Internet of Things (IoT): Security of LeFun Baby Monitor

Koneru Keerthi *(kxk170003)*[*], Lakshmi Priyanka Parimi *(lxp160730)*[*], Ankita Patil *(asp160730)*[*], and Arpita Mothukuri *(axm163631)*[*]

[*]*Department of Computer Science, University of Texas at Dallas*

***Abstract*—Internet of Things (IoT), also known as galaxy of gadgets, has gained high attention from researches due to the rapid growth of internet connected devices through wired and wireless network structure creating a platform for the smart human life. It allows communication and sharing of information among real-world things, and perpetuate about the condition of things and the surrounding environment with people, software systems and other machines. In this paper, we focused on the security of video baby monitor, particularly, LeFun Baby Monitor. Video baby monitors are of high interest for security exploration as they are positioned as safety and security device but can transfer data to plenty of other areas. We have explained details about the security camera, analysis on the network traffic, and the packets transmission based on the time, motion of the objects, and movement of the camera. The research also includes the security analysis of the IoT device and the potential vulnerabilities that can be exploited by attackers. This research can be further extended to the analysis of data by deriving a feature vector to classify the still view network packets from motion network packets, and observe the attacks based on the cloud security.**

***Index Terms*—Baby Monitor, Internet of Things (IoT), Network Traffic, Privacy, Security, Surveillance.**

I. DEVICE DESCRIPTION

LEFUN Baby Monitor is used to witness or monitor baby's activity from other house/business/office using a good Wi-Fi connection of 2dBi antenna range. The camera accepts the Wi-Fi of 2.4GHz but not 5GHz. The camera has a high resolution of 720 pixels, which provides HD image and HD video. The device provides motion detection alerts, and the data can be stored on micro SD card as shown in Figure 1, that can be connected to camera. It provides a wider range angle with pan of 350 degrees and a tilt of 100 degrees. The camera also supports Intelligent Digital Zoom, and IR Night Vision up to 32 feet. The camera consists of built-in microphone and speaker that enables voice communication between the MIPC app (a smart application used to monitor the video from the camera on other smart device) and camera. Intelligent motion alert system present in the camera sends snapshot/message alert to ensure safety of the system [1]. The specifications of the camera are as shown in the Figure 2 The camera is connected to smart devices through the MIPC application. The application is available for android devices and iOS devices and is also available for tablets. The application can be used as remote control for rotating camera. Additional key features of these device are live streaming, plug and play. Some of the specifications of this device are listed below [1]:

Fig. 1: LeFun Baby Monitor.

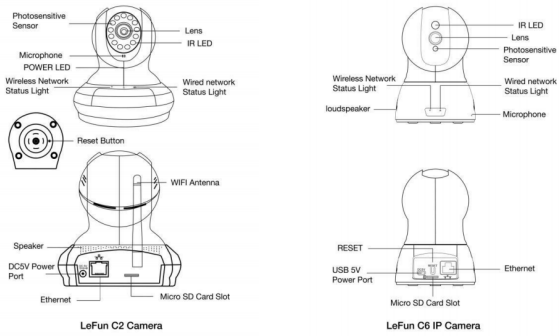


Fig. 2: Specifications of LeFun Baby Monitor.

1) Distance: 30 feet resolution
2) Frame rate: Real time 25FPS
3) Night vision: 12 infrared LEDs
4) Sensor: 1/4 "color CMOS sensor
5) Video/Audio Compression: H.264/AAC
6) Ethernet: 10/100 Mbps RJ45 interface
7) Wireless networks: 2.4G Wi-Fi (IEEE802.11b/g/n) by External antenna
8) Alarm notification: Real time App push notifications
9) Resolution: 1280x720 (720P), 640x360, 320x180, 160x90 (selectable)
10) Video storage: Micro SD card up to 64 GB storage

II. CONFIGURATION OF SETUP

In this paper, to perform the analysis on the we have used a laptop as an access point to connect the LeFun baby monitor

