https://doi.org/10.33778/kcsa.2024.24.3.143

IP 카메라의 보안 취약점과 보안성 강화에 관한 연구

김 량 래*, 조 승 현*, 김 지 윤**

요 약

IP 카메라는 사용자의 위치와 상관없이 실시간으로 영상을 시청할 수 있다. 이러한 장점으로 가정에서는 영유아, 반려동물, 노인의 상태 등을 모니터링하는데 사용되고, 기업에서는 데이터센터나 창고와 같이 보안 구역의 물리적 보안 통제 및 감시의 목적으로 널리 사용되고 있다. 그러나 적절한 보안기술이 적용되지 않은 IP 카메라는 악의적인 공격자에 의해 영상 정보를 감청당할 수 있다. 본 연구에서 무차별 대입 공격과 같이 IP 카메라의 여러 가지 보안 취약점을 가지고 해킹 공격이 수행 가능함을 보인다. 이에 따라 IP 카메라의 취약점에 대응하는 아키텍처를 제시하여 IP 카메라의 보안성을 강화하기 위해 할 수 있는 방안을 제안하고 보안성 검증 및 가용성 평가를 통해 제안 기법이 안전하고 효과적으로 IP 카메라의 영상 정보 암호화와 사용자 인증을 제공할 수 있음을 보였다.

A Study on Security Vulnerability and Enhancement for IP Camera

Ryang Rae Kim*, Seoung Hyeon Jo*, Jiyoon Kim**

ABSTRACT

IP cameras allow users to view live video regardless of their location. Due to this advantage, they are used in homes to monitor infants, pets, and the elderly, and they are widely utilized in companies for physical security control and monitoring of secure areas, such as data centers and warehouses. However, IP cameras that lack appropriate security measures can be eavesdropped on by malicious attackers. This study demonstrates that hacking attacks can be executed by exploiting various security vulnerabilities in IP cameras, including brute force attacks. Accordingly, we propose an architecture that addresses these vulnerabilities, suggesting measures to enhance the security of IP cameras. Also, we shows that the proposed method can safely and effectively provide video information encryption and user authentication for IP cameras through security verification and availability evaluation.

Key words : IP Camera, Information Security, End-to-End Protection

접수일(2024년 08월 12일), 게재확정일(2024년 09월 02일)

* 경상국립대학교 컴퓨터공학과 학부과정

** 경상국립대학교 컴퓨터공학과 조교수(교신저자)

1. 서 론

폐쇄 회로 텔레비전(Closed-circuit Television, CCTV)은 시설 안전 및 보안 목적으로 설치되는 영상 기록 장치다. CCTV는 녹화 기록을 열람하고 반출하기 위해서는 녹화 저장 장치에 물리적으로 접근해야만 가능하다는 특징이 있다. 이는 CCTV를 물리적으로 폐쇄된 환경에 두어 기록의 신뢰성과 안정성을 높이기도 하지만, 접근성과 편의성 측면에서 그 효용이 떨어진다. CCTV의 낮은 접근성 문제를 개선하기 위해, 인터넷 스트리밍을 통해 녹화된 영상을 실시간으로 시청할 수 있는 IP(Internet Protocol) 카메라가 개발되었다. IP 카메라는 사용자의 위치와 관계없이 인터넷에 접근이 가능한 환경이라면 어디서든 실시간으로 영상을 시청할 수 있다는 장점이 있다. 이러한 장점으로 가족 구성원이나 반려동물의 상태 확인 등에 활용되고 있다. 가정용 IP 카메라는 민감 정보인 개인의 사생활을 녹화하고 이를 공개된 인터넷을 통해 전송한다. 따라서 복잡한 비밀번호를 사용하고 암호화된 통신 프로토콜을 도입하여 보안 사고 대응에 각별한 주의를 기울일 필요가 있다. 하지만 이런 노력에도 불구하고, IP 카메라의 대중화와 적절한 보안기술이 적용되지 않아 보안 사고가 끊임없이 발생하고 있으며 [1-8], 그중 인세캠 사건과 같이 전 세계적 규모의 민감 정보 유출 사고가 발생하기도 하였다. 이러한 상황에서 IP 카메라의 영상 정보가 유출되는 경우 사생활 침해를 넘어 기밀 정보 유출, 환자 정보 유출 등 광범위한 피해가 발생할 수 있다. 보안 사고에 대응하기 위해 주기적으로 관리자 계정의 아이디와 비밀번호를 복잡하게 설정하고 주기적으로 변경하는 등의 보안 대책도 중요하지만, 근본적으로 IP 카메라 시스템의 취약점에 대한 대비가 필요하다. 특히, IP 카메라의 영상을 원격지에서 스트리밍할 수 있게 매개하는 중간 서버나 통신 구간의 취약점으로 인해 보안 사고가 발생할 수 있다 [3]. 신뢰할 수 없는 통신 구간을 거쳐 전달되는 경우 IP 카메라는 스니핑(Sniffing), 스푸핑(Spoofing) 공격에 취약하다. IP 카메라를 비롯한 IoT 기기의 보안 문제를 개선하기 위해, 제조사에서는 HTTPS와 같은 암호화된 통신 프로토콜을 도입하고 있다 [7]. HTTPS 연결은 서버와 클라이언트 간의 안전한 통신 환경을 생성하지만, 중간 서버의 데이터가 유출되거나 백도어 등의 악의적인 공격에는 대응할 수 없다.

