KIPS Trans. Comp. and Comm. Sys.
Vol.12, No.3 pp.111~118
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2023.12.3.111

A Study on IP Camera Security Issues and Mitigation Strategies

Seungjin Shin† · Jungheum Park†† · Sangjin Lee†††

ABSTRACT

Cyber attacks are increasing worldwide, and attacks on personal privacy such as CCTV and IP camera hacking are also increasing. If you search for IP camera hacking methods in spaces such as YouTube, SNS, and the dark web, you can easily get data and hacking programs are also on sale. If you use an IP camera that has vulnerabilities used by hacking programs, you easily get hacked even if you change your password regularly or use a complex password including special characters, uppercase and lowercase letters, and numbers. Although news and media have raised concerns about the security of IP cameras and suggested measures to prevent damage, hacking incidents continue to occur. In order to prevent such hacking damage, it is necessary to identify the cause of the hacking incident and take concrete measures. First, we analyzed weak account settings and web server vulnerabilities of IP cameras, which are the causes of IP camera hacking, and suggested solutions. In addition, as a specific countermeasure against hacking, it is proposed to add a function to receive a notification when an IP camera is connected and a function to save the connection history. If there is such a function, the fact of damage can be recognized immediately, and important data can be left in arresting criminals. Therefore, in this paper, we propose a method to increase the safety from hacking by using the connection notification function and logging function of the IP camera.

Keywords : IP Camera, Hacking, Vulnerability, GoAhead Web Server, Illegal Filming

IP 카메라 보안의 문제점 분석 및 보완 방안 연구

신 승 진† · 박 정 흠†† · 이 상 진†††

요 약

세계적으로 사이버 공격이 증가하고 있으며 CCTV, IP 카메라 해킹과 같은 개인의 사생활에 대한 공격도 증가하고 있다. 유튜브나 SNS, 다크웹과 같은 공간에서 IP 카메라 해킹 방법에 대해 검색해보면 손쉽게 자료를 구할 수 있고, 해킹 프로그램 또한 판매되고 있다. 해킹 프로그램이 이용하는 취약점이 존재하는 IP 카메라를 사용하면 비밀번호를 주기적으로 변경하거나 특수문자와 영어 대소문자, 숫자를 포함한 복잡한 암호를 사용하더라도 쉽게 해킹 피해를 본다. 뉴스나 언론 매체를 통해 IP 카메라 보안성에 대해 문제를 제기하고 피해 방지를 위한 대책을 제시하였으나 해킹 사건은 꾸준히 발생하고 있다. 이러한 해킹 피해를 막기 위하여 해킹 사건 원인을 파악하고 이에 대한 구체적인 대응 방안이 필요하다. 먼저 IP 카메라 해킹 사건의 원인으로 취약한 계정 설정과 IP 카메라의 웹 서버 취약점을 분석하고 이에 대한 해결 방법을 제시하였다. 그리고 해킹에 대한 구체적인 대응 방안으로 IP 카메라에 접속하면 알림이 오도록 하는 기능과 접속 기록을 저장하는 기능이 추가되어야 한다고 제안하였다. 이와 같은 기능이 있다면 피해 사실을 즉각 알아차릴 수 있고, 범인을 검거하는 데 중요한 자료를 남길 수 있다. 따라서 본 논문에서는 IP 카메라에 접속 알림 기능과 로깅 기능을 사용하여 해킹으로부터 안전성을 높이는 방법을 제시하였다.

키워드 : IP 카메라, 해킹, 취약점, GoAhead 웹 서버, 불법 촬영물

1. 서 론

IT 기술이 발전함에 따라 많은 사람이 실생활에서 IT 기술을 사용하며 살아가고 있다. 자주 이용하는 스마트폰부터 시작해서 컴퓨터, 인터넷, 금융 서비스와 같은 기술이 없으면 생활을 할 수 없을 정도로 밀접하게 사용하고 있다. 이와 더불어 IT 기술이 발전하는 만큼 그에 따른 사이버 보안 문제도 계속하여 증가하고 있다. IT 보안 솔루션을 제공하는 Check Point Software Technologies가 발표한 '2022 Cyber Security Report'에 따르면 2020년 대비 2021년에 사이버 공격이 50% 증가하였다[1]. 비트코인, 이더리움과 같은 암호화폐 해킹, 랜섬웨어, 디도스 공격 및 악성코드 유포로 인한 내부 정보 탈취 등 각종 사이버 공격으로부터 위협받고 있다.

다양한 사이버 공격 중에서 IP 카메라 해킹 사건이 뉴스에서 심심치 않게 보도되고 있다. 몸캠 피싱 사건에서 노출되는 영상이나 사진은 일시적일 수 있다. 하지만 IP 카메라 해킹은

† 준 회 원 : 고려대학교 정보보호대학원 디지털포렌식학과 석사과정
†† 비 회 원 : 고려대학교 정보보호대학원 조교수
††† 종신회원 : 고려대학교 정보보호대학원 교수
Manuscript Received : September 13, 2022
First Revision : October 27, 2022
Accepted : October 31, 2022
* Corresponding Author : Jungheum Park(jungheumpark@korea.ac.kr)

카메라의 전원을 끄지 않는 이상 계속하여 사생활이 노출된다. IP 카메라에 접속한 뒤 민감한 사생활 장면이 나올 때까지 지켜보다 이를 저장하는 것이다. 이처럼 해킹으로 인한 지속적인 피해 사실을 알아차리기가 쉽지 않아 무엇보다 예방이 중요한 사건 중 하나이다.

IP 카메라의 구체적인 해킹 피해 사례로 2018년에 4,912대의 IP 카메라에 무단 접속한 후 민감한 사생활 장면을 녹화하여 27,328개의 동영상(1.4 TB)을 보관한 사건이 있었다. 39,706회 무단 접속한 후 계속하여 지켜보다가 민감한 장면이 나올 때만 화면을 녹화하는 것처럼 IP 카메라 해킹으로 사생활이 지속적으로 노출된다. 2021년에는 아파트 월패드를 해킹해 불법 촬영하고 불법 촬영물을 다크웹에서 0.1 BTC (한화 800만 원)에 판매하는 사례가 있었다. 또한, 2022년에는 IP 카메라에 무단 접속하여 불법 촬영을 하였고, 불법 촬영물을 SNS를 통해 판매하려다 검거된 사건이 있었다.

