

Final Report

A Multidisciplinary Approach to Internet-of-Things (IoT) Cybersecurity Research to Develop the Research Capacity of ROTC Students

ONR Contract# N00014-20-1-2798

Developed by:

Meredith Carroll, Terrence O'Connor, Siddhartha Bhattacharyya, Maria Chaparro, Andrew Nakushian, Tricia Prior, Summer Rebensky, Daniel Campos, Jared Blanco, Dylan Jessie, Anubhav Gupta, Adolf D'Costa, Pearson Kerchner, Liam Avery Yu, and Chandler Hake

**Florida Institute of Technology
150 University Blvd.
Melbourne, FL 32901**

Technical Contact:
Dr. Meredith Carroll
Associate Professor
321-674-8374
mcarroll@fit.edu

Administrative Contact:
Ms. Carolyn Lockyer,
Director of Sponsored Programs
(321) 674-7490
clockyer@fit.edu

**Performance Period:
August 1, 2020 – July 31, 2021**

Submitted October 13, 2021

Table of Contents

Executive Summary	3
Introduction.....	4
Major Goals	5
Objectives and Approach	5
Objective 1. Research Approaches for Identifying IoT Privacy Violations	5
Objective 2. Research and Development of IoT Privacy and Security Policies.....	6
Objective 3. Human Use Experimentation and Design Recommendation Development	7
Objective 4. ROTC Student Mentoring, Training and Education	7
Objective 5. Coordination with Military STEM and Cybersecurity Stakeholders	8
Project Schedule and Milestones.....	9
Accomplishments.....	10
Objective 1: Research Approaches for Identifying IoT Privacy Violations	10
Task 1.1 Build a Robust Dataset of IoT Device Behaviors (e.g., analytics, video recording, lock state changes, firmware updates, motion reporting) for a Group of Widely Popular IoT Devices.....	10
Task 1.2 Develop a Methodology for Querying Vendor APIs to Systematically Apply Labels Against Encrypted Network Flows	14
Task 1.3 Construct a Publicly Accessible Framework for Querying The Dataset and Constructing Future Crowd-Sourced Datasets.....	18
Objective 2. Research and Development of IoT Privacy and Security Policies	24
Task 2.1 Ontological Representation of IoT Devices	24
Task 2.2 Extending the CSADL Framework to Integrate IoT Scenarios	40
Task 2.3 Modeling of Human Behavior	46
Task 2.4 Modeling and Analysis of the Composition of IOT and Human to Identify Security Policies.....	50
Objective 3. Human Use Experimentation and Design Recommendation Development.....	57
Tasks 3.1 Up front Analysis and Literature Review.....	57
Task 3.2 User Survey Research and Recommendations.....	67
Task 3.3 User Experimental Research and Results	76
Objective 4. ROTC Student Mentoring, Training and Education.....	95
Tricia Prior, ROTC Cadet Studying Forensic Psychology at Florida Tech.....	95
Jared Blanco, ROTC Cadet Studying Software Engineering at Florida Tech.....	96

Dylan Jesse, ROTC Cadet Studying Computer Science at Florida Tech	97
Pearson Kerchner, ROTC Cadet Studying Information Systems at Florida Tech.....	98
Liam Avery Yu, ROTC Cadet Studying Information Systems at Florida Tech.....	98
Chandler Hake, ROTC Cadet Studying Computer Science at Florida Tech	98
Objective 5. Coordination with Military STEM and Cybersecurity Stakeholders	99
DoD Stakeholder Presentations.....	99
US Army Combat Capabilities Development Command (DEVCOM)	99
US Army Cyber Command.....	100
Dissemination	100
Academic Conference Presentations and Proceedings.....	100
Refereed Journal Articles	101
Vulnerability Disclosures.....	101
Participants.....	102
References.....	103

Executive Summary

The Internet-of-Things (IoT) are rapidly becoming commonplace. The current 30.73 billion devices are predicted to grow to 75.44 billion by 2025. The ubiquitous reach of these devices has extended to all aspects of our lives, including fitness tracking, smart home appliances, industrial solutions, and battlefield sensors. However, this dynamic expansion of the network with mobile IoT devices introduces a major challenge to security, especially related to privacy and disclosure of personal information. Traditional models for computer security cannot extend to the limited resources of these devices. To this end, users are neither aware of nor can control the perpetual flow of device analytics to the cloud. This is a problem that is incredibly relevant to the Navy. With individual Warfighter use of IoT devices, this extends beyond the official Naval systems to the systems owned and operated by each individual Sailor and Marine. With the widespread use of IoT devices in both homeland and deployed settings, there is a range of different IoT security threats that are relevant. The goals of this research effort were to develop the research capacity of ROTC students in a multidisciplinary research program that studied IoT-based cybersecurity threats that span a broad range of Naval operational domains. This included (1) understanding the interconnected flow of information to and from these devices and threats to privacy, (2) developing strategic policies that provide protections, and (3) studying how users interact with the devices. Six ROTC students served as dedicated research assistants to the project, working 10-15 hours per week to support the research efforts. Second, approximately 20 ROTC students took part as research participants, providing exposure to the research methods.

These efforts included tactical cybersecurity research in which we first created an automatically labeled dataset of IoT device behaviors, constructed labels from multiple data sources, including querying vendor application programming interfaces, hooking the notification subsystem of the companion applications, and leveraging trigger-action frameworks to generate and identify device activities. We leveraged this dataset further to understand security and privacy violations of IoT devices, reporting seven critical vulnerabilities in IoT devices and identifying a systemically flawed design approach to encryption on IoT companion applications. Efforts also included strategic cybersecurity research in which we performed an analysis of the composition of IoT devices using an ontology and device representations in CSADL/architecture allowing us to analyze potential actions that could lead to violations such as disclosing private information. Human behavior modeling interaction with the IoT device was then modeled to identify additional security vulnerabilities, which further aid in the creation of security-based policies. Finally, efforts included human factors research in which we administered a survey to 179 IoT device users to examine user perceptions, knowledge, behaviors, and experiences associated with IoT device privacy. These findings revealed a lack of user knowledge of how IoT devices are using their data and a failure to take security precautions that users know will increase their privacy. Based on these findings we provided recommendations to guide security approaches and developed a testbed to evaluate interventions designed to increase user safe behaviors. We then conducted an experiment with over 100 participants to evaluate the effectiveness of the interventions at influencing users safe behaviors, with the results indicating the interventions led users to both read the terms and conditions associated with an IoT device and adjust settings appropriately. The following report details the methods and results of these research efforts.

Introduction

The Internet-of-Things (IoT) are rapidly becoming commonplace. The current 30.73 billion devices are predicted to grow to 75.44 billion by 2025. The ubiquitous reach of these devices has extended to all aspects of our lives, including fitness tracking, smart home appliances, industrial solutions, and battlefield sensors. IoT has provided a flexible platform for a large number of heterogeneous devices to dynamically join and leave the network. This enhances the availability of a diverse range of services provided by a network. However, this dynamic expansion of the network with mobile IoT devices introduces a major challenge to security, especially related to privacy and disclosure of classified or secret information. A lack of transparency and control has accompanied the growth of these devices. Traditional models for computer security cannot extend to the limited resources of these devices. To this end, users are neither aware of nor can control the perpetual flow of device analytics to the cloud.

The bulk aggregation of user data presents a significant privacy threat. Strava, a fitness tracking database used by devices like Fitbit, offers a publicly accessible database. The Strava heat map offers fitness enthusiasts the opportunity to find new exercise routes in their area. However, researchers cross-referenced the heat-map against Google Maps to identify a French military base in Niger, an Italian military base in Djibouti, and an unknown military base in Mogadishu (N.a, 2018). This security compromise illustrates that even privacy-aware military members are not immune to IoT-enabled privacy disclosures. This problem is complicated by the lack of control that accompanies IoT. To illustrate this paradigm, consider the case of the Ring doorbell. Ring allows police to turn on and capture 12 hours of video if a crime has occurred within a half-square mile in the last forty-five days (Harwell, 2019). Users should have the control to disable a doorbell and receive verification that the doorbell is disabled. However, this approach by Ring allows surreptitious video recording despite a user enforcing access controls.

This is a problem that is incredibly relevant to the Navy. According to the 2018 Naval Research and Development Framework, cyber threats are evolving and proliferating at unprecedented rates; and with an increasingly interconnected force, full-spectrum cyber approaches must be developed to protect our networks, data, and information systems (U.S Navy, 2018). With individual Warfighter use of IoT devices, this extends beyond the official Naval systems to the systems owned and operated by each individual Sailor and Marine. With the widespread use of IoT devices in both homeland and deployed settings, there is a range of different IoT security threats that are relevant. From the potential for Fitbits to provide geolocation data to foes to web cameras sending unauthorized video from secure areas, there is a need for the Navy to educate their current and future workforce on these threats and ensure they have the research capacity necessary to combat such threats. To this end, there is a need to conduct research to understand the threat that IoT devices pose to our Navy and Marine Corps and to identify cyber approaches across the full spectrum of operations that can mitigate these threats and “deter conflict or win decisively and return safely” (U.S Navy, 2018).

As such, research needs to be conducted to understand the interaction among IoT devices and generate cybersecurity defenses, both tactical and strategic, to ensure secure and effective human use. Further, as this is an area of science and technology that impacts the entire Naval workforce, especially those in STEM, there is a need to ensure that those entering the workforce

have both a solid understanding of IoT cybersecurity threats, as well as the research capacity to be able to support their organization, wherever that may be.

Major Goals

The major goals of this research effort were to develop the research capacity of ROTC students in a multidisciplinary research program that (1) studied IoT-based cybersecurity threats that span a broad range of Naval operational domains and (2) developed mitigations for reducing the impact of these threats to the Warfighter. This domain of study presented an interesting intersection between (a) tactical cybersecurity defense, (b) strategic cybersecurity policies, and (c) human cybersecurity decision-making. IoT devices/networks must be designed to be robust against cybersecurity threats at the operational level. This includes understanding and controlling the interconnected flow of information to and from these devices and the associated threats to privacy and disclosure of classified or secret information. However, given that these devices are part of a network of other devices and objects, it is necessary to develop strategic policies that provide protections. Pertinent to both the tactical and strategic implementation of these protections is how the users will interact with the devices and react to the policies put in place. To achieve a harmonious human-machine system, it was important to consider these aspects collectively and to allow findings from one area of study to ultimately inform research and development conducted in the other areas.

Objectives and Approach

This research effort develops the research capacity of ROTC students in a multidisciplinary research program that (1) researched approaches for identifying IoT privacy violations, (2) researched and developed IoT privacy and security policies, and (3) conducted human use experimentation to examine the impact of such policy and approaches on human interaction with IoT devices. This effort aligned with three priority areas outlined in the Naval Research and Development Framework, including (a) Communications and Networking, (b) Sensors and Sensor Processing, (c) Machine Learning, Reasoning, and Intelligence. This effort developed the research capacity of university students, in particular, those enrolled in the ROTC program, in these three priority areas in two key ways. First, six ROTC students served as dedicated RAs to the project, working 10-15 hours per week to support the three main thrusts: (a) tactical cybersecurity defense, (b) strategic cybersecurity policies, and (c) human cybersecurity decision-making. Second, approximately 20 ROTC students took part as research participants, providing them exposure to the research methods. These opportunities have the potential to lead to improved education and training outcomes and connections to the military and potentially naval, STEM careers in cybersecurity and electronic warfare. The following sections detail the five objectives and associated approaches within the efforts.

Objective 1. Research Approaches for Identifying IoT Privacy Violations

We first created an automatically labeled dataset of IoT device behaviors. This dataset includes both packet captures alongside the labeled activities of the devices. Combining these data sources provides ground truth for existing and future research approaches to identify device activities. We constructed these labels from multiple data sources, including querying vendor

application programming interfaces, hooking the notification subsystem of the companion applications, and leveraging trigger-action frameworks to generate and identify device activities. We leveraged this dataset further to understand security and privacy violations of IoT devices, reporting seven critical vulnerabilities in IoT devices and identifying a systemically flawed design approach to encryption on IoT companion applications. We believe the military can significantly benefit from an understanding of these privacy violations for targeted signals intelligence. Under this objective, we accomplished the following tasks:

Task 1.1 Built a robust dataset of IoT device behaviors (e.g., analytics, video recording, lock state changes, firmware updates, motion reporting) for a group of widely popular IoT devices.

Task 1.2 Developed a methodology for querying vendor APIs to systematically apply labels against encrypted network flows.

Task 1.3 Constructed a publicly accessible framework for querying the dataset and constructing future crowd-sourced datasets.

Objective 2. Research and Development of IoT Privacy and Security Policies

We got students involved in the research for policy generation concurrently, collaborating with the team working on Objective 1. The main objective of the research method focused on compositional analysis of IoT devices as these devices interact over the cloud by representing the inputs, outputs, and the expected actions. To perform automated analysis for the composition of IoT devices the first step involved identifying the devices, then their relationships based on input and the corresponding output, which was modeled in an ontology. This was followed by the device representations in CSADL/architecture and then analyzing potential actions that could be executed based on the input. This involved relational analysis along with “*If This then That*,” type of analysis, which were performed by creating a library that stores this knowledge. This enabled automated analysis to identify the possible actions that may lead to violations such as, disclosing secret positions or classified actions to be taken, based on which policies can be derived. Finally, human behavior modeling interaction with the IoT device was modeled to identify additional security vulnerabilities, which further aid in the creation of security-based policies. Under this objective we accomplished the following tasks:

Task 2.1 Ontological representation of IoT devices: This involved representing the devices, their dependencies, and the actions that can be performed by them or on them.

Task 2.2 Extended the CSADL framework to integrate IOT scenarios: This involved extending the modeling and analysis framework by incorporating concepts and terminologies inherited from IOT. This task included identification of the syntax and semantics essential in representing the IoT devices, which then enabled compositional analysis of the architecture. The reasoner represented assume-guarantee based reasoning to identify the possible interactions, thus leading to identifying violations.

Task 2.3 Modeling of human behavior: This involved extending the framework to model human behavior based on their roles and how they interact with the IOT system.

Task 2.4 Modeling and analysis of the composition of IOT and human to identify security policies: This task involved design and implementation of the automated reasoner to include the assumptions and guarantees related to architectural representations and human interactions.

Objective 3. Human Use Experimentation and Design Recommendation Development

We then examined human perceptions, knowledge, behaviors, and experiences associated with IoT devices. This included conducting an up-front analysis of operator awareness, experience, and perceptions of IoT security, as well as user needs associated with such technology. Perceptions such as user understanding of what type of, how much and how often information is transmitted from IoT devices was examined to help identify areas that Naval STEM education efforts should target. Based on user needs defined in the up-front analysis, we provided recommendations to guide security approaches and developed a testbed to evaluate privacy approaches. Finally, we conducted a small-scale experiment with ROTC and other participants to examine human behaviors associated various security approaches. Under this objective we accomplished the following tasks:

Task 3.1 Conduct user interview/questionnaire-based research to examine operator awareness, experience, and perceptions of IoT security, and user needs associated with IoT technology.

Task 3.2 Analyze interview and questionnaire data and develop recommendations for approaches, policies, experimentation, and experimental testbed.

Task 3.3 Plan and conduct a small-scale experiment to examine operator susceptibility, detection, and response to IoT cybersecurity threats utilizing privacy approaches and security policies developed under Objectives 1 and 2.

Objective 4. ROTC Student Mentoring, Training and Education

Key to this project was developing the cybersecurity research capacity of the ROTC students at FIT. Within this effort, six ROTC students served actively on the research team as research assistants (RAs), to learn research approaches for studying cybersecurity. RAs were selected based on their background and achievements. RAs were then be matched to work associated with either Objective 1, 2 or 3 as their primary focus. Each ROTC RA received mentoring from a faculty member and graduate student(s) in the focus areas of each objective, with the goal of creating meaningful experiences that met Naval STEM education and workforce priorities, and that exposed them to elements such as Navy and Marine Corps STEM knowledge and skills. The RAs were active researchers on the project supporting the tasking necessary to achieve project goals. Further, each RA performed a small amount of cross-training under the other two objectives, with the aim of exposing the RA to the tools and techniques utilized in each discipline to research and develop cybersecurity defense tools and approaches. Under this objective we accomplished the following tasks:

Task 4.1 Selected RAs from a pool of ROTC students available, and match RAs to a focus objective area based on background, achievement, and student strengths.

Task 4.2 Developed mentoring plans and tasking work plan for ROTC RA support of research and development efforts.

Task 4.3 Per mentoring plans developed, faculty and graduate students provided continual oversight, guidance and assistance in the RAs completing their tasking, including regular meetings and work sessions to assist in educating and developing their cybersecurity research skills.

Objective 5. Coordination with Military STEM and Cybersecurity Stakeholders

We coordinated with Military STEM and Cybersecurity Stakeholders with the goal of creating meaningful experiences for the ROTC students that meet Naval STEM education and workforce priorities, and that exposed them to elements such as US Military (including Navy and Marine Corps) STEM skills, content, careers, and personnel. Further, coordination with stakeholders was sought to connect relevant people and organizations to explicitly develop broader projects for affecting a range of cybersecurity communities. The performers on this project had close ties to several branches of the military, including the Navy, and coordinated closely to ensure the research program aligned with STEM and Cyber priorities, and to ensure ROTC students were exposed to these domains within a military context. Toward this end, we coordinated with LTC Jimmy Crook (Florida Tech Army ROTC), CW4 Matt McDougall (Technology Integrations Cell, 1st Special Forces Command), and MAJ (P) Ryan Hand (Geographic Team Leader, US Army Cyber Command). Under this objective we accomplished the following tasks:

Task 5.1 Identified relevant STEM and Cybersecurity stakeholders across Navy, Marine Corps, and other services.

Task 5.2 Developed coordination plan for alignment of research program and exposure of ROTC students to military STEM and Cybersecurity contexts

Task 5.3 Met regularly, virtually, with stakeholders, including ROTC RAs when possible.

Project Schedule and Milestones

Table 1.

Schedule of Milestones in Months After Contract Award (MACA), including Planned and Actuals

Task	Planned	Actual	Milestone
1.1	4	7	Dataset of IoT device behaviors.
1.2	8	7	Approach for labeling network flows.
1.3	12	10	Publicly accessible dataset.
2.1	3	5	Ontology representing IOT scenarios
2.2	6	6	Software to perform input-output interaction/architecture analysis
2.3	9	10	Model of human interaction with IOT for analysis
2.4	12	12	Results of human-IOT model analysis
3.1	3	6	Results of up-front analysis of cybersecurity perceptions and user needs
3.2	4	9	Recommendations for approaches, policies, experimentation, experimental testbed.
3.3	6	9	Research plan for experimentation
3.3	12	12	Results of Experimentation
4.1	0	0	ROTC RAs hired and matched to focus area
4.2	1	1	Mentoring and Work Plans
4.3	6, 12	6, 12	Midterm and final assessment of mentoring progress
5.1	1	2	Initial contact with stakeholders
5.2	2	2	Coordination Plan
5.3	12	14	Report detailing Stakeholder Meetings

Accomplishments

Objective 1: Research Approaches for Identifying IoT Privacy Violations

Task 1.1 Build a Robust Dataset of IoT Device Behaviors (e.g., analytics, video recording, lock state changes, firmware updates, motion reporting) for a Group of Widely Popular IoT Devices

The pervasive use of Internet-of-Things (IoT) devices has accelerated in the last two years, with 21.5 billion devices actively connected worldwide (Lueth, 2020), (Schindler, et al., 2013). IoT actuators and sensors connect us to our homes through a variety of devices, including wireless doorbells, security cameras, locks, movement sensors, thermostats, and security alarms. To accompany this growth, vendors have begun offering IoT-related products and services in this domain by leveraging turnkey solutions to the always-on and always-connected cloud. However, security and privacy issues have plagued this rapid growth with a lack of established standards and protocols (O'Connor, Enck, & Reaves, 2019), (Choi, et al., 2019), (Antonakakis, et al., 2017), (Stellios, Kotzanikolaou, Psarakis, Alcaraz, & Lopez, 2018), (Freed, et al., 2017), (Janes, Crawford, & O'Connor, 2020), (Lau, Zimmerman, & Schaub, 2018), (Yuan, Jia, Xing, Jin, & Zhang, 2020).

The lack of transparency and control in IoT devices has complicated user security and privacy. A recent class-action lawsuit argued that Ring Inc. allowed attackers to access users' cameras covertly and surreptitiously (Paul, 2020). In a separate incident, an ADT technician pled guilty to remotely spying on customers over 9,600 times in a four-year period (Dooley, 2021). Due to the limited interfaces on IoT devices, victims are left unaware of their devices' actions or how to implement access controls (He, et al., 2018). IoT devices occupy our most personal spaces with cameras and microphones. Unfortunately, this lack of transparency and control has enabled intimate partner violence by using IoT devices to spy and harass victims (Freed, et al., 2017), (Dooley, 2021), (Alshehri, Ben Salem, & Ding, 2020). Labeling and identifying traffic flows by purpose (i.e., camera streaming) offers the promise of providing greater transparency to users. The goal of our work is to construct a robust dataset of IoT device behaviors to overcome the limitations of this lack of transparency and control.

Methods. To construct the dataset, we examined the challenges and previous works. Our work is informed by leveraging application programming interfaces, trigger-action frameworks, and companion notifications to automatically label events from encrypted network traces.

Encrypted communication protocols and device resource constraints complicate transparency and the examination of these devices' activities. IoT devices' limited interfaces have left consumers blinded without the ability to interact directly with operating systems, resulting in a lack of awareness of the data collected and sent by IoT sensors and actuators. Largely, consumers are left to trust the vendor to control the processing and storage of the massive data produced by these devices. In addition to malicious actors, vendors have monetized users' data without clear transparency to the end-users. As an example, Ring partnered with over 1,300 law enforcement agencies to share camera recordings (Kelley & Guariglia, 2020), (Cameron & Mehrotra, 2021).

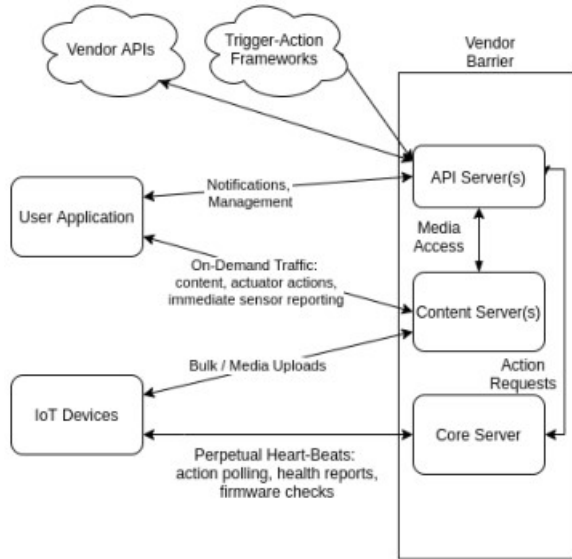
Previous works have examined collecting IoT device communication datasets (Huange, Apthorpe, Acar, Li, & Feamster, 2019), (Sivanathan, et al., 2018), (Ren, et al., 2019), (Trimananda, Varmarken, Markopoulou, & Demsky, 2020), (Miettinen, et al., 2017), (Perdisci, Papastergiou, Alrawi, & Antonakakis, 2020), (Parmisano, Garcia, & Erquiaga, 2020). Previous dataset approaches include logging plaintext protocols such as DHCP and DNS requests (Huange, Apthorpe, Acar, Li, & Feamster, 2019) or full network captures (Perdisci, Papastergiou, Alrawi, & Antonakakis, 2020), (Miettinen, et al., 2017). However, previous datasets lack fine-grained labels to determine the ground truth for device activities (e.g., when a motion detection camera is transmitting video.) They are often broadly focused on creating a binary division between benign traffic and attack traffic (e.g., a device controlled by the Mirai botnet versus a device in normal operation) (Mudgerikar, Sharma, & Bertino, 2019), (Parmisano, Garcia, & Erquiaga, 2020). Or they contain coarse-grained labels identifying specific device models (Miettinen, et al., 2017), (Huange, Apthorpe, Acar, Li, & Feamster, 2019). Coarse-grained approaches lack labels that identify devices' on-demand event activities (e.g., a camera streaming video). Datasets that include fine-grained labels are created manually, recording the actions of a lab assistant performing these actions repeatedly (Miettinen, et al., 2017). This approach cannot scale to support the sample demands for supervised learning algorithms. There is a growing need to create fine-grained labeled and scalable datasets to enable future research on classifying encrypted IoT traffic.

A key insight of our work is the use of application programming interfaces, trigger-action frameworks, and companion notifications to automatically label events from network traces. This insight allows us to construct fine-grained labels of device behaviors. Further, we leverage trigger action frameworks and vendor APIs to remotely trigger events, generating an appropriate scale of events for machine learning.

Previous works have hypothesized that machine learning approaches can identify and classify network traffic on IoT devices to overcome transparency issues (Wang, et al., 2020), (O'Connor, et al., 2019), (Acar, et al., 2020), (Trimananda, Varmarken, Markopoulou, & Demsky, 2020), (Singh, et al., 2018). Machine learning can predict on-demand events (e.g., a camera detecting motion or transmitting video) by analyzing the statistics of encrypted network flows. However, the precision of such approaches requires a training dataset of known IoT events and traffic. Current datasets lack the fine-grained detail and scale to train algorithms effectively. Our work provides a dataset capable of enabling the further study of algorithmic approaches for identifying when IoT device network traffic contains sensitive events.

Figure 1.

Trigger-Action Frameworks, Vendor APIs, and Companion Applications Enable Overcoming IoT Vendor Barriers That Abstract Transparency and Control Away from Users



Results. We construct our dataset based on two unique IoT purposes: sensing and actuating (Distenfino, Merlino, & Puliafito, 2012). Sensors report environmental and physical stimuli in the world. Actuators enable remote control of IoT devices. Sensors observe and report environmental and physical changes in IoT devices. Examples include microphones that listen to sound, infrared sensors that detect motion, humidity sensors that detect moisture, or thermostats that measure temperature. IoT devices also sense and report changes to their physical state. For example, smart locks sense and report when an owner physically unlocks a door. These always-on sensors provide an always-current state of their device through perpetual connections to internet servers. Actuators allow owners to change or modify the state of a device. For example, a smart-lock owner can remotely unlock the front door for package delivery. Or an owner can remotely trigger an electronic relay to change the color of smart lights. In industrial IoT solutions, actuators exist in the form of remote valve controls, where users can modify the flow rate of a water or gas line or even remotely activate electrical breakers. To enable the always-availability of actuators, IoT devices periodically poll internet-connected servers for owner requests and commands. The combination of sensing and actuating offers the convenience of IoT. An internet-connected thermostat that detects a change in temperature can trigger an actuator to turn on the air-conditioning unit. However, to broker these connections requires an IoT ecosystem of hybrid servers. IoT ecosystems bridge the gap between perpetual sensor reports and periodic actuator polling.

Further, our dataset is constructed from traffic from two areas: IoT API Gateways and Content Distribution Networks. IoT API Gateways expose the functionality of IoT devices to the users and applications. Gateways perform essential functions, including authentication, registration, device management, and provisioning. They bridge the communication between users and the perpetually connected core servers by relaying user commands (e.g., begin

recording video). Further, APIs connect users to the IoT-produced media on content distribution networks (e.g., recorded video files). IoT device architectures leverage heavily optimized content distribution networks to store and transmit large data. In managed IoT environments, these networks store bulk media (e.g., audio/video recordings, sensor logs, device histories.) By offloading storage and processing to the cloud, IoT vendors can rapidly scale their infrastructure (Amazon Web Services, 2021). CDNs generally store attributeless media and implement access control by generating unique identifiers and access tokens. Intra-server communication between CDNs and API gateways relay these controls to users and applications.

Major Findings and Key Outcomes.

Finding 1 - Leveraging Trigger Action Frameworks: Users enjoy the convenience of IoT sensors and actuators interacting autonomously based on a set of pre-defined rules. For example, a proximity sensor can trigger a wireless garage door to open and power on the outdoor lights. This cross-vendor interoperability presents a unique challenge for users with a heterogeneity of device vendors. Third-party trigger-action frameworks, such as Alexa and If-This-Then-That (IFTTT), overcome this challenge by creating centrally managed locations to define rules and automate actions. Third-party trigger-action frameworks rely on a set of pre-defined rules that automate API calls across different vendors' managed IoT architectures. In the previous example, an owner may grant IFTTT access to make API calls across different vendors, including their SmartThings proximity sensor, MyQ garage door opener, and Philips Hue Smart Lights. Instead of the API calls happening directly to the device - they occur across the managed cloud environments for the SmartThings, MyQ, and Philips Hue vendors. While third-party frameworks automate convenience for the owner, they also provide us an opportunity to automate actions for labeling device activities. For example, we can set a time-based rule for the IFTTT trigger-action framework to record a 30-second video clip on an Arlo camera. Third-party trigger-action frameworks and time-based triggers present an opportunity to create a scalable dataset of IoT device behaviors. For example, we remotely locked and unlocked a smart lock 176 times in our experiment. This solution allows us to overcome the scalability limitations of previous IoT datasets created by manual triggers (Miettinen, et al., 2017). In the following subsections, we examine the type of traffic we can observe in network traces.

Finding 2 - Distinguishing On-Demand Activity: We distinguish IoT device traffic into two main categories: perpetual heartbeats and on-demand activity. Our work focuses on detecting and labeling spontaneous on-demand activity. Perpetual Heartbeats IoT devices perpetually connect to core servers to provide availability for users. As maintaining long-running connections are costly, IoT devices achieve perpetual connections by periodically polling core servers at fixed intervals. In addition to regularly polling for instructions, IoT devices may regularly push health checks such as battery state or request firmware updates. We call these traffic heartbeats due to the periodic nature that connects them to device management. Previous works have observed that this type of traffic is predictable with fixed signatures (O'Connor, Enck, & Reaves, 2019), (Hariri, Giannelos, & Arief, 2019). Previous work also refers to this traffic as idling (Trimananda, Varmarken, Markopoulou, & Demsky, 2020), (Ren, et al., 2019). However, we find this description problematic as it fails to capture the traffic's purpose. We use the term heartbeat to describe connections necessary to the overall health of the always-available aspect of IoT. As this traffic happens periodically regardless of user interaction, we can gather samples without any external triggers. As Huang examined, DNS data

is often sufficient to label heartbeat traffic (Huange, Apthorpe, Acar, Li, & Feamster, 2019). On-Demand Activity On-demand traffic occurs when users or applications request sensor data or actuator actions. The convenience of IoT is provided by rapidly supporting these on-demand requests. For example, a user may request that a camera upload streaming video to a content distribution network. Other on-demand traffic examples including performing specific actuators' actions (e.g., locking a door) or immediately sensing and reporting (e.g., checking the temperature). While users generally force on-demand traffic, we can also use the previously discussed trigger-action frameworks to trigger on-demand traffic. Labeling on-demand traffic enables us to identify traffic anomalies in network traces that match the characteristic of on-demand traffic but do not appear in device histories or logs (e.g., a Ring doorbell transmitting video to police servers).

Task 1.2 Develop a Methodology for Querying Vendor APIs to Systematically Apply Labels Against Encrypted Network Flows

Our work proposes a solution to automatically generate and label on-demand events from IoT devices across unique vendors and types. This section discusses the challenges to this problem and explores the ideas behind triggering and labeling events. Several challenges accompany this problem. In particular, we examine the challenges of applying fine-grained labels that describe device activity in the presence of pervasive encryption. Further, we address the need to generate enough samples to facilitate further machine learning research. Our work addresses these challenges by integrating a hybrid of solutions by using trigger-action frameworks, interfacing with vendor APIs, and intercepting companion application notifications.

C1) Pervasive Encryption. The pervasive use of encryption in IoT ecosystems complicates inferring device activity from network traces. Previous work has measured the use of encryption in IoT ecosystems (Ren, et al., 2019). We echo their finding that unencrypted protocols correspond to the maturity of vendors. To label device histories of mature vendors' traffic requires overcoming encryption limitations by extracting device activity labels from trigger-action frameworks, vendor APIs, and application notifications.

C2) Fine-Grained On-Demand Event Labels. Identifying unintended device activity requires fine-grained labels that clearly distinguish the different activities of IoT devices (e.g., remotely toggling power, detecting motion, locking a door.) Previous work has addressed this challenge by relying on the IFTTT framework to trigger events (Trimananda, Varmarken, Markopoulou, & Demsky, 2020). However, relying solely on IFTTT proves problematic as it is unsupported by several popular vendors (Trimananda, Varmarken, Markopoulou, & Demsky, 2020). We overcome this challenge by directly interfacing with vendor APIs and intercepting companion application notifications.

C3) Scale of On-Demand Samples. To classify and identify unintended device activity requires a dataset with an appropriate number of labeled samples. Generating labeled samples through manual interaction proves problematic as it is laborious to reproduce (Miettinen, et al., 2017). Previous work has addressed this by leveraging the IFTTT trigger action framework (Trimananda, Varmarken, Markopoulou, & Demsky, 2020). We complement this approach by describing the use of IFTTT time-based trigger recipes to remotely schedule events and generate an appropriate set of labeled samples.

Methods. The key insight of our work is exploring a hybrid model of trigger-action frameworks, vendor APIs, and companion application notifications to generate and label on-demand events. In the following paragraphs, we provide an overview of how we generate and label events.

Triggering Actions. We generate (or trigger) on-demand actions either manually or by leveraging vendor APIs and trigger-action frameworks. As depicted in Figure 2, manually interacting with a device (such as walking by a motion detection camera) will generate network traces as the camera signals motion detection and uploads video to a content distribution network. Manually triggering events is problematic for reproducibility and scale. Previous work identified IFTTT trigger action framework offers an opportunity to repeatedly generate on-demand events (Trimananda, Varmarken, Markopoulou, & Demsky, 2020). We improve this effort by taking advantage of a recent improvement to the IFTTT framework. As depicted in Figure 3, IFTTT recently enabled support to schedule on-demand events repeatedly on an hourly basis. This addition greatly simplified our approach, generating 24 samples daily for 14 devices in our dataset across eight unique device activities. This included two locks, as depicted in Figure 4.

