DISSERTATION

NAVIGATING THE MAZE: THE EFFECTIVENESS OF MANUFACTURER SUPPORT IN APPLYING USER-CONTROLLED SECURITY AND PRIVACY FEATURES

Submitted by

Kelvin R. Shorts

Department of Systems Engineering

In partial fulfillment of the requirements

for the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Spring 2025

Doctoral Committee:

Advisor: Steve Simske

Jeremy Daily
Marie Vans
Brad Reisfeld

ABSTRACT

NAVIGATING THE MAZE: THE EFFECTIVENESS OF MANUFACTURER SUPPORT IN APPLYING USER-CONTROLLED SECURITY AND PRIVACY FEATURES

Internet of Things (IoT) technologies have reshaped the home computer environment by offering extraordinary levels of convenience, automation, and efficiency. With technologies ranging from thermostats that adjust for cost savings to water leak detectors that protect homes from costly water damage, IoT devices in the residential space are here to stay. Collectively, these interconnected devices targeted for the consumer home environment are commonly referred to as a "smart home". Despite the many capabilities that smart home IoT technologies offer, many consumers/end-users are still struggling with effectively securing their internet-connected devices, safeguarding personal data, and ensuring that their smart home network remains secure from potential threats. The responsibility for safeguarding smart home IoT devices is shared by both manufacturers and consumers/end-users; however, the extent to which manufacturers are providing clear, comprehensive, and accessible guidance to assist consumers/end-users with safeguarding IoT devices remains unclear.

This research study explores the level of support provided by smart home IoT manufacturers in applying user-controlled security and privacy features. User-controlled security and privacy features are settings within an IoT device that only the end-user can adjust (e.g. passwords, multi-factor authentication, device permissions, data backup, etc.). A systems engineering–focused, mixed-methods approach was adopted to evaluate how effectively smart home IoT manufacturers guide and assist consumers in understanding, implementing, and

maintaining user-controlled security and privacy features in their smart home IoT devices and systems. The study unfolds across four systems engineering phases: (1) Requirements Analysis, (2) Usability Testing, (3) Focus Group Technical Deep Dive, and (4) Recommendations and Future Implementations. A review of smart home IoT device manuals, online resources, and other manufacturer-provided materials established a baseline for how well the reference material aligned with cybersecurity industry standards, best practices, and recommendations. Through structured surveys, proficiency tests, and qualitative focus group technical deep dive feedback, the study identified gaps in smart home IoT manufacturers' guidance that compromise users' ability to configure essential security settings. Employing systems engineering principles, this research study underscored the importance of user-centric design and comprehensive security and privacy guidance to help bridge the gap between cybersecurity best practices and a diverse consumer/end-user skill base.

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my greatest appreciation to my advisor, Dr. Steve Simske, whose guidance, insight, and unwavering support have been cornerstones of my doctoral journey. Your mentorship has not only shaped the scope and direction of my research but also encouraged me to think critically, to question prevailing assumptions, and to continually refine my work. I am equally indebted to the members of my dissertation committee, whose expertise and constructive feedback have significantly enriched my research project. To my wife, Katrina, you have been my anchor throughout this PhD journey. Watching you conquer medical school with brilliance and grace was as inspiring as it was humbling. Your unwavering love, patience, and encouragement have been the pillars of my success. Thank you for believing in me and for showing me that, yes, there really can be two doctors under one roof (even if only one of us can actually save a life!). To my daughter, Robyn, and my son, Ryan—your laughter and curiosity served as daily reminders of why I embarked upon this journey in the first place. Your smiles ignited my determination to excel and kept my spirits lifted. I hope my pursuit of knowledge and perseverance will, in turn, inspire you in your own future endeavors. To my parents, Kenneth and Marsha, I owe an immeasurable debt of gratitude. From my earliest days in grade school through my service in the U.S. Navy, and continuing through graduate school and beyond, your unwavering love, sacrifices, and steadfast support have formed the bedrock upon which all my successes rest. You instilled in me the values of diligence, resilience, and humility, and I remain forever grateful for everything you have done to guide me to this milestone.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1. INTRODUCTION

The concept of full home automation has existed since the early 20th century, but it wasn't until the invention of Internet of Things (IoT) devices that the vision of a "connected home" truly became a reality. Today, IoT devices are everywhere and serve multiple purposes. Some of the most popular IoT devices that are in use today are designed specifically for a residential environment and can be linked together creating what has come to be known as the "smart home." Smart home IoT devices include things such as energy-saving thermostats, connected sprinkler systems, interactive refrigerators, surveillance cameras, water sensors, and essentially any other internet-connected device that provides remote management and convivence to the consumers/end-users. Over the past 25 years, the number of IoT devices in personal and residential use has grown significantly, and this trend is expected to continue, with projections indicating that global IoT device adoption could reach 125 billion devices by 2030 (IHS Markit, 2017). This rapid growth in IoT adoption has not only modernized our home environments but has also transformed the consumers' expectation to have convenience, efficiency, and connectivity to the home environment.

Despite the convenience brought to consumers by current and emerging smart home IoT devices, concerns about smart home IoT safety, security, and privacy remain a major concern (E. Fernandes, 2016) (al. W. Z., 2019) (al. Y. J., 2020). Securing and maintaining the privacy of smart home IoT devices is a shared responsibility between the smart home IoT manufacturers and the consumer/end-user. Consumers have an expectation that smart home IoT manufacturers are currently selling and will continue to sell IoT devices that are secure-by-design, equipped with built-in security and privacy protective measures that "just work" right out of the box. Many users

prioritize simplicity and reliability, and trust that IoT manufacturers will handle the security aspects so they can focus on using their devices seamlessly and safely. Unfortunately, previous studies have pointed out that smart home IoT manufactures often prioritize rapid deployment and user convenience over security and privacy best practices (S. Sicari, 2015). Smart home IoT manufacturers often operate under the assumption that consumers/end-users will independently follow security and privacy best practices and recommendations on their own. However, this approach overlooks the reality that many consumers/end-users buying smart home IoT devices lack the technical expertise or awareness needed to effectively secure their IoT device or smart home system. Furthermore, many of the recommended safeguards are user-controlled, meaning that they must be properly configured and activated by the consumer/end-user. Without clear, accessible guidance and built-in support, these critical security and privacy features may remain misconfigured or unused, leaving smart home IoT devices vulnerable to potential threats.

User-controlled security and privacy features include settings such as passwords, pin numbers, multi-factor authentication, device permissions, and data backup options, which are directly managed by the consumer/end-user rather than smart home IoT manufacturers. These user-controlled features shift an essential portion of responsibility for protecting and safeguarding smart home IoT devices onto the consumer/end-user, granting them the full-autonomy to tailor device settings to their needs and tolerance for risk. Previous researchers (Ho, et al., 2016) (Fletcher & Malalasekera, 2016) concentrated research on developing secure IoT devices prior to mass production, along with best practices and guidelines for end-users. Yet, many consumers/end-users continue to struggle with keeping up to date with evolving device features and security settings. This highlights a noticeable gap between industry recommended security and

privacy best practices and what is realistically being done to protect smart home IoT devices on a day-to-day basis.

This research study uses a systems engineering-focused, mixed methods (qualitative and quantitative) approach to evaluate how effectively smart home IoT manufacturers guide consumers/end-users in understanding, implementing, and maintaining user-controlled security and privacy features. The methodology unfolds across four system engineering phases:

1. Requirements Analysis (Phase 1): An in-depth review of smart home IoT device manuals, online support pages, and supplementary resources to establish baseline security and privacy requirements, aligned with known industry best practices, standards, and recommendations.
2. Usability Testing (Phase 2): Understand the users' needs, preferences, and behaviors through structured surveys and proficiency test to gather data on how users interact with smart home IoT device manuals and security/privacy features. Verification confirmed that the IoT user manual covered all required security and privacy settings, while validation measured how effectively participants could follow the guidance in real-world scenarios.
3. Focus Group Technical Deep Dive (Phase 3): Conducted technical deep dive with a focus group to discuss data received and barriers they have experienced with applying user-controlled security and privacy features.
4. Recommendations and Future Implementations (Phase 4): Findings from the earlier phases were integrated to address identified gaps between industry recommend best practices and smart home IoT manufacture provided security guidance.

By using a systems engineering approach, this research study provides a holistic view of how user-controlled security and privacy features function in a smart home IoT environment and identifies areas needing improvement. Findings from this research are intended to guide both smart home IoT manufacturers and consumers/end-users toward strategies that would enhance the overall security and privacy landscape in the smart home environment.

1.1 Background

IoT technologies continue to enhance consumer efficiency and functionality through the interconnected design of a smart home, however this comes with significant security and privacy risk that must be controlled. A 2015 study conducted by Hewlett-Packard (HP) discovered 70% of the IoT devices commonly used, primarily within consumers' households, have an average of 25 vulnerabilities per device: according to the study, "80% of devices failed to require passwords of sufficient complexity and length, 70% did not encrypt local and remote traffic communications, and 60% contained vulnerable user interfaces and/or vulnerable firmware" (Rawlinson, 2015). Many consumers/end-users are not taking the recommend precautions and steps needed to secure their smart home IoT devices.

One of the major reasons why consumers are failing to apply user-controlled security and privacy features like they should is the lack of guidance provide in IoT setup/configuration material. Consumers/users may find it challenging to comprehend security settings, don't understand the risk at hand, and just focus on getting the device working, leaving the vulnerabilities exposed. Additionally, IoT manufactures might be prioritizing ease of use and rapid deployment, vs setting a delivering an IoT device with robust security measures built in. Smart home IoT manufacturers have a huge incentive to be first in releasing their products to the market ahead of other competitors. Being the first to market with a new IoT product could give a new startup

technology company a competitive advantage and potentially establish the company as a major player in the industry. The accelerated pace of technological advancement and the fiercely competitive landscape mean that being first to market can significantly influence a product's success or failure (Evans, 2012). This urgency is causing a major shift in the smart home IoT market, where speed often takes precedence over thoroughness in product development, user testing, and cybersecurity. Historically, IoT manufacturers have invested a substantial amount of time and resources into extensive testing phases, including rigorous security assessments and user trials, before releasing devices to the public (Rose, 2015). Devices are frequently released with minimal testing, under the assumption that any security vulnerabilities or bugs can be addressed post-launch through software updates (Sicari, 2015). This practice, although convenient for IoT manufactures, ends up shifting the burden of cybersecurity and privacy to the user. User-controlled security features are usually built into IoT device setting, this would include things like such as customizable passwords, privacy settings, and authentication protocols, but provide limited guidance on how to configure them effectively (Emami-Naeini, 2019). Consumers/end-users that lack a certain level of technical expertise or cybersecurity knowledge are left responsible for securing their devices against increasingly sophisticated cyber threats (Zeng, 2017).

Studies have shown that consumers may not fully understand the risks or lack the knowledge to implement necessary security measures (Redmiles, 2016). The complexity of security configurations, combined with inadequate documentation, exacerbates this issue, leaving many devices vulnerable to exploitation (Feng, 2019). For example, the widespread use of default passwords and failure to apply security updates are common issues that can lead to significant security breaches (Das, 2018). Cybersecurity training courses through various avenues have constantly expressed the importance of changing default usernames and passwords, yet this issue

continues to be an issue. Default passwords are often easily guessable and widely known, as manufacturers tend to use simple, generic credentials like "admin" or "password" to simplify initial setup (Sicari, 2015). When consumers/end-users do not change default credentials on their device, that device remains vulnerability until corrective action is taken. One of the most famous examples of a default password vulnerability being utilized in an attack is the Mirai botnet attack in 2016. This Mirai attack used default passwords to infiltrate thousands of IoT devices, orchestrating a massive, distributed denial-of-service (DDoS) attack that disrupted major internet services (Josiah White, 2024).

