A NOVEL REMOTE ACCESS CONTROL FOR THE REAL-TIME STREAMING DATA OF IP CAMERAS

Kuen-Liang Sue and Ting-Yuan Wu

Department of Information Management, National Central University
Taoyuan, Taiwan

ABSTRACT

The massive consumer often has security concerns about Internet transmissions, and the remote access of the IP Camera is also full of challenges from the consumer market for privacy and security. In this context, when the user account of the security monitoring system is maliciously used, the security protection mechanism provided by the IP Camera itself is one of the topics most concerned to consumers. In order to improve the security of the remote connection of IP Camera, based on SIP protocol and practical experience, this study designs a set of feasible processes for the management of public key, which will help consumers protect their privacy rights in using the security monitoring system and the security when remotely operating the IP Camera. Finally, the experiment results prove that it will not impact the users' experience when accessing the IP Camera remotely.

KEYWORDS

IP Camera, P2P, Authentication, SIP, Digital Signature

1. INTRODUCTION

IP Cameras are becoming more and more popular. For security consideration, they are heavily used to monitor houses, workplace, public places and roads. Due to the installation position, most access methods are remote access. Hence, How to authorize users to prevent illegal access attempts has become a very important issue. This study aims to provide a classification of registration and login mechanisms of those famous security monitoring systems in the market as shown in Table 1. The findings are those systems all provide the mobile App as the mainmanaging tool for users. Moreover, while logging in the systems, the systems only do Single-Factor Authentication (SFA) to the password.

Table 1. Registration and login mechanisms of various security monitoring systems.

System	Method of Registration	Login Authentication
Arlo	E-mail	SFA
Netatmo	E-mail	SFA
mydlink	E-mail	SFA
Mi	E-mail / Mobile Phone	SFA

When a user account has a suspected abnormal login, only few security monitoring systems send the alert to the account owner as shown in Table 2. If the account owner cannot manage this situation at once, for example, immediately log into the security monitoring system to change the user password, or actively notify the system administrator to stop the network camera operation

through the backend system, the network camera will not refuse to connect with the account thief and lead the damage of the account owner's privacy rights. As pointed out in the introduction to this paper, the importance of re-identifying the visitor's identity before the IP camera accepts the video streaming connection.

Table 2. The security mechanism of various monitoring systems.

System	Failure of Sign-in	Suspicious Sign-in	Brute-force Attack
Arlo	No alerts	No alerts	No protection
Netatmo	No alerts	Email alerts	No protection
mydlink	No alerts	No alerts	No protection
Mi	No alerts	No alerts	No protection

2. REAL-TIME STREAMING PROTOCOL

A real-time streaming protocol (RTSP) is the main stream live video streaming signalling of IP camera [1]. However, when it comes to NAT-blocked remote network transmission, the security monitoring system must provide a transmission path for the video stream relaying through the server, which causes the system service provider to bear considerable bandwidth costs.

2.1. Accessing Live Streaming Remotely

In order to save the bandwidth cost of relaying instant video streaming through the server, the security monitoring system service provider begins to think about the peer-to-peer mechanism as a remote instant video streaming solution between the user and the network camera. Application of Session Traversal Utilities for NAT (STUN) can solve most of the problems caused by NAT in point-to-point transmission [2], supplemented by Traversal Using Relays around NAT (TURN) as a backup solution when NAT cannot be successfully penetrated [3]. Finally, only the signalling protocol needs to be relayed through the server, shown as Figure 1.However, the video stream itself does not contain data that can effectively verify the identity of each other. Therefore, the signalling protocol becomes the key role for the IP cameras to actively verify the identity of the visitor [4].

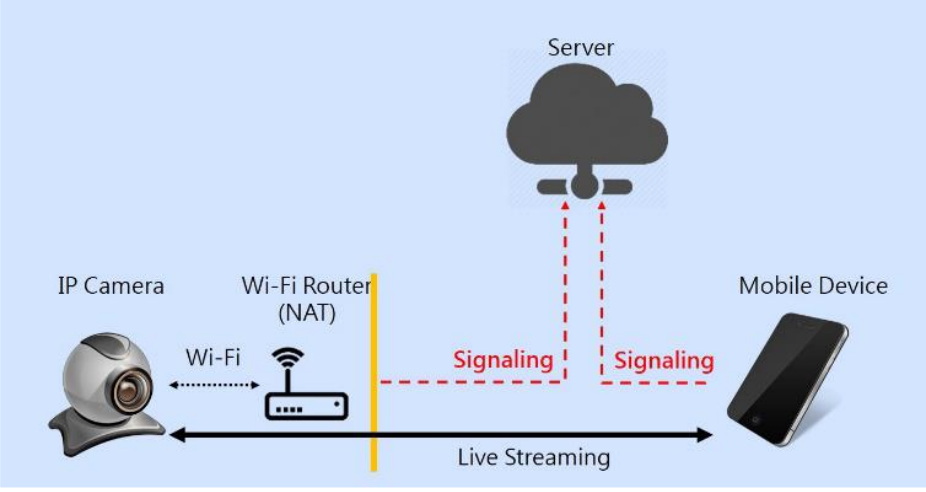

Figure 1. Overview of the remote access to live streaming.