Logging Events Repeatedly. Scheduled triggers prove helpful in generating a scalable label event history. However, it is necessary to capture and label the noise, motion, and vendor-specific events that occur manually within the lab environment. We leverage IFTTT trigger-action frameworks, exposed vendor APIs, and capture companion application notifications to label manual events. This hybrid approach allowed us to overcome limitations exposed by vendor implementations. Using IFTTT recipes, we captured manually triggered events with IFTTT by writing the event to a log file. However, as all devices do not support IFTTT (Trimananda, Varmarken, Markopoulou, & Demsky, 2020), our approach considered other labeling methods for manually triggered events. Vendor APIs, such as the Samsung SmartThings API, maintain a forensically rich event history. In our experiment, we queried the Samsung SmartThings API to discover the detailed logs of seven devices not exposed by IFTTT. IoT companion applications, hosted on mobile phones and tablets, often provide the only transparency to IoT end-users. We captured the companion applications’ notifications by hooking the push notification system of a mobile phone paired to our IoT devices. This approach discovered the detailed event histories of 21 devices not exposed by IFTTT or vendor APIs. Our experiments demonstrate the benefit of this heterogeneous approach to labeling events.

Figure 2.

IFTTT Recipes, Vendor APIs, and Companion Applications All Provide Opportunities to Capture and Precisely Label Manually Triggered Events

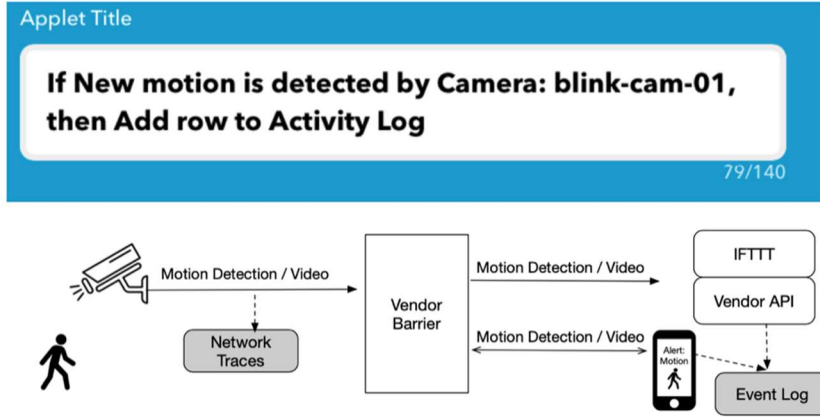
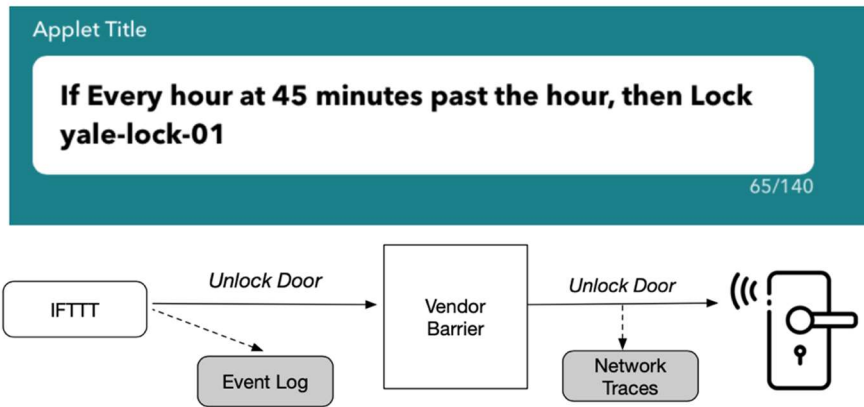


Figure 3.

Scheduling Repeated IFTTT Recipes Enables Us to Automatically Trigger and Label Device Activities



Experiment Results. In the following paragraphs, we discuss the structure and execution of an experiment to capture and label a dataset of IoT traffic. We examine the devices in our dataset, our capture and label methodologies. IoT devices: As illustrated in Table 2, our dataset consists of a representative set of 57 smart home IoT devices for consumers, available from well-known US retailers, including Best Buy, Walmart, Target, and Amazon. We focus our collection on devices within smart home automation categories, including cameras, doorbells, locks, alarm systems, lights, plugs, environmental sensors, and hubs. Of the 57 devices, 26 connect through smart hubs, and 31 connect directly to the internet over a wired or wireless connection. Capture Hardware: Our capture hardware consists of a Linksys WRT1900AC router running OpenWRT, a Dell PowerConnect 6248P hardware switch, and a

pfSense Server. The Linksys router offers the physical layer connection (either wired or wireless for devices), mirroring the routers commonly used in smart homes.

The Linksys router operates in AP Mode, forwarding the traffic over the hardware switch to the pfSense server for network layer IP addressing and routing. To ease future classification efforts, we reserved static IP addresses for all IoT devices. We leverage the switch's port mirroring technology to mirror both outbound and inbound traffic from the router's outgoing port into a second port on the server, which performs the capture. Further, the captures are temporarily written to an in-memory filesystem, preventing packet loss during bursty traffic. We then rotate and move captures to a physical disk on an hourly basis for long-term storage

Major Findings and Key Outcomes. Our experiment informed the following major findings.

Finding 1 - Network Captures. We recorded 468,933 network flows and 16,686 unique events from March 08, 2021, at 1:30 PM GMT to March 15, 2021, at 9:16 PM GMT. We generated labels by remotely triggering events using IFTTT recipes and capturing notifications and logs from companion applications, IFTTT, and vendor APIs.

Finding 2 - Labeled Events. We remotely triggered 4,944 events (or 29.63% of labeled events in our dataset). We further labeled 11,742 events by manually interacting with devices (or the remaining 70.37% events in our dataset.) To manually trigger events, a researcher visited the lab daily and interacted with devices by unlocking doors, ringing doorbells, walking by nearby motion detection cameras, and speaking loudly. Manually triggered events include any event generated by an environmental change, which can have an automatic source. The Philips Hue Lights, for example, indirectly trigger CV-dependent motion sensors when the lights change state. Several actuators also triggered audio sensors when the lock physically switched states.

Figure 4.

Smart Door Locks



Note. When supported, we leveraged IFTTT triggers to remotely cause on-demand events such as locking and unlocking two of the seven door locks in our dataset, which produced 706 events.

Table 2.
Overview of the Number of Events and Traffic Flow

Device	Total Packets	Traffic (In / Out)	Flows (TCP / UDP)	Total Events	Labeled Activities	Label Source
Arlo Base Station	815,751	41.19 MiB / 454.19 MiB	3,703 / 4,569	353	arm,disarm	IFTTT Triggers
→Arlo Pro Smart Security Camera 1				214	motion,record	IFTTT Logs,IFTTT Triggers
→Arlo Pro Smart Security Camera 2				222	motion,record	IFTTT Logs,IFTTT Triggers
August Connect Wi-Fi Bridge	295,033	12.01 MiB / 17.68 MiB	175 / 2	0		
→August Smart Lock Pro (3rd Gen)				61	lock,unlock	IFTTT Logs
August Connect Wi-Fi Bridge	294,712	11.97 MiB / 17.56 MiB	192 / 2	0		
→Yale Real Living Assure Lock Deadbolt				21	lock,unlock	IFTTT Logs
Blink Sync Module	203,619	7.67 MiB / 8.02 MiB	61 / 739	353	arm,disarm	IFTTT Triggers
→Blink Indoor Home Security Camera 1	23,861	596.10 KiB / 19.63 MiB	37 / 39	39	motion	IFTTT Logs
→Blink Indoor Home Security Camera 2	22,835	611.67 KiB / 17.87 MiB	39 / 41	42	motion	IFTTT Logs
→Blink Indoor Home Security Camera 3	25,434	654.57 KiB / 20.37 MiB	42 / 44	45	motion	IFTTT Logs
Geeni Aware Surveillance Camera 1	407,569	12.88 MiB / 69.77 MiB	19,381 / 4,727	486	motion	Companion App
Geeni Aware Surveillance Camera 2	415,853	13.28 MiB / 75.79 MiB	19,418 / 4,638	529	motion	Companion App
Geeni Doorpeek Smart Wi-Fi Doorbell	263,380	6.88 MiB / 41.38 MiB	902 / 102	232	motion,ring	Companion App
Geeni Doorscreen Smart Wi-Fi Doorbell	2,382,015	117.12 MiB / 144.34 MiB	627 / 676	96	ring,motion	Companion App
Geeni Look Indoor Smart Security Camera 2	252,425	6.80 MiB / 38.70 MiB	819 / 83	601	motion,sound	Companion App
Geeni Sentinel Smart Camera	1,674,494	169.98 MiB / 249.50 MiB	1,525 / 5,749	981	motion	Companion App
Merkury Innovations Smart Wifi Camera	204,070	5.24 MiB / 33.66 MiB	773 / 109	83	motion	Companion App
Merkury Smart Wi-Fi Doorbell Camera	256,006	7.03 MiB / 46.42 MiB	859 / 191	110	motion,ring	Companion App
Nest Cam IQ Indoor	14,905,585	494.64 MiB / 2.69 GiB	52 / 25	194	person,motion,sound	Companion App
Nest Hello Smart Wi-Fi Video Doorbell	780,899	26.53 MiB / 115.66 MiB	83 / 2	60	motion,person,ring,sound,	Companion App
Night Owl Doorbell 1	4,010,530	781.92 MiB / 272.51 MiB	124,227 / 27,891	76	motion,ring	Companion App
Night Owl Doorbell 2	4,044,239	787.20 MiB / 276.69 MiB	124,462 / 27,910	110	motion,ring	Companion App
Philips Hue Bridge	212,863	4.05 MiB / 34.31 MiB	1,052 / 2,702	0		
→Philips Hue White and color				353	off,on	IFTTT Triggers
→Hue Ambiance Smart LED Bar Light 1				353	off,on	IFTTT Triggers
→Hue Ambiance Smart LED Bar Light 2				352	off,on	IFTTT Triggers
→Hue Ambiance Smart LED Bar Light 3				352	off,on	IFTTT Triggers
→Hue Ambiance Smart LED Bar Light 4				352	off,on	IFTTT Triggers
Ring Alarm Base Station 1st Generation	190,361	10.87 MiB / 18.00 MiB	416 / 3,000	0		
→Ring Alarm Contact Sensor 1				61	open,batt,close	Companion App
→Ring Alarm Contact Sensor 2				69	open,close	Companion App
→Ring Alarm Contact Sensor 3				82	open,close	Companion App
→Ring Alarm Motion Detector 1				76	motion	Companion App
→Ring Alarm Motion Detector 2				74	motion	Companion App
→Ring Alarm Motion Detector 3				69	motion	Companion App
Ring Spotlight Cam	3,064,828	114.44 MiB / 2.32 GiB	698 / 874	117	motion	Companion App
Ring Video Doorbell 1	654,039	34.42 MiB / 384.91 MiB	399 / 814	182	motion,ring	Companion App
Ring Video Doorbell 2	617,518	31.83 MiB / 359.76 MiB	355 / 718	166	motion,ring	Companion App
Ring Video Doorbell Pro	7,620,669	228.94 MiB / 6.24 GiB	1,071 / 1,308	341	motion,ring	Companion App
Schlage Encode Smart WiFi Deadbolt	8,603	319.50 KiB / 883.65 KiB	15 / 13	37	lock,unlock,batt	Companion App
Sifely Lock Gateway G2	19,427	612.15 KiB / 796.64 KiB	466 / 3	0		
→Sifely Keyless Entry Door Lock				4	unlock	Companion App
SimpliCam HD Indoor Security Camera	328,044	7.29 MiB / 244.23 MiB	20 / 4,509	14	motion	Companion App
Simplisafe Video Doorbell Pro	595,814	12.68 MiB / 494.38 MiB	39 / 6,615	291	motion,ring	Companion App
SmartThings Hub	535,465	54.41 MiB / 32.25 MiB	11,989 / 9,755	0		
→Kwikset Electronic Deadbolt				49	unlock,lock	Smartthings Logs
→SmartThings Motion Sensor				931	motionstart,motionend,temp	Smartthings Logs
→SmartThings Multipurpose Sensor				657	temp.move.open,close,	Smartthings Logs
→Samsung Smartthings Outlet				343	off,on	Smartthings Logs
→SmartThings Water Leak Sensor				603	temp.waterstart,waterend	Smartthings Logs
→Yale Touchscreen Deadbolt				379	unlock,lock,timeoutunlock	Smartthings Logs
SmartThings Smart Camera	494,353	26.05 MiB / 217.58 MiB	2,514 / 3,762	2,598	rss,lqi,soundend,personend, soundstart,motionstart,personstart,record, motionend	Smartthings Logs
TP-Link Kasa Spot Camera	4,091,964	103.10 MiB / 3.39 GiB	2,213 / 15,731	1,546	sound,motion,off,on,	Companion App,IFTTT Triggers
Ultraloq Bridge WiFi Adapter	38,040	1.49 MiB / 1.83 MiB	52 / 60	0		
→Ultraloq U-Bolt Smart Deadbolt				357	unlock,lock	IFTTT Logs,IFTTT Triggers
Wyze Cam v2	1,658,118	53.04 MiB / 716.46 MiB	10,743 / 12,157	970	motion,sound,record,restart, off,on	IFTTT Logs,IFTTT Triggers
Totals	51,408,416	3.11 GiB/18.96 GiB	329,396 / 139,537	16,686		

Note. Our dataset contains 16,686 labeled events over 468,933 network flows from 57 devices focused on smart home automation categories, including cameras, doorbells, locks, alarm systems, lights, plugs, environmental sensors, and hubs.

Task 1.3 Construct a Publicly Accessible Framework for Querying The Dataset and Constructing Future Crowd-Sourced Datasets

The goal of our work was to construct a publicly accessible dataset that would inform future research. To this end, our dataset is currently available via <https://research.fit.edu/IoT>. The data, labels, and build scripts are available for download to inform future research.

Methods. In our work, we captured companion application notifications from 27 unique devices across ten vendors to label events. Capturing companion notifications allows us to label events from IoT vendors who do not integrate with trigger-action frameworks or permit API

access. Companion applications implemented on phones and tablets often serve as the only transparency for IoT devices. Vendors often achieve this transparency through the use of push notifications. For example, these notifications inform users that their smart doorbell has detected audio or motion. While vendor implementations vary, they ultimately deliver notifications to a standardized phone or tablet notification subsystem API. Notifications are implemented pervasively across IoT companion applications to implement the always-on, always-available aspects of IoT. In our work, we hook the Android Notification Service to read and log IoT device notifications. Figure 5 depicts an example of the resulting hooked logs, showing motion and audio detection on our TP-Link Kasa Camera. This approach enabled us to record 6,366 total events that would have otherwise been unobservable with the same precision. We implemented this functionality in a Python script and published it to provide reproducibility.

Figure 5.

JSON Formatted Log

```
{ "package": "com.tplink.kasa_android", "title": "kasa-cam-01detected
motion", "text": "", "date": "March_12,_2021_at_01:46:05PM" }

{ "package": "com.tplink.kasa_android", "title": "kasa-cam-01detected
sound", "text": "", "date": "March_12,_2021_at_02:01:45PM" }
```

Note. We hooked the Android Notification Service to read and log IoT device notifications, delivering JSON formatted logs that provide transparency of IoT device events.

Figure 6.

Example of a Fine-Grained Label of Device Event History

```
"March_15,_2021_at_04:31:41AM", "smarththings-cam-01", "event\_soundstart""
March_15,_2021_at_04:31:53AM", "smarththings-cam-01", "event\_soundend""
March_15,_2021_at_04:44:13AM", "smarththings-outlet-01", "event\_off""
March_15,_2021_at_04:59:05AM", "smarththings-outlet-01", "event\_on"" }"
March_15,_2021_at_04:30:12AM", "yale-lock-01", "event\_unlock"" }"
March_15,_2021_at_04:53:11AM", "smarththings-multi-01", "event\_temp"
```

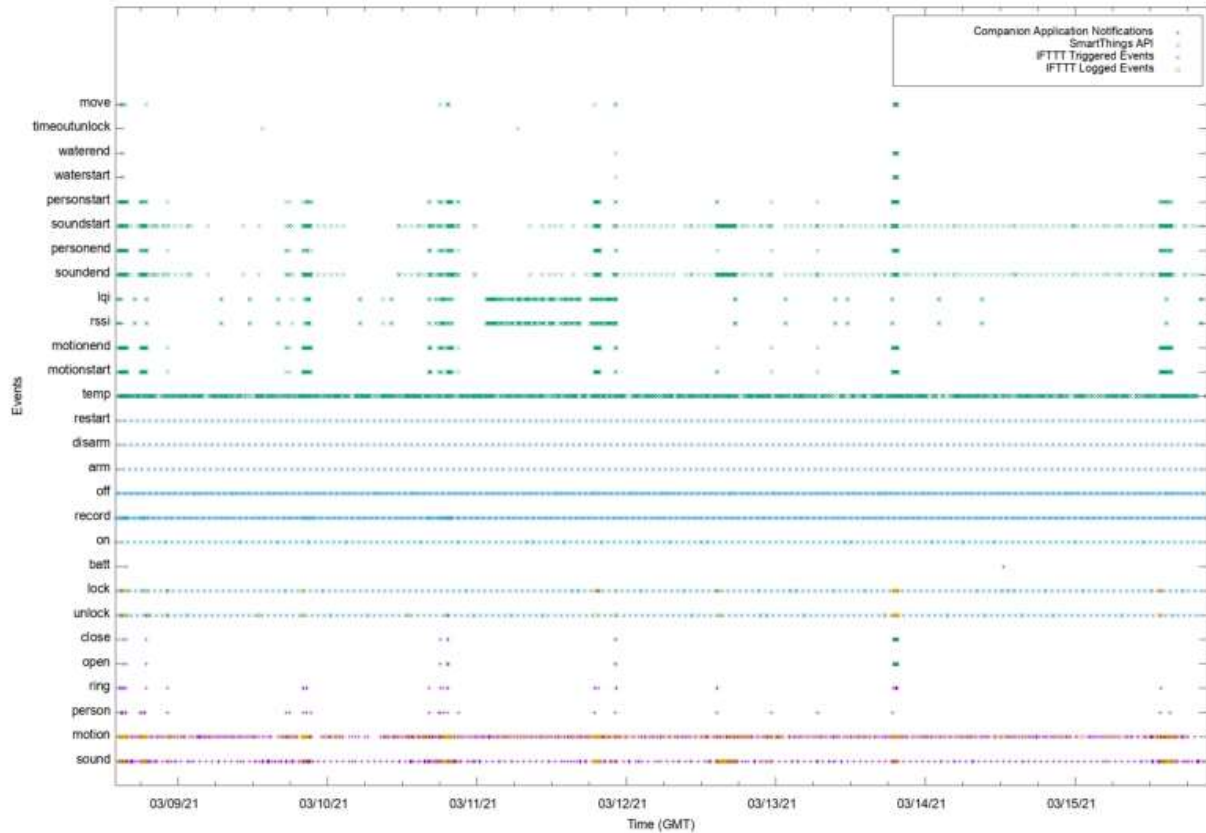
Note. We leverage event-driven logs from vendor application programming interfaces (APIs), including the SmartThings platform, to produce fine-grained labels of the device history.

IoT vendors often expose their devices' control and logging through application programming interfaces (APIs.) This transparent approach enables broad adoption of their products into other vendor ecosystems. Further, offering this unified set of capabilities supports enables cross-vendor integration into their ecosystems. As an illustration of these APIs, the widely popular SmartThings platform exposes a broad array of device capabilities and logs. Figure 6 depicts a partial history of SmartThings devices in our lab. In our work, we leverage these event-driven logs to produce fine-grained labels of the device history. Although IFTTT supports limited SmartThings integration, directly interfacing with the API exposes a fuller set of logged activity. As an example, our SmartThings water-leak sensor identifies and reports two events: the initial moisture detection and when the sensor no longer detects moisture. Only the initial moisture detection is available through IFTTT, whereas the complete picture is available

in the vendor API. In observation, vendor APIs offered better fidelity of their device histories than what is observable through IFTTT. Three environmental sensors that observed temperature (a multi-sensor, a water sensor, and a motion sensor) reported 1,618 events (or 9.70% of the aggregate of all labeled events in our dataset.)

Figure 7.

Summary of Device Activities Captured in Dataset



Note. We remotely triggered 4,944 events (29.63% dataset events) and automatically labeled an additional 11,742 events (70.37% events) created when researchers visited the lab daily and interacted with devices by unlocking doors, ringing doorbells, turning plugs on and off, walking nearby motion detection cameras, and speaking loudly.

We leveraged the IFTTT trigger action framework to trigger and log events, constructing 77 IFTTT recipes for 20 unique devices. We separated our approach into two IFTTT recipe types: recipes that logged manual events and recipes that automatically triggered events. The aggregate of our 77 IFTTT recipes generated roughly a third of all labeled activity in our dataset. Manual IFTTT recipes logged four different events (lock, unlock, motion, sound) across 10 IoT devices in our dataset, recording only 613 device events (or only 3.67% of total events.) While IFTTT was capable of manually logging more devices, we sourced labels from companion app notifications and vendor APIs with more precise time labels. Unfortunately, IFTTT only provides minute-level precision in timestamps, making it an unattractive source for manual logs. Automatic time-based trigger recipes generated eight events (arm, disarm, lock, unlock, turn off, turn on, record, restart) for 14 devices in our dataset, triggering 4,944 labeled events (29.63% of

our labeled events.) We leveraged IFTTT triggers in devices that controlled lighting and actuators to collect activities for environment sensors, like smart lighting and door locks. Both devices trigger significant environmental changes, which can be detected by CV-based motion detectors and audio sensors, allowing us to collect data from [environment] sensors without requiring physical interaction.

Figure 8.

During the Experiment, Motion Detection from 29 Devices Produced the Most Events and Accounted for 32.75% of Total Labeled Events



Major Findings and Key Outcomes.

Finding 1 - Impact of Motion Detection Source. During the experiment, motion detection produced the most events and accounted for 32.75% of total labeled events. Sound detection accounted for the next highest event at 16.85% of all labeled events. This percentage is unsurprising as 29 of our 57 devices offered motion-detection capability. However, we observed an interesting finding in the number of motion events per device. Despite the cameras being co-located in the lab as depicted in Figure 8 and set to the highest sensitivity rating, they reported varying degrees of motion events. As illustrated in Table 3, the Geeni Sentinel camera recorded 981 motion events during the period while the SimpliCam Security Camera observed a mere 14. We included multiple instances of the device for six camera models, including the Geeni Aware, Ring Video Doorbell, Ring Alarm motion, NightOwl doorbell, Blink camera, and Arlo Pro camera.

Examining these devices in Table 3 demonstrates that motion-event reporting corresponds to the device model as the same models report a similar number of events. Particular camera models may be more sensitive to detection depending upon if they use passive infrared (PIR) or computer vision (CV) sensors. CV sensors are cheaper to implement as their functionality is primarily implemented in software and is device-independent. CV is also popular on devices in areas that require the use of exclusion or inclusion zones, in which an end-user can select what areas can trigger motion detection events. PIR is typically used in Battery-powered devices as it requires no processing power to function. Including a PIR sensor can increase device complexity but vastly reduces the number of false detection events as a heat-

emitting object is required to trigger the sensor. With devices utilizing CV sensors, we observed significantly more events due to varying light sources in the lab. The most significant source of events occurred in periodic 15-minute intervals that correlated to when we remotely triggered our Phillips Hue LED bar lights. We surmised this action triggered the CV-based cameras during the experiment. We can contrast this behavior with our PIR-based devices, which only triggered when the camera sensors detected researchers in the vicinity.

Table 3.

Motion-Event Reporting Corresponded to Device Model as the Same Models Report A Similar Number of Events

Device	Motion / Sound	Flows	Sensor Type
Geeni Sentinel Smart Camera	981/0	1,525	CV
Geeni Aware Surveillance Camera 2	529/0	19,418	CV
Geeni Aware Surveillance Camera 1	486/0	19,381	CV
SmartThings Smart Camera	422/1,273	2,514	CV
SmartThings Motion Sensor	376/0	11,989	PIR
Ring Video Doorbell Pro	308/0	1,071	CV
Simplisafe Video Doorbell Pro	244/0	39	CV
TP-Link Kasa Spot Camera	211/983	2,213	CV
Geeni Doorpeek Smart Wi-Fi Doorbell	194/0	902	CV
Wyze Cam v2	191/74	10,743	CV
Nest Cam IQ Indoor	163/4	52	CV
Ring Video Doorbell 1	159/0	399	CV
Ring Video Doorbell 2	139/0	355	CV
Geeni Look Indoor Smart Security Camera 2	126/475	819	CV
Ring Spotlight Cam	117/0	698	CV
Merkury Innovations Smart Wifi Camera	83/0	773	CV
Geeni Doorscreen Smart Wi-Fi Doorbell	80/0	627	CV
Ring Alarm Motion Detector 1	76/0	416	PIR
Ring Alarm Motion Detector 2	74/0	416	PIR
Night Owl Doorbell 2	74/0	124,462	PIR
Ring Alarm Motion Detector 3	69/0	416	PIR
Night Owl Doorbell 1	47/0	124,227	PIR
Arlo Pro Smart Security Camera 2	46/0	3703	PIR
Blink Indoor Home Security Camera 3	45/0	42	PIR
Blink Indoor Home Security Camera 2	42/0	39	PIR
Blink Indoor Home Security Camera 1	39/0	37	PIR
Arlo Pro Smart Security Camera 1	38/0	3,703	PIR
Nest Hello Smart Wi-Fi Video Doorbell	31/2	83	CV
SimpliCam HD Indoor Security Camera	14/0	20	PIR

Note. Particular camera models may be more sensitive to detection depending upon if they use computer vision (CV) over passive infrared (PIR) sensors.

Finding 2 - Event Reporting to Flow Correlation. Previous work has proposed developing per-flow or per-packet classifiers to identify IoT device on-demand events (O'Connor, et al., 2019), (Trimananda, Varmarken, Markopoulou, & Demsky, 2020), (O'Connor, Enck, & Reaves, 2019), (Hariri, Giannelos, & Arief, 2019). Examining the ratio of events to network flows from our experiment offers insight into both approaches' practicality and

feasibility. Per-flow classifiers assume that classifiers can broadly apply labels to network flows (e.g., a particular flow is a motion-detection event.) This approach appears feasible by examining the Blink Cameras in our dataset. We observed our three battery-powered Blink Cameras recorded a total of 126 motion events over 121 short-lived TLS connections during the experiment. Due to the battery constraints, the Blink cameras exclusively communicated when they detected motion. However, this generalization does not apply across all devices. We observed 194 events from our Nest Camera, including 163 motion, 27 person-detection, and four sound events. Despite reporting 194 events, we only observed 52 unique TLS connections in our network traces. We surmised that the NEST Camera leverages persistent, long-lived TLS connections to report events. These long-lived flows consist of both idle and on-demand traffic. This finding echoes previous works that argue that packet signatures are a better indicator of on-demand events (O'Connor, Enck, & Reaves, 2019), (Hariri, Giannelos, & Arief, 2019), (Trimananda, Varmarken, Markopoulou, & Demsky, 2020).

Finding 3 - Impact of Using Turnkey Providers. Correlating DNS captures to event logs, we uncovered that four vendors exclusively queried DNS entries for turnkey providers. An additional vendor (Wyze) queried both turnkey providers and an in-house vendor-developed solution. These third-party or turnkey providers offer complete solutions that provide the required infrastructure and hardware components for an IoT ecosystem. For example, the Sciener turnkey platform provides the app SDK, Cloud API, and software libraries to rapidly develop an IoT ecosystem for a smart lock. Turnkey provider solutions reduce technical requirements for entering the IoT market by abstracting away development and allowing vendors to focus on manufacturing and deploying new products. Table 4 lists the vendors that leverage these turnkey providers and the on-demand actions they implement.

We uncovered that Geeni devices and their parent company Merkury, predominately rely on turnkey infrastructure from Tuya to handle reporting on-demand events. The Geeni DoorScreen, a recently purchased but now discontinued device, also leverages the Apexis turnkey platform. We investigated the Geeni DoorScreen camera and identified it was running the Apexis turnkey software as a corollary to this research. MITRE published a high-risk vulnerability for this platform in 2017. We subsequently reported three new Common Vulnerabilities and Exposures (CVEs) caused by integrating the Apexis platform on the Geeni DoorScreen doorbell. As the rapid proliferation of IoT devices continues and vendors expand, we must continue to seek greater transparency on these platforms' transport, storage, and processing methods.

Table 4.*Vendors that Leverage Turnkey Providers*

Device	Supported Actions	Turnkey Provider
Geeni Aware Surveillance Camera	motion	Tuya
Geeni Doorpeek Smart Doorbell	motion, ring	Tuya
Geeni Doorscreen Smart Doorbell	ring, motion	Tuya, ThroughTek, Apexis Alarms
Geeni Look Indoor Smart Camera	motion, sound	Tuya
Geeni Sentinel Smart Camera	motion	Tuya
Merkury Innovations Smart Camera	motion	Meari, Tuya
Merkury Smart Wi-Fi Doorbell Camera	motion, ring	Meari, Tuya
Schlage Encode Smart Deadbolt	lock, unlock, batt	Allegion ENGAGE, Amazon IoT-Core
Sifely Keyless Entry Door Lock	unlock	Sciener
Ultraloq U-Bolt Smart Deadbolt	unlock, lock	Amazon IoT-Core
Wyze Cam v2	motion, sound, record, restart, off, on	Internal, ThroughTek, Amazon IoT-Core

Note. We uncovered vendors and devices that exclusively relied on turnkey providers for their ecosystem development by correlating domain name requests to event logs.

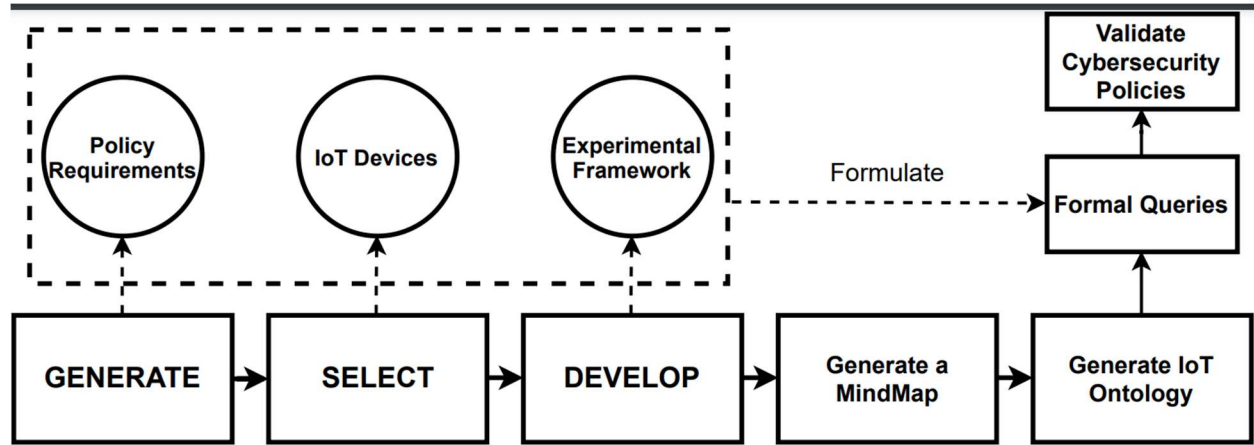
Objective 2. Research and Development of IoT Privacy and Security Policies

Task 2.1 Ontological Representation of IoT Devices

The availability and usage of the Internet of Things (IoT) have grown significantly over the last decade. This growth in ubiquitous computing has enabled continuous observation, decision making, and execution of actions to improve the livelihood of millions. However, IoT has also increased cybersecurity risk by making the user vulnerable to attacks from the outside or disclosing information without the user's knowledge. As a result, it becomes essential to understand the behavior of IoT devices and then model the behavior at a higher level of abstraction that enables automated reasoning, reducing the gap between policy requirements and its analysis. Towards this end, we have developed our proposed framework, which combines structured experimentation performed on the IoT devices, followed by modeling to store the knowledge for analysis. We leverage the experiment findings to formulate the model that enables automated analysis to check the potential behavior exhibited by the IoT device. The automated analysis guides the process of generating policies if the outcomes indicate a violation of security requirements. We demonstrate our approach by investigating the behavior of IoT devices and developing an Ontology of the same to check if the IoT device executes risky cybersecurity behavior.

Methods. Research indicates that modeling the behavior of IoT is important in order to formulate cybersecurity policies. In this research effort, we come up with a proposed methodological framework (Figure 9) that helps to model the behavior of IoT for the generation of cybersecurity policies.

Figure 9.
IoT Cybersecurity Policy Generation Methodology



We begin by generating “Policy Requirements” for the IoT devices that can help to increase user trust and privacy. For instance, a user might be interested in knowing if the IoT device used by him/her interacts with a cloud-based server that is located in a country outside his/her country of residence. After the requirements have been generated, we go ahead and “Select” IoT devices that will be used for experimentation. We then develop the experimental framework and perform experiments on the selected IoT devices. The experiments performed on the selected IoT devices aid the process of generating requirements for the Mind Map. A Mind Map is a diagram that is used to visually organize information. The information gathered from the experiment is transferred to the Mind Map which, helps to visually organize the information and makes it much easier to understand and comprehend. It lists all the entities along with their relationships and the associations between different entities. Using the entities and relationships listed in the Mind Map, we come up with a formal IoT ontology model which helps to run automated reasoning and draw inferences.

These experiments, along with policy requirements and device selection, help to formulate queries that are executed on the ontology to infer knowledge from the ontological model. The outcome of the query reasoning helps to validate the policies and detect any kind of violations. The experiments performed on the selected IoT devices aid the process of generating requirements for the Mind Map. A Mind Map is a diagram that is used to visually organize information. The information gathered from the experiment is transferred to the Mind Map which, helps to visually organize the information and makes it much easier to understand and comprehend. It lists all the entities along with their relationships and the associations between different entities. Using the entities and relationships listed in the Mind Map, we come up with a formal IoT ontology model which helps to run automated reasoning and draw inferences.

Generating Policy Requirements. One of the main areas of focus of this research effort is to aid the process of understanding the need for policies that help in increasing IoT trust and privacy. The aim is to develop a knowledge base that models the behavior of IoT devices for automated analysis, which is guided by some of the already existing and identified vulnerabilities related to security and privacy. For instance, in 2018, the US Military announced to reexamine its security policies after fitness tracker data was shared on social media that revealed bases and patrol routes (Hsu, 2018). Many such similar data privacy breaches have raised serious concerns

regarding security policies with respect to IoT. Through this research effort, we aim to come up with formal policies that can help prevent such security lapses.