Another simple user-controlled security feature that is often ignored, but could have severe consequences if not addressed, is firmware and software security updates. Failure to apply security updates leaves devices exposed to known vulnerabilities that manufacturers have already addressed in newer firmware versions (Fernandes, 2016). Many people will admit that they have ignored or delayed firmware and security updates, this is mainly due to inconvenience or a lack of understanding of their importance. Consumers need to actively manage their device settings and manufacturers need to support the consumers and emphasize the importance of changing default credentials and maintaining up-to-date software (Weber, 2010).

There is a critical need to examine the level of support and guidance provided by smart home IoT manufacturers to empower users in comprehending and implementing user-controlled cybersecurity and privacy features. This research study will use systems engineering methods to explore these issues comprehensively, aiming to provide actionable insights and recommendations that can bridge the divide between smart home IoT manufacturers and consumers.

1.2 Problem Statement

The problem evaluated in this research study is the varying degrees of support that consumers receive from smart home IoT manufacturers, specifically pertaining to the comprehension and implementation of user-controlled cybersecurity and privacy measures. While smart home IoT devices offer great deal of benefits to the consumer, IoT devices can also introduce significant security and privacy risk if not properly configured and maintained. Smart home IoT consumers expect manufacturers to provide clear, comprehensive, and accessible guidance to help them operate and use their devices in a private and secure manner. However, a gap exists in the quality, comprehensiveness, and availability of guidance to assist consumers/users will applying user-controlled security and privacy features.

This gap is demonstrated in several areas of smart home IoT security. The clarity of security guidance found within a smart home IoT instruction manual varies by manufacture, often containing technical jargon, ambiguous language, or insufficient detail, making it challenging for the average consumer to understand how to implement essential security settings (Redmiles, 2016). Similarly, the comprehensiveness and clarity of security guidance varies by manufactures. Many smart home IoT manufacturers ship products that include setup guides and/or instruction manuals that primarily focus on basic functionality and device setup, but neglect to include detailed and usable information on security features and privacy controls. The accessibility of additional support outside of what documentation comes with the device packaging or online support also presents challenges. Some users may find it difficult to access assistance when they encounter issues or have questions specific to their use case. Limited “live person” customer support availability, unresponsive help channels, and a lack of multilingual resources also contribute to this problem. Furthermore, support material that are provided by IoT manufactures may not be

optimized for accessibility, failing to consider users with disabilities or used at different levels of technological expertise.

The consequences of this gap are widespread. Consumers/end-users who do not effectively configure and maintain security and privacy settings are more susceptible to things like: unauthorized access, data breaches, invasions of privacy, and many more. Additionally, vulnerable devices can be exploited by malicious actors to gain access to personal information, monitor user home activities, or even launch attacks on other networks (e.g. Mirai botnet attack in 2016). This gap also hinders consumer/user comprehension so they can utilize the full potential of the user-controlled security and privacy features available to them on smart home IoT devices. User-controlled security and privacy features are designed to allow users to take an active role in protecting their devices and personal data through adjusting and customizing settings to their individual personal use case. However, when users do not understand or are unable to access the user-controlled features due to inadequate support, they miss the opportunity to secure their devices leaving their Home Area Networks (HAN) vulnerable.

The problem statement highlights a critical gap that should be evaluated to determine what type of support are users receiving from smart home IoT manufacturers to help them secure their devices through user-controlled security and privacy features. Addressing this gap will contribute to the cybersecurity body of knowledge in providing better support mechanisms and tools to increase the use of security and privacy recommendations and best practices. This research study anticipates uncovering several core themes—ranging from the clarity of smart home IoT manufacture provided instructions to the complexity of password management—that influence how effectively consumers/end-users configure smart home IoT security and privacy features.

1.3 Research Questions

This research study is based on the following hypothesis:

- Hypothesis: Consumers who receive clear and comprehensive security guidance from manufacturers through device manuals will utilize a greater number of user-controlled security features compared to those who receive minimal or ambiguous guidance.

To explore this hypothesis, this research study addresses two primary research questions (RQ):

- RQ1 – To what extent does the clarity and comprehensiveness of security guidance provided by smart home IoT manufacturers influence the consumers understanding and utilization of user-controlled security and privacy features?

Research Question 1 aims to assess the direct impact the quality of security guidance on consumers' engagement with and application of security and privacy features. By evaluating the different levels of guidance, clarity, and comprehensiveness, this research study seeks to determine whether security and privacy guidance embedded into smart home IoT instruction manuals, and other manufacture provided support material, can significantly enhance the adoption rate of security measures among users.

- RQ2 – What barriers do consumers face in implementing user-controlled security and privacy features, and how can clear and comprehensive guidance address these barriers?

Research Question 2 acknowledges that consumers currently have and will continue to encounter various difficulties when attempting to user-controlled security and privacy settings on their smart home IoT devices. These difficulties can include things like lack of technical expertise, not fully understanding technical jargon, time constraints, understanding and/or comprehending the importance of security features, etc. By identifying and analyzing these challenges, this

research study aims to uncover specific areas where consumers struggle and study how/if enhanced guidance can help overcome some of these obstacles.

1.4 Conceptual Framework

The conceptual framework adopted for this research study is built on systems engineering principles and practices to construct a methodology to analyze the interactions between smart home IoT devices and human factors. Systems Engineering is a transdisciplinary and integrative approach that enables the successful comprehension, use, and retirement of engineered systems, smart homes for example, by applying systems principles, concepts, and scientific, technological, and management methods (INCOSE, 2024). The Systems Engineering discipline focuses on balancing and integrating stakeholders' goals and requirements throughout the system's lifecycle, from conception to disposal, by considering technical and consumer needs (Kossiakoff, 2020). In the context of smart home IoT networks and systems, Systems Engineering is used to assists in delivering smart home IoT solutions that meet consumer/user needs while maintaining user-focused designs focused on security and privacy.

This research is conducted in two key phases: Phase 1 evaluates the clarity and comprehensiveness of smart home IoT device documentation, while Phase 2 examines user interaction through usability tests and focus groups. To establish a baseline understanding of how consumers/users configure user-controlled security and privacy features, the research study begins with a systems focused requirements analysis. In this initial step, industry and government recommended best practices are identified by benchmarking against established frameworks and IoT security guidelines from organizations such as the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), National Security

Agency (NSA), Consumer Technology Association (CTA), Open Worldwide Application Security Project (OWASP), and Industry IoT Consortium (IIC).

The design phase of this research study incorporates the previously identified baseline requirements into user-focused security and privacy guidance. Next, in the implementation phase, the guidance is used in a controlled setting: participants are given a customized smart home IoT device manual, built from the baseline requirements, and are evaluated on their ability to recognize and configure user-controlled security and privacy best practices. Continuing to use systems engineering principles, the research study employes verification and validation process to evaluate the effectiveness of the security and privacy guidance created. Verification would ensure that the security guidance meets all specified requirements derived from best practices, while validation would assess whether users can successfully use the guidance to configure their devices correctly (Kossiakoff, 2020). Research data is then gathered through usability testing, structured surveys, observation, and focus group feedback, capturing both quantitative performance metrics and qualitative insights. Through examining how clear and comprehensive the guidance is presented; the research study aims to assess any correlation between these factors and the participants' understanding or interpretation of the provided security and privacy instructions. Within this framework, we examine the entire smart home IoT device lifecycle—from initial configuration to ongoing security updates—and incorporate user feedback loops to ensure that both technical solutions and consumer behaviors are fully considered (INCOSE, 2024).

1.5 Terms and Definitions

The following terms and definitions are cybersecurity, privacy, and systems engineering words used in this research study are below in Table 1.

Terms	Definition
Access Control	A method that restricts access to IoT devices and networks, allowing only authorized users to interact with the system.
Cloud Security	The set of policies, controls, and technologies used to protect data, applications, and infrastructure hosted on cloud-based platforms.
Cybersecurity	The practice of protecting systems, networks, and devices from digital attacks, theft, or damage.
Data Privacy	The right of individuals to control the collection, usage, and sharing of their personal information.
Data Sharing	The transmission of personal information collected by IoT devices to third-party services or companies.
Default Password	A pre-configured password set by the manufacturer on IoT devices, often weak and should be changed by the user immediately after installation.
Default Settings	The pre-configured options or features of an IoT device that are often less secure and should be modified by users.
Denial-of-Service (DoS) Attack	An attack intended to make a device or network unavailable by overwhelming it with a flood of traffic or requests.
Device Permissions	The specific permissions users grant IoT devices to access data, networks, or features, such as camera and microphone access.
Device Vulnerabilities	Weaknesses or flaws in an IoT device that can be exploited by attackers to gain unauthorized access or control.
Documentation Review	A process in systems engineering where existing system documentation is examined to ensure completeness, accuracy, and relevance to the current system design.
Encryption	The process of converting data into a code to prevent unauthorized access, used to secure communications and data stored by IoT devices.
Firmware	Permanent software programmed into a device's read-only memory, essential for controlling hardware functions and ensuring device security.
Firmware Update	The process of updating a device's firmware to enhance performance or patch security vulnerabilities.
Firewall	A network security device that monitors and controls incoming and outgoing traffic based on predetermined security rules.
Multi-Factor Authentication (MFA)	A security feature requiring two or more verification methods, such as passwords and biometrics, to enhance the security of IoT devices.
Network Segmentation	Dividing a computer network into smaller, isolated segments to reduce the potential impact of a cyberattack on IoT devices.
Personal Data	Any information that relates to an identifiable individual, such as names, addresses, or location data, collected by IoT devices.

Terms	Definition
Privacy Settings	Options within IoT devices that allow users to manage what personal information is collected, stored, and shared with third parties.
Remote Wipe	A feature that allows users to erase all data on an IoT device remotely in case it is lost or stolen.
Requirements Analysis	A key process in systems engineering that involves determining the functional and technical requirements for developing a system, including IoT security needs.
Risk Assessment	The process of identifying, evaluating, and estimating the risks to a system, especially the threats posed by IoT device vulnerabilities.
Security Best Practices	The recommended actions and guidelines that users and manufacturers should follow to ensure the security and privacy of IoT devices.
Security Configuration	The process of adjusting settings to ensure that IoT devices meet security requirements and protect against unauthorized access.
Security Patch	A software update released by manufacturers to fix known vulnerabilities in IoT devices.
Smart Device	Any internet-connected device, such as a thermostat or security camera, that can be controlled remotely and integrated into a smart home ecosystem.
Smart Home Hub	A central device that connects and controls various IoT devices in a smart home, often used to automate tasks and enhance security.
System Architecture	The conceptual model that defines the structure, behavior, and more views of a system, including the security features in an IoT system.
System Design	The process of defining the system's components, modules, and interfaces, particularly focusing on how user-controlled security features can be integrated.
System Integration	The process of bringing together different subsystems and components into a whole system, such as integrating different smart home IoT devices securely.
Systems Engineering	An interdisciplinary approach to designing and managing complex systems over their life cycles, including IoT device security and privacy measures.
Two-Factor Authentication (2FA)	A method of enhancing security by requiring two types of credentials to verify user identity, such as a password and a phone-based confirmation code.
Unauthorized Access	The act of gaining access to an IoT device or network without permission, often with malicious intent.
Usability Testing	A method in systems engineering for testing how easily users can understand and apply IoT security and privacy features.
User Interface (UI)	The means by which users interact with an IoT device, typically involving buttons, touchscreens, or mobile apps.
Verification	The process evaluating an IoT system to answer the question, "Did we build the system right?"
Validation	The process of determining whether an IoT system meets the needs of the user and functions as intended.
Virtual Private Network (VPN)	A service that encrypts internet traffic, allowing users to securely connect to their IoT devices remotely.

