Pattern-of-Life Modeling Using Data Leakage in Smart Homes

Captain Steven Beyer

Co-Authors:

Dr. Barry Mullins

Dr. Scott Graham

Major Jason Bindewald

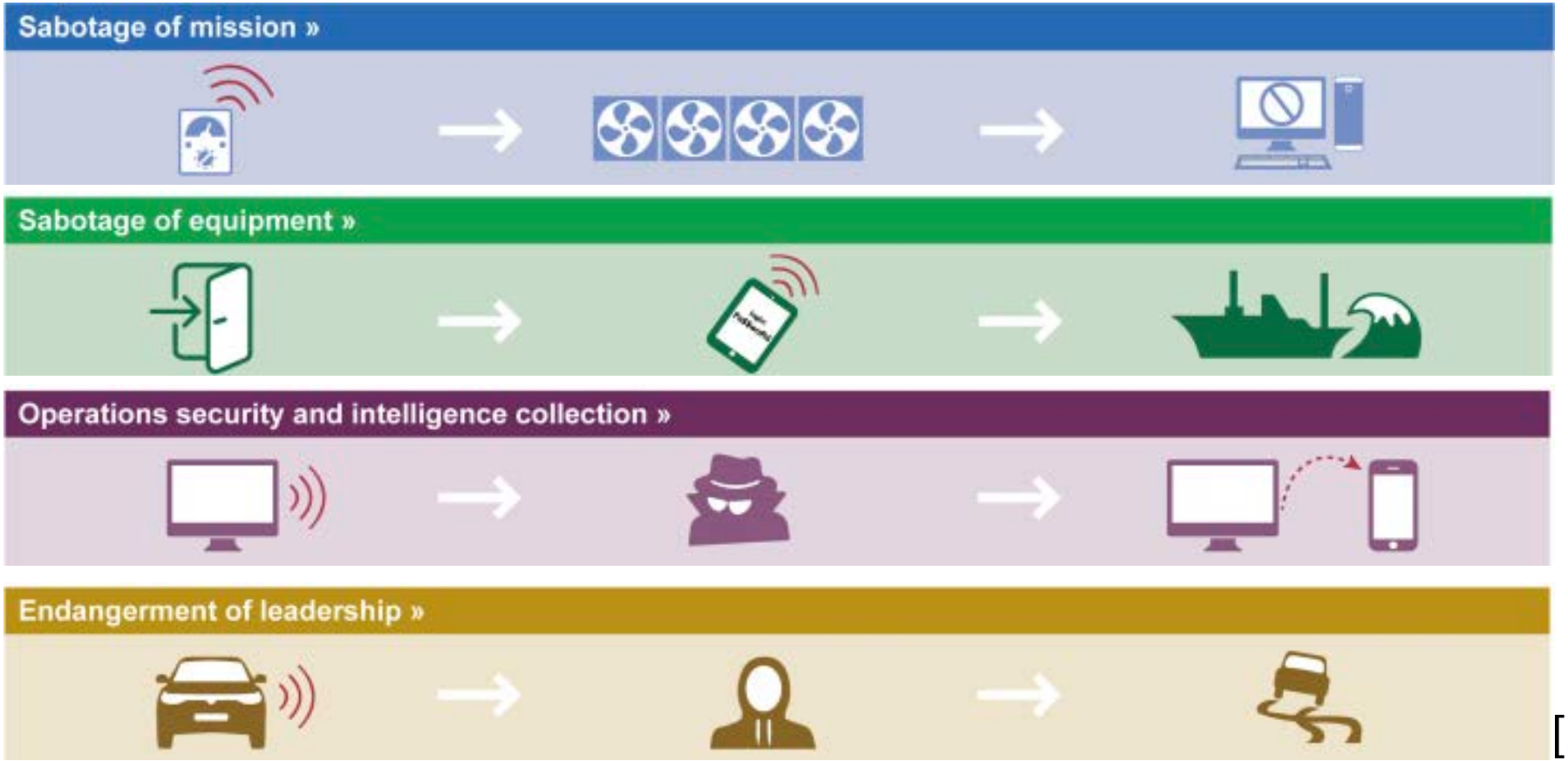
AFIT/ENG

May 8, 2018

Agenda

- Motivation
- Problem statements
- Related work
- Goals
- Smart home architecture
- Device leakage and vulnerability investigation
- Data leakage tool
- Mitigation tool
- Conclusion
- Significance of research
- Future work

Motivation



[1]

In 2017 the US Government Accountability Office released a report to Congress stressing the need of assessment/guidance on IoT in the DoD [1].

Motivation

[1]

Researchers need to investigate the security ramifications IoT devices have on **operations security**, **intelligence collection**, and **leadership safety** [1].

Motivation

[1]

40.8 million smart home devices are expected to ship in the US in 2018 [2].

Problem Statements

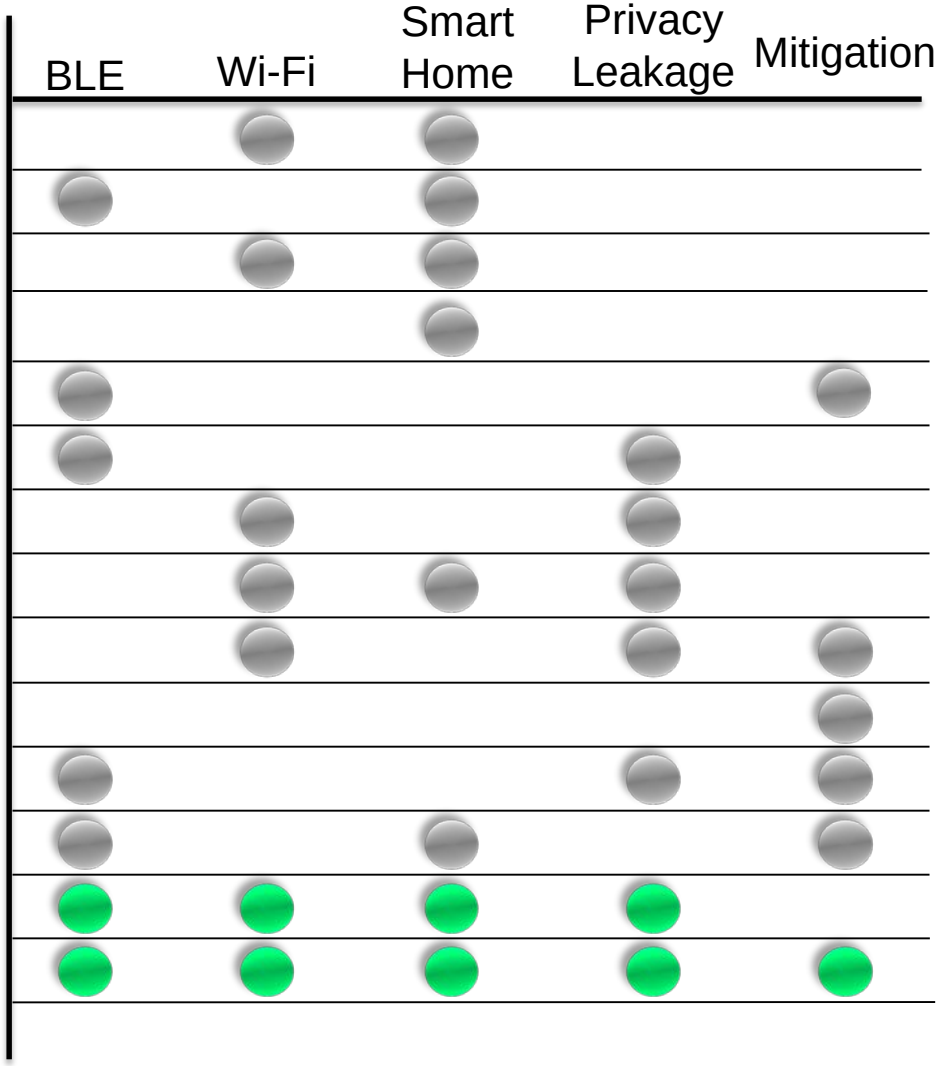
1. What kind of privacy data do smart home devices leak?

2. How can an attacker exploit data leakage to threaten operational and physical security?

3. Are there ways to defend against these vulnerabilities?

Related Work

- Skoudis (2017) [3]
- Rose and Ramsey (2016) [4]
- Jourdois (2016) [5]
- Slawomir (2016) [6]
- Gutierrez, et al. (2017) [7]
- Das, et al. (2016) [8]
- Zhou, et al. (2014) [9]
- Madrigal (2017) [10]
- Gruteser and Grunwald (2005) [11]
- Rivest (1998) [12]
- Fawaz, et al. (2016) [13]
- Gutierrez, et al. (2017) [14]
- Beyer, et al. (2018)
- Beyer, et al. (2018)



Goals

1. **Develop a smart home architecture** to analyze IoT data leakage in the wild.

2. **Identify data leakage and vulnerabilities** in smart home devices.

3. **Utilize data leakage and vulnerabilities** to classify devices, identify events, track users, and gain physical access to a smart home.

4. **Mitigate data leakage and vulnerabilities** to create a safer smart home.

Goals

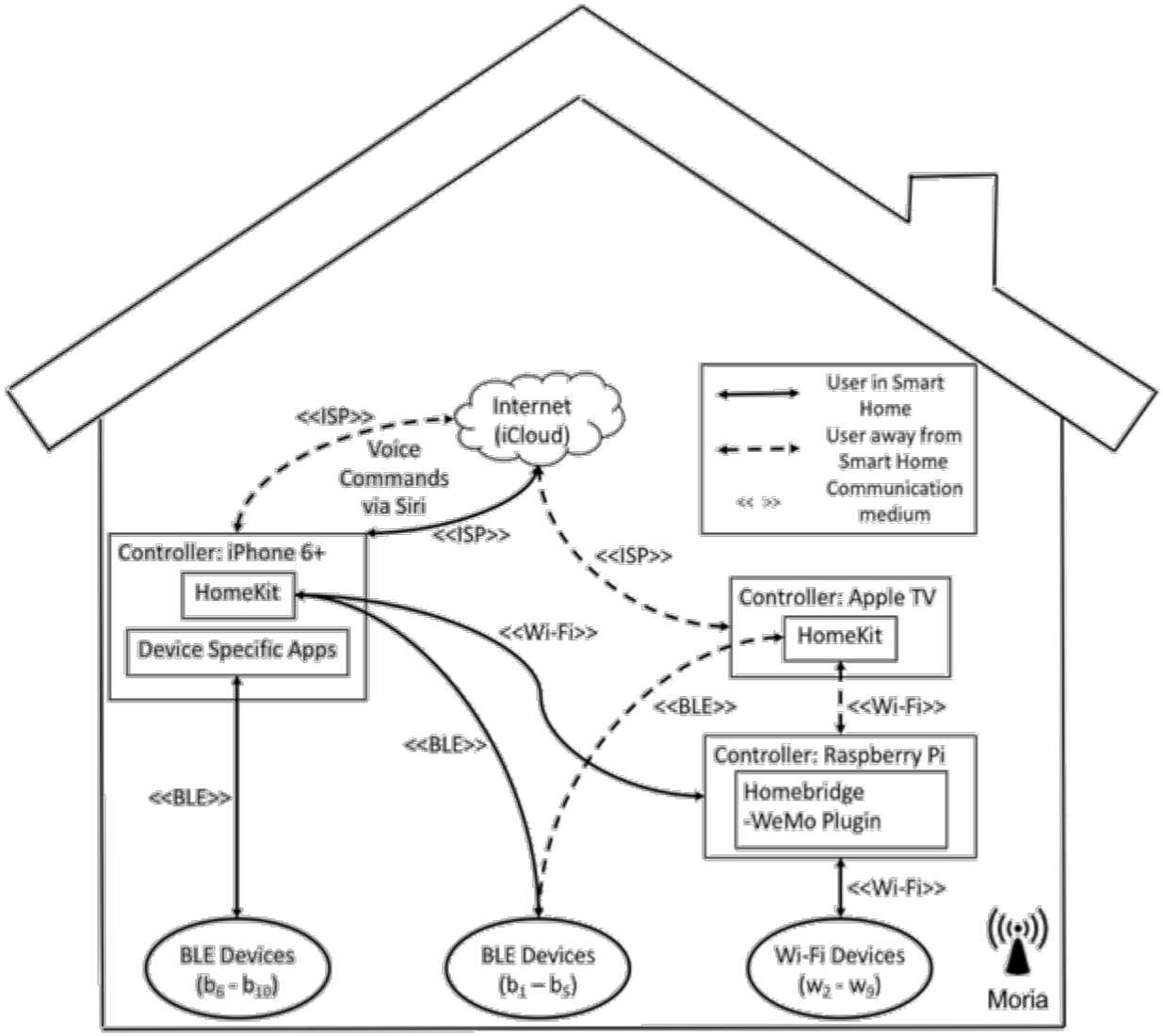
1. **Develop a smart home architecture** to analyze IoT data leakage in the wild.

2. **Identify data leakage and vulnerabilities** in smart home devices.

3. **Utilize data leakage and vulnerabilities** to classify devices, identify events, track users, and gain physical access to a smart home.

4. **Mitigate data leakage and vulnerabilities** to create a safer smart home.

Smart Home Automation Architecture



Smart Home Automation Architecture

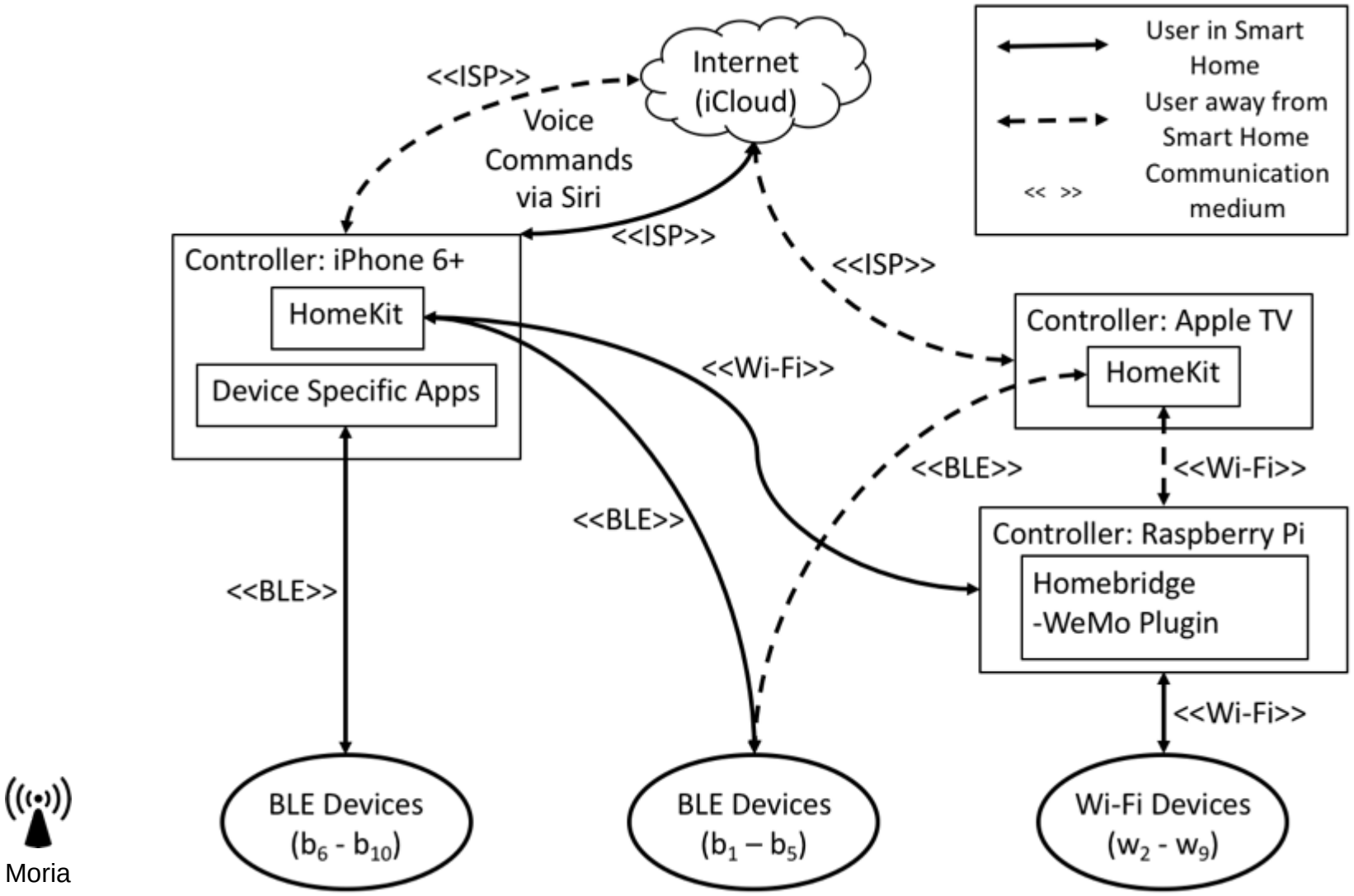
Wi-Fi Devices

ID	Manuf	Device Type	Device Name
w_1	Calix	Wireless Router	Moria
w_2	Belkin	Camera	NetCam
w_3	Belkin	Outlet	Switch1
w_4	Belkin	Outlet	Switch2
w_5	Belkin	Outlet	Switch3
w_6	Belkin	Outlet	Switch4
w_7	Belkin	Motion Sensor	Motion
w_8	Belkin	Energy Outlet	Insight
w_9	Belkin	Mini Outlet	Mini
w_{10}	Raspberry Pi 3B	Computer	Pi
w_{11}	Apple	iPhone 6+	Steves-phone
w_{12}	Apple	TV 2	Apple-TV

BLE Devices

ID	Manuf	Device Type	Device Name
b_1	Elgato	Indoor Temperature	Eve Room
b_2	Elgato	Outdoor Temperature	Eve Weather
b_3	Elgato	Motion Sensor	Eve Motion
b_4	Elgato	Outlet	Eve Energy
b_5	Elgato	Door Sensor	Eve Door
b_6	Instant Pot	Smart Cooker	Instant Pot
b_7	MPow	Lightbulb	Playbulb
b_8	ZKTeco	Lock	BioLock
b_9	BitLock	Lock	Bike lock
b_{10}	SafeTech	Gunsafe	Gunsafe
b_{11}	Apple	iPhone 6+	Steves-phone
b_{12}	Apple	TV 2	Apple TV

Smart Home Automation Architecture



Moria

Goals

1. **Develop a smart home architecture** to analyze IoT data leakage in the wild.

