

사물인터넷(IoT) 환경에서 프라이버시 보호 기술: 네트워크 카메라 사례 연구

Privacy Protection Technologies on IoT Environments: Case Study of Networked Cameras

김미희

한경대학교 컴퓨터공학과

Mihui Kim(mhkim@hknu.ac.kr)

요약

물리적인 세계의 모든 사물들이 디지털화되고 통신이 이루어지는 사물인터넷(Internet of Things; IoT) 기술은 새로운 패러다임으로 부각되고 있고 편리하고 효율적인 생활을 제공할 것으로 기대되고 있다. 그러나 성공적인 기술의 실현을 위해서는 IoT 보안이라는 중요한 선결 이슈가 존재하며, 특히 인간과 직접 관계된 사물 통신이라는 점에서 프라이버시 보호는 더욱 중요시 될 것으로 예상된다. 본 논문에서는 IoT 환경에서의 보안과 프라이버시 위협에 대해 기술하고, 쇼단(인터넷에 연결된 라우터, 스위치, 공유기, 웹캠, IoT 기기 등을 찾아주는 합법적인 백door 검색엔진)을 통한 IoT 장비의 보안과 프라이버시 노출 가능성을 지적한다. 마지막으로 현재 많이 사용되고 있는 네트워크 카메라의 실제 사례들을 통해 프라이버시 보안 위협들을 비교하며 대응방안에 대해 기술한다.

■ 중심어 : | 사물인터넷 | 프라이버시 보호 | 사례연구 | 네트워크 카메라 | 쇼단 |

Abstract

Internet of Things (IoT) technology makes every things in physical world being digitalized and communicated with each other. The technology is emerging as a new paradigm and is expected to provide a convenient and effective life. However, for the successful realization of the IoT technologies, IoT security issues are an important prerequisite, and particularly the privacy protection is expected to become more important in view of object communication directly related with human. In this paper we describe for the security and privacy threats in IoT environment and introduce the shodan (a legitimate search engine that finds backdoor routers, switches, webcams, IoT devices connected to the Internet etc.) that can expose the security and privacy problems. Lastly, we compare the privacy threats through real-world case study of network cameras currently in use and finally derive the countermeasures for the threats.

■ keyword : | Internet-of-Thing (IoT) | Privacy Preservation | Case Study | Networked Camera(Webcam) | Shodan |

* 이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임
(No. 2015R1D1A1A01057362)

접수일자 : 2016년 05월 24일

수정일자 : 2016년 06월 02일

심사완료일 : 2016년 06월 02일

교신저자 : 김미희, e-mail : mhkim@hknu.ac.kr

I. 서론

세상의 사물을 연결하는 초인터넷 세상을 가능하게 하는 IoT(Internet of Things) 기술은 빠른 속도로 발전하고 있다. 시장조사기관인 가트너(Gartner)에 의하면 전 세계 인터넷 접속 기기가 2020년에는 250억대를 넘어설 것이라고 전망하고 있다[1]. 2016년 1월 미국 라스베이거스에서 세계 최대 규모의 국제전자제품박람회(CES 2016)가 개최됐다. 이 행사에서는 작년에 이어 IoT가 단연 화제가 되었고, 4대 주요 이슈로 손꼽혔다. 작년과 달라진 점은 IoT 장치 개발에서 IoT 서비스 디자인으로 그 방향이 바뀌었다는 것이다[2][3]. P&G사의 방향제(air freshener)는 온도, 습도를 감지하는 Nest사의 온도계와 연결되어 에어컨이 작동하는 시간에 함께 작동하도록 하여 그 향기가 더 멀리 퍼지게 한다. 월풀사의 세탁기는 아마존의 대시(Dash) 버튼을 통해 세제를 주문할 수 있도록 한다. 이러한 IoT 제품은 편리하고 효율적인 서비스로서 우리의 삶에 한발 더 다가오고 있다.

IoT의 기술은 자동차, 의료기기, 공공기반, 가정 등 많은 분야에서 발전하고 있다. 그러나 이런 광범위한 영역에서 수집된 수많은 다양한 데이터들은 개인정보 유출로 인한 프라이버시 침해로 남고 있고 그 연구의 중요성은 증대되고 있다[4][5]. 실제로 HP는 IoT기기의 70%가 패스워드 보안, 승인, 암호화 측면에서 취약점을 갖고 있다고 발표했다[6]. 그리고 Cisco의 보안 전문가는 IoT 적용 분야가 너무 방대해 시나리오별로 보안 분석을 수행하기 어려운 상황이라고 진단했다[7].

실제 보안 위협 사례로는 2013년 8월, 미국 라스베이거스에서 스마트 TV에 탑재된 카메라를 해킹해 사생활 영상을 유출하는 시연이 열려, 인터넷에 연결된 가정기기의 보안 취약성이 보고되기도 하였다[8]. 2014년 9월, 서울 'ISEC 2014'에서 블랙필 시큐리티는 로봇청소기 원격조종을 위해 필요한 앱의 인증방식 취약점과 로봇청소기에 연결된 무선공유기의 보안 설정상의 취약점 등을 이용해 해킹하여, 로봇청소기에 탑재된 카메라로 실시간 모니터링이 가능하다는 것을 시연하였다. 또한 2016년의 새로운 해킹 트렌드로서 IoT 좀비 봇넷을 꼽고 있다[9]. IoT장비로서 사용되는 감시카메라, 스

마트TV, 홈자동화시스템 등이 DDoS 공격을 위한 해커들의 봇넷 군대로 사용될 것으로 예상되며 이에 대한 감지가 더 어려울 것으로 예상하고 있다. 이러한 사례들로도 나타나듯이 IoT 보안 위협의 문제는 해결이 시급한 상황이며 성공적인 IoT 환경 구축을 위해서는 필수적인 선결조건이다[10].

