PhantomMotion: Laser-Based Motion Injection Attacks on Wireless Security Surveillance Systems

Yan He
University of Oklahoma
heyan@ou.edu

Guanchong Huang
University of Oklahoma
guanchong.huang@ou.edu

Song Fang
University of Oklahoma
songf@ou.edu

***Abstract*—Wireless security surveillance systems are widely deployed due to their increased affordability. Motion detection is often integrated into them as the linchpin of the security they provide, detecting when someone is present in its range and then triggering the system to start recording or notifying the property owner. In this paper, we present *PhantomMotion*, a new attack framework to fool the motion detection function of those security systems. It can create fake motion stimuli stealthily by aiming laser beams into the motion detection range, and it confirms a r esponse t o t he s timuli v ia s niffing wi reless traffic. *PhantomMotion* does not require any professional equipment or to perform physical motion within the monitored area. It consists of a novel hardware platform integrating laser control and WiFi sniffing, and a new generative mechanism of motion injection. We develop a smartphone app to implement *PhantomMotion*, validating its efficacy a gainst 1 8 p opular w ireless motion-activated security systems. Experimental results show that *PhantomMotion* can always generate fake motion to successfully trigger the systems, within an average of 12.8 seconds and via moving the laser spot for a mean distance of 1.1 m. Notably, we verify that PhantomMotion works from a distance of up to 120 meters.**

I. Introduction

Wireless surveillance systems have made property security accessible and are widely deployed in smart homes, as they are easy to install and increasingly affordable [1]. Passive Infrared (PIR) motion sensors are often integrated with such systems and play vital roles in providing security. They automate device controls (e.g., videotaping detected activity and generating intrusion alarms) for an energy-efficient and safe home. The global wireless video surveillance market was valued at 21 billion US dollars in 2021 and is projected to reach 64.1 billion US dollars by 2031 [2]. Also, the global motion sensor market is expected to grow at an annualized average growth rate of 12.3% from 2023 to 2033, reaching a market size of 2 billion US dollars by 2033 [3].

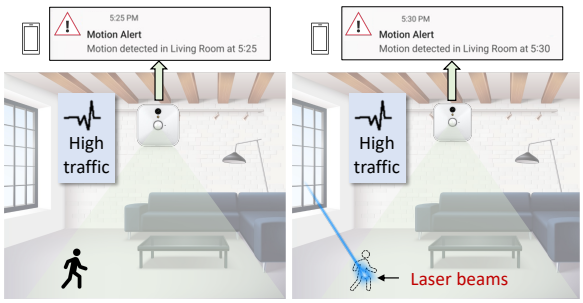
The availability of wireless security systems is a two-edged sword. On one side, such devices improve the safety of our property and family by monitoring and reporting trespassing or other unauthorized activity [4], [5]. On the other side, they may be used for unauthorized tracking or video recording [6], [7], violating individuals' privacy. The spy camera epidemic problem, targeted mostly at women and girls [8], has been a pressing issue in certain countries. For example, in South Korea, more than 30,000 cases of surreptitious filming with hidden cameras were reported to the police between 2013 and 2018 [9], [10]. People rightly value their privacy and do not wish to be recorded in secret, and similarly, malicious individuals such as burglars also do not wish to be recorded.

It is valuable to determine the existence of such cameras or pinpoint them, whether for the innocent individual seeking to protect privacy or the malicious individual seeking to get away with a crime. Emerging research efforts explore wireless camera detection or localization [11], [12], [13], [14], [15], [16], [17], [18], but they share a common weakness, i.e., the requirement to perform human motion in front of the camera. Not all users are willing to perform preset motions, especially a significant one such as jump [11], [12]. In case a user is suffering from physical disabilities, he/she may find it difficult to follow through the required motion schedules [15]. Also, the person performing motion may inevitably expose themselves to the risk of being recorded during the reconnaissance phase. Hence, we are motivated to investigate the feasibility of triggering wireless systems without labor-intensive or pre-designed human motion near the target systems.

Embedded PIR sensors in wireless systems convert received infrared radiation into a voltage. If the voltage exceeds a predefined threshold, the system will be triggered. We explore how to inject radiation similar to what humans generate and fool the PIR sensor, and describe how to utilize a laser, a narrow beam of concentrated light, as the attack signal. Our key idea comes from the fact that lasers can rapidly heat materials via energy transfer [19]. By controlling the laser beams to simulate human motion in the detection area, an adversary can generate fake motion signals to trigger motion-activated wireless security systems, even with a long attack distance. We refer to this attack as *PhantomMotion*.

We use a sample wireless camera as an example to illustrate how *PhantomMotion* works. Figure 1 (a) shows a scenario with real human motion, where a user comes inside the motion detection range. The camera sits in standby mode in static environments. Upon detecting motion, it immediately turns on, starts recording to the cloud, and sends a notification to the property owner's phone. Accordingly, the network exhibits sudden high wireless traffic.

Network and Distributed System Security (NDSS) Symposium 2026
23-27 February 2026, San Diego, CA, USA
ISBN 979-8-9919276-8-0
https://dx.doi.org/10.14722/ndss.2026.231454
www.ndss-symposium.org



(a) Real motion (b) Phantom motion

Fig. 1. Creating phantom motion to trigger cameras.

Now consider the scenario in Figure 1 (b): there is no human motion in the camera's motion detection area, but the attacker wants to fool the camera into believing that motion similar to Figure 1 (a) is occurring. To this end, the attacker shoots a laser beam into the area through the window. The laser is controlled to heat the chosen position for a period until a desired temperature (i.e., around normal body temperature) is reached. As a result, the radiation captured by the PIR sensor embedded in the camera becomes similar to that of a human, triggering the camera, which then generates high traffic and sends out a motion alert. In practice, the camera may be hidden, and the attacker may not know where the exact motion detection range is or if the laser is within it. We accordingly design a customized laser scanning method, which plots a route consisting of evenly distributed points and then determines whether the current laser point lies in the motion detection zone by correlating observed wireless traffic and laser heating time at the point.

Another important challenge is how to control laser heating to generate appropriate radiation at each laser point to activate the camera. Heating for a random duration may produce either insufficient or excessive radiation. The former will not trigger the camera, while the latter will make the relationship between laser heating and traffic difficult to distinguish correctly. Our research reveals that the attacker can achieve laser control by reverse-engineering the motion detection mechanisms of PIR sensors and calculating the laser heating time accordingly.

Besides these issues, there are a variety of wireless traffic flows generated by varying devices. *PhantomMotion* sniffs encrypted wireless packets to detect motion-activated wireless systems. We first coarsely detect the device type by inspecting the Media Access Control (MAC) addresses of captured packets. A MAC address is a persistent globally unique identifier. Consequently, we can flag suspicious traffic flows generated by wireless security systems. By controlling laser heating, we can achieve more fine-grained detection of the security system that monitors the target area.

Unlike existing laser-involved studies (e.g., [20], [21]), which require users to manually operate laser beams, we develop hardware/software prototypes that enable the user to operate entirely through a non-rooted smartphone, making *PhantomMotion* easily accessible to non-technical users. We conduct a real-world evaluation, showing that an attacker can always fool the PIR sensors to activate the wireless system by injecting motion via laser heating, with a mean time of 12.8 seconds. We also verify that *PhantomMotion* can work at a distance of 120 meters, and even when the laser beams are within the non-line-of-sight (NLOS) of the target system.

Impact of Fake Motion Injection: The core value of *PhantomMotion* lies in its ability to remotely simulate human motion, triggering wireless security systems and enabling both offensive and defensive use. Attackers can probe a location without real motion to determine whether it is being monitored, avoiding being caught and forensic exposure. If fake motion triggers a noticeable response, the attacker can avoid that location or select another target. Also, repeated false triggers may harass or desensitize users through a "cry wolf" effect, where frequent false alarms reduce the credibility of true ones [22]. Besides, activation consumes energy, accelerating battery drain for battery-powered systems. Defensively, privacy-seeking individuals can use *PhantomMotion* to detect hidden cameras without physically revealing themselves.

Our main contributions are summarized as follows.

- We propose *PhantomMotion*, the first practical method to activate wireless systems without requiring physical motion in close proximity to them. It can be carried out with a smartphone and needs neither professional equipment nor access to the target system's network.
- We discover an inherent vulnerability of wireless motion-activated systems, where a laser can create a controlled heated position in motion detection zones to inject fake motion signals and trigger the systems.
- We show how a visible laser triggers the system without being recorded by the camera by taking advantage of how the motion detection range and the field of view of the camera's optics are not exactly the same, and how *PhantomMotion* stealthily works with a wall or other obstacles between the camera and the laser.
- We build a low-cost platform with off-the-shelf sensors and develop an app to automate *PhantomMotion* and validate its feasibility, efficiency, and robustness.

II. Principle of Motion Detection

PIR sensors are widely used in wireless security systems, due to their small size, low price, high sensitivity, and ability to work in dark environments. A PIR sensor contains a pyroelectric sensing element that produces voltage output when exposed to heat in the form of infrared radiation (IR) [23]. Figure 2 shows its general structure. A Fresnel lens array condensing light can provide a larger range of IR and focus it to a small point (i.e., the focal point where the pyroelectric sensing element is mounted) [24]. When a warm body, like a person, moves from Location A to B, the emitted IR, denoted as the red dot, passes through the Fresnel lens array. When the person is at Location A, the IR intercepts only half of the sensor (positive element), causing a positive differential change between the two halves; likewise, when the person moves to Location B, only the other half of the sensor (negative element) recognizes the IR, leading to a negative differential

TABLE I
COMPARISON WITH PRIOR RESEARCH EFFORTS IN WIRELESS CAMERA DETECTION.

	Motion in Front of Camera	Carrying a Device during Motion	Motion Type	Motion Duration
DeWiCam [11], [12]	✓	✓ (a phone)	walk/halt; wave hands; jump	default: 15 sec
MotionCompass [13], [14]	✓	✓ (a phone)	walk along a specific route	average: 135∼143 sec
SCamF [18]	✓	✓ (a phone)	stand still; wave hands in varying postures	30 sec (20-sec standing and 10-sec movement)
SNOOPDOG [15]	✓	✓ (a phone and a laptop)	stop-start-stop-start-stop; jump jacks; walk; stand still	Detection: 40 sec; n-trial localization: $30n$ sec
Lumos [17]	✓	✓ (a phone or tablet)	walk around the space's perimeter	within 30 minutes
CSI:DeSpy [16]	✓	×	sedentary/physical activities	8 sec or longer
PhantomMotion	×	×	none	0 (no human motion)

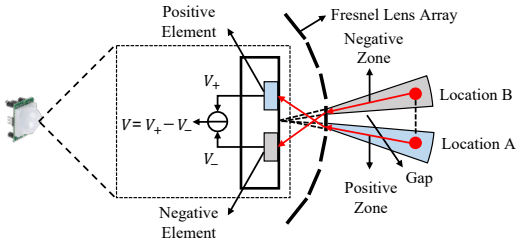


Fig. 2. Structure of a PIR sensor.

change. The sensor's two elements generate respective output voltages, V_+ and V_-, yielding the final output $V = V_+ - V_-$. The absolute value of V is quantized based on a pre-defined threshold V_0 to generate a binary event [25]: motion is detected if $|V| > V_0$; otherwise, no human presence is detected.

Heat Signature: PIR sensors detect the heat (infrared) signature of an object, represented by the physical temperature difference between the object and the background (referred to as ΔT) [26]. According to Stefan-Boltzmann law [27], the power density P, i.e., the energy in watts (W) per unit surface area in unit time, of electromagnetic radiation emitted by a black object (i.e., a hypothetical physical body absorbing all incident electromagnetic radiation) is directly proportional to the fourth power of its absolute temperature. Let Q denote the increased generated heat (i.e., net heat) when the exposure time of the object is t. Let T_e denote the background apparent temperature. Mathematically, we then have

$$Q = P \cdot t = [(T_e + \Delta T)^4 - T_e^4] \cdot \sigma \cdot s \cdot t, \qquad (1)$$

where s is the size of the considered surface (in square meters), and σ is the Stefan-Boltzmann constant and equal to 5.67×10^{-8} $\mathrm{W/m^2K^4}$. The SI (International System of Units) [28] unit for T_e or ΔT is the kelvin (i.e., K for short).

III. RELATED WORK

Wireless Camera Detection: Existing studies to detect a wireless camera mainly include the following categories.

