HomeSpy: Inferring User Presence via Encrypted Traffic of Home Surveillance Camera

Yushi Cheng
Zhejiang University
Hangzhou, Zhejiang
Email: yushicheng@zju.edu.cn

Xiaoyu Ji
Zhejiang University
Hangzhou, Zhejiang
Email: xji@zju.edu.cn

Xinyan Zhou
Zhejiang University
Hangzhou, Zhejiang
Email: xinyanzhou@zju.edu.cn

Wenyuan Xu
Zhejiang University
Hangzhou, Zhejiang
Email: xuwenyuan@gmail.com

***Abstract*—Wireless cameras are widely deployed in homes and offices for security guarding, and play as an important part of smart home devices. Those security cameras, which are supposed to provide protection services, however, may in turn leak personal privacy that can result in security issues. In this paper, we reveal that attackers are able to eavesdrop the traffic of wireless cameras and analyze whether you are at home or not without entering the house. We propose `HomeSpy`, an attack tool that infers the house status by inspecting the bitrate variation of the wireless camera traffic. We implement `HomeSpy` on the Android platform and validate it on 3 cameras. The evaluation results show that `HomeSpy` can achieve a successful attack rate of 97.2%.**

I. Introduction

Home security cameras are widely deployed to provide protection services ranging from home security, baby monitoring, to fall detection. WiFi wireless cameras, i.e., Internet protocol cameras equipped with WiFi modules, are booming among home security camera market due to their flexibility and usability. According to Technavio [1], the global wireless video surveillance market will continue to grow at a rate of 21.35% over 2014-2019. However, despite of its popularity and convenience, we discover that wireless security camera, which is supposed to provide protection services, is likely to leak personal privacy and becomes a tool for attackers.

Already, an increasing attention has been paid to the privacy issues caused by wireless cameras. Much work has been proposed to safeguard personal privacy against cameras. Ashok et al. [2] introduces an "invisible light beacon" implemented on the eye-wear to prevent unauthorized videotaping. The authors in [3] focus on the privacy concerns caused by "first-person" wearable cameras. Birnbach et al. [4] detects drones carrying out privacy invasion attacks with on-board cameras.

Different from previous work, our paper focuses on the wireless security camera and reveals from a perspective of attackers that, home security camera may leak your personal information. We propose `HomeSpy`, an attack tool that is able to analyze whether you are at home or not, by eavesdropping the wireless camera traffic. As shown in Fig. 1, an attacker tries to figure out whether there are humans inside a target house. She runs `HomeSpy` on her smartphone outside the house to infer the house status. `HomeSpy` overhears and analyzes the wireless traffic, and informs the attacker that the owner is not at home. Obtained this information, the attacker may conduct further malfeasance and result in serious security issues.

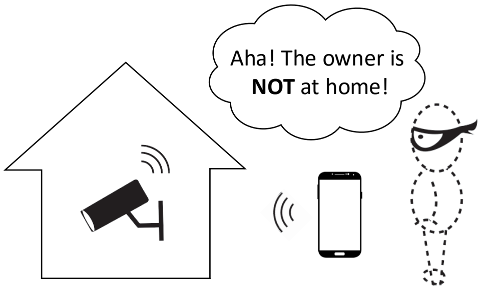


Figure 1: `HomeSpy` is able to infer the house status by eavesdropping the wireless camera traffic.

The underlying principle of `HomeSpy` is that the number and size of video/ audio frames of wireless camera traffic are not fixed and depend on the video/ audio content. If a human is within the filming range of the wireless camera, the frame number and size will change with the human intervention (i.e., motion and sound). By exploring the human intervention in wireless camera traffic, `HomeSpy` shall be able to infer whether the owners are at home or not, i.e., the house status.

Inferring the house status via wireless camera traffic is promising yet challenging. Since an attacker has no access to the house as well as its WiFi network, `HomeSpy` shall work without joining the network. In addition, there might be various devices inside the house that generate wireless traffic, `HomeSpy` shall figure out whether there is a wireless camera and which packets belong to the wireless camera. Furthermore, camera traffic is encrypted and thus traditional image/ audio processing techniques are invalid in this scenario. `HomeSpy` shall exploit new angle to reveal the information ensconced in the camera traffic.

