한국컴퓨터정보학회 동계학술대회 논문집 제25권 제1호 (2017. 1)

와이파이를 이용하는 드론의 취약점 분석

정인수[O], 홍득조[*]
[O*]전북대학교 IT정보공학과
e-mail: jns00416@gmail.com[O], deukjo.hong@jbnu.ac.kr[*]

Vulnerability Analysis of Drones Using Wi-Fi

In-Su Jung[O], Deuk-Jo Hong[*]
[O*]Dept. of Information Technology, Chonbuk National University

● 요 약 ●

드론 기술이 발전하면서 물품 배달에 드론이 이용되는 등 드론은 우리 생활 전반에 자리 잡으려 하고 있다. 하지만 대부분의 드론이 기본적인 사용자 인증 과정도 없이 보안에 매우 취약한 상태이다. 본 논문에서는 드론의 취약점을 증명하기 위해 Parrot 사의 AR. Drone을 대상으로 Wi-Fi 연결을 통한 인증해제, telnet을 통한 명령 수행, ftp 서버를 통한 파일 변조 공격을 적용해 보고, 이러한 취약점에 대해 무선 AP의 비밀번호를 복잡하게 설정하는 방법, 무선 침입 방지 시스템을 사용하는 방법, NAP 또는 NAC 솔루션을 구축하는 방법과 같은 적절한 대응 방안을 논의한다.

키워드: 인증 해제(deauthentication), telnet, ftp, 무선 침입 방지 시스템(WIPS)

I. 서론

드론 기술이 발전하면서 드론은 우리 생활 전반에 자리 잡으려 하고 있다. 드론은 목적에 따라 군사용, 민수용으로 구분하여 생산되고 있다. 군사용 드론은 정찰용 드론과 공격용 드론으로 나뉘며, 정보 수집, 정찰 및 수색 임무를 수행한다. 민수용 드론은 군사용 드론보다 더 다양한 용도로 쓰인다. 드론에 장착된 카메라를 이용해 항공 촬영을 하거나 딥 러닝을 접목시켜 재난에 대비할 수 있고, 스모그 제거, 인공 강우 등의 목적으로 사용되기도 한다. 가장 주목받는 분야는 배달 서비스이다. 현재 중국의 알리바바, 독일의 DHL, 미국의 아마존에서 드론을 이용한 물품 배달 서비스를 시험 중이고, 각각 최근에 소형 물품 배달에 성공했다.

드론은 대부분 2.4GHz 대역의 주파수를 사용해 통신하며, 최근에는 Wi-Fi로 스마트폰과 연결하여 조종하는 드론이 많이 생산되고 있다. 그런데 드론은 인증 체계가 갖추어져 있지 않은 경우가 많기 때문에 공격자가 시스템에 쉽게 접근할 수 있다. 본 논문에서는 Parrot 사의 'AR. Drone'을 대상으로 Wi-Fi를 이용해 인증 해제 공격, telnet에 접속하여 특정 명령을 내리는 공격, ftp 서버에 접속하여 미디어 파일을 변조하는 공격을 수행한 결과를 보이고, 그에 대한 적절한 대응방안에 대해 모색한다.

II. AR. Drone 2.0

실험 대상은 '그림 1'에 보이는 Parrot사의 'AR. Drone 2.0 Elite Edition' 이다. 스마트폰과의 Wi-Fi 연결을 통해 조종하는 방식이며, HD 카메라가 부착되어 있어 비행 중 사진 및 동영상 촬영이 가능하다. 사진은 JPEG 확장자로 저장이 되며, 원격 장치나 USB 플래시 드라이브로 비행 중 동영상이 저장된다.

그림 1. Parrot사의 'AR. Drone 2.0'

이 실험에서는 'aircrack-ng', 'netdiscover', 'nmap' 등의 해킹 툴이 사용된다. 그러한 이유에서 실험의 편의를 위해 다양한 해킹 툴이 내장되어 있는 Kali Linux OS(ver.2016.02)를 사용했다.

III. 적용 공격 기법

1. 인증 해제

인증 해제 공격을 통해 드론과 스마트폰의 연결을 해제할 수 있다. 사용하고 있는 무선 랜의 인터페이스 명을 알아낸 후, 해당 인터페이스의 사용을 명령하면 Monitor 모드의 인터페이스가 추가된다. 추가된 인터페이스를 이용해 Wi-Fi로 연결된 드론의 MAC address와 채널 정보를 알아낼 수 있다. 그리고 인터페이스와 MAC address, 채널 정보를 이용하면 해당 드론에 연결되어 있는 스마트폰의 MAC address까지도 알아낼 수 있다. 드론의 MAC address와 연결된 스마트폰의 MAC address, 그리고 사용되는 인터페이스 명을 알고 있으면 드론과 스마트폰 사이의 연결을 해제하는 명령을 내릴 수 있다. 명령을 수행하는 횟수에 따라 한 번만 끊어지거나 공격이 수행되는 동안 재 연결이 불가능하도록 할 수 있다.

