Journal of The Korea Society of Computer and Information
Vol. 24 No. 1, pp. 107-113, January 2019
www.ksci.re.kr
https://doi.org/10.9708/jksci.2019.24.01.107

Security Problems and Measures for IP Cameras in the environment of IoT

Gil-uk Kang*, Sang-Hoon Han*, Ho Lee*

Abstract

Along with the development of IOT, the number of people using IOT devices has enormously increased and the IOT era has come. Especially, people using the IP cameras among Internet devices have been drastically increasing. It is because the IP cameras are well networked and comparatively cheap compared with CCTVs, and they can also be monitored and controlled in real time through PCs and smart phones for the purposes of general theft prevention and shop surveillance. However, due to the user's serious lack of security awareness and the fact that anyone can easily hack only with simple hacking tools and hacking sites information, security crimes that exploit those have been increasing as well. Therefore, this paper describes how easily the IP cameras can be hacked in the era of IOT, what kind of security incidents occurred, and also suggests possible government measures and new technical solutions to those problems.

▸Keyword: Internet of Thing, IP camera, Cracking, Default Password, Shodan, Brute Force Attack

I. Introduction

사물인터넷 세상은 지능화된 사물들이 인터넷을 통해 연결되어 상호 소통하며, 지능화된 인프라와 서비스 기술을 제공하고, ICT(Information & Communication Technology)를 기반으로 모든 사물들이 초연결된 상태에서 정보를 공유하여 인간의 삶의 질을 높여주고 있다.

가트너에서 발간한 보고서에 보면 PC, Tablet, Smart Phone을 제외한 사물인터넷 기기가 2020년에 260억대에 달할 것으로 전망되고, 맥킨지는 2025년까지 인류의 삶을 변화시킬 가능성이 큰 기술을 사물인터넷 기술로 꼽고 있으며, 사물인터넷 기술이 모든 산업에 적용 될 것으로 전망하고 있다.

사물인터넷 환경에서 연결되는 디바이스의 형태는 다양해지고 있다. 특히 인터넷에 직접 연결될 수 있는 기기들이 늘어나고 있으며, 유선 및 무선으로 연결되고 있다. 크게 영상정보를 전송할 수 있는 장치에서부터 블루투스를 이용한 네트워크 장치, RFID 기술을 활용한 장치, NFC기반 장치, USN 기반의 장치들과 같이 매우 작은 형태의 디바이스들이 개발되어 우리 실생활에 빠르게 스며들고 있다.

이에 따라, 현재 사물인터넷(IoT) 기술은 자동차, 의료기기, 사회 인프라, 가정, 기업 등 다양한 분야의 시장에 침투되어 빠른 속도로 발전해가고 있으며, 인간에게 편리함과 풍요로움을 제공하고 하고 있다. 하지만 사물인터넷 디바이스들이 취약한 암호화 과정과 무선 통신의 이용으로 데이터가 쉽게 노출 될 수 있는 점이 보안에 많은 취약점을 드러내고 있다. 특히 여러 가지 디바이스들에 의해 얻어진 데이터들이 외부로 유출되는 경우 심각한 문제들을 야기하게 되고, 개인 정보의 유출로 인해 사생활 침해라는 부작용을 낳기도 한다. 이런 상황에서 사물인터넷에서 존재하는 보안 위협들에 대처하기 위한 보안 기술들은 디바이스의 발전 속도를 따라가지 못하는 실정이다.

본 연구에서는 다양한 사물인터넷 기기 중 영상 정보를 수집하고 관리하는 IP Camera를 중심으로 발생하는 해킹 문제를 분석하고, 해결책을 제안하고자 한다.

IP Camera는 카메라 본체, 카메라 모듈, CPU로 구성된 영상

• First Author: Gil-Uk Kang, Corresponding Author: Sang-Hoon Han, Co-Author : Ho Lee
*Gil-Uk Kang (kki8984@daum.net), Dept. of Computer Information Security, Korea National University of Welfare
*Sang-Hoon Han (shhan@knuw.ac.kr), Dept. of Computer Information Security, Korea National University of Welfare
*Ho Lee (lho@knuw.ac.kr), Dept. of Computer Information Security, Korea National University of Welfare
• Received: 2018. 11. 19, Revised: 2018. 12. 03, Accepted: 2018. 12. 04.
* This paper is an extension of the "IP Camera Hacking Analysis And Measure" presented at the Winter Conference of the Korea Society of Computer and Information in January 2018.

