드론 환경에서의 WiFi 패스워드 크래킹 취약점 분석 및 실증 : A와 B 드론을 대상으로

정원빈[O], 김진욱[*], 송희원[*], 홍세준[*], 이경률[*]
[O]목포대학교 정보보호학과,
[*]목포대학교 정보보호학과
e-mail: {goblebin[O], wlsdnr0816[*], s193816[*], s193828[*]}@mokpo.ac.kr, carpedm@mnu.ac.kr[*]

Vulnerability Analysis and Demonstration of WiFi Password Cracking in Drone Environment: Based on Products A and B

Wonbin Jeong[O], Jinwook Kim[*], Heewon Song[*], Sejun Hong[*], Kyungroul Lee[*]
[O]Dept. of Information Security Engineering, Mokpo National University,
[*]Dept. of Information Security Engineering, Mokpo National University

● 요 약 ●

최근 개발되는 드론은 사용자의 편의를 위하여, 사진이나 동영상과 같은 파일을 휴대 기기로 전송하거나 휴대 기기로 드론을 조종하는 것과 같은 휴대 기기를 통한 다양한 기능들을 제공하며, 이러한 기능들은 와이파이를 기반으로 이루어진다. 그러나, 와이파이는 인증 해제 공격이나 Evil Twin 공격과 같은 취약점이 존재하며, 이러한 취약점으로 인하여 드론에서 제공하는 다양한 기능들과 관련된 보안 위협이 발생할 가능성이 존재한다. 따라서, 본 논문에서는 와이파이를 사용하는 드론에서 발생 가능한 취약점을 미리 분석하고 방어하기 위한 목적으로, 와이파이에서 발생 가능한 취약점 중 하나인 패스워드 크래킹 취약점을 분석하였다. 실험 결과, 드론에서 제공하는 와이파이의 패스워드를 크래킹함으로써 공격자가 드론 네트워크 내부로 진입이 가능한 것을 실증하였다. 향후, 드론 환경에서 패스워드 크래킹 뿐만 아니라, 와이파이에서 발생 가능한 다양한 취약점을 분석하고 실증할 예정이다.

키워드: 드론(Drone), 취약점 분석(Vulnerability analysis), 패스워드 크래킹(Password cracking), 와이파이(WiFi)

I. 서론

드론은 농업이나 건설, 환경 보호와 같은 다양한 산업에서 특화된 용도로 활용되며, 이는 드론에서 사진이나 동영상 촬영, 자동 조종과 같은 다양한 기능들을 제공하기 때문이다. 최근 개발되는 대부분 드론은 드론에서 촬영한 사진이나 동영상과 같은 파일을 휴대 기기로 전송하거나 휴대 기기를 이용하여 드론을 조종하는 이러한 기능들을 제공하기 위하여, 주로 와이파이를 이용한다. 그러나, 와이파이는 인증 해제 공격이나 Evil Twin 공격과 같은 다양한 취약점이 존재하며, 이러한 취약점으로 인하여, 드론 내부의 정보가 탈취되거나 악의적인 목적으로 드론을 사용하는 것과 같은 보안 위협이 발생하는 실정이다 [1, 2, 3].

따라서, 본 논문에서는 드론의 안전성을 향상시키기 위한 목적으로, 와이파이 기반 드론에서 발생 가능한 취약점을 분석하고 대응하기 위하여, A와 B 드론들을 대상으로 와이파이 패스워드 크래킹 취약점을 분석하고 실증한다.

II. 와이파이 패스워드 크래킹 취약점 분석 및 실증

본 논문에서는 총 7단계로 구성된 공격 과정을 통하여, 상용 A와 B 드론들을 대상으로 와이파이 패스워드 크래킹 취약점을 분석하고 실증한다.