본 논문에서 IP 카메라 해킹 사건 사례를 살펴보고 해킹이 발생한 원인을 파악하고자 한다. 이를 통해 해킹이 어떤 방식으로 일어나는지, 아직도 그러한 방식이 통하는지, 대응 방안은 무엇인지 알아본다. 먼저 2절에서 관련 연구를 알아보고 3절에서는 IP 카메라 보안의 특징을 살펴본다. 이어서 4절에서는 IP 카메라 보안 위험 완화와 사고 대응 전략을 위한 보안 및 포렌식 내재화 방안을 제안한 뒤 5절에서 결론을 내고자 한다.

2. 관련 연구

IP 카메라와 같은 IoT 기기가 널리 보급되면서 IoT 기기 해킹 문제가 발생하자 보안에 관한 연구가 점차 진행되었다. 국내는 물론 국외에서도 보안 권고 지침이나 데이터 수집 및 분석에 관한 연구가 다양하다. 보안 권고 지침에는 IP 카메라, 스마트 TV, 로봇 청소기와 같은 IoT 기기들의 해킹 사례와 취약점을 설명하고 이에 대해 보안성을 강화하기 위한 권고사항을 제시한 사례가 있다. 데이터 수집 및 분석에서는 IP 카메라, 스마트 스피커를 중점으로 IoT 포렌식을 진행한 사례가 있다.

자세한 보안 권고 지침에 대해서는 먼저 IP 카메라 제품을 개발하기 전에 관계자들이 모여 제품의 잠재적인 위협을 찾아내는 보안위협모델링과 국제공통평가기준을 이용하여 보안 요구 사항을 분석한 사례가 있다[2]. 여기서 IP 카메라와 같은 IoT 제품들이 일상생활에 밀접하게 사용되어 높은 수준의 신뢰성이 요구되고, 이와 같은 신뢰성을 제공하기 위해 제품 개발의 첫 단계인 요구사항 도출 단계에서부터 완전한 요구사항을 도출하기 위한 연구가 필요하여, IoT 제품 중 IP 카메라를 대상으로 보안성 평가 관점에서 보안위협모델링을 통해 체계적으로 요구사항을 도출하는 방법을 제시하였다.

다음으로 IoT 환경에서 개인 정보 보호 기술을 제안한 사례가 있다[3]. IoT가 물리적인 세계를 디지털화하여 새로운 패러다임을 제시하고 있는데, 이것이 성공적으로 이루어지기 위해서는 IoT 보안이라는 중요한 문제가 있다고 하였다. 스마트 TV의 카메라를 해킹하여 영상을 유출하는 사례와 로봇 청소기 원격 조종 앱 취약점을 이용하여 로봇 청소기의 카메라를 해킹하는 사례를 설명하며 IoT 기기들의 전반적인 보안상 취약점을 제시하였다. 마지막에는 네트워크 카메라의 실제 사례들을 살펴보고 이에 대응하는 방안으로 철저한 인증 과정, 사용자의 로깅(logging), 제품의 보안성 모니터링, 암호화 보안 기능을 제시하였다.

스마트 홈 환경을 위한 IoT 기기들의 취약점을 연구한 사례도 있다[4]. 많은 IoT 장치가 스마트 홈을 이루고 있지만 IoT 장치들에서 심각한 보안 취약성이 노출되고 그 때문에 DDoS 공격에 사용되는 기기가 많다는 사례를 설명하였다. 그리고 이러한 취약점을 찾기 위해 오픈 소스 도구를 이용하여 스마트 홈 IoT 기기를 분석하는 방법을 설명하였다. 여기에는 원격 접속 취약점, 펌웨어 취약점, 모바일 애플리케이션 취약점, 웹 애플리케이션 취약점과 같은 취약점들을 파악하여 데이터 및 개인의 사생활에 대한 보호 방법을 제시하였다.

마지막으로 Non-PC 봇넷을 탐지하고 예방하기 위한 연구에서는 security infrastructure에 취약점이 있어 봇넷으로 활용된다고 하였다[5]. 특히 PC나 노트북에 국한되지 않고 스마트폰, 냉장고, 의료기기와 같은 IoT 제품에도 봇넷 공격이 이루어진다고 하였다. 현존하는 취약점으로는 초기 비밀번호 사용, IP 카메라 취약점, IPv6 취약점과 같은 것이 있으며 이에 대응하기 위해 인증된 애플리케이션 설치, 강력한 비밀번호 사용, 백신과 같은 프로그램을 사용하라고 제안하였다.

IoT 기기 데이터 수집 및 분석에 관한 연구에서는 먼저 무선 카메라를 포렌식하기 위한 방법으로 카메라 네트워크 트래픽을 모니터링하고 수집하여 분석하는 것이 있다[6]. 네트워크 트래픽 수집 결과에서 IP 주소를 필터링하여 외부 접속은 없었는지 확인할 수 있다. 또한, 네트워크 패킷들의 전송 시간을 계산하여 외부 공격은 없었는지 파악한다. 다만 이 방법은 네트워크 트래픽을 지속해서 모니터링해야 하는 필요가 있어 다소 큰 비용이 필요할 수 있다.

다음으로 IoT 기기가 증가함에 따라 Amazon Echo를 중점으로 IoT 포렌식을 진행한 사례가 있다[7]. 여기에서는 UART(Universal Asynchronous Receiver/Transmitter) 포트를 이용하여 획득 및 분석을 진행하였고, 분석된 데이터는 디바이스 정보, 할당된 IP 주소, 사용자 계정과 비밀번호 같은 개인 정보를 확인할 수 있다. 획득한 데이터가 암호화되어 있지 않고 평문 그대로 저장되어 있어 직접 값을 확인할 수 있다. 하지만 여기서 사용한 방식처럼 UART 포트를 이용하려면 제품을 분해하고 작업을 해야 한다.