본 논문에서는 2장에서 IoT 기기의 보안 및 프라이버시 취약점과 위협 공격을 살펴보고, 3장에서 IoT 기기를 검색해 볼 수 있는 쇼단 사이트를 통해 IoT 장비의 보안과 프라이버시 노출 가능성을 소개한다. 4장에서 3가지 사례를 통해 IoT 제품, 특히 사생활 위협이 가장 큰 네트워크 카메라의 보안위협과 프라이버시 침해요인에 대해 분석보고, 5장에서 보안 대책을 도출하고 본 논문의 결론을 맺는다.

II. IoT 기기의 보안 및 프라이버시

2.1 IoT 기기의 취약점

기존의 IoT는 주로 사물이 수집한 자료를 사용자에게 전달하거나 사용자가 사물을 컨트롤 하는 수준이었다면 미래에는 사물과 사물 사이에서 데이터의 교환이 발생하고 그 데이터가 데이터마이닝 되어 사용자에게 가치 있는 정보로 제공될 것이다. 이것이 진정한 의미의 사물인터넷이다.

이와 같은 IoT 서비스가 가능하기 위해서는 사물이 데이터를 스스로 확보하고 처리하는 기능을 탑재해야 한다. 그러나 아직까지는 IoT 디바이스는 연산 및 처리 능력이 단순하고 성능이 떨어져 보안 정책도 허술하다. 그래서 이 디바이스들은 사이버 공격의 주요 대상이 될 수 있고 보안에 취약하다. 특히 현재 많은 IoT 기기들은 [표 1]과 같이 보안상의 취약점이 분석되고 있다[11].

IoT 기기 중에 많은 제품들이 카메라를 장착하고 있다. 주요 목적은 방법(Home security, surveillance), 유아 모니터링, 유아 완구, 반려동물 관리 등의 목적으로 사용된다. 또한 통신기능이 있어 특정 영역에 대한 이미지 변화 시 스마트폰으로 알려주거나 또는 이미지 분석을 위해 클라우드에 그 이미지가 전달된다. 암호화 통신이 제공되는 장비도 있지만, 장비의 낮은 성능으로

약한 키 관리 체계로 이루어진 경우가 많다[12].

표 1. IoT 기기들의 보안상 취약점

취약점	설명
평문 로컬 API 사용	로컬 통신이 암호화 되지 않음
평문 클라우드 API 사용	원격 통신이 암호화 되지 않음
평문 저장	저장장치에 평문으로 저장됨
원격으로 시스템 접속	시스템에 접속하여 CLI(Common Line Interface)로 제어 가능
쉬운 백도어 계정	계정이 쉽게 추측 가능(예, admin)
직렬연결접속	내부 공격자가 물리적으로 직렬연결(UART)에 접속하여 인증없이 장치에 접근하거나 다른 장치로 교체 가능

카메라를 사용하는 IoT 기기 중에서도 감시용 네트워크 카메라가 가장 많이 사용되고 있다. 2014년 조사 보고에 의하면 2억 4500만 여대의 감시카메라가 공공 장소에 설치되어 있고, 개인적인 네트워크 카메라를 고려하면 훨씬 많은 수의 네트워크 카메라가 사용되고 있음을 알 수 있다[13]. 문제는 앞서 기술한대로 관련 기기의 보안상 취약점과 운영자의 보안인식 부족으로 인하여 해킹 위협에 노출되어 있다는 점이다.

카메라가 장착된 또 하나의 IoT 기기로 아이들의 스마트 장난감(인형)을 꼽을 수 있다. 켈컴의 스마트테디베어, IDX랩의 수호자곰(Teddy the Guardian), 유명완구회사 마텔의 헬로바비, 구글의 빅브라더 등이 대표적 제품이다[14]. 이들 제품은 마이크, 스피커, 카메라, 다양한 센서, WiFi 등의 통신모듈 등이 장착되어 있어 아이와 대화를 하여 클라우드에 기록 및 분석하고 이에 대한 반응으로 감정표현을 한다든지 아이의 체온 및 심장박동 등이 측정 및 저장되고, 집안의 가전제품을 제어하는 기능 등이 있다. 이 제품들은 아이의 생체 정보 및 언어, 행동 패턴 등 개인정보 등이 클라우드에 저장되어 분석되어 프라이버시 문제가 있고, 악용될 경우 홈페이지 권한이 해커에게 넘겨질 수는 심각한 보안문제가 있다.

유아 모니터링 기기의 사례 연구를 통하면 다음과 같은 취약점이 존재함을 알 수 있다[11][15]. 권한 상승(Privilege Escalation)으로 인한 허가되지 않은 오퍼레이션 수행, 백도어 자격 습득으로 인증 없이 비정상적인 접근, 저장된 XSS 공격(Reflective Stored Cross

Site Script; 일반사용자가 시스템에 접속하여 사용하는 비밀정보들을 공격자에게 보낼 수 있도록 공격 스크립트 저장)[16], 예상할 수 있는 정보 누출(예, 기본 아이디, 패스워드)로 인증 우회, 직접 영상/오디오 정보 브라우징, 평문 전송이 수행되는 클라우드 API사용으로 정보 노출 가능성 높다는 것이다.

