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

Yan He, Guanchong Huang, Song Fang
University of Oklahoma

NDSS 2026

NDSS
SYMPOSIUM

Outline

Step 1

Motivation

Step 2

Threat Model

Step 3

Technical Challenges

Step 4

Evaluation

Background

U.S. FBI Crime Report 2024*

14,000,000 cases

Property offenses

1,221,345 cases

Violent offenses

Market Volume of Surveillance Cameras

$43.65 Billion

2024

$81.37 Billion

2030

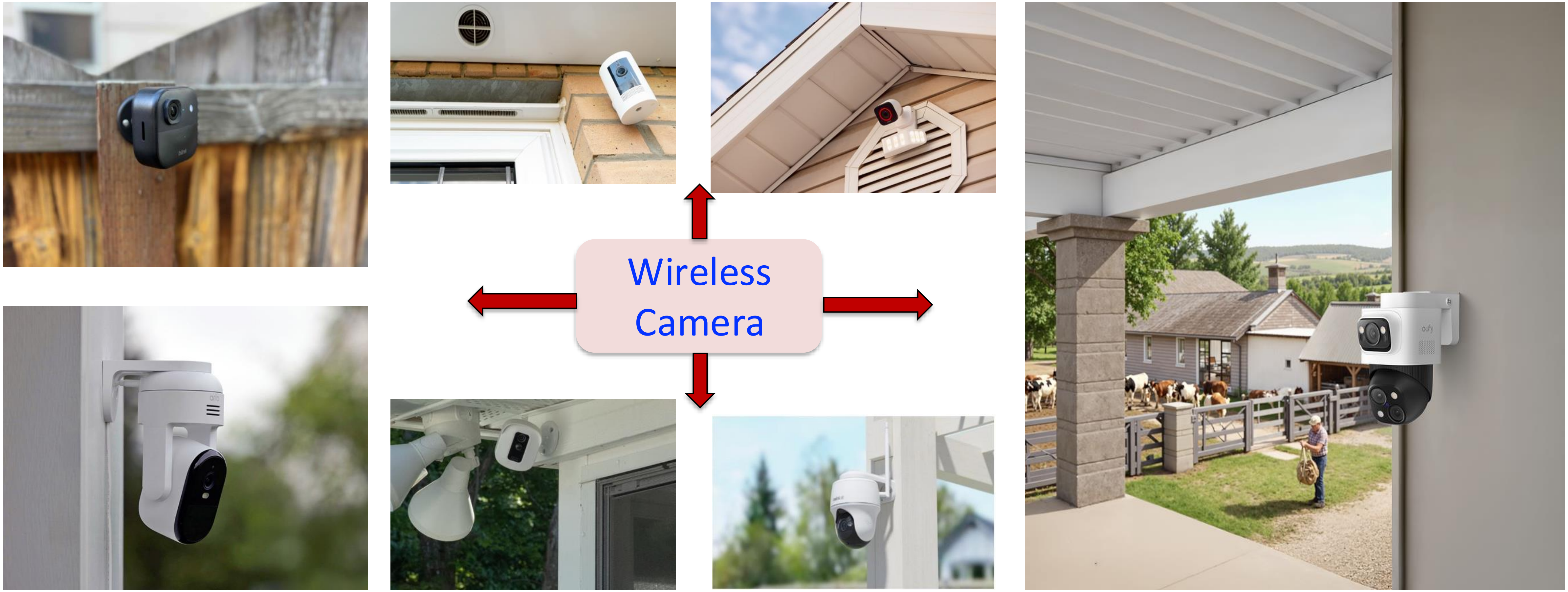
11.2 %

Annual Growth rate

* Report from FBI: https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/explorer/crime/special-reports

Wireless Cameras are Widely Deployed

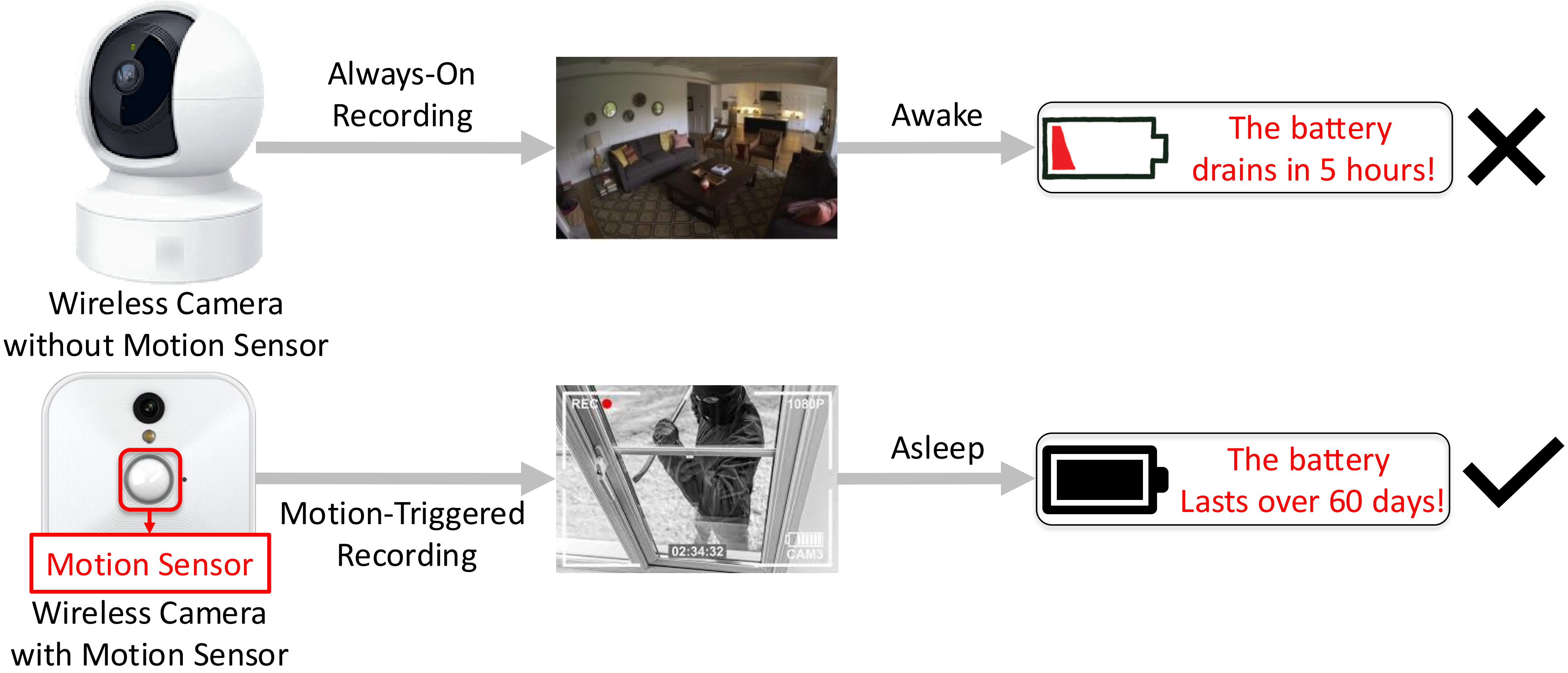
- Wireless cameras can be installed freely to monitor the property



Wireless Camera

Modern Camera Design

- **The Challenge: Unpredictable Events**
  - Critical events (e.g., deliveries, accidents, or intrusions) occur randomly.
- **The Solution: Event-based Activation**
  - The camera sleeps to save power, waking up only when motion detected.