끝으로 OWASP's Top 10 IoT Project에서 IoT 제품의 다양한 취약점을 보여주고 이를 활용하여 IP 카메라 제품을 중점으로 포렌식을 진행한 사례가 있다[8]. 패치 되지 않은 취약점이 존재하면 UART를 이용하여 컴퓨터에 USB로 연결 후 시리얼 통신으로 root shell을 실행하여 telnet backdoor를 열 수 있다. 그리고 암호화된 passwd 파일을 탈취하고 크랙하여 비밀번호를 얻을 수 있다. 일반적으로 사용자는

같은 계정과 비밀번호를 다른 서비스에서도 사용하기 때문에 IP 카메라만 노출되는 것이 아니라 다른 서비스의 개인 정보 또한 노출될 수 있음을 경고하였다.

3. IP 카메라 보안의 특징

IP 카메라 보안의 특징으로는 먼저 비밀번호 설정에 제한이 없다. 금융 서비스와 같은 대부분 서비스에서 비밀번호를 설정할 때 길이 8자 이상, 숫자와 특수문자를 포함해야 한다는 규칙이 있는 것에 비해 IP 카메라에는 특별한 정책이 없다. 따라서 '1234', 'root', 'admin'과 같은 간단한 비밀번호를 설정할 수 있다. 다음으로 로그인 시도에 제한이 없다. 비밀번호를 틀리게 입력하여 로그인에 실패하더라도 어떠한 제한이 없어 계속하여 로그인 시도를 할 수 있다. 이러한 문제로 Brute force 공격이나 Dictionary 공격에 취약하다. 그리고 비밀번호를 IP 카메라 내부 파일에 저장하는데, 별도의 암호화 작업 없이 평문 값을 그대로 저장한다. 이 때문에 비밀번호가 저장된 파일이 노출될 경우 비밀번호가 쉽게 노출된다. 마지막으로 IP 카메라를 사용하기 위한 뷰어 프로그램에 취약점이 존재할 수 있다. 이러한 보안의 문제점과 취약점을 이용하여 IP 카메라를 해킹하면 카메라 영상이 무방비로 노출된다.

3.1 IP 카메라 뷰어 프로그램 작동 방식

IP 카메라 뷰어 프로그램 작동 방식에 대한 Context Diagram은 Fig. 1과 같다. 기능별 설명을 하자면, 먼저 IP 카메라 제조사는 IP 카메라 하드웨어 및 소프트웨어를 개발하여 제품을 판매하고, IP 카메라에 접근하여 실시간 영상을 볼 수 있는 뷰어 프로그램을 제공한다. 뷰어 프로그램은 안드로이드 및 아이폰과 같은 스마트폰 전용 애플리케이션과 웹 브라우저 기반 프로그램이 있다. 그리고 이 프로그램은 사용자와 IP 카메라의 중간 위치에서 사용자의 접근 요청이 있으면 인증을 수행하고, 인증이 완료되면 IP 카메라에 실시간 영상을 요청하여 사용자에게 보여준다.

뷰어 프로그램 중 웹 브라우저 기반 프로그램은 IP 카메라에 웹 서버가 존재할 경우 제공된다. 이 프로그램은 IP 카메라에 할당된 IP 주소와 사용자 계정, 비밀번호만 알면 어디서나 누구든지 접속할 수 있다. 뷰어 프로그램에 접속하면 실시간 영상을 볼 수 있을 뿐만 아니라 기기 정보, 네트워크 목록, DDNS 정보와 같은 여러 가지 정보를 확인할 수 있다. 게다가 사용자의 비밀번호도 변경할 수 있다. IP 카메라에서 비밀번호 찾기와 같은 기능은 제공되지 않기 때문에 비밀번호가 변경되었을 때 이를 해결하기 위해서는 IP 카메라를 초기화해야 한다.

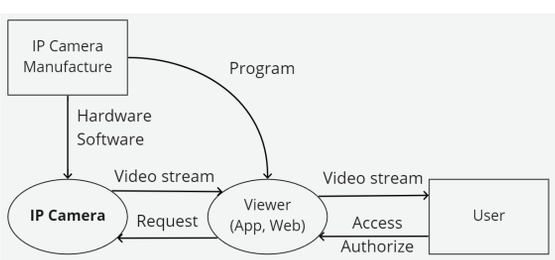

Fig. 1. Context Diagram of IP Camera

3.2 IP 카메라 관련 보안 문제

IP 카메라 보안의 특징은 대부분 뷰어 프로그램 문제에서 비롯된다. IP 카메라를 사용하려면 뷰어 프로그램을 필수로 사용해야 한다. 하지만 IP 카메라 사용자는 기기가 정상 동작하는 것에만 집중하고, 보안에 대해서는 크게 생각하지 않고 있다. 과학기술정보통신부에서 작성한 '2021년 정보보호 실태조사'에 따르면 IP 카메라 사용자의 28.4%가 IP 카메라에 접근하는 PC 및 스마트폰의 보안 설정 강화를 한다고 하였다[9]. 뷰어 프로그램 보안에 문제가 있는 만큼 다양한 해킹 가능성이 존재한다.

1) IP 카메라 해킹 가능성

IP 카메라 사용자의 47.8%가 기기의 디폴트 비밀번호를 변경한다고 하였다[9]. 많은 사용자가 아직도 계정과 비밀번호를 디폴트 그대로 사용하고 있다. 그 때문에 포트 스캔과 같은 방법으로 IP 카메라에 할당된 IP 주소만 확인되면 해킹이 쉽게 가능하다. 하지만 디폴트 비밀번호를 사용하지 않고 어렵게 변경한 사용자들도 해킹 피해를 보고 있다. IP 카메라 해킹에 대비하기 위하여 조치를 취하였음에도 IP 카메라 내부적인 취약점 문제로 비밀번호가 노출된 것이다.

