드론 환경에서의 DHCP 고갈 공격 취약점 분석: 도구 개선 결과를 기반으로

이준권[1], 정지인[2], 정원태[3], 이경률[1]
[1]목포대학교 정보보호학과
[2]대구가톨릭대학교 컴퓨터소트프웨어학부
[3]목포대학교 정보보호기술학협동과정
kwonl57@mokpo.ac.kr, ddd0444@cu.ac.kr, dnjsxo4354@mokpo.ac.kr, carpedm@mnu.ac.kr

Vulnerability Analysis of DHCP Exhaustion Attack in Drone Environment: Based on Open Source Tools Improvement Results

Junkwon Lee[1], Jiin Jeong[2], Wontae Jung[3], Kyungroul Lee[1],
[1]Dept. of Information Security, Mokpo National University
[2]School of Computer Software, Daegu Catholic University
[3]Interdisciplinary Program of Information & Protection, Mokpo National University

요 약

드론과 관련된 기술의 발전으로 인하여, 다양한 민간 및 공공 산업에서 활용되는 실정이며, 이에 따라 드론 시장 역시 확대되면서 일반인들도 드론을 접하거나 활용하는 기회가 많아지고 있다. 특히, 일반인들이 접근하기 용이하고 사용하기 쉬운 WiFi 기반의 상용 드론이 생산되면서 수요 역시 증가하는 추세이다. 이와 같이, 드론이 많이 발전하는 긍정적인 측면과는 반대로, 드론에서 발생하는 다양한 취약점으로 인하여 보안 위협이 발생한다. 최근에는 WiFi 기반의 드론들을 대상으로 공개된 도구를 사용하여 DHCP 고갈 공격의 취약점을 분석하는 연구가 진행되었으며, 공격 결과로 실제 드론이 DHCP 고갈 공격으로 인하여 IP 주소를 할당받지 못하는 보안위협이 도출되었다.

하지만, 이 연구는 대표적인 DHCP 공격 도구인 DHCPig와 Yersinia를 활용하였으며, 이 도구들은 무선이 아닌 유선 네트워크를 기반으로 제작되었기 때문에, 드론 환경에 그대로 적용하기에는 한계점이 존재하며, 실제로 발생 가능한 취약점을 검증하지 못하는 한계점도 존재한다. 따라서 본 논문에서는 WiFi 기반 상용 드론을 대상으로 DHCP 고갈 공격의 취약점을 분석하기 위하여, 공개된 도구들의 문제점을 분석하고 개선함으로써, 드론 환경에서의 DHCP 고갈 공격의 가능성을 검증한다. 본 연구 결과는 DHCP를 제공하는 드론 환경의 안전성을 향상하기 위한 지표로 활용될 것으로 사료된다.

1. 서론

드론 기술이 발전함에 따라, 산림보호나 화재 발견과 같은 소방이나 범죄지역 조사와 같은 치안 관련 공공 및 민간분야에서 활용되고 있다[1]. 이러한 긍정적인 측면과는 반대로, 불법적인 목적으로 드론을 악용하기도 하며, 이에 대응하기 위한 비인가 드론의 전파방해 및 추적과 같은 드론 보안과 관련된 연구도 증가하는 추세이다[2].

최근 상용 WiFi 기반 드론은 AP 역할을 하는 드론이 접속하는 단말의 IP 주소를 부여하기 위하여 DHCP (Dynamic Host Configuration Protocol)를 이용하며, IP 주소를 할당받은 단말이 조종기 역할을 한다. DHCP의 특징은 자동으로 IP 주소를 할당하고 관리함으로써 편리한 장점이 있지만, 서버와 클라이언트 간 인증을 하지 않는 취약점이 존재한다[3]. 기존 DHCP에서는 이러한 문제점을 악용함으로써, 공격자가 DHCP 서버에서 할당 가능한 모든 IP 주소들을 소진시키는 DHCP 고갈 공격이 등장하였으며, 드론에서도 정당한 사용자가 드론을 사용하지 못하도록 할당 가능한 모든 IP 주소를 소진시키는 드론에서의 DHCP 고갈 공격이 등장하였다.

기존 연구는 공격을 위하여, 공개된 DHCP 고갈 공격 도구들을 사용하였지만, 이러한 도구들은 유선에서의 DHCP 서버를 대상으로 구현되었기 때문에, 무선에서의 DHCP 서버를 대상으로 공격하기에는 한계점이 존재한다. 따라서 본

논문에서는 드론 환경에서의 DHCP 고갈 공격 취약점을 분석하기 위하여, 공개 도구들의 소스코드를 분석하고 무선 및 드론 환경에서 공격이 가능한 도구로 개선하고, 드론 환경에서의 DHCP 고갈 공격의 가능성을 분석하고 실증한다.