Always-On Recording

Awake

The battery drains in 5 hours! ✗

Wireless Camera without Motion Sensor

Motion Sensor

Motion-Triggered Recording

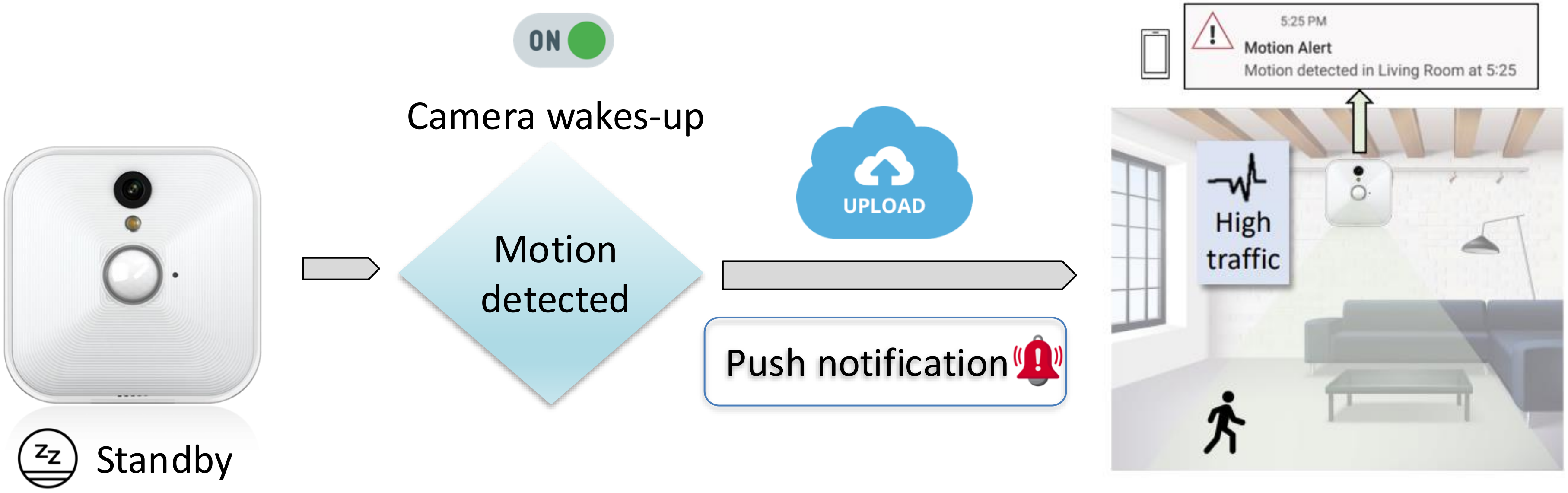
Asleep

The battery Lasts over 60 days! ✓

Wireless Camera with Motion Sensor

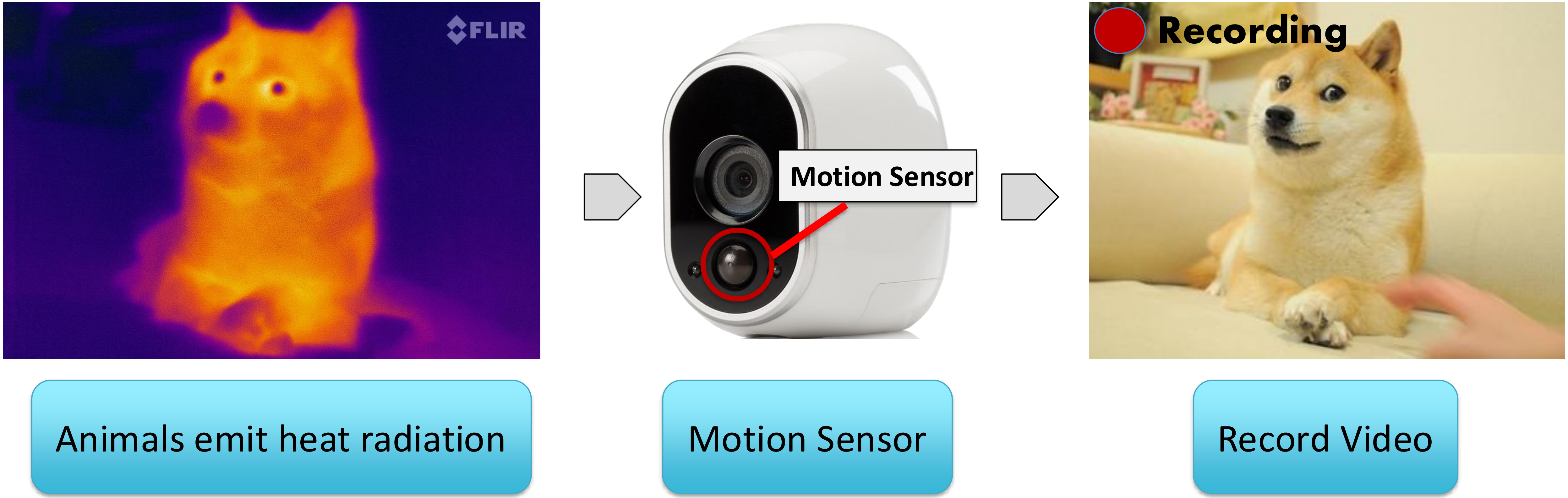
Modern Camera Design contd.

- **The User Constraint**—Users cannot always respond to alerts immediately (e.g., driving, sleeping, or working).
- **The System Mechanism**—Once motion is detected, the camera performs two simultaneous actions:
  1. **Push Notification**: Sends an instant alert to the user's smartphone.
  2. **Cloud Upload**: Automatically records and uploads the video footage to the cloud server for evidence preservation.