To overcome all aforementioned challenges, `HomeSpy` eavesdrops network traffic near the target house with a smartphone and detects the existence of wireless cameras inside the house based on their MAC addresses. Then, `HomeSpy` examines the existence of human beings inside the house by inspecting the bitrate variation. In summary, our contribution includes below.

- We reveal that wireless security cameras are potential sources of privacy leakage, i.e., the house status, which may result in serious security issues.
- We propose `HomeSpy`, an attack tool that is able to analyze whether owners are at home or not, by eavesdropping the network traffic of wireless security cameras.

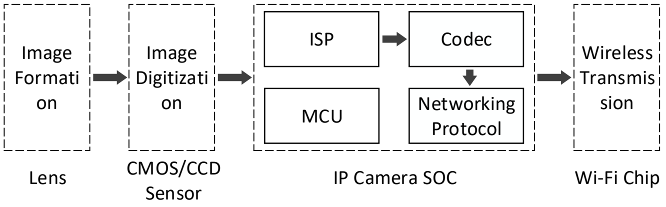


Figure 2: Hardware modules inside a wireless camera.

- We implement HomeSpy on the Android platform, and validate it on 3 popular wireless security cameras (Ezviz, Dahua and Yi). The results demonstrate that HomeSpy can successfully attack with a probability of 97.2%.

II. Background

A. Basics

Wireless home security cameras provide real-time video surveillance through a wireless network operating at license-free frequencies (e.g., 2.4 GHz). With the build-in image and audio sensors, wireless cameras can monitor target environments (e.g., homes and offices) and generate continuous video and audio streams. Typically, instead of saving records locally, wireless cameras process the video/ audio streams and then upload them through an access point (AP) of a wireless local area network (WLAN) to a remote cloud server. Modern wireless cameras therefore allow users to achieve remote monitoring by accessing the cloud server.

The hardware modules for a wireless camera are shown in Fig. 2. Image scenes from the lens are first digitalized by the CMOS/ CCD sensors which continuously generate raw video/ audio frames. The raw multimedia frames are then fed into an SOC (system on chip), i.e., a multimedia SOC that contains a MCU and three additional submodules: (1) Image signal processing (ISP) submodule that performs functions such as noise filtering. (2) Codec submodule that compresses video/ audio frames to decrease frame sizes. It utilizes the redundancy between consecutive frames and outputs a series of coded frames whose number and size depend on the video/ audio content. (3) Networking protocol submodule that encrypts traffic to ensure privacy safety and guarantees reliable transmission of multimedia stream via streaming protocol like RTSP (real-time streaming protocol).

B. Human Impact on Wireless Camera

For privacy protection, the camera traffic is encrypted in the SOC chip. Thus, an attacker cannot obtain the video/ audio content from the traffic directly. However, after conducting an exhaustive research on the working mode of the wireless camera, we find that the encrypted camera traffic can still reveal privacy information.

As mentioned above, the number and size of video frames are not fixed and depend on the video content. When the video content changes, the number and size of frames increase to capture the discrepancy of the content. That is to say, if a human is within the filming range of the wireless camera, he may alter the frames of the inside wireless camera. If the wireless camera captures his movement, the number and size of the frames may change along with the human motion. Similarly, the voice from the human also increases the audio traffic.

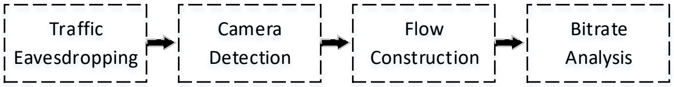


Figure 3: The workflow of HomeSpy.

Thus, both motions and voices from a human being may increase the frame number and size of the wireless camera, which will result in a larger amount of traffic and thus a higher bitrate. This finding sheds light upon the insights of HomeSpy. As humans may impact the traffic of the inside wireless camera, the bitrate of the wireless camera may in turn reveal whether there is any people inside the house.

