ASEE'S VIRTUAL CONFERENCE
At Home with Engineering Education
JUNE 22 - 26, 2020 #ASEEVC
Paper ID #29634

Internet of Things Forensics in Smart Homes: Design, Implementation and Analysis of Smart Home Laboratory

Shinelle Hutchinson, Purdue University at West Lafayette

I am a Ph.D. student at Purdue University studying Digital and Cyber Forensics. I obtained my Masters of Science in Digital Forensics from Sam Houston State University and my Bachelor's of Science in Computer Science from the University of the West Indies. I have research interests in Internet of Things (IoT) Forensics, Mobile Forensics, and IoT and Mobile Security and Privacy.

Yung Han Yoon, Purdue University
Ms. Neesha Shantaram
Dr. Umit Karabiyik, Purdue University

Dr. Umit Karabiyik is an Assistant Professor in the Department of Computer and Information Technology at Purdue University. Prior to his appointment at Purdue, Dr. Karabiyik was an Assistant Professor in the Department of Computer Science at Sam Houston State University from 2015 to 2018. Dr. K received his M.S. and Ph.D. degrees from Florida State University in 2010 and 2015 respectively. His research interests broadly lie in Digital and Cyber Forensics, User and Data Privacy, Artificial Intelligence, Computer and Network Security. He is a recipient of federal grants from National Institute of Justice. He is an Associate Editor-in-Chief for Journal of Digital Forensics, Security and Law, and technical program committee (TPC) member of high quality international conferences in Digital Forensics and Security.

Internet of Things Forensics in Smart Homes: Design, Implementation and Analysis of Smart Home Laboratory

Shinelle Hutchinson, Yung Han Yoon, Neesha Shantaram, and Umit Karabiyik

{hutchi50,yoon127,nshantar,umit}@purdue.edu
Department of Computer and Information Technology
Purdue University

Abstract

The Internet of Things (IoT) has skyrocketed to the forefront of everyone's lives, whether they know it or not. IoT devices have been incorporated into all facets of life, from the medical industry to transportation and it has even made its way into our homes. These devices have access to vast amounts of data, especially personal data. However, due to the compact nature of these devices, insufficient effort has been made to incorporate security into their design. With that in mind, IoT devices are treasure-troves of potential evidentiary data for forensic investigators, especially when these devices are used to aid in criminal activities. Concerning IoT devices, there is a need to investigate these devices to find answers to questions such as, what data can be recovered from these devices along with their respective smartphone applications? What methods would be best suited for collecting and analyzing this data? What data do these devices share with each other? Are there any privacy concerns when using these devices? Are there any security vulnerabilities when using these devices? Finding answers to these questions will considerably reduce the amount of time investigators spend collecting evidence during a case. New IoT devices are always becoming available and the research into each cannot keep up. As such, there is a gap in the literature regarding both the privacy and security of these devices and the most efficient methods to investigate them. Therefore, in this study, we aim to address this need by first building our own IoT forensics laboratory at Purdue University. Several students (undergraduate and graduate) work under the supervision of their faculty advisor to populate this lab with relevant IoT devices to simulate that of a smart home. This setup would allow us to simulate possible real-world smart home events (i.e. IoT device compromise, IoT device as a witness) which we can then investigate to both find answers to aforementioned questions and develop efficient methods to investigate these IoT devices. In this paper we will discuss several ways in which IoT devices in a smart home can be compromised and also investigate these devices after the compromise to determine what data can be recovered, how to recover the data and where this data resides.

1 Introduction

Internet connected devices are constantly being introduced to the public as convenient and secure ways to improve human lives, especially in a home setting. A smart home is a collection of Internet connected devices that are used for automation, security and even entertainment, within a house. In this paper, we will use the term Internet of Things (IoT) to refer to these devices. The global smart home market is forecasted to exceed 53 billion US dollars by 2022 [1] while smart home devices, like sensors, plugs, switches, smart speakers and smart home security cameras were among the most popular smart devices sold worldwide in 2017 and 2018 [2].

Although IoT devices continue to be adopted in the home at an alarming rate, there continues to be reports of cyber attacks and privacy issues with them [3, 4]. In a recent study conducted by Avast, two out of every five smart homes worldwide have at least one IoT device that is susceptible to cyber attacks [5]. Such prevalence necessitates conducting more research into developing better methods of increasing IoT device security and privacy for smart home owners. Security and privacy are two requirements smart home owners are becoming more concerned with experiencing from their IoT devices as 75% of persons do not trust how their IoT devices handle and share their data [6].

In this paper, we describe our smart home (IoT) lab setup, provide an overview of conducting a forensic investigation of smart home devices and discuss how the lab can be used to investigate possible threat scenarios that effect common smart homes today. The IoT lab will be used by the UMIT2 (Ubiquitous and Mobile Investigative Techniques and Technologies) Research group as well as the Digital Forensics and Cyber Security departments at Purdue University to allow students and faculty access to some of the popular and newly released IoT devices for use in classes and novel research endeavors. Data generated from the IoT lab will facilitate our quest to find answers to the following research questions:

1. What data can be recovered from smart home devices along with their respective smartphone applications (apps)?
2. Are there any privacy concerns when using these smart home devices?
3. Are there any security vulnerabilities when using these smart home devices?
4. What methods would be best suited for collecting and analyzing smart home device data?
5. What data do these smart home devices share with each other?

The rest of this paper is organized as follows: Section 2 provides background information on IoT forensics and Smart Home devices. In Section 3 we identify the components of our smart home lab while in Section 4 we present the digital forensic investigative process and how this process was used in our lab. In Section 5 we discuss possible threat scenarios that effect smart homes. In Section 6 and Section 7, we discuss the student involvement in this research as well as how our smart home lab will be used to further the educational activities at Purdue University with current industry reach-out efforts. Finally, we conclude our work in Section 8.

2 Related Work

In this section, the related work and background information regarding challenges and frameworks in IoT forensics and Smart Home devices are discussed. We pay particular attention to the challenges faced as they relate to IoT devices, IoT Forensics, and Smart Home security.

As discussed in Section 1, IoT devices are employed in various disciplines, therefore it is important to ensure their security. On the other hand, IoT devices pose security and forensic challenges due to some novel factors in IoT forensics. These novel factors include (1) the presence of large amounts of data in diverse formats which lack real time log analysis, (2) the restricted visibility of data with a low survival evidence period, (3) the restricted access to cloud data due to service level agreements, (4) the complex computing architectures, and (5) proprietary hardware and software [7].

The need for securing IoT devices and detecting cyber attacks geared toward IoT devices is increasing daily. Conti et al. [8] pointed out some major challenges for IoT environment security as: (1) the need for efficient authentication with distribution and management of keys, especially in the absence of Certificate Authority, (2) authorization to each type of IoT node with limited access, (3) identifying the nodes and collecting private data while notifying the users of data management, and (4) the need of a secure architecture that caters to Software Defined Networks and Cloud Infrastructure. While these were some of the security challenges, the authors also shed light on some of the forensic issues, such as (1) the lack of various methods for creating forensic images of IoT devices, (2) the lack of logging time records thus making evidence correlation strenuous, and (3) the absence of proper documentation of the activity makes it difficult for identification purposes.

In order to increase the familiarity with data residue from different IoT devices and show how they can be useful for investigative purposes, a recent study [9] was conducted by Servida and Casey. During their analysis, the authors found that the user commands allow the system activity logs and the event details to be recorded by the IoT devices and smartphones. The authors also discussed the challenges they faced while analyzing the IoT devices. One of the issues was the analysis of numerous, unstructured network traffic packets alongside a few limitations in configuration setting. Due to the disordered nature of network packets, there are some latency issues on the physical devices.

As the home environment has increasingly become a part of the internet due to the different devices that are connected, a study in [10] informs readers that smart home environments will be a source of evidence in the near future. This eventually leads to a discussion on some of the smart home forensics challenges such as the need for standardization, security and forensics by design, and forensically sound tools and other factors such as logging capabilities. The authors also presented their proposed seven phase framework that can be deployed in various scenarios.

As there are many challenges involved in the field of IoT forensics, the authors in [11] present a framework to address some of these challenges and support digital investigations. The concept of IoT was introduced with a mention of Distributed Denial of Service (DDoS) attack, commonly used by hackers as a gateway into the network. These attacks are unpredictable in nature and hence, they tend to expose vulnerabilities in the systems. The authors further discuss the IoT ecosystem that consists of three stacks, (1) a layered architecture of IoT, (2) components of the IoT ecosystem, and (3) possible forensic openings. Furthermore, the steps, search and seize are considered to be of utmost importance. The authors also discussed that it is crucial to identify the smart devices and preserve the digital crime scene. The proposed framework was useful in producing meaningful evidence in an IoT crime scene.