2.2. Signalling Protocol

Session Initiation Protocol (SIP) is widely applied in VoIP. The session communication process between point to point in the network is shown in Figure 2. Unlike RTSP, SIP supports NAT penetration with STUN. If the network camera uses SIP protocol, it is assumed that Caller is the user's App, and Callee is the IP camera. However, this paper expects that the IP camera can actively reject illegal, unauthorized, malicious connections during the initial INVITE phase of the session.

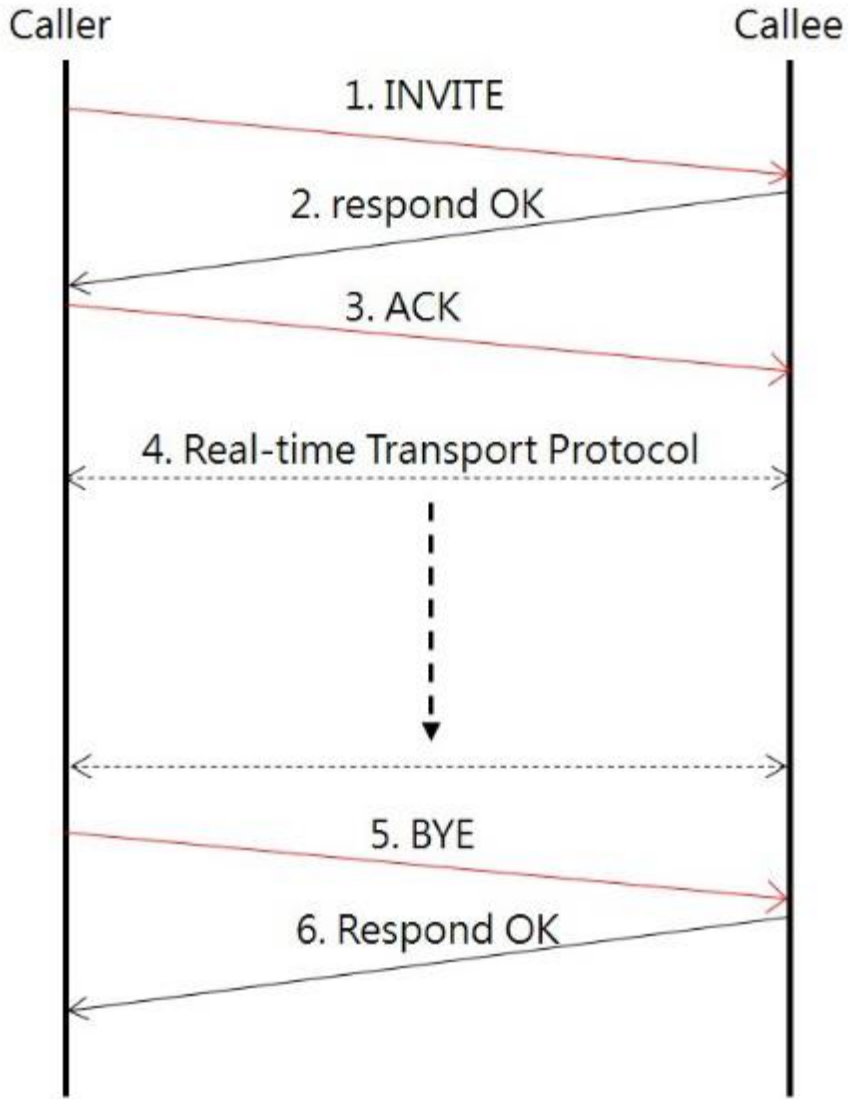

Figure 2. Session communication process in SIP.

The SIP packet is transmitted in readable plaintext, and the packet structure is shown in Figure 3. The header part mainly includes the information such as the originator (From), the receiver code (To), the session identifier (Call-ID), and the time (Date). The part of the payload contains two separate session description protocols (SDP) [5]. Authenticated Identity Body (AIB) is defined in RFC 3893 [6], which is a message digest for SIP to verify the identity of the session initiator. It must include the From, To, CSeq, Date of the SIP Header. , Call-ID and Contact or any other

attribute that can make AIB a unique value. Finally, DS represents the digital signature calculated from AIB [7].

Figure 3. SIP packet with authentication information

According to the definition of the above SIP related specification documents, the IP camera can utilize the digital signature to achieve the purpose of actively verifying the identity of the visitor. Nevertheless, from a pragmatic point of view, for exploring the security of the IP camera, it must avoid that the extra steps required by the user before viewing the live video stream, or greatly increase the waiting time for the authentication. In addition, from the perspective of the security monitoring system service provider, it is also necessary to consider the stability of the verification efficiency and mechanism, and the related system construction costs derived from the introduction of the verification mechanism. Therefore, prior to entering the implementation phase, an analysis of its applicability to the safety monitoring system is required.

3. APPLICABILITY ANALYSIS

In order to evaluate the applicability of the digital signature more objectively and cautiously, the authors listed five evaluation indicators for the application of the authentication mechanism to network cameras and their security monitoring systems which are based on the practical experience of working with such equipment manufacturers.

3.1. Evaluation Indicators

1) Validity: Refer to the authentication method, whether there are potential problems, or security vulnerabilities, so that the verification mechanism cannot continue to operate stably, or vulnerable to the threats of dictionary attack and brute force attack. [8].

2) Hidden Ability: Whether the transmission path of a private key or a digital certificate is transmitted through the Internet or a third-party server, if the secret key or digital certificate must be frequently transmitted over the Internet, there will be a higher probability of being intercepted by a malicious attacker [9].

