CamBurglar: Detection of Hidden Wi-Fi Cameras

Project Repository: https://github.com/yuxi-wu/camburglar

May Nakari, Jessica Wang, Ratul Esrar, Yuxi Wu

ABSTRACT

The goal of this paper is to present a system, *CamBurglar*, that can detect hidden cameras, thus giving both individuals and organizations the resources to adequately protect themselves from the possible malicious threat that hidden cameras may hold. This is accomplished through the use of Wi-Fi traffic analysis and RFI localization techniques in order to accurately determine the presence and possible location of potential hidden Wi-Fi cameras. We perform traffic analysis, RF localization, and magnetic frequency data collection in two different home settings.

1. INTRODUCTION

As technology advances, it becomes easier and easier to produce smaller and cheaper cameras that can be easily concealed. A search on Amazon for “hidden cameras” produces over 10,000 results, with cameras costing as little as $7.90. The cameras are disguised as a wide variety of items, ranging from clothes hooks to pens to USB ports.

Obviously, these cameras can be used in a positive manner – providing surveillance and intruder detection to give the user security. However, it cannot be ignored that these cameras can also be utilized for a more sinister purpose. Ease of access to these hidden cameras raises a new problem of the abuse of these cameras.

There have been multiple instances of illegal and harmful activity. On August 9th, 2017, a hidden camera disguised as an outlet in a toilet stall was discovered inside a women’s bathroom in an Illinois Walgreens, with 20 victims caught on the camera [1]. In addition, the online marketplace and hospitality service Airbnb has had a multitude of scandals and concerns regarding the use of hidden cameras. On October 11th, 2017, a Florida man was charged after a couple found a hidden camera in the smoke detector of his Airbnb property [2]. These instances of misuse and abuse of hidden cameras clearly bring up issues of security and privacy for regular consumers.

The potential to detect hidden cameras holds significant implications in terms of security and privacy. For private individuals, being able to detect these hidden cameras can prevent unsuspecting people from falling victim to surveillance without their permission. Even for professional law enforcement use, hidden camera detection can be an asset to guard against espionage and other criminal acts. Building an application, that can detect cameras concealed within objects, gives both individuals and organizations the resources to adequately protect themselves from the possible malicious threat that these hidden cameras hold.

The goal of this paper is to successfully detect the presence of a hidden camera through a Wi-Fi inspection application built in Python, *CamBurglar*. This is accomplished through a three-step process. First, we use a standard Wi-Fi receiver (a laptop) to passively packet sniff the transmissions from surrounding Wi-Fi devices using the “sniffer” feature in Wireless Diagnostics on macOS. Using the WireShark application’s command line tools, we are able to extract key information from the sniffed data, such as MAC addresses and RSS values.

Once the data is collected, we analyze the traffic to differentiate the camera from all the other devices within the environment. Through this analysis, we identify key features that demonstrate the presence of a hidden camera – specifically, these distinguishing factors are small, constant streams of sent Wi-Fi packets. We then extract the MAC address and the RSSI of the suspicious device for further analysis.

We then proceed to use RF localization techniques in order to accurately localize the hidden camera. This paper focuses on hidden cameras used indoors, meaning that the GPS trackers within smartphones cannot be used. Instead we gather the (x,y) data for the room of focus ahead of time. Using sniffing to capture the RSSI and MAC address data at each foot, we can then filter by the known MAC addresses of the suspicious devices that we extract from traffic analysis. Given the MAC address, we apply the log-distance path loss (LDPL) model to return the estimated (x,y) coordinates of the suspicious device. We plot a map of the room displaying the (x,y) location of the camera.

We apply the technique of adversarial localization using RF signals to determine the location of the suspicious device. While adversarial localization is commonly associated with criminal and illegal acts, this hidden camera detection ultimately utilizes adversarial localization for good [3].

