드론을 이용한 무선네트워크 공격 시나리오와 대응방안

김선광°, 문은정, 김초영, 안하영, 김승준, 한철규*
{중앙°, 수원, 공주, 부산, 인하}대학교, LG_CNS*
blueksg0307@gmail.com°, {trace0919,kimchoyoung7,dkdlel0229}@naver.com

A study of Modeling and Simulation for Analyzing wireless Attack with drone

Kim Seonkwang°, Moon Eunjung, An Hayoung, Kim s
{Chung-Ang°, Suwon, kongju National, Pusan, Inha University. LG_CNS*

요 약

우리는 모든 것이 연결되는 4차 산업혁명 시대에 살고 있다. 그와 마찬가지로 보안 위협들도 새롭게 연결된 형태로 나타나고 있다. 본 논문에서는 드론과 정보통신기술이 융합된 형태의 공격 방법을 제시하고 그에 대한 대응방안을 제시한다.

1. 서론

오늘날 우리는 4차 산업혁명의 시대에서 살고 있다. 그러므로 모든 것이 융합되고 연결된 형태로 나타나고 있다. 이러한 모습은 산업에서만 나타나는 것이 아니라 우리를 위협하는 보안문제도 융합된 형태로 나타난다.[1] 전통적인 방법의 웜과 바이러스를 통한 공격방법에서 전통적인 방법과 다른 분야를 결합한 사회공학적인 공격으로 변화하고 있다. 더욱 심각한 것은 이러한 공격이 금전적인 피해를 유발하는 형태로 이루어지고 있다는 점이다.

본 논문에서는 드론을 이용한 무선네트워크 공격 시나리오를 연구하고 시나리오 안에서 단계별 위험요소에 대해 살펴볼 것이다. 무분별한 무선네트워크 사용에 대한 심각성을 재고시키며 국내외에서 시행하는 기술적인 대응방법을 조사하여 단계적으로 발생하는 취약점들에 대한 대응방안을 제안하였다.

2. 배경

과거에는 드론이 주로 군사용으로 개발되었으나, 최근에는 다양한 분야로의 활용가능성이 높아지면서 산업 및 민간용 시장으로 빠르게 확산되고 있다.[2] 또한 차세대 드론 산업은 제조·서비스 융합모델로 주목받고 있으며, 특히 IT 기술 및 다양한 서비스 등과 융합하면서 시너지가 창출되고 있다. 그러나 드론은 스마트폰과 마찬가지로 무선통신과의 접목이 필수적이므로 정보통신기술에 사용된다면 보안적인 문제를 가지고 있다. 그리고 다수의 스마트폰이나 노트북 등 휴대용 컴퓨터 장치 때문에 이를 수용하기 위한 무선 AP 환경도 증가하고 있다. 또한 디바이스 사용자를 위해 대부분의 장소에서 무료 와이파이를 제공하고 있다. 이런 환경에서 여러 사용자가 함께 내부IP에 있기 때문에 개인정보 유출이 쉽게 발생한다. 하지만 대부분의 사용가자 이러한 위험성을 제대로 인식하지 못하고 있는 것이 현실이다.

3. 공격 시나리오 도출

3.1 연구 환경

	실험환경
드론	Parrot AR.Drone 2.0 Elite Edition Quadcopter
피해환경	Nox
공격환경	kali linux
Software	aircrack-ng
공유기	iptime n5-i

표.1 실험환경

본 논문에서 제안하는 공격 시나리오는 드론을 이용한 상황, 공유기 공격, Mac address 변조, 악성 앱 설치라는 단계를 거친다. 그러므로 단계적인 실험을 위해 다음과 같은 실험 환경을 구축하고 실험하였다.

3.2 시나리오 흐름도

다음은 시나리오의 흐름도이다. 가장 처음에 발생하는 상황은 사람들이 많은 곳에 무선 AP를 내장한 드론이 나타나 이목을 집중시킨다. 공격자는 해당 지역의 공용 네트워크를 분석하고 공격하여 이용불가능하게 만든다. 그리

고 공격자가 가진 AP를 공용네트워크인척 변경한 후 접속을 유도한다. MAC 주소 위조를 통한 개인정보를 수집한 다음에 악성 URL을 보내 앱 설치를 유도한 후 개인정보를 유출한다.