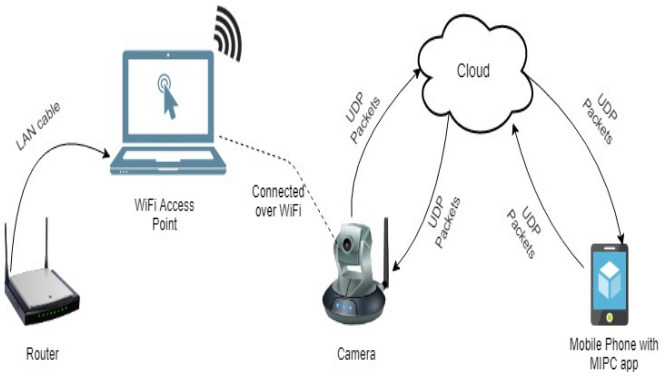


Fig. 3: Block Diagram showing the Configuration Setup

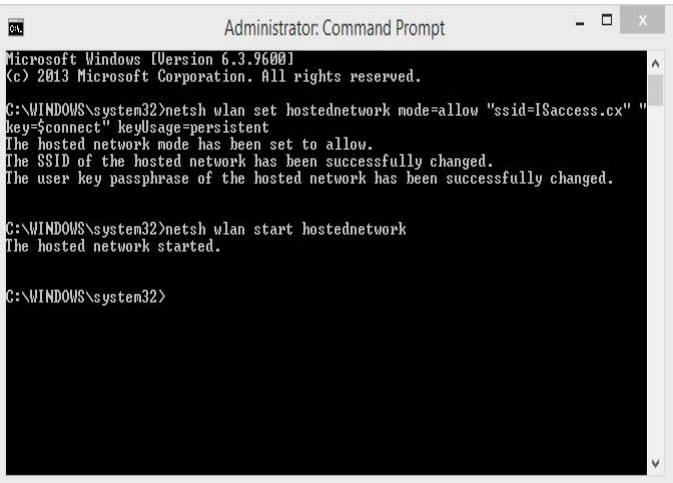


Fig. 4: Creation of Wi-Fi access point

Fig. 5: MIPC app

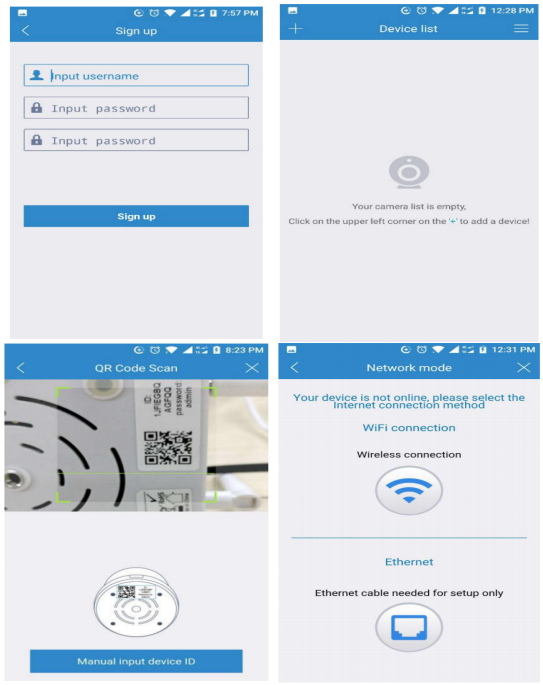


Fig. 6: Configuration of device in MIPC APP

to Wi-Fi. The configuration involves setup of Wi-Fi access point, MIPC app credential sign up, and connecting Wi-Fi to the security camera. The total configuration setup is as shown in the Figure 3.

A. Creating Wi-Fi Access point

Initially, the laptop (with Windows 8 OS) is connected to router via LAN cable. Access point (Microsoft virtual hosted network) should be created on the laptop. To create the hosted network, the following commands should be used in command prompt (cmd), while running the cmd as administrator [2].

```
> netsh wlan set hostednetwork mode=allow
ssid=<ssid> key=<password>
```

The property of the existing LAN connection should be Enabled, to share with the newly created access point in the ”Network and Sharing Center”, so that the other network users can connect through this new access point [3]. Then, the network should be started as shown in Figure 4.

B. Creation of credentials in MIPC APP

In this step, we connect the mobile device to the newly created access point through Wi-Fi. This was connected only for connecting the camera to Wi-Fi of the access point through the configuration shown in section C. After that, the mobile can be connected to any network, to access the video or camera. Then, the MIPC app was installed in the mobile from its APP store as shown in Figure 5. When the app was opened, the sign up screen was shown to create new user account. Then the user logs-in and adds the camera device to the application. In the MIPC app, click on the ”+” symbol on the left hand corner to add device. The screen shots in Figure 6 show the setup of the MIPC app [4].

C. Connecting Wi-Fi to the security camera

In the final step of configuration, the camera is plugged to power and the RESET button was clicked, which is present at the bottom of the camera. After reset, in the app, it asks for the Wi-Fi credentials required for the camera to connect. Here, we provide the credentials of our created access point to observe the network traffic. Then camera produces a RF-sound which is captured by the MIPC app and converts it into QR code. This QR code was captured by the camera lens, which ensures that the camera is connected to the Wi-Fi of the given credentials as shown in Figure 7. At this point, the camera is configured with Wi-Fi and the video is transferred from camera to the MIPC app.

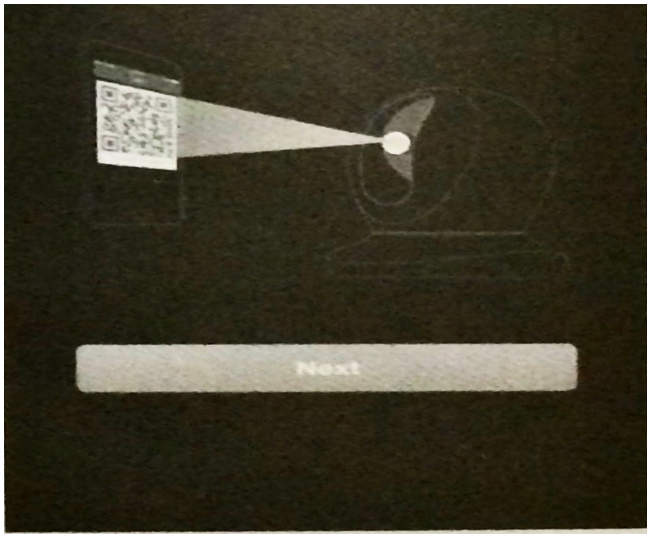


Fig. 7: Configuration of device in MIPC APP

The same MIPC credentials can be used to login into different devices at the same time to monitor the video, to control the camera etc. [4].

III. PRIVACY POLICY DESCRIPTION

Privacy policy is a document which states the policies to which a company should abide to while collecting, using, managing and disclosing the customers data. The main goal of this document is to safeguard the privacy of the customers. It ensures that personal data of the customer will not be disclosed to any third parties. As per the research, the Lefun Baby monitor does not have any specified privacy policy provided by the company. Hence, in this research, we present the privacy policies to be followed by baby surveillance cameras based on the various manufacturer published policies.

A. Privacy Policy to be possessed by Baby Monitors:

Baby monitors should possess end to end encryption with a secure network connection. It should clearly state the data to be collected [5], which will be categorized as automatically collected information without user consent. These include, type of device, IP address of the device connected to network, images/ video captured from the device, and date, time at which the data is captured using this device. It should be isolated from memory at which the personal information was stored and should be used only for gathering statistical information to improve the services provided by the vendor.

Privacy policy should also list out any third party services which company uses for data analytics and web analysis. It should also mention about the application used to monitor the camera video sequences such as MIPC. MIPC records the IP address of the device through it is logged in. It should also provide the information about the newly added devices to same account. This data should be stored with the user email address along with the information about Wireless camera, data collected by the device, a history of device settings and any other related information [5].

