 설명과 일관성이 있음을 입증해야 한다.

ASE_CCL.1.10C 준수 선언의 이론적 근거는 보안목표명세서의 보안요구사항에 대한 설명이 그 보안목표명세서가 준수하는 보호프로파일의 보안요구사항 설명과 일관성이 있음을 입증해야 한다.

평가자 요구사항

ASE_CCL.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### ASE_ECD.1 확장 컴포넌트 정의

종속관계 : 없음

개발자 요구사항

ASE_ECD.1.1D 개발자는 보안요구사항에 대한 설명을 제공해야 한다.

ASE_ECD.1.2D 개발자는 확장 컴포넌트 정의를 제공해야 한다.

증거 요구사항

ASE_ECD.1.1C 보안요구사항에 대한 설명은 확장된 모든 보안요구사항을 식별해야 한다.

ASE_ECD.1.2C 확장 컴포넌트 정의는 각각 확장된 보안요구사항에 대한 확장 컴포넌트를 정의해야 한다.

ASE_ECD.1.3C 확장 컴포넌트 정의는 각 확장 컴포넌트가 기존의 공통평가기준 컴포넌트, 패밀리, 클래스와 어떻게 연관되는지를 서술해야 한다.

ASE_ECD.1.4C 확장 컴포넌트 정의는 기존의 공통평가기준 컴포넌트, 패밀리, 클래스와 방법론을 모델로 하여 표현해야 한다.
ASE_ECD.1.5C 확장 컴포넌트는 각 엘리먼트에 대한 준수 여부를 입증할 수 있도록 측정 가능하고 객관적인 엘리먼트로 구성되어야 한다.

평가자 요구사항
ASE_ECD.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ASE_ECD.1.2E 평가자는 확장된 컴포넌트가 기존의 컴포넌트를 이용하여 명확히 표현할 수 없음을 확인해야 한다.

**ASE_INT.1 보안목표명세서 소개**

종속관계 : 없음

개발자 요구사항
ASE_INT.1.1D 개발자는 보안목표명세서 소개를 제공해야 한다.

증거 요구사항
ASE_INT.1.1C 보안목표명세서 소개는 보안목표명세서 참조, TOE 참조, TOE 개요, TOE 설명을 포함해야 한다.
ASE_INT.1.2C 보안목표명세서 참조는 유일하게 보안목표명세서를 식별해야 한다.
ASE_INT.1.3C TOE 참조는 TOE를 식별해야 한다.
ASE_INT.1.4C TOE 개요는 TOE의 용도와 주요 보안 특성을 요약해야 한다.
ASE_INT.1.5C TOE 개요는 TOE 유형을 식별해야 한다.
ASE_INT.1.6C TOE 개요는 TOE에서 요구되는 비-TOE에 해당하는 하드웨어/소프트웨어/펌웨어를 식별해야 한다.
ASE_INT.1.7C TOE 설명은 TOE의 물리적인 범위를 서술해야 한다.
ASE_INT.1.8C TOE 설명은 TOE의 논리적인 범위를 서술해야 한다.

평가자 요구사항
ASE_INT.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ASE_INT.1.2E 평가자는 TOE 참조, TOE 개요, TOE 설명이 서로 일관성이 있음을 확인해야 한다.

**ASE_OBJ.2 보안목적**

종속관계: ASE_SPD.1 보안문제정의

개발자 요구사항
ASE_OBJ.2.1D 개발자는 보안목적에 대한 설명을 제공해야 한다.
ASE_OBJ.2.2D 개발자는 보안목적의 이론적 근거를 제공해야 한다.

증거 요구사항
ASE_OBJ.2.1C 보안목적에 대한 설명은 TOE에 대한 보안목적과 운영환경에 대한 보안목적을 서술해야 한다.

ASE_OBJ.2.2C 보안목적의 이론적 근거는 TOE에 대한 각 보안목적을 보안목적에 의해 대응되는 위협과 보안목적에 의해 수행되는 조직의 보안정책으로 추적해야 한다.
ASE_OBJ.2.3C 보안목적의 이론적 근거는 운영환경에 대한 각 보안목적을 보안목적에 의해 대응되는 위협, 보안목적에 의해 수행되는 조직의 보안정책, 보안목적에 의해 지원되는 가정사항으로 추적해야 한다.
ASE_OBJ.2.4C 보안목적의 이론적 근거는 보안목적이 모든 위협에 대응함을 입증해야 한다.
ASE_OBJ.2.5C 보안목적의 이론적 근거는 보안목적이 모든 조직의 보안정책을 수행함을 입증해야 한다.
ASE_OBJ.2.6C 보안목적의 이론적 근거는 운영환경에 대한 보안목적이 모든 가정사항을 지원함을 입증해야 한다.

평가자 요구사항
ASE_OBJ.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

**ASE_REQ.2 도출된 보안요구사항**

종속관계: ASE_OBJ.2 보안목적
ASE_ECD.1 확장 컴포넌트 정의

개발자 요구사항
ASE_REQ.2.1D 개발자는 보안요구사항에 대한 설명을 제공해야 한다.
ASE_REQ.2.2D 개발자는 보안요구사항의 이론적 근거를 제공해야 한다.

증거 요구사항
ASE_REQ.2.1C 보안요구사항에 대한 설명은 보안기능요구사항과 보증요구사항을 서술해야 한다.
ASE_REQ.2.2C 보안기능요구사항 및 보증요구사항에서 사용되는 모든 주체, 객체, 오퍼레이션, 보안속성, 외부 실체, 기타 조건들은 정의되어야 한다.
ASE_REQ.2.3C 보안요구사항에 대한 설명은 보안요구사항에 대한 모든 오퍼레이션을 식별해야 한다.
ASE_REQ.2.4C 모든 오퍼레이션은 정확히 수행되어야 한다.
ASE_REQ.2.5C 보안요구사항의 각 종속관계는 만족되어야 하며, 그렇지 않을 경우에는 보안요구사항의 이론적 근거에 그에 대한 정당화가 제공되어야 한다.
ASE_REQ.2.6C 보안요구사항의 이론적 근거는 각 보안기능요구사항을 TOE에 대한 보안목적으로 추적해야 한다.
ASE_REQ.2.7C 보안요구사항의 이론적 근거는 보안기능요구사항이 TOE에 대한 모든 보안목적을 만족한다는 것을 입증해야 한다.
ASE_REQ.2.8C 보안요구사항의 이론적 근거는 보증요구사항이 선택된 이유를 설명해야 한다.
ASE_REQ.2.9C 보안요구사항에 대한 설명은 내부적으로 일관성이 있어야 한다.

평가자 요구사항
ASE_REQ.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

**ASE_SPD.1 보안문제정의**

종속관계 : 없음

개발자 요구사항
ASE_SPD.1.1D 개발자는 보안문제정의를 제공해야 한다.

증거 요구사항
ASE_SPD.1.1C 보안문제정의는 위협을 서술해야 한다.
ASE_SPD.1.2C 모든 위협은 위협원, 자산, 공격 행동의 관점에서 서술되어야 한다.
ASE_SPD.1.3C 보안문제정의는 조직의 보안정책(OSP)을 서술해야 한다.
ASE_SPD.1.4C 보안문제정의는 TOE 운영환경에 관한 가정사항을 서술해야 한다.

평가자 요구사항
ASE_SPD.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

**ASE_TSS.1 TOE 요약명세**

종속관계: ASE_INT.1 보안목표명세서 소개
ASE_REQ.1 명시된 보안요구사항
ADV_FSP.1 기본적인 기능명세

개발자 요구사항
ASE_TSS.1.1D 개발자는 TOE 요약명세를 제공해야 한다.

증거 요구사항
ASE_TSS.1.1C TOE 요약명세는 TOE가 어떻게 각각의 보안기능요구사항을 만족시키는지 서술해야 한다.

평가자 요구사항
ASE_TSS.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ASE_TSS.1.2E 평가자는 TOE 요약명세가 TOE 개요 및 TOE 설명과 일관성이 있음을 확인해야 한다.

### 6.2.2. 개발

**ADV_ARC.1 보안 아키텍처 설명**

종속관계: ADV_FSP.1 기본적인 기능명세
ADV_TDS.1 기본적인 설계

개발자 요구사항
ADV_ARC.1.1D 개발자는 TSF의 보안특성이 우회되지 않도록 TOE를 설계하고 구현해야 한다.
ADV_ARC.1.2D 개발자는 신뢰되지 않은 능동적 실체에 의한 침해로부터 TSF 자체를 보호할 수 있도록 TSF를 설계하고 구현해야 한다.
ADV_ARC.1.3D 개발자는 TSF의 보안 아키텍처 설명을 제공해야 한다.

증거 요구사항
ADV_ARC.1.1C 보안 아키텍처 설명은 TOE 설계 문서에 서술된 SFR-수행 추상화 설명에 알맞는 상세수준으로 서술되어야 한다.

ADV_ARC.1.2C 보안 아키텍쳐 설명은 TSF에 의해서 SFR과 일관성 있게 유지되어야 하는 보안 영역을 서술해야 한다.
ADV_ARC.1.3C 보안 아키텍쳐 설명은 TSF 초기화 과정이 어떻게 안전한지 서술해야 한다.
ADV_ARC.1.4C 보안 아키텍쳐 설명은 TSF가 침해로부터 자신을 보호함을 입증해야 한다.
ADV_ARC.1.5C 보안 아키텍쳐 설명은 TSF가 SFR-수행 기능성의 우회를 방지함을 입증해야 한다.

평가자 요구사항
ADV_ARC.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

**ADV_FSP.2 추가적인 오류 정보를 제공하는 준정형화된 완전한 기능명세**

종속관계: ADV_TDS.1 기본적인 설계
ADV_IMP.1 TSF에 대한 구현의 표현

개발자 요구사항
ADV_FSP.5.1D 개발자는 기능명세를 제공해야 한다.
ADV_FSP.5.2D 개발자는 기능명세에서 SFR로의 추적성을 제공해야 한다.

증거 요구사항
ADV_FSP.5.1C 기능명세는 TSF를 완전하게 표현해야 한다.
ADV_FSP.5.2C 기능명세는 준정형화된 방식을 사용하여 TSFI를 서술해야 한다.
ADV_FSP.5.3C 기능명세는 모든 TSFI에 대한 목적과 사용 방법을 서술해야 한다.
ADV_FSP.5.4C 기능명세는 각 TSFI와 관련된 모든 매개변수를 식별 및 서술해야 한다.
ADV_FSP.5.5C 기능명세는 각 TSFI에 관련된 모든 행동을 서술해야 한다.
ADV_FSP.5.6C 기능명세는 TSFI를 호출한 결과 발생하는 모든 직접적인 오류 메시지를 서술해야 한다.
ADV_FSP.5.7C 기능명세는 TSFI를 호출한 결과 이외의 원인으로 인해 발생하는 모든 오류 메시지를 서술해야 한다.
ADV_FSP.5.8C 기능명세는 TSF 구현에 포함되지만 TSFI를 호출한 결과 이외의 원인으로 인해 발생하는 각 오류 메시지에 대한 이론적 근거를 제공해야 한다.
ADV_FSP.5.9C 추적성은 SFR이 기능명세 내의 TSFI로 추적됨을 입증해야 한다.

평가자 요구사항
ADV_FSP.5.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족함을 확인해야 한다.
ADV_FSP.5.2E 평가자는 기능명세가 SFR을 정확하고 완전하게 실체화하는지 결정해야 한다.

**ADV_IMP.2 완전히 대응되는 TSF에 대한 구현의 표현**

종속관계 : ADV_TDS.3 기본적인 모듈화 설계
ALC_TAT.1 잘 정의된 개발 도구
ALC_CMC.5 고급 지원

개발자 요구사항

ADV_IMP.2.1D 개발자는 전체 TSF에 대한 구현의 표현을 가용하게 해야 한다.

ADV_IMP.2.2D 개발자는 TOE 설계 설명과 전체 구현의 표현간의 대응관계를 제공해야 한다.

증거 요구사항

ADV_IMP.2.1C 구현의 표현은 더 이상의 설계과정 없이 TSF가 생성될 수 있는 상세수준으로 TSF를 정의해야 한다.

ADV_IMP.2.2C 구현의 표현은 개발 인력이 사용한 형태이어야 한다.

ADV_IMP.2.3C TOE 설계 설명과 전체 구현의 표현간의 대응관계는 이들의 일치성을 입증해야 한다.

평가자 요구사항

ADV_IMP.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

**ADV_TDS.3 최소화된 복잡도를 갖는 TSF 내부**

종속관계 : ADV_IMP.1 TSF에 대한 구현의 표현
ADV_TDS.3 기본적인 모듈화 설계
ALC_TAT.1 잘 정의된 개발 도구

개발자 요구사항

ADV_INT.3.1D 개발자는 전체 TSF가 잘 구조화된 내부를 가지도록 설계하고 구현해야 한다.

ADV_INT.3.2D 개발자는 TSF 내부에 대한 설명과 정당화를 제공해야 한다.

증거 요구사항

ADV_INT.3.1C 정당화는 “잘 구조화된” 및 “복잡도“의 의미를 판단하는 데 사용된 특성을 서술해야 한다.

ADV_INT.3.2C TSF 내부 설명은 전체 TSF가 잘 구조화되었고 지나치게 복잡하지 않음을 입증해야 한다.

평가자 요구사항

ADV_INT.3.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

ADV_INT.3.2E 평가자는 전체 TSF에 대해 내부 분석을 수행해야 한다.

**ADV_SPM.1 정형화된 TOE 보안정책모델**

종속관계 : ADV_FSP.4 완전한 기능명세

개발자 요구사항

ADV_SPM.1.1D 개발자는 [할당: 정형화된 방식으로 모델링된 정책 목록]에 대한 정형화된 보안정책모델을 제공해야 한다.

ADV_SPM.1.2D 정형화된 보안정책모델에서 다루는 각 정책에 대하여, 그 모델은 정책을 구성하는 SFR의 관련 부분을 식별해야 한다.

ADV_SPM.1.3D 개발자는 모델과 정형화된 기능명세 간의 일치성에 대한 정형화된 증거를 제공해야 한다.

ADV_SPM.1.4D 개발자는 모델과 기능명세 간의 일치성 입증을 제공해야 한다.

증거 요구사항

ADV_SPM.1.1C 모델은 요구되는 경우 설명문이 지원되는 정형화된 방식이어야 하며, 모델링된 TSF의 보안정책을 식별해야 한다.

ADV_SPM.1.2C 모델링된 모든 정책에 대해 모델은 TOE에 대한 보안성을 정의하고, TOE가 안전하지 않은 상태가 될 수 없다는 정형화된 증거를 제공해야 한다.

ADV_SPM.1.3C 모델과 기능명세 간의 일치성은 정확한 정형화 수준이어야 한다.

ADV_SPM.1.4C 일치성은 기능명세가 모델에 대하여 일관성 있고 완전함을 보여야 한다.

평가자 요구사항

ADV_SPM.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

**ADV_TDS.5 완전한 준정형화된 모듈화 설계**

종속관계 : ADV_FSP.5 추가적인 오류 정보를 제공하는 준정형화된 완전한 기능명세

개발자 요구사항

ADV_TDS.5.1D 개발자는 TOE 설계를 제공해야 한다.

ADV_TDS.5.2D 개발자는 기능명세의 TSFI와 TOE 설계에서 사용 가능한 가장 상세수준 분해간의 대응관계를 제공해야 한다.

증거 요구사항

ADV_TDS.5.1C 설계는 TOE의 구조를 서브시스템 측면에서 서술해야 한다.

ADV_TDS.5.2C 설계는 각 모듈을 SFR-수행, SFR-지원 또는 SFR-비-간섭으로 지정하여 TSF를 모듈 측면에서 서술해야 한다.

ADV_TDS.5.3C 설계는 TSF의 모든 서브시스템을 식별해야 한다.

ADV_TDS.5.4C 설계는 TSF의 각 서브시스템에 대한 준정형화된 설명을 제공해야 하며, 필요한 경우 비정형화된 설명문이 지원되어야 한다.

ADV_TDS.5.5C 설계는 TSF의 모든 서브시스템들 간의 상호작용에 대한 설명을 제공해야 한다.

ADV_TDS.5.6C 설계는 TSF 서브시스템과 TSF 모듈간의 대응관계를 제공해야 한다.

ADV_TDS.5.7C 설계는 각 모듈을 모듈의 목적, 상호작용, 인터페이스, 인터페이스로부터의 반환 값, 다른 모듈에서 호출된 인터페이스 등의 측면에서 준정형화된 설명을 제공해야 하며, 필요한 경우 비정형화된 설명문이 지원되어야 한다.

ADV_TDS.5.8C 대응관계는 모든 TSFI가 TOE 설계 내에 서술된 행동으로 추적함을 입증해야 한다.

평가자 요구사항

ADV_TDS.5.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해 야 한다.

ADV_TDS.5.2E 평가자는 설계가 모든 보안기능요구사항을 정확하고 완전하게 실체화하는지 결정해야 한다.

### 6.2.3. 설명서

**AGD_OPE.1 사용자 운영 설명서**

종속관계: ADV_FSP.1 기본적인 기능명세

개발자 요구사항

AGD_OPE.1.1D 개발자는 사용자 운영 설명서를 제공해야 한다.

증거 요구사항

AGD_OPE.1.1C 사용자 운영 설명서는 각각의 사용자 역할에 대해 안전한 처리환경 내에서 통제되어야 하는 사용자가 접근 가능 기능 및 특권에 대해 적절한 경고를 포함해서 서술해야 한다.

AGD_OPE.1.2C 사용자 운영 설명서는 각각의 사용자 역할에 대해 TOE에 의해 안전한 방식으로 제공되는 인터페이스의 사용 방법을 서술해야 한다.

AGD_OPE.1.3C 사용자 운영 설명서는 각각의 사용자 역할에 대해 사용 가능한 기능 및 인터페이스를 서술해야 한다. 특히 사용자의 통제 하에있는 모든 보안 매개변수에 대해 안전한 값을 적절하게 표시해야 한다.

AGD_OPE.1.4C 사용자 운영 설명서는 각 사용자 역할에 대해 수행되어야 할 사용자가 접근할 수 있는 기능과 연관된 보안-관련 사건의 각 유형을 명확히 제시해야 한다. 여기에는 TSF의 통제하에 있는 실체에 대한 보안 특성의 변경도 포함되어야 한다.

AGD_OPE.1.5C 사용자 운영 설명서는 (장애 후의 운영 또는 운영상의 오류 후의 운영을 포함) TOE의 모든 가능한 운영 모드, 그 영향 및 안전한 운영 유지를 위한 관련사항들을 식별해야 한다.

AGD_OPE.1.6C 사용자 운영 설명서는 각각의 사용자 역할에 대해 보안목표명세서에 서술된 대로 운영환경에 대한 보안목적을 만족시키기 위해 준수해야 하는 보안 대책을 서술해야 한다.

AGD_OPE.1.7C 사용자 운영 설명서는 명확하고 타당해야 한다.

평가자 요구사항

AGD_OPE.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

**AGD_PRE.1 준비 절차**

종속관계 : 없음

개발자 요구사항

AGD_PRE.1.1D 개발자는 준비 절차를 포함하여 TOE를 제공해야 한다.

증거 요구사항

AGD_PRE.1.1C 준비 절차는 배포된 TOE의 안전한 인수를 위해 필요한 모든 단계를 개발자의 배포 절차와 일관되게 서술해야 한다.