2. 관련 연구

2.1. DHCP

DHCP는 동일한 네트워크를 사용하는 단말의 IP 주소를 자동으로 할당하는 프로토콜로, 관리의 효율성과 편의성을 제공하는 프로토콜이다[4]. 드론과 컨트롤러 간 DHCP에서의 IP 주소 할당 과정을 살펴보면, 드론이 DHCP 서버의 역할을 하고, 사용자의 스마트폰과 같은 단말인 컨트롤러가 DHCP 클라이언트 역할을 한다.

먼저, 컨트롤러가 Discover 메시지를 드론에 전달하여 할당 가능한 IP 주소를 요청한다. 드론은 사용되지 않은 IP 주소를 컨트롤러에게 Offer 메시지로 전달하며, 컨트롤러는 드론이 제안한 IP 주소를 사용하기 위하여 request 메시지에 해당 IP 주소를 사용하겠다는 내용을 드론에게 전달한다. 마지막으로 드론은 컨트롤러로부터 전달받은 Request 메시지의 내용을 토대로 Ack 메시지를 전달함으로써 최종적으로 IP 주소를 할당한다[5].

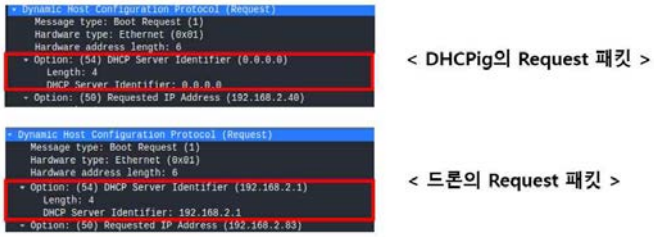
하지만, 이 과정에서 확인할 수 있듯이, 악의적인 공격자가 패스워드 크래킹과 같은 공격 기술을 활용하여 드론 내부 네트워크로 침입한다면, 가짜 Offer 메시지를 지속적으로 송신함으로써 드론에서 할당 가능한 모든 IP 주소를 고갈시키는 취약점이 발생한다.

2.2. DHCP 고갈 공격

DHCP 고갈 공격이란, DHCP 서버를 대상으로 Discover 메시지를 조작하여, 서버에서 할당 가능한 모든 IP 주소들을 고갈시키는 공격이다[6]. 무선 환경에서의 DHCP는 MAC 주소를 기반으로 IP 주소를 할당하기 때문에, 악의적인 공격자가 임의의 MAC 주소로 조작한 Discover 메시지를 생성하여 할당 가능한 모든 IP 주소를 고갈시킬 때까지 지속적으로 드론에게 메시지를 전달한다. 공격에 성공한다면, 드론은 할당 가능한 모든 IP 주소들이 존재하지 않는 MAC 주소를 가진 단말에 연결된 것으로 판단하여 정상적인 사용자도 IP 주소를 할당받지 못함으로써 드론 내부 네트워크로의 접근이 거부된다.

3. DHCP 고갈 공격 도구 분석 및 개선

DHCP 고갈 공격을 제공하는 공개 도구로, DHCPig와 Yersinia가 있으며, DHCPig는 Python 라이브러리인 scapy와 Python 2.7.18을 기반으로 작성되었고[7], Yersinia는 네트워크 프로토콜의 취약점 일부를 이용하여 공격하도록 설계된 도구이다[8]. DHCPig를 사용하여 드론 환경에서의 Request 패킷을 분석한 결과를 그림 1에 나타내었다.



(그림 1) DHCPig를 사용한 드론 환경에서의 Request 패킷 분석 결과

그림을 살펴보면, Request 패킷에는 패킷을 수신할 DHCP 서버의 IP 주소인 DHCP Server Identifier가 포함되어있다. 실제 드론의 Request 패킷에는 드론의 IP 주소가 있지만 DHCPig의 Request 패킷에는 0.0.0.0으로 명시된 것을 확인할 수 있다. 이와 같이, DHCPig는 드론이나 무선 네트워크를 대상으로 제작된 공격 도구가 아니므로, 드론 환경에서의 DHCP 고갈 공격을 수행하기 위한 개선이 요구되는 것으로 판단하였으며, DHCPig에서 일부 소스코드를 수정한 부분을 그림 2에 나타내었다.

```
//수정 전
  dhcp_req = Ether(src=mymac,dst="ff:ff:ff:ff:ff:ff")/
    IP(src="0.0.0.0",dst="255.255.255.255")/
    UDP(sport=68,dport=67)/
    BOOTP(chaddr=[mac2str(localm)],xid=localxid,flags=0xFFFFFF)/
    DHCP(options=[("message-type","request"),("server_id","sip"),
     ("requested_addr",myip),("hostname",myhostname),("param_req_list","pad"),"end"])
  LOG(type="--&amp;gt;", message= "DHCP_Request "+myip)
  sendPacket(dhcp_req)

//수정 후
  dhcp_req = Ether(src=mymac,dst="ff:ff:ff:ff:ff:ff")/
    IP(src="0.0.0.0",dst="255.255.255.255")/
    UDP(sport=68,dport=67)/
    BOOTP(chaddr=[mac2str(localm)],xid=localxid,flags=0xFFFFFF)/
    DHCP(options=[("message-type","request"),("server_id","192.168.2.1"),
     ("requested_addr",myip),("hostname",myhostname),("param_req_list","pad"),"end"])
  LOG(type="--&amp;gt;", message= "DHCP_Request "+myip)
  sendPacket(dhcp_req)
```