2. **Identify data leakage and vulnerabilities** in smart home devices.

3. **Utilize data leakage and vulnerabilities** to classify devices, identify events, track users, and gain physical access to a smart home.

4. **Mitigate data leakage and vulnerabilities** to create a safer smart home.

Goals

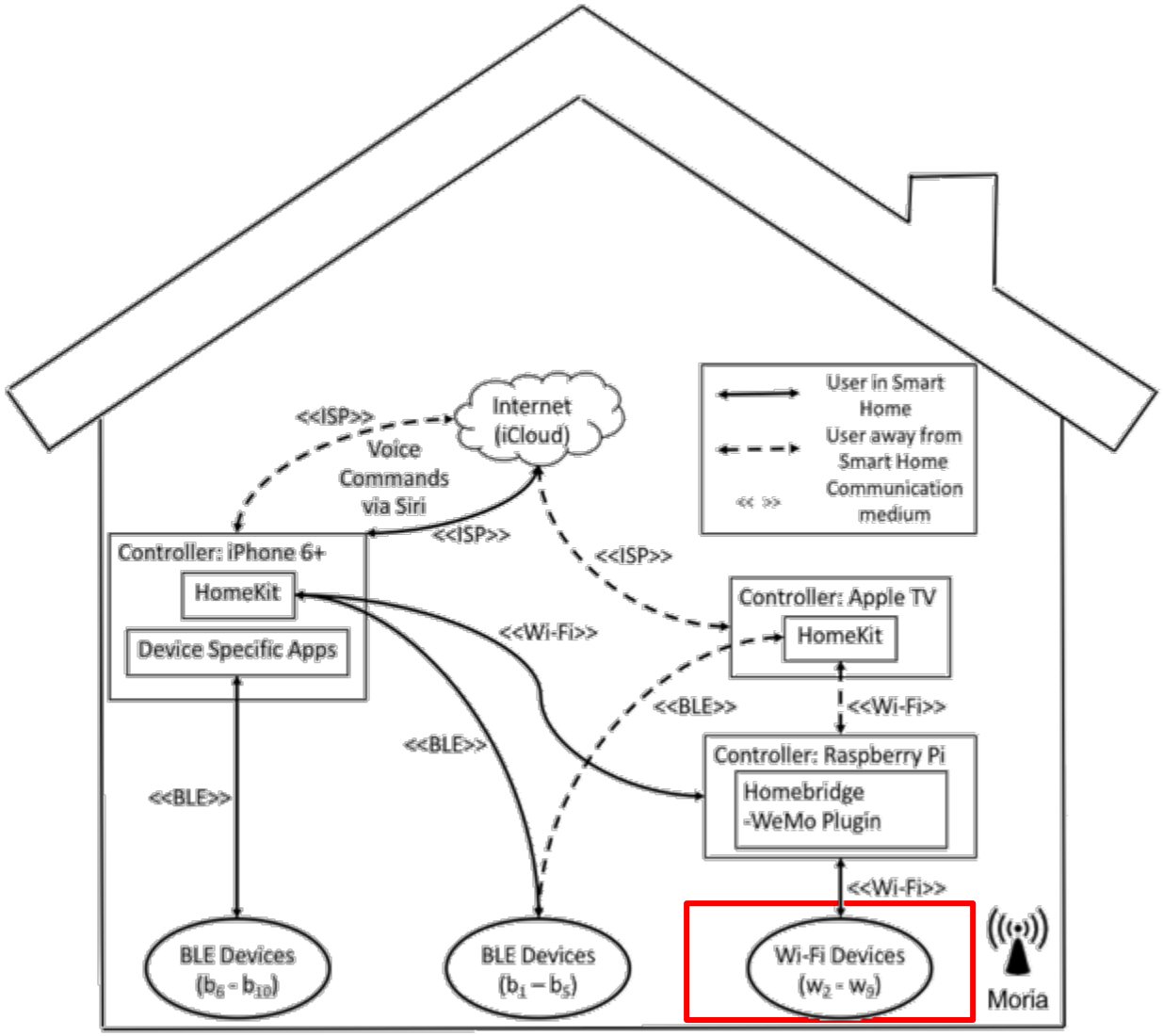
1. **Develop a smart home architecture** to analyze IoT data leakage in the wild.

2. **Identify data leakage and vulnerabilities** in smart home devices.

3. **Utilize data leakage and vulnerabilities** to classify devices, identify events, track users, and gain physical access to a smart home.

4. **Mitigate data leakage and vulnerabilities** to create a safer smart home.

Smart Home Automation Architecture



Wi-Fi Protocol

- MAC Protocol Data Unit (MPDU)

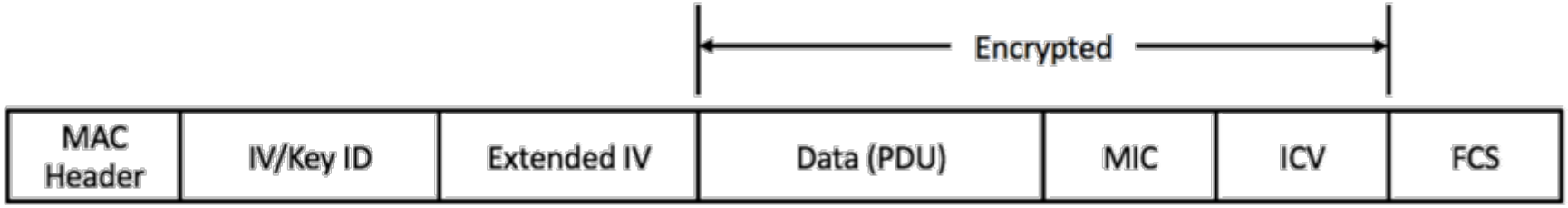


Figure 1. MPDU format when using WPA2

- Frame Size
- Packet Timestamp

Wi-Fi Protocol

- MAC Protocol Data Unit (MPDU)

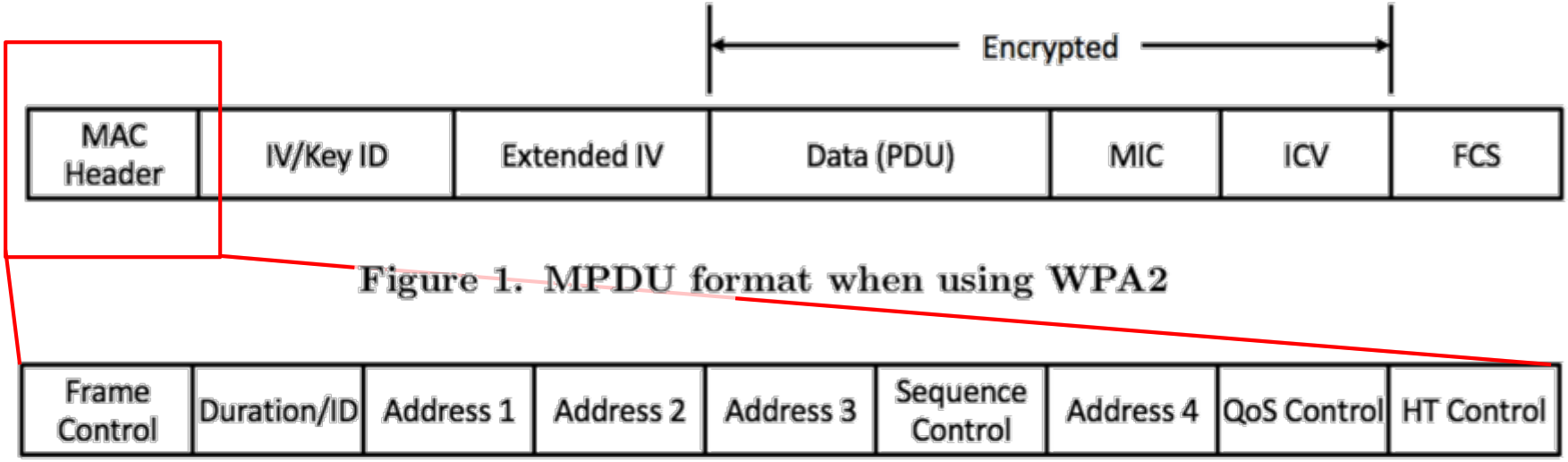


Figure 1. MPDU format when using WPA2

Figure 2. MAC header frame format

- Frame Size
- Packet Timestamp

Wi-Fi Protocol

- MAC Protocol Data Unit (MPDU)

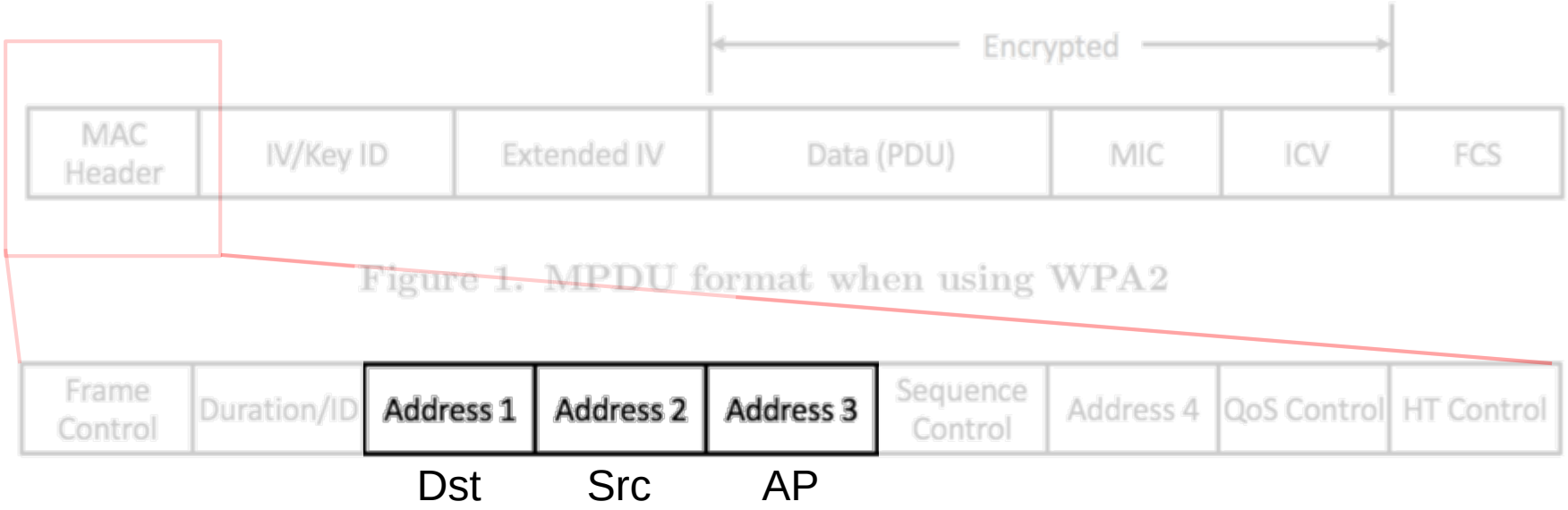


Figure 1. MPDU format when using WPA2

Figure 2. MAC header frame format

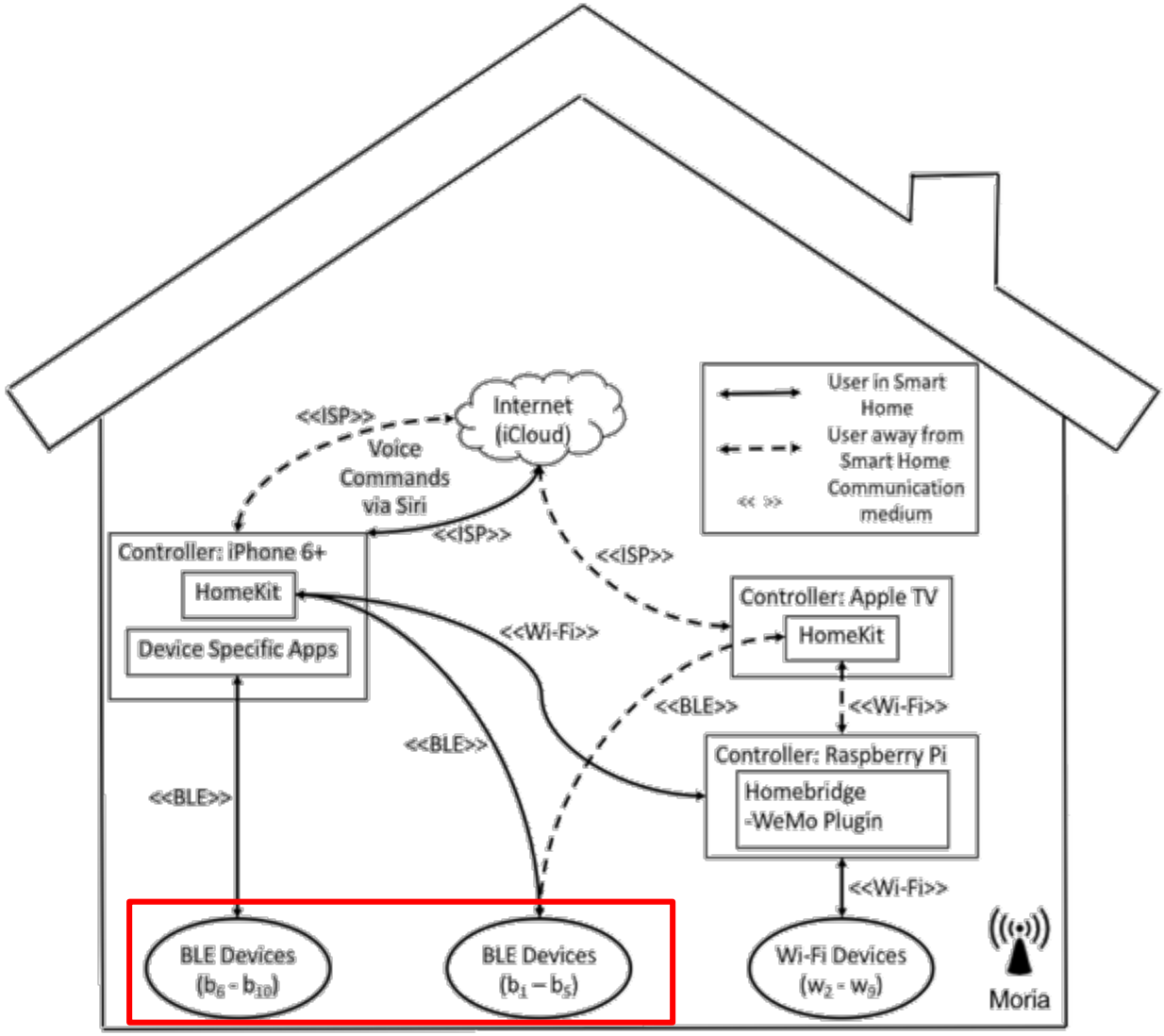
- Frame Size
- Packet Timestamp

Wi-Fi Device Traffic Investigation

- Traffic captured using Alfa Card
- Capture investigated using Wireshark
- Compared event time with traffic looking for trends

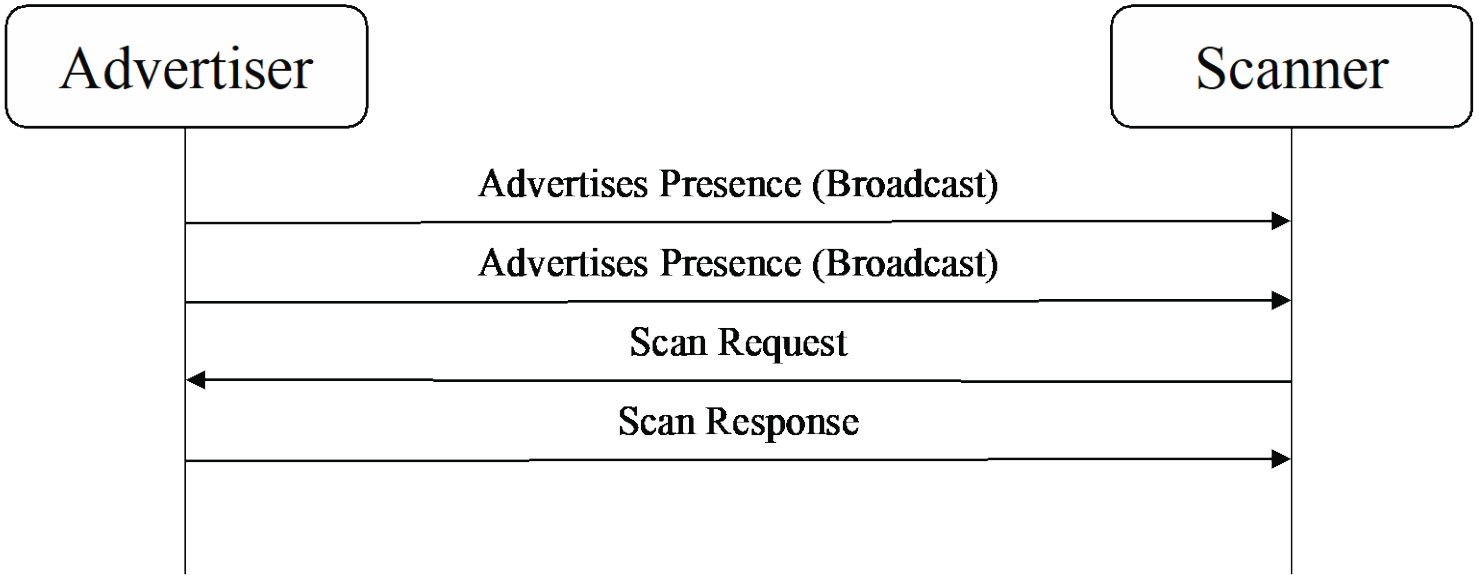
Time	Source	Destination	Length
07:10:18.199197	Raspberr…	BelkinIn…	619
07:10:18.199195	Raspberr…	BelkinIn…	619
17:48:39.951841	Raspberr…	BelkinIn…	619
17:48:39.952858	Raspberr…	BelkinIn…	619
18:00:14.203301	Raspberr…	BelkinIn…	619
18:00:14.204835	Raspberr…	BelkinIn…	619

Smart Home Automation Architecture



BLE Protocol

- Active Scanning




```
▼ Advertising Data
  ▼ Device Name: Eve Door 91B3
      Length: 14
      Type: Device Name (0x09)
      Device Name: Eve Door 91B3
```

BLE Device Traffic Investigation

- 3x Ubertooth One Bluetooth adapters
- Capture investigated using Wireshark
- Compared event time with traffic looking for trends

Time	Source	Destination	Length	Info
07:04:27.10659…	5b:53:55…	f0:3a:a4…	53	CONNECT_REQ

- ADV_IND, SCAN_RESP, and CONNECT_REQ

- Found that ZKTeco BLE BioLock communication sends passwords in the clear

```
▼ Bluetooth Attribute Protocol
    ▶ Opcode: Write Request (0x12)
    ▶ Handle: 0x001c (Unknown: Unknown)
      Value: 41542b504153534b45593d3132333435360d0a

0000  22 d6 80 00 00 00 00 00  27 00 af 73 65 50 02 1a   "....... '..seP..
0010  16 00 04 00 12 1c 00 41  54 2b 50 41 53 53 4b 45   .......A T+PASSKE
0020  59 3d 31 32 33 34 35 36  0d 0a 6e 40 54            Y=123456 ..n@T
```

Goals

1. **Develop a smart home architecture** to analyze IoT data leakage in the wild.

