IP 카메라 보안 취약점과 대응 방안에 관한 연구

허은정, 고다원, 오찬석, 이서연, 최석환*

연세대학교

dmswjd4315@yonsei.ac.kr, da0ne@yonsei.ac.kr, chan1225@yonsei.ac.kr, ysl04030@yonsei.ac.kr, sh.choi@yonsei.ac.kr

A Study on the vulnerabilities and countermeasures of IP Camera

Heo Eun Jung, Ko DaWon, Oh Chan-Seok, Lee Seo-Yeon, Choi Seok-Hwan

Yonsei University

요 약

IP 카메라는 CCTV와 다르게 집 밖에서도 핸드폰을 이용해 실시간으로 확인이 가능하다는 점에서 가정이나 기업 등 여러 곳에서 사용이 증가하고 있다. 이러한 증가량과 함께 보안 위협의 수도 증가하며 사생활 침해와 같은 문제가 끊임없이 발생하는 추세이다. 하지만 이러한 상황에도 불구하고 IP 카메라 사용자들의 보안 의식이 부족하다. 따라서 본 논문에서는 IP 카메라의 보안 취약점을 네트워크와 시스템 측면에서 소개하고 이에 대한 대응 방법을 소개한다.

Ⅰ. 서 론

Internet of Things(IoT) 기술이 발전함에 따라서 실생활과 매우 밀접한 부분까지 IoT 디바이스들이 사용되고 있다. 그중에서도 유무선 네트워크와 연결되어 실시간으로 PC나 스마트기기를 통해 관찰 및 녹화할 수 있는 Internet Protocol(IP) 카메라에 대한 수요가 급증하고 있다. 시장조사 전문기관 IMS 리서치에 따르면 전 세계 Artificial Intelligence(AI) CCTV 시장은 2021년 기준 298억 달러(한화 약 32조 원) 규모로 이 당시 약 1,000억 원 안팎으로 추산되는 국내 시장에 비해 300배 이상의 규모로 매우 큰 시장임을 알 수 있다. 하지만, IP 카메라의 사용량이 증가함과 동시에 보안 취약점 또한 대두되고 있다. 지난 2022년 1월 러시아에서 운영되는 사이트에 전 세계 개인 및 기관이 설치한 1만 7천 대의 IP 카메라 영상이 중계되었고, 그중에서 한국의 2,600곳도 실시간 생중계되었다[1]. 또한, 과학기술정보통신에 의하면 최근 5년간 국내 IP 카메라(웹캠)의 보안 조치 건수가 1만 1,982건인 것으로 확인되었다. 이러한 문제들은 IP 카메라 사용자들에 대한 개인정보 유출 가능성을 증가시키고 있다. 따라서, 본 논문에서는 IP 카메라의 최근 보안 취약점들을 두 가지로 분류하고 소개한다. 또한, 이러한 보안 취약점들에 대한 대응 방안에 관해 설명한다.

본 논문의 구성은 다음과 같다. 2장에서는 다양한 IP 카메라 보안 취약점을 네트워크와 시스템을 중심으로 간략히 소개하고, 이에 대한 대응 방안을 간략히 소개한다. 3장에서는 본 논문의 결론을 서술한다.

Ⅱ. 본론

1. 네트워크 취약점

IP 카메라는 네트워크 기반 서비스로 IP 주소와 Media Access Control (MAC) 주소, 포트 정보를 가지고 데이터 전송을 수행한다. 또한, 실시간 영상 데이터가 물리 계층에서부터 네트워크 계층의 망을 통해 전송되기 때문에 이 과정에서 다양한 공격기법들이 등장하였다[2].