In order to do so, we begin with the generation of policy requirements which have been categorized into four different categories:

1. Interaction: Does the system interact with external systems (Systems located outside a defined geographical location)?
2. Server Ownership: Who owns the server with which the system is interacting continuously?
3. Frequency: How often does the communication/packet sharing happen?
4. Size and Type (Secured or Unsecured) of Data: What is the size and type of data that is being shared by the system?

Policies pertaining to “*Interaction*” primarily focus on the interactions between the system and the outside world. They help to identify whether the system is interacting with any external servers and if the servers are trustworthy. For instance, a user might be interested in knowing if the IoT device used by him interacts with a server that is located outside his/her country of residence. Similarly, network packet monitoring might be of importance, and knowing the periodicity of communication can reveal some important insights about the system. Moreover, knowledge about the “Type and Size of Data” being shared by the device also helps to draw some important inferences relative to the security of the system. Knowing if the shared data is secured or unsecured is important since it will help to detect and prevent security vulnerabilities within the system. The knowledge about “Server Ownership” is also useful as the user might be interested in knowing whether the device interacts with a server that is owned by the manufacturing company of the device or does the company outsource it to a third-party cloud-based company. All these policy requirements not only increase user trust and privacy but also help to identify any type of violations or security breaches.

Experiments. Through the experimentation process, this study aims to come up with an abstract representation of the behavior of an IoT device that can be represented as an ontology so that we can build a knowledge base that can be used to perform automated reasoning to guide the generation of security policies. The *IoT Lab* at *Florida Tech* was set up and configured to perform experiments on fifty-six different types of IoT devices. As part of an ongoing experiment to automate device flow labels in *Florida Tech's IoT Lab*, IoT traffic was captured over a period of seven days on fifty-six devices. All the communication between the devices present inside the lab, and the outside world (network traffic entering and exiting the lab) was saved as packet capture files on a monitoring server while vendor APIs were periodically queried for event labels. For this study, we have particularly chosen Smart Doorbell IoT device because we believe that it will allow us to model an OWL representation that can be further generalized to represent any type of multimedia IoT device.

Figure 10.

Packets Are Ingested and Processed into a Queryable Format for Analysis

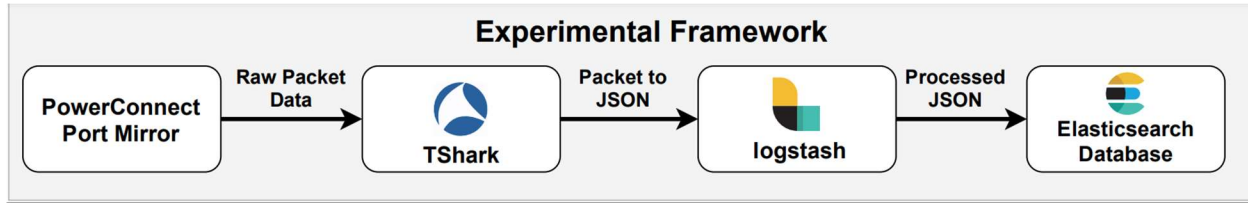
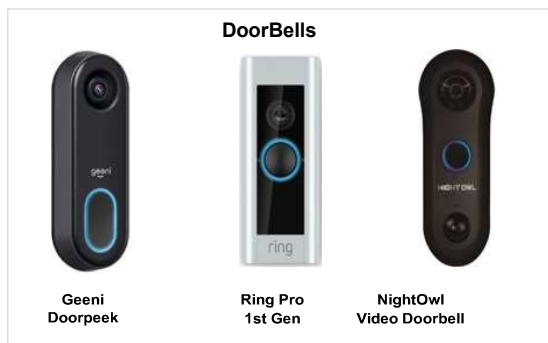


Figure 10 above represents the experimental framework. To start with, a Port Mirror is used to generate packet data in the raw format. Since the experiments were performed inside the University, Port Mirror helped in mirroring the packets and allowed for transparent packet capture, thereby emulating a home environment. This approach allowed to capture network packets from a setup that used the same components of the network in a passive and transparent manner. For interactive analysis, captured data is fed to Wireshark’s command line processor, TShark (a network protocol analyzer), which converts the captured packet data into JSON objects. These JSON objects are then processed into Elasticsearch’s logstash (server-side data processing pipeline), which buffers and post-processes the ingested data. This results in network packet data which are in the form of processed JSON objects that can be stored inside a database and queried for analysis. Finally, this information is stored in the Elasticsearch database so that it can be analyzed in Kibana (a query language and data visualization dashboard for ElasticSearch), which allows us to perform aggregations and visualizations on each device separately and independently.

Figure 11.

Doorbells Used for Experimentation



For this study, three different doorbells (Figure 11) were selected for analysis based on “availability,” “observed maturity,” and “vendor popularity.” The devices were obtained by purchasing through popular online retailers and physical stores. To represent major vendors, a Ring Video Doorbell Pro 1st generation was selected. We selected a Geeni Doorpeek 1080p Wireless Doorbell and a NightOwl Video Doorbell as these were widely available. We term NightOwl’s vendor as an “immature” vendor because it was realized during the experimentation that it employs industry-wide bad practices, which could be due to a lack of experience in the IoT security domain.

Hardware Analysis. Vendors have a wide variety of hardware components that they can integrate into the final product. Generally, only major components are publicly identified, obscuring common dependencies or features that may exist across multiple devices. For this paper, we disassembled the three doorbells to identify common hardware patterns and components.

We discovered that the Night Owl and Geeni Doorbells shared the most components. Both utilized a “HiSilicon” based ARM processor and an “SPI-based” flash chip for storing the operating system software. Alongside these components, we discovered a “UART” serial console and a small battery source to keep the system online during intermittent power outages. All devices contained a removable camera module and USB-based WiFi module, as well as a USB port for powering the device without the use of a doorbell transformer. Device-specific components, like NightOwl’s PIR sensor, are further documented in the Mind Map (Figure 13).

Firmware Analysis. During our analysis, we discovered a few calls from the HiSilicon based devices, which we could not map to specific features. We previously identified that these devices utilized an ARM processor and an SPI flash chip for storing code. We hypothesized that an offline SPI programmer might be able to download the device firmware for offline analysis. Furthermore, if code signing or boot verification was not discovered, we could modify and upload the new firmware to perform dynamic analysis on the devices.

To perform the chip read and write, we utilized a CH341a SPI programmer, as indicated in Figure 12. The programmer is available on several online retailers with a non-invasive clip to allow chip interaction without removing components. Firmware was downloaded and extracted using popular tools like Binwalk and Binary Ninja to perform extraction and analysis. Additionally, both devices contained telnet daemons and hard-coded admin credentials for remote management, which we overwrote to allow local access for dynamic analysis.

Figure 12.

A Disassembled View of Doorbell to Identify Ligh-Level Hardware Components



Note. Firmware can also be downloaded when applicable to identify network flows.

Generalized Observations. As indicated in Table 5, we discovered variations on APIs contacted, hosting providers used, the use of encryption, and the demographic presence of all three devices. Most notably, Ring appeared to utilize services that were both demographically internal and first-party in nature. We contrasted this with the Geeni doorbell, where services appeared to be completely third-party in nature but demographically internal. Night Owl used a

mix of first- and third-party services. We observed similar patterns in the use of hosting providers when first-party sources were used. All vendors used Amazon Web Services almost exclusively, but Night Owl included an additional hosting provider for their first-party sources.

Ring transmitted the largest amount of data, with Night Owl following closely. These transmissions occurred primarily on event boundaries and were destined for identified CDN endpoints that mirror audio and video style uploads. This is contrasted with the Geeni Doorbell, which sent the least amount of data. The Geeni doorbell only generated small amounts of data which could coincide with single frame uploads. We also observed several time-bounded flows which repeatedly occurred when dealing with update and API end- points.

Generalized IoT Environments. For the following sections, specific environment traits are compared with the typical IoT model, which separates CDNs, API, and Core servers from users and end devices. For all data tables, DNS and NTP traffic was filtered. While both are necessary for device function, neither significantly contributes to any of our findings.

Ring Doorbell Pro. The Ring Doorbell recorded a total of 341 event labels over the course of the experiment. Of these events, 33 were generated by physically ringing the doorbell, and 308 were generated by triggering the device motion sensor. Along with these events, we identified a total of 1,720 flows. Six hundred forty-eight flows were performed over UDP connections to what appeared to be CDN server pools. Four TCP connections were made to `lpd.ring.com` and were long-lived in nature, mirroring Core Server / idle connection functionality for on-demand events. Four hundred nineteen TCP connections were made to `fw.ring.com`, performing what we believe were firmware update checks. LPD and FW connections transferred less than 30MB of data in a 7-day period, emphasizing the possibility of API-exclusive data.

`Es.ring.com` was resolved using the DNS alias `event-sink-gw.ring.com`. We observed the creation of 250 TCP connections which occurred around event boundaries. Only one connection stayed open for more than 3 seconds, with a large majority closing within 0-1 seconds. Most data was transmitted to unresolved addresses over 399 TCP and 648 UDP connections for 1GB and 5GB of data, respectively. For both categories of data, we observed connection times typically ranging from 10-60 seconds, mirroring typical media upload behaviors. 206 IP addresses were returned as possible endpoints for `es.ring.com` versus 352 possible endpoints for the CDN-styled endpoints. We contrast this with LPD, which only returned 19 possible endpoints. We hypothesize that a significantly larger pool of media-oriented endpoints exists to handle the larger amount of transmitted media. ES and LPD scale down accordingly, which appears to correlate with the amount of handled data. Table 6 summarizes the behaviors observed during the experimentation process.

NightOwl Doorbell. The NightOwl doorbell recorded 76 total events. Of these events, 29 were generated by physically pressing a button, while 47 were generated by triggering the device motion sensor. While the doorbell press events were close to what we observed with the Ring doorbell, the motion events were drastically reduced. We hypothesize that NightOwl's decision to include a dedicated motion-sensing hardware component caused this reduction. Many motion sensors were triggered by lab lights periodically cycling on and off. PIR-based sensors were not activated by these events, mirroring the behavior observed in the NightOwl doorbell, which corresponded with in-person movement events.

NightOwl spread connections over four first-party domains and six unresolved endpoints. Of the four first-party domains, both host.nightowl domains are hosted under Liquid Web LLC. Update and cloud storage are hosted under Amazon Web Services. Of the six unresolved endpoints, five are used to facilitate P2P streaming of the camera’s video feed. These endpoints are configured globally, with two endpoints located in China, one in the Netherlands and the remainder in the United States. One unknown TCP endpoint hosts an insecure web server used to generate push notification events.

Update.nightowlsuper.com also hosted an insecure web server used to indicate when a software update was available. Over the course of the experiment, the NightOwl doorbell connected twice to this endpoint. The two host.nightowl.com endpoints maintained long-lived UDP connections, which periodically transmitted data. The sent data was not deeply investigated, but very few bytes changed between packets indicating a lack of or poorly implemented encryption. The only encrypted connections were made under a cloud-storage.nightowlconnect.com, which was hosted on Amazon Web Services. Conveniently, this endpoint appears to connect exclusively over port 443/TCP, which is a common endpoint for web-based APIs. We observed 124,126 unique connections to this endpoint, with connection times ranging from 0 seconds to 2 days, with an average time of 3 seconds. Furthermore, almost 1GB of data is transferred during our experiment, indicating its use as a potential CDN on top of API data. Over all endpoints, cloud-storage.nightowlconnect.com appeared to be the only endpoint that utilized encryption. All others were either performed over insecure HTTP or used a poor implementation on top of an unknown protocol. Table 7 summarizes the observations and lists the important data flows.

Geeni Doorpeek Doorbell. The Geeni doorbell recorded a total of 232 events. Of these events, 38 corresponded to physical button presses, and 194 corresponded to motion events. This correlates with the Ring Doorbell reported events and matches our previous hypothesis that the Night Owl reduction is caused by the hardware sensor. Geeni also reports changing light conditions as motion, bolstering its numbers up to Ring’s reported numbers which use similar technology. However, Ring still reported 100 additional events that the Geeni doorbell failed to detect.

We did not detect any first-party domains for the Geeni doorbell. Instead, we observed the direct use of Tuya endpoints, AWS Storage gateways, and two direct AWS S3 endpoints over 903 TCP flows. Under Tuya, we discovered two endpoints, aws4nat and aws3nat, which are used to assist in P2P applications like video and audio streaming. These endpoints represent six UDP flows out of the 909 total. ty-us-storage30’s 193 TCP connections and the 38 unknown connections resolve to Amazon Web Services S3 endpoints, which are used to upload and retrieve data in the cloud. We also observe that the sum of both services comes out to 231 unique connections, one event short of our reported event count. This bolsters our theory on its use as a CDN endpoint and also verifies that the device is only uploading to these endpoints on event boundaries. m2.tuya.com connections are exclusively MQTT which is traditionally used for long-lived idle connections for real-time commands on end devices. This mirrors Ring’s use of lpd.ring.com for holding long-term connections to control devices. Finally, a2.tuya.com connects exclusively over port 443, leverage fast, on-demand connections for small bursts of data over 633 short-lived connections. This corresponds with firmware update checks, event data, or API requests. Table 8 summarizes the experimental observations.

Table 5.
Experimental Observations

Device	First/Third Party	Host/Vendor	Demographic Presence
Ring Video Doorbell Pro	First	Amazon AWS	Internal
Geeni Doorpeek	Third Mixed	Tuya, AWS	Internal
Nightowl Doorbell		First Party - Amazon AWS, Liquid Web Third Party - Unknown / Private	Mixed

Table 6.
Ring Doorbell Experimental Observations

DNS	Encrypted	Load Balanced	TCP / UDP Flows	Total Data Sent / Received	Purpose
lpd.ring.com	Y	Y	4 / 0	26.10 MB	API
es.ring.com	Y	Y	250 / 0	142.78 MB	API
fw.ring.com	Y	Y	419 / 0	4.66 MB	Updates
N/A	Y	Y	399 / 648	1.08 GB TCP / 5.20 GB UDP	CDN / Unk

Table 7.
Nightowl Doorbell Experimental Observations

DNS	Encrypted	Load Balanced	TCP / UDP Flows	Total Data Sent / Received	Purpose
cloud-storage.nightowlconnect.com	Y	Y	124126 / 0	916.04 MB	API / CDN
host.nightowldvr07.com	N	N	0 / 3	69.11 MB	Unk
host.nightowldvr08.com	N	N	0 / 3	69.12 MB	Unk
update.nightowlsuper.com	N	Y	2 / 0	2.16 KB	Update
N/A	N	N	98 / 15	123.03 KB TCP / 7.84 KB UDP	PNS / P2P

Table 8.
Geeni Doorpeek Doorbell Experimental Observations

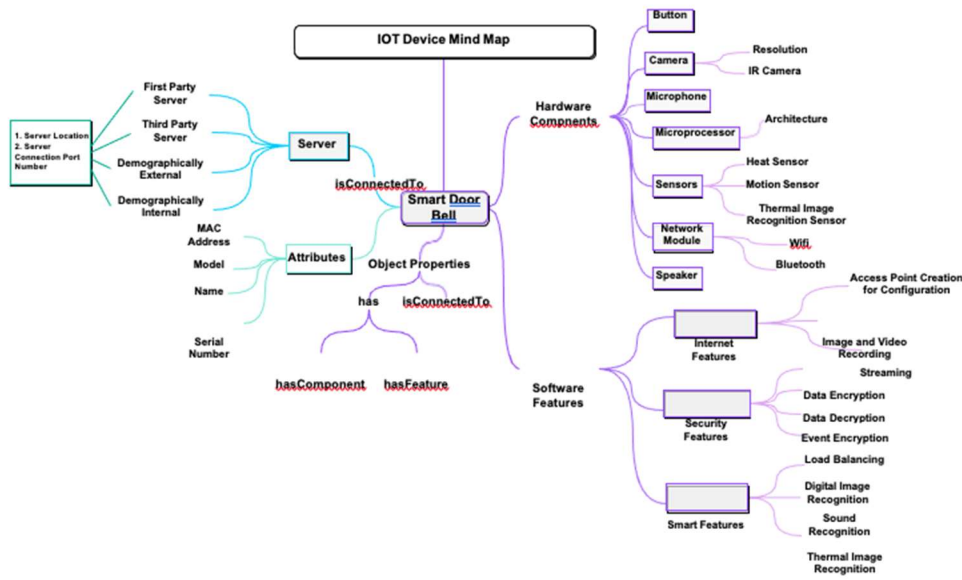
DNS	Encrypted	Load Balanced	TCP / UDP Flows	Data	Purpose
aws3nat.tuyaus.com	Y	Y	0 / 3	4.20 KB	P2P
aws4nat.tuyaus.com	Y	Y	0 / 3	3.17 KB	P2P
a2.tuyaus.com	Y	Y	633 / 0	3.40 MB	API
m2.tuyaus.com	Y	Y	39 / 0	6.59 MB	API
ty-us-storage30...	Y	Y	193 / 0	13.22 MB	CDN
N/A	Y	Y	38 / 0	1.94 MB	CDN

Requirement Generation for IoT Ontology Framework. Based on the extensive experimentation which was conducted on different Smart Doorbell devices, the requirements for IoT Ontology were identified. The experimentation helped to identify the various components that are present in the Smart Doorbell device and also aided in formulating the relationship between the various entities.

The captured information for the IoT Ontology is depicted through a Mind Map in Figure 13. Mind Map is a concept used for information mapping and assists in the diagrammatic organization of information (Mahoney, et al., 2010). It is often created around a single concept to which other objects/entities are linked using associated representations. Mind Map helps to visually organize information that may otherwise be hard to comprehend. At the core of the IoT Mind Map (Figure 13) is the *Smart Doorbell* class that has different types of *Hardware Components* such as *Button*, *Camera*, *Microphone*, *Microprocessor*, *Sensors*, *Network Module* and *Speaker*. Each of these hardware components further has sub classes indicating the specific type of hardware component that is present in the Smart Doorbell. For instance, some of the doorbells had all three kinds of sensors (*Heat Sensor*, *Motion Sensor*, and *Thermal Image Recognition Sensor*), whereas some had only a few of them. Similarly, some doorbells had *IR Camera*, whereas some had a normal camera with no infrared capabilities. The smart doorbells also have *Software Features* such as *Internet Features*, *Security Features*, and *Smart Features*. Each feature is further composed of sub-features that are incorporated within their functionality. As part of *Internet Features*, the doorbells create an access point for configuration and initialization and also stream the audio and video data over the network. Some doorbells undergo data encryption and decryption, thereby adding more security to the packet communication. Some specific bells even perform load balancing to avoid packet overloading while data communication. Modernized doorbells have some specific smart features built-in

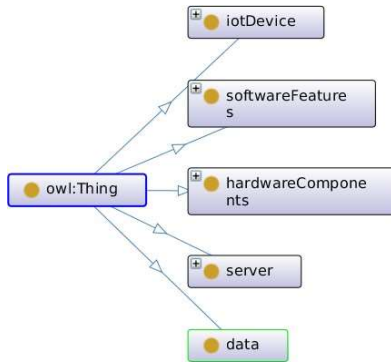
them, such as *Digital Image Recognition*, *Sound Recognition*, and *Thermal Image Recognition*. Almost all the smart doorbells are connected to the server and based on their types; the servers have been classified into *First Party*, *Third Party*, *Demographically External*, and *Demographically Internal* servers. Different *Attributes* of a smart doorbell such as *MAC Address*, *Model*, *Name*, and *Serial Number* were identified, which are stored in the IoT Ontology Framework in order to create the knowledge base. These requirements help to come up with an IoT Ontology Framework wherein we can create a knowledge base to draw inferences through automated reasoning.

Figure 13.
IoT Mind Map



Model. Formal representation capability for different kinds of knowledge is provided within an Ontology framework. A knowledge framework can be constructed and formalized for a specific ontology by leveraging an ontology language. OWL, endorsed by the W3C, is one of the most recent developments in standard ontology language. We use Protege 5.5.0 (Musen, 2015), a free, open-source ontology editor and knowledge base construction tool, to develop an IoT Framework and use automated reasoning to infer knowledge from already existing knowledge. It consists of different built-in elements such as Classes Tab, Object Properties Tab, Data Properties Tab, Individuals Tab, Rules Tab, etc. Protege's most important feature is that it can be executed by a DL reasoner that provides for classification, consistency checking, and policy validation within the knowledge framework. In this work, we use protégé to formally model and represent the requirements that have been graphically listed through the Mind Map. We further go on to create instances in order to build a knowledge base that can be reasoned using Pellet reasoner (Parsia & Sirin, 2004). The inferences are drawn from reasoning assist in invalidating the need for policies.

Figure 14.
OWL Thing Class, Data Properties, and Object Properties Are Omitted



To begin with, every model in Ontology contains a superclass known as the “*Thing*” class which then flows down into other sub-classes. All other classes are sub-classes of the “*Thing*” class. The IoT device Ontology’s Thing class has five child classes, namely “*IoTDevice*,” “*server*,” “*softwareFeatures*,” “*data*,” and “*hardwareComponents*,” as seen in Figure 14. It is noteworthy that all five classes are disjoint with each other. The “*IoTDevice*” class is further decomposed into sub-classes, as represented in Figure 15. The “*smartDoorBell*,” “*smartDoorLock*,” and “*smartWatch*” are child classes that inherit all the features and properties of the “*IoTDevice*” class. We mainly focus on the “*smartDoorBell*” and create instances with data properties for each of the vendors we experimented with. The data properties that have been generated during the experimentation process are used to formulate the knowledge base within the IoT Ontology. We can then perform automated reasoning on this knowledge base for consistency checking and validation. We try to list all important data properties that we believe will help in drawing insightful inferences. The “*IoTDevice*” class is disjoint with the “*server*” class, indicating that a server cannot be an IoT device and vice-versa. The “*IoTDevice*” is associated with the “*server*” through the “*isConnectedTo*” object property association, indicating that each IoT device is connected to at least one or more servers. The “*server*” class is a representation of a cloud-based server that provides connectivity to IoT devices for data storage and other types of communication such as encryption-decryption, TLS handshaking, etc. It might be of relevance to know the location of the server with which the IoT device is interacting. Moreover, it is also important to know if the server is owned by the manufacturing company itself or it is being outsourced. Every instance of a server has certain data property attributes such as “*encryptedConnection*,” “*portNumber*,” “*serverLocation*,” “*thirdPartyorFirstParty*,” “*demographicallyExternalorInternal*,” and “*serverType*” that define its behavior.

Figure 15.

OWL IoT device Class, Data Properties, and Object Properties are Omitted

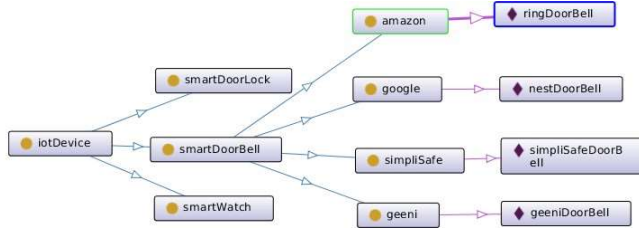


Figure 16 represents the “*softwareFeatures*” class which is a subclass of “*Thing*” and is disjoint with the “*IoTDevice*” class. It represents various software features that are found in smart doorbells. The features have been categorized into three broad categories, which are “*securityFeatures*,” “*internetFeatures*,” and “*smartFeatures*.” Each category is further sub-categorized and is indicative of the features that are present in the doorbells. Security features such as “*loadBalancing*,” “*eventEncryption*,” etc., make the device and communication secure. Similarly, Internet Features such as “*streaming*,” “*imageRecognition*,” etc., indicate the general behavior of the doorbell. There are some bells that incorporate certain smart features into their functionality, such as “*soundRecognition*,” “*thermalImageRecognition*,” etc. Every doorbell has a unique behavior and may contain one or more of such features. The data properties are formulated in a way that querying can indicate if a particular doorbell supports a feature or not. For instance, we can query to find out if the “Ring” doorbell performs “*eventEncryption*” or “*dataEncryption*.”

Figure 16.

OWL Software Features Class, Data Properties, and Object Properties are Omitted

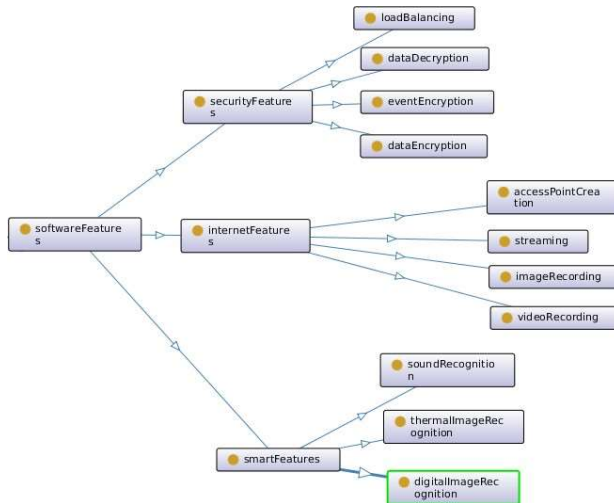
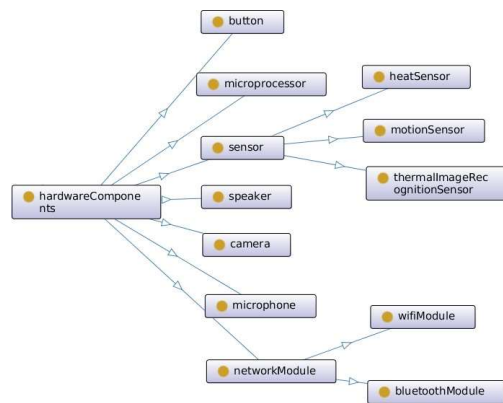


Figure 17.

OWL Hardware Components Class, Data Properties, and Object Properties are Omitted



The “*hardwareComponents*” class shown above in Figure 17 is disjoint with the “*IoTDevice*” class and represents the various hardware components that are present inside the doorbell. A majority of the doorbells have a “*button*,” “*microprocessor*,” “*speaker*,” “*camera*,” and “*microphone*.” Some doorbells like the smart doorbells provide additional functionalities such as “*heatSensor*,” “*motionSensor*,” “*thermalImageRecognitionSensor*,” and “*networkModule*.” Depending on the components present inside a doorbell, we have created instances of each and listed the data properties that help to create the knowledge base. Similarly, the “*Data*” class, as shown in Figure 14, represents the data that is sent and received by the IoT device. It has attributes to store certain data properties such as the Type and Size of data which are essential to infer knowledge and come up with secure policies. The “*smartDoorBell*” class is connected to the “*Data*” class through an object property assertion “*sendsAndReceives*.”

Automated Reasoning in Protege. Reasoning within ontology helps draw inferences and can be achieved using in-built reasoners. In its normal distribution, Protege includes a variety of reasoners. Pellet is available in Protege through a reasoner Plug-in, thereby providing Pellet’s special capabilities for checking ontology consistency. Reasoning helps infer new knowledge from the existing knowledge within an ontology. Classification is one of the most widely known usages of an automated reasoner. Classification is invoked as soon as we run the Pellet reasoner in Protege. The classification process involves three steps. Firstly, it checks whether the structure of OWL ontology satisfies all axioms or not. If it does not satisfy all the axioms, it will classify the model to be inconsistent and return a warning. All inconsistencies must be rectified in order to move forward and perform reasoning. Secondly, it will check whether there exists a structure that satisfies all the axioms in the model and in which A has an instance, say y, where A is a class and y is an instance of any class. Lastly, for any two class names, say X and Y, that occur in the model, the reasoner tests whether each instance of X is also an instance of Y. The results of these tests are shown in the Protege OWL editor in the form of the inferred class hierarchy. For our model, Figure 18 graphically depicts the inferred class type for the instance ring. Even though we do not explicitly specify its type, the reasoner based on the inherited knowledge defines it as a “*smartDoorBell*.”

Figure 18.

Inferred Knowledge For Ring Instance Using Pellet Reasoner



After classification using the Pellet reasoner, we perform automated reasoning on the IoT Ontology framework using SPARQL (Liang & Xue, 2010) query to infer knowledge from the existing knowledge base. SPARQL (Liang & Xue, 2010), being a Resource Description Format (RDF) query language, allows to retrieve and manipulate information stored in ontology in RDF format. SPARQL querying allows for more deductive powerful reasoning than OWL alone and provides similar strong formal guarantees when performing inferences. OWL allows for automated reasoning using different web rule languages such as SPARQL, SWRL, RuleML, etc. We prefer SPARQL over SWRL and other querying languages because it is being used more extensively for automated reasoning and allows support with the latest version of Protege. SPARQL allows querying of the entire knowledge base, which is a set of “*subject-predicate-object*” triples. It specifies four different query variations for specific purposes: 1. **SELECT** query, 2. **CONSTRUCT** query, 3. **ASK** query, and 4. **DESCRIBE** query. The “SELECT” query is used to extract raw values from a SPARQL endpoint, the “CONSTRUCT” query transforms the extracted information into valid RDF, the “ASK” query is a question query that returns true/false, and the “DESCRIBE” query also helps to extract RDF graph from the SPARQL endpoint, but it gives more freedom and flexibility to the maintainer. To query our model, we mainly use the “SELECT” and the “ASK” query to infer knowledge from the knowledge base. The queries are executed against the knowledge base, which returns a list of tuples of ontology values that satisfy the query.

Results. In this section, we present the results of policy requirements that were validated through SPARQL reasoning and querying. As discussed in the previous sections, we began by listing and categorizing the policy requirements, which guided the experimental flow. The experiments discussed above helped in providing the formal requirements for the ontology. We formally modeled these requirements after identifying the various components, attributes, and their associations. After modeling, the automated reasoning helped to check for any inconsistencies and flaws within the framework, which were rectified. As part of the last step, validation of the four main policies was achieved through querying.

Table 9.
Policy Requirements, SPARQL Based Queries, Outcomes

Requirements	Query	Outcome
1. Interaction	SELECT ?name ?server ?Demographics ?Location WHERE { ?name test:isConnectedTo ?server. ?server test:demographicallyExternalorInternal ?Demographics . ?server test:serverLocation ?Location}	name, server, Demographics, Location ring, server2, “Internal,” “USA” geeni, server1, “Both,” “USA, Belgium” nightOwl, server3, “External,” “China”
2. Server Ownership	ASK {test:ring test:isConnectedTo test:server2 . test:server2 test:thirdPartyorFirstParty ”First”^^xsd:string}	True
3. Frequency	SELECT ?name ?server ?FrequencyOfInteraction WHERE { ?name test:isConnectedTo ?server. ?server test:frequencyofInteraction ?FrequencyOfInteraction}	name, server, FrequencyOfInteraction ring, server2, “continuous” geeni, server1, “periodic” nightOwl, server3, “discrete”
4. Size and Type (Secured or Unsecured) of Data	SELECT ?name ?data ?SizeOfData ?TypeOfData ?Security WHERE { ?name test:sendsAndReceives ?data. ?data test:totalSize ?SizeOfData . ?data test:typeOfData ?TypeOfData . ?data test:dataEncryption ?Security}	name, data, SizeOfData, TypeOfData, Security geeni, dataGeeni, “13.22Mb,” “Multimedia,” “Unsecured” ring, dataRing, “26Mb,” “JSON,” “Secured” nightOwl, dataNight, “51Mb,” “Multimedia,” “Both”

Table 9 lists the different categories of policy requirements along with the SPARQL based queries and their outcomes. We first list the policy requirement for “*Interaction*” wherein the user might be interested in knowing if the system interacts with systems that are located outside a defined geographical region. The result of the query lists the name of the countries where the servers are located with which the system is interacting and sharing information. We then list the formal query for “*Server Ownership*,” wherein the user might be interested in knowing the company that owns the server. The “*ASK*” query results in a Boolean value indicating that the ring doorbell is interacting with a server that is a first party server and is owned by the company itself. Next, the frequency policy requirement is translated into a formal

representation. The result of the query lists the frequency of interaction between the doorbell and the server to which it is connected. For instance, the ring doorbell continuously interacts with the server to share information. Lastly, a user might be interested in knowing some properties of the data (size, type, and security) that are being shared by the device with the server. In total, we listed around 50 formal queries from different categories. The outcomes of these queries not only help to infer knowledge, identify potential security vulnerabilities but can also help to validate the existing policies. The checking of violation of security, potential security vulnerabilities are important to identify because it'll help to formulate new policies in the future that are more secure and ensure user privacy. For instance, the users might want to restrict interactions with servers that are located outside a defined geographical region. This specifically becomes important when the devices are being used for special tasks or by special forces deployed by national agencies. In order to ensure the same, a policy can be formulated that restricts any interaction with the outside world. We believe the proposed formalization and framework will help to bridge the knowledge gap or lack of awareness that exists.

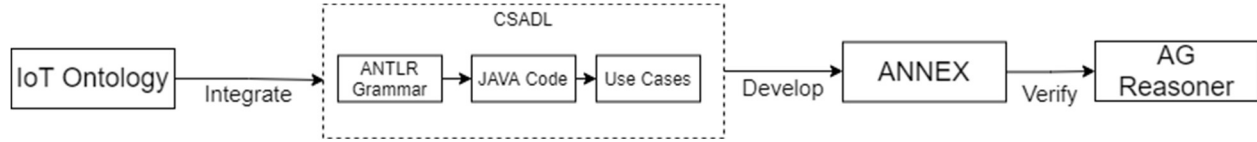
Major Findings and Key Outcomes. The major finding of our research was the detection of suspicious behavior exhibited by IoT devices. These suspicious behaviors were guided by a structured approach to capturing them as requirements. In this research effort, we hypothesized and formulated a framework that enables capturing relevant information regarding the behavior of IoT devices guided by requirements focusing on capturing security vulnerabilities. We then employed the captured experimental knowledge to develop an ontological representation at a higher level of abstraction to perform automated reasoning. Our effort also demonstrated the integration of experimental knowledge with formal modeling to enable reasoning at a level of abstraction closer to requirements. It includes modeling objects and associations for automated reasoning. The models allow future research efforts to focus on context-based mitigation of security vulnerabilities by including human-machine interactions.