How Motion Sensors Work

- **How motion sensors detect humans using heat radiation**
  - Humans and animals naturally emit heat radiation
  - Motion sensors detect heat radiation changes
  - The camera automatically records when motion is detected



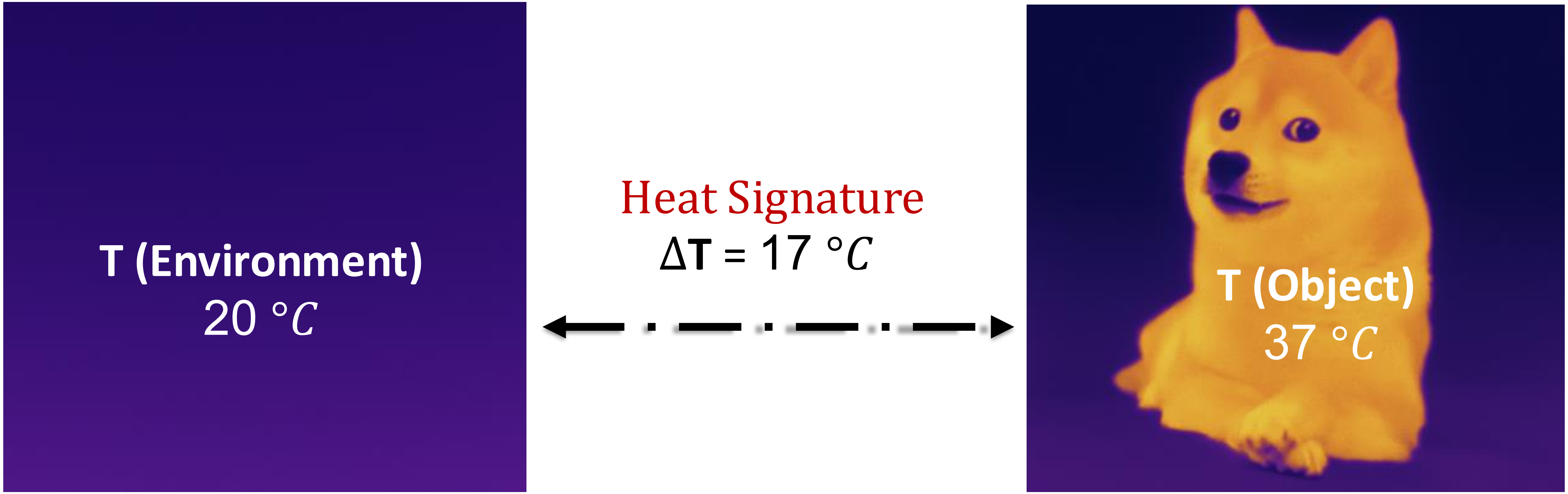
Animals emit heat radiation

Motion Sensor

Record Video

Heat Signature

- **Motion sensors detect the heat signature of an object**
  - The signature is the temperature difference between the **object** and the **background**
  - We denote this **difference** as the heat signature, ΔT



T (Environment)
20 °C

Heat Signature
ΔT = 17 °C

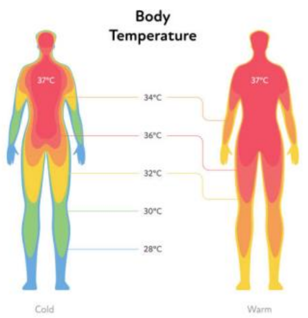
T (Object)
37 °C

Motion Sensor Advantages

- **Motion sensors have several key advantages:**
  - Compact sensor size
  - Fast response time (near-instant sensor output)
  - Affordable (approximately $1 USD per sensor)

Found me quickly!

Fake Motion Generation



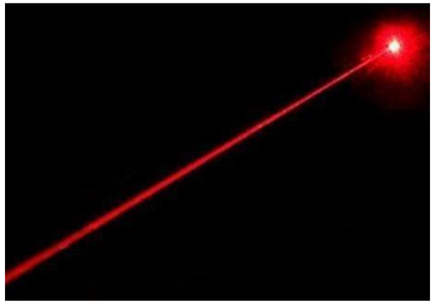
→ Heat signature from human

- This is mainly derived from **body temperature**
- Average human body temperature is **37 °C**

It's possible to simulate a human body by generating heat

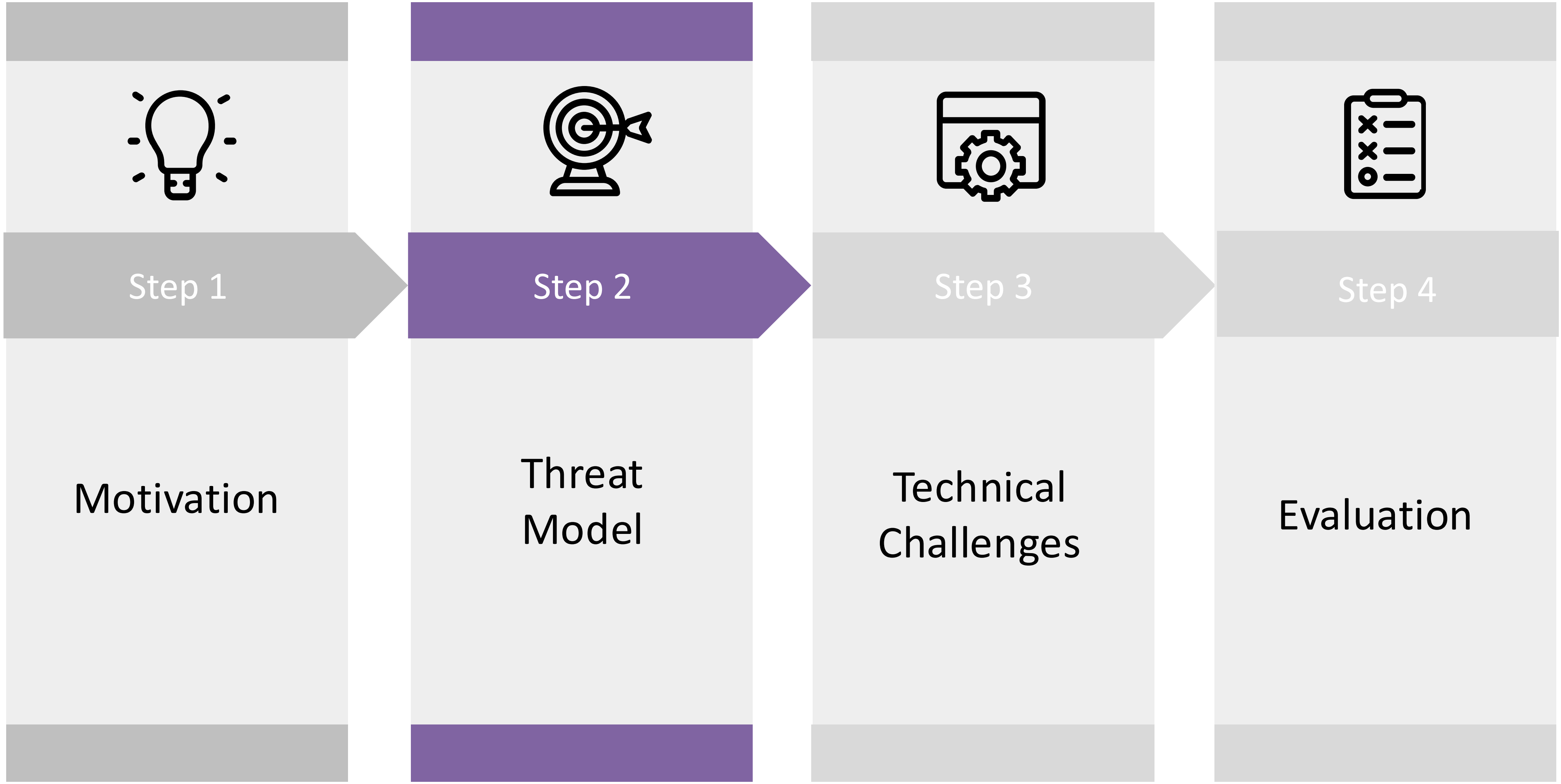
→ Laser can simulate the heat signature

- Laser's energy can be focused into an intense spot
- Laser generates heat in short time
- Laser light can travel long distance



