Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study

Brittany D. Davis, Janelle C. Mason, and Mohd Anwar

***Abstract*— Internet of Things technology has revolutionized our daily lives in many ways — whether it is the way we conduct our day-to-day activities inside our home, or the way we control our home environments remotely. Unbeknownst to the users, with adoption of these "smart home" technologies, their personal space becomes vulnerable to security and privacy attacks. We conducted studies of vulnerabilities and security posture of smart home IoT devices. We started with a literature review on known vulnerability studies of the IoT devices, considering four categories of attacks: physical, network, software, and encryption. We then conducted our own vulnerability experiments that compared security postures between well-known and lesser-known vendors through misuse and abuse case analysis, followed by a review of coverage in major vulnerability databases. Based on our analysis, the main finding was the need for a stronger focus on the security posture of lesser-known vendor devices as they are often less regulated and face less scrutiny.**

***Index Terms*— abuse cases, cybersecurity, Internet of Things, home automation, misuse cases, security postures, smart devices, smart homes, vulnerabilities**

I. Introduction

INTERNET of Things (IoT) is a concept to realize the vision of a connected world through machine-to-machine communication over the Internet. IoT devices allow users to easily automate tasks and services through the help of connected software applications, systems, and voice assistants. In 2019, iProperty Management reported there are over 26 million IoT connected devices in the United States [1]. These devices are integrated in our daily lives, such as in smart homes. A smart home is composed of IoT devices and appliances that operate in a home environment.

Currently, there are no security standards developed for IoT devices. As a result, security vulnerabilities are exposed during the usage, which makes IoT security threats not well understood or studied. Vulnerability studies are conducted to uncover the ways in which IoT devices can undergo attacks. It is important for vulnerability studies to be well-rounded when covering all aspects of attack vectors. However, the majority of the studies conducted target well-known IoT devices manufactured by Amazon, Google and alike.

Due to well-known IoT vendors undergoing more scrutiny with regards to security in their products, they may show strong security postures. However, the security postures of lesser-known vendors are rarely studied, and they may lax on their security practices. In this vein, we conduct two studies to test these two claims: (i) most vulnerability studies target well-known devices and vendors, and (ii) lesser-known devices may have weaker security postures in comparison to well-known vendors. In the first study, we review prior vulnerability studies conducted on smart home devices as well as the uncovered vulnerabilities. The second study is divided into two parts and focuses on two IoT vendors of different types of devices and four IoT vendors of the same type of device. Each vendor is classified into well-known or lesser-known. Both studies were performed to compare the security mechanisms of the smart home IoT devices.

Our contributions are as follows.

- A comprehensive review of known vulnerability studies of smart home devices
- A process of conducting vulnerability analysis in IoT devices
- A review on vulnerability repositories – Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database (NVD)
- A comparative study on security postures of lesser-known vendors (e.g., Leeo and Feit Electric) and well-known vendor (e.g., Google and Philips Hue)

The remainder of this paper is organized as follows. Section II outlines IoT devices in smart home environments. Section III presents background and related work on security vulnerabilities in IoT and smart home environments. This section also includes our evaluation of IoT vulnerability studies, recommendations to IoT vendors and the limitation of this research study. Section IV presents study approach and a discussion on vulnerability status of well-known versus lesser-known vendors. Lastly, Section V summarizes our contributions and offers recommendations for future work.

II. Overview of Smart Home Environments

One of the largest markets for IoT devices is the smart home market. Globally, there are more than 120 new IoT devices that make a connection to the Internet per second [2]. In the United States, each person averages 8 connected devices per household and that number is projected to increase to 13.6 by 2022 [3]. Smart home devices consist of a wide range of devices from cameras to voice assistants to thermostats to

Manuscript received October 30, 2019; revised February 21, 2020; accepted March 22, 2020. Date of publication; date of current version. This work was supported in part partially by the U. S. Government, including the National Science Foundation Scholarship for Service under the award number DUE-1662469 and partially by the U. S. Department of Education under the Title III Historically Black Graduate Institutions (HBGI) grant. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U. S. Government. The U. S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright annotation therein.

B. D. Davis, J. C. Mason, and M. Anwar are with the Department of Computer Science, North Carolina A&T State University, Greensboro, NC, USA 27411 (e-mail: bddavis2@aggies.ncat.edu, jcmason@aggies.ncat.edu, manwar@ncat.edu).

Digital Object Identifier: 10.1109/JIOT.2020.2983983

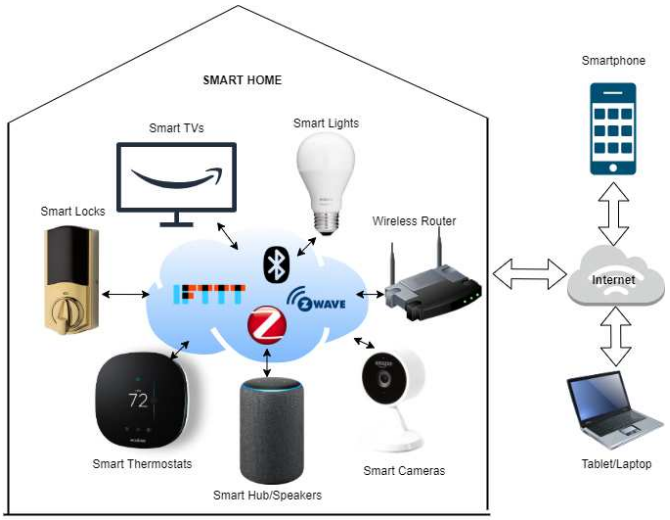

Fig. 1. An example of a smart home environment.

lights. The connectivity of the IoT devices and the services they provide create smart home environments. For example, consider a scenario of a family where the parents are watching their children after school while they are at work. Amazon's smart home products, e.g., Amazon Cloud Cam, Amazon Key (with lock), Amazon Echo (with Alexa voice assistant) and Amazon FireTV, are used to accomplish this. The parents would use the cameras and smart lock to let the kids in the house. The kids could turn on the lights and TV using the voice assistant while the parents monitor the kids' activities and set parental controls on their smartphones. The automation of these commands, tasks and services, through the assistance of connected smart IoT devices, provide ease and comfort for homeowners. Fig. 1 is an example smart home environment architecture.

