JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 20, No. 5, pp. 1069-1077, May 2019

사물인터넷의 경량 IP 카메라 취약점을 이용한 해킹 공격 및 대응 방안

조 이 든 · 박 수 진 · 강 남 희*
덕성여자대학교 공과대학 IT미디어공학과

Hacking Attacks and Countermeasures using Vulnerabilities of Lightweight IP Camera in Internet of Things

Eden Cho · Soojin Park · Namhi Kang*
Department of IT Media Engineering, College of Engineering, Duksung Women's University

[요 약]

사물인터넷(IoT: Internet of Thing) 기술은 사용자 주변의 일상 사물들이 상호 연결되어 정보를 공유할 수 있도록 해준다. 이러한 혁신적인 기술은 인간의 삶에 긍정적인 변화를 가져올 수 있다. 그러나 적절한 보안 기술이 적용되지 않으면 민감한 개인 정보가 인터넷에 공개 될 수 있다. IoT 환경에서 보안은 민감한 개인 정보 유출뿐만 아니라 생명에 직결된 문제가 발생 할 수 있기 때문에 반드시 지원되어야 하는 핵심 기술이다. 본 논문에서는 IoT 장치(IP 카메라를 예로 적용)에 대한 해킹 공격을 수행하여 IoT 경량 장치는 여러 가지 잠재적인 취약성을 가지고 있기 때문에 안전하지 않다는 사실을 보인다. 해킹 테스트에서 공격자는 쇼단(Shodan) 검색 엔진을 사용하여 대상 IP 카메라를 발견하고, 대상 장치의 비디오 데이터를 훔칠 수 있다. 또한 공격 대상 장치의 동작을 강제로 종료(즉, 서비스 거부 공격 수행)시킬 수 있다. 본 논문은 시험을 통해 분석된 잠재적 보안 위협을 분석하여 각 공격들에 대처할 수 있는 방안들을 제시한다.

[Abstract]

The IoT(Internet of things) technology enable various daily-life objects around user to be connected with each other for sharing information. Such an innovative technology can lead to positive changes in human life. However, if there is no proper security mechanism, private and sensitive data around human can be revealed to public Internet. To support security is the mandatory requirement in IoT services because it is related to the disclosure of private information but also directly related to the human safety. In this paper, we perform hacking attacks against an IoT device (IP Camera as an example) to show that such an lightweight IoT device is not secure because it has several potential vulnerabilities. In the hacking scenario, an attacker can discover the target IP camera by utilizing the Shodan search engine, then he can steal private video data from the target device. Further he forcibly terminate the operation of the target device (i.e. denial of service attack). In addition, this paper describes potential security threats analyzed through attacking test and suggests several countermeasures to cope with the attacks.

색인어 : 사물인터넷, IP 카메라 취약점, 쇼단, 스누핑, 서비스거부 공격

Key word : Internet of Things, IP Camera Vulnerabilities, Shodan, Snooping, Dos Attacks

http://dx.doi.org/10.9728/dcs.2019.20.5.1069

Received 25 April 2019; **Revised** 09 May 2019
Accepted 27 May 2019

***Corresponding Author; Namhi Kang**

Tel: +82-2-901-8349
E-mail: kang@duksung.ac.kr

Ⅰ. 서 론

사물인터넷(IoT: Internet of Things) 기술은 통신 인프라에서 주로 수행되었던 사람과 사람, 사람과 사물 간의 연결에서 생활 속 모든 것(물리 객체 및 가상 객체 포함)들을 인터넷 기술을 이용하여 상호 연결시키려는 기술로 생각할 수 있다. 즉, IoT 기술은 주변의 다양한 기기들과 더 나아가 가상의 프로세스와 자원들까지 인터넷에 연결하여 서비스의 요구사항을 만족시켜주는 사물지능통신으로 발전되고 있다[1].

네트워크에 연결되는 IoT 기기가 증가하면 민감한 개인 정보, 의료 정보 등 노출 될 수 있는 데이터의 양이 증가하며, 사람의 생명에 직결될 수 있는 문제가 발생할 수 있기 때문에 IoT 환경에서의 보안기술은 반드시 제공되어야 하는 핵심기술이다. 그러나 IoT 환경의 종단 디바이스로 동작되는 기기들은 대부분 자원이 제한적이고 배터리에 의존하여 동작된다. 보안을 제공하기 위한 복잡한 기능을 수행하기에 연산 능력과 저장 능력에 제한을 받는다. 또한 기기 간 연결에 사용되는 무선 통신 접속 기술도 저전력 사용을 목표로 설계되다보니 데이터 전송량이 작고, 무선 매체의 특성으로 인한 손실과 지연이 발생할 수 있기 때문에 IoT 환경의 모든 기기들에 적합한 보안 기술을 개발하는 것은 쉽지 않다. 따라서 보안 기술의 경량화는 핵심 요구사항 중 하나이다[2].

미국의 인터넷 도메인 서비스(DNS: Domain Name System) 전문 업체인 딘(Dyn)에 대규모 서비스거부(DDoS: Distribute Denial of Service) 공격이 발생한 사례가 있다. 당시 해당 공격의 주요 원인은 악성코드인 미라이에 감염된 사물인터넷 기기들로 보고되고 있다. 미라이 바이러스는 보안이 취약하고 초기 암호를 변경하지 않은 사물인터넷 기기를 DDoS의 좀비 장치로 사용 하였다. 이러한 공격은 IoT 기기에 설정된 초기 비밀 접속정보를 바꾸면 경감 할 수 있지만, IoT 기기는 설정을 위해 필요한 입력기기(e.g. 키보드)나 출력기기(e.g. 모니터)가 부재하고, 보안지식이 부족한 일반사용자가 보안 구성을 안전하게 설정하기에는 어려움이 있다[3]. IoT 기기의 접속 정보나 인증 기술이 안전하지 않을 경우, 상기 예시로 든 공격 이외에도 다양한 문제가 발생될 수 있다. 개인 주변에 많이 설치되어있는 IoT 기기를 통해 정보가 유출될 수 있고, 유출된 정보는 2차 보안 공격에 악용될 수도 있다.