GoAhead 웹 서버를 사용한 IP 카메라는 해킹에 취약하다. 그 이유는 제품 제조 당시 IP 카메라에 보안 취약점이 있어서 사용자가 아무리 어려운 비밀번호로 변경하였더라도 이 취약점을 이용하면 손쉽게 비밀번호를 알아낼 수 있기 때문이다[5, 10]. 이 취약점을 이용한 해킹 프로그램도 등장하였다. 또한, 이 취약점뿐만 아니라 인터넷에서 GoAhead 웹 서버 취약점을 검색하면 2001년부터 꾸준히 발견된 것을 확인할 수 있다.

GoAhead 웹 서버를 사용한 IP 카메라가 시중에 널리 퍼져있어 IP 카메라 해킹 사건이 계속하여 발생할 수 있다. 규모를 정확하게 파악할 순 없지만 구글 플레이스토어에서 IP 카메라 뷰어 애플리케이션 다운로드 횟수가 100만 회 이상인 것으로 보면 대략 100만 대 이상 시중에 판매된 것으로 볼 수 있다. 또한, 보안 취약점을 가진 시스템을 찾아내는 사이트인 shodan.io에서 GoAhead-Webs를 검색하면 약 300만 개가 조회된다.

2) IP 카메라 해킹 원인 분석

IP 카메라 해킹 사건 사례에서 피해자들의 계정과 비밀번호를 탈취하여 저장한 텍스트 파일이 발견되었다. 879개의 해킹 자료를 분석한 결과 IP 카메라 제조 당시 설정된 디폴트 계정과 비밀번호(admin:admin, user:user, guest: guest 등)를 그대로 사용하여 탈취된 내역이 551건(63%)이며, 디폴트가 아닌 어려운 암호로 변경했음에도 탈취된 내용이 328건(37%)이었다. 해킹 원인으로는 취약한 계정 설정과 웹 서버의 취약점 존재로 나눌 수 있다.

a) 취약한 계정 설정으로 인한 해킹

IP 카메라의 취약점 평가를 주제로 작성한 논문에서는 평가 테스트한 제품의 70%는 디폴트 비밀번호를 사용하였다고 한다[11]. 이처럼 비밀번호를 변경하지 않고 디폴트 비밀번호를 사용하는 사람들이 많으며, 디폴트 값으로 사용할 경우 비밀번호 크랙킹 도구를 이용하면 30분 이내에 비밀번호를 탈취할 수 있다[12]. 더구나 크랙킹 도구를 이용하지 않더라도 제조사별 IP 카메라 디폴트 계정과 비밀번호는 인터넷에서 검색만 하면 손쉽게 구할 수 있다[13]. 별다른 기술 없이 포트 스캔만 한 뒤 디폴트 계정과 비밀번호로 접속하면 쉽게 해킹을 할 수 있는 것이다.

취약한 계정 설정에 대하여는 디폴트 비밀번호를 의무적으로 변경하도록 '단말장치 기술기준' 행정규칙을 개정함으로써 보완하였다. 2019년 2월 7일부터 국내에서 판매되는 제품은 디폴트 비밀번호를 그대로 사용할 수 없다. 따라서 이전 제품들은 취약한 계정 설정으로 인한 해킹 피해가 발생할 수 있다. 하지만 이후 제품들은 적어도 이로 인한 해킹 피해는 발생하지 않는다.

b) 웹 서버 취약점으로 인한 해킹

IP 카메라 해킹 사건 사례에서 해킹 피해는 모두 웹 브라우저 기반 뷰어 프로그램을 통해 이루어졌다. 디폴트 계정과 비밀번호를 사용하지 않고 어려운 암호로 바꿨음에도 해킹 피해가 발생한 것은 IP 카메라가 사용하는 GoAhead 웹 서버에 취약점이 존재하기 때문이다. 최신 버전이 아닌 취약점이 존재하는 버전을 사용해서 해킹 피해가 발생한 것이다. 2022년 3월에 판매되는 새 제품을 구매하여 테스트한 결과 여전히 웹 서버에 취약점이 존재하였다.

3.3 웹 서버 취약점 목록

1) CVE-2002-2427

디지털 기기의 취약점 목록인 CVE(Common Vulnerabilities and Exposures)에서 GoAhead 웹 서버 관련 취약점(CVE-2002-2427)이 발견되었다[14]. 이 취약점은 URL에 추가적인 slash '\' (%5c)를 입력하면 GoAhead 웹 서버의 security handler가 인증하지 않고 데이터에 접근하는 것이다. 이를 이용한 해킹 프로그램은 별도의 공격 도구 없이 특정 IP의 서버가 열려있는지 확인한 뒤 해당 취약점이 존재하는 웹 서버의 응답일 경우, '\' (%5c)를 추가로 입력하여 사용자의 계정과 비밀번호를 탈취한다.

해킹 프로그램의 실행 화면은 Fig. 2와 같다. 천리안(千里眼)이라는 이름으로 중국에서 개발되어 인터넷에서 유통되고 있다. 이 프로그램에서 1번 항목은 포트 스캔할 시작 IP 주소와 끝 IP 주소를 지정하고, 2번 항목에서 포트 스캔 간격 시간, 포트 스캔 횟수, 포트 번호를 입력하고, 3번 항목에서 공격에 성공할 경우 IP 주소, 포트 번호, 사용자 계정과 비밀번호, 웹 서버, IP 카메라 UID를 리스트로 보여준다.

천리안 해킹 프로그램이 동작할 때 네트워크 통신을 모니터링하는 wireshark 프로그램으로 패킷을 캡처한 내용은 Fig. 3, 4와 같다. 포트 스캔할 시작 IP 주소부터 끝 IP 주소까지 각 IP 주소에 서버가 동작하고 있는지 확인하고, 동작하는 서버가 만약 GoAhead 웹 서버라면 '희생자 IP/%5clogin.cgi'으로 요청하여 취약점을 공격한다. 공격에 성공하면 이에 대한 응답으로 어떠한 인증도 수행하지 않고 사용자 계정과 비밀번호를 회신한다.

