와이파이 기반 드론 네트워크에서 드론 제어장치 식별에 관한 연구

홍준기, 김슬기, 손성호, 김태훈■

국립한밭대학교 컴퓨터공학과

{20191759, 20211870, 20201773}@edu.hanbat.ac.kr thkim@hanbat.ac.kr

A Study on Identifying Drone Controller in WiFi-based Drone Networks

Jungi Hong, Seulki Kim, Seongho Son, Taehoon Kim■

Dept. of Computer Engineering, Hanbat National University

요 약

무선통신 네트워크의 활용 범위가 다양해지면서 보안 취약점이 문제가 되고 있다. 최근 드론 관련 산업은 빠르게 확장되어 현대 사회의 다양한 분야에 이용되고 있기에, 본 연구에서는 WiFi 기반으로 동작하는 드론을 활용하여 무선네트워크 보안 취약점을 분석하고자 한다. 드론의 하이재킹을 시도하는 과정에 우선적으로 드론과 드론 제어기기의 인증해제 작업을 선행해야 하는데, 드론에 한 개 이상의 드론 제어기기가 연결되어있는 경우에 인증해제를 수행해야 하는 특정 단말을 식별하는 데 어려움이 있다. 네트워크 패킷을 캡처하고 분석해 드론을 제어하고 있는 드론 제어기기의 MAC 주소를 특정하여 사용자가 인지하기 전에 인증해제를 성공적으로 수행할 수 있도록 한다.

Ⅰ. 서 론

인터넷 기술이 발전함에 따라 Wi-Fi 기반 연결 방식을 이용하는 기기들이 많아지고 있다 [1]. 하지만 Wi-Fi는 기술적, 물리적, 관리적 관점에서 다양한 보안 취약점을 가지고 있다. 본 논문에서는 기술적 취약점 중 하나인 암호화하지 않은 통신에 대한 도청이 가능하다는 점을 이용하여 보안 취약점을 실험적으로 확인하려고 한다. Wi-Fi 연결 방식을 이용하는 기기들 중 드론은 상대적으로 일반인들에게 노출되기 쉽다. 드론은 택배 사업에 이용되는 등 점점 많은 분야에 이용되고 있다 [2]. 하지만 이러한 드론들은 Wi-Fi 인증해제 공격만으로도 제어권을 잃거나 빼앗기는 특성을 지닌다. 앞서 진행된 연구들을 통해서 와이파이 기반 드론 네트워크가 얼마나 인증해제 공격에 취약한지 알려진 바 있다 [3]. 인증해제 공격이란 AP에 연결하는 기기의 인증 과정에 간섭해 기존의 연결을 해제시키거나 새로운 연결을 제한하는 공격이다. 본 논문에서는 Wi-Fi로 연결 및 제어되는 드론을 하이재킹해보고, 그 과정에서 발생하는 문제점을 보완하고자 한다.

Ⅱ. 실험 설계

본 논문에서는 교육용 드론인 Tello 드론을 활용하고자 한다. Tello 드론은 WiFi 네트워크의 Access Point (AP) 역할을 수행하며, 드론의 제어기기(Controller)는 AP에 접속한 후 무선랜을 통해 드론 제어 명령을 드론에게 송신한다. 본 논문에서는 Tello 드론을 인증해제 공격하는 과정 중 드론의 AP에 여러 기기들이 동시에 연결되어 있는 상황을 가정한다. Tello 드론(이하 A)을 모바일 기기(이하 B)가 제어하고, 기타 기기들이 A의 AP에 추가로 연결되어 있다. 이를 노트북(이하 C)의 Kali Linux OS 상 모듈들을 통해 하이재킹한다. 공격자인 C는 airodump-ng 명령을 통해 AP 검색을 하며, AP 검색을 통해 드론의 AP에 연결되어 있는 모든 기기들의 MAC 주소를 확인할 수 있지만 하이재킹 공격을 하기 위해서는 검색된 기기들 중 어떤 기기가 현재 드론을 제어하고 있는지 알아야 한다.

■ Corresponding Author: Taehoon Kim (thkim@hanbat.ac.kr)

이 때, 순차적인 인증해제 공격을 통해 각 기기의 연결을 해제시켜 드론의 상태를 확인할 수는 있지만, 이 방법은 육안으로 드론이 확인되지 않거나 드론이 실시간으로 움직이지 않는 등 변수에 영향을 받는다. 혹은 기존 사용자가 연결이 강제로 해제되는 상황을 통해 공격받고 있다는 사실을 인지할 수 있다.

그림 1 실험 진행 환경

따라서 드론에 연결된 기기들에 영향이 가지 않게 실제 제어권을 가진 기기를 확인하는 방법이 필요한데, 이 때 네트워크 패킷 캡처를 이용할 수 있다.

Ⅲ. 실험

먼저 공격자 노트북의 Kali Linux에서 airodump-ng 명령을 이용해 드론의 공개 AP를 검색함과 동시에 해당 AP의 패킷을 캡처한다. 그림 2는 C에서 A의 AP를 검색하는 과정이다. 명령어 인자들을 통해 검색할 AP의

이름을 필터링하고, 검색 중 발생하는 패킷들을 저장하게 한다.