프라이버시 취약점은 카메라를 장착한 IoT기기에서만 국한된 것은 아니다. 홈 제어기기인 써모스탯(Thermostat)은 2014년 구글의 32억불의 인수로 큰 관심을 받은 네스트(Nest)사의 학습용 온도조절기로 북미에서 큰 인기를 받고 있는 대표적 IoT 기기이다. 단순히 온도를 측정하여 냉난방기를 조절하는 기기를 넘어서, 사용자의 시간별/일별 선호 온도에 대한 학습기능을 갖추고 있고 부재중일 경우 모션센서를 사용하여 감지하여 실내 난방중지가 가능하다. 특히 2016년 제품에는 P&G 사의 방향제(air freshener)와 연결되어 에어컨이 작동하는 시간에 함께 작동 하도록 하여 그 향기가 더 멀리 퍼지게 하는 등 그 기능을 더해가고 있다. 그러나 이 제품은 개인별 선호도 및 맥내 사용자 부재여부가 센싱되어 인터넷에 노출될 경우 프라이버시 침해 문제가 생길 수 있다[12].

2.2 IoT 기기의 보안 및 프라이버시 위협

앞 절에서 살펴보았듯이 현존하는 많은 IoT 기기들은 보안 및 프라이버시 측면 상 취약점이 존재하다. 이로 인해 IoT 보안 위협 사례가 갈수록 증가하고 있다.

이러한 문제점을 그대로 노출한 DDoS 공격 사례가 2014년 3월 발생하였다[13]. 이는 전 세계 240대 CCTV가 해킹당해 DDoS 봇넷의 공격에이전트가 되어 클라우드 서버에 초당 2만개 메시지를 생성하는 HTTP Get 플러딩 공격을 수행하였다. 이번 공격에 해킹당한 CCTV는 ELF 뮐웨어가 수행되어 공격된 것으로 밝혀졌고, 이 뮐웨어는 BusyBox라는 유틸리티 패키지를 사용하는 리눅스 OS의 CCTV를 찾고 brute force 사전공격에 취약한 telnet/ssh서버가 수행되는 장비를 찾아 해킹하여 공격에이전트로 만들었다. [그림 1]은 공격에 가담된 해킹된 CCTV의 분포도이다[16].

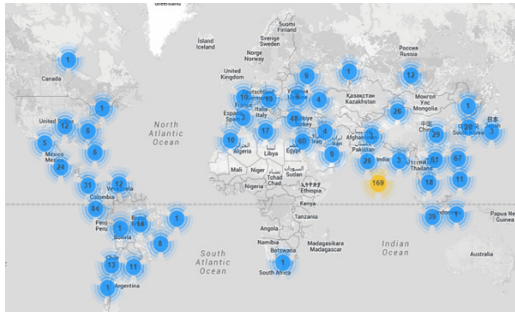


그림 1. DDoS공격의 에이전트로 사용된 CCTV 분포도

이 공격 사례에서도 알 수 있듯이 대표적 IoT 네트워크 장비인 CCTV의 대부분은 리눅스를 사용하고 있고, 외부에서 제어를 위해 telnet/ssh를 사용하고 있으며, 장비의 기본 패스워드(예> admin, password)나 추측하기 쉬운 패스워드(예> 1234, default)를 많이 사용하고 있어서 루트권한이 노출되기 쉽다는 것을 알 수 있다. 또한 CCTV의 루트권한이 해커에게 넘겨진 경우 해당 지역 실시간 영상자료가 노출되므로 프라이버시 문제가 생겨 그 위험의 정도가 더 높아지게 된다.

이러한 실제 공격 사례들로 인해 많은 전문가들은 IoT 기기 및 서비스 자체에 대한 신뢰성 저하로 관련 시장의 성장에 큰 위협이 될 것으로 우려하고 있다. 그러므로 신뢰할 수 없는 사물인터넷 제품과 서비스는 시장에서 절대 활성화되기 어렵기 때문에 보안과 프라이버시 중요성은 더욱 강조되고 있다.

III. 쇼단(Shodan)

쇼단(<https://www.shodan.io>)은 합법적인 백도어 검색엔진으로서 인터넷에 연결된 라우터, 스위치, 공유기, 웹캠, 복합기 등을 찾아준다[9]. 쇼단에서 간단한 검색으로 다른 곳의 CCTV를 찾아 볼 수 있으며 일부 시스템에 접근하여 시스템을 통제할 수 있다. 실제로 이것들이 악용될 경우, 인증 절차가 없는 디바이스에 접근하여 개인정보 및 사생활을 침해할 수 있다. 뿐만 아니라 공공기반의 시스템을 장악하여 혼란을 야기할 수 있다[17].

특히, 쇼단은 특정 필터(예, city, country, geo, hostname, net 등)를 사용하여 사용자가 원하는 정보를 쉽게 얻을 수 있게 되어 있다. 'refrigerator', 'webcam' 등의 필터를 통해 인터넷에 연결된 냉장고나 웹캠 등 IoT 장비를 쉽게 검색할 수 있고, 'default password' 필터를 통해 장비의 기본 패스워드를 쉽게 찾을 수도 있다. [표 2]는 쇼단에서 사용할 수 있는 필터를 정리하였다.