입력 장치와 디코더, 영상 압축, 네트워크 전송 장치로 구성된 영상 전송 장치로 이루어진 디지털 비디오카메라의 일종으로, Web Cam, Network Camera라고도 불리고 있다. 아날로그 방식의 CCTV의 문제점인 저 화질, 복잡한 배선, 비용 문제 등을 극복하여 별도의 DVR장치가 없더라도 손쉽게 영상을 녹화하고 캡처가 가능하다는 점과 어느 공간에서든 네트워크에 연결 할 수 있어서 실시간으로 영상을 모니터링과 제어가 가능하다는 점 등이 장점으로 부각되고 있다. 이러한 장점들 때문에 기업들뿐만 아니라 최근 들어서는 홈오토메이션에 관심이 있는 가정, 어린아이들을 키우고 있는 가정, 몸이 불편한 노인이 있는 가정, 그리고 애완동물을 키우고 있는 가정들 사이에서도 IP카메라의 수요가 나날이 증가하고 있다. 그림 1에서 보듯이 아날로그 카메라에 비해 IP 카메라의 증가 속도는 매우 빠른 속도로 늘어나고 있음을 알 수 있다.[1,2]

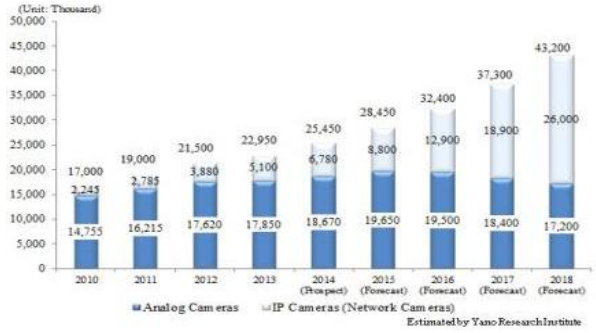

Fig. 1. Transition and Forecast of Global Surveillance Camera Market Size

한국인터넷진흥원에 따르면 우리나라에 유통 중인 IP 카메라 53개 제조사, 400개 제품을 대상으로 공장 출하 시 초기에 설정된 ID 및 비밀번호의 취약점을 조사한 결과, 국내 제품인 경우 48개 제품, 해외 제품인 경우 78개 제품에서(총 31.5%) 보안취약점이 발견됐다고 전했다.

실제 국내에서도 IoT 보안 취약점 신고 및 조치 건수가 해마다 증가하고 있으며, 이로 인해 IP카메라에서 수집된 다양하고 수많은 데이터들이 개인정보 유출로 인한 프라이버시 침해를 낳고 있어 현재 다양한 사회적 문제가 발생하고 있다.

본 논문에서는 2장에서 IP 카메라 해킹에 의한 피해사례와 그에 대한 연구들을 살펴보고, 3장에서는 쇼단 사이트를 통한 IP 카메라의 문제점을 기술하고, 비밀번호 크래킹을 통해 존재하는 위협요인을 분석하고 보안대책을 논의한다. 마지막으로 4장에서 결론을 맺고자 한다.

II. Preliminaries

1. Case of Domestic Damages by IP Camera Hacking

현재 신문지상이나 인터넷에서 보안기술이 미흡한 상태의 IP카메라를 설치하는 사례가 증가하고, 영상 장치를 활용하고자 하는 수요가 가정에서부터 매우 빠르게 증가함에 따라 해킹에 의한 피해도 급격히 증가하고 있는 추세이다. 실제로 IP카메라 해킹을 통해 녹화한 성관계, 탈의실 영상들을 버젓이 성인사이트 및 P2P사이트에 유포 및 판매한 범죄자가 무더기 입건되기도 했으며, 국내 반려동물 사이트를 해킹해 이와 연계된 IP카메라에 접속한 후, 4개월 동안 사생활을 엿보거나 불법 녹화한 범죄자가 검거되는 등 최근까지도 IP카메라 해킹 범죄로 인한 프라이버시 침해 문제가 끊임없이 발생하고 있다. 그림 2는 러시아의 IP로 추정되는 사이트로 (http://www.i***c***.com) 무방비 카메라만 7만여 대의 목록을 가지고 있다. 이와 같이 보안설정의 중요성을 보여주기 위한 사이트라고 주장하며 자신들이 해킹한 IP카메라를 국가별로 목록화해 제공해주고 있는 내용을 보여주고 있다.