AGD_PRE.1.2C 준비 절차는 TOE의 안전한 설치 및 운영환경의 안전한 준비를 위해 필요한 모든 단계를 보안목표명세서에 서술된 운영환경에 대한 보안목적과 일관되게 서술해야 한다.

평가자 요구사항

AGD_PRE.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

AGD_PRE.1.2E 평가자는 TOE가 운영을 위해 안전하게 준비될 수 있음을 확인하기 위해 준비 절차를 적용해야 한다.

### 6.2.4. 생명주기 지원

### ALC_CMC.5 고급 지원

종속관계 : ALC_CMS.1 TOE 형상관리 범위
ALC_DVS.2 보안대책의 충분함
ALC_LCD.1 개발자가 정의한 생명주기 모델

개발자 요구사항

ALC_CMC.5.1D 개발자는 TOE 및 그에 대한 참조를 제공해야 한다.
ALC_CMC.5.2D 개발자는 형상관리 문서를 제공해야 한다.
ALC_CMC.5.3D 개발자는 형상관리 시스템을 사용해야 한다.

증거 요구사항

ALC_CMC.5.1C TOE는 유일한 참조를 위한 레이블을 붙여야 한다.
ALC_CMC.5.2C 형상관리 문서는 형상항목을 유일하게 식별하는 데 사용된 방법을 서술해야 한다.
ALC_CMC.5.3C 형상관리 문서는 수용절차가 모든 형상항목의 변경을 충분하고 적절하게 검토한다는 것을 정당화해야 한다.
ALC_CMC.5.4C 형상관리 시스템은 모든 형상항목을 유일하게 식별해야 한다.
ALC_CMC.5.5C 형상관리 시스템은 형상항목에 인가된 변경만을 허용하는 자동화된 수단을 제공해야 한다.
ALC_CMC.5.6C 형상관리 시스템은 자동화된 수단을 이용하여 TOE의 생산을 지원해야 한다.
ALC_CMC.5.7C 형상관리 시스템은 형상항목을 형상관리 내에 수용하는 책임자와 형상항목 개발자가 다르다는 것을 보장해야 한다.
ALC_CMC.5.8C 형상관리 시스템은 TSF를 구성하는 형상항목을 식별해야 한다.
ALC_CMC.5.9C 형상관리 시스템은 자동화된 수단을 이용하여 감사 증적에서 사건 주체, 날짜, 시간을 포함하여 TOE에 대한 모든 변경을 감사할 수 있도록 지원해야 한다.
ALC_CMC.5.10C 형상관리 시스템은 주어진 형상항목의 변경으로 영향을 받는 다른 모든 형상항목을 식별하기 위한 자동화된 수단을 제공해야 한다.
ALC_CMC.5.11C 형상관리 시스템은 TOE가 생성되는 소스코드의 버전을 식별할 수 있어야 한다.
ALC_CMC.5.12C 형상관리 문서는 형상관리 계획을 포함해야 한다.
ALC_CMC.5.13C 형상관리 계획은 형상관리 시스템이 TOE 개발에 사용되는 방법을 서술해야 한다.
ALC_CMC.5.14C 형상관리 계획은 변경되거나 새로 생성된 형상항목을 TOE의 일부로 수용하는데 사용된 절차를 서술해야 한다.
ALC_CMC.5.15C 증거는 모든 형상항목이 형상관리 시스템 하에 유지되고 있음을 입증해야 한다.
ALC_CMC.5.16C 증거는 형상관리 시스템이 형상관리 계획에 따라 운영되고 있음을 입증해야 한다.

평가자 요구사항

ALC_CMC.5.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ALC_CMC.5.2E 평가자는 생산지원 절차를 적용할 경우 TOE가 시험 평가활동을 위해 개발자가 제공한 대로 구성된다는 것을 결정해야 한다.

### ALC_CMS.5 개발도구 형상관리 범위

종속관계 : 없음

개발자 요구사항

ALC_CMS.5.1D 개발자는 TOE에 대한 형상목록을 제공해야 한다.

증거 요구사항

ALC_CMS.5.1C 형상목록은 TOE, 보증요구사항에서 요구하는 평가증거, TOE를 구성하는 부분, 소스코드, 보안 결함 보고서 및 해결 상태, 개발도구 및 관련 정보를 포함해야 한다.

ALC_CMS.5.2C 형상목록은 형상항목을 유일하게 식별해야 한다.

ALC_CMS.5.3C 형상목록은 각 TSF 관련 형상항목의 개발자를 표시해야 한다.

평가자 요구사항

ALC_CMS.5.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다..

**ALC_DEL.1 배포 절차**

종속관계 : 없음

개발자 요구사항

ALC_DEL.1.1D 개발자는 소비자에게 TOE나 TOE 일부를 배포하는 절차를 문서화하여 제공해야 한다.

ALC_DEL.1.2D 개발자는 배포 절차를 사용해야 한다.

증거 요구사항

ALC_DEL.1.1C 배포 문서는 TOE를 소비자에게 배포할 때 보안을 유지하기 위해 필요한 모든 절차를 서술해야 한다.

평가자 요구사항

ALC_DEL.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

**ALC_DVS.2 보안대책의 충분함**

종속관계 : 없음

개발자 요구사항

ALC_DVS.2.1D 개발자는 개발보안 문서를 작성하여 제공해야 한다.

증거 요구사항

ALC_DVS.2.1C 개발보안 문서는 개발환경 내에서 TOE 설계 및 구현 과정의 비밀성과 무결성을 보호하기 위하여 필요한 모든 물리적, 절차적, 인적 및 기타 보안대책을 서술해야 한다.

ALC_DVS.2.2C 개발보안 문서는 보안대책이 TOE의 비밀성과 무결성을 유지하기 위하여 필요한 수준의 보호를 제공함을 정당화해야 한다.

평가자 요구사항

ALC_DVS.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

ALC_DVS.2.2E 평가자는 보안대책이 적용되고 있는지 확인해야 한다.

**ALC_LCD.1 개발자가 정의한 생명주기 모델**

종속관계 : 없음

개발자 요구사항

ALC_LCD.1.1D 개발자는 TOE의 개발과 유지에 사용되는 생명주기 모델을 수립해야 한다.

ALC_LCD.1.2D 개발자는 생명주기 정의 문서를 제공해야 한다.

증거 요구사항

ALC_LCD.1.1C 생명주기 정의 문서는 TOE의 개발과 유지에 사용되는 모델을 서술해야 한다.

ALC_LCD.1.2C 생명주기 모델은 TOE의 개발과 유지에 필요한 통제를 제공해야 한다.

평가자 요구사항

ALC_LCD.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

**ALC_TAT.3 모든 부분에서 적용된 구현표준**

종속관계 : ADV_IMP.1 TSF에 대한 구현의 표현

개발자 요구사항

ALC_TAT.3.1D 개발자는 TOE에 사용된 각 개발 도구를 식별한 문서를 제공해야 한다.

ALC_TAT.3.2D 개발자는 각 개발 도구에 대해 구현-종속적인 선택사항을 문서화하여 제공해야 한다.

ALC_TAT.3.3D 개발자는 TOE의 모든 부분에 대해 개발자 및 제3의 제공자가 적용하는 구현표준을 서술하여 제공해야 한다.

증거 요구사항

ALC_TAT.3.1C 구현에 사용된 각 개발 도구는 잘 정의된 것이어야 한다.

ALC_TAT.3.2C 각 개발 도구 문서는 구현에 사용된 모든 규정과 지시어 뿐만 아니라 모든 명령문의 의미를 모호하지 않게 정의해야 한다.

ALC_TAT.3.3C 각 개발 도구 문서는 모든 구현-종속적인 선택사항의 의미를 모호하지 않게 정의해야 한다.

평가자 요구사항

ALC_TAT.3.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

ALC_TAT.3.2E 평가자는 구현표준이 적용되었는지 확인해야 한다.

### 6.2.5. 시험

**ATE_COV.3 시험범위의 엄밀한 분석**

종속관계 : ADV_FSP.2 보안-수행 기능명세
ATE_FUN.1 기능 시험

개발자 요구사항

ATE_COV.3.1D 개발자는 시험범위의 분석을 제공해야 한다.

증거 요구사항

ATE_COV.3.1C 시험범위의 분석은 시험 문서 내의 시험항목과 기능명세 내의 TSFI 간의 일치성을 입증해야 한다.
ATE_COV.3.2C 시험범위의 분석은 기능명세 내의 모든 TSFI가 완전히 시험되었음을 입증해야 한다.

평가자 요구사항
ATE_COV.3.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### ATE_DPT.3 모듈화 설계 시험

종속관계 : ADV_ARC.1 보안 아키텍쳐 설명
ADV_TDS.4 준정형화된 모듈화 설계
ATE_FUN.1 기능 시험

개발자 요구사항
ATE_DPT.3.1D 개발자는 시험의 상세수준 분석을 제공해야 한다.

증거 요구사항
ATE_DPT.3.1C 시험의 상세수준 분석은 시험 문서 내의 시험항목과 TOE 설계 내의 TSF 서브시스템 및 모듈 간의 일치성을 입증해야 한다.
ATE_DPT.3.2C 시험의 상세수준 분석은 TOE 설계 내의 모든 TSF 서브시스템이 시험되었음을 입증해야 한다.
ATE_DPT.3.3C 시험의 상세수준 분석은 TOE 설계 내의 모든 TSF 모듈이 시험되었음을 입증해야 한다.

평가자 요구사항
ATE_DPT.3.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### ATE_FUN.2 순서화된 기능시험

종속관계 : ATE_COV.1 시험범위의 증거

개발자 요구사항
ATE_FUN.2.1D 개발자는 TSF를 시험하고 그 결과를 문서화해야 한다.
ATE_FUN.2.2D 개발자는 시험 문서를 제공해야 한다.

증거 요구사항
ATE_FUN.2.1C 시험 문서는 시험계획, 예상 시험결과, 실제 시험결과로 구성되어야 한다.
ATE_FUN.2.2C 시험계획은 수행되어야 할 시험항목을 식별하고 각 시험 수행의 시나리오를 서술해야 한다. 이러한 시나리오는 다른 시험결과에 대한 순서 종속관계를 포함해야 한다.
ATE_FUN.2.3C 예상 시험결과는 시험의 성공적인 수행으로 기대되는 결과를 제시해야 한다.
ATE_FUN.2.4C 실제 시험결과는 예상 시험결과와 일관성이 있어야 한다.
ATE_FUN.2.5C 시험 문서는 시험절차의 순서 종속관계에 대한 분석을 포함해야 한다.

평가자 요구사항

ATE_FUN.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

**ATE_IND.2 독립적인 시험 : 표본 시험**

종속관계 : ADV_FSP.2 보안-수행 기능명세
AGD_OPE.1 사용자 운영 설명서
AGD_PRE.1 준비 절차
ATE_COV.1 시험범위의 증거
ATE_FUN.1 기능 시험

개발자 요구사항
ATE_IND.2.1D 개발자는 시험할 TOE를 제공해야 한다.

증거 요구사항
ATE_IND.2.1C TOE는 시험하기에 적합해야 한다.
ATE_IND.2.2C 개발자는 개발자의 TSF 기능 시험에 사용된 자원과 동등한 자원을 제공해야 한다.

평가자 요구사항
ATE_IND.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ATE_IND.2.2E 평가자는 개발자 시험 결과를 검증하기 위하여 시험문서 내의 시험항목에 대한 표본 시험을 수행해야 한다.
ATE_IND.2.3E 평가자는 TSF가 명세된 대로 동작함을 확인하기 위하여 TSF의 일부를 시험해야 한다.

### 6.2.6. 취약성 평가

**AVA_VAN.5 고도의 체계적인 취약성 분석**

종속관계 : ADV_ARC.1 보안 아키텍쳐 설명
ADV_FSP.4 완전한 기능명세
ADV_TDS.3 기본적인 모듈화 설계
ADV_IMP.1 TSF에 대한 구현의 표현
AGD_OPE.1 사용자 운영 설명서
AGD_PRE.1 준비 절차
ATE_DPT.1 기본설계 시험

개발자 요구사항
AVA_VAN.5.1D 개발자는 시험할 TOE를 제공해야 한다.

증거 요구사항
AVA_VAN.5.1C TOE는 시험하기에 적합해야 한다.

평가자 요구사항

AVA_VAN.5.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
AVA_VAN.5.2E 평가자는 TOE의 잠재적 취약성을 식별하기 위해 공개 영역에 대한 조사를 수행해야 한다.
AVA_VAN.5.3E 평가자는 TOE의 잠재적 취약성을 식별하기 위해 설명서, 기능명세, TOE 설계 및 보안 아키텍쳐 설명, 구현의 표현을 이용하여 독립적이고, 체계적인 취약성 분석을 수행해야 한다.
AVA_VAN.5.4E 평가자는 TOE가 높은 공격 성공 가능성을 가진 공격자에 의해 행해지는 공격에 내성이 있음을 결정하기 위해, 식별된 잠재적 취약성에 근거하여 침투시험을 수행해야 한다.

## 6.3. 요구사항의 이론적 근거

보안요구사항의 이론적 근거는 서술된 보안요구사항이 보안목적을 만족시키기에 적합하고, 그 결과 보안문제를 다루기에 적절함을 입증한다.

### 6.3.1. 보안기능요구사항의 이론적 근거

보안기능요구사항의 이론적 근거는 다음을 입증한다. 각 TOE에 대한 보안목적은 적어도 하나의 보안기능요구사항에 의해서 다루어진다. 각 보안기능요구사항은 적어도 하나의 TOE에 대한 보안목적을 다룬다.

| 보안기능컴포넌트 | O. 감사 기록 | O. 정보 흐름 통제 | O. 잔여 정보 보호 | O. 식별 및 인증 | O. 복구 | O. 무결성 | O. 가용성 | O. 기능 관리 |
|---|---|---|---|---|---|---|---|---|
| FAU_GEN.1 | X | | | | | | | |
| FAU_STG.1 | X | | | | | | | |
| FAU_STG.3 | X | | | | | | | |
| FAU_STG.4 | X | | | | | | | |
| FDP_IFC.1 | | X | | | | | | |
| FDP_IFF.1 | | X | | | | | | |
| FDP_RIP.1 | | | X | | | | | |
| FIA_UAU.1 | | | | X | | | | |
| FIA_UID.1 | | | | X | | | | |
| FMT_MOF.1 | | X | | | | | | X |
| FMT_MSA.1 | | X | | | | | | X |
| FMT_MSA.3 | | X | | | | | | X |
| FMT_MTD.1 | | | | X | X | X | X | X |
| FMT_SMF.1 | | | | | | | | X |
| FMT_SMR.1 | | | | | | | | X |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| FPT_FLS.1 | | X | | | X | | | |
| FPT_RCV.1 | | | | | X | | | |
| FPT_TST.1 | | | | | | X | | X |
| FRU_PRS.1 | | | | | | | X | |
| FRU_RSA.1 | | | | | | | X | |

[표 14] 보안목적과 보안기능요구사항 대응

**FAU_GEN.1 감사 데이터 생성**

본 컴포넌트는 감사대상 사건을 정의하고 감사 레코드를 생성하는 능력을 보장하므로 TOE 보안목적 O.감사기록을 만족시킨다.

**FAU_STG.1 감사 증적 저장소 보호**

본 컴포넌트는 인가되지 않은 변경 및 삭제로부터 감사 레코드를 보호하는 능력을 보장하므로 TOE 보안목적 O.감사기록을 만족시킨다.

**FAU_STG.3 감사 데이터 손실 예측 시 대응 행동**

본 컴포넌트는 감사 증적이 미리 정의한 한도를 초과하는 경우 대응행동을 취하는 능력을 보장하므로 TOE 보안목적 O.감사기록을 만족시킨다.

**FAU_STG.4 감사 데이터의 손실 방지**

본 컴포넌트는 감사 증적이 포화되는 경우 대응행동을 취하는 능력을 보장하므로 TOE 보안목적 O.감사기록을 만족시킨다.

**FDP_IFC.1 부분적인 정보흐름통제**

본 컴포넌트는 TOE 정보흐름통제를 위한 보안정책이 정의되고, TOE 내부에서 전송되는 데이터의 정보흐름을 통제하는 능력을 보장하므로 TOE 보안목적 O.정보흐름통제를 만족시킨다.

**FDP_IFF.1 단일 계층 보안속성**

본 컴포넌트는 보안속성에 기반하여 정보흐름을 통제하는 규칙을 만족하므로 TOE 보안목적 O.정보흐름통제를 만족시킨다.

**FDP_RIP.1 부분적인 잔여정보 보호**

본 컴포넌트는 사용자 애플리케이션이 사용한 메모리에 대하여 작업 종료 후, 저장되어 있는 모든 데이터를 소거하는 것으로 정보 노출을 방지하는 능력을 보장하므로 TOE 보안목적 O.잔여정보보호를 만족시킨다.

**FIA_UAU.1 인증**

본 컴포넌트는 사용자를 성공적으로 인증하는 능력을 보장하므로 TOE 보안목적 O.식별및인증을 만족시킨다.

**FIA_UID.1 식별**

본 컴포넌트는 사용자를 성공적으로 식별하는 능력을 보장하므로 TOE 보안목적 O.식별및인증을 만족시킨다.

**FMT_MOF.1 보안기능 관리**

본 컴포넌트는 인가된 관리자가 보안기능을 관리하는 능력을 보장하므로 TOE 보안목적 O.정보흐름통제와 O.기능관리를 만족시킨다.

**FMT_MSA.1 보안속성 관리**

본 컴포넌트는 인가된 관리자가 보안속성을 관리하는 능력을 보장하므로 TOE 보안목적 O.정보흐름통제와 O.기능관리를 만족시킨다.

**FMT_MSA.3 정적 속성 초기화**

본 컴포넌트는 정보흐름통제 정책에 적용되는 보안속성의 초기값의 적용규칙과 그 값을 제공하므로 TOE 보안기능 O.정보흐름통제와 O.기능관리를 만족시킨다.

**FMT_MTD.1 TSF 데이터 관리**

본 컴포넌트는 인가된 관리자가 무결성 검증 데이터, 자원 할당 최대치 등 TSF 데이터에 대한 접근 및 관리하는 능력을 제공하므로 TOE 보안목적 O.식별및인증, O.복구, O.무결성, O.자원할당, O.기능관리를 만족시킨다.

**FMT_SMF.1 관리기능명세**

본 컴포넌트는 TSF가 수행해야 하는 보안기능, 보안속성, TSF 데이터 등의 관리기능을 명세하도록 요구하므로 TOE 보안목적 O.기능관리를 만족시킨다.

**FMT_SMR.1 보안 역할**

본 컴포넌트는 사용자를 인가된 관리자와 일반 사용자로 분류하여 연관시키며 역할별로 권한을 보장하므로 TOE 보안목적 O.기능관리를 만족시킨다.

**FPT_FLS.1 장애 시 안전한 상태 유지**

본 컴포넌트는 TOE가 고장 시에도 정보흐름통제 기능과 복구 기능을 포함한 핵심적인 보안기능의 동작을 위해 안전한 상태를 유지하는 것을 보장하므로 TOE 보안목적 O.정보흐름통제와 O.복구를 만족시킨다.

**FPT_RCV.1 수동 복구**

본 컴포넌트는 TOE의 일정 임계치 이상의 비인가 접근 횟수가 감지되거나 TOE의 고장 상태 인지되는 경우, TOE를 복구하기 위한 관리모드로 전환하는 기능이 제공되므로 TOE 보안목적 O.복구를 만족시킨다.