In the privacy policy, the various ways of using security protocols, while collecting data from users should be described. It should also provide information required for the user account creation and how these details are safe guarded over network. They should only be used to retrieve comments from users to improve services, business operations and protection against illegal activity. It should replicate the reasons for disclosing any data to third party individuals or business operations. The document should include the security precautions to ensure that the user data is not compromised, destructed or manipulated. Most of the policies specify that Secure Socket Layer (SSL) protocol provides good encryption of data, while transferring over the network. The details about other security protocols like Data Transport Layer Security, if utilized, should be explained [6]. Data retention, Opt-out rights and policy changes should also be listed in the document. It should emphasize that the device abides to COPPA - Children's Online Privacy And Protection Act. This Act governs the collection, use, and disclosure of personal information collected from children under age 13. The personal information includes photo, video, or audio file which contains the childs image or voice [7].

B. Privacy policy of the Cloud (MIPC CLoud) and Standalone application (MIPC App):

The baby monitor usually requires a cloud to which the captured data is uploaded to transfer to the smart device governing the camera. In this research, content will be uploaded into MIPC cloud from which it will be transferred on to MIPC app on the smart device for the users to view their baby movements. As per the privacy policy of MIPC [8], personal data will not be shared with other parties for commercial or marketing purposes without the user consent except in some cases which are listed below:

- When user gives consent, data might be shared with other partners when user signs up for the application.
- When user has some trouble resolving the problem data might be shared with vendors, service providers and technician for trouble shooting or answering the queries.
- If the company is acquired or transferred, then user data might be shared to acquiring company.
- For legal use, data might be shared.

MIPC has explicitly mentioned that non-personal information will be shared with their partners for analyzing the usage of energy. It also mentioned that the data transmission is ensured through HTTPS, TLS/SSL protocol, AES or RSA data encryption for preserving its security.

As per the MIPC privacy policy [8], it follows some of the Fair Information Practices. The manufacturer provides full disclosure of data. As mentioned in [8], *"This Privacy Policy for MIPC web site describes that information Mipc Technology Co.,Ltd. and its subsidiaries and affiliates (collectively, Mipc) collect, use, share, and store, including personal information (i.e., information that personally identifies you, such as your name, email address or billing information, or other data that can be reasonably used to infer this information)"*. It states that user consent is not required for collecting data. The

document states that it doesn't comprise of any minimizing of user data collection or minimizing identification of data with individuals as it uses cookies to track information. They ahve also stated that *"Like many websites, we and our third-party partners analyze log file information and other data collected through cookies, web beacons, and other tracking technology, to collect information about your browsing behavior when you visit our site, including for example, your browser type, domains, page views, IP address, referring/exit pages, information about how you interact with our sites web pages and with third-party links, traffic and usage trends on the service, etc."*. The document states that it tries to secure user data but it doesnt give complete assurance on security of data, as given in, *"We use commercially reasonable physical, administrative, and technological methods to transmit your data securely including HTTPS, TLS/SSL protocol, AES and RSA data encryption. The data is stored using Amazons S3 cloud service. However, MIPC cannot guarantee that unauthorized third parties will never be able to defeat our security measures or use your personal information for improper purposes"*.

IV. CAPTURING NETWORK PACKETS FROM THE DEVICE

Observing network traffic from or to a device provides lot of interest for the hackers as they can find or reach out to some of the vulnerabilities to hack the device. It would aid the hackers to get important information, particularly video data from the baby monitor. It also helps to know whether there are any people in the house or not, they can attempt to perform unwanted things or scare babies. Based on the references in [9], [10], [11], there is a dire need to know about the traffic of the baby monitor, how the data is being transferred and the available open ports of the device, whether the data is securely transmitted to and from the cloud etc.

In this project, we have observed the open ports through Nmap. Nmap, also known as Network Mapper, is one of the most popular security scanner that discovers the hosts, open ports and services on a given network. It helps to determine the security of the network [12]. The flowchart used for observing the network traffic is as shown in the Figure 8.

We have also observed the network traffic through Wireshark. It is the most common tool having a Graphical User Interface (GUI) for the analysis of the packets by capturing the packets, filtering the packets, network troubleshooting etc.

A. NMAP Traffic Observation

As shown in the Figure 8, the IoT device is plugged in to start. The camera does not act as an Wi-Fi access point, and hence it is connected to newly created access point to observe the traffic. The IP address of the device can be obtained from the MIPC app (Network Tab). To find the open ports the Nmap is run on the acquired IP address. The nmap is run using the following command:

$$> \text{nmap} \ -\text{sV} \ -\text{O} \ -\text{v} \ \ 192.168.137.76$$

The output of the nmap shows the open ports on the network are port 80 and port 8600. Port 80 is the common Internet