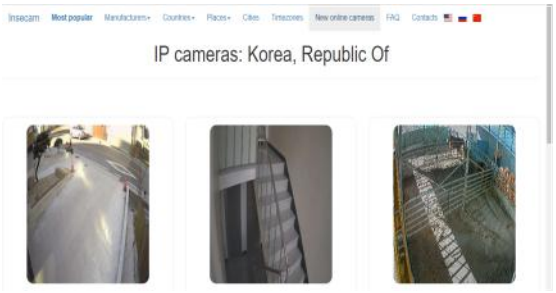

Fig. 2. Site Listing IP Cameras that were hacked

목록에서 보면 해킹된 한국의 IP 카메라는 7,000여대 정도 존재하고 있으며, 더 중요한 것은 이 사이트에서 실시간 영상 전송 및 구글 맵 서비스와 연계해 IP카메라가 설치된 위치 및 상세정보까지 제공하고 있다는 점이다. 위치 정보가 연결되면 개인의 사생활 침해문제가 생길 수 있으며, 사회적 문제가 생길 수 있는 여지가 높아진다. 그리고 이런 영상 정보를 제공해주는 사이트가 한 곳이 아니고 수 십여 곳에 달해 그대로 방치하고 있으면 더 큰 사회적 문제가 발생할 것으로 보인다.

2. Search Engine : Shodan

쇼단(Shodan) 사이트는 사물인터넷(IoT) 기반으로 인터넷에 연결된 장치를 검색하는 검색엔진으로 2009년 John Matherly에 의해 개발됐으며, 보안 전문가들이 인터넷에 연결되어 있는 라우터, 스위치, 공유기와 같은 네트워크 장치나 인터넷에 직접 연결되어 있는 웹캠, 복합기와 같은 다 기능 장치 등을 손쉽게 검색하고, 취약점을 찾아내어 보안성을 강화하기 위해 만들어졌다. 하지만, 노출된 기기들이 생각보다 보안에 매우 취약한 경우가 대부분이라서 어둠의 구글, 해커들의 놀이터라고도 불리고 있다.

실제로 우리나라에서는 여수에 있는 국내 가스 측정 시스템의 정보와 인천 국제공항의 내부 장비의 정보가 유출된 적이 있기도 하며, 쇼단에서 가장 인기있는 검색어인 cctv와 webcam으로 국내 기기를 검색 시 검색 결과 개수가 세계에서

각각 1위와 3위에 해당하고 있어 쇼단에 대한 각별한 주의가 필요하다. 그림 3이 쇼단 사이트의 첫 화면으로 평범해 보이는 사이트(https://www.shodan.io)이나 실제로 악용될 경우에 개인정보의 유출과 같은 피해를 입을 수 있다.

Fig. 3. Homepage of Shodan

3. Password Crack tool

사물 인터넷 환경에서 네트워크에 연결되어 있는 취약점이 존재하는 유/무선 공유기와 IP카메라의 비밀번호는 무작위 대입공격(brute force attack)이나 사전 공격(Dictionary Attack)에 의해서 쉽게 뚫릴 수 있다. 또한 이런 공격에 사용되는 도구들도 인터넷에서 쉽게 찾을 수 있다는 점이 심각성을 더하고 있다. 무선 랜의 비밀번호를 크래킹하기 위한 도구로는 aircrack-ng 이라는 툴이 있고, IP 카메라의 비밀번호를 크래킹하는 도구로는 Hydra같은 툴이 존재한다. 또한 사전 대입 공격을 하기위한 사전들도 이미 만들어져있는 사전의 종류도 많이 존재하고 있으며, 무선 랜 해킹을 위한 사전이라고 해서 5GB에 해당하는 사전 파일도 존재한다. 이 정도의 크기면 무작위 대입공격과 같은 효과를 얻을 수 있을 것으로 보인다.[14-16]