III. Attack Model

A. Workflow of HomeSpy.

The workflow of HomeSpy is composed of four steps: traffic eavesdropping, camera detection, flow construction and bitrate analysis, as shown in Fig. 3. First, HomeSpy sets the WiFi card on the smartphone into monitor mode and captures network traffic over wireless channels near the target house. Then, HomeSpy detects the existence of wireless cameras inside the house based on their MAC addresses. In the flow construction step, HomeSpy only extracts the Length and Source MAC Address fields [5], and discards other unnecessary information to improve processing efficiency. Finally, HomeSpy feeds the constructed camera flow into the bitrate analysis model and examines the existence of human beings inside the house by inspecting the bitrate variation.

B. Traffic Eavesdropping.

A straightforward method to eavesdrop the network traffic is to join the network, however, the attacker usually has no access to the WiFi password. Even she does, most WLANs are encrypted with WPA/ WPA2-PSK. These methods exploit per-client, per-session keys, which are derived from the WiFi passwords and the information exchanged when a client joins the network [6]. As a result, even with the WiFi password, it is difficult for the attacker to capture all four handshake packets to derive the keys.

To eavesdrop the wireless traffic of the target house without joining the network, HomeSpy collects data with smartphone's WiFi card set in monitor mode. Normally, a smartphone sets its WiFi card in managed mode in which packets not destined for this smartphone are discarded [7]. However, HomeSpy requires to eavesdrop the nearby wireless traffic for analysis. To this end, the WiFi card shall be set into monitor mode such that HomeSpy is able to capture and record all the passing packets.

We implement the monitor mode function on the Android platform based on an open-source project named Nexmon [8]. Nexmon provides a basic API for WiFi driver modification. We use a UDP socket to read packets from the rawproxy application which connects to the WiFi card buffer in Nexmon.

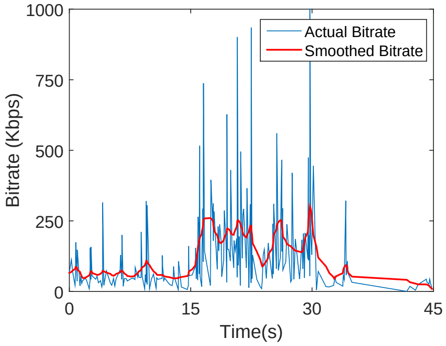


Figure 4: Impact of human beings on the bitrate of the camera flow.

Once receiving a packet via the UDP socket, the packet is decoupled and collected for camera detection. In this way, HomeSpy is able to eavesdrop the network traffic on the sly.

C. Camera Detection.

HomeSpy detects whether there are wireless cameras inside the house based on their MAC addresses. Most home security cameras in the market are from several well-known manufacturers, such as Hikvision, Dahua, YI and 360. We can simply diagnose the existence of them by examining the first 24-bit of their MAC addresses. These bits are assigned to manufacturers by the Institute of Electrical and Electronics Engineers (IEEE) and thus represent the identity of the manufacturers. For example, cameras from Hikvision have MAC addresses beginning with 8C:18:D9, A4:14:37, BC:AD:28 and etc. Cameras from Dahua may have the first 24-bit like 4C:11:BF, and 3C:EF:8C. For YI cameras, it shall be 58:70:C6.

Therefore, we are able to detect a wireless camera by investigating its MAC address. After eavesdropping wireless traffic in the air, HomeSpy examines the source MAC addresses to detect the existence of cameras. It compares collected MAC addresses with a camera MAC address list to locate camera flows as well as filter the non-camera traffic.

D. Flow Construction.

In the flow construction step, HomeSpy constructs collected camera packets into flows. It only extracts the Length and the Source MAC Address fields of the camera traffic, and discards other unnecessary information to improve processing efficiency.

If there are more than one camera, HomeSpy groups collected packets into each flow for each camera device according to their MAC addresses. Then, the camera flow, which is in a time sequence, is fed into the bitrate analysis.

E. Bitrate Analysis.

As mentioned in Sec. II, if a human is within the filming range of the wireless camera, the frame number and size will change with the human intervention (i.e., motion and sound), as well as the bitrate. An illustration is shown in Fig. 4, in which a human keeps moving during the period from 15 s to 30 s. As a result, the bitrate of the camera flow also shows a rise during this period and there is only a one second lag between the reactive bitrate of the camera and the movement. With this observation, we are able to utilize the bitrate variation of the camera flow to infer the house status: void or non-void.