Terms	Definition
Vulnerability	A weakness in a system that can be exploited by an attacker to gain unauthorized access or cause harm.
Wi-Fi Protected Access (WPA)	A security protocol used to protect Wi-Fi networks, including IoT devices, through encryption and authentication mechanisms.

Table 1. Common Smart Home IoT Cybersecurity and Systems Engineering Terms

1.6 Scope, Limitation, and Delimitations

The scope of this research study was limited to smart home IoT devices; however, this is not intended to represent the sole method for mitigating security and privacy risks. This research study was designed to develop guiding practices for smart home IoT manufactures and consumers to understand and mitigate security and privacy risks by addressing the guidance and support given to consumers/users in the application of user-controlled features.

This research study was delimited to focus solely on smart home IoT devices, specifically those devices that are commonly used in residential setting, such as thermostats, home security systems, smart lighting, televisions, and baby monitors. IoT devices in other domains, such as personal IoT technologies (e.g., wearables, health and wellness products), were deliberately excluded from the study. Additionally, larger IoT devices like those related to the smart cities, smart grid, smart meters, renewable energy, electric vehicles, and energy usage tracking systems, were not considered within the scope of this research study. This delimitation was intended to maintain a focused investigation on devices with direct relevance to residential smart home IoT cybersecurity and privacy practices.

Several limitations also impacted the research study. First, the selection of smart home IoT devices was restricted to those available on the market and the time of the study. It is understood that this limitation may have excluded newer or emerging technologies that could present different security and privacy challenges. Additionally, this research study primarily evaluated user interactions with smart home IoT device documentation, not real-time system performance. The

research study was further limited by its focus on user-controlled security and privacy features, excluding other security measures, such as those embedded at the network level or controlled by manufacturers. While user experience was analyzed through structured surveys and focus groups, the sample size and demographic diversity were limited, potentially influencing the representatives of the findings across different user groups.

1.7 Chapter Summary

Chapter 1 presented the central problem statement, hypothesis to be tested, research questions, conceptual methodology, and systems engineering framework to be used in the research study. Additionally, this chapter outlines systems engineering research approach to analyze how effectively consumers/end-users are guided in applying user-controlled security and privacy features. This chapter also defined key Systems Engineering, Cyber Security, and Smart home IoT terms that were used throughout the study.

Chapter two presents a literature review on the topic of IoT, Smart homes, and Systems Engineering that is relevant to this research including: Title Searches, Articles, Documents, and Journals Researched, IoT Definition, IoT Evolution, IoT Architecture, Smart homes, Future of Smart homes, Smart home IoT Security Recommendations, User-controlled Security and Privacy Features for Smart homes, Smart home IoT Laws and Regulations, Systems Engineering and IoT Security, and Gaps In The Literature.

CHAPTER 2. LITERATURE REVIEW

A literature review is conducted to inform and focus the research by exploring what has, and what has not been done to contribute to the system engineering and cybersecurity body of knowledge. The literature review presented in this chapter identified and evaluated existing studies in the systems engineering and cybersecurity field of study related to IoT smart home consumer cybersecurity, privacy, and awareness. This chapter begins with a background of IoT and its evolution to create what is known as the "smart home". The sections thereafter will explore IoT Architecture, risks and vulnerabilities, laws and regulations, and systems engineering. The different types of smart home technology are discussed as well, along with some of the common vulnerabilities and strategies that can be adopted to resolve them. The chapter will close with a summary of the key points.

2.1 Title Search, Articles, Documents, and Journals Researched

This literature review included an extensive search of peer-reviewed literature, and other resources such as books, conference papers, reports, news stories, grey literature (i.e. technical reports), and websites that clearly addressed smart home IoT technology, consumer IoT security behaviors, associated risks, and systems engineering methods. The researcher queried several online scholarly library databases such as ProQuest, IEEE Xplore, ACM Digital Library, Springer Link, Google Scholar, INCOSE and other available resources through the Colorado State University library. The researcher employed searches leveraging keywords and phrases and derivatives of such to collect the greatest ensemble of literature available. The keywords and phrases used by the researcher to conduct an exhaustive search of literature included Internet of Things (IoT), consumer IoT, cybersecurity, smart home technology, IoT consumer behavior, IoT device user manuals, IoT best practices, cyber-crime prevention, security education and training,

user-centric design, privacy setting in IoT, systems engineering approaches, security systems engineering, and systems engineering methodology. IoT manufactures and device types were compiled from product manufactures websites, and major IoT publications, magazines, and newsletters. The researchers searched were limited to the past ten years to facilitate the retrieval of recent and relevant literature. References that are later than 2014 are used to give historical or theoretical bases for the research.

2.2 IoT Definition

Gartner defines the Internet of Things as a "network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" (Gartner, 2022). The U.S. government defines IoT as "the concept of connecting and interacting through a network with a broad array of "smart" devices, such as fitness trackers, cameras, door locks, thermostats, vehicles, or jet engines" (GAO, 2017) and offers three categories of IoT: industry, consumer, and public sector. According to the Institute of Electrical and Electronics Engineers (IEEE), the

> "Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited using intelligent

interfaces and is made available anywhere, anytime, and for anything taking security into consideration (IEEE, 2015)."

The many definitions of the IoT share a common trait, they all connect previously non-networked physical standalone device to one another via network protocol. For the purposes of this research, the term "IoT smart home devices" excludes computers, laptops, and tablets. Furthermore, industry-controlled systems are also outside of the scope of this study. Industrial control systems are controlled within the context of corporate or utility and therefore should have the organizational support that home IoT users lack (Mitchell, 2020).

2.3 IoT Evolution

The phrase "Internet of Things" was first used by Kevin Ashton, executive director of the AutoID Centre - MIT, during a presentation discussing the possibilities of linking RFID (Radio-frequency identification) to the internet (Ashton, 2009). At the time in 1999, he was trying to convey that all data on the internet was first captured and created by humans. If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing, or recalling, and whether they were fresh or past their best (Ashton, 2009).

Since then, Internet of things have evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems. Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of Things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", covering devices and appliances (such as lighting fixtures,

thermostats, home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers (Engineers, 2019).

One of the first smart home devices was created by Westinghouse Electric engineer Jim Sutherland in the mid 1960s. Jim created the Electronic Computing Home Operator (ECHO 4), which was used to control appliances and temperature in the home (Cortesi, 2022). In the mid 1970s, Pico Electronics created a protocol named X10 for communications around electronic devices used for home automation, sometimes referred to as Domotics. The dominant approach was to automate regulation of Heating, Ventilation and Air Conditioning (HVAC) equipment, control of energy consuming appliances such as water heaters, control of lighting, and automatic control of shutters and awnings (Cortesi, 2022). In 1989, X10 introduced the first low-cost self-installed wireless security system. Then came the Voice Dialer security system, the Monitored security system, as well as Personal Assistance versions. In 1995, X10 set up its own monitoring station called Orca Monitoring Services in Seattle, Washington. Today, it monitors security systems developed and manufactured by X10 for Radio Shack, Phillips Consumer Electronics, (Magnavox) and the X10 Powerhouse brand. In the 1990s, the consumer mix of Smart home devices mix fell into two categories, the ultra-high-end, with systems of $100,000 and up, and the mass market, with systems of $2,000 and $35,000 (Edward B. Driscoll, n.d.). In the early 2000s many of the available Smart home devices were mainly used by the wealthy and tech geeks but, as devices became more affordable, many of today's consumers began to adopt a digital lifestyle to secure their homes, control energy consumption, and reduce time to complete routine household' tasks (Jose, 2015). In the early 2000s, wireless technologies such as Radio Frequency Identification (RFID), Bluetooth, Wi-fi, Zigbee, Z-wave and others unlocked previously

impossible smart home capabilities. These new technologies began an influx of IoT devices to the market with a proliferation of competing standards and even more proprietary, incompatible systems. (Seitz, n.d.) This is perhaps not surprising as there used to be very little economic incentive for manufacturers to address security vulnerabilities. Over the years we have continued to see examples of what insecure IoT devices can do. Figure 1 shows the IoT evolutions over the years.

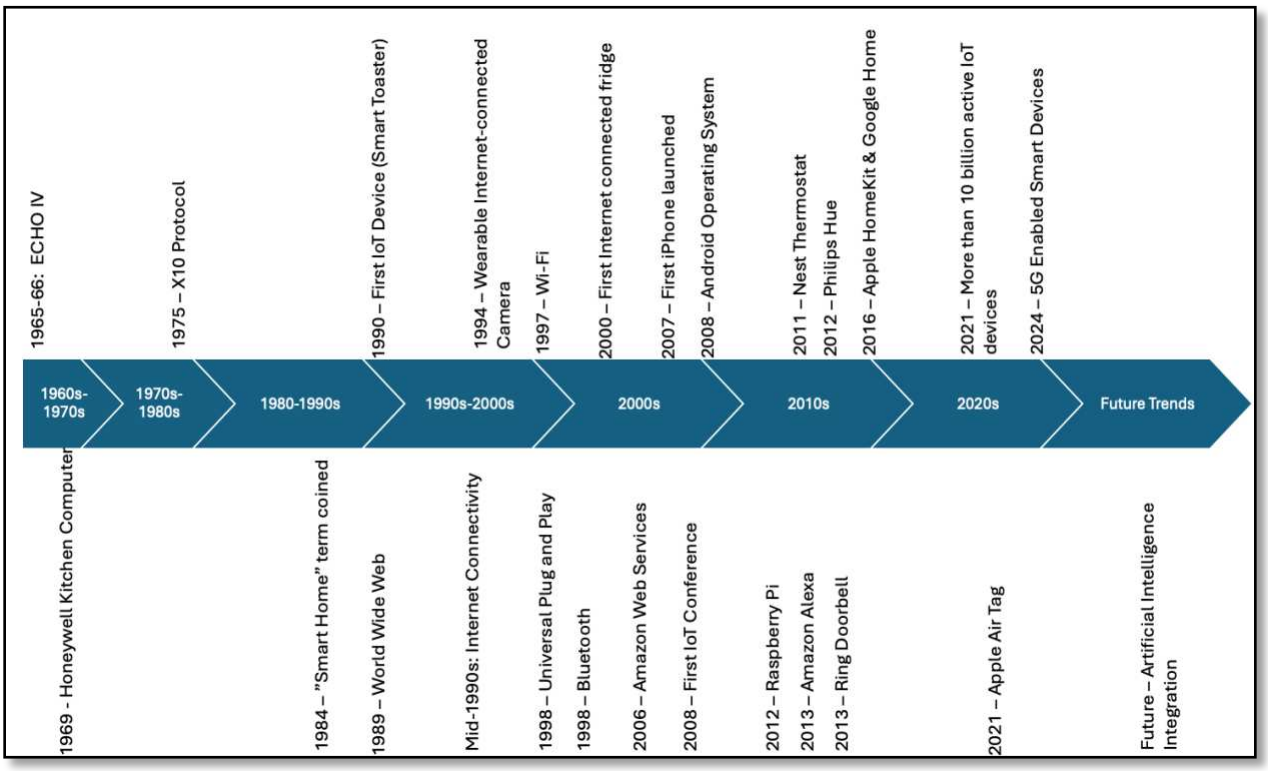


Figure 1. Smart Home IoT Evolution

Radio Frequency Identification (RFID)

RFID is a technology that uses radio frequencies to transmit data (P. Suresh, 2014). The first patent for an RFID system was filed in 1973 by Mario Cardullo, an engineer at IBM. The technology was initially used for security purposes, such as identifying whether a person was

authorized to enter a restricted area. Over the years, RFID technology has become increasingly sophisticated, with the ability to store and transmit large amounts of data.