**FPT_STM.1 신뢰할 수 있는 타임스탬프**

본 컴포넌트는 신뢰할 수 있는 타임스탬프를 제공하는 것을 보장하므로 TOE 보안목적 O.감사기록, O.식별및인증, O.복구, O.무결성, O.기능관리를 만족시킨다.

**FPT_TST.1 TSF 자체 시험**

본 컴포넌트는 TOE의 정확한 운영을 위하여 최초 실행 간, 일정 주기 간, TSF 데이터 변경 시 자체 시험을 보장하고, TSF 데이터의 무결성을 검증하는 기능을 제공하므로 TOE 보안목적 O.무결성과 O.기능관리를 만족시킨다.

**FRU_PRS.1 자원사용 우선순위 : 부분적용**

본 컴포넌트는 각 주체별 우선순위를 할당하여 주체 및 객체가 운영 가능한 메모리 영역 및 용량과 CPU의 점유 시간에 대한 접근을 관리하는 것을 보장하므로 TOE 보안목적 O.자원할당을 만족시킨다.

**FRU_RSA.1 최대 할당치**

본 컴포넌트는 각 주체가 TSF 데이터 상에 명세된 기간 동안 주체 및 객체가 운영 가능한 메모리 영역 및 용량과 CPU의 점유 시간의 활용 가능한 최대 할당치를 강제하는 것을 보장하므로 TOE 보안목적 O.자원할당을 만족시킨다.

### 6.3.2. 보증요구사항의 이론적 근거

본 보안목표명세서의 보증등급은 TOE가 보호하는 자산의 가치, 위협 수준 등을 고려하여 EAL6으로 선정하였다. EAL6은 개발자가 심각한 위험으로부터 높은 가치의 자산을 보호하기 위한 최상의 TOE를 생산하기 위하여 엄격한 개발환경에서 보안공학 기법을 응용하여 얻을 수 있는 높은 보증을 제공한다. EAL6은 보호되는 자산의 가치가 추가적인 비용을 정당화할 수 있는 높은 위험 상황에서 사용하기 위한 보안 TOE를 개발할 경우에 적용 가능하다. EAL6은 보안 행동을 이해하기 위해 기능 및 완전한 인터페이스 명세, 설명서, TOE에 대한 설계, 구현을 이용하여 완전한 보안목표명세서에 포함된 보안기능요구사항을 분석함으로써 보증을 제공한다. 선택된 TOE 보안정책의 정형화된 모델, 기능명세와 TOE 설계의 준정형화된 표현을 통해서도 추가적인 보증을 제공한다. 또한 모듈화되고 계층화 및 단순화된 TSF 설계가 요구된다. 이 분석은 TSF의 독립적인 시험, 기능명세 및 TOE 설계에 기반하여 개발자가 수행한 시험의 증거, 개발자가 수행한 시험결과 표본의 독립적인 확인, 높은 공격 성공 가능성을 가진 공격자의 침투 공격에 대한 내성을 입증하는 독립적인 취약성 분석에 의해 뒷받침된다. 또한, EAL6은 구조화된 개발 과정, 개발환경 통제, 완전한 자동화를 포함하는 포괄적인 TOE의 형상관리, 안전한 배포 절차의 증거를 통하여 보증을 제공한다. EAL6은 보다 포괄적인 분석, 구조화된 구현의 표현, 보다 체계적인 구조(예: 계층화), 보다 포괄적이고 독립적인 취약성 분석, 개선된 형상관리와 개발환경 통제 등을 요구함으로써 EAL5보다 높은 보증을 제공한다.

## 6.4. 종속관계에 대한 이론적 근거

종속관계의 이론적 근거는 서술된 보안요구사항과 보증요구사항의 종속관계를 기반으로 입증한다.

### 6.4.1. 보안기능요구사항의 이론적 근거

TOE 기능 컴포넌트의 종속관계를 보여준다.

| 번호 | 보안기능컴포넌트 | 종속관계 | 참조번호 |
|---|---|---|---|
| 1 | FAU_GEN.1 | FPT_STM.1 신뢰할 수 있는 타임스탬프 | 22 |
| 2 | FAU_STG.1 | FAU_GEN.1 감사 데이터 생성 | 1 |
| 3 | FAU_STG.3 | FAU_STG.1 감사 증적 저장소 보호 | 2 |
| 4 | FDP_IFC.1 | FDP_IFF.1 단일 계층 보안속성 | 10 |
| 5 | FDP_IFF.1 | FDP_IFC.1 부분적인 정보흐름통제<br>FMT_MSA.3 정적 속성 초기화 | 9<br>16 |
| 6 | FDP_RIP.1 | - | - |
| 7 | FIA_UAU.1 | FIA_UID.1 식별 | 13 |
| 8 | FIA_UID.1 | - | - |
| 9 | FMT_MOF.1 | FMT_SMF1. 관리기능명세<br>FMR_SMR.1 보안 역할 | 18<br>19 |
| 10 | FMT_MSA.1 | FDP_IFC.1 부분적인 정보흐름통제<br>FMT_SMF1. 관리기능명세<br>FMR_SMR.1 보안 역할 | 9<br>18<br>19 |
| 11 | FMT_MSA.3 | FMT_MSA.1 보안속성 관리<br>FMT_SMR.1 보안 역할 | 15<br>19 |
| 12 | FMT_MTD.1 | FMT_SMF1. 관리기능명세<br>FMR_SMR.1 보안 역할 | 18<br>19 |
| 13 | FMT_SMF.1 | - | - |
| 14 | FMT_SMR.1 | FIA_UID.1 식별 | 13 |
| 15 | FPT_FLS.1 | - | - |
| 16 | FPT_RCV.1 | AGD_OPE.1 사용자 운영 설명서 | - |
| 17 | FPT_TST.1 | - | - |
| 18 | FRU_PRS.1 | - | - |
| 19 | FRU_RSA.1 | - | - |

[표 15] TOE 기능 컴포넌트 종속관계

### 6.4.2. 보증요구사항의 이론적 근거

정보보호시스템 공통평가기준에서 제공하는 각 보증 패키지의 종속관계는 이미 만족된다.

# 7. TOE 요약 명세

이 장은 TOE 내부에 구현된 보안기능들에 대해 설명하고 해당 보안기능이 어떠한 보안기능요구사항을 만족시키지 서술한다.

## 7.1. TOE에 구현된 보안기능

TOE의 보안 기능성은 보안감사, 체크포인트-복구, 커널 스케줄링 기능 등으로 구분할 수 있다. 이후 이 장에서는 앞서 명세하였던 보안기능 요구사항을 TOE가 만족시키는 방법을 서술한다.

### 7.1.1. 보안감사 기능

TOE는 특정 이벤트 발생 시 보안위협에 대한 검토 및 확인을 위해 보안감사기능을 제공하며 TOE의 비인가 접근 이벤트 발생 시 보안위협을 검토하기 위해 이벤트 모니터링 알고리즘 및 Capability에 대하여 저장하는 감사기록 저장 및 관리 알고리즘을 지원한다. 생성되는 감사 기록은 감사 기능의 시작과 종료, 사건 일시, 사건 유형, 주체의 신원, 사건 결과에 대한 내역과 비인가 접근 유형 시에 해당 주체의 Capability와 접근하고자 하는 객체의 Capability 정보를 포함한다. TOE의 감사 기록은 감사 증적 크기가 지정된 한도를 초과한 경우, 사전 정의한 방식인 오래된 감사 레코드 덮어쓰기에 따라 처리한다. 해당 보안감사 기능에 의해 감사기록이 생성되는 사건의 종류는 아래 [표 16]과 같다.

| 번호 | 컴포넌트 | 감사대상사건 | 추가적인 감사기록내용 |
|---|---|---|---|
| 1 | FAU_GEN.1 | 감사 데이터 발생 | - |
| 2 | FAU_STG.1 | 감사 데이터에 대한 접근 | - |
| 3 | FAU_STG.3 | 감사 데이터 저장 | - |
| 4 | FAU_STG.4 | 감사 데이터 저장을 위한 잔여공간의 부족 | - |
| 5 | FDP_IFC.1 | 없음 | - |
| 6 | FDP_IFF.1 | 오퍼레이션 거부 | - |
| 7 | FDP_RIP.1 | 없음 | - |
| 8 | FIA_UAU.1 | 사용자 인증 요청 | - |
| 9 | FIA_UID.1 | 사용자 인증 요청 | - |
| 10 | FMT_MOF.1 | TSF 기능의 상태 변경 | - |
| 11 | FMT_MSA.1 | 주체나 정보에 대한 관리 기능 수행 | - |
| 12 | FMT_MSA.3 | 객체나 정보의 생성 | - |
| 13 | FMT_MTD.1 | TSF 데이터에 대한 관리 기능 수행 | - |
| 14 | FMT_SMF.1 | TSF 기능에 대한 모든 변경 | - |
| 15 | FMT_SMR.1 | 보안 역할 대한 모든 변경 | - |
| 16 | FPT_FLS.1 | 스레드의 안전 상태식별 | 기능 작동 원인 |
| 17 | FPT_RCV.1 | 스레드의 불안전 상태식별 | - |
| 18 | FPT_TST.1 | 분기 발생 | 이상 데이터 해시 값 |
| 19 | FRU_PRS.1 | 우선순위에 따른 자원 할당 | 미준수 주체 혹은 TSF 정보 |
| 20 | FRU_RSA.1 | 메모리 할당 | - |

[표 16] 감사대상 사건

해당 보안감사 기능의 경우 다음과 같은 보안기능요구사항을 만족한다:

- FAU_GEN.1 (감사 데이터 생성)
- FAU_STG.1 (감사 증적 저장소 보호)
- FAU_STG.3 (감사 데이터 손실 예측 시 대응 행동)
- FAU_STG.4 (감사 데이터 손실 방지)

### 7.1.2. 사용자데이터 보호 기능

TOE에서 사용되는 사용자 데이터의 보안 속성을 서술하며, 이를 이용하여 데이터 전송 및 수신 시 데이터 무결성을 보장하는 기능을 제공한다. 이때, 사용자 데이터의 보안 속성은 사용자의 IP주소, Port번호, ID, PW와 같이 보안기능과 연관된 사용자의 정보를 말한다. 모든 객체들의 보안 속성은 해당 객체에 대한 보호 프로파일에 작성되어 있어야 하며, TOE는 해당 객체에 대한 접근 또는 관리 시 해당 보호프로파일을 검증한다. 또한, TOE는 외부 객체로부터 메시지를 전달받았을 때 외부 객체에 대한 보안 속성을 검증하여 비 인가된 객체로부터 전달받은 메시지일 경우 시스템 내부 객체로의 접근을 제한한다. TOE는 과거에 사용된 사용자 데이터가 물리적 메모리에 남아 이후 연산에 영향을 미치거나 해당 데이터가 유출되지 않도록 방지하기 위해 새로운 TSF 기능이 실행되기 이전 해당 TSF 기능에 할당되는 물리적 메모리를 0으로 초기화한다.

해당 사용자데이터보호 기능의 경우 다음과 같은 보안기능요구사항을 만족한다:

- FDP_IFF.1 (단일 계층 보안 속성 관리)
- FDP_IFC.1 (부분적 접근통제)
- FDP_RIP.1 (부분적 잔여 정보 보호)

### 7.1.3. 인증 기능

TOE는 시스템에 접근하여 시스템의 기능을 사용하고자 하는 사용자 및 시스템 내 생성된 프로세스를 유일하게 식별하고 인증할 수 있는 기능을 제공한다. 식별을 위해 사용되는 ID의 경우 부호가 없는 정수(Unsigned Integer) 자료형의 4 Byte 범위 안에서 결정되어 생성된다. 생성된 ID는 프로세스 및 사용자를 유일하게 식별하기 위해 중복되지 않도록 중복 검사를 수행하며, 중복되었을 경우 다시 새로운 값을 생성한다. 주체에 대한 인증의 경우 ID 식별 이후 해당 주체가 소유한 Secret Value에 대한 검증을 통해 수행된다. Secret Value는 20 ~ 32 Byte 범위 사이의 크기를 갖는 부호가 없는 정수형으로 결정 및 생성되며, 의사 난수 생성기(Pseudo Random Number Generator)를 통해 생성된다. 커널은 특정 주체에 대해 생성된 2가지 값(ID, Secret Value)을 사전(Dictionary)형태로 관리하며 ID값을 Key로 관리하고 이에 대한 Value로 Secret Value를 저장한다. 해당 사전의 경우 커널만 접근할 수 있는 영역에 안전하게 저장한다. 커널은 이렇게 저장된 사전을 활용하여 서비스를 요청하거나 자원을 할당받고자 하는 주체에 대해 인증을 수행하며, 최대 인증 시도회수 만큼 인증에 실패할 경우 해당 프로세스 및 유저에 대한 인증 과정을 종료한다.

해당 인증 기능의 경우 다음과 같은 보안기능요구사항을 만족한다:

- FIA_GEN.1 (인증)
- FIA_UID.1 (식별)

### 7.1.4. 보안 관리 기능

TOE는 시스템에 접근하는 주체와 시스템 내에서 처리되는 정보의 보안 속성을 관리하는 기능을 제공하고, 해당 기능에 접근할 수 있는 권한을 인가된 주체에게만 부여해야 한다. 인가된 주체는

2가지(인가된 관리자, 인가된 사용자)의 역할로 구분되며, 인가된 관리자의 경우 [표 17]과 같은 보안기능들에 대한 관리 기능에 접근할 수 있고, 인가된 사용자의 경우 제한적인 기능에만 접근할 수 있다.

| 보안기능 |
|---|
| 감사데이터 생성/저장 |
| 암호키 생성/파기 |
| 암호 연산 |
| 정보 흐름 통제 |
| 잔여 정보 보호 |
| 식별/인증 |
| 보안기능 데이터 관리 |
| 복구/재시작 |
| 무결성 검사 |
| 자원 할당 |

[표 17] 인가된 관리자가
관리할 수 있는 보안기능 목록

주체가 접근 가능한 권한을 Capability 보안속성으로 정의하고, 기능 및 객체의 Capability와 접근 주체의 Capability를 비교하여 동일 수준 이상의 Capability를 가질 경우 접근할 수 있다. 이러한 Capability의 경우 인가된 관리자만이 부여할 수 있으며, TOE 내에 구현된 보안기능들이 연산을 수행하기 위해 해당 보안기능이 처리하는 정보에 접근할 수 있는 최소 Capability를 부여받는다. 또한, 객체나 정보 생성 시 보안기능정책에 따라 객체나 정보를 제어하기 위해 초기 Capability값을 부여하며, 이러한 초기 Capability값은 관리자에 의해 임의의 값으로 설정될 수 있다.

해당 보안 관리 기능의 경우 다음과 같은 보안기능요구사항을 만족한다:

- FMT_MOF.1 (보안 기능 관리)
- FMT_MSA.1 (보안 속성 관리)
- FMT_MSA.3 (정적 속성 초기화)
- FMT_MTD.1 (TSF 데이터 관리)
- FMT_SMF.1 (관리 기능 명세)
- FMT_SMR.1 (보안 역할)

### 7.1.5. 체크포인트-복구 기능

시스템이 불안전한 상태에 빠진 것을 방지하기 위해 TOE는 체크포인트-복구 기능으로 시스템의 무결성을 주기적으로 검증한다. 이때 안전한 상태란 시스템의 흐름이 분기되는 시점에서 메모리상 안전한 주소로 분기되는 경우를 말하며, 메모리상 안전한 주소가 아닌 공격으로 인한 임의의 주소로 분기되거나 메모리 초기화 과정에서 설정된 Stack Guard 값이 임의의 값으로 변경될 경우 이를 불안전한 상태라고 말한다. TOE는 자신의 상태가 안전한지 판단할 수 있도록 본 마이크로커널에 탑재될 TSF 제어 흐름에서 분기 가능한 주소를 컴파일 시점에서 미리 파악하여 분기 가능 주소 테이블을 정적으로 생성한다. 이후 분기가 발생할 때마다 분기 목적 주소와 분기 가능 주소 테이블을 비교하여 해당 분기가 올바른 분기인지 파악한다. 또한 Stack Guard의 경우 스레드가 새로 할당되는 시점에 스택 내에서 일반 변수가 저장되는 영역과 스레드의 제어흐름을 결정할 수 있는 정보(ret 주소 등)가 저장되는 영역 사이에 고유한 특정 값을 일정크기만큼 채워둔다. 이후 스택에 대한 접근이 발생할 때마다 해당 영역에 대한 검사를 수행하며 만약 해당 영역이 기존에 채워둔

값과 상이할 경우 허가되지 않은 침범이 일어났다고 간주하여 불안전한 상태로 판단하게 된다. 일반 스레드가 아닌 TSF의 경우 TSF가 생성한 보안 이벤트 감사기록과 실제로 모니터링을 통해 얻은 감사기록을 서로 비교하여 일치할 경우 안전한 상태로 판단하게 되고, 그렇지 않을 경우 TSF가 올바르게 동작하지 못하여 불안전한 상태라고 판단하게 된다. 수행 중인 프로그램이 안전한 상태라고 판단되는 경우 해당 시점을 가장 최근 복원지점(Checkpoint)로 지정하고, 해당 시점의 메모리 값들과 레지스터 값 등 해당 스레드의 제어 흐름에 관한 모든 정보를 백업한다. 이후 TOE가 자신의 상태를 불안전하다고 판단할 경우 먼저 시스템은 무선 통신 스레드, 센서 처리 스레드와 같이 외부와 상호작용하는 스레드들을 Block 상태로 변환하여 안전모드로 진입한다. 이렇게 안전모드에 진입한 드론은 더 이상 외부로부터의 간섭을 받지 않도록 설정되어 안전하게 자가복구 기능을 수행할 수 있다. 안전모드에 진입한 후 불안전한 상태로 판단된 스레드의 종류에 따라 자가복구 과정이 두 가지로 나뉘게 된다. 첫 번째로, 불안전한 상태로 판단된 스레드가 자가복구를 수행하는 스레드 자신일 경우에는 사전에 프로그래머가 지정한 초기화 값을 이용하여 자기 자신을 초기화한다. 두 번째로, 타 스레드(예: 응용프로그램)가 불안전한 상태라고 판단된 경우 이전에 생성한 최근 복원지점으로 해당 스레드를 복원한다.