- 1 단계. 공격 환경 구성
- 2 단계. 무선 랜카드의 모니터 모드 변경
- 3 단계. 주변 AP 탐색
- 4 단계. 무선 랜카드 채널 설정
- 5 단계. 드론 AP 패킷 캡처
- 6 단계. 드론 와이파이 인증 해제 공격
- 7 단계. 드론 와이파이 패스워드 크래킹

각 단계를 상세하게 설명하면, 1단계는 '**공격 환경 구성**'으로, 본 논문에서는 다음과 같은 실험 환경을 구성하였다. 와이파이 패스워드 크래킹 취약점을 분석하기 위한 다양한 도구를 지원하는 우분투 운영체제와 드론 AP(Access point)를 탐지하기 위한 모니터 모드를 지원하는 무선 랜카드를 사용하였다. 또한, 와이파이 패스워드 크래킹 공격을 시도하기 위한 다양한 도구를 사용하였으며, 무선 랜카드를 모니터 모드로 전환하는 airmon-ng 도구, 주변 무선 네트워크의 패킷을 캡처하는 airodump-ng 도구, 패스워드 크래킹 공격을 지원하는 aircrack-ng 도구를 사용하였다.

2단계는 '**무선 랜카드의 모니터 모드 변경**'으로, 드론 AP에서 송수신되는 와이파이 신호와 관련된 접근 및 처리를 위하여, 공격자의 무선 랜카드의 모드를 유선 랜카드의 프로미스큐어스 모드와 같이 모니터 모드로 변경하는 단계이다. 무선 랜카드를 모니터 모드로 변경한다면, 주변의 AP를 탐색하거나 패킷 캡처, 패킷 삽입과 같은 행위가 가능하다.

무선 랜카드의 모니터 모드를 변경하는 명령어는 "airmon-ng start <*무선 랜카드 이름*>"이며, 무선 랜카드 이름은 'iwconfig' 명령어로 확인한다. 실험 환경에서의 무선 랜카드 이름을 확인한 결과, 'wlp2s0'인 것을 확인하였으며, 최종적으로, 그림 1과 같이, "airmon-ng start wlp2s0" 명령어를 입력함으로써, 무선 랜카드의 모드를 모니터 모드로 변경한다.

```
root@asteria-Swift-SFG14-42:/home/asteria# airmon-ng start wlp2s0

Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    622 avahi-daemon
    629 NetworkManager
    668 wpa_supplicant
    679 avahi-daemon

PHY     Interface       Driver          Chipset

phy0    wlp2s0          mt7921e         MEDIATEK Corp. Device 0616
                (mac80211 monitor mode vif enabled for [phy0]wlp2s0 on [phy0]wlp
2s0mon)
                (mac80211 station mode vif disabled for [phy0]wlp2s0)
```

Fig. 1. 2단계: 무선 랜카드의 모니터 모드 변경 결과 일례

3단계는 '**주변 AP 탐색**'으로, 모니터 모드로 변경된 무선 랜카드로 공격자 주변의 AP를 탐색한다. 향후, 드론을 대상으로 공격이 진행될 예정이므로, 결국, 주변 AP를 탐색함으로써, 드론 AP를 발견하고 관련 정보를 수집하는 것이 목표이다. 주변 AP 정보를 수집하는 명령어는 "airodump-ng <*무선 랜카드 이름*>"이며, 그림 2와 같이, "airodump-ng wlp2s0mon" 명령어를 입력함으로써, 주변 AP를 탐색한다.

```
CH 120 ][ Elapsed: 24 s ][ 2023-12-12 12:58

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

[redacted]:FF:94:73   -1        0        0    0  -1   -1                  <length:  0>
[redacted]:74:52:A0   -1        0        0    0  -1   -1                  <length:  0>
[redacted]:DD:37:12  -43        5        0    0 157  390   WPA2 CCMP   PSK  [redacted]
[redacted]:6F:CE:84  -49        6        0    0   1  130   WPA2 CCMP   PSK  MNU_Guest
```

Fig. 2. 3단계: 주변 AP 탐색 결과 일례

3단계 결과를 살펴보면, 탐색된 다수의 주변 AP의 MAC 주소 및 채널번호와 같은 다양한 정보를 확인할 수 있다. 그러나, 이 결과는 본 논문의 목표인 드론 AP만 탐색되는 것이 아닌, 주변의 모든 AP가 탐색되므로, 드론 AP의 정보를 수집하고 전달되는 패킷을 캡처하기 위하여, 4단계인 '무선 랜카드 채널 설정' 단계가 필요하다.