RFID technology consists of two main components: a reader and a tag. The reader emits a radio frequency signal, which is received by the tag. The tag then responds with a unique identifier or other information, which is transmitted back to the reader. The communication between the reader and tag can occur over short or long distances, depending on the frequency of the radio waves and the strength of the signal. The tags contain transponders that emit messages readable by specialized RFID readers. Most RFID tags store some sort of identification number; for example, a customer number or product SKU (stock-keeping unit) code. A reader retrieves information about the ID number from a database, and acts upon it accordingly. RFID tags can also contain writable memory, which can store information for transfer to various RFID readers in different locations. This information can track the movement of the tagged item, making that information available to each reader (Weinstein, 2005). RFID tags fall under two categories:

- Active tags – Has an internal power supply. The on-board power capability makes these types of tags larger and more expensive, catering to larger devices that require tracking over long distances. Active tags operate at higher frequencies; commonly 455 MHz, 2.45 GHz, or 5.8 GHz.
- Passive tags – No internal power supply; This makes these types of tags very inexpensive. Passive tags typically operate at frequencies of 128 kHz, 13.6 MHz, 915 MHz, or 2.45 GHz, and have read ranges of a few inches to 30 feet.

RFID technology has a wide range of applications across many different industries. Some of the most common applications of RFID include:

1. Inventory Management - RFID tags can be attached to products or containers to track inventory in real-time, making it easier for businesses to manage their supply chain and reduce stockouts.
2. Retail - RFID tags can be used to track products throughout the supply chain, from the manufacturer to the store shelves, reducing the risk of lost or stolen merchandise.
3. Healthcare - RFID technology is used to track medical equipment, patient records, and medication, improving the efficiency and accuracy of healthcare operations.
4. Transportation - RFID tags can be used to track vehicles and containers, improving logistics and supply chain management.
5. Livestock and Agriculture - RFID tags can be used to track and manage livestock and crops, improving productivity and reducing waste.

Bluetooth

Bluetooth technology was developed in the late 1990s by Ericsson, a Swedish telecommunications company, as a wireless alternative to serial cables for communicating between devices. The name "Bluetooth" was inspired by Harald Bluetooth, a Danish king who united warring factions in Denmark and Norway in the 10th century. The name was chosen to reflect the goal of the technology: to unite different devices and platforms into a single, wireless network.

The first Bluetooth specification was released in 1999, and the first Bluetooth-enabled devices hit the market in 2001. Since then, Bluetooth has undergone several updates and improvements, with the latest version, Bluetooth 5.2, released in 2020. Bluetooth technology uses minimal power to exchange data among devices over an approximate 10 meters (33ft) range. It employs UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz (Muller, 2002). Many devices utilizing Bluetooth technology today are the development of “Bluetooth low energy

(BLE)" and "Bluetooth smart" technology. Many IT professionals would say that IoT is a reality today because of advancements of Bluetooth technologies. Ever since its inception in 1998, Bluetooth has seen tremendous advancements in terms of technology.

Bluetooth technology has a wide range of applications, from consumer electronics to industrial automation. Some of the most common applications of Bluetooth include:

1. Wireless Audio - Bluetooth technology powers wireless headphones, speakers, and soundbars, allowing users to stream audio from their devices without the need for cables or wires.
2. Home Automation - Bluetooth technology is used in smart home devices, such as light bulbs, thermostats, and security systems, allowing users to control their homes from their smartphones or other devices.
3. Automotive - Bluetooth technology is used in car audio systems and hands-free calling systems, allowing drivers to make phone calls and stream music without taking their hands off the wheel.
4. Healthcare - Bluetooth technology is used in medical devices, such as blood glucose monitors and heart rate monitors, allowing patients to track their health data and share it with their healthcare providers.

Wi-Fi (Wireless Fidelity)

Wi-Fi is a technology that allows wireless networking and data transfer between devices. Wi-Fi uses radio waves to transmit data over short distances, typically within a few hundred feet. It is commonly used in homes, offices, public places, and other settings to provide internet access to multiple devices. Some of the key technologies and standards associated with Wi-Fi include:

- IEEE 802.11: The standard that governs the technical aspects of Wi-Fi, including the frequencies, transmission speeds, and other specifications.
- Wi-Fi Alliance: An industry consortium that promotes Wi-Fi technology and certifies devices as being compatible with Wi-Fi standards.
- Wi-Fi Protected Access (WPA), WPA2, and WPA3: Security protocols that encrypt Wi-Fi transmissions to prevent unauthorized access.
- Multiple Input Multiple Output (MIMO): A technology that uses multiple antennas to improve the speed and reliability of Wi-Fi connections.

Several implementations of the IEEE 802.11 standard have been defined by IEEE since its creation in 1997 (see Table 2). All the standards use the Ethernet protocol and the CSMA/CA access method.

Standard	Frequency	Maximum Speed	Backwards compatibility
802.11	2.5 GHz	2 Mbps	-
802.11a	5 GHz	54 Mbps	-
802.11b	2.4 GHz	11 Mbps	-
802.11g	2.4 GHz	54 Mbps	802.11b
802.11n	2.4 and 5 GHz	600 Mbps	802.11a/b/g
802.11ac	5 GHz	1300 Mbps	802.11a/n
802.11ad	2.4 GHz, 5 GHz and 60 GHz	7 Gbps	802.11a/b/g/n/ac

Table 2. IEEE 802.11 Standards

Wi-Fi technology has a wide range of applications across various industries and settings. Some of the most common applications of Wi-Fi include:

1. Internet connectivity: One of the most common uses of Wi-Fi technology is to provide internet access to devices such as smartphones, laptops, and tablets. Wi-Fi allows users to connect to the internet wirelessly from almost anywhere within range of a Wi-Fi network.
2. Home networking: Wi-Fi can also be used to create a home network that allows devices to communicate with each other and share resources such as printers and files.

3. Public hotspots: Many public places such as airports, cafes, and libraries provide Wi-Fi hotspots that allow users to access the internet wirelessly.
4. Education: Wi-Fi is commonly used in educational settings to provide internet access to students and teachers, as well as to enable online learning platforms and educational resources.
5. Healthcare: Wi-Fi is increasingly being used in healthcare settings to enable electronic health records, telemedicine, and other health-related applications.
6. Manufacturing and logistics: Wi-Fi technology can be used in manufacturing and logistics to track inventory, monitor production processes, and automate various tasks.
7. Retail: Wi-Fi can be used in retail settings to enable mobile point-of-sale systems, track inventory, and provide personalized customer experiences.
8. Hospitality: Wi-Fi is a key amenity in the hospitality industry, with hotels and resorts providing Wi-Fi access to guests.
9. Smart homes and cities: Wi-Fi is a critical technology for smart homes and cities, enabling connected devices to communicate with each other and with the internet to provide a range of services and applications.

ZigBee

Zigbee is a low-power wireless communication protocol designed for devices that need to communicate with each other in close proximity. It operates on the IEEE 802.15.4 standard and uses the 2.4 GHz, 900MHz and 868MHz frequency bands. Zigbee is often used in home automation and Internet of Things (IoT) applications where devices need to communicate wirelessly with each other. Zigbee networks use a mesh topology, which means that devices can

communicate with each other directly if they are in range, or indirectly by relaying messages through other devices in the network. This allows for greater flexibility and resilience in the network, as devices can continue to communicate even if some devices fail or are out of range.

Zigbee coordinator is responsible for creating and maintaining the network. Each electronic device (i.e. Washing Machine, Television, Lamp etc.) in the system is a Zigbee device managed by the coordinator. All communication between devices propagates through the coordinator to the destination device. The ZigBee standard provides 250kbps data rate, and as 40kbps can meet the requirements of most control systems, it is sufficient for controlling most home automation devices. The low installation and running cost offered by ZigBee helps tackle the expensive and complex architecture problems with existing home automation systems (Khusvinder Gill, 2009). One of the major contrasting features about ZigBee is that it's cheaper than Bluetooth and Wi-Fi. This boosts the feasibility of its deployment for IoT applications. It uses AES 128-bit encryption for security. This reliable an128-bithealing attributes of ZigBee is added merit to the IoT stream. Due to its immense qualities many commercial home automation products use ZigBee technology.

Some common applications of ZigBee include:

1. Smart home automation: ZigBee can be used to connect and control various smart devices, including lighting, heating and cooling systems, smart plugs, security systems, and more. ZigBee provides reliable and low-power communication between devices, making it a popular choice for smart home automation.
2. Industrial automation: ZigBee is used in industrial automation applications for machine-to-machine (M2M) communication, monitoring and control systems, and remote sensing.

It is commonly used in building automation systems, HVAC systems, and lighting control systems in commercial buildings.

3. Healthcare monitoring: ZigBee is used in wireless healthcare monitoring systems to collect and transmit data from medical devices, such as blood glucose meters, blood pressure monitors, and pulse oximeters. It can also be used in home healthcare monitoring applications, such as tracking the activity levels of elderly or disabled people.
4. Asset tracking: ZigBee is used in asset tracking applications, such as tracking the location of equipment, vehicles, and inventory in warehouses, factories, and other industrial settings.
5. Agriculture monitoring: ZigBee can be used to monitor and control environmental conditions in agriculture, such as temperature, humidity, and soil moisture levels. This can help improve crop yields and reduce water usage.
6. Smart city applications: ZigBee can be used to create smart city applications, such as intelligent street lighting, traffic management, waste management, and environmental monitoring.

Z-Wave

Z-Wave is a wireless communication protocol designed for home automation and IoT applications. It operates on the 900 MHz frequency band and uses a mesh network topology similar to Zigbee. Z-Wave is often used for devices that need to communicate wirelessly with each other in a home or building, such as smart thermostats, door locks, and lighting systems. Like Zigbee, Z-Wave uses a mesh network topology, which means that devices can communicate with each other directly or indirectly through other devices in the network. This provides greater flexibility and resilience in the network, as devices can continue to communicate even if some devices fail

or are out of range. One of the key advantages of Z-Wave is that it operates on a dedicated frequency band, which means that it is less susceptible to interference from other wireless devices. This can lead to more reliable and stable communication in the network. Some common applications of Z-Wave include:

1. Smart home lighting: Z-Wave can be used to control smart lights, allowing users to adjust brightness and color, set schedules, and create automated lighting scenes.
2. Home security: Z-Wave can be used to connect door and window sensors, motion detectors, and cameras, allowing users to monitor and secure their homes remotely.
3. Smart thermostats: Z-Wave can be used to connect smart thermostats, allowing users to adjust their heating and cooling settings remotely and create schedules to save energy.
4. Home entertainment: Z-Wave can be used to control home entertainment systems, including TVs, speakers, and streaming devices, allowing users to create personalized entertainment experiences.
5. Smart locks: Z-Wave can be used to control smart locks, allowing users to lock and unlock their doors remotely and create customized access codes for family members and guests.
6. Energy management: Z-Wave can be used to connect smart plugs and switches, allowing users to monitor and control their energy usage remotely.