Table I lists a set of popular smart home devices by utility category [4-7]. With the global smart home market projected to exceed 40 billion by 2020 [8], the manufacturers and vendors of these devices are under pressure to win the market, and a strong security posture may not be their priority.

TABLE I
HOME IOT DEVICES PER UTILITY CATEGORY

Utility Categories	Popular Devices
Smart Security Cameras	Amazon Cloud Cam, NetGear Arlo Q, Nest Cam IQ, Wyze Cam Pan
Doorbell Cameras	Google Nest Hello, Ring Video Doorbell, Arlo Audio Doorbell
Smart Locks	Kwikset with Amazon Key, August Smart Lock Pro
Smart Speakers	Amazon Echo, Google Home Max, Apple's HomePod
Smart Hubs	Wink Hub 2, Samsung SmartThings Hub, Google Wifi
Smart Light Bulbs	Philips Hue, GE C-Life Smart Bulbs
Smart Thermostats	Nest Thermostat E, Ecobee4 SmartThermostat
Smart Switches	TP-Link HS200 Smart Wi-Fi Light Switch
Smart Security Systems	SimpleSafe, Ring
Smart Plugs	Belkin WeMo Insight Smart Plug, TP-Link Kasa Smart Wi-Fi Plug, Amazon Smart Plug
Smart Smoke Detectors	Google Nest Protect, Ring Alarm
Smart Appliances	LG Signature Series Refrigerator, Samsung Electric Cooktop, LG TurboSteam Washer and Dryer
Smart Vacuums	iRobot Roomba, Shark IQ Robot, ECOVACS DEEBOT

The most prevalent utility categories based on market shares and sale volumes [4-7].

III. VULNERABILITY STUDIES OF SMART HOME DEVICES

A. Literature Review

There have been some research efforts to investigate vulnerabilities in IoT devices in a smart home environment, where security challenges are discussed and attack classifications are presented. The work of [9] classifies attacks into four distinct categories – physical, network, software, and encryption. This form of classification of attacks provides a broader perspective on how to observe vulnerabilities.

1) Physical: In the physical attacks category, hardware of an IoT device/system undergoes an attack. The attacker needs to obtain physical access to the device/system to conduct such an attack. Some physical attacks are as follows: node tampering, Radio Frequency (RF) Interference on Radio Frequency IDentifiers (RFIDs), node jamming in wireless sensor networks, malicious node injection, physical damage, social engineering, sleep deprivation, and malicious code injection [9].

2) Network: Network attacks are categorized based on attacks that are launched on the IoT network. In this type of attack, it is not essential for the attacker to be in close proximity of the IoT system to conduct the attack. The network attacks identified in [9] are traffic analysis, RFID spoofing/cloning/unauthorized access, sinkhole, man-in-the-middle, denial of service, routing information, and sybil.

3) Software: Software attacks, sometimes called firmware attacks, exploit vulnerabilities that exist in the software of IoT systems through malicious software, such as worms, viruses, etc.

Some of the software attacks that have been presented in [9] are phishing, malicious scripts, Trojan horse, spyware, adware, and denial of service that exploit buffer overflows, SQL injections and other types of vulnerabilities. These software vulnerabilities may exist at different layers within the smart home architectures: individual device, control hub, and cloud services. At an individual device level, a software vulnerability is catered to a specific device only. At a control hub level, a software vulnerability affects a control hub like Samsung's SmartThings which potentially affects all the devices connected to that hub. A vulnerability in cloud service software not only affects the smart devices connected to the cloud service, but it also affects everything connected to that cloud service.

4) Encryption: The last category of attacks we will consider in this research is encryption. Encryption attacks take place when an attacker breaks the encryption mechanism that is used in an IoT system. In [10], the authors investigate encryption vulnerabilities on IoT devices. Because IoT devices

TABLE II
EVALUATION OF KNOWN VULNERABILITY STUDIES OF SMART HOME DEVICES

Utility Categories	Physical	Network	Software	Encryption	Specific Devices	Study Source
Smart Security Cameras	No Studies Found	Man-in-the-Middle attacks	Cross-site request forgery Cross-site scripting Hard-coded credentials	Information disclosure Hard-coded credentials Man-in-the-Middle attacks Unprotected communication	TRENDnet IP-connected camera AvTech camera CCTV camera	[39-42, 61]
Smart Light Bulbs	No Studies Found	Man-in-the-Middle attacks	No required authentication	Unprotected communication No required authentication Man-in-the-Middle attacks	Philips Hue smart light bulbs JB Smart Bulb Hao Deng Smart Bulb TP-Link Smart LED Light Bulb	[36, 40, 43-48, 50]
Smart Thermostat	Exposed access Board level exploitation Chip level exploitation	Deduce Wi-Fi network passwords	Exposed cross device access Information disclosure USB booting capability	Deduce Wi-Fi network passwords USB booting capability	Google Nest Thermostat Nest Learning Thermostat - 2nd Generation (T200577) Honeywell 7 Day Programmable Wi-Fi Thermostat (RTH6580WF)	[40, 51-55]

The Physical, Network, Software, and Encryption criteria columns displays the number of vulnerability findings within research studies for each utility category.

have limited computing power to support strong cryptographic protocols, they are vulnerable to side channel, cryptanalysis, and man-in-the-middle attacks [9].

B. Survey of Vulnerability Studies

Table II presents the evaluation of research studies based on the aforementioned four IoT security vulnerability categories, i.e., physical, network, software, and encryption. We conducted our evaluation on vulnerability studies by searching literature for research studies with security vulnerabilities as the topic. Keywords used in searches included types of utility categories, types of specific smart home devices, vulnerability categories, IoT manufacturers, types of attacks and more. Our literature search covered multiple sources (e.g., Google Scholar and IEEE) and disciplines. Our criteria for searches are as follows.