Task 2.2 Extending the CSADL Framework to Integrate IoT Scenarios

The objective of this research is to expand the design of an existing assurance framework for cybersecurity with assume-guarantee reasoning, which allows the integration of IoT scenarios. In the past, we proposed a software engineering-based formal approach to model and analyze cybersecurity, that along with the identification of concrete requirements, enables automated analysis to guarantee cybersecurity properties are satisfied within the network. At present, this research is focused on developing a system/software engineering approach for designing a security framework to check the satisfaction of critical properties early in the design phase. In this research, we formally model IoT scenarios within the Cybersecurity Architecture Definition Language (CSADL), in-order to formally verify critical properties that help eliminate the risks associated with security and privacy.

Methods. Figure 19 illustrates the method used in this study.

Figure 19.
Proposed Methodological Framework



As part of this research work, we expanded an ontology-guided assume-guarantee-based formal approach to model and analyzed an IoT network. We first developed an IoT Ontology within Protégé, an OWL development environment. After knowledge representation within OWL, we integrated the IoT Ontology and formulated a new specification language, ANTLR Grammar. Using the ANTLR Grammar, we ran a JAVA program to interface the knowledge representation with reasoning constructs to develop an Assume-Guarantee reasoner. We ran few use cases on the reasoner to verify certain specifications within the IoT Ontology. The reasoner allows for reasoning at a higher level of abstraction, thereby hiding all the minute and technical details from the user.

Figure 20.
IoT Ontology ANTLR Grammar

```

grammar security;

csadl: BEGIN statement+ END ;

statement: (assumption1 | assumption2 | guarantee1 | guarantee2 ) ENDSYMBOL ;
assumption1: ASSUMPTION ASSET_IOT_DEVICE ASSOCIATION_CONNECT ASSET_SERVER ;
assumption2: ASSUMPTION ASSET_COMPUTER ASSOCIATION_CONNECT (ASSET_SERVER | ASSET_COMPUTER | ASSET_IOT_DEVICE) ;
assumption3: ASSUMPTION ASSET_IOT_DEVICE ASSOCIATION_HAS (ASSET_SOFTWARE_FEATURE | ASSET_HARDWARE_COMPONENT) ;

guarantee1: GUARANTEE ASSET_IOT_DEVICE ACTION_COMMUNICATE THING ASSET_SERVER ;
guarantee2: GUARANTEE ASSET_COMPUTER ACTION_COMMUNICATE THING (ASSET_SERVER | ASSET_COMPUTER | ASSET_IOT_DEVICE);
guarantee3: GUARANTEE ASSET_IOT_DEVICE ACTION_HAS SOFTWARE_FEATURE ; // come up with a guarantee for hardware components

// assumption1: ASSUMPTION ASSET ASSOCIATION (ASSET|MESSAGE) ;
// assumption2: ASSUMPTION MESSAGE SENSITIVITY CONTENT;
// guarantee: GUARANTEE ASSET ACTION (ASSET|MESSAGE) ;

```

Figure 20 depicts a snippet of the ANTLR grammar that has been developed to incorporate formal reasoning within the IoT Ontology. A statement specified by the user is a set of assumptions and guarantees, and the reasoner will validate the guarantees based on the specified assumptions. For instance, a generalized representation of an assumption-guarantee pair is as follows:

AG Pair 1:

```

assumption1: ASSUMPTION ASSET_IOT_DEVICE ASSOCIATION_CONNECT
ASSET_SERVER; guarantee1: GUARANTEE ASSET_IOT_DEVICE
ACTION_COMMUNICATE THING ASSET_SERVER;

```

The possible example specifications for this pair are:

```

assume IoTDeviceA isConnectedTo serverA;

```

guarantee IoTDeviceA send data serverA;	guarantee IoTDeviceA
send message serverA;	guarantee IoTDeviceA receive data serverA;
guarantee IoTDeviceA receive message serverA;	

AG Pair 2:

```
assumption2: ASSUMPTION ASSET_COMPUTER ASSOCIATION_CONNECT
(ASSET_SERVER | ASSET_COMPUTER | ASSET_IOT_DEVICE)
```

guarantee2: GUARANTEE ASSET_COMPUTER ACTION_COMMUNICATE THING
(ASSET_SERVER | ASSET_COMPUTER | ASSET_IOT_DEVICE)

The possible example specifications for this pair are:

```
assumption asset_computer association_connect asset_server;
```

assume computerA isConnectedTo serverA;

```
assumption asset_computer association_connect asset_computer;
```

assume computerA isConnectedTo computerB;

```
assumption asset_computer association_connect asset_IoT_device;
```

```
assume computerA isConnectedTo IoTDeviceA;
```

```
(guarantee asset_computer action_communicate thing (asset_server | asset_computer |
asset IoT_device);)
```

guarantee asset_computer action_communicate thing asset_server;

guarantee computerA send data serverA;

guarantee computerA send message serverA;

guarantee computerA receive data serverA;

guarantee computerA receive message serverA;

guarantee asset_computer action_communicate thing asset_computer;

guarantee computerA send data computerB;

guarantee computerA send message computerB;

guarantee computerB receive data computerB;

guarantee computer receive message computerB;

guarantee asset_computer action_communicate thing asset_IoT_device;

guarantee computerA send data IoTDeviceA;

guarantee computerA send message IoTDeviceA;

guarantee computerB receive data IoTDeviceA;

guarantee computer receive message IoTDeviceA;

AG Pair3:

assumption3: ASSUMPTION ASSET_IOT_DEVICE ASSOCIATION_HAS
(ASSET_SOFTWARE_FEATURE | ASSET_HARDWARE_COMPONENT);

guarantee3: GUARANTEE ASSET_IOT_DEVICE ACTION_HAS SOFTWARE_FEATURE;

The possible example specifications for this pair are:

(assumption asset_IoT_device association_has (asset_software_feature |
asset_hardware_component);)

assumption asset_IoT_device association_has asset_software_feature;

assume IoTDeviceA has internetFeature;

assume IoTDeviceA has securityFeature;

assume IoTDeviceA has smartFeature;

assumption asset_IoT_device association_has asset_hardware_component;

```

assume IoTDeviceB has hardwareComponentCamera;

assume IoTDeviceC has hardwareComponentMicroprocessor;

```

```

(guarantee asset_IoT_device action_has software_feature;)

```

```

guarantee IoTDeviceA performs accessPointCreation;

```

```

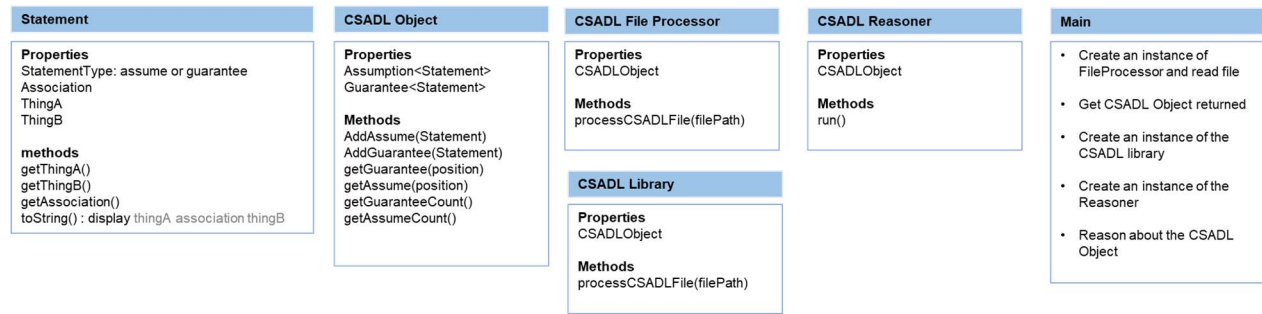
guarantee IoTDevice performs thermalImageRecognition;

```

As part of the next step, these AG pairs will be modeled as a reasoning framework within the AADL environment and will be added to AADL as a safety annex. The user will just have to specify the AG pairs in order to validate the specifications. We envision developing a reasoning framework that is based on knowledge representation within OWL.

Results. The CSADL language has been extended with the classes, associations, object, and data properties that are needed for IoT devices. The existing reasoner code was refactored to make it more modular and incorporate reasoning for new knowledge. A higher level representation of the components designed and developed for CSADL are shown below in Figure 21.

Figure 21.
CSADL Components



New properties were added along with new methods. CSADL object along with CSADL library was created so that the reasoner is more general and can be easily extended in the future. As part of the next step, we ran few use-cases to validate the formal specifications.

Use Cases. We formulated a few hybrid action-association mapping that can be used to validate certain properties using CSADL.

1. Perform Motion Sensing. The first specification will check if the IoT device can perform motion sensing. A set of AG pairs will be specified by the user to validate the specification

```
library.put("", "hasMotionSensor");
```

```
library.put("performMotionSensing", "hasFeatureMotionSensing");
```

Similarly, there are few other use cases that we plan to validate in CSADL.

2. Can the IoT device perform thermal image recognition

```
library.put("", "hasThermalSensor");
```

```
library.put("performThermalImageRecognition", "hasFeatureThermalSensing");
```

3. Does the doorbell stream data

```
library.put("recordImage", "hasCamera");
```

```
library.put("provideWirelessConnectivity", "hasNetworkModule");
```

4. Does the IoT device has sound recognition feature

```
library.put("produceAudio", "hasSpeaker");
```

```
library.put("recordAudio", "hasMicrophone");
```

```
library.put("provideWirelessConnectivity", "hasNetworkModule");
```

5. Does the device send and receive secure data?

```
library.put("sendData", "isConnectedTo");
```

```
library.put("receiveData", "isConnectedTo");
```

```
library.put("canEncryptData", "hasFeatureDataEncryption");
```

```
library.put("canDecryptData", "hasFeatureDataDecryption");
```

6. Is the connection between the server and device secure?

```
library.put("sendData", "isConnectedTo");
```

```
library.put("receiveData", "isConnectedTo");
```

```
library.put("canEncryptEvent", "hasFeatureEventEncryption");
```

The following use cases are specified at higher level of abstraction. The user can validate and infer knowledge by just writing simple English language statements. This tool will help to validate systems, thereby making them more safe, secure, and trustworthy.

Major Findings and Key Outcomes. The ontological representations play a significant role in the creation of a new language by verifying the inconsistencies that could arise while designing the new language. The extensions for IoT devices were successfully implemented. As a result, assume-guarantee-based modeling and automated analysis can be performed to identify any violations of security requirements or errors in design.

Task 2.3 Modeling of Human Behavior

The objective of this task has been to understand the behavior of human interaction with IoT devices to mitigate privacy and security concerns. The behavior is then modeled at a higher level of abstraction that enables automated reasoning, reducing the gap between policy requirements and its analysis.

The goals were to extend the existing IoT ontology use case of a Smart doorbell (SDB) with the inclusion of human interaction to mitigate the following security concerns:

1. The ability to secure and constraint external interaction
2. The ability to monitor the frequency of interaction with servers
3. The ability to control the server ownership
4. The ability to implements data integrity
5. This task extends the existing SDB-IoT ontology by including Human-machine interaction. The inclusion of the interactions is based on the analysis of the above security constraints to understand how the role of a human would help to make an IoT environment more private and secure.

Methods. Although IoT devices are helpful to us in assisting humans with day-to-day activities, being constantly connected to the internet, they also expose us to a wide range of cyber security vulnerabilities. A survey (Chaparro, Nakushian, Prior, Rebensky, & Carroll, In Preperation) was conducted to examine individuals' knowledge, perceptions, experiences, and behaviors related to IoT cybersecurity and privacy, including:

1. What IoT devices are currently owned and their uses.
2. Level of knowledge and understanding of IoT device privacy.
3. Current perceptions regarding privacy associated with IoT devices.
4. Current behaviors when interacting with IoT devices.
5. The reasons for the behaviors.

6. Willingness to change behaviors.
7. Experiences they have had with IoT cyber events.

The data from this survey helped us understand the following security drawbacks and lack of features in today's IoT environments including:

1. Participants did not have a lot of experience with smart home IoT devices.
2. Degree of Trust in the security of data collected showed that users do not fully trust their devices and are aware that IoT devices are not secure.
3. Users are generally aware that their data is not completely safe; however, they do not always take safety precautions when using their IoT devices.
4. They are aware of the risks of features such as cameras and recordings. They are not willing to read the terms and conditions for these features as they feel that they are not meant to be read, and they would not understand them.
5. Participants are unsure as to what would indicate their device was being accessed, and some feel that it is impossible to know that their data is being accessed without Consent.
6. Providing individuals with the tools to help them become more educated and secure will aid them in making more informed decisions and taking safer actions
 - a. Security language should be clear, concise, and void of technical jargon
 - b. Ensure security behaviors do not take long or users will not perform them

The survey shows that we can build a more secure private network by including a human's perspective in modeling the IoT environment where the role of a human would be primary to impose certain constraints and monitor the interactions of the IoT device with the external environment to increase privacy and mitigate any security risks.

Methods for Ontology Development. Methods for developing ontologies were researched to come with the extended security framework for the smart doorbell ontology; the ontologies investigated are:

The Mentor Methodology. The mentor methodology is defined as a “methodology for enterprise reference ontology development,” it enhances knowledge sharing among organizations, allowing its users to keep their own knowledge representations and producing a reference ontology for the subject domain. It “brings together the building and re-engineering of ontologies related to mapping competencies” (Gonzalez-Gil, Martinez, & Skarmeta, 2020).

Tasks on distributed and heterogeneous systems demand support from more than one ontology. Multiple ontologies need to be accessed by the same but also different systems. The distributed nature of ontology development has led to dissimilar ontologies for the same or overlapping domains. Thus, various parties with different ontologies often do not understand each other. To solve these problems, it is necessary to use ontology mapping geared for interoperability. The MENTOR methodology (Sarraiapa, Silva, Jardim-Goncalves, & Monteiro, 2008) supports the development of a common reference ontology for a group of enterprises sharing a business domain.

This methodology is based on the concept of Mediator Ontology (MO), which assists the semantic transformations among each enterprise's ontology and the referential one. The MO

enables each organization to keep its own terminology, glossary, and ontological structures, providing seamless communication and interaction with the others.

NeOn Methodology. This is a scenario-based methodology, which provides guidance for all main activities in ontology engineering. The context these activities are considered is that of a networked world. A network of ontologies or an ontology network is a collection of ontologies related together via a variety of relationships, such as alignment, modularization, version, and dependency. Accordingly, a networked ontology is an ontology included in such a network, sharing relationships with a potentially large number of other ontologies (Suarez-Figueroa, Gomez-Perez, & Fernandez-Lopez, 2011).

The NeOn Methodology framework provides,

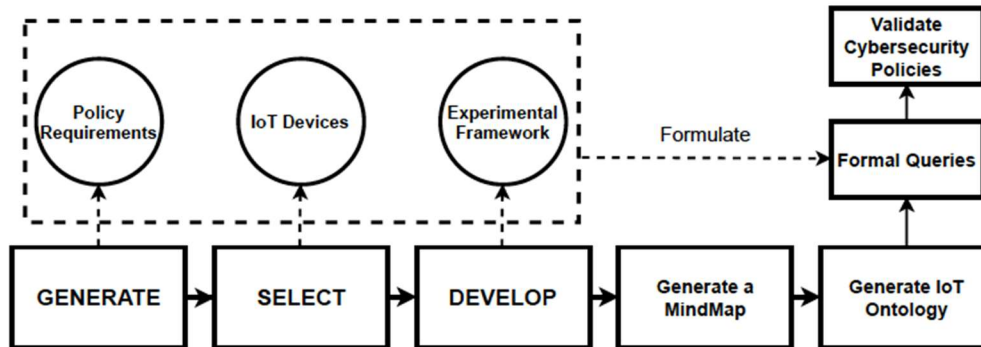
1. a glossary of processes and activities involved in the development of ontologies,
2. two ontology life cycle models, and
3. a set of methodological guidelines for different processes and activities, which are described as (a) functionally, in terms of goals, inputs, outputs, and relevant constraints; (b) procedurally, by means of workflow specifications; and (c) empirically, through a set of illustrative examples.

Ontology-Driven Automation of IoT-Based Human-Machine Interfaces (HMI)

Development. Another approach we came across as a part of the background research was the ontology-driven approach to automatically generate a firmware for devices and middleware for applications where high-level tools are developed to automate the process of creating interfaces for HMI with the help of ontologies (Ryabinin, Chuprina, & Belousov, 2019). Different HMI requires different hardware interfaces to interact with machines. It is necessary to combine old systems with smart ones and bring human-centric innovation to drive a composition on IoT systems. The main problem is that users lack knowledge in both electronics and programming for complex sensor-based interconnections. And hence, there is a need for a simple user interface where this ontology-driven approach could be used to build smart systems to automatically generate a firmware for IoT devices and middleware for applications. It is a way to automate the firmware and middleware generation where IoT devices are used as part of the HMI with third-party software.

Results. We built a human interactions ontology within the existing ontology of IoT devices and relationships to indicate the human interactions to mitigate the security and privacy risks. The proposed framework can be considered as a combination of the methods described above. Figure 22 shows the existing methodology that was developed to model the behavior of IoT for the generation of cybersecurity policies.

Figure 22.
Existing Methodology



We extend the existing methodology to include requirement gathering and human perspective to the IoT ontology as shown in Figure 23. We begin with the existing IoT device and generate policy requirements for the IoT device that can help to increase user trust and privacy by keeping human interaction in mind. These requirements are generated by the evaluation of user surveys where we understand the knowledge and experience of the users with IoT devices, the degree of trust with their data being collected and the privacy and security concerns with being constantly monitored by these IoT devices. We also gather requirements from other IoT-HMI ontologies and requirements to build features specifically for HMI interface with security.

Figure 23.
Proposed Methodology for HMI-IoT Ontology



These requirements are then formulated into a Mind Map to visually organize the information. The information gathered from the experiment is transferred to the Mind Map

which, helps to visually organize the information and makes it much easier to understand and comprehend.

It lists all the entities along with their relationships and the associations between different entities. Using the entities and relationships listed in the Mind Map, we come up with a formal IoT ontology model which helps to run automated reasoning and draw inferences. These requirements for the IoT device help to formulate queries, that are executed on the ontology to infer knowledge from the ontological model. The queries identify how including human machine interaction to control the behavior of the IoT device helps make the environment more private and secure. The outcome of the query reasoning helps to validate the policies and detect any kind of violations.

Major Findings and Key Outcomes. One of the major findings was that the proposed methodology helped us in capturing the human interactions that needs to be modeled to strengthen security and privacy. In the process, it helped us identify the requirements such as, the security application and the relevant human centric interactions that will enable actions that can be taken by the human for security and privacy.

Task 2.4 Modeling and Analysis of the Composition of IOT and Human to Identify Security Policies

The objective is to improve the existing ontology to include “*Human*” to interact with a third party “*security application*” to control the interaction with the “*server*” to protect, always restrict and monitor a secure connection. One of the other motivations is to design a model, which implements automated reasoning to verify if the modeled human machine interaction implements the security and privacy behavior that strengthen cybersecurity for IoT. The goals were to increase security and privacy of the IoT environment by including human interaction to control interaction with the server. Additionally, the development of knowledgebase required to enhance the security of IoT devices.

Methods.

Generation of HMI Requirements. One of the focuses of this part of research is to aid the process of understanding the need for policies that help in increasing IoT trust and privacy by including the human as the operator controlling the interactions to strengthen security. The aim is to develop a knowledge base that models the behavior of human interaction with IoT devices for automated analysis, which is guided by some of the already existing and identified vulnerabilities related to security and privacy from the existing framework. As described in task 2.3, these requirements are generated by the evaluation of user surveys, from other cyber security IoT ontologies and from related existing HMI-IoT ontologies, where we understand the knowledge and experience of the users with using IoT devices, the degree of trust they have with their data being collected and the privacy and security concerns with being constantly monitored by these IoT devices.

Few of the existing HMI-IoT ontologies related to cybersecurity explored during background research also helped us formulate these policies. For example, in the SciVi ontology

(Ryabinin, Chuprina, & Belousov, 2019), the authors developed high-level tools to automate the process of creating interfaces for Human-machine interaction with the help of an ontological driven approach to automatically generate firmware for devices and middleware for applications. They developed a hardware device which turns human gestures into semantics of spatIoTemporal deixis which relates to verbal behavior of people having different psychological types.

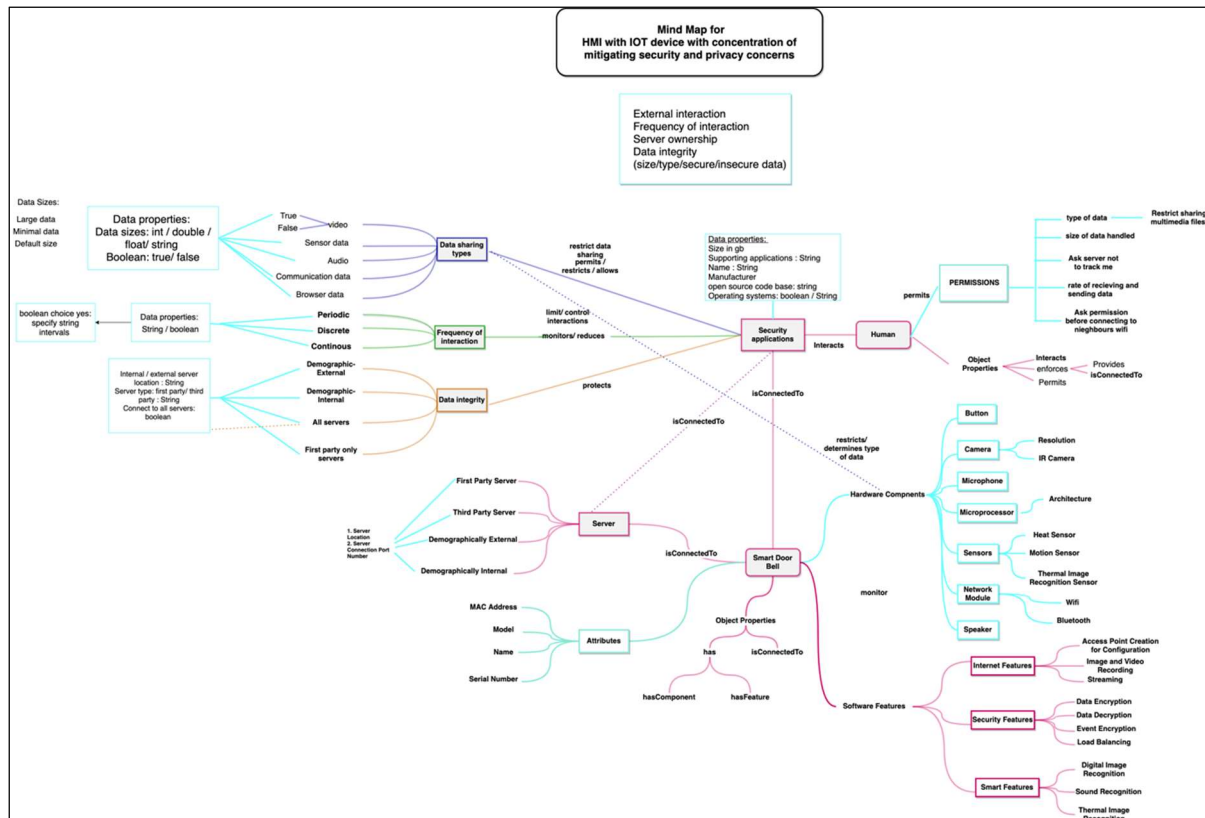
Through this research, we learnt that it is necessary to combine old systems with smart ones and bring human centric innovation to drive a composition on the IoT system. Most users lack the qualification or knowledge in both electronics and programming to operate complex sensor-based interconnections that are involved with IoT devices, and hence there is a need a simple user interface with an ontology driven approach to build smart systems to automatically generate firmware for IoT devices and middleware for applications, which is a way to automatically create software for IoT based HMI. Through this example, and the data gathered from the requirements survey (Chaparro, Nakushian, Prior, Rebensky, & Carroll, In Preperation) (mentioned in Task 2.3), we learnt that following a ontological human centric approach is best to extend the existing IoT ontology to include cyber security features to mitigate privacy and security concerns.

We categorize the HMI-IOT policy requirements into three main entities which guide us to develop the extended ontology,

1. Data integrity
2. Frequency of interaction
3. Data sharing types

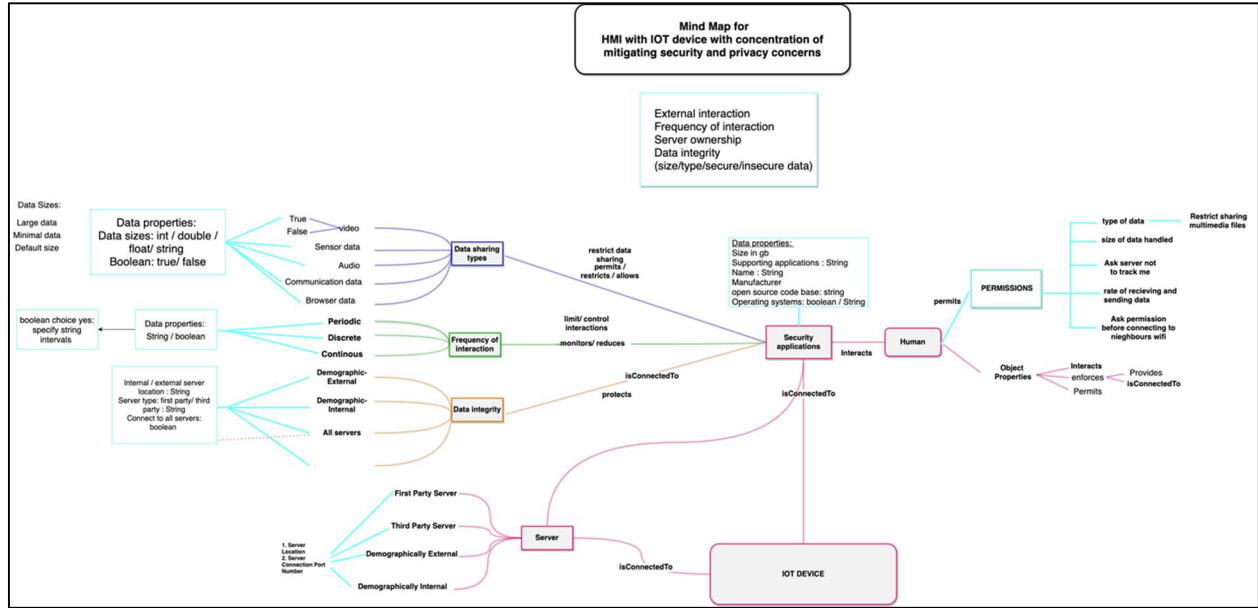
These requirements and security constraints are modelled with a human perspective as an extension to the existing SDB-IoT ontology to analyze and understand how the role of a human would help to make an IoT environment more private and secure.

Figure 24.
Mind Map for HMI with IoT device Ontology



The captured information for the HMI- IoT Ontology is depicted through a Mind Map (Figure 24). A mind map is a concept used for information mapping and assists in diagrammatic organization of information (Mind Map, n.d.). It is often created around a single concept to which other objects/entities are linked using associated representations. Mind Map helps to visually organize information that may otherwise be hard to comprehend.

Figure 25.
Mind Map for Human Centric IOT Ontology



We analyze the Mind Map in two parts, the first part (Figure 25) which depicts the Human interaction with the third-party security application is the addition ontology to the existing smart doorbell ontology. As the core of the HMI IOT Mind Map, we have the Security application class which acts as an interface for the Human to control and interact with the IoT device and server.

The Human class is considered as the center of control which decides the connections and permissions of different interactions of the IoT device and server. A third-party security app that is installed on the IoT device, which is operated by the human enables the human centric control. Hence, we have the relation “*Interacts*” between the Human and Security application. The “*Human*” class has a permission component with categories indicating the permissions to the type of data allowed, size of data, server tracking permission, rate of transmission of information to and from the server. These are the permissions, that are enforced on the server-IoT device connection through the Security application.

The three main policy requirements: Data integrity, Frequency of interaction, Data sharing types are modeled as subclasses to the security application. The “*Security application*” is a class that is an interface for the human to interact with the IoT device, it has features like data integrity, frequency of interaction, data sharing types. The data integrity class controls the type of interaction with the server, by selecting if the server is external/internal, or third-party server, through the security application the human permits these connections between the IoT device and server.

Through the “*Frequency of interaction*” sub-class, the human can monitor If the connection between the server and IoT device has to Periodic, Discrete or Continuous. It has data properties of Boolean and String, to indicate the selected type and interval of connection.

The “*Data sharing*” types of requirements are modelled as a sub-class to the security application with the restricts/ allows association. It depicts the types of data transmission to and from the IoT device like, audio, video, sensor, communication, or browser data. The human can restrict data sharing permissions with the data property like Boolean to select the appropriate type of incoming or outgoing data for the current session, specify the data size to be shared using int/double/float/string.

Results.

Modeling the HMI-IoT ontology. Once the model of the ontology is built, we present the results of policy requirements that were validated through SPARQL reasoning and querying. As discussed in the previous sections, we began by listing and categorizing the policy requirements, which guided the experimental flow. We formally modeled these requirements after identifying the various components, attributes, and their associations. After modelling, the automated reasoning helped to check for any inconsistencies and flaws within the framework which were rectified. As part of the last step, validation of the four main policies listed in the previous section was achieved through querying.

Table 10 shows the queries written to test the connections between the Human, security application, server and IoT device. Table 11 shows the SPARQL queries to test the main policy requirements mentioned in the above sections, the queries along with the description and results are mentioned in the queries.

Table 10.
Connection Tests in SQARQL

Query	Description	Outcome	
		Subject	object
SELECT ?subject ?object WHERE {?subject test:interacts ?object}	Human to security application connection	Human	securityApp1
SELECT ?subject ?object WHERE {?subject test:controls ?object}	Security application to Data connection	securityApp1	Data1
SELECT ?subject ?object WHERE {?subject test:isConnectedTo ?object}	Device to server connection	nestDoorBell	Server2
		geeni	Server1
SELECT ?subject ?object WHERE {?subject test:connects ?object}	Server to device connection	Server 2	nestDoorBell
		Server 1	Geeni
SELECT ?subject ?object WHERE {?subject test:isConnected ?object}	Device to security application connection	geeni	SecurityApp1
SELECT ?subject ?object WHERE {?subject test:connectsTo ?object}	Security application to the device connection	securityApp1	geeni
INFERENCE CONNECTIONS:			
SELECT ?securityApplication ?server WHERE {?securityApplication test:connectsTo ?device . ?device test:isConnectedTo ?server}	Infers the connection between Security_Application and server	securityApp1	server1

Table 11.
Results of Requirements Testing in SQARQL

Requirements	Query	Description	Outcome		
			subject	object	result
Frequency of interaction		Testing for continuous interaction	nestDoorBell	Server2	“continuous”
	SELECT ?subject ?object ?FrequencyOfInteraction WHERE { ?subject test:isConnectedTo ?object. ?object test:frequencyofInteraction ?FrequencyOfInteraction }	Testing for periodic interaction	geeni	Server1	“periodic”
	ASK {test:R2D2 test:interacts test:securityApp1 . test:securityApp1 test:controls test:data1 . test:securityApp1 test:connectsTo test:nestDoorBell . test:nestDoorBell test:isConnectedTo test:server2 }	Human restricts interaction with the server (testing if human can restrict the connection between security app and nestdoorbell)	Human(R2D2)	nestDoorBell	True
Data Integrity	SELECT ?subject ?object WHERE { ?subject test:security ?object }	Encrypted or non-encrypted data	Data1	“encrypted”	
Data Sharing types	SELECT ?subject ?object WHERE { ?subject test:type ?object }	Type of data	Data1	“video”	
Size of Data	SELECT ?subject ?object WHERE { ?subject test:size ?object }	Restrict size of data shared	Data1	10mb	

Objective 3. Human Use Experimentation and Design Recommendation Development

Tasks 3.1 Up front Analysis and Literature Review

Cybersecurity is increasingly becoming a threat across a range of different industries. In a report by the United States Government Accountability Office (GAO), 23 of the 24 major federal agencies noted information security as a major problem that needed more management, with 19 of those agencies noting their weakness in information security procedures. The number of cybersecurity incidents for federal agencies has increased from 5,503 in 2006 to 77,183 in 2015 (U.S. Government Accountability Office, 2017). In 2016, the U.S. Navy experienced a breach of 134,386 sailor names and social security numbers from the compromise of only one laptop (Chief of Naval Personnel Public Affairs, 2016). These threats are not limited to the government and military, as three billion users were affected by the Yahoo! Inc. hack in 2016 and 143 million by the Equifax Inc. hack in 2017 (Morgan, 2017).

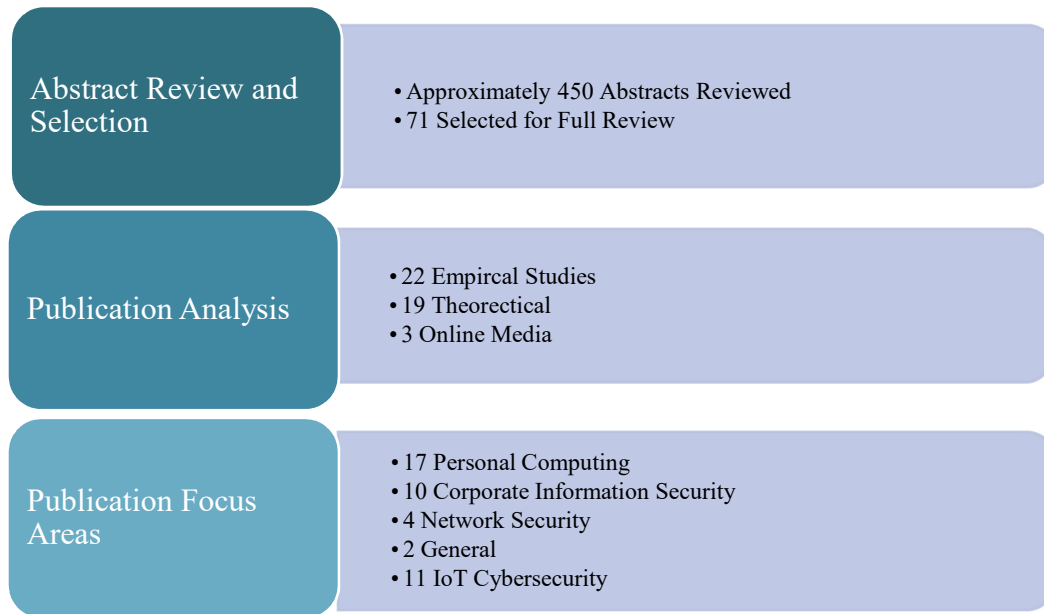
Prevention of breaches in cybersecurity has typically focused on providing technical solutions such as hardening networks and improving computer systems that detect intrusions and enhance safe information sharing, with little focus on the device user (U.S. Government Accountability Office, 2017). However, the device user is often the last line of defense. In fact, in 2017 the U.S. GAO highlighted the lack of properly trained personnel as one of the needed areas of improvement for cybersecurity effectiveness and noted a lack of sufficiently trained staff and procedures for cybersecurity response (U.S. Government Accountability Office, 2017). Although it is the last line of defense, “the human factor remains the security’s weakest link in cyberspace” (Wiederhold, 2014, p. 131). This highlights some critical questions. Are device users equipped with the training and tools necessary to recognize cybersecurity vulnerabilities and detect when a system is being compromised? Do device users know how to respond once a cybersecurity event is detected?