해당 체크포인트-복구 기능의 경우 다음과 같은 보안기능요구사항을 만족한다:

- FAU_GEN.1 (감사기록 생성)
- FPT_FLS.1 (안전한 상태 유지)
- FPT_ RCV.2 (자동 복구)
- FPT_TST.1 (TSF 자체 시험)

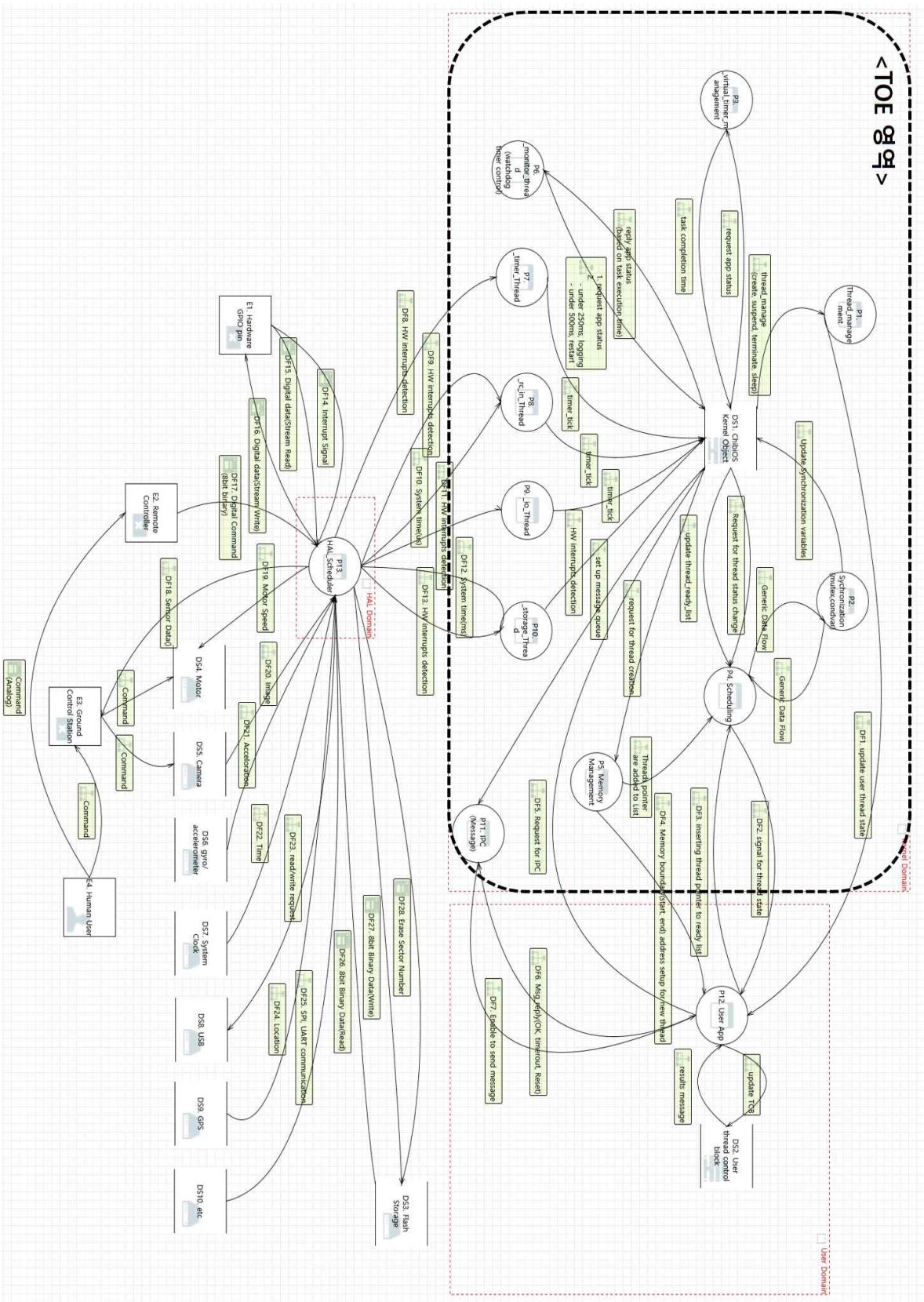
### 7.1.6. 실행횟수 기반 커널 스케줄링

드론 시스템이 무응답 상태에 빠지지 않도록 TOE는 스레드 실행횟수에 따라 자원에 대한 우선순위를 동적으로 부여함으로써 시스템의 가용성을 보장한다. 이때 무응답 상태는 드론 시스템에 탑재된 TOE 내 결함이나 에러에 의해 외부에서 요청한 서비스를 처리할 수 없는 상태를 의미한다. 먼저 실행햇수 기반 스케줄링을 수행하기 위해 TOE는 스케줄링 큐를 스캔하여 실행 상태가 ‘준비(Ready)’인 스레드 중 우선순위가 가장 높은 준비 스레드들을 우선적으로 식별한다. 가장 높은 우선순위를 가지는 준비 스레드의 수가 복수일 경우, TOE는 해당 스레드들의 실행횟수에 반비례한 순서로 스레드가 자원(CPU, Central Processing Unit)에 접근시킨다. 실행 횟수는 스레드 스레드가 자원을 얼마나 자주 할당받았는지에 대한 횟수를 의미하는 정보로 스레드 제어 블록에 저장된다. 이때 스레드 제어 블록에는 실행 횟수 뿐만 아니라 스레드가 자원을 사용할 수 있는 시간을 나타내는 타임 슬라이스 값이 존재하며, 해당 값은 타이머에 의해 틱(tick)이 발생할 때마다 1씩 감소한다. 타임 슬라이스가 다 사용되면 TOE는 현재까지 자원을 할당했던 스레드를 스케줄링 큐의 끝에 추가하고 자원을 회수한다. 이후 TOE는 실행횟수 기반 커널 스케줄링 기법에 따라 스케줄링 큐를 스캔한 후, 그 결과를 바탕으로 자원에 대한 접근을 허용할 새로운 스레드를 선택함으로써 TOE가 탑재된 전체 시스템의 가용성을 보장한다.

해당 실행회수 기반 커널 스케줄링 기능의 경우 다음과 같은 보안요구사항을 만족한다:

- FRU_PRS.1 (자원사용 우선순위)
- FRU_RSA.1 (최대 할당치)

# <부록 A. DFD>




[그림 3] 데이터 흐름도

# <부록B. 공격라이브러리>

| 번호 (AL = Attack Library) | 구분 (S, T, R, I, D, E) | | 이름/식별자 (논문 제목, CVE ID, CWE ID) | 취약점 발생 위치 | 취약점 내용 |
|---|---|---|---|---|---|
| AL1 | S | 논문 | Unmanned Aircraft Capture and Control Via GPS Spoofing | 센서 (GPS) | 공격자가 GPS 신호를 스푸핑하여 UAV의 지정된 제어 범위 초과 비행을 유도함으로써 드론을 획득하는 방법 제시 |
| AL2 | S | 논문 | Effect of Spoofing on Unmanned Aerial Vehicle using Counterfeited GPS Signal | 센서 (GPS) | 공격자가 GPS 신호를 스푸핑하여 UAV의 지정된 경로 이탈 등 비정상적인 작동을 유발하는 방법 제시 |
| AL3 | I | 논문 | Drone-Assisted Public Safety Networks: The Security Aspect | 와이파이 통신 | 공격자가 ARP 요청 재전송을 통해 다수의 IV(Initial Vector)값을 누적 수집하여 암호화 키를 해독하는 방법 제시 |
| AL4 | S | 논문 | | 센서 (GPS) | 공격자가 GPS 신호를 스푸핑하여 드론의 실시간 위치를 위조하고 공격자가 원하는 장소에 착륙하도록 유도하는 방법 제시 |
| AL5 | I | 논문 | Security of unmanned aerial vehicle systems against cyber-physical attacks | 와이파이 통신 | 공격자가 Wi-Fi 기반 통신 프로토콜을 사용하는 UAV를 크래킹하여 비행 경로를 조작하고 영상 피드를 획득하는 방법 제시 |
| AL6 | E | 논문 | Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things | 센서 | 공격자가 라즈베리파이를 통해 Wi-Fi에 연결된 드론과 제어 장치간 인증을 해제하여 드론을 탈취하는 방법 제시 |
| AL7 | E | 논문 | Security analysis of drones systems: Attacks, limitations, and recommendations | 기지국 (Ground Control Station) | 공격자가 원격 제어의 Reverse-shell TCP 페이로드를 만들어 기지국을 운영하는 시스템에 설치하는 방법 제시 |
| AL8 | T | | | 와이파이 통신 | 원격 측정 피드는 차량을 모니터링하고 개방형 무선 통신을 통해 정보를 전송하므로, 데이터 차단, 비행 경로 변경 등 데이터를 변조할 수 있는 취약점이 존재 |
| AL9 | S | | | 센서 (RF, GPS) | 공격자가 RF나 GPS 스푸핑을 통해 위조 신호를 전송하여 드론의 지정된 비행 경로를 변경하는 방법 제시 |
| AL10 | T | | | 와이파이 통신 | 공격자가 네트워크 트래픽을 가로채서 지속적으로 요청을 보내 드론과의 연결을 방해하는 방법 제시 |
| AL11 | I | CVE | CVE-2019-13120 | RTOS | Amazon FreeRTOS v1.4.8까지는 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | prvProcessReceivedPublish에 대한 길이 검사를 안하기 때문에 임의의 메모리 콘텐츠가 유출될 수 있는 취약점이 존재 |
| AL12 | I | CVE | CVE-2019-7715 | RTOS | Green Hills INTEGRITY RTOS 5.0.4의 Interpeak IPCOMShell TELNET 서버에서 sysvar 명령어를 이용하여 환경 변수 ipcom.shell.greeting 값을 설정하면 로그인 중에 사용자가 제어하는 형식 문자열이 생성되어 메모리 주소의 Information Leak이 발생하는 취약점이 존재 |
| AL13 | I | CVE | CVE-2019-7712 | RTOS | Green Hills INTEGRITY RTOS 5.0.4에있는 Interpeak IPCOMShell TELNET 서버의 handler_ipcom_shell_pwd에서 pwd 명령어를 사용할 때 적절한 검사가 시행되지 않아 사용자가 지정 형식 문자열을 확인하는 형식 문자열 수정자를 포함하는 경로를 위조하여 메모리 주소의 Information Leak이 발생하는 취약점이 존재 |
| AL14 | S | CVE | CVE-2018-16598 | RTOS | AWS FreeRTOS 1.3.1 이하 버전과 FreeRTOS V10.0.1 이하 버전, WITTENSTEIN WHIS Connect 미들웨어 TCP/IP는 xProcessReceivedUDPPacket 및 prvParseDNSReply에서 수신된 모든 DNS 응답이 전송된 DNS 요청과 일치하는지 확인하지 않고 수락하는 취약점이 존재 |
| AL15 | E | CVE | CVE-2018-16528 | RTOS | AWS FreeRTOS 1.3.1 이하 버전에서 prvSetupConnection의 mbedTLS 컨텍스트 객체 손상과 AWS TLS 연결 모듈의 GGD_SecureConnect_Connect로 인해 원격 공격자가 임의 코드를 실행할 수 있는 취약점이 존재 |
| AL16 | I | CVE | CVE-2014-2534 | RTOS | BlackBerry QNX Neutrino RTOS 6.4.x 및 6.5.x의 /sbin/pppoectl을 이용하면 로컬 사용자가 /etc/shadow에서 루트 암호 해시를 읽는 것처럼 오류메시지의 잘못된 매개 변수 행을 읽어 민감한 정보를 획득할 수 있는 취약점이 존재 |
| AL17 | I | CVE | CVE-2002-2409 | RTOS | QNX Neutrino RTOS 6.1.0 및 6.2.0의 Photon microGUI를 이용하여 16진수로 인코딩된 사용자 ID를 이름으로 갖는 디렉토리 내에서 1.TEXT 파일에 대한 요청을 통해 사용자 클립보드 정보를 열람할 수 있는 취약점이 존재 |
| AL18 | I | 논문 | Attack on the Drones | 부트로더 | 드론 Flight Controller의 부트로더가 잘 문서화되어 있어 해당 정보를 활용해 임의의 Custom Firmware를 업로드할 수 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 있는 취약점이 존재 |
| AL19 | I | | | 부트로더 | 부트로더가 통신에 사용하는 프로토콜이 제조사 또는 개발자에 의해 잘 정리되어 있어 이 정보를 이용하거나, 포트 스니핑 도구를 통해 직렬 통신 내용을 관찰하는 것으로 해당 프로토콜을 역공학할 수 있는 취약점이 존재 |
| AL20 | T, I | | | 펌웨어 | I2C, SPI 프로토콜에 대한 스니핑을 통해 드론 메모리 내 센서 데이터블록이 저장되는 위치를 특정하고, 해당 센서 데이터를 조작하여 펌웨어의 센서 정보 처리 루틴이 오동작하도록 유도할 수 있는 취약점이 존재 |
| AL21 | I, (E) | | | 하드웨어 (메인보드) | 아두이노와 같은 오픈소스 하드웨어일 경우 또는 목표 드론에 탑재된 메인보드(하드웨어)정보를 알고있을 경우 해당 정보를 통해 비슷한 전용 Testbed 하드웨어를 제작하여 이를 통해 센서 데이터를 획득하고 펌웨어를 변경할 수 있는 취약점이 존재 |
| AL22 | I, T | | | 센서 (GPS) | 펌웨어를 임의로 수정하여 GPS 센서 정보를 조작하거나 GPS 데이터를 획득하고, 위성신호와 동일한 주파수의 신호를 통해 GPS 정보를 변경하여 드론을 임의의 위치에 착륙시키거나 드론의 임무수행을 방해할 수 있는 취약점이 존재 |
| AL23 | S | | | 제어국 | 무인으로 운용되는 드론은 일반적으로 지상에 설치된 제어국(Ground Control Station)과 연결되어 있는데 이때 해당 제어국과 통신하는 특수한 프로토콜을 통하면 따로 관리자 인증없이 드론의 설정정보를 변경하는 등을 할 수 있음. 이를 통해 지상 제어국의 직렬 포트(UART, JTAG 등)에 직접 연결하여 해당 프로토콜을 역공학 하고, 획득한 정보를 통해 드론에게 원하는 명령을 내릴수 있는 취약점이 존재 |
| AL24 | S, T | 논문 | Vulnerability Analysis of AR.Drone 2.0, an | 와이파이 통신 | 드론은 Telnet과 FTP와 같은 포트들이 모두 열려 있고, 암호화가 수행되지 않아 외부 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 공격자가 중간에서 패킷을 변조하거나, 가짜 패킷을 만들어서 전송할 수 있는 취약점이 존재 |
| AL25 | E | | Embedded Linux System | 펌웨어 | 외부 공격자가 드론과 같은 네트워크에 연결하고 드론과 Telnet 연결을 하면 root 권한의 shell을 얻을 수 있음, 이를 통해 누구나 드론의 모든 파일에 접근할 수 있고, 파일 변조, 혹은 드론 재부팅 및 종료 명령을 실행하여 작동을 멈출 수 있는 취약점이 존재 |
| AL26 | S | | | 와이파이 통신 | 드론은 iptables를 사용하여 페어링 된 컨트롤러가 아닌 장치에서 패킷을 삭제하는데, 외부 공격자가 Python 라이브러리 Scapy를 통해 컨트롤러의 MAC주소를 스푸핑하고 시퀀스 번호를 변경하여 전송하면 페어링된 컨트롤러를 변경할 수 있는 취약점이 존재 |
| AL27 | E | CVE | CVE-2017-16544 | RTOS | 드론에서는 BusyBox를 실행하는데, 로컬 사용자가 BusyBox의 1.27.2 버전까지 libbb/lineedit.c에 있는 add_match 함수에서 디렉토리의 파일 이름 목록을 가져오는데 사용되는 쉘의 탭 자동 완성 기능은 파일 이름을 삭제하지 않고 터미널에서 이스케이프 시퀀스를 실행하여, 코드 실행, 임의 파일 쓰기를 할 수 있는 취약점이 존재 |
| AL28 | E | CVE | CVE-2014-9645 | RTOS | 1.23.0 이전 버전의 BusyBox에 있는 modutils/modprobe.c의 add_probe 함수를 통해 로컬 사용자가 모듈 이름에 / 문자를 사용하여 커널 모듈 로드에 대한 제한을 우회할 수 있는 취약점이 존재 |
| AL29 | D | CVE | CVE-2016-2147 | RTOS | 1.25.0 이전 버전의 BusyBox에서 DHCP 클라이언트의 Integer Overflow는 외부 공격자가 잘못된 RFC1035로 인코딩된 도메인 이름을 통해 서비스 거부 공격을 유발하여 Out-Of-Bound(범위를 벗어난) 힙 쓰기를 트리거할 수 있는 취약점이 존재 |
| AL30 | I, E | 논문 | Exploring security vulnerabilities of unmanned aerial vehicles | 와이파이 통신 | 드론의 Wi-Fi는 암호화 체계로 WEP(Wired Equipvalent Privacy)를 사용하므로, 외부 공격자에 의해 크래킹 될 수 있는 취약점이 존재 |
| AL31 | I | CVE | CVE-2019-5747 | RTOS | 1.30.0까지의 BusyBox의 udhcp 구성 요소에서 읽는 범위를 벗어난 경우 외부 공격자가 제작한 DHCP 메시지를 보내 스택에서 중요한 정보가 유출될 수 있는 취약점이 존재 |
| AL32 | I | CVE | CVE-2018-20679 | | |

| | | | | | |
|---|---|---|---|---|---|
| AL33 | T | CVE | CVE-2018-1000517 | RTOS | BusyBox wget 버전 8e2174e9bd836e53c8b9c6e00d1bc6e2a718686e 커밋 이전 BusyBox 프로젝트에 Heap Buffer Overflow를 일으킬 수있는 Busybox wget의 Buffer Overflow 취약점이 존재 |
| AL34 | T | CVE | CVE-2017-15874 | RTOS | BusyBox 1.27.2의 archival/libarchive/decompress_unlzma.c에는 읽기 액세스 위반이 가능한 Integer Underflow 취약점이 존재 |
| AL35 | T | CVE | CVE-2017-15873 | RTOS | BusyBox 1.27.2의 archival/libarchive/decompress_bunzip2.c에 있는 get_next_block 함수에는 쓰기 액세스 위반이 가능한 Integer Overflow 취약점이 존재 |
| AL36 | E | CVE | CVE-2011-2716 | RTOS | 1.20.0 이전 버전 BusyBox의 DHCP 클라이언트(udhcp)를 이용하면 원격 DHCP 서버가 HOST_NAME, DOMAIN_NAME, NIS_DOMAIN, TFTP_SERVER_NAME 호스트 이름 옵션의 쉘 메타 문자를 통해 임의의 명령을 실행할 수 있는 취약점이 존재 |
| AL37 | I | CVE | CVE-2014-2534 | RTOS | BlackBerry QNX Neutrino RTOS 6.4.x 및 6.5.x의 /sbin/pppoectl을 사용하면 로컬 사용자가 /etc/shadow에서 루트 암호 해시를 읽는 것처럼 오류 메시지의 잘못된 매개 변수 행을 읽어 민감한 정보를 획득할 수 있는 취약점이 존재 |
| AL37 | I, E | 논문 | Hacking and securing the AR.Drone 2.0 quadcopter: investigations for improving the security of a toy | 커널 | 공격자가 USB 드라이브를 드론에 연결하면 /data/video/usb/ 에 연결되어 USB 장치에 직접 액세스 할 수 있으며, 기밀 데이터에 액세스하거나 악성 파일을 저장할 수 있는 취약점이 존재 |
| AL38 | E | 논문 | Hacking and securing the AR.Drone 2.0 quadcopter: investigations for improving the security of a toy | 커널 | Telnet 포트에 연결하면 루트 계정으로 연결되는데, 루트 계정은 암호로 보호되지 않으므로 원격 공격자가 전체 드론 운영 체제에 자유롭게 액세스할 수 있는 취약점이 존재 |
| AL39 | E | 논문 | Hacking and securing the AR.Drone 2.0 quadcopter: investigations for improving the security of a toy | 커널 | 쉘 스크립트 /bin/reset_config.sh는 재설정 버튼을 사용하면 구성 파일 /data/config.ini만 재설정 되고 다른 파일은 그대로 유지됨. 이를 통해 원격 공격자가 재설정 버튼을 사용한 후에도 항상 드론에 액세스할 수 있는 취약점이 존재 |
| AL40 | S, T, | 논문 | Hacking and securing the AR.Drone 2.0 quadcopter: | 와이파이 통신 | 5556포트(ATCMD)가 UDP를 사용하므로, MiTM 공격을 통해 시퀀스 번호를 1로 새 |

