캡스톤디자인II 중간보고서

<table>
<tr><td rowspan="2">제 목</td><td colspan="2">국문</td><td colspan="3">이중 통신을 이용한 보안 드론 제작</td></tr>
<tr><td colspan="2">영문</td><td colspan="3">Analysis of security vulnerabilities in drone-based wireless networks</td></tr>
<tr><td rowspan="2">진 행
상 황</td><td>중요마일스톤</td><td colspan="4">1) 드론 제작 및 통신 프로토콜 이해- 픽스호크 f450를 제작 후 Python을 사용하여 드론을 조작하는 기본 API를 테스트
2) 보안 알고리즘 설계 및 적용- 선행 연구가 없는 알고리즘을 고안하여 보안 알고리즘을 설계 및 제작 드론에 적용
3) RF 신호처리 알고리즘 구현 - RF 송수신 기기에서 얻은 GPS 정보를 기반으로 신호 세기를 판단하여 GPS 스푸핑을 감지할 수 있는 신호 처리 알고리즘을 개발.
4)보안 위협 시뮬레이션 - 캡스톤I 실습 내용을 이용해 Deauth 공격으로 드론의 통제권을 획득 및 GPS 스푸핑 시도
5) 패킷 분석 - 4) 의 시도에서 얻게된 패킷을 확인하여 암호화가 되어있는지 확인.
6) 연구 보고서 작성 - 보안 취약점, 개선된 보안 메커니즘을 종합하여 보고서를 작성</td></tr>
<tr><td>진행상황</td><td colspan="4">1. Kali Linux 툴을 사용한 패킷 스니핑, Deauth, Brute Force실습 및 GPS 스푸핑 실습 완료
2. WIFI와 RF(Radio Frequency) 기반의 이중 통신을 통해 동일한 정보를 전송한 후, WIFI로 받은 정보와 RF로 받은 정보가 일치하는지 확인하는 보안 알고리즘 구상 완료
3. GPS 스푸핑을 방지하기 위해 신호 세기를 조절하는 알고리즘 구상 완료</td></tr>
<tr><td>t산출물</td><td colspan="5">요구사항 정의서(별첨 1), 중간보고서(별첨 2)</td></tr>
<tr><td rowspan="4">팀
구성원</td><td>학년</td><td>학 번</td><td>이 름</td><td colspan="2">연락처(전화번호/이메일)</td></tr>
<tr><td>4</td><td>20211870</td><td>김슬기</td><td colspan="2">010-5269-1194
20211870@edu.hanbat.ac.kr</td></tr>
<tr><td>4</td><td>20191759</td><td>홍준기</td><td colspan="2">010-4814-9218
20191759@edu.hanbat.ac.kr</td></tr>
<tr><td>4</td><td>20201773</td><td>손성호</td><td colspan="2">010-9436-7994
20201773@edu.hanbat.ac.kr</td></tr>
</table>

컴퓨터공학과의 프로젝트 관리규정에 따라 다음과 같이 요구사항 정의서와 중간보고서를 제출합니다

2024년 9월 6일

책임자 : 김슬기 (인)

지도교수 : 김태훈 (인)

[별첨1]