앞으로도 IoT 장치에 대한 공격이 증가할 것이라는 전망 가운데, 시만텍은 IoT 장치가 증가하는 만큼 장치를 이용한 분산 서비스거부 공격도 활발할 것으로 예측하고 있다[4]. 또한 글로벌 보안 기업 트렌드마이크로는 2017년 보안 예측 보고서에서 랜섬웨어 공격의 대상이 될 수 있는 시스템의 범위를 IoT 장치로 확장시킬 것이라고 전망했다[5].

본 논문에서는 이러한 보안 공격이 실생활에 적용된 IoT 기기에서도 가능할 수 있음을 보인다. 공격자가 주변에 설치되어 있는 취약한 IoT 카메라를 발견하고, 대상 장치의 영상을 유출하고, 더 나아가 대상 장치의 동작을 방해할 수 있는 공격들을 구현하여 시험한다. 또한, 공격 가능성에 해당하는 잠재 위협을 분석하여 공격에 대응할 수 있는 방안을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 해킹 공격에 사용되는 쇼단(Shodan)과 서비스 거부 공격을 설명한다. 3장에서는 IP 카메라를 대상으로 영상 유출과 서비스 거부 공격을 수행한 결과를 보인다. 4장에서는 잠재적 위협에 대처할 수 있는 대응 방안들을 제시하고, 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

2-1 쇼단(Shodan)을 이용한 사물인터넷 기기 정탐

사물인터넷의 활성화로 기존에 연결을 고려하지 않은 다양한 종류의 기기들이 인터넷에 연결되면서 쇼단이라는 검색 엔진이 관심을 받고 있다. 구글과 같은 일반 웹 검색 엔진은 웹 페이지의 데이터를 크롤링 한 다음 검색을 위한 색인을 생성한다. 이와 다르게 쇼단은 인터넷에 연결되어있는 기기의 포트를 검색하고, 결과로 전달 받은 배너를 색인화 한다. 이를 통해 웹 카메라, 라우터, VoIP, 산업용 시스템 등 인터넷에 연결된 모든 장치들을 검색하게 된다. 다음 그림 1은 쇼단에서 기기의 배너 정보를 획득하여 검색 데이터베이스를 갱신하는 기능의 흐름을 나타낸다[11].

쇼단은 합법적인 웹 기반 서비스로 이용자는 인터넷에 연결된 네트워크 연결 상태, IP주소, 서버의 종류와 같은 장치의 정보를 검색할 수 있다. 또한, 인터넷에 연결되어 있는 장치의 취약점을 알려주어 보안에 대해 위험성을 알릴 수 있다. 이 정보들이 기기에 직접적인 보안 위협을 가하지 않을 수 있지만 이를 악용할 수 있다는 점이 문제이다. 쇼단은 공격자들에 의해 악용되어 기기의 정보나 콘텐츠가 유출되기도 하고, 2차 보안 공격에 활용하기 위한 정탐 도구로도 활용될 수 있다.