| | | | | | |
|---|---|---|---|---|---|
| | I | | investigations for improving the security of a toy | | 명령을 전송하여 악의적인 명령을 전송할 수 있는 취약점이 존재 |
| AL41 | R | CVE | CVE-2010-0271 | HAL | Sun OpenSolaris snv_51에서 snv_130까지의 hald는 감사 로그에 기록하려는 지정되지 않은 시도 중에 proc_audit 권한을 갖지 않으므로, 로컬 사용자가 Hardware Abstraction Layer(HAL)을 지원하는 연결된 하드웨어 장치 세트에 대한 변경 사항을 감지하는 것을 우회할 수 있는 취약점이 존재 |
| AL42 | T, I, E | CVE | CVE-2018-16525 | RTOS | Amazon Web Services(AWS) FreeRTOS 1.3.1 버전까지, FreeRTOS V10.0.1 버전까지 및 WITTENSTEIN WHIS Connect 미들웨어 TCP/IP를 사용하면 원격 공격자가 prvParseDNSReply의 DNS\LLMNR 패킷을 파싱하는 동안 Buffer Overflow로 인해 임의 코드를 실행하거나 정보를 유출 가능 |
| AL43 | T, I, E | CVE | CVE-2018-16526 | RTOS | Amazon Web Services(AWS) FreeRTOS 1.3.1 버전까지, FreeRTOS V10.0.1 버전까지 및 WITTENSTEIN WHIS Connect 미들웨어 TCP/IP를 사용하면 원격 공격자가 usGenerateProtocolChecksum과 prvProcessIPPacket의 프로토콜 체크섬을 생성하는 동안 Buffer Overflow로 인해 임의 코드를 실행하거나 정보를 유출할 수 있는 취약점이 존재 |
| AL44 | I | CVE | CVE-2018-16524 | RTOS | AWS FreeRTOS 1.3.1 버전까지, FreeRTOS V10.0.1 버전까지 및 WITTENSTEIN WHIS Connect 미들웨어 TCP/IP는 prvCheckOptions에서 TCP 옵션을 구문 분석하는 동안 Information Leak 됨 |
| AL45 | I | CVE | CVE-2018-16527 | RTOS | AWS FreeRTOS 1.3.1 버전까지, FreeRTOS V10.0.1 버전까지 및 WITTENSTEIN WHIS Connect 미들웨어 TCP/IP는 prvProcessICMPPacket에서 ICMP 패킷을 구문 분석하는 동안 Information Leak이 발생할 수 있는 취약점이 존재 |
| AL46 | I | CVE | CVE-2018-16599 | RTOS | AWS FreeRTOS 1.3.1 버전까지, FreeRTOS V10.0.1 버전까지 및 WITTENSTEIN WHIS Connect 미들웨어 TCP/IP는 prvTreatNBNS에서 NBNS 패킷을 구문 분석하는 동안 범위를 벗어난 메모리 액세스가 Information Leak을 유발할 수 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 있는 취약점이 존재 |
| AL47 | I | CVE | CVE-2018-16600 | RTOS | AWS FreeRTOS 1.3.1 버전까지, FreeRTOS V10.0.1 버전까지 및 WITTENSTEIN WHIS Connect 미들웨어 TCP/IP는 eARPProcessPacket에서 ARP 패킷을 구문 분석하는 동안 범위를 벗어난 메모리 액세스가 Information Leak을 유발할 수 있는 취약점이 존재 |
| AL48 | D | CVE | CVE-2018-16601 | RTOS | AWS FreeRTOS 1.3.1 버전까지, FreeRTOS V10.0.1 버전까지 및 WITTENSTEIN WHIS Connect 미들웨어 TCP/IP는 악의적으로 제작된 IP헤더를 통해 prvProcessIPPacket에서 전체 메모리 공간 복사를 트리거하여 서비스 거부 및 원격 코드를 실행할 수 있는 취약점이 존재 |
| AL49 | I | CVE | CVE-2018-16602 | RTOS | AWS FreeRTOS 1.3.1 버전까지, FreeRTOS V10.0.1 버전까지 및 WITTENSTEIN WHIS Connect 미들웨어 TCP/IP는 prvProcessDHCPReplies에서 DHCP 응답을 구문 분석하는 동안 범위를 벗어난 메모리 액세스가 Information Leak을 유발할 수 있는 취약점이 존재 |
| AL50 | I | CVE | CVE-2018-16603 | RTOS | AWS FreeRTOS 1.3.1 버전까지, FreeRTOS V10.0.1 버전까지 및 WITTENSTEIN WHIS Connect 미들웨어 TCP/IP는 xProcessReceivedTCPPacket의 TCP 소스 및 대상 포트 필드에 대한 경계를 벗어난 액세스를 통해 데이터가 공격자에게 유출될 수 있는 취약점이 존재 |
| AL51 | T | CVE | CVE-2019-12256 | RTOS | Wind River VxWorks RTOS 6.9 및 vx7에는 IPv4 패킷의 IP 옵션을 구문 분석 시 발생 가능한 Buffer Overflow 취약점이 존재 |
| AL52 | T | CVE | CVE-2019-12257 | RTOS | Wind River VxWorks RTOS 6.6~6.9에는 idhcpc 내부 DHCP Offer/ACK 구문 분석 시 발생 가능한 Heap Overflow 취약점이 존재 |
| AL53 | I | CVE | CVE-2019-12265 | RTOS | Wind River VxWorks RTOS 6.5, 6.6, 6.7, 6.8, 6.9.3, 6.9.4에는 IGMPv3 클라이언트에 Memory Leak이 있어 특정 회원 보고서를 통한 IGMP 정보가 유출될 수 있는 취약점이 존재 |
| AL54 | T | CVE | CVE-2019-12263 | RTOS | Wind River VxWorks RTOS 6.9.4 및 vx7에는 Race Condition으로 인한 TCP Urgent Pointer State Confusion 때문에 TCP에 발생 가능한 Buffer Overflow 취약점이 존재 |

| | | | | | |
|---|---|---|---|---|---|
| AL55 | T | CVE | CVE-2019-12261 | RTOS | Wind River VxWorks RTOS 6.7~6.9 및 vx7에는 원격 호스트에 대한 connect() 동안 TCP Urgent Pointer State Confusion 때문에 TCP에 발생 가능한 Buffer Overflow 취약점이 존재 |
| AL56 | D | CVE | CVE-2019-12258 | RTOS | Wind River VxWorks RTOS 6.6 및 vx7에는 잘못된 TCP 옵션을 통해 세션이 고정되는 TCP 연결 DoS가 있는 취약점이 존재 |
| AL57 | T | CVE | CVE-2019-7714 | RTOS | Green Hills INTEGRITY RTOS 5.0.4의 Interpeak IPWEBS에서 HTTP 인증 헤더에 60 바이트를 할당하는데, 이 헤더를 복사하여 구문 분석할 때 헤더 크기를 확인하지 않아 스택 기반 Buffer Overflow 취약점이 존재 |
| AL58 | T | CVE | CVE-2019-7713 | RTOS | Green Hills INTEGRITY RTOS 5.0.4의 Interpeak IPCOMShell TELNET 서버에서 사용자 정의 수정자가 프로세스 ID, IP 주소 또는 현재 작업 디렉토리와 같은 정보를 표시하는데 사용되는 경우, 쉘 프롬프트를 출력하는 기능에 힙 기반 Buffer Overflow 취약점이 존재 |
| AL59 | I | CVE | CVE-2019-7711 | RTOS | Green Hills INTEGRITY RTOS 5.0.4의 Interpeak IPCOMShell TELNET 서버에서 문서화되지 않은 쉘명령 Prompt는 쉘의 프롬프트 값을 설정하는데, 이는 printf에 대한 형식 문자열 입력으로 사용되어 메모리 주소의 Information Leak 취약점이 존재 |
| AL60 | I | CVE | CVE-2017-5251 | 센서 (라디오 통신) | Insteon의 Insteon Hub 버전 1012에서는 허브와 연결된 장치 간의 통신에 사용되는 Radio 전송이 암호화되지 않는 취약점이 존재 |
| AL61 | D | CVE | CVE-2018-20823 | 센서 (자이로 스코프) | Xiaomi Mi 5s 기기의 자이로스코프를 사용하면 공격자가 MEMS 초음파 공격이라고하는 20.4kHz 오디오 신호를 통해 서비스 거부를 유발할 수 있는 취약점이 존재 |
| AL62 | I | CVE | CVE-2014-9689 | 센서 (자이로 스코프) | 41.0.2272.76 이전 Chrome의 content / renderer / device_sensors / device_orientation_event_pump.cc는 고속 자이로스코프 데이터에 대한 액세스를 적절하게 제한하지 않으므로 원격 공격자가 제작 된 웹 사이트를 통해 기기의 물리적 환경에서 음성 신호를 쉽게 획득할 수 있는 취약점이 존재 |
| AL63 | T | CVE | CVE- 2019-9534 | 센서 (GPS) | Cobham EXPLORER 710, 펌웨어 버전 1.07은 펌웨어 이미지의 유효성을 검사하지 않기 때문에, 개발단계동안 사용된 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 디버그용 스크립트가 펌웨어 내부에 남아있어 해당 스크립트를 활용하여 인증되지 않은 로컬 공격자가 GPS 트래픽을 스푸핑하거나 가로챌 수 있는 취약점이 존재 |
| AL64 | S | CVE | CVE-2020-0133 | 센서 (GPS) | MockLocationAppPreferenceController.java에서는 권한 우회로 인해 장치의 GPS 위치를 변경할 수 있는 취약점이 존재 |
| AL65 | E | CVE | CVE-2019-15340 | 센서 (GPS) | com.huaqin.factory 앱 (versionCode = 1, versionName = QL1715_201805292006)을 사용하면 액세스 권한 없이도 Wi-Fi, Bluetooth 및 GPS를 프로그래밍 방식으로 비활성화 및 활성화할 수 있는 취약점이 존재 |
| AL66 | T | CVE | CVE-2017-14918 | 센서 (GPS) | MSM 용 Android, MSM 용 Firefox OS, QRD Android에서 Linux 커널을 사용하는 CAF의 모든 Android Release와 GPS 위치 무선 인터페이스에서 Use After Free 발생 가능 |
| AL67 | E | CVE | CVE-2016-6727 | 센서 (GPS) | Android One 기기에서 Android의 Qualcomm GPS 하위 시스템을 사용하면 원격 공격자가 임의 코드를 실행할 수 있는 취약점이 존재 |
| AL68 | I | CVE | CVE-2016-6540 | 센서 (GPS) | TrackR Bravo에서 유지 관리하는 클라우드 기반 서비스에 대한 인증되지 않은 액세스는 적기 ID 번호를 사용하여 모든 Trackr 장치에 대한 GPS 데이터를 물어보거나 전송할 수 있는 취약점이 존재 |
| AL69 | S | CVE | CVE-2016-5348 | 센서 (GPS) | 4.4.4 이전 Android 4.x의 GPS는 중간 공격자가 스푸핑 된 Qualcomm gpsonextra.net 또는 izatcloud.net 호스트에서 큰 xtra.bin 또는 xtra2.bin 파일을 실행하여 서비스 거부를 유발할 수 있는 취약점이 존재 |
| AL70 | S | CVE | CVE-2016-5341 | 센서 (GPS) | 2016-12-05 이전 Android의 GPS를 사용하면 중간자 공격자가 스푸핑 된 Qualcomm gpsonextra의 잘못된 xtra.bin 또는 xtra2.bin 파일을 실행하여 서비스 거부를 할 수 있는 취약점이 존재 |
| AL71 | I | CVE | CVE-2014-9969 | 센서 (GPS) | Linux 커널을 사용하는 CAF의 Android 릴리스가 포함 된 모든 Qualcomm 제품에서 GPS 클라이언트가 안전하지 않은 암호화 알고리즘을 사용하는 취약점이 존재 |
| AL72 | I | CVE | CVE-2012-6335 | 센서 (GPS) | Android 용 AVG AntiVirus의 도난 방지 서비스를 사용하면 물리적으로 가까운 공격자가 GPS 위치 스푸퍼를 통해 임의의 위치 데이터를 제공할 수 있는 취약점이 |

| | | | | | 존재 |
|---|---|---|---|---|---|
| AL73 | I | CVE | CVE-2012-6334 | 센서 (GPS) | Samsung Galaxy 장치의 Android 용 SamsungDive 하위 시스템의 내 모바일 추적 기능은 위치 API를 제대로 구현하지 못하기 때문에, 물리적으로 가까운 공격자가 간단한 GPS 위치 스푸퍼를 통해 임의의 위치 데이터를 제공할 수 있는 취약점이 존재 |
| AL74 | S, E | CVE | CVE-2020-9349 | 센서 (카메라) | CACAGOO Cloud Storage 인텔리전트 카메라 TV-288ZD-2MP (펌웨어 3.4.2.0919 포함)를 사용하면 비밀번호 없이 RTSP 서비스에 액세스할 수 있는 취약점이 존재 |
| AL75 | S, E | CVE | CVE-2020-6852 | 센서 (카메라) | CACAGOO Cloud Storage 인텔리전트 카메라 TV-288ZD-2MP (펌웨어 3.4.2.0919)는 TELNET 액세스 인증이 취약하여 비밀번호 없이 루트 권한을 획득할 수 있는 취약점이 존재 |
| AL76 | S | CVE | CVE-2020-3507 | 센서 (카메라) | Cisco Video Surveillance 8000 Series IP 카메라에 대한 Cisco Discovery Protocol 구현 취약점으로 인해 인증되지 않은 인접 공격자가 원격으로 코드를 실행하거나 IP 카메라를 reload할 수 있는 취약점이 존재 |
| AL77 | S | CVE | CVE-2020-3506 | 센서 (카메라) | Cisco Video Surveillance 8000 Series IP 카메라에 대한 Cisco Discovery Protocol 구현 취약점으로 인해 인증되지 않은 인접 공격자가 원격으로 코드를 실행하거나 IP 카메라를 reload할 수 있는 취약점이 존재 |
| AL78 | S | CVE | CVE-2020-3110 | 센서 (카메라) | Cisco Video Surveillance 8000 Series IP 카메라에 대한 Cisco Discovery Protocol 구현 취약점으로 인해 인증되지 않은 인접 공격자가 원격으로 코드를 실행하거나 IP 카메라를 reload할 수 있는 취약점이 존재 |
| AL79 | I | CVE | CVE-2020-11625 | 센서 (카메라) | AvertX 카메라 HD838 및 HD438에서 존재하는 사용자 이름을 사용하여 웹 로그인 요청이 ISAPI / Security / sessionLogin / capabilities로 전송되면 암호가 잘못된 경우에도 해당 사용자 이름에 제공된 솔트 값을 반환하여, 브루트 포싱 공격할 수 있는 취약점이 존재 |
| AL80 | E | CVE | CVE-2020-0997 | 센서 (카메라) | Windows 카메라 코덱 팩이 메모리의 개체를 부적절하게 처리하는 경우 원격 코드를 실행할 수 있는 취약점이 존재 |
| AL81 | I | CVE | CVE-2020-0328 | 센서 (카메라) | Android-11 Android ID : A-150156131(취약점 참조 번호) 카메라에서 정수 오버플로우로 인해 시스템 실행 권한과 로컬 정보를 노출할 수 있는 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 취약점이 존재 |
| AL82 | S, E | CVE | CVE-2019-9657 | 센서 (카메라) | Alarm.com ADC-V522IR 0100b9 장치에는 VPN 인증서의 잘못된 보호로 인해 부적절한 접근통제를 할 수 있는 취약점이 존재 |
| AL83 | I | CVE | CVE-2019-7729 | 센서 (카메라) | Android 1.3.1 이전의 Bosch 스마트 카메라 앱에서 안전하지 않은 권한 설정으로 인해 악성 앱은 클립 공유를 위해 저장된 비디오 클립 또는 스틸 이미지를 검색할 수 있는 취약점이 존재 |
| AL84 | S | CVE | CVE-2019-7728 | 센서 (카메라) | Android 1.3.1 이전의 Bosch 스마트 카메라 앱에서 부적절하게 구현된 TLS 인증서 검사로 인해 원격 공격자가 일부 연결에 대해 중간자 공격을 실행할 수 있는 취약점이 존재 |
| AL85 | S, E | CVE | CVE-2019-5288 | 센서 (카메라) | ELLE-AL00B 9.1.0.193 (C00E190R2P1) 이전 버전의 P30 스마트 폰은 특정 매개 변수에 대한 불충분한 검사로 인해 정수 오버플로우 취약점이 존재하고, 이를 통해 공격자는 사용자를 속여 악성 애플리케이션을 설치하고 루트 권한을 획득할 수 있는 취약점이 존재 |
| AL86 | S, E | CVE | CVE-2019-5287 | 센서 (카메라) | ELLE-AL00B 9.1.0.193 (C00E190R2P1) 이전 버전의 P30 스마트 폰은 특정 매개 변수에 대한 불충분한 검사로 인해 정수 오버플로우 취약점이 존재하고, 이를 통해 공격자는 사용자를 속여 악성 애플리케이션을 설치하고 루트 권한을 획득할 수 있는 취약점이 존재 |
| AL87 | I | CVE | CVE-2019-5037 | 센서 (카메라) | Nest Cam IQ Indoor 카메라 버전 4620002에는 특수 제작된 Weave 패킷으로 인해 정수 오버플로우가 발생하고 매핑되지 않은 메모리에서 범위를 벗어난 부분의 정보를 획득할 수 있는 취약점이 존재 |
| AL88 | S | CVE | CVE-2019-3423 | 센서 (카메라) | C520V21 스마트 카메라 장치의 V2.1.14 이하 버전에는 공격자가 디렉토리 탐색 및 기타 무단 파일 또는 리소스에 대한 액세스할 수 있는 취약점이 존재 |
| AL89 | D | CVE | CVE-2019-14458 | 센서 (카메라) | 펌웨어가 0x20x 이전 인 VIVOTEK IP 카메라 장치는 제작된 HTTP 헤더를 통해 서비스 거부 공격 취약점이 존재 |
| AL90 | T | CVE | CVE-2019-14457 | 센서 (카메라) | 펌웨어가 0x20x 이전 인 VIVOTEK IP 카메라 장치에 제작된 HTTP 헤더를 통한 스택 기반 오버플로우 취약점이 존재 |
| AL91 | I | CVE | CVE-2019-13953 | 센서 (카메라) | YI M1 미러리스 카메라 V3.2-cn의 BLE (Bluetooth Low Energy) 인증 모듈에는 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 공격자가 BLE 명령을 전송하여, 민감한 데이터를 유출하거나, 카메라를 제어하여 녹화, 촬영할 수 있는 취약점이 존재 |
| AL92 | I, E | CVE | CVE-2019-12920 | 센서 (카메라) | Shenzhen Cylan Clever Dog Smart Camera DOG-2W 및 DOG-2W-V4 장치에서 공격자는 TELNET 로그인 프롬프트에서 하드 코딩된 루트 계정 비밀번호 12345678을 통해 카메라에 원격으로 로그인하여 루트 권한을 획득할 수 있는 취약점이 존재 |
| AL93 | S | CVE | CVE-2019-12919 | 센서 (카메라) | Shenzhen Cylan Clever Dog Smart Camera DOG-2W 및 DOG-2W-V4 장치에서 로컬 네트워크의 공격자는 포트 8000의 HTTP 서비스를 통해 내부 SD 카드에 인증되지 않은 액세스를 할 수 있는 취약점이 존재 |
| AL94 | I | CVE | CVE-2019-12763 | 센서 (카메라) | Android 1.6.8까지의 보안 카메라 CZ 애플리케이션은 녹화된 비디오를 외부 데이터 저장소에 저장하여 모든 애플리케이션에서 접근 가능한 취약점이 존재 |
| AL95 | D | CVE | CVE-2019-11878 | 센서 (카메라) | XiongMai Besder IP20H1 V4.02.R12.00035520.12012.047500.00200 카메라에서 동일한 로컬 네트워크에 있는 공격자는 정수 오버플로우를 통해 0x80000000보다 큰 크기의 필드를 가진 메시지를 전송하여 120초간 카메라를 크래시할 수 있는 취약점이 존재 |
| AL96 | S, I | CVE | CVE-2019-11014 | 센서 (카메라) | Eye4 응용 프로그램 (Android, iOS 및 Windows 용)에서 사용되는 VStarCam vstc.vscam.client 라이브러리 및 vstc.vscam 공유 개체는 카메라 서버의 스푸핑을 방지하지 않기 때문에, 가짜 카메라 서버를 제작하여 카메라 로그인 시 클라이언트가 전송하는 모든 정보를 획득할 수 있는 취약점이 존재 |
| AL97 | E | CVE | CVE-2019-10999 | 센서 (카메라) | D-Link DCS 시리즈 Wi-Fi 카메라에는 카메라의 웹 서버 인 alphapd에 스택 기반 버퍼 오버플로우 취약점이 존재하기 때문에, wireless.htm을 요청할 때 WEPEncryption 매개 변수에 긴 문자열을 제공하여 원격으로 인증된 공격자가 임의 코드를 실행할 수 있는 취약점이 존재 |
| AL98 | D | CVE | CVE-2018-9158 | 센서 (카메라) | AXIS M1033-W (IP 카메라) 펌웨어 버전 5.40.5.1 장치에서 공격자는 hping3 도구를 사용하여 IPv4 flooding 공격을 수행할 수 있는 취약점이 존재 |
| AL99 | S, | CVE | CVE-2018-7816 | 센서 | Pelco Sarix Enhanced Camera의 웹 기반 |