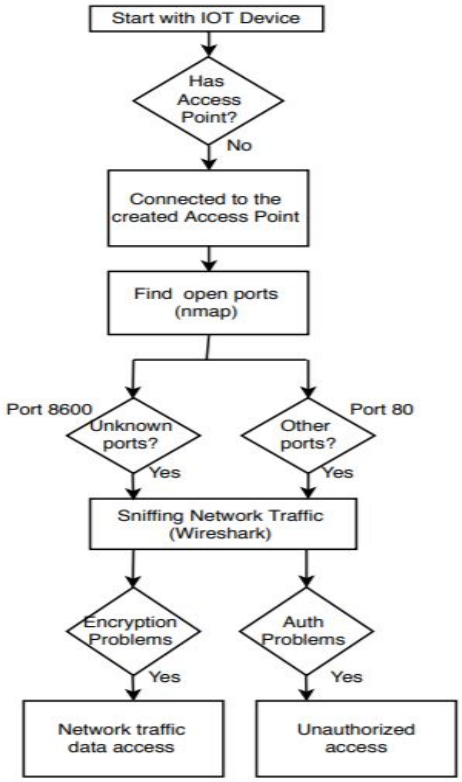
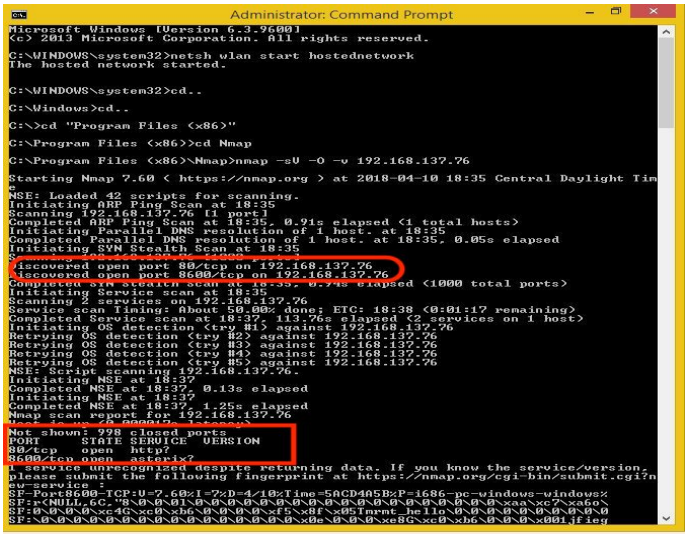


Fig. 8: Flow chart of capturing network packets



Communication Protocol, which is used to connect to internet. As the device is connected to internet, this port is used [13].

The other open port is 8600 port, which refers to All purpose STructured Eurocontrol suRveillance Information eXchange (ASTERIX). Asterix is a format used in air traffic control to transmit radar data. A major warning observed while using this port is that it might close any app that runs under Java, and is used by this port [14]. The output of the Nmap is as shown in the Figure 9

Apart from the open ports, you can also observe that the

Fig. 9: Output of Nmap command

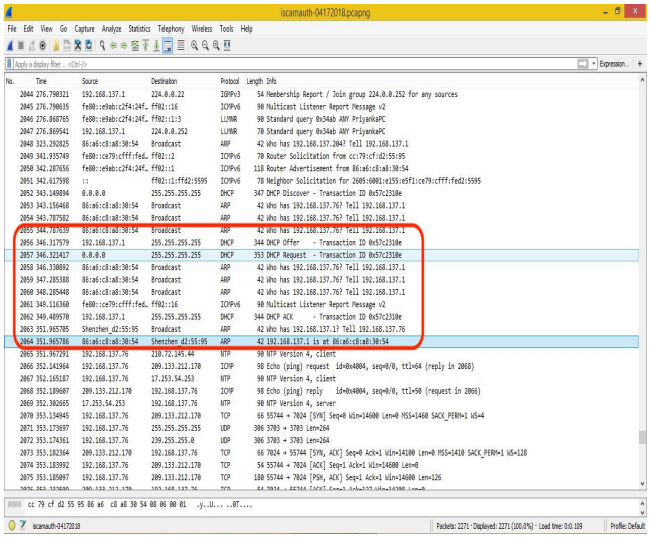


Fig. 10: Address Resolution Protocol between security camera and Wi-Fi access point

Device ID is clearly available. Also the MAC Address of the device and the Network Distance can also be obtained. The network distance indicates the number of devices, which are connected between the connected device and the Wi-Fi Access Point.

B. Wireshark Traffic Capture

Wireshark is one of the best network sniffing tools, that helps to capture the network traffic from the any network. In this, we have started the Wireshark process, before plugging in the camera. When the camera is plugged in, an Address Resolution Protocol (ARP) was carried out to ensure that the device is connected to required Wi-Fi [15]. The flow of the ARP is as shown in Figure 10.

After the connection was set, the data was sent to the cloud of MIPC app, which was observed to be the IP address 209.133.212.170. The data is continuously monitored, which

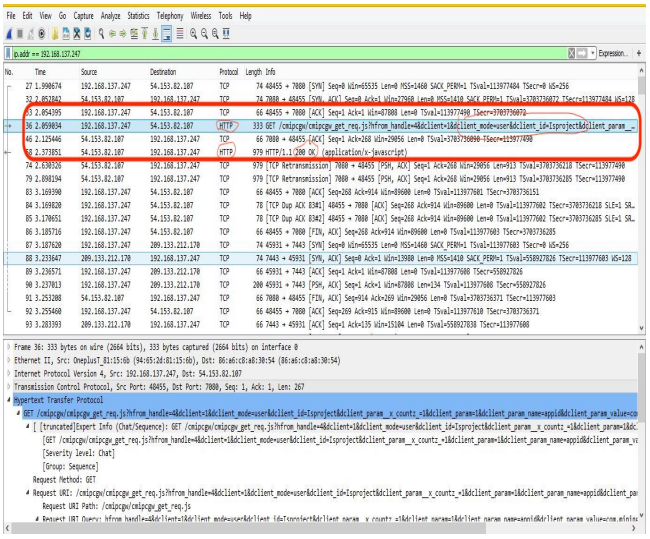


Fig. 11: Login Attempt from Smart Phone into MIPC app

was sent in the form of UDP packets. Also, while capturing packets, we have observed that the device does not send any authentication details to the cloud through the network indicating that the camera was power plugged at a particular moment.

We have captures packets, while monitoring the video through MIPC app and observed that whenever the app is opened, it is sending the login credentials for that account to the cloud, to ensure video camera associated with that account would be monitored as shown in Figure 11. In the above figure, we can clearly observe that the GET login request is sent through HTTP request, and the Login Success (Code:200) is received through HTTP request. Also the login id has been clearly shown in the request and later, the data from cloud is sent to device comprising of the MIPC app in the form of UDP packets.