2. **Identify data leakage and vulnerabilities** in smart home devices.

3. **Utilize data leakage and vulnerabilities** to classify devices, identify events, track users, and gain physical access to a smart home.

4. **Mitigate data leakage and vulnerabilities** to create a safer smart home.

Goals

1. **Develop a smart home architecture** to analyze IoT data leakage in the wild.

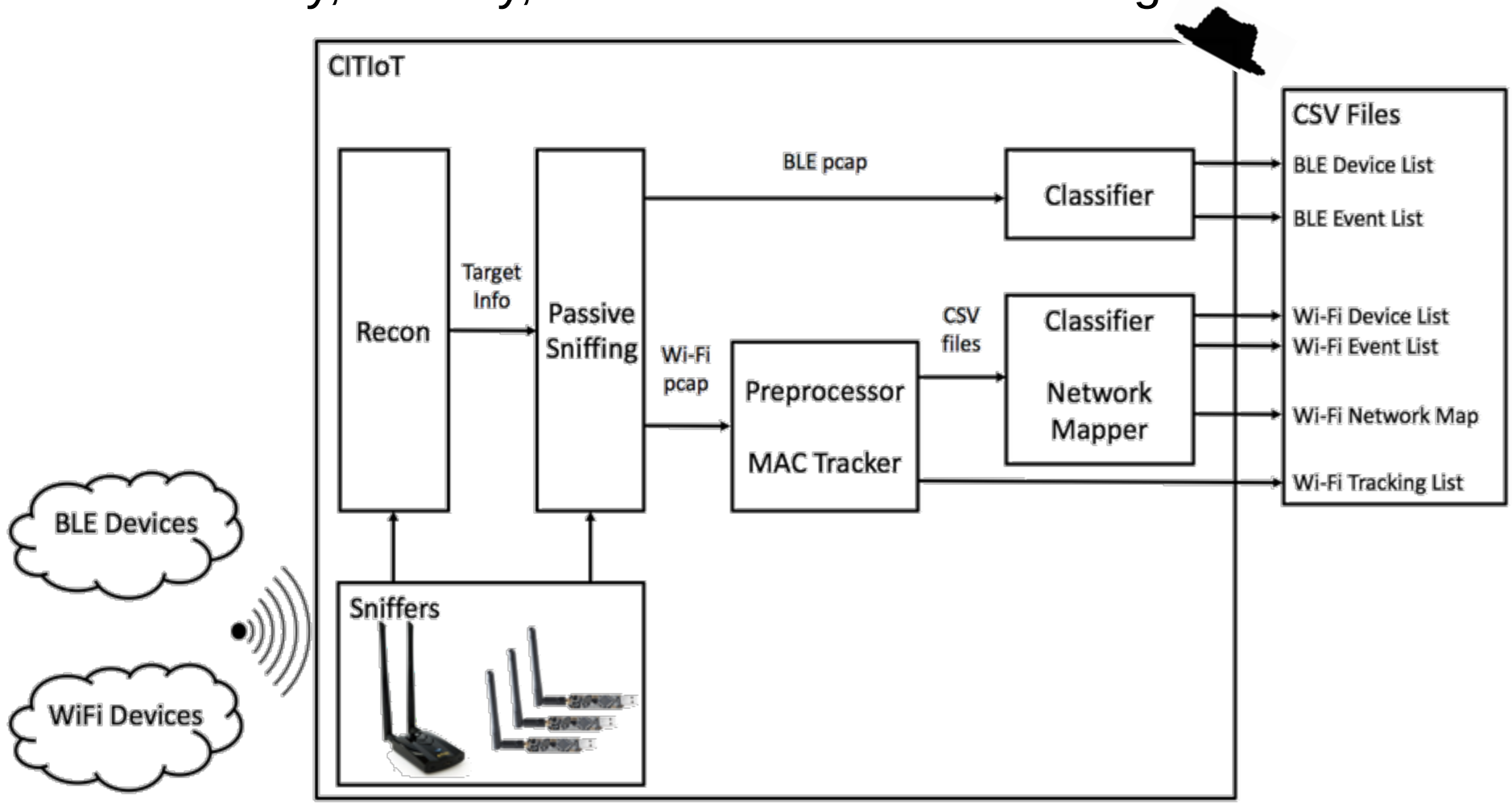
2. **Identify data leakage and vulnerabilities** in smart home devices.

3. **Utilize data leakage and vulnerabilities** to classify devices, identify events, track users, and gain physical access to a smart home.

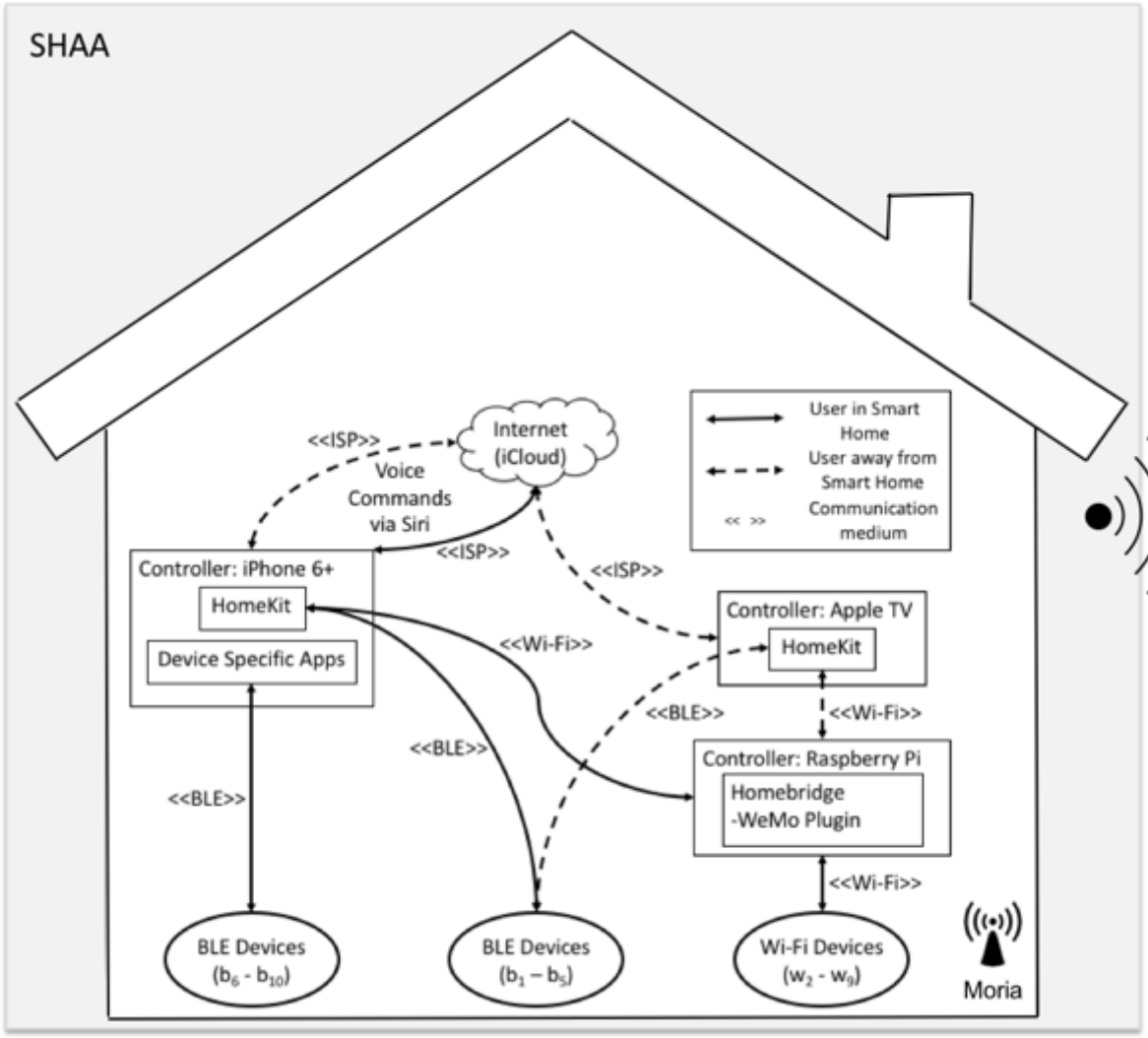
4. **Mitigate data leakage and vulnerabilities** to create a safer smart home.