Optical reflection-based: Reflections may be observed as the light bounces off a camera's lens. Traditional optical detectors, such as SpyGuy Camera Detector [29], emanate red light to assist judgment with reflections. A recent study proposes to detect cameras using high-intensity reflection from lenses [30], while such methods require the user to be in close proximity (e.g., 0.5 m) to the camera and scan every corner of the area. The near-distance and frequent scanning process may inevitably disclose the user to the camera.

Thermal/Electromagnetic emission-based: Thermal cameras can reveal heat traces on devices. A Deep Neural Network (DNN) model is built to detect cameras based on their heat dissipation patterns in thermal images [31]. Such a method needs a training process to pre-build a dataset of visual and thermal images. It thus may not be feasible in a strange or uncontrollable environment. If a camera model is unseen in training, the detection performance degrades accordingly. Also, this technique needs the user to repeat trials of taking pictures in front of the camera, posing a significant risk of user disclosure. Another study [32] proposes a camera detection method leveraging electromagnetic emissions stimulated via light. However, its detection range is limited (around 40 cm), and users moving this close may be recorded.

Wireless-based: Recently, many studies have shown the success of leveraging wireless traffic to detect wireless cameras (e.g., [11], [12], [13], [14], [18], [15], [17], [16]). By stimulating the camera with human motion, the resultant wireless traffic may disclose the existence or even the location of the camera. However, all these techniques require the user to laboriously perform motion in front of the camera, and most of them require the user to carry a smartphone to sense the motion via an accelerometer. Such preconditions may cause significant discomfort to the user, and also bring risks of getting caught. *PhantomMotion* gets rid of real human motion and can trigger wireless cameras remotely. We compare our work and previous wireless camera detection schemes in Table I.

WiFi Jamming or Deauthentication Against Cameras: The attacker may utilize a WiFi signal jammer to send signal interference with the same radio frequency as the wireless camera [33], so that the traffic generated by the camera will be disrupted. Also, the attacker can send deauthentication packets, causing the camera to disconnect from the network and attempt to re-authenticate. However, such two suppression methods would wreak havoc on the network and disable all nearby WiFi connections. Besides, as the camera goes offline, the camera app will display an offline status message and an alert accordingly. Moreover, deauthentication attacks do not work for a network with WPA3 - a security protocol employing protected management frames [34]. On the contrary, network

reconnaissance that *PhantomMotion* employs is non-invasive and universal, having no impact on surrounding WiFi devices and working with networks that use various security protocols.

Laser-based Attacks: Recent studies utilize lasers to attack different systems such as unmanned aerial vehicles [35], voice-controllable systems [20], optical beam smoke detectors [36], Light Imaging Detection and Ranging (LiDAR) systems [37], [38], and image recognition systems [21]. For example, as microphones often unintentionally respond to light as if it was sound, [20] injects commands into voice-controllable systems via laser light; [21] manages to fool traffic light recognition by exploiting the rolling shutter of the CMOS sensor. However, such attacks require the laser to point directly at a small area, such as one microphone port [20] or a camera on a vehicle [21]. In contrast, our work is the first laser-based attack targeting widely deployed wireless security systems. It does not need to localize the target system in advance, as the motion detection range is normally much wider, and the proposed laser scanning method can help determine the laser destination.

Another work [39] triggers a PIR sensor by employing a CO_2 laser with a 6 W output that uses a carbon dioxide gas mixture. However, the laser used in that setup is prohibitively expensive, costing several thousand US dollars, and poses significant safety risks due to its high power. Moreover, the study does not evaluate any real-world security system. By comparison, our attack is the first practical method for activating wireless security systems without specialized equipment, with a total cost of approximately 80 US dollars. Meanwhile, [40] uses a 5 mW laser but requires precise alignment with the light sensor. If the laser beam is disrupted or misaligned, the sensor detects a drop in light intensity, triggering the alarm. In contrast, *PhantomMotion* uses a fundamentally different mechanism: it triggers the security system by injecting fake motion signals rather than altering light conditions.

IV. Adversary Model

PhantomMotion remotely simulates human motion, with two general application domains, as aforementioned: (1) as an *attack* targeting wireless security surveillance systems, and (2) as a *defense* targeting spy cameras. In a typical offensive scenario, a malicious user (e.g., a burglar) may (i) find blind spots (i.e., areas not within the camera's peripheral vision) to evade being recorded [41]; (ii) trigger repeated false alerts to harass or desensitize users; (iii) accelerate battery drain by consecutively activating battery-powered cameras. A thief reportedly exploited a surveillance camera's blind spot to steal 5.1 million US dollars from a bank's vault [42]. In a defensive context, a normal user may detect unauthorized recording and obtain corresponding motion detection zones, protecting privacy without being recorded. For the remainder of this paper, we define the "adversary" as an individual (avoiding authority or seeking privacy) interested in triggering the target wireless camera without being detected. Towards the goal, the adversary uses a laser to stealthily simulate human motion, tricking the camera to generate motion alerts when there is no human present in the monitoring area. More specifically, we have the following assumptions.

No Human Motion: Unlike all existing studies (e.g., [11], [12], [13], [14], [15]) requiring human intervention within the proximity of the cameras to activate them, *PhantomMotion* removes such a requirement. Note that introducing real human motion is not an optimal strategy for the adversary, as she or her accomplice (who performs motion) may get caught during this triggering process. We argue that our assumptions are more reasonable than those of the related work, as the adversary will prefer to stay hidden rather than intrude into the monitoring area and disclose her location/identity.

WiFi Sniffing: We assume the adversary can sniff wireless traffic. By triggering the camera and monitoring the resultant traffic, the adversary can determine whether a camera is monitoring the area. In this case, the camera will be activated by the manipulated and fake motion, but will record no event.

Line-of-sight: We assume that the adversary is out of the camera's field of view, with line-of-sight access to the target area, towards which the attacker directs the laser. A scope can be used to observe targets remotely. As heat can transfer, *PhantomMotion* works within the non-line-of-sight (NLOS) of the target system. Note that pre-determining material is unnecessary. The attacker calculates the required heating time for different materials, as discussed in Section V-D2, and can increase heating time as needed.

Knowledge of the Camera's Location is Unnecessary: Commonly, in the "attack" domain, wireless doorbells are installed at doorsteps, and people make wireless security cameras visible as deterrence. For example, property owners may post signs or stickers to warn that the area is monitored by a security camera. Such visibility could help the adversary to quickly determine the possible motion detection range of the camera. However, in the "defense" domain, the spy camera's location is often hidden. Note that when the camera's location is unknown, *PhantomMotion* still works, as it can recognize the existence of wireless cameras by analyzing wireless traffic induced by injected phantom motion.

V. Injecting Motion via Laser Light

A. Feasibility Analysis of Motion Injection

Suppose the human temperature T_h is 37 °C (i.e., 310.15 K). The Celsius scale has an origin translated into 273.15 K as regards the Kelvin one. A human body is not a perfect black body, but it is proved that the difference between the radiation emission characteristics of a human body and a black body is small [43]. Considering the approximate size of a laser point is 1 cm × 1 cm, we regard a unit area $s = 10^{-4}$ m^2. According to Equation 1, when the background temperature T_e is 20 °C, the power density of the radiation emitted by a human body with a unit area can be denoted by

$$\begin{aligned} P_h &= ({T_h}^4 - {T_e}^4) \cdot \sigma \cdot s \\ &= (310.15^4 - 293.15^4) \times 5.67 \times 10^{-12} = 0.01 \text{ W}. \end{aligned} \tag{2}$$

A human may have to disclose at least U unit areas to the sensor to generate enough radiation. Let P_l denote the power

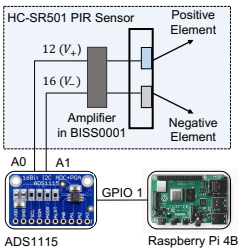


Fig. 3. Raw output.

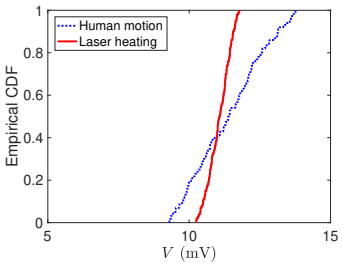


Fig. 4. CDFs of output.

of the utilized laser. When we have $P_l \geq P_h \cdot U$, i.e., the generated power of a laser point is equal to or higher than that generated by a human, the laser is able to trigger the PIR sensor with the generated radiation.

Empirical Verification: We utilize the two sources (i.e., laser and human) to simulate a PIR sensor (with model HC-SR501 [44]) and compare the resultant responses from the PIR sensor. We utilize a FLIR One Pro thermal camera [45] attached to a phone to capture the infrared radiation, which is invisible to the naked eye, and determine that the surface temperature of a walking person is 37 °C, which serves as a reference for the cut-off temperature of laser heating. As discussed in Section II, the PIR sensor only provides a binary output, i.e., 0 (representing no motion) and 1 (indicating motion). The raw voltage output of a PIR sensor can provide fine-grained information about the captured radiation.

We disassemble the HC-SR501 PIR sensor and identify its controller BISS0001, which uses an amplifier to boost the motion-induced voltage [46]. As shown in Figure 3, we use a Raspberry Pi to connect with an ADS1115 module [47] via GPIO 1, where GPIO stands for General Purpose Input/Output; the ADS1115 is a 16-bit analog-to-digital converter (ADC), and its the inputs (A0 and A1) connect to the controller's two outputs (pins 12 and 16), allowing the Raspberry Pi to calculate the PIR's final voltage output $V = V_+ - V_-$.

We let human motion (walking) trigger the PIR sensor. Meanwhile, when no motion occurs, we use a laser to heat the place where the user walks. We monitor the real-time temperature of the heating point via the thermal camera and cut off the heating once the temperature reaches the reference (i.e., 37 °C). For both human motion and laser heating, we perform 100 trials. Likewise, all laser heating attempts successfully activate the PIR sensor. Figure 4 plots the empirical cumulative distribution functions (CDFs) of V under both conditions. We see that the generated voltage for human motion ranges from 9 to 14 mV, while laser heating induces a comparable voltage, varying from 10 to 12 mV, verifying the possibility of using a laser to mimic human motion for triggering PIR sensors.

B. System Overview

PhantomMotion consists of three core phases, *target search*, *spoofing preparation*, and *motion injection*, as illustrated in Figure 5. The initial phase obtains the wireless traffic associated with wireless surveillance devices. The attacker captures the IEEE 802.11 traffic flows over the air, and groups the

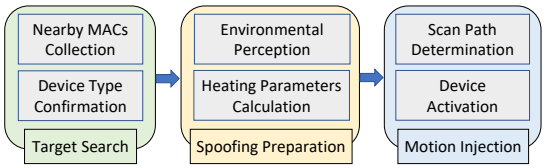


Fig. 5. Three core phases of the proposed scheme.

collected packets based on their embedded MAC addresses. The device type for each scanned MAC can be predicted accordingly. After flagging the traffic flows belonging to potential target wireless security systems, the attacker enters the second phase, consisting of two sequential tasks: (i) to perceive key environmental factors (such as the temperature and heating material); (ii) to determine the corresponding parameters (e.g., heating time at each spot) for laser heating. Finally, *PhantomMotion* monitors traffic flows flagged in the first phase and initializes laser heating along the chosen scan path to inject fake motion into the target wireless security system. By correlating the laser heating time with the wireless traffic that the monitored system generates, *PhantomMotion* can figure out whether the target system is triggered or not. We present the details of *PhantomMotion*'s design below.

C. Target Search

PhantomMotion needs to determine the traffic flow belonging to the device. We identify candidates of the device via the public manufacturer information embedded in MAC addresses.

1) Nearby MACs Collection: PhantomMotion cannot access the same WiFi with the target device and needs to scan all channels the device may operate on. Wireless sniffing tools, such as Airmon-ng [48] that is open source, enable *monitor mode* (i.e., monitoring all wireless traffic nearby) on wireless interfaces. Modern Android smartphones with built-in WiFi chips that support monitor mode can work as traffic sniffers, while it is often required to root the devices [49] and pre-install customized firmware (e.g., [50]).

IEEE 802.11 wireless protocols are used in almost all commodity network devices [51], including various wireless security cameras and alarm systems. Though WiFi networks employ security protocols (WEP, WPA, WPA2, and WPA3) to encrypt transmitted wireless data, IEEE 802.11 management frames are unencrypted, from which we can extract the MAC addresses of the devices that generate the corresponding packets. With a wireless interface in monitor mode, *PhantomMotion* can capture raw wireless packets and collect all MACs, which are fed to the next module for winnowing out the traffic flows belonging to the target security system.