프로젝트명 : 이중 통신을 이용한 보안 드론 제작

소프트웨어 요구사항 정의서

Version 1.0

개발 팀원 명(팀리더):김슬기

홍준기

손성호

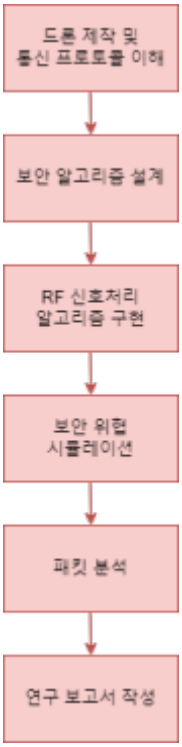
대표 연락처:010-5269-1194

e-mail: 20211870@edu.hanbat.ac.kr

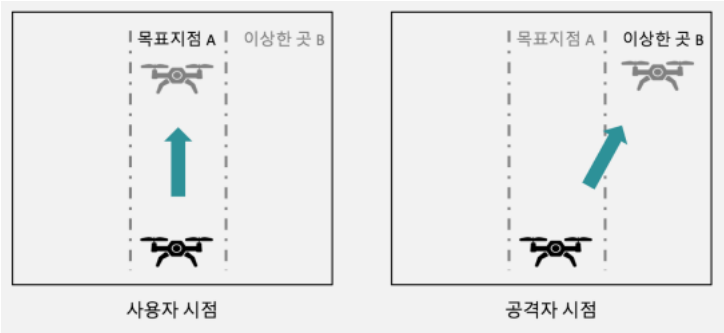
목차

1. 시스템 개요

무료 서비스인 와이파이는 다른 무선 네트워크 서비스에 비해 보안이 취약하다는 단점이 있다. 게다가 비밀번호를 설정하더라도, 너무 간단한 비밀번호는 딕셔너리 공격에 취약해 보안이 쉽게 뚫릴 수 있다는 단점이 있다. 따라서 와이파이 네트워크 운영 시 보안 강화를 위해 추가적인 RF 신호를 이용해 무선 네트워크의 취약점을 보완한다. 시스템의 구성은 다음과 같다.



프로젝트의 목표는 드론을 GPS 스푸핑과 통제권 탈취와 같은 공격으로부터 안전하도록 제작하는 것이다. 주요 기능은 컨트롤러를 이용해 드론을 조종할 때, 수신 신호가 빠른 WiFi와 수신 신호가 느린 RF 신호를 동시에 송수신하는 것이다. 드론은 WiFi 신호의 명령을 따라 움직이며, 명령의 순서를 기억해 RF 신호와 대조하여 이상이 발생했다고 판단되면 RF 신호를 이용하여 GPS 신호를 수신하고, 수신받는 신호의 세기를 일정하게 유지함으로써 GPS 스푸핑을 방지한다.



2. 시스템 장비 구성요구사항

■ **작성 내역(기본 사항- 반드시 작성)**

≫ 장비품목: 픽스호크 f450, Kali Linux, Raspberry Pi, HackRF-one, Telescopic Antenna wrl-13002

≫ 장비 수량 : 픽스호크 f450 1개, Kali Linux 1개, Raspberry Pi 1개, HackRF-one 1개, Telescopic Antenna wrl-13002 1개

≫ 장비 기능 :

- 픽스호크 f450: 보안 알고리즘 및 GPS 스푸핑 방지 기능을 추가할 드론
- Kali Linux: 검증 테스트에서 패킷 분석과 공격 진행
- Raspberry Pi: 드론세팅 및 알고리즘 추가 방법
- HackRF-one, HackRF: GPS 스푸핑 검증 테스트에서 사용 될 무선 신호 송수신 장치

≫ 장비 성능 및 특징 :

- 픽스호크 f450: 와이파이를 통한 연결, RF 신호로 검증 하도록 조정
- Kali Linux: Linux 기반 운영체제로 해킹 툴이 내장됨
- Raspberry Pi: 초소형/초저가 PC
- HackRF-one, HackRF: 무선 신호를 생성하여 신호 변조(스푸핑) 가능

3. 기능 요구사항

요구사항고유번호		SFR-FA-001		
요구사항 명칭		Kali Linux		
요구사항 분류		기능	응락수준	필수
요구사항 세부내용	정의	모의해킹을 위한 Kali Linux		
	세부 내용	- 다양한 해킹 툴이 내장되어 있어 인증해제, 브루트 포스 등의 공격이 가능		

4. 성능 요구사항

요구사항고유번호		PER-002		
요구사항 명칭		접근 차단		
요구사항 분류		성능	응락수준	필수
요구사항 세부내용	정의	보안 알고리즘의 성능		
	세부 내용	- 기존 사용자의 통제권 보호를 위해 보안 알고리즘은 공격자의 중간자 공격을 감지 및 차단할 수 있어야 함		