Matter

An open-source interoperability standard called Matter (Dimitri Belli, 2024) was created in collaboration with some of the major smart home IoT manufactures including Apple, Amazon, Google, and Samsung SmartThings to increase compatibility between IoT devices. Matter is built using Internet Protocol version 6 (IPv6) and operates at the application layer of the OSI model to facilitate interoperability among smart home devices, mobile applications, and

associated cloud services. While Matter addressed interoperability issues when it comes to smart home IoT devices, it is not a “one size fits all” solution. Matter is not compatible with all smart home IoT devices, and the protocol must be adapted by the IoT manufacture. Additionally, older IoT devices or those with proprietary protocols will not work with Matter.

2.4 IoT Architecture

The IoT can be classified into three layers: 1- Perception layer, 2-Network Layer, and 3-Application Layer. These layers support IoT devices through data collection and processing and go beyond the traditional OSI model to include the transformation of data into useable information. This three-layer architecture is depicted in Figure 2.

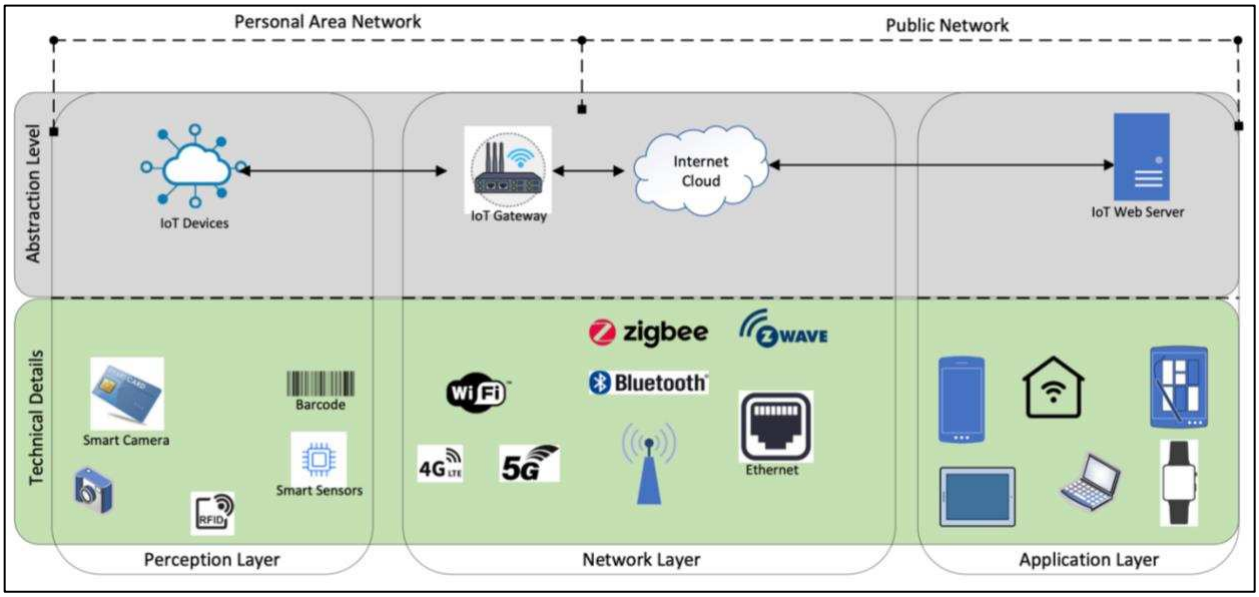


Figure 2. Generic architecture of an IoT system

2.4.1 Perception layer

The perception layer involves the collection of information. This layer is classified into two sections, namely, the perception node (sensors, controllers, and so on) and the perception network that interconnects the network layer (Yan, 2014). Data is acquired and controlled at the

perception node, while control instructions for sending and controlling data are carried out at the perception network layer. Perception layer technologies include all types of sensors, such as RFID, ZigBee, sensor nodes, and sensor gateways. This is where the data comes from. The data could be gathered from any number of sensors on the connected device. Actuators, which act on their environment, are also at this layer of the architecture.

Overall, there are three main security issues present at the perception layer. First is signal strength of wireless signals, many IoT devices use wireless technologies in the 2.4 GHz frequency band, whose efficiency can be compromised by disturbing waves. Second is sensor node tampering, IoT devices can installed/used anywhere and everywhere, putting hardware components at risk to tampering by attackers and owners. Lastly is the network topology, unlike traditional network architectures that remain mostly the same after configuration, IoT topologies can be very dynamic in nature. The perception layer mostly consists of RFIDs and sensors, which due to their small storage capacity, low power consumption, and little computational capability, make them very prone to attacks. Common security threats of the perception layer are:

- Eavesdropping: an unauthorized real-time attack where private communications, such as phone calls, text messages, fax transmissions or video conferences are intercepted by an attacker. It tries to steal information that is transmitted over a network. It takes advantage of unsecure transmission to access the information being sent and received. (Muhammad Burhan, 2018)
- Node Capture: It is one of the hazardous attacks faced in the perception layer of IoT. An attacker gains full control over a key node, such as a gateway node. It may leak all information including communication between sender and receiver, a key used to make

secure communication and information stored in memory (Bharathi, Tanguturi, Jayakumar, & Selvamani, 2012)

- Fake Node and Malicious: It is an attack in which an attacker adds a node to the system and inputs fake data. It aims to stop transmitting real information. A node added by an attacker consumes precious energy of real nodes and potentially control in order to destroy the network. (Muhammad Burhan, 2018)
- Replay Attack: It is also known as a play back attack. It is an attack in which an intruder eavesdrops on the conservation between sender and receiver and takes authentic information from the sender. An intruder sends the same authenticated information to the victim that had already been received in his communication by showing proof of his identity and authenticity. The message is in encrypted form, so the receiver may treat it as a correct request and take action desired by the intruder (Puthal, Nepal, Ranjan, & Chen, 2016).
- Timing Attack: It is usually used in devices that have weak computing capabilities. It enables an attacker to discover vulnerabilities and extract secrets maintained in the security of a system by observing how long it takes the system to respond to different queries, input or cryptographic algorithms (Muhammad Burhan, 2018).

2.4.2 Network layer

The network layer provides network transmission and information security and delivers pervasive access environment to the perception layer, that is, data transmission and storage awareness (Pongle, 2015). At this layer, cloud computing platforms, Internet gateways, switching, and routing devices etc. operate by using some of the very recent technologies such as WiFi, LTE, Bluetooth, 3G, Zigbee etc. (R. Mahmoud, 2015) The network gateways serve as the mediator

between different IoT nodes by aggregating, filtering, and transmitting data to and from different sensors (M. Leo, 2014).

The network layer of the IoT is at risk of attacks related to confidentiality and privacy. Some of these potential attacks include DoS attacks, traffic analysis, eavesdropping, and passive monitoring. These attacks have a high likelihood of occurrence because of the remote access mechanisms and data exchange of devices. Common security threats and problems to network layers are:

- Denial of Service (DoS) Attack: A DoS attack is an attack to prevent authentic users from accessing devices or other network resources. It is typically accomplished by flooding the targeted devices or network resources with redundant requests in an order to make it impossible or difficult for some or all authentic users to use them (Prabhakar, 2017).
- Main-in-The-Middle (MiTM) Attack: MiTM attack is an attack where the attacker secretly intercepts and alters the communication between sender and receiver who believe they are directly communicating with each other. Since an attacker controls the communication, he or she can change messages according to their needs. It causes a serious threat to online security because they give the attacker the facility to capture and manipulate information in real time (Conti, Dragoni, & Lesyk, 2016).
- Storage Attack: The information of users is stored on storage devices or the cloud. Both storage devices and cloud can be attacked by the attacker and user's information may be changed to incorrect details. The replication of information associated with the access of other information by different types of people provides more chances for attacks. (Muhammad Burhan, 2018).

- Exploit Attack: An exploit is any immoral or illegal attack in the form of software, chunks of data or a sequence of commands. It takes advantage of security vulnerabilities in an application, system or hardware. It usually comes with the aim of gaining control of the system and steals information stored on a network (Muhammad Burhan, 2018).

2.4.3 Application layer

The application layer is what the users see. This could be an application to control a device in a smart-home ecosystem, or a tablet showing the status of multiple devices which are part of a system. The application layer is the uppermost layer and is visible to the end-user. Applications, such as smart grid, smart city, healthcare system, and intelligent transportation protocols, constitute this layer (Yan, A survey on trust management for Internet of Things, 2014). An application layer protocol is distributed over multiple end systems, in which the application in one end system uses a protocol to exchange information packets with an application in another end system (Nolin, 2016). An application layer typically comprises a middleware, a machine-to-machine (M2M) communication protocol, cloud computing, and a service support platform (Khorov, Lyakhov, Krotov, & Guschin, 2015). If you have ever used an app to turn your lights on at home, you have used the application layer. Common security threats and problems of the application are:

- Cross Site Scripting: It is an injection attack. It enables an attacker to insert a client-side script, such as java script in a trusted site viewed by other users. By doing so, an attacker can completely change the contents of the application according to his needs and use original information in an illegal way (Gupta & Gupta, 2017).
- Malicious Code Attack: It is a code in any part of software intended to cause undesired effects and damage to the system. It is a type of threat that may not be blocked or controlled

by the use of anti-virus tools. It can either activate itself or be like a program requiring a user's attention to perform an action (Muhammad Burhan, 2018).

- Mass Data: Due to a large number of devices and a massive amount of data transmission between users, it has no ability to deal with mass data processing according to the requirements. As a result, it leads to network disturbance and data loss (Muhammad Burhan, 2018).

2.5 Smart Homes

A smart home is any residence that is equipped with a network of interconnected devices, systems, and subsystems that can be remotely monitored, controlled, and accessed over the internet. This integration of technology can enhance the living experience by automating tasks, increasing energy efficiency, improving security, and providing greater convenience (Babar, 2018). Smart homes offer many conveniences through automation, remote control, and voice command features that allow users to manage and control things like lighting, climate, and entertainment systems effortlessly. For example, some smart home devices such as Amazon Alexa and Google Assistant allow consumers/end-users to control home functions by using simple voice commands, making everyday tasks more manageable and accessible (Zeng, 2017). Additionally, smart homes can enhance home security by integrating physical security measures like smart door locks and doorbells, which allow for real-time monitoring of entry points, while sensors detect leaks, smoke, and other hazards, providing safety reminders to prevent potential disasters (Roman, 2013). Energy efficiency is another significant benefit of smart homes technologies, this is achieved through devices like smart thermostats, which adjust heating and cooling based on occupancy and user preferences, thereby reducing energy consumption (Yang, 2017). Smart plugs

and outlets are another example of energy monitoring devices that help users identify and manage high-energy consumption devices.

Smart lighting systems, like the Phillips Hue®, allow users to control brightness, color, and scheduling, with options for integrating motion sensors for automated lighting based on occupancy. Entertainment systems, including smart TVs and speakers, offer seamless content streaming controlled via voice or mobile devices, enhancing the home entertainment experience (Patel, 2012). Smart appliances, like refrigerators and washing machines, offer advanced features such as inventory tracking, recipe suggestions, and remote control of laundry cycles (Choi, 2017).

One significant example of how smart home IoT technology can addresses a common problem is the use of a smart water monitors, like the Moen Flo ®, and shutoff devices to prevent water damage. Water damage affects over 40% of homes often resulting in costly repairs and even the loss of property entirely. Smart water monitors can continuously track the flow of water through the home's main water line and can detect small leaks before they become major problems. When a leak is detected, these devices alert the homeowner via text message, email, and/or phone call and, if necessary, automatically shut off the water supply, without any action from the user, to prevent extensive damage. By addressing issues promptly and effectively, smart water monitors and shutoff devices provide peace of mind and significant cost savings for homeowners (Nguyen, 2017).