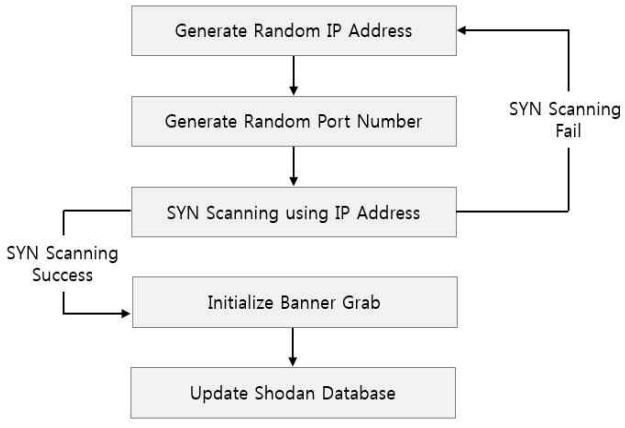

그림 1. 쇼단 스캐닝 기능 흐름도
Fig. 1. Shodan Scanning Function Flow

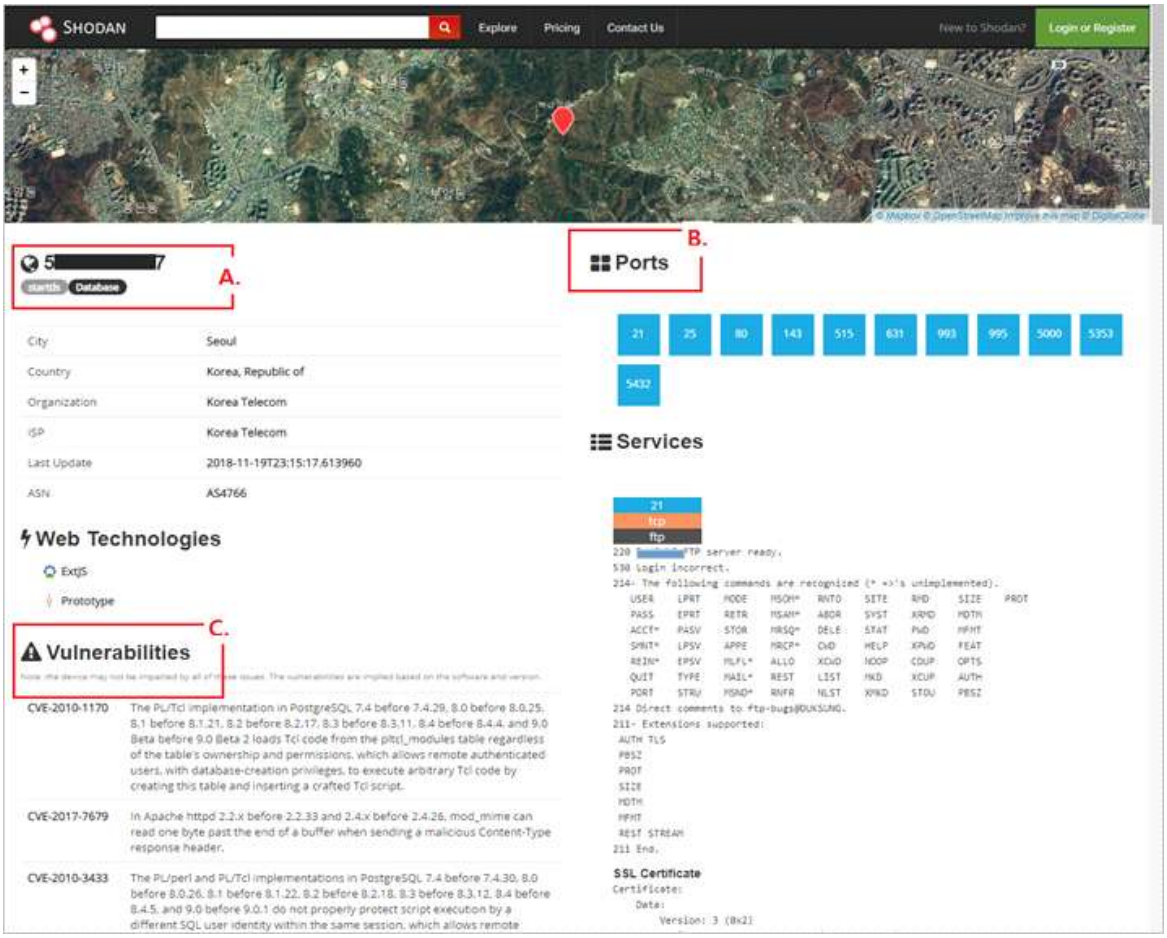

그림 2. 쇼단을 통한 정탐
Fig 2. Reconnaissance by using Shodan

그림 2는 저자들의 소속 기관 이름을 쇼단에서 검색한 결과를 나타낸다. 그림의 A 부분은 검색된 기기의 기본 정보, B 부분은 접속 가능한 포트 번호, 그리고 C 부분은 해당 시스템의 알려진 취약점들이 공지된다. 해당 시스템은 SSL 인증서를 사용한 인증을 제공하고 있지만 주어진 취약점에 대한 대응을 하지 않았다면 오히려 취약점 정보들을 악용하여 해킹 공격이 가능해진다. 상기 설명한 바와 같이 보안 기술이 적용되어있고 전문 담당자가 관리하는 인터넷 기반 시스템의 경우도 해킹 위협이 존재하는데, 전문가가 아닌 일반 사용자가 설정하고 관리하는 사물인터넷 장치들은 더욱 쉽게 노출될 수 있고 해킹 공격에 취약함을 쉽게 예상할 수 있다.

쇼단은 나라, 위/경도, 특정IP, 운영체제 등의 검색 필터를 이용하여 특정 장치를 검색할 수 있다. 예를 들어, 기본 값으로 자주 사용되는 아이디 'admin'과 비밀번호 '1234'를 입력하면 해당 아이디와 비밀번호를 가진 장치들을 쉽게 찾아낼 수 있다. 실제로 해커들이 쇼단을 이용하여 웹 카메라, CCTV, 베이비 모니터 등에서 찍힌 동영상이 인터넷에 공개되기도 했다. 이는 웹 카메라 등에 제조나 설치 시 설정된 기본 비밀번호를 쉽게 획득할 수 있기 때문에 공격이 쉽게 감행된 것이다. 해커들은 이를 위해 가정에서 동영상, 음악 파일 등을 다운로드 받을 때 웹캠에 접근이 가능하도록 하게 해주는 악성코드를 추가하여 침투시켰다. 악성코드에 의해 감염이 되면 PC는 웹캠의 디폴트 비밀번호를 쇼단에 전송하고 해커들은 이를 이용하여 동영상을 확보하는 것이다[12].

2.2 서비스 거부 (DoS: Denial of Service) 공격

DoS 공격은 서비스 가용성(Availability)을 저해하려는 목적을 갖는 공격으로 시스템이나 네트워크의 제한된 자원 (통신 대역, 인프라 시스템, 서버 자원 등)에 대한 불필요한 사용을 극대화하도록 유도하여 정상적인 서비스를 방해하거나 정상 사용자의 자원 이용을 막는 행위를 의미한다.

DDoS(Distributed DoS) 공격은 분산된 공격 엔티티(entity)들이 다수 참여하여 동시 다발적으로 목표 시스템에 DoS 공격을 수행하는 행위로 볼 수 있다. DDoS 공격은 1996년 네트워크 자

원을 고갈시키는 방식의 공격으로 등장한 이후 인터넷 환경의 발달과 함께 공격 횟수 및 규모, 그리고 피해액이 끊임없이 증가하고 있다. 다수의 사용자가 동시 접속을 시도하는 웹서버의 경우 DDoS 공격에 대해 효과적인 탐지 방법의 적용에는 어려움이 있다. DDoS 공격에 이용되는 컴퓨터의 고성능, 네트워크 인프라의 발전으로 전송 대역의 증가, 봇넷의 증가, 침해 시 책임 추적의 어려움 등으로 정보보안과 침해영향력에 있어 가장 큰 위협이 된다[6].