2) Device Type Confirmation: Wireless security systems rely on systems-on-a-chip (SoCs) from manufacturers such as Texas Instruments, Broadcom, and Qualcomm to provide critical wireless communication capabilities. An SoC has a MAC address consisting of 6 bytes (48 bits) that are typically represented as 12 hexadecimal characters. The first 3 bytes are the Organizationally Unique Identifier (OUI), which identifies a manufacturer or a vendor, and the rest 3 bytes represent the

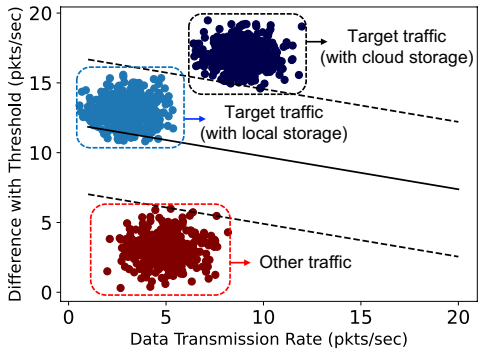


Fig. 6. Traffic flow identification via the built SVM models.

unique device ID. *PhantomMotion* builds a library with public OUI IDs of wireless security systems and utilizes it to look up the device manufacturer for each collected MAC. If a match is found, the traffic carrying the MAC is regarded as being generated by a wireless security system.

MAC Spoofing: The MAC address can be spoofed or randomized. Specifically, a wireless surveillance device can utilize a MAC with OUI belonging to other types of devices. Also, a non-surveillance device can use a MAC with OUI indicating a surveillance system manufacturer. Both cases would confuse OUI-based traffic identification. To overcome such shortcomings, the studies [51], [52] propose to retrieve a device's original MAC with its Universally Unique IDentifier-Enrollee (UUID-E) for building WiFi Protected Setup (WPS) connections. Also, different types of devices may have varying wireless traffic patterns [12], and we can take advantage of this observation to distinguish wireless traffic flows belonging to wireless security systems.

The SoC chip of a wireless system provides data processing and encoding solutions. For example, a wireless camera's SoC (e.g., Ambarella's CV2S SoC [53]) often pre-determines the video encoding methods, including H.264, H.265, and MJPEG. If the wireless system has local storage, it normally sends out event notifications and stores the recorded content locally. To classify traffic flows, we utilize the scikit-learn library [54] to train Support Vector Machine (SVM) models with linear kernels for multi-class classification. The method we use is one-versus-one (ovo). The common 80/20 split is applied to the training dataset for training and validation. Different types of devices may have varying data transmission rates. We set a threshold based on the average data transmission rates of various wireless devices in the environment. For each traffic flow, we calculate the difference between its data transmission rate and the threshold. Figure 6 shows the results after running 2 SVM models on 400 traffic flows from each of the three classes: target device (i.e., wireless security system) with local storage, target device with cloud storage, and non-surveillance devices, demonstrating the success of the traffic flow identification technique.

Limitations of MAC-based Passive Traffic Analysis: MAC-based passive traffic analysis can reveal the presence of wireless devices, but cannot confirm whether a camera is actively monitoring a specific target area. To overcome this, *PhantomMotion* introduces controlled fake motion and correlates it with the resulting traffic patterns. If the observed traffic indicates that the target camera has been activated, we can infer that the injected motion occurred within the camera's motion detection range. Moreover, in crowded environments where multiple cameras may coexist across different locations, passive traffic analysis may yield several candidate devices. Note that even when MAC spoofing occurs, target traffic flows can still be recognized using the built SVM classifier, which recognizes distinctive traffic patterns. *PhantomMotion* then leverages fine-grained traffic-motion correlation to significantly narrow down the set of possible candidates and accurately winnow out the target device monitoring the area.

D. Spoofing Preparation

1) Environmental Perception: To determine the laser heating time at a chosen point, we need to know the environmental temperature T_e and the solid heating material.

We utilize a temperature sensor (e.g., DHT11 [55]) to capture T_e. As the material's temperature increases, the heat is stored in its molecules. When the material cools down, the stored heat is released. Let T_t denote the target temperature that can trigger the motion-activated wireless security system. We aim to simulate human motion with laser heating, and set $T_t = 37$ °C. Different materials may have varying densities and specific heat capacities, which affect the amount of heat required to raise the temperature of a unit volume of a substance. For common building materials (such as wood, iron, and steel), we build a library containing different materials' densities and specific heat capacities, which is prepared for the next step to calculate the heating parameters.

2) Heating Parameters Calculation: Let Q denote the amount of heat required to increase a substance's temperature by ΔT (i.e., $T_t - T_e$) with a volume v. We then have

$$Q = \rho \cdot c \cdot v \cdot \Delta T, \tag{3}$$

where ρ and c are the density and specific heat capacity of the target object, respectively [56]. The laser beam has a spot size of 1 cm $\times$ 1 cm and only needs to heat the surface of the material. Without loss of generality, we consider heating a thin layer with a thickness of 1 mm. Thus, we have $v = 0.1$ cm^3. When the heating power of the employed laser is P, we can then obtain the time t_{min} that it takes for the laser to generate the required heat, i.e.,

$$t_{min} = \frac{Q}{P} = \rho \cdot c \cdot \frac{v \cdot (T_t - T_e)}{P}. \tag{4}$$

For three popular building materials including wood, stone, and brick [57], we calculate t_{min} under varying environmental temperatures based on Equation 4. Meanwhile, we also perform real-world experiments to measure the required time for each material to reach the temperature of T_t with laser heating. Specifically, we utilize a FLIR One Pro thermal camera to monitor the temperature of the laser spot. We cut off the laser once the temperature increases to T_t and

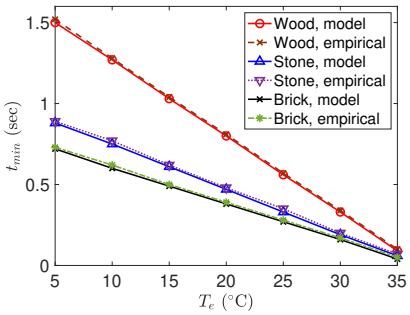


Fig. 7. Required heating time.

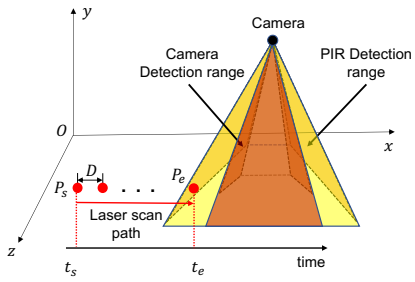


Fig. 8. Outside-in scanning.

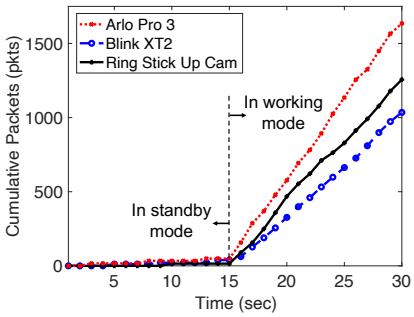


Fig. 9. Cumulative packets.

record the laser heating time. We perform 20 trials for every temperature and compute the average laser heating time. We use the pigpio library [58] to control a GPIO port connected to the laser module, with a sampling rate between 100,000 and 1,000,000 times per second. As a result, we can achieve initiating/stopping the laser heating with the 10 microseconds level of time accuracy.

Figure 7 plots the required time for increasing each material's temperature to T_t with a 100 mW laser under different scenarios, as well as the empirically obtained mean laser heating time. We see that the theoretical and empirical laser heating time values are consistent, and they are inversely proportional to the environmental temperature. Also, regardless of the environmental temperature, the required laser heating time is in the increasing order of brick, stone, and wood.

E. Motion Injection

As discussed in Section IV, in a "defense" scenario, the user may use laser heating to trigger wireless hidden cameras without worrying about disclosing the laser beam; in an "attack" scenario, the malicious user may want to avoid arousing the suspicion of the security camera's owner and thus try to prevent the camera from recording visible laser beams. Accordingly, we propose an *outside-in scanning* strategy to spoof motion via laser heating for triggering most security cameras (including Arlo Pro 2/3, Blue by ADT, and Ring), whose field of view (FOV) is no larger than that of its embedded PIR sensor. For example, a Ring floodlight camera has an FOV of 140° while the FOV of its PIR sensor is 270° [59]. We consider a wireless camera deployed on a vertical wall. Such a case aligns with most practical scenarios. To obtain the maximum horizontal breadth, the camera body is often mounted perpendicular to the wall. Thus, the leftmost or rightmost areas may not be covered by the camera's FOV. Let L denote the distance between the laser and the wall.

As shown in Figure 8, the attacker performs laser heating along the path, which should avoid the camera's FOV and meanwhile monitors the traffic, including the following steps,

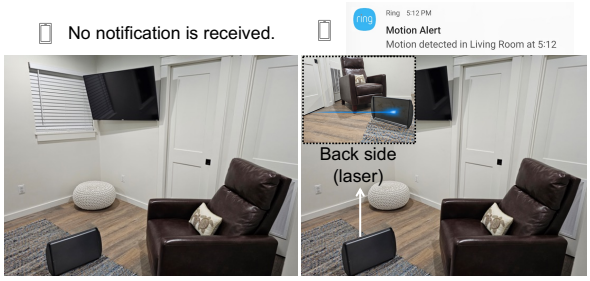
1. Initially select a starting point P_s at the leftmost (or rightmost) area, and track the corresponding time t_s.
2. Heat the selected position to the pre-determined temperature for a period of t_{min}.
3. If the camera is not activated, move the laser point for a distance of D (referred to as the moving step) to the right (or left), and jump to step 2; otherwise, at time t_e, the ending location is marked as P_e, and record the moving angle of the laser beam as θ.

To move the laser point for a distance of D, we need to turn the laser beam for an angle of about $\arcsin(\frac{D}{L})$. Suppose that the laser scans N locations along the path. Accordingly, the length S of the laser scan path can be computed as $S \approx L \cdot \sin\theta = N \cdot D$. For the total time T_o for the spoofed motion to activate the camera, we thus have $T_o = t_e - t_s = N \cdot t_{min} + (N-1) \cdot t_0$, where t_0 is the time spent for shifting the laser beam from one location to another. When the laser angle adjustment process is fast, t_0 becomes negligible, causing $T_o \approx N \cdot t_{min}$. Occasionally, a whole scan path is not within the target motion detection range, leading to the failure of triggering the camera at all locations along the initially chosen scan path. A new scan path can then be selected, and the above three steps are repeated until the attack succeeds.

System Activation Detection: When the wireless security system is triggered from the standby mode, it enters the working mode and responds accordingly (e.g., starting to record videos and send push notifications). The total wireless packets generated by the security system would thus increase at a faster speed within the activation period. The large deviation between the packet generation rates in standby and working modes provides a clue to distinguish the two modes.

We also empirically verify such a phenomenon by installing an Arlo Pro 3, a Blink XT2, and a Ring Stick Up Cam on a wall to monitor a target area. We perform a 30-second test for each device and collect its generated packets. For the beginning 15 seconds, the cameras are in standby mode, while we trigger the cameras for the remaining 15 seconds. Figure 9 plots the count variation of the cumulative packets. In standby mode, the packet count increases quite slowly as only a small number of packets, i.e., periodic heartbeat signals, are generated for synchronization with the server. On the contrary, in working mode, the count of cumulative packets increases with time at a much higher rate, and they show a nearly linear correlation regardless of the camera type.

The discovered correlation between the working duration (when the camera is activated) and total packet count can be explored to determine whether the camera is activated by the



(a) Normal situation. (b) Launching the attack.

Fig. 10. Comparison of camera feeds.

spoofed motion induced by laser heating.

F. Exploring Stealthy Attacks

Occasionally, if the laser beam happens to appear in the FOV of the camera and triggers the camera, it may be spotted via the recordings. To further improve optical stealthiness, the attacker can use an invisible laser wavelength [60] to avoid having the user spot the laser light aimed at the target area. However, there are three disadvantages associated with using an invisible laser: (1) normally, an invisible laser is significantly more expensive than a visible one; (2) an invisible laser is also invisible to the attacker, complicating attack verification; (3) as the body's protective glare aversion response (i.e., blink reflex) can be triggered only by visible light, the exposure risk to invisible laser beams is increased.

Attack in Non-line-of-sight Scenarios: Furthermore, considering that heat can transfer over opaque obstacles/walls, *PhantomMotion* also works within non-line-of-sight (NLOS) of the target wireless system. We can utilize a solid daily object or wall as camouflage. One side of the object faces the camera while we shoot the laser beam at the opposite side of the object. The camera can be triggered once enough heat is transferred to the side facing it.