(그림 2) DHCPig 일부 소스코드 수정 부분

DHCPig의 소스코드 일부를 살펴보면, scapy를 이용하여 Request 패킷을 생성하는 부분에 DHCP Server Identifier로 판단되는 "server_id"가 명시되며, 해당 부분을 드론의 IP 주소로 수정하였고, 2계층이나 3계층에서 생성한 패킷을 전송하기 위한 코드 일부를 수정하였다.

4. 실험 결과

실험 환경은 다음과 같다. 공격 대상은 WiFi 기반의 드론인 DJI Tello, DJI Spark, Parrot Bebop 2, Parrot AR Drone 2.0이며, 공격 환경은 VMware Workstation 16 Pro, Kali Linux 2022.2이다. DHCPig를 개선한 도구를 토대로, DHCP 고갈 공격의 실험 결과를 표 1에 나타내었다.

<표 1> DHCP 고갈 공격 실험결과

드론명	DHCPig	Yersinia	DHCPig 개선 도구
DJI Tello	X	X	X
DJI Spark	X	X	O
Parrot Bebop 2	O	X	O
Parrot AR Drone 2.0	X	X	X

(그림 3) DJI Spark 고갈 공격 결과 일례
(위: 공격 전, 아래: 공격 후)

기존의 DHCPig 도구를 사용할 경우, Parrot Bebop 2 드론만 DHCP 고갈 공격이 성공하였지만, 개선 도구를 활용할 경우에는 DJI Spark 드론도 공격에 성공하였다.

DJI Spark 드론은 하나의 단말만 연결하기 때문에, 공격을 위하여 컨트롤러가 드론에 접속하기 전에 개선한 도구로 DHCP 고갈 공격을 수행하였다. 이후 드론과 연결된 모든 단말을 해제하고 새로운 컨트롤러가 접속을 시도하였을 때, 드론에게 IP 주소를 할당받지 못하는 것을 확인하였으며, 그 결과를 그림 3에 나타내었다.

5. 결론

본 논문에서는 기존 DHCP 고갈 공격을 제공하는 DHCPig와 Yersinia를 분석하고, 이를 드론 환경에서도 공격이 가능하도록 WiFi 기반의 드론을 대상으로 DHCPig 도구를 개선하였다. 개선된 도구를 활용한다면, 기존의 DHCPig 도구에서 실패하였던 DHCP 고갈 공격이 DJI Spark에서 성공한 것을 실증하였다. 향후에는 Yersinia와 같은 다른 도구들을 분석함으로써, 드론을 대상으로 DHCP 고갈 공격을 성공하기 위한 방안 및 대응방안을 연구할 예정이다.

감사의 글

1. 이 논문은 ETRI부설연구소의 위탁연구과제 [2022-072]로 수행한 연구결과입니다.
2. 이 논문의 내용을 발표하는 때에는 ETRI부설연구소에서 수행한 위탁결과임을 밝혀야 합니다.

참고문헌

[1] 구도형, 김승주, 이상진, "정찰 드론 보안성 평가 기준에 대한 연구", 정보보호학회논문지, vol.32, no.3. pp. 591-605, 2022.
[2] 김륜우, 송홍종, 반태원, "군집 비행을 이용한 불법 드론 추적 기법", 한국정보통신학회논문지, vol. 26, no. 6, pp. 943-948, 2022.
[3] 노진원, 박동규, "기업형 무선 네트워크 환경에서의 능동적 Rogue DHCP 공격 영향 분석", 한국통신학회논문지, vol. 46, no. 4, pp. 651-657, 2021.
[4] 권영미, 이극, "DHCP를 사용한 Mobile IP 프로토콜의 설계 및 구현", 디지털콘텐츠학회 논문지, vol. 3, no. 2, pp. 187-196, 2002.
[5] 우형석, 박홍근, 류인호, 김형진, "정보보안을 위한 네트워크 신뢰성 분석에 관한 연구", 한국산학기술학회논문지, vol. 11, no. 10, pp. 3935-3941, 2010.
[6] H. Mukhtar, K. Salah, and Y. Iraqi, "Mitigation of DHCP starvation attack", Computers & Electrical Engineering, vol. 38, no. 5, pp. 1115-1128, 2012.
[7] DHCPig, https://github.com/kamorin/DHCPig, 2022년 9월 7일 접속.
[8] Yersinia, https://github.com/tomac/yersinia, 2022년 9월 7일 접속.