표 2. 쇼단의 필터와 예

키워드	설명	예
country	특정 나라의 장비 검색	country:KR //한국의 장비 검색
city	특정 도시의 장비 검색	city:seoul //서울의 장비 검색
net	특정 네트워크 장비 검색	net:211.241.0.0/16 //211.241.* 네트워크 장비 검색
server	특정 서버가 운영되는 장비 검색	server:SQ-WEBCAM //SQ-WEBCAM 서버가 운영되는 장비 검색
hostname	특정 호스트이름을 갖고 있는 장비 검색	hostname:samsung //호스트이름에 samsung이 들어간 장비 검색
IP	특정 IP 장비 검색	IP:203.254.192.9 //203.243.192.9 장비 검색
os	특정 OS로 운영되는 장비 검색	os:linux //linux OS로 운영되는 장비 검색

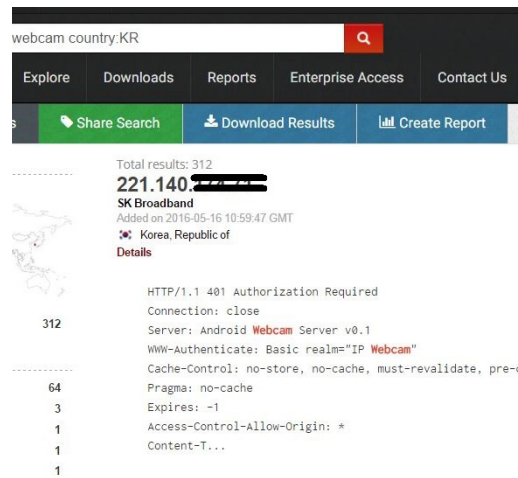


그림 2. 쇼단에서 한국 웹캠(webcam)을 검색한 화면

[그림 2]는 쇼단에서 한국에 있는 웹캠을 검색한 결과화면이다. 왼쪽에는 검색결과가 위치한 지도와 함께 통계정보가 보여 지고, 오른쪽에는 검색한 결과내용이

나열되어 있다. 해당 시스템의 IP, 소속 ISP, 서버 종류와 버전, 설정정보가 보여진다. [그림 3]은 [그림 2]에서 검색한 결과의 통계정보를 보여주고 있다. 해당 장치들이 위치한 지도와 함께 장소 분포, 운영 서버가 사용하는 포트(서비스) 분포, 연결된 ISP업체 분포, 해당 장비의 OS, 장치 종류 등의 정보를 제공한다. 검색된 장비의 IP를 클릭하면 인증 설정이 되어 있으면 사용자이름과 패스워드가 요청되고, 설정이 되어 있지 않으면 바로 실시간 웹캠 정보가 보여진다. 본 저자가 검색하여 인증 설정이 안 된 웹캠을 어렵지 않게 찾을 수 있고, 실시간 영상을 볼 수 있어 사용자들이 보안 특히 프라이버시 보호에 대한 인식이 얼마나 낮은지 알 수 있었다.

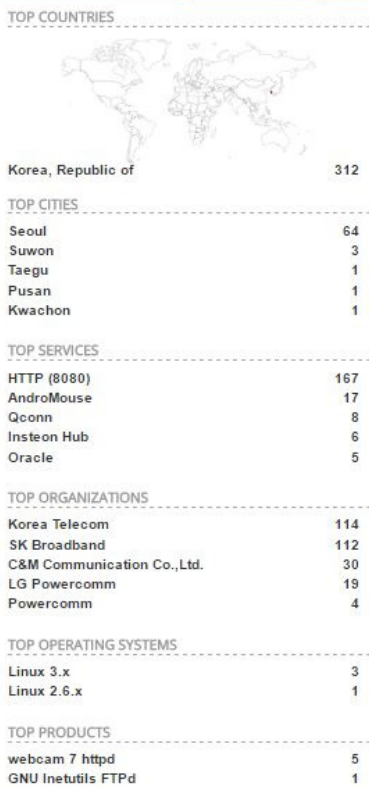


그림 3. 그림2의 검색 결과의 통계정보

이번에는 쇼단에서 'default password' 필터로 검색해 보았다. 그 결과, 시스템에서 기본 패스워드로 무엇을 사용하는지 구성화일이 출력되며 알아 볼 수 있었다.

예를 들어, 시스코 장비의 경우 기본 사용자 이름과 패스워드는 'cisco/cisco'임을 알 수 있고, 본 저자가 검색을 통해 해당 기본 인증 정보로 텔넷 접속이 가능한 스위치를 어렵지 않게 찾을 수 있었다. [그림 4]는 이렇게 검색된 장비 중 특정 장비의 IP를 클릭하여 상세 정보를 출력한 화면으로 해당 장비가 위치한 자세한 지도 정보와 함께, IP, 위치, 조직, ISP, 최종 업데이트 시간, 장비이름, ASN, 그리고 운영 중인 포트 즉 서비스 종류와 각 서비스에 대한 설정정보를 함께 보여준다. 해당 서비스가 노출된다는 것은 그 서비스를 통해 얼마든지 원격 접속하여 제어가 가능하다는 취약점을 보여주고 있다.