3) Operational Convenience: It refers to the users need to perform additional operations from the time when the user decides to view the live video streaming of the IP camera. If there are steps that interfere with the user before viewing the live video streaming, it will have a negative impact on the experience [10].

4) Derived System Construction Cost: After integrating the authentication method, it is necessary to consider the subsequent system construction and operation costs that may be derived, such as the establishment of the certificate management center [11].

5) Verification Efficiency: Under the same Internet quality, the interval between the mobile App sending the INVITE signalling and the mobile App receiving the live video streaming will also affect the user experiences and the opinions of the quality of the IP camera. Therefore, the time taken for the verification process must be stable and not too long [12].

3.2. Verification Scenario

In the scenario studied in this paper, the mobile App is the initiator of the signalling communication, which is the verified end; the network camera is the signalling receiver, which is the verifying end. After the IP camera receives the INVITE signalling, the digital signature is extracted, and use the pubKey paired with priKey to decrypt the digital signature and verify if it is correct. The verification calculation process is as follows:

1) When the mobile App initiates the INVITE signalling to the IP camera, the mobile App signs digital signature with AIB by using private key stored on the mobile device, as in (1).

$$DS = E(priKey,H(AIB)) . (1)$$

where DS is digital signature obtained after operation. E is the private key encryption algorithm. priKey is the private key held by mobile App. H is the HASH algorithm such as SHA or MD5.

2) After IP camera receiving the INVITE signalling, the DS of INVITE signalling needs to be decrypted with the paired private key stored in IP camera, as in (2).

$$message = D(pubKey,DS) , (2)$$

where message is the digital signature. D is the private key encryption algorithm. pubKey is the private key.

3) After IP camera receiving the INVITE signalling, the DS of INVITE signalling needs to be decrypted with the paired private key stored in IP camera, as in (3).

$$isValid = (message = = H(AIB)) , (3)$$

where isValid is the verification result.

3.3. Applicability Evaluation of Digital Signature

According to the above scenario, the application of the digital signature as the five evaluation analysis of the authentication mechanism is described as follows:

1) Validity: Digital signatures are less likely to be compromised by dictionary attacks or brute force attacks. In addition, the digital signature is sent with the signalling at the same time and does not need to be passed through a third party. Therefore, it rarely fails to transmit to lead the verification mechanism invalided.

2) Hidden Ability: In the above scenario, since the private key and the public key are respectively stored in the mobile device and the IP camera, and the digital signature will not be transmitted through Internet during the verification process. Therefore, the digital signature will not with the hidden ability issue.

3) Operational Convenience: As a result, since the private key has been stored in the mobile device, the user does not need to perform additional steps when initiating the INVITE signalling. Due to the related specification documents such as SIP and RFC 3893, there are no instructions or suggestions on how to transmit and manage the public key. Therefore, it is necessary to design a

process mechanism for the Mobile App transmits the public key to the network camera without affecting the user's operation convenience.

4) Derived System Construction Cost: In the process of generation and verification of the public-private key, it only involves the encryption and decryption of the mobile App and the IP camera, there is no other additional system required.

5) Verification Efficiency: While computing asymmetric encryption and decryption, the hardware performance of embedded system needs to be concerned. The computing abilities of embedded systems like IP camera is subject to further evaluation.

To sum up the above statement, the preliminary evaluation results of the above five indicators are summarized in Table 3. Therefore, this paper will continue to design a process mechanism for the mobile App to transmit the public key to the IP camera without affecting the user's operational convenience. In addition, the verification efficiency has been evaluated via actual experiments. The result shows the verification efficiency is acceptable. The detail of experiment results will be shown and discussed in section 5.

Table 3. Preliminary evaluation of the applicability.

Indicator	Applicability
Validity	**Good**
Hidden Ability	**Good**
Operational Convenience	**Good**
Derived System Construction Cost	**Good**
Verification Efficiency	Acceptable

4. TRANSMIT AND MANAGE PUBLIC KEY

In practical applications, because there is no further specification or suggestion on how the public key should be transmitted and managed in SIP's RFC 3261, RFC 3893 and other related specifications. Therefore, in the following content, this paper will explain a feasible mechanism for how the mobile App can transmit the public key to the IP camera and how the subsequent IP camera manages multiple sets of public keys. Refer to the process of adding new IP camera from users which is designed by the security monitoring system provider in the market, the main purpose is to transmit sensitive information such as the binding token of the user account and the IP camera, the wireless network SSID of the home router and the password from mobile App to IP camera through near-end communication. This process can also provide a good path for the public key to be transmitted to the IP camera by the mobile App.

4.1. Adding the First Public Key

Figure 4 shows the mechanism for adding the new IP camera to the security monitoring system in the market from the actual investigation and analysis. It is speculated that the main purpose is to enable the mobile app to transmit sensitive information such as user account, a bind token and home router's wireless network SSID and password to the IP camera through near-end communication. It is speculated that the main purpose is to enable the mobile app to transmit sensitive information such as user account, a bind token, wireless SSID and password of home router to the IP camera through near-end communication.