DDoS 공격은 침해 기술의 복합 고도화, 인프라 장치에서 응용 서비스까지 공격 범위 및 목표의 확대, 불분명한 공격 목적, 체계화된 범죄 조직화 등 다양하고 지능화된 형태로 진화되고 있다. 따라서 공격에 대응할 수 있는 방어 기술은 물론, 가능한 공격 방안을 사전에 예측할 수 있는 방어기재의 필요성이 계속 요구되고 있다[6].

러시아 보안 전문회사인 Kaspersky의 2017년 통계 자료에 의하면 DDoS 공격 형태는 SYN Flooding이 1분기 48%, 2분기 53%, 3분기 60%로 점차 증가하고 있고, 전체 공격의 과반 이상을 차지하고 있다. 또한 공격자가 서버에게 단순한 요청 패킷 전송에 대한 상대적으로 많은 양의 응답을 보내는 서버 증폭(DNS 등) 공격 대신 증폭 없이 스푸핑된 IP 주소 사용으로 채널에 과부화를 주는 SYN Flooding 공격이 지속 사용되고 있다[7]. 이에 대한 탐지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, DDoS 장비 등 네트워크 기반 보안장비가 시판되고 있으며 탐지방식은 TCP/IP(프로토콜 3/4 레이어) 이상행위 기반의 통계적 방식 'rate-limit'이 사용되고 있다. 하지만 통계적 방식은 스푸핑된 다수의 봇넷에 의한 slowris DDoS 공격과 정상 사용자와의 구분이 불가능한 어려움이 있다. 이를 해결하기 위해 정상 패킷과 스푸핑된 SYN Flooding DDoS 공격 패킷을 검출하는 방안도 제시되고 있다[6].

사물인터넷 서비스의 경우도 미라이 바이러스에 감염된 사물인터넷 기기들 도메인 서비스 업체에 대규모 DoS 공격을 시도한 사례가 있다. 사물인터넷 기기의 인증 취약성과 항상 인터넷에 접속되어 있는 점을 악용한 사례이다.

Ⅲ. IoT 경량 카메라 공격 시험

3-1 해킹 공격 구성도 및 개요

다음 그림 3은 사물인터넷의 해킹 공격을 위한 시험 네트워크의 구성도를 나타낸다. 공격 대상이 되는 IP 카메라는 대중적인 오픈하드웨어 라즈베리파이와 전용 카메라 모듈을 사용했다. 영상 전송 서비스를 제공하기 위해 VLC 프로그램을 설치하여 구축했다[8, 9]. 적법한 영상 수신기는 PC에 VLC 영상 플레이어 설치하여 사용했다.

그림 3. 해킹 공격을 위한 시험 구성도
Fig 3. Test Architecture for Hacking Attack

보안 공격을 수행하기 위해 칼리 리눅스가 설치된 공격 서버를 구축했고, 공격의 편의성을 위해 스마트폰에 앱(그림에 나타낸 IRIS)을 개발하여 원격 공격 제어기로 활용했다. IRIS 앱은 기기 검색 엔진인 쇼단을 이용하여 공격 대상 장치를 정탐하여 해당 장치의 인증 취약점을 확인할 수 있다. 인증 기술이 적용되지 않은 IP 카메라는 비인가 접속을 구분할 수 없고, 암호화되지 않은 영상 데이터는 모두 노출되어진다. 공격 시험을 위해 IP 카메라가 설치된 라즈베리파이에는 인증 기술이나 암호화 기술을 구현하지 않았다. 또한, IRIS는 쇼단을 통해 대상 기기의 접속 정보 (IP 주소, 포트 번호)를 획득하여 공격 서버에 전송해준다. 공격 서버는 대상 장치의 접속 정보를 기반으로 SYN 플로딩을 악용한 DoS 공격을 시도한다.

3-1 IoT 기기 취약점을 이용한 공격 시험

공격 시험을 통해 사물인터넷 서비스에서 다음과 같은 보안 서비스가 침해될 수 있음을 검증했다.

- IoT 기기 및 서비스 무단 접속: 기기 인증(Entity Authentication) 우회 접근, 초기 설정 비밀번호 정탐
- 데이터 유출: 기밀성(Confidentiality) 침해
- 서비스 거부: 가용성(Availability) 침해

취약한 기기 인증이 구현된 경량 IP 카메라는 영상 데이터를 수신할 수 있는 사용자와 공격자를 구분할 수 없다. 인증이 정상적으로 동작된다 해도 전송하는 영상 데이터가 암호화되어 있지 않아 전송되는 모든 데이터가 유출될 수 있음을 확인했다. 쇼단을 통해 기본 설정된 접속 정보를 사용하는 기기를 검색할 수 있어 본 시험과 유사한 공격이 쉽게 수행될 수 있음을 알 수 있다.