One of the major challenges due to the increased use of IoT devices, is not finding potential evidence, but rather being able to collect evidence and analyze massive amounts of data in a timely manner. In [12], authors present a concept called "the changing landscape of crime", which stated that an increase in connectivity tends to lead to an increase in cybercrimes. Cybercrimes mainly involve three components, a computer used to commit crime, a computer to store information generated during the crime, and a target computer. The paper identifies the main challenges posed by an IoT based crime as size of the objects, location, relevance of devices, legal issues, blurry networks and availability of adequate tools. The Internet of Anything can include devices from drones, autonomous systems to household devices such as refrigerators and lights. Evidence gathered from the mentioned devices can be classified into three categories: (1) Evidence collected from smart devices or sensors, (2) Evidence collected from hardware and software used for communication and, (3) Evidence from hardware and software that are outside the network under investigation. Considering these different categories, it is a significant challenge for forensic investigators to go through voluminous data. The paper concluded on the note that some practical study in this field would be more insightful to answer the challenges and provided additional ways to support the field.

As the devices are considered to be smart in a smart home setting, there is a possibility of them snitching on users and providing confidential information. In [13], the authors stated a few statistics involving the pervasiveness of IoT devices and then went into detail about the IoT forensics research challenges on acquisition and analysis of iOS devices. The authors noted some of these challenges as being the diversity of protocols due to proprietary Operating Systems (OS), the data volatility due to real time OS and smart home ecosystem with the capabilities of companion - client analysis, cloud analysis, network analysis and IoT device analysis.

Considering the above scenario and keeping the challenges in mind, using technologies alongside the knowledge acquired from the studies referred, we answer the questions and direct more attention to IoT forensics.

3 Smart Home Lab Setup

In order to utilize the full potential of a smart home, one needs to include a smart hub. This smart hub would function as the brain of the home and all other smart devices would be connected to it, either via Zigbee, Z-wave, or another IoT communication protocol [14]. Another major component of a smart home is having a dedicated internet connection that all smart devices in the home can connect to.

Our smart home lab includes 11 devices which are identified in Table 1. We first connected each IoT device to the Internet through their corresponding apps on a smartphone. The network

Table 1: Summary of devices in our smart home lab.

Name	**Function**
TP-link Archer C1900	Networking
Google Nest Hub Max	Smart Hub
Samsung Galaxy A50	Smart Home Controller
Amazon Fire TV Cube	Entertainment
August Smart Lock Pro	Home Security
August Smart Doorbell Pro	Home Security
TP-Link Smart Bulb	Lighting
Wyze Camera, Door Contacts, Motion Sensor	Security
Gosund Smart Plug	Automation
Fitbit Versa 2	Fitness Tracker
Bitdefender Box 2	Network Security

connections made between and among the IoT devices are illustrated in Figure 1. Once the IoT devices were connected to the Internet, we linked each device with the Google Nest Hub Max via the Google Home app. This enabled the devices to operate with each other interactively, such as controlling the smart light bulb from the Google Nest Hub Max itself. Each device's application account is added to the smartphone which in turn is used to link each account with the Google Nest Hub Max, as pictured in Figure 2.

3.1 IoT Forensics Investigation Process

IoT Forensics is becoming more and more essential for forensic investigations as IoT devices can aid in proving the guilt or innocence of suspects. However, for IoT forensics to be viable, we must first establish an investigative process to follow. The authors in [15] divide IoT forensics into three broad categories: (1) Cloud Forensics, (2) Network Forensics, and (3) Device-level Forensics. Depending on the type of incident being investigated, not all three categories would be required. The authors further identify the digital forensics investigative process that should be followed when dealing with an IoT environment. The process includes the following phases [15]:

1. **Initialization**: In this phase, preparatory steps are taken before ever interacting with any device at the incident scene. During this phase, investigators should:
   (a) Understand how the IoT ecosystem works.
   (b) Identify potential data sources: Data can be stored at various locations within an IoT environment such as on IoT devices themselves in the form of internal memory or SD Cards, smartphones, or even in the cloud. Identifying where data is stored would allow investigators to determine what devices to acquire, what forensic tools would be needed, as well as what legal actions need to be taken, such as obtaining a new search warrant.
2. **Acquisition**: In this phase, IoT devices and data sources are collected in a forensically sound manner. During this phase, investigators should:

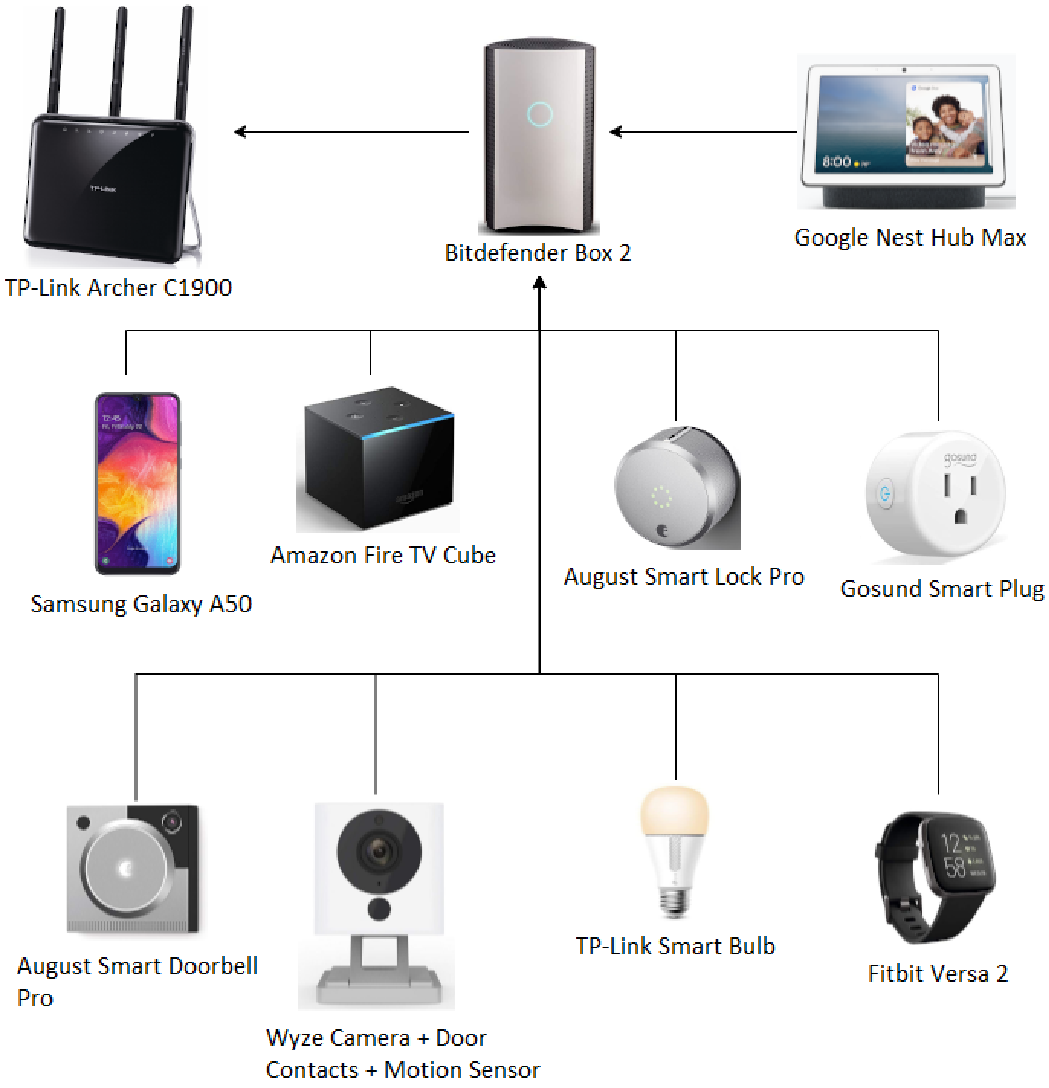


Figure 1: Network Diagram of Smart Home Lab IoT Devices.

(a) Take steps to preserve the data to be collected.

(b) Acquire any relevant devices and data sources using forensically verified methods and tools.

3. **Investigation**: In this phase, the investigator examines the acquired data to determine its relevance to the incident and analyzes any relevant data to determine what happened, who is responsible, when exactly the incident took place, why the suspect did or did not do it, and how it was done. Once these questions are answered (not all questions may be relevant depending on the type of incident being investigated), the investigator ends the investigative process by reporting all his/her relevant findings.