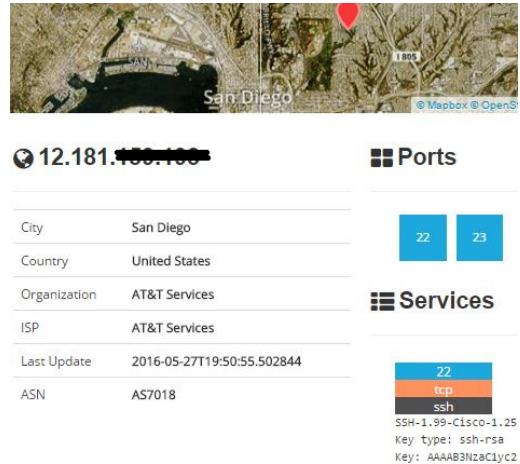






그림 4. 쇼단에서 'default password' 필터로 검색하여 특정 장비 상세 정보 출력

이와 같이 너무나 쉽게 IoT 장비뿐만 아니라 인터넷에 연결된 디바이스의 보안 취약점을 공격하는 다양한 수단이 존재한다. 그리고 이러한 문제점들을 해결하기 위한 확실한 방법들이 반드시 필요하다.

IV. 네트워크 카메라의 보안 위협 사례 분석

본 장에서는 대표적인 IoT 기기 중 하나인 네트워크 카메라(CCTV)에 대해 대표적 제작법 3 가지(웹캠, 스마트폰, 오픈하드웨어)[18]를 사용하여 제작, 설치하고 쇼단을 통한 보안 및 프라이버시 취약성을 비교분석한다.

표 3. 웹캠을 이용하여 네트워크 카메라를 만드는 프로그램 비교

웹캠프로그램				
웹캠프로그램지원 OS	Windows, IOS	Windows	Android, IOS	Windows
지원 장치	PC+웹캠, 노트북+카메라, 안드로이드, 아이폰	PC+웹캠, 노트북+카메라	안드로이드폰, 아이폰, 아이패드, 아이팟	PC+웹캠, 노트북+카메라
뷰 프로그램	- 안드로이드/아이폰 용 뷰프로그램 지원	- 안드로이드/아이폰 용 뷰프로그램 지원	- Firefox on PC - 웹캠 프로그램으로 뷰 기능 지원	- 일반 웹브라우저
특징	- 실시간 영상 원격 감시 - IP설정 불필요 - 움직임 감지 시 경고음/문자 전송 - 사진, 동영상 PC 저장	- 웹캠 쪽 시스템으로 음성 전송 - 라이브/녹화 영상 보기	- 여러 뷰어와 카메라 지원 - 움직임 감지 기능 - 양방향 토크 - 원격 웹캠 제어	- 여러 소스 화면 동시지원 - 움직임/소리 감지 및 자동 녹화 - 원격 웹캠 제어
가격	- 개인용 무료 - 부가서비스(경고음 전송, 움직임 감지 시 문자, 영상 전송 등) 유료	- 1분영상보기 무료 - 지속 영상보기 유료	- 무료 - 인앱 구매 가능	- 2개 소스 화면 지원 무료 - 부가 서비스(더 많은 소스 화면 지원 소리 감지 IP/Pwd 인증) 유료
개발지	국내	국내	국외	국외

4.1 웹캠을 이용한 네트워크 CCTV

국내외 포털사이트에서 블로그 및 전문 사이트를 이용하여 자신만의 CCTV를 쉽게 제작할 수 있다. 실제 무료 웹캠 프로그램들을 검색한 결과 HOMECCCTV[19], JenausCam[20], Alfred[21], webcamXP[22] 등 많은 프로그램들이 검색되어 사용되고 있다. 이 프로그램들은 국내외에서 제작되었으며 웹캠을 통해 외부에서 PC와 모바일로 촬영 화면을 볼 수 있는 프로그램들이다. [표 3]은 이들 프로그램을 비교하여 정리한 표이다.

이 프로그램들을 쇼단을 통해 검색해 본 결과 webcamxp5, webcam7 서버가 검색 가능했다. 검색된 내용의 IP주소로 접속을 하면 관리자 계정이 설정되지 않은 서버에 한해 촬영장면이 노출된다. 쇼단에서 무료 계정을 통해 'country:KR webcamxp'라는 검색어 결과로 2016년 3월 6일 기준으로 26개의 결과가 나왔다(유료 계정의 경우 더 많은 결과가 검색될 수 있다). 이 중 일부가 인증 절차 없이 접속하여 촬영장면을 확인할 수 있었다.

웹캠을 통해 CCTV로 이용하고자 하는 대부분의 사람들이 IP나 서버를 만드는 등의 기본적인 지식이 없어도 포털사이트의 검색된 블로그나 카페에 기재된 글을 통해 쉽게 제작하여 사용할 수 있다[23]. 간단한 과정은 다음과 같다. 1) PC에 웹캠을 연결하거나 카메라가 장착된 노트북을 준비한다. 2) 웹캠 프로그램을 다운받는다(<http://www.webcamxp.com/download.aspx>). 3) 프

로그램을 설치한다. 4) 설정화면의 Web/Broadcast 메뉴에서 서버를 구동한다(activate). 5) 웹캠이 구동되는 서버가 사설아이피를 사용하는 경우 공유기의 포트포워딩 기능을 설정한다. 6) 외부 웹브라우저나 폰에서 PC 아이피와/포트정보를 이용하여 접속하여 실시간 영상을 출력해 본다.