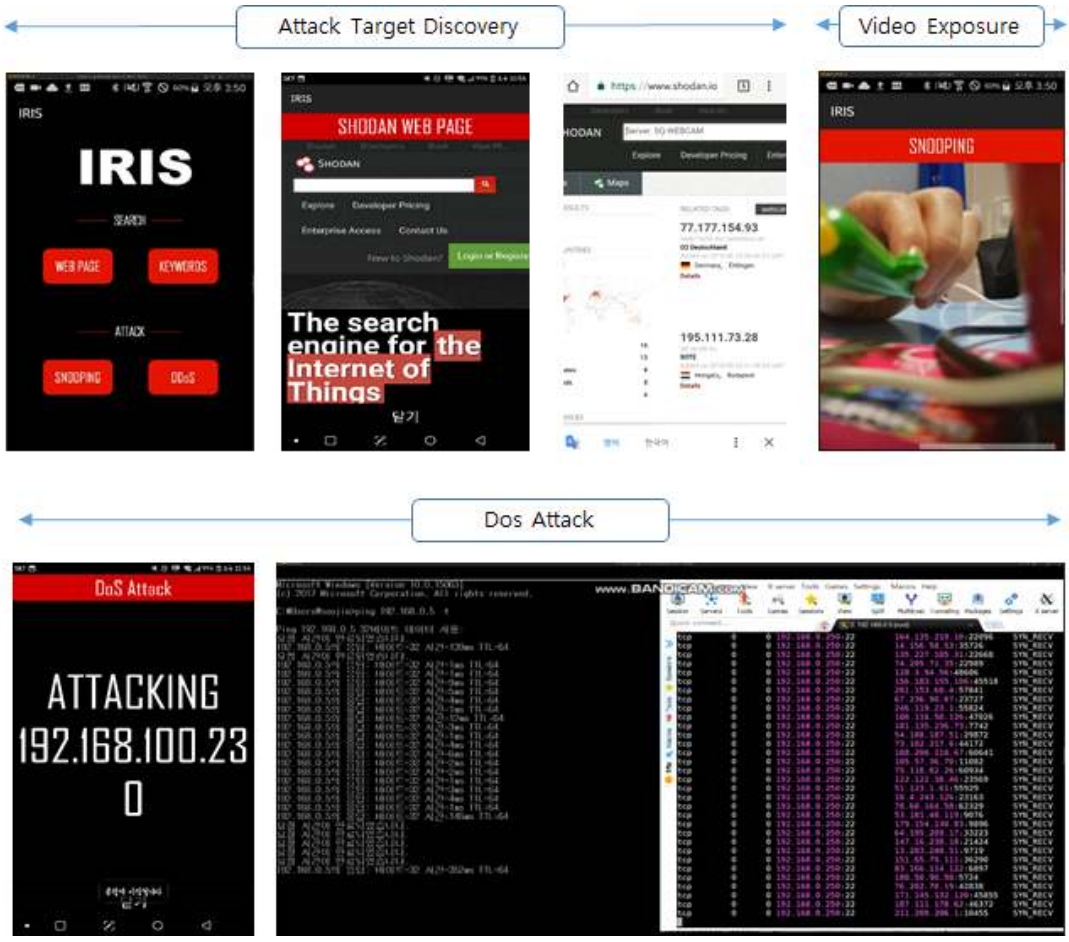

그림 4. 해킹 공격 시험 결과
Fig 4. Test Results of Hacking Attack

사물인터넷 기기의 경우 자원(가용 메모리, CPU 연산 능력 등)이 제한적인 특성으로 서비스 거부 공격에 취약함을 확인했다. 시험에 적용한 서비스거부 공격은 TCP 소켓 개설의 과정을 악용한 대표적 DoS 공격인 TCP SYN Flooding 공격을 사용했다. TCP 통신에서 세션 연결을 위해 서버에게 SYN 패킷을 보내면 서버는 SYN+ACK로 응답을 하고, SYN_RECV 상태가 된다. 클라이언트에게 응답(ACK)를 받기 전까지는 그 상태를 일정 시간 동안 유지하고 있게 된다. 이점을 악용한 TCP SYN Flooding 공격은 공격 대상 기기에 대량의 SYN 트래픽을 전송하여 서버의 가용 리소스를 소모하게 한다. 본 시험에서 스마트폰은 원격 제어기의 역할을 수행하고, 실제 공격은 동일 네트워크에 공격 서버를 구축하여 시험했다. 공격 서버가 IRIS 앱으로부터 공격 수행 메시지를 받으면 대상 IP 카메라에게 SYN 패킷을 보내기 시작하고, 앞서 설명한 공격 동작 원리에 따라 IP Camera는 더 이상 영상 송출을 할 수 없게 된다.

다음 그림 4는 스마트폰에 구현한 IRIS 앱이 공격 대상 장치를 정탐하고 해킹에 성공한 시험 결과를 나타낸다. IRIS 앱은 공격 대상 장치를 정탐하기 위해 쇼단 검색 엔진에 장치검색 메시지를 전송하여 기기의 인증 정보 및 접속 정보를 획득한다. 그림 4, 상단의 제일 왼편 이미지에 표시된 것처럼 IRIS 앱은 쇼단에서 가장 많이 검색되는 키워드도 확인할 수 있다. IRIS 앱은 기기 검색 후 획득한 정보를 기반으로 IP 카메라의 영상을 유출할 수 있다. 또한 접속 정보와 함께 공격 대상 기기에 DoS 공격을 수행하도록 하는 명령 메시지를 공격 서버에 보낸다. DoS 공격 서버는 IRIS로부터 전달받은 공격 대상 장치의 접속 정보로 대량의 SYN 플루딩 패킷을 전송하여 장치의 자원을 고갈시키게 된다. 쇼단을 통한 정탐은 정상 IP를 적용하여 시험했고, DoS 공격의 경우 소속 기관의 보안 정책으로 사설 네트워크를 구축하여 시험했다.