Let ΔT_0 denote the difference in temperature between the hot surface (heated by the laser) and the cold side (within the motion detection range). The distance between the hot and cold sides (i.e., the material's thickness) is denoted as Δx. Accordingly, the quantity of heat energy transferred (denoted with q) can be obtained from Fourier's law [61],

$$\frac{q}{\Delta t} = -A \cdot k \cdot \frac{\Delta T_0}{\Delta x}, \tag{5}$$

where Δt is the time taken, A is the area of the surface that emits heat, and k is the thermal conductivity (i.e., a property indicating the ability to transfer heat). As the heat flows from the side at a higher temperature to the one at a lower temperature, the heat transfer rate $\frac{q}{\Delta t}$ is always negative.

Meanwhile, during the heat transfer process, there may exist heat loss, causing a temperature drop ΔT_1, which can be modeled via Newton's Law of Cooling [62],

$$\Delta T_1 = \Delta T_0 (1 - e^{-\frac{k}{\Delta x} t}), \tag{6}$$

where t signifies the elapsed time.

TABLE II
TESTED WIRELESS SECURITY DEVICES.

ID	Model	WiFi Chipset	PIR Amount
1	Arlo Pro 2	Cypress	1
2	Arlo Pro 3	Cypress	1
3	Blue by ADT	Cypress	1
4	Blink XT2	TI	1
5	eufyCam E	Hisilicon	1
6	Google Nest Cam	Ambarella	1
7	Google Nest Doorbell	Ambarella	1
8	IHOXTX DF22 Cam	MediaTek	1
9	LaView N15 Cam	MediaTek	1
10	Reolink Argus 2	MediaTek	1
11	Ring Spotlight	TI	2
12	Ring Spotlight Pro	TI	2
13	Ring Stick Up Cam	TI	2
14	Simplisafe Cam	Telit	1
15	Wyze Cam Outdoor v2	Ingenic	1
16	Arlo Home Security System	Cypress	1
17	Ring Alarm System	Quectel	1
18	Simplisafe Safety Alarm	Espressif	1

Let Q represent the heat generated by laser heating, which can be determined with Equation 3. The power of the laser is P and the laser heating time is t_{h_0}. Thus, we have $Q = P \cdot t_{h_0}$. With Equation 5, we can calculate the time t_t needed for heat transfer, i.e., $t_t = \frac{Q}{A \cdot k \cdot \Delta T_0 / \Delta x}$. With obtained t_t and Equation 6, we can obtain the temperature drop ΔT_1 and further compute the laser reheating time t_{h_1} for compensating the heat loss. The total time needed for the heat produced and transferred to the target surface equals $t_{h_0} + t_{h_1} + t_t$. Figure 10 shows a camera triggered by using a laser to heat the backside of an object whose front faces the camera. We see that although the camera is triggered, the captured image remains identical to that in the normal (no-attack) situation.

VI. Experimental Evaluation

We build *PhantomMotion* with low-cost commercial devices and develop an Android app for controlling the hardware platform, with its user interface (UI) presented in Appendix A.

A. Evaluation Setup

To sniff all WiFi data, existing techniques usually utilize specific models of laptops [15], [63] or rooted Android platforms [13], which can enter monitor mode. However, not all laptops support monitor mode, and it may not be convenient to bring a bulky laptop. Also, rooting a smartphone is non-trivial and may make the device vulnerable to cyberattacks [64], [65].

Alternatively, we design a comprehensive, low-cost, and portable system that integrates WiFi sniffing and laser control, as shown in Figure 11, including (1) a temperature sensor (e.g., DHT11) for measuring environmental temperature, (2) a WiFi adapter (e.g., AWUS1900 [66]) in monitor mode, (3) a laser module (e.g., LD-F405E04 100 mW) with a laser level swivel base, and (4) a Raspberry Pi 4B controller interacting with other components. The app connects to the Raspberry Pi board via Bluetooth Low Energy (BLE) to obtain system information

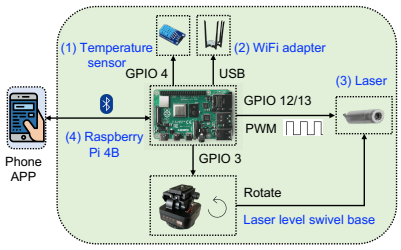


Fig. 11. The testbed that we implement.

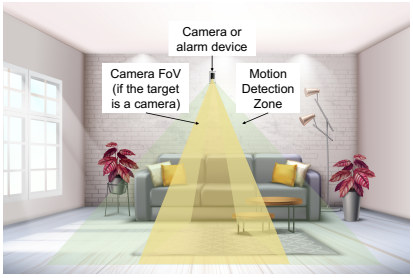


Fig. 12. Experiment environment.

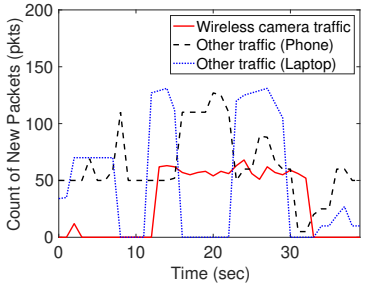


Fig. 13. Traffic observation.

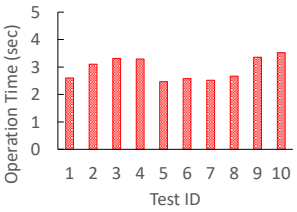


Fig. 14. Operation time.

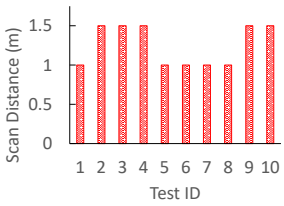


Fig. 15. Scan distance.

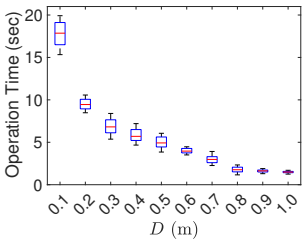


Fig. 16. Time vs. D.

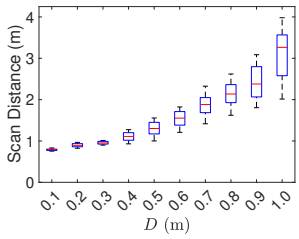


Fig. 17. Distance vs. D.

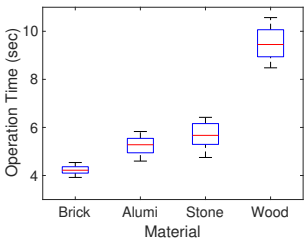


Fig. 18. Time vs. heating material.

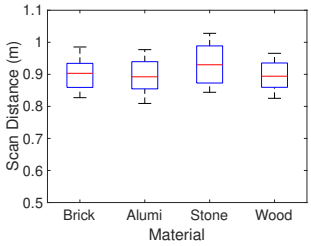


Fig. 19. Distance vs. heating material.

such as laser exposure time and environmental temperature. It can also send commands to the board to turn on/off the laser remotely as well as tilt or rotate the laser level swivel base.

We test 18 popular wireless security devices (15 cameras and 3 alarm systems), as listed in Table II. Three cameras (ID 11-13, referred to as Type 2) have two PIR sensors, while the rest (categorized as Type 1) have one. Figure 12 shows the testing setup: a 400 square feet (20 ft $\times$ 20 ft) living room with a wireless security device mounted on the wall for monitoring.

Metrics: We use the following four metrics.

- *Success Rate:* the ratio between the number of successful injection attacks (i.e., activating the target device) and the total number of attack trials.
- *False Positive Rate:* the possibility that the device is inadvertently triggered by other heat sources (other than real motion and generated fake motion).
- *Operation Time:* the total time spent on triggering the device via the laser-generated fake motion.
- *Scan Distance:* the distance between the initial and the final laser point, at which the device is triggered.

B. Case Study

A Ring Stick Up wireless camera is installed in the room, as shown in Figure 12. *PhantomMotion* is launched 10 times, each with the camera repositioned to cover a different area. The laser module is placed six meters away from the wall with the mounted camera. We set the moving step length D (i.e., the distance between two successive laser points) as 0.5 m.

Figure 13 depicts the nearby traffic flows. The user injects fake motion, and we observe a strong correlation between the camera traffic throughput and the laser heating. The other two traffic flows do not have an obvious relationship with the phantom motion, and they belong to an iPhone in use (online chatting) and a MacBook Pro laptop in web browsing mode, respectively. *PhantomMotion* successfully triggers the target camera for all 10 tests, i.e., the success rate reaches 100%. The false positive rate is 0. The operation time and scan distance are shown in Figures 14 and 15. We see that the average operation time and scan distance are 2.9 sec and 1.25 m, respectively, indicating the efficiency of *PhantomMotion*.

C. Influential Factors

1) Impact of Moving Step Length D: When D is small, the laser may need to point to many spots until triggering the camera, while a large D may lead to a long laser scan path. We vary D from 0.1 to 1.0 m in 0.1 m increments and perform 100 *PhantomMotion* trials for each D, with the camera's location and motion detection range randomized after each attempt. The success rate maintains 100%, and no false positive is observed. As shown in Figure 16, we observe that the median operation time is inversely proportional to D. It is 1.5 sec when D is 1.0 m, and becomes 17.8 sec when D decreases to 0.1 m. This is because a small D requires heating more points until the device is triggered. Figure 17 shows the relationship between D and the scan distance. We see that the median scan distance increases with D, from 0.8 m at $D = 0.1$ m to 3.2 m at $D = 1$ m. These results show that selecting D is a tradeoff between scan distance and operation time. To achieve a desired scan

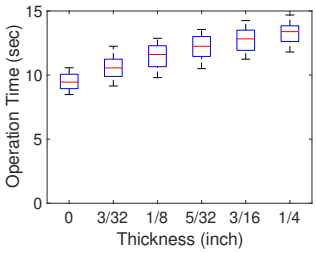


Fig. 20. Time vs. glass thickness.

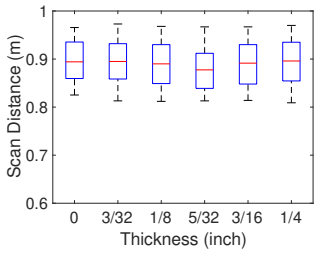


Fig. 21. Distance vs. glass thickness.

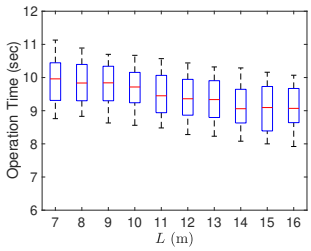


Fig. 22. Time vs. L.

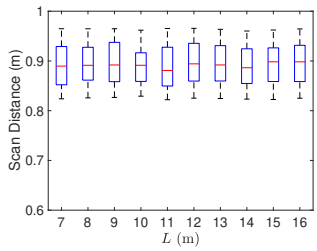


Fig. 23. Distance vs. L.

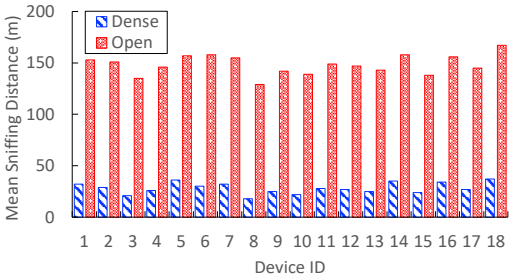


Fig. 24. Sniffing distances for all devices.

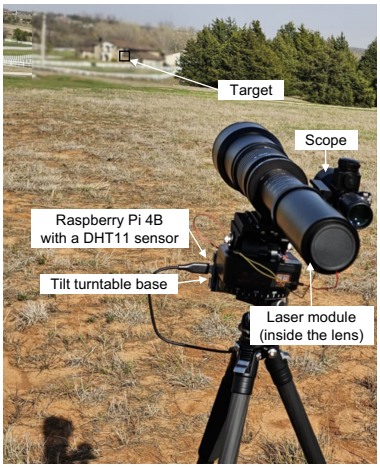


Fig. 25. Laser aiming at the target across the field.

distance (less than 1 m) and a comparably short operation time, we employ $D = 0.2$ m for the following discussions.