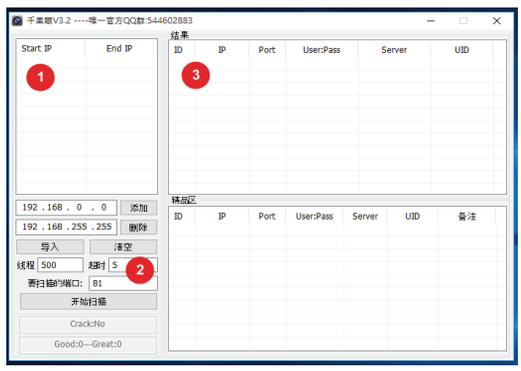

Fig. 2. Start Screen in '千里眼' Hacking Program

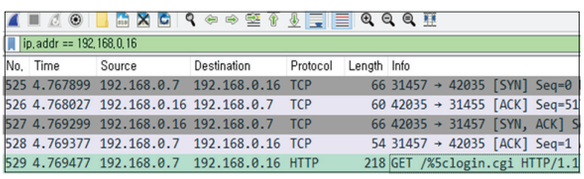

Fig. 3. Record of Attacks by Entering '/%5clogin.cgi'

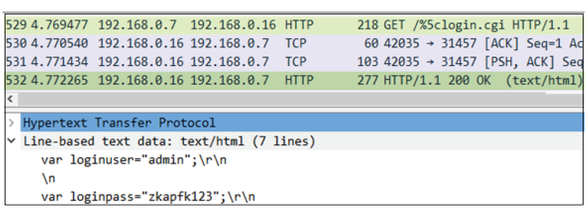

Fig. 4. Content Returned from IP Camera Server

Fig. 5. Partial Contents of the Text File Created After Hacking

천리안 해킹 프로그램을 실행하고 종료하면 IP 주소와 포트, 사용자 계정과 비밀번호, 웹 서버, IP 카메라 UID를 정리한 텍스트 파일이 생성된다. Fig. 5에서 보는 바와 같이 GoAhead 웹 서버를 사용하는 IP 카메라는 'ohdy070201', 'dbfl864100', 'ok0609!!'와 같은 어려운 비밀번호임에도 해킹에 성공한다. 웹 서버 취약점으로 인한 해킹과 더불어 취약한 계정 설정으로 인한 비밀번호 '888888', '88888888', 'admin'도 쉽게 노출된다. 이 정보를 가지고 IP 카메라에 무단 접속하는 것이다.

2) CVE-2017-5674

GoAhead 웹 서버에서 취약점(CVE-2017-5674)도 발견되었다[15]. 이 취약점은 사용자 비밀번호가 저장된 system.ini 파일을 GET 방식으로 요청할 때 경로에 '/'를 제거하고 요청하면 인증 없이 파일을 다운로드하는 것이다. CVE-2002-2427와 마찬가지로 GoAhead 웹 서버의 security handler가 인증하지 않고 데이터에 접근하여 문제가 발생한다.

현재 판매되고 있는 GoAhead 웹 서버를 사용하는 IP 카메라에 기존에 알려진 CVE-2002-2427, CVE-2017 -5674 취약점은 존재하지 않는다. 하지만 두 개의 취약점을 혼합하여 공격한 결과 사용자 비밀번호가 저장된 파일을 다운로드할 수 있다.

Fig. 6에서 보는 바와 같이 정상적인 코드가 수행된다면 계정과 비밀번호가 필요한 경우 인증을 요구하고, 인증이 되지 않으면 HTTP 401 Unauthorized 에러로 데이터를 회신하지 않는다. 인증이 필요한 경우 --uesr 및 --password 옵션을 추가하여 요청해야 한다. 계정과 비밀번호 모두 일치해야 데이터를 회신하며, 하나라도 틀리면 데이터를 회신하지 않는다.

Fig. 7은 CVE-2002-2427, CVE-2017-5674를 혼합한 공격 방법으로 사용자 비밀번호가 저장된 system.ini 파일을 요청할 때 URL에 '\' (%5c)를 추가하여 요청할 경우 별도의 인증을 요구하지 않고 데이터가 회신되는 것을 보여준다. Fig. 8처럼 다운로드받은 system.ini 파일을 hex 뷰어로 보면 사용자 비밀번호를 알아낼 수 있다. 이와 같은 방식으로 천리안 해킹 프로그램을 일부 수정하면 현재 판매되는 IP 카메라도 손쉽게 비밀번호를 탈취할 수 있다.

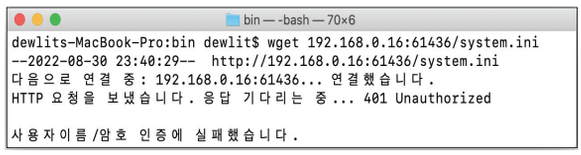

Fig. 6. Authentication Fails with a Normal Request

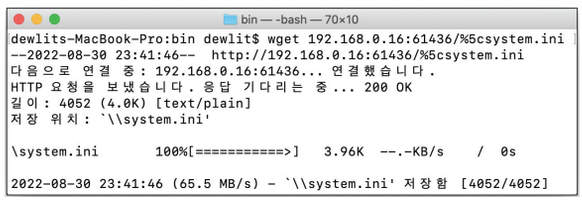

Fig. 7. Result for Abnormal Request by Appending %5c

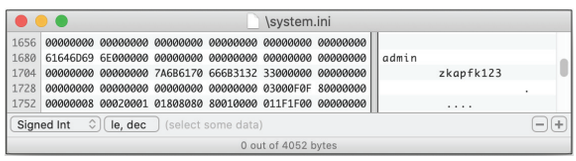

Fig. 8. Expose User Password in Leaked system.ini File

3.4 웹 서버 취약점 발생 원인 및 해결 방법

GoAhead 웹 서버에 취약점 CVE-2002-2427, CVE-2017-5674이 존재하는 원인은 GoAhead 웹 서버 코드를 분석해보면 찾을 수 있다. GoAhead 웹 서버는 오픈 소스로 코드가 공개되어 있으며, 취약점이 존재하는 2.1 버전으로 코드를 분석하였다. Fig. 9는 GoAhead 웹 서버에 접속했을 때 동작하는 Flowchart이며, Table 1은 함수별 기능에 대한 설명이다.