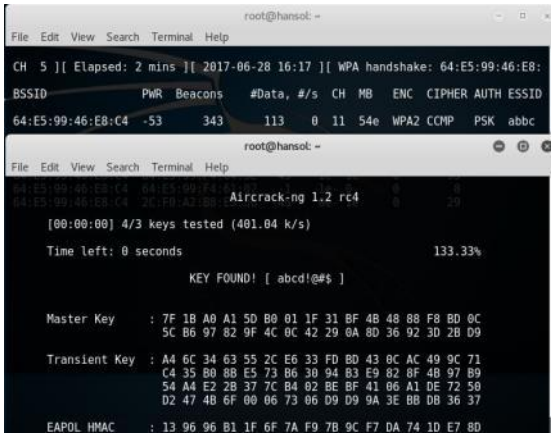

Fig. 4. Example of Aircrack-ng Tool

그림 4는 aircrack-ng 툴을 이용하여 WPA2 방식으로 암호화가 적용된 환경에서 비밀번호를 크랙하는 과정을 보여주고 있다. 비밀번호를 크랙하는데 소요되는 시간은 조금 많이 필요하지만 인내심을 가지고 작업을 수행하면 충분히 효과를 보고 있는 것으로 알려져 있다.

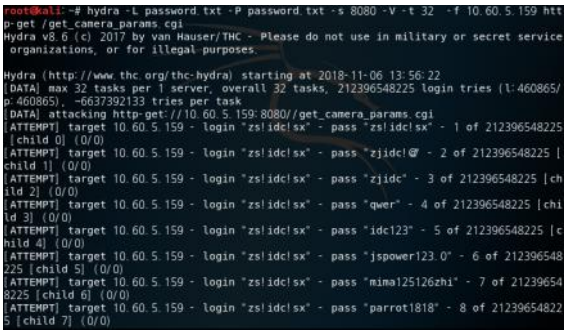

Fig. 5. Example of Hydra Tool

그림 5는 Hydra 툴의 실행화면을 보여주는 것으로 네트워크상에서 로그인정보인 아이디와 패스워드를 크래킹하는 과정을 보여주고 있다. 여기서는 특정 IP주소(10.60.5.159)를 갖고 있는 카메라에서 사용되는 인증관련 CGI 파일을 찾아서 아이디와 패스워드를 입력받아 전달하는 변수에 사전 공격방법을 적용하여 비밀번호를 크래킹하는 과정을 보여주고 있다.

4. Related works

IP 카메라의 보안성 문제들을 인식하고, 여러 가지 관점에서 IP 카메라의 취약점들을 해결하고자 노력하고 있다. 기본적인 노력으로 IoT 기기들에게 적용되어야 하는 소형 장치에 적합한 암호화 기술의 개발, 인증 과정에서 발생하는 아이디와 비밀번호의 관리, 인증과정에서 ID와 패스워드가 평문으로 전송되는 것을 고려하여 공개키 기반의 키 교환 프로토콜의 적용 등 다양한 방법이 진행되고 있다. IP 카메라의 철저한 인증관리의 필요성을 강조하며, 기본적인 보안과정인 사용자 인증 과정을 반드시 적용하여 Default Password로 남아 있지 않도록 제안하고, 로깅의 중요성과 제품 개발자나 관리자들의 관리의 중요성을 강조하기도 하고, 네트워크 기반의 IP 카메라에서 IP의 노출 문제와 해킹으로 인해 발생하는 성능저하 문제를 제시하고 있으며, IP 카메라의 전송구간에서 발생하는 취약점을 해결하기 위해 스위치 단에서의 보안성 강화 방법을 제시하고 있다.[3-7]

IP 카메라를 안전하게 사용할 수 있는 방안을 심리적 관점에서 접근하여 비밀번호를 변경하고 소프트웨어를 업데이트 하려는 의도를 높이는 방안을 연구한 사례도 있다.[8]

정부차원에서도 심각성을 깨닫고 'IP카메라 종합 대책'의 추진과 IoT 보안 인증제를 도입했다. 정부의 대책에서도 초기 비밀번호의 관리, IP 카메라에 보안체크리스트를 적용하여 제조, 수입업체를 대상으로 이행권고 등의 내용을 담고 있다. 하지만 정부에서 발표한 계획에도 불구하고 현재 IP카메라 해킹 문제는 여전히 발생하고 있어 더욱 실효성 있는 대책이 필요할 것으로 보인다.[9,10]