2) Impact of Heating Material: We compare four commonly used residential materials: brick, aluminum (abbreviated as alumi), stone, and wood. Their specific heat capacities are 800, 900, 1,000, and 1,700 J/kg · K. For each material, we perform 100 trials of *PhantomMotion*. Again, we achieve a 100% success rate and a zero false positive rate for all heating materials. Figure 18 shows that the operation time increases with the specific heat capacity, while it remains consistently small (less than 10.5 sec) for varying materials. We obtain the median operation time values of 4.2, 5.2, 5.6, and 9.4 sec for brick, aluminum, stone, and wood, respectively. Figure 19 presents the corresponding scan distances. We observe that the scan distance slightly changes with the heating material. The median scan distances for all materials are below 1.0 m. Besides, Appendix B shows that *PhantomMotion* easily adapts to varying heating materials even in NLOS scenarios.

3) Impact of Glass: Soda-lime glass, the most widely used type of glass globally, accounts for around 90% of the flat glass market due to its cost-effectiveness and durability [67]. We select soda-lime flat glass samples with five typical thicknesses: 3/32 inch (single-strength), 1/8 inch (double-strength), 5/32 inch, 3/16 inch, and 1/4 inch [68]. Thicker window glass, including 3/16 inch or greater, is often recommended or required for enhanced protection in hurricane-prone regions [69].

We use 18-inch × 24-inch soda-lime glass sheets of varying thicknesses to simulate residential window glass. For each thickness, we perform 100 trials of *PhantomMotion*, directing the laser through the glass sheet. Experiments without any glass in the laser transmission path are also conducted as a baseline for comparison. Figure 20 presents the obtained operation time. We see that *PhantomMotion* remains effective within a short time (less than 15 seconds), regardless of the glass thickness. As the thickness increases, the mean operation time slightly increases. Specifically, with 3/32-inch glass, the operation time ranges from 9.1 to 12.2 seconds, while at 1/4-inch thickness, it increases to a range of 11.8 to 14.6 seconds. This slight increase appears to result from laser power attenuation, as thicker glass leads to marginally increased absorption and scattering of the laser beam. Figure 21 shows the corresponding scan distances. We see that the scan distance remains consistent across varying glass thicknesses. With glass, *PhantomMotion* dynamically adjusts the laser heating time, while the scan distance is largely unaffected.

4) Impact of Laser Transmission Path Length: We vary the distance L between the laser and the system (i.e., laser transmission distance) from 7 to 15 m in 1 m increments. For each L, we perform 100 trials of *PhantomMotion* and all succeed. Figure 22 shows the obtained operation time. We see the median operation time is always less than 10 sec. With L increasing, the operation time slightly decreases. This appears as for a larger L, the required angle that the laser needs to turn is smaller for moving the laser point with a distance of moving step (i.e., D). The decreased time for laser angle adjustment lowers the operation time. Figure 23 plots the corresponding scan distances. We observe for different L, the scan distance ranges are similar and the median scan distances are all less than 0.9 m, showing L has little influence on the scan distance. This is because the scan distance is mainly affected by the moving step distance D, which remains constant.

Long-distance Tests: The above experiments verify that

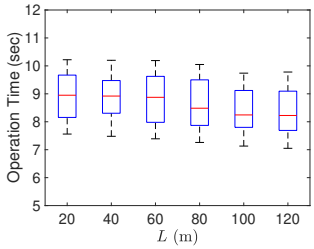


Fig. 26. Operation time in long-distance tests.

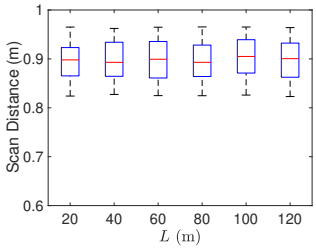


Fig. 27. Scan distance in long-distance tests.

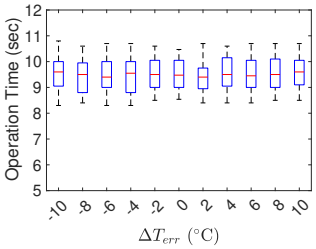


Fig. 30. Time vs. ΔT_{err}.

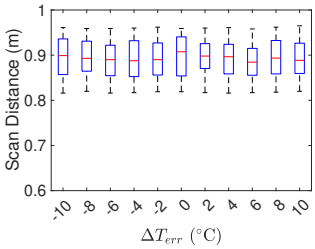


Fig. 31. Distance vs. ΔT_{err}.

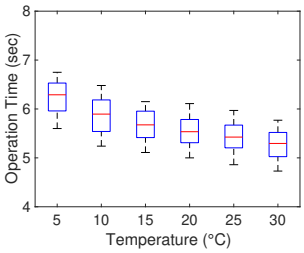


Fig. 28. Time vs. temperature.

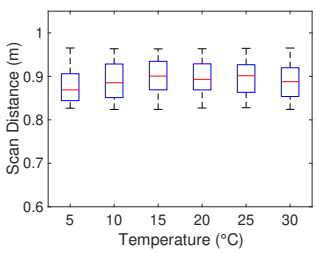


Fig. 29. Distance vs. temperature.

PhantomMotion always works for a short laser transmission distance, while focusing the laser with the small lenses for a longer laser transmission distance (e.g., above 20 m) is difficult. To address this, we adopt a telephoto lens (Opteka 650-1300mm [70]) to focus the laser, and achieve laser transmission distances of up to 120 meters (the maximum safety distance restricted by the testing environment). The experiments were conducted on a secured 35-acre private farmland, enclosed by fences, as shown in Figure 25. We implemented all laser safety measures and confirmed that all occupants of the farmland had left before starting our tests. Access to the experimental area was restricted to other people, and during the whole tests, we always directed the laser towards the designated area. We also use a scope (TRUGLO TRU-BRITE 30 TG8539TL [71]) for providing a clear view of targets up to 600 yards (about 549 meters).

The maximum attack distance is bounded by the *sniffing distance*, i.e., the maximum distance between the sniffer and the target where the sniffer can capture wireless signals generated by the target. The sniffing distance depends on the target, the communication environment, and the sniffer. We utilize Alfa AC1900 to sniff wireless traffic, and its distance of range is 500 feet (i.e., 152.4 m) in an open area. To explore the attack distance, we install each device in two typical environments, (i) a dense area: a room in an apartment complex where there are walls and other objects (e.g., cars) interfering, and (ii) an open area: a farmhouse with an open field surrounding it. For every device in each environment, we perform 15 independent trials to measure the sniffing distance, and calculate average values, as shown in Figure 24. We see that the sensing distances for all devices are quite large (ranging from 129 to 167 m) in an open environment, while they consistently plummet in a dense scenario.

We vary L from 20 to 120 m with increments of 20, and perform 100 trials for each L. The environmental temperature remains the same. We consistently obtain a 100% success rate and a 0 false positive rate. Figures 26 and 27 display the operation time and scan distances. We see shorter operation time compared with short-distance tests. The median operation time for 20 m is 8.9 sec, and decreases to 8.2 sec at 120 m. Again, a larger L requires a smaller rotation angle of the laser beam, leading to decreased operation time. The observation for scan distance is similar to that in short-distance tests.

5) Impact of Environmental Temperature: We utilize a digital thermometer (Smart Thermostat Premium [72]) working with the HVAC to adjust the room temperature from 5 to 30 °C, with increments of 5. We conduct 100 attempts for each specified temperature. The success rate and the false positive rate still maintain 100% and 0, respectively. Figure 28 illustrates the operation time. We observe that the median operation time slightly increases as the temperature decreases, and it is 5.3 sec at 30 °C, while it increases to 6.3 sec at 5 °C. This is because a lower temperature results in a longer laser heating time. On the other hand, the scan distance exhibits minor fluctuation with the temperature, as shown in Figure 29. Particularly, the median scan distance remains consistently below 0.9 m for varying temperatures.

Robustness to Inaccurate Environmental Sensing: We simulate environmental temperature estimation errors by varying the estimated temperature from 10 to 30 °C in steps of 2 °C, while the ground-truth temperature is set as 20 °C. This results in a temperature estimation error ΔT_{err} from -10 to +10 °C. For each ΔT_{err}, we perform 100 trials of *PhantomMotion*. *PhantomMotion* works under all tested values of ΔT_{err}. This is due to the fact that the temperature estimation is used primarily as a coarse-grained guideline, and the actual heating time can be flexibly adjusted (shortened or extended) based on real-time traffic analysis that determines when the camera switches to its working mode. Figure 30 shows the corresponding operation time, which is consistent and shows no significant fluctuations across all ΔT_{err} values. At $\Delta T_{err} = 0$, the operation time ranges from 8.5 to 10.5 sec. For $\Delta T_{err} \neq 0$, it is similarly stable, ranging from 8.3 to 10.8 sec. Figure 31 plots the associated scan distances, which are also consistent under different ΔT_{err} values, remaining below 1 m. These results confirm that the inaccurate temperature estimation can be effectively corrected by real-time traffic analysis, confirming reliable performance of *PhantomMotion*.

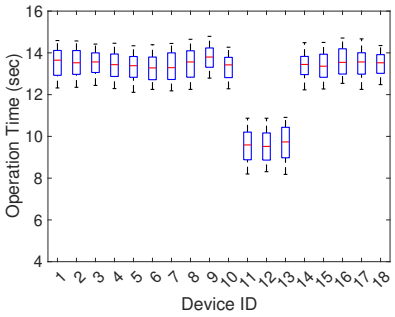


Fig. 32. Overall operation time.

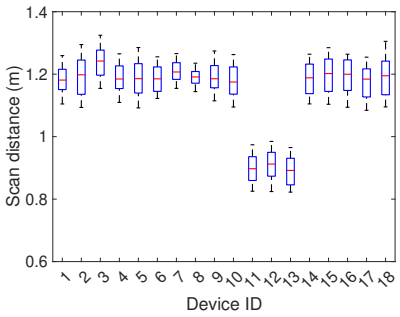


Fig. 33. Overall scan distance.

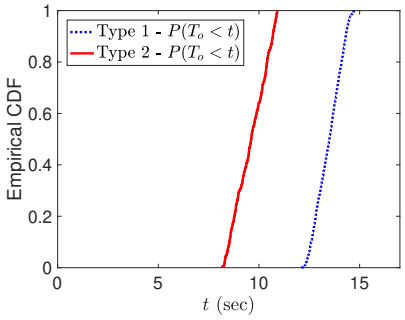


Fig. 34. CDFs of operation time T_o.

D. Overall Attack Impact

We perform 100 attack trials for each device and have $18 \times 100 = 1,800$ attempts in total. Again, *PhantomMotion* achieves a 100% success rate and a zero false positive rate. For each attempt, we record the operation time and scan distance, as shown in Figures 32 and 33. We see three tendencies. First, *PhantomMotion* always achieves a short operation time (from 8.1 to 14.7 sec) and a small scan distance (from 0.8 to 1.3 m). Second, on average, a device with two PIR sensors (Type 2, ID 11-13) causes a shorter operation time and requires a smaller scan distance than a device with one PIR sensor (Type 1, ID 1-10&14-18). This is because a Type 2 camera has a larger motion detection zone, requiring fewer heated positions to trigger activation. Third, the performance is quite consistent across devices with the same amount of PIR sensors. For Type 1 or 2 devices, the mean operation times range from 13.2 to 13.8 sec, and 9.5 to 9.7 sec, respectively. Meanwhile, the respective mean scan distances stay around 1.2 and 0.9 m.

Figures 34 and 35 plot the CDFs of the operation time T_o and the scan distance S. We see for Type 1, T_o is less than 14.5 sec with a 97.5% probability; for Type 2, T_o is less than 10.8 sec with a 98.3% probability. Also, S is less than 1.26 m for Type 1 with a probability of 92.0%, and less than 0.96 m for Type 2 with the same probability. These results again show that more PIR sensors may lead to a shorter operation time and a smaller scan distance, and confirm conclusively that *PhantomMotion* is robust against different devices.

E. User Study

We conduct a user study to evaluate the real-world practicality of *PhantomMotion*, focusing on whether non-experts can successfully perform the attack and achieve consistent results. We recruited 12 volunteers (U1-U12; aged 19-36 years old; 6 female and 6 male), from our institution via email lists and campus flyers. All volunteers were non-experts with no prior experience in camera detection. We target non-experts to demonstrate that the attack does not require specialized skills, thereby highlighting the broad applicability and accessibility of the attack. Given their technical background, expert users are expected to perform the attack with equal or greater effectiveness. This participant-based evaluation is consistent with previous camera detection studies (e.g., [11], [12], [13], [15], [17], [18]). Our institutional office of compliance provides training slides and a safety quiz for participants. To minimize bias, no performance feedback or coaching was provided during the trials. Our app only operates the laser once the user affirms the safety measures. Each user performed *PhantomMotion* 100 times to trigger a wireless motion-activated device randomly selected and deployed at a random location inside the living room, as shown in Figure 12. We make sure that the motion detection area is not fully blocked. Each participant received a $20 Amazon gift card as compensation.