- Find at least five publications on each utility category from Table I.
- Search the Google Scholar database first. If five papers were not found per utility category in Google Scholar, other databases were searched. The other databases we used were IEEE, ACM, ScienceDirect and SpringerLink.
- Select papers between 2010 to 2019.
- Search keywords following certain patterns: each utility category + "vulnerability" (e.g., "smart security cameras vulnerability"), each vulnerability classification + "in smart homes" (e.g., "network vulnerability in smart homes"), and a specific device + "vulnerability" ("Google Home Mini vulnerability").

We reviewed each publication to see what types of vulnerabilities were found in specific device(s), if any. The type of vulnerability attacks found in each utility category within the studies were added in Table II, and if no study was found for an attack type, "No Studies Found" was put in the table for that criterion. The source of every vulnerability study was documented in the last column. We repeated each step for every utility category.

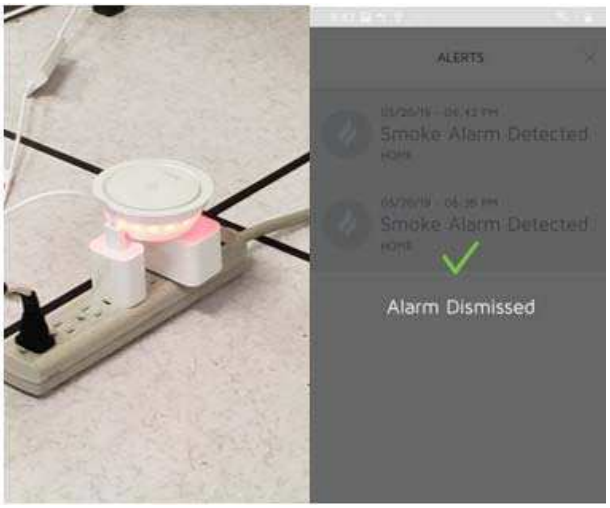

Fig. 2. Leeo Smart Alert shows smoke alarm is detected still after alarm was dismissed. The beginning of the denial of service (DoS).

Our review of known vulnerability studies of smart home devices listed in Table II, provided a broad evaluation of current research under the four IoT security vulnerability categories. The entire Table II is included in the Appendix (http://anwar.ncat.edu/recent-publications/technical-report/vulnerability-studies-of-SHD.pdf). We observe a gap in literature that prior studies are not comprehensive to cover the various types of IoT devices and vendors who create them.

1) *Limitations of Survey*

Our survey was limited to research publications we reviewed. Many security researchers may have posted their vulnerability

TABLE III

MISUSE AND ABUSE CASE FOR LEEO SMART ALERT AND GOOGLE HOME MINI

Cases	Leeo Smart Alert™	Google Home Mini
Misuse Case	*Misuse Case Name:* Obtain Leeo Account Credentials (Authenticate User) *Actor:* Adversary *Goal:* Adversary obtains and later misuses user's password for the Leeo app by intercepting messages sent through a compromised network host during user's log on *Preconditions:* 1) User/Admin has a registered account. *Basic Path:* 1) Adversary hacks Leeo network between client app and Leeo servers 2) Install some IP packet sniffer 3) Intercept messages sent that has strings like username, usrnm, logon, passwd, password, etc. 4) Adversary collects possible usernames and passwords along with IP addresses 5) The uses compiled list to gain access to the systems functionality *Alternative Paths:* 1) Adversary intercepts messages using the user's smartphone 2) Adversary has access to network and hacking is not required *Capture Points:* 1) Communication interception is not possible due to encryption or the like 2) The password does not work because it is for a different account or IP address 3) The password does not work because the password was changed *Extension Points:* 1) Includes misuse case " Intercept network"	*Misuse Case Name:* Accidental Triggering (Similar sounding trigger words) *Actor:* Something that executes natural language, e.g., friend, parrot, TV, adversary *Goal:* Actor voices trigger word or similar sounding to activate the system without consent of system owner *Preconditions:* 1) Google Home Mini is setup properly and connected to a reliable Wi-Fi *Basic Path:* 1) Actor speaks trigger phrase “Hey Google” a) Optionally, the actor speaks trigger phrase “Okay Google” 2) Google Home Mini acknowledges phrase by lighting up 3) Actor voices language *Alternative Paths:* 1) Adversary voices malicious command to gain access to sensitive information *Capture Points:* 1) Google Home Mini completes command 2) Google Home states “Sorry, I am not sure how to help with that yet” 3) Google Home states nothing
Abuse Case	*Associated Use Case/Functionality:* Authenticate User *Abuse Case Name:* Attacker bypasses the authentication system for the Leeo App *Attack Pattern Name and ID:* Authentication Bypass, 115 *Abuse Case Objective:* An attacker gains access to Leeo app with privileges of an authorized user by bypassing the authentication system. *Precondition/Prerequisite:* An authentication mechanism that uses forms of authentication *Resources:* A client application or a scripting language *Flow of Events:* The system flow of events is: a) Targeted system displays content b) Attacker enters content through known application page c) Attacker gains access to content avoiding the authentication step *Post Condition:* The attacker has access to protected data without being authenticated *Solution & Mitigation Recommendation:* Design and implement proper checkpoints for the authentication system of the Leeo app.	*Associated Use Case/Functionality:* Give Voice Command *Abuse Case Name:* Attacker elicits information about owner *Attack Pattern Name and ID:* Information Elicitation, 410 *Abuse Case Objective:* The attacker maliciously elicits information that will execute the system in an unintended manner maintained by the target system in user-accessible locations. *Precondition/Prerequisite:* The system preconditions are: a) Target system is user-accessible b) Information is maintained in target system’s storage areas *Resources:* The attacker needs a tool capable of playing/stating custom inputs for the attack *Flow of Events:* The system flow of events are: a) Attacker determines the state of the target system b) The attacker commands target system for contents and observes the effects c) The attacker can violate the owner’s privacy in order to perform illegitimate actions after determining the information stored in the target system’s storage areas *Post Condition:* Attacker can get access to sensitive information *Solution & Mitigation:* The system mitigations are: a) Avoid sensitive information in user-accessible systems b) Do not rely on user-accessible systems to maintain integrity and confidentiality c) Ensure confidentiality and integrity with any sensitive information that is part of the user state with encryption or some other form of security

This table contains one misuse and abuse case of devices from Leeo and Google.

studies via blog, forum and various other forms of media. Even though our evaluation is not fully exhaustive, but our survey adequately supports our claims.