To detect the changes of bitrate caused by human beings, HomeSpy utilizes the cumulative sum control chart (CUSUM) [9] algorithm to detect the rising edges of the bitrate sequence r. CUSUM is a sequential analysis technique typically used for change monitoring. The CUSUM algorithm for bitrate variation detection is as follows:

$$U_n = \begin{cases} 0, & n = 0 \\ \max\left(0, U_{n-1} + r_n - w_n\right), & n > 0 \end{cases} \tag{1}$$

$$Condition : U_n > \delta, n = 0, 1...N \tag{2}$$

where U_n is the upper cumulative sum at the time n. w is the likelihood estimation of the bitrate sequence. δ is the threshold for detecting inside human beings. If the value of U_n exceeds δ, HomeSpy outputs that the owners of the house are at home, otherwise, HomeSpy believes they may have gone out.

IV. Performance Evaluation

In this section, we evaluate the performance of HomeSpy. We first present the setup, then the evaluation metrics, and finally the results of attacks.

A. Experimental Setup

Experiment Scene. We perform experiments in an apartment with a wireless camera installed in the bedroom. The attacker is outside the apartment with a distance of $3m$ and runs HomeSpy application on a LG Nexus 5 smartphone in realtime to infer the house status.

Camera brands. We select 3 typical cameras from several well-known manufacturers on the market in our experiments: Ezviz [10], Dahua [11] and Yi [12].

B. Performance Metrics

True Positive Rate (TPR). We define TPR as the rate of correctly inferring of human existence.

True Negative Rate (TNR). We define TNR as the rate of correctly inferring of human absence.

Successful Attack Rate (SAR). HomeSpy attacks the wireless camera to infer the house status. Thus, both true positive and true negative are successful attacks. Hereby we define $SAR = \frac{TP+TN}{TP+TN+FP+FN} \times 100\%$ as the successful attack rate.

C. Attack Performance

1) Overall Performance: In the first set of experiments, we evaluate the overall performance of HomeSpy.

Three volunteers participate in the experiments. To simulate the non-void status, the volunteers are asked to walk around for 15 seconds inside the apartment. For the void status, the apartment has no human beings inside. For each status, we utilize HomeSpy for inference and repeat 30 times.

The results in Tab. I reveal that HomeSpy can successfully attack with an average SAR of 97.2%. It verifies that home

Table I: The overall TPR, TNR and SAR of HomeSpy.

Brand	TPR (%)	TNR (%)	SAR (%)
Ezviz	96.7	96.7	96.7
Dahua	100	93.3	96.7
Yi	96.7	100	98.3

security cameras can indeed leak the house status. False positives mainly come from the fluctuation of bitrate resulted from the dynamic of network environment. Based on the ROC curve in Fig. 5(a), we utilize a large threshold and sacrifice a bit of accuracy to achieve a low false positive rate.

Next, we consider several factors that could affect our ability to infer the house status.

2) Impact of Motion Range: Due to that the bitrate variation is resulted from human motions, motion range may affect the inference performance. Larger motion range results in more bitrate variation, and thus may improve the inference accuracy.

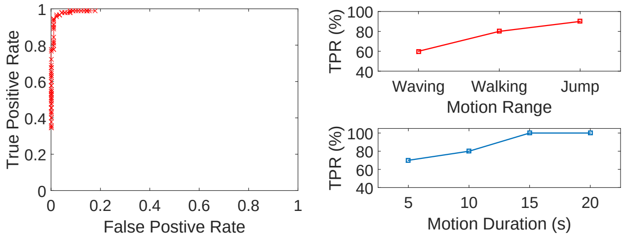
To investigate the impact of motion range, we conduct experiments with three common motions: waving (wave hands), walking (walk around the room) and jump (jump up and down). Apparently, the intensity of motion is strengthened from front to back. In the experiments, motion duration is set to 10 s and 10 attacks are lunched for each motion. The results in Fig. 5(b) show that the TPR does increase with the growth of motion range. Even with slight movements such as waving hands, HomeSpy can still successfully attack with a rate of 60% while jump holds the highest probability with 90%.