We can remotely simulate fake motion using laser

Outline



Step 1

Motivation

Step 2

Threat Model

Step 3

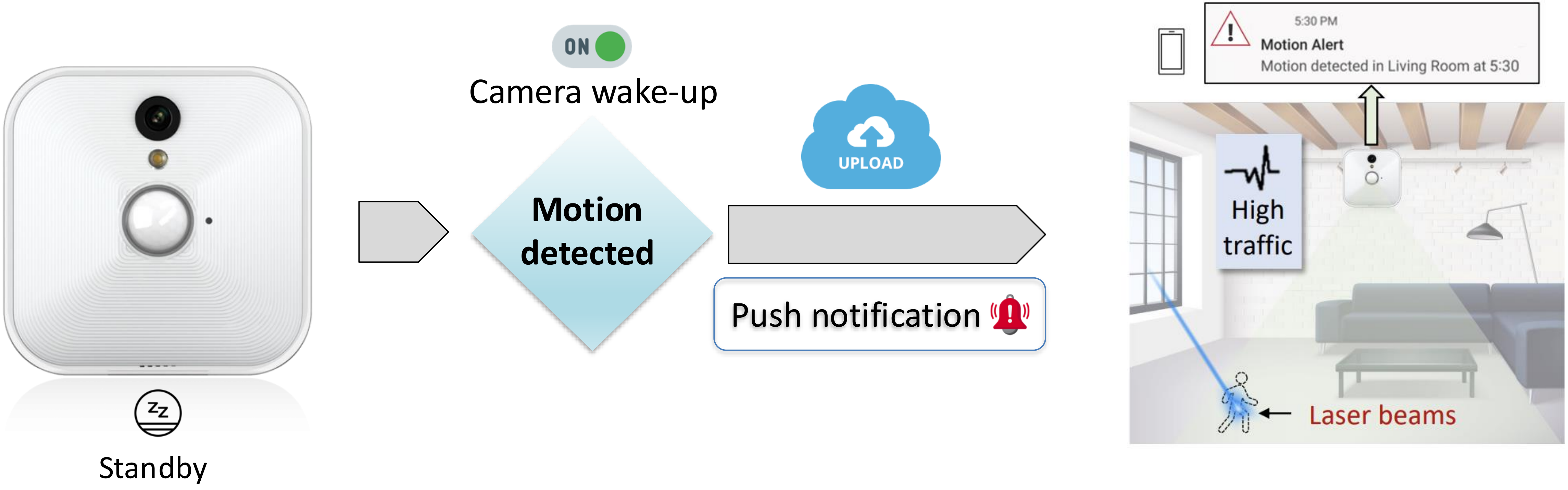
Technical Challenges

Step 4

Evaluation

Vulnerability: Laser-Generated Fake Motion

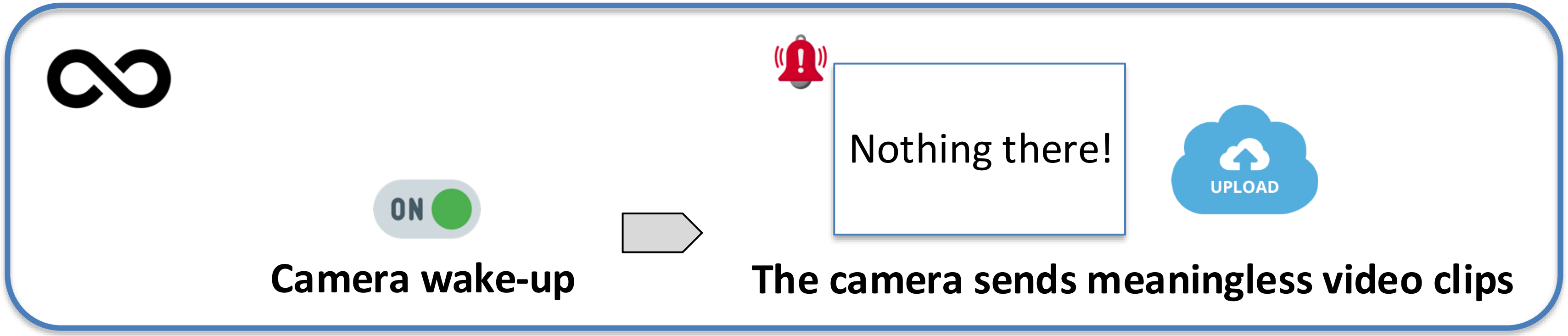
- **Security cameras are vulnerable to laser-generated fake motion**
  - This attack can simulate motion without any human presence
  - It activates the camera in the same way as real motion



5:30 PM
Motion Alert
Motion detected in Living Room at 5:30

Laser Fake Motion

- **This leads to two major problems**:
  - The camera records and uploads empty video clips because the laser spot is too small or invisible
  - Repeating this attack continuously triggers the camera's motion activation process



Camera wake-up

Nothing there!

The camera sends meaningless video clips

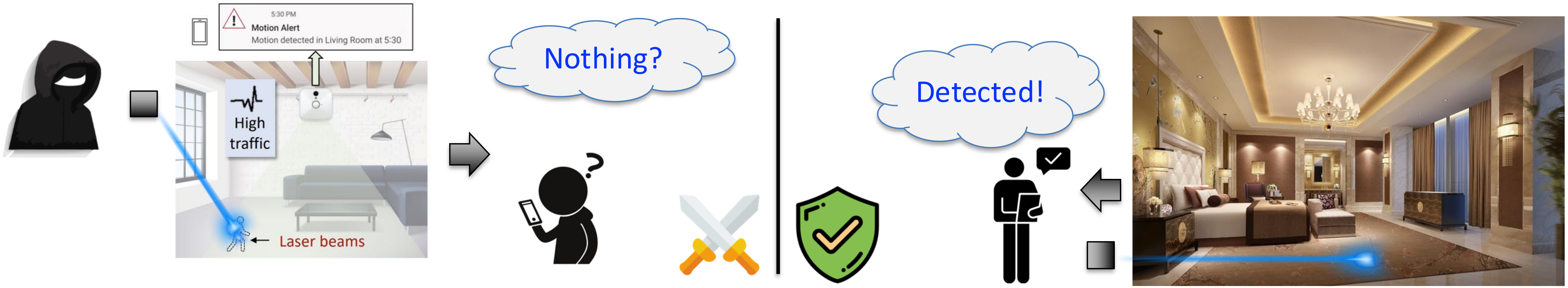
The user experiences "alert fatigue"

The camera is disabled due to battery depletion
(For battery powered cameras)

Threat Model

1. General Application Domains

- **Attack:** Targeting and compromising wireless security surveillance systems.
- **Defense:** Identifying and neutralizing hidden or unauthorized spy cameras.



2. Adversary Capabilities & Methodology

- **WiFi Sniffing**
- **Line-of-Sight (LoS)**

3. Operational Constraints

- **No Human Motion:** Avoid being caught or identified by the surveillance system.