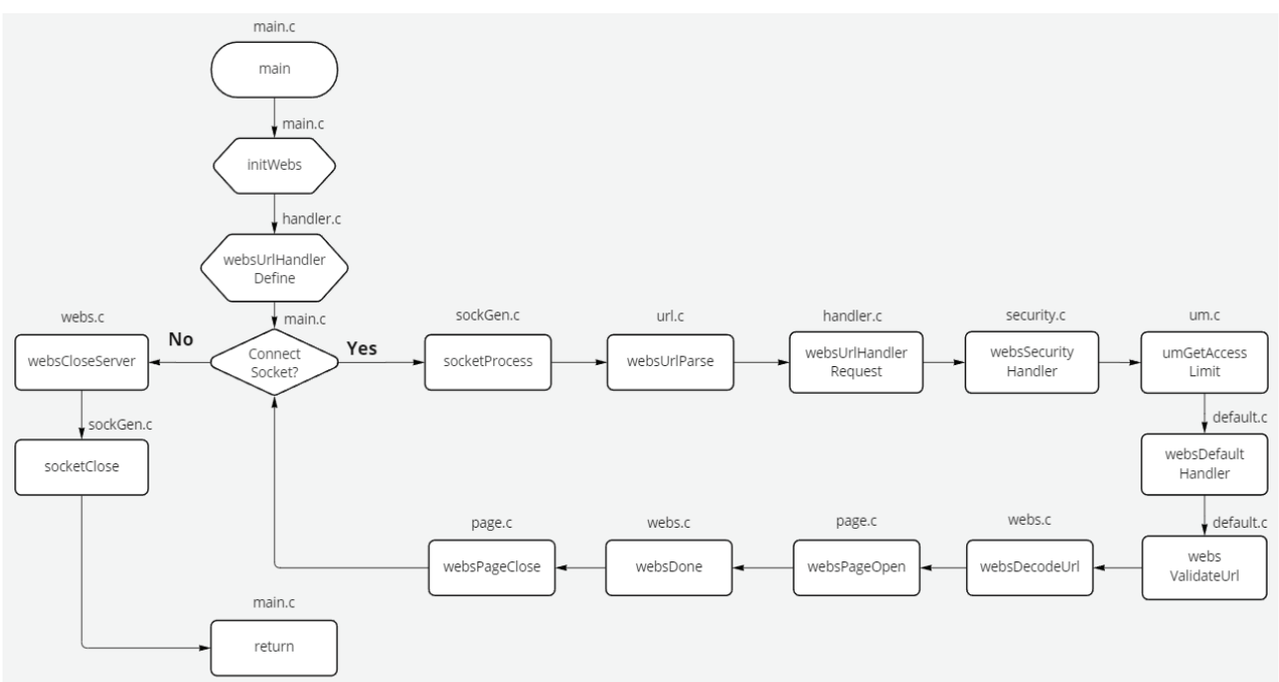

Fig. 9. Flowchart with GoAhead Web Server Running

Table 1. Description of GoAhead Web Server Function

Function	Description
initWebs	Initialize web server program
websUrlHandlerDefine	Set handler for each web page URL path
Connect Socket	Program main infinite loop, waiting for socket to be connected
socketProcess	Run socket process
websUrlParse	Parse URL (host, path, port, method, etc)
websUrlHandlerRequest	Request handler set in URL
websSecurityHandler	Security (authentication) handler that is called first among handlers
umGetAccessLimit	Check if the page is accessible to the user as one of the User Management functions
websDefaultHandler	Handler called by default
websValidateUrl	Validate URL
websDecodeUrl	Decode %nn string
websPageOpen	Open file requested by URL
websDone	Terminate http request
websPageClose	Close file requested by URL
websCloseServer	Clear web server program memory, prepare to exit
socketClose	Clear socket connection

먼저 웹 서버 프로그램을 시작하기 위해 초기화 작업을 하고 메인 무한 루프가 진행된다. 이후 웹 브라우저 기반 뷰어 프로그램에 사용자가 접속하면 security handler가 수행되면서 인증을 진행한다. 그다음 default handler가 동작하여 IP 카메라의 실시간 영상을 볼 수 있는 웹 페이지를 열어 영상을 볼 수 있게 한다.

웹 서버가 동작하는 과정에서 취약점이 존재하는 원인은 '\' (%5c)가 입력되었을 때 예외 처리되지 않은 두 가지이다.

먼저 인증을 요구하지 않은 경우이다. 이는 websSecurity Handler 함수에서 umGetAccessLimit을 호출하여 User가 접근할 수 있는 페이지인지 검사하는 기능이 있다. 하지만 '\' (%5c)를 에러 처리하지 않아 security handler가 비정상적으로 종료되고, 이후 인증을 요구하는 코드가 실행되지 않는 것이다.

다음 '\' (%5c)을 포함한 요청이 왔을 때 서버에 존재하지 않는 페이지 또는 파일에 대한 접근으로 HTTP 404 Not Found 에러를 처리하지 않는 것이다. 이는 webs Default Handler 함수에서 websDecodeUrl를 호출하여 요청한 URL에 '%nn' 형식의 URL 인코딩을 디코드하는 기능이 있다. 디코드한 URL에 '\' (%5c)가 포함되면 에러 처리하여야 한다. 그러나 에러 처리 코드가 없어 '\' (%5c)를 무시하고 요청한 페이지를 보여준다.

4. IP 카메라 보안 위험 완화 및 사고 대응 전략

4.1 보안 내재화를 통한 보완

보안 내재화(Security by design)란 서비스 요구사항 분석 및 설계 단계에서부터 꼭 필요한 기능들만 선별해 제품에 내재화하는 것으로, IoT 장치의 소프트웨어 업데이트 및 패치가 쉽지 않아 제품을 개발할 때 추가되어야 할 기능을 정하는 것이다[16]. IP 카메라 사용자들도 소프트웨어를 최신 버전으로 업데이트하는 비율은 42.4%에 그쳐[9] 제품 개발 당시 보안 내재화가 중요하다.