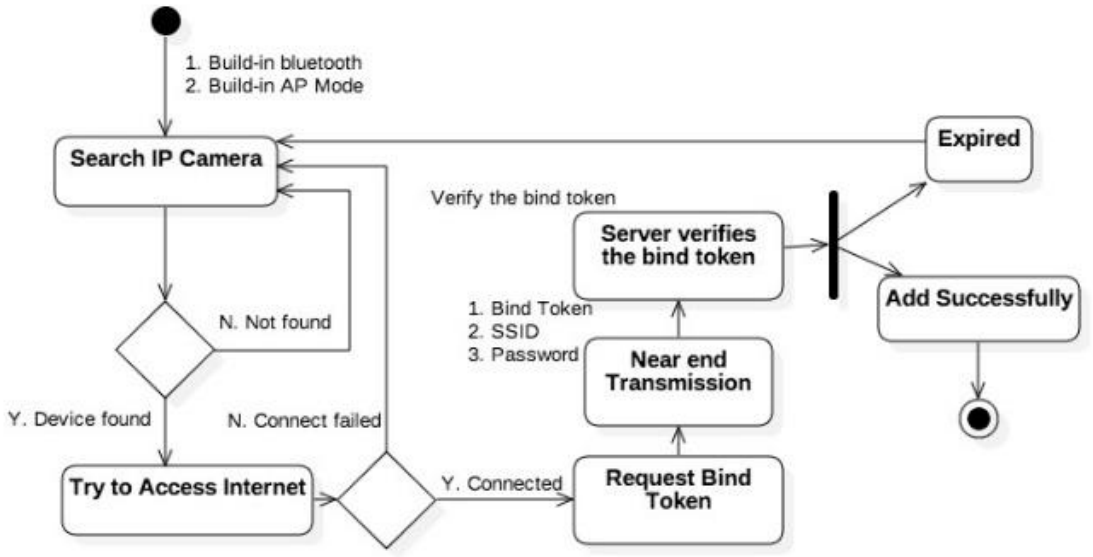

Figure 4. Mechanism for adding the new IP camera

The above mechanism can be integrated with the delivery of the first public key, and the process is described as follows:

Step 1. When the App is installed to the mobile device and is executed for the first time, the key pairing of the public key (pubKey) and the private key (priKey) is randomly generated and stored in the mobile device for subsequent fixed usage.

Step 2. The mobile App searches for and connects to the IP camera through a near-end network, such as the Bluetooth, or the AP Mode of the wireless network. After the connection is built, the mobile App can inquire the hardware information from the IP camera.

Step 3. The mobile App requests the server for a bind token to associate the user account with the IP camera.

Step 4. The mobile App transmits the bind token, along with the wireless network SSID and password of the home router selected by the user, and the pubKey, to the IP camera via the near-end transmission, and stores the pubKey for subsequent verification of the SIP.

Step 5. The IP camera is connected to the home wireless router according to the wireless network SSID and password received in Step 4 to obtain the internet connection capability.

Step 6. The IP camera sends the bind token received in Step 4 and its own hardware information to the server. The server accepts the subsequent communication of the IP camera according to the bind token, and records the association between the user account and the IP camera hardware information in the database.

Step 7. After the server processed the Step 6 and the mobile App receives the server notification, the user can start using the IP camera.

Since this study also expects the same set of user IDs (userID) can be authorized for different mobile devices. Therefore, when the IP camera stores the pubKey, it can use the unique string spliced by the user ID and the device ID of the mobile device, such as the International Mobile Equipment Identify (IMEI) of the Android system, and the index is stored to index the pubKey and note that this is the first new adding public key. The method of indexing is shown as:

$$index = contact(usrID,deviceID) , (4)$$

where index is an index string. contact is the method for combining the 2 strings. userID is the identifier of the user account. deviceID is the identifier of the IP camera.

The subsequent IP camera can export the corresponding pubKey according to the value of index and use the digital signature to verify. However, the SIP INVITE packet must also have the device ID information of the mobile device in order to enable the IP camera to re-establish the correct index before performing the verification. Therefore, an additional set of Device-ID fields needs to be extended for the SIP header to send the mobile device deviceID along with the INVITE packet. The above method is clearly presented in the activity diagram as shown in Figure 5.