Outline

Step 1

Motivation

Step 2

Threat Model

Step 3

Technical Challenges

Step 4

Evaluation

Challenge 1 - Find Target Camera

How to collect MAC addresses?

WiFi Sniffer
(Monitor Mode)

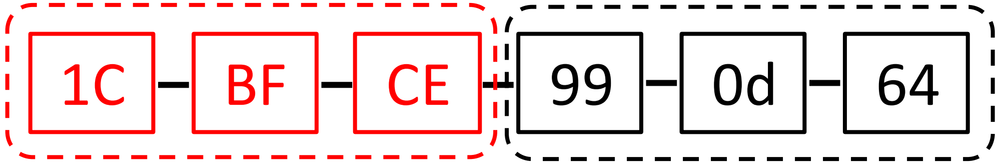
Android Phone
(Rooted)

MAC Address Broadcasting

802.11 Header
(Unencrypted)

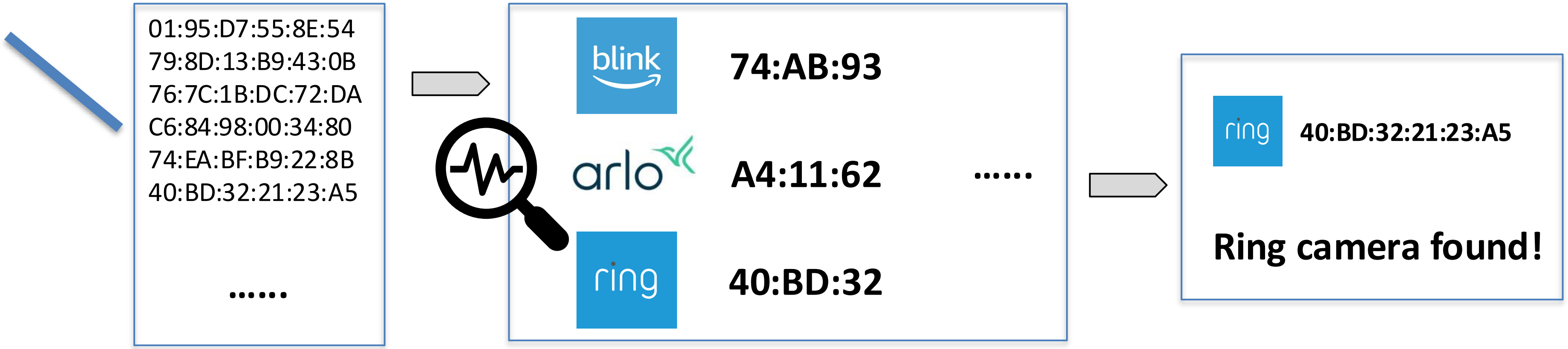
- **MAC address** is determined by corresponding SoC manufacturer and has the following format:

OUI → device manufacturer and device type
(Organizationally Unique Identifier)



Device ID

- **Camera-labeled OUI table lookup**: contain OUIs of all cameras on the market



01:95:D7:55:8E:54
79:8D:13:B9:43:0B
76:7C:1B:DC:72:DA
C6:84:98:00:34:80
74:EA:BF:B9:22:8B
40:BD:32:21:23:A5
……

blink	**74:AB:93**
arlo	**A4:11:62**
ring	**40:BD:32**

……

ring **40:BD:32:21:23:A5**

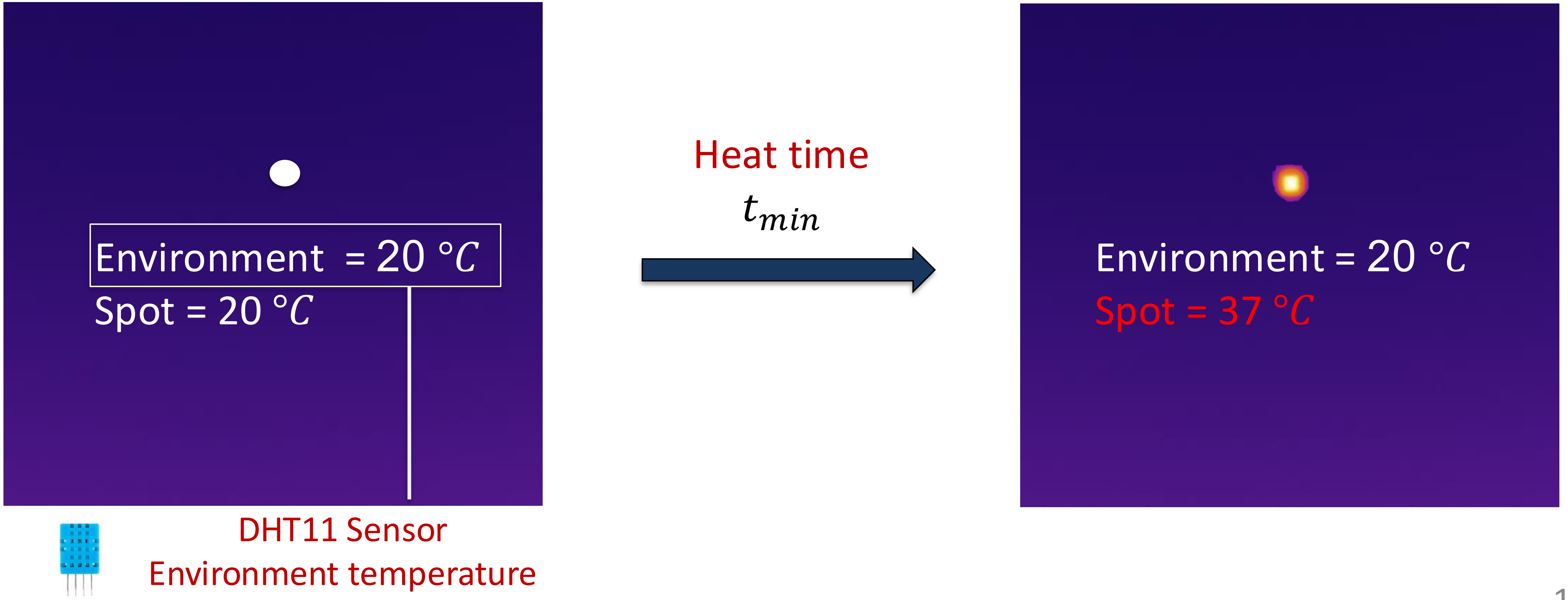
Ring camera found!