The surveyed literature does not compare specifically well-known vendors versus lesser-known vendors by their found vulnerabilities. That claim was explored in the next study. Likewise, the survey did not provide information to determine

if security postures vary between well-known and lesser-known devices and vendors. These knowledge gaps were explored in Section IV.

IV. Vulnerability Studies

To explore our second claim whether a lesser-known vendor is likely to have a weaker security posture compared to a well-known vendor, we conducted two vulnerability studies with IoT devices from two vendors of different utility categories and four vendors from the same utility category, smart lighting.

A. Vulnerability Study I: Leeo and Google

The first vulnerability study involved vendors 'Leeo' and 'Google'. Leeo Inc. is a lesser-known technology company that has developed and produced a Leeo Ping Service as well as a Leeo Smart Alert™ [11]. The Leeo Smart Alert™ is a fire and flood prevention alert system that notifies the user if a smoke, carbon monoxide or water alarm is activated in the user's home [11]. The alert system also calls the user's emergency contact list for backup if the user is not reachable, which is the Leeo Ping Service. The Leeo Smart Alert™ also works as a night light with the capability to change the lighting hue.

Google LLC is a large well-known technology corporation that has a strong presence in multiple countries. There are various products Google is known for, which include cloud computing, Internet analytics, IoT devices, etc. [12]. In this research study, we use the Google Home Mini, a voice-controlled speaker that was created by Google. It is a miniaturized version of the Google Home. Some of the functionalities of the Google Home Mini consist of operating as a smart speaker, which is able to receive and respond to vocal commands by the user, control smart home devices, and more [12].

1) Approach: We followed the software engineering methods of use case, misuse case and abuse case modeling to define and model the security vulnerabilities of Leeo Smart Alert™ and Google Home Mini. Use cases are a design component of Unified Modeling Language (UML) and is typically described in a use case diagram [13, 14]. Misuse and abuse cases have been used interchangeably, but they differ in implementation. The misuse case concept is not a widely adopted modeling technique outside of the research community [15]. The originators of the misuse case defined misuse cases as the inverse of use cases [13, 16], while [17] defined misuse cases as use cases with hostile intent. Abuse cases are associated with a use case but are defined by security threats [18-20] or attack patterns [21].

With this approach, we constructed use cases according to the smart device functionality and assumptions of interconnectivity defined by the manufacturer. Misuse cases were defined with the same tactic. The attack pattern method was used to define the abuse cases. Attack patterns for abuse cases was searched using MITRE's Common Attack Pattern Enumeration and Classifications (CAPEC) database [22]. We labeled each misuse and abuse case with a vulnerability criterion based on the type of attack: physical, network, software or encryption. After the use, misuse, and abuse cases were modeled for each device, we applied the misuse and abuse cases on each device. If the attack was successful, we considered the attack as a viable vulnerability for that device. We searched each vulnerability in both vulnerability repositories, CVE by MITRE and NVD by NIST [23, 24] and noted if the vulnerability was described or not. Lastly, we discussed our findings and the overall vulnerability analysis includes use, misuse and abuse cases.

2) Misuse, and Abuse Cases of Leeo Smart Alert and Google Home Mini: Table III describes one misuse and one abuse case of the Leeo Smart Alert™ and Google Home Mini. Other misuse cases tested, not shown in Table III, were account lockout, retrieving sensitive data and manipulating system state. Abuse cases White Box Reverse Engineering (CAPEC-167), Session Hijacking (CAPEC-593), Sniff Application Code (CAPEC-65), and Inducing Account Lockout (CAPEC-2) were tested for the Leeo Smart Alert™ and Manipulating User State (CAPEC-74) and Retrieve Embedded Sensitive Data (CAPEC-37) were tested for the Google Home Mini [22]. The misuse and abuse cases provide a definition of the vulnerabilities and understanding of the impact of those vulnerabilities to the users and vendors. With the misuse cases, we perform penetration testing to evaluate the smart home devices from the perspective of an attacker.

3) Results: Table IV contains the results of our vulnerability study of devices from both well-known and lesser-known companies, which are the Leeo Smart Alert™ and the Google Home Mini. The table presents vulnerabilities that are applicable to the four categories of vulnerabilities - physical, network, software, and encryption, as they relate to the respective device.

4) Discussion: As of now, Leeo has not provided an update to consumers regarding the *Krack* vulnerability. Leeo's physical vulnerabilities, Smart Plug Connection and Extension Connection, create radio frequency interference, which causes a communication interruption between the Leeo Smart Alert™ and Leeo mobile application. During the experiment with the Leeo Smart Alert™ and the Leeo mobile application, we experienced denial of service with both entities. We triggered a false alarm, which was detected by the Leeo Smart Alert™ device and in the Leeo mobile application as shown in Fig. 2. Afterwards, the alarm was acknowledged in the Leeo mobile application; however, the Leeo Smart Alert™ device continued in alert mode as though the alarm was still going off like it had not been acknowledged in the Leeo mobile application. As a result, neither the Leeo mobile application nor the Leeo Smart Alert™ device were any longer communicating with each other, which caused a disruption in service. No vulnerabilities have been identified regarding the vendor Leeo in the CVE and NVD databases at the time of this study.

The vulnerabilities presented in Table IV for Google Home Mini were discovered in 2017. However, the version of the Google Home Mini that we are using in this study, these vulnerabilities have been patched. According to reference [25], the guidance provided in the documentation indicates to configure the Google Home Mini to auto-update, which

TABLE IV
VULNERABILITIES FOUND IN LEEO SMART ALERT VERSUS GOOGLE HOME MINI

Devices	Physical Vulnerability	Network Vulnerability	Software Vulnerability	Encryption Vulnerability
Leeo Smart Alert™	Smart Plug Connection Extension Connection	Krack	Denial of Service	No current vulnerabilities found
Google Home Mini	No current vulnerabilities found	No current vulnerabilities found	Adversarial System Triggering	No current vulnerabilities found

Vulnerability attacks categorized in four categories of vulnerabilities: Physical, Network, Software, and Encryption. No current vulnerabilities found in a category was noted as such.