4단계는 '**무선 랜카드 채널 설정**'으로, 드론 AP의 정보를 수집하고 전달되는 패킷을 캡처하기 위하여, 무선 랜카드의 채널을 설정한다. 채널번호를 설정하는 명령어는 "iwconfig <*무선 랜카드 이름*> channel <*목표 AP 채널번호*>"이며, 드론 AP의 채널번호는 157번이므로, 최종적으로, 그림 3과 같이, "iwconfig wlp2s0mon channel 157" 명령어를 입력함으로써, 무선 랜카드의 채널을 설정한다.

```
root@asteria-Swift-SFG14-42:/home/asteria# iwconfig wlp2s0mon channel 157
root@asteria-Swift-SFG14-42:/home/asteria#
```

Fig. 3. 4단계: 무선 랜카드 채널 설정 결과 일례

결과를 살펴보면, 별다른 출력은 없지만, 무선 랜카드의 채널을 드론 AP의 채널과 일치시켰으므로, 드론 AP에서 전달되는 패킷의 캡처가 가능하다.

5단계는 '**드론 AP 패킷 캡처**'로, 드론 AP에서 전달되는 패킷을 캡처한다. 이 과정은 이후 과정에서 드론 AP에 연결된 사용자 단말의 연결을 해제하고, 사용자 단말이 드론 AP에 재연결되는 과정에서 전달되는 패스워드 정보를 포함한 EAPOL(Extensible Authentication Protocol Over LAN) 패킷을 캡처하기 위한 선행 과정이다. 즉, 공격자는 드론 AP에서 전달되는 패킷을 캡처하는 상태에서 사용자 단말로 인증 해제 공격을 시도하므로, 이 단계에서 드론 AP에서 전달되는 모든 패킷의 캡처를 시도한다. 패킷을 캡처하는 명령어는 "airodump-ng --bssid <*목표 AP MAC 주소*> -c <*목표 AP 채널번호*> -w output <*무선 랜카드 이름*>"이며, 드론 AP MAC 주소는 '**:**:**:DD:37:12'이므로, 최종적으로, 그림 4와 같이, "airodump-ng --bssid **:**:**:DD:37:12 -c 157 -w output wlp2s0mon" 명령어를 입력함으로써, 드론 AP에서 전달되는 모든 패킷을 캡처하여 PCAP 파일인 'output.pcap' 파일에 저장한다.

```
CH 157 ][ Elapsed: 1 min ][ 2023-11-27 13:11 ][ WPA handshake: [redacted]:DD:37:

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH

[redacted]:DD:37:12  -53 100      767       23    0 157  390   WPA2 CCMP   PSK

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Pro

[redacted]:DD:37:12 [redacted]:83:12:80  -29    6e- 6e     0       76  EAPOL
```

Fig. 4. 5단계: 드론 AP 패킷 캡처 결과 일례

6단계는 '**드론 와이파이 인증 해제 공격**'으로, EAPOL 패킷을 캡처하기 위하여 드론 와이파이에 인증 해제 공격을 시도하는 단계이다. 공격자가 드론 와이파이에 인증 해제 공격을 시도하면, 사용자 단말은 와이파이 인증 정보를 포함한 EAPOL 패킷을 드론에게 재전송하며, 공격자는 이 과정에서 재전송되는 패킷을 캡처함으로써, 다음 단계인 패스워드 크래킹 공격에서 활용한다. 인증 해제 공격을 시도하는 명령어는 "aireplay-ng --deauth <*인증 해제 공격 수행 횟수*> -a <*목표 AP MAC 주소*> <*무선 랜카드 이름*>"이므로, 최종적으로 "aireplay-ng --deauth 100 -a **:**:**:DD:37:12 wlp2s0mon"명령어를 입력함으로써, 인증 해제 공격을 수행한다.