그림 2 AP의 네트워크 패킷 캡처

그림 3은 그림 2의 명령을 실행했을 때 B와 D의 연결이 검색된 장면이다. 명령어를 실행하면 현재 A의 AP와 연결된 기기들의 MAC 주소를 보여준다. BSSID는 드론 AP의 MAC 주소, STATION이 연결된 B와 D의 MAC 주소이다. 이 중 어떤 기기가 현재 A의 제어권을 가졌는지 알 수 없는 상황이다. 제어중인 기기를 특정하기 위해 캡쳐된 패킷에서 드론과 통신이 이루어진 MAC 주소를 찾는다.

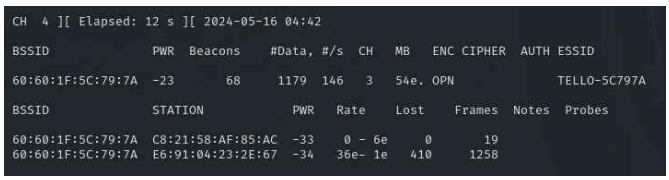

그림 3 AP에 연결된 기기들

그림 4는 캡쳐된 패킷 파일에서 B가 A로부터 정보를 받았다는 것을 보여준다. B의 MAC 주소 E6:91:04:23:2E:67이 특정되었으니 B가 드론을 제어중이다. 이제 aireplay-ng 명령어를 이용해 드론을 제어중인 기기에 인증해제 공격을 한다.

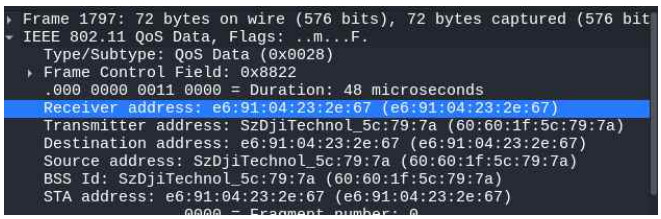

그림 4 캡쳐된 패킷에 나타난 MAC 주소

그림 5는 C에서 B를 인증해제 공격하는 장면이다. 인증해제 공격을 받은 B는 AP와 연결이 해제되고, 공격자는 A의 제어권을 획득한다. 이렇게 드론 하이재킹이 완료되는 시점까지 A의 기존 사용자는 아무런 이상도 감지하지 못한다.

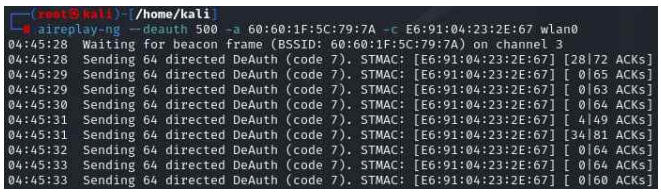

그림 5 드론 제어중인 기기 인증해제 공격

Ⅳ. 결론

Wi-Fi의 보안 취약점이 어떤 식으로 공격자에게 활용되는지 알아보기 위해 Tello 드론을 공격했다. 오픈소스 툴을 사용하는 간단한 명령어만으로 Wi-Fi의 암호화 방식에 상관없이 Wi-Fi에 연결한 기기들의 정보가 공격자에게 전달되는 모습을 확인할 수 있었다. 실험에서는 드론의 하이재킹을 목적으로 인증해제 공격을 준비할 때 드론의 AP에 여러 기기가 연결되어 있어도 실제로 드론을 제어하는 기기는 하나뿐이라는 특성을 이용했다. 실험을 진행하면서 드론을 제어하는 명령이 캡처한 패킷 파일에서 나타났는데, 이를 응용하면 드론뿐만 아니라 AP을 통해 제어하는 기기는 특별한 암호화가 없다면 대부분 같은 방식으로 보안이 무력화될 것이라 생각된다. Wi-Fi 보안 취약점 개선이 필요한 이유이다.

ACKNOWLEDGMENT

본 연구는 2024년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음(2022-0-01068)

참 고 문 헌

[1] W. Hlaing, S. Thepphaeng, V. Nontaboot, N. Tangsunantham, T. Sangsuwan and C. Pira, "Implementation of WiFi-based single phase smart meter for Internet of Things (IoT)," 2017 International Electrical Engineering Congress (iEECON), Pattaya, Thailand, pp. 1-4, 2017

[2] 내년부터 우체국 택배 '드론 배송'… 첫 시범지역 어디? - 디지털타임스

[3] J. Gordon, V. Kraj, J. H. Hwang and A. Raja, "A Security Assessment for Consumer WiFi Drones," 2019 IEEE International Conference on Industrial Internet (ICII), Orlando, FL, USA, pp. 1-5, 2019

[4] 이규호, 김태현, 방인규, 김태훈, "와이파이 네트워크에서 드론 인증 해제 공격 구현에 관한 연구," 한국통신학회 동계종합학술발표회 논문집, pp. 1,080-1,081, 2023.

[5] 이규호, 김태현, 김정훈, 방인규, 김태훈, "와이파이 기반 드론 네트워크에서 드론 하이재킹 구현에 관한 연구," 한국통신학회 하계종합학술발표회 논문집, pp. 558-559, 2023.