There are a vast number of benefits to using consumer smart home IoT devices. However, due to the open nature of wireless communications, smart home platforms are facing many new challenges, especially in the aspect of security and privacy (Yan Meng, 2018). As consumers continue to purchase and/or regularly use IoT devices, manufacturers must address the vulnerabilities in their IoT devices and simplify security protocols to protect consumers (Guillet,

2017). Many of the vulnerabilities found in IoT could be mitigated through recognized security best practices. The UK government reported in 2018 that many severe cyber security issues stem from poor security design and bad practice in products sold to consumers (DCMS, 2018).

In 2015, Symantec published a study on 50 different smart home devices, demonstrating IoT devices were vulnerable to cybersecurity attacks (Barcena, 2015). The Symantec security researchers discovered none of the devices required strong login credentials or protected consumers against the most common threats and vulnerabilities (Barcena, 2015). Available data indicates IoT devices are plagued with vulnerabilities making them susceptible to exploitation (McGee, 2016) . To lower the attack surface and reduce the scope of vulnerabilities from the devices, consumers require a thorough understanding of the security flaws in smart home IoT devices malicious actors exploit using several different techniques and tools (McGee, 2016).

Smart homes represent the convergence of technology and daily living, offering enhanced convenience, security, energy efficiency, and safety. By integrating various smart home IoT components, consumers can create a personalized smart home environment that meets their specific requirements and preferences. As technology continues to advance, the capabilities of smart home systems will expand, providing even more innovative solutions to common household challenges.

2.6 Future of Smart Homes

The continuous advancement and growth of new technologies like artificial intelligence (AI), machine learning (ML), and satellite internet access have the potential to expand the capabilities of smart homes that we know of today. AI driven and assisted systems are expected to predict user preferences and behaviors, enabling homes to adapt dynamically to the needs of their inhabitants (Chen, 2020). The introduction of AI and machine learning in smart home IoT systems

have the potential to boost the adoption of smart home IoT devices in consumer residences through better personalization and the ability to learn and cater to individual consumer/user needs and/or requirements. Below are some potential advancements and innovations in smart home technologies:

1. Greater Integration with AI: As AI technology becomes more prevalent in our everyday lives, smart homes IoT devices will be able to use AI to better adapt to consumer/user needs and preferences more effectively. Currently, AI-assisted systems like Amazon Alexa can already control smart home IoT devices, but in the future, they may also be able to learn from a consumer/user's behavior and adjust settings/preferences accordingly.
2. Increased Privacy Protections: Many smart home IoT devices collect personal data, such as voice commands, health information, and location details. Machine learning has the potential to help to manage this data by recognizing user patterns and determine what data needs to be shared with external services and what data should remain private.
3. Increased Security Protections: Smart home IoT systems could benefit from more adaptive cybersecurity measures. Future smart home systems could potentially use AI, machine learning, and real-time user data to update security protocols as needed, respond to emerging threats, and patch vulnerabilities as they arise without requiring user intervention.
4. Enhanced connectivity and resilient home area networks: Smart home IoT systems/networks could benefit from satellite internet access by allowing the integration of multiple smart home IoT product no matter where the device resides. There are also potential benefits to reduce the dependency on wired or cellular networks.

As smart home IoT technology continues to grow, we can anticipate that our lives and personal data will become even more embedded into these systems leading to a need for even more

protections. Future smart home IoT systems and networks will need to incorporate more robust cybersecurity and privacy measures to protect personal data and ensure the integrity of smart home systems remains resilient. Although AI and machine learning have a lot of benefits to future smart home IoT advancements, these technologies also introduce a new security and privacy concerns regarding how much control users will continue to have over their data and how autonomous smart home systems will become. It will be essential that the right balance is struck between the convenience of automation and user control to prevent the potential unauthorized release or misuse of personal data. The continued development and adaptation of governance and regulatory standards will be necessary to ensure that machine learning and AI technologies are used ethically and responsibly.

2.7 Smart Home IoT Security Recommendations

Security researchers and governments worldwide use several different techniques to discover, report, and mitigate different vulnerabilities related to the IoT, many of which share commonalities. In March 2018, the United Kingdom government published a "Secure by Design" report that proposed a code of practice for Security in Consumer IoT Products and associated services (UK Department for Digital, 2018). The steps outlined in the Code of Practice (CoP) are not meant to be a "silver bullet", but a set of guidelines to support all parties involved in the development, manufacturing and retail consumer IoT to ensure products are secure by design and easier for consumers to stay connected and secure (DCMS, 2018). The Proposed Code of Practice for Security in Consumer IoT Products and Associated Services are as follows:

1. No default passwords – Best practices on passwords and other authentication methods should be followed (UK Department for Digital, 2018). For example: Many IoT devices are sold with universal default usernames and passwords. According to Cui and Stolfo

(2010), over 540,000 publicly accessible embedded devices configured with factory default root passwords. These devices range from enterprise equipment such as firewalls and routers to consumer appliances such as VoIP adapters, cable and IPTV boxes to office equipment such as network printers and video conferencing units.

2. Implement a vulnerability disclosure policy – IoT manufactures should set up a mechanism for users and operators of IoT devices to report vulnerabilities and disclose vulnerabilities (UK Department for Digital, 2018). According to Pil (2023), Vulnerabilities cannot be revealed unless they cause specific risks or the person who finds vulnerabilities discloses them. Therefore, it is reasonable to understand that most vulnerabilities have not been discovered yet.

3. Keep Software Updated – Software components in internet-connected devices should be securely updateable. Updates should be timely and should not impact on the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable (UK Department for Digital, 2018).

4. Securely Store Credentials and Security-Sensitive Data – Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable (UK Department for Digital, 2018).

5. Communicate Securely – Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage (UK Department for Digital, 2018).

6. Minimize Exposed Attack Surfaces - All devices and services should operate on the 'principle of least privilege'; unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used, and code should be minimized to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality (UK Department for Digital, 2018).

7. Ensure Software Integrity – Software on IoT devices should be verified using secure boot mechanisms. If an unauthorized change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function (UK Department for Digital, 2018).

8. Ensure that personal data are protected – Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law. Device manufacturers and IoT service providers must provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed based on consumers' consent, this must be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time. Consumers should also be provided with guidance on how to securely set up their device, as well as how they may eventually securely dispose of it (UK Department for Digital, 2018).

9. Make systems resilient to outages – Resilience should be built into IoT devices and services where required by their usage or by other relying systems, considering the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect (UK Department for Digital, 2018).

10. Monitor system telemetry data - If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies (UK Department for Digital, 2018).

11. Make it easy for consumers to delete personal data - Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data (UK Department for Digital, 2018).

12. Make installation and maintenance of devices easy - Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device (UK Department for Digital, 2018).

13. Validate input data - Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated (UK Department for Digital, 2018).

The Open Web Application Security Project (OWASP) started the OWASP Internet of Things Project in a way to help Developers, Manufacturers, Enterprises, and Consumers to make better decisions regarding the creation and use of IoT systems. This Project released the OWASP IoT Top 10 in 2018 (updated from 2014), which represents the top ten things to avoid when building, deploying, or managing IoT systems (OWASP, 2018). The OWASP IoT Top 10 2018 Mapping Project is a comprehensive initiative designed to identify and address the most critical security risks associated with Internet of Things (IoT) devices (OWASP, 2018). The project outlines the top 10 vulnerabilities in IoT ecosystems, including insecure default settings, poor data encryption, and insufficient privacy protections. These vulnerabilities are then mapped against best practices and standards to provide developers, manufacturers, and consumers with actionable guidance on securing IoT devices. The project's goal is to create a clear, structured framework for assessing IoT security, with a focus on mitigating risks associated with device configuration, data transfer, and user privacy. The project also emphasizes the importance of user education and documentation. A smart home IoT system bears more security risks than a traditional system: various vulnerabilities are inherited from the IoT and legacy system, and new vulnerabilities are generated in the special context that can be exploited by hackers (Sun, 2022). The OWASP Top 10 list as is follows:

1. Weak Guessable, or Hardcoded Passwords. Use of easily brute forced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems (OWASP, 2018).

2. Insecure Network Services. Unneeded or insecure network services running on the device itself, especially those exposed to the internet, which compromise the confidentiality,

integrity/authenticity, or availability of information or allow unauthorized remote control (OWASP, 2018).

3. Insecure Ecosystem Interfaces. Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering (OWASP, 2018).

4. Lack of Secure Update Mechanism. Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changed due to updates (OWASP, 2018).

5. Use of Insecure or Outdated Components. Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain (OWASP, 2018).

6. Insufficient Privacy Protection. User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission (OWASP, 2018).

7. Insecure Data Transfer and Storage. Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing (OWASP, 2018).

8. Lack of Device Management. Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities (OWASP, 2018).

9. Insecure Default Settings. Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations (OWASP, 2018).

10. Lack of Physical Hardening. Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device (OWASP, 2018). Physical security is essential to protect consumers and SHT devices from hackers attempting to harm, steal, tamper with, or damage consumers' devices, resources, or data (Li, 2016).

The National Security Agency (NSA) released the "Best Practices for Securing Your Home Network" Cybersecurity Information Sheet (CSI) in 2023 to help teleworkers protect their home networks from malicious cyber actors. The document outlines best practices for enhancing the security of home environments, offering recommendations on topics such as updating and patching devices, enabling strong password policies, securing home Wi-Fi networks, and implementing multi-factor authentication. Additionally, the CSI emphasizes the importance of regularly

reviewing and adjusting privacy and security settings on smart home devices. The NSA's guidance aims to empower users to better protect their personal data and devices from potential cyber threats by promoting cybersecurity awareness and the best practices for securing a home network. The NSA's best practices for securing a home network include:

- Upgrade to a modern operating system and keep it up-to date – The latest versions of operating systems include default security features that help prevent common attack vectors, making it harder for adversaries to gain privileged access. It is important to enable automatic updates or manually install patches regularly for both desktop and IoT devices to ensure continued security (NSA, 2023).
- Secure routing devices and keep them up-to-date – To enhance control over your home network, consider using a personal router connected to the ISP-provided modem and enable features like a guest network for improved security. Regularly update your router with the latest patches, preferably through automatic updates, and replace it when it reaches end-of-life to prevent vulnerabilities and protect other devices on the network (NSA, 2023).
- Implement WPA3 or WPA2 on the wireless network – Ensure your wireless access point supports WPA3 for secure communications or use WPA2/3 for compatibility with older devices. Configure a strong passphrase of at least 20 characters, enable protected management frames if available, and avoid hiding the SSID as it offers no additional security (NSA, 2023).
- Implement wireless network segmentation – Leverage network segmentation on your home network to keep your wireless communication secure. At a minimum, your wireless network should be segmented between your primary Wi-Fi, guest Wi-Fi, and IoT network.

This segmentation keeps less secure devices from directly communicating with your more secure devices (NSA, 2023).

- Employ firewall capabilities – Ensure that your personally owned routing device supports basic firewall capabilities. Verify that it includes network address translation (NAT) to prevent internal systems from being scanned through the network boundary. If your ISP supports IPv6, ensure your router supports IPv6 firewall capabilities (NSA, 2023).
- Protect passwords – Passwords and challenge question answers must be strong, unique for each account, and securely protected to prevent unauthorized access. Using a password manager is recommended, as it enables the use of complex, unique passwords without the need to memorize them.