5. 인터페이스 요구사항

요구사항고유번호		SIR-001		
요구사항 명칭		조작 편의성		
요구사항 분류		인터페이스	응락수준	필수
요구사항 세부내용	정의	사용자 이용 편의성		
	세부 내용	- 이용자가 보안과 프로그래밍에 대한 지식 없이도 간단한 설치를 통해 드론의 보안 강화가 가능해야 함 - 공격자에 의해 변형된 프로그램의 설치를 방지해야 함 - 드론의 연결 시간이 짧아야 하고 복잡하지 않아야 함		

6. 테스트 요구사항

요구사항고유번호	TER-001		
요구사항 명칭	보안 테스트		
요구사항 분류	테스트	응락수준	필수
요구사항 세부내용	- 시스템은 기존 컨트롤러 외의 다른 컨트롤러에 대해 연결이 불가해야 함 - 사용자가 소프트웨어 설치를 진행할 때 드론과 컨트롤러를 모두 설치해야만 하고, 이때 해시값을 이용해 인증을 진행함 - 컨트롤러가 바뀐다면 새롭게 설치하고 해시값을 갱신함		

7. 보안 요구사항

요구사항고유번호	SER-001		
요구사항 명칭	무선 네트워크 보안		
요구사항 분류	보안	응락수준	필수
요구사항 세부내용	- 드론의 무선 네트워크는 WPA2 보안 방식을 이용해야 함		

요구사항고유번호	SER-002		
요구사항 명칭	암호화 보안		
요구사항 분류	보안	응락수준	필수
요구사항 세부내용	- 보안 알고리즘 상 암호화는 OTP(One-Time Password) 기법을 이용함 - OTP는 구글 사의 것을 이용함		

요구사항고유번호	SER-003		
요구사항 명칭	이중 통신 보안		
요구사항 분류	보안	응락수준	필수
요구사항 세부내용	- RF 신호, WiFi 신호 두 개를 상호 검증하며 통신 과정에서 이상이 없는지 감지함		

8. 품질 요구사항

요구사항고유번호		QUR-001		
요구사항 명칭		결함 관리		
요구사항 분류		품질	응락수준	필수
요구사항 세부내용	정의	품질관리(기술 관점)		
	세부 내용	- 드론의 보안 알고리즘에서 문제가 발견되면 새로운 알고리즘을 구현, 탑재함 - 비밀번호 변경을 통해 임시적으로 보안 문제 해결 가능		

요구사항고유번호		QUR-002		
요구사항 명칭		매뉴얼 관리		
요구사항 분류		품질	응락수준	필수
요구사항 세부내용	정의	사용성, 접근성 관리		
	세부 내용	- 드론의 연결 및 조작, 보안 강화 등의 방법이 담긴 사용 설명서를 github에 업로드 - 변경사항이 있으면 업데이트하여 이용에 차질이 없게 함		

9. 제약 사항

요구사항고유번호	COR-001		
요구사항 명칭	시스템 구성 언어		
요구사항 분류	제약사항	응락수준	필수
요구사항 세부내용	- 드론의 연결, 조작 및 보안 관리를 Python 프로그래밍으로 구성함 - 보안 테스트는 Kali Linux의 모듈들을 이용해 진행함		