TABLE V
VULNERABILITIES FOUND IN SMART LIGHTING UTILITY CATEGORY

Devices	Physical Vulnerability	Network Vulnerability	Software Vulnerability	Encryption Vulnerability
Philips Hue Smart Lighting	Motherboard Hack	Replay Attack DNSSEC DNS Spoofing Fake Server	"Keeps track of secret keys" Fake Server	Man-in-the-Middle attacks Unprotected communication (e.g., HTTP commands)
GE C-Life Smart Bulbs	Motherboard Hack	No Current Vulnerabilities Found	Unreliable Hub Linking	No Current Vulnerabilities Found
Feit Electric Party Bulbs	No Current Vulnerabilities Found	Not Applicable	Not Applicable	Not Applicable
HaoDeng Smart Bulbs	Motherboard Hack	Unencrypted communication	Buffer Overflow attack	Unprotected communication Information Disclosure

Vulnerability attacks categorized in four categories of vulnerabilities: Physical, Network, Software, and Encryption. No current vulnerabilities found in a category was noted as such, as well as, if a category is not applicable to the device.

enables the security patches to be implemented automatically. If auto-update is not configured for the Google Home Mini, it is possible for vulnerabilities to exist on the smart speaker device. The CVE and NVD searches yielded some vulnerabilities like Cross-site scripting (XSS) and directory traversal for the Google Home Mini, but those vulnerabilities have since been patched. Additional security best practices are provided in [26]. Even though security updates are provided for the Google Home Mini, the adversarial system triggering study conducted with misuse case #1 and abuse case #1 in Table III are still relevant security concerns due to voice recognition and Natural Language Processing (NLP) configured for the device.

B. Vulnerability Study II

The first vulnerability study between two distinct devices seemed viable towards our claim but scientifically, we need more evidence to support our claim. Therefore, we investigate four devices of the same utility category, smart lighting. We conducted a second vulnerability study that followed the same approach and process as the first. The additional vulnerability studies we conducted on smart IoT devices, specifically smart lighting, have been developed by both well-known and lesser-known companies. The two well-known companies we consider for this research are Philips Lighting and General Electric (GE). Philips Lighting is the maker of Philips Hue smart bulbs, (the new company name is Signify) [26]. The most basic functionality provided through Philips Hue smart lights is the ability to control the lighting in a location with the use of your smartphone, through voice commands and/or scheduling [27]. Some additional Philips Lighting products are Philips Hue Bridge, Philips Hue Dimmer Switch, and various types of Hue lamps and light bulbs [27]. Another smart bulb company is GE, which produces GE C-Life Smart Bulbs [28]. Configuring the GE C-Life Smart Bulb is very simple through the use of the Google Home application. GE produces some additional products such as GE C-Reach hub, GE Smart Switches, etc. [28, 29].

The two lesser-known smart lighting bulbs that we assess in our research are the Feit Electric Company, Inc. and HaoDeng. The Feit Electric Company, Inc. is a lighting company driven to deliver the latest breakthrough interior and exterior illumination [30]. The Feit Electric Company produces several smart bulbs. We assess the Feit Electric LED Party Bulb where one can manually switch through the 16 color choices and consists of four color rotation modes [31]. The second light bulb we consider is the HaoDeng Bluetooth Mesh LED Light bulb. It is mostly available via the Amazon website. HaoDeng is controlled by an app that can serve a maximum of 64 light sources and control 16 million colors [32]. According to [32], the lamps have the ability to communicate with each other automatically, where it appears as though they built their own LAN.

1) Results: Table V contains the results of our vulnerability study of the smart lighting devices from well-known and lesser-known companies. It presents vulnerabilities that are applicable to the four categories - physical, network, software, and encryption, as they relate to the respective device. Fig. 3 provides a depiction of the smart lighting setup and architecture that is used in the study.

2) Discussion: Well-known vendors are more liable to state their patch notes. There is a website of release notes

for the Philips Hue Bridge V2 that updates users to security patches of firmwares that coincides with CVEs and NVDs for the device. All CVE and NVD vulnerabilities for the smart lighting Philips Hue and GE can be found in these databases and at http://anwar.ncat.edu/recent-publications/technical-report/CVE_NVD-Results.pdf. In 2016, researchers identified a remotely accessible vulnerability with the Philips Hue bulbs, which was patched prior to public knowledge [33].

The GE C-Life Smart Bulb connects to the Google Home Mini, where there are no current vulnerabilities that exist in the CVE and NVD databases for these devices. The main vulnerability that exists is the "Motherboard Hack" vulnerability. The "Motherboard Hack" is an attack where the bulb is cracked open gaining access to the motherboard within the smart light bulb. Some manufactures store unencrypted information, e.g., WiFi SSID and encryption key in plaintext, in this location [34]. See Table V to see where this attack exists in the smart bulbs.

The Feit Electric smart bulbs are not susceptible to network, software, and encryption vulnerabilities because the bulb's connectivity to the remote does not rely on WiFi technology.

HaoDeng does not have many vulnerabilities but we could not find if the vulnerabilities they do contain like buffer overflow were patched.

V. Conclusion

The vulnerability studies of IoT devices to date are not all-inclusive and, in some cases, target well-known vendors or devices. Our studies showcased that physical, network, software and/or encryption attacks are viable for several IoT devices. Our searches in both Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database (NVD) repositories revealed that IoT devices from lesser-known vendors were not studied. Therefore, these vendors may not show strong security posture.

Our experiments seem to indicate that well-known vendors/devices have stronger security postures, whereas lesser-known manufactures/devices have a weaker security posture. These claims are also supported through our vulnerability findings in Table IV and more so, in Table V.

We recommend that the national vulnerability repositories and the research community expand their studies to lesser-known IoT device vendors. Overall, the security requirements of devices must be standardized along the utility categories and attack dimensions, i.e., physical, network, software, and encryption. Consequently, our future work will aim at conducting a more extensive vulnerability study in a fully equipped smart home environment, inclusive of devices from lesser-known vendors.

Appendix

Table VI provides a full list of Table II [35-94] and is located at http://anwar.ncat.edu/recent-publications/technical-report/vulnerability-studies-of-SHD.pdf.