1.1 중간자 공격

중간자 공격은 스푸핑, 스니핑 및 스누핑 등의 기법을 기반으로 통신 과정 중간에 데이터를 탈취하는 공격기법이다. Boyarinov 등은 Ettercap을 사용하여 Address Resolution Protocol(ARP) 스푸핑으로 Man In The Middle(MITM) 공격 시스템이 갖춰질 수 있음을 보였다[3]. Doughty 등은 Xeoma Surveillance 앱을 통해 암호화된 패킷에서 사용자 이름과 암호를 성공적으로 스니핑 할 수 있음을 보였다[4]. R Das 등은 네트워크 스니핑 프로그램인 Wireshark를 기반으로 패킷 추적 및 분석에 대한 앱을 구현해 IP 카메라로 송수신되는 네트워크 패킷이 위치 정보를 쉽게 얻을 수 있음을 증명했다[5].

1.2 포트 스캔 공격

포트 스캔 공격은 TCP/UDP 스캔 등의 스캔으로 이뤄진 공격으로, 서비스를 제공하는 서버의 포트를 조사해 포트의 활성화 여부를 확인한 후 정보를 얻어오는 공격기법이다. Bugeja, Jönsson, 등은 인터넷 노드의 열린 포트를 스캔 후 헤더와 배너 정보를 인덱싱할 때 장치 유형, 모델, 공급업체, 펌웨어 버전 및 기타 정보를 쉽게 얻을 수 있음을 보였다[6].

2. 시스템 취약점

IP 카메라는 카메라 기기 이외에도 공유기, 영상 확인 웹사이트 등을 필요로하기 때문에 이와 관련한 취약점을 활용하는 공격기법들이 등장하였다.

2.1 백도어

백도어란 원래 시스템이나 프로그램의 설계자 등의 관리, 유지 및 보수를 위하여 '특수한 계정을 인정하는 코드'를 의미한다. 즉, 백도어는 시스템설계자 등이 정상적인 인증 절차 없이도 시스템 등에 접근하여 시스템이나 프로그램을 관리, 유지 및 보수할 수 있는 통로가 된다. 이러한 긍정적인 의도와는 달리, 백도어가 악용되기도 한다[7]. IP 카메라는 기본적으로 오픈 인터넷망에 연결된다는 특성이 있어 IP 카메라에 백도어를 설치할 시,

영상을 탈취할 수 있다는 취약점이 존재한다. 민소연 등은 소니의 IPELA Engine IP 카메라에 설치된 2가지 백도어가 Telnet을 통해 'primana'와 'debug'를 원격 조정할 수 있음을 언급했다[8]. 또한, 고윤성 등은 백도어를 이용하여 IP 카메라와 클라우드 시스템의 VPN 통신을 통해 사설망 통제 시스템과 보안 프로그램 우회로 내부망에 접근해 2차 공격을 가할 수 있음을 보였다[9].

2.2 펌웨어 취약점

펌웨어 관련 공격기법들은 일반적으로 기기에 탑재된 펌웨어를 분석하거나 특정한 포트를 열고 정보입력을 기다리는 프로세스를 찾아낸 후, 직접 수정한 가짜 악성 펌웨어를 주입하여 좀비 PC처럼 DDoS 공격을 수행한다. Liranzo 등은 오래된 펌웨어에서 IP 카메라 장치에 대한 root shell 접근 권한을 얻은 후 장치를 손상시키거나 내부 데이터를 탈취하고, 백도어를 이식시키는 등 다양한 펌웨어 취약점이 존재함을 보였다[10]. 또한, A Tekeoglu 등은 IP 카메라에서 공격자들이 카메라를 하이잭한 후 펌웨어를 바꿀 수 있는 취약점이 존재함을 보였다[11].

2.3 비밀번호 해킹

비밀번호 해킹은 무작위 대입 공격(brute force attack), 사전공격(dictionary attack), 레인보우 테이블 어택 등 여러 유형의 비밀번호 해킹 공격을 사용하여 접근 권한을 탈취하는 것이다. 한상훈 등은 IP 카메라를 이용하여 초기 비밀번호와 복잡성을 더한 비밀번호에 대해 사전공격을 시도했을 때 크래킹에 성공함을 보여 IP 카메라의 비밀번호 취약점이 존재함을 증명했다[12]. 또한, G Kang 등은 여러 가지 비밀번호에 대해 hydra 툴을 이용하여 사전공격을 진행했을 때 무작위 영문과 다른 문자 조합의 패스워드를 제외한 방식들이 크래킹에 성공하여 비밀번호 취약점이 존재함을 보였다[13]. IP 카메라에 대한 이러한 비밀번호 해킹 취약점은 영상 확인을 위한 앱과 웹뿐만 아니라 영상 데이터 파일을 전송하는 공유기 등에서도 적용된다.