V. ANALYSIS OF THE CAPTURED PACKETS

In the analysis of the captured packets from previous sections, we have observed that initially, the LeFun Baby Monitor broadcasts its IP address to establish connection with the specific access point. The length of each UDP packet sent from the camera to the cloud is nearly vary from 900 bytes to 1400 bytes. UDP (User Datagram Protocol) is a connection-less and unreliable protocol mainly used for establishing low-latency and loss tolerating connections in-between the applications on the Internet. As the User Datagram protocol run on top of the Internet Protocol (IP), we sometimes refer it as UDP/IP protocol. While TCP is much more reliable, but using UDP for video streaming is preferable for the following reasons: [16]

- TCP prevents the use of IP multicast, but UDP is very well suited for IP multicast.
- Using TCP, the OS buffers all the unacknowledged segments.
- Live video stream would be of constant bandwidth typically, but it is difficult or TCP to serve live video

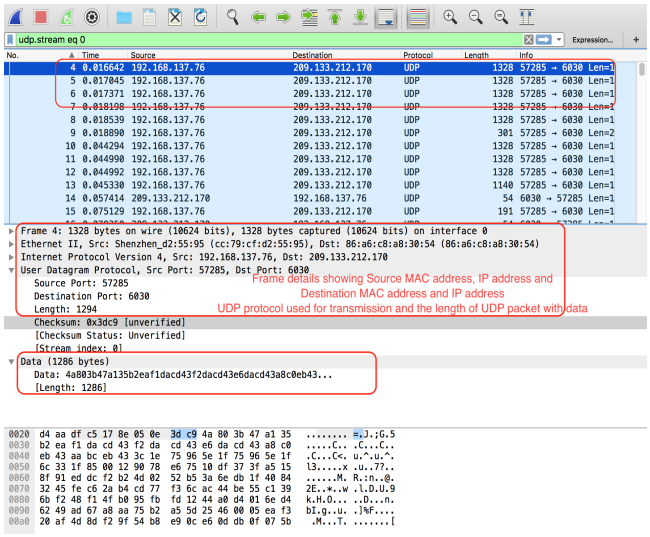


Fig. 12: Details of UDP packet transferred from Lefun baby monitor to cloud.

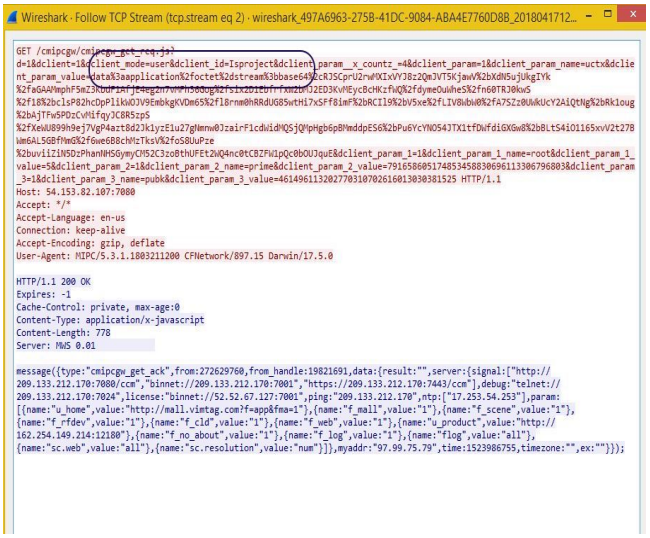


Fig. 13: Login URL description sent to cloud from MIPC app

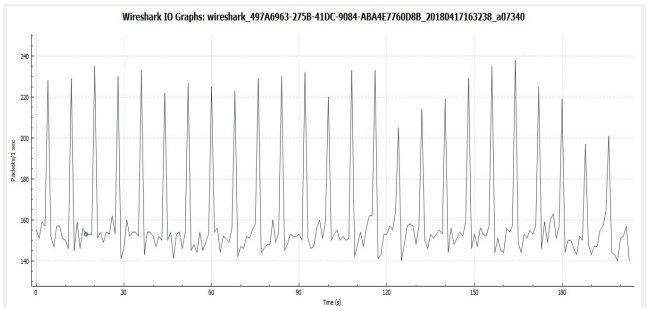


Fig. 14: Number of packets transmitted in still mode

streaming at constant bandwidth due unusual connection breaks.

The UDP packet with data sent from the baby monitor to the cloud is as shown in Figure 12. From the above figure, we can observe the UDP packets include the source and destination address, length of data sent from the packet and the length of the UDP packet. Also, we can clearly observe that the UDP protocol is using only Simple Service Discovery Protocol (SSDP) on top of it. The SSDP is a network protocol used for the discovery network services and presence information. SSDP does not use any encryption mechanism or signature mechanism. [17]. This shows that the UDP packets directly transfer the data without any encryption.

Apart from the camera to cloud network traffic, the packets transferred between cloud and smart phone are also analyzed. When the data is GET request is sent from MIPC app to cloud to authenticate the data is sent in the form of HTTP packet. The HTTP packet consists of GET information as shown in Figure 13, which was analyzed, and we have observed that the GET request sends parameters of client user name and the encoding used for the sending the URL through the network is ”data application octect stream Base 64 encoding”. There are open tools available online to decode the GET URL and obtain parameter values from it.

As already mentioned in the description, the Wi-Fi camera can be controlled using MIPC app. The camera can be moved in all the four directions using the app. The packets are captured and analyzed using Wireshark in five possible scenarios:

- When the view in front of camera is in still mode.
- When the view is in continuous motion in front of the camera.
- When the camera is rotated using the MIPC app
- When the activity in front of camera is normal.
- When the camera is operated in night mode.