References

[1] J. Bustamante, "2019 IoT Statistics: Number of Enabled Devices & Industry Growth," 2019.

[2] (2019). *McKinsey Global Institute*. Available: https://www.mckinsey.com/mgi/overview

[3] (2019). *IoT Has Quietly and Quickly Changed Our Lives | NCTA — — — The Internet & Television Association*. Available: https://www.ncta.com/whats-new/iot-has-quietly-and-quickly-changed-our-lives

[4] (2017). *7 Wi-Fi Enabled Smart Appliances for a Smarter Home*. Available: https://www.ajmadison.com/learn/7-wi-fi-enabled-smart-appliances-for-a-smarter-home/

[5] (2018). *10 Best Smart Home Devices - 42 West, the Adorama Learning Center*. Available: https://www.adorama.com/alc/10-best-smart-home-devices

[6] C. d. Looper. (2019). *Best smart home devices 2019: get comfy with smart lighting, heating and more*. Available: https://www.techradar.com/news/smart-home-devices

[7] A. Colon and E. Griffith, "The Best Smart Home Devices for 2019," 2019.

[8] (2019). *Smart Home Statistics | National Council For Home Safety and Security*. Available: https://www.alarms.org/smart-home-statistics/

[9] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, 2015, pp. 180-187.

[10] L. Costa, J. Barros, and M. Tavares, "Vulnerabilities in IoT Devices for Smart Home Environment," presented at the 2019 5th International Conference on Information Systems Security and Privacy (ICISSP), 2019.

[11] (2019). *Leeo | About Us*. Available: https://www.leeo.com/about-us

[12] (2019). *Google Home*. Available: https://store.google.com/gb/product/google_home

[13] G. Sindre and A. L. Opdahl, "Capturing security requirements through misuse cases," *NIK 2001, Norsk Informatikkonferanse 2001, http://www.nik. no/2001,* 2001.

[14] T. Srivatanakul, J. Clark, and F. Polack, "Writing Effective Security Abuse Cases," 01/01 2004.

[15] J. J. Pauli and D. Xu, "Misuse case-based design and analysis of secure software architecture," in *International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II*, 2005, vol. 2, pp. 398-403: IEEE.

[16] G. Sindre and A. L. Opdahl, "Templates for misuse case description," in *Proceedings of the 7th International Workshop on Requirements Engineering, Foundation for Software Quality (REFSQ'2001), Switzerland*, 2001: Citeseer.

[17] I. Alexander, "Initial industrial experience of misuse cases in trade-off analysis," in *Proceedings IEEE Joint International Conference on Requirements Engineering*, 2002, pp. 61-68.

[18] C. Heitzenrater and A. Simpson, "Misuse, Abuse and Reuse: Economic Utility Functions for Characterising Security Requirements," presented at the 2016 11th International Conference on Availability, Reliability and Security (ARES), 2016.

[19] J. McDermott and C. Fox, "Using abuse case models for security requirements analysis," in *Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99)*, 1999, pp. 55-64.

[20] sw_integrity. (2016). *Abuse cases: How to think like a hacker | Synopsys*. Available: https://www.synopsys.com/blogs/software-security/abuse-cases/

[21] I. Williams, X. Yuan, J. Todd McDonald, and M. Anwar, "A Method for Developing Abuse Cases and Its Evaluation," *Journal of Software,* vol. 11, no. 5, pp. 520-527, 2016.

[22] CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC) [Online]. Available: https://capec.mitre.org/index.html

[23] CVE - Common Vulnerabilities and Exposures (CVE) [Online]. Available: https://cve.mitre.org/index.html

[24] NVD - Home [Online]. Available: https://nvd.nist.gov/

[25] @symantec, "Everything You Need to Know About the Security of Voice-Activated Smart Speakers," 2019.

[26] Hillary, "Signify is the new company name of Philips Lighting, the maker of Hue smart bulbs," 2018-03-16 2018.

[27] R. Crist, "The complete guide to Philips Hue," 2020.

[28] (2020). *Innovative Smart Home Products | C by GE*. Available: https://www.cbyge.com

[29] C. Davenport, "Review: The GE C-Life is an affordable smart light bulb perfect for Google Home, no Wi-Fi necessary," 2019-02-08 2019.

[30] FeitElectricInc, "About Us - Feit Electric," 2020.

[31] FeitElectricInc, "Remote Control Color Changing LED - Feit Electric," 2020.

[32] "HaoDeng," 2020.

[33] R. Crist, "New study details a security flaw with Philips Hue smart bulbs," 2020.

[34] T. Nardi, "Don't Toss That Bulb, It Knows Your Password," ed, 2019.

[35] E. Kim, M. B. Jensen, D. Poreh, and A. M. Agogino, "Novice Designer's Lack of Awareness to Cybersecurity and Data Vulnerability in New Concept Development of Mobile Sensing Devices," presented at the Proceedings of the DESIGN 2018 15th International Design Conference, 2018.

[36] D. Dreyer, "IoT Security Overview and Attacks," 2018.

[37] R. M. Ogunnaike, "Vulnerability detection and resolution in Internet of Things (IoT) devices," 2017.

[38] D. N. Serpanos and A. Papalambrou, "Security and privacy in distributed smart cameras," *Proceedings of the IEEE,* vol. 96, no. 10, pp. 1678-1687, 2008.

[39] Y. Seralathan *et al.*, "IoT security vulnerability: A case study of a Web camera," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, 2018, pp. 172-177: IEEE.

[40] V. Sivaraman, H. H. Gharakheili, C. Fernandes, N. Clark, and T. Karliychuk, "Smart IoT devices in the home: Security and privacy implications," *IEEE Technology and Society Magazine,* vol. 37, no. 2, pp. 71-79, 2018.

[41] A. Sivanathan, D. Sherratt, H. H. Gharakheili, V. Sivaraman, and A. Vishwanath, "Low-cost flow-based security solutions for smart-home IoT devices," in *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2016, pp. 1-6: IEEE.

[42] J. Bugeja, D. Jönsson, and A. Jacobsson, "An Investigation of Vulnerabilities in Smart Connected Cameras," in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2018, pp. 537-542: IEEE.