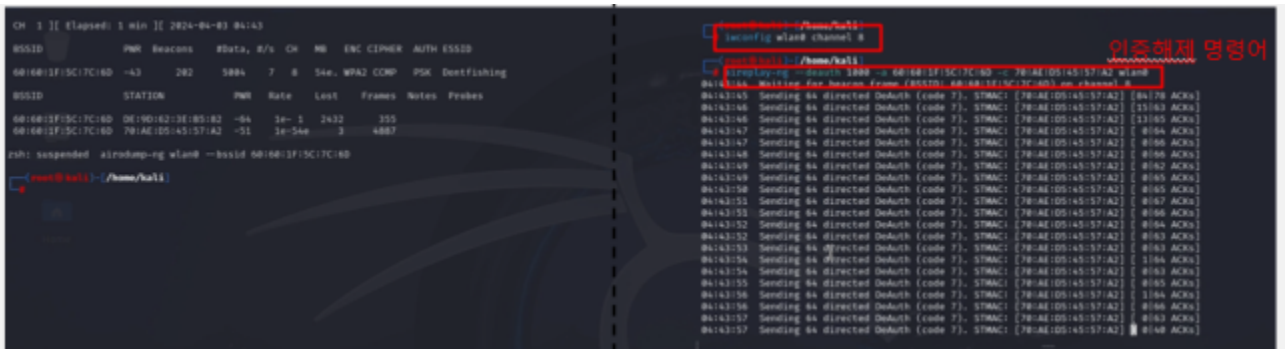
요구사항고유번호	COR-002		
요구사항 명칭	시스템 요소 제한		
요구사항 분류	제약사항	응락수준	필수
요구사항 세부내용	- 소프트웨어, 하드웨어의 구성을 조절해 명령 반응속도와 연결 시간을 목표 수치 이하로 유지해야 함		

[별첨2]

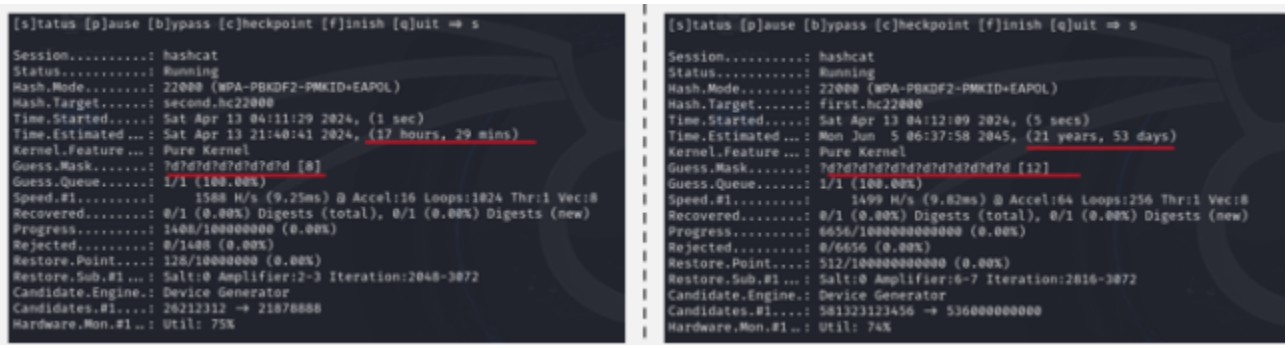
중간보고서

1. 요구사항 정의서에 명세된 기능에 대하여 현재까지 분석, 설계, 구현(소스코드 작성) 및 테스팅한 내용을 기술하시오.