Sniff Nearby devices

OUI Table

Challenge 2: Laser Heating Control

- **The laser's heating time determines the spot temperature**
  - **Goal:** Laser spot temperature = human temperature (increase ΔT)
  - We define t_{min} as the minimum heating time required to achieve this ΔT



Environment = 20 $°C$
Spot = 20 $°C$

Heat time
t_{min}

Environment = 20 $°C$
Spot = 37 $°C$

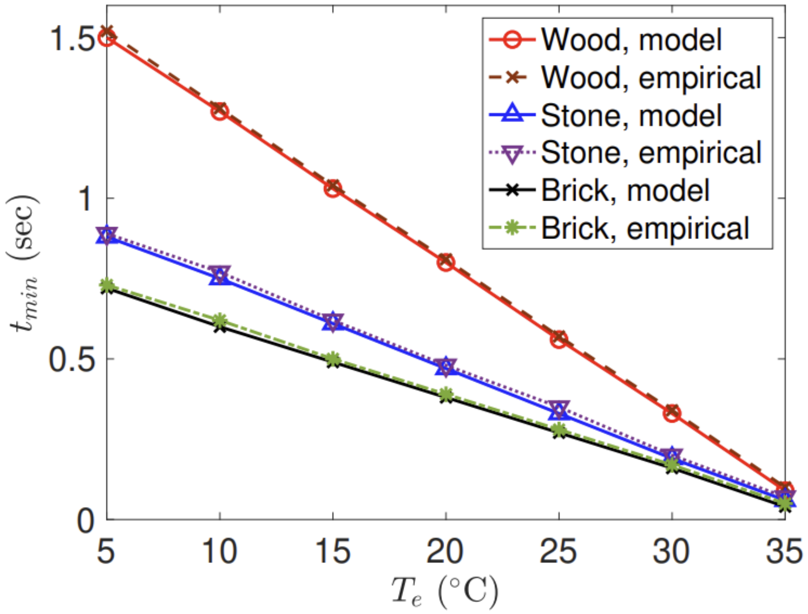
DHT11 Sensor
Environment temperature

Heating Time Modeling

- **As defined, t_{min} is the laser-on time required to generate the necessary heat**
  - This heating time varies across different materials
  - We modeled the heating process for three common materials

Different heat time

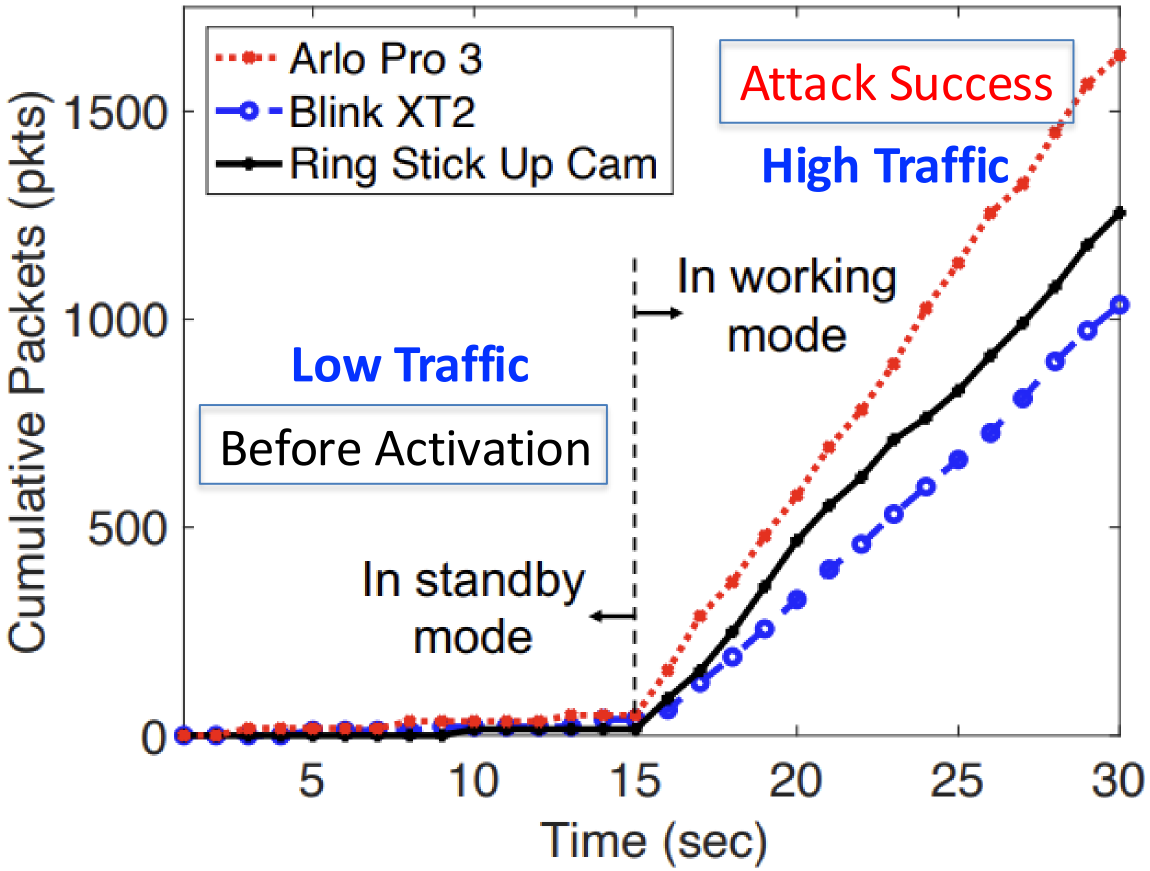
t_{min}



Different building materials

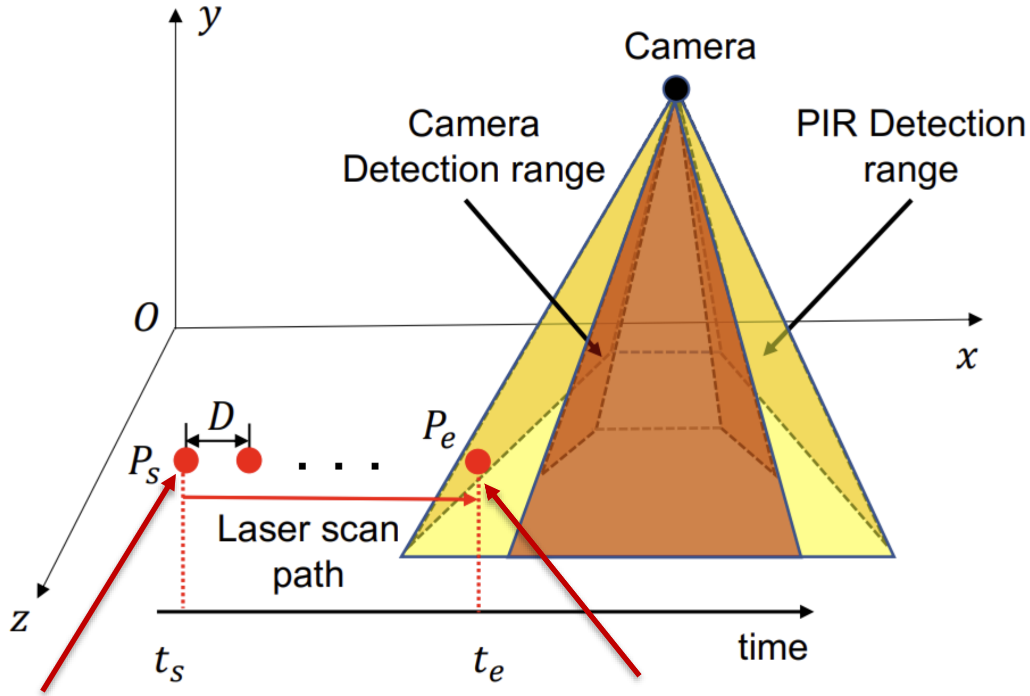
Challenge 3 : Device Activation Detection