[43] M. B. Barcena and C. Wueest, "Insecurity in the Internet of Things," *Security response, symantec,* p. 20, 2015.

[44] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow," in *2016 11th International conference on availability, reliability and security (ARES)*, 2016, pp. 147-156: IEEE.

[45] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home IoT devices," in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015, pp. 163-167: IEEE.

[46] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "IoT goes nuclear: Creating a ZigBee chain reaction," in *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 195-212: IEEE.

[47] M. Wang, J. Santillan, and F. Kuipers, "ThingPot: an interactive Internet-of-Things honeypot," *arXiv preprint arXiv:1807.04114,* 2018.

[48] N. Dhanjani, "Hacking lightbulbs: Security evaluation of the philips hue personal wireless lighting system," *Internet of Things Security Evaluation Series,* 2013.

[49] M. Markovic *et al.*, "Towards automated privacy risk assessments in IoT systems," in *Proceedings of the 5th Workshop on Middleware and Applications for the Internet of Things*, 2018, pp. 15-18.

[50] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, "An experimental study of security and privacy risks with emerging household appliances," in *2014 IEEE conference on communications and network security*, 2014, pp. 79-84: IEEE.

[51] G. Hernandez, O. Arias, D. Buentello, and Y. Jin, "Smart nest thermostat: A smart spy in your home," *Black Hat USA,* pp. 1-8, 2014.

[52] C. Hunter, L. Moody, A. Luan, R. Nazerali, and G. K. Lee, "Superior gluteal artery perforator flap: the beauty of the buttock," *Annals of plastic surgery,* vol. 76, pp. S191-S195, 2016.

[53] O. Arias, K. Ly, and Y. Jin, "Security and privacy in IoT era," in *Smart Sensors at the IoT Frontier*: Springer, 2017, pp. 351-378.

[54] M. Burrough and J. Gill, "Smart thermostat security: turning up the heat," ed, 2015.

[55] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for internet of things using blockchain technology," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, 2018, pp. 769-773: IEEE.

[56] R. Baumann, K. M. Malik, A. Javed, A. Ball, B. Kujawa, and H. Malik, "Voice Spoofing Detection Corpus for Single and Multi-order Audio Replays," *arXiv preprint arXiv:1909.00935,* 2019.

[57] C. Champion, I. Olade, C. Papangelis, H. Liang, and C. Fleming, "The Smart ^{2} Speaker Blocker: An Open-Source Privacy Filter for Connected Home Speakers," *arXiv preprint arXiv:1901.04879,* 2019.

[58] E. Kim, M. B. Jensen, D. Poreh, and A. M. Agogino, "Novice designer's lack of awareness to cybersecurity and data vulnerability in new concept development of mobile sensing devices," in *DS 92: Proceedings of the DESIGN 2018 15th International Design Conference*, 2018, pp. 2035-2044.

[59] Y. Gong and C. Poellabauer, "An overview of vulnerabilities of voice controlled systems," *arXiv preprint arXiv:1803.09156,* 2018.

[60] H. Chung, M. Iorga, J. Voas, and S. Lee, "Alexa, can I trust you?," *Computer,* vol. 50, no. 9, pp. 100-104, 2017.

[61] N. Apthorpe, D. Reisman, and N. Feamster, "A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic," *arXiv preprint arXiv:1705.06805,* 2017.

[62] B. Visan, J. Lee, B. Yang, A. H. Smith, and E. T. Matson, "Vulnerabilities in hub architecture IoT devices," in *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2017, pp. 83-88: IEEE.

[63] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2017, pp. 1292-1297: IEEE.

[64] D. Mauro Junior, L. Melo, H. Lu, M. d'Amorim, and A. Prakash, "A Study of Vulnerability Analysis of Popular Smart Devices Through Their Companion Apps," in *2019 IEEE Security and Privacy Workshops (SPW)–SafeThings Workshop*, 2019.

[65] C. Chhetri and V. G. Motti, "Eliciting privacy concerns for smart home devices from a user centered perspective," in *International Conference on Information*, 2019, pp. 91-101: Springer.

[66] A. K. Simpson, F. Roesner, and T. Kohno, "Securing vulnerable home IoT devices with an in-hub security manager," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017, pp. 551-556: IEEE.

[67] B. Ali and A. I. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," *Sensors (Basel),* vol. 18, no. 3, Mar 8 2018.

[68] A. Amokrane, "Internet of things: security issues, challenges and directions," *C&ESAR 2016,* p. 70, 2016.

[69] B. Copos, K. Levitt, M. Bishop, and J. Rowe, "Is anybody home? Inferring activity from smart home network traffic," in *2016 IEEE Security and Privacy Workshops (SPW)*, 2016, pp. 245-251: IEEE.

[70] M. Daniel, "Hidden dangers of Internet of Things," in *Women in Security*: Springer, 2018, pp. 69-75.

[71] M. W. Denko, "A Privacy Vulnerability in Smart Home IoT Devices," 2017.

[72] R. Egert, T. Grube, D. Born, and M. Mühlhäuser, "AVAIN-a Framework for Automated Vulnerability Indication for the IoT in IP-based Networks," in *2019 International Conference on Networked Systems (NetSys)*, 2019, pp. 1-3: IEEE.

[73] A. Gai, S. Azam, B. Shanmugam, M. Jonkman, and F. De Boer, "Categorisation of security threats for smart home appliances," in *2018 International Conference on Computer Communication and Informatics (ICCCI)*, 2018, pp. 1-5: IEEE.

[74] A. J. Hussain, D. M. Marcinonyte, F. I. Iqbal, H. Tawfik, T. Baker, and D. Al-Jumeily, "Smart home systems security," in *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2018, pp. 1422-1428: IEEE.

[75] Y. Jia, Y. Xiao, J. Yu, X. Cheng, Z. Liang, and Z. Wan, "A Novel Graph-based Mechanism for Identifying Traffic Vulnerabilities in Smart Home IoT," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, 2018, pp. 1493-1501.

[76] A. Larsson Forsberg and T. Olsson, "IoT Offensive Security Penetration Testing: Hacking a Smart Robot Vacuum Cleaner," ed, 2019.