종단 간 암호화(end-to-end encryption)는 중요한 데이터가 신뢰할 수 없는 통신 구간을 거쳐야 하는 경우 데이터를 안전하게 전송시킬 수 있는 기법 중 하나이다. 종단 간 암호화는 HTTPS와 같이 송수신자 간의 안전한 통신 환경을 보장한다. 또한 악의적인 공격자에 의해 전송 중이던 데이터가 유출되는 경우에도 원본 데이터의 내용이 암호화되어 있기 때문에 공격자는 유출된 데이터의 내용을 확인하기 어렵다. 종단 간 암호화의 주요 과제는 상호 간의 신원이 파악되지 않은 최초 연결 수립 상황에서 인증 과정을 거쳐 데이터를 안전하게 암호화하는 것이다. 본 연구에서는 사용자와 IP 카메라 간의 인증을 수행하고 대칭키를 통해 IP 카메라의 영상 정보를 종단 간 암호화한다. 암호화한 영상 정보는 HTTPS를 통해 사용자에게 전송하는 기법을 제안한다.

또한 문헌 조사 및 테스트베드 환경에 기반하여 기존 IP 카메라의 잠재적 보안 취약점을 유형별로 파악한다. 파악한 취약점을 분석하여 사전 공격 및 무차별 대입 공격에 대응하기 위해 인증 시간 제한과 CAPTCHA와 HTTPS의 중간자 공격에 대응하기 위해 인증서 인증기관(Certificate Authority, CA)에서 발급한 인증서를 적용하여 안전한 IP 카메라 모델을 구현하고자 한다. 종단 간 암호화를 비롯하여 각 유형별 보안 취약점에 대응할 수 있는 해결 방안을 제시한다. 마지막으로, 보안성 평가 및 가용성 평가를 통해 제시하는 해결 방안의 실용성을 검토하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 IP 카메라의 보안 취약점을 소개하고, 3장에서는 본 연구에서 제안하는 기법을 제안한다. 4장에서 제안하는 기법을 평가하고, 5장에서 결론을 소개하고자 한다.

2. 선행 연구 및 문헌 조사

본 연구에서는 IP 카메라의 취약점을 유형별로 분류하기 위한 선행 연구 및 문헌 조사를 진행하였으며, 테스트베드 환경에서의 실증을 진행하였다.

2.1 관련 연구

[1]에서는 IP 카메라 보안 취약점을 네트워크와 취약점의 두 분류로 나누어 조사하였으며 VPN 기능에 해당하는 침입에 대한 방지 기능, DDoS 공격 탐지 기법, 계정과 비밀번호의 복잡성을 높이는 등의 대응 방안을 제안하였다. [2]에서는 반송정수장의 암호화되지 않은 CCTV망에서 L2/L3 구간에서의 해킹 위협을 분석하였다. Access 구간의 L2 스위치를 보안 스위치로 교체하고, 비인가 IP/MAC 접근을 차단하고 트래픽 흐름을 실시간 수집하여 보안성을 개선하였다. [3]에서는 월패드(Wall Pad) 해킹 사생활 유출 사건 등 IoT 기기의 해킹 사건을 조사하였으며, 데이터 유출 방지를 위해 암호화를 도입하고, 주기적 업데이트를 진행하며 엄격한 인증 절차를 추가해야 함을 보였다. [4]에서는 QCAM3000, LG-LW130W IP 카메라 제품을 대상으로 사전 공격을 진행하였으며, 주기적으로 패스워드와 계정을 변경하고 복잡성이 높은 암호를 사용하며, MAC 주소 필터링과 기본 포트 변경 등의 대응책을 제안하였다. [5]에서는 MAC 주소, IP 주소, 전자서명을 이용한 IP 카메라의 진위 여부를 판단하기 위한 기술을 분석하고, IP 카메라의 시그니처와 IP 주소, MAC 주소 등을 이용한 주기적 진위 여부 판단 시스템을 제안하였다. [6]에서는 TLS 통신 환경에서 발생 가능한 주요 취약점을 정리하고, 라즈베리파이4 기반 테스트 환경에서 TLS 1.2와 TLS 1.3의 Handshake 처리 속도 비교를 진행하였다. 그 결과 TLS 1.3이 1.2 대비 약 40% 향상된 Handshake 처리 속도를 보였으며 테스트 환경과 유사한 IoT 기기에는 가급적 TLS 1.3을 도입할 것을 제안하였다.