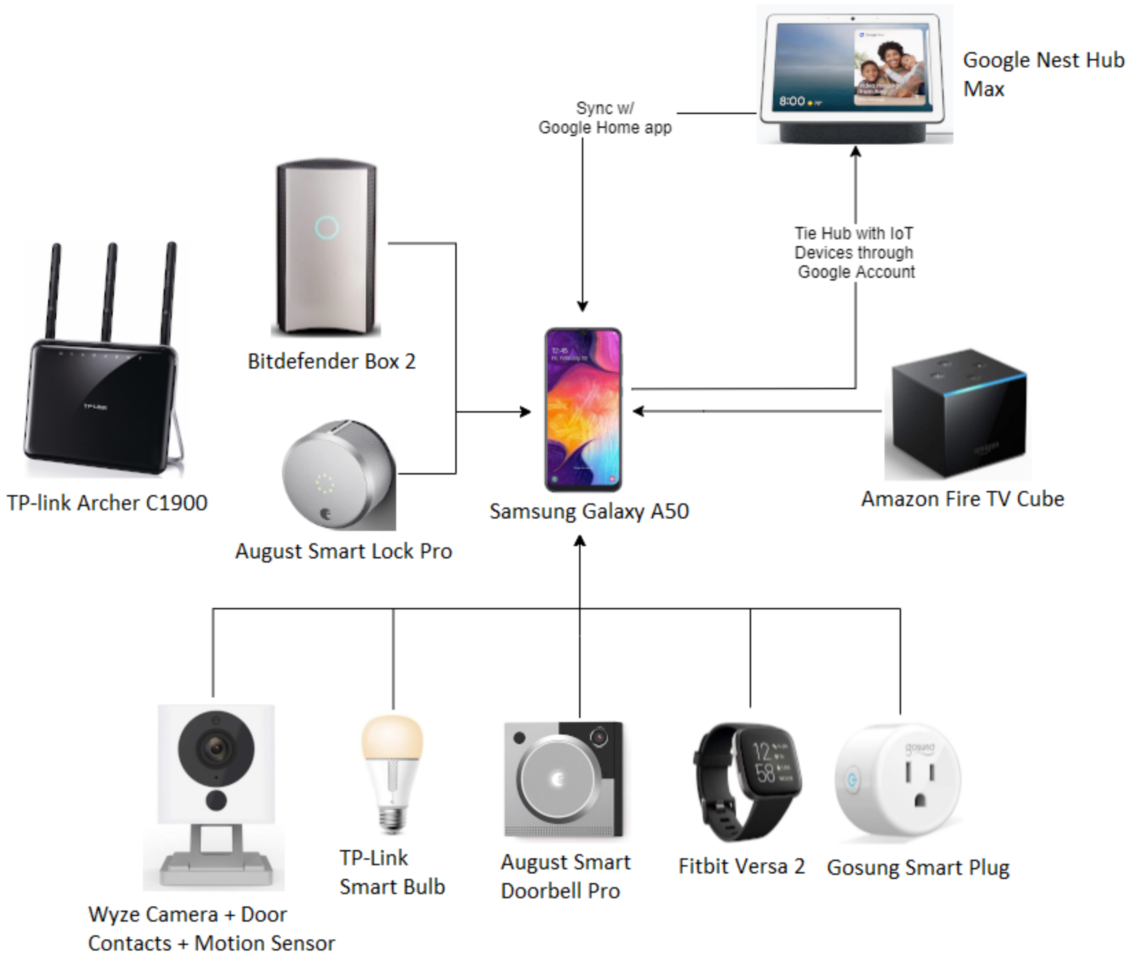


Figure 2: Account associations among IoT devices

4 Forensic Analysis of A Smart Home

During the course of our research, we conducted a brief forensic investigation into the devices in our smart home lab following the process described in Section 3.1. Specifically, we performed trivial interactions with each device via their associated apps and via voice control through the hub. Examples of the interactions we performed are presented in Table 2.

After interacting with the IoT devices, we acquired, i.e. forensically imaged, the rooted Samsung Galaxy A50 smartphone using the forensic tool, XRY [16]. XRY created a physical image of the device meaning, it made a bit-by-bit copy (henceforth called the image) of the smartphone. We then used XAMN [17] to view the image and analyze it for evidence of our interactions with the IoT devices and privacy leaks that may be present. Results from this examination are presented in Section 4.1.

Table 2: Summary of the interactions with the IoT devices.

Name	Interaction
August Smart Lock Pro	Unlock/Lock
August Smart Doorbell Pro	Ring doorbell; Answer doorbell call;
TP-Link Smart Blub	Turn on/off
Wyze Camera, Door Contacts, Motion Sensor	View camera feed; motion detection enabled;
Gosund Smart Plug	Turn on/off device
Google Nest Max Hub	Use voice to perform device interactions; Ask trivial questions;

4.1 Preliminary Investigation of Smart Home Lab

In this section, we present some of the results obtained after interacting with our IoT devices. These results answer one of our main research questions: *What data can be recovered after interacting with specific IoT devices commonly found in smart homes?* Moreover, we will also discuss how students working in this designed IoT lab can benefit from our research findings.

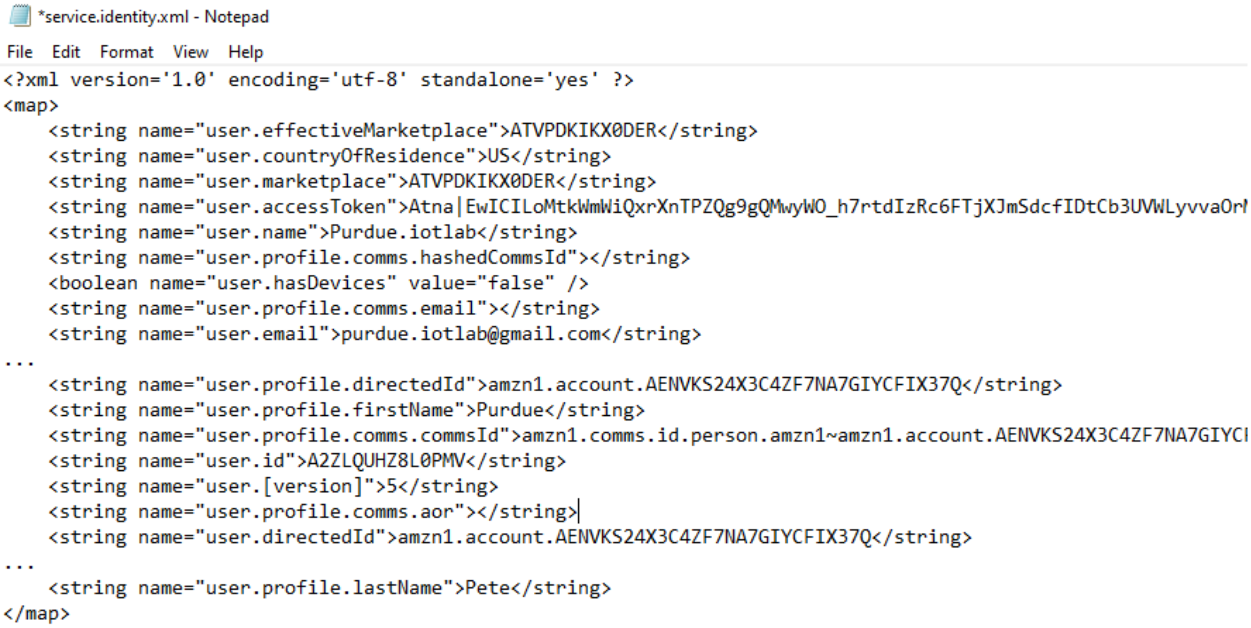
4.2 Application Privacy Concerns

The privacy concerns that we found after examining each IoT device application is described hereinafter. Privacy leaks within one of these applications can have detrimental effects on users. For example, if an attacker is able to recover the images from security cameras, those images could facilitate other crimes like blackmail. More sensitive information such as a user's contact information or residence address could also facilitate crimes, ranging from increased spam and cyber harassment to burglary.

4.2.1 Streaming Media Player Analysis

The Amazon Alexa and FireTV apps are used to interact with the Fire TV cube streaming device. We analyzed both apps for privacy leaks. Account information was discovered that poses a threat to privacy as it could be used by adversaries to conduct blackmailing or phishing attacks. This data could be used to craft tailored phishing attacks. A very powerful narrative can be crafted by the attacker who has access to detailed information which includes the victim's username as shown in Figure 3 (note that some content is redacted for double-blind review process), associated email address, full name and the make and model of the phone the home owner uses to manage their home IoT environment. The availability of our proposed IoT lab environment will allow students conducting future research to determine what data may be available after more extensive device usage and data population.