The smart home IoT security recommendations from the United Kingdom government's "Secure by Design" report, the OWASP IoT Top 10 2018 Mapping Project, and the National Security Agency's (NSA) "Best Practices for Securing Your Home Network" Cybersecurity Information Sheet emphasize the critical importance of robust security measures in consumer IoT products. The common theme amongst all the guidelines should be the encouragement for manufacturers to implement strong authentication practices, such as unique default passwords and support for multi-factor authentication, to prevent unauthorized access to devices. They all highlighted the importance of regular software updates and patch management to address vulnerabilities promptly, to ensure IoT devices remain secure for their lifetime. The recommendations and best practices all stress the importance of data encryption for both data at rest and data in transit. The recommendations and best practices also encourage smart home IoT manufacturers to provide clear and accessible user education and support materials to assist consumers with understanding and configuring the security and privacy settings available. Overall,

these best practices and recommendations aim to promote a security-by-design approach, where security and privacy is integrated into smart home IoT devices and throughout the product lifecycle.

2.8 User-Controlled Security and Privacy Features for Smart Homes

User-controlled security features are configurable settings within a smart home IoT device that require direct consumer/end-user involvement to activate, configure, and maintain. Table 3 list a several user-controlled security features associated with smart home cybersecurity best practices.

User-controlled Security Feature	User Action Required
Passwords	• Use different passwords on different systems and accounts. • Use the longest password or passphrase permissible by each password system. • Develop mnemonics to remember complex passwords. • Avoid using passwords based on personal information. • Avoid using words that can be found in any dictionary of any language. • Consider using a password manager to maintain several different passwords
Password Changes	Regularly change password to reduce the risk of unauthorized
Multi-Factor Authentication	Enable multi-factor authentication for all accounts, where available. Requires users to provide two or more distinct authentication factors to access an account or system. • Something you know: password or pin. • Something you have: security token, smart card, one-time code, etc. • Something you are: fingerprint, facial recognition, iris scan.
Antivirus and Anti-Malware Software	Install, configure, and maintain updates of antivirus and anti-malware software to perform system/network scan per user preference
Application Permissions	Review and manage the permissions granted to IoT devices, limiting access to sensitive device features and data.
Notifications	Customize when and how notification is received. This feature is used to inform the user about events such security issues, potential problems in the device, or any other custom notice.

User-controlled Security Feature	User Action Required
API Access Control	Review and manage access that is granted to third-party IoT devices, applications, and service integrations.
Update and Patch Management	Have awareness of IoT device software versions and install patches when available. Automatic updates can be enabled too so the user does not forget. Notifications can also be used to alert the user of an update or patch.
Email Filtering	Setup email filtering rules to lower the risk of spam and phishing attempts. Specify email from known contacts and mark others potentially harmful to raise caution.
Authorized Devices	View and manage the devices that have access to an account or system
Account Recovery	Setup account recovery option, such as alternate email addresses, phone numbers security questions, in case of password loss or account compromise.
Device Lock	Enable the device lock feature on any mobile device (laptop, table, phone, watch, etc.) to automatically lock and require authentication to open after a certain period of time.
Remote Wiping	Remote wiping can be used to remotely erase a device that has been lost or stolen to protect user data.
Data Sharing	When sharing data with others, decide what data is collected, how it is used, and with whom it is shared by adjusting privacy settings in applications and/or online services.
Network Segmentation	Set up a separate network or VLAN (Virtual Local Area Network) for IoT devices to isolate them from the rest of your home area network.
Email Encryption	When sending sensitive data via email, encryption can protect sensitive content
Virtual Private Networks (VPNs)	When traveling away from your home network, use VPN technologies as a secure way to protect your internet connection, data, and communications.
Audit Logs	Keep and maintain access logs or activity history so home network activity can be reviewed if needed.
Data Backups	Setting up backup schedules and choosing where to store backups to ensure the availability of their data in case of data loss or a cyberattack.
Restrict Default Administrative Access	Create a secondary user account with limited permissions needed for ordinary usage; this account will become the primary account that is used. Only used the administrative account when necessary to make administrative setting updates or changes.

Table 3. User-Controlled Security Features

User-controlled security features could be considered to be a smart home IoT system's first line of defense. These user-controlled security settings allow consumer/end-users to have full control in tailoring security settings to their individual specific needs. Past research has shown that

many security incidents have occurred out of unintentional mistakes such as negligence, carelessness, and human errors (Nader Safa, 2016). Many of these unintentional mistakes often come from a lack of awareness or understanding of the security features available to users (Albrechtsen, 2010). Many consumers/end-users do not know or understand the risks associated with improper configuration of their smart home IoT devices. For example, failure to the change default username/password, continuing to ignore software updates, or misconfiguring data privacy settings can expose smart home systems to cyber threats, vulnerabilities, and unintentional. consequences (Furnell, 2008). Additionally, many of the security settings and configuration user interface pages associated with smart home IoT devices could be very confusing to some consumers/end-users, leading to user errors and/or complete avoidance. When security features are not user-friendly or are difficult to navigate, users often become frustrated, increasing the likelihood of negligence (Harbach, 2014).

User-controlled privacy features refer to settings and/or options within a smart home IoT device's setting that allow a consumers/end-user to manage and protect their personal data, access control, data sharing preferences, data retention, permissions, consent, data syncing, etc. Furthermore, these privacy settings/features give consumers/end-users the capability to decide how their data is collected, stored, shared, and used by the smart home IoT device or associated cloud service. Privacy features include controls over data sharing with third parties, disabling location tracking, managing camera and microphone access, and configuring consent management options (Perera, 2015). Table 4 list a few user-controlled privacy features associated with smart home IoT privacy best practices.

User-controlled Privacy Feature	User Action Required
Location Services	Be mindful of what applications have location services enabled. Some applications don't need to always track you.
Data Sharing	Disable data sharing with users/services you don't need.
Camera Usage	Turn off, disable, or block the camera when not in use to prevent unintended video sharing/recording.
Microphone Control	Mute or disable the microphone when not in use to prevent unintended auto sharing/recording.
Multi-Factor Authentication to Adjust Privacy Settings	Require multi-factor authentication to adjust or amend privacy settings you have previously set.
Delete Personal Data	Periodically delete personal stored data to minimize the amount of personal data stored.
Child and Guest Access	Limit or disable access to children and/or guest.
Disable Unnecessary/Unused features	Disable any unnecessary or unused features to reduce data collected.
Advertising Opt-out	Opt-out of unwanted vendor advertising to prevent tracking and the use of personal data used for advertisements.
Data Sharing Opt-out	Opt-out of options to share usage data with the manufacturer to prevent the sharing of personnel data.
Firmware/Software Updates	Regularly update firmware/software to ensure privacy vulnerabilities are patched.
Device Permissions	Regularly review device permissions to ensure only trusted users or apps have access
Cloud Backup Settings	Limit or disable data being backup to the cloud
Limit Third-Party App Access	Restrict access to only third-party apps that you have given permission too for a certain purpose.
Disable Auto-Sync	Disable automatic syncing of IoT device with other apps, devices, services.
Restrict Social Media Sharing	Disable automatic sharing of IoT device history on social media platforms.
Delete Device History	Clear history of device activities or search history.
Disable Cloud Data Storage	Use local storage options instead of cloud storage to maintain control of data.
Restrict Data Retention Period	Set limits on how long data is stored on the IoT device or cloud storage.
Disassociation of device	Perform a factory reset of the device when disposing or selling an IoT device to ensure all personal data is removed.
Disable Usage Analytics	Disable or opt-out of sharing usage analytics with manufactures or service providers.

Table 4. User-Controlled Privacy Features

Smart home IoT consumers/end-users are tasked with managing a growing number of IoT devices that collect vast amounts of data, often without clear transparency on how that data is being used (Ziegeldorf, 2014). For example, the Amazon Alexa virtual assistant is configured from the manufacture to continuously listen for commands, and if the consumer/end-user does

not properly configure the privacy settings, private conversation could be recorded and sent to Amazon. The ability to disable microphone access or limit voice data retention through user-controlled privacy settings provides consumers with greater control over their personal environments, ensuring that sensitive information is safeguarded (Feldman, 2016). The National Cybersecurity Alliance recommends for users to be aware of what data, including audio recordings, the speaker collects and how that data is stored (National Cybersecurity Alliance, 2024). However, without the proper guidance from smart home IoT manufactures on how to access and configure security and privacy settings, consumers/end-users may overlook key steps, misinterpret the available options, or frankly just skip it is all together.

2.9 Smart Home IoT Laws and Regulations

Historically, there have been very few laws, regulations, or oversight for Smart Home IoT devices. In a 2015 interview, Robert Bigman, former chief information officer at the CIA, said that a lack of federal policy governing the Internet of Things has left a security vacuum (Lyngaas, 2015). oversight for Smart Home IoT.

1. General Data Protection Regulation (GDPR): The GDPR is a European Union regulation that sets out rules for the collection, use, and storage of personal data. This regulation requires that companies shall obtain explicit consent from consumers/end-users before collecting their data and provides consumers/end-users with the right to access, modify, and delete their data. This regulation currently applies to all companies that collect data from EU citizens, including those that manufacture smart home IoT devices (Union, 2018).
2. California Consumer Privacy Act (CCPA): The CCPA is a California law that provides consumers with greater control over their personal data. This law requires companies

to disclose the types of data they collect and share with third parties and allows consumers to opt-out of the sale of their personal data. The law applies to companies that collect data from California residents, regardless of where the company is based (California, 2024).

3. Children's Online Privacy Protection Act (COPPA): COPPA is a US federal law that sets out rules for the collection of personal data from children under the age of 13. The law requires that companies obtain parental consent before collecting personal information from children and sets out requirements for the storage and use of that information. This law applies to companies that manufacture smart home IoT devices that are marketed to children (Commission, 2013).
4. National Institute of Standards and Technology (NIST) Cybersecurity Framework: The NIST Cybersecurity Framework provides guidelines for securing IoT devices against cyberattacks. The framework outlines five core functions: identify, protect, detect, respond, and recover. These functions provide a framework for companies to assess and improve their cybersecurity posture, including the security of smart home IoT devices (NIST, 2024).
5. Internet of Things Cybersecurity Improvement Act (2020): This bill requires the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) to take specified actions and steps to increase cybersecurity for Internet of Things (IoT) devices. “Specifically, the bill requires NIST to develop and publish standards and guidelines for the federal government on the appropriate use and management by agencies of IoT devices owned or controlled by an agency and connected to information systems owned or controlled by an agency, including

minimum information security requirements for managing cybersecurity risks associated with such devices" (Congress, 2020).

6. Joe Biden administration Executive Order 14208, Improving the Nation's Cybersecurity: "This executive order requires several government agencies to enhancing cybersecurity through a variety of initiatives. Specifically, this EO tasks the National Institute of Standards and Technology (NIST) and the Federal Trade Commission (FTC) to initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of Internet-of-Things (IoT) devices (NIST, 2021)." In February 2022, NIST issued: Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products and Recommended Criteria for Cybersecurity Labeling of Consumer Software. The EO outlines several key actions that the federal government must take to improve its cybersecurity, including:
    1. Modernizing federal cybersecurity: Federal agencies are directed to move to secure cloud services, adopt a zero-trust architecture, and implement multi-factor authentication and encryption.
    2. Enhancing software security: The EO calls for the development of standards and guidelines for secure software development and the adoption of a "software bill of materials" that lists the components used in software.
    3. Strengthening incident response capabilities: The EO calls for the establishment of a Cyber Safety Review Board to review significant cyber incidents and provide recommendations for improving cybersecurity.