These questions are of particular interest to the IoT device industry as everyday electronic devices are becoming more connected to the outside world. Suresh et al. (2014) defines the Internet of Things as “a connection between humans – computers – things (2014, p. 2).” From doorbells to refrigerators to smart phones, more devices are being connected to the internet than ever before. Consumers are adding these devices into their homes and connecting them with the internet creating “Smart Homes” (Covington, 2019). These smart home devices are now ubiquitous in homes and workplaces of many people. While these smart devices may seem benign in terms of cybersecurity risks, they are connected to the internet and as such they pose a risk to private personal information leaks. Despite the widespread usage of IoT devices, there is a significant lack of knowledge in IoT security. Many smart Homeowner’s do not recognize risks associated with the IoT devices and trust device manufactures to protect their privacy (Zheng, Aphorpe, Chetty, & Feamster, 2018). Further, individuals who are knowledgeable about the risks of IoT devices do not use the recommended safety best practices (Breitinger, Tully-Doyle, & Hassenfeldt, 2020). For example, many users understand two factor authentication can better protect their devices and accounts but still fail to utilize this technique as they find the cost of doing so to outweigh the associated risks (Choi, Park, & Jung, 2018). As such, it is important to understand if consumers can effectively recognize and respond to potential cybersecurity threats to applications such as these.

The goal of this effort was to examine the human factors surrounding detection of, and response to, a cybersecurity event by a device user, who is not a cybersecurity expert. Specifically, how do device users, whose focus is not cybersecurity, make decisions regarding potential privacy vulnerabilities or events, and what steps can be taken to better prepare them to respond to such events? To achieve this, we reviewed the literature to determine what research has found regarding the human factors of cybersecurity decision making. The effort examined research conducted to date in various domains including IoT. The methods and findings, along with recommendations for promoting effective cybersecurity decision making in IoT and beyond, are described in the following sections.

Methods. A literature review was conducted to identify what research exists regarding consumer preparation for, and decision making associated with, cybersecurity vulnerabilities and cybersecurity events across several domains, including IoT. Using a compiled list of keywords targeting user decision making associated with cybersecurity events, we performed an extensive keyword search of databases including Sage Journals, ScienceDirect, Wiley Online, IEEE Xplore, Proquest, SpringerLink, Defense Technical Information Center, Taylor and Francis Online, and Florida Institute of Technology library holdings. The following keyword phrases were utilized: trust and cyber-attack, human factors and cyber-attack, cyber event and trust, system hack and trust/aviation, human detection of cyber events, human behavior cyber-attack, human cyber detection, cyber situational awareness, human cyber malicious attack, human cognitive cyber information hacking, prospect theory behavioral cyber threat, information security, IoT Cybersecurity, Smart Home, user trust of IoT devices, and framing theory. Throughout the duration of the literature review, we reviewed approximately 450 abstracts to determine if the articles focused on human factors of cybersecurity events. Abstracts were reviewed to ensure the focus of the article was on the device user and the decision process, detection of cybersecurity events, influencing factors, or the human response to cybersecurity events. Of the initially reviewed abstracts, we selected 71 of the publications for full review to determine if they were relevant to a device user's cybersecurity decision process. Based on a full review of these publications, we selected a total of 43 publications for analysis. We examined literature from several domains that explored how individuals make decisions related to cybersecurity events and associated human factors concerns. The domains included: Personal Computing (e.g., individual home computer use), Corporate Information Security (e.g., system security, encrypting files, updating software), Network Security (e.g., observing network activity on a server), IoT (e.g., smart home devices, artificial intelligence assistants), and General Cybersecurity (e.g., articles that addressed cybersecurity as a whole or across multiple domains). Twenty-two empirical studies, eighteen theoretical publications, and three online media sources were reviewed in detail and analyzed. See the summary of the literature review process is presented in Figure 26.

Figure 26.
Literature Review Process



Each article was analyzed and data related to human interaction with the cybersecurity event was extracted, including: (a) the type of event, (b) factors that influenced the decision process during the event, (c) the factors that influenced user response to the event, (d) how the event influenced a user's performance on, and future trust in, a system, and (e) mitigations, or steps that can be taken to improve human response to similar events. The research team then analyzed the data for trends and extracted two types of categorical themes: (a) stages of human response to cybersecurity events and (b) factors that influence human response to cybersecurity events. From this, a framework of factors which impact the three stages of human response to cybersecurity events was developed.

Results. Three stages of cybersecurity decision making were evident from the literature reviewed, including: (1) Susceptibility, the stage preceding the event which primarily encompasses behaviors that impact vulnerability to a cybersecurity event, (2) Detection of the event when it occurs, and (3) Response to the event after it occurs. Second, nine factors were identified from that literature that influenced a user's cybersecurity decision making process across these three stages, including: (a) perceived susceptibility, (b) safeguard cost effectiveness, (c) system trust, (d) system reliability, (e) system knowledge, (f) cybersecurity knowledge and experience, (g) saliency of the cybersecurity event, and (h) system transparency. Table 12 presents a mapping of the three stages of the cybersecurity decision making process to the nine factors which influence these stages. Also included in the table are descriptions and examples of the three stages, number of publications that provide support for each stage, and indication (via an X) of which stages are influenced by each factor.

Susceptibility Phase. The first stage of cybersecurity decision process, susceptibility, is the a priori state of the individual prior to experiencing a cybersecurity event. This stage focuses on one's perceptions of the likelihood of an attack. This includes awareness of potential cybersecurity events, how individuals view the security of their systems, and the preventative

steps an individual user takes. There are several factors which impact an individual's susceptibility to experiencing a cybersecurity event. The following section describes the factors that influence the stage of susceptibility in individuals across a range of domains.

Perceived Susceptibility. Perceived susceptibility to cybersecurity events is a critical factor that influences susceptibility and all the subsequent stages of the cybersecurity decision process. If someone does not feel that they are susceptible, when an anomaly occurs, they will not consider the possibility that a cybersecurity threat is the cause, and in turn, may not respond effectively (Pienta, Sun, & Thatcher, 2016). Further, if individuals understand that they are susceptible and that there is a threat, they are more likely to exhibit safe security behaviors (Mittal, 2017). Research across multiple domains has shown that many individuals exhibit optimism bias, the belief that they are not at risk and do not need to take steps to prevent cybersecurity events (Rhee, Ryu, & Kim, 2012), (Pfleeger & Caputo, 2012).

For example, research has shown that executives often see their companies as less likely to be targeted and believe that they better protect themselves from a cybersecurity threat than their competitors (Coover, Dreibelbis, & Borum, 2016). Research has also shown that, with respect to IoT devices, younger generations, regardless of gender, expressed more concern towards the risk of susceptibility to cyberattacks, when compared to older generations, and these concerns were more likely to influence purchasing decisions (Albert, Rodan, Aggarwarl, & Hill, 2019).

Table 12.
Cybersecurity Decision Response Framework

	Phase		
	Susceptibility	Detection	Response
Hypothetical Examples	Checking the last time an application was updated to gauge current risk. Feeling hesitant to open a link in an email with poor spelling.	Noticing changes in device displays that were not initiated by the user or frequent and inexplicable program crashes.	Checking security information to determine website safety; subsequent use/disuse of website after cybersecurity event.
# Of Supporting Studies	15	14	5
Factors Influencing Decision Process	Perceived Susceptibility	X	X
	Perceived Safeguard Cost & Effectiveness		X
	System Trust	X	
	System Reliability	X	
	System Knowledge		
	Cybersecurity Knowledge & Experience	X	X
	Saliency of Cybersecurity Event	X	
	System Transparency	X	
	Privacy Fatigue		X

Safeguard Cost and Effectiveness. Individuals will not engage in security compliance or assurance behaviors, such as frequently changing passwords, if they do not perceive safeguards as effective (i.e., do not understand how their behaviors improve cybersecurity), or feel that it is not their job or that the safeguard is too costly (Zaccaro, Dalal, Tetrick, & Steinke, 2016). This can lead to negative attitudes towards security, and psychological distancing from security responsibility (Hoffman, et al., 2009). The resulting lack of effective security behaviors can leave systems more vulnerable to attacks. For example, Breitinger et al. (2020). explain that while most individuals will use passwords on their smartphones, they do not take part in other

recommended safe practices such as using a VPN while connected to public WiFi and turning off unused features, resulting in mobile devices being less secure than desktop computers.

Trust and Reliability. Trust in the system plays a key role in the susceptibility stage and is highly dependent on another factor, system reliability. Trust in a system is dynamic and contingent on system reliability and performance, and can be comprised of attitudes, expectations, attributes, feelings, intention, and traits (Hoffman, et al., 2009). If a system is highly reliable, individuals are likely to form habitual trust, which can decrease perception of risk, and as a result, decrease awareness and detection of a cybersecurity event (Pienta, Sun, & Thatcher, 2016). Similar to findings from the trust-in-automation literature (Lee & See, 2004), consistent shutdowns or false alerts from a system can degrade a user's trust in that system's performance, this could eventually lead to disregard of a cybersecurity alert during a cybersecurity event that shares similar characteristics (Conti, Ahamad, & Stasko, 2005). Therefore, system reliability is critical to ensure trust is properly calibrated. Research has also shown that ease of use, perceived usefulness, community interest, as well as an individual user's social network can also influence trust (Al Hogail, 2018). For example, smart homeowners trust the device manufactures to protect their private data, and the user's perception of how useful and convenient the IoT device is influences their privacy behaviors and trust (Zheng, Apthorpe, Chetty, & Feamster, 2018).

System Knowledge and Cybersecurity Knowledge/Experience. System knowledge impacts susceptibility to a cybersecurity event. Users who have system knowledge and understand associated cybersecurity vulnerabilities are more likely to trust a system's ability to protect information confidentiality, integrity, and availability, whereas individuals who lack system knowledge tend to exhibit misplaced trust in a system (Jang, Chang, & Tsai, 2014). For example, IoT device use is ubiquitous in the modern world and these devices are used in places where many people may not consider cyber-vulnerabilities (e.g., utilizing a QR code in a grocery store (Daubert, Wiesmaier, & Kikiras, 2015). If a device is connected to the internet in any way, then it is not 100% secure from cybersecurity threats. Therefore, the question arises: do users have the knowledge of the system to protect themselves, as devices that were not originally connected become connected?

Knowledge of, and experience with, cybersecurity events also influence susceptibility. A study in 2010 found that the perceived damage after a cybersecurity attack affects an individual's likelihood to continue to use that system (Lee & Lee, 2010). If there are comparable alternatives, individuals are more likely to move to comparable systems, even if the affected system has a higher perceived usefulness. Further, individuals who do not have a full mental model of how cybersecurity threats occur can develop ineffective coping mechanisms, which could include avoiding the use of a susceptible system altogether (Furman, Theofanos, Choong, & Stanton, 2012).

Detection Phase. The second stage of the cybersecurity decision process is detection of the cybersecurity event. This includes the ability of a user to detect and correctly identify a cybersecurity event or distinguish a cybersecurity attack from a system anomaly due to a potential system error. Several of the factors that influence susceptibility also influence how likely an individual is to detect a cybersecurity event. The following section describes the factors that influence the stage of detection.

Cybersecurity Knowledge and Experience. A user's knowledge of, and experience with cybersecurity events can also affect their ability to detect such events. A study conducted by Ben-Asher and Gonzalez (2015), which examined participants' response to malicious network attacks, found that cybersecurity experts, or those with extensive cybersecurity experience and knowledge, were more effective at detecting malicious attacks, and had significantly fewer false alarms than their novice counterparts. The authors suggest this may be due to the experts' ability to detect relevant cues and meaningful patterns indicative of a cybersecurity attack. IoT device users are often unaware of security setting or security mitigations for the device (Covington, 2019) and as such, users are vulnerable to IoT manufacturers pulling personal data from the IoT device. Many users do not perceive the risk associated with IoT devices or regard them as convenient enough to be worth the risk (Zheng, Apthorpe, Chetty, & Feamster, 2018).

System Knowledge and System Transparency. A user's system knowledge can influence their ability to detect a cybersecurity event. Multiple studies have shown that users must have sufficient knowledge about how the system operates to determine whether system behavior is abnormal, and potentially indicative of a cybersecurity attack (Grazioli, 2004), as cited in (Furman, Theofanos, Choong, & Stanton, 2012), (Ben-Asher & Gonzalez, 2015), (Proctor & Chen, 2015), (Legg, 2016), (Hirshfield, et al., 2015). System transparency also impacts detection of a cybersecurity event. A user must use information that the system provides to determine if a threat is occurring. If the system does not provide information related to current system processes (e.g., confirmation that the most up-to-date security patches are installed), new software installed, or system status (e.g., system resources currently being overloaded), individuals cannot determine if the abnormal system behavior is due to a cybersecurity event (Mahoney, et al., 2010). Furthermore, manufactures are often not transparent with device security and frequently users cannot change the security settings (Liang & Xue, 2010) (Covington, 2019). This practice leads to a lack of awareness of the risks the device poses and means by which to instill protections.

Saliency of Cybersecurity Event. Saliency of a cybersecurity event can also influence detection. For example, a conspicuous attack is one that results in obvious cues, such as a computer crashing or control of the computer being taken over, versus a less salient attack which may only result in slowed system response. A study conducted by Hirshfield et al. (2015) found that users are more likely to detect salient cybersecurity attacks than less salient attacks that appear to be due to a user or system error.

Response Phase. The third stage of the cybersecurity event response is user execution of a response to the cybersecurity event. The literature suggests that multiple factors impact how an individual responds to cybersecurity events. The following section describes the factors that influence the response stage.

Perceived Susceptibility, Safeguard Cost Effectiveness, and Privacy Fatigue. In a study examining computer user response to spyware, Huigang and Yajiong (2010) found that individual response to potential cybersecurity threats was influenced by a chain reaction of inter-related factors. Individuals must 1) believe the threat exists (perceive susceptibility), (2) believe that the threat is avoidable (perceive safeguard effectiveness), and be willing to burden safeguard cost (e.g., financial, time-related, or resources costs with implementing safeguards such as frequently changing passwords), and 3) detect the threat. If the threat is perceived as low risk or

safeguards costs are perceived as either too high cost or ineffective at combating the threat, individuals may not take the steps necessary for cybersecurity protection. Choi et al. (2018) explain that as data breaches increase in frequency individuals may feel tired of taking actions to prevent data loss and will stop devoting energy to safeguarding information. This is because the “fatigued” individuals believe the safeguard cost is greater than the safeguard effectiveness. This phenomenon is called privacy fatigue. Interestingly, the attitudes individuals have towards cybersecurity and their behaviors tend to differ, a phenomenon referred to as the privacy paradox (Acquisti, Taylor, & Wagman, 2016); while many individuals may state that they care about protecting the security of their devices, due to a perception of high safeguard costs, safeguards necessary to ensure security are not implemented. The concern and worry expressed towards cybersecurity events also depends on the type of information being held by the device (Brough & Martin, 2020). For example, users tend to be more concerned about the privacy of bank account information compared to height and weight information.

Cybersecurity Knowledge and Experience. A user’s cybersecurity knowledge and experience can impact detection as presented above but can also influence how they respond to a cybersecurity event. In a study examining participant response to secure and insecure websites, Kelly and Betenthal (2016) found that participants with high levels of cybersecurity knowledge collected more information before proceeding with a login (as indicated by mouse trajectories), than individuals with low levels of cybersecurity knowledge. As a result, those with high levels of cybersecurity knowledge were also more likely to proceed in logging into secure websites whereas those with low levels of cybersecurity knowledge failed to recognize the right cues and logged into insecure websites. In a study conducted by Rosoff, Cui, and John (2013), computer users were asked how they would respond to a cybersecurity dilemma encountered while downloading online music or buying from an online store. Results indicated that recall of prior cybersecurity experiences influenced how the users would respond: recall of negative cybersecurity experiences (e.g., experienced a loss of data due to a virus) led to less-risky responses; recall of positive cybersecurity experiences (e.g., remained unaffected during a security breach) led to higher-risk responses.

Strategies for Improving Response. The three stages presented in the framework of a device user’s cybersecurity decision process provide opportunities to better support the user in making the right decision. The literature review uncovered numerous mitigation strategies that can be utilized to achieve this. Below we present mitigation strategies, including system design, training, and procedure recommendations that can be utilized to target each of the three stages of the cybersecurity decision process across numerous domains, whether an individual is using an IoT device at the office or using their personal computer at home.

Mitigations for the Susceptibility Stage.

Increase Awareness of Cybersecurity Vulnerabilities. Users need to be aware of cybersecurity vulnerabilities and how these can affect their systems. Employees who do not manage security as their main job, often do not understand how their behaviors affect security (Zaccaro, Dalal, Tetrick, & Steinke, 2016). Removing the bias that they are not susceptible is the first step. SETA (Security Education, Training, and Awareness) programs, or programs focusing on improving attitudes, effort, and one’s responsibilities to improve cybersecurity, have shown to decrease unsafe behaviors and improve precaution taking (Burns, Roberts, Posey,

Bennet, & Courtney, 2015). Increased awareness training could provide users insight into the vulnerabilities in their IoT devices. For example, users could be made aware of their own current exposure to cybersecurity threats such as the sharing of their private information with third party vendors. Since many users do not perceive themselves at risk, demonstrating their actual exposure could influence them to change their behaviors and take more precautions. Similarly, awareness could be increased by a company's own IT department explaining actual events that have happened at the company.

Develop Procedures and Training for Cybersecurity Safeguards. Users should be trained on procedures that can help protect their systems from potential cybersecurity vulnerabilities. Given that steps to ensure security may cost users much needed time to perform their primary task, safeguards must be quick, logical, and easy to complete. Individuals are likely to avoid effective security behaviors if a) they believe they are unlikely to be targeted, b) risks are low, c) they find safeguards ineffective, d) they find safeguards too costly, or e) they lack the skills to implement safeguards (Liang & Xue, 2010). An example, of a procedure to help maintain user compliance with cybersecurity safeguards would be to provide a "security status update" which would highlight current vulnerabilities and ways to protect oneself in a brief and easy to understand format. This status update could be sent to users on a weekly basis the same way some smartphones send a weekly activity log. These updates would convey best practices, and over time, train users to have better cybersecurity habits.

Utilize Positive Framing in Training. Too much fear instilling during training can cause users to not exhibit safe security behaviors. Framing training in a positive frame (i.e., what you will gain from protection), versus loss (i.e., what will happen if you do not protect your systems) has been shown to be a more effective method for security training (Mittal, 2017), (Rosoff, Cui, & John, 2013), (Sharma, 2017). For example, a company could create a cybersecurity training course that highlights the benefits of following these recommended best practices. Instead of telling users, "If you do not take precautions, you will get hacked", the training could convey "taking precautions will keep you safe and save you precious time and energy in the long run."

Mitigations for the Detection Phase.

Increase System Transparency. It is important that the information systems provide users with information regarding data source, validation, and update feeds. This includes detail regarding activity, changes, inconsistencies, and potential compromises that are relevant to the cybersecurity of their system information. If the display does not give enough detail on information sources and the status of these sources, it will be very difficult for an individual to correctly determine if an event is a cybersecurity attack (Mahoney, et al., 2010). Many IoT systems such as a smart watch and fitness tracking applications collect personal information and track user behavior (Jia, et al., 2017), (Ben-Asher & Gonzalez, 2015), (Lee & Kobsa, 2016). These devices should make it evident to individual users what information is being collected, where it is being stored, and how it is being used. Applications should also inform users about the integrity of the storage location, whether it is being stored locally on the device or remotely on a server, and what parties have access to this information.

Provide System Feedback. Information systems should provide feedback when false alarms, errors, or failures occur, allowing users to have a better understanding of "normal"

system behavior (Hoffman, et al., 2009). Users need to understand what unreliable system behavior looks like (e.g., from error alerts), to have a baseline with which to compare a cybersecurity event.

Provide Security Alerts and Status. Information systems should incorporate automated detection and alert of cybersecurity vulnerabilities and compromises, where possible. Given that most users are not cybersecurity experts, they will need support in detecting and diagnosing these events. Further, during normal operations, information systems should provide symbols or notifications that connections are secure, safe, and up to date (Kelley & Bertenthal, 2016), (Conti, Ahamad, & Stasko, 2005). For example, providing security messages, when users' private information is requested, that prompt users to decide what information to share and whether to accept or deny a request to access specific information (Jia, et al., 2017). Providing alerts such as these allows devices to be more transparent to users.

Train System Knowledge. Users need to have an understanding of where each incoming information comes from and where outgoing information goes. This allows a user to discern between system behavior and cybersecurity threat behavior. System knowledge has shown to improve a user's correct detection of a cybersecurity attack across information security, networking, and personal computing domains (Jang, Chang, & Tsai, 2014), (Furman, Theofanos, Choong, & Stanton, 2012), (Ben-Asher & Gonzalez, 2015), (Kelley & Bertenthal, 2016). Increasing system knowledge in less reliable systems will assist users in understanding what is causing behavior in the system, and whether or not it should raise concern (Pienta, Sun, & Thatcher, 2016), (Hoffman, et al., 2009), (Jang, Chang, & Tsai, 2014). For example, IoT devices should inform users about different aspects of the system and implications for cybersecurity and privacy, including disclosing the type of sensors, what data is collected, when the next security update will be, what physical actuations the device has, purpose of data collection, and where data is being stored (Emami-Naeini, Agarwal, Faith Cranor, & Hibshi, 2020). Providing this information will allow a user to be aware of what the device is doing with their information and detect any suspicious activity.

Mitigations for the Response Phase.

Develop Procedures and Training for Cybersecurity Response. Users should be provided procedures for how to respond to a potential cybersecurity threat. Providing individuals with procedures to determine if a cybersecurity attack has occurred can improve the rate of correctly identifying cybersecurity events (Conti, Ahamad, & Stasko, 2005), (Furman, Theofanos, Choong, & Stanton, 2012), (Bowen, Devarajan, & Stolfo, 2011). An example of a system that helps one determine whether a cybersecurity event has occurred would be an antivirus software on a PC. These software packages give step by step instructions for handling the event. Implementing software packages like this on all IoT devices would have users better identify and respond to cybersecurity events.

Provide Opportunity to Report Potential Cybersecurity Events. Users should be given access to a reporting system that allows reporting of any system behavior that they suspect might be due to a cybersecurity vulnerability. Such a system provides the opportunity to improve the system security and inform procedures and training (Fagan, Megas, Scarfone, & Smith, 2020). For example, many banking applications will show users how to identify and report unauthorized

account activity. In the case of IoT devices this could be a form on the manufacturer's website or within the controlling application.

Train Basic Cybersecurity Knowledge. While training all users as cybersecurity experts is infeasible, training users on basic cybersecurity knowledge, relevant to their systems, will increase their ability to detect the onset of cybersecurity events and to effectively respond. It is inevitable that as information systems, whether they be smart home IoT systems or smartphones become more automated and digitized, future users will need to exhibit more computer aptitude to support more effective performance (Meneghello, Calore, Zucchetto, Polese, & Zanella, 2019).

Major Findings and Key Outcomes. This research effort sought to explore the human factors associated with the cybersecurity decision process for device users who are not cybersecurity experts. A review of literature in this domain revealed three key stages in this process that are influenced by nine separate factors. Based on the literature review findings, this paper puts forward recommended mitigations for influencing these nine factors and improving cybersecurity response in a range of domains. Such mitigations have shown great promise. For instance, in federal agency network systems, there has been a 50% drop in incident reports from 2015 to 2016, due to the implementation of mitigation strategies such as adding cybersecurity infrastructure for reporting and managing cybersecurity events (U.S. Government Accountability Office, 2017). By taking the necessary actions, the human factors associated with cybersecurity and privacy can be more effectively managed. Developers can use this framework to design features that allow users to make more educated decisions about managing their data. If one understands how the apparent safeguard costs affect decision making regarding user settings, developers could develop better applications and companies could educate their employees on making good privacy decisions to protect company data.

Future steps in this effort involved validating the framework. Currently we are administering an online survey to college students and military personnel examining their cybersecurity perceptions, knowledge and behaviors associated with IoT device use. The results of this ongoing study will provide information to help develop guidance for the development of applications to address all three stages. Future studies should empirically examine user response to simulated cybersecurity or privacy events to more thoroughly examine the proposed influencing factors and to explore the effectiveness of the recommended mitigations.

Task 3.2 User Survey Research and Recommendations

To better understand all the factors contributing to users' perceptions of their IoT devices and their lack of action, it is important to identify which safe practices users already take while considering their existing awareness and attitudes (Zheng, Apthorpe, Chetty, & Feamster, 2018). Then recommendations for increasing privacy-related actions while mitigating deterrents such as privacy fatigue can be generated. The purpose of the current study was to examine, by administering a user survey, individuals' perceptions, knowledge, experiences, and behaviors related to IoT device information security and associated privacy implications, to understand how to encourage users to utilize industry recommended practices to maintain the security of their information.

Methods. The survey sample consisted of 179 participants. Recruitment of participants took place through a STEM University in the Southeast United States. The participants were recruited from the university's student and faculty population via email list services, class distributions, Sona Systems®, and by asking participants to pass the survey link on to friends and colleagues. Additionally, the survey was distributed via the social media networking site LinkedIn. Although 179 participants completed the study, responses associated with 40 participants were removed. Twenty-six participant responses were not included as less than 20% of the questionnaire was completed. Four participant responses were removed due to not properly completing the survey leading to a final sample of 139 participant responses. The final sample was comprised of 91 (65%) males and 47 (34%) females between the ages of 18 – 77. When examined by generation, 47 (34%) participants were Generation Z, 18 (13%) were millennials, 20 (14%) were Generation X, and 7 (5%) were Baby Boomers. One-hundred two (51%) of the participants were active college students, 26 (13%) had commercial sector jobs, 25 (12.5%) worked in academia, 16 (8%) were Reserve Officers' Training Program (ROTC) cadets, 12 (6%) had past military experience, 7 (3.50%) were active-duty military, 7 (3.5%) were employed within the government, and 5 (2%) were civilian employees of the military. Participation was voluntary; extra credit was offered to students who participated through university courses.

Survey Instrument. The survey study was a mixed-methods survey design delivered via Qualtrics software. The survey gathered a combination of quantitative data and qualitative data to obtain richer information about user behaviors. The questions were not forced response questions, and participants could answer or skip whatever questions they chose. The survey was divided into the following sections: (a) demographics questions, (b) experience questions, (c) knowledge questions, (d) perception questions, and (e) safe behaviors questions; the survey took approximately 20 minutes for participants and was a mix of multiple-choice, multiple-selection, matrix, and constructed response questions.

The demographics section gathered information about age, gender, race, nationality, employment status, household composition, and military experience for the participants who have served in the military. The data presented in the following section are associated with a subset of these areas, focusing on user perceptions, knowledge, experience, and behaviors. The relevant sections are discussed in further detail below.

Experience Sections. The experience sections of the survey examined device use and event experience. The device use section gathered information about the participants' use and experience with different types of IoT devices. Participants were first asked to answer for what purpose they used smart home devices in three categories, including smart home, which consisted of devices such as smart doorbells and virtual home assistants, smart mobiles: smartphones, smart wearables, and tablets, and computer: laptops and desktops. Participants were then asked to rate their experience with each device from 1- no experience to 4- extensive experience. An area for additional comments was included if a participant felt they wanted to add more information or clarify.

The event experience section examined whether the participants or anyone close to the participants had ever experienced an event in which their data was accessed and utilized without their consent. These questions were multiple choice. The participants were then asked to

elaborate using open-ended response questions if they had experience with their data being accessed without their consent or were unsure whether it had happened. The participants were also asked if they felt their level of trust changed following an event in which their data was accessed without their consent. This item was scored on a five-point Likert type scale with response choices from 1- strongly decreased to 5- strongly increased.

Knowledge Questions. The system knowledge section gathered participants' knowledge of what kind of third parties (e.g., internet service providers, device manufactures, the government) accessed data from the devices. Participants were asked what type of data they thought that third-party entities were accessing and for what purposes the collected data is used.

The information security knowledge section consisted of two parts. The first gathered what participants believed would indicate unauthorized access to their IoT devices; this used two open-ended response questions that asked what would indicate that one of the users' devices was being accessed by an outside party and how they could prevent someone from accessing their information without their consent. A dichotomously scored (Yes/No) question asked if participants would change how they interacted with the device if someone accessed it without their consent. They were then given an open-ended text box to explain why. The second part examined participants' knowledge of cybersecurity using questions developed by the Pew Research Center related to knowledge of cybersecurity terminology and concepts (Olmstead & Smith, 2017).

Perception Questions. The users' perceptions of the security of their IoT devices were collected using Likert-type items. Participants were asked to what degree they trust the information security of the collected data and how concerned the participants are about the information security of the collected data. Trust and concern were measured on five-point Likert Type scales, from 1- did not trust and not at all concerned, to 5- completely trust and extremely concerned, respectively. Participants were given a space for additional comments if they felt they could not express their response to the other questions in the section.

The questionnaire also gathered participants' perceptions of the susceptibility of their IoT devices to being accessed without their consent using Likert-type items. Participants were then asked what they perceived the risks to be of their data being accessed or utilized without their consent. The participants were then asked to rate the susceptibility of each type of device (smart home, smart mobile, and computer) to being accessed without their consent using a Likert-type scale that ranged from 1- not at all susceptible to 5- completely susceptible.

Safe Behavior Questions. The safe behaviors section examined what features (i.e., crash reports, location services, etc.) and security practices (e.g., two-factor authentication, antivirus) participants use. Participants were also asked whether they connect to public WIFI. This question was dichotomously scored (Yes/No).

Procedure. Potential study participants were provided a link to the survey via email or social media site. Upon clicking the link, they were presented with the informed consent form explaining the purpose of the study and their right to end the survey at any time free of consequences. After consenting, they were provided with a brief overview of the study and the types of relevant devices. They were informed that they had as much time as they needed to take

the survey. When the participants completed the survey, they were allowed to provide an email address for any potential follow-up studies and prompted to submit the survey.

Data Analysis. The quantitative data were analyzed descriptively by obtaining response frequencies for each survey item. This allowed the researchers to identify trends in participants' perceptions, knowledge, experiences, and behaviors. The qualitative data was analyzed by categorizing the open-ended item responses into themes. This was done by reviewing responses for each qualitative question and extracting common themes. The themes were then reviewed, and similar themes were condensed. Each response was then categorized into one of the themes, allowing the researchers to obtain frequency counts of how many responses fit into each theme.

Results.

User Experience. All the participants had experience with mobile devices and computers; however, only 92 (66%) participants owned smart home devices. Among the participants who owned smart home devices, the most frequently owned devices were streaming devices (75 participants, 82%), AI personal assistants (45 participants, 49%), and smart appliances (25 participants, 27%). Sixty-two (45%) participants responded that they had experienced a situation in which their data was accessed without their consent, 31 (22%) participants responded that they had not experienced such an event, and 43 (31%) participants were unsure. Sixteen (26%) participants who experienced an event where their data was accessed without their consent expressed that their trust level did not change, and 12 (19%) expressed that their trust level increased after their data was accessed without their consent.

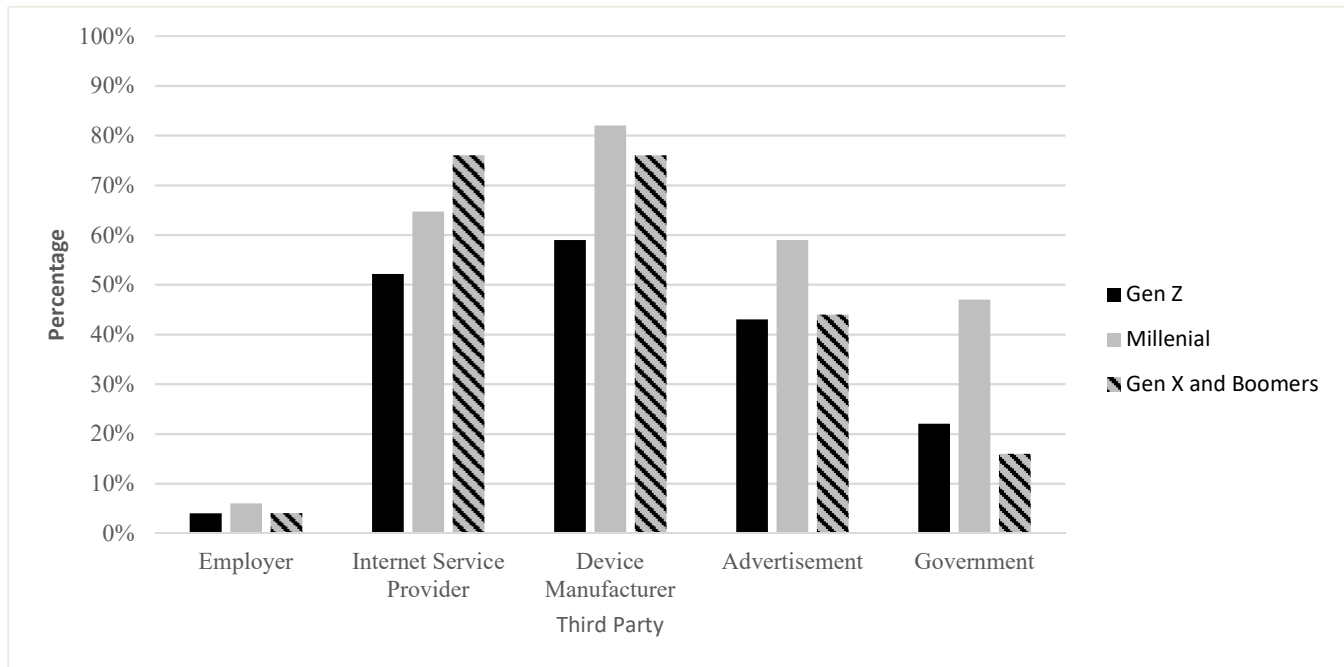
User Knowledge. Overall, a majority of the participants were aware of which third parties/service providers were accessing their data for all three device types. Participants were least familiar with which third parties were accessing their smart home device data, with 61 (44%) of participants responding with unsure. More participants were familiar with what third parties were accessing their smart mobile device and computer data, with 31 (22%) and 34 (24%) participants responding unsure, respectively. The difference in the level of knowledge regarding data access between smart home, smart mobile, and computer devices was also present when participants were asked what types of data are being accessed. Fifty-six (40%) participants responded that they were unsure of what data is being accessed by their smart home devices, 22% of participants responded unsure for both smart mobile and computer devices with 31 and 30 participants responding, respectively. Furthermore, 46 (33%) smart home, 21 (15%) smart mobile, and 24 (17%) computer users reported being unsure of the purposes for which their data is being accessed.