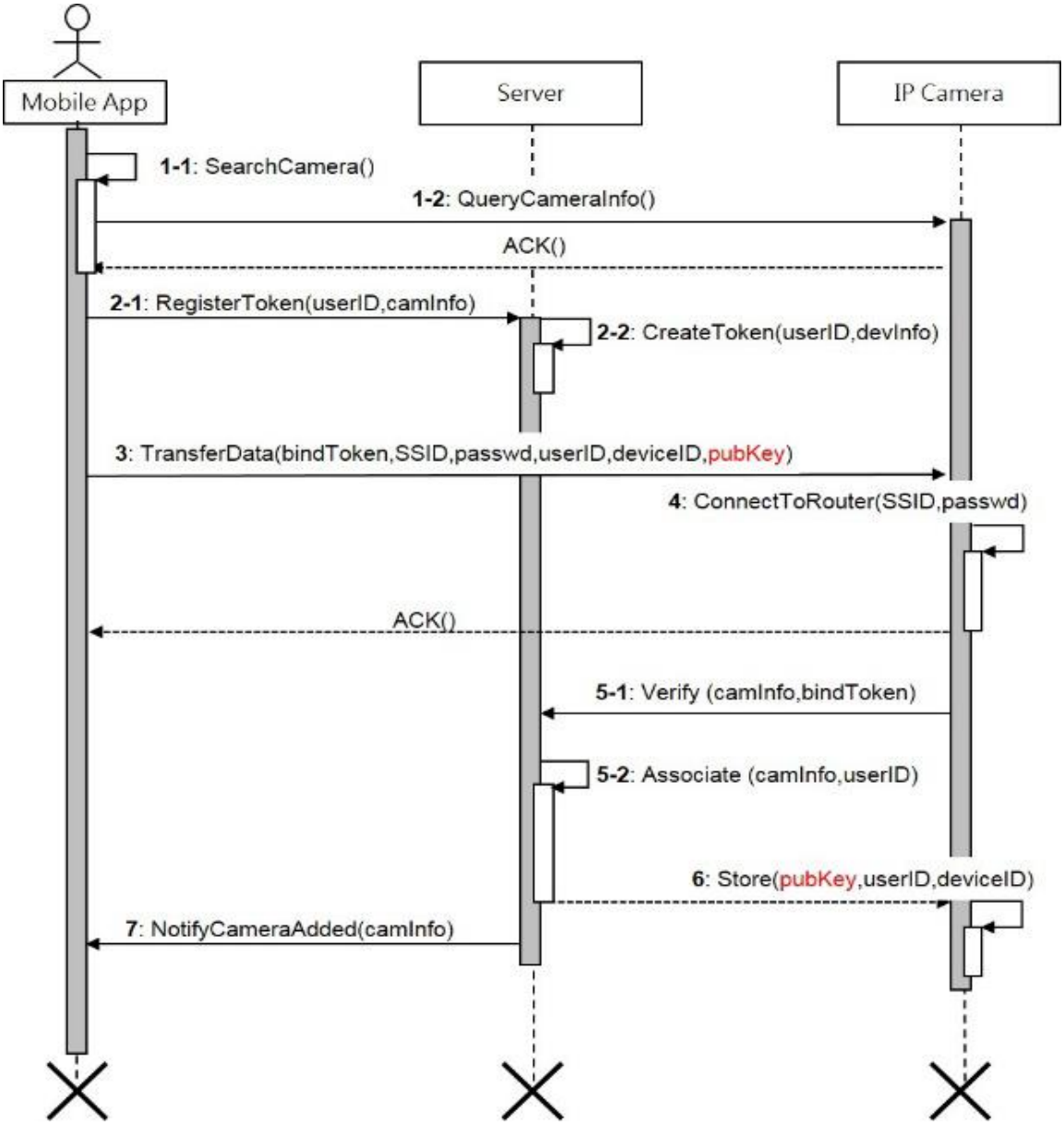

Figure 5. Delivery of public keys mechanism for adding the new IP camera

4.2. Adding Other Public Key(s)

However, after the user successfully adds an IP camera, it may be placed in an inaccessible location such as a ceiling or the roof, or anyplace out from the near-end communication range. If other members of the user's family also want to use their personal mobile devices to connect the IP camera, it is not conducive to reusing the near-end communication to add other user accounts and their mobile devices. As a consequence, it is obviously necessary in conjunction with the functioning digital signature verification mechanism to design a set of procedures for remotely forwarding other public keys to the IP camera through the server relay to achieve the function of adding other user accounts and their mobile devices.

Through the first public key stored in the IP camera, with the aid of digital signature verification, the IP camera can be relayed through the server and transmitted the public key of other mobile devices as shown in Figure 6.

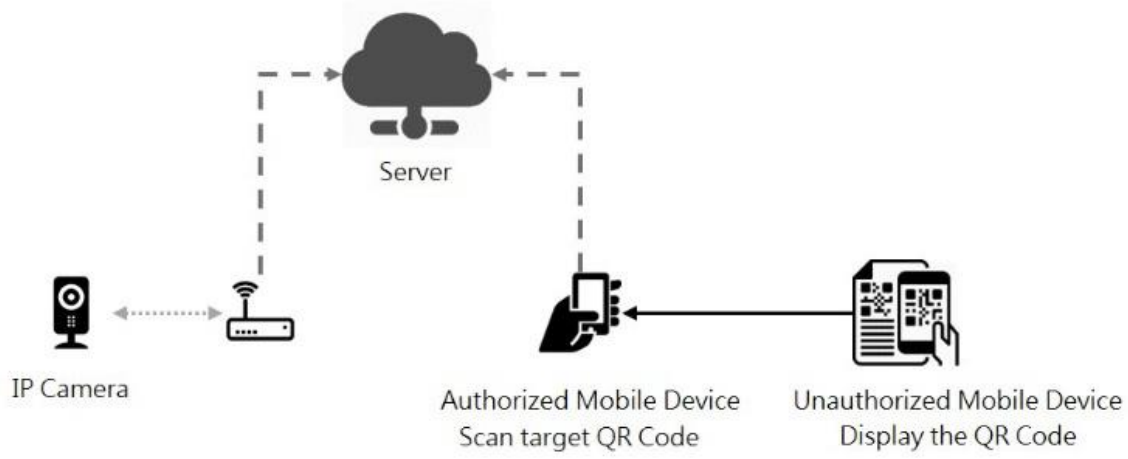

Figure 6. Illustration of add other public key(s).

Due to the limited storage space of the IP camera, this study has set the maximum number of public keys that can be stored by the IP camera to 16 groups. The detailed process is described as follows:

1) After the new mobile device splicing its public key (pubKey2), device ID (deviceID2) and user account (userID2) into a request string (reqValue), the reqValue is displayed in the QR code to the network. The camera establishes a pre-scan of the remotely connected mobile device.