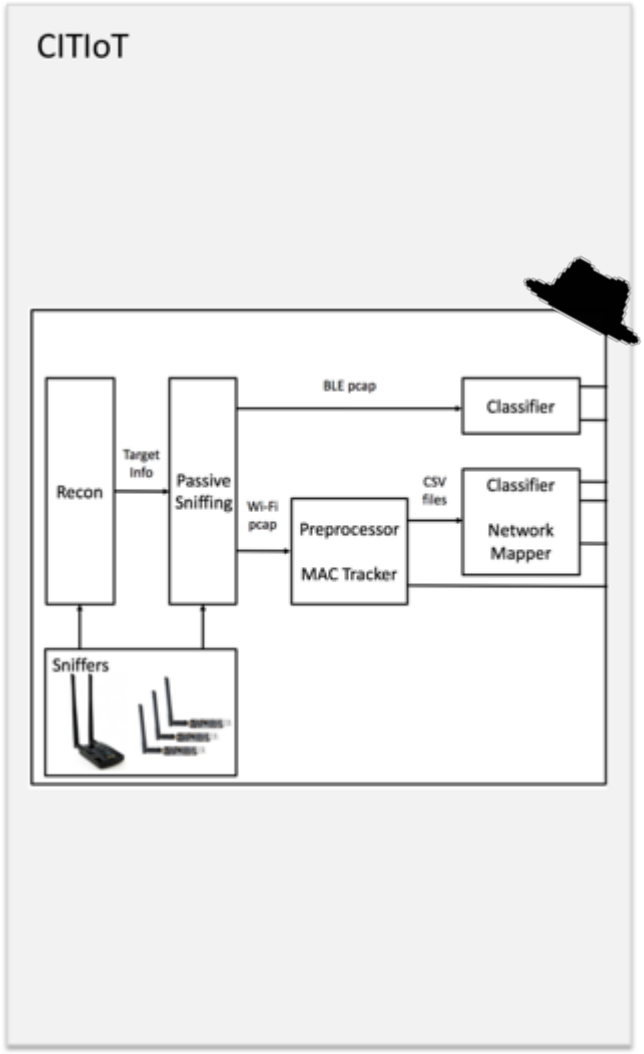
CITIoT

- Classify, Identify, and Track Internet of Things



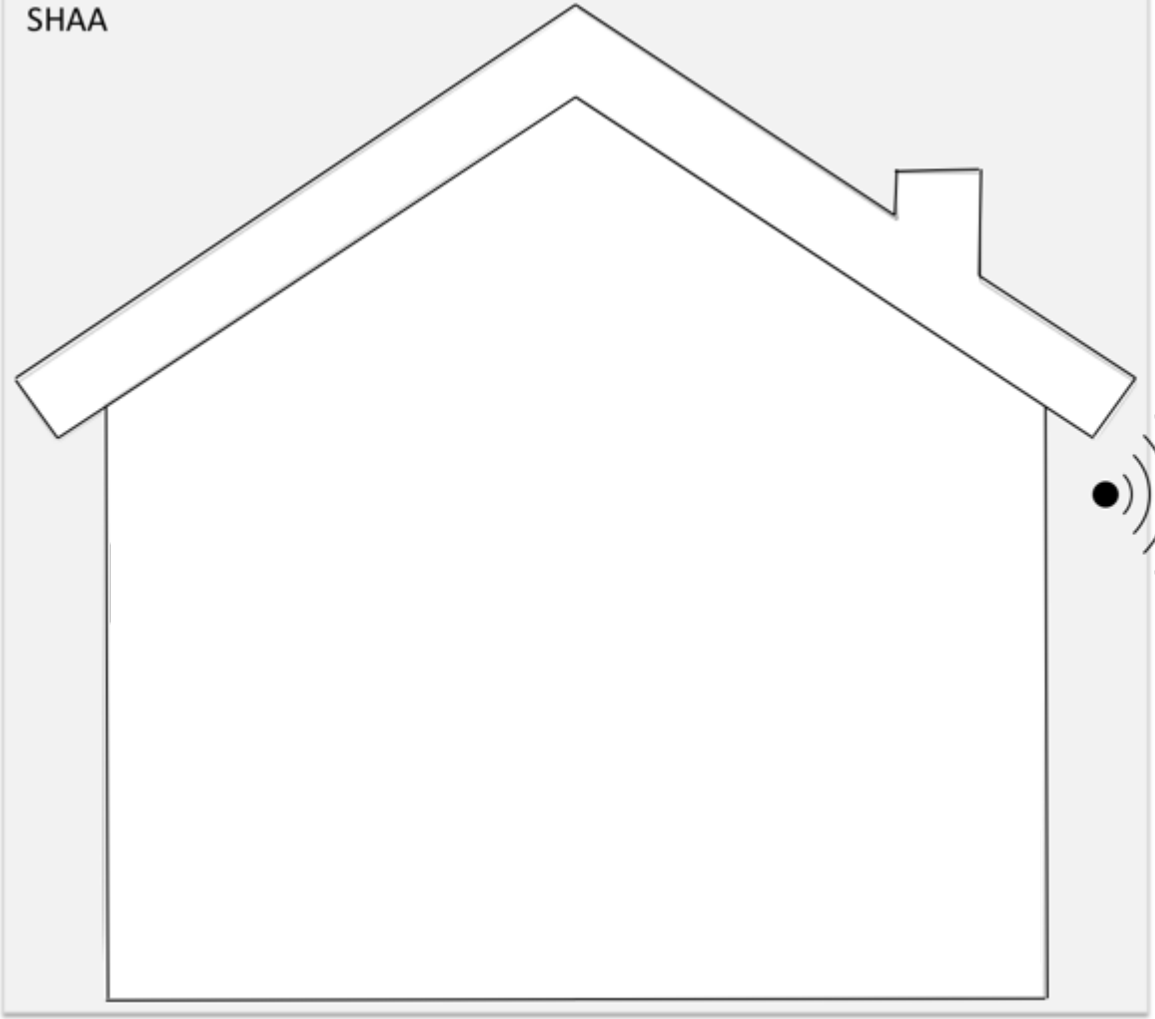
System Diagram



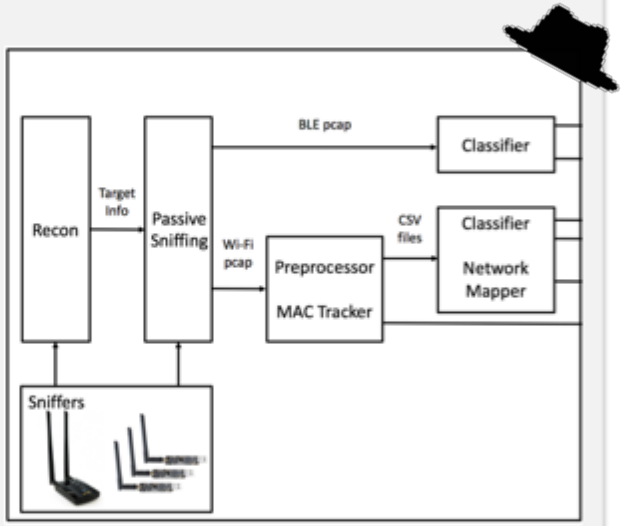


Attacker's Perspective

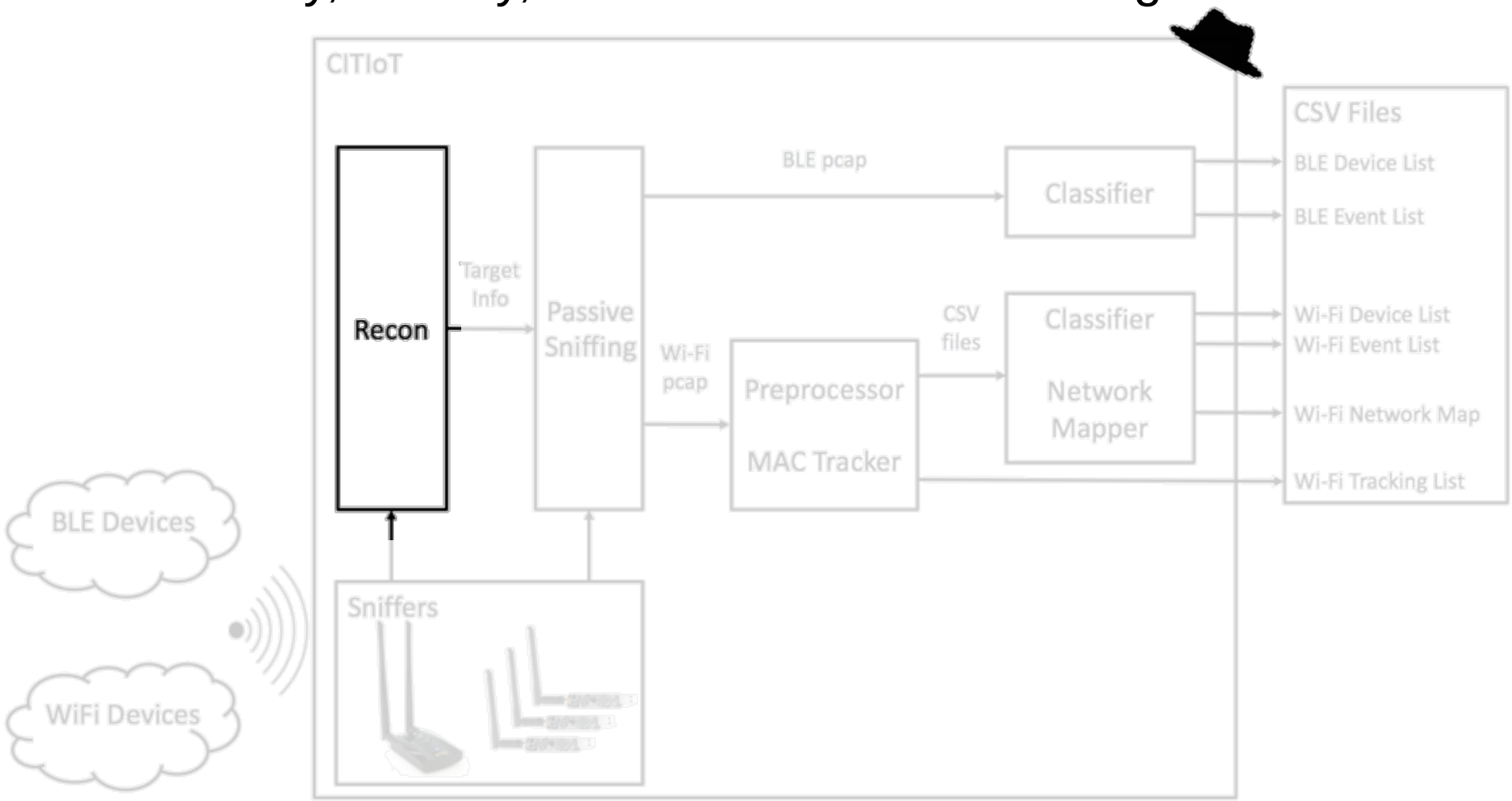
SHAA



CITIoT



- Classify, Identify, and Track Internet of Things



Reconnaissance and Scanning

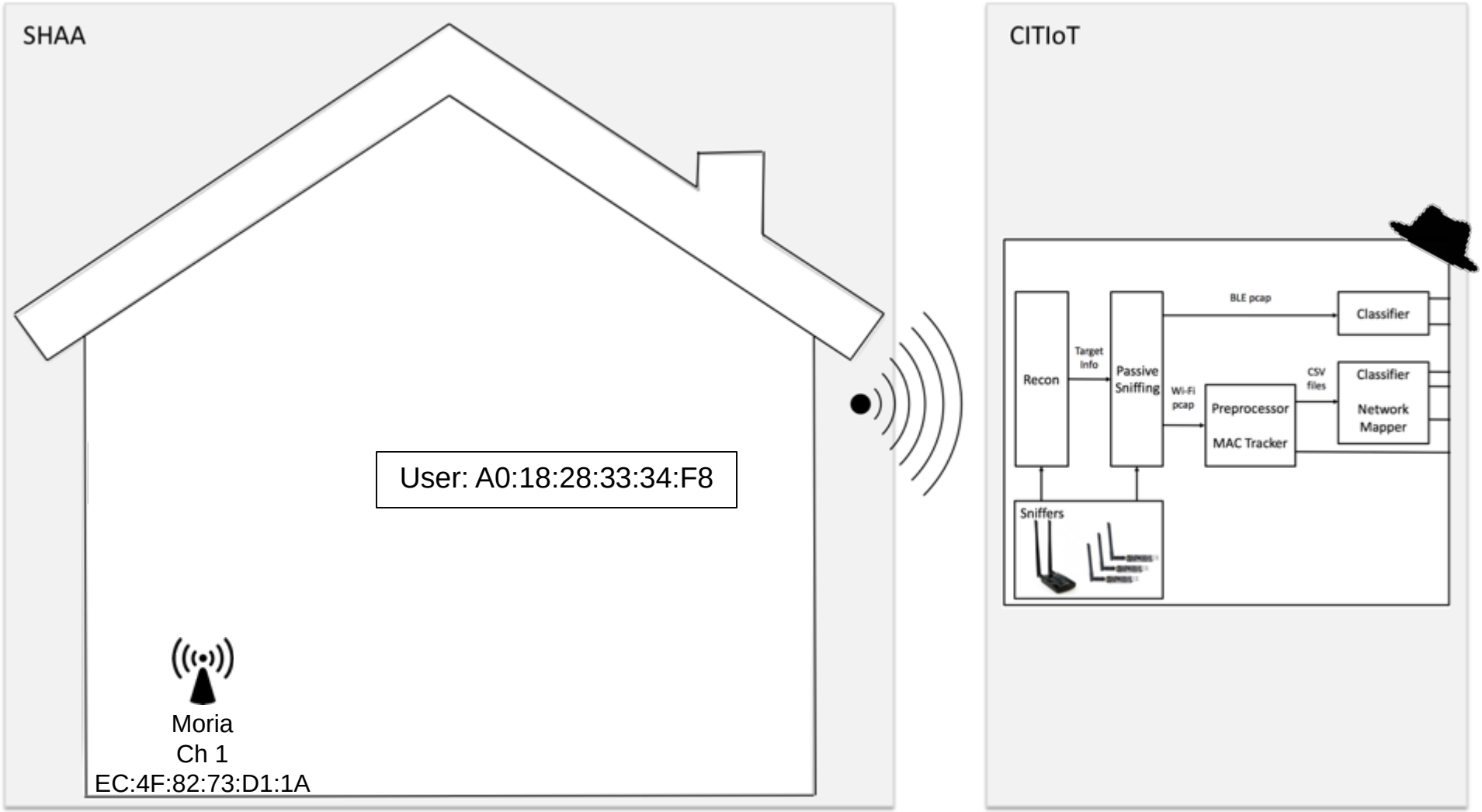
- Target acquisition
  - Target MAC address
  - Target's AP MAC address and channel
  - MAC address of other devices connected to target AP
  - BLE device names

Reconnaissance

1. Target MAC address
2/3. Target's AP MAC address and name
4. AP channel

```
root@gimli:gimli# airodump-ng wlan1

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 44:1C:A8:D5:E9:67  -63        2        0    0   6  54e  WPA2 CCMP   PSK  EIL
 EC:4F:82:73:15:AF  -46        2        0    0   1  54e  WPA2 CCMP   PSK  Buckeyes2.4
 EC:4F:82:73:D0:AE  -66        2        0    0   1  54e  WPA2 CCMP   PSK  EMF_411WS_106_2.4
 EC:4F:82:73:D1:1A  -35        2        0    0   1  54e  WPA2 CCMP   PSK  Moria
 EC:4F:82:73:15:B8  -65        2        0    0   1  54e  WPA2 CCMP   PSK  EMF_411WS_402_2.4
 B8:EE:0E:E9:82:7E  -60        3        0    0   1  54e. WPA2 CCMP   PSK  MySpectrumWiFi78-2G
 68:14:01:A8:E4:67  -49        3        0    0   1  54e  WPA2 CCMP   PSK  EWING-2.4
 B8:A1:75:23:60:43  -48        2        0    0   1  54e  WPA2 CCMP   PSK  <length: 22>
 EC:4F:82:73:17:0E  -67        2        0    0   1  54e  WPA2 CCMP   PSK  EMF_411WS_105_2.4
 EC:4F:82:73:D3:87  -52        3        0    0   1  54e  WPA2 CCMP   PSK  EMF_411WS_302_2.4

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 EC:4F:82:73:D1:1A  A0:18:28:33:34:F8  -12    0 -24      3         5
```

Attacker's Perspective



MAC address of other devices connected to target AP

```
root@gimli:gimli# airodump-ng wlan1 --bssid ec4f8273d11a

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 EC:4F:82:73:D1:1A  -23      242       47    0   1  54e  WPA2 CCMP   PSK  Moria

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 EC:4F:82:73:D1:1A  EC:1A:59:E4:FD:41  -23   54e-54e     0     64269
 EC:4F:82:73:D1:1A  EC:1A:59:F1:FB:21  -23   54e-46e     0     61572
 EC:4F:82:73:D1:1A  94:10:3E:2B:7A:55  -28   54e-54e     0     31353
 EC:4F:82:73:D1:1A  B4:75:0E:0D:33:D5  -36   46e-54e     0     32601
 EC:4F:82:73:D1:1A  60:38:E0:EE:7C:E5  -39   54e- 1e     0     48631
 EC:4F:82:73:D1:1A  B8:27:EB:09:1A:81  -38   54e-54e     0    301214
 EC:4F:82:73:D1:1A  14:91:82:C8:6A:09  -41   54e-46e     0     28617
 EC:4F:82:73:D1:1A  A0:18:28:33:34:F8  -45   54e-24    476    205282
 EC:4F:82:73:D1:1A  14:91:82:24:DD:35  -48   54e-54e     0     42845
 EC:4F:82:73:D1:1A  08:66:98:ED:1E:19  -49   54e-54e   238     32549
 EC:4F:82:73:D1:1A  B4:75:0E:0D:94:65  -55   36e- 1e     0     31496
```

Scanning

OUI Search	Results
EC:1A:59:E4:FD:41	Belkin International Inc.
EC:1A:59:F1:FB:21	Belkin International Inc.
94:10:3E:2B:7A:55	Belkin International Inc.
B4:75:0E:0D:33:D5	Belkin International Inc.
60:38:E0:EE:7C:E5	Belkin International Inc.
B8:27:EB:09:1A:81	Raspberry Pi Foundation
14:91:82:C8:6A:09	Belkin International Inc.
A0:18:28:33:34:F8	Apple, Inc.
14:91:82:24:DD:35	Belkin International Inc.
08:66:98:ED:1E:19	Apple, Inc.
B4:75:0E:0D:94:65	Belkin International Inc.

Attacker's Perspective

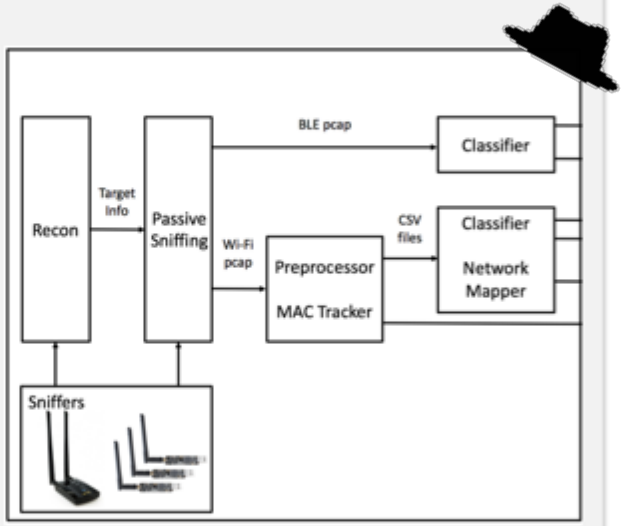
SHAA

User: Apple iPhone

Wi-Fi devices:
8x Belkin Devices
2x Apple Devices
1x Raspberry Pi

Moria

CITIoT



BLE device names

```
root@gimli:gimli# service bluetooth start
root@gimli:gimli# hciconfig hci0 up
root@gimli:gimli# hcitool lescan
LE Scan ...
EB:6E:E4:03:A0:67 Eve
EB:6E:E4:03:A0:67 Eve Energy 556E
FA:1B:EF:55:41:C8 Eve
FA:1B:EF:55:41:C8 Eve Motion 31A7
08:7C:BE:30:69:31 BLELock
08:7C:BE:30:69:31 BLELock
20:C3:8F:EC:29:DC Instant Pot Smart
F0:3A:A4:B1:3D:F0 Eve
F0:3A:A4:B1:3D:F0 Eve Weather 943D
AC:E6:4B:0A:74:81 PLAYBULB
FA:1B:EF:55:41:C8 Eve
FA:1B:EF:55:41:C8 Eve Motion 31A7
08:7C:BE:30:69:31 BLELock
08:7C:BE:30:69:31 BLELock
20:C3:8F:EC:29:DC Instant Pot Smart
F0:3A:A4:B1:3D:F0 Eve
F0:3A:A4:B1:3D:F0 Eve Weather 943D
AC:E6:4B:0A:74:81 PLAYBULB
FA:67:4F:5E:5C:CA Eve
FA:67:4F:5E:5C:CA Eve Door 91B3
DA:68:F2:6F:AC:72 Eve Room 4A04
```

Attacker's Perspective

SHAA

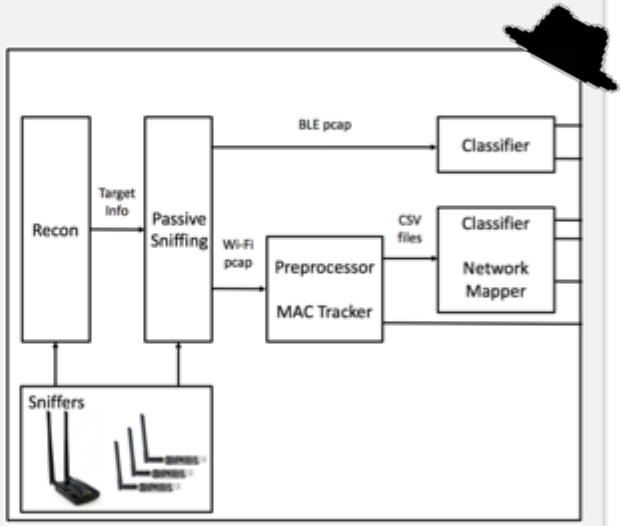
User: Apple iPhone

Wi-Fi devices:
8x Belkin Devices
2x Apple Devices
1x Raspberry Pi

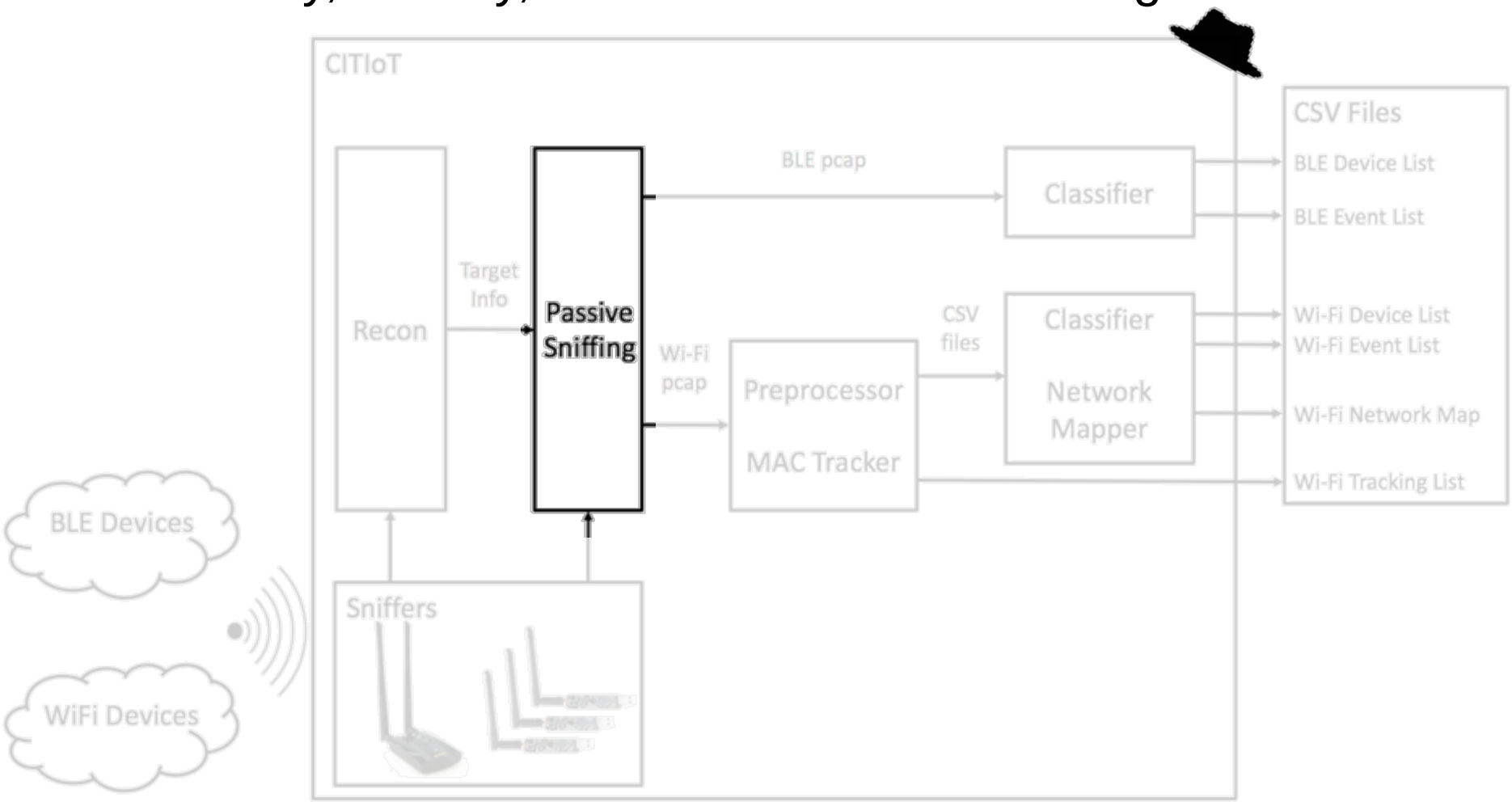
BLE devices:
5x Eve Devices
1x Playbulb
1x Instant Pot
1x BLE Lock