4. Improving information sharing: The EO calls for the establishment of a government-wide endpoint detection and response initiative and the development of a plan for sharing threat information with service providers.

2.10 Systems Engineering and IoT Security

Systems engineering plays an important role in the lifecycle of smart home IoT devices, systems, and networks by understanding and integrating security and privacy protections at every stage of the system lifecycle to include design, development, deployment, operations/maintenance, and retirement. Systems engineering bridges the gap between the traditional engineering disciplines (Kossiakoff, 2020). According to Boehm et al. (2006), systems engineering is designed to design and manage complex systems, ensuring that security protections are considered and/or embedded into all facet of the system that is built and data that flows through it. As it relates to smart home IoT devices, systems engineering is a tool that can be used to help ensure that security and privacy features are not just an afterthought but are "baked in" from the ground up to align with the overall system functionality, usability, and performance that is expected. Additionally, even end-users can use systems engineering and/or systems thinking to evaluate their current smart home IoT security posture (separate from IoT manufacture support) and make necessary adjustments or enhancements to maintain an acceptable security posture.

Some of the main systems engineering principles that can be applied to smart home IoT security and privacy is system integration, systems thinking, and user-centric design. Systems Thinking is a holistic approach to understanding and analyzing a complex system by examining the interactions and relationships between the smart home components rather than focusing solely on individual smart IoT devices (Meadows, 2008). Systems Engineering in the context of smart home IoT systems begins with identifying security and privacy requirements, and best practices

during the conceptual design phase and should continue through implementation, testing, deployment, and ongoing system maintenance. For smart home IoT devices, systems, and networks, this holistic view would ensure that all system layers, from physical hardware inside the home to cloud-based services outside the home, are protected against potential threats and risks.

System integration consists of taking delivery of the implemented system elements which compose the system-of-interest (SoI), assembling these implemented elements together, and performing the verification and validation actions (V&V actions) during the assembly (INCOSE, 2024). Applying this concept to smart home systems integration, all elements of the smart home that interact with each other across the entire system lifecycle would be considered, vs only evaluating each smart home IoT device on an individual (per device) basis. This provided a gives a holistic view of the smart home system that looks beyond individual smart home IoT device settings and recognizes that individual consumer/end-user actions like keeping software/firmware up-to-date and enabling multi-factor authentication will impact the overall security posture, not just one device. For example, a consumer/end-user may not understand how a setting a weak password on an IoT device might translate in a vulnerability if the manufacture provided documentation fails to explain that the same password will be linked to a cloud account. If this information was disclosed, a user might determine to set a different password. This systems thinking/systems engineering perspective highlights potential gaps in smart home IoT manufacture guidance to ensure all elements of the system (i.e. device permissions, privacy settings, data exchange protocols, etc.) all reinforce each other in a cohesive fashion.

User-centric design in systems engineering addresses the reality that all consumers/end-users of the smart home IoT system do not possess the same level of technical understanding or are familiar with cybersecurity industry and government best practices and would benefit from a

system that is designed from their viewpoint (INCOSE, 2024). Systems engineering can serve as a unifying tool for embedding user-focused considerations early in the smart home IoT device lifecycle to guide IoT manufactures to provide clear and comprehensive security and privacy guidance, and layered instructions to accommodate a range of consumers/end-users with diverse technical skills. By using a user-centric design, and putting the user experience at the forefront, IoT manufactures can reduce the likelihood of consumers/end-users overlooking key security and privacy setting due to confusion or a perceived inconvenience.

Finally, systems engineering acts as both a technical and human-centric framework for evaluating how effectively smart home IoT manufacturers can help guide consumers/end-users in applying user-controlled security and privacy features. Through system integration, systems thinking, and a focus on user-centric design, smart home IoT manufacturers should be providing guidance through support resources (e.g. user manuals, support web pages, FAQs, etc.) and user interfaces that empower consumers/end-users to confidently secure their devices and smart home systems.

2.10.1 Requirements Analysis in Cybersecurity

A core principle of systems engineering is the analysis of the requirements. Requirements analysis is the process used to determine the needs and expectations of a system. “As the system design evolves, Requirements Analysis activities support allocation and derivation of requirements down to the system elements representing the lowest level of the design (DAU, 2024).” In the context of smart home IoT security and privacy protections, requirements analysis involves translating security and privacy industry best practices, the foundation principles of the CIA triad (confidentiality, integrity, and availability), and government regulations into actionable requirements that can be used to build, support, and maintain a smart home system architecture.

Previous research has highlighted the importance of user-focused requirements analysis for IoT devices, as non-technical consumers/end-users are often tasked with managing their security configurations. Without proper alignment between security standards, best practices, government regulations, and user needs, even the most technically sound security and privacy features can remain underutilized or misconfigured (Gonzalez, 2019).

As it pertains to Government requirements, the National Institute of Standards and Technology (NIST) provides widely accepted guidelines for conducting requirements analysis in IoT cybersecurity. NIST's Cybersecurity Framework recommends a structured approach that includes identifying potential threats, what assets that need to be protected, and the risks associated with various attack vectors (NIST- Cybersecurity Framework, 2024). The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly published the ISO/IEC 27001 emphasizes the need to tailor security requirements to the specific context of the device and its environment (ISO/IEC, 2022). For example, the security needs and requirements of a smart home surveillance camera will have much different requirements or needs for a camera monitoring a government facility.

Systems engineers must also account for the human element when conducting a requirements analysis. One of the most common failures in IoT security is the disconnect between technical requirements and user capabilities (Ur, 2016). Where we so often fail – The requirements meet all the criteria for good requirements, but it did not meet the need (Lockheed Martin, 2024).

2.10.2 Verification and Validation in Systems Engineering

Once security and privacy requirements, consumers/end-user needs, and features have been identified and integrated into a smart home IoT system, they must be verified and validated (V&V) to ensure that everything meets both the technical security requirements and the usability needs of

the users. In systems engineering, requirements verification is the process that confirms the product or service meets the requirements, while requirement validation is the process to determine if the requirements meet the needs of the consumer/end-user. In the context of smart home IoT, verification checks if the system was built according to industry best practices/guidelines and are applied consistently across all IoT devices in the smart home system. Validation goes a step further by ensuring that the smart home IoT system functions as intended in the real world and can be effectively used by all users (technical and/or non-technical). In practice, smart home IoT system validation not only focuses on the security features and user requirements but also includes the usability of the overall interfaces. This holistic approach considers the entire user experience, from initial setup to ongoing maintenance and security monitoring, to ensure that consumers/end-users have the support they need throughout the system lifecycle (Pfleeger, 2012). Additionally, V&V includes feedback loops in which real-world data from consumers/end-users inform improvements and enhancements to security and privacy features.

2.11 Gaps in the Literature

The literature review shows that a lot of research has been done on IoT devices, sensors, vulnerabilities, and cyber security recommendations focused on the enterprise and government environments. However, there is a lack of literature relating to the assistance/support IoT smart home manufacturers provide to consumers/end-users to install/configure user-controlled security and privacy features. Previous studies that have examined user-controlled security features have largely focused on the technical aspects such as IoT device vulnerabilities and attack vectors, with very limited attention given to the human factors involved in what support consumers/end-users are given by smart home IoT manufactures in securing these devices through user-controlled security and privacy features. This research seeks to bridge the gap in the literature by conducting

a systems engineering focused research study on the clarity, comprehensiveness, accessibility, and usability of the security and privacy guidance provided by smart home IoT manufacturers through user manuals and/or manufacture provided support materials.

2.12 Chapter Summary

Chapter two reviewed the available literature on the evolution of the IoT, IoT architecture, smart home threats and vulnerabilities, user-controlled security and privacy features, IoT laws and regulations, and systems engineering. Consumers are inept at knowing many of the security risks associated with IoT smart devices and struggle with ways to mitigate the vulnerabilities (Guillet, 2017). Additionally, many of the methods recommended for mitigation are complicated and require advanced technical skills to perform, leaving most consumers unable to protect themselves. Existing research primarily focuses on technical vulnerabilities, enterprise-level cybersecurity, and broad cybersecurity frameworks, often neglecting the user's role in securing personal IoT type devices. This lack of attention to user-controlled features, such as password management, multi-factor authentication, and data encryption, creates a critical gap in understanding how effectively consumers can safeguard their smart home environments. This systems engineering focused research study aims to address this gap by evaluating the clarity, comprehensiveness, and usability of security guidance provided by smart home IoT manufacturers. Chapter three presents and discusses the systems engineering focused research methodology; population of the study; sampling technique; data collection procedures and rationale; internal and external validity; and plan for data analysis.

CHAPTER 3. METHODOLOGY

The purpose of this systems engineering focused mixed-methods (qualitative and quantitative) research study was to explore the level of support smart home IoT manufacturers provide to consumers/end-users in helping them to understand, activate, and maintain user-controlled security and privacy features. More specifically, the objectives of this research study were to examine the clarity, comprehensiveness, and accessibility of the security guidance provided through smart home IoT manufacture provided materials (e.g. user guides, installation manuals, online resources, etc.). Lastly, the researcher provided insights, themes, and smart home IoT industry recommendations to solving the disparity with consumers/end-users comprehending security risk and implementing user-controlled security and privacy features appropriately.

The study used systems engineering methods and methodologies to guide the research. In chapter three, the researcher outlines the steps in the systems engineering process necessary to perform the research study. This chapter also includes a discussion regarding the research method, population, data collection procedures, validity and reliability, ethical assurance, limitations and a plan for data analysis. Chapter three concludes with a summary of the key points of the research methodology to accomplish the goals of the study and a brief introduction discussion of Chapter four.

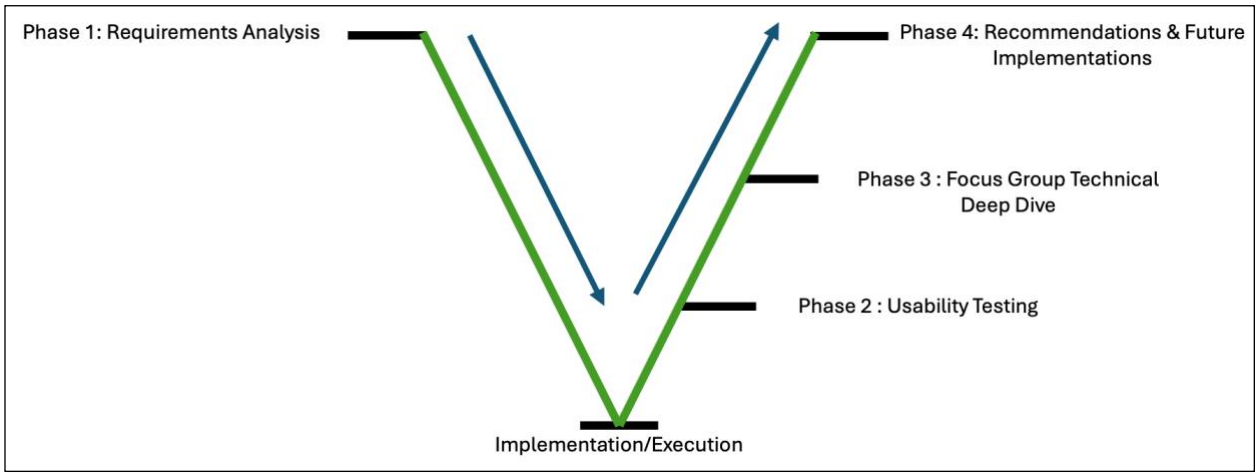
3.