2) The digital signature is signed by the private key (priKey1) of the authorized mobile device with the reqValue as in (5).

signature = E (priKey1,H(regValue)) , (5)

where E is the encryption algorithm.

3) The IP camera adopts the userID1 and deviceID1 to rebuild the index for exporting the stored public key (pubKey1), and decrypts the signature as in (6).

Digest = D(pubKey1,signature) , (6)

where Digest is the message digest; D is the public key decryption algorithm; pubKey1 is the first public key stored in the IP

4) The IP camera uses the logic as in (7) to determine whether or not to accept the new public key.
isValid = (Digest = = H(regValue)) , (7)

If isValid is TRUE, the IP camera can use the string of userID2 and deviceID2 to index and store pubKey2. The communication process of the above steps is sequenced, as shown in Figure 7.

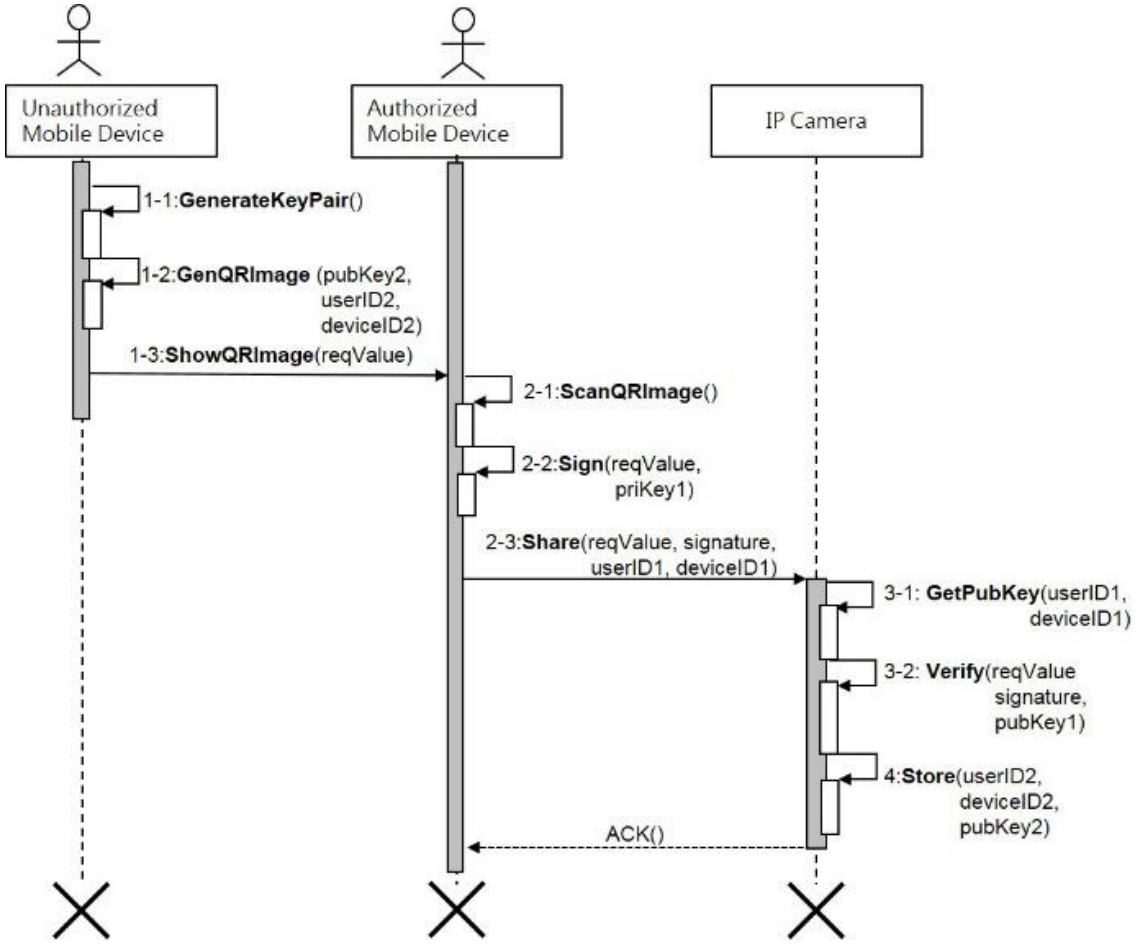

Figure 7. Communication schematic of adding other public key(s).

4.3. Removal of Other Public Key(s)

Removal of other user accounts that have been authorized to use this IP camera and their mobile devices, the IP camera can be notified by the specified authorization information by the same means of delivery and verification. The difference is that the IP camera must firstly be queried to obtain a combined list of authorized user accounts and their mobile device IDs, and then the user can select the target of removal through a dedicated application shown as Figure 8 below.

