Poster: Data Protection of IoT End Device

Jinseong Kim, Chang-O Eun, Im Y. Jung*
School of Electronics Engineering
Kyungpook National University, South Korea
{jin7733, ay3213}@knu.ac.kr, iyjung@ee.knu.ac.kr

***Abstract*—Recently, many vulnerabilities of IoT end devices appear. One example is IP camera vulnerability. IP camera can be attacked through bypassing IP camera authentication and authorization, analyzing and reusing the packets of IP camera video stream and so on. However, the countermeasures to these attacks are dependent on each manufacturer of IP camera. In this paper, we propose a solution to protect the data stream of IP camera at home network, which does not depend on the manufacturer.**

I. Introduction

In recent years, a hacker attacked an IP camera at home network and spread someone's private videos [1]. The IP camera via Internet provides the ability for users to receive real-time data stream remotely. The users can use their IP cameras to monitor their pet, child or house whether thieves came into home. However, as shown in Fig. 1, there is a problem that a hacker can control the IP camera [2][3][4][5], and also sniff the packets of IP camera video stream when users use IP cameras remotely.

Fig. 2 shows a detailed data flow when a user wants to view the video stream of his/her IP camera at home from outside using a smartphone. The replay server in Fig. 2 which is provided or specified by the IP camera manufacturer, informs the IP and port so that the smartphone can access the IP camera. We focused on three problems, as shown in the red parts in Figure 2. First, since the server has IP camera information, a third party can view the video stream of the IP camera by the server. Secondly, the data stream from IP camera and IP camera application packets are not encrypt and are vulnerable to sniffing. Third, the security vulnerability of IP camera itself allows hackers to bypass IP camera authentication/authorization and to view the images in the data stream.

To solve these problems, we studied a solution that allows only the original user to view the IP camera streaming data. This solution encrypts the streaming video of the IP camera at the home gateway and decrypts it from the user's smartphone. With this method, the security of IP cameras can be improved while maintaining compatibility with existing IP cameras. For this solution to be realized, it is important how to design a light and secure protocol between the gateway and the smartphone, and how to address the performance degradation expected from the encryption/decryption of realtime data stream.

Network and Distributed Systems Security (NDSS) Symposium 2018
18-21 February 2018, San Diego, CA, USA
ISBN 1-1891562-49-5
http://dx.doi.org/10.14722/ndss.2018.23xxx
www.ndss-symposium.org

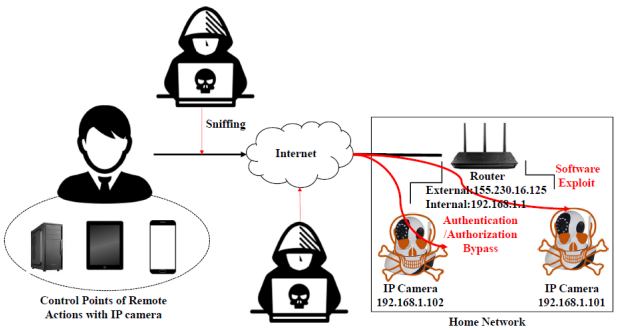


Fig. 1. Vulnerability of IP Camera

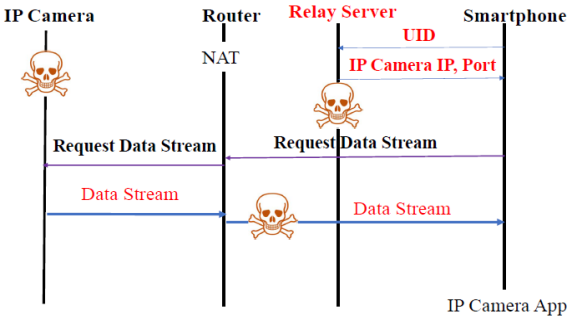


Fig. 2. The data flow at the remote control of IP Camera using smart device and the threat model

TABLE I
IP CAMERA PRODUCTS USING RELAY SERVER [6]

Manufacturer(Country)	China	USA	Tailand	Italy	Brazil
IP Cameras	25,863	8,625	6,118	4,735	4,058

II. Threat Model

In this paper, our target is limited to the IP camera products where the IP camera at home network is connected with the user's smartphone through the relay server. Table I shows the number of IP camera products in the world using relay server.

The relay server provides the user IP camera's IP and port using UID. However, some IP cameras had a backdoor planted when it had been created. Therefore, the streaming video of the IP camera can be stored on the relay server although the

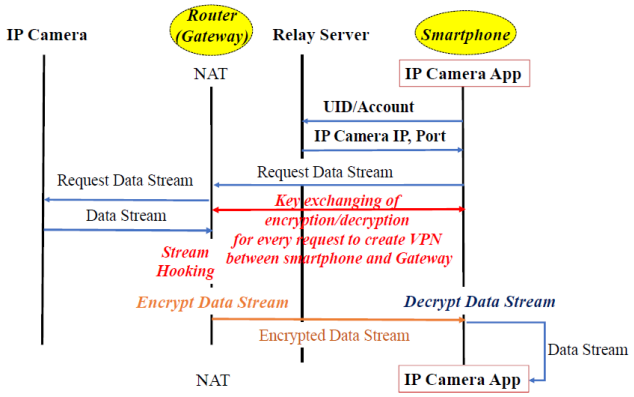


Fig. 3. A protection scheme of IP camera video stream

user does not know it. A malicious user can view the streaming video of IP camera through the server [5].