이러한 과정을 통해 실제로 CCTV를 제작하였다. 이 프로그램의 경우 설치 후, 서버로 사용할 IP주소를 설정한 후 (무료 프로그램인 경우) 계정 생성 없이 바로 실행이 가능하다. 실행된 서버를 쇼단을 통해 검색하여 그 결과를 확인하였다. [그림 5]는 직접 제작한 CCTV가 쇼단에서 노출된 화면을 캡처한 것이다. 개인 공간의 감시 목적으로 활용될 수 있는 CCTV가 쇼단의 간단한 검색으로 노출되고 있음을 확인할 수 있었다.



그림 5. 쇼단에서 'country:KR webcamxp'로 검색하여, 실험 서버에 접속한 결과

4.2 스마트 폰을 이용한 CCTV

무선랜이 가능한 스마트 폰 한 대로 쉽게 CCTV를 제작할 수 있다. 2015년 9월 10일 기준으로 안드로이드 폰을 사용해 Google Play에서 'IP camera'으로 검색하면 250여개의 검색 결과가 나온다. 가장 상단에 위치한 'IP Webcam'을 다운받아 설치했다[24]. 'IP Webcam'은 스마트 폰을 다양한 옵션을 가진 CCTV로 만들어 주고, 다른 스마트 폰이나 웹 브라우저를 통해 카메라를 볼 수 있도록 해준다. 이 외에도 Dropbox, ftp, email로 영상 업로드가 가능하고, 영상 채팅, 야간보기, 움직임/소리 감지 및 알림/녹화 기능 등이 지원된다. 기본적인 라이브러전은 무료이며 인앱 구매가 가능하다. 스마트 폰을 이용한 CCTV를 제작하는 이 방법은 비용이나 시간이 적게 들어 많은 사람들이 이용하고 있다. 또한, 'IP Webcam'은 쇼단을 통해 검색이 가능하며, 일부 서버에 인증 없이 접속하여 촬영영상을 볼 수 있다.

스마트 폰을 이용하여 제작해 본 결과, 계정을 생성하지 않고 바로 실행이 가능하다. 그리고 가정에서 사용하는 사설IP 주소를 통해 외부에서 서버로 접속하여 촬영화면을 확인할 수 있다. [그림 6]은 실제 촬영한 장면을 외부에서 서버로 접속하여 촬영 화면을 캡처한 것이다.

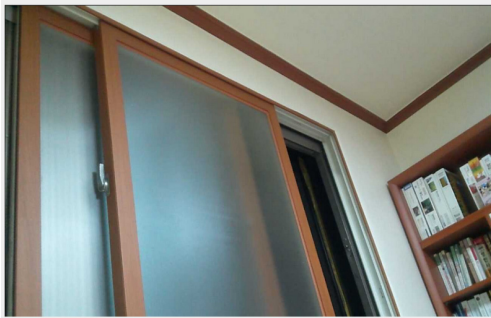


그림 6. 외부에서 'IP Webcam'서버로 접속하여 촬영한 화면

4.3 오픈하드웨어(라즈베리파이)를 이용한 CCTV

대표적 오픈소스하드웨어인 라즈베리파이를 이용하여 간단한 CCTV를 제작할 수 있다. 라즈베리파이의 경우 라즈베리파이의 전용 카메라 모듈을 이용하여

VLC 프로그램을 설치하고[25], 라즈베리파이의 IP 주소를 이용해 외부에서 VLC 플레이어를 통해 촬영장면을 확인할 수 있다. VLC 플레이어는 IPv4 및 IPv6 네트워크에서 스트리밍 서비스를 제공하는 프로그램으로 라즈베리 파이 카메라 모듈로 촬영한 화면을 인터넷을 통해 실시간으로 제공한다.

쇼단을 통해 'VLC'로 검색하면 VLC 서버들을 확인할 수 있다. VLC 프로그램으로 서버 주소에 접속하면 일부 서버는 아무런 인증 과정 없이 촬영 장면을 확인할 수 있다. [그림 7]은 라즈베리 파이 이용하여 직접 제작한 CCTV이고 [그림 8]은 이를 촬영한 내용을 스마트 폰 VLC 미디어 플레이어를 통해 확인한 것이다. 이 외에도 데스크탑PC나 노트북에 VLC 플레이어를 설치하여 외부에서도 확인 가능하다.

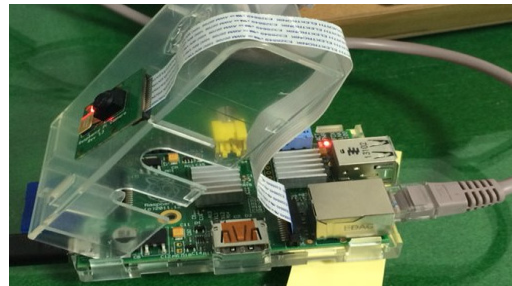


그림 7. 라즈베리파이에 전용카메라 모듈을 연결하여 만든 CCTV

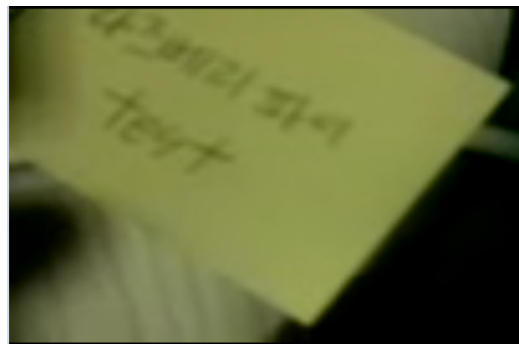


그림 8. 라즈베리파이를 통해 촬영한 화면

[표 4]는 이상 3가지 종류별 네트워크 카메라를 제작하여 실험한 결과를 정리한 표이다.