In the final part of our process, we collect data to confirm whether or not the suspicious device is indeed a camera. The user can navigate to the predicted (x,y) location of the device, and collect the magnetometer readings. We have determined typical ranges of a camera so that the user can determine whether or not the suspicious device is, in fact, a hidden camera.

We performed numerous experiments in two different residential apartments and on-campus environments. Our work seeks to emphasize the importance of hidden camera detection.

2. BACKGROUND

There has been more and more research produced on indoor Wi-Fi localization, as its potential as a vital information service for mobile devices has become more apparent. Currently, the majority of existing works utilize AoA (angle-of-arrival), Bluetooth, radio frequency techniques, and more [3]. However, most of these methods require constant communication with a target and would therefore be unideal for the purpose of illegal or unwanted surveillance.

Adversarial localization refers to situations where an attacker attempts to locate wireless transmitters using localization techniques. However, with the knowledge that unwanted hidden cameras are becoming more and more common, our app – CamBurglar – focuses on utilizing similar methods found in adversarial localization attacks to instead detect hidden cameras broadcasting on a wireless network.

Previous experiments to pinpoint a transmitter location utilize antenna arrays, directional arrays, and signal reflectors to cap transmission coverage. However, these methods incur a much higher cost and are constrained by environmental factors. Although prior research in this field has found that device anonymization is effective in concealing a device by its ID, traffic detection and analysis of signals can be used to effectively categorize different types of devices, like cameras [5]. We demonstrate this in our process of Wi-Fi transmission sniffing.

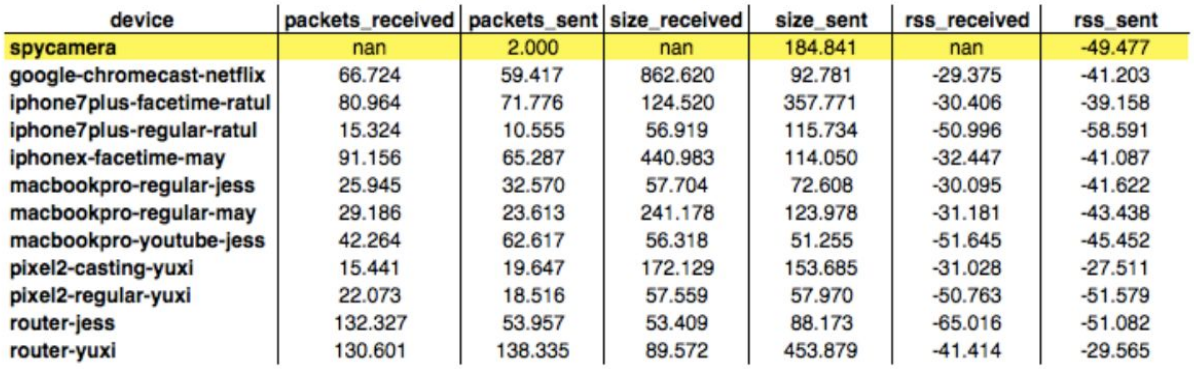
RSS-based localization is one of the most widely-used and cheap techniques for localizing targets in an indoor and outdoor environment. RSS methods convert signal strength to a receiver using different distance measurements [4]. It is known that RSS data can, however, be impacted due to obstacles like walls, objects, etc., that reflect the signals. Therefore, we will test the accuracy of CamBurglar when a hidden camera is obfuscated by another body.

3. SOLUTION

1. TRAFFIC ANALYSIS

3.1.1 PACKET SNIFFING

In order to accurately differentiate the camera, we use a standard Wi-Fi receiver (a laptop) to passively packet sniff the transmissions from surrounding Wi-Fi devices using WireShark on macOS. Using WireShark's command line tools and Python data analysis techniques, we are able to extract key information from the sniffed data, such as MAC addresses, packets sent and received, and RSS values.