| | | | | | |
|---|---|---|---|---|---|
| | T | | | (카메라) | GUI에는 원격 공격자가 임의의 파일을 삭제할 수 있는 액세스 제어 취약점이 존재 |
| AL100 | D | CVE | CVE-2018-6479 | 센서 (카메라) | Netwave IP 카메라 장치에서 인증되지 않은 공격자가 큰 크기의 POST 요청을 URI로 전송하여 장치를 크래시할 수 있는 취약점이 존재 |
| AL101 | D | CVE | CVE-2018-6413 | 센서 (카메라) | V4.1.2 빌드 160203 이전의 Hikvision 카메라 DS-2CD9111-S에는 버퍼 오버플로우 취약점을 통한 서비스 거부 공격 취약점이 존재 |
| AL102 | I | CVE | CVE-2018-3947 | 센서 (카메라) | Yi Home Camera 27US 1.8.7.0D에는 네트워크 트래픽을 스니핑하여 정보를 획득할 수 있는 취약점이 존재 |
| AL103 | T | CVE | CVE-2018-3938 | 센서 (카메라) | Sony IPELA E 시리즈 카메라 G5 펌웨어 1.87.00의 802dot1xclientcert.cgi 기능에 악용할 수 있는 스택 기반 버퍼 오버플로우 취약점이 존재 |
| AL104 | E | CVE | CVE-2018-3937 | 센서 (카메라) | Sony IPELA E 시리즈 카메라 G5 펌웨어 1.87.00의 measurementBitrateExec 기능에 명령어를 주입할 수 있는 취약점이 존재 |
| AL105 | E | CVE | CVE-2018-3935 | 센서 (카메라) | Yi Home Camera 27US 1.8.7.0D에는 제작된 UDP 패킷 전송을 통해 네트워크 기능에 악용할 수 있는 코드 실행 취약점이 존재 |
| AL106 | E | CVE | CVE-2018-3934 | 센서 (카메라) | Yi Home Camera 27US 1.8.7.0D에는 제작된 UDP 패킷 전송을 통해 펌웨어 업데이트 기능에 악용할 수 있는 코드 실행 취약점이 존재 |
| AL107 | E | CVE | CVE-2018-3928 | 센서 (카메라) | Yi Home Camera 27US 1.8.7.0D에는 제작된 UDP 패킷 전송을 통해 펌웨어 업데이트 기능에 악용할 수 있는 코드 실행 취약점이 존재 |
| AL108 | E | CVE | CVE-2018-3910 | 센서 (카메라) | Yi Home Camera 27US 1.8.7.0D에는 조작된 SSID를 통해 명령 주입을 유발하여 클라우드 OTA 설정 기능에 악용 가능한 코드 실행 취약점이 존재 |
| AL109 | T, E | CVE | CVE-2018-3900 | 센서 (카메라) | Yi Home Camera 27US 1.8.7.0D의 QR 코드 스캔 기능에 버퍼 오버플로우를 통해 악용 가능한 코드 실행 취약점이 존재 |
| AL110 | T, E | CVE | CVE-2018-3899 | 센서 (카메라) | Yi Home Camera 27US 1.8.7.0D의 QR 코드 스캔 기능에 버퍼 오버플로우를 통해 악용 가능한 코드 실행 취약점이 존재 |
| AL111 | T, E | CVE | CVE-2018-3898 | 센서 (카메라) | Yi Home Camera 27US 1.8.7.0D의 QR 코드 스캔 기능에 버퍼 오버플로우를 통해 악용 가능한 코드 실행 취약점이 존재 |

| | | | | | |
|---|---|---|---|---|---|
| AL112 | T, E | CVE | CVE-2018-3892 | 센서 (카메라) | Yi Home Camera 27US 1.8.7.0D의 시간 동기화 기능에 버퍼 오버플로우를 통해 악용 가능한 펌웨어 다운그레이드 취약점이 존재 |
| AL113 | T, E | CVE | CVE-2018-3891 | 센서 (카메라) | Yi Home Camera 27US 1.8.7.0D의 펌웨어 업데이트 기능에 버퍼 오버플로우를 통해 악용 가능한 펌웨어 다운그레이드 취약점이 존재 |
| AL114 | E | CVE | CVE-2018-3890 | 센서 (카메라) | Yi Home Camera 27US 1.8.7.0D의 펌웨어 업데이트 기능에 논리 결함과, 명령 주입을 통해 악용 가능한 코드 실행 취약점이 존재 |
| AL115 | S, E | CVE | CVE-2018-20342 | 센서 (카메라) | Floureon IP 카메라 SP012는 적절한 액세스 제어없이 UART 직렬 인터페이스에 루트 터미널을 제공하는 취약점이 존재 |
| AL116 | S | CVE | CVE-2018-1170 | CAN 네트워크 | 무단 펌웨어 업데이트에 대한 적절한 보호 메커니즘이 없기 때문에 공격자가 임의의 CAN 메시지를 삽입 가능한 취약점이 존재 |
| AL117 | I | CVE | CVE-2010-4565 | CAN 네트워크 | Linux 커널 2.6.36 이하의 CAN에 있는 net/can/bcm.c의 bcm_connect 함수는 커널 메모리 주소가 포함 된 파일 이름을 사용하여 공개적으로 액세스 할 수있는 파일을 생성하고, 로컬 사용자가 이 파일 이름을 나열하여 커널 메모리 사용에 대한 민감한 정보 획득 가능한 취약점이 존재 |
| AL118 | D | CVE | CVE-2010-3874 | CAN 네트워크 | 64 비트 플랫폼의 2.6.36.2 이전 Linux 커널의 CAN에 있는 net/can/bcm.c의 bcm_connect 함수에서 로컬 사용자가 힙 기반 버퍼 오버플로우를 발생시켜 연결 작업을 통해 서비스 거부 공격 가능한 취약점이 존재 |
| AL119 | D | CVE | CVE-2010-2959 | CAN 네트워크 | 2.6.27.53 이전 Linux 커널의 CAN에 있는 net/can/bcm.c의 정수 오버플로우를 통해 공격자가 제작한 CAN 트래픽으로 임의의 코드를 실행하거나 서비스 거부 공격 가능한 취약점이 존재 |
| AL120 | S, I, E | 컨퍼런스 | Embedded Reversing - Recon2017 | RTOS | FreeRTOS는 C언어로 개발되었기 때문에 strcpy 등의 취약한 함수를 통해 버퍼오버플로우, 힙 커럽션 등 보안문제 발생 가능한 취약점이 존재 |
| AL121 | D | 논문 | Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR | 센서 (카메라) | 카메라에 다수의 노이즈 또는 스푸핑된 객체를 주입하여 사물(교통 표지판, 신호등) 인식 부하를 통한 서비스 거부 공격 가능한 취약점이 존재<br>(Google Driverless Car가 이런 문제에 취약) |
| AL122 | S, | 논문 | | 센서 | LiDAR(광 펄스를 방출하고 물체에 |

| | | | | | |
|---|---|---|---|---|---|
| | I | | | (범위 탐색) | 반사되어 돌아오는 시간을 측정하는 범위 탐색 센서)는 인코딩되지 않는 펄스를 방출하기 때문에, 중계기를 통해 재생 공격, 릴레이 공격을 하여 가짜 신호를 전송 가능한 취약점이 존재 |
| AL123 | S | 논문 | | 센서 (범위 탐색) | LiDAR는 인코딩되지 않는 펄스를 방출하기 때문에 스푸핑 공격을 통해 가짜 물체 생성 가능한 취약점이 존재 |
| AL124 | S, T | 논문 | | 무선 통신 | 공격자가 무선 통신 채널을 통해 장거리 차량 제어 가능한 취약점이 존재 |
| AL125 | I | 논문 | | 무선 통신 | 공격자가 무선 통신 채널을 통해 위치 정보 및 오디오 정보 유출 가능한 취약점이 존재 |
| AL126 | S, T, E | 논문 | | CAN 네트워크 | 공격자가 자동차 버스 시스템인 CAN 버스를 공격하여 운전자의 조작을 무시하고, 경고등, 에어백 제어, 브레이크 비활성화, 엔진 중지 등을 수행할 수 있는 취약점이 존재 |
| AL127 | S, T | 논문 | Fingerprinting Electronic Control Units for Vehicle Intrusion Detection | 차량 네트워크 | 공격자가 차량 내 네트워크에 스푸핑된 ID를 가진 임의의 메시지를 주입하여 차량 제어가 가능한 취약점이 존재 |
| AL128 | S, T | 논문 | | | 공격자가 안 메커니즘(예: 공유 비밀 키)을 구현하기 위해 사용되는 데이터를 포함하여 메모리에 저장된 모든 데이터에 대한 완전한 권한을 획득하여 예방 보안 메커니즘(예: MAC)이 ECU에 내장될 경우에도, 이를 비활성화 가능한 취약점이 존재 |
| AL129 | S, E | 논문 | Security Authentication System for In-Vehicle Network | CAN 네트워크 | 공격자가 ECU 소프트웨어를 악성 프로그램으로 대체 후, CAN 네트워크에 메시지를 전송할 수 있는 취약점이 존재 |
| AL130 | S, I | 논문 | Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks | CAN 네트워크 | CAN에서 전송되는 메시지는 모든 노드에 브로드 캐스트되므로, 악성 노드가 삽입될 경우 버스를 쉽게 도청하고 모든 프레임의 내용을 확인 가능한 취약점이 존재 |
| AL131 | S, E | 논문 | | CAN 네트워크 | CAN은 발신자를 인증하는 필드가 포함되지 않기 때문에, 다른 노드로 위장하여 메시지 전송 가능한 취약점이 존재 |
| AL132 | D | 논문 | | CAN 네트워크 | 공격자는 우선 순위가 높은 ECU로 CAN 버스를 채워서 다른 ECU가 전송을 하지 못하도록 유도 가능한 취약점이 존재 |
| AL133 | S, T | 논문 | | CAN 네트워크 | CAN은 CRC를 사용하여 메시지가 수정되었는지 확인하기 때문에 CRC를 위조하여 올바른 메시지로 위장 가능한 취약점이 존재 |

| | | | | | |
|---|---|---|---|---|---|
| AL134 | R | 논문 | | CAN 네트워크 | 올바른 ECU가 메시지를 보내거나 받지 않았음을 증명할 방법이 없는 취약점이 존재 |
| AL135 | S, R | 논문 | A System to Recognize Intruders in Controller Area Network (CAN) | CAN 네트워크 | CAN은 노드가 정상적인 노드인지 인증하지 않기 때문에, 공격자가 손상된 노드를 통해 메시지 전송 가능한 취약점이 존재 |
| AL136 | S | 논문 | | CAN 네트워크 | 공격자가 OBD 포트를 통해 CAN 버스에 액세스하여 포트와 상호 작용하여 CAN 네트워크 노드로 위장 가능한 취약점이 존재 |
| AL137 | I | 논문 | Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures | CAN 네트워크 | CAN 버스로 전송된 메시지는 해당 버스 시스템에 연결된 다른 모든 ECU에 의해 수신되기 때문에, 공격자는 CAN 버스 시스템에서 정보를 수집하여, 운전자의 개인 정보(운전 습관) 등 수집이 가능한 취약점이 존재 |
| AL138 | S, T | 논문 | | CAN 네트워크 | CAN 버스 메시지에 포함된 checksum이 올바르지 않을 경우 수신 노드에서 메시지의 위/번조 감지가 불가능한 취약점이 존재 |
| AL 139 | D | 논문 | Fork Bomb Attack Mitigation by Process Resource Quarantine | 커널 | 공격자나 커널 내부 오류로 인해 시스템 내 다량의 프로세스(스레드)가 생성되어 메모리와 CPU를 과도하게 점유하기 때문에 커널이 정상적으로 동작할 수 없는 취약점이 존재 |
| AL 140 | D | 논문 | How Attackers Abuse Computing Systems | 커널 | 공격자가 쉘 커맨드를 활용하여 시스템 내 다량의 프로세스(스레드)를 생성시켜 커널이 정상적으로 동작할 수 없게 만드는 취약점이 존재 |

[표 18] 공격 라이브러리

## <부록 C. 도출된 위협 목록>

| DFD Element | | No | STRIDE | 취약점 설명 | Attack Library 매핑 |
|---|---|---|---|---|---|
| P1 | thread_management | T1 | S | 공격자의 스레드가 Manager 스레드로 위장하여 일반 스레드에 대해 월권행위를 수행 | |
| | | T2 | T | 오버플로우 또는 언더플로우로 인한 허가되지 않은 메모리 쓰기를 통한 스레드 관리 데이터 변경 | AL34, AL35 |
| | | T3 | R | - | |
| | | T4 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | AL16, AL34 |
| | | T5 | D | 스레드를 강제로 종료시키거나 “Blocked“상태로 바꿔서 사용자의 요청에 대한 응답을 할 수 없도록 방해 | |
| | | T6 | E | 탑재될 모듈(스레드 프로그램)의 이름에 특수 문자를 삽입하여 커널의 모듈 로드 정책을 무시하고 임의의 모듈을 로드시킬수 있음 | AL28 |
| P2 | synchronization | T7 | S | 공격자의 스레드가 Syncronization 스레드로 위장하여 공유 메모리에 강제로 Mutex Lock 오퍼레이션 수행 | |
| | | T8 | T | 허가되지 않은 메모리 쓰기를 통한 임계영역에 위치한 데이터의 무단 변경 | AL34, AL35 |
| | | T9 | R | - | |
| | | T10 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | AL16, AL34 |
| | | T11 | D | 공유 자원에 대해 강제로 Mutex Lock 오퍼레이션을 수행하여 해당 자원을 사용할 수 없도록 방해 | |
| | | T12 | E | 공격자가 권한 상승을 위해 악성코드를 공유메모리에 삽입 | |
| P3 | _virtual_timer_management | T13 | S | 공격자의 스레드가 Virtual Timer Management 스레드로 위장하여 타이머에 대해 월권 행동을 수행 | |
| | | T14 | T | 허가되지 않은 메모리 쓰기를 통해 타이머의 시간값을 변경 | AL34, AL35 |
| | | T15 | R | - | |
| | | T16 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | AL16, AL34 |
| | | T17 | D | 가상 타이머에 잘못된 시간값을 입력하여 일반 스레드에 대한 강제적인 Timeout 유도 | |
| | | T18 | E | - | |
| P4 | scheduling | T19 | S | 공격자의 스레드가 Scheduling 스레드로 위장하여 임의의 스레드의 우선순위를 강제로 높히고 기아현상 유도 | |
| | | T20 | T | 허가되지 않은 메모리 쓰기 가능 스케줄링 우선순위를 임의의 순위로 변경 | AL34, AL35 |
| | | T21 | R | - | |
| | | T22 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | AL16, AL34 |
| | | T23 | D | 임의의 스레드의 우선순위를 강제로 높혀 기아현상을 유도 | |
| | | T24 | E | - | |
| P5 | memory management | T25 | S | 공격자의 스레드가 Memory Management 스레드로 위장하여 메모리 자원에 접근 | |
| | | T26 | T | 오버플로우 또는 언더플로우로 인한 허가되지 않은 | AL34, |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 메모리 쓰기 가능 | AL35 |
| | | T27 | T | ROP로 인한 부적절한 코드의 쓰기가 발생 | AL20 |
| | | T28 | R | 메모리 자원에 대한 오퍼레이션(Read, Write, Paging 등)을 수행 후 로그기록을 삭제 | |
| | | T29 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | AL16, AL34 |
| | | T30 | D | 스레드가 요구하는 메모리 자원을 할당해주지 않는 것으로 서비스 수행 방해 | |
| | | T31 | E | 시스템 리셋시 전체 메모리가 초기화되지 않고 특정 환경 설정만 초기화되어 초기화 이후에도 공격자의 악성 데이터가 남아있을 수 있음 | A39 |
| P6 | _monitor_thread | T32 | S | 공격자의 스레드가 monitor 스레드로 위장하여 일반 스레드에 대한 감시권한 획득 | |
| | | T33 | T | 허가되지 않은 메모리 쓰기를 통해 감사 내용을 무단으로 변경하거나 감사 기능을 무력화 | AL34, AL35 |
| | | T34 | R | - | |
| | | T35 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | AL16, AL34 |
| | | T36 | D | - | |
| | | T37 | E | 공격자의 스레드가 일반 스레드에 대한 감시 권한을 획득하여 해당 스레드에 대해 특정 관리기능 수행 | |
| P7 | _timer_thread | T38 | S | 공격자의 스레드가 timer 스레드로 위장하여 일반 스레드에 올바르지 않은 시간정보 제공 | |
| | | T39 | T | 허가되지 않은 메모리 쓰기를 통해 스레드 실행에 필요한 시스템 시간 정보를 무단으로 변경 | AL34, AL35 |
| | | T40 | R | - | |
| | | T41 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | AL16, AL34 |
| | | T42 | D | 잘못된 시간정보를 입력하여 일반 스레드가 정상적인 서비스를 제공하거나 제공받지 못하게 방해 | |
| | | T43 | E | - | |
| P8 | _rc_in_thread | T44 | S | 공격자의 스레드가 rc in 스레드로 위장하여 잘못된 조작 신호를 입력 | |
| | | T45 | T | 허가되지 않은 메모리 쓰기를 통해 원격 조종기로부터 수신한 데이터의 무단 변경 | AL34, AL35 |
| | | T46 | R | 원격 조종기와 기기 사이에 인증 및 전자서명이 없으므로 조작 신호를 입력하고 입력하지 않았다고 부인 | |
| | | T47 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | AL16, AL34 |
| | | T48 | I | 라디오 통신(기기과 리모트 콘트롤 기기 간의 통신)에 사용되는 데이터와 신호가 암호화되어 있지 않아 기기 제어정보가 유출될 수 있음 | AL60 |
| | | T49 | D | 대량의 조작신호를 입력하여 기기가 사용자의 신호를 처리하지 못하도록 방해 | |
| | | T50 | E | 주변 장치에 대한 액세스 권한 없이 커널 내부 스레드의 특정 행동을 통해 주변 장치를 강제로 활성화 시키거나 비활성화 시킬 수 있음 | AL65 |
| P9 | _io_thread | T51 | S | 공격자의 스레드가 io 스레드로 위장하여 잘못된 센서 값을 입력 | |