Ⅳ. 위협 분석 및 공격 대응 방안

4-1 개체 상호 인증 및 기밀성 제공 방안

정보 유출을 방지하기 위해 IoT 기기는 서비스에 접근 가능한 사용자를 식별하고 인증할 수 있어야 한다. 또한, 무선으로 전송되는 데이터는 도청이나 유출이 용이하므로 암호화해서 기밀성을 제공해야 한다. IoT 서비스 환경에서 특별히 고려할 사항은 장치의 경량 특성이다. IoT에 많이 적용되고 있는 경량 기기는 자원이 제한적이어서 적용되는 보안 기술도 경량화 되어야 한다[2, 10, 21].

IoT 경량 장치 사이에서 데이터 기밀성(Confidentiality)과 무결성(Integrity)을 제공하기 위해 다양한 국제 표준 기구들 (예: IETF, oneM2M, OMA 등)은 TLS와 DTLS 보안 표준 기술의 적용을 권고하고 있다. 특히, IETF에서는 IEEE 802.15.4와 같은 저전력 무선 네트워크를 사용하여 데이터를 전송하는 경량 장치 간 통신을 위해 CoAP를 표준화하였고, CoAP을 사용하는 장치 간 보안 전송을 위해 DTLS의 적용을 권고하고 있다 [2, 13, 14, 20].

DTLS 프로토콜을 IoT에 적용하여 그대로 사용하는 경우, 인터넷 환경에서 사용하고 있는 프로토콜을 재사용함으로써 호환성이 높일 수 있다는 장점이 있다. 하지만 DTLS 프로토콜은 컴퓨팅 자원에 제한이 없고, 네트워크 성능이 뛰어난 인터넷 환경에서 사용하던 프로토콜이므로 CPU나 메모리, 배터리와 같은 컴퓨팅 자원이 제한되어 있는 IoT 환경에 적용하기 위해서는 IoT의 환경적 특성이 고려되어야 한다.

IoT 경량 기기에 DTLS를 적용하여 상호 인증을 수행하고, 전달되는 데이터에 암호 통신을 제공하기 위해 사전 수행되는 DTLS 핸드쉐이크 과정은 경량 기기에 큰 부담이 된다[2, 10]. 또한, IoT 기기 간 적용되는 무선 통신 규격에서는 대부분이 적은 크기의 MTU(Maximum Transmission Unit)를 지원하므로 각 단계에서 전송되는 메시지는 수많은 프레임으로 분할되어 전송된다. 각각의 분할된 패킷은 지연 및 분실로 인해 재전송될 수 있고, 이는 네트워크 성능을 저하시킨다. 뿐만 아니라 분할 패킷은 “fragment duplication attack”이나 “buffer reservation attack” 등의 위험을 증가시킨다[15]. 또한, DTLS 프로토콜을 사용할 경우 핸드쉐이크 계층의 에너지 소비량은 레코드 계층 대비 약 8배 이상을 소모하므로 경량화된 방안을 적용해야 한다[10].

4-2 기본(default) 비밀정보 재설정

IoT 서비스 환경에서 개체 인증 및 기밀성을 제공하기 위해서는 기기에 설정된 초기 비밀값(접속 비밀번호, 사전 설정 비밀키 등)을 안전하게 설정할 수 있는 방안이 필요하다. 그러나, IoT 서비스 환경에 많이 적용되고 있는 대다수의 IoT 경량 기기는 공장 출하 시 일괄적으로 설정된 기본값을 사용한다. IoT 장치들에는 사용자 인터페이스(UI: User-device Interfaces)가 제한되거나 경우에 따라 구현되어 있지 않아 일반 사용자가 직접 장치를 설정하거나 구성하기 어렵다. 따라서, 초기 설정 단계에서 장치의 제조사나 설치자가 초기 설정을 해주는 경우가 일반적이다. 이 경우 설치자(혹은 제조자)와 시스템 관리자 사이의 신용(trust)은 중요한 이슈이다. 그러나 서비스 제공자와 설치자, 제조사 등 사이의 신용을 완벽하게 관리하는 일은 쉽지 않다. 이러한 이슈를 해결하기 위해 다양한 기술들이 제안되고 있다.

독일의 Olaf Bergmann은 IPv6와 CoAP을 기반으로한 무선 센서 네트워크에서 제한된 장치를 초기 설정하기 위해 3단계로 구성된 프로토콜을 제안하였다[16]. 제안 시스템은 버튼이나 LED와 같은 저렴한 사용자 인터페이스를 사용한다. 국내 사물인터넷 포럼 표준기술에서는 IoT 경량 기기를 제조하는 업체, 시스템관리자, 그리고 설치자의 신뢰가 보장되지 않은 환경에서 안전하게 비밀 정보를 설정하고 재설정 할 수 있는 기술을 제안하고 있다. 제안 기술에서는 NFC를 사용하여 사용자가 원하는 시점에 비밀키를 재설정 하며 인증 서버와 상호인증을 통해 신규기기를 안전하게 등록할 수 있는 방법을 사용한다. QR이나 NFC와 같은 전송 방식 이외에도 소리, 빛과 같은 저비용 전송 매체를 부가 채널의 요소로 활용될 수 있다. 소리와 빛을 사용할 경우는 각 전송 매체의 보안 특성과 적용 환경을 고려해야 한다. 자동차 글로브 박스에 적용되는 빛은 보안성이 강한 매체이고 공개된 장소에서 소리를 부가 채널로 사용할 경우 약한 보안 매체로 인식해야 한다[3].