선행 연구 조사 결과 IP 카메라와 같은 IoT 장치들의 해킹 시도는 빈번하게 발생하고 있으며, 공격 유형은 사전 공격, 무차별 대입 공격, DoS 공격, 펌웨어와 프레임워크 취약점을 이용한 공격, 암호화되지 않은 데이터의 중간 탈취 공격이 주를 이루고 있었다.

2.2 IP 카메라 취약점

2.2.1 쇼단 검색 엔진(Shodan Search Engine)을 이용한 IP 카메라 검색

쇼단은 사물인터넷 검색 엔진으로서 인터넷이 연결되어 있는 사물인터넷 기기를 검색하여 장치의 정보와 IP 주소, 열려진 포트 등의 검색 결과를 보여준다. 검색 결과의 IP주소와 포트를 이용하여 IP카메라의 관리도구 웹 페이지, 실시간 스트리밍 프로토콜(Real Time Streaming Protocol, RTSP)에 접속할 수 있다. 이때 IP 카메라가 제조 시 설정된 기본 비밀번호를 사용하거나 'admin' 과 같이 시스템에서 자주 사용되는 접속 정보를 입력하면 영상 정보를 시청할 수 있다 [9].

2.2.2 접속 정보 탈취

접속 정보 탈취는 무차별 대입 공격(brute force attack), 사전 공격 (dictionary attack) 등 여러 유형의 공격을 통해 아이디와 비밀번호를 알아내는 공격 기법이다. 테스트베드 환경에서 RTSP 프로토콜 기반 IP 카메라의 접속 정보를 쉬운 아이디와 비밀번호로 설정하고 사전 공격을 시도하였다. 공격 프로그램을 실행한 후 몇 분 뒤 접속정보를 찾는데 성공하였다. 이에 따라, 무차별 대입 공격과 사전 공격은 가능한 모든 조합을 시도하는 간단한 형태의 공격이지만 계정 정보를 주기적으로 변경하지 않거나 짧은 길이의 암호를 사용하는 경우 이 공격에 취약하다. 그리고 복잡한 암호를 사용하더라도 IP카메라는 최대 로그인 시도 횟수 제한과 같은 보안 기능 등을 포함하여야 한다.

2.2.3 펌웨어 취약점

IP 카메라의 펌웨어 내에 취약점을 이용하여 공격을 진행할 수 있다. CVE-2020-7879에 따르면 IP카메라와 네트워크 결합 스토리지 (Network Attached Storage, NAS) 서버와 연동할 때 NAS 에서 보낸 setCookie('[COOKIE']) 문자열을 파싱하여 사용한다. 파싱한 문자열은 쿠키 값에 대한 검증 없이 NAS로 wget의 header 옵션으로 데이터 전송하여 명령 삽입

취약점이 발생한다 [9].

2.3 보안성 강화 방법

도출한 취약점에 대한 보안성 강화를 위해 다양한 기법을 조사하였다.

2.3.1 HTTP Over TLS

하이퍼텍스트 전송 프로토콜 보안(Hypertext Transfer Protocol Secure, HTTPS)는 인터넷 상에서의 안전한 통신을 위한 하이퍼텍스트 전송 프로토콜(HTTP)이다. HTTPS는 전송 계층 보안(Transport Layer Security, TLS) 프로토콜에 의존하여 클라이언트와 서버 간에 전송되는 데이터를 암호화함으로써 데이터의 무결성, 기밀성, 인증을 보장한다 [10].

TLS를 통해 HTTPS가 안전하게 동작하려면 인증서 인증 기관 (Certificate Authority, CA)에서 발급한 인증서를 사용하여야 한다. CA 인증서는 클라이언트에서 서버로 접속할 때 신뢰할 수 있는지를 증명하며 중간자 공격 (Man-In-The-Middle, MITM)을 방지하는데 효과적이다.