| | | | | | |
|---|---|---|---|---|---|
| | | T52 | T | 허가되지 않은 메모리 쓰기를 통해 읽기/쓰기 대상 주소의 변경 | AL34, AL35 |
| | | T53 | R | 센서와 기기 사이에 인증 및 전자서명 과정이 없으므로 임의의 센서값을 입력하고 이를 부인 | |
| | | T54 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | AL16, AL34 |
| | | T55 | D | 대량의 센서 데이터를 입력하여 정상적인 데이터를 처리하지 못하도록 방해 | |
| | | T56 | E | 주변 장치에 대한 액세스 권한 없이 커널 내부 스레드의 특정 행동을 통해 주변 장치를 강제로 활성화 시키거나 비활성화 시킬 수 있음 | AL65 |
| P10 | _storage_thread | T57 | S | 공격자의 스레드가 storage 스레드로 위장하여 내부 메모리에 쓰기를 시도 | |
| | | T58 | T | 허가되지 않은 메모리 쓰기를 통해 데이터 쓰기 목적 주소의 변경 | AL34, AL35 |
| | | T59 | R | 공격자가 저장공간에 접근을 시도한 후 해당 시도에 대한 기록을 삭제 | |
| | | T60 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | AL16, AL34 |
| | | T61 | D | 저장공간이 저장할 수 있는 양보다 많은 데이터를 저장하려고 시도하여 정상적인 운영이 불가하도록 방해 | |
| | | T62 | E | 시스템 리셋시 전체 메모리가 초기화되지 않고 특정 환경 설정만 초기화되어 초기화 이후에도 공격자의 악성 데이터가 남아있을 수 있음 | A39 |
| P11 | IPC | T63 | S | 공격자의 스레드가 IPC 스레드로 위장하여 통신을 위한 공유 메모리(버퍼, 메시지 큐 등)에 접근 | |
| | | T64 | T | 오버플로우 또는 언더플로우로 인한 허가되지 않은 메모리 쓰기 가능 | AL34, AL35 |
| | | T65 | R | IPC 요청 및 IPC 연결을 수락하고 관련한 기록을 삭제하여 이를 부인 | |
| | | T66 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | AL16, AL34 |
| | | T67 | D | 공유 메모리를 모두 사용하여 IPC 대상 프로세스간 정상적인 통신이 불가능하도록 방해 | |
| | | T68 | E | 특정 프로세스에 대해 권한이 없는 공격자가 해당 프로세스가 IPC에 사용하는 공유 메모리에 접근하여 임의의 코드 또는 값을 입력 | |
| DS1 | ChibiOS kernel object | T69 | T | 허가되지 않은 메모리 쓰기를 통해 커널 관리 데이터를 변조할 수 있음 | AL34, AL35 |
| | | T70 | R | 커널 오브젝트에 특정한 값을 삽입하고 관련 접근 기록을 삭제하여 이를 부인 | |
| | | T71 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | AL16 |
| | | T72 | D | 커널 오브젝트의 설정 값을 임의의 값으로 변경하여 커널의 행동을 방해 | |
| DF1 | update user thread state | T73 | T | 올바르지 않은 정보로 사용자 스레드를 업데이트 | |
| | | T74 | R | 공격자가 임의의 스레드에 대한 임의의 상태를 강제로 업데이트하고 이를 부인 | |
| | | T75 | I | 현재 실행중인 사용자 스레드 정보 유출(실행 중인 사용자 스레드 정보가 유출될 시 공격자는 자신의 코드를 실행시키기 위해 어느 메모리에 악성 코드를 올려야 할 | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 지 알 수 있다) | |
| | | T76 | D | DF1 - T와 연계, 스레드 상태를 강제로 “Suspend“ 또는 “Dead“로 업데이트 하여 서비스 거부 반응을 일으킬 수 있음 | |
| DF2 | signal for thread state | T77 | T | “Wake up“ 시그널을 “Suspend“ 또는 “Dead“ 시그널로 변조 | |
| | | T78 | R | - | |
| | | T79 | I | 시그널을 스니핑하여 “Wake up“ 대상 사용자 프로세스를 식별 | |
| | | T80 | D | “Wake up“ 시그널을 가로채어 스레드가 응답하지 않도록 조작 | |
| DF3 | inserting thread pointer to reay list | T81 | T | 잘못된 영역을 가리키는 포인터를 준비 리스트(Ready Queue)에 입력 | |
| | | T82 | R | - | |
| | | T83 | I | 해당 메시지를 스니핑하여 스레드에 접근할 수 있는 스레드 포인터 획득 | |
| | | T84 | D | 대량의 스레드 포인터를 입력하여 정상적으로 처리할 수 없도록 방해 | |
| DF4 | memory boundary address setup for new thread | T85 | T | 전달되는 메모리 영역을 공격자가 원하는 임의의 영역으로 변조 | |
| | | T86 | R | - | |
| | | T87 | I | 새로운 스레드가 사용할 메모리 영역의 주소 유출 | |
| | | T88 | D | 메시지를 가로채어 스레드가 생성되지 않도록 방해 | |
| DF5 | request for IPC | T89 | T | IPC 대상 프로세스 주소 및 PID를 공격자 임의의 프로세스로 변경 | |
| | | T90 | R | 공격자가 임의의 프로세스에 대한 IPC 요청을 보낸 후 이를 부인 | |
| | | T91 | I | 요청 메시지를 스니핑하여 IPC 대상 프로세스를 식별 | |
| | | T92 | D | 대량의 Request 메시지 전송 | |
| DF6 | message reply | T93 | T | 메시지 내용을 OK에서 Reset으로 변조 | |
| | | T94 | R | - | |
| | | T95 | I | 응답 메시지 내용을 스니핑하여 기밀정보 획득 | |
| | | T96 | D | 강제로 Reset 메시지를 전송하여 프로세스 간 IPC를 마비 | |
| | | T97 | D | 메시지를 여러번 반복하여 시스템 마비 | |
| DF7 | enable to send message | T98 | T | 정상적인 메시지 전송허가가 안되도록 메시지 변조 | |
| | | T99 | R | 공격자가 임의의 프로세스에 IPC 권한을 허가하고 하지 않았다고 부인 | |
| | | T100 | I | IPC 메시지 전송에 사용될 공유메모리 주소 유출 | |
| | | T101 | D | 정상 프로세스가 메시지를 송신할 수 없도록 강제로 메시지 거부 | |
| P12 | user application | T102 | S | 공격자가 사용자 스레드로 위장하여 커널에 부적절한 API 호출 | |
| | | T103 | T | 오버플로우 또는 언더플로우로 인한 허가되지 않은 메모리 쓰기 가능 | AL34, AL35 |
| | | T104 | R | 공격자가 사용자 스레드에 특정 서비스를 요청하고 하지 않았다고 이를 부인 | |
| | | T105 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 애플리케이션의 내부 정보 유출 가능 | AL16 |

| | | | | | |
|---|---|---|---|---|---|
| | | T106 | D | 공격자가 사용자 스레드에 대량의 데이터를 입력하여 정상적인 처리를 하지 못하도록 방해 | |
| | | T107 | E | P12 - S와 연계, 공격자가 사용자 스레드로 위장하여 시스템 콜을 통해 잘못된 인자를 커널에 전달 및 권한 획득 | |
| DS2 | user thread control block | T108 | T | 사용자 정의 스레드를 관리하기 위한 데이터를 무단으로 변경 | |
| | | T109 | R | TCB(Thread Control Block)에 특정한 값을 삽입하고 관련 접근 기록을 삭제하여 이를 부인 | |
| | | T110 | I | 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 시스템 내부 정보 유출 가능 | |
| | | T111 | D | TCB의 설정 값을 임의의 값으로 변경하여 커널의 행동을 방해 | |
| DF8 | HW interrupts detection | T112 | T | 인터럽트가 발생한 하드웨어의 종류 및 식별자를 조작할 수 있음 | |
| | | T113 | R | 인터럽트를 발생시키고 이에 대해 부인할 수 있음 | |
| | | T114 | I | 인터럽트에 대한 주요한 정보(인터럽트 주체, 인터럽트 내용 등)를 스니핑할 수 있음 | |
| | | T115 | D | 인터럽트 탐지 메시지를 대량으로 보내 SR(Interrupt Sevice Routine)이 제대로 된 처리를 할 수 없도록 방해 | |
| DF9 | HW interrupts detection | T116 | T | 인터럽트가 발생한 하드웨어의 종류 및 식별자를 조작할 수 있음 | |
| | | T117 | R | 인터럽트를 발생시키고 이에 대해 부인할 수 있음 | |
| | | T118 | I | 인터럽트에 대한 주요한 정보(인터럽트 주체, 인터럽트 내용 등)를 스니핑할 수 있음 | |
| | | T119 | D | 인터럽트 탐지 메시지를 대량으로 보내 ISR(Interrupt Sevice Routine)이 제대로 된 처리를 할 수 없도록 방해 | |
| DF10 | system time | T120 | T | 공격자가 시간정보를 조작하여 센서의 올바르지 않은 동작을 유도할 수 있음 | |
| | | T121 | R | - | |
| | | T122 | I | - | |
| | | T123 | D | 공격자가 시간정보를 조작하여 센서가 올바른 처리를 할 수 없도록 유도할 수 있음 | |
| DF11 | HW interrupts detection | T124 | T | 인터럽트가 발생한 하드웨어의 종류 및 식별자를 조작할 수 있음 | |
| | | T125 | R | 인터럽트를 발생시키고 이에 대해 부인할 수 있음 | |
| | | T126 | I | 인터럽트에 대한 주요한 정보(인터럽트 주체, 인터럽트 내용 등)를 스니핑할 수 있음 | |
| | | T127 | D | 인터럽트 탐지 메시지를 대량으로 보내 ISR(Interrupt Sevice Routine)이 제대로 된 처리를 할 수 없도록 방해 | |
| DF12 | system time | T128 | T | - | |
| | | T129 | R | - | |
| | | T130 | I | - | |
| | | T131 | D | 공격자가 시간정보를 조작하여 센서가 올바른 처리를 할 수 없도록 유도할 수 있음 | |
| DF13 | HW interrupts detection | T132 | T | 인터럽트가 발생한 하드웨어의 종류 및 식별자를 조작할 수 있음 | |
| | | T133 | R | 인터럽트를 발생시키고 이에 대해 부인할 수 있음 | |

| | | | | | |
|---|---|---|---|---|---|
| | | T134 | I | 인터럽트에 대한 주요한 정보(인터럽트 주체, 인터럽트 내용 등)를 스니핑할 수 있음 | |
| | | T135 | D | 인터럽트 탐지 메시지를 대량으로 보내 ISR(Interrupt Sevice Routine)이 제대로 된 처리를 할 수 없도록 방해 | |
| P13 | HAL_scheduler | T136 | S | 공격자가 스레드를 스케줄링 스레드로 위장하여 우선순위를 강제로 높일 수 있음 | |
| | | T137 | T | 공격자가 인터럽트가 발생한 하드웨어의 주소 및 인터럽트 내용을 무단으로 변경 | AL34, AL35 |
| | | T138 | R | HAL 프로세스(모듈)에 대한 적절하지 않은 권한 설정으로 HAL에 연결된 하드웨어 장치의 변경사항이 올바르게 기록되지 않을 수 있음 | AL41 |
| | | T139 | I | 공격자가 함수 또는 프로세스 호출 시 잘못된 매개변수를 읽어들여 중요 내부 정보 유출 가능 | AL16 |
| | | T140 | D | 임의의 스레드 우선순위를 강제로 높여 기아현상을 유도 | |
| | | T141 | E | - | |
| DF14 | digital command | T142 | T | 전송되는 조작 명령어를 변조하여 원하는 동작 명령 가능 | |
| | | T143 | R | 조작 명령어를 전송하고 해당 감사기록을 삭제하여 이를 부인 | |
| | | T144 | I | 전송되는 조작 명령어를 스니핑하여 기기의 동작을 예측 가능 | |
| | | T145 | D | 대량의 조작 명령어를 전송하여 정상적으로 움직일 수 없도록 방해 | |
| DF15 | sensor data | T146 | T | 전송중인 센서데이터를 변조하여 기기가 올바르게 동작할 수 없도록 방해 | |
| | | T147 | R | - | |
| | | T148 | I | I2C, SPI 프로토콜에 대한 스니핑을 통해 센서 데이터 정보 및 데이터 저장 위치를 파악 가능 | AL20 |
| | | T149 | D | 대량의 센서 데이터를 전송하여 정상적인 데이터 처리를 방해 | |
| DF16 | motor speed | T150 | T | 공격자가 원하는 모터 속도 값으로 변조 | |
| | | T151 | R | - | |
| | | T152 | I | I2C, SPI 프로토콜에 대한 스니핑을 통해 모터의 속도 정보와 정보가 저장되는 위치를 파악 가능 | AL20 |
| | | T153 | D | 대량의 모터 속도에 대한 데이터를 전송하여 모터가 정상적으로 동작하지 못하도록 방해 | |
| DF17 | acceloration | T154 | T | 센서의 가속도 정보를 변조할 수 있음 | |
| | | T155 | R | - | |
| | | T156 | I | I2C, SPI 프로토콜에 대한 스니핑을 통해 기기의 자세 정보가 처리되는 위치를 파악 가능 | AL20 |
| | | T157 | D | 가속도 정보를 비정상적으로 높이거나 줄여서 기기가 정상적인 동작을 할 수 없도록 방해 | |
| DF18 | time | T158 | T | 공격자가 시간 정보를 조작하여 센서의 올바르지 않는 동작을 유도 | |
| | | T159 | R | - | |
| | | T160 | I | I2C, SPI 프로토콜에 대한 스니핑을 통해 센서 데이터의 입출력 시간 정보와 저장되는 위치를 파악 가능 | AL20 |
| | | T161 | D | 공격자가 시간정보를 조작하여 센서가 올바른 처리를 할 수 없도록 유도 | |

| | | | | | |
|---|---|---|---|---|---|
| DF19 | read/write request | T162 | T | 읽기/쓰기 대상 메모리 주소를 임의의 주로로 변조할 수 있음 | |
| | | T163 | R | 공격자가 데이터 읽기/쓰기를 요청하고 이를 부인 | |
| | | T164 | I | 사용자가 보낸 읽기/쓰기 메시지를 스니핑하여 공격자가 자신의 코드를 입력할 수 있도록 사용자에게 읽기/쓰기가 허락된 메모리 주소 정보를 획득 | |
| | | T165 | D | 대량의 데이터 읽기/쓰기 요청을 보내 디바이스가 정상적인 읽기/쓰기 처리를 할 수 없도록 방해 | |
| DF20 | location | T166 | T | 공격자가 전송되는 위치 정보를 변조할 수 있음 | |
| | | T167 | R | - | |
| | | T168 | I | I2C, SPI 프로토콜에 대한 스니핑을 통해 위치 데이터 정보를 획득할 수 있음 | AL20 |
| | | T169 | D | 잘못된 위치값을 전송하여 기기가 정상적인 동작을 수행할 수 없도록 방해 | |
| DF21 | SPI, UART communication | T170 | T | 주고받는 SPI, UART 데이터를 변조하여 공격자가 임의의 데이터를 입력할 수 있음 | |
| | | T171 | R | - | |
| | | T172 | I | SPI, UART를 통해 전송되는 신호정보를 추출하여 기기 내부에서 발생하는 데이터 입출력 정보 획득 가능 | AL20 |
| | | T173 | D | 공격자가 버퍼 오버플로우 또는 정수 오버플로우를 유발시키는 데이터를 전송하여 임의의 코드를 실행 시키거나 서비스 거부 공격을 일으킬 수 있음 | AL119 |
| DF22 | 8bit binary data (write) | T174 | T | 전송중인 데이터를 변조하여 저장장치에 쓸 수 있음 | |
| | | T175 | R | - | |
| | | T176 | I | 악성 데이터 전송으로 내부 메모리 정보를 유출시킬 수 있음 | |
| | | T177 | D | 대량의 데이터를 쓰기 시도하여 장치의 입출력 기능을 방해할 수 있음 | |
| DF23 | 8bit binary data (read) | T178 | T | - | |
| | | T179 | R | - | |
| | | T180 | I | 전송중인 데이터를 스니핑 할 수 있음 | |
| | | T181 | D | 대량의 데이터를 읽어들여 장치의 입출력 기능을 방해할 수 있음 | |
| DF24 | erase sector number | T182 | T | 삭제될 영역 번호를 조작하여 중요한 영역을 파괴할 수 있음 | |
| | | T183 | R | - | |
| | | T184 | I | 해당 메시지를 스니핑 하여 삭제될 영역의 위치를 알아내 공격 코드를 탑재하기 위해 필요한 여유공간의 위치를 식별할 수 있음 | |
| | | T185 | D | 해당 메시지를 가로채어 데이터 삭제를 막는 것으로 저장공간을 확보하지 못하도록 방해할 수 있음 | |
| P14 | gyro/accelorator | T186 | S | 공격자가 자이로/가속도 센서로 위장하여 올바르지 않은 가속도 값을 입력할 수 있음 | |
| | | T187 | T | 장치에 업로드 되는 펌웨어에 개발 단계동안 사용된 디버그용 코드와 같은 내용을 제대로 삭제하지 않아 이를 통해 악성 사용자가 임의의 커스텀 펌웨어나 소프트웨어를 업로드 할 수 있음 | AL63 |
| | | T188 | R | - | |
| | | T189 | I | - | |