4-3 DoS 공격 대응 방안

경량 IoT 기기로 구성되어진 서비스의 경우 기존 인터넷 기반 DoS 공격 이외에도 다양한 위협요소들이 존재한다. DoS 공격은 물리 계층에서 응용 계층까지 모든 통신 계층에서 가능하다. 물리 계층에선 전송 매체의 디지털/아날로그 신호를 복제한 이후 다량의 재전송을 통한 공격이나 대상 기기로의 재밍 신호 브로드캐스트 공격으로 기기의 서비스를 중단시킬 수 있다. 또한, 에너지 효율을 높이기 위해 동작되는 경량 기기의 sleep 모드를 방해하는 공격도 가능하다.

2계층에 해당하는 네트워크 접속 프로토콜의 특성을 악용한 DoS 공격도 가능하다. 특히, 사물인터넷에 주로 사용되는 무선 통신 프로토콜은 전송 성능 및 저전력 효과를 달성하기 위해 작은 크기의 프레임(즉, 작은 MTU 크기)을 주로 사용한다. 단거리 IoT 통신 규격으로 많이 적용되고 있는 IEEE 802.15.4의 경우 127 byte 크기의 MTU를 사용하고, 장거리 통신 규격으로 활용되고 있는 LoRa나 OMA의 SMS의 경우 각각 65 byte와 140 byte의 크기를 사용한다. 센서에서 취득된 상황 정보나 단순 제어를 위한 명령 메시지들은 상기 제시된 MTU를 사용하더라도 단일 프레임으로 전송이 가능하지만, 보안 소켓(예, DTLS)을 개설하기 위한 설정(핸드쉐이크) 메시지나 펌웨어 업데이트 메시지의 경우 메시지의 단편화(fragmentation)가 불가피하다. 공

격자는 단편화되어 전송되는 프레임을 악의적으로 손실/오염시키거나, 복사 후 삽입하는 형태의 공격으로 종단 시스템의 자원을 고갈시킬 수 있다.

인터넷 계층부터 응용 계층까지는 기존 인터넷에서 악용되는 다양한 DoS 공격들이 재현될 수 있다. 본 논문의 공격 시험에 사용되는 SYN Flooding 기반 DoS 공격도 이에 포함된다. 공격자의 위치를 감추기 위해 스푸핑된 SYN Flooding 공격을 많이 사용한다.

스푸핑된 SYN Flooding DDoS 공격에 대응하기 위해 다양한 방법들이 제시되고 있다. 가장 직관적인 방법으로 네트워크에 입/출력(Ingress/Egress)되는 데이터를 필터링하는 방식이 있다. 필터링 방식은 사전에 할당된 IP 주소 대역 이외의 IP 주소로 설정된 패킷들을 차단한다[17]. 이 방식은 네트워크에 설치되어 있는 모든 입/출력 라우터들의 처리 부하 증가가 불가피하여 전체 전송 속도를 저하시키는 성능의 문제가 있다.

TCP 가로채기(Intercept) 방식은 목적지로 전송되는 TCP SYN 패킷을 라우터가 가로채기 하고 TCP SYN+ACK 패킷을 출발지로 전송하고 출발지로부터 ACK 패킷을 수신하면 정상 연결로 판단하여 양종단간 연결을 투명하게 포워딩하여 연결시켜주는 방식이다[18]. 이 기법도 관련된 모든 라우터마다 연결 세션관리가 필요하므로 라우터의 전송속도 저하에 대한 한계가 있다.

출발지 IP 주소를 스푸핑한 공격을 차단해 줄 수 있는 기술로 라우터가 패킷을 받으면 출발지 IP 주소를 확인하여 해당 IP로 갈 수 있는 역경로(reverse path)가 존재하는지 확인함으로써 출발지 IP 주소를 확인하는 방식도 제안되었다[19]. 이 방식은 단일 네트워크가 아닌 다수의 라우팅 경로가 존재하는 비대칭 네트워크 구조를 가지고 있을 경우 적용과 구현의 한계가 있다.

스푸핑된 SYN Flooding DDoS 공격에 대한 탐지 정확성을 높이고 정상 사용자에 대한 웹서비스 가용성을 높이기 위한 다단계 탐지기법도 제안되었다. 이 방식은 정상적인 SYN 패킷들도 차단될 수 있는 기존 방식의 한계를 제거하고자 세션대비 트래픽 부하량 비교를 탐지 기능의 시작점으로 두고 있다. 또한 네트워크 노드들과 인터넷 전체를 제어해야 하는 부담에서 벗어나 단일한 네트워크 기반 보안장비에서 쉽게 구현 가능한 동일한 순서번호 중복 검사와 TTL 필드값 비교에 의한 비정상 트래픽 선별 제거 기능을 제시하고 있다[4].

Ⅴ. 결 론

본 논문에서는 다양한 산업 영역에서 활용되고 있는 IoT 기술의 잠재적 보안 위협으로 인해 발생할 수 있는 취약점을 해킹 공격을 구현하여 확인했다. 사용자 주변에 설치되어 있는 IoT 기기를 공격하여 개인 정보를 유출할 수 있고 DoS 공격을 통해 서비스 가용성을 침해할 수 있음을 보였다. 또한 각 취약점을 해결할 수 있는 방안을 제시했다. 자원이 제한적인 IoT 기기의 특성으로 모든 보안 기술의 적용이 쉽지 않지만 표준화된 통신 암호 기술과 접속 비밀번호의 안전한 재설정을 통해 기본적인 보안은 제공받을 수 있을 것으로 판단한다.

감사의 글

본 논문은 덕성여자대학교 2018년도 교내연구비 지원에 의해 수행되었습니다.