3) Impact of Motion Duration: Another influencing factor of HomeSpy is the motion duration time. Long duration of human intervention helps to overcome the transient variation of bitrate caused by the dynamic network environment and thus may decrease the false positive rate.

To evaluate the impact of motion duration, we conduct experiments with four typical time durations: 5 s, 10 s, 15 s and 20 s. The results are also revealed in Fig. 5(b), which confirm that the longer the time duration is, the better the attack accuracy will be. Even with only 5 s of human intervention, HomeSpy is able to successfully attack with a rate of 70%. With the increasing of the duration time, the TPR is promoted to 100% with 15 s as well as 20 s.

V. Related Work

Recently, an increasing attention is paid to the privacy issues caused by cameras. Most work safeguards personal privacy against cameras from the view of defenders. Ashok et al. [2] introduces an "invisible light beacon" implemented on the eye-wear to prevent unauthorized videotaping, by which the privacy preferences of photographed users are communicated to photographing cameras. The authors in [3] focus on the privacy concerns caused by "first-person" wearable cameras. They propose methods to identify and prevent the sharing of sensitive images captured by wearable cameras. Birnbach et al. [4] detects drones carrying out privacy invasion attacks with on-board cameras. This work analyzes the RSSI (received signal strength indicator) of the wireless traffic from the cameras on the drone to detect the approaching of drones.



(a) The ROC curve of HomeSpy.

(b) The impact of motion range and motion duration.

Figure 5: The ROC curve (a) and impact of motion range and duration (b) of HomeSpy.

HomeSpy is inspired by previous work and reveals that home security cameras can leak personal information, i.e., the house status, form the perspective of attackers.

VI. Conclusion

In this paper, we reveal that home security cameras can leak personal privacy that may result in security issues. We propose HomeSpy, an attack tool that is able to analyze whether you are at home or not, by eavesdropping the wireless home security cameras. We implement HomeSpy on the Android platform and validate it on 3 cameras. The evaluation results show that HomeSpy can achieve a successful attack rate of 97.2%. As directions for future work, it is worth investing whether home security cameras can leak more personal information.

VII. Acknowledgment

This work is supported by China NSFC Grant 61702451, the Fundamental Research Funds for the Central Universities 2017QNA401.

References

[1] Technavio, *Global Video Surveillance Market 2016-2020*, November 2015, http://www.technavio.com/report/global-it-security-video-surveillance-market.

[2] M. Korayem, R. Templeman, D. Chen, D. Crandall, and A. Kapadia, "Enhancing lifelogging privacy by detecting screens," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 4309–4314.

[3] R. Templeman, M. Korayem, D. J. Crandall, and A. Kapadia, "Placeavoider: Steering first-person cameras away from sensitive spaces," in *NDSS*, 2014.

[4] S. Birnbach, R. Baker, and I. Martinovic, "Wi-fly?: Detecting privacy invasion attacks by consumer drones," in *NDSS*, 2017.

[5] I. C. S. L. M. S. Committee *et al.*, "Wireless lan medium access control (mac) and physical layer (phy) specifications," 1997.

[6] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, "A survey on wireless security protocols (wep, wpa and wpa2/802.11 i)," in *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*. IEEE, 2009, pp. 48–52.

[7] D. Bradbury, "Hacking wifi the easy way," *Network Security*, vol. 2011, no. 2, pp. 9–12, 2011.

[8] D. W. M. Schulz, *Nexmon*, April 2005, https://github.com/seemoo-lab/nexmon.

[9] Wikipedia, *CUSUM*, March 2017, https://en.wikipedia.org/wiki/CUSUM.

[10] Ezviz, *C2C*, March 2017, https://www.ys7.com/item/12.html.

[11] Dahua, *Lechange TC1*, March 2017, https://www.lechangebuy.com/index.php/product-62.html.

[12] Yi, *2*, March 2017, http://www.xiaoyi.com/homeCamera/first/first.html.