2.3.2 CAPTCHA

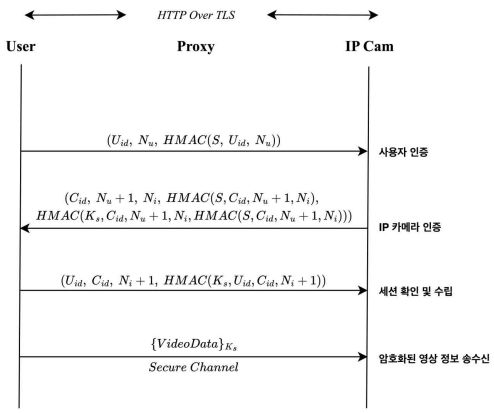
CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)는 인간과 컴퓨터를 구별하기 위해 사용되는 자동화 테스트이다. CAPTCHA는 왜곡된 문자나 숫자가 기재된 이미지를 사용자가 입력함으로써 애플리케이션에 봇의 접근을 차단하여 자동화된 공격을 방지하는데 사용된다 [11].

2.3.3 해시 기반 메시지 인증 코드

해시 기반 메시지 인증 코드(Hash-based Message Authentication Code, HMAC)는 메시지의 무결성과 인증을 보장하기 위해 해시 함수를 사용하는 알고리즘이다. HMAC은 메시지 인증 코드(Message Authentication Code, MAC)에 해시 함수를 적용시킨 것으로 해시 함수는 원본 데이터가 조금이라도 변하면 완전히 다른 결과값을 반환하기 때문에 메시지의 변조 여부를 쉽게 판단할 수 있다. HMAC 알고리즘은 상호 간 사전 공유된 비밀 키를 필요로 한다 [12].

3. 제안 기법 (CamSec)

본 연구에서는 중간자 공격, 무차별 대입 공격 등의 IP 카메라 취약점에 대응하기 위해 HMAC과 HTTPS을 통해 안전한 정보 송수신 기법인 CamSec을 제안한다. 제안하는 기법은 정형화 검증 도구인 Scyther를 통해 보안성 검증을 진행하였으며, 테스트베드 환경에서의 성능 평가를 진행하였다.



(그림 1) 제안 기법 다이어그램

3.1 암호화를 위한 정보

데이터 전송 절차의 무결성과 각 메시지의 무결성을 검증하며, 암호화된 데이터 전송을 위해 다음과 같이 정의하였다.

3.1.1 IP 카메라 일련번호

IP 카메라가 출고 시 생성되는 고유 식별자이다. 장치 일련번호는 IP 카메라 하드웨어에 종속되며 폐기될 때까지 동일한 일련번호를 사용한다. 사용자는 IP 카메라 장치에 기재된 일련번호를 IP 카메라 영상 뷰어 프로그램에 입력하여 사용하며 IP 카메라는 카메라 설정 정보를 통해 일련번호를 가져와 사용할 수 있다.

3.1.2 IP 카메라 ID

IP 카메라의 최초 설치 기능을 통해 랜덤하게 생성되는 UUID(Universally Unique Identifier) 형식의 고유 식별자이다. 장치 ID는 소프트웨어 기반으로 관리되며 장치 초기화 이후, IP 카메라 최초 설치 기능을 통해 다시 생성하면 이전 장치 ID와 다르게 생성된다.

3.1.3 사용자 ID

IP 카메라 영상 뷰어 프로그램을 통해 장치 등록 시 랜덤하게 생성되는 UUID(Universally Unique Identifier) 형식의 고유 식별자이다. 사용자 ID는 소프트웨어 기반으로 관리되며 IP 카메라 영상 뷰어 프로그램에서 장치 등록을 다시 진행하는 경우 이전 사용자 ID와 다르게 생성되고 프로그램을 삭제하는 경우 이전 사용자 ID는 폐기된다.

3.1.4 Nonce

사용자와 IP 카메라 간 통신 시 사용되는 요청/응답 메시지의 고유 식별자이다. Nonce를 생성할 때에는 난수를 추측하거나 역추적할 수 없도록 하드웨어 정보, 시간 등 다양한 요소를 기반으로 시드 값을 설정하여 랜덤 값을 생성한다. 사용자와 IP 카메라 간 통신할 때 Nonce 값을 포함하여 각 메시지의 유효성을 검증하기 위해 사용한다. 요청을 보낼 때마다 Nonce 값을 변경하여 전송하고 수신자는 값을 검증함으로써 재전송 공격을 방지할 수 있다.