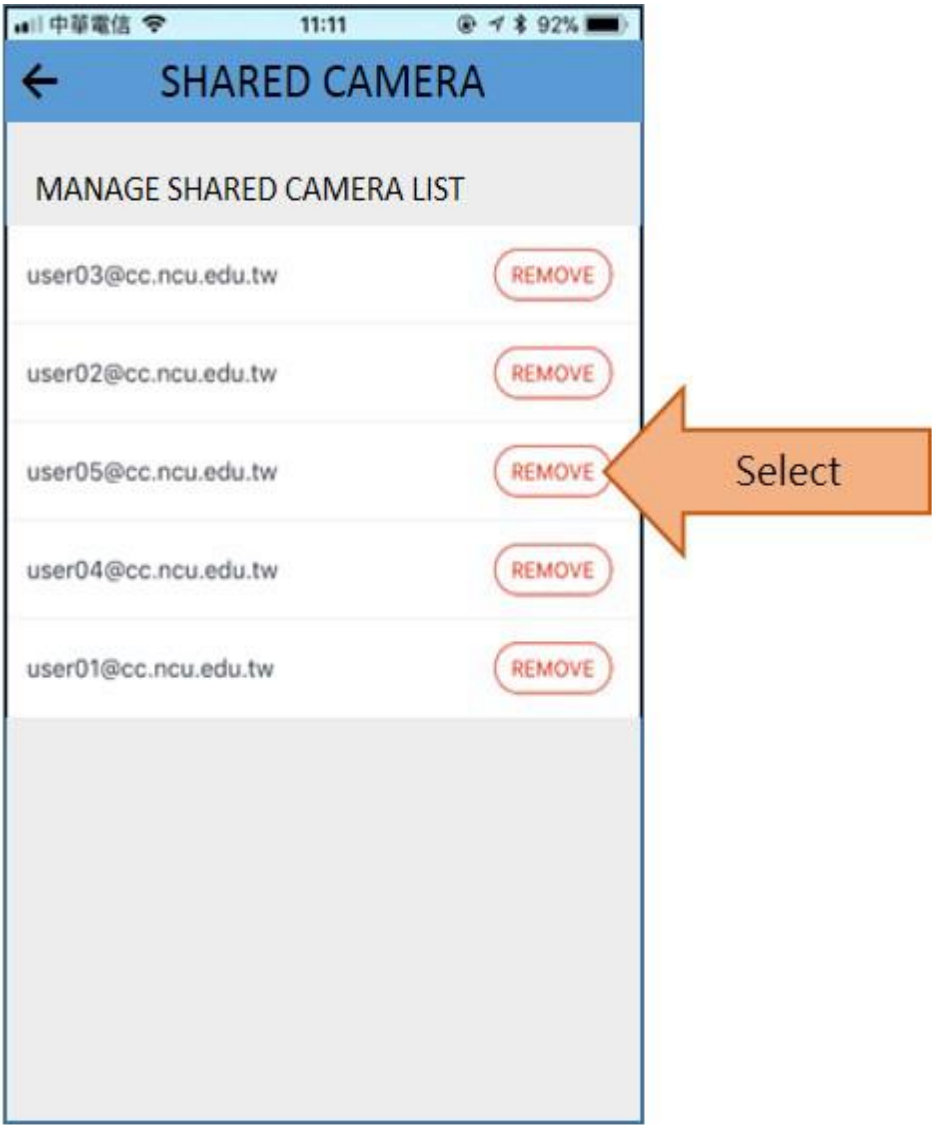

Figure.8. Friendly App GUI for managing public key(s).

Due to its process and verification method are similar to add the new public key, so it will not be elaborated here. In particular, the query request sent by the IP camera does not affect the correction of operating the verification mechanism, and the query request itself has no clear message digest. Therefore, it is not recommended to verify the identity when querying the combo list.

5. VERIFICATION EFFICIENCY ASSESSMENT

Since the user experience is also affected by the interval of video to be displayed on the mobile App, the verification time of executing an asymmetric decryption algorithm on embedded systems is concerned. Therefore, this study actually uses a low-level IP camera to execute the digital signature mechanism with 2048-bit public-private key pair, and proves the verifications will not significantly affect the user experience by actual experimental data.

5.1. Experimental Method

The random pre-generated 2048 bits key pairs are respectively stored in the mobile device and the IP camera in advance, and then the digital signature is computed by using the pre-set AIB in the mobile App, and then the digital signature is moved to the IP camera manually. In the method of quantitative analysis through experiments, the mobile device and the IP camera perform for each 1,000 times, 10 rounds, and a total of 10,000 times generate digital signatures and verification operations. By the experimental data, the extra waiting time can be evaluated. In addition, since the digital signature is in the form of an attachment and is transmitted along with the INVITE signalling, the factor of network transmission is not included in the evaluation of the extra waiting time of the user.

.

5.2. Experimental Environment

The IP camera was developed and manufactured by domestic S company in 2017. Its hardware specifications are shown in Table 4, which belongs to the lower-level products of the company's product line. The execution environment for running digital signature verification is the Node.js Runtime environment embedded in it.

Table 4. Hardware specification of IP camera.

Component	Specification Description
Processor	Dual 600MHz 32-bit RISC
RAM	DDR3 128MB
Flash	SPI Flash 16MB

The mobile device is the Android system mobile phone launched by the Japanese S brand in 2016. The model number is F8132. And the execution environment for running the digital signature is to directly interface with the Android Studio through the USB cable.

5.3. Experimental Results

The average computing time and maximum computing time of IP camera and mobile device are summarized in Table 5 and Table 6 separately. Therefore, the user experience will not be impacted significantly by referencing the experimental result.

Table 5. Executed time of digital signature verification on IP camera.

Sequence	Avg. Time (Unit: millisecond)	Max. Time (Unit: millisecond)
Round 1	9.318469836	90.981818
Round 2	9.216010678	68.560485
Round 3	8.955744001	98.729697
Round 4	9.863399754	231.379393
Round 5	9.758593940	64.823273
Round 6	9.757688231	56.909576
Round 7	9.363185448	68.760242
Round 8	9.180566325	98.769454
Round 9	8.976063986	78.470788
Round 10	9.338684107	61.998546

Table 6. Executed time of generating digital signature on mobile device.