[77] C. Lee, L. Zappaterra, K. Choi, and H.-A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in *2014 IEEE Conference on Communications and Network Security*, 2014, pp. 67-72: IEEE.

[78] X. Lei, G.-H. Tu, A. X. Liu, K. Ali, C.-Y. Li, and T. Xie, "The Insecurity of Home Digital Voice Assistants–Amazon Alexa as a Case Study," *arXiv preprint arXiv:1712.03327,* 2017.

[79] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of internet of things: A case study of the smart plug system," *IEEE Internet of Things Journal,* vol. 4, no. 6, pp. 1899-1909, 2017.

[80] H. Liu, T. Spink, and P. Patras, "Uncovering Security Vulnerabilities in the Belkin WeMo Home Automation Ecosystem," in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2019, pp. 894-899: IEEE.

[81] Z. A. Markel, "Designing networked objects to achieve reasonable security," Massachusetts Institute of Technology, 2017.

[82] D. Mauro Junior, L. Melo, H. Lu, M. d'Amorim, and A. Prakash, "A Study of Vulnerability Analysis of Popular Smart Devices Through Their Companion Apps," *Journal Name: 2019 IEEE Security and Privacy Workshops (SPW) – SafeThings Workshop; Journal Volume: null; Journal Issue: null; Conference: null; Patent File Date: null; Patent Priority Date: null; Other Information: null; Related Information: null,* p. Medium: X; Size: 181 to 186; Quantity: null; OS: null; Compatibility: null; Other: null, 2019.

[83] N. Redini *et al.*, "Bootstomp: on the security of bootloaders in mobile devices," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017, pp. 781-798.

[84] R. J. Robles, T.-h. Kim, D. Cook, and S. Das, "A review on security in smart home development," *International Journal of Advanced Science and Technology,* vol. 15, 2010.

[85] A. Rose and B. Ramsey, "Picking Bluetooth low energy locks from a quarter mile away," *DEF CON,* vol. 24, 2016.

[86] M. Schiefer, "Smart home definition and security threats," in *2015 ninth international conference on IT security incident management & IT forensics*, 2015, pp. 114-118: IEEE.

[87] F. Ullrich, J. Classen, J. Eger, and M. Hollick, "Vacuums in the cloud: analyzing security in a hardened IoT ecosystem," in *13th {USENIX} Workshop on Offensive Technologies ({WOOT} 19)*, 2019.

[88] A. Wang and S. Nirjon, "A False Sense of Home Security—Exposing the Vulnerability in Away Mode of Smart Plugs," in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2019, pp. 316-321: IEEE.

[89] T. Wang, M. Lei, J. Chen, S. Deng, and Y. Yang, "Dynamically-Enabled Defense Effectiveness Evaluation in Home Internet Based on Vulnerability Analysis," in *International Conference on Cloud Computing and Security*, 2017, pp. 805-815: Springer.

[90] M. Ye, N. Jiang, H. Yang, and Q. Yan, "Security analysis of Internet-of-Things: A case study of august smart lock," in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2017, pp. 499-504: IEEE.

[91] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*, 2015, pp. 1-7.

[92] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: Lessons for securing commodity internet of things devices," in *Proceedings of the 11th ACM on Asia conference on computer and communications security*, 2016, pp. 461-472.

[93] A. Said, A. Jama, F. Mahamud, J. Mohan, and P. Ranganathan, "Smart Home Vulnerabilities–A Survey," in *Proceedings of the International Conference on Embedded Systems, Cyber-physical Systems, and Applications (ESCS)*, 2018, pp. 83-87: The Steering Committee of The World Congress in Computer Science, Computer ….

[94] N. P. Hoang and D. Pishva, "A TOR-based anonymous communication approach to secure smart home appliances," in *2015 17th International Conference on Advanced Communication Technology (ICACT)*, 2015, pp. 517-525: IEEE.

Brittany D. Davis was born in Portsmouth, Virginia, USA. She received her B.S. (with a concentration in Business) and M.S. degrees in computer science from Virginia Commonwealth University in Richmond, Virginia, and Virginia State University in Petersburg, Virginia in 2014 and 2015, respectively.

She is currently pursuing her PhD degree in computer science with a concentration in cyber security and information technology at North Carolina A&T State University, Greensboro, North Carolina as a National Science Foundation (NSF) Cyber Defender Scholarship for Service (SFS) PhD Fellow. Her current research interests include cybersecurity, wireless sensor networks, Cyber-Physical Systems (CPS), Internet of Things (IoT), and natural language processing (NLP).

Janelle C. Mason was born in Charlottesville, Virginia, USA. She has received the B.S. degree in computer science from North Carolina Agricultural and Technical State University, Greensboro, North Carolina. Her M.S. degree was attained from North Carolina Agricultural and Technical State University, in computer science with two concentrations in information assurance and software engineering. Currently, she is pursuing her Ph.D. degree in computer science at North Carolina Agricultural and Technical State University, Greensboro, NC.

While pursuing her M.S., she was a National Science Foundation (NSF) Cyber Defender Scholarship for Service (SFS) Fellow. As a Ph.D. student, she is a Chancellor's Distinguished Title III Historically Black Graduate Institutions (HBGI) Fellow. Her research interest includes cybersecurity, biometrics, data science, machine learning, identity, Internet of Things (IoT), and multi-agent systems.

Mohd Anwar is an associate professor of computer science and a center director at North Carolina A&T State University. He is an interdisciplinary computer scientist with research expertise in two main areas: (1) cybersecurity and (2) smart and connected health. The former is focused on intrusion/malware detection, usable security, cyber identity and differential privacy, and the latter is focused on mHealth technology-based individual-level health monitoring and health service delivery as well as AI-powered, secondary data-driven (e.g., social media data) public health monitoring. Towards pursuing his research goals, he uses AI, Human-Computer Interaction (HCI), and Data Science techniques as well as apply theories from Social Sciences (e.g., Protection Motivation Theory, Theory of Planned Action, etc.) to design solutions. Dr. Anwar has more than 90 peer-reviewed publications, and his research has extensively been funded by NSF, DoD, Air Force, NSA, and NIH.