Moria

CITIoT

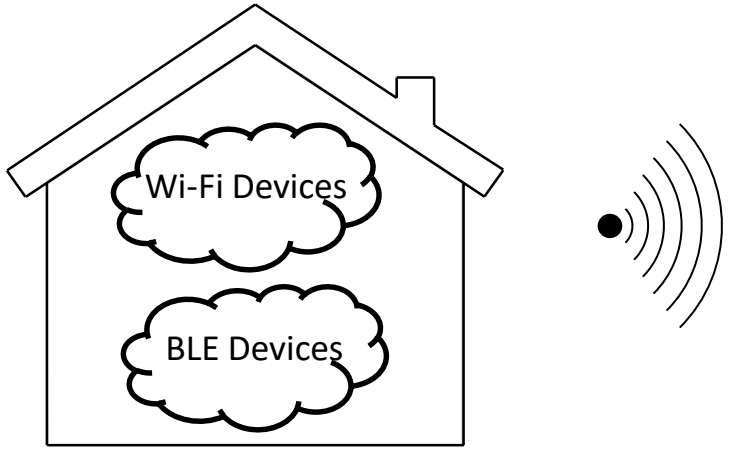


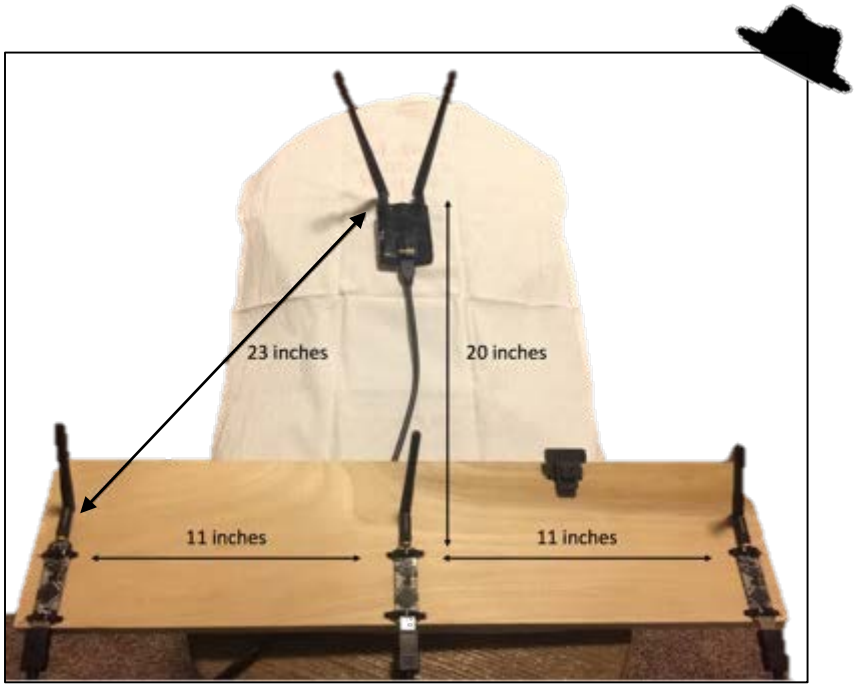
- Classify, Identify, and Track Internet of Things



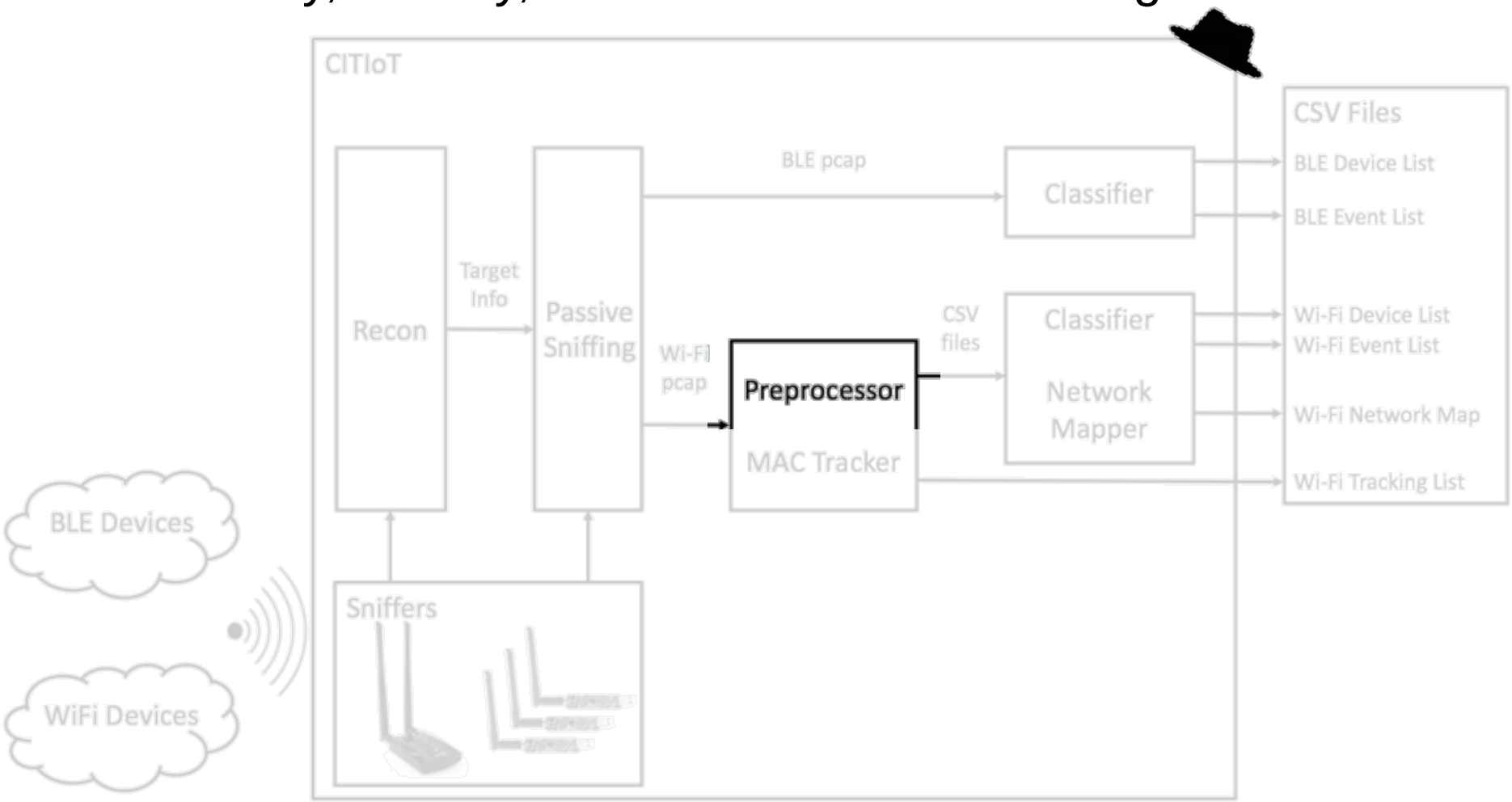
Passive Sniffing

```
# airodump-ng –c 1 wlan1 -o pcap –w wifi
--bssid ec4f8273d11a

# ubertooth-btle –f -U0 –A37 –qble.pcap
```





- Classify, Identify, and Track Internet of Things

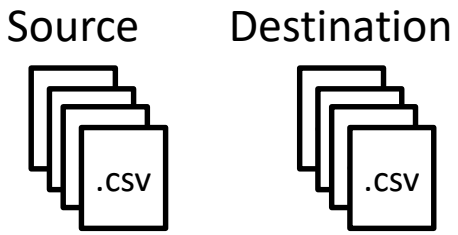


Wi-Fi Preprocessor

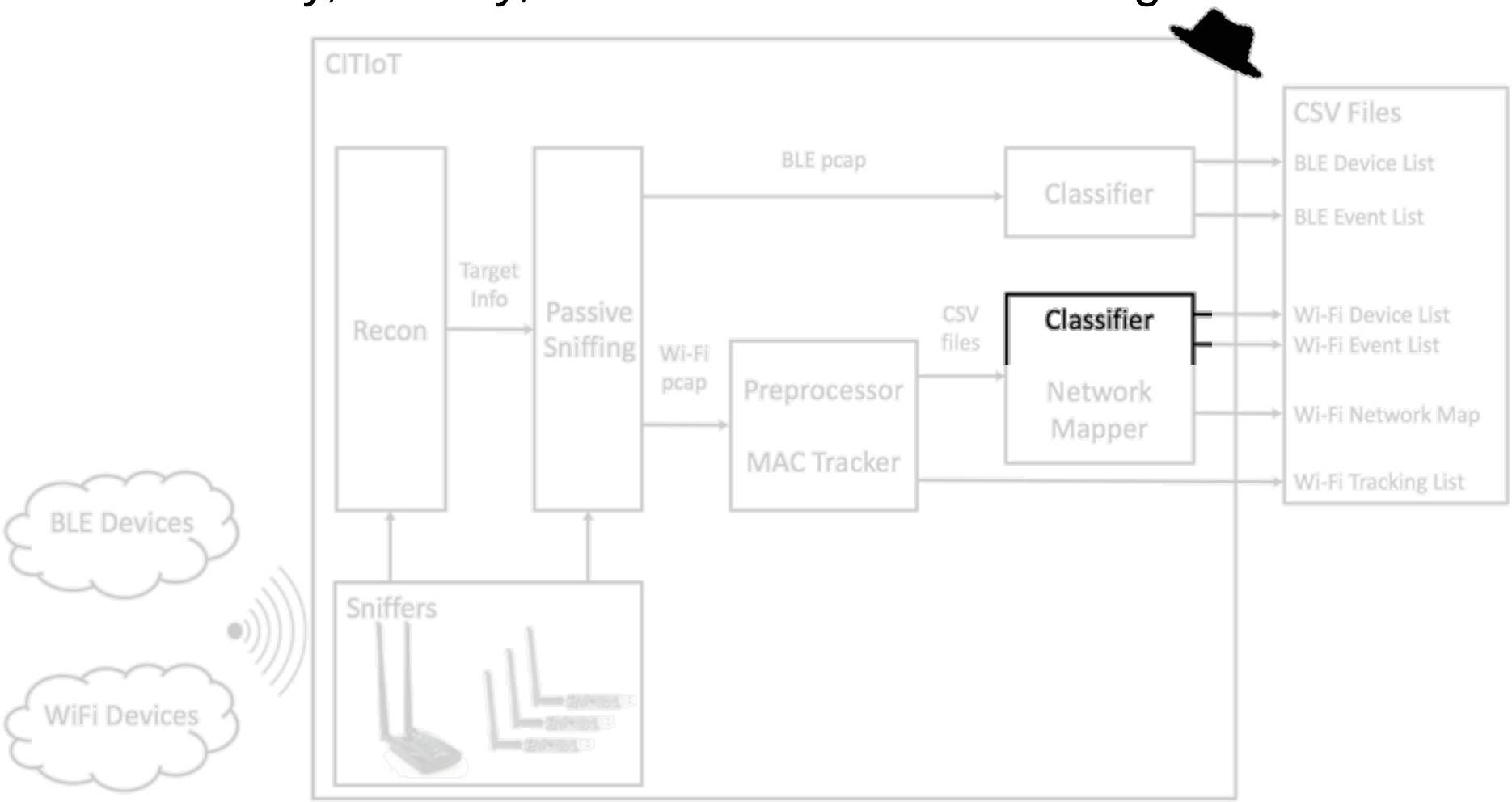
- Parse packets from capture and organize for classifier into CSVs
- Python script using Pyshark, a wrapper allowing packet parsing with Wireshark dissectors

```
$ python wifi.py –p wifi.pcap
```

Packet Time	Frame Size	Source	Destination



- Classify, Identify, and Track Internet of Things

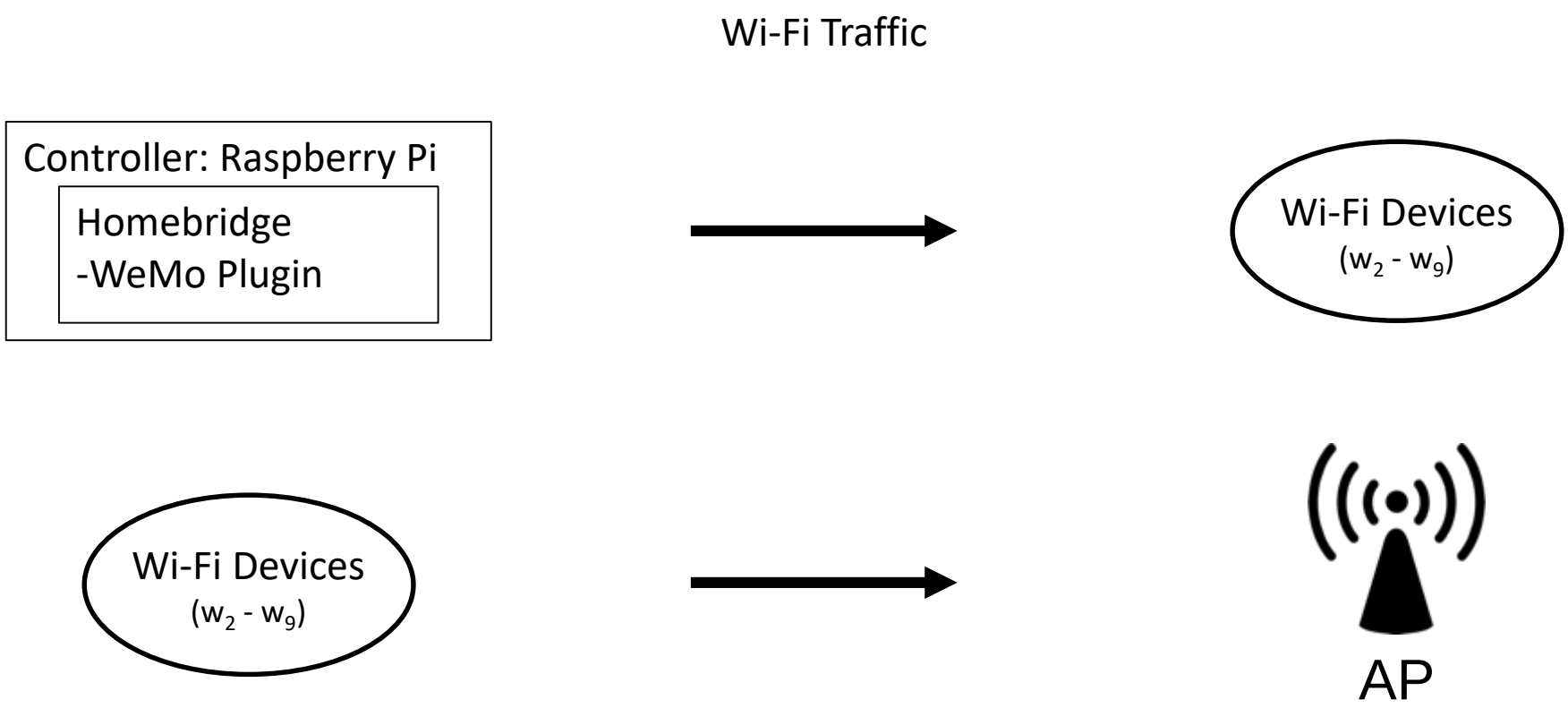


Wi-Fi Classifier Trainer

- Use characteristic packet traffic to train a classifier that can:
  - Classify devices
  - Identify events
- 10-hour classifier training trial

Time	Device	Device	Action
8/14/17 6:57	B4:75:0E:0D:33:D5	Switch 1	ON
8/14/17 6:58	B4:75:0E:0D:94:65	Switch 2	ON
8/14/17 7:16	B4:75:0E:0D:33:D5	Switch 1	OFF
8/14/17 7:17	B4:75:0E:0D:94:65	Switch 2	OFF

Wi-Fi Classifier Trainer



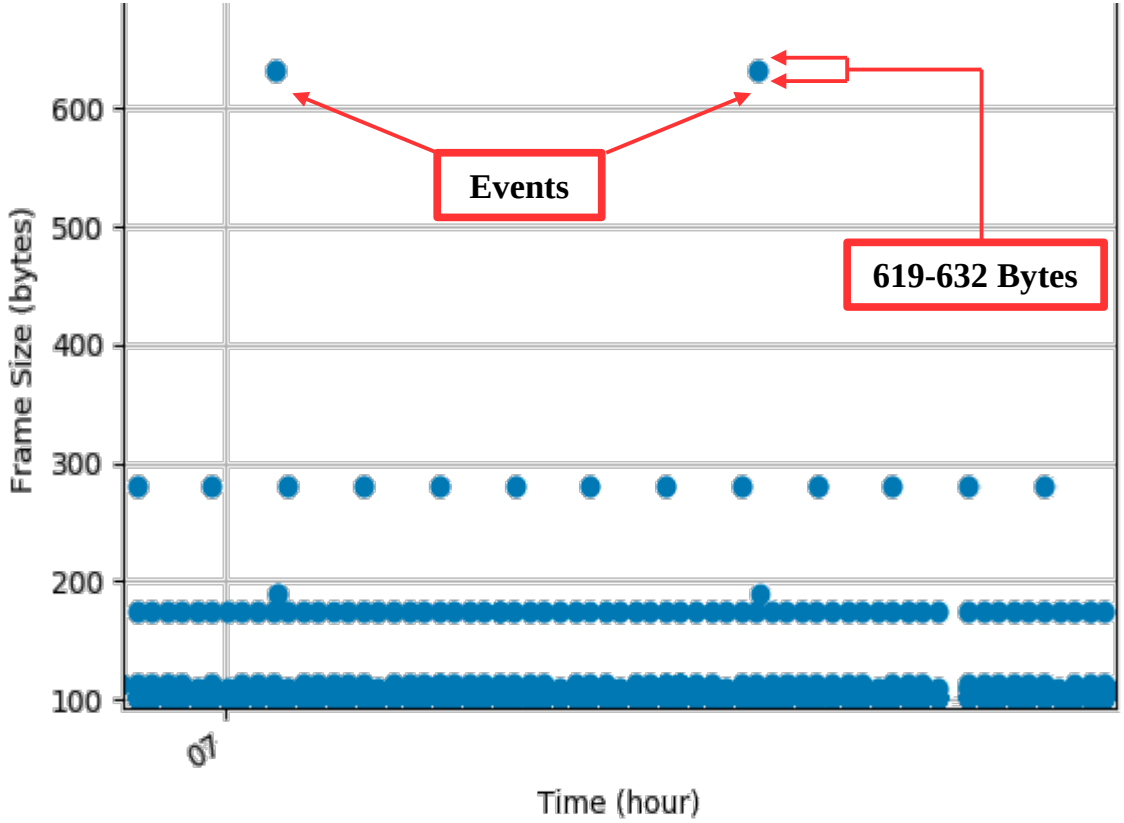
Wi-Fi Classifier Trainer

Controller: Raspberry Pi

Homebridge
-WeMo Plugin

Wi-Fi Traffic

Wi-Fi Devices
(w_2 - w_9)