Sequence	Avg. Time (Unit: millisecond)	Max. Time (Unit: millisecond)
Round 1	1.596123654	4.921407
Round 2	1.598761786	7.975573
Round 3	1.575180051	5.427969
Round 4	1.572203218	5.007917
Round 5	1.572916926	5.106354
Round 6	1.579009886	4.868646
Round 7	1.576987239	4.982343
Round 8	1.596798118	10.156823
Round 9	1.610583293	8.422709
Round 10	1.600438932	4.436041

6. CONCLUSIONS

Based on the point-to-point video streaming, the proposed security of signalling negotiation is enhanced by applying digital signature verification. Not only the bandwidth cost of service providers can be reduced, but also the consumers can obtain a more reliable guarantee of their privacy rights while using the security monitoring system. Compared with the products currently on the market, the five applicability assessment results of the digital signature verification mechanism are more able to meet the consumer's expectations for safety and compliance with the operator's operating costs. The actual experimental data of the performance analysis shows that the efficiency of the asymmetric decoding operation will not impact on the user experience significantly while being executed on lower-level IP cameras.

However, there is an inconvenient scenario which might become the limit of the proposedmechanism. Due to the operation of the digital signature verification mechanism, the first public key needs to be set and stored in the IP camera by the user in advance. Once the first mobile device used to add a new IP camera is faulty or lost, the user can only clear all the stored first mpublic keys by resetting the IP camera and adding it again to remove its license restrictions. If mthe user has added multiple IP cameras by using the same mobile device, it will be inconvenient for users in such condition. Hence, how to enhance the procedures of updating and restoring key pairs, which is necessary to be executed when the mobile device fails or is lost, more efficiently is considerable study in future.

REFERENCES

[1] Davor Doder, Nenad Četić , Miroslav Popović , and Jelena Kovačević, (2016) "Realisation of Server Application for Acoustic Sensors Based on RTSP, RTP Protocols", the 23rd Telecommunications Forum Telfor (TELFOR), pp. 316−319...

[2] Ha Tran Thi Thu, Jaehyung Park, Yonggwan Won, and Jinsul Kim, (2014)"Combining STUN Protocol and UDP Hole Punching Technique for Peer-To-Peer Communication Across NetworkAddress Translation", 2014 International Conference on IT Convergence and Security, pp. 101−104.

[3] R. Mahy, P. Matthews, and J. Rosenberg, (2010) "Traversal Using Relays Around NAT (TURN):Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, IETF.

[4] Konstantin Boyarinov and Aaron Hunter, (2017)" Security and Trust for Surveillance Cameras ", 2017 IEEE Conference on Communications and Network Security, pp. 384−385.

[5] H. Hakan Kilinc and Tugrul Yanik, (2014)" A Survey of SIP Authentication and Key AgreementSchemes ", IEEE Communications Surveys & Tutorials, vol. 16, no. 2, pp. 1005-1023..

[6] J. Peterson, (2004) "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format", RFC 3893, IETF.

[7] Ahmadreza Montazerolghaem, Mohammad Hossein, Yaghmaee Moghaddam, and Alberto Leon-Garcia, (2013) " OpenSIP: Toward Software-Defined SIP Networking ", IEEE Transactions on Network and Service Management, vol. 15, no. 1, pp. 184-199.

[8] Changda Wang, Syed Rafiul Hussain, and Elisa Bertino, (2016)" Dictionary Based Secure Provenance Compression for Wireless Sensor Networks ", IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 405-418.

[9] Vahe Seferian, Rouwaida Kanj, Ali Chehab, and Ayman Kayssi, (2018) " Identity Based Key Distribution Framework for Link Layer Security of AMI Networks ", IEEE Transactions on Smart Grid, pp. 17-20, vol. 9, no. 4, pp.3166-3179

[10] Anush Krishna Moorthy, Lark Kwon Choi, Alan Conrad Bovik, and Gustavo de Veciana, (2012)" Video Quality Assessment on Mobile Devices: Subjective, Behavioral and Objective Studies ", IEEE Journal of Selected Topics in Signal Processing, vol. 6, no. 6, pp.652-671.

[11] Saurav Malani, Jangirala Srinivas, Ashok Kumar Das, Kannan Srinathan, and Minho Jo,(2019) " Certificate-Based Anonymous Device Access Control Scheme for IoT Environment ", IEEE Internet of Things Journal., vol. 6, no. 6, pp. 9762-9773.

[12] Christodoulos Asiminidis1, George Kokkonis2 and Sotirios Kontogiannis, (2018) " Database Systems Performance Evaluation for IOT Applications ", International Journal of Database Management Systems, vol. 10, no. 6, pp. 1-14.

Authors

Kuen-Liang Sue received the M.S. degree in computer science and information engineering and the Ph.D. degree in information management from National Chiao- Tung University, Hsinchu, Taiwan. He is currently an assistant professor with the Department of Information Management, National Central University, Zhongli, Taiwan. His research topics include mobile computing, IoT, and network security.

Ting-Yuan Wu received the B.S. degree in computer science and information engineering from Tamkang University, Taipei, Taiwan and the M.S. degree in information management from National Central University, Taoyuan, Taiwan. He is currently an R.D. team leader. His research topics include mobile network, IoT, image processing and network security.