IP 카메라 보안 내재화가 필요한 또 다른 이유는 IP 카메라 해킹 사건의 특징이다. 이것은 피해자들이 피해 사실을 인식하지 못하여 스스로 신고하는 경우가 드문 것이다. 그로 인해 범행 지속 시기가 길어져 다수의 사생활 영상이 유출된다. 이에 대한 IP 카메라 보안 내재화 방안으로 스마트폰 알림 기능 활용이 있다. 금융 애플리케이션에서 입출금 기록이 발생하면 스마트폰에서 알림 기능으로 알려주는 것처럼 누군가 IP 카메라에 접속하면 뷰어 애플리케이션에서 알림이 오도록 기능을 추가하면 된다. 접속 기록 저장 기능은 발생한 해킹 피해를 조사하고 후속 피해를 막는 데 도움을 주는 것에 비하여 알림 기능은 피해 사실을 즉각적으로 알아차릴 수 있게 해준다. 알림 기능이 추가된 제품을 사용하면 피해 발생 시 기기 전원을 끄거나 카메라 화면을 가리고 수사기관에 신고할 수 있어 보다 빠른 대처를 할 수 있다.

4.2 포렌식 내재화를 통한 보완

포렌식 내재화(Forensic by design)란 디지털 포렌식 준비도 관점에서 새로운 패러다임이며, 보안 내재화와 유사하지만 'forensic-ready' 시스템을 얻기 위해 시스템의 설계 및 개발 단계에서 추가되어야 할 기능을 정하는 것이다[17]. 해킹 피해를 본 IP 카메라를 포렌식하여 분석해 본 결과, 기기 정보나 카메라 설정 값만 확인될 뿐, 범인의 침입 흔적을 찾을만한 데이터가 없었다.

IP 카메라 포렌식 내재화가 필요한 이유 중 하나는 IP 카메라 해킹 사건이 발생하였다면 더 이상 영상이 유출되지 않도록 대응하는 것도 중요하지만, 범인을 검거하여 또 다른 피해자들이 발생하지 않는 것도 중요하다. 해킹당한 IP 카메라를 분석하여 범인을 추적하기 위한 포렌식 내재화 방안으로 IP 카메라에 접속 기록을 저장하는 기능을 추가하면 된다. 접속 기록이 있다면 외부 침입 흔적을 쉽게 발견할 수 있다. 일부 제품에서는 접속 기록을 남기는 기능이 있으나 대부분의 IP 카메라에서는 접속 기록을 관리하지 않는다. 접속 기록을 남긴다고 해서 IP 카메라에 접속하는 시간이 현저하게 느려진다거나 저장 공간이 막대하게 필요하지 않음에도 대부분의 IP 카메라는 해당 기능을 제공하지 않는다.

IP 카메라 보안 및 포렌식 내재화 방안을 정리하면 Fig.

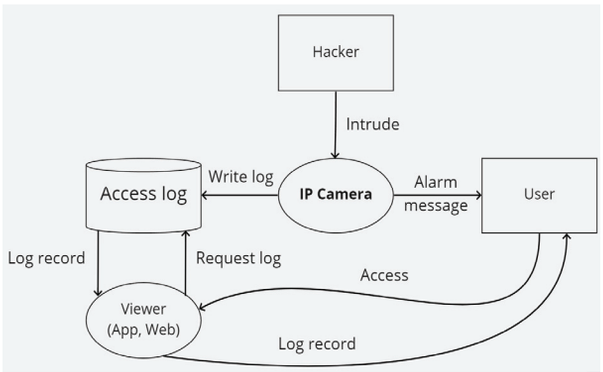

Fig. 10. Security and Forensic by Design for IP Cameras

10과 같다. 먼저 보안 내재화 측면에서 IP 카메라에 누군가 침입할 경우 뷰어 애플리케이션을 통해 알림 메시지를 전달한다. 이 알림 기능만 있다면 해킹 피해가 발생했을 때 즉시 알아차릴 수 있다. 다음 포렌식 내재화 측면에서는 IP 카메라에 접속 시도나 성공 기록을 로그에 저장한다. 그리고 사용자는 뷰어 프로그램을 통해 로그 기록을 확인하여 비정상적인 접근이 있었는지 확인한다. 이를 통해 해킹 피해가 발생하였더라도 범인을 추적할 단서를 찾을 수 있다.

5. 결 론

본 논문에서는 IP 카메라 보안의 특징을 알아보았고, 그 중 뷰어 프로그램의 보안 문제점과 관련된 해킹 가능성을 확인하였다. 이를 바탕으로 해킹 사건 사례에서 수집한 데이터와 해킹 프로그램을 기반으로 해킹 피해가 발생한 원인을 분석하였다. 뷰어 프로그램의 취약점을 이용한 해킹 프로그램은 IP 대역만 설정하여 실행하면 취약점이 있는 IP 카메라의 IP 주소, 포트, 사용자 계정과 비밀번호, 웹 서버, IP 카메라 UID를 정리한 텍스트 파일이 생성된다. 이를 이용해 피해자들의 IP 카메라에 무단 접속하여 사생활 장면을 불법 촬영한다. 뷰어 프로그램의 취약점이 발생한 원인은 특정 문자열을 입력하였을 때 예외 처리가 되지 않아 문제가 발생하였고, 이에 대한 해결 방법은 오픈 소스 코드 분석을 통해 확인하였다.

그리고 IP 카메라 해킹 사건이 발생하더라도 피해 사실을 즉각 알아차리기 위한 보안 내재화 방안으로 접속 알림 기능을 제안하였다. 이 기능이 없다면 피해자들은 해킹 피해 사실을 알아차리기 어려워 계속하여 사생활이 노출될 수 있다. 또한, 범인을 검거하기 위한 포렌식 내재화 방안으로 접속 기록 저장 기능을 제안하였다. 이 기능을 통해 적어도 범인이 언제, 어디서 피해자의 IP 카메라에 접속했는지 확인할 수 있고, 이를 통해 범인을 추적할 수 있다. 이와 같은 기능이 추가된 제품을 사용하면 해킹으로부터 안전할 수 있다.