III. Related Experiments and Results

1. Scanning with shodan

쇼단에서는 검색어만을 이용하여 검색만 해도 검색되는 기기의 수는 엄청 나다. 그러기 때문에 사용자가 원하는 정보를 검색어만으로는 손쉽게 찾기 힘들기 때문에 사용자가 원하는 정보를 효율적으로 얻을 수 있도록 고급기능을 제공한다. 고급기능에는 필터 검색을 통하여 검색범위를 효과적으로 지정할 수 있고, 스크립트 언어와 프로그래밍 언어에서 제공되는 API를 이용하여 전문가들이 사용할 수 있는 환경을 제공하고 있다. 하지만, API와 스크립트는 유료 계정에만 사용할 수 있어서 본 논문에서는 필터 검색을 이용해 우리나라의 IP카메라만을 스캐닝한다. 표 1은 쇼단에서 사용되는 필터를 제시하고 있다.[11]

Table 1. Filters used in Shodan

Keyword	Explanation
country	해당 나라의 장비 검색
geo	해당 위도/경도의 장비 검색
product	해당 제품의 장비 검색
net	해당 IP와 서브넷 마스크의 장치 검색
os	해당 OS로 운영되는 장비 검색
port	해당 포트의 장비 검색

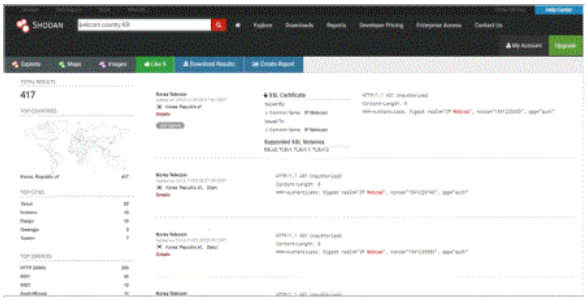

Fig. 6. Result of Retrieval using contry:KR Filter

검색을 하면 그림 6에서 보듯이 오른쪽에는 검색된 기기의 IP명과 상세정보(Details)를 통해 해당 기기의 정보를 볼 수 있고, 왼쪽에는 총 검색된 개수와 검색된 결과 중 상위 도시, 서비스, ISP(Internet Service Provider), 운영체제(OS)등의 통계정보를 확인할 수 있는 형태로 이루어져있다.

Fig. 7. Access to Domestic IP Camera without Authentication

실험에서는 많은 필터 중 country:KR 필터를 통해 cctv와 webcam을 검색한 결과, 총 1146개와 417개가 검색됐으며 대부분의 기기 경우 접속 시 아이디와 패스워드를 요구하는 페이지인 인증페이지로 접속되어지고 있었다. 하지만, 다수 기기들이 인증페이지 내에서도 각 제조사 별 디폴트 패스워드로 접속되는 경우가 많았으며, 심지어는 그림 7 처럼 사용자 인증 과정이 없이 바로 IP카메라로 접속할 수 있는 기기들도 어렵지 않게 찾을 수 있었다. 이를 통해, 실제 해커가 유료계정을 구매 해 API를 이용하거나 다양한 필터 검색을 통해 더 질 좋은 검색결과를 얻어낼 시 국내에서 해킹될 수 있는 기기의 수는 기본적으로 수 천개이상 일 것으로 보인다.

2. Experiment Result

본 논문에서는 시중에서 유통되고 있는 중국산 IP 카메라가 얼마나 쉽게 해킹되는 지를 보이기 위하여 시중에 판매되는 2가지 종류의 IP 카메라에서 서버와 교신하는 CGI파일과 데이터 전송 제출에 사용되는 요청 방식을 그림 8과 같이 웹브라우저의 개발자 도구를 통해 전송방식과 계정과 비밀번호에 대한 파라메터 변수를 알아낸 다음, hydra툴을 이용해 무작위 대입 공격의 한 유형인 사전 공격을 진행했다.

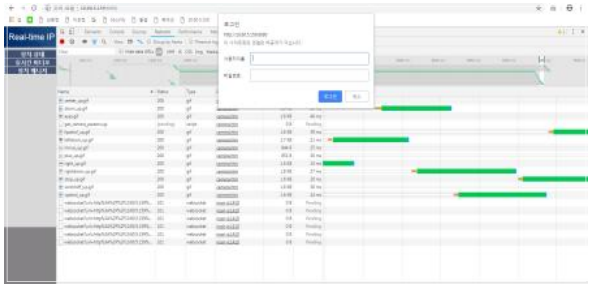

Fig. 8. Finding Parameter Information using Development Tools

첫 번째 실험에서는 쇼단에서 검색된 기기들에서 많이 보였던 디폴트 패스워드를 가진 기기들이 얼마나 취약한지를 보여주기 위해 기기의 패스워드를 각 제조사 별 디폴트 패스워드로 설정하여 3번의 실험을 진행했으며, 그 결과 그림 9와 같이 비밀번호 크래킹에 성공했으며, 표 2는 디폴트 패스워드로 설정된 경우에 30분 이내에 크래킹 성공 상황을 나타내고 있다.