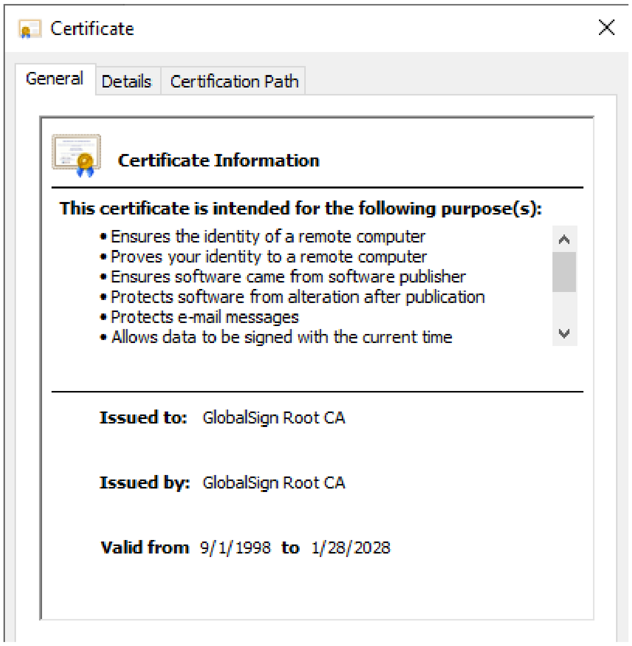
The applications and devices themselves may have security concerns due to the root certificate (See Figure 4), encryption key secret (See Figure 5), access tokens (See Figure 6), and keystore files (See Figure 7) that are present in the packages. Students may wish to find out whether these tokens and other methods of authentication for the application can be used in an attack. Examples



```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="user.effectiveMarketplace">ATVPDKIKX0DER</string>
    <string name="user.countryOfResidence">US</string>
    <string name="user.marketplace">ATVPDKIKX0DER</string>
    <string name="user.accessToken">Atna|EwICILoMtkWmWiQxrXnTPZQg9gQMwyWO_h7rtdIzRc6FTjXJmSdcfIDtCb3UVWLyvvaOr
    <string name="user.name">Purdue.iotlab</string>
    <string name="user.profile.comms.hashedCommsId"></string>
    <boolean name="user.hasDevices" value="false" />
    <string name="user.profile.comms.email"></string>
    <string name="user.email">purdue.iotlab@gmail.com</string>
...
    <string name="user.profile.directedId">amzn1.account.AENVKS24X3C4ZF7NA7GIYCFIX37Q</string>
    <string name="user.profile.firstName">Purdue</string>
    <string name="user.profile.comms.commsId">amzn1.comms.id.person.amzn1~amzn1.account.AENVKS24X3C4ZF7NA7GIYC
    <string name="user.id">A2ZLQUHZ8L0PMV</string>
    <string name="user.[version]">5</string>
    <string name="user.profile.comms.aor"></string>
    <string name="user.directedId">amzn1.account.AENVKS24X3C4ZF7NA7GIYCFIX37Q</string>
...
    <string name="user.profile.lastName">Pete</string>
</map>
```

Figure 3: User data such as email, Amazon generated ID and name. Also contained OAuth tokens

could include creating fake certificates signed with the root certificate or pushing out malicious versions of apps signed with the keys contained in the keystore files. Even if students' attempts fail in creating a successful attack, in the process of developing an exploit they would have learned valuable skills in security focused analysis and increased their knowledge of important ideas like web certificates, access tokens, and application signing.



Certificate Information

This certificate is intended for the following purpose(s):

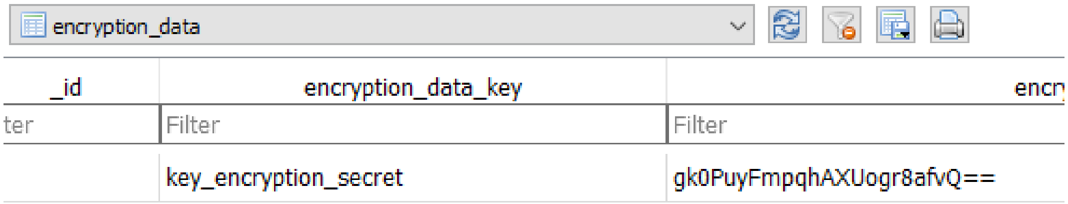
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Allows data to be signed with the current time

Issued to: GlobalSign Root CA

Issued by: GlobalSign Root CA

Valid from 9/1/1998 **to** 1/28/2028

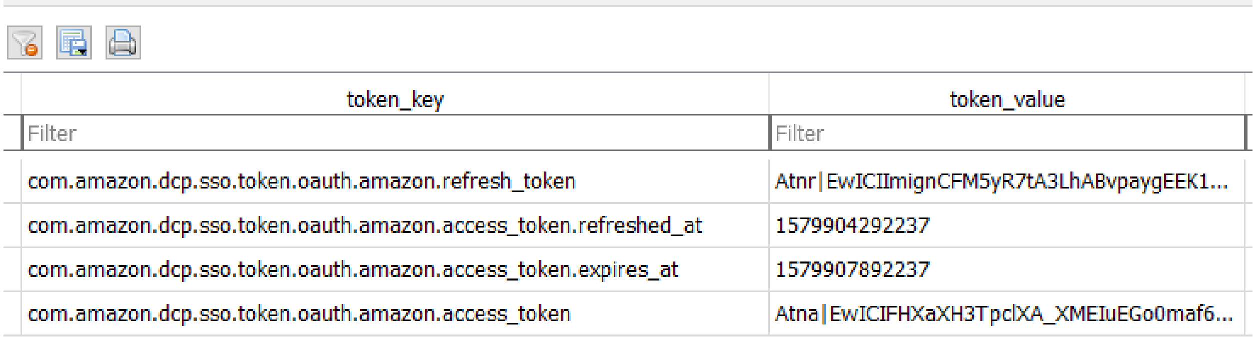
Figure 4: Certificate uses and issuing body contained in the rootca_list.crt file



encryption_data

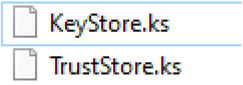
_id	encryption_data_key	encr
ter	Filter	Filter
	key_encryption_secret	gk0PuyFmpqhAXUogr8afvQ==

Figure 5: Encryption key secret found in encryption_data database table



token_key	token_value
Filter	Filter
com.amazon.dcp.sso.token.oauth.amazon.refresh_token	Atnr|EwICIImignCFM5yR7tA3LhABvpaygEEK1...
com.amazon.dcp.sso.token.oauth.amazon.access_token.refreshed_at	1579904292237
com.amazon.dcp.sso.token.oauth.amazon.access_token.expires_at	1579907892237
com.amazon.dcp.sso.token.oauth.amazon.access_token	Atna|EwICIFHXaXH3TpclXA_XMEIuEGo0maf6...

Figure 6: OAuth token information

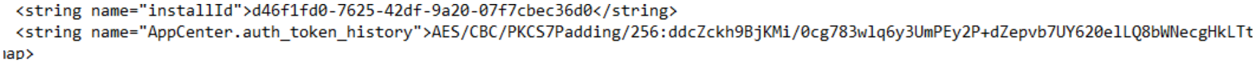


KeyStore.ks
TrustStore.ks

Figure 7: KeyStore files

4.2.2 Smart Watch Analysis

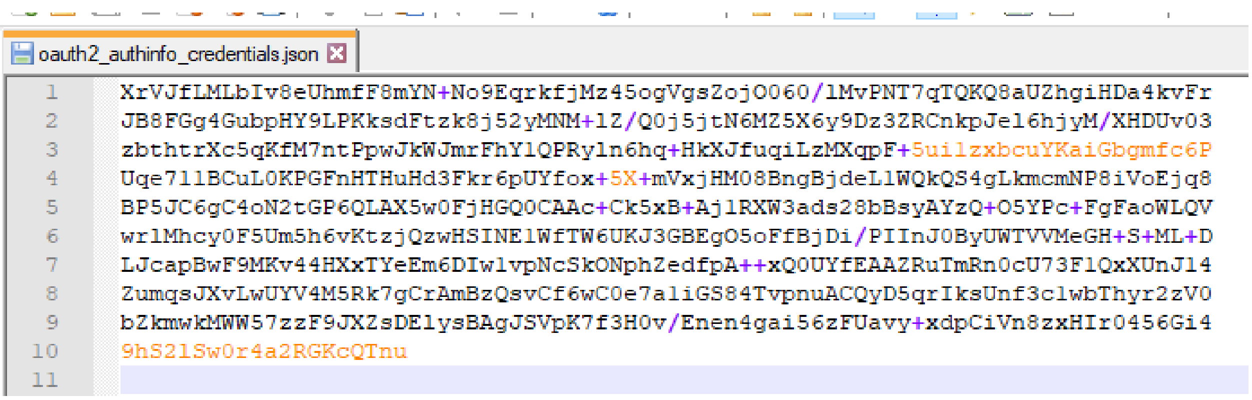
Similar to Amazon apps, artifacts were found in the Fitbit application package which could compromise user privacy, as well as application security. User data, including names and email addresses, are present and can pose a security risk, albeit potentially not as serious as Amazon Alexa and FireTV. Security concerns exist again with the authentication token (See Figure 8) and OAuth credential (Figure 9) information being stored in plaintext. The OAuth credentials file may be encrypted as the file has a JSON extension yet the contents look nothing like structured JSON data. Figuring out what can be done, if anything, to attack such a file could be a worthwhile student project.



```
 <string name="installId">d46f1fd0-7625-42df-9a20-07f7cbec36d0</string>
 <string name="AppCenter.auth_token_history">AES/CBC/PKCS7Padding/256:ddcZckh9BjKMi/0cg783wlq6y3UmPEy2P+dZepvb7UY620elLQ8bWNecgHkLTt
ıap>
```

Figure 8: Auth token history stored with encryption algorithm and mode, along with padding style used and token length.