When asked how they would know that their devices were being accessed, 42 (30%) participants cited targeted advertisements, 33 (24%) participants cited alerts and notifications, and 32 (23%) participants cited devices acting abnormally. When asked which third parties they believed to be accessing their devices, 101 (72%) participants responded with the device manufacturer, and 89 (64%) responded with the internet service provider. When responses regarding who was accessing their data were broken down by generation, there are some differences between the generational groups. The largest and most interesting difference was with respect to the government accessing their information. Forty-seven percent (8/17) of millennials believed that the government was accessing their information, compared to 22%

(10/46) of Generation Z and 16% (4/25) of Baby Boomer and Generation X participants. There was also a noticeable difference between Generation Z and Boomers/Generation X regarding the perception that service providers were accessing their smart home devices. Overall, as a general trend for all categories except service providers, millennials tended to respond higher than the other generational groups. These results are shown in Figure 27.

Figure 27.

Perceptions of Third Parties Accessing Smart Home Devices by Generation



The average participant score on the five technical security questions taken from the Pew Research Center study was 58%. (N=136). Twenty-four participants (approx. 17%) were only able to answer one question correctly, 66 participants (approx. 48%) were only able to answer two to three questions correctly, and 49 participants (approx. 36%) were able to answer four-five of the questions. Table 13 presents a question-by-question breakdown of the percentage of participants that answered each question correctly in the present study compared to the Pew Research Study conducted in 2017. As a general trend, participants in the present study scored higher than the participants in the Pew Research Study. The most noticeable difference between the scores was regarding the Global Positioning System (GPS) tracking question. In the present study, 99 (73%) participants answered the question correctly, while in the original study, 548 (52%) answered the question correctly. The second most noticeable difference was in the https:// question, in which 73 (54%) of participants answered correctly in the present student versus 348 (33%) in the original study

User Perceptions. Users indicated that they do not fully trust their devices. Of the 139 participants: 41 (29%) indicated that they do not trust, 46 (33%) indicated that they somewhat distrust, 27 (19%) indicated that they neither trust nor distrust, 24 (17%) indicated that they somewhat trust, and none indicated that they completely trust the information security of the data collected by their devices. Nearly all (96%) of the participants had some degree of concern regarding the security of their personal information.

Table 13.
Percentage of Participants That Got Each Question Correct

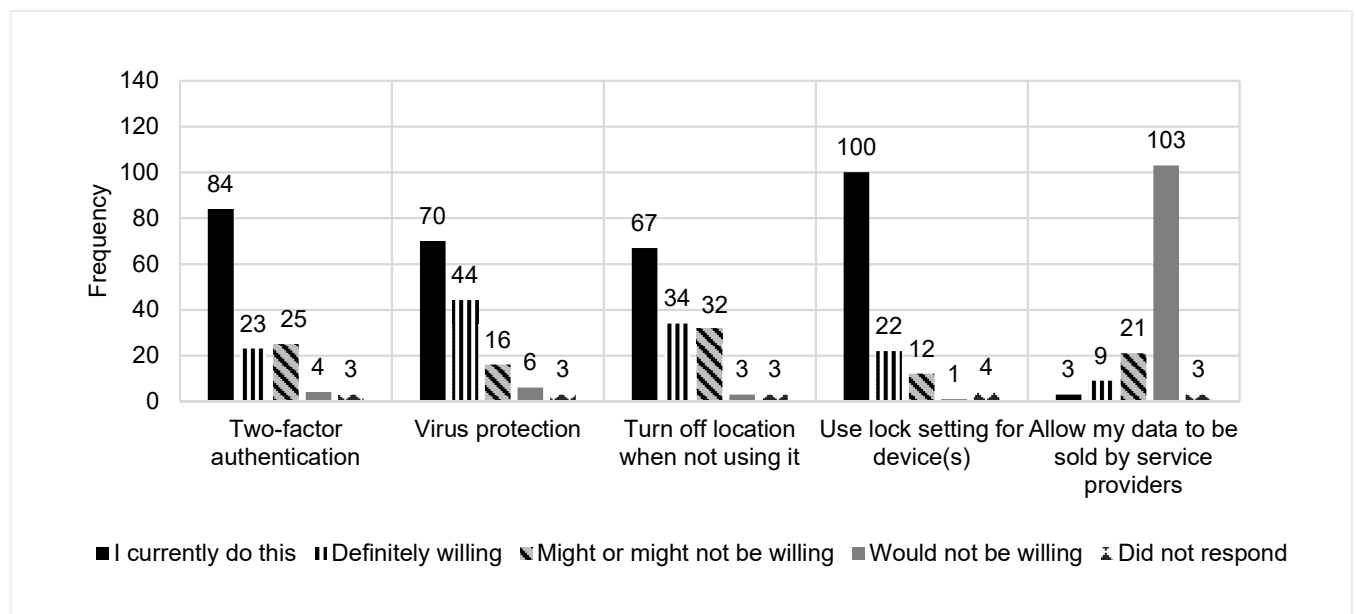
Question	All Wi-Fi traffic is encrypted by default on all wireless routers	What does the “https://” at the beginning of a URL denote, as opposed to http:// (without the “s”)?	Turning off the GPS function of your smartphone prevents any tracking of your phone’s location	If a public Wi-Fi network requires a password to access, is it generally safe to use that network for sensitive activities such as online banking?	What kind of information security risks can be minimized by using a Virtual Private Network (VPN)?
Pew Research	45% Correct	33% Correct	52% Correct	73% Correct	16% Correct
Current IoT Study	54% Correct	54% Correct	73% Correct	80% Correct	21% Correct

When asked about the susceptibility of their devices to being accessed without their consent, AI home assistants had the highest frequency of “extremely susceptible” ratings, with 43 (31%) participants responding in that manner. The next highest was smart security cameras, where 39 (28%) participants rated the cameras as “extremely susceptible.” Overall, 133 (96%) participants expressed some level of concern regarding the susceptibility of their IoT devices being accessed without their consent.

The most frequently reported risk perceived by the participants across all IoT devices was private information being tied back to them. Sixty-five (46%) smart home device users, 109 (78%) mobile device users, and 104 (75%) computer users reported this. Participants also reported that they were most concerned about having their private conversations recorded and their data being sold and shared. For the purposes of this study, recording of private conversations differs from private information being tied back as private information could be text messages/emails while conversations are audio recordings.

User Behaviors. Participants were generally willing to utilize or were already performing safe behaviors/recommended practices, including two-factor authentication, virus protection, turning off location services when not using it, and utilizing lock settings. Further, participants overwhelmingly did not want service providers to sell their data. Of the 103 participants who said they were unwilling to have their data sold, most did not read the terms and conditions, which allows them to learn whether the service provider is selling their data. The participants who did not read the terms and conditions, for the most part, still enabled the features. Figure 28 presents the frequency of willingness of IoT device users to partake in safe behaviors to maintain their privacy.

Figure 28.
Behaviors Participants Are Willing to Partake In



The study found that overall participants do not read terms and conditions for various services/features. Seventy-two percent of participants responded that they do not read the terms and conditions for AI assistance. Additionally, 97 (70%) and 95 (60%) participants do not read the terms and conditions for speech recognition features of their devices and for location services, respectively. Furthermore, only 17 (12%) participants expressed that they would be more cautious if they experienced their device being accessed without their consent.

Major Findings and Key Outcomes.

User Experience. Overall, the survey found that smart home devices are not as prevalent as other devices such as cellphones and computers, which nearly every participant owned. Approximately two-thirds of the participants had smart-home devices, which may be due to the number of students who took the survey.

A plurality (66 participants, 45%) of participants had experienced their data being accessed without their consent, and results indicated that receiving targeted advertisements were

the most common way participants could detect this. Seeing targeted advertisements for a product an individual may have discussed in front of an AI assistant is seemingly proof that conversations are being recorded and data is being provided to advertisers.

The finding that 16 (12%) participants did not have a change in device trust and 12 (9%) had an increase in device trust after such an event also shows that the privacy paradox is alive and well in users of IoT devices. One-hundred-thirty-three (96%) participants expressed some level of concern regarding the security of the information collected by their IoT devices. However, only 17 (12%) said they would act in a more cautious way if their device was accessed without their consent. This indicates that while individuals may say they care about privacy, their actions suggest that they do not. This is in line with findings in the extant literature (Norberg, Horne, & Horne, 2007), (Acquisti, Taylor, & Wagman, 2016).

User Knowledge. Another interesting finding was that participants scored an average of 58% on the cyber knowledge quiz. When compared with the Pew Research Center findings from 2017, the participants from the current study scored notably higher on each of the questions. For example, 99 (73%) participants from the present study knew that turning off the GPS function of a phone does not prevent tracking of the phone's location. In comparison, only 548 (52%) participants know that from the 2017 Pew Study (Olmstead & Smith, 2017). A potential explanation for this finding is that the sample used in the current study has more knowledge of cybersecurity than the general population. This explanation is the most plausible explanation for this finding because most sample participants came from a STEM University. What is interesting about that demographic, though, was that despite the sample coming from a STEM university, the average score was less than 60%—indicating that even among more technical individuals, there is a notable lack of cybersecurity knowledge. Another plausible explanation is that, over the four years since the original study was conducted, the public has become more aware of cybersecurity issues because of heightened coverage by the media. Examples include the 2017 Equifax breach and the 2018 Marriott data breach.

User Perceptions. Although nearly three-quarters of the participants expressed that their biggest concern regarding risks to their privacy for both computers and mobile was private information being tied back to them, less than half responded the same for smart home devices. This is despite the fact that many smart home devices record audio and video information. A possible explanation for the disparity is that smart home device users lack the knowledge of the types of information their devices collect and what the service providers do with that information.

Interestingly, millennials were more likely to be concerned about the government accessing their private information than Generation Z or Generation X/Boomers. A potential explanation for this finding is the environment in which millennials grew up. Millennials grew up with the advent of modern technology but still remember a time before it was as ubiquitous as it is now. Additionally, millennials were in early to mid-adulthood in 2013 when Edward Snowden leaked information that the National Security Agency (NSA) in the United States was spying on American citizens' cell phone and internet data without a warrant or user consent (Wizner, 2017), (Bajaj, 2014). Many members of Generation Z were still children when this happened, and it may not have had the same breach of trust as it did with millennials. The finding that millennials perceive that the government is accessing their devices supports the idea

that participants may lack knowledge of their system because they are more worried about a perceived threat than the actual present privacy threat.

User Behaviors. The majority of participants were using or willing to use safe behaviors to protect their personal information; participants who were willing to partake in safe device behaviors expressed that they would do it because it protects privacy, enhances security, and is beneficial for device performance. However, many participants expressed reasons for not being willing to take actions that seek to protect their privacy, including inconvenience, financial cost, and past negative experiences. These findings are in line with the extant research on privacy calculus (Gerber, Gerber, & Volkamer, 2018). Privacy calculus is the idea that the cost of taking privacy-enhancing actions outweighs the benefits. The presence of privacy calculus demonstrates that the privacy paradox is present among users of IoT devices because despite stating that they care about privacy, their actions illustrate otherwise (Zheng, Aphorpe, Chetty, & Feamster, 2018).

The current study found that a large percentage of the participants did not read the terms and conditions for AI assistance, speech recognition, and location services. Previous research has shown that many users do not read the terms and conditions, especially if they require the user to access them separately (Milne & Culnan, Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices, 2004), (Steinfeld, 2016). As many IoT devices do not present the terms and conditions on the main setup screen, many users do not access this information and are therefore unaware of what the service provider does with their private data. Additionally, users tend not to read the terms and conditions of websites that they are familiar with, despite not knowing what the company is doing with their information (Milne & Culnan, Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices, 2004). In line with the privacy paradox, participants expressed that they were concerned with the security of their data but never actually researched who was accessing their information.

Recommendations. The data obtained in the current study resulted in the creation of two primary recommendations for the internet privacy community and IoT device manufacturers. First, IoT device users should be provided with the tools to help them become more educated and take safer actions regarding their privacy. The primary way device manufacturers can do this is by rewriting privacy policies, terms and conditions, and other security language to be clear, concise, and free of technical jargon. According to the National Institutes of Health (NIH), the average resident of the United States reads at an 8th grade (ages 13-14) reading level; this means that instructions and privacy policies should be written at an 8th-grade reading level or lower (Stossel, Segar, Gliatto, Fallar, & Karani, 2012). A second recommendation is that when users must perform a behavior to ensure their privacy, the behaviors should be quick and easy, or users will not perform them. For example, having to make multiple extra clicks or scrolling to access terms and conditions or to a place to completely privacy enhancing behaviors is likely to cause users to ignore them (Obar & Oeldorf-Hirsch, 2020). Additionally, research has shown that when a task takes more than three clicks, users perceive that task as more difficult (Jimenez Iglesias, Aguilar Paredes, Sanchez Gomez, & Gutierrez, n.d). Because the extant literature explains that privacy fatigue sets in when users perceive tasks as difficult, it is important for interface designers to reduce the number of clicks required to complete privacy enhancing behaviors to three or fewer.

Limitations and Future Research. These findings must be interpreted with caution as the present study had several limitations. The first limitation was the convenience sampling method which could limit generalizability. A second limitation of the study was that there was a great deal of missing data. The questions were not forced response questions, and as a result, some of the questions presented later in the questionnaire had fewer responses, likely from survey fatigue. Another limitation was that many of the questions referred to groups of devices (e.g., smart home devices), and this may have prevented finding variability in the data that might have been revealed asking about specific devices (e.g., responses associated with a smart vacuum are likely to be different than responses associated with a smart lock). Unfortunately, querying users about each specific device would have resulted in the survey length being prohibitive.

Future research needs to be conducted to examine methods to effectively increase users' knowledge of what types of data are collected by their devices and who is accessing the data. If users have a better understanding of their IoT device security settings and associated implications, they will make more informed decisions regarding protecting their privacy. Research also should be conducted to address how to make behaviors necessary to protect user privacy less burdensome on users. Research has shown that privacy fatigue occurs when the measures to protect data are too costly (Choi, Park, & Jung, 2018). A follow-on study currently underway is examining the effectiveness of a range of different techniques in lessening the burden on users, including a terms and conditions “guru” to briefly clarify information in the terms and conditions and privacy setting profiles to reduce the time to tailor privacy settings to user needs.

Task 3.3 User Experimental Research and Results

IoT devices such as smart wearables and smart machines are becoming increasingly prevalent in our 21st-century digital world. These devices have become integral to our private lives, with the rise in affordability and diversity of smart home devices such as smart plugs, smart doorbells, and virtual home assistants (Dahmen, Cook, Wang, & Honglei, 2017). Although IoT devices provide owners with many benefits such as streamlining tasks through their ability to communicate with nearby devices, they are also vulnerable to attacks. IoT devices collect large amounts of information from their environment which is shared and analyzed which, depending on settings applied by users, may be performed by more than simply the device manufacturer. It is therefore important for users to understand how these devices function so that users can take steps to configure the devices appropriately.

Previous research has shown that users of IoT devices have little to no understanding of what data is collected by their IoT devices and where it is transmitted (Olmstead & Smith, 2017). Given the increased use and prevalence of IoT devices, users lack knowledge associated with how these devices function is of concern. A Pew Research Study conducted with 1,055 individuals surveyed on their habits related to devices connected to the internet, found that the median score on a quiz of cybersecurity/internet privacy knowledge was only 38% (Olmstead & Smith, 2017). Further, IoT device users have expressed that it is incredibly important that their personal information remains confidential (Williams, Nurse, & Creese, 2017). However, users do not take the appropriate steps to ensure that their information is confidential, such as reading the terms and conditions or reviewing settings information that can inform them of proper settings for their privacy (He, 2019); (He, Bahirat, Knijnenburg, & Menon, 2019). Companies

are required by law to disclose how they utilize users' data within their privacy policy or terms and conditions (Nissenbaum, 2011). However, users overwhelmingly do not read the terms and conditions; a study from 2014 found that only .2% of internet users read the terms and conditions (Bakos, Marotta-Wurgler, & Trossen, 2014). Several reasons have been cited for why users do not read the terms and conditions, including the length of the terms and conditions and the legal jargon utilized, giving users the impression that terms and conditions were not intended to be read by users (Choi, Park, & Jung, 2018); (Obar & Oeldorf-Hirsch, 2020); (Robinson & Zhu, 2020).

Users have cited the complicated language in terms and conditions/privacy policy statements as a reason for privacy fatigue (Robinson & Zhu, 2020). Terms and conditions are often written by lawyers utilizing legal jargon to comply with government regulations and to limit the respective company's legal liability (Nissenbaum, 2011). This makes it difficult for any individual outside of those practicing law to understand the information being provided. The National Institutes of Health (NIH) advises that the average resident of the United States reads at an 8th-grade (ages 13-14) reading level and that instructions should be written at that level or lower (Stossel, Segar, Gliatto, Fallar, & Karani, 2012). Given this, many terms and conditions/privacy policies are not written in a manner in which most IoT device users would be able to understand.

Studies have also examined how different presentations of internet privacy policies have affected users reading of these policies. For example, one study by (Steinfeld, 2016) using eye-tracking technology found that when the users were presented with the terms and conditions by default, they read the terms and conditions. However, when users had to take the extra step of clicking into the terms and conditions, they were more likely to skip them. Additionally, studies have found that individuals who do access the terms and conditions spend an average of 73 seconds of reading time (Obar & Oeldorf-Hirsch, 2020). The average adult reading speed should yield a time of approximately 30 minutes to read typical terms and conditions. This finding suggests that even the participants who access the terms and conditions do not read them closely. In fact, a study by (McDonald & Cranor, 2008) found that if every person read the terms and conditions associated with each device or application they interact with, they would spend 40 minutes each day reading terms and conditions agreements. This time commitment is unrealistic for users who are already feeling that the information is not presented in a digestible format (McDonald & Cranor, 2008). In an attempt to ensure users, read the terms and conditions, many applications require users to select that they read the terms and conditions in order to use the application. Users are therefore put in a position in which they must either agree to the terms of service or not use the product. As a result, users often select that they have read, and agree to, the terms and conditions, even when they have not, in order to gain access to the product (Obar & Oeldorf-Hirsch, 2020); (Nissenbaum, 2011). If the expectation is for users to read the full terms and conditions, then the terms and conditions should be brief and presented in a format and use language that is easily digestible by an everyday user. Further, information in the terms and conditions that is relevant to the user should be easily accessible and not require additional steps to access.

When examining why users do not take the time to set up their devices appropriately, many of the same themes appear. Users have also been found to ignore privacy settings during setup and installation (Felt, et al., 2012); (He, 2019) The complexity of manually setting up

privacy preferences leads users to either skip the setup process or manage settings as the need for a particular setting becomes apparent (He, 2019). The effort and time required for users to set up their device appropriately leads to discouraged users (Milne & Culnan, 2004). Additionally, there are times in which the need for the feature outweighs the privacy risk. Users are forced to choose between an appropriate setting and the feature (He, 2019). Research has been conducted looking into different approaches to encourage users to take the time to apply settings to their devices. Transparency and increased control by users have not yielded useful results as even when users have more control and a better understanding of what applying a certain setting means, users do not change settings appropriately (Turow, Hennessy, & Draper, 2015). Users have been found to make irrational settings decisions related to their privacy, either enabling too many or too few settings (He, 2019). Therefore, users need more guidance as to what settings are appropriate to their needs. A common approach to provide this is through the use of nudges, wherein users are presented with summarized information through the use of an application. Nudges tell the user about settings but lack personalization and are not always relevant to how the user intends to use the IoT device (Almuhimedi, et al., 2015). Therefore, users can begin to ignore nudges as they do not feel they are relevant. Users need limited information about settings that are relevant to how they use the device. Furthermore, given that many devices are now located in shared space and used by multiple users, settings options need to take this diversity into account.

The purpose of the current study was to evaluate two interventions designed to address these needs. First, in an attempt to both increase users accessing, and understanding of the terms and conditions, an intervention was designed for IoT device terms and conditions in the form of a Terms and Conditions Guru that presented information throughout the IoT device set up. The Terms and Conditions Guru summarizes important information relevant to the user at their stage of device set up (e.g., information about voice recordings is included on the portion of the device set up that covers voice recordings) using brief, plain language. The summary presented by the Terms and Conditions Guru was designed to allow IoT device users to see what the device manufacturer is doing with their information in a brief and understandable format. Additionally, a second intervention was designed in an attempt to encourage the users to adjust the settings to ensure their information was protected to the degree that was consistent with the way in which they use the device (e.g., if they were not going to have more than one person using their device, then Guest Connect would be turned off to protect their device from getting controlled by external users). This intervention, presented in the form of settings profiles, aimed to also condense the setup time. Participants were able to look at a user profile menu that provided an overview of each profile and allowed the user to compare, select, and adjust the profile that aligned most with their IoT device use. The following sections describe the methods and results associated with an experiment evaluating these two interventions.

Methods.

Participants. A total of 148 participants completed all, or a significant portion of, the evaluation study (control = 83, treatment = 65). Participants were recruited via Amazon Mechanical Turk (MTurk), social media, email list service, and word of mouth. Inclusion criteria were that individuals must be over the age of 18, and the participants recruited through MTurk were required to hold an MTurk rating of 98% or higher. The survey was simultaneously distributed to students, faculty, and their contacts from the Florida Institute of Technology

(Florida Tech) via a university email list service, personal emails, and postings on both the university and research lab's LinkedIn and Facebook pages. All participants were provided with the same link to a Qualtrics questionnaire to complete the study.

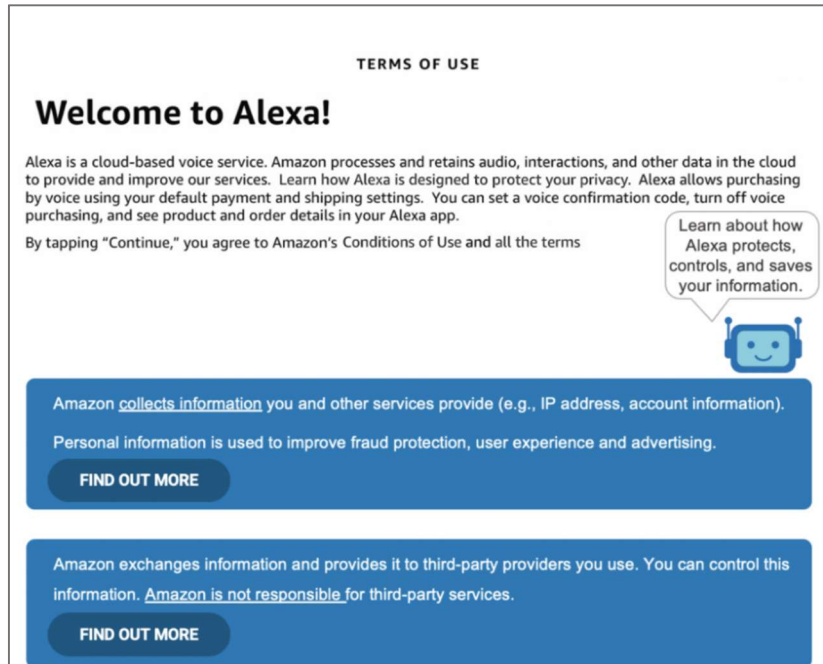
Experimental Design. The experiment utilized a between-subjects post-test-only design. Participants were randomly assigned to either the control or treatment group using Qualtrics' randomization logic. The treatment group received two interventions designed to influence their interactions with IoT devices, specifically, the terms and conditions and settings. The treatment interventions included (a) a Terms and Conditions Guru who presented blue summaries of contents from the terms and conditions related to their stage in the device setup, and (b) user settings profiles that were presented as personas of four typical users with preconfigured settings based on how these users would typically use the device. The control group did not receive any intervention; instead, they were presented with the traditional layout of the terms and conditions and settings.

Table 14.
Experimental Groups

IV = Intervention	
Control Group = No Intervention	Treatment Group = Intervention Present
Received no interventions and set up the device as normal	Received the Terms and Conditions Guru, who summarized relevant information as they set up the device and also given four user profile options

Intervention 1: Terms and Conditions Guru. The Terms and Conditions Guru intervention was designed as a metaphor for a customer service representative who walks an individual through a contract (e.g., a rental car contract), summarizing what each section of the technical jargon means in plain language. The Terms and Conditions Guru was portrayed as a cartoon robot head featured above dark blue summaries, with a text bubble next to the guru, orienting the reader to what would be covered in his summary below. The Terms and Conditions Guru's summaries were presented on dark blue rectangles with white text. The Terms and Conditions Guru summarized relevant information from the terms and conditions on the sign-up screen, the terms of use screen, the add device screen, the setup screen, the name verification screen, and the screen on which users verified their phone number. Each summary also contained a direct link to the terms and conditions page. *Figure 29* presents an example. The Terms and Conditions Guru's information was additionally embedded into the full terms and conditions document above each section. This allowed users to skim the terms and conditions, reviewing the summaries to understand what content was in the terms and conditions. This was intended to allow participants to quickly scroll down to find the information they were looking for and then read the associated terms and conditions related to the summary.

Figure 29.
Example of the Terms and Conditions Guru



Note. The dark blue summaries above condense important information from sections in the terms and conditions which are relevant to where the user is in the set-up process.

Intervention 2: Settings Profiles. The settings profiles intervention was designed to help users find the safest combination of settings based on their device use. Profiles included Tech Adopter, Informed User, Connected User, and Tech Lover. *Figure 30b* shows the menu from which participants could select one of the four user profiles. This menu provided device users with a brief overview of the four profiles to allow users to make a side-by-side comparison to determine with which profile they most closely aligned. These four user profiles were created and varied based on the level of experience and extent of smart home device use. If the participants felt aligned with any of the profiles, they could click into the profile and access the settings.

Figure 30.

User Profile Menu and Settings Associated with the Tech Adopter User Profile

30a. User Profile Menu

30b. Tech Adopter Profile

	Tech Adopter	Informed User	Connected User	Tech Lover
Who will be using your Echo Show?	FRIENDS	MYSELF	HOUSEHOLD	ANYONE
How much oversight would you like to have with your Echo Show?	LOW	HIGH	HIGH	LOW
How many features of the Echo Show do you plan to use?	ALL	SOME	MOST	ALL
How much experience do you have with devices?	LOW	HIGH	MEDIUM	HIGH

	Enable	Disable
Purchase Confirmation Sets a confirmation for Amazon Purchases and Payments	☒	☐
Voice Purchasing When enabled, Amazon purchases and payments can be made by voice.	☒	☐
Alexa Hands-Free Alexa responds to your voice any time you say "Alexa" when the app is open and in use.	☐	☒
Deletions by Voice Delete recordings by saying "Alexa, delete what I just said" or "Alexa, delete everything I said today"	☒	☐
Use Messages to Improve Transcriptions Allow Amazon to use messages you send with Alexa to improve transcription accuracy.	☐	☒
Use of Voice Recordings Training Alexa with recordings to improve Amazon's services.	☐	☒
Guest Connect Friends and family can connect their Alexa to your Echo.	☒	☐

Note. The user profile menu above allows for users to quickly compare the four profiles side by side and quickly access any that they want to further explore.

Note. The above figure highlights what the settings page associated with one of the four user profiles looked like. Each of the user profiles had a series of preconfigured settings that users could accept as configured or reconfigure to their personal liking.

All profiles had deletions by voice and whisper mode enabled, as well as brief mode disabled. The tech adopter profile was geared toward users who intended for friends to use the device, did not want much oversight on their device, planned to use as many features as possible associated with the device, and did not have much experience with IoT devices. Therefore, purchase confirmations, voice purchasing, deletions by voice, guest connect, real time text, and drop in were enabled. Informed Users were those who intended to use the device themselves, wanted oversight with their Amazon Echo, only wanted to use features relevant to their needs, and had a fair amount of experience with devices. These users are those who have a better understanding of devices, the threats they present, and have purchased the device for specific benefits/reasons. Therefore, purchase confirmations, Alexa hands-free, and deletions by voice were enabled. The Connected User profile is geared towards users who will have multiple individuals connecting to their device, would like high levels of oversight, to maximize the use of features, and have a fair amount of experience with devices. Therefore, purchase confirmation, Alexa hands-free, deletions by voice, guest connect, and drop in were enabled. The tech lover profile was created for those will allow anyone to use their device, do not want oversight but instead want to utilize all features of their device, and are device experts as they have a wealth of experience with devices. These individuals enabled all features except purchase

confirmations, and Alexa hands-free. All settings were preconfigured by default. However, each setting was editable so participants could customize their settings to their liking. Figure 31 shows the settings associated with each profile. *Figure 30a* shows what a user profile looked like on the settings level, including the settings associated with the Tech Adopter profile. All of the settings were easily configurable by clicking the blue toggle button to the right side of each setting option on the screen.

Figure 31.
Settings Across Each Profile

Settings Description	Profiles			
	Tech Adopter	Informed User	Connected User	Tech Lover
Purchase Confirmation Sets a confirmation for Amazon Purchases and Payments	☐	☐	☐	☐
Voice Purchasing When enabled, Amazon purchases and payments can be made by voice.	☐	☐	☐	☐
Alexa Hands-Free Alexa responds to your voice any time you say “Alexa” when the app is open and in use.	☐	☐	☐	☐
Deletions by Voice Delete recordings by saying “Alexa, delete what I just said” or “Alexa, delete everything I said today”	☐	☐	☐	☐
Use Messages to Improve Transcriptions Allow Amazon to use messages you send with Alexa to improve transcription accuracy.	☐	☐	☐	☐
Use of Voice Recording Training Alexa with recordings to improve Amazon’s services.	☐	☐	☐	☐
Guest Connect Friends and family can connect their Alexa to your Echo.	☐	☐	☐	☐
Enhanced Features Allows group calls and group drop ins, calls not stored	☐	☐	☐	☐
Real Time Text Send written messages over calls.	☐	☐	☐	☐

Drop In Call and message your friends and family that have Echo Devices.	☐	☐	☐	☐
Brief Mode When enabled, Alexa speaks less and may play a short sound instead of giving a voice response.	☐	☐	☐	☐
Whisper Mode When you whisper to Alexa, responses will be whispered back.	☐	☐	☐	☐

Experimental Task. Participants completed an online survey that was created to allow participants to “click” through the survey as if interacting with a mobile device display. The experimental task simulated the Amazon Echo Show 5 smart-home-device setup process and was implemented through Qualtrics software to allow the task to be performed remotely from a home computer or laptop. Participants were instructed to set up their device as if it was their personal device. The participants then completed the task. To perform the task, the participant stepped through the process of signing up for an Amazon Alexa account, including providing a username, email, and password. Users did not need to provide personal information in this process as fictitious user information was provided. Next, participants were required to step through the process of adding a device, connecting their phone number, and configuring their device settings. Participants in the control and treatment groups complete the same process; however, participants in the treatment group had access to the terms and conditions and settings profile interventions described in the previous section.

Experimental Setup. The experiment was conducted online using Qualtrics software. Qualtrics is a survey-building software that allows for the creation of different types of questions. One of the types of questions that can be created in Qualtrics is the hotspot question. The hotspot question allows for survey designers to take a still image and create clickable areas on it. Utilizing these clickable areas, Qualtrics’ question display features, and JavaScript, the authors were able to create an interactive task-performance testbed. To create an interactive testbed that best approximated the setup of an IoT device, a series of screenshots were taken of each stage of the Amazon Echo Show setup process on a mobile device. These screenshots provided a capture of every menu and option during the setup. For each of these screenshots, clickable areas were created over links to menus and the continue button. These hotspots were then configured to allow the user to advance to various pages as if they were navigating through the setup of a mobile device. For the treatment group, the screenshots were edited to incorporate the interventions, which were formatted to blend with the style of Amazon’s Echo Show 5 interface.

Measures.

Demographic Measures. Demographic information was captured using a questionnaire that requested participants’ age, sex, whether the English language was their first language, participants’ proficiency with the English language, and occupational status (student, military, academia, etc.). A multiple-choice question was also included asking if they have ever owned an Amazon Echo Show. Participants could indicate that they had owned, currently owned, or never

owned an Amazon Echo Show. Participants were also asked to rate their experience with virtual assistants like Alexa, from 1= *No experience* to 4= *Extensive experience*. An area for additional comments was included in case a participant felt they wanted to add more information or clarify.

Behavioral Measures.

Terms and Conditions. Three behavioral measures related to reviewing the terms and conditions were captured while participants were completing the device setup task. First, whether or not a participant accessed the terms and conditions, and second, the frequency of their access to the terms and conditions were collected using JavaScript embedded into Qualtrics. Both of these measures were collected for the control and treatment groups to see if the intervention provided to the treatment group led them to interact differently with the terms and conditions. The amount of time in milliseconds that a participant spent in the terms and conditions was also collected using JavaScript embedded into Qualtrics for both groups to determine how much time was spent reading the terms and conditions.

Settings. Four behavioral measures associated with device setting interactions were captured while participants were completing the device setup task. First, whether the participants accessed the settings was captured via JavaScript embedded into Qualtrics for both the control and treatment. The JavaScript also captured the frequency of access of settings, allowing determination of how many settings were accessed by control group participants for comparison to treatment group participants. The number of changes made to the settings was collected for both the treatment and control groups using JavaScript embedded into Qualtrics. Finally, the time in milliseconds that a participant spent on each settings screen (if accessed) and the time spent in each profile were collected. The time spent on each screen allowed the determination of how much time was spent reviewing the profiles and/or settings.