TABLE III
OFFICIAL VS. EMPIRICAL BATTERY LIFE: NORMAL USE VS. ATTACK.

ID	Official Battery Life	Battery Life Under the Attack	Impact (%, × faster)
1	5 months [73]	11.5 hours	0.32, 313
2	6 months [73]	11.3 hours	0.26, 382
3	2-3 months [74]	6.2 hours	0.29-0.43, 232-348
4	up to 24 months [75]	15.7 hours	$\geq$ 0.09, $\leq$1,101
5	12 months [76]	13.3 hours	0.15, 650
6	3 months [77]	7.5 hours	0.35, 288
7	2.5 months [77]	6.0 hours	0.33, 300
8	12 months [78]	9.7 hours	0.11, 891
9	up to 200 days [79]	8.5 hours	$\geq$ 0.18, $\leq$565
10	20 days-6 months [80]	6.7 hours	0.16-1.4, 72-645
11	12 months [81]	12.5 hours	0.14, 691
12	6-12 months [82]	9.3 hours	0.11-0.22, 465-929
13	6-12 months [83]	8.5 hours	0.10-0.20, 508-1,016
14	up to 3 months [84]	5.2 hours	$\geq$ 0.24, $\leq$415
15	6 months [85]	12.7 hours	0.29, 340

Consistently, all users achieve a 100% success rate and no false positive is observed. Figure 36 shows their operation time. We see the maximum operation time for each user is always below 6.5 sec, and some users (e.g., users 3 and 7) can obtain an operation time as short as 5.2 sec. Figure 37 presents the scan distances. We see a consistent median scan distance for all users varying between 0.88 and 0.91 m. These results demonstrate consistent attack efficiency across users and verify the practicality of *PhantomMotion*.

F. Impact on Battery Consumption

We measure how quickly the battery of each tested security camera depletes when *PhantomMotion* consecutively activates the camera. Each camera is fully charged and positioned to monitor the same residential front yard. We conduct two groups of experiments: (i) *without the attack*, where the camera

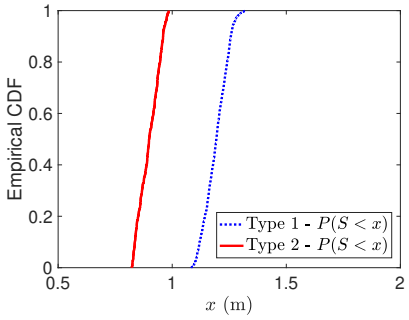


Fig. 35. CDFs of scan distance S.

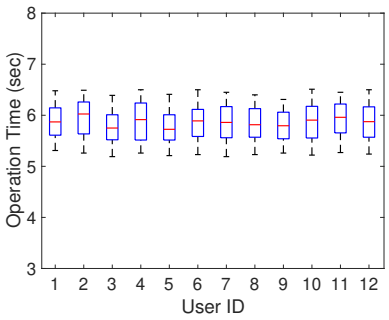


Fig. 36. Users' operation time.

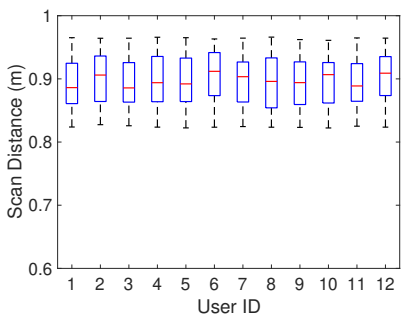


Fig. 37. Users' scan distances.

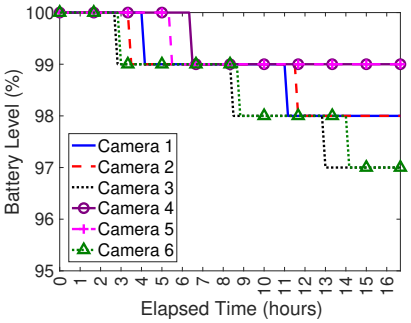


Fig. 38. Battery drain without the attack.

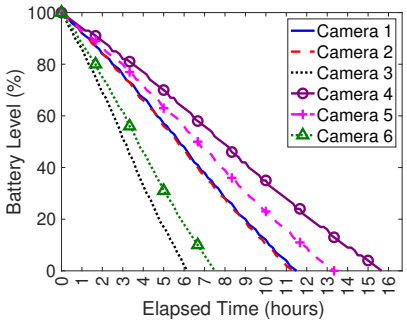


Fig. 39. Battery drain under the attack.

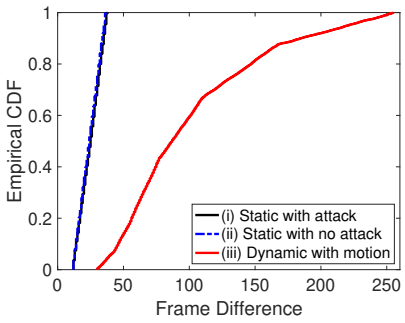


Fig. 40. CDFs of frame differences.

is triggered by natural motion (e.g., passing pedestrians or vehicles); (ii) *with the attack*, where the camera is continuously triggered by *PhantomMotion*. We record the battery level using the camera's mobile app every 10 minutes, collecting 100 samples over 16 hours and 30 minutes.

Figures 38 and 39 show the battery drain of the first six cameras (ID 1-6 in Table II) over time without and with the attack. We observe under normal usage (i.e., without the attack), all cameras retain at least 97% of their battery capacity after 16.5 hours. In contrast, with the attack, the cameras experience accelerated battery drain, with lifespans ranging from 6.2 to 15.7 hours. We record the battery life of all cameras under the attack and obtain the officially advertised battery life on a single charge from camera vendor websites under normal or default usage. Table III presents both values, along with the percentage of remaining battery life with the attack relative to the official specification, and the corresponding fold increase in battery drain rate caused by the attack. The accelerated battery drain results from *PhantomMotion* keeping the camera continuously active in its high-power operational state.

VII. Discussion

A. Limitation

Line-of-sight Access: Like other light-based attacks, *PhantomMotion* inherits the limitations of light-related physics, i.e., it requires line-of-sight (LOS) to the heating material. However, for *PhantomMotion*, the material does not necessarily lie in the LOS of the target system due to radiation heat transfer.

Customized Motion Detection Zones: Our experiments are performed with the security systems in factory default settings. Some systems do not support activity zone customization, such as Simplisafe Cam and Ring Alarm System, while some allow manually creating activity zones in certain circumstances. For example, users can customize the motion zones of an Arlo wireless camera when they purchase an Arlo Secure Subscription plan [86]. If a user manages to narrow the motion detection zone, *PhantomMotion* still works while it may need to scan a larger area, resulting in an increased operation time. Meanwhile, a decreased motion detection zone may also degrade the system's ability to detect intrusion accordingly.

Security Systems Without WiFi Connection: *PhantomMotion* sniffs WiFi and does not work with non-WiFi networks such as 4G-LTE or 5G. The cellular space brings new challenges. For example, a cellular device does not broadcast its MAC and uses the Temporary Mobile Subscriber Identity (TMSI), which can be changed frequently. However, by combining techniques that can achieve cellular traffic tracking (e.g., [87], [88], [89]), *PhantomMotion* may still work.

B. Defense Strategies

One straightforward defense is to *manually turn off the motion sensor* [90], disabling motion-triggered alerts. However, this is impractical, as it prevents timely intrusion detection.

Multi-factor Motion Authentication: A practical way to detect the attack is to incorporate another type of sensor (e.g., an ultrasonic detector [91], RGB color sensor [92], wireless transceiver [93], [94], [95], [96], or geophone [97], [98]) unaffected by injected thermal radiation for verifying motion. However, they require deploying extra hardware and effort. Also, each new sensor may introduce a new attack surface.

Video Processing based Solutions: A wireless camera can analyze the recorded video to verify motion authenticity.

This solution entails advanced computer vision and machine learning algorithms to distinguish human motion (e.g., [99], [100], [101]). Specifically, the camera may achieve motion detection by employing light-weight frame-by-frame comparison (e.g., [102], [103]) or performing video analysis in the cloud using resource-intensive machine learning without significantly increasing device cost or reducing battery life. Also, modern SoCs may support computer vision tasks and image processing on edge devices. Among them, Ambarella CV-series chips with the "S" suffix are optimized for security cameras and intelligent surveillance, while TI's AM6xA processors are designed for vision applications. For instance, the Ambarella CV22S SoC [104] can perform real-time, lightweight frame comparisons locally for 4K video at 30 FPS, and the TI AM62A low-power SoC [105] achieves real-time performance for advanced image processing at the edge. These recent advancements, which enable low-latency on-device video processing, make this defense direction promising.

We utilize a Ring Stickup Cam at 15 frames per second (FPS) to capture 100 clear clips of 5-second video footage in three scenarios, (i) a static case in which *PhantomMotion* launches in NLOS of the camera and generates fake motion to trigger the camera; (ii) an environment with neither real nor fake motion; and (iii) where real motion is performed to trigger the camera. Figure 40 presents the corresponding frame differences (i.e., the sum of all pixel differences between two successive frames) under the three scenarios. We can see that the frame differences for cases (i) and (ii) are quite similar, while they both share some overlap with that for the third case with real motion. The results indicate that the technique of frame differencing may be able to successfully determine whether the large-amplitude motion (leading to high frame differences) is true or fake, while it may not be able to distinguish subtle motion (causing comparably smaller frame differences) from generated phantom motion.

The accuracy of video-based techniques, however, highly depends on the light condition. Also, if the fake motion appears only in the non-overlapping area that belongs to the motion detection zone but not the camera's field of view, this method fails as the camera cannot capture the position where the motion occurs. Besides, performing detection on raw videos may reveal the privacy of innocent people in the video [106], and these systems may suffer from image injection attacks [107], where an attack makes a camera misperceive an actual scene or perceive a non-existent scene.

VIII. Conclusion

We present *PhantomMotion*, a novel technique for remotely triggering wireless motion-activated security systems (such as widely deployed IoT cameras and alarm systems) with a laser. It is the first to activate security systems requiring neither penetrating into the same network with target systems nor physical human motion in close proximity to the systems. By exploiting the working mechanisms of motion sensors, we manage to create fake motion signals and inject them into an area to stimulate a security system monitoring this area to emit wireless traffic, which can be collected and correlated with the laser-based stimulus to check whether the system activates. Our real-world evaluation with 18 popular off-the-shelf wireless security systems shows the effectiveness and efficiency of *PhantomMotion* under varying conditions.

Ethics Considerations

Laser Safety: For lasers with intermediate power (5-500 mW), i.e., Class 3b laser, they may heat skin and other materials, but are not considered a burn hazard normally [108]. Class 3b lasers are often used for entertainment light shows. The more powerful the laser, the sooner the heat will build up. Direct viewing of the Class 3b laser beam may be hazardous to the eye, while diffuse reflections from paper or matte surfaces are not harmful. We used a Class 3b laser with a power of 100 mW at the low end. This study has been approved by our institution's IRB, and experiments were conducted under a Standard Procedure approved by our institutional Office of Compliance. The office examined our laser devices and procedures; safety precautions were taken to ensure no harm was caused, such as avoiding direct viewing of the laser beam, providing users with laser goggles, and adequately covering windows with laser safety curtains to prevent any inadvertent laser escape. We urge that researchers receive formal laser safety training and approval of experimental designs before attempting to reproduce our work.

Responsible Disclosure: Following the practice of responsible disclosure, we have reported our findings to mainstream camera vendors, including Arlo, Blink, Google, Ring, SimpliSafe, and Wyze. They have acknowledged receipt of our vulnerability report and appreciated our submission. Arlo has successfully validated our identified vulnerability, confirmed that it could be replicated, and awarded us a bug bounty.

Acknowledgment

The authors would like to thank all anonymous reviewers for their insightful comments. This work was supported in part by the National Science Foundation under Grants No. 2155181 and No. 2424439.

References

[1] A. Dellinger. (2022, October) Wired vs. wireless security cameras: How to choose which is best for you. [Online]. Available: https://www.cnet.com/home/security/wired-vs-wireless-security-cameras-how-to-choose-which-is-best-for-you/

[2] Allied Market Research. (2022, August) Wireless video surveillance market. [Online]. Available: https://www.alliedmarketresearch.com/wireless-video-surveillance-market-A17130

[3] Fact.MR. (2022, November) PIR sensor market. [Online]. Available: https://www.factmr.com/report/pir-sensor-market

[4] J. Pierce, "Smart home security cameras and shifting lines of creepiness: A design-led inquiry," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ser. CHI '19. ACM, 2019, p. 1–14.