In each possible scenario, the data is observed such that number of packets are transmitted between the device and cloud. The transmitted packets can be used by an attacker to estimate the environment surrounding baby such as detecting the presence of a person around baby or not. An attacker can also monitor all the activities of baby and might learn about baby’s daily routine, his habits,etc. The observations are taken out using the exclusive graph creation feature present in Wireshark. The Wireshark calculates the number of packets sent per second using the IO Graphs. It helps to determine the density of the traffic in the network [18].

A. When the view in front of the camera is in still mode:

We have created this scenario at home, by ensuring that there is no movement of objects present in the frame. The traffic was captured using Wireshark per tick (0.05 seconds) and the graph was created. The graph consists of Number of packets per second on the Y-axis and seconds scale on the X-axis. Based on the requirements, the graph can be updated for obtaining the number of bits or bytes transferred per second.

From the graph in Figure 14 it can be clearly observed that the number of UDP packets that are sent from camera to cloud is uniform at regular intervals of time. It can be concluded from the graph in Figure 13 that the uniform number of UDP packets are being transferred in regular intervals of time. The graph is taken for packet transfer of about 200s (nearly

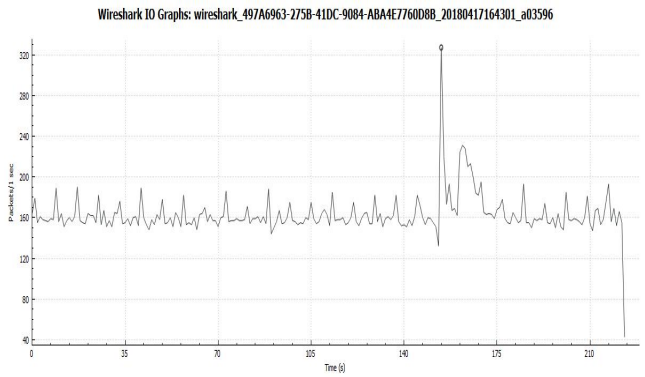


Fig. 15: Number of packets transmitted in continuous motion

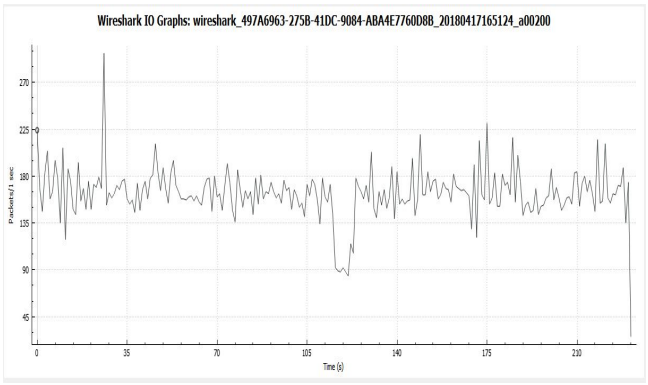


Fig. 16: Number of packets transmitted when camera is in motion

3.5 minutes). The number of packets being transferred on an average is around 230 per second.

The low points in the graph represent the ping messages sent by the camera using ICMP protocol. The ping messages were observed to be sent mostly for about every 2 seconds, as there exists no motion, the camera tries to ensure the connectivity of network as similar frames were transmitted in still. The poor connectivity could be due to the fluctuations in the Wi-Fi network, which might lead to the disturbances in the connection. Hence, the ping messages were sent by the camera.

B. When the view is in continuous motion in front of the camera:

This setup was ensured by creating continuous motion such as some one is moving or walking, or doing some work in front of the camera. The packets are captured in this scenario and the graph is as shown in Figure 15. This graph also shows the overall traffic captured in packets per second. The number of packets being transferred on an average is around 180 per second in this view. But the low points are very less, which as observed have shown that, there are minimal pings or ICMP packets being transferred in this situation, as there is continuous frame change occuring.

We have noticed that the average number of UDP packets being transferred per second during continuous motion view is less than the average number of packets being transferred per second in still view. The length of the packets transferred during motion view is also observed to be greater than the length of the packets transferred in still view. The less number of packets transferred per second might be due to the capture of relative changes by the camera. The sudden notch in the graph is due to the change of continuous motion to a still position at one moment of time. This was clearly observed, as Wireshark provides a great feature of observing the graph simulataneously, when the network traffic was captured.

C. When the camera is rotated using the MIPC app

As already mentioned, MIPC app provides the privilege to rotate the camera (that is, it acts as a remote). This scenario was observed when the camera is rotated using the app in a smart phone. At this scenario, the packets are captured in

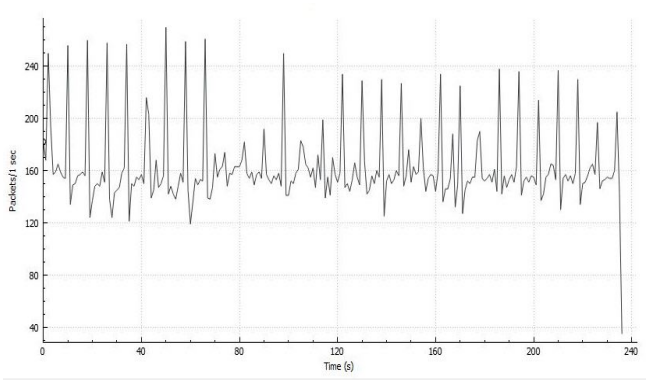


Fig. 17: Number of packets transmitted in normal mode

Wireshark and the graph is generated with number of packets per second on Y-axis and seconds on X-axis as shown in 16. The graph is more similar to the graph obtained when the camera is in continuous motion, because, when the camera rotates, the view infornt of the camera always change and hence the data is continuously updating. As a result, it similar to the existence of continuous motion infront of the camera.

The sudden spikes in the camera at the end of the graph is due to the movement of vigorously, such that it is hard for the camera to identify the new frame and transmit it. Hence, in such situations the camera works as in still mode, as it cannot differentiate frames.