- **How can we identify when the camera is activated by a laser?**
  - When activated, camera has a rapid increase in network packets
  - We can observe this traffic pattern to confirm if the attack was successful



Challenge 4 - Laser Scanning

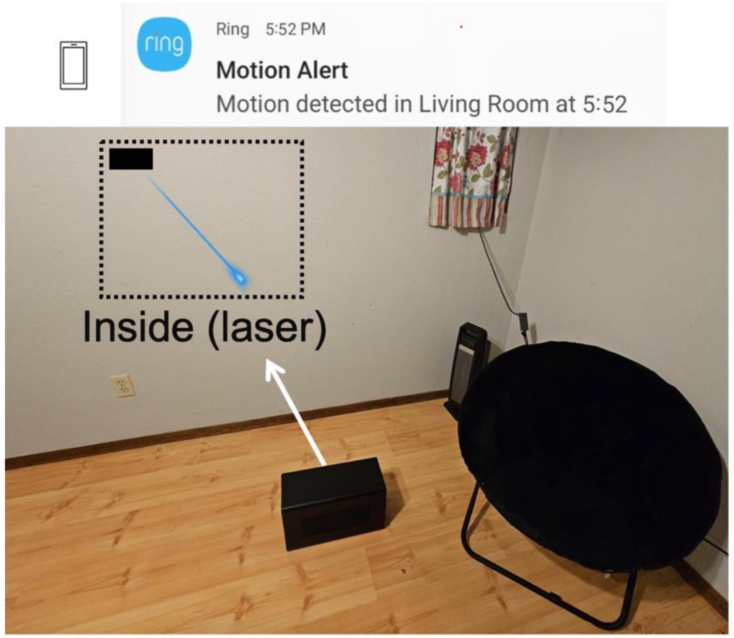
- **Scanning is required to find the motion sensor's coverage area**
  - We select a starting point, P_s, which is often the leftmost point of the area
  - The gap between scanned points is defined as D
  - Each point is heated for a duration of t_{min}



Start point (No traffic)

End point (High traffic)