표 4. 네트워크 카메라 비교

이용 장비	웹캠	스마트폰	오픈하드웨어 (라즈베리파이)
구축 난이도	중	하	상
구축 비용	하	상	중
장점	- 여러 소스 지원 - 양방향 통신 - 움직임 감지	- 미사용 스마트폰이 있는 경우 추가비용 없이 쉽게 구축 가능	- 여러 센서를 부착하여 원하는 기능 추가 가능 - 보안관련 기능 추가 구현가능
단점	- 부가 기능 유료 - 프라이버시 노출 위험도 상	- 프라이버시 노출 위험도 상	- 구축 난이도 상
프라이버시 노출 위험도	상	상	하

V. 보안 대책

쇼단에 노출되는 수많은 IoT 장비들의 많은 부분 기본적인 인증과정이 없거나 기본 인증정보를 사용하여 문제가 되고 있다. 앞장의 실험을 통해 IoT 장비들이 가져야 하는 기본적인 보안장치의 필요성과 프라이버시 측면의 문제점을 살펴보았다. 웹캠, 스마트폰, 라즈베리파이를 이용하여 만든 이 세 가지 방식의 CCTV를 만드는 과정 자체는 일반 사용자들이 가장 많이 사용하거나 검색의 상단에 위치하는 애플리케이션이나 가장 쉬운 방법을 통해 제작하였다. 위 세 가지 방식의 CCTV는 쉽게 제작하여 사용할 수 있다는 장점은 있으나 개인 프라이버시를 침해하는 보안위협에 노출되어 있음을 알 수 있었다. 또한 다음과 같은 보안 대책이 시급하다.

첫째, 단순한 IoT 기기에도 철저한 인증과정이 필요하다. 그러나 실험 결과, 세 방식 모두 계정을 생성하지 않아도 사용이 가능했다. 쇼단에서 webcam을 이용하여 만든 CCTV를 검색했을 때 일부 서버는 접속하여 촬영장면을 볼 수 있었다. 이들 대부분은 프로그램을 설치 후 계정을 만들지 않고도 사용이 가능하기 때문에 사용자들이 이를 중요하게 여기지 않아 자신의 CCTV가 노출이 되고 있었다. 이처럼 계정을 생성해 인증하는 것은 프로그램을 사용하는 사용자와 개발자, 서비스 제공자 모두에게 필수적이고 기본적인 보안과정이라는 인식이 필요하다.

또한 계정을 생성하는 대부분의 프로그램에는 기본 인증 정보(password) 존재한다. 쇼단 혹은 웹에서 'Default Password'로 검색하면 많은 검색결과를 확인할 수 있다. 따라서 장치의 기본 아이디와 패스워드는 사용 시 곧바로 수정할 수 있게 하여 철저한 계정 인증 과정이 필요하다. 그리고 철저한 인증을 위해서 주기적으로 사용자들은 사용 암호를 변경할 필요가 있다. 또한 IoT 장비의 긴급한 업데이트를 수시로 확인하고 최신 버전을 유지하기 위한 노력이 필요하다.

두 번째, IoT 기기 사용의 로깅(logging)이 중요하다. 그러나 세 방식 중 유일하게 'webcamxp' 프로그램만 서버에 접속한 IP를 확인할 수 있다. 다른 누군가가 자신의 서버에 접속해 있는지를 확인할 수 있는 기능이다. 개인용 CCTV는 자신이 사용하는 것 외에 다른 사람들이 확인할 수 없어야 하는 점에서 누군가 접속하고 있다는 것을 아는 것만으로도 보안상 문제를 빠르게 해결할 수 있다. 그러나 'webcamxp'에서의 해당 기능의 아쉬운 점은 악의적인 접근을 통한 허락되지 않은 사용자가 접속을 했을 때 차단 및 경고 알림을 보낸다거나 접속한 대상의 로그기록을 남겨 확인할 수 있는 기능이 없다는 것으로 이 기능은 추가될 필요가 있다.

세 번째, IoT 서비스/제품 제공자나 관리자들은 해당 제품이나 서비스가 쇼단과 같은 검색 사이트에서 검색이 되는지 모니터링 할 필요가 있다. 무료 웹캠 프로그램들 중에서 'webcam7', 'webcamXP'를 제외한 대부분의 프로그램들은 쇼단의 기본 무료계정에서는 검색이 불가능 하였다. 검색을 할 수 없는 이유는 정확히 알 수 없으나 다른 프로그램들처럼 장치와 로컬 네트워크간의 분리를 통해 원격공격을 사전에 예방하는 것이 중요하다. 따라서 제품의 개발자 및 관리자들은 해당 위협 가능성을 인지하여 쇼단을 포함한 웹 검색 후 해당 IoT 서비스/제품이 인증과정 없이 검색되어 사용가능한 경우, 사용자들에게 그 결과를 알려주는 서비스를 제공할 필요가 있다.

네 번째, IoT기기 성능에 맞는 보안 기능이 제공되어야 한다. 소형 IoT 장비의 경우 전력소모량, CPU 성능 등 제약이 따르기 때문에 기존 암호 기술을 적용하는 것은 현실적으로 불가능하다. 그래서 이 점을 고려한

경량 암호 프로세스가 필요하다. 또는 암호화 및 인증 서비스를 클라우드 시스템을 이용하여 제공하는 방법을 모색해야 한다.