IP 카메라 제조사들은 본 논문에서 연구한 결과를 바탕으로 취약점 때문에 해킹이 발생할 수 있는 사실을 인지하여야 한다. 그래서 제품에 들어가는 소프트웨어의 알려진 취약점을 분석하고 해당 취약점이 없는지 테스트하고 제품을 만들어야 한다. 제조사뿐만 아니라 한국정보통신기술협회와 같은 인증 기관에서도 취약점을 테스트하는 케이스를 추가하여 인증을 부여해야 한다.

본 논문에서 진행한 연구 과정과 결과를 보면 취약점이 존재하는 웹 서버와 같은 소프트웨어가 IP 카메라 같은 IoT 제품에서 사용될 경우 발생할 수 있는 문제점을 확인하였다. 취약점이 발견된 지 오래되었음에도 지금까지도 문제가 될 수 있고, 패치가 정상적으로 되지 않을 수도 있음을 확인하였다. 또한, IP 카메라 사용자들은 어떤 방법으로 해킹 피해를 보는지, 자신들이 사용하는 제품은 문제가 없는지 확인할 수 있다.

이번 논문에서는 GoAhead 웹 서버의 취약점 중에서 간단하면서도 결정적인 취약점에 대해 분석하였다. IP 카메라에 사용되는 웹 서버는 다양하고, 취약점 또한 많으며, 앞으로도 발견될 수 있을 것이다. 이 논문에서 분석한 방식으로 다른 취약점 또한 분석하여 그에 대한 원인과 해결 방법을 마련할 수 있을 것이다.

References

[1] M. Horowitz, “2022 Cyber Security Report,” Check Point Software Technologies, pp 34-38, 2002.

[2] J. Park and S. Kim, “Security requirements analysis on IP camera via threat modeling and common criteria,” *KIPS Transactions on Computer and Communication Systems*, Vol.6, No.3, pp.121-134, 2017.

[3] M. Kim, “Privacy protection technologies on IoT environments: Case study of networked cameras,” *The Journal of the Korea Contents Association*, Vol.16, No.9, pp.329-338, 2016.

[4] L. Costa, J. Barros, and M. Tavares, “Vulnerabilities in IoT devices for smart home environment,” in *Proceedings of the 5th International Conference on Information Systems Security and Privacy*, Portugal, pp.615-622, 2019.

[5] J. P. Singh and A. Chauhan, “Detection and prevention of non-PC botnets,” CIISE, Concordia University, Montreal, Quebec, Canada, 2017.

[6] R. Alshalawi and T. Alghamdi, “Forensic tool for wireless surveillance camera,” *19th International Conference on Advanced Communication Technology*, PyeongChang, pp.536-540, 2017.

[7] S. Li, K. K. R. Choo, Q. Sun, W. J. Buchanan, and J. Cao, “IoT forensics: Amazon echo as a use case,” *IEEE Internet of Things Journal*, Vol.6, No.4, pp.6487-6497, 2019.

[8] I. Sutherland, E. D. Martin, and J. Kargaard, "IoT security and forensics: A case study," *20th European Conference on Cyber Warfare and Security*, pp.278, 2021.
[9] "2021 Survey on information security," Ministry of Science and ICT, 2022.
[10] K. Tamiya et al., "Dangers of IP Camera-An Observational Study on Peeping," Journal of Information Processing, vol. 28, pp.502-510, 2020.
[11] B. Cusack and Z. Tian, "Evaluating IP surveillance camera vulnerabilities," *The Proceedings of 15th Australian Information Security Management Conference*, Perth, pp.25-32, 2017.
[12] G. Kang, S. Han, and H. Lee, "Security problems and measures for IP cameras in the environment of IoT," *Journal of The Korea Society of Computer and Information*, Vol.24, No.1, pp.107-113, 2019.
[13] M. S. Aslan, IP camera default password list [Internet], https://www.nvripc.com/ip-camera-default-password-list-2021.
[14] CVE-2002-2427: National vulnerability database [Internet], https://nvd.nist.gov/vuln/detail/CVE-2002-2427.
[15] CVE-2017-5674: National vulnerability database [Internet], https://nvd.nist.gov/vuln/detail/CVE-2017-5674.
[16] S. Jeong, Y. Choi, and I. Lee, "Cyber killchain based security policy utilizing hash for internet of things," *Journal of Digital Convergence*, Vol.16, No.9, pp.179-185, 2018.
[17] A. Akilal and M. T. Kechadi, "An improved forensic-by-design framework for cloud computing with systems engineering standard compliance," *Forensic Science International: Digital Investigation*, Vol.40, 2022.

신 승 진

https://orcid.org/0009-0000-7117-5834
e-mail : dewlit@icloud.com
2014년 한성대학교 컴퓨터공학과(학사)
2020년 ~ 현 재 경기남부청 사이버수사과 디지털포렌식계 분석관
2021년 ~ 현 재 고려대학교 정보보호대학원 디지털포렌식학과 석사과정
관심분야 : Digital Forensics, IoT Forensics

박 정 흠

https://orcid.org/0000-0001-7796-7699
e-mail : jungheumpark@korea.ac.kr
2014년 고려대학교 정보보호대학원(박사)
2014년 ~ 2019년 미국 국립표준기술연구원 방문연구원
2021년 ~ 현 재 고려대학교 정보보호대학원 조교수
관심분야 : Digital Forensics, Cybercrime Response

이 상 진

https://orcid.org/0000-0002-6809-5179
e-mail : sangjin@korea.ac.kr
1994년 고려대학교 수학과(박사)
1989년 ~ 1999년 ETRI 선임연구원
1999년 ~ 현 재 고려대학교 정보보호대학원 교수
2008년 ~ 현 재 고려대학교 디지털포렌식연구센터 센터장
2017년 ~ 현 재 고려대학교 정보보호대학원 원장
관심분야 : Digital Forensics, Cryptanalysis, Steganography