3.1.5 영상 정보 암/복호화 대칭키

영상 정보 암/복호화 대칭키는 IP 카메라-프록시-사용자 간의 영상 정보를 안전하게 송수신하기 위해 사용되는 대칭키이다. IP 카메라는 영상을 캡처하여 대칭키 암호화를 한다. 암호화된 영상 정보는 프록시 서버를 통해 사용자에게 전달되며, 사용자는 동일한 대칭키를 사용하여 복호화함으로써 원본 영상을 확인할 수 있다.

3.2 제안 기법의 알고리즘

제안하는 기법은 사용자 인증, IP 카메라 인증, 세션 확인 및 수립, 영상 정보 암/복호화로 구성된 4개의 과정으로 진행되며, 각 과정의 세부 절차는 아래와 같다. 제안하는 기법에서 사용된 기호는 <표 1>과 같다.

<표 1> 기호표

기호	의미
S	IP 카메라 일련번호
U_{id}	사용자 ID
C_{id}	IP 카메라 ID
N_u	사용자의 Nonce
N_i	IP 카메라의 Nonce
K_s	영상 정보 암/복호화 대칭키
M_x	x번째 메시지 인증 코드

3.2.1 사용자 인증 과정

사용자가 IP 카메라에게 인증을 요청하는 알고리즘을 다음과 같이 구현한다.

① 사용자는 IP 카메라로 요청을 보내기 위해 사용자의 Nonce N_u를 생성한다.

② 사용자는 카메라 일련번호 S, 사용자 ID U_{id}, 사용자의 Nonce N_u를 사용하여 HMAC M_1을 계산한다.

③ ②에서 계산한 HMAC M_1과 사용자 ID U_{id}, 사용자의 Nonce N_u를 IP 카메라로 HTTPS를 사용하여 전달한다.

④ IP 카메라는 카메라 설정 정보에 저장된 카메라 일련번호 S를 가져온다.

⑤ ④에서 가져온 장치 일련번호 S와 ③에서 전달받은 사용자 ID U_{id}, 사용자의 Nonce N_u를 사용하여 HMAC M_1을 계산한다.

⑥ ③에서 전달받은 HMAC M_1과 ⑤에서 계산한 HMAC M_1을 서로 비교하여 같은지 확인한다. 두 값이 같다면 3.2.2 IP 카메라 인증 과정을 진행하고 서로 다르다면 인증 실패를 응답으로 전송한다.

3.2.2 IP 카메라 인증 과정

IP 카메라는 3.2.1 사용자 인증 과정에서 사용한 값을 기반으로 사용자에게 인증 정보를 전달하여 다음과 같이 인증 과정을 수행한다.

① IP 카메라는 사용자에게 응답을 보내기 위해 카메라의 Nonce N_i를 생성한다.

② IP 카메라는 IP 카메라 일련번호 S, 사용자의 Nonce N_u, ①에서 생성한 카메라의 Nonce N_i를 조합한 문자열을 SHA-256을 해시 알고리즘을 통해 대칭키 K_s를 생성한다.

③ IP 카메라는 카메라 설정 정보에 저장된 카메라 일련번호 S, 카메라 ID C_{id}, 사용자의 Nonce+1 N_u+1, 카메라의 Nonce N_i를 사용하여 HMAC M_2을 계산한다. 그리고 ②에서 생성한 대칭키 K_s, 카메라 ID C_{id}, 사용자의 Nonce+1 N_u+1, 카메라의 Nonce N_i, HMAC M_2를 사용하여 HMAC M_3을 계산한다.

④ ③에서 계산한 HMAC M_2, HMAC M_3, 카메라 ID C_{id}, 사용자의 Nonce+1 N_u+1, 카메라의 Nonce N_i를 사용자에게 HTTPS를 통해 전달한다.

⑤ 사용자는 ④에서 전달받은 사용자의 Nonce N_u+1와 자신이 소유한 사용자의 Nonce N_u의 차이가 1인지 확인한다. 두 값의 차이가 1이 아니라면 인증 실패를 오류 메시지를 표시한다.

⑥ 사용자는 IP 카메라 일련번호 S, 사용자의 Nonce N_u, 카메라의 Nonce N_i를 조합하여 대칭키 K_s를 생성한다.