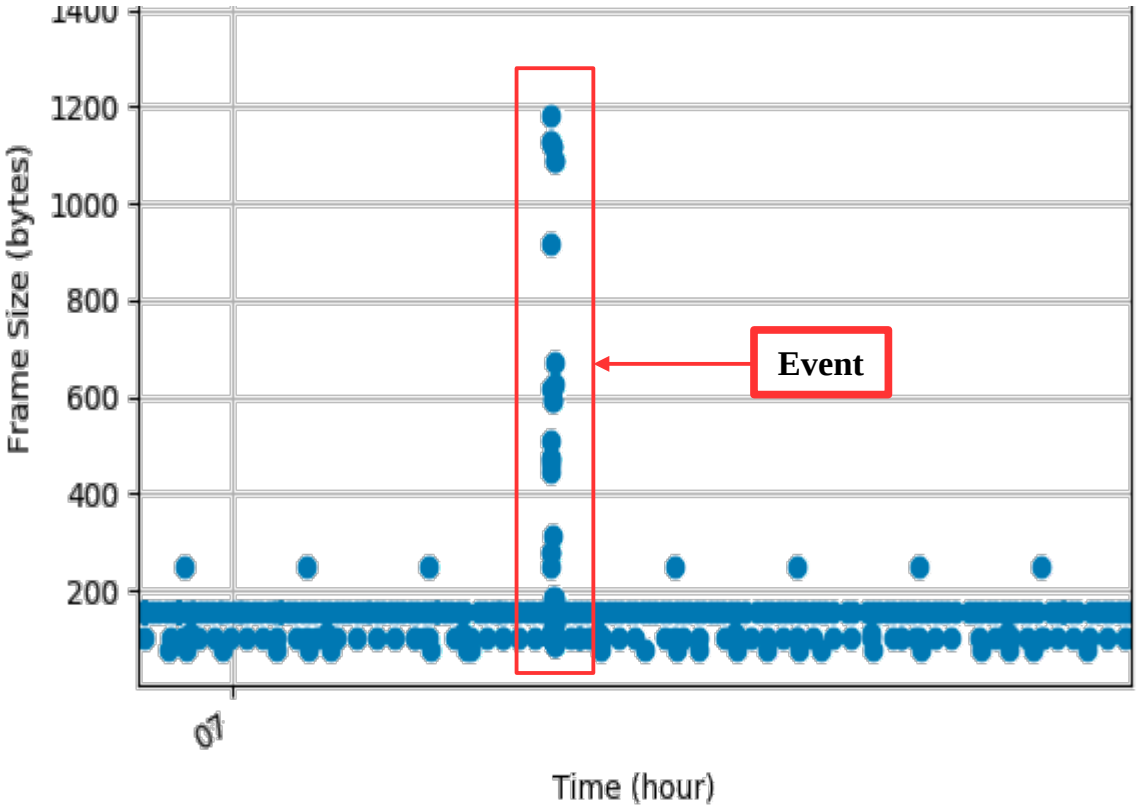


Wi-Fi Classifier Trainer

Wi-Fi Devices
(w_2 - w_9)

Wi-Fi Traffic

AP



Device Classification Criteria

Device Type	Device Classification Criteria
Outlet	$619\ bytes \leq FSize_{Incoming} \leq 632\ bytes$
Sensor	$if\ device\ != outlet \quad and \quad FSize_{Incoming} = 269\ bytes$
Camera	$if\ device\ != outlet \quad and \quad FSize_{Incoming} = 281\ bytes$

Event Identification Criteria

	Event Identification Criteria
Outlet Event	$if\ device = outlet \quad and \quad 619\ bytes \leq FSize_{Incoming} \leq 632\ bytes$
Sensor Event	$if\ device = sensor \quad and \quad \sum_{t}^{t+60s} FSize_{Outgoing} > 10{,}000\ bytes$
Camera Event	$if\ device = camera \quad and \quad \sum_{t}^{t+60s} FSize_{Outgoing} > 100{,}000\ bytes$

Wi-Fi Classifier

- Uses packet traffic and criteria to classify devices and identify events

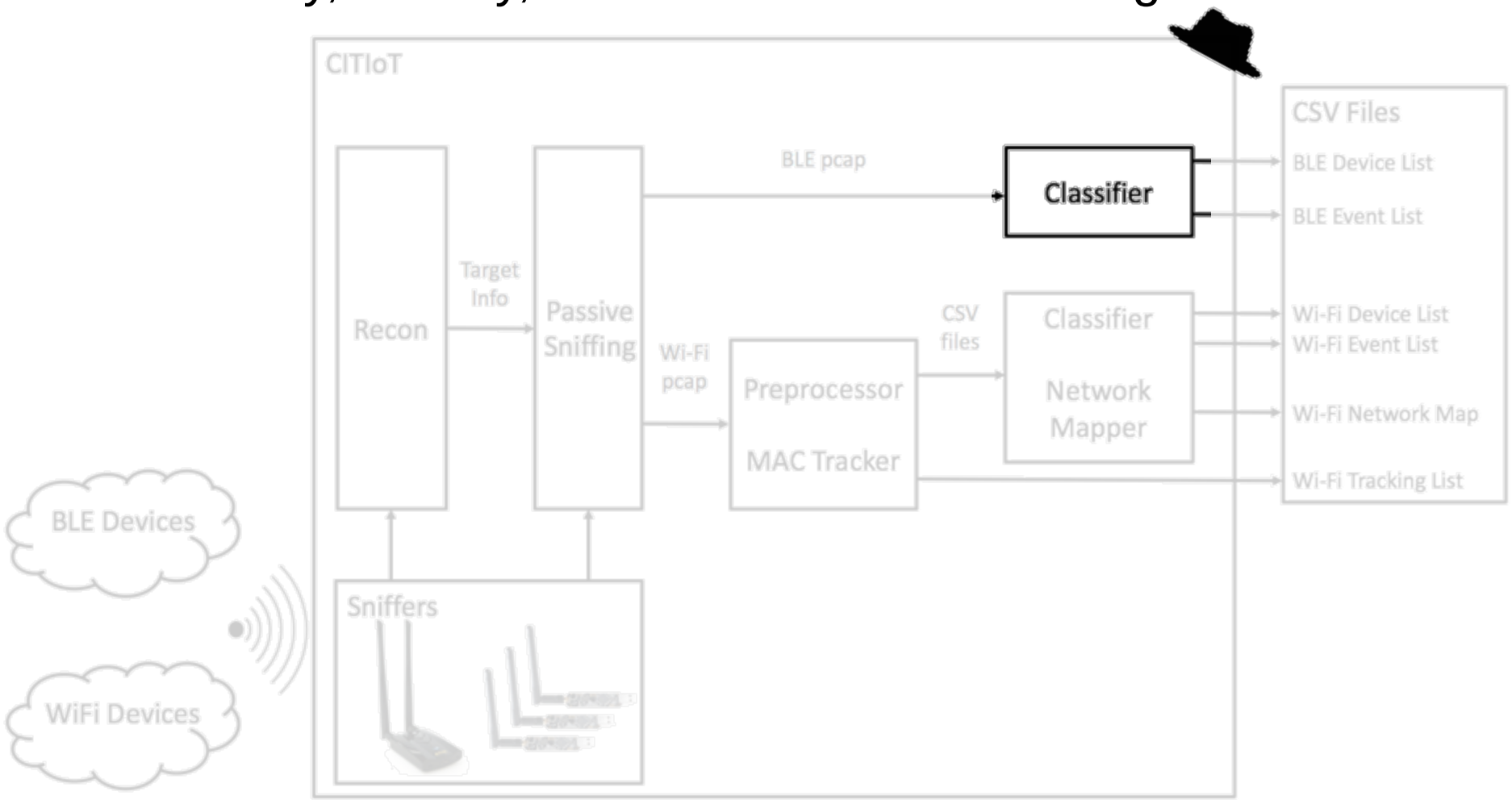
```
$ python wifi.py -c
```

Device	Classification
EC:1A:59:F1:FB:21 (Motion)	Sensor
14:91:82:24:DD:35 (Insight)	Outlet

Event Time	Device
8/16/17 7:05	B4:75:0E:0D:33:D5 (Switch1)
8/16/17 7:15	EC:1A:59:E4:FD:41 (NetCam)

CITIoT

- Classify, Identify, and Track Internet of Things



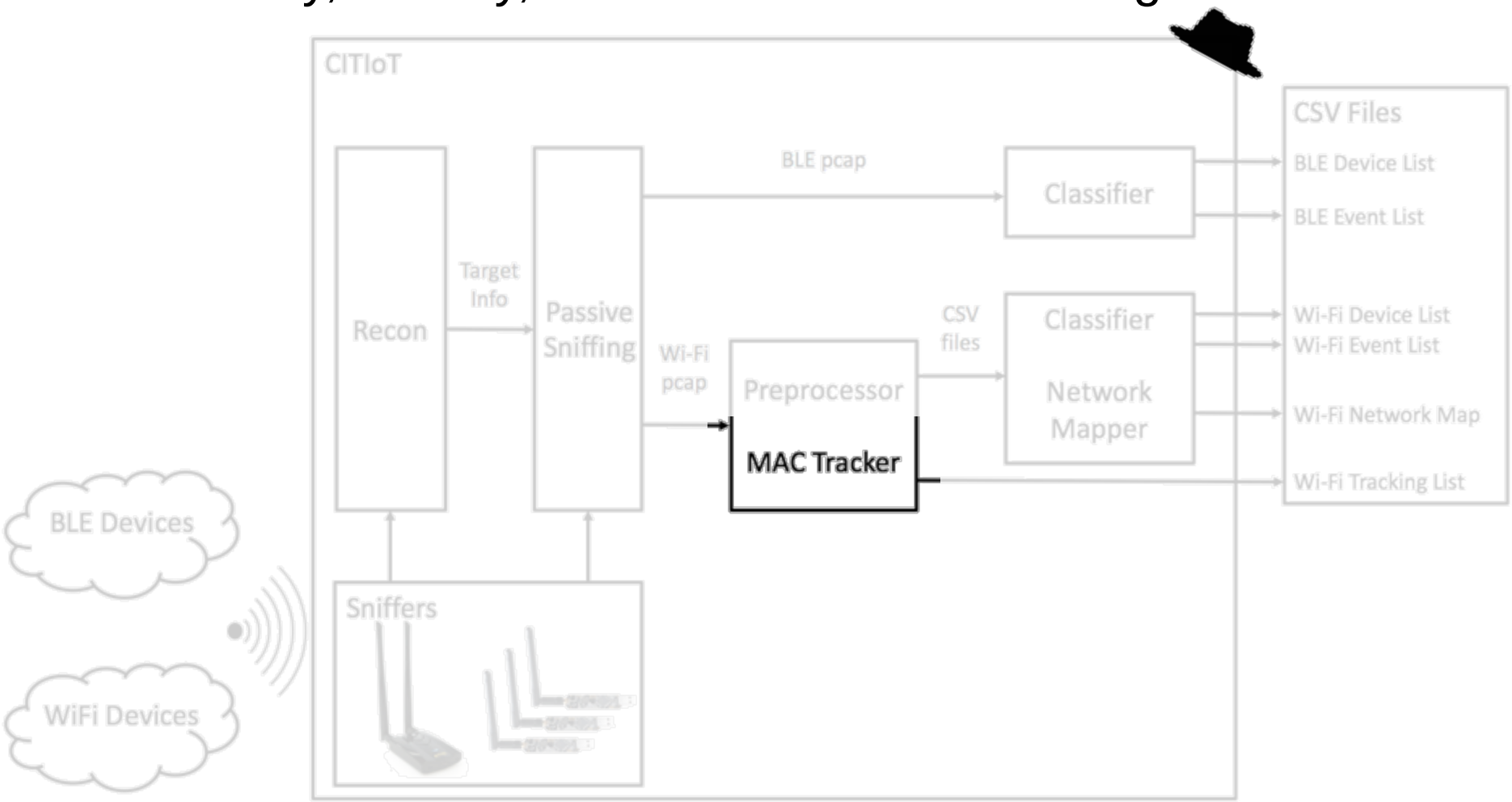
BLE Classifier

- ADV_IND and SCAN_RESP packets used to identify devices
- CONNECT_REQ packets used to identify events

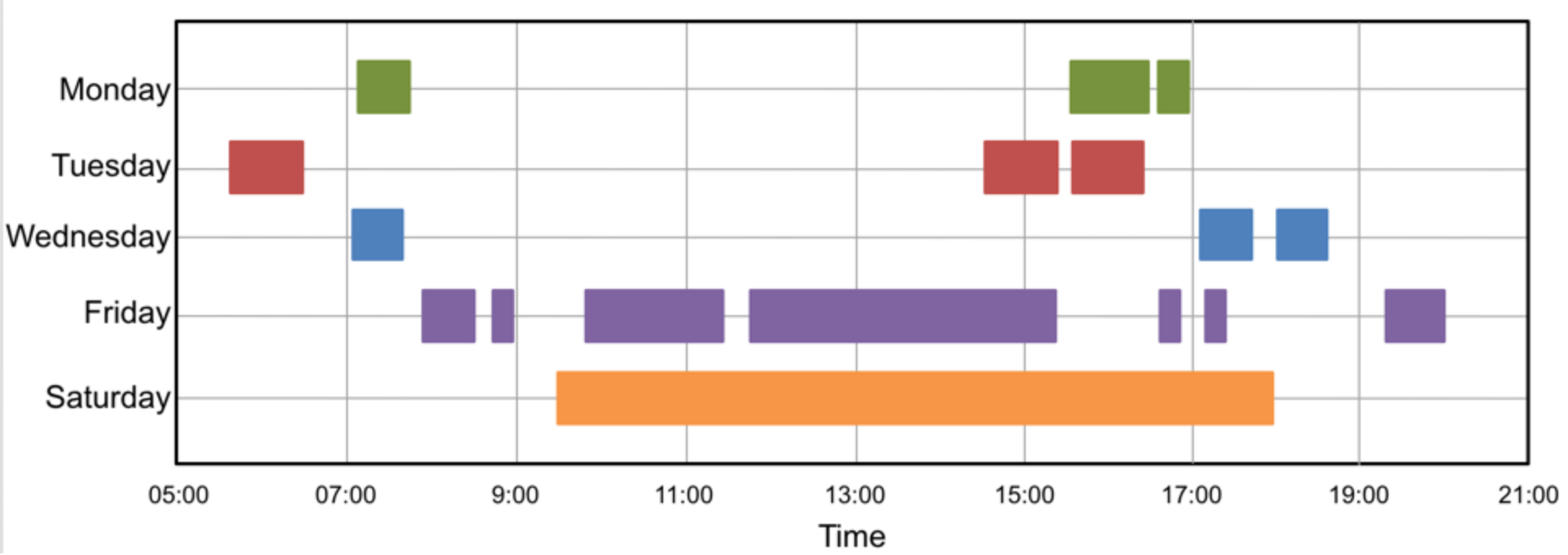
```
$ python ble.py –c ble.pcap
```

Event Time	Device
8/22/17 6:14	PLAYBULB
8/22/17 16:24	Gunbox

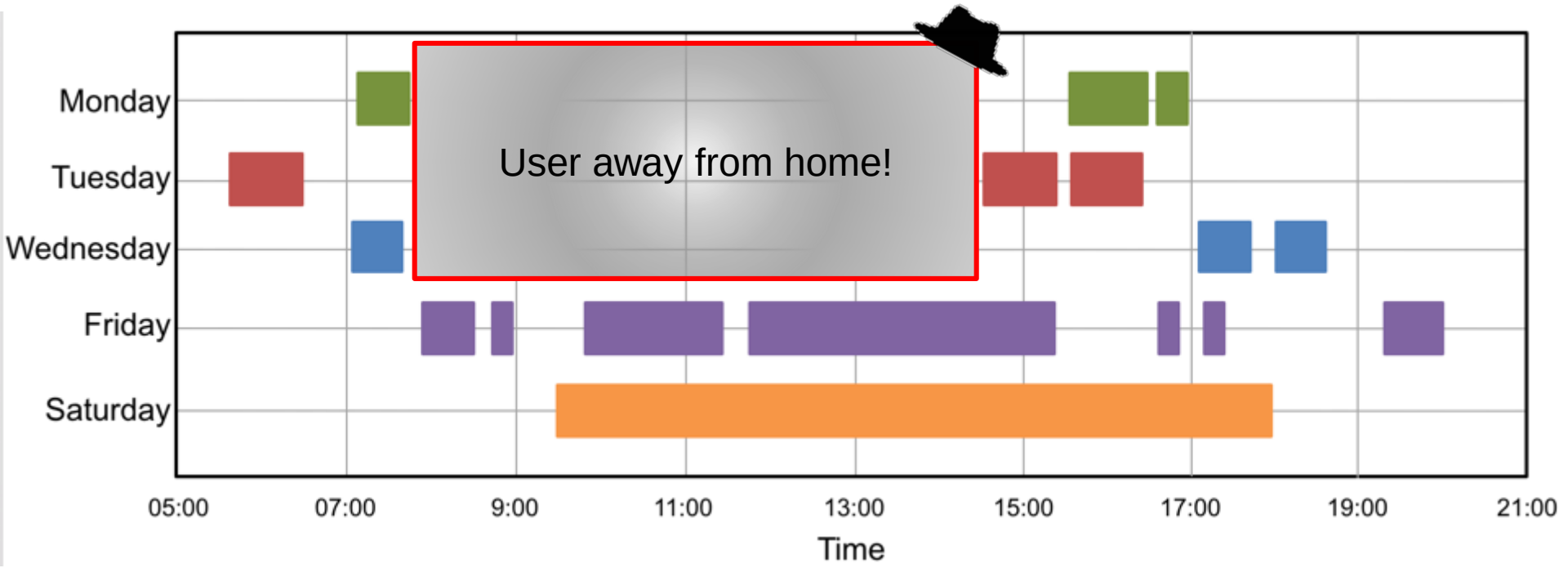
- Classify, Identify, and Track Internet of Things