참고문헌

[1] Shancang Li, Li Da XuEmail, Shanshan Zhao, “The internet of things: a survey,” *Information Systems Frontiers,* Springer, Vol. 17(2), pp. 243~259, April 2015.

[2] J. Park, H. Kwon , N. Kang, “IoT-Cloud Collaboration to Establish a Secure Connection for Lightweight Devices,” Springer *Wireless Networks,* pp. 1~12(on-line published), 2016.

[3] Hyo Jin Ban, Namhi Kang, “Survey on Secure Initial Bootstrapping Technologies for Lightweight Devices in Internet of Things” *Information and Communications Magazine*, Vol. 34(3), pp. 74-79, 2017.02

[4] B. Kenyon, Symantec, 2016, “Security in 2017 and Beyond: Symantec’s Predictions for the Year Ahead,” [Internet]. Available: https://www.symantec.com/connect/blogs/security-2017-and-beyond-symantecs-predictions-year-ahead.

[5] TRENDMICRO, 2016, “The Next Tier- Trend Micro Security Predictions for 2017,” [Internet]. Available: http://www.trendmicro.co.kr/cloud-content/kr/pdfs/the_next_tier_kr.pdf.

[6] Baik, Namkyun, Namhi Kang. "Multi-Phase Detection of Spoofed SYN Flooding Attacks." *Int. Jr. of Grid and Distributed Computing*, Vol. 11.3, pp. 23-31, 2018

[7] Kaspersky DDOS attacks in Q1 2017, May 11 (2017), [Internet]. Available: https://securelist.com/ddos-attacks- in-q1-2017/78285/

[8] Raspberry Pi Projects, “Streaming Video Using VLC Player,” [Internet]. Available: http://www.raspberry-projects.com/pi/pi-hardware/raspberry-pi-camera/ streaming-video-using-vlc-player

[9] Mihui Kim, “Privacy Protection Technologies on IoT Environments: Case Study of Networked Cameras,” *The Journal of the Korea Contents Association,* Vol. 16(9), pp. 329-338, 2016.09.

[10] Hyeokjin Kwon, Jiye Park, Namhi Kang. "Challenges in deploying CoAP over DTLS in resource constrained environments." *International Workshop on Information Security Applications,* Springer, Aug. 2015.

[11] Verma, Sajal. "Searching Shodan for fun and profit." Research paper. [Internet]. Available: http://www. exploit-db. com/docs/33859. pdf. 2014.

[12] Bodenheim, Roland, et al. "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices." *International Journal of Critical Infrastructure Protection* 7.2 (2014): 114-123.

[13] IETF RFC 6347, “Datagram Transport Layer Security (DTLS) Version 1.2,” 2012

[14] IETF RFC 7252, “The Constrained Application Protocol (CoAP),” 2014

[15] R. Hummen, J. Hiller, H. Henze, H.Shafagh, K. Wehrle, “6LoWPAN Fragmentation Attacks and Mitigation Mechanisms” in *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, ACM, p.55-66, (2013)

[16] O. Bergmann, S. Gerdes, S. Schafer, F. Junge, C. Bormann, “Secure Bootstrapping of Nodes in a CoAP Network”, *Proceedings of IEEE WCNC*, Apr. 2012.

[17] Tao Peng, Christopher Leckie and Kotagiri Ramamohanarao, “Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems,” *ACM Computing Surveys,* Apr 12 (2007), Vol.39

[18] Configuring TCP Intercept (Preventing Denial-of- Service Attacks), [Internet]. Available: https://www.cisco.com/c/en/us/td/docsios/12_2/security/configuration/guide/fsecur_c/scfdenl.html?dtid=osscdc000283/

[19] Unicast Reverse Path Forwarding (uRPF) Enhancements for the ISP-ISP Edge, 2005., [Internet]. Available: https://www.cisco.com/c/dam/en_us/about/security/intelligence/urpf.pdf/

[20] Seohyang Kim, Chongkwon Kim, "Analysis of Recent IETF Research Trends and Implementation of RPL- TSCH Testbed," *KIISE Transactions on Computing Practices,* Vol. 24, No. 6, pp. 295-300, 2018. 6

[21] Taehwan Park, Hwajeong Seo, Shinwook Heo, Howon Kim, "The Recent Research Trend and Prospective on Authenticated Encryption Schemes," *KIISE Transactions on Computing Practices,* Vol. 24, No. 10, pp. 563-568, 2018. 10

조이든(I-Deun Cho)

2019년 : 덕성여대 공과대학 IT미디어공학과(공학사)

2015년~2019년: 덕성여자대학교 IT미디어공학과
※관심분야 : 정보보호(Personal Information), 빅데이터, 인공지능

박수진(Soo-Jin Park)

2019년 : 덕성여자대학교 IT 미디어공학과 (공학사)

2015년~2019년: 덕성여자대학교 IT미디어공학과
※관심분야 : 정보보호(Personal Information), 인터넷 보안, 사물인터넷 보안

강남희(Namhi Kang)

1999년 : 숭실대학교 정보통신공학과 (공학사)
2001년 : 숭실대학교 정보통신대학원 (공학석사)
2005년 : University of Siegen 컴퓨터공학과(공학박사-인터넷및시스템보안)

2009년~2017년: 덕성여대 정보미디어대학 디지털미디어학과 부교수
2018년~현 재: 덕성여대 공과대학 IT미디어공학과 교수
2006년~현 재: 덕성여대 학교기업 DCS 대표
※관심분야 : 유무선 인터넷통신, 인터넷보안, 시스템 보안, 사물인터넷 보안