⑦ 사용자는 카메라 일련번호 S, ④에서 전달받은 카메라 ID C_{id}, 사용자의 Nonce+1 N_u+1, 카메라의 Nonce N_i를 사용하여 HMAC M_2을 계산한다. 그리고 ⑥에서 생성한 대칭키 K_s, 카메라 ID C_{id}, 사용자의 Nonce+1 N_u+1, 카메라의 Nonce N_i, HMAC M_2를 사용하여 HMAC M_3을 계산한다.

⑧ ④에서 전달받은 두 개의 HMAC M_2, M_3과 ⑦에서 계산한 두 개의 HMAC M_2, M_3을 각각 서로 비교하여 같은지 확인한다. 두 값이 같다면 3.2.3 세션 확인 및 수립 과정을 진행하고 서로 다르다면 인증 실패를 오류 메시지로 표시한다.

3.2.3 세션 확인 및 수립 과정

사용자는 3.2.1 사용자 인증 과정 및 3.2.2 IP 카메라 인증 과정에서 사용한 값을 기반으로 IP 카메라로 인증 정보를 전달하여 다음과 같이 세션 확인 및 수립 과정을 수행한다.

① 사용자는 대칭키 K_s, 사용자 ID U_{id}, 카메라 ID C_{id}, 카메라의 Nonce+1 N_i+1을 사용하여 HMAC M_4을 생성한다.

② 사용자는 ①에서 생성한 HMAC M_4, 사용자 ID U_{id}, 카메라 ID C_{id}, 카메라의 Nonce+1 N_i+1를 IP 카메라에게 HTTPS를 통해 전달한다.

③ IP 카메라는 ②에서 전달받은 카메라의 Nonce N_i+1와 자신이 소유한 카메라의 Nonce N_i의 차이가 1인지 확인한다. 두 값의 차이가 1이 아니라면 인증 실패를 응답으로 전송한다.

④ IP 카메라는 대칭키 K_s, 사용자 ID U_{id}, 카메라 ID C_{id}, 카메라의 Nonce+1 N_i+1를 사용하여 HMAC M_4을 계산한다.

⑤ ②에서 전달받은 HMAC M_4과 ④에서 생성한 HMAC M_4을 비교하여 같은지 확인한다. 두 값이 같다면 세션을 수립하고 서로 다르다면 인증 실패를 응답으로 전송한다.

3.2.4 영상 정보 암/복호화 과정

IP 카메라에서 영상 정보를 암호화하여 사용자에게 전달하고 IP 카메라 영상 뷰어 프로그램에서 암호화된 영상 정보를 복호화하여 사용자에게 보여준다. 다음과 같이 암/복호화를 진행한다.

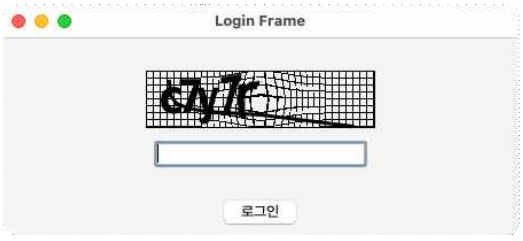
① IP 카메라는 장착된 카메라를 통해 영상을 녹화한다.
② 녹화한 비디오 스트림을 대칭키 K_s로 AES-256 암호 알고리즘을 사용해 암호화한다.
③ 암호화된 영상 정보를 HTTPS를 사용하여 전달한다.
④ 사용자는 ③을 통해 전달받은 암호화된 영상 정보를 대칭키 K_s로 복호화한다.
⑤ 사용자에게 복호화한 영상 정보를 보여준다.

3.3 제안 기법의 구현

(그림 2)와 (그림 3)과 같이 로그인 화면과 IP 카메라 영상 뷰어 화면을 구현하였다.

3.3.1 로그인 화면

로그인 화면은 사용자가 IP 카메라로 안전하게 접속하기 위해 다양한 보안 인증 요소를 포함하고 있다. (그림 2)에서와 같이 텍스트 기반 캡챠 문자열을 입력하고 로그인하면 프록시 서버를 통해 IP 카메라 서버로 접속할 수 있다. 캡챠 문자열 또는 사용자 인증 키가 올바르지 않은 경우 1초간 지연을 발생하고 연속해서 3회 이상 올바르지 않은 접근을 시도하는 경우 3분 지연을 발생하여 무차별 대입 공격 시도를 지연시킨다.



(그림 2) IP 카메라 영상 로그인 화면

(그림 3) IP 카메라 영상 뷰어 화면

3.3.2 IP 카메라 영상 뷰어 화면

(그림 3)은 IP 카메라 영상 뷰어 프로그램이 IP 카메라에 접속하면 프록시 서버를 거쳐 전달받은 암호화된 영상 정보를 복호화하여 사용자에게 영상을 송출하는 장면을 보여준다.