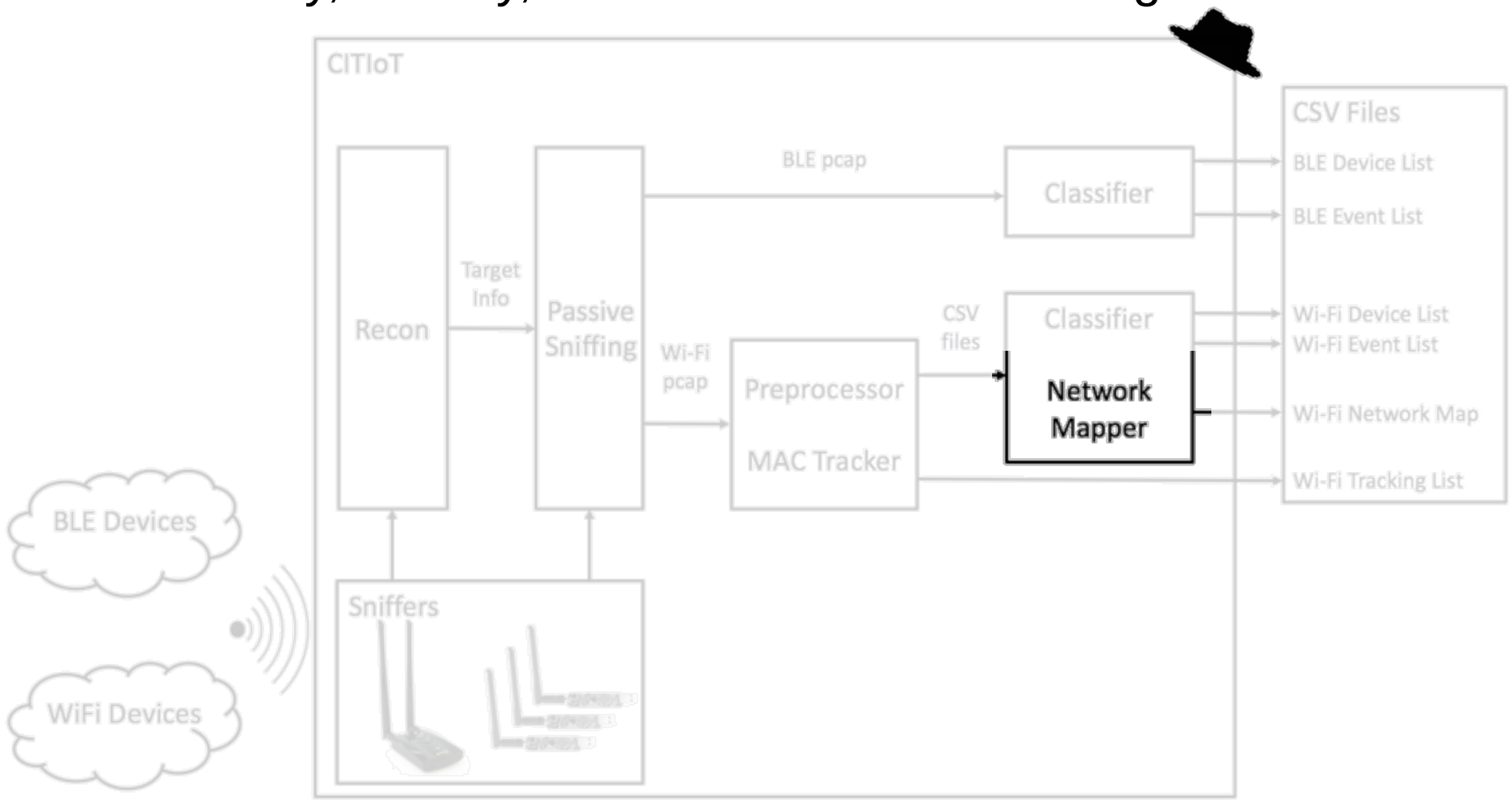
MAC Tracker


Monday
Tuesday
Wednesday
Friday
Saturday
05:00
07:00
9:00
11:00
13:00
15:00
17:00
19:00
21:00
Time

MAC Tracker


User away from home!
Monday
Tuesday
Wednesday
Friday
Saturday
05:00
07:00
9:00
11:00
13:00
15:00
17:00
19:00
21:00
Time

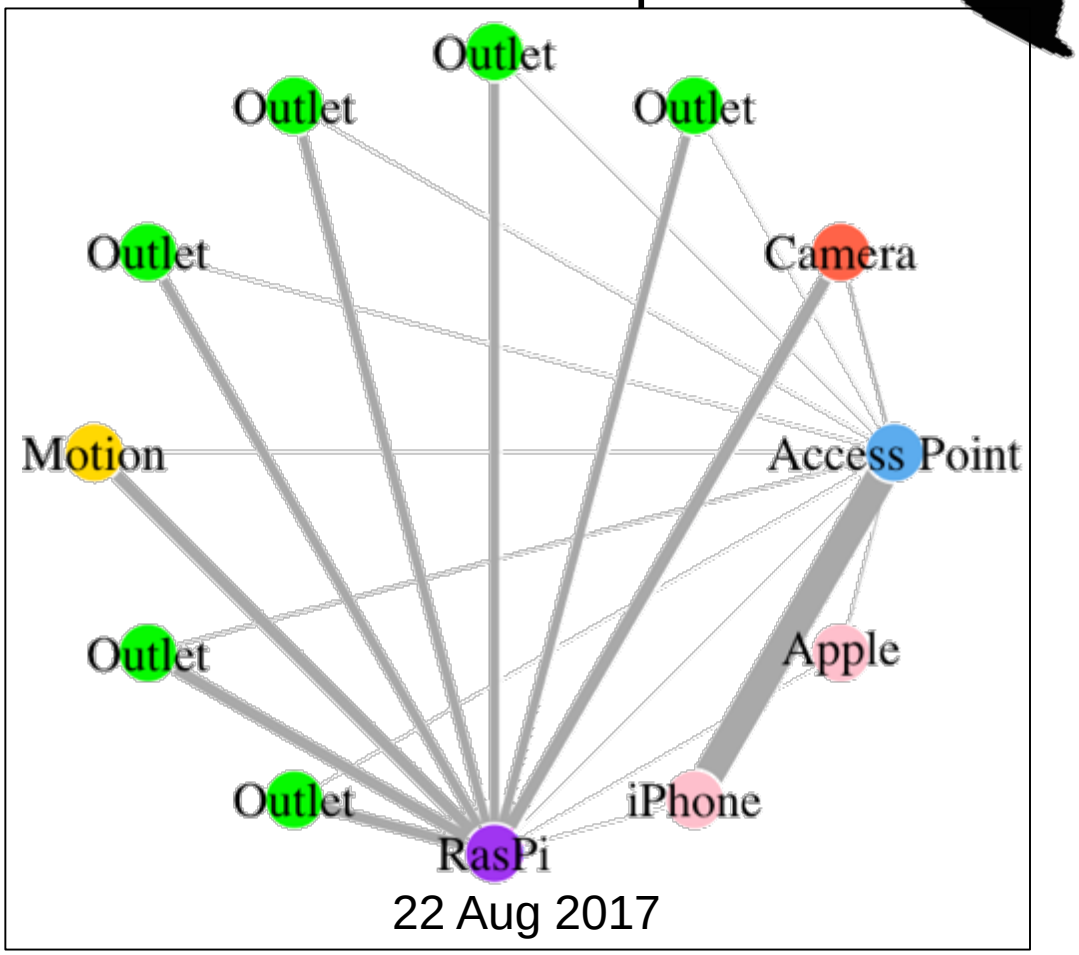
- Classify, Identify, and Track Internet of Things



Wi-Fi Network Mapper

- Uses traffic sent between devices to map network

Thicker lines indicate more data sent between devices



Attacker's Perspective

SHAA

Apple Device

User: Apple iPhone

<<BLE>>

Raspberry Pi

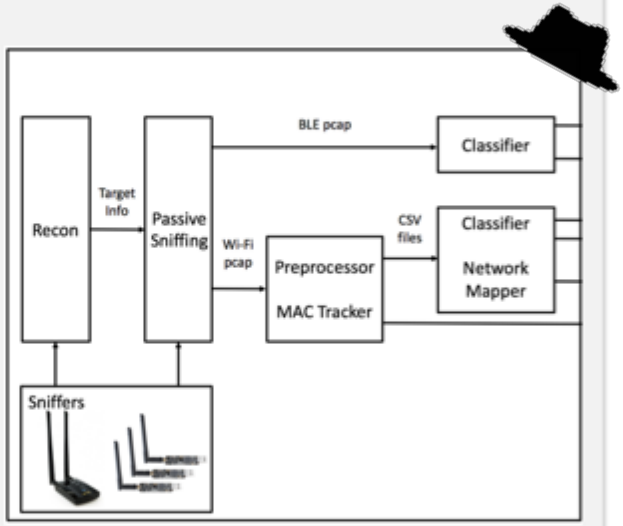
<<Wi-Fi>>

6x Outlets
1x Sensor
1x Camera

5x Eve Devices
1x Playbulb
1x Instant Pot
1x BLE Lock

Moria

CITIoT



Physical Access

- Using device list, captured traffic, and vulnerabilities able to determine:
  - When users are away from the home
  - What security devices are in a home
  - How to gain physical access to the home

- Replay attack on BLE Lock to unlock
  - Uses gatttool to send commands

BLE Lock

BLE Lock

Goals

1. **Develop a smart home architecture** to analyze IoT data leakage in the wild.

2. **Identify data leakage and vulnerabilities** in smart home devices.

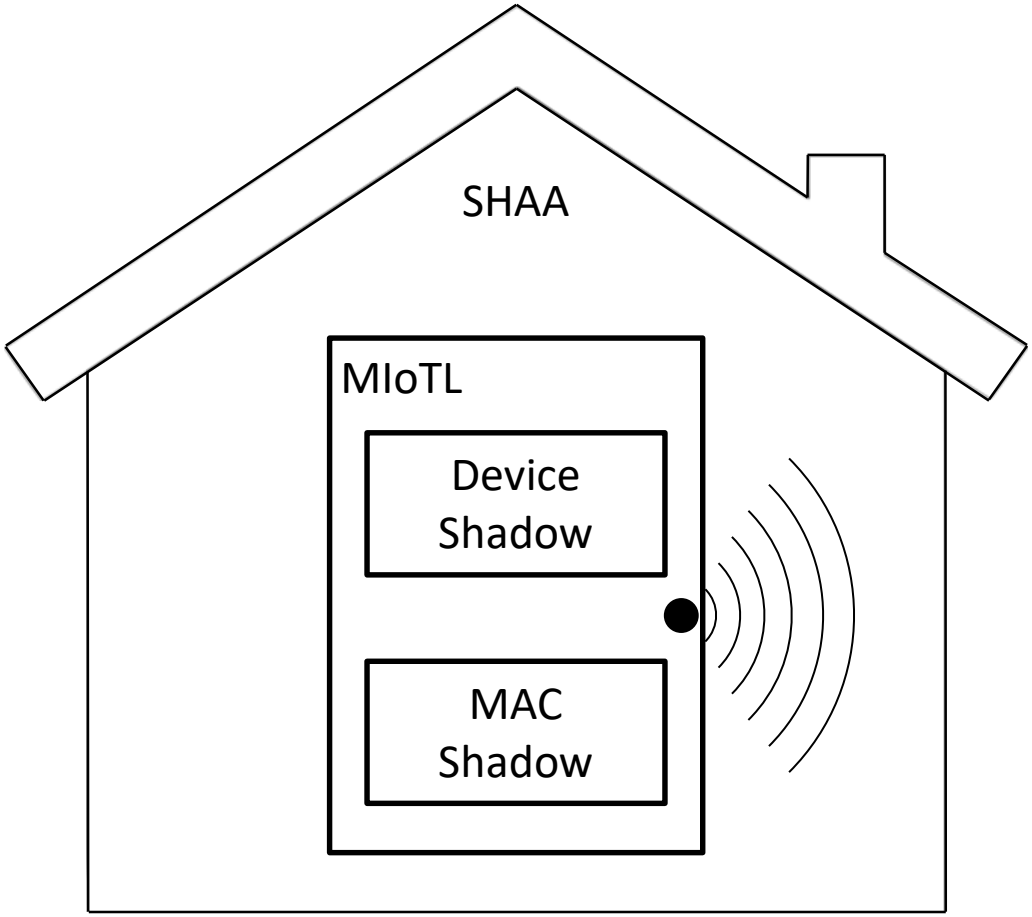
3. **Utilize data leakage and vulnerabilities** to classify devices, identify events, track users, and gain physical access to a smart home.

4. **Mitigate data leakage and vulnerabilities** to create a safer smart home.

Goals

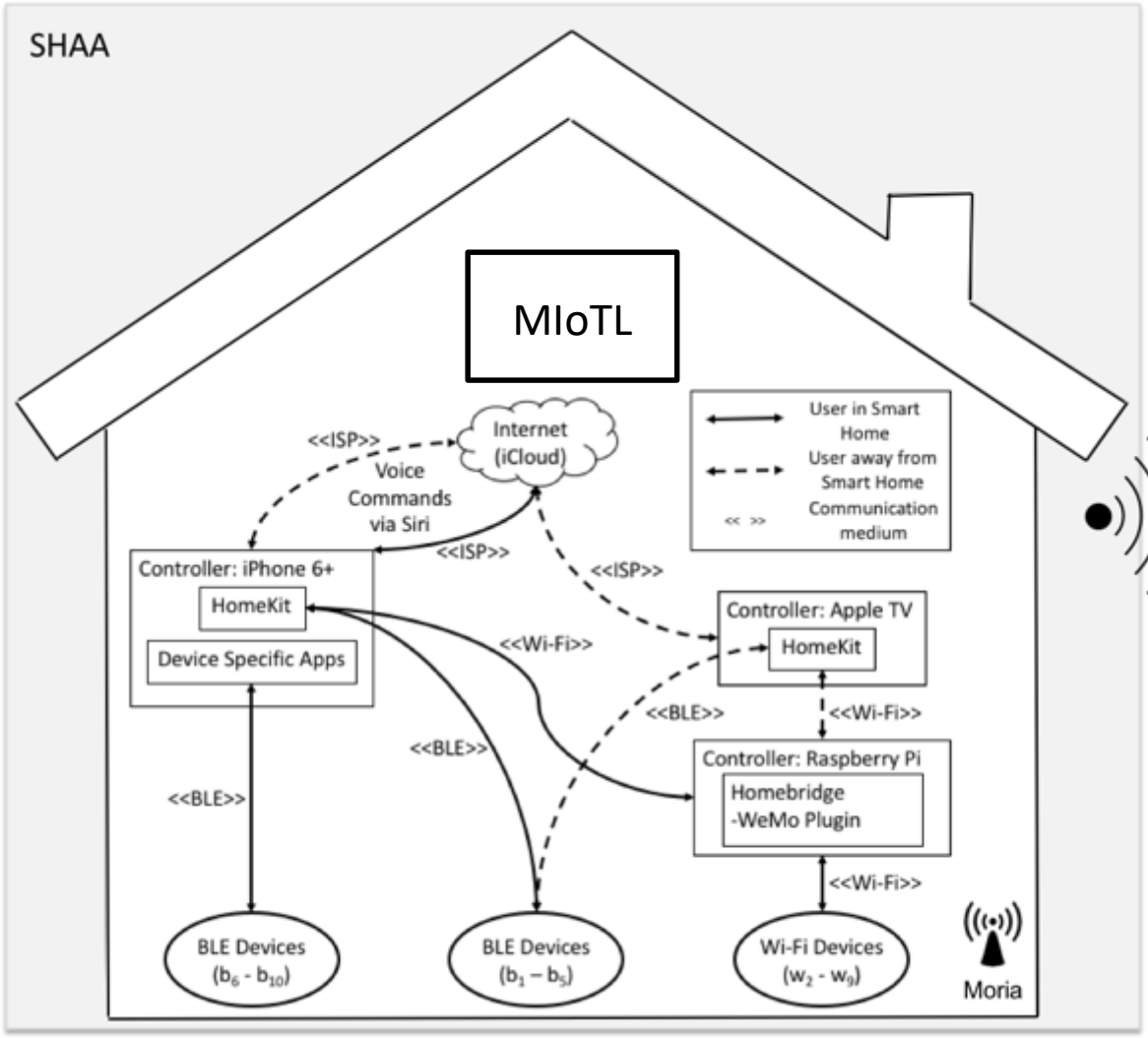
1. **Develop a smart home architecture** to analyze IoT data leakage in the wild.
2. **Identify data leakage and vulnerabilities** in smart home devices.
3. **Utilize data leakage and vulnerabilities** to classify devices, identify events, track users, and gain physical access to a smart home.
4. **Mitigate data leakage and vulnerabilities** to create a safer smart home.