3 대응 방안

앞서 언급한 IP 카메라의 네트워크 및 시스템 취약점에 대한 대응 방안은 다음과 같다. 네트워크 취약점의 경우, VPN 기능에 해당하는 네트워크 침입에 대한 방지 기능을 제공하고 IP 카메라의 접근제어 기능을 보완하여 취약점을 개선할 수 있다[2]. 또한, 스푸핑된 DDoS 공격에 대한 탐지 기법의 적용을 통해 상기 언급한 네트워크 취약점에 대해 대응할 수 있다.

시스템 취약점의 경우, 제조사의 디폴트 값으로 IP 카메라의 계정을 설정하지 않고, 크래킹 시간이 최대한 길어지도록 패스워드와 계정의 복잡성을 높이고 주기적인 비밀번호 변경을 통해 취약점을 개선할 수 있다. 또한, 펌웨어의 주기적인 업데이트를 통해 펌웨어 관련 취약점을 개선할 수 있다[14].

Ⅲ. 결론

본 논문에서는 IP 카메라 취약점을 시스템과 네트워크 측면으로 분류하여 소개하고 이에 대한 대응책을 소개하였다. 향후 연구에서는 IP 카메라의 취약점들에 대한 통합적인 대응을 제공하는 보안 플랫폼의 설계 및 개발을 진행할 것이다.

ACKNOWLEDGMENT

본 논문은 2022년 과학기술정통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었습니다.(2019-0-01219)

참 고 문 헌

[1] 중앙일보(2022) ""내 거실 들여다보고 있었다" 韓2600곳 실시간 생중계 쇼크" 1월 13일

[2] 김윤하, 윤성원, 김진훈, 오은, 최현주, "IP 카메라의 전송구간 취약점 분석을 통한 보안강화 및 관리개선 사례에 관한 연구", 2018

[3] K Boyarinov, A Hunter, "Security and trust for surveillance cameras", 2017

[4] T Doughty, N Israr, U Adeel, "Vulnerability analysis of ip cameras using arp poisoning", 2019

[5] R Das, G Tuna, "Packet Tracing and Analysis of Network Cameras with Wireshark", 2017

[6] Joseph Bugeja, Désirée Jönsson, Andreas Jacobsson, "An Investigation of Vulnerabilities in Smart Connected Cameras", 2018

[7] 정연부, "정보보안 침해 사건 분석에 기초한정보보안의 법적 개념 요소 도출", 2013

[8] 민소연, 이재승, "IoT 환경에서 IP 카메라의 효율적 운용을 위한 키 관리 및 보안 설계 프로토콜", 2020

[9] 고윤성, 박관혁, 김창수. "물리보안 관제시스템의 보안위협 사례를 통한 취약점 분석 및 대응방안 연구". 2016.

[10] J Liranzo, T Hayajneh, "Security and Privacy Issues Affecting Cloud-Based IP Camera", 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)

[11] A Tekeoglu, AS Tosun, "Investigating Security and Privacy of a Cloud-Based Wireless IP Camera: NetCam", 2015 24th International Conference on Computer Communication and Networks (ICCCN)

[12] 한상훈, 장진희, 강길욱, 반한솔,."IP 카메라 해킹 분석과 대책", 2018.

[13] G Kang, SH Han, H Lee, "Security Problems and Measures for IP Cameras in the environment of IoT", 2019

[14] D THAKAR, "SURVEY ON IP CAMERA HACKING AND MITIGATION", 2020