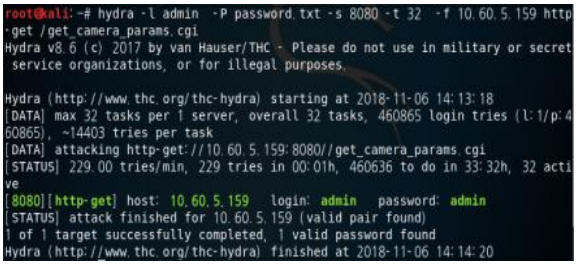

Fig. 9. Cracking Password using Hydra Tool

Table 2. Cracking result after setting Default Password

Password	Time	Result
admin	10 min	O
root	30 min	O
1234	10 min	O

두 번째 실험에서는 기기의 아이디는 admin으로 둔 후, 패스워드를 영단어로만 조합된 패스워드로 설정하여 3번의 실험을 한 결과 모두 성공했으며, 추가적으로 계정도 영단어로만 조합된 문자로 변경한 후 2번의 실험을 더 진행했는데 소요 시간만 길어졌을 뿐 모두 성공했다.

세 번째 실험에서는 기기의 아이디는 두 번째 실험과 동일하게 한 후, 패스워드를 현재 자주 쓰이는 영단어+숫자 조합으로 설정하여 3번의 실험을 진행하였다. 그 결과 모두 성공하였으나 최대 길이였던 12자일 경우 시간이 2일 소요됐다. 추가적으로 계정도 영단어로만 조합된 문자로 변경한 후 한 번 더 실험을 진행했는데 이 역시 일주일 내로 성공했다.

네 번째 실험에서는 기기의 아이디는 두 번째 실험과 동일하게 한 후, 패스워드에 더 높은 복잡성 부여를 위해 무작위 영문+특수문자, 영단어+특수문자, 무작위 영문+숫자로 3번의 실험을 진행하였다. 그 결과 표 3에서 보듯이 안전한 패스워드인 경우에는 영단어+특수문자만 크래킹에 성공하였으며, 무작위 영문과 다른 문자를 조합한 형태의 패스워드는 시간이 많이 소요되었음에도 불구하고 크래킹이 되지 않았다.

Table 3. Cracking Result after setting Safe Password

Password	Time	Result
guardian!	2 days	O
addiuwqej!	Unknown	X
erprmvdwg57	Unknown	X

총 4번의 실험에서 무작위로 구성된 영문+다른 문자조합일 경우에만 실패한 것으로 보아, 현재 우리가 일반적으로 사용하고 있는 패스워드의 해킹 난이도 수준이 매우 낮다는 걸 알 수 있다. 따라서 해커가 시간적 여유와 사용자의 대한 기본적인 정보가 존재한다면 대부분 해킹에 성공할 것으로 보인다.

비밀번호에 관한 기존 연구에서도 보면, 무선 랜 환경에서 공유기에 대하여 접속 비밀번호를 크래킹하는 실험을 aircrack-ng 툴을 이용하여 실시했었는데 이때의 실험결과도 비슷한 결과가 나왔다. WEP, WPA. WPA2 방식의 암호화를 적용한 경우에도 비밀번호가 크래킹 되었다. 공유기에 대한 문제점들이 지적되어 공유기 제품을 생산하는 단계에서 적용할 보안 가이드를 제정하여 초기 비밀번호를 부여 했음에도 불구하고 비밀번호가 노출되는 현상이 발생하였다. 초기 비밀번호가 안정성있게 10자리에 문자와 숫자의 조합이라도 무작위 대입법과 같은 공격에는 노출될 수 밖에 없다.[12]

사물 인터넷 환경에서 IP 카메라의 취약점을 해결하기 위한 노력으로 제시되는 정책을 정리하여 보면 다음과 같다.