Note that the Fitbit Versa 2 was paired with the device using a new user account but due to constraints in time and resources no data was populated using the Versa 2 beyond the basic Bluetooth pairing. It is possible that students who populate data using an appropriate methodology would have more significant findings.



oauth2_authinfo_credentials.json

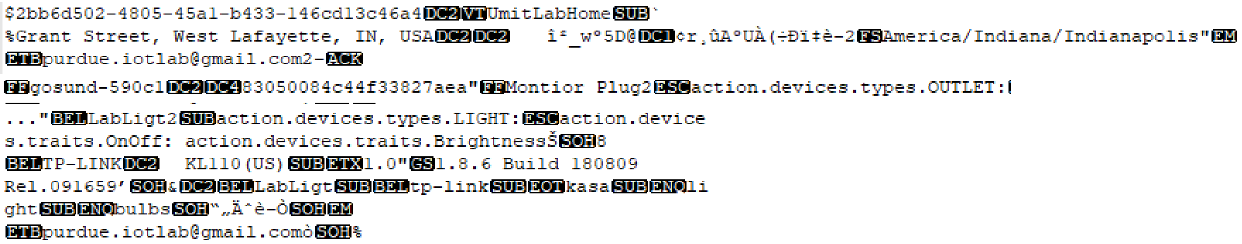
```
XrVJfLMLbIv8eUhmfF8mYN+No9EqrkfjMz45ogVgsZojO060/1MvPNT7qTQKQ8aUZhgiHDa4kvFr
JB8FGg4GubpHY9LPKksdFtzk8j52yMNM+1Z/Q0j5jtN6MZ5X6y9Dz3ZRCnkpJel6hjyM/XHDUv03
zbthtrXc5qKfM7ntPpwJkWJmrFhY1QPRyln6hq+HkXJfuqiLzMXqpF+5uilzxbcuYKaiGbgmfc6P
Uqe71lBCuL0KPGFnHTHuHd3Fkr6pUYfox+5X+mVxjHM08BngBjdeL1WQkQS4gLkmcmNP8iVoEjq8
BP5JC6gC4oN2tGP6QLAX5w0FjHGQ0CAAc+Ck5xB+Aj1RXW3ads28bBsyAYzQ+O5YPc+FgFaoWLQV
wrlMhcy0F5Um5h6vKtzjQzwHSINElWfTW6UKJ3GBEgO5oFfBjDi/PIInJ0ByUWTVVMeGH+S+ML+D
LJcapBwF9MKv44HXxTYeEm6DIwlvpNcSkONphZedfpA++xQ0UYfEAAZRuTmRn0cU73F1QxXUnJ14
ZumqsJXvLwUYV4M5Rk7gCrAmBzQsvCf6wC0e7aliGS84TvpnuACQyD5qrIksUnf3clwbThyr2zV0
bZkmwkMWW57zzF9JXZsDElysBAgJSVpK7f3H0v/Enen4gai56zFUavy+xdpCiVn8zxHIr0456Gi4
9hS21Sw0r4a2RGKcQTnu
```

Figure 9: OAuth2 credential information stored in JSON file.

4.2.3 Smart Hub Analysis

The Google Home smartphone app contained artifacts which had a significant impact on user privacy. When first setting up the Google Nest Hub Max, a name for the house is required. Considering users will likely put their names, this could be a data privacy concern. The email address of the user account is also exposed. More significantly however, the full address of the users home is listed in the document, excluding their ZIP code.

Additionally, the names of the devices that were integrated with the Google Nest Hub Max are also available. Some of the device information, such as the manufacturer company name, is also shown. Alone, this information is not useful to an attacker. However, an attacker seeking to gain further access into a victims home network could use this information to aid them as it would be a great resource for reconnaissance. Knowing the names of the various devices, how many IoT devices have been connected to the Google Nest Hub Max, as well as some brand and manufacturer information can help attackers to discover new vulnerable devices to target next in an attempt to gain more access and control over the home network. The artifacts found are shown in Figure 10 (note that some content is redacted for double-blind review process).



```
$2bb6d502-4805-45a1-b433-146cd13c46a4DC2VTUmitLabHomeSUB`
%Grant Street, West Lafayette, IN, USADC2DC2   îª_w°5D@DC1¢r¸ûA°UÀ(÷Ðï‡è-2FSAmerica/Indiana/Indianapolis"EM
ETBpurdue.iotlab@gmail.com2-ACK
```

```
FFgosund-590c1DC2DC483050084c44f33827aea"FFMontior Plug2ESCaction.devices.types.OUTLET:|
```

```
..."BELLabLigt2SUBaction.devices.types.LIGHT:ESCaction.device
s.traits.OnOff: action.devices.traits.BrightnessŠSOH8
BELTP-LINKDC2   KL110(US)SUBETX1.0"GS1.8.6 Build 180809
Rel.091659'SOH&DC2BELLabLigtSUBBELtp-linkSUBEOTkasaSUBENQli
ghtSUBENQbulbsSOH"„Äˆè-ÒSOHEM
ETBpurdue.iotlab@gmail.comòSOH%
```

Figure 10: Excerpts of file showing email address, full home address, device names, and brands

4.2.4 Smart Doorbell and Smart Lock Analysis

The August smart lock and smart doorbell are controlled by the August Home app. After examining the August Home app, we identified the location of relevant data to be under the package name, *com.august.luna*. We were able to recover potentially relevant data that would be useful in an investigation. We found log information (see Figure 11), doorbell pictures, that were automatically taken after a motion detection event (see Figure 12), and user interactions with the August devices (see Figure 13). These three pieces of information can be vital in determining the whereabouts of a suspect or identifying package thieves. Information about who was granted access to the August devices could also be recovered along with logs of their interactions with the smart devices.

4.2.5 Network Security Application analysis

Bitdefender Box requires the use of the Bitdefender Central app, which allows users to conveniently monitor their home network for security threats. For added security, Bitdefender Central advises users to also install the Bitdefender Security app. After examining the two apps, we identified their app packages as *com.bitdefender.centralmgmt* and *com.bitdefender.security*.

In regard to the Bitdefender Central app, we were able to identify the user's email address and name, in plaintext, from the *\app\webview\Cookies.db* file, shown in Figure 14 (note that some content is redacted for double-blind review process). In the *\databases\cache-database.db* file, we recovered identifying information, such as MAC addresses, about each device that had been connected to the network, along with timestamps. Scanning our network with Bitdefender Central did not show any vulnerabilities with our IoT devices. The Bitdefender Security app provided us with timestamps of when a virus scan was run and could also show us apps that were added to the blacklist, which is the list of apps that are categorized as having malware.

4.2.6 Smart Plug Analysis

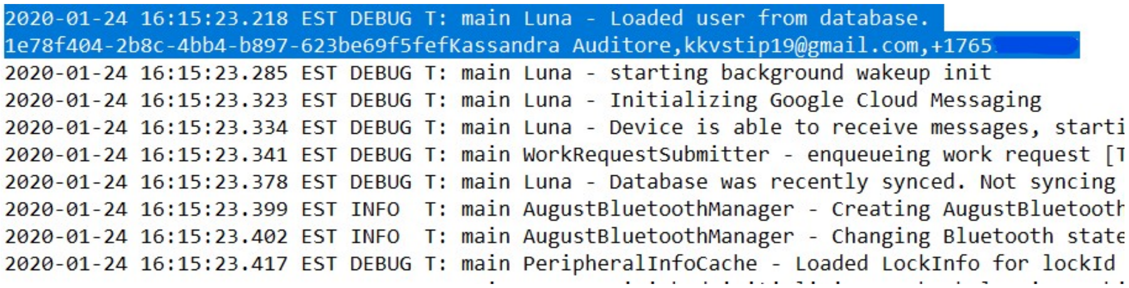
The GoSmart app was used to control the smart plug in our smart home setup. After our examination of the GoSmart app, we were only able to recover logs of our interactions with the smart plug, that were found in the *\com.cuco.smart\databases\tuyasmart_cipher.db* file. However, these logs were not descriptive and did not explicitly identify the actions we took when interacting with the smart plug. Instead, the type of interaction was labeled as 1, 2 or 3, and the event tag had a value of "Event". The logs did include a duration tag and a timestamp, though further investigation would be required to determine exactly what the duration tags record. An example of a log entry is shown in Figure 15.

4.2.7 Smart Camera Analysis

The Wyze app is among one of the most secure apps we've investigated in our smart home lab. The database, *support_base_db_encrypt*, was encrypted and there were no pictures from the camera in the cache folder, even after motion detection events. We were able to recover the user's email address and device information for the various Wyze devices we had setup in our lab (see Figure 16 with redacted content for double-blind review process), from the *\com.hualai\shared_prefs\HuaLaiCamData.xml* file.