Some IP camera products do not encrypt packets when IP camera transmits the streaming video to smartphone, when IP camera application sends UID to the relay server or when the application requests an authentication of IP camera [3][4]. Therefore, if the attacker can sniff the user's packet, he/she can control the IP camera through the IP camera's UID, and its account. As a result, an attacker can view or leak the streaming video.

Even if all packets transmitted from the IP camera are encrypted, an attacker can bypass the authentication and auorization using the vulnerability of the IP camera. As a result, an attacker can control IP cameras or view the streaming video [2]. These attacks are constantly being reported and the vendors of IP cameras are not immediately providing the patches to protect their products.

III. A Protection Scheme of IP Camera Video Stream

We propose a scheme to defend against the above problems without relying on the manufacturers of IP cameras.

As IoT device, all IP cameras on home network go through a router(gateway) for Internet connectivity. Therefore, we propose a scheme to solve the above problems by encrypting the streaming data of the IP camera in the router, that is home gateway, and decrypting the encrypted streaming data in the smartphone as shown in Fig. 3. The streaming data decoded from the smartphone is transmitted to the IP camera application at the smartphone. The proposed solution does not require any modifications to IP cameras, the relay servers of the manufacturers of IP cameras, and IP camera applications.

A. Security Analysis

Even if the replay server knows the information of the IP camera, the decryption is required to view the streaming data.

Even if an attacker collects the data from the IP camera through sniffing, the streaming data is encrypted and transmitted by the router, so the hacker can not decrypt the live streaming data.

TABLE II
AES-128 Performance [6]

SoC	CPU	OpenSSL version	AES-128 B/sec	Encryption msec/KB
Broadcom BCM4906	ARM Cortex-A53	1.0.2j	77820920	0.013
MediaTek MT7621 SoC	MIPS 1004Kc v2.15	1.0.2h	33467730	0.031
Qualcomm Atheros QCA9558 v1 revo	MIPS 74Kc v5.0	1.0.2d	13288740	0.770
ARMv7 rev5(v71)	BCM2709	1.0.2	31322790	0.032

Hackers can access the IP camera using the vulnerability of IP camera. However, the streaming data from the IP camera is encrypted and transmitted by the router, so the hackers can not see the streaming data.

B. Advantages

The proposed solution has wide compatibility with IP cameras because it does not modify the IP cameras and IP camera applications provided by its manufacturer. In addition, the encryption/decryption process works on the existing routers and smartphones, so there is no cost burden.

C. Performance Prediction

The proposed solution is applicable to IP camera products using RTP and RTSP.

IP cameras are designed to show live streaming to users. Therefore, an important factor in the proposed solution is delay time, which affects live streaming. Generally, a low-end CPU is used for routers. Table II shows the AES-128 encryption performance using the OpenSSL which is cryptographic library. We measured that the RTP packet of the IP camera was transmitted in 1KB. The column of msec/KB in Table II means the time of milisecond to encrypt 1KB in the router. In addition, since the CPU of the smartphone has higher performance than the router, the encryption/decryption time is less than 1ms. Therefore, user can not feel the delay with the proposed scheme added.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2017R1D1A1B03034950).

References

[1] http://mashable.com/2017/06/19/china-webcam-hacking/
[2] P. Kim, "Multiple vulnerabilities found in wireless ip camera (p2p) wificam cameras and vulnerabilities in custom http server," IT Security Research, 2017.
[3] T. Spring, "Two Popular IP Cameras Riddled With Vulnerabilities", Threatpost — The first stop for security news, 2017.
[4] A. Serper, "Zero-day exploits could turn hundreds of thousands of IP cameras into IoT botnet slaves", Cybereason.com, 2017.
[5] C. Brook, V. rarr, T. Spring, and M. Mimoso, "Hikvision Patches Backdoor in IP Cameras", Threatpost — The first stop for security news, 2017.
[6] https://wiki.openwrt.org/doc/howto/benchmark.openssl

Data Protection of IoT End Device

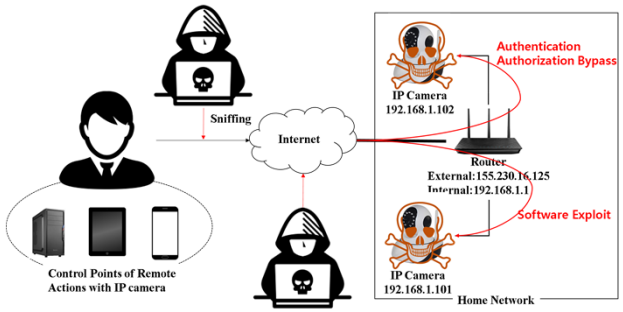
Jinseong Kim(jin7733@knu.ac.kr), Chang-O Eun(ay3213@knu.ac.kr), Im Y. Jung(iyjung@ee.knu.ac.kr)
School of Electronics Engineering, Kyungpook National University, South Korea