① IP 카메라 초기 비밀번호 보안성 확보
② 보안 수준이 높은 제품으로 전환 유도
③ 쇼단과 같은 사이트에 노출된 기기들의 모니터링
④ 사용자들의 보안의식 강화
⑤ IoT 보안 인증제를 실시
⑥ 지능화된 보안 기술 개발

이러한 대책들은 반드시 필요한 필수 대책으로 보고 있으며, IP 카메라의 초기 비밀번호를 부여한다고 해도 비밀번호 크래킹 툴을 이용하며 쉽게 노출될 수 있기 때문에 추가적인 다음의 보안 요구 사항들이 필요하다고 본다.

첫째는 초기 비밀번호의 길이를 10자 이상으로 3가지 문자 조합을 반드시 사용하도록 하고, 무작위 대입 공격에 대비하여 3회 이상 패스워드가 틀렸을 경우에는 인증페이지의 세션을 종료시키거나 다른 인증방식을 요구하는 보안 정책을 의무화하여 본 논문에서 실험했던 것과 같은 무작위 대입 공격이 지연될 수 있도록 하는 기능을 제도화해야 한다. 또한 카메라를 관리하는 관리자들이 편의에 의해서 비밀번호를 모두 쉽고 간단하게 변경하는 사례들이 있는데 이를 방지하기 위한 나쁜 목록(Bad List)을 적용하여 목록에 있는 많이 사용하는 해당 비밀번호는 사용할 수 없도록 해야 한다. 예를 들면, 목록의 qwert1234%, qwe123!@#, qwert!1234 등의 자판의 순서에 따른 비밀번호들은 사용할 수 없도록 해야 할 것이다.

둘째, 쇼단과 같은 사이트에 노출된 기기들은 후에 봇이 되어 큰 문제를 야기할 가능성이 충분히 있기 때문에 정부와 기업은 쇼단을 주기적으로 모니터링하여 노출된 IP 카메라 취약점을 인지 및 분석하여 적극적인 대응은 물론, 개인의 카메라가 노출되지 않도록 원격공격을 예방하는 보안정책의 개발도 필요하다.

셋째, 정부는 IP 카메라 종합 대책과 함께 IoT 보안 인증제를 실시하였으나, 현재 강제성이 없어 신청한 업체가 소수에 불과하다. 하지만, 앞으로 사물인터넷시대가 도래하게 된다면 해당 기기들의 보안은 필수불가결하기 때문에 미리 IoT 보안 인증제의 의무화가 필요하다.

넷째, 정부는 기업에게 무선 공유기와 같이 접근통제가 가능하도록 IP 주소나 MAC 필터링 기능 및 쇼단에서 필터검색을 통해 찾아내지 못하도록 사용자에게 기본 포트 변경을 의무화하여 기기에 허용된 인가자만 접속할 수 있도록 해야 한다.

IV. Conclusion

본 논문에서는 IP 카메라 보안의 문제점을 쇼단과 같은 사이트의 검색과 비밀번호 크래킹 툴을 이용하는 실험을 통해서, 기본적인 보안 정책을 적용했음에도 불구하고 취약점들이 존재한다는 것을 보여주고 있다. 아직도 수많은 IP 카메라들이 비밀번

호가 없거나 디폴트 패스워드(Default Password)를 사용하는 상태에서 작동되고 있다. 현재 사용자들과 기업들은 자신이 관리하는 IP 카메라의 보안문제가 얼마나 심각한지를 인식하고, 소프트웨어의 업데이트나 비밀번호의 설정 등을 통하여 안전한 IP 카메라가 될 수 있도록 해야 할 것이며, 정부는 사용자들의 보안 의식을 강화할 수 있도록 홍보와 교육에 힘을 써야 할 것이다. 이는 결코 IP 카메라 기기 하나의 문제가 아닌 모든 IoT 기기의 문제이며, 현재 상태대로 라면 추후 사물인터넷이 더욱 더 발전될 시 보안이 미흡한 기기들로 인해 사회적 문제가 발생할 가능성은 필연적이므로 정부, 기업은 물론 개인도 보안에 대한 높은 경각심을 가져야 할 것이다.

REFERENCES

[1] Jeon Young Sung, Han Jong Wook, Cho Hyun Sook, "Technology Trend of Next Generation Video Security", REVIEW OF KIISC, 20(3), pp. 9-17, 2010.

[2] Hong Soon Ho, "IP Camera Market and Trend in the Video Security Industry", REVIEW OF KIISC, Vol. 20, No. 3, pp. 18-23, 2010.