4.2.8 Smart Bulb Analysis

The Kasa app was used to control the smart light bulb in our smart home lab. Relevant data was recovered from the *\com.tplink.kasa_android\databases\iot.1.db* file. Within this file, the



```
2020-01-24 16:15:23.218 EST DEBUG T: main Luna - Loaded user from database.
1e78f404-2b8c-4bb4-b897-623be69f5fefKassandra Auditore,kkvstip19@gmail.com,+1765[redacted]
2020-01-24 16:15:23.285 EST DEBUG T: main Luna - starting background wakeup init
2020-01-24 16:15:23.323 EST DEBUG T: main Luna - Initializing Google Cloud Messaging
2020-01-24 16:15:23.334 EST DEBUG T: main Luna - Device is able to receive messages, starti
2020-01-24 16:15:23.341 EST DEBUG T: main WorkRequestSubmitter - enqueueing work request [T
2020-01-24 16:15:23.378 EST DEBUG T: main Luna - Database was recently synced. Not syncing
2020-01-24 16:15:23.399 EST INFO  T: main AugustBluetoothManager - Creating AugustBluetooth
2020-01-24 16:15:23.402 EST INFO  T: main AugustBluetoothManager - Changing Bluetooth state
2020-01-24 16:15:23.417 EST DEBUG T: main PeripheralInfoCache - Loaded LockInfo for lockId
```

Figure 11: August user info found in log file.

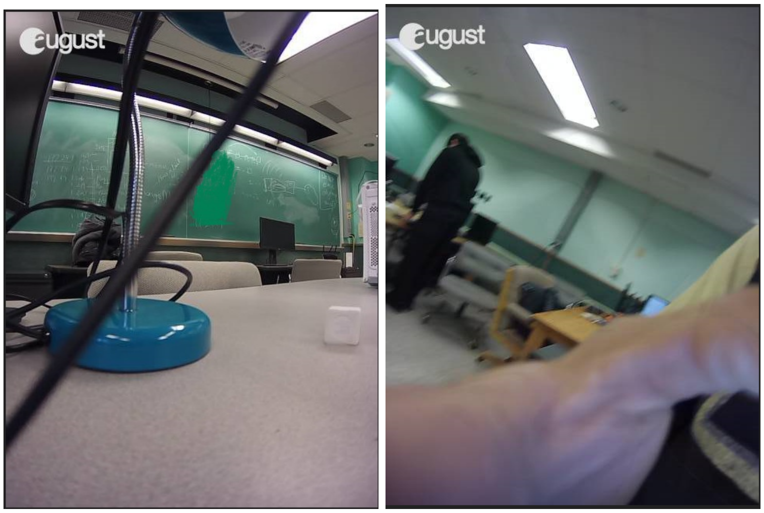
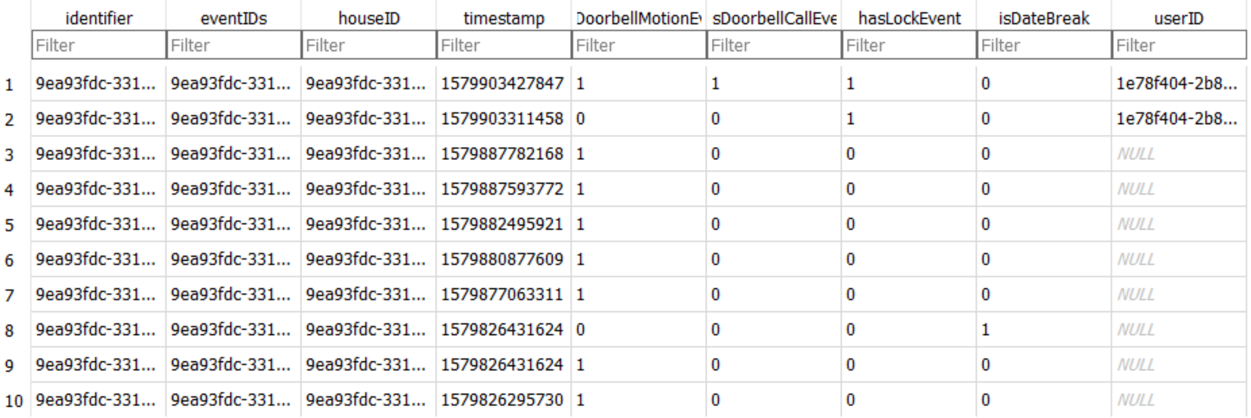
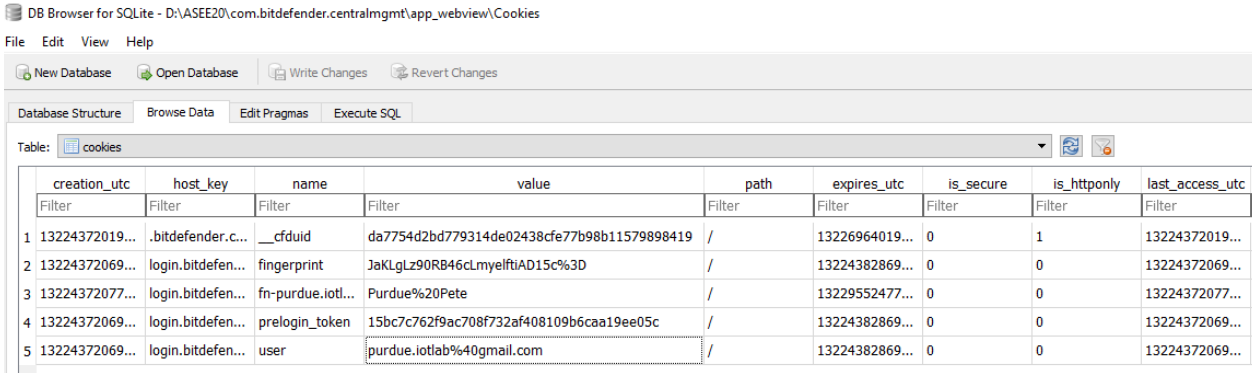


Figure 12: Pictures taken due to August doorbell camera motion detection event.



	identifier	eventIDs	houseID	timestamp	DoorbellMotionE	sDoorbellCallEve	hasLockEvent	isDateBreak	userID
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	9ea93fdc-331...	9ea93fdc-331...	9ea93fdc-331...	1579903427847	1	1	1	0	1e78f404-2b8...
2	9ea93fdc-331...	9ea93fdc-331...	9ea93fdc-331...	1579903311458	0	0	1	0	1e78f404-2b8...
3	9ea93fdc-331...	9ea93fdc-331...	9ea93fdc-331...	1579887782168	1	0	0	0	NULL
4	9ea93fdc-331...	9ea93fdc-331...	9ea93fdc-331...	1579887593772	1	0	0	0	NULL
5	9ea93fdc-331...	9ea93fdc-331...	9ea93fdc-331...	1579882495921	1	0	0	0	NULL
6	9ea93fdc-331...	9ea93fdc-331...	9ea93fdc-331...	1579880877609	1	0	0	0	NULL
7	9ea93fdc-331...	9ea93fdc-331...	9ea93fdc-331...	1579877063311	1	0	0	0	NULL
8	9ea93fdc-331...	9ea93fdc-331...	9ea93fdc-331...	1579826431624	0	0	0	1	NULL
9	9ea93fdc-331...	9ea93fdc-331...	9ea93fdc-331...	1579826431624	1	0	0	0	NULL
10	9ea93fdc-331...	9ea93fdc-331...	9ea93fdc-331...	1579826295730	1	0	0	0	NULL

Figure 13: User interactions with August devices.



	creation_utc	host_key	name	value	path	expires_utc	is_secure	is_httponly	last_access_utc
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	13224372019...	.bitdefender.c...	__cfduid	da7754d2bd779314de02438cfe77b98b11579898419	/	13226964019...	0	1	13224372019...
2	13224372069...	login.bitdefen...	fingerprint	JaKLgLz90RB46cLmyelftiAD15c%3D	/	13224382869...	0	0	13224372069...
3	13224372077...	login.bitdefen...	fn-purdue.iotl...	Purdue%20Pete	/	13229552477...	0	0	13224372077...
4	13224372069...	login.bitdefen...	prelogin_token	15bc7c762f9ac708f732af408109b6caa19ee05c	/	13224382869...	0	0	13224372069...
5	13224372069...	login.bitdefen...	user	purdue.iotlab%40gmail.com	/	13224382869...	0	0	13224372069...

Figure 14: User Account information from Bitdefender Central.