7단계는 '**드론 와이파이 패스워드 크래킹**'으로, 드론 AP의 와이파이 패스워드 크래킹을 시도한다. 이전 단계까지 결과를 통하여 와이파

이 패스워드를 크래킹하기 위한 정보가 모두 수집되었으므로, 패스워드 크래킹 속도가 빠른 오프라인 패스워드 크래킹으로 드론의 패스워드를 탈취할 수 있다. 오프라인 패스워드 크래킹은 brute force 공격, 사전 공격, 레인보우 테이블 공격과 같은 다양한 패스워크 크래킹 공격을 제공하며, 본 논문에서는 사전 공격으로 패스워드를 크래킹한다. 사전 공격은 패스워드로 예상되는 문자나 문자열을 사전 파일로 저장한 후, 사전 파일의 패스워드를 하나씩 비교하는 방법이며, 이 공격은 패스워드가 저장된 사전 파일이 반드시 요구된다. 취약점 실증을 위하여, 이미 만들어진 사전 파일을 활용하였으며, 사전 공격으로 패스워드를 크래킹하는 명령어는 "aircrack-ng *<EAPOL 패킷이 캡처된 PCAP 파일 이름>* -w *<사전 파일 이름>*"이다. 본 논문에서 PCAP 파일 이름은 'output-01.cap', 사전 파일 이름은 test이므로, 최종적으로, 그림 6과 같이, "aircrack-ng output-01.cap -w test" 명령어를 입력함으로써, 와이파이 패스워드를 크래킹한다.

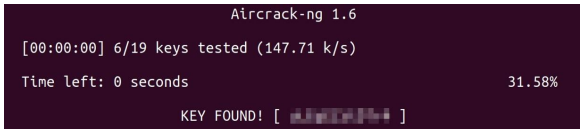

Fig. 5. 7단계: 드론의 와이파이 패스워드 크래킹 결과 일례

III. 결론

본 논문은 상용 드론들 중, A와 B 제품을 대상으로, 와이파이 패스워드 크래킹 취약점을 분석하고 실증하였다. 이를 위하여, 총 7단계로 구성된 공격 과정을 도출하였으며, 각 단계에 따른 실험결과, 사전 공격으로 드론의 와이파이 패스워드 크래킹에 성공하였다. 하지만, 사전 공격이나 패스워드 크래킹 공격은 짧은 패스워드를 사용하거나 숫자, 또는 소문자, 대문자로만 구성된 보안성이 낮은 패스워드를 사용하는 경우에는 쉽게 패스워드를 탈취할 수 있다.

그러나, 숫자, 소문자, 대문자로 구성된 12자리 이상의 패스워드를 사용한다면, brute force 공격으로 패스워드를 탈취하기까지 약 2,000년 이상 소요되는 결과를 가진다. 따라서, 소문자, 대문자, 숫자를 조합한 12자리 이상의 패스워드를 사용한다면, 사전 공격 및 brute force 공격으로부터 패스워드를 안전하게 보호할 수 있을 것으로 사료된다. 향후, 패스워드 크래킹을 포함하여, 드론 환경에서의 와이파이를 포함한 무선 네트워크에서 추가적으로 발생 가능한 취약점 및 그 대응방안을 연구할 예정이다.

ACKNOWLEDGEMENT

이 성과는 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2021R1A4A2001810). 본 과제(결과물)는 2023년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역 혁신 사업의 결과입니다.(2021RIS-002, 1345370809)

REFERENCES

[1] G, Lee, T. Kim, I. Bang, and T. Kim, "Implementation of Drone Deauthentication Attack in WiFi Networks," Proceedings of the Winter Conference on the Korean Institute of Communications and Information Sciences, pp. 1080-1081, Feb. 2023.

[2] T. Kim, G. Lee, M, Seo, I. Bang, and T. Kim, "Implementation of Evil Twin Attack in WiFi-based Drone Networks," Proceedings of the Summer Conference on the Korean Institute of Communications and Information Sciences, pp. 550-551, Jun. 2023.

[3] The Register, "How Wi-Fi spy drones snooped on financial firm," *https://www.theregister.com/2022/10/12/drone-roof-attack*, accessed on December 28, 2023.