[3] J. Y. Park, C. H. Song, S. Y. Kim, J. H. Park, J. H. Park, "IP Camera Authentication and Key Exchange Protocol Using ID-Based Signature Scheme", Journal of the Korea Institute of Information Security & Cryptology, 28(4), pp. 789-801, 2018.

[4] S. D. Yoo, D. H. Ryu, "A study on the Promotion Method of Domestic Video Security Industry", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 17, No. 3, pp. 9-21, 2017.

[5] Tae Woong Seo, Sung Ryoul Lee, Byung Chul Bae, E-Joong Yoon, Chang Soo Kim, "An Analysis of Vulnerabilities and Performance on the CCTV Security Monitoring and Control", Journal of Korea Multimedia Society, 15(1), pp. 93-100, 2012.

[6] Kim Yun Ha, Yun Seong Won, Kim Jin Hun, OH EUN, Choi Hun Ju, "The Case Study on Security Reinforcement and Network Management Improvement using Vulnerability Analysis of Transmission Section for IP Camera", Proceedings of Symposium of the Korean Institute of Communications and Information Sciences, pp. 759-760, 2018.

[7] Jin Young Park, Chi-ho Song, Suk-young Kim, Ju-hyun Park, Jong Hwan Park, "IP Camera Authentication and Key Exchange Protocol Using ID-Based Signature Scheme", Journal of The Korea Institute of Information Security & Cryptology, 28(4), pp. 789-801, 2018.

[8] K. Y. Kim, K. S. Lee, B. S. Kim, "Protection Motivation of IP Camera Users: A Mixed Methods Approach", The e-Business Studies, 19(10, pp. 227-245, 2018.

[9] DongHyuk Lee, Namje Park, "A Study on Security Authentication and Security Management Method for IoT Products", The Journal of The Korean Institute of Communication Sciences, 33(12), pp. 28-34, 2016.

[10] Ministry of Science and ICT, Korea Communications Commission, National Police Agency, "Comprehensive Countermeasures for IP Cameras", 2017.

[11] MiHui Kim, "Privacy Protection Technologies on IoT Environments : Case Study of Networked Cameras", Journal of THE KOREA CONTENTS ASSOCIATION, 16(9), pp. 329-338, 2016.

[12] Sang-hoon Han, Kyo-Rim Koo, Han-Sol Park, Hyun-Tae Kim, Do-Yong Song, "A Security Analysis by Cracking in Wireless Routers", Proceedings of the Korean Society of Computer Information Conference, 25(2), pp. 400-401, 2017.

[13] Sang-Hoon Han, Jin-Hui Jang,Gil-Uk Kang, Han-Sol Park, "IP Camera Hacking Analysis And Measure", Proceedings of The Korean Society of Computer Information Conference, 26(1), pp. 165-166, 2018.

[14] Ishwadeep Badgujar, "How to Hack CCTV Private Cameras", https://null-byte.wonderhowto.com/forum/hack-cctv-private-cameras-0159437

[15] Hydra tool, http://tylerrockwell.github.io/defeating-basic-auth-with-hydra/

[16] Andy O'Donnell, "How to Secure Your IP Security Cameras", https://www.lifewire.com/secure-your-ip security-cameras-2487488

Authors

Gil-Uk Kang is currently in the third grade of Computer Information Security at the Korea National University of Welfare. He is interested in Information Security, Internet of Thing(IoT) and Network Security.

Sang-Hoon Han received the B.S., M.S. and Ph.D. degrees in Computer Science and Engineering from Dongguk University, Korea, in 1990, 1995 and 2002, respectively Dr. Han joined the faculty of the Department of Computer Information Security at Korea National University of Welfare, Pyeongtaek, Korea, in 2003. He is currently a Professor in the Department of Computer Information Security, Korea National University of Welfare. He is interested in Information Security, Internet of Thing(IoT) and Computer Vision, and multimedia computing.

Ho Lee received the B.S. degree in Computer Science from Dongguk University, Korea, in 1982. He received the M.S. degree in Computer Science from Vrije Universiteit Brussel, Belgium, in 1989. He received the Ph.D. degree in Information Engineering from Sungkyunkwan University, Korea, in 2002. Dr. Lee joined the faculty of the Department of Computer Information Security at Korea National University of Welfare, Pyeongtaek, Korea, in 2002. He is currently a Professor in the Department of Computer Information Security at Korea National University of Welfare. He is interested in Information Security, Computer Networks and ICT.