device	packets_received	packets_sent	size_received	size_sent	rss_received	rss_sent
spycamera	nan	2.000	nan	184.841	nan	-49.477
google-chromecast-netflix	66.724	59.417	862.620	92.781	-29.375	-41.203
iphone7plus-facetime-ratul	80.964	71.776	124.520	357.771	-30.406	-39.158
iphone7plus-regular-ratul	15.324	10.555	56.919	115.734	-50.996	-58.591
iphonex-facetime-may	91.156	65.287	440.983	114.050	-32.447	-41.087
macbookpro-regular-jess	25.945	32.570	57.704	72.608	-30.095	-41.622
macbookpro-regular-may	29.186	23.613	241.178	123.978	-31.181	-43.438
macbookpro-youtube-jess	42.264	62.617	56.318	51.255	-51.645	-45.452
pixel2-casting-yuxi	15.441	19.647	172.129	153.685	-31.028	-27.511
pixel2-regular-yuxi	22.073	18.516	57.559	57.970	-50.763	-51.579
router-jess	132.327	53.957	53.409	88.173	-65.016	-51.082
router-yuxi	130.601	138.335	89.572	453.879	-41.414	-29.565

Table 1: Device data used in our experiment.

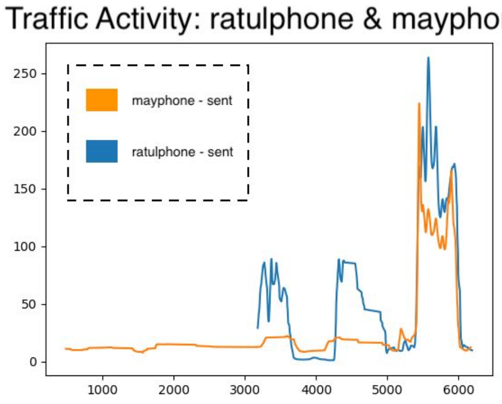


Figure 1: Traffic activity of ratulphone and mayphone.

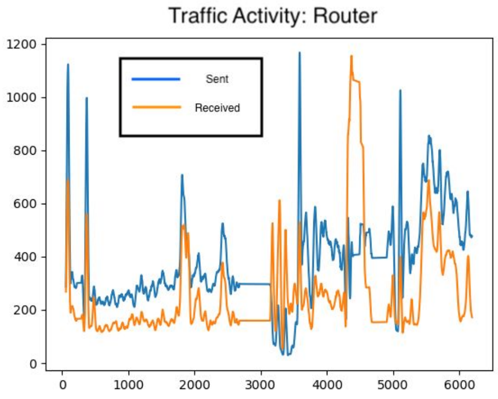


Figure 2: Traffic activity of Netgear router.

3.1.2 MEASUREMENTS

We performed measurements on a DigiHero Wi-Fi Spy Hidden Camera disguised as a mobile smartphone wall charger. We placed this hidden camera in 2 different residential apartments, and also used other devices that could potentially produce similar traffic – using smartphones, laptops, Google Home, and a ChromeCast to stream. In addition, we staged a FaceTime video-call, between two smartphones within the apartment for further comparisons. Two laptops (Apple Macbook Air & Macbook Pro) were used to sniff the data. The results are displayed in Table 1.

3.1.3 TRAFFIC DIFFERENTIATION

Once we collected the data of the different devices, we plotted the data in order to graphically display the traffic activity. The figures for mayphone & ratulphone (Figure 1), the Netgear router (Figure 2), and the hidden spy camera (Figure 3 - next page), are displayed.

The hidden spy camera has a very distinctive activity signature as compared to the other devices. *Packets_received*, *size_received*, and *rss_received* are all *nan* (not a number). In addition, the *packets_sent* rate is exactly 2 packets/second, which is a huge contrast to the traffic activity of other devices.

With this knowledge, we extract the MAC address and the RSSI of the suspicious device for further analysis.