D. When the activity in front of camera is normal:

The graph shown in Figure 17 includes the view camera in normal mode as similar to a camera present in a home having normal activity. There are combination of both still frames and motion frames in this graph. The number of packets being transferred on an average is around 180 per second. But, as it can be observed in the graph, It can be noticed that the graph is not uniform, at a particular interval, the low spikes are observed when there is motion in front of the camera. Hence, the UDP packets are not transferred with a constant bandwidth. In still view, we observed that more number of packets were transferred per second than the number of packets transferred during motion view. The lowest points in the graph represent

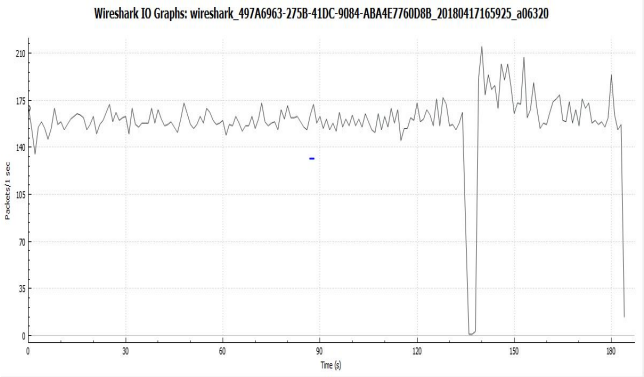


Fig. 18: Number of packets transmitted in night mode

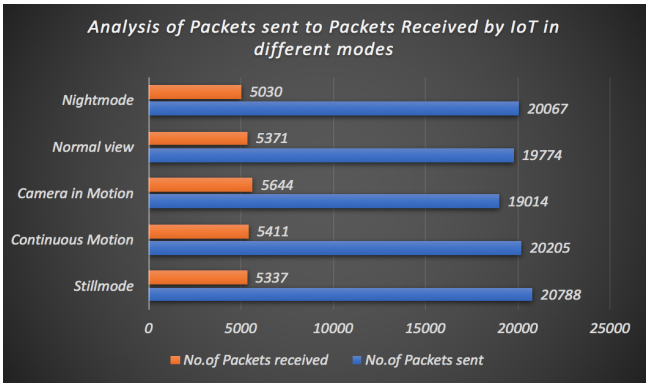


Fig. 19: Number of packets transmitted in night mode

the ping messages sent by the camera to the server using ICMP protocol.

E. When the camera is operated in night mode:

The Lefun baby monitor has an extra ordinary characteristic of collecting data packets during nights using its IR night mode. There is a switch at the top of the camera, which helped us to enable the night mode and observe the traffic. The graph shown in Figure 18 shows packets captured per second in night mode. We have captured packets continuously by creating the motion at the beginning of the process and kept the view at still mode after a while. It was noticed that there isnt significant change in the average number of packets transferred per second in day light view and night view. Almost length of the packets in both the cases were similar.

Also, while observing the video from the app, we have noticed a significant amount of lag in the video in spite of the data being transferred using the User Datagram protocol (UDP).

F. Analysis of transmitted packets to received packets in different modes:

Till the previous section, we have observed only the number of packets transmitted at each mode. In this subsection, we will analyze the number of packets transmitted to the number of received by the camera. Whenever the camera is communicating with the cloud it sends UDP packets to transfer the data. The cloud sends the UDP packets to the camera. These packets comprise of 54 bytes of which 12 bytes include data. The other 42 bytes include Ethernet header, IP header and UDP header. These headers include the source and destination addresses of communicating devices.

We have clearly observed from the Wireshark pcap file that the transmitted and received packets include data attribute. The values are obtained by using the filters in Wireshark such as ip.addr (shows the packets of specific ip address), ip.src (shows the transmitted packets from specific ip address), ip.dst(shows the received packets by a specific ip address), frame.number(shows the packets of specified number in required time interval), frame.len(to observe the length of the packets transmittedd or received). The graph of the number of packets received and the number of packets sent based on different modes is as shown in Figure 19.

As shown in the above figure, we can observe that the number of packets transmitted is almost similar in all the modes on an average of 200 seconds, though they differ significantly at a particular second. Though the still mode sends high number of packets, as it has to ping to check network connectivity, it does not send packets when the ICMP calls were made, where as, in the continuous motion mode the packets are continuously transferred and hence, though they send less number of packets they send equivalent number of packets as in still mode over the given time interval. This interesting analysis shows that the attacker or intruder can know the difference between still mode and motion mode only when he observes the number of transmitted packets per second, but not based on the transmitted packets over an interval of time.

Also, the received packets by the camera have the same scenario of similar count over the certain interval of time. We can also clearly observe from the graph that the number of received packets are nearly one fourth of the total transmitted packets over the selected interval of time. From this, we have observed that in the network traffic, a packet was received from cloud for every four transmitted packets from the baby monitor.

VI. SECURITY ANALYSIS OF THE DEVICE

Pertaining to the functionality of the LeFun Baby Monitor, it should be the secure, as it tracks the activities of the babies and transfer to the MIPC app through cloud. One of the major issues is that the attacker can easily determine the existence of still view and motion in front of the by analyzing the network packets. This could help the attacker to perform malicious activities such as break into house, or scaring the baby by sending unwanted noises through traffic etc. This can be reduced to an extent, if the camera automatically rotates at regular intervals of time.

The LeFun baby monitor can be operated only through the MIPC app. Hence, the analysis is conducted in two parts.

A. Security Analysis based on the LeFun Baby Monitor

The Lefun baby monitor consists of default user name and password, which needs to be updated by the user, after the

initial configuration. If it is not changed, it can allow others to use same credentials, if the device is lost and obtain the recorded credentials. In this baby monitor the videos can be recorded only on the MicroSD card, through the slot provided in the camera rather than storing on some secure cloud. It can let the hackers to steal the camera and obtain video information of the babies.

