캡스톤디자인 I 계획서

<table>
<tr><td rowspan="2">제 목</td><td>국문</td><td colspan="4">드론 기반 무선 네트워크의 보안 취약점 분석</td></tr>
<tr><td>영문</td><td colspan="4">Analysis of security vulnerabilities in drone-based wireless networks</td></tr>
<tr><td>프로젝트 목표
(500자
내외)</td><td colspan="5">이 프로젝트에서는 무선 네트워크 보안의 취약점을 개선한 드론을 제작한다. 칼리 리눅스와 Tello SDK를 이용해 Tello 드론의 무선 네트워크를 해킹하고, GPS 및 카메라 신호를 조작하거나 기존 사용자의 연결을 해제해 통제권을 탈취하는 하이재킹을 시도한다. 이후 무선 네트워크만의 인증 방식이 아닌 별도의 사용자 인증 알고리즘을 구상하여 드론과 공용 와이파이에 접목하고, 궁극적으로는 현대 사회의 무선랜 보안 강화를 목표로 한다.</td></tr>
<tr><td>프로젝트
내용</td><td colspan="5">이 프로젝트의 구성은 Wifi 해킹, 드론 하이재킹, 취약점 개선의 3가지로 나눌 수 있다.
Wifi 해킹 - 오늘날 드론을 무선 네트워크로 연결할 때 주로 사용되는 WPA2 보안 방식의 Wifi 해킹을 시도한다. 칼리 리눅스를 이용해 네트워크 암호를 알아내고 네트워크의 연결 인원수 제한을 해제한다.
드론 하이재킹 - Tello 드론의 보안 무력화를 목표로 한다. 알려진 취약점을 공략하거나 Tello 드론 자체의 취약점을 이용해 드론 제어용 무선 네트워크에 연결하고, 기존 사용자의 입력 신호를 분석해 GPS 및 카메라 신호를 위조, 출력하여 기존 사용자가 드론이 탈취된 사실을 바로 알아차리지 못하도록 한다. 기존 사용자의 네트워크 연결을 해제하여 통제권을 탈취하는 것을 목표로 한다.
취약점 개선에서는 Wifi 해킹, 드론 하이재킹에서 발견된 약점들을 보완한 드론을 제작한다. IP, MAC 스니핑을 방지할 수 있는 사용자 검증 알고리즘을 구상해 드론 네트워크에 접목한다. 앞서 시도한 방식들을 이용했을 때 드론의 보안이 무력화되지 않으면 공용 AP에도 적용하여 문제점이 발생하지 않는지 확인한다.</td></tr>
<tr><td>중심어(국문)</td><td colspan="2">와이파이</td><td>드론</td><td>보안</td><td>하이재킹</td></tr>
<tr><td>Keywords
(english)</td><td colspan="2">Wifi</td><td>Drone</td><td>Security</td><td>hijacking</td></tr>
<tr><td>멘토</td><td>소속</td><td colspan="2"></td><td>이름</td><td></td></tr>
<tr><td rowspan="4">팀
구성원</td><td>학년
/반</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">01052691194/20211870@edu.hanbat.ac.kr</td></tr>
<tr><td>4</td><td>20191759</td><td>홍준기</td><td colspan="2">01048149218/20191759@edu.hanbat.ac.kr</td></tr>
<tr><td>4</td><td>20201773</td><td>손성호</td><td colspan="2">01094367994/20201773@edu.hanbat.ac.kr</td></tr>
</table>

컴퓨터공학과의 캡스톤디자인 관리규정과 모든 지시사항을 준수하면서 본 캡스톤디자인을 성실히 수행하고자 아래와 같이 계획서를 제출합니다.

2024년 3월 8일

책 임 자 : 김슬기 (인)

희망 지도교수: 김태훈교수님

1. 캡스톤디자인의 배경 및 필요성

무선랜은 전파를 통신매개로 이용하기 때문에 보안을 고려하지 않고 이용한다면 유선랜에 비해 보안이 취약하다.[1] 무선랜을 이용하는 드론의 경우, 군사형 드론은 항공기 또는 순항미사일의 방어시스템 수준으로 보안이 철저한 반면에 상용되는 저가형 드론은 보안이 취약하거나 보안을 고려하지 않은 상태에서 활용되는 경우가 많다. 이런 경우, 공격자가 드론의 제어권을 쉽게 획득하여 정보를 유출하거나 조작할 가능성이 있다.[2]