2. telnet을 통한 명령 수행

Wi-Fi 연결을 통해 드론의 telnet에 접속할 수 있다. telnet에 접속하면 드론 내부에 저장된 파일들을 모두 확인하고 실행할 수 있다. 'bin' 디렉터리 내부에서 확장자가 '.sh' 인 파일들을 확인할 수 있는데, 이 파일들이 드론에 특정 명령을 내리는 스크립트 파일들이다. 이 파일을 실행하면 드론이 그 파일에 해당하는 동작을 수행하게 된다.

3. ftp 서버를 통한 파일 변조

ftp는 파일의 전송을 담당하는 프로토콜이다. 이 ftp 서버에 접속하기만 하면 드론에 저장되어 있는 모든 미디어 파일들을 확인할 수 있을 뿐만 아니라 파일 다운로드 및 다른 파일로 변조하는 것까지 가능하다.

IV. 공격 기법 적용

1. 인증 해제

인증 해제 공격에는 'aircrack-ng'라는 툴이 사용되었다. 'aircrack-ng'는 무선 랜에 대한 crack과 analysis를 지원하는 툴로 'aircrack-ng', 'airmon-ng', 'aireplay-ng' 등을 포함한다.

그림 2. Monitor 모드의 인터페이스 추가

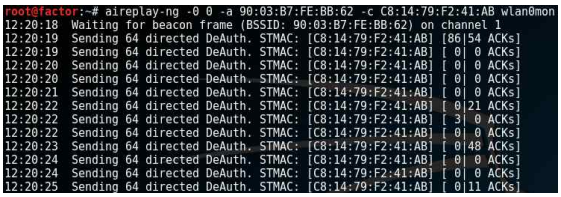

그림 3. 횟수 제한 없는 연결 해제 명령

먼저 'airmon-ng'를 사용해 현재 사용 중인 무선 랜의 인터페이스를 확인하고 해당 인터페이스를 사용하겠다는 명령을 내렸다. '그림 2'처럼 Monitor 모드의 인터페이스가 추가된 것을 확인할 수 있었다. 이 인터페이스와 'airodump-ng'를 사용해 드론의 MAC address와 채널을 알아낸 후, 드론에 연결된 스마트폰의 MAC address까지 알아낼 수 있었다. 마지막으로 'aireplay-ng'를 사용하여 드론에 연결 해제 명령을 보내 드론과 스마트폰의 연결을 해제할 수 있었다. 공격을 받은 드론은 hovering 상태가 되어 아무런 동작을 수행하지 않았다. 연결 해제 명령을 한 번만 보낼 경우 스마트폰으로 드론에 다시 연결할 수 있었지만, '그림 3'과 같이 연결 해제 명령을 계속해서 보내도록 하면 공격이 수행되는 동안에는 드론에 다시 연결할 수 없었다.

2. telnet을 통한 명령 수행

telnet에 접속해 특정 명령을 수행하도록 하는 공격에서는 'netdiscover'와 'nmap'이라는 툴이 사용되었다. 'netdiscover'는

arp 정보를 알려주는 툴이고, ‘nmap’은 네트워크의 어떤 포트가 열려있는지 스캔하기 위한 툴이다.

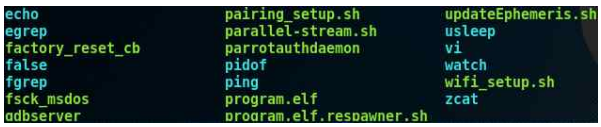

그림 4. telnet 파일 목록

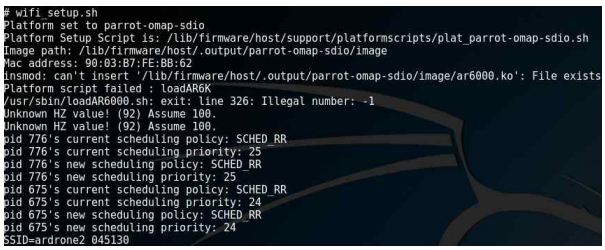

그림 5. ‘wifi_setup.sh’ 실행 화면

telnet에 접속하기 위해 ‘netdiscover’를 사용해 연결된 드론의 IP address를 조회했다. 이후, ‘nmap’을 사용해 해당 IP address에 21번 포트(ftp)와 23번 포트(telnet)가 열려있는 것을 확인할 수 있었다. 조회했던 드론의 IP address를 이용해 telnet에 접속하고 ‘ls’ 명령으로 드론 내부의 파일들을 조회했다. ‘bin’디렉터리 내부에 ‘그림 4’와 같이 확장자가 ‘.sh’인 파일들이 있는데, 이 파일들이 드론에 특정 명령을 수행하도록 하는 스크립트 파일이다. 이 파일들 중 ‘wifi_setup.sh’를 실행하자, ‘그림 5’와 같은 내용을 화면에 출력하면서 스마트폰과 드론의 연결이 해제되었다.