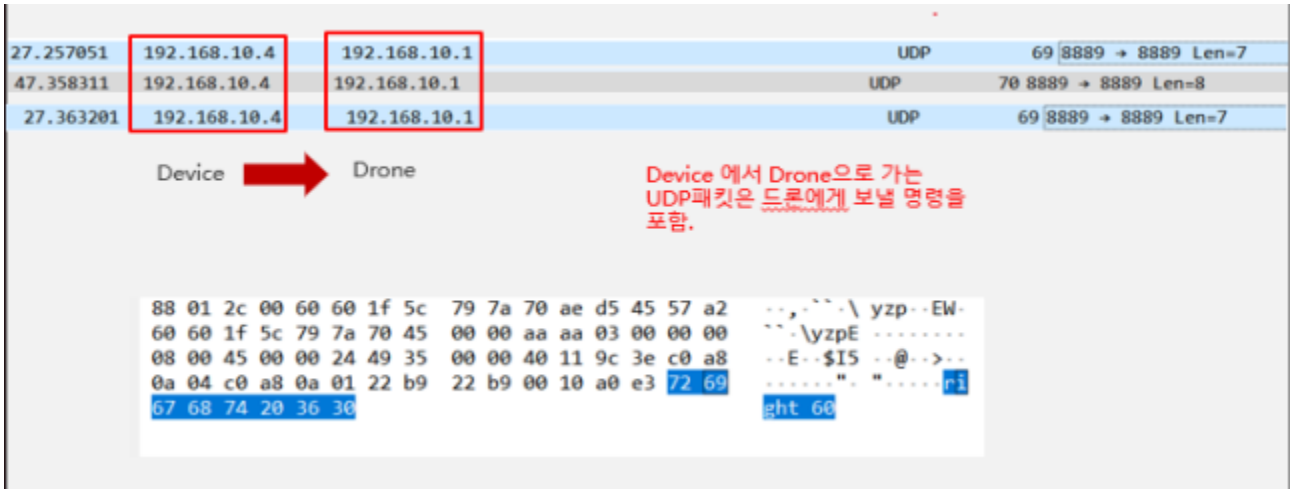
- 칼리 리눅스 설치
- Deauth Attack 패킷 캡처



- Brute Force를 이용한 WPA2 비밀번호 크랙



- 드론 하이재킹
- 패킷 분석



2. 프로젝트 수행을 위해 적용된 추진전략, 수행 방법의 결과를 작성하고, 만일 적용과정에서 문제점이 도출되었다면 그 문제를 분석하고 해결방안을 기술하시오.

- 패킷을 분석하는 과정에서 캡처한 패킷 파일의 정보가 누락이 될 때가 있었는데, 캡처하는 기기의 네트워크 채널 변경을 통해 정보 누락을 없앰

- 드론이 통신하는 과정에서 RF 신호와 Wi-Fi 신호를 복합적으로 이용하는 문제가 있어 이를 역이용해 신호의 교차 검증을 통한 암호화 기능 고안

- RF 신호와 Wi-Fi 신호의 유효 거리, 속도가 다른 점으로 인해 신호 검증에 초 단위의 지연이 발생

- WPA2 방식의 보안이 적용된 Wi-Fi를 Brute Force 공격해보았고 소요 시간이 매우 길어 드론의 AP에 유효하지 않은 공격이라고 판단

평가도구	평 가 항 목	평 가 점 수				
		1	2	3	4	5
중간 보고서 및 실행 결과	1. 요구사항 정의서(기능, 성능, 인터페이스 등)가 구체적으로 작성되었는가?					
	2. 요구분석, 설계 산출물(모델, 프로토타입 등)의 내용이 충실한가?					
	3. 설계 및 구현 문제를 위해 적용한 이론, 문제해결 방법이 제시되었으며 그 적용이 적합한가?					
	4. 구현된 소프트웨어(또는 이와 동등한 하드웨어 시스템)가 버그 없이 실행되었는가?					
	5. 구현된 소프트웨어(또는 이와 동등한 하드웨어 시스템)의 성능 요구사항은 충족되었는가?					
도구활용	6. 설계 및 구현을 위해 도구가 적절히 활용되었는가?					
	7. 도구의 활용수준(능숙도)은 프로젝트 수행에 적합한가?					
팀원의 업무 및 역할	8. 팀원의 업무분담에 따른 역할 및 협력이 충실히 이루어졌는가? (평가자에 의한 질의)					
	9. 프로젝트 중간 진척상황에 대해 팀원이 충분히 인지하고 있는가?(평가자에 의한 질의)					
합계						

***검토 의견(최종완료 때까지 보완해야할 점에 대해 작성 요망)**

심사위원(소속): **(이름)** **(인)**

캡스톤 디자인 I 중간보고서 채점표