2. RF LOCALIZATION

We then proceed to use RF localization techniques in order to accurately localize the hidden camera. Since our focus is on hidden

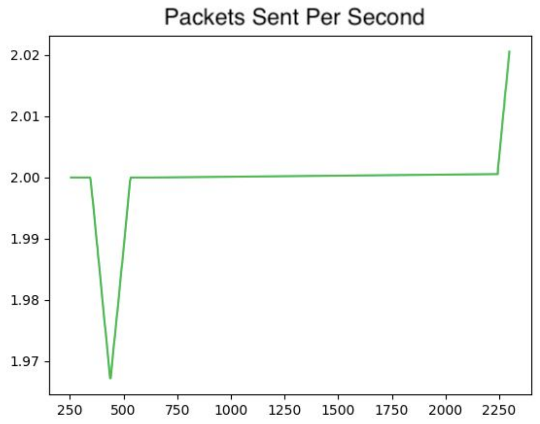


Figure 3: Traffic activity of USB spy camera.

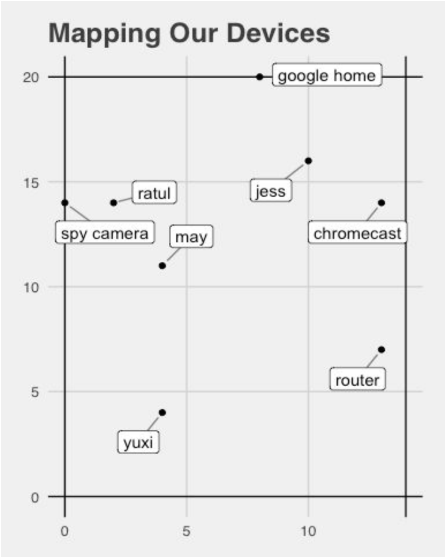


Figure 4: Localization mapping of devices.

cameras that are generally used indoors, the GPS trackers within smartphones cannot be used to localize the camera. Instead, we gather the coordinate (x,y) data for the room of focus ahead of time in feet.

After sniffing to capture the RSSI and MAC address data in a room by walking along the walls, we can then filter by the known MAC addresses of the suspicious devices that we extract from traffic analysis. Given the MAC address, we apply the log-distance path loss (LDPL) model to return the estimated (x,y) coordinates of the suspicious device. The LDPL model is one that is well-known and robust against biased spatial coverage [7].

DEVICE	MAGNETIC FREQUENCY (μT = micro Tesla)
General Environment	30 µT
USB Hidden Spy Camera	50-60 µT
MacBook Pro Camera	70 µT
Target Self-Checkout Camera	100-110 µT
Stove	130 µT
Apartment Doorbell Buzzer	1,200 µT
iPhone X Front Camera	1,500 µT

Table 2: Magnetic frequency data.

Once we localize the camera, we can plot a map of the room displaying the (x,y) location of the camera in relation to other known devices. This is displayed in Figure 4.

3. MAGNETIC CONFIRMATION

In the final part of our process, we collect data to confirm whether or not the suspicious device is a hidden camera. The user navigates to the predicted (x,y) location of the device. Then, using the magnetometer readings, we determine typical ranges of a camera so that the user can determine whether or not this isa hidden camera.

We use an Android application, *Hidden Camera Detector,* that utilizes the magnetic sensor on the Android smartphone. The magnetic frequency is read in μT (micro Tesla). We test to determine whether the hidden camera displays any notable trends in magnetic frequency that the user can read to confirm whether the suspicious device is, indeed, a hidden camera. We compare the magnetic readings of the USB spy camera to readings of other devices, such as iPhones, Macbook laptops, stoves, and apartment buzzers. The data are displayed in Table 2.

The results show that the USB spy camera does emit 60 μT on average, which is similar in value to other cameras such as the Macbook Pro camera. Because the ambient environment measures to an average of around 30 μT, it is clear that this hidden spy camera gives off a noticeable electromagnetic frequency. However, the accuracy of the readings can be strongly affected by the surrounding environment – refrigerators, outlets, and TVs give off electromagnetic waves that greatly impact the reading from the magnetometer on a smartphone.