Abstract

- Recently, many vulnerabilities of IoT end devices appear. One example is IP camera vulnerability.
- IP camera can be attacked through bypassing IP camera authentication and authorization, analyzing and reusing the packets of IP camera video stream and so on.
- However, the countermeasures to these attacks are dependent on each manufacturer of IP camera.
- In this paper, we propose a solution to protect the data stream of IP camera at home network, which does not depend on the manufacturer

Introduction

- A hacker can control the IP camera using authentication/authorization bypass or software vulnerability. A hacker can also sniff the packets of IP camera video stream when users use IP cameras remotely, and steal the user account information or the data stream.



Vulnerability of IP Camera

- **Problems**
  - A third party can view the video stream of the IP camera by the server.
  - The data stream from IP camera and IP camera application packets are not encrypt and are vulnerable to sniffing.
  - The security vulnerability allows hackers to bypass IP camera authentication/authorization.
- **Challenges**
  - Allows only the original user to view the IP camera streaming data.
  - Improve the security of IP cameras
  - Maintain compatibility with existing IP cameras

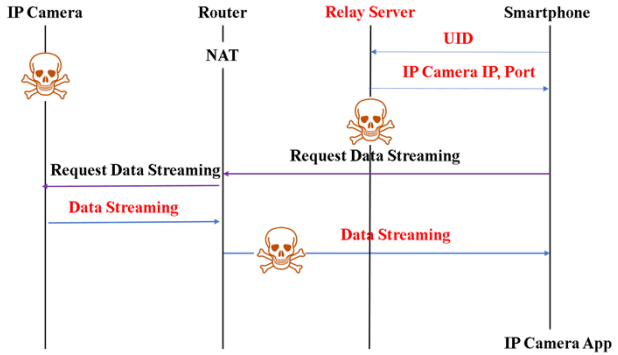
Threat Model

- **Target Environment**

Country	Numbers
China	25,863
United States	8,625
Thailand	6,118
Italy	4,735
Brazil	4,058

IP cameras using relay server

- IP camera of home network is connected with the user's smartphone
- User's smartphone receives IP and port of IP camera from relay server

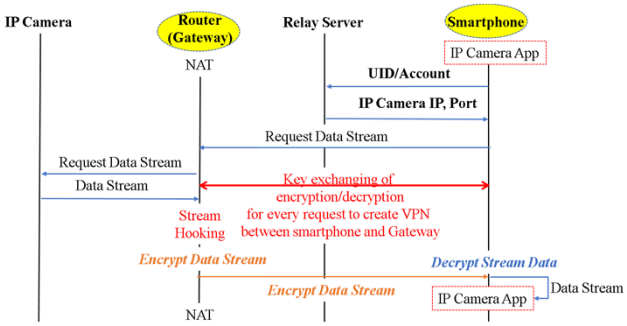


The data flow at the remote control of IP Camera using smart device and the threat model

- **Relay Server**
  - The relay server provides the user IP camera's IP and port using UID
  - The streaming video of the IP camera can be stored on the relay server
  - A malicious user can view the streaming video of IP camera through server
- **Unencrypted Packet**
  - Some IP camera products do not encrypt packets
  - The attacker can sniff the user's packet,
  - An attacker can view or leak the streaming video.
- **Authentication/Authorization Bypass**
  - An attacker can bypass the authentication and authorization using the vulnerability
  - The vendors of IP cameras are not immediately providing the patches to protect their products.

Security Analysis

- **A Protection Scheme of IP camera data stream**
  - IP cameras go through a router for Internet connectivity.
  - Encrypting the streaming data of the IP camera in the router(gateway)
  - Decrypting the encrypted streaming data in the smartphone



A protection scheme of IP camera video stream

- **Security Analysis**
  - **Relay Server:** The server can not decrypt the live streaming data
  - **Sniffing:** The hacker can not decrypt the live streaming data
  - **Vulnerability:** The hacker can not see the streaming data
- **Advantages**
  - This solution has wide compatibility with IP camera
  - This solution doesn't modify IP cameras and IP camera applications
  - There is no cost burden
- **Performance Prediction**
  - This solution is applicable to IP camera using RTP and RTSP
  - The RTP packet of the IP camera was transmitted in 1KB
  - The encryption/decryption time is less than 1ms

SoC	CPU	OpenSSL version	AES-128 B/sec	Encryption Kbytes/msec
Broadcom BCM4906	ARM Cortex-A53	1.0.2j	77820920	0.013
MediaTek MT7621 SoC	MIPS 1004Kc v2.15	1.0.2h	3467730	0.031
Qualcomm Atheros QCA9558 v1 revo	MIPS 74Kc v5.0	1.0.2d	13288740	0.770
ARMv8 rev5(v71)	BCM2709	1.0.2	31322790	0.032

AES-128 Performance