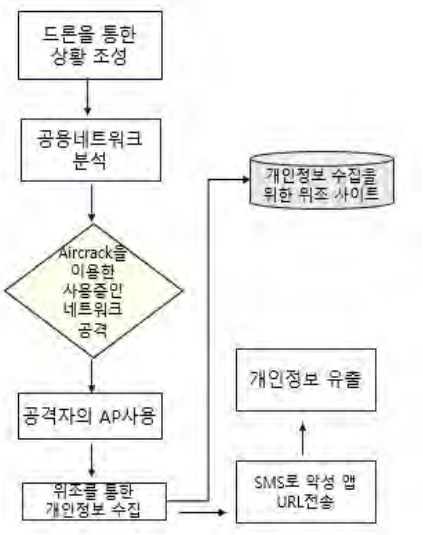

그림.1 시나리오 흐름도

공용 네트워크 분석 단계에서는 해당 네트워크가 가지는 지역성, 특수성을 파악하게 된다. 해당 단계에서 파악된 지역성이나 특수성은 후에 위조 사이트를 제작하거나 URL링크의 신뢰성을 높이는 데에 사용된다. 아래 그림은 지역성을 활용한 위조 사이트이다.[3]

그림.2 위조 사이트 예시

네트워크 분석 후 aircrack-ng로 네트워크를 공격한다. 패킷을 수집 후 수집한 정보를 바탕으로 해당 공유기의 비밀번호를 알아낸다.[5] 비밀번호의 해킹확률을 높이기 위해 비밀번호로 자주 사용되는 키워드들을 파악하여 입력해 놓는다. 네트워크 해킹 후 해당 네트워크에 속해있는 장비를 선정하여 IP, MAC주소를 파악한다. 또한 사용 중인 공용 와이파이 해제를 위해 공용 네트워크서버를 공격한다. 이후 미리 제작한 위조 사이트를 희생자에게 보여준다. 이 과정에서 희생자의 신뢰도를 높이기 위해 위에서 수집한 지역성과 특수성을 이용한다. 이러한 신뢰성을 기반으로 희생자는 자신의 개인정보를 입력 후 '완료' 버튼을 누르면 해당 정보가 공격자의 PC로 전송되게 된다.

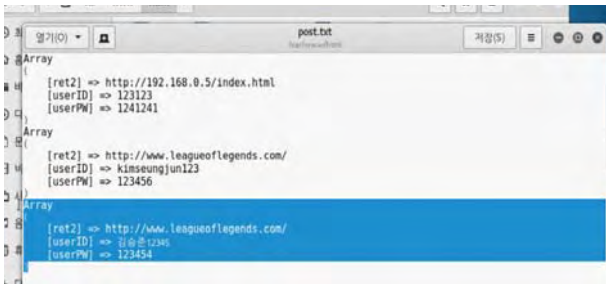

그림 3. 피해자의 개인정보 수집

위조 사이트를 통해 전화번호를 탈취한 후, 해당 전화번호로 URL을 보낸다. URL을 클릭한 희생자의 휴대폰에 앱이 설치되고 앱을 통해 다양한 정보를 탈취하게 된다. 위의 과정에서 역시 신뢰성을 높이기 위해 여러 기법들이 사용된다. 본 연구에서 분류한 신뢰성을 높이는 방법은 다음과 같다.

- 신뢰성 있는 기관에서 온 메시지
- 신뢰성 있는 사람에서 온 메시지
- 자신의 이익과 관련된 일에 대한 메시지
- 위급한 상황에 대한 메시지

그림.4 신뢰성을 높인 URL 예시

위의 URL을 클릭하여 앱을 다운로드하면 해당 핸드폰의 해킹이 완료된다. 해킹이 완료되면 해당 핸드폰의 카메라를 실행시키거나 메시지 내용을 확인하는 등의 개인정보 해킹이 가능하다

4. 대응 방안

무선 랜은 선이 없고 데이터가 공기 중으로 날아다니므로 악의적인 공격자가 데이터를 중간에 훔쳐보는 것이 가능하다. 또한, 무선 네트워크는 개인만이 아닌 민감한 정보가 많은 기업 내부에서도 사용되므로 보안에 더욱 더 유의해야 한다. 여기에선 무선 장치 측면에서의 방어와 개인이 취할 수 있는 방어에 대해 제시한다.