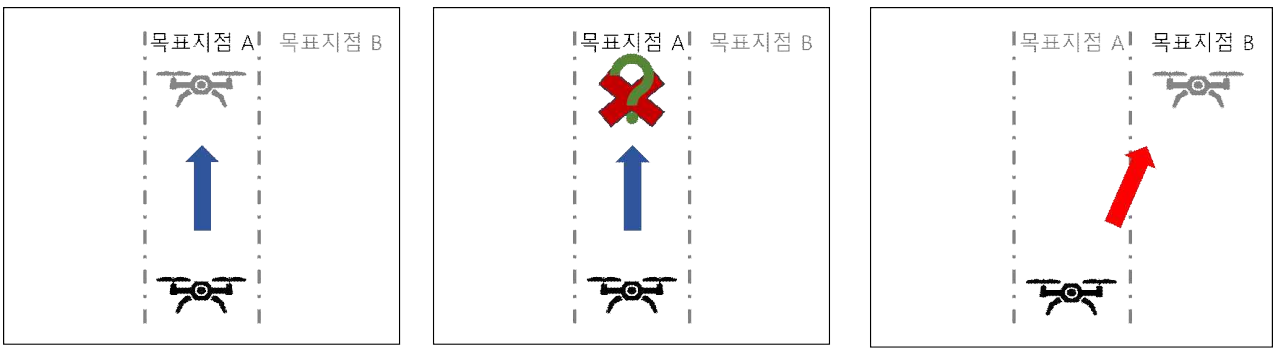
기술이 발전함에 따라 드론의 사용은 인명구조, 물류 및 시설 관리, 그리고 모니터링 등 다양한 분야에서 드론이 적극적으로 활용되고 있다. 하지만 무선랜을 사용한 드론이 보안 위협을 받는다면 생명을 구할 수 있는 기회를 놓칠 수도 있고, 물류나 시설 관리를 위해 사용되던 드론이 해킹당한다면 시설의 보안이 약화되거나 물류 과정이 마비 될 수 있을 것이다. 실제로 활용중인 드론이 보안 위협을 받는다면 위와 같은 다양한 피해가 예상된다. 따라서 드론 해킹에 대한 대응책을 마련하고 보안을 강화하는 것이 매우 중요하다.

2. 캡스톤디자인 목표 및 비전

무선랜 이용량이 늘어남에 따라 안전한 무선랜 이용을 위한 대응방법을 구축하는 것이 중요하다. 대중화된 드론의 무선 네트워크 취약점을 분석하고, 드론 하이재킹(hijacking)을 시도해 실제 사례에서 예상되는 기존 사용자의 피해 규모를 파악한다. IP 혹은 MAC 스니핑(sniffing)을 방지할 수 있는 무선 네트워크 사용자 검증 알고리즘을 구성하고, 이를 활용하는 자체 드론을 제작해 기존 방식의 해킹이 무력화되었는지 확인한다.

무선 네트워크의 보안 형태에 따라 각각 다른 보완점을 적용해 현대 사회의 전반적인 무선랜 보안을 강화한다.

3. 캡스톤디자인 내용



사용자 시점 공격자 시점

- 시나리오(사용자, 공격자)

1. 사용자가 Tello 드론을 연동하여 사용하고 있음
2. 공격자가 사용자의 Tello 드론의 제어권을 탈취함(하이재킹)
3. GPS Spoofing

3-1. 사용자 화면: 드론은 사용자가 의도한 목표지점 A로 이동하는 것처럼 보임

3-2. 실제로 드론은 공격자의 의도대로 목표지점 B로 이동

4. Tello에서 나아가 제작 드론에 적용
5. 무선랜 보안 취약점을 보완하는 알고리즘 제안

- 캡스톤디자인의 범위

정보보호, 네트워크 프로그래밍, 암호학, 네트워크 보안, GPS 보안

- 주요 기능

기능	내용
하이재킹	Tello SDK를 이용해 조작 중인 드론을 칼리 리눅스에서 무선 네트워크 해킹을 시도하여 권한을 탈취한다.
GPS Spoofing	드론에 장착된 GPS, 카메라 송수신값을 조작하여 사용자가 스푸핑 된 사실을 모르도록 한다.
보안 알고리즘 제안	WPA 방식은 사용자 인증의 취약점을 이용한 해킹이 이루어지는데, 이 스니핑 공격을 방지하기 위해 사용자를 한번 더 검증하는 알고리즘을 구현 및 제안한다.

- 비기능적 요구사항

제품 요구사항	사용성 요구사항: 사용자는 비밀번호를 통해 사용자임을 증명 효율성 요구사항: 새로운 기능 추가시 기존 성능을 해치지 않도록 함 이식성 요구사항: 새로 등록 한 사용자도 사용 가능
조직 요구사항	배포 요구사항: 기본 프로그램 이용 구현 요구사항: python 사용 표준 요구사항: kali-linux를 사용하여 네트워크 관리
외부 요구사항	상호운용성 요구사항: GPS와 드론 컨트롤러의 입력값을 실시간으로 비교 윤리적 요구사항: 알아낸 사용자 정보를 다른 목적으로 사용하지 않음 법적 요구사항: 드론 사용 규정 및 보안 규정을 준수

4. 캡스톤디자인 추진전략 및 방법

- 추진전략

수행 내용	1	2	3	4	5	6	7	8	9	10	...
자료수집 및 설계방식 구상											
실험 환경 구축											
하이재킹/Gps Spoofing 시도											
제작 드론 활용											
보안 취약점 분석 알고리즘 제안											
보고서 및 전시회 준비											

- 역할

학번	이름	역할
20211870	김슬기	Tello 활용법 전달, 하이재킹, Gps Spoofing, 알고리즘 제안
20191759	홍준기	Tello API 활용, 칼리 리눅스, 하이재킹
20201773	손성호	칼리 리눅스, 하이재킹, 알고리즘 제안

5. 참고문헌

1. 국내 무선랜(WiFi) 보안 운영 현황 및 정책 방향, 한국인터넷진흥원, 2011, 백종현.

2. Vulnerability Case Analysis of Wireless Moving Vehicle, 한국융합학회논문지, 2018, 오상윤.