As discussed in section IV, the data transmitted to cloud is not secure as it does not use any security protocol. Hence, this could potentially let the attackers to send the same video frames that would be transmitted to the MIPC app (Replay attack). As a result, the potential user cannot differentiate between the replay frames and new frames. The attacker can also perform Man-in-the-Middle (MITM) attack by modifying the data in UDP packets. This can also be a greater threat for the users to know the difference between real frames and hacked frames. Also, when the camera is plugged in again, it does not send any authentication details to the cloud. This would add to another vulnerability of the device, due to the potential threat of replay attack by the intruders.

The observations also show that the MAC address and device ID are visible in the Network traffic and Nmap analysis. As a result, address spoofing can be possible if attacker can get hold of the MAC address. He can send packets as to the cloud as the legitimate device and get hold of the packets sent from the camera.

B. Security Analysis based on MIPC App

The traffic was observed when the MIPC app of the camera is connected through both android and iOS device. We did not observe any comprehending security issues when the data is transferred from two different devices. In this scenario, the MIPC app provides multiple authentication with same credentials on different devices. When a new device having credentials logs in to monitor, it is not notified to other existing users. Also, there is no option available in the camera to know how many users are accessing the camera at the same time. This could be a potential issue when the credentials of the app are compromised.

As already mentioned in the capturing network packets section, the user login of the MIPC application involves octect base 64 encoding, which is not highly secure as SSL encryption. It can be a potential threat that an attacker can either try to get the password, or use the same GET request to authenticate again. Also, when the application is logged in once through the mobile, it does not log out automatically, when the camera connection is lost or when the user closes the app. The user get access or control to LeFun baby monitor by clicking on the application. This could be an important issue when the smart device monitoring the IoT device is lost, a malicious user can get hold of this IoT device, as there is no feature to disconnect an unwanted device from the account. In this case, the malicious person can control the camera, spy on the activities of baby etc. that would affect the privacy of users.

The sign up instructions of the MIPC app includes some requirements as [4]:

- Username should contain at least 6 characters beginning with a letter.
- Password should contain 6-20 characters.
- Password should start with a letter but can include only letters and numbers.
- You should confirm the password before sign up once it is entered.

During login, the application does not require any email id, but the user can bind the email id after logging in. This can be used to obtain password reset link. If the user forgot the password, and did not bind the email, the account credentials can never be retrieved. In this case, the user should recreate a new account.

ACKNOWLEDGMENT

The authors would like to thank Department of Computer Science of University of Texas at Dallas (UTD) and Prof. Dr. Alvaro Cardenas for providing the setup and equipment required to perform this research. The authors would like to thank personally Prof. Dr. Alvaro Cardenas for providing all the guidance and support through out the research and for supporting to understand the concepts involved in Network Security and Information Security.

REFERENCES

[1] *LeFun Wireless Camera, Baby Monitor WiFi IP Surveillance Camera HD 720P*, https://www.lefunsmart.com/products/lefun-c2-wifi-camera?variant=5042536129, 2018

[2] Jinish KG, Nourdine M *Enable WiFi Access point in Windows 8*,https://social.technet.microsoft.com/wiki/contents/articles/16495.enable-wifi-access-point-in-windows-8.aspx, March 20, 2013.

[3] *Configuiring WINDOWS 7 to provide secure wireless access point services to Wi-Fi Clients - Turn WINDOWS into an access point*, http://www.firewall.cx/microsoft-knowledgebase/windows-xp-7-8/968-windows-7-access-point.html, April 20, 2018.

[4] *LeFun IP Camera Quick Install Guide*, http://files.lefunsmart.com/docs/LeFun%20C2&C6%20User%20Manual.pdf

[5] *Data Privacy Policy*, https://babycamapp.com/dpp.html, 2017.

[6] *Baby Monitor's Direct Privacy Policy*, http://babymonitorsdirect.com.au/privacy.html, 2012.

[7] Deborah K,*Overview of CIPA, COPPA, and FERPA*, https://www.spps.org/cms/lib/MN01910242/Centricity/Domain/11270/OverviewofCIPACOPPAandFERPA12.2015.pdf, Technology Services, 2015.

[8] *Privacy Policy for Mipc Web Sites*, http://mipcm.com/disclaim/index.htm.

[9] Wash L, *Mother: Hacked baby monitor discovered after son heard voice*, https://www.kiro7.com/news/mother-says-she-discovered-hacked-baby-monitor-aft/43487803, April 20, 2015.

[10] Charlie DM, *Baby monitor hacker sends a frightening message to Indianapolis family*, http://fox59.com/2015/08/27/baby-monitor-hacker-sends-a-frightening-message-to-indianapolis-family/, October 1, 2015

[11] Craig S, *7 Creepy Baby Monitor Stories That Will Terrify All Parents*, https://www.buzzfeed.com/craigsilverman/creeps-hack-baby-monitors-and-say-terrifying-thing?utm_term=.gbD3zmjXw#.be490kQy5, July 24, 2015.

[12] *Nmap Tutorial: Common Commands*,https://www.networkcomputing.com/networking/nmap-tutorial-common-commands/520799832, April 1, 2018.

[13] *Port 80*, https://www.techopedia.com/definition/15709/port-80.

[14] *ASTERIX*, https://wiki.wireshark.org/ASTERIX, September 2014.

[15] Chris H, *How to Use Wireshark to Capture, Filter and Inspect Packets*, June 14, 2017.

[16] Eddie P, *TCP vs UDP on video stream*, https://stackoverflow.com/questions/6187456/tcp-vs-udp-on-video-stream, May29, 2015

[17] Ting C, Paul L, Ye G, Yaron YG, Shivaun A, *Simple Service Discovery Protocol/1.0*,https://tools.ietf.org/html/draft-cai-ssdp-v1-01.

[18] *IO Graphs*, https://www.packtpub.com/mapt/book/networking_and_servers/9781783989522/3/ch03lvl2sec26/io-graphs