4. 평가

본 연구에서는 제안하는 IP 카메라 아키텍처가 보안 위협에 대해서 안전한지 평가하고 가용성 측면에서 우수한지 평가하였다.

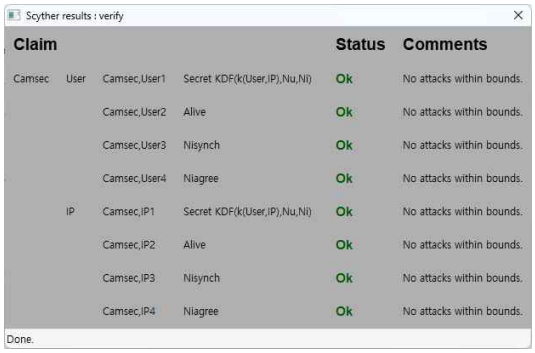
4.1 보안성 평가

Scyther는 보안 프로토콜 분석 도구로 다양한 통신 프로토콜의 설계와 분석에 사용된다. Scyther는 자동화된 방식으로 다양한 시나리오를 시뮬레이션하여 취약점을 발견하고 프로토콜의 다양한 실행 경로를 분석해 보안 위협을 검증한다. 직관적인 그래픽 사용자 인터페이스(GUI)와 명령줄 인터페이스(CLI)를 통해 복잡한 구성 없이 다양한 공격 모델에 대한 분석이 가능하다. Scyther는 프로토콜의 형식적 검증을 지원하며 프로토콜 간의 상호작용과 특정 공격 시나리오를 모델링할 수 있어 보안 프로토콜의 신뢰성을 높이고 잠재적인 위협을 예방하는 데 중요한 역할을 한다 [13]. 본 논문에서는 Scyther를 이용하여 제안한 보안 기법에 대해 보안성 평가를 진행하였으며, (그림 4)에 따르면 제안한 보안 기법은 공격으로부터 안전함을 알 수 있다.

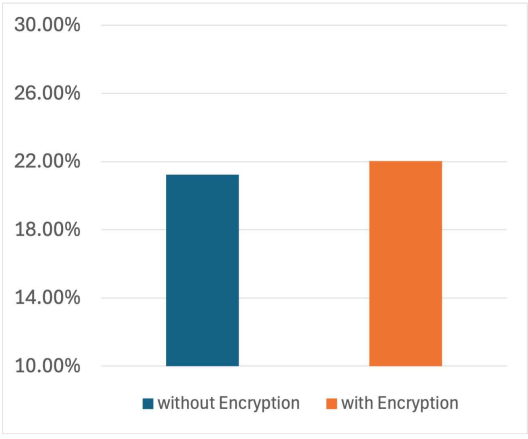
4.2 가용성 평가

제안 기법을 평가하기 위해 암호화가 적용되지 않은 아키텍처와 암호화가 적용된 아키텍처를 CPU와 메모리 사용량의 차이로 비교하였다.

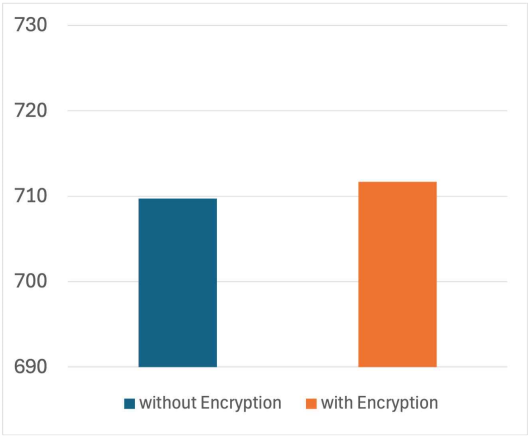
암호화가 적용되지 않은 아키텍처의 평균 CPU 사용량이 21.25%로 나타났고 암호화가 적용된 아키텍처의 평균 CPU 사용량은 22.04% 으로 나타났다. (그림 5)과 같이 암호화 적용 여부에 따라 CPU 사용량은 큰 변화가 없었다.



(그림 4) Scyther 보안성 평가 결과 화면



(그림 5) 암호화 적용 여부에 따른 CPU 사용량



(그림 6) 암호화 적용 여부에 따른 메모리 사용량

암호화가 적용되지 않은 아키텍처의 평균 메모리 사용량이 709.73MB로 나타났고 암호화가 적용된 아키텍처의 평균 메모리 사용량은 711.71MB 으로 나타났다. (그림 6)과 같이 암호화를 적용 여부에 따라 메모리 사용량은 큰 변화가 없었다.