Stealth Attack

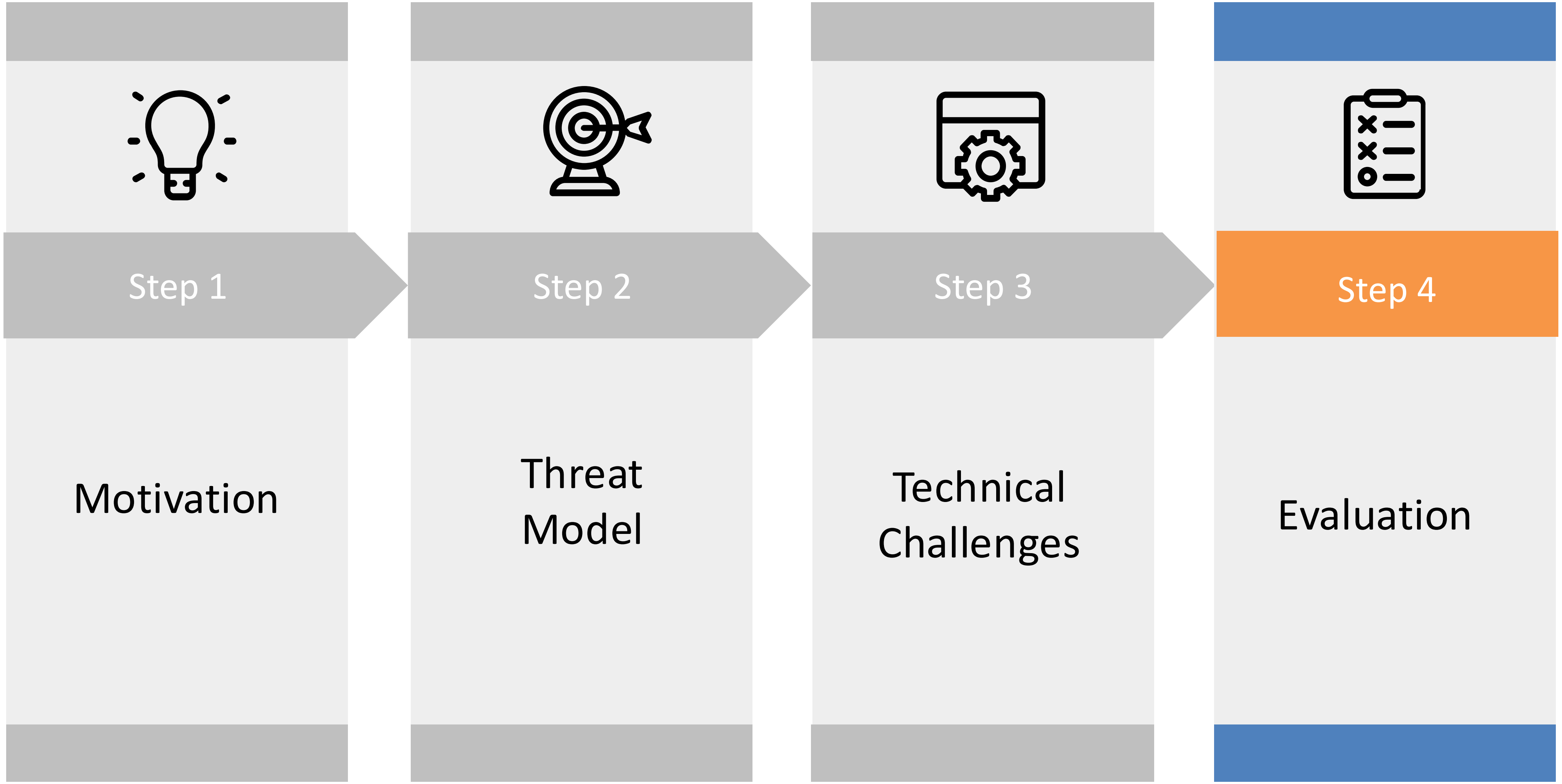


Ring 5:52 PM

Motion Alert

Motion detected in Living Room at 5:52

Outline



Step 1

Motivation

Step 2

Threat Model

Step 3

Technical Challenges

Step 4

Evaluation

Evaluation Setup

- Tested devices: 15 Cameras, 3 Security Systems

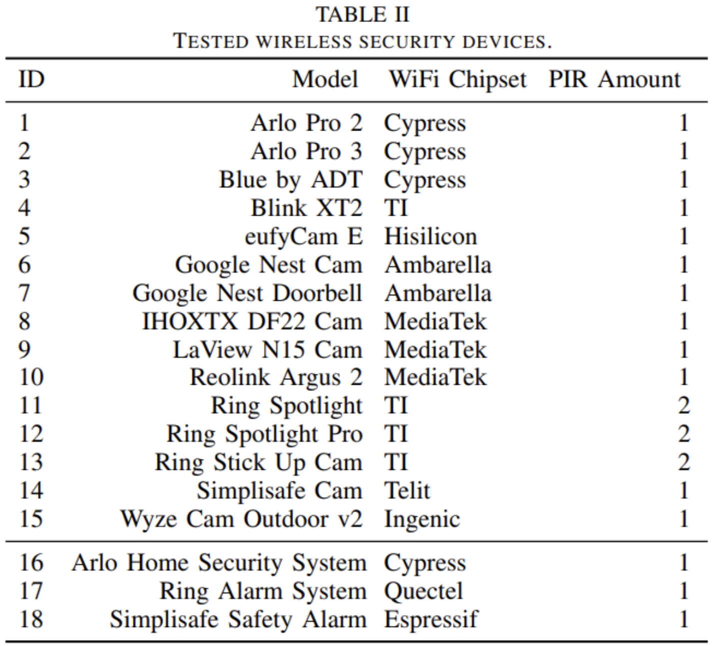
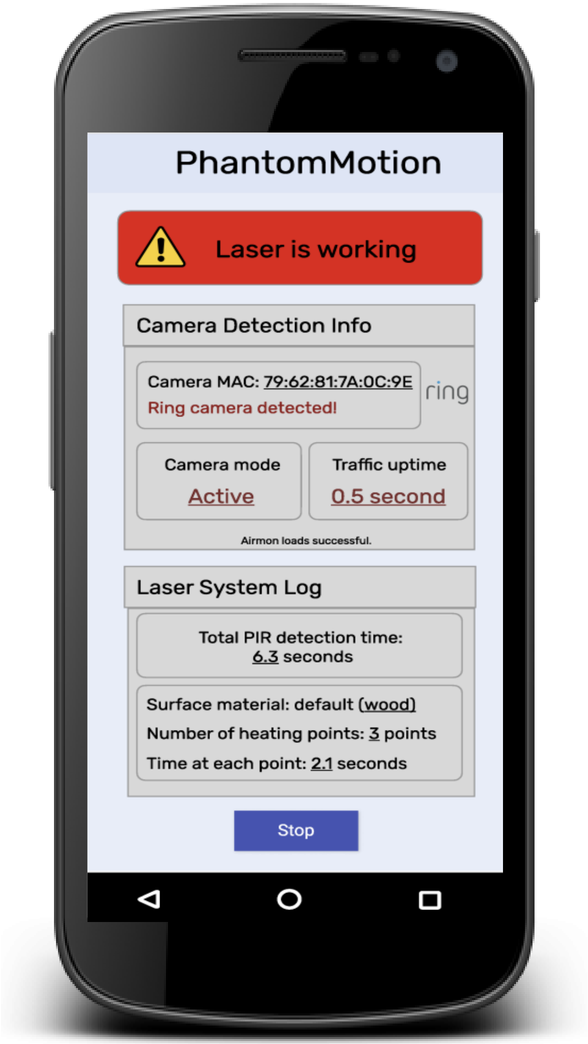


TABLE II
TESTED WIRELESS SECURITY DEVICES.

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

- Metrics: (1) Success rate; (2) False Positive Rate;
  (3) Operation time; (4) Scanning distance



PhantomMotion

⚠ Laser is working

Camera Detection Info

Camera MAC: 79:62:81:7A:0C:9E
Ring camera detected!

Camera mode: Active

Traffic uptime: 0.5 second

Airmon loads successful.

Laser System Log

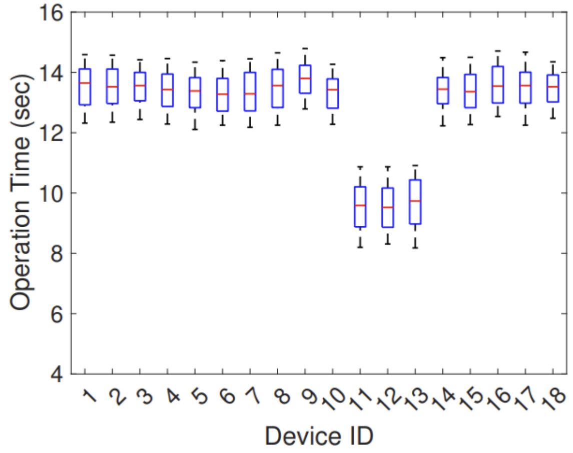
Total PIR detection time: 6.3 seconds

Surface material: default (wood)
Number of heating points: 3 points
Time at each point: 2.1 seconds

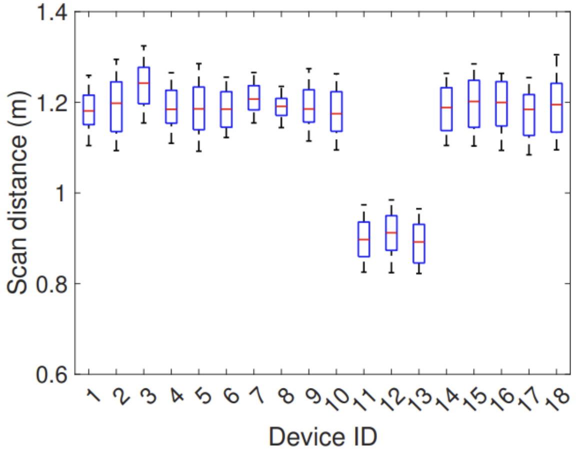
Our phone APP

Performance Across Cameras

- The success rate is consistently 100%
- The false positive rate is consistently 0%

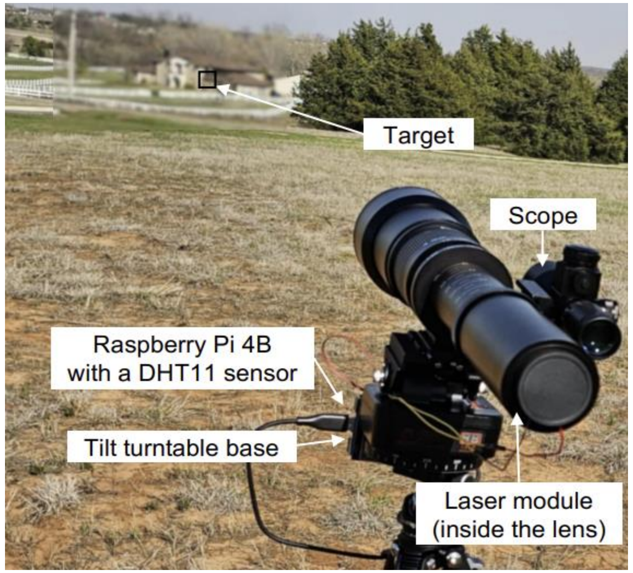


Overall operation time



Overall scan distance

- ✓ The observed operation time is under 15 seconds
- ✓ The observed scan distance is less than 1.4 meters



Target
Scope
Raspberry Pi 4B with a DHT11 sensor
Tilt turntable base
Laser module (inside the lens)

☞

- ✓ The **max distance**:
  - 120 meters

Thank you!

Questions and Answers