[5] Y. He, Q. He, S. Fang, and Y. Liu, "When free tier becomes free to enter: A non-intrusive way to identify security cameras with no cloud subscription," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 651–665.

[6] S. Mare, F. Roesner, and T. Kohno, "Smart devices in airbnbs: Considering privacy and security for both guests and hosts." *Proc. Priv. Enhancing Technol.*, vol. 2020, no. 2, pp. 436–458, 2020.

[7] M. Kwan and K. Fu, "Regulating the sale and use of hidden cameras," *The Regulatory Review*, 2021.

[8] B. D. Teshome, "Spy camera epidemic in korea: a situational analysis," *Asian Journal of Sociological Research*, pp. 1–13, 2019.

[9] T. May and S.-H. Lee. (2018) Is there a spy camera in that bathroom? In Seoul, 8,000 workers will check. https://www.nytimes.com/2018/09/03/world/asia/korea-toilet-camera.html.

[10] H. Barr and H. R. Watch, *"My Life is Not Your Porn": Digital Sex Crimes in South Korea*. Human Rights Watch, 2021, https://www.hrw.org/report/2021/06/16/my-life-not-your-porn/digital-sex-crimes-south-korea.

[11] Y. Cheng, X. Ji, T. Lu, and W. Xu, "Dewicam: Detecting hidden wireless cameras via smartphones," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ser. ASIACCS '18. ACM, 2018, p. 1–13.

[12] ——, "On detecting hidden wireless cameras: A traffic pattern-based approach," *IEEE Transactions on Mobile Computing*, vol. 19, no. 4, pp. 907–921, 2020.

[13] Y. He, Q. He, S. Fang, and Y. Liu, "Motioncompass: Pinpointing wireless camera via motion-activated traffic," in *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '21. ACM, 2021, p. 215–227.

[14] ——, "Precise wireless camera localization leveraging traffic-aided spatial analysis," *IEEE Transactions on Mobile Computing*, vol. 23, no. 6, pp. 7256–7269, 2024.

[15] A. D. Singh, L. Garcia, J. Noor, and M. B. Srivastava, "I always feel like somebody's sensing me! A framework to detect, identify, and localize clandestine wireless sensors," in *30th USENIX Security Symposium*. USENIX Association, Aug. 2021, pp. 1829–1846.

[16] M. Salman, N. Dao, U. Lee, and Y. Noh, "Csi:despy: Enabling effortless spy camera detection via passive sensing of user activities and bitrate variations," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 6, no. 2, Jul 2022.

[17] R. A. Sharma, E. Soltanaghaei, A. Rowe, and V. Sekar, "Lumos: Identifying and localizing diverse hidden IoT devices in an unfamiliar environment," in *31st USENIX Security Symposium*. USENIX Association, Aug. 2022, pp. 1095–1112.

[18] J. Heo, S. Gil, Y. Jung, J. Kim, D. Kim, W. Park, Y. Kim, K. G. Shin, and C.-H. Lee, "Are there wireless hidden cameras spying on me?" in *Proceedings of the 38th Annual Computer Security Applications Conference*, ser. ACSAC '22. ACM, 2022, p. 714–726.

[19] T. Qiu and C. Tien, "Heat transfer mechanisms during short-pulse laser heating of metals," *Journal of Heat Transfer (Transactions of the ASME (American Society of Mechanical Engineers), Series C);(United States)*, vol. 115, no. 4, 1993.

[20] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands: Laser-Based audio injection attacks on Voice-Controllable systems," in *29th USENIX Security Symposium*. USENIX Association, Aug. 2020, pp. 2631–2648.

[21] C. Yan, Z. Xu, Z. Yin, X. Ji, and W. Xu, "Rolling colors: Adversarial laser exploits against traffic light recognition," in *31st USENIX Security Symposium*. USENIX Association, Aug. 2022, pp. 1957–1974.

[22] N. H. Tan, R. Y. Wong, A. Desjardins, S. A. Munson, and J. Pierce, "Monitoring pets, deterring intruders, and casually spying on neighbors: Everyday uses of smart home cameras," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, ser. CHI '22. ACM, 2022.

[23] J. Gong, Y. Zhang, X. Zhou, and X.-D. Yang, "Pyro: Thumb-tip gesture recognition using pyroelectric infrared sensing," in *Proceedings of the 30th Annual ACM Symposium on User Interface Software and Technology*, ser. UIST '17. ACM, 2017, p. 553–563.

[24] S. Narayana, R. V. Prasad, V. S. Rao, T. V. Prabhakar, S. S. Kowshik, and M. S. Iyer, "Pir sensors: Characterization and novel localization technique," in *Proceedings of the 14th International Conference on Information Processing in Sensor Networks*, ser. IPSN '15. ACM, 2015, p. 142–153.

[25] X. Liu, T. Yang, S. Tang, P. Guo, and J. Niu, "From relative azimuth to absolute location: Pushing the limit of pir sensor based localization," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '20. ACM, 2020.

[26] O. Dev, S. Dayal, A. Dubey, and S. Abbas, "Multi-layered textile structure for thermal signature suppression of ground based targets," *Infrared Physics & Technology*, vol. 105, p. 103175, 2020.

[27] D. V. Schroeder, *An Introduction to Thermal Physics*. Oxford University Press, USA, 2021.

[28] I. B. of Weights, Measures, B. N. Taylor, and A. Thompson, *The international system of units (SI)*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2001.

[29] SpyGuy. (2024) Scout hidden camera detector. https://www.spyguy.com/products/scout-hidden-camera-detector.

[30] S. Sami, S. R. X. Tan, B. Sun, and J. Han, "Lapd: Hidden spy camera detection using smartphone time-of-flight sensors," in *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, ser. SenSys '21. ACM, 2021, p. 288–301.

[31] Z. Yu, Z. Li, Y. Chang, S. Fong, J. Liu, and N. Zhang, "Heatdecam: Detecting hidden spy cameras via thermal emissions," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '22. ACM, 2022, p. 3107–3120.

[32] Z. Liu, F. Lin, C. Wang, Y. Shen, Z. Ba, L. Lu, W. Xu, and K. Ren, "Camradar: Hidden camera detection leveraging amplitude-modulated sensor images embedded in electromagnetic emanations," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 6, no. 4, jan 2023.

[33] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of rf interference on 802.11 networks," in *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, ser. SIGCOMM '07. New York, NY, USA: Association for Computing Machinery, 2007, p. 385–396.

[34] D. Schepers, A. Ranganathan, and M. Vanhoef, "Let numbers tell the tale: Measuring security trends in wi-fi networks and best practices," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 100–105.

[35] D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, "Controlling UAVs with sensor input spoofing attacks," in *10th USENIX Workshop on Offensive Technologies (WOOT 16)*. Austin, TX: USENIX Association, Aug. 2016.

[36] H. Shin, J. Noh, D. Kim, and Y. Kim, "The system that cried wolf: Sensor security analysis of wide-area smoke detectors for critical infrastructure," *ACM Trans. Priv. Secur.*, vol. 23, no. 3, p. 1–32, jun 2020.

[37] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," *Black Hat Europe*, vol. 11, no. 2015, p. 995, 2015.

[38] Y. Cao, S. H. Bhupathiraju, P. Naghavi, T. Sugawara, Z. M. Mao, and S. Rampazzi, "You can't see me: Physical removal attacks on lidar-based autonomous vehicles driving frameworks," in *32nd USENIX Security Symposium*, 2023.

[39] R. H. Schleijpen and F. J. van Putten, "Using a co2 laser for pir-detector spoofing," in *Technologies for Optical Countermeasures XIII*, vol. 9989. SPIE, 2016, pp. 113–119.

[40] (2020) Laser / PIR alarm. [Online]. Available: https://projecthub.arduino.cc/Avilmaru/laser-pir-alarm-312e44

[41] A. Li. (2024) Security camera blind spots: How to find and avoid them. [Online]. Available: https://reolink.com/blog/find-and-avoid-security-camera-blind-spots/

[42] I. Fernandez. (2023) Costa Rica bank thief spent stolen money on lottery. https://ticotimes.net/2023/11/10/costa-rica-bank-thief-bet-stolen-money-on-lottery.

[43] I. Ignatov, O. Mosin, H. Niggli, C. Drossinakis, and G. Tyminski, "Methods for registering non-ionizing radiation emitted from the human body," *European Reviews of Chemical Research*, vol. 3, no. 1, pp. 4–24, 2015.

[44] (2024) HC-SR501 PIR motion detector. https://www.mpja.com/download/31227sc.pdf.

[45] Teledyne FLIR LLC. (2023) Pro-grade thermal camera for smartphones: FLIR ONE pro. [Online]. Available: https://www.flir.com/products/flir-one-pro/

[46] (2024) BISS0001: Micro power PIR motion detector IC. [Online]. Available: http://www.ladyada.net/media/sensors/BISS0001.pdf

[47] Texas Instruments Incorporated. (2023) ADS1115. [Online]. Available: https://www.ti.com/lit/ds/symlink/ads1115.pdf

[48] Aircrack-ng. (2024) Airmon-ng. https://www.aircrack-ng.org/doku.php?id=airmon-ng.

[49] S.-T. Sun, A. Cuadros, and K. Beznosov, "Android rooting: Methods, detection, and evasion," in *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, ser. SPSM '15. ACM, 2015, p. 3–14.

[50] (2024) Qualcomm QCACLD WiFi (Android) monitor mode. https://github.com/kimocoder/qualcomm_android_monitor_mode.

[51] J. Martin, E. Rye, and R. Beverly, "Decomposition of mac address structure for granular device inference," in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, ser. ACSAC '16. ACM, 2016, p. 78–88.

[52] J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. C. Rye, and D. Brown, "A study of mac address randomization in mobile devices and when it fails," *Proceedings on Privacy Enhancing Technologies*, vol. 4, pp. 268–286, 2017.

[53] Ambarella. (2025) CV2S: Computer vision SoC for IP cameras. [Online]. Available: https://www.ambarella.com/wp-content/uploads/CV2S_Product_Brief_07OCT2020.pdf

[54] (2025) Scikit-learn: Machine learning in python. [Online]. Available: https://scikit-learn.org/stable/

[55] (2024) DHT11–temperature and humidity sensor. https://components101.com/sensors/dht11-temperature-sensor.

[56] D. W. Waples and J. S. Waples, "A review and evaluation of specific heat capacities of rocks, minerals, and subsurface fluids. part 1: Minerals and nonporous rocks," *Natural resources research*, vol. 13, no. 2, pp. 97–122, 2004.

[57] S. K. Duggal, *Building materials*. Routledge, 2017.

[58] (2025) pigpio. https://github.com/joan2937/pigpio.

[59] Ring LLC. (2023) Proper positioning for your floodlight cam. https://support.ring.com/hc/en-us/articles/360000124983-Proper-Positioning-for-Your-Floodlight-Cam.

[60] D. J. Coluzzi and A. Robert, "Laser fundamentals," *Principles and Practice of Laser Dentistry. St. Luis Missoiri2011*, pp. 12–26, 2015.

[61] J. P. Holman, *Heat transfer*. McGraw Hill, 1986.

[62] R. Winterton, "Newton's law of cooling," *Contemporary Physics*, vol. 40, no. 3, pp. 205–212, 1999.

[63] S. Munari, C. E. Palazzi, G. Quadrio, and D. Ronzani, "Network traffic analysis of a small quadcopter," in *Proceedings of the 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*, ser. DroNet '17. ACM, 2017, p. 31–36.

[64] A. Singh. (2022) How to root Android 13. https://www.ytechb.com/how-to-root-android-13/.

[65] N. Shafqat, C. Topcuoglu, E. Kirda, and A. Ranganathan, "Experience report on the challenges and opportunities in securing smartphones against zero-click attacks," *arXiv preprint arXiv:2211.03015*, 2022.

[66] ALFA Network Inc. (2023) AWUS1900. [Online]. Available: https://www.alfa.com.tw/products/awus1900?variant=36473966231624

[67] Research and Markets. (2024) Soda lime glass market outlook. [Online]. Available: https://www.researchandmarkets.com/report/soda-lime-glass-market

[68] ASTM International. (2025) Standard specification for flat glass. [Online]. Available: https://store.astm.org/c1036-21.html

[69] (2025) Building code. [Online]. Available: https://codelibrary.amlegal.com/codes/honolulu/latest/honolulu/0-0-0-13990

[70] Opteka. (2023) Opteka 650-1300mm: High definition telephoto zoom lens. https://opteka.com/products/op6501300.