5. 결 론

IP 카메라는 네트워크를 통해 영상 정보를 전송하여 지속적인 모니터링이 필요한 환경에서 적극적으로 활용되어 왔다. 그러나, 적절한 보안기술이 적용되지 않은 환경에서 IP 카메라의 영상 정보가 유출되는 사고가 다수 발생하였으며, 주요 취약점으로 프록시가 지적되었다. IP 카메라에서 취급하는 영상 정보는 개인의 사생활뿐만 아니라 기업의 시설 정보와 같이 민감한 정보가 포함하고 있기에 이에 대한 보호가 필수적이다. 따라서, 본 연구에서는 IP 카메라 보안 기법을 제안하여 카메라 영상 스트림의 암호화와 사용자 인증을 안전하고 효과적으로 수행할 수 있는 방법을 제시하였다. 제안된 기법은 보안성 평가를 통해 높은 수준의 안전성을 입증하였으며, 가용성 평가를 통해 암호화를 용하지 않은 아키텍처와 비교하였을 때 CPU와 메모리 사용량이 변화가 없음을 확인하였다. 향후 연구로는 제안한 보안 기법을 확장하여 IP 카메라와 유사한 경량 연산 장치를 보호할 수 있는 방법을 모색하고자 한다.

참고문헌

[1] 허은정, 고다원, 오찬석, 이서연, 최석환, "IP 카메라 보안 취약점과 대응 방안에 관한 연구", 한국통신학회 학술대회논문집, pp. 1112-1113, 2023.

[2] 김윤하, 윤성원, 김진훈, 오은, 최현주, "IP카메라의 전송구간 취약점 분석을 통한 보안강화 및 관리개선 사례에 관한 연구", 한국통신학회 학술대회논문집, pp. 759-760, 2018.

[3] 임한비, 이가현, 이훈재, "IoT 기기의 해킹 사건과 보안 동향", 한국컴퓨터정보학회 학술발표논문집, 제31권, 제2호, pp. 219-220, 2023.

[4] 한상훈, 장진희, 강길욱, 박한솔, "IP카메라 해킹 분석과 대책", 한국컴퓨터정보학회 학술발표논문

집, 제26권, 제1호, pp. 165-166, 2018.
[5] 박재경, 김현우, "사물인터넷 보안을 위한 IP 카메라에 관한 연구", 한국컴퓨터정보학회지, 제26권, 제2호, pp. 1-7, 2018.
[6] 강동희, 임재덕, "IoT 환경에서의 네트워크 보안 프로토콜 성능 분석", 정보보호학회논문지, 제32권, 제5호, pp. 955-963, 2022.
[7] 보안뉴스, "또 다시 터진 IP 카메라 해킹 영상 유출 사태, 그간 어떤 사건 있었나", 2024. https://www.boannews.com/media/view.asp?idx=125345.
[8] 조이든, 박수진, 강남희, "사물인터넷의 경량 IP 카메라 취약점을 이용한 해킹 공격 및 대응 방안", 디지털콘텐츠학회논문지, 제20권, 제5호, pp. 1069-1077, 2019.
[9] CVE-2020-7879. NATIONAL VULNERABILITY DATABASE. 2021. https://nvd.nist.gov/vuln/detail/CVE-2020-7879.
[10] E. Rescorla, "HTTP Over TLS", RFC 2818, 2000.
[11] The Official Captcha Site., http://www.captcha.net/.
[12] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, 1997.
[13] Cas Cremers, "Operational Semantics and Verification of Security Protocols", Springer, 2012.

〔저자소개〕

김 량 래 (Ryang Rae Kim)
2020년 3월~현재 경상국립대학교 컴퓨터공학과 학사과정
email : rrkim@gnu.ac.kr

조 승 현 (Seoung-Hyeon Jo)
2020년 3월~현재 경상국립대학교 컴퓨터공학과 학사과정
email : gmelan@gnu.ac.kr

김 지 윤 (Jiyoon Kim)
2018년 2월 순천향대학교 정보보호학과 학사
2020년 9월 순천향대학교 정보보호학과 석사
2022년 2월 순천향대학교 정보보호학과 박사
2022년 9월~현재 경상국립대학교 컴퓨터공학과 조교수
email : jykim92@gnu.ac.kr