Knowledge Measures. The post-survey measured participants' knowledge of the content within the terms and conditions using a 5-item researcher-developed test related to Alexa's terms and conditions. The test included items such as a true/false question of "all Amazon devices require an internet connection to use their features" (scored using a trichotomous multiple-choice: True/False/I do not know). An open-ended response question was included to evaluate whether participants thoroughly read the terms and conditions, specifically, by assessing if they read the "Gotcha Clause." A gotcha clause is a nested piece of information comprised of an outrageous and unreasonable demand. The gotcha clause stated, "if payment lapses occur due to past payments being missed, Alexa reserves the right to sell your house and anyone living inside of your home." Participants were asked what Alexa reserves the right to do if payment lapses or is missed in an open-ended question.

Experiences and Reactions.

Terms and Conditions Intervention. Participants in the treatment group were asked a series of questions designed to assess their experience with and reactions to the terms and conditions interventions. The first question in this section asked whether the participants read the information provided by the Terms and Conditions Guru during the setup and was scored dichotomously (yes/no). The next question asked whether they found the information provided by the Terms and Conditions Guru helpful and why or why not.

Settings Intervention. A series of questions were administered to participants to determine if the settings profile intervention impacted how participants interacted with the device settings. First, a multiple-choice question queried about the number of user profiles reviewed to measure whether the participants viewed only one profile or explored all profiles before deciding which profile to use. The multiple-choice question provided options from one to four profiles as well as an option stating, “I did not review any of the user profiles”. To obtain participants’ reactions to the profiles, they were asked whether they felt they aligned with any user profiles. The multiple-choice question provided descriptions of each profile, such as, “Tech Adopter—many users, low oversight, use of all features, and low device experience.” This question also included an option for not aligning with any profiles. Next, a Likert-type question was included in which participants rated the extent to which they felt that they aligned with the profile(s) from 0= *Not at all aligned* to 4= *Extremely aligned*.

Experimental Procedure. All participants were provided with a Qualtrics link to the survey. Participants were given two weeks to sign up and participate in the study and encouraged to complete it in one sitting. Responses in progress were set to close after 48 hours automatically. Upon clicking on the link, participants were presented with an informed consent form explaining the purpose of the study and their right to withdraw at any time, free of consequences. After agreeing to the informed consent, a description was provided of the upcoming task. After the task description, the participants completed the demographics questions, the task, and the post-task survey, which included knowledge measures, experiences with terms and conditions and settings interventions, and reactions to terms and conditions and settings interventions. None of the items were forced response questions, which meant that the participants could freely choose which questions they answered. After participants completed the post-task survey, they received a screen thanking them for their time and informing them that the study was over.

Results. The results of the study are presented in the following paragraphs. First, participant demographics are presented. Next, the behavioral, knowledge, and experiences and reactions measures related to terms and conditions are presented. Finally, the behavioral, and experiences and reactions measures related to settings and profiles are presented.

Demographics. A total of 244 individuals participated in the survey. Of these, 148 participants met the criteria for inclusion. Inclusion criteria included being 18 years or older, completing the device setup task within the survey, and completing the entire survey in no less than 3 minutes (this was to screen out those who clicked through the survey without actually reading the questions). Of the participants who met the inclusion criteria, 148 completed the task of setting up the Amazon Echo Show (control: 83, treatment: 65). Of the participant who completed the task, 119 participants also completed the survey questions that followed the task (control: 73, treatment: 46). Table 15 presents the demographic breakdown of the sample. Similar experience for the Amazon Echo Show was found between both groups. Fifty-one participants (43%) had owned an Amazon Echo Show (15 treatment group, 59%; 36 control group, 49%).

Table 15.
Participant Demographics

Demographic Variable	N	%
Sex		
Male	50	34%
Female	98	66%
Age		
9 - 24 (<i>Generation Z</i>)	20	14%
25 – 40 (<i>Millennials</i>)	90	61%
41 – 56 (<i>Generation X</i>)	26	18%
57 – 66 (<i>Baby Boomers</i>)	10	7%
Did not Report	2	1%
Occupation*		
Employee of the Commercial Sector	81	55%
Employee of Academia	24	16%
Student	25	17%
Military	19	13%
Total	148	100%

Note. *This question was multiple select; that is, participants could provide more than one occupation

Terms and Conditions Behavioral Measures.

Terms and Conditions Access. First, we examined differences between whether or not participants in the control group and the treatment group accessed the terms and conditions pages. In total, 60 participants accessed the terms and conditions, with 20 in the control group and 40 in the treatment group. When examining frequencies, on average, 1 out of 3 participants in the control group accessed the terms and conditions ($M = 0.35$, $SD = 0.72$). However, on average, participants in the treatment group accessed the terms and conditions more than once ($M = 1.23$, $SD = 1.68$). A chi-square test of independence was performed to examine whether the relationship between condition and those who accessed the terms and conditions was statistically significant (see Figure AA). The relationship between these variables was significant, $\chi^2(1, N = 148) = 21.20$, $p < .0001$. Those in the treatment group were more likely to access the terms and conditions than those in the control group. Further, when comparing only those in the treatment and control who accessed the terms and conditions, participants in the treatment group accessed the terms and conditions more frequently ($M = 2$, $SD = 1.75$) compared to the control ($M = 1.45$, $SD = .76$). A chi-square test of independence was conducted to examine whether the frequency of access to the terms and conditions was significantly different between groups. The relationship between the groups and accessing the terms and conditions was significant, $\chi^2(3, N = 148) = 21.77$, $p < .001$. Those in the treatment group who accessed the terms and conditions did so significantly more frequently than participants in the control group.

Figure 32.
Number of Participants who Accessed Terms and Conditions

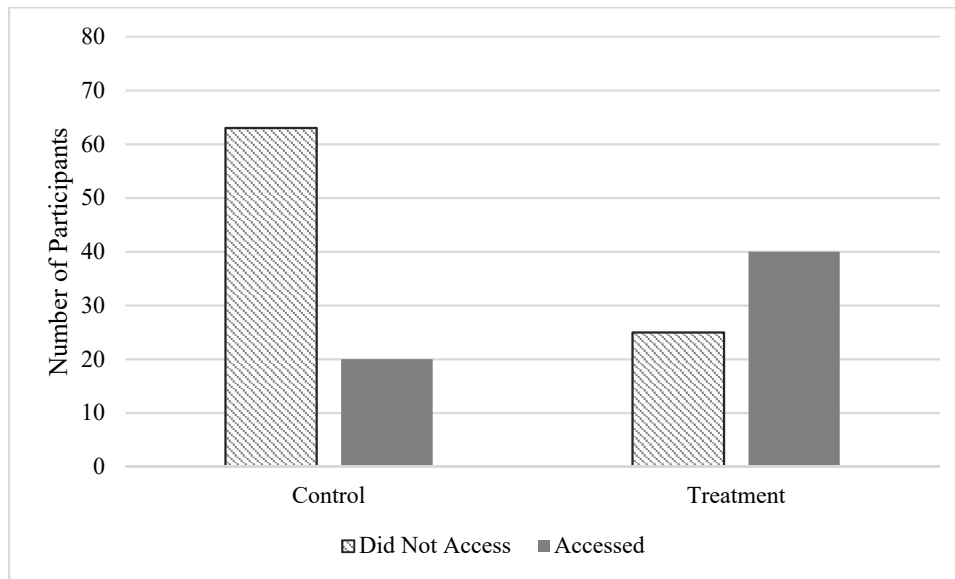
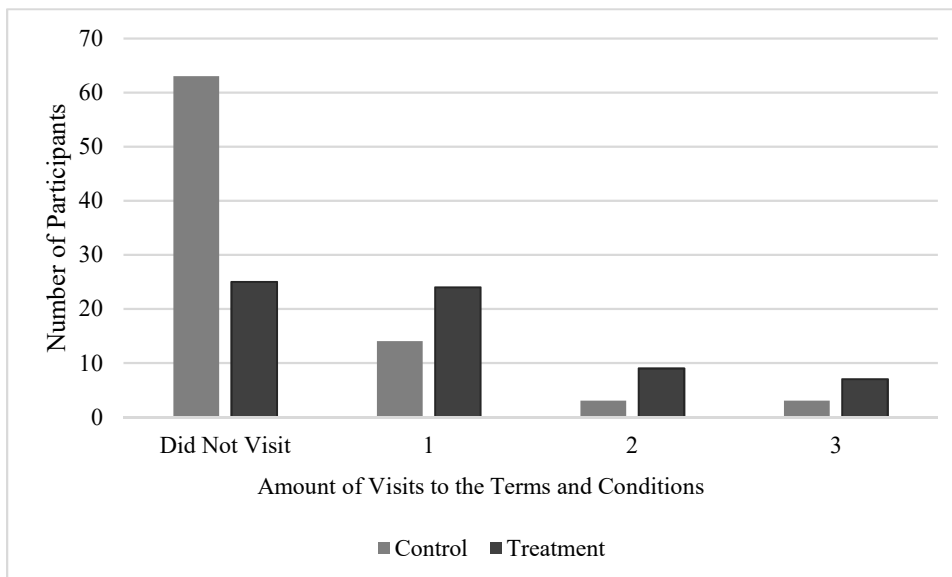


Figure 33.
Frequency of Access to Terms and Conditions



Time Spent in Terms and Conditions. Next, we examined differences between the treatment and control group in time spent accessing the terms and conditions pages. Participants in the treatment group spent more time ($M = 93$ s, $SD = 196$ s) accessing the terms and conditions compared to the control group ($M = 31$ s, $SD = 26$ s). A t -test assuming unequal variances was conducted to examine whether the difference between time spent in the terms and conditions between groups was significant, revealing a significant difference between the two

groups, $t(42) = 1.97, p = .028$. Those in the treatment group spent significantly more time, on average 62 seconds more, in the terms and conditions than the control group.

Knowledge Measures.

Test Scores. The difference in knowledge test scores between participants who accessed the terms and conditions and those who did not were examined. Participants who accessed the terms and conditions ($n = 47$) scored an average of 11 points higher ($M = 71\%, SD = 19\%$) compared to those who did not access the terms and conditions ($n = 79, M = 60\%, SD = 19\%$). When comparing the knowledge test scores between those in the control and treatment group who accessed the terms and conditions, participants in the control group ($M = 64\%, SD = 19\%$) had a similar score on the knowledge test as the treatment ($M = 63\%, SD = 24\%$). A two-way analysis of variance (ANOVA) was conducted with IVs of the terms and conditions access (accessed vs. did not access) and condition (control vs. treatment) on the knowledge test scores. A main effect of terms and conditions accessed was significant, $F(1, 125) = 10.15, p = .001$. However, there was not a significant effect of condition, $F(1, 125) = 1.89, p = .17$, nor was there a significant interaction between condition and terms and conditions accessed on knowledge test scores $F(1, 125) = .08, p = .77$.

Gotcha Clause. A review of participant responses to the gotcha clause was conducted to determine whether any participants correctly identified the unreasonable phrase inserted into the terms and conditions. When breaking out those who responded to the gotcha clause by group (control = 68, treatment = 39), no participants in the control group correctly identified the gotcha clause (0% of control participants). However, two participants in the treatment correctly identified the gotcha clause, (5% of treatment participants). Of the incorrect answers, 31% of participants indicated that they did not know the answer and 68% incorrectly answered the question.

Terms and Conditions Intervention Reactions Measures. A thematic analysis was conducted examining the responses regarding the reasons why participants in the treatment group felt the information provided by the Terms and Conditions Guru was or was not helpful. Themes were extracted from written responses and then similar themes were combined to create the categories included in Table 16 below. Forty-eight participants in the treatment condition (74%) reported whether or not they felt the Terms and Conditions Guru was helpful. Of those participants who responded, more than half ($n = 29, 60\%$) felt that the information provided by the Terms and Conditions Guru was helpful. The participants who provided reasons as to why felt the information was helpful cited the information was brief, pointed out helpful issues, and provided useful hints (see Table 16 below). Participants made comments such as, “I found that [the Terms and Conditions Guru] included information that would help me learn about the product.” However, many participants ($n = 19, M = 40\%$) felt that the summaries provided by the Terms and Conditions Guru were not helpful, citing reasons such as too much information, not reading them, or that they took too long to read. Participants made comments such as, “I don’t spend time reading that [*sic*] kind of summaries.”

Table 16.*Thematic Analysis of Participants' Responses to the Terms and Conditions Guru*

Why Not Helpful	#	Why Helpful	#
Too much or too difficult information	5	Useful important information	7
Not relevant, distracting	4	Provided guidance or support	5
I did not read them	3	Easy to understand	4
Obvious or repetitive information	2	Brief information	2

Note. Although 48 participants in the treatment condition indicated that the Terms and Conditions Guru's summaries were helpful, not all participants indicated why. Some participants provided more than one reason and some participants did not provide answers that were relevant, these were not included.

Settings Behavioral Measures.

Settings Access. Whether participants accessed settings and the number of changes made to the settings were collected to analyze whether there was a difference in the interactions with settings between conditions. Unfortunately, the changes to the settings for the control group were not collected due to a technical issue with the testbed. When examining the treatment group, 42 out of the 65 participants in the treatment group accessed a profile. Almost half of those who accessed a profile ($n = 18$) made changes to the profile. The breakdowns of how many participants chose each profile and the number of associated changes can be seen in Table 17. When examining profiles chosen, the Informed User ($n = 16$) and Connected User ($n = 19$) were selected the most often by participants. Of those who selected them, half made changes to the Informed User profile and one out of three participants made changes to the Connected User profile. On average participant who chose those profiles made approximately three changes. The Tech Lover profile was not chosen by many participants ($n = 5$), however, of those who chose it, only two made changes and on average they made one change. Tech adopter was the least selected profile ($n = 2$) by participants, and participants, on average, made four changes to the profile.

Table 17.

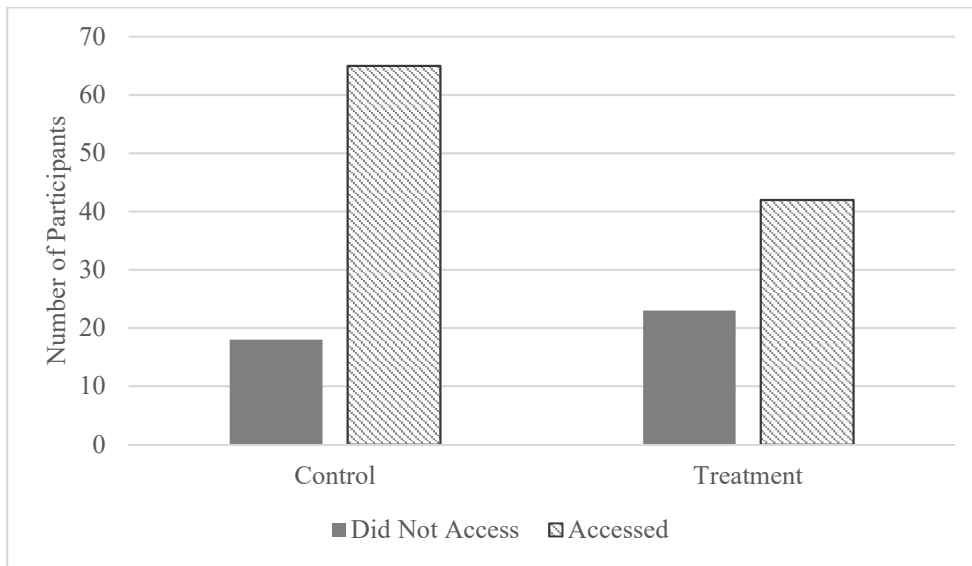
Number of Profiles Selected by Users, Number of People who Made Changes to Profiles and the Average Number of Changes made to a Profile

Profile Name	Number of Participants who		Average Number of Changes to the Profile*
	Chose Profile	Chose and Changed Profile	
	<i>n</i>	<i>n</i> (%)	<i>M</i>
Tech Adopter	2	2 (100%)	4
Tech Lover	5	2 (40%)	1
Informed User	16	8 (50%)	3.25
Connected User	19	6 (32%)	3.33

Note. 23 people in the treatment did not choose a profile; 24 people chose a profile and did not make changes. *Per participant who changed the profile

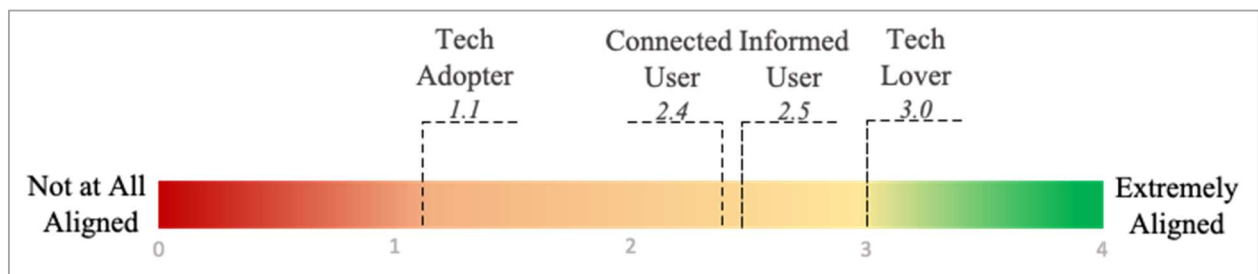
The number of participants accessing the settings page was collected to compare differences between treatment and control groups. In the control group, 65 participants (78%) accessed at least one settings page. In the treatment group, 42 participants (65%) accessed at least one profile, giving them access to all of the settings. There was a significant difference between the number of participants who accessed the settings in each group, $\chi^2(1, N=148) = 3.415, p = .048$. Significantly more participants in the control group accessed the settings page than participants in the treatment group. Each profile in the treatment condition contained all of the settings, whereas for the control group, the settings were spread across the eight settings pages of the Alexa interface. When examining the amount of time spent in the settings between groups, participants in the control group spent approximately 49 more seconds in the settings ($M = 85$ s, $SD = 86$) compared to participants in the treatment group ($M = 35$ s, $SD = 34$). A *t*-test assuming unequal variances was conducted to examine the time spent in settings by group. The difference was statistically significant, $t(113) = -4.85, p < .0001$. This difference was expected as those in the treatment group only had four profile options and within each profile all settings were included on one page, compared to those in the control group who had eight pages of settings.

Figure 34.
Number of Participants who Accessed at least one Settings Page



Settings Intervention Reaction Measures. The extent to which a participant felt that they aligned with the settings profile they chose was collected to analyze how well the user profiles fit general users (See Figure 26). The Tech adopter profile was rated the lowest ($M = 1.1$, $SD = .90$), indicating that participants did not align to the profile. Participants rated the Informed User profile ($M = 2.5$, $SD = .85$) and Connected User profile ($M = 2.4$, $SD = .87$) similarly, that is as moderately aligned. Tech Lover was rated the highest in alignment ($M = 3.0$, $SD = .58$), indicating that those who chose the profile strongly aligned with the profile description.

Figure 35.
Average Participant Ratings Alignment Felt with each Settings Profile



Major Findings and Key Outcomes.

Discussion. This evaluation sought to examine whether terms and conditions, and setting interventions utilized during device set up impacted users' behaviors, knowledge, and experience, and user reactions to these interventions. Results indicate that the interventions had a significant impact on user behavior.

Terms and Conditions Interventions. When examining the interactions with the terms and conditions, those in the treatment group accessed the terms and conditions significantly more frequently than participants in the control and for a significantly longer time period. The Terms and Conditions Guru's summaries may have sparked participants interest in the terms and conditions causing them to explore the full terms and conditions for further information. The fact that summaries were short and used plain language may have also led users to feel more comfortable accessing the terms and conditions (Choi, Park, & Jung, 2018); (Palka & Lippi, 2021). For example, (Turow, Hennessy, & Draper, 2015) suggest that short and specific privacy notices can lead users to read their information. When examining time spent in the terms and conditions, participants in the treatment group spent significantly more time than participants in the control group. Although 93 seconds may not seem like a practically significant amount of time, it is enough to skim relevant sections of the terms and conditions. Further, this amount of time is far greater than times reported in previous studies. A study by (Obar & Oeldorf-Hirsch, 2020) examined whether people would review terms of service and privacy policy on a fake social media website, using two gotcha clauses. Participants in their study were required to review the terms and conditions and spent on average 14 seconds in the terms and conditions. In comparison, participants in the current evaluation study were not required to access the terms and conditions, but spent more time, increasing their likelihood of obtaining additional information about the product's terms and conditions. The fact that individuals who accessed the terms and conditions spent far less than time than needed to read the full terms and conditions is in line with previous studies (Bakos, Marotta-Wurgler, & Trossen, 2014); (Obar & Oeldorf-Hirsch, 2020). However, it is important to note that participants in the current study may have only scrolled until they reached the summary that sparked their interest. Future studies should attempt to determine how much of the time in the terms and conditions is spent reading and how much is spent locating information. This could be achieved using screen recording software. Additionally, alternative methods of displaying the terms and conditions should be examined, such as expandable grids with summaries to allow participants to easily locate the relevant sections instead of having to scroll through a large amount of text. Expandable grids also allow users to easily expand sections to read further information in that section, which may lead to more time spent reading, rather than locating, information.

Participants who accessed the terms and conditions were found to score significantly higher on the knowledge test than those who did not access the terms and conditions. However, no significant difference was found in knowledge scores between the treatment and control groups. This may be due to the researcher-developed questions, as they may not have been effective questions for assessing terms and conditions knowledge. Some of the questions may have been too easy, allowing participants to guess the correct answer. Additionally, although the summaries provided by the Terms and Conditions Guru may have sparked interest in the terms and conditions, the format of the terms and conditions may not have led users to have an increased understanding of the content included in the terms and conditions. A study by (Barocas & Nissenbaum, 2009) found that even when users read privacy policies within the terms and conditions, they are not entirely clear on what is collected by their publisher, third parties, and what is provided to the third parties who have privacy policies of their own. Future studies should ensure the content validity of knowledge questions and look into different ways of presenting the terms and conditions information to improve user understanding. For example, the interface could allow users to select a simplified language option within the terms and conditions. Future studies should also examine the verbiage used in privacy awareness

techniques, which use simplified language to make users aware of privacy risks) and attempt to apply it to terms and conditions interventions (Ziegeldorf, Morchon, & Wehrle, 2014). Two participants in the treatment group also correctly identified the gotcha clause, while no participants in the control group identified the gotcha clause. (Obar & Oeldorf-Hirsch, 2020) included a gotcha clause in their study, in which 9 out of 543 people found the gotcha clause, which is .01% compared to the 4% found in the current evaluation study's treatment group. This indicates that there were some participants who did read the terms and conditions in the treatment group. Potentially, the summaries by the Terms and Conditions Guru did promote reading for some of those in the treatment group. Most of the participants in the treatment group felt that the Terms and Conditions Guru's information was helpful. However, some of the participants felt there was too much information. Although most set-up screens contained only one summary, there was one screen in which three summaries were included. It may therefore be more beneficial to include no more than one summary from the Terms and Conditions Guru per page, as it may overwhelm users setting up their device. Additionally, the information provided by the Guru could be improved to reduce word count and present information more likely to be unknown by the average user.

Settings Interventions. Participants in the control group accessed the settings pages more than participants in the treatment group. This may be due to the familiarity of the settings format, compared to the matrix format from which the treatment group had to select a profile option. A study by Bohme and Kopsell found that users tend to interact and respond better to information presented in formats with which they have more experience (2010). If the goal is to have users review all settings, it may be important to provide a template that is similar to a users' traditional set up expectations. Potentially a survey-based approach instead of a table format would be more beneficial for presenting default settings to the user. This would eliminate the need for profile titles and allow users to directly select who would be using the device, how much oversight they would like to have, the extent of feature use, and experience. However, 24 users selected a profile and did not change any of the default settings associated with the profile, much like the typical user who accepts settings without reviewing (He, Bahirat, Knijnenburg, & Menon, 2019). Participants in the treatment group who chose a profile at least had the opportunity for their default settings to be tailored to their device users, whether they accessed a settings page or not. Perhaps the profile led some users to trust the recommended settings without accessing the settings page. While not ideal, this is an improvement over accepting generic default settings.

Participants in the treatment condition spent significantly less time in the settings than those in the control condition by 49 seconds. The fact that settings were presented on the same page for the treatment group, minimized the need to navigate to other areas, potentially minimizing the time it took to access all settings. The complexity of manually setting up privacy preferences leads users to commonly skip the setup all together (He, 2019). The fact that 65% of participants in the treatment group selected a profile and spent more time examining the settings compared to participants in the control group is an improvement potentially pointing to the benefit of presenting all settings in one area. Future studies should examine different settings presentations as well as presenting all settings on a single page, to see if there is a different method which will produce more efficient interactions.

As previously mentioned, the number of changes made to the settings by the control group were not collected; however, for those in the treatment group, the profiles chosen, and changes made to the profiles were collected. The Connected User profile was selected the most with a portion of participants making a few changes. Participants may have felt the name was easy to understand or that the information which corresponded to this profile in the user profile menu was appropriate for them leading them to click into the profile. When taking the time to review the profile some participants may have felt that the settings did not represent their needs. When looking at the degree to which the users who chose Connected User rated their alignment to the profile it was more than moderate but not quite very aligned. A similar trend emerges for the Informed User, with a similar number of participants selecting the profile, however half of those who chose the profile made a few changes. The Tech Lover profile was not selected frequently but less than half of those who did select the profile made an average only one change to the profile. Tech Lover had the highest alignment rating (very much aligned) out of all of the profiles. Potentially there are not that many individuals who are passionate enough about technology to refer to themselves as Tech Lovers, however, those who do felt that the settings did align with their needs. Tech Adopter was chosen the least out of all of the profiles and all participants who chose it made on a few changes. The Tech Adopter also received the lowest rating for alignment. The name of the profile may have been too unclear for participants to know what to expect, and the menu information may not have been relevant or applied well to the typical user, leading less participants to click on the profile. Those who did select the profile may not have felt that the settings accurately represented what they expected given the name. Future research should both adjust the profiles based on the results of this study and collect additional empirical data in an attempt to increase user relevancy and alignment.

Further, the way the profile menu presented the settings may not have been relevant to how the user intends to use the IoT device, which has been found to lead the user to skip set up (Almuhimedi, et al., 2015). Future profiles should ensure the names, descriptions, and default settings are appropriate and relevant to users. Names should make users more aware of what settings to expect. Profiles should be adjusted to include appropriate settings to the user. Further, different settings configurations should be examined, and information related to what settings are and are not changed in each profile should be used to inform more appropriate profiles. Additionally, the profiles could be improved by finding a way to present how settings changes alter the security of the device without adding clutter (e.g., a small popup). Research should also examine how clarifying the level of privacy associated with the profile, as opposed to level of oversight associated with a profile, affects user perceptions. Finally, research should be conducted exploring additional questions to ask users to extract appropriate settings as there may be more relevant factors driving profile settings.

When examining settings accessed by the control group, more individuals in the control group accessed settings compared to the treatment group. This may be due to the way in which the treatment group settings were depicted. For example, it may not have been clear to participants that profiles pages were where to access settings, leading them to skip the section. Future research should try using different techniques that makes it clear the settings are located in this area or providing the option for users to set up their device in the traditional way (settings menu).

Limitations. These findings should be interpreted with caution given several limitations. The survey took around 9 minutes to complete and may have led to survey fatigue. The sample size was not very large, future studies should attempt to recruit a larger number of participants. Many participants did not answer questions in the survey, future studies should look at adding other alternatives like forced response on questions. Due to the nature of the survey study, many of the participants did not finish the full study and their data were not included in the final analyses. Additionally, the use of the Qualtrics testbed prevented collecting the actual changes made to the settings by participants. Future studies should evaluate other testbed options that provide more flexibility in data collection. Additionally, given the limitations of the platform used, not all settings options could be included. Only those that would span a page, and that the researchers felt were relevant to the user's privacy, were included. Therefore, future studies should look to include all information in the settings within profiles.

Conclusion. The current study evaluated the effectiveness of two interventions designed to influence user safe behaviors during IoT device setup. Specifically, we examined whether presenting information via a Terms and Conditions Guru that summarized important information about device terms and conditions throughout the setup could increase user's accessing, and understanding of, the terms and conditions. Additionally, we evaluated whether settings profiles, which helped users find the safest combination of settings based on their device use, and compare, select, and adjust their profile, could reduce setup time, and encourage users to adjust settings to ensure their information was protected to a degree that was consistent with the way in which they use their device. The results suggest that both interventions were effective in influencing user behaviors. Specifically, the Terms and Condition Guru led to users accessing and spending more time in the terms and conditions. Further, settings profiles led participants to access the settings less than those in the control, also spending less time. This may suggest a more efficient setup process. These results provide preliminary evidence for the utilization of such interventions to influence user privacy behaviors. Future research and development efforts should expand on these findings with the goal of encouraging users to take appropriate action to ensure their personal information is utilized safely by IoT devices.

Objective 4. ROTC Student Mentoring, Training and Education

Six ROTC Cadets participated in the research effort as research assistants. Included in the following sections are summaries of the mentoring, training, and education that each cadet experienced.

Tricia Prior, ROTC Cadet Studying Forensic Psychology at Florida Tech

Mentoring. Cadet Prior received mentoring from two graduate students, a post-doctoral researcher, and a Florida Tech professor. Mentoring included guidance on how to conduct human factors research, utilize a range of human factors research technology and tools, guidance and feedback on research tasking, networking opportunities within the DoD, human factors and cybersecurity communities and guidance in development of publications for academic conferences and refereed journals. Her mentors also provided a presentation about building a strong resume and LinkedIn profile.

Knowledge and Skills Training. Cadet Prior learned a range of different knowledge and skills necessary to conduct effective human factors research. This included learning to conduct literature reviews to provide insight into the theoretical foundations and practical implications of IoT research. She also completed research ethics training and learned how to develop Institutional Review Board protocols and complete the approval process. She was also trained in conducting survey-based research, including survey design, implementation, data scoring, coding and visualization, qualitative thematic data analysis, and data interpretation.

Technology and Tools Training. Cadet Prior also learned to utilize an array of research technology and tools. She learned how to use Qualtrics Online Survey Tool and Microsoft Excel for data analysis. This included creating part of a user survey on Qualtrics, including different question formats, and exporting data for analysis. Cadet Prior learned to use MS Excel to separate, organize and analyze data, including creating tables and graphs to display the results.

Tasking Guidance and Feedback. Cadet Prior met with the team met each week to receive assigned tasking, and to follow up on previous tasks and progress. She was in constant communication via the ATLAS Lab's virtual lab space on Discord and virtual meetings via Zoom to collaborate and ensure tasks were completed to standard.

Networking. Tricia attended the virtual I/ITSEC military conference and took notes on presentations, papers, and tutorials relevant to IoT research. She attended the ATCA and HFES conferences to gain more information surrounding IoT and cybersecurity. She also attended meetings with stakeholders, including Mr. Apurva Shah and Col Benjamin Sangster. Cadet Prior also attended a mentoring meeting with Vice Admiral (retired) TJ White who provided mentoring on a range of topics including advice regarding entering a new career field and the critical threats facing the nation in cyberspace.

Publication. Cadet Prior has had the opportunity to co-author three publications including two academic conference proceedings and one refereed journal articles.

Jared Blanco, ROTC Cadet Studying Software Engineering at Florida Tech

Mentoring. Cadet Blanco received mentoring from two graduate students and a Florida Tech professor. Mentoring included guidance on how to conduct cybersecurity research, including modeling cyber threat actors and attack motivations, conducting experimental evaluations, data collection, classification, and visualization, and protocol analysis. His mentors also helped him create a resume and application for an internship at the US Army Cyber Center of Excellence.

Knowledge and Skills Training. Cadet Blanco learned a range of different knowledge and skills necessary to conduct effective cybersecurity research. This included learning to conduct literature reviews to provide insight into IoT research's theoretical foundations and practical implications.

Technology and Tools Training. Cadet Blanco learned to utilize an array of research techniques and tools. He learned how to analyze protocols using tcpdump and Wireshark. He learned how to build machine learning models in scikit-learn. Further, he learned to analyze the

security of network protocols using mitmproxy, snort, and zeek. He learned about specific IoT analysis frameworks, including Binwalk and Centrifuge.

Tasking Guidance and Feedback. Cadet Blanco met with the team met each week to receive assigned tasking and to follow up on previous tasks and progress both virtually (on Discord) and in-person in the Florida Tech IoT S&P lab to collaborate and ensure tasks were completed to standard.

Networking. Based on our mentorship and networking efforts, Cadet Blanco earned an internship at the US Army Cyber Center of Excellence at Fort Gordon, GA. Cadet Blanco also attended a mentoring meeting with Vice Admiral (retired) TJ White, who provided mentoring on a range of topics, including advice regarding entering a new career field and the critical threats facing the nation in cyberspace.

Dylan Jesse, ROTC Cadet Studying Computer Science at Florida Tech

Mentoring. Cadet Jesse received mentoring from two graduate students and a Florida Tech professor. Mentoring included guidance on conducting cybersecurity research, including modeling cyber threat actors and attack motivations, conducting experimental evaluations, data collection, classification, visualization, and protocol analysis. His mentors also helped him prepare for national-level cybersecurity competitions, understanding binary, and web exploitation topics.

Knowledge and Skills Training. Cadet Jesse learned a range of different knowledge and skills necessary to conduct effective cybersecurity research. This included learning to conduct literature reviews to provide insight into the theoretical foundations and practical implications of IoT research. Further, Cadet Jesse learned how to perform responsible disclosure, notifying vendors and appropriate parties about the findings. In this capacity, he learned methods for effective communication for communicating findings in precise language to both technical and non-technical levels.

Technology and Tools Training. Cadet Jesse learned to utilize an array of research technology and tools. He learned how to analyze protocols using tcpdump and wireshark. He learned how to build machine learning models in scikit-learn. Further, he learned to analyze the security of network protocols using mitmproxy, snort, and zeek. He learned about specific IoT analysis frameworks, including Binwalk and Centrifuge. He learned to analyze web vulnerabilities using the Burpe Suite.

Tasking Guidance and Feedback. Cadet Jesse met with the team met each week to receive assigned tasking and to follow up on previous tasks and progress both virtually (on Discord) and in-person in the Florida Tech IoT S&P lab to collaborate and ensure tasks were completed to standard.