3. ftp 서버를 통한 파일 변조

ftp 서버에 접속하는 방법 또한 ‘netdiscover’와 ‘nmap’을 사용해 IP address와 열려있는 포트 번호를 조회한 후에 수행된다.

그림 5. ftp 서버 디렉터리 조회

ftp 서버에 접속해서 디렉터리를 조회한 결과 ‘그림 5’처럼 어떤 미디어 파일도 찾을 수 없었다.

V. 드론 취약점 대응 방안 논의

드론 기술이 발전함에 있어서 우선적으로 다뤄져야할 문제점은 대부분의 드론이 드론과 사용자 간에 인증과정이 없다는 것이다. 이 부분에 대해서는 일차적으로 드론에 연결할 시 Wi-Fi 비밀번호를 입력하도록 하는 방법이 있다. 하지만 비밀번호 설정만으로는 여전히 보안에 취약하다. Wi-Fi 비밀번호의 암호화에는 WEP, WPA, WPA2 등의 방식이 사용되는데, 이 암호화 방식들에 대한 해킹 방법은 이미 잘 알려져 있다. 그러므로 추가적인 보안 대책이 필요하다. Wi-Fi를 이용해 연결하는 드론의 보안 대책으로는 Wi-Fi 해킹 공격에 대한 보안 대책이 동일하게 적용될 수 있다.

먼저, 무선 액세스포인트(AP)의 비밀번호를 복잡하게 설정해야 한다. 숫자와 영어, 특수문자를 혼합해 길이가 긴 암호를 설정하면 비밀번호를 알아내는데 긴 시간이 필요하기 때문에 비밀번호의 복잡함 정도에 따라 비밀번호를 알아내는 것이 거의 불가능해질 수 있다.

무선 침임 방지 시스템(WIPS)을 사용해야 한다. 해커는 비인증 AP를 설정하거나 서비스 거부 공격을 수행할 수 있다. 이러한 공격들을 감지하고 방어하기 위해서는 무선 침입 방지 시스템을 구축해야 한다. 무선 침입 방지 시스템은 무선 AP 사용 현황을 실시간으로 관찰하여 허용하지 않은 접속을 막고, 보안 취약점을 야기할 수 있는 부적절한 접속을 방지한다.

NAP(Network Access Protection) 또는 NAC(Network Access Control) 솔루션을 구축해야 한다. 이것들은 클라이언트 식별과 정의된 정책 준수를 기반으로 네트워크 접속을 추가적으로 제어할 수 있게 한다. 몇몇 NAC 솔루션에는 네트워크 침입 방지와 탐지 기능이 포함되기는 하지만 무선 보호 기능도 제공되는지의 여부를 확인해봐야 한다.

IV. 결론

본 논문에서는 Parrot사의 AR. Drone을 대상으로 Wi-Fi 연결을 통한 다양한 공격을 적용해보고, 이러한 취약점에 대해 적절한 대응 방안을 논의하였다. 인증 해제, telnet을 통한 명령 수행, ftp 서버를 통한 파일 변조 공격을 적용하였다. 인증 해제 공격 시 어려움 없이 연결되어 있던 스마트폰과 연결이 해제되는 것을 확인할 수 있었고, telnet을 통한 명령 수행 공격에서도 ‘wifi_setup.sh’ 스크립트 파일을 실행하자, 연결되어 있던 스마트폰과 연결이 즉시 해제되는 것을 확인하였다. ftp 서버를 통한 파일 변조 공격에서는 디렉터리 내부에서 미디어 파일을 찾을 수 없었다.

이러한 공격에 대한 대응 방안으로는 무선 AP의 비밀번호를 복잡하게 설정하는 방법, 무선 침입 방지 시스템을 사용하는 방법, NAP 또는 NAC 솔루션을 구축하는 방법을 제시하였다.

현재 장비만 갖추어진다면 Wi-Fi를 이용하지 않는 무선 기기에 대한 해킹 또한 가능한 상태이다. 그에 따라 향후 연구에서는 Wi-Fi를 이용하는 다양한 드론으로 실험 대상을 확대하고, Wi-Fi 이외의 무선 통신 공격을 적용해 본 후, 그에 대한 대응 방안을 논의할 예정이다.

References

[1] focus news, http://www.focus.kr/view.php?key=20160 40600152955538

[2] Hyun-Chul Jung , Heejo Lee, “Study on Security Reinforcement Method by Wireless Security Status Survey and Analysis,” Korea Information Processing Society, May 2006.

[3] Se-Hwan Kwon, “Wire and Wireless VoIP Hacking Attacks through the Analysis of Vulnerability against Wireless APs,” Hoseo University, August 2012.

[4] ciokorea, http://www.ciokorea.com/print/10828