VI. 결론

본 논문에서는 IoT기기의 보안 및 프라이버시 취약점과 위협을 알아보고, 쇼단을 소개하였다. 또한 네트워크 카메라를 종류별로 제작 실험하여 해당 기기의 보안 위협을 알아보고 보안 대책을 도출하였다. 이를 바탕으로 네트워크 카메라 개발 및 운영에 적용한다면 더욱 안전하고 신뢰할 수 있는 제품 및 서비스를 이용할 수 있을 것이다. 본 논문에서는 네트워크 카메라에 대한 사례연구를 하였지만, 앞으로 이 외의 많은 각종 IoT 장비의 공격 유형과 그에 대응하는 보안 및 프라이버시 대책의 연구가 필요할 것이다. 이러한 연구를 바탕으로 향후, 디바이스, 서비스, 네트워크, 플랫폼을 아우를 수 있는 프라이버시 보호 프레임워크를 설계하고자 한다.

참고 문헌

- [1] 양철승, 사물인터넷이 쏟아올린 제 4의 물결, 2015, http://m.hankooki.com/m_view.php?m=&WM=po&WEB_GSNO=10182663
- [2] 이정현, 'CES 2016'서 주목해야 할 4대 이슈, ZDNet Korea 2016, http://www.zdnet.co.kr/news/news_view.asp?artice_id=20160105150649
- [3] Stacey Higginbotham, "The 6 Things CES Taught Us About The Internet of Things," <http://fortune.com/2016/01/11/ces-internet-of-things/>
- [4] 신숙조, 김선주, 조인준, "스마트폰에서 가상 디스크 플랫폼을 사용한 프라이버시 데이터 보호 방안", 한국콘텐츠학회논문지, 제13권, 제12호, pp.560-567, 2013.
- [5] 김미희, "위치공유기반 서비스의 프라이버시 보호 방안의 설계 방향 제시," 한국콘텐츠학회논문지, 제15권, 제2호, pp.101-108, 2015.
- [6] 이유미, 시큐아이, 사물인터넷 보안 플랫폼 개발, 이테일리, 2014, http://www.pstock.co.kr/2005pstock/common/ncomnews/ncomnews_view.asp?nco_num=940&num=524613&page=1
- [7] 조근희, "ICT Spot Issue," 정보통신기술 진흥센터, 2015년 7호, http://webzine.iitp.kr/down/vol02/issue/ICT_Spot_Issue_2015_7.pdf
- [8] 최중선, IoT 보안 이슈와 시사점, 2015, <http://lugenzhe.blog.me/220457659484>
- [9] Kim Zetter, The Biggest Security Threats We'll Face in 2016, Security, 2016, <https://www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016/>
- [10] 김호원, "사물인터넷상에서의 보안 및 프라이버시 보호 이슈," 지역정보화 동향분석, 제7호, 2015.
- [11] Mark Stanislav and Tod Beardsley, *HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities*, Rapid7's report, September 2015.
- [12] 이호원, "사물인터넷보안 및 프라이버시 이슈," KRNET, 2014.
- [13] Ofer Gayer and Or Wilder, "CCTV Botnet In Our Own Back Yard, CCTV Botnet In Our Own Back Yard," <https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html>
- [14] 이재구, 구글, 말 동무 슈퍼장난감 특허...빅브라더 논란, 전자신문, 2015, <http://www.etnews.com/20150525000015>
- [15] "Hacking IoT: Hackers can Hijack baby monitors easily," <http://www.hackcave.net/2015/09/hacking-iot-hackers-can-hijack-baby.html>
- [16] Cross Site Scripting (XSS) Attacks, <https://www.incapsula.com/web-application-security/cross-site-scripting-xss-attacks.html>
- [17] 김영훈, 양준근, 김학범, "M2M/IoT 동향과 보안 위협," 정보보호학회지, 제24권, 제6호, 2014.

- [18] 이현경, 김미희, “사물인터넷(IoT) 환경에서 프라이버시 보호 기술에 관한 연구,” 한국정보처리학회 추계학술대회, 2015(10).
- [19] <http://www.homecctv.kr/>
- [20] <http://www.jenauscam.com/>
- [21] <https://www.my-alfred.com/>
- [22] <http://www.webcamxp.com/home.aspx>
- [23] <http://hoon258.tistory.com/entry/웹캠을-이용한-가정용-CCTV-구축하기-웹캠-cctv-프로그램-webcamXP>
- [24] IP Webcam, <https://play.google.com/store/apps/details?id=com.pas.webcam>
- [25] Streaming Video Using VLC Player, <http://www.raspberry-projects.com/pi/pi-hardware/raspberry-pi-camera/streaming-video-using-vlc-player>

저 자 소 개

김 미 희(Mihui Kim)

정회원



- 1997년 2월 : 이화여대 전자계산학과(공학사)
- 1999년 2월 : 이화여대 컴퓨터학과(공학석사)
- 1999년 ~ 2003년 : 한국전자통신연구원 연구원
- 2007년 2월 : 이화여대 컴퓨터학과(공학박사)
- 2007년 ~ 2009년 : 이화여대 컴퓨터학과 전임강사
- 2009년 ~ 2010년 : 노스캐롤라이나주립대학교 연구원
- 2011년 3월 ~ 현재 : 한경대학교 컴퓨터공학과 교수
<관심분야> : 네트워크 성능 분석 및 보안, 무선네트워크 보안, 침입대응