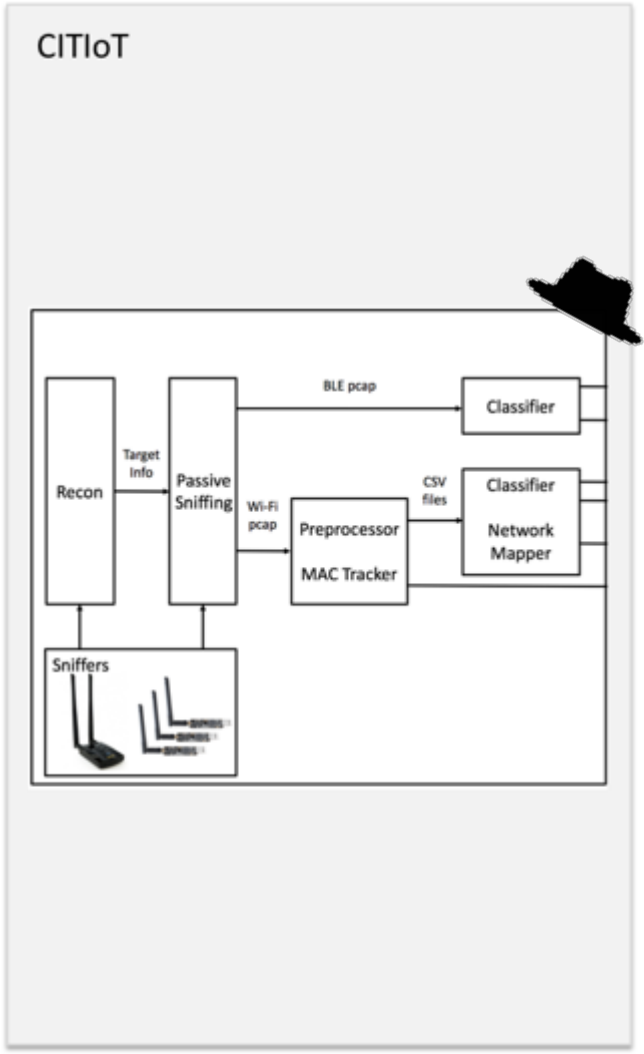
MIoTL



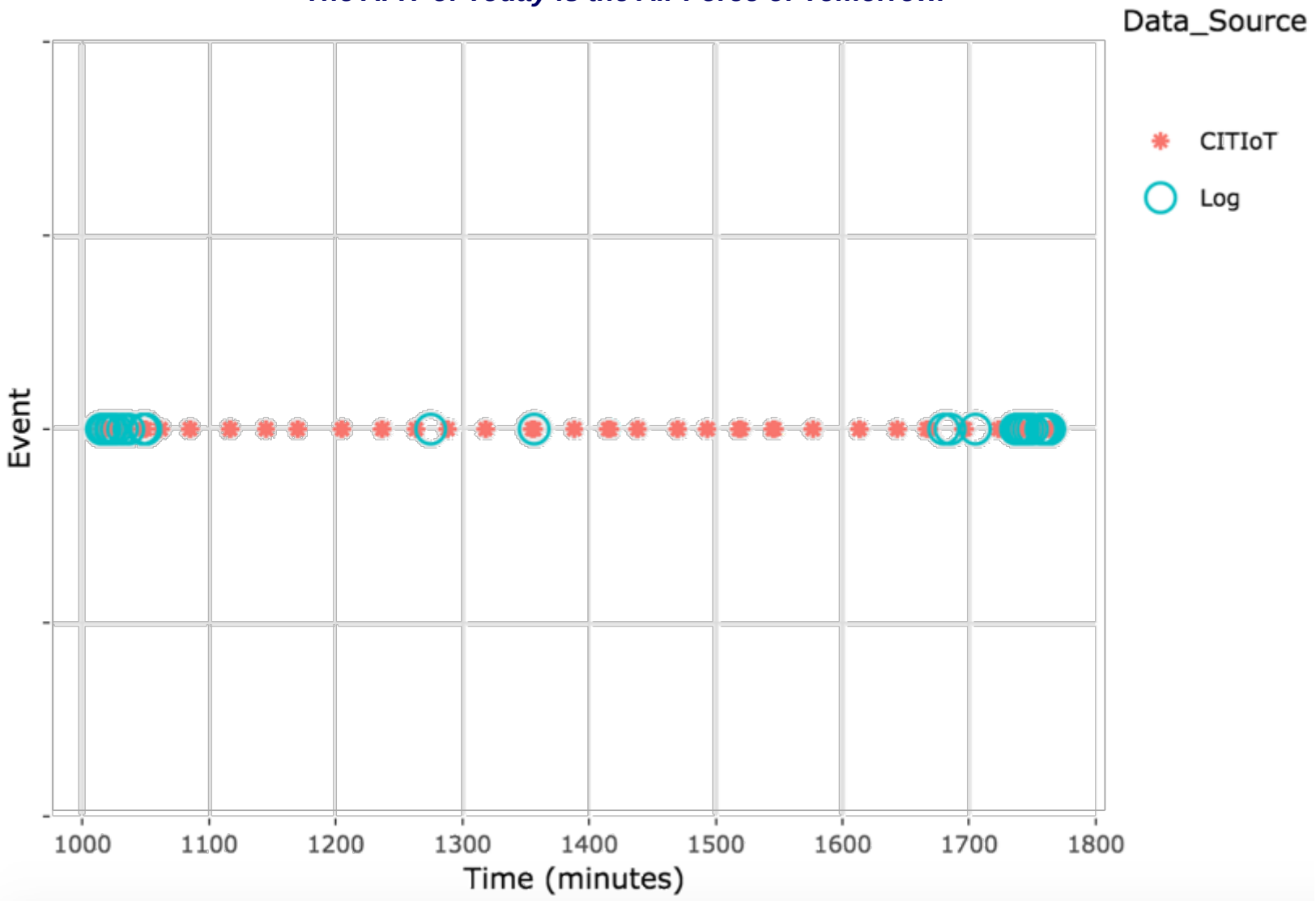
- Device Shadow
  - Spoof packets sent from Raspberry Pi to IoT devices and from IoT devices to the router
- MAC Shadow
  - Spoof packets sent from a user's device when user is away from the home
- Five trial days with mitigation active and user activating Wi-Fi devices within home

System Diagram



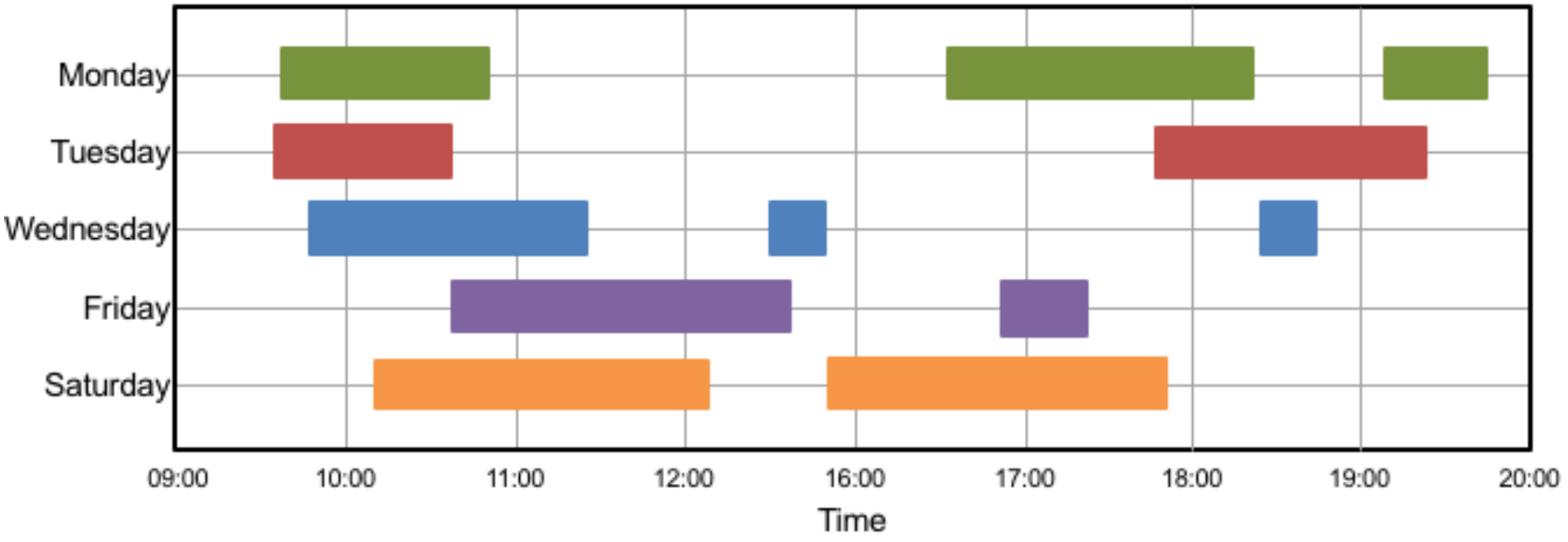


Event Identification with Mitigation

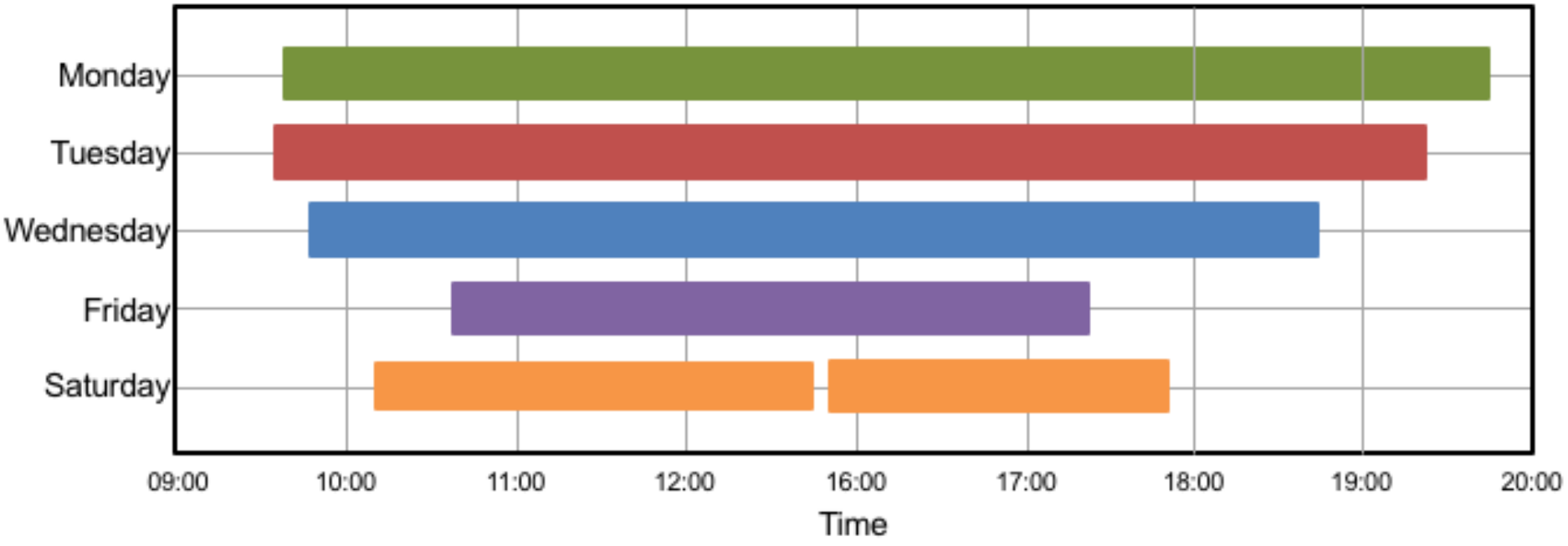


MAC Tracker

- Without Mitigation



- With Mitigation



Goals

1. **Develop a smart home architecture** to analyze IoT data leakage in the wild.
2. **Identify data leakage and vulnerabilities** in smart home devices.
3. **Utilize data leakage and vulnerabilities** to classify devices, identify events, track users, and gain physical access to a smart home.
4. **Mitigate data leakage and vulnerabilities** to create a safer smart home.

Results

- Compare CITIoT findings with logs to determine
  - Accuracy
    - Classify devices
    - Identify events
    - Track users
  - Performance
    - Processing time
    - Storage requirement
- With and without mitigation
- Statistical analysis done in R

Mean Results

CITIoT Metric	Without Mitigation	With Mitigation
Device Classification	94.4%	75.0%
Event Identification True Positive Rate	95.0%	79.8%
Event Identification False Positive Rate	3.2%	88.8%
Positive Predictive Value	96.1%	10.7%
User Tracking	96.1%	1.9%

- One tailed, two sample t-test for:
  - True positive rate ($p = 0.001426 < 0.05$)
  - False positive rate ($p = 4.675 \times 10^{-13}$)

Mean Results

CITIoT Metric	Without Mitigation	With Mitigation
Device Classification	94.4%	75.0%
Event Identification True Positive Rate	95.0%	79.8%
Event Identification False Positive Rate	3.2%	88.8%
Positive Predictive Value	96.1%	10.7%
User Tracking	96.1%	1.9%

- One tailed, two sample t-test for:
  - True positive rate ($p = 0.001426 < 0.05$)
  - False positive rate ($p = 4.675 \times 10^{-13}$)

Goals

1. **Develop a smart home architecture** to analyze IoT data leakage in the wild.

2. **Identify data leakage and vulnerabilities** in smart home devices.

3. **Utilize data leakage and vulnerabilities** to classify devices, identify events, track users, and gain physical access to a smart home.

4. **Mitigate data leakage and vulnerabilities** to create a safer smart home.

Conclusion

1. What kind of privacy data do smart home devices leak?

2. How can an attacker exploit data leakage to threaten operational and physical security?

3. Are there ways to defend against these vulnerabilities?

Conclusion

- IoT device leakage can be used to create a tool that can:
  - Classify devices
  - Identify events
  - Track users
  - Map networks
  - Gain physical access

- A mitigation tool can be created to:
  - Conceal devices and events within the smart home
  - Make it appear that users are always home

Conclusion

1. **Develop a smart home architecture** to analyze IoT data leakage in the wild.
2. **Identify data leakage and vulnerabilities** in smart home devices.
3. **Utilize data leakage and vulnerabilities** to classify devices, identify events, track users, and gain physical access to a smart home.
4. **Mitigate data leakage and vulnerabilities** to create a safer smart home.

Significance of Research

- Contributions:
  - SHAA
  - Vulnerability Analysis
  - CITIoT
  - MIoTL
  - Synthesis

Future Work

- More devices!
- Track user's actual location using signal strength
- Machine learning to train classifier
- Mitigation for BLE traffic

Questions

References

1. United States Government Accountability Office, “Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD,” 2017, accessed Feb 11, 2018. [Online]. Available: www.gao.gov/assets/690/686203.pdf.
2. Consumer Technology Association, “2018 tech industry revenue to reach record $351 billion, says CTA,” 2018, accessed Jan 7, 2018. [Online]. Available: www.cta.tech/News/Press-Releases/2018/January/2018-Tech-Industry-Revenue-to-Reach-Record-$351-Bi.aspx.
3. E. Skoudis, “Internet of things, Voice Control, AI, and Office Automation,” 2016, presented at DerbyCon, accessed Dec 8, 2017. [Online]. Available: www.irongeek.com/i.php?page=videos/derbycon6/.
4. A. Rose and B. Ramsey, “Picking Bluetooth Low Energy locks from a quarter mile away,” 2016, presented at DEF CON 24, accessed Aug 30, 2017. [Online]. Available: www.media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/.
5. S. Jourdois, “BtleJuice: Bluetooth smart (LE) man-in-the-middle framework,” 2016, accessed Aug 30, 2017. [Online]. Available: www.github.com/DigitalSecurity/btlejuice.
6. J. Slawomir, “A Node.js package for BLE using man-in-the-middle and other attacks,” 2016, accessed Aug 30, 2017. [Online]. Available: www.github.com/securing/gattacker.
7. G. del Arroyo, J. Bindewald, and B. Ramsey, “Securing Bluetooth Low Energy enabled industrial monitors,” in Proceedings of the 12th International Conference on Cyber Warfare and Security. Academic Conferences and publishing limited, 2017, pp. 167–176.
8. A. K. Das, P. H. Pathak, C.-N. Chuah, and P. Mohapatra, “Uncovering privacy leakage in BLE network traffic of wearable fitness trackers,” in Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications. ACM, 2016, pp. 99–104.

References

9. M. Zhou, Z. Tian, K. Xu, X. Yu, X. Hong, and H. Wu, “SCaNME: Location tracking system in large-scale campus Wi-Fi environment using unlabeled mobility map,” Expert Systems with Applications, vol. 41, no. 7, pp. 3429–3443,2014.
10. C. Madrigal, “Tracking/Monitoring WiFi devices without being connected to any network,” 2017, presented at Cyphercon 2.0. Accessed Dec 8, 2017.[Online]. Available: www.irongeek.com/i.php?page=videos/cyphercon2/.
11. M. Gruteser and D. Grunwald, “Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis,” Mobile Networks and Applications, vol. 10, no. 3, pp. 315–325, 2005.
12. R. Rivest, “Chaffing and winnowing: Confidentiality without encryption,” Crypto Bytes (RSA laboratories), vol. 4, no. 1, pp. 12–17, 1998.
13. K. Fawaz, K.-H. Kim, and K. G. Shin, “Protecting privacy of BLE device users,” in25th USENIX Security Symposium, 2016, pp. 1205–1221.
14. J. G. del Arroyo, J. Bindewald, S. Graham, and M. Rice, “Enabling Bluetooth Low Energy auditing through synchronized tracking of multiple connections,” International Journal of Critical Infrastructure Protection, 2017.
15. Wireless LAN Medium Access Control, MAC, and Physical Layer, PHY, Specification, IEEE Standard 802.11, 2016, accessed Aug 27, 2017. [Online]. Available: ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68.