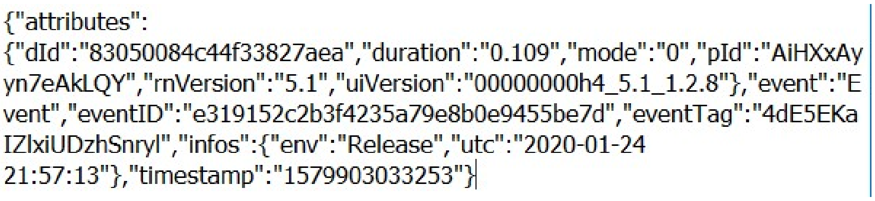

```
{"attributes":
{"dId":"83050084c44f33827aea","duration":"0.109","mode":"0","pId":"AiHXxAy
yn7eAkLQY","rnVersion":"5.1","uiVersion":"00000000h4_5.1_1.2.8"},"event":"E
vent","eventID":"e319152c2b3f4235a79e8b0e9455be7d","eventTag":"4dE5EKa
IZlxiUDzhSnryl","infos":{"env":"Release","utc":"2020-01-24
21:57:13"},"timestamp":"1579903033253"}
```

Figure 15: Log entry from GoSmart app.

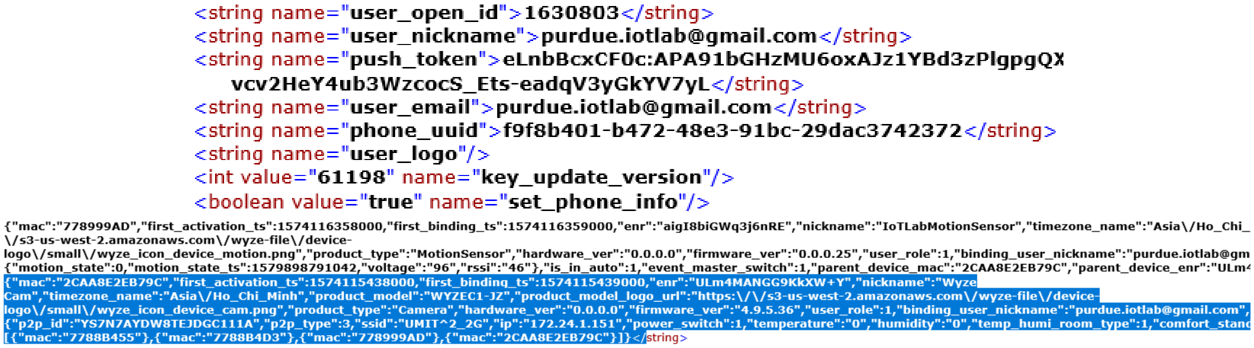
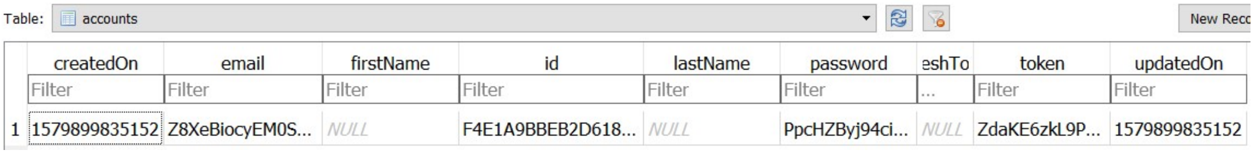

```
<string name="user_open_id">1630803</string>
<string name="user_nickname">purdue.iotlab@gmail.com</string>
<string name="push_token">eLnbBcxCF0c:APA91bGHzMU6oxAJz1YBd3zPlgpgQX
   vcv2HeY4ub3WzcocS_Ets-eadqV3yGkYV7yL</string>
<string name="user_email">purdue.iotlab@gmail.com</string>
<string name="phone_uuid">f9f8b401-b472-48e3-91bc-29dac3742372</string>
<string name="user_logo"/>
<int value="61198" name="key_update_version"/>
<boolean value="true" name="set_phone_info"/>
{"mac":"778999AD","first_activation_ts":1574116358000,"first_binding_ts":1574116359000,"enr":"aigI8biGWq3j6nRE","nickname":"IoTLabMotionSensor","timezone_name":"Asia\/Ho_Chi_
\/s3-us-west-2.amazonaws.com\/wyze-file\/device-
logo\/small\/wyze_icon_device_motion.png","product_type":"MotionSensor","hardware_ver":"0.0.0.0","firmware_ver":"0.0.0.25","user_role":1,"binding_user_nickname":"purdue.iotlab@gm
{"motion_state":0,"motion_state_ts":1579898791042,"voltage":"96","rssi":"46"},"is_in_auto":1,"event_master_switch":1,"parent_device_mac":"2CAA8E2EB79C","parent_device_enr":"ULm4
{"mac":"2CAA8E2EB79C","first_activation_ts":1574115438000,"first_binding_ts":1574115439000,"enr":"ULm4MANGG9KkXW+Y","nickname":"Wyze
Cam","timezone_name":"Asia\/Ho_Chi_Minh","product_model":"WYZEC1-JZ","product_model_logo_url":"https:\/\/s3-us-west-2.amazonaws.com\/wyze-file\/device-
logo\/small\/wyze_icon_device_cam.png","product_type":"Camera","hardware_ver":"0.0.0.0","firmware_ver":"4.9.5.36","user_role":1,"binding_user_nickname":"purdue.iotlab@gmail.com",
{"p2p_id":"YS7N7AYDW8TEJDGC111A","p2p_type":3,"ssid":"UMIT^2_2G","ip":"172.24.1.151","power_switch":1,"temperature":"0","humidity":"0","temp_humi_room_type":1,"comfort_stand
[{"mac":"7788B455"},{"mac":"7788B4D3"},{"mac":"778999AD"},{"mac":"2CAA8E2EB79C"}]}</string>
```

Figure 16: Wyze user's email and Wyze device information.

accounts table holds the user's Personally Identifiable Information (PII), however, the email address and password are encrypted and the user's first and last names are not present in the table (see Figure 17). The devices table provides information on all TP-link connected devices including device alias, which is the name the user sets for the device, the device state, the device type, etc. We also identified two tables containing location information. One location table holds location data of compatible TP-Link devices and the other records information about the *AwayHomeStatus* variable.

5 Possible Smart Home Threat Scenarios

With our newly created IoT lab, students will be able to explore different security facets of smart home automation. Investigations can be forensically focused on finding what data is generated by



	createdOn	email	firstName	id	lastName	password	eshTo	token	updatedOn
	Filter	Filter	Filter	Filter	Filter	Filter	...	Filter	Filter
1	1579899835152	Z8XeBiocyEM0S...	NULL	F4E1A9BBEB2D618...	NULL	PpcHZByj94ci...	NULL	ZdaKE6zkL9P...	1579899835152

Figure 17: Kasa account information found in the database file.

smart home IoT devices and its possible implications from both the user's privacy and law enforcement perspectives. Investigations could be focused on assessing the security of devices for possible vulnerabilities that a malicious actor could exploit to cause damage to the homeowners or residents. Beyond that, there are other possible uses for this lab such as being a test bed for student-developed apps, or even development and production of their own IoT devices that would integrate with existing smart home hub devices to provide added security protections or intrusion prevention functionality. This smart home lab can also facilitate the creation of assignments for different courses at Purdue University. For example, we can execute various scenarios using the devices in our lab, create forensic images of control devices and assign these images to students to perform forensic analyses to determine various events. We describe four possible threat scenarios below.

One case study of a potential threat vector and how students could engage with it using an active learning project is the investigation of the smart plug device. Using the IoT lab, students would be able to investigate what security measures exist to protect smart plugs from potential damage. The impacts of successfully attacking the smart plugs can vary depending on how the smart plugs are used in the house. The impact of smart plugs can be trivial, such as controlling a lamp or light, to more serious, if it was connected to electrical appliances, baby monitors, even refrigerators. The IoT lab could be used by students to test different cases where the smart plugs are installed in different use cases, then use the infrastructure provided by the lab to conduct vulnerability assessments on the smart plugs. Students could then setup and configure a small device, such as a Raspberry Pi, to act as a firewall to block any malicious attacks that they now know could shut off the device without the owner's consent.

Another potential threat is one that affects WiFi cameras. It is very easy to find Wi-Fi security cameras that cost less than $100. These budget cameras may not offer the same data protections and user privacy that the more expensive cameras tend to provide. Students and faculty can use our smart home lab to investigate different Wi-Fi cameras for privacy leaks and security vulnerabilities. Wi-Fi cameras are especially vulnerable to cyber attacks as compromising them results in the ultimate lost of privacy to the victims. Attacking a Wi-Fi camera can start by subjecting the camera to a deauthorization attack in which the attack forces the camera to drop off its Internet connection. Such an attack will result in the live stream from the camera being stuck and motion detection events will go unreported. At this point, bad actors would be able to physically traverse the home without fear of being recorded.

Although the features offered by the Google Nest Hub Max are highly utilitarian, some features could pose serious threats once compromised. In regard to the broadcast function of the Google Home app, an intruder can trigger the devices in the house and gain control over them remotely. Consider another scenario where using the Google Home app to record reminders, could be detrimental. In this case, the intruders can gain access to personal information, such as routine schedules of the person(s) in the house, without much difficulty. A similar scenario is the capability of the Google Home application to set-up the hub for all the smart home devices. Here, the effect of one malicious attack on a single device could easily threaten the entire hub system as it is interconnected, thus leading to the compromise of vital data.