4.1 무선 네트워크 장비 차원의 방어

무선 장치가 초기 출시 될 때, 모든 비밀번호가 기본설정으로 변경된다는 점과 다른 단말기나 다른 장치와 통신할 때 자신의 SSID가 담긴 Broadcast를 보낸다는 점 등 무선기 자체만으로 가지고 있는 취약점이 많으므로 이 설정을 다음과 같이 변경해 취약점을 최소화 하는 것을 권장한다.[4][5][6]

- 무선 랜의 초기 비밀번호 변경하기
- 권장된 비밀번호 만들기
- SSID의 Broadcast 기능 제한
- 관리자 모드의 SSID 숨김모드 사용
- 무선 랜 전파범위 제한
- 가장 안전한 WPA2와 AES 암호화 알고리즘 권장
- 암호화에 사용되는 AES의 Key값 변경하기
- reset 버튼이 있는 공유기는 물리적 접근을 제한

4.2 사용자 차원의 방어

무선 랜을 통한 해킹은 모두 피해자가 될 수 있다. 사용자들의 편의를 위해 하는 행동에 취약점이 발생한다. 공격자가 악의적으로 만든 무선 네트워크에 접속하게 되더라도 다음과 같은 항목만 지킨다면 피해를 예방할 수 있다.

- 공공장소의 무선 네트워크 이용 제한
- 모르는 네트워크 환경에서 개인정보 입력 금지
- 핸드폰 백신 앱 사용
- MSG로 전송된 URL에 함부로 접속 금지
- 정식 앱 스토어를 통해서만 앱 다운로드
- '알 수 없는 출처 앱 설치' 기능 해제
- 주기적인 운영체제 업데이트

5. 결론

본 연구에서는 최근 급속도로 다양해지고 지능화된 사회 공학적 기법을 이용한 무선 네트워크 공격에 대한 시나리오를 수립하고 테스트해 보았다. 여러 가지 소프트웨어를 이용한 공격을 진행하였으며 위협을 가할 수 있는 공격이 어렵지 않고, 주변에서 쉽게 일어날 수 있을 만한 일이라는 것을 확인하였다. 또한 보안 위협에 대한 대응을 본 연구를 통해 제시하였다. 따라서 본 연구에서 제시한 해결 방안을 준수한다면 개인 보안 유지에 큰 도움이 될 것이라 기대한다. 이외에도 보안 위협에 대한 효율적 대응을 위해서는 상용화된 많은 공격용 툴을 사용해 보며 어떤 식으로 보안위협이 발생하는지 정보보호 전문가들의 관심과 체계적인 보안 기술이 개발되어야 할 것이다.

참고문헌

[1] 남기호 "융합보안 기술 동향 및 이슈" 정보통신기술진흥센터 주간기술동향 (2014.11)

[2] 이아름 "드론 시장 및 산업 동향" 융합연구정책센터 (2017.01) vol.53

[3] 이동휘, 최경호, 이동춘, 김귀남, 박상민 "사회공학기법을 이용한 피싱 공격 분석 및 대응기술" 정보보안 논문지 제 6권 제4호 (2006.12)

[4] 정현철, 이희조 "무선 랜 보안 실태 조사 및 분석을 통한 보안 강화 방안 연구" 한국정보과학회지(2002.04)

[5] 최진호, 오수현 "무선 랜 환경 인증 메커니즘의 취약성 분석 및 대응방안 연구" 情報保護學論文誌 (2012.11)

[6] "제2010-12호-무선랜_보안안내서" 한국인터넷진흥원 KISA 안내 제2010-12호(2010.01)

"본 논문은 2017년 한이음 ICT멘토링 프로젝트의 결과물입니다."