Networking. Cadet Jesse had the opportunity to represent our lab at national-level cybersecurity competitions. We coached his team to take 2nd place at the National Cyber League tournament and 3rd Place at the US Cyber Quest Easter Regionals. Dylan received a prestigious scholarship for his performance at the US Cyber Quest tournament. Cadet Jesse had the

opportunity to brief his research to US Army Cyber Command, disclosing the security implications of his findings. Cadet Jesse also attended a mentoring meeting with Vice Admiral (retired) TJ White, who provided mentoring on a range of topics, including advice regarding entering a new career field and the critical threats facing the nation in cyberspace.

Publication. Cadet Jesse has had the opportunity to co-author two academic conference proceedings.

Pearson Kerchner, ROTC Cadet Studying Information Systems at Florida Tech

Liam Avery Yu, ROTC Cadet Studying Information Systems at Florida Tech

Chandler Hake, ROTC Cadet Studying Computer Science at Florida Tech

Mentoring. All the three Cadets received mentoring from two graduate students, and a Florida Tech professor. Mentoring included guidance on how to conduct research in modeling and analysis, which involved exploring formal modeling and analysis for IOT, guidance and feedback on research tasking, networking opportunities within the DoD, modeling and cybersecurity communities and guidance in development of publications for academic conferences and refereed journals.

Knowledge and Skills Training. All the three Cadets learned the required knowledge and skill for performing research in the area of modeling and analysis. This included learning to conduct literature reviews to develop an understanding of the theoretical foundations and practical applications. They were trained in research methodologies, ontology, designing Mind Map and requirement analysis.

Technology and Tools Training. Cadet Hake also learned to utilize an array of research technology and tools. They learned to use tools such as Protégé in developing ontologies, using draw.io to model Mind Map, automated reasoners such as SparQL for executing automated queries.

Tasking Guidance and Feedback. All the three cadets met with the team each week to receive assigned tasking, and to follow up on previous tasks and progress. He was in constant communication via the ASSIST Lab's virtual lab space on Teams and virtual meetings via Zoom to collaborate and ensure tasks were completed to standard.

Networking. The cadets attended meetings with stakeholders. They also attended a mentoring meeting with Vice Admiral (retired) TJ White who provided mentoring on a range of topics including advice regarding entering a new career field and the critical threats facing the nation in cyberspace.

Publication. Cadet Hake has the opportunity to co-author the paper on Modeling human machine interaction to mitigate IOT risk.

Objective 5. Coordination with Military STEM and Cybersecurity Stakeholders

We identified four DoD organizations with whom our research efforts align. Each of the stakeholders identified have unique program needs and objectives with which our research program aligns. These organizations and associated points of contact (POCs), program descriptions and program alignments are summarized in Table 18.

Table 18.
Stakeholders Organizations, Points of Contact (POC)

Organization	POC	Program Description	Research Effort Alignment
Navy Cyber Defense Operations Command	CDR Matt Caylor, Strategic Director	NCDOC is responsible for executing defensive cyber operations through proactive cyber defense.	Aligns with understanding threats posed by IoT defenses so POC can construct reactive defense to IoT abuse.
US Naval Academy, Cyber Sciences	Dr. Dennis Dias, ONR Chair	USNA ONR is responsible for STEM-based education for US Naval Officer Corps.	Aligns with mentoring efforts of ROTC Cadets. (Reducing barriers to entry) and survey-based research.
US Army Cyber Command	Col Benjamin Sangster, Senior Advisor Maj Ryan Hand, Team Leader	POC is responsible for talent acquisition and development within US Cyber Command.	Aligns with mentoring efforts of ROTC Cadets and recommendations and results from human use experimentation.
U.S. Army Combat Capabilities Development Command (DEVCOM)	Mr. Apurva Shah, Director Cyber Technology Branch, CO2 Division C5ISR Center	POC is responsible for the examining IoT security and developing offensive/defensive capabilities.	Aligns with development of IoT Dataset for machine-learning model being developed by POC.

We briefed two of the four organizations and plan to brief the other two organizations in the coming months in a newly related project funded under this same program. The briefings conducted are summarized below.

DoD Stakeholder Presentations

US Army Combat Capabilities Development Command (DEVCOM)

Methods for Labeling IoT Traffic Datasets” presented to Technical Cyber Technology Branch, CO2 Division, C5ISR Center, Oct 1, 2020.

“Implication of IoT SPI Flash Attacks” presented to Technical Cyber Technology Branch, CO2 Division, C5ISR Center, Oct 19, 2020.

“IoT Dataset Findings & IoT Man-in-the-Middle Vulnerabilities” presented Technical Cyber Technology Branch, CO2 Division, C5ISR Center, May 13, 2021.

US Army Cyber Command

“Vulnerabilities in Commercial Smart Home Cameras and Doorbells,” presented to US Army Cyber Command, Dec 2020.

“IoT Dataset Findings & IoT Man-in-the-Middle Vulnerabilities” presented to US Army Cyber Command, May 14, 2021.

Dissemination

This research effort resulting in a total of 17 publications/presentations, including seven academic conference presentations/proceedings, four refereed journal publications, and one master’s Thesis. This effort also resulted in seven vulnerability technical reports. These publications are listed below.

Academic Conference Presentations and Proceedings

Rebensky, S., Carroll, M., Nakushian, A., Chaparro, M., & Prior, T. (2021). Understanding the last line of defense: Human response to cybersecurity events. *Human Computer Interaction International 2021*.

Chaparro, M., Nakushian, A., Prior, T., Rebensky, S., & Carroll, M. (Under Review). User experience, knowledge, perceptions, and behaviors associated with Internet of Things (IoT) device information security. *ACSAC 2021*.

O’Connor, T.J., Jesse, D. & Campos, D. (2021). Through the spyglass: Toward IoT companion app man-in-the-middle attacks. *USENIX Cyber Security Experimentation and Test Workshop (CSET) 2021*.

Campos, D. & O’Connor, T.J. (2021). Towards labeling on-demand IoT traffic. *USENIX Cyber Security Experimentation and Test Workshop (CSET) 2021*.

Alhazmi, A., Kilani, G., Allen, W., & O’Connor, T.J. (2021). A replication study for IoT privacy preferences. *IEEE Conference on Omni-Layer Intelligent Systems (COINS)*.

O’Connor, T.J. & Stricklan, C. (2021). Teaching a hands-on mobile and wireless cybersecurity course. *ACM Innovation and Technology in Computer Science Education (ITiCSE)*.

O’Connor, T.J., Jesse, D., & Campos, D. (2021). Towards examining the security cost of inexpensive smart home IoT devices. In Submission.

Refereed Journal Articles

Bhattacharyya, S., Gupta, A., & Nembhard, F. (2021). Assume guarantee reasoning for IoT devices with CSADL. *IEEE Systems*.

Bhattacharyya, S., Hake, C., Kiran, H., & Gupta, A. (2021). Modeling human interactions to mitigate IOT risk. *ACM transactions on IOT*.

Chaparro, M., Nakushian. A., Prior, T., Rebensky, S., & Carroll, M. (In Preparation).

Gupta, A., Campos, D., Bhattacharyya, S., O'Connor, T.J., & Dcosta, A. (2021). Modeling Internet-of-Things (IoT) behavior for enforcing security and privacy policies. *IEEE IOT*.

Theses and Dissertations

Campos, D. (2021). Ground Truth: Towards Labeling On-Demand IoT Traffic, Master's Thesis, Florida Institute of Technology.

Vulnerability Disclosures

Technical report on vulnerability in Geeni Doorbell, reported to MITRE (CVE-2020-28998)

Technical report on vulnerability in Geeni Camera, reported to MITRE (CVE-2020-28999)

Technical report on vulnerability in Geeni Camera, reported to MITRE (CVE-2020-29000)

Technical report on vulnerability in Geeni Camera, reported to MITRE (CVE-2020-29001)

Technical report on vulnerability in NightOWL Doorbell, reported to MITRE (CVE-2020-28713)

Technical report on vulnerability in NightOWL Doorbell, reported to MITRE (CVE-2021-31793)

Technical report on vulnerability in Kangaroo Camera, reported to MITRE (CVE-2021-33559)

Participants

Name	Role	Person Months Worked
Tactical Cyber Defense Team		
Dr. TJ O'Connor	Co-PI	1 month
Daniel Campos	Graduate Research Assistant (MS)	5 months
Jared Blanco	ROTC Cadet Researcher	1 months
Dylan Jessie	ROTC Cadet Researcher	3 months
Strategic Cyber Defense Team		
Dr. Sid Bhattacharyya	Co-PI	0.5 month
Anubhav Gupta	Graduate Research Assistant (PhD)	4 months
Adolf D'Costa	Graduate Research Assistant (MS)	1 month
Pearson Kerchner	ROTC Cadet Researcher	1.5 months
Liam Avery Yu	ROTC Cadet Researcher	0.5 months
Chandler Hake	ROTC Cadet Researcher	1 month
Human Cyber Decision-Making Team		
Dr. Meredith Carroll	Co-PI	3 months
Maria Chaparro (PhD)	Graduate Research Assistant (PhD)	7 months
Andrew Nakushian (MS)	Graduate Research Assistant (MS)	6 months
Tricia Prior	ROTC Cadet Researcher	2.5 months

References

- Acar, A., Fereidooni, H., Abera, T., Sikder, A., Miettinen, M., Aksu, H., . . . Uluagac, S. (2020). Peek-a-boo: I see your smart home activities, even encrypted. *Conference on Security and Privacy in Wireless and Mobile Networks*, (pp. 207-218).
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509.
- Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 54(2), 442-492. doi:doi:10.1257/jel.54.2.442
- Air Line Pilots Association. (2017). *Aircraft cybersecurity: the pilot's perspective*.
- Al Hogail, A. (2018). Improving IoT technology adoption through improving consumer trust. *Technologies*, 6(3), 64. doi:https://doi.org/10.3390/technologies6030064
- Albert, L., Rodan, S., Aggarwarl, N., & Hill, T. (2019). Gender and generational differences in consumers' perceptions of Internet of Things (IoT) devices. *E-Journal of Social & Behavioural Research in Business*, 10(3), 41-53.
- Aleisa, N., Renaud, K., & Bongiovanni, I. (2020). The privacy paradox applies to IoT devices too: a Saudi Arabian study. *Computers & Security*, 96.
- Alfageeh, A., Bhattacharyya, S., & Patel, M. (2019). Assurance for cybersecurity with assume-guarantee reasoning. . *IEEE-UEMCON*.
- Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., & Agarwal, Y. (2015). Your location has been shared 5,398 times! A field study on mobile app privacy nudging . *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, (pp. 787-796).
- Alrawi, O., Lever, C., Antonakakis, M., & Monroe, F. (2019). Sok: security evaluation of home-based IoT deployments. . *2019 IEEE Symposium on Security and Privacy (SP)*.
- Alshehri, A., Ben Salem, M., & Ding, L. (2020). Are smart home devices abandoning IPV victims. *Conference on Trust, Security, and Privacy in Computing and Communications* (pp. 1368-1375). IEEE.
- Amazon Web Services . (2021). *Cloud object storage- store and retrieve data anywhere- Amazon Simple Storage Service (S3)*. Retrieved from Amazon Web Services: <https://aws.amazon.com/s3/>
- Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., . . . Zhou, Y. (2017). Understanding the mirai botnet . *USENIX Security*, (pp. 1093-1110).
- Bajaj, K. (2014). Cyberspace: post-Snowdon. *Strategic Analysis*, 4, 582.

- Bakos, Y., Marotta-Wurgler, F., & Trossen, D. (2014). Does anyone read the fine print? Consumer attention to standard-form contracts? *The Journal of Legal Studies*, 43(1), 1-35.
- Barocas, S., & Nissenbaum, H. (2009). On notice: The trouble with notice and consent. *The First International Forum on the Application and Management of Personal Electronic Information*.
- Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51-61. doi:<https://doi.org/10.1016/j.chb.2015.01.039>
- Bohme, R., & Kopsell, S. (2010). Train to accept? A field experiment on consent dialogs . *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, (pp. 2403-2406).
- Bowen, B., Devarajan, R., & Stolfo, S. (2011). Measuring the human factor of cybersecurity. *Technologies for Homeland Security (HST), 2011 IEEE International Conference*, 230-235.
- Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness, and education. *Computers & Security* . doi:<https://doi-org.portal.lib.fit.edu/10.1016/j.cose.2019.101647>
- Brough, A., & Martin, K. (2020). Critical roles of knowledge and motivation in privacy research. *Current Opinion in Psychology*, 31, 11-15. doi:<https://doi-org.portal.lib.fit.edu/10.1016/j.copsyc.2019.06.021>
- Burns, A., Roberts, T., Posey, C., Bennet, R., & Courtney, J. (2015). Assessing the role of security education, training, and awareness on 'insiders' security-related behavior: an expectancy theory approach. *2015 48th Hawaii International Conference on System Sciences*.
- Cameron, D., & Mehrotra, D. (2021). *Ring's neighbors data let us map Amazon's home surveillance network*. Retrieved from Gizmodo : <https://gizmodo.com/ring-s-hidden-data-let-us-map-amazons-sprawling-home-su-1840312279>
- Carroll, M., Wilt, D., Carstens, D., Sanchez, P., Pittorie, W., & Lindsey, S. (2018). *NextGen human factors considerations for information of varying levels of integrity, reliability, and security on the flight deck. (DTFAWA-16-D-00003)*.
- Chaparro, M., Nakushian, A., Prior, T., Rebensky, S., & Carroll, M. (In Preparation). User Experience, Knowledge, Perceptions, and Behaviors associated with Internet of Things (IoT) Device Information Security.
- Chief of Naval Personnel Public Affairs. (2016, November 22). *Security breach notification of sailors' PII*. Retrieved from America's Navy : http://www.navy.mil/submit/display.asp?story_id=97820

- Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42-51.
- Choi, J., Anwar, A., Alasmary, H., Spaulding, J., Nyang, D., & Mohaisen, A. (2019). IoT malware ecosystem in the wild: a glimpse into analysis and exposures. *Symposium on Edge Computing* (pp. 413-418). ACM.
- Conti, G., Ahamad, M., & Stasko, J. (2005). Attacking information visualization system usability overloading and deceiving the human. *Proceedings of SOUPS '05*.
- Coover, M., Dreibelbis, R., & Borum, R. (2016). Factors influencing the human-technology interface for effective cybersecurity performance. . In S. Zaccaro, R. Dalal, L. Tetrick, & J. Steinke, *Psychosocial Dynamics of Cybersecurity* (pp. pp. 267-290). Routledge.
- Cortesi, A., Hils, M., & Kriechbaumer, T. (2010). *Mitmproxy: a free and open source interactive HTTPS proxy, 2010*. Retrieved from <https://mitmproxy.org>
- Covington, H. (2019). Smart homes: IoT security and ethical concerns. *Proceedings for the Northeast Region Decision Sciences Institute (NEDSI)*, 531-547.
- Dahmen, J., Cook, D., Wang, X., & Honglei, W. (2017). Smart secure homes: a survey of smart home technologies that sense, assess, and respond to security threats. *Journal of Reliable Intelligent Environments*, 3(2), 83-98.
- Daubert, J., Wiesmaier, A., & Kikiras, P. (2015). A view on privacy & trust in IoT. *2015 IEEE International Conference on Communication Workshop, ICCW 2015*, 2665-2670. doi:10.1109/ICCW.2015.7247581
- Distenfanso, S., Merlino, G., & Puliafito, A. (2012). Sensing and actuation as a service: a new development for clouds. *International Symposium on Network Computing and Applications, IEEE*, 272-275.
- Dooley, E. (2021). *ADT technician pleads guilty to hacking home security footage*. Retrieved from United States Department of Justice : <https://www.justice.gov/usao-ndtx/pr/adt-technician-pleads-guilty-hacking-home-security-footage>
- Emami-Naeini, P., Agarwal, Y., Faith Cranor, L., & Hibshi, H. (2020). Ask the experts: what would be on an IoT privacy and security label? *2020 IEEE Symposium on Security and Privacy*, 447-464. doi:<https://doi-org.portal.lib.fit.edu/10.1109/SP40000.2020.00043>
- Fagan, M., Megas, K., Scarfone, K., & Smith, M. (2020). *Foundational cybersecurity activities for IoT device manufacturers*. US Department of Commerce, National Institute of Standards and Technology.
- Felt, A., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: user attention, comprehension, and behavior . *Proceedings of SOUPS '12*, (pp. 1-14).

- Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2017). A stalkers paradise: how intimate partner abusers exploit technology ., (pp. 2177-2184). International Conference on Distributed Computing Systems (ICDCS) .
- Furman, S., Theofanos, M., Choong, Y., & Stanton, B. (2012). Basing cybersecurity training on user perception. *IEEE Security & Privacy*, 10(2).
- Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: a systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77, 226-261.
- Gonzalez-Gil, P., Martinez, J., & Skarmeta, A. (2020). Lightweight data-security ontology for IoT. *Sensors*, 20(3), 801.
- Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet. *Group Decision and Negotiation*, 13, 149-172.
- Hariri, A., Giannelos, N., & Arief, B. (2019). Selective forwarding attack on IoT home security kits. *European Symposium on Research in Computer Security* (pp. 360-373). Springer .
- Harwell, D. (2019, November 19). *Police can keep Ring camera video forever and share with whomever they'd like, Amazon tells senator*. . Retrieved from Washington Post: <https://wapo.st/2u46Y0d>
- He, Y. (2019). Recommending privacy settings for Internet-of-Things.
- He, W., Golla, M., Padhi, R., Ofek, J., Durmuth, M., Fernandes, E., & Ur, B. (2018). Rethinking access control and authentication for the home Internet of Things (IoT) . *USENIX Security* , (pp. 255-272).
- He, Y., Bahirat, P., Knijnenburg, B., & Menon, A. (2019). A data-driven approach to designing for privacy in household IoT. *ACM Transactions on Interactive Intelligent Systems*, 10(1), 1-47.
- Hirshfield, L., Bobko, P. B., Costa, M., Funke, G., Mancuso, V., Finomore, V., & Knott, B. (2015). The role of the device user's' suspicion in the detection of cyber attacks. *International Journal of Cyber Warfare and Terrorism*, 5(3), 28-44.
- Hoffman, R., Lee, J., Woods, D., Shadbolt, N., Miller, J., & Bradshaw, J. (2009). The dynamics of trust in cyberdomains. *IEEE Intelligent Systems*, 24(6).
- Hsu, J. (2018, 1 29). *The strava heat map and the end of secrets*. Retrieved from Wired: <https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/>
- Huang, D., Apthorpe, N., Acar, G., Li, F., & Feamster, N. (2019). IoT inspector: crowdsourcing labeled network traffic from smart home devices at scale. *Proceedings of the ACM on Interactive, Mobile, Wearable, and Ubiquitous Technologies*., 4(2).

- Huigang, L., & Yaijong, X. (2010). Understanding security behaviors in personal computer usage: a threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.
- Janes, B., Crawford, H., & O'Connor, T. (2020). Never ending story: authentication and access control design flaws in shared IoT devices. *Security and Privacy Workshops (SPW)* (pp. 104-109). IEEE.
- Jang, Y., Chang, S., & Tsai, Y. (2014). Smartphone security: understanding smartphone 'users' trust in information security management. *Security and Communication Networks*, 7, 1313-1321.
- Jia, Y., Chen, Q., Wang, S., Rahmati, A., Fernandes, E., Mao, Z., & Prakash, A. (2017). ContextIoT: towards providing contextual integrity to appified IoT platforms. *NDSS*, 2(2), 2-2.
- Jimenez Iglesias, L., Aguilar Paredes, C., Sanchez Gomez, L., & Gutierrez, M.-M. (n.d). User experience and media. The three click rule in newspapers' webs for smartphones. *Revista Latina de Comunicacion Social*, 73, 595-613. doi:<https://doi.org/10.4185/RLCS-2018-1271>
- Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). My data just goes everywhere: User mental models of the internet and implications for privacy and security. . 2015 *Symposium on Usable Privacy and Security* , 39-52.
- Keith, M., Maynes, C., Lowry, P., & Babb, J. (2014). Privacy fatigue: the effect of privacy control complexity on consumer electronic information disclosure. . *International Conference on Information Systems (ICIS 2014)*, 14-17.
- Kelley, J., & Guariglia, M. (2020). *Amazon Ring must end its dangerous partnerships with police*. Retrieved from Electronic Frontier Foundation: <https://www.eff.org/deeplinks/2020/06/amazon-ring-must-end-its-dangerous-partnerships-police>
- Kelley, T., & Bertenthal, B. (2016). Real-world decision making: logging into vs. insecure website . *USEC '16*.
- Knijnenburg, B. (2015). *A user-tailored approach to privacy decision support*. University of California, Irvine.
- Kokolakis, S. (2017). Privacy attitudes and privacy behavior: a review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122-134. doi:<https://doi.org/10.1016/j.cose.2020.101897>
- Lau, J., Zimmerman, B., & Schaub, F. (2018). "Alexa, are you listening?" privacy perceptions concerns and privacy seeking behaviors with smart speakers. *Human-Computer Interaction* 2, (pp. 1-31).

- Lee, H., & Kobsa, A. (2016). Understanding user privacy in Internet of Things environments. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 407-412. doi:doi:10.1109/wf-iot.2016.7845392
- Lee, J., & See, K. (2004). Trust in automation: designing for appropriate reliance. *Human Factors*, 46(1), 50-80. doi:https://doi.org/10.1518/hfes.46.1.50_30392
- Lee, M., & Lee, J. (2010). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on internet. *Information Systems Frontiers*, 14(2), 375-393.
- Legg, P. (2016). Enhancing cyber situation awareness for non-expert users using visual analytics. *. Cyber Situational Awareness, Data*.
- Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: a threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394.
- Lueth, K. (2020). *State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time*. Retrieved from IoT Analytics: <https://IoT-analytics.com/state-of-the-IoT-2020-12-billion-IoT-connections-surpassing-non-IoT-for-the-first-time/>.
- Mahoney, S., Rother, E., Steinke, K., Pfautz, J., Wu, C., & Farry, M. (2010). A cognitive task analysis for cyber situational awareness. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 54(4).
- McDonald, A., & Cranor, L. (2008). The cost of reading privacy policies. *A Journal of Law and Policy for the Information Society*, 4(3), 543-568.
- Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, 6(5), 8182-8201.
- Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A., & Tarkoma, S. (2017). IoT sentinel: automated device-type identification for security enforcement in IoT. *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*.
- Miettinen, M., Marchal, S., Hafeez, I., Frassetto, T., Asokan, N., Sadeghi, A., & Tarkoma, S. (2017). IoT sentinel demo: automated device-type identification for security enforcement in IoT. *International Conference on Distributed Computing Systems (ICDCS)*, (pp. 2511-2514).
- Milne, G., & Culnan, M. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3), 15-29. doi:https://doi.org/10.1002/dir.20009
- Mind Map*. (n.d.). Retrieved from Wikipedia : [https://en.wikipedia.org/wiki/Mind map](https://en.wikipedia.org/wiki/Mind_map)

- Mittal, S. (2017). Understanding the human dimension of cybersecurity. *Indian Journal of Criminology & Criminalistics*, 34(1), 141-152.
- Morgan, S. (2017). *2017 cybercrime report*. Cybersecurity Ventures.
- Mudgerikar, A., Sharma, P., & Bertino, E. (2019). E-Spion: a system-level intrusion detection system for IoT devices. *Asia Conference on Computer and Communications Security* (pp. 493-500). ACM. doi:10.1145/3321705.3329857
- Musen, M. (2015). The protege project: a look back and a look forward. *AI Matters*, 1(4), 4-12.
- N.A. (2015). *Hackable at any height. Cybersecurity in the aviation industry*. Retrieved from London Cyber Security.
- N.A. (2018). *That was way too easy*. . Retrieved from Free Thought Blog: <https://freethoughtblogs.com/stderr/2018/01/21/that-was-too-easy/>
- Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, 140(4), 32-48.
- Norberg, P., Horne, D., & Horne, D. (2007). The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100.
- Noy, N., & McGuinness, D. (2001). Ontology development 101: a guide to creating your first ontology.
- Obar, J., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication, & Society*, 23(1), 128-147.
- O'Connor, T., Enck, W., & Reaves, B. (2019). Blinded and confused: uncovering systemic flaws in device telemetry for smart-home Internet of Things. *ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 140-150). ACM.
- O'Connor, T., Mohamed, R., M., M., Enck, W., Reaves, B., & Sadeghi, A. (2019). Homesnitch: behavior transparency and control for smart home IoT devices. *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 128-138.
- Olmstead, K., & Smith, A. (2017). *What the public knows about cybersecurity*. The Pew Research Center.
- Palka, P., & Lippi, M. (2021). Big data analytics, online terms of service and privacy policies. In *Research Handbook on Big Data Law*. Edward Elgar Publishing.
- Parmisano, A., Garcia, S., & Erquiaga, M. (2020). A labeled dataset with malicious and benign IoT network traffic.
- Parsia, B., & Sirin, E. (2004). Pellet: an OWL DL reasoner. *3rd International Semantic Web Conference*, (p. 13).

- Paul, K. (2020). *Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs*. Retrieved from The Guardian: <http://www.theguardian.com/technology/2020/dec/23/amazonring-camera-hack-lawsuit-threats>.
- Perdisci, R., Papastergiou, T., Alrawi, O., & Antonakakis, M. (2020). IoT finder: efficient large-scale identification of IoT devices via passive DNS traffic analysis. *European Symposium on Security and Privacy* (pp. 474-389). IEEE.
- Pfleeger, S., & Caputo, D. (2012). Leveraging behavioral science to mitigate cybersecurity risk. *Computers & Security*, 31(4), 597-611.
- Pienta, D., Sun, H., & Thatcher, J. (2016). Habitual and misplaced trust: The role of the dark side of trust between individual users and cybersecurity systems. *2016 International Conference on Information Systems*.
- Pienta, D., Sun, H., & Thatcher, J. (2016). Habitual and misplaced trust: the role of the dark side of trust between individual users and cybersecurity systems. . *2016 International Conference of Information Systems*. .
- Pinkston, J., Undercoffer, J., Joshi, A., & Finin, T. (2004). A target-centric ontology for intrusion dection. *Proceeding of IJCAI-03 Workshop on Ontologies and Distribted Systems*. .
- Proctor, R., & Chen, J. (2015). The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. *Human Factors*, 57(5), 721-727.
- Rebensky, S., Carroll, M., Nakushia, A., Chapparro, M., & Prior, T. (2021). Understanding the last line of defense: Human response to cybersecurity events. *Human Computer International 2021*.
- Ren, J., Dubois, D., Choffnes, D., Mandalari, A., Kolcun, R., & Haddadi, H. (2019). Information exposure from consumer IoT devices . *Internet Measurement Conference* (pp. 267-279). ACM.
- Rhee, H., Ryu, Y., & Kim, C. (2012). Unrealistic optimism on information security management. *Computers & Security*, 31(2), 221-232.
- Rittenberg, L., & Tregarthen, T. (2018). *Principles of Microeconomics* . Saylor.
- Robinson, E., & Zhu, Y. (2020). Beyond "I Agree": users' understanding of web site terms of service. *Social Media and Society*.
- Rosoff, H., Cui, J., & John, R. (2013). Heuristics and biases in cybersecurity dilemmas. *Environment Systems and Decisions*, 33(4), 517-529.
- Ryabinin, K., Chuprina, S., & Belousov, K. (2019). Ontology-driven automation of IoT-based human-machine interfaces development. doi:10.1007/978-3-030-22750-0_9

- Sarraipa, J., Silva, R., Jardim-Goncalves, R., & Monteiro, A. (2008). MENTOR- a methodology for enterprise reference ontology development. *4th International IEEE Conference Intelligent Systems* (pp. 32-40). IEEE. doi:10.1109/IS.2008.4670436.
- Schindler, H., Cave, J., Robinson, N., Horvath, V., Hackett, P., Gunashekar, S., . . . Graux, H. (2013). *Europe's policy options for a dynamic and trustworthy development of the Internet of Things: SMART 2012/0053*. RAND Corporation. doi:10.7249/RR356
- Schultz, E. (2002). A framework for understanding and predicting insider attacks. *Journal of Computers & Security*, 21, 526-531.
- Sharma, K. (2017). *Impact of framing and priming on 'users' behavior in cybersecurity*. .
- Singh, A., Murali, S., Rieger, L., Li, R., Hommes, S., State, R., . . . Schulzrinne, H. (2018). HANZO: Collaborative network defense for connected things . *Principles, Systems, and Applications of IP Telecommunications (IPTComm)* (pp. 1-8). IEEE.
- Sivanathan, A., Gharakheili, H., Loi, F., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2018). Classifying IoT devices in smart environments using network traffic characteristics . *Transactions on Mobile Computing* (pp. 1745-1759). IEEE.
- Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behavior*, 55, 992-1000. doi:<https://doi-org.portal.lib.fit.edu/10.1016/j.chb.2015.09.038>
- Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *20(4)*, 3453-3495.
- Stossel, L., Segar, N., Gliatto, P., Fallar, R., & Karani, R. (2012). Readability of patient education materials available at the point of care. *Journal of General Internal Medicine*, 27(9), 1165-1170. doi:<https://doi.org/10.1007/s11606-012-2046-0>
- Suarez-Figueroa, M., Gomez-Perez, A., & Fernandez-Lopez, M. (2011). The NeOn methodology for ontology engineering. In M. Suárez-Figueroa, A. Gómez-Pérez, E. Motta, & A. Gangemi, *Ontology Engineering in a Networked World* (pp. 9-34). Springer. Retrieved from https://link.springer.com/chapter/10.1007%2F978-3-642-24794-1_2
- Suresh, P., Daniel, J., Parthasarathy, V., & Aswathy, R. (2014). A state of the art review on the Internet of Things (IoT) history, technology, and fields of deployment. *2014 International Conference on Science Engineering and Management Research (ICSEMR)*, 1-8. doi:<https://doi.org/10.1109/ICSEMR.2014.7043637>
- Syed, Z., Padia, A., Finin, T., Mathews, L., & Joshi, A. (2016). UCO: A unified cybersecurity ontology. . *Workshops at the thirtieth AAAI Conference on Artificial Intelligence* .
- Taddicken, M. (2014). The 'privacy paradox' in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, 19(2), 248-273.

- Trimananda, R., Varmarken, J., Markopoulou, A., & Demsky, B. (2020). Packet-level signatures from smart home devices. *Network and Distributed Systems Security Symposium* (pp. 1-18). Internet Society.
- Turow, J., Hennessey, M., & Draper, N. (2015). *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them to exploitation* .
- U.S Navy. (2018). *Naval research and development. A framework for accelerating to the Navy and Marine Corps after next*.
- U.S. Government Accountability Office. (2017). *Cybersecurity: actions needed to strengthen U.S. capabilities, GAO-17-440T*.
- Wang, C., Kennedy, S., Li, H., Hudson, K., Atluri, G., Wei, X., . . . Wang, B. (2020). Fingerprinting encrypted voice traffic on smart speakers with deep learning. *Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 254-265). ACM.
- Wiederhold, B. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking*, 17, 131-132.
- Williams, M., Nurse, J., & Creese, S. (2017). Privacy is the boring bit: user perceptions and behaviour in the Internet-of-Things. *15th Annual Conference on Privacy, Security, and Trust (PST)*, 181-189. doi:<https://doi.org/10.1002/asi.24113>
- Wizner, B. (2017). What changed after Snowden? A U.S. perspective. . *Journal of Communication* , 897+.
- Wu, P. (2019). The privacy paradox in the context of online social networking: a self-identity perspective. *Journal of the Association for Information Science & Technology*, 70(3), 207-217. doi:<https://doi.org/10.1002/asi.24113>
- Yuan, B., Jia, Y., Xing, L., Jin, H., & Zhang, Y. (2020). Shattered chain of trust: understanding security risks in cross-cloud IoT access delegation . *USENIX Security* , (pp. 1183-1200).
- Zaccaro, S., Dalal, R., Tetrack, L., & Steinke, J. (. (2016). *Psychosocial dynamics of cyber security* . Routledge .
- Zaccaro, S., Dalal, R., Tetrack, L., & Steinke, J. (2016). *Psychosocial Dynamics of Cybersecurity*. Routledge.
- Zheng, S., Aphorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction*, 1-20. doi:<https://doi.org/10.1145/3274469>
- Ziegeldorf, J., Morchon, O., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks*, 7(12), 2728-2742.

REPORT DOCUMENTATION PAGE				
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.				
1. REPORT DATE October 13, 2021	2. REPORT TYPE Final Performance Report	3. DATES COVERED START DATE 08/03/2020 END DATE 08/02/2021		
4. TITLE AND SUBTITLE A Multidisciplinary Approach to Internet-of-Things (IoT) Cybersecurity Research to Develop the Research Capacity of ROTC Students				
5a. CONTRACT NUMBER N/A	5b. GRANT NUMBER N00014-20-1-2798	5c. PROGRAM ELEMENT NUMBER N/A		
5d. PROJECT NUMBER N/A	5e. TASK NUMBER N/A	5f. WORK UNIT NUMBER N/A		
6. AUTHOR(S) Carroll, Meredith, O'Connor, Terrence, Bhattacharyya, Siddhartha, Chaparro, Maria, Nakushian, Andrew, Prior, Tricia, et al.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Florida Institute of Technology 150 West University Blvd. Melbourne, FL 32901-6975			8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Office of Naval Research 875 N. Randolph Street, Suite 1425 Arlington, VA 22203-1995		10. SPONSOR/MONITOR'S ACRONYM(S) N/A	11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for Public Release; Distribution is Unlimited.				
13. SUPPLEMENTARY NOTES N/A				
14. ABSTRACT The goal of this research effort was to develop the research capacity of ROTC students in a multidisciplinary research program that studied IoT-based cybersecurity threats that span a range of Naval operational domains. This included (1) understanding the interconnected flow of information to and from these devices and the threats to privacy, (2) developing strategic policies that provide protections, and (3) studying how the users interact with the devices. The methods and results of this effort are discussed in detail.				
15. SUBJECT TERMS Internet of Things, Cybersecurity, Privacy, Human Factors				
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT None	b. ABSTRACT None	c. THIS PAGE None	UU	112
19a. NAME OF RESPONSIBLE PERSON Dr. Meredith Carroll			19b. PHONE NUMBER (Include area code) 321-674-8374	