[71] TRUGLO. (2023) Tru•brite 30 series. https://www.truglo.com/tru-brite-30-series/.

[72] ecobee. (2023) Smart thermostats. https://www.ecobee.com/en-us/smart-thermostats/.

[73] Arlo. (2025) How long do Arlo camera batteries last? [Online]. Available: https://kb.arlo.com/1202753/How-long-do-Arlo-camera-batteries-last

[74] A. Bradford. (2023) Adt self setup outdoor wireless camera review. [Online]. Available: https://www.safewise.com/adt-blue-camera-review/

[75] Blink. (2025) How long do the blink camera batteries last? [Online]. Available: https://support.blinkforhome.com/en_US/f-a-q/how-long-do-the-indoor-and-xt-camera-batteries-last

[76] (2025) Wireless home security camera system, eufy security, eufycam e 365-day battery life. [Online]. Available: https://www.amazon.com/Security-eufyCam-Wireless-Weatherproof-Compatible/dp/B07KWNMB8Z

[77] Google. (2025) Save battery for nest cameras and doorbells. [Online]. Available: https://support.google.com/googlenest/answer/10901611

[78] (2025) IHOXTX DF22 wireless outdoor camera. [Online]. Available: https://www.amazon.com/IHOXTX-Security-Wireless-Detection-Waterproof/dp/B0BKG4Z1NK

[79] (2025) Laview security cameras wireless outdoor. [Online]. Available: https://www.amazon.com/LaView-Security-Rechargeable-Waterproof-Detection/dp/B08F2GV9QV

[80] (2024) Wireless camera battery life explained: What you need to know. [Online]. Available: https://reolink.com/blog/wireless-camera-battery-life/

[81] Ring LLC. (2025) Ring Spotlight battery life. [Online]. Available: https://ring.com/support/products/lights/spotlight-battery?page=1

[82] (2025) Ring Spotlight Pro camera. [Online]. Available: https://www.abt.com/Ring-Spotlight-Cam-Pro-Black-Battery-Powered-Camera-B09DRHPRT6/p/187712.html

[83] (2025) Ring outdoor cam (stick up cam) review. [Online]. Available: https://www.pcmag.com/reviews/ring-outdoor-cam

[84] SimpliSafe. (2025) Maximizing battery life of the wireless outdoor security camera. [Online]. Available: https://support.simplisafe.com/articles/outdoor-cameras/maximizing-battery-life-of-the-wireless-outdoor-security-camera/63449297c307775b63814d0d

[85] Wyze Labs. (2025) Wyze cam outdoor v2. [Online]. Available: https://www.wyze.com/products/wyze-cam-outdoor

[86] Arlo. (2023) Arlo secure: A command center for all your security. https://www.arlo.com/en-us/arlosecure.html.

[87] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, "New privacy threat on 3G, 4G, and upcoming 5G AKA protocols," *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 3, pp. 108–127, 2019.

[88] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4G and 5G cellular paging protocols using side channel information," *Network and distributed systems security (NDSS) symposium2019*, 2019.

[89] S. Bae, M. Son, D. Kim, C. Park, J. Lee, S. Son, and Y. Kim, "Watching the watchers: Practical video identification attack in LTE networks," in *31st USENIX Security Symposium*. USENIX Association, Aug. 2022, pp. 1307–1324.

[90] Reolink. (2023) How to turn on/off the PIR sensor. https://support.reolink.com/hc/en-us/articles/360004379493-How-to-Turn-on-off-the-PIR-Sensor.

[91] J. M. Sabatier and A. E. Ekimov, "Ultrasonic methods for human motion detection," Mississippi University National Center for Physical Acoustics, Tech. Rep., 2006.

[92] T.-K. Woodstock and R. F. Karlicek, "Rgb color sensors for occupant detection: An alternative to pir sensors," *IEEE Sensors Journal*, vol. 20, no. 20, pp. 12 364–12 373, 2020.

[93] F. Adib, Z. Kabelac, D. Katabi, and R. C. Miller, "3d tracking via body radio reflections," in *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*. Seattle, WA: USENIX Association, Apr. 2014, pp. 317–329.

[94] J. Wang, J. Xiong, H. Jiang, K. Jamieson, X. Chen, D. Fang, and C. Wang, "Low human-effort, device-free localization with fine-grained subcarrier information," *IEEE Transactions on Mobile Computing*, vol. 17, no. 11, pp. 2550–2563, 2018.

[95] Y. Meng, H. Zhu, J. Li, J. Li, and Y. Liu, "Liveness detection for voice user interface via wireless signals in iot environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 6, pp. 2996–3011, 2021.

[96] F. Zhang, C. Wu, B. Wang, H.-Q. Lai, Y. Han, and K. J. R. Liu, "Widetect: Robust motion detection with a statistical electromagnetic model," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 3, no. 3, sep 2019.

[97] M. Mirshekari, S. Pan, J. Fagert, E. M. Schooler, P. Zhang, and H. Y. Noh, "Occupant localization using footstep-induced structural vibration," *Mechanical Systems and Signal Processing*, vol. 112, pp. 77–97, 2018.

[98] J. Han, A. J. Chung, M. K. Sinha, M. Harishankar, S. Pan, H. Y. Noh, P. Zhang, and P. Tague, "Do you feel what i hear? enabling autonomous iot device pairing using different sensor types," in *2018 IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 836–852.

[99] I. Haritaoglu, D. Harwood, and L. Davis, "W/sup 4/: real-time surveillance of people and their activities," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 8, pp. 809–830, 2000.
[100] M. Suk, A. Ramadass, Y. Jin, and B. Prabhakaran, "Video human motion recognition using a knowledge-based hybrid method based on a hidden markov model," *ACM Trans. Intell. Syst. Technol.*, vol. 3, no. 3, may 2012.
[101] C. Amrutha, C. Jyotsna, and J. Amudha, "Deep learning approach for suspicious activity detection from surveillance video," in *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 2020, pp. 335–339.
[102] D. A. Migliore, M. Matteucci, and M. Naccari, "A revaluation of frame difference in fast and robust motion detection," in *Proceedings of the 4th ACM International Workshop on Video Surveillance and Sensor Networks*, ser. VSSN '06. New York, NY, USA: Association for Computing Machinery, 2006, p. 215–218.
[103] N. Prabhakar, V. Vaithiyanathan, A. P. Sharma, A. Singh, and P. Singhal, "Object tracking using frame differencing and template matching," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 4, no. 24, pp. 5497–5501, 2012.
[104] Ambarella. (2025) Intelligent devices for enhanced safety. https://www.ambarella.com/products/security/.
[105] Texas Instruments. (2025) Texas instruments am62a vision processor. https://www.ti.com/video/6339718991112.
[106] J. Guo, P. Zheng, and J. Huang, "An efficient motion detection and tracking scheme for encrypted surveillance videos," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 13, no. 4, sep 2017.
[107] Y. Man, M. Li, and R. Gerdes, "GhostImage: Remote perception attacks against camera-based image classification systems," in *23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)*. USENIX Association, 2020, pp. 317–332.
[108] Laser Institute of America. (2022) The ANSI Z136.1 for safe use of lasers. https://www.lia.org/store/product/ansi-z1361-2022-safe-use-lasers-electronic-version.
[109] X. Guo, S. Cheng, W. Cai, Y. Zhang, and X.-a. Zhang, "A review of carbon-based thermal interface materials: Mechanism, thermal measurements and thermal properties," *Materials & Design*, vol. 209, p. 109936, 2021.

APPENDIX

A. User Interface

We develop a mobile app *PhantomMotion* and its designed user interface (UI) is presented in Figure 41.

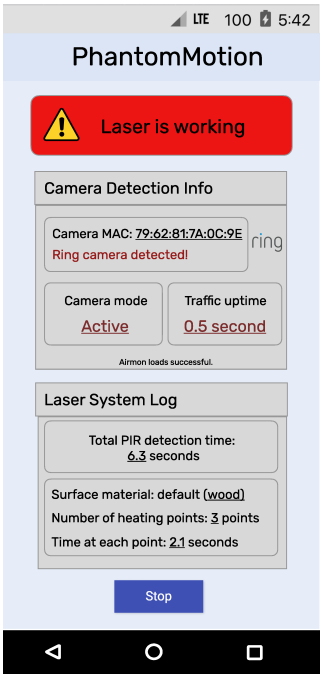


Fig. 41. The UI snapshot when the target camera is activated.

TABLE IV
OPERATION TIME VS. MATERIAL IN NLOS SCENARIOS.

Material	Operation Time (seconds)		
	Average	Minimum	Maximum
Copper	5.7	5.3	6.2
Brass	6.7	6.2	7.1
Aluminum	10	9.7	10.3
Stone	308.4	299.4	319
Brick	399.3	392.6	406.5

B. Non-Line-of-Sight Scenarios

We test a 1-centimeter-thick wall with six common materials that can block visible lasers, including: aluminum, brass, copper, brick, stone, and wood. Their respective values of thermal conductivity rate λ, denoting the material's intrinsic ability to conduct heat [109], are 130, 146.9, 398, 1.03, 1.3, and 0.13 watts per meter kelvin (W/mK). A fraction of a side of the wall is inside the motion detection range of the camera, while the laser is shot from the opposite side of the wall. Some heat may thus traverse the wall to trigger the camera. The camera is unable to record the laser beams when it is activated. As λ of wood is too low, its heat transmission is too inefficient to generate phantom motion within an appropriate time (e.g., several minutes). We focus on the rest materials, and perform 100 trials of *PhantomMotion* for each. The success rate stays at 100%. Table IV presents the mean, minimum, and maximum operation time. We observe the operation time is almost inversely proportional to λ, which indicates the thermal transfer efficiency. A high λ would reduce the laser heating time at each point along the scan path. As shown in Figure 42, the scan distances for different materials are similar, within the range of 0.82 to 0.97 m. The material has no apparent impact on scan distance.

Impact of Material Thickness: We test aluminum sheets (with the designation 6061-T651) of varying thicknesses, including 1/16, 1/8, 1/4, 1/2, and 1 inch, sold on Amazon. We heat one side of the sheet with the laser, monitor the temperature of the other side, and record the heating time spent for it to reach the target temperature to trigger the camera. We perform 50 independent such experiments. Figure 43 presents the average heating time. We also plot the theoretical heating time, as discussed in Section V-F (with the temperature $T_e = 20$ °C and the target temperature $T_t = 37$ °C). We can see that the required heating time increases with thickness, and the empirical values are slightly higher than theoretical ones.

Special NLOS Case: For a more covert attack, we develop a "black-box" attack method, in which we put a laser system in a closed box made of opaque materials that can transfer heat within a reasonable time, such as the five materials we test above. The laser can be controlled wirelessly via the smartphone. It can then heat the interior surface of the box, and also the corresponding exterior surface of the box via a spontaneous heat transfer process. When this exterior surface of the box happens to face the target camera, the generated fake motion

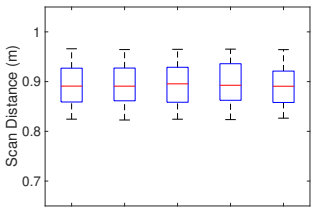


Fig. 42. Scan distance vs. material.

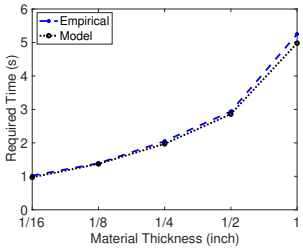
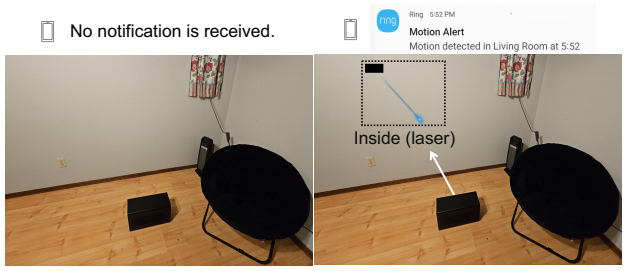


Fig. 43. Required heating time vs. material thickness.



(a) No motion is detected with no attack. (b) Motion is detected with the attack.

Fig. 44. Camera feeds before and after the black-box attack.

signals may trigger the camera accordingly. Figure 44 demonstrates such an attack case, where *PhantomMotion* successfully triggers the camera. By comparing the camera feeds before and after the attack occurs, we see that there is no visual difference.