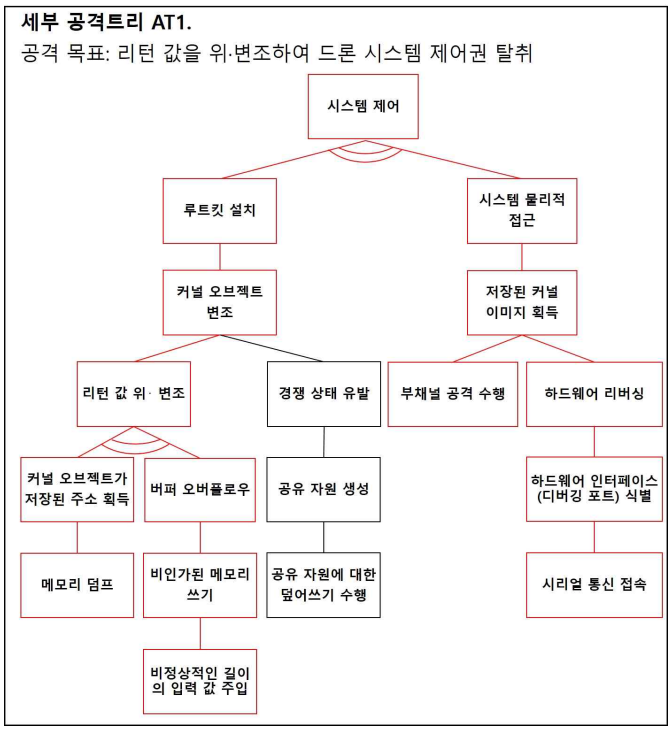
| | | | | | |
|---|---|---|---|---|---|
| | | T190 | D | 자이로스코프와 같은 MEMS 장치에 특정 주파수의 오디오 신호를 통해 서비스 거부 공격을 일으킬 수 있음 | AL61 |
| | | T191 | E | 자이로스코프 센서에 대한 권한 상승을 통해 공격자는 잘못된 자세제어 및 비행을 유도할 수 있음 | |
| P15 | system clock | T192 | S | 공격자가 하드웨어 RTC로 위장하여 올바르지 않은 시간 값을 입력 | |
| | | T193 | T | 시스템 시간 값을 임의의 값으로 변경 가능 | |
| | | T194 | R | - | |
| | | T195 | I | - | |
| | | T196 | D | 복수의 타이머 객체가 생성되어 시스템 성능을 저하시킬 수 있음 | |
| | | T197 | E | - | |
| P16 | GPS | T198 | S | 가짜 GPS 신호를 센서에 입력하여 현재 기기의 위치 정보에 대한 위장 가능 | AL1, AL2, AL4, AL9, AL22 |
| | | T199 | S | GPS 위성과 동일한 주파수의 신호를 GPS 센서에 보내서 현재 기기위치정보를 속일 수 있음 | AL22 |
| | | T200 | T | GPS 장치 내부적으로 적절하지 않은 데이터 검증 및 권한 검사로 인해 가짜 신호를 입력하지 않고 강제로 위치정보를 변경시킬 수 있음 | AL64 |
| | | T201 | T | GPS 모듈 내부에 개발에서 사용된 디버그용 코드가 잔존하여 이를 통해 악성 사용자가 임의의 GPS 신호를 전송할 수 있음 | AL63 |
| | | T202 | T | Use After Free 취약점을 통해 메모리 변조 가능 | AL66 |
| | | T203 | R | - | |
| | | T204 | I | GPS 신호 송출시 안전하지 않은 암호화 알고리즘을 사용하여 중간 공격자에게 정보가 유출될 수 있음 | AL71 |
| | | T205 | D | 잘못된 GPS 위치값을 통해 드론이 정상적인 임무를 수행할 수 없도록 방해 | |
| | | T206 | E | GPS 센서에 대한 권한 상승을 통해 공격자는 잘못된 목표위치로의 비행을 유도 가능 | |
| P17 | ETC | T207 | S | 공격자가 특정 센서로 위장하여 거짓된 센서 데이터를 입력 | |
| | | T208 | T | 펌웨어 내부에 디버그용 코드가 존재하여 공격자가 임의의 악성 펌웨어를 업로드 할 수 있음 | AL63 |
| | | T209 | I | 센서가 수집하고 처리한 데이터를 스니핑할 수 있음 | |
| | | T210 | D | 잘못된 센서 측정 값을 입력하여 정상적인 처리를 하지 못하도록 방해 | |
| | | T211 | D | 스니핑으로 획득한 신호를 지속적으로 재전송하여 서비스가 정상적으로 제공되지 못하도록 방해 | |
| | | T212 | E | 센서에 대한 권한 상승을 통해 잘못된 신호정보를 통해 오작동을 유도할 수 있음 | |
| DS3 | Flash Storage | T213 | T | 공격자가 변조된 데이터를 전송하거나 저장 가능 | |
| | | T214 | R | - | |
| | | T215 | I | 펌웨어, 부트로더에 대한 정보(메모리 구조, 내용 등)가 모두 문서화 되어있어 커스텀 펌웨어, 부트로더에 대한 정보를 획득할 수 있음 | AL18, AL19 |
| | | T216 | I | 특정 디렉토리 내부에 있는 파일에 대한 읽기 요청을 통해 클립보드와 같이 메모리 내부에 저장된 데이터가 | AL17 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 유출될 수 있음 | |
| | | T217 | I | 특정 프로토콜 또는 알고리즘으로 인하여 파일 생성시 해당 파일 이름에 관련 커널 메모리 주소가 포함될 수 있고 이로 인해 파일 이름을 통해 특정 내부 데이터의 위치가 유출될 수 있음 | AL117 |
| | | T218 | D | 저장장치 내부를 불필요한 데이터로 가득채워 더 이상 정상적인 데이터를 저장할 수 없도록 방해 | |
| DS4 | motor driver | T219 | T | 모터 회전속도를 조작하여 시스템이 모터에 불필요한 전력 또는 부족한 전력을 전달할 수 있음 | |
| | | T220 | R | - | |
| | | T221 | I | - | |
| | | T222 | D | 기능 수행 명령을 끊임없이 전달하여 시스템 성능이 저하될 수 있음 | |
| DS5 | USB | T223 | T | 변조된 데이터를 전송하거나 저장할 수 있음 | |
| | | T224 | R | USB를 통해 데이터 읽기/쓰기를 수행한 뒤, 접근 기록을 삭제하여 접근 사실을 부인할 수 있음 | |
| | | T225 | I | 특정 디렉토리 내부에 있는 파일에 대한 읽기 요청을 통해 클립보드와 같이 메모리 내부에 저장된 데이터가 유출될 수 있음 | AL17 |
| | | T226 | I | 드라이버 파일 또는 특정 메모리 영역에 접근하여 USB장치 내부에 존재하는 기밀 데이터에 접근할 수 있음 | AL37 |
| | | T227 | D | 대량의 데이터를 입출력하여 USB 장치가 정상적으로 동작할 수 없도록 방해 | |
| | | T228 | E | 드라이버 파일 또는 특정 메모리 영역에 접근하여 USB장치 내부에 임의의 데이터를 저장할 수 있음 | AL37 |
| E1 | remote controller | T229 | S | 공격자가 위장된 원격 조종 명령을 전송하여 기기를 임의대로 조종 가능 | |
| | | T230 | R | 공격자가 기기에 임의의 명령을 내린 후 자신이 하지 않았다고 이를 부인 | |
| E2 | ground control station | T231 | S | 일반 사용자가 관리자로 위장하여 원하는 명령을 지상 기지국을 경유하여 드론에 보낼 수 있음 | AL23 |
| | | T232 | S | 무단 펌웨어 업데이트로 인하여 공격자가 원하는 메시지 또는 명령어(예: backdoor를 트리거 시키는 명령어 등)를 내부에 강제로 탑재하여 정상 명령어처럼 위장할 수 있음 | AL116 |
| | | T233 | R | 공격자가 기지국을 통해 기기에 특정 서비스를 요청한 후 이를 부인 | |
| | | T234 | E | Reverse-shell TCP 페이로드를 설치하여 드론 또는 기지국 운영체제의 관리 권한 획득 가능 | AL7 |
| E3 | human | T235 | S | 공격자가 임의의 정상 사용자 및 관리자로 위장 | |
| | | T236 | R | 공격자가 특정한 서비스에 대해 요청한 후 이를 부인 | |

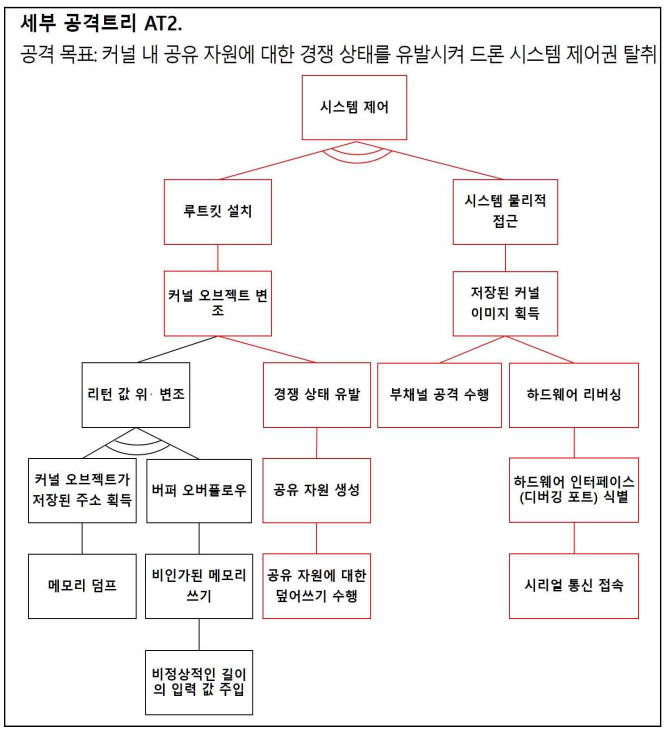
[표 19] 위협 목록

# <부록 D. 공격 트리>

## ○ 시스템 제어권 탈취 관련 공격 트리

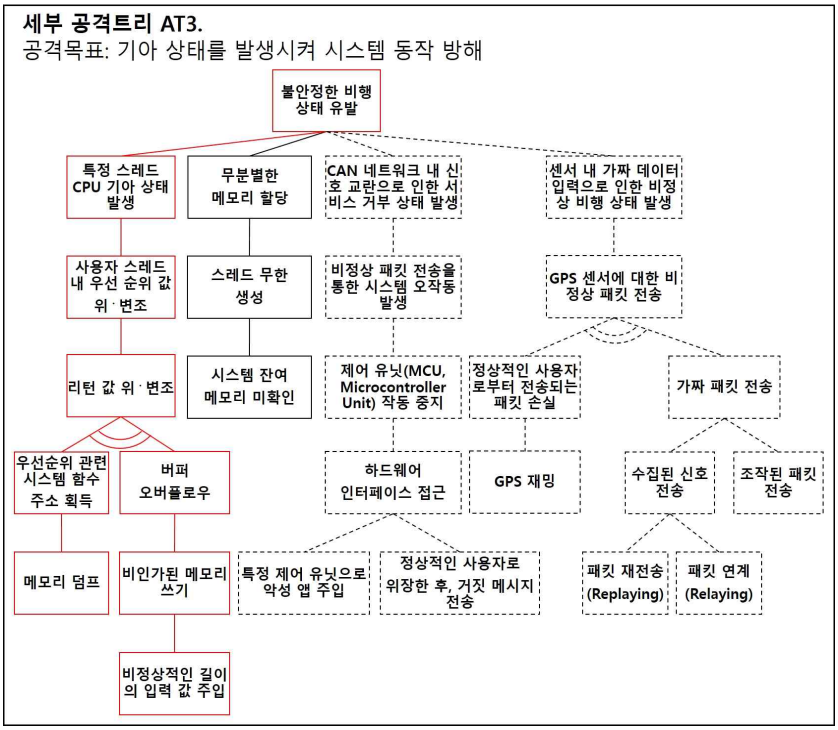



[그림 4] 세부 공격트리1

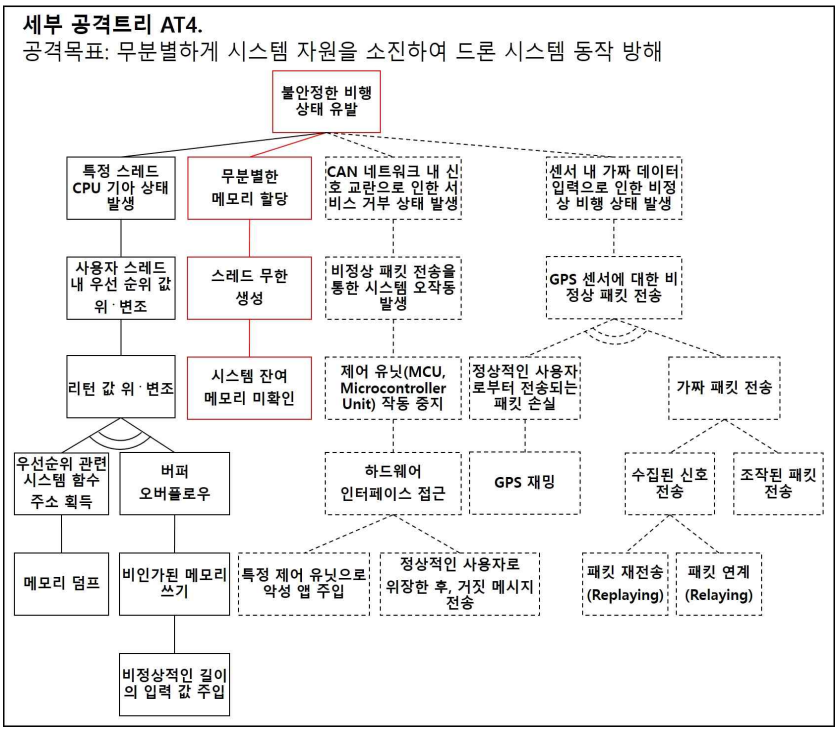



[그림 5] 세부 공격트리2

○ 불안정한 비행 상태 유발 관련 공격 트리




[그림 6] 세부 공격트리3




[그림 7] 세부 공격트리4

# <부록 E. 보안기능 요구사항 도출>

○ 시스템 제어권 탈취 관련 공격을 완화할 수 있도록 보안기능 요구사항 매핑

| 공격 목표 | | | | | | | | 위협 | 관련 보안기능 요구사항 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 시스템 제어 | | | | | | | - | |
| AND | 1.1 | 루트킷 설치 | | | | | | - | |
| | OR | 1.1.1 | 커널 오브젝트 변조 | | | | | - | |
| | | OR | 1.1.1.1 | 리턴 값 위·변조 | | | | - | |
| | | | AND | 1.1.1.1.1 | 커널 오브젝트 관리 함수의 주소 획득 | | | - | |
| | | | | | 1.1.1.1.1.1 | 주 메모리 덤프 | | T27, T75, T87, T100, T164 | |
| | | | AND | 1.1.1.2.1 | 버퍼 오버플로우 | | | - | |
| | | | | | 1.1.1.2.1.1 | 비인가된 메모리 쓰기 | | - | |
| | | | | | | 1.1.1.2.1.1 | 비정상적인 길이의 입력 값 주입 | T2, T8, T14, T20, T26, T33, T39, T45, T52, T58, T64, T69, T103, T108, T137, T185 | 안전 상태 유지 (FPT_FLS) |
| | | | | | | | | | 안전한 복구 (FPT_RCV) |
| | | | | | | | | | 자체 시험 (FPT_TST) |
| | | | | | | | | | 식별 (FIA_UID) |
| | | | | | | | | | 보안 역할 (FMT_SMR) |
| | | OR | 1.1.1.2 | 경쟁조건 취약점 공격 | | | | - | |
| | | | | 1.1.1.2.1 | 공유 자원에 대한 덮어쓰기 수행 | | | - | 식별 (FIA_UID) |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 보안 역할 (FMT_SMR) |
| | | | | | 1.1.1.2.1.1 | 공유 자원 생성 | T24, T31, T174 | |
| AND | 1.2 | 시스템 물리적 접근 | | | | | - | |
| | AND | 1.2.1 | 저장된 커널 이미지 획득 | | | | - | |
| | | OR | 1.2.1.1 | 부채널 공격 수행 | | | - | |
| | | OR | 1.2.1.2 | 하드웨어 리버싱 | | | - | |
| | | | | 1.2.1.1.1 | 하드웨어 인터페이스(디버깅 포트) 식별 | | - | |
| | | | | | 1.2.1.1.1.1 | 시리얼 통신 접속 | T160, T164, T168, T172, T180 | |

[표 20] 세부 공격트리1,2를 완화할 수 있도록 보안기능 요구사항 매핑

○ 불안정한 비행 상태 유발과 관련된 공격을 완화할 수 있도록 보안기능 요구사항 매핑

| 공격 목표 | | | | | | | | 위협 | 관련 보안기능 요구사항 |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 불안정한 비행 상태 유발 | | | | | | | - | |
| OR | 2.1 | 스레드에 대한 CPU 기아 상태 유발 | | | | | | - | |
| | OR | 2.1.1 | 사용자 스레드 내 우선순위 값 위·변조 | | | | | - | |
| | | | 2.1.1.1 | 리턴 값 위·변조 | | | | - | |
| | | | AND | 2.1.1.1.1 | 우선순위 관련 시스템 함수 주소 획득 | | | - | |
| | | | | | 2.1.1.1.1.1 | 메모리 덤프 | | T160, T164, T168, T172, T180, T182, T184 | |
| | | | AND | 2.1.1.1.2 | 버퍼 오버플로우 | | | - | |
| | | | | | 2.1.1.1.2.1 | 비인가된 메모리 쓰기 | | - | |
| | | | | | | 2.1.1.1.2.1.1 | 비정상적인 길이의 입력 값 주입 | T2, T8, T14, T20, T26, T33, T39, T45, T52, T58, T64, T69, T103, T108, T137, T185 | 안전 상태 유지 (FPT_FLS.1) |
| | | | | | | | | | 안전한 복구 (FPT_RCV.1) |
| | | | | | | | | | 자체 시험 (FPT_TST.1) |
| | | | | | | | | | 우선순위 부분적용 (FRU_PRS.1) |
| | | | | | | | | | 인증 (FIA_UAU) |
| | | | | | | | | | 보안속성 관리 (FMT_MSA) |
| | | | | | | | | | 식별 (FIA_UID) |
| | | | | | | | | | 보안기능 관리 (FMT_MOF) |
| OR | 2.2 | 무분별한 메모리 할당 | | | | | | - | |
| | | 2.2.1 | 스레드 무한 생성 | | | | | - | |
| | | | 2.2.1.1 | 시스템 잔여 메모리 미확인 | | | | T67 | 최대 할당치 제한 |

| | | | | | | | | (FRU_RSA.1) |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 식별 (FIA_UID) |
| | | | | | | | | 보안기능 관리 (FMT_MOF) |
| | | | | | | | | 관리기능 명세 (FMT_SMF) |
| | | | | | | | | TSF 데이터 관리 (FMT_MTD) |
| OR | 2.2 | CAN 네트워크 내 신호 교란으로 인한 서비스 거부 상태 발생 | | | | | - | |
| | OR | 2.2.1 | 비정상 패킷 전송을 통한 시스템 오작동 발생 | | | | - | |
| | | | 2.2.1.1 | 제어 유닛(MCU, Microcontroller Unit) 작동 중지 | | | - | |
| | | | AND | 2.2.1.1.1 | 하드웨어 인터페이스 접근 | | T170, T172, T190, T191, T199, T206, T207, T208, T212 | |
| | | | | OR | 2.2.1.1.1.1 | 특정 제어 유닛으로 악성 앱 주입 | T149, T153, T157, T161 | |
| | | | | OR | 2.2.1.1.1.2 | 정상적인 사용자로 위장한 후, 거짓 메시지 전송 | T186, T192, T198, T199, T207 | |
| OR | 2.3 | 잘못된(거짓) 센서 데이터 입력 | | | | | - | |
| | OR | 2.3.1 | GPS 센서에 대한 비정상 패킷 전송 | | | | - | |
| | | AND | 2.3.1.1 | 정상적인 사용자로부터 전송되는 패킷 손실 | | | - | |
| | | | | 2.3.1.1.1 | GPS 재밍 | | - | |
| | | AND | 2.3.1.2 | 가짜 패킷 전송 | | | - | |
| | | | | 2.3.1.2.1 | 수집된 신호 전송 | | - | |
| | | | | OR | 2.3.1.2.1.1 | 패킷 재전송 (Replaying) | T211 | |
| | | | | | 2.3.1.2.1.2 | 패킷 연계 (Relaying) | T198, T200, T207 | |
| | | | | 2.3.1.2.2 | 조작된 패킷 전송 | | T198, T200, T205 | |

[표 21] 세부 공격트리3, 4를 완화할 수 있도록 보안기능 요구사항