There have been issues regarding Alexa eavesdropping on users [18], collecting or listening to private conversations and recording those conversations. This could raise concerns regarding the kind of data that might have been collected by smart home devices. This could also pose a major red flag regarding the IoT device as recorded conversations may be attainable to anyone with back-end (database) access to the server. Another potential case is that Alexa-enabled devices can be used to create a botnet environment that can cause network traffic problems through all connected devices that could result in their malfunctioning. An equally critical threat scenario can be the DDoS attack, where massive chunks of data traffic is directed to the system. This could cause lack of resource availability which could impact the overall functioning of the system.

6 Student Involvement

This project was done under the supervision of a faculty member with expertise in Digital and Cyber Forensics. One Cyber Forensics doctoral student lead the project and two Cyber Forensics Master's students later joined the project. All three students are still enrolled at Purdue University. The project was done between September 2019 and January 2020. Table 3 shows the student information and contributions to this project.

Table 3: Summary of student involvement in this research.

Name	Degree Program	Contribution	Duty
Shinelle Hutchinson	Cyber Forensics	Started the project Sep 2019 to April 2020	Purchasing, Implementation, Digital Forensics, Data Collection and Analysis, Report Preparation, Paper Writing and Editing
Yung Han Yoon	Cyber Forensics	Worked on the project Nov 2019 to April 2020	Implementation, Digital Forensics, Data Collection and Analysis, Report Preparation, Paper Writing and Editing
Neesha Shantaram	Cyber Forensics	Worked on the project Nov 2019 to April 2020	Implementation and Report Preparation, Paper Writing and Editing

7 Learning Outcomes, Educational Activities and Industry Support

During the course of our research we designed, developed, tested and investigated the proposed smart home laboratory particularly for the purpose of understanding potential security, privacy, and forensics issues on commonly used IoT devices. Currently our lab is fully functional, and it will be used in two courses offered during the Spring 2020 semester in the Department of Computer and Information Technology. The first course is Basic Cyber Forensics, which is taught at the senior level and is considered as a large lecture with four lab sections. The second course is

Mobile and Embedded Systems Forensics and is taught at the graduate level. Currently, six undergraduate students are enrolled in this graduate course and four of them are working on research projects using our newly designed lab.

7.1 Learning Outcomes and Assessment

The related, expected learning outcomes for students enrolled in the above courses include being able to: (1) Identify and compare various mobile/IoT devices and their characteristics, (2) Apply forensically sound investigative procedures to devices/networks available in the lab, and (3) Evaluate the security and privacy of data in smart home components. In order to assess the students' competence of the learning outcomes, the instructors will create hands-on lab activities and term projects with research components on the available devices in the smart home lab. Students will be asked to present their research and findings in class and the duration of the presentation will be limited to 10 minutes for each team.

7.2 Educational Activities

The pedagogical method used in these courses will be a project based learning approach. Project based learning is an excellent instructional design approach to engage students actively in the labs [19]. Therefore, the students will work in groups and the course instructor will encourage group discussions on the findings retrieved from different groups on particular topics. The instructor will also pay attention to Self Determination Theory (SDT) [20] and allow students to determine their own project topics and related devices in the lab which aims to provide autonomy to meet their psychological needs in learning.

Moreover, this lab will be extremely important for the other courses (new or currently available) in which the instructors may create related assignments, projects and labs utilizing the data collected from our proposed lab. These potential courses are Vulnerability Assessment and Penetration Testing, Small Scale Digital Device Forensics, Malware Forensics, IoT Forensics, Network Forensics, etc. which are/can be taught at both the undergraduate and graduate levels. Last but not least, all the students who participated in this research had significant experience on security, privacy, and forensic analysis of contemporary IoT devices, both individually and as a research group. These skills will be indispensable for their academic success in the rest of their studies.

Furthermore, we strongly believe that the methodology used in this work can be also revised and followed to create a similar lab for various other domains such as SCADA and Industrial Control Systems, and smart grid/cities etc. Finally, the forensics data collected during the activities in our lab can be used for purposes beyond education, such as law enforcement and/or cybersecurity professional training.

7.3 Industry Support

As part of our industry reach out and support activities, we have contacted with MOBILedit for their education support programs. We are in the process of having access to their mobile and IoT forensics product to conduct continuous research on already available and future devices. We will also be reaching out to industry partners for collaborations and internship opportunities that our students can benefit the most from.

8 Conclusion

Smart devices are being incorporated into homes at a profound rate. Having all these interconnected and Internet connected devices, introduce vulnerabilities in the home network. We need to be prepared regarding the types of devices forensic investigators may encounter in a smart home, the vulnerabilities that exist or threaten IoT devices, the viable methods of investigating these IoT devices, and what potential evidence can be recovered regarding the use of these smart devices. To that end, our smart home lab will serve as a training ground and research lab for students and faculty interested in learning about IoT Forensics and conducting research in the IoT domain.

Our future goal is to expand the IoT lab to contain a larger variety of devices, introduce additional security devices and test the claimed features of various security enhancing products on the market. Faculty and students participating in this research will conduct their further research on the devices and develop investigative frameworks for practitioners based on their findings. These frameworks will be important sources for examiners/practitioners when they need systematic investigation on a particular device or smart home as a whole.

References

[1] “Forecast market size of the global smart home market from 2016 to 2022 (in billion u.s. dollars)*,” 2019.

[2] “Smart home device sales/shipments worldwide in 2017 and 2018, by category.” https://www.statista.com/statistics/873539/worldwide-smart-home-annual-device-sales/, 2019. Last Accessed: 03-16-2020.

[3] A. Ng, “Three plead guilty to creating mirai botnet used to crash web.” https://www.cnet.com/news/mirai-botnet-hacker-behind-2016-web-outage-pleads-guilty/, 2017.

[4] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi, “Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach,” in *Proceedings of the Internet Measurement Conference*, pp. 267–279, 2019.

[5] “Avast smart home security report 2019.” https://press.avast.com/hubfs/media-materials/kits/smart-home-report-2019/Report/Avast%20Smart%20Home%20Report_EN.pdf?hsLang=en, 2019. Last Accessed: 03-16-2020.

[6] “The trust opportunity:exploring consumers’ attitudes to the internet of things.” https://www.internetsociety.org/wp-content/uploads/2019/05/CI_IS_Joint_Report-EN.pdf, 2019. Last Accessed: 03-16-2020.

[7] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. A. Kazmi, and C. S. Hong, “Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges,” *Future Generation Computer Systems*, vol. 92, pp. 265–275, 2019.

[8] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of things security and forensics: Challenges and opportunities,” 2018.

[9] F. Servida and E. Casey, “Iot forensic challenges and opportunities for digital traces,” *Digital Investigation*, vol. 28, pp. S22–S29, 2019.

[10] A. Goudbeek, K.-K. R. Choo, and N.-A. Le-Khac, “A forensic investigation framework for smart home environment,” in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 1446–1451, IEEE, 2018.

[11] S. Sathwara, N. Dutta, and E. Pricop, “Iot forensic a digital investigation framework for iot systems,” in *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. 1–4, IEEE, 2018.

[12] A. MacDermott, T. Baker, and Q. Shi, “Iot forensics: Challenges for the ioa era,” in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5, IEEE, 2018.

[13] G. Dorai, S. Houshmand, and I. Baggili, “I know what you did last summer: your smart home internet of things and your iphone forensically ratting you out,” in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1–10, 2018.

[14] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, “Internet of things (iot) communication protocols,” in *2017 8th International conference on information technology (ICIT)*, pp. 685–690, IEEE, 2017.

[15] V. R. Kebande and I. Ray, “A generic digital forensic investigation framework for internet of things (iot),” in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 356–362, IEEE, 2016.

[16] P. Eklund, “Xry physical.” `https://www.msab.com/products/xry/xry-physical/`. Last Accessed: 03-16-2020.

[17] “Xamn - analyze.” `https://www.msab.com/products/xamn/`, Dec 2019. Last Accessed: 03-16-2020.

[18] B. Stegner, “7 ways alexa and amazon echo pose a privacy risk.” `https://www.makeuseof.com/tag/alexa-amazon-echo-privacy-risk/`, Jan 2018. Last Accessed: 03-16-2020.

[19] J. S. Vogler, P. Thompson, D. W. Davis, B. E. Mayfield, P. M. Finley, and D. Yasseri, “The hard work of soft skills: augmenting the project-based learning experience with interdisciplinary teamwork,” *Instructional Science*, vol. 46, no. 3, pp. 457–488, 2018.

[20] E. L. Deci and R. M. Ryan, “Self-determination theory.,” 2012.

Appendix A.

Software

- XRY
- Magisk Manager
- Magisk
- Samsung A505G Stock Firmware (Trinidad and Tobago) -
- Odin
- TWRP