4. EVALUATION

We evaluate *CamBurglar* in the practical settings of different apartments using a DigiHero Wi-Fi Spy Hidden Camera disguised as a mobile smartphone wall charger. We test how accurate our methods of data collection are in the presence of multiple devices transmitting information and how accurately we can pinpoint the suspected device on an (x,y) plane using the LPDL model. Finally, we observe CamBurglar's error tolerance and possible limitations to take into consideration.

Experiment Setup. Our experiments take place in two different apartments. We connect and turn on the DigiHero hidden camera so that it is recording video. In the first apartment, other known devices in the room transmitting data include a Google Home, an iPhone 7 Plus, an iPhone X, two MacBook Pros, a Google Pixel 2, and a Netgear router. Our results from sniffing traffic data using one of our Macbooks can be seen in Table 1.

Limitations. We face some limitations that could also be possible challenges for future applications similar to CamBurglar. When using the DigiHero Wi-Fi Spy Hidden Camera, we find that the camera's magnetic readings are too small to be picked up as significant. When we attempt to detect its lens using a magnetometer, sometimes we would only pick up the readings from the outlet it is connected to, indicating that the spy camera's magnetic field is greatly affected by its electronic connection or battery. Therefore, this could imply that hidden cameras disguised as objects might not be accurately flagged as suspicious by a user when searching for a hidden camera based on magnetic reading alone. Another limitation in our camera detecting technique is that we can only sniff for devices on the same Wi-Fi channel. Currently, WireShark's command line tools do not allow for specifying which channels to sniff. A future development version of this application may include a way to iterate over different channels, at least for 2.4 GHz networks, which are limited to channels 1-11 in the United States. Extending this application's functionality to cover 5.0 GHz networks poses further challenges, as the available channels increase exponentially. Moreover, when we plot the general (x,y) locations of devices using the LPDL model, we've found that there is an error margin of about a 4-5 feet radius. Lastly, the user must have knowledge of the target room's layout in order to pinpoint the possible location of a hidden camera.

5. CONCLUSION

In this paper, we propose *CamBurglar*, a hidden camera detection system. We performed traffic analysis, RF localization, and magnetic frequency data collection in two different home settings. By building an application that can detect cameras concealed within objects, this gives both individuals and organizations the resources to adequately protect themselves from the possible malicious threat that these hidden cameras hold.

REFERENCES

[1] Wls. 2017. 20 victims recorded on hidden camera found in Walgreens restroom. (August 2017). Retrieved March 11, 2018 from http://abc7chicago.com/20-victims-recorded-on-hidden-camera-found-in-walgreens-restroom/2289719/

[2] Katie Reilly. 2017. Florida Airbnb Host Arrested, Charged With Video Voyeurism. (October 2017). Retrieved March 11, 2018 from http://time.com/4977477/airbnb-florida-video-voyeurism/

[3] Haitao Zheng, Zhijing Li, Yanzi Zhu, Irene Pattarachanyakul, and Ben Zhao. 2018. Adversarial Localization against Wireless Cameras. (February 2018). http://people.cs.uchicago.edu/~htzheng/publications/pdfs/iot-hotmobile18.pdf

[4] Tareq Alhmiedat, Amer Abu Salem, and Ghassan Samara. 2013. An Indoor Fingerprinting Localization Approach for ZigBee Wireless Sensor Networks. (July 2013). https://arxiv.org/pdf/1308.1809.pdf

[5] Bianca BOBESCU and Marian ALEXANDRU. MOBILE INDOOR POSITIONING USING WI-FI LOCALIZATION. http://www.afahc.ro/ro/revista/2015_1/119.pdf

[6] Neelanjana Dutta, Abhinav Saxena, and Sriram Chellappan. Defending Wireless Sensor Networks Against Adversarial Localization. http://www.csee.usf.edu/~sriramc/10_mpdmst_dsc.pdf

[7] L. Li and et al. 2014. Experiencing and Handling the Diversity in Data Density and Environmental Locality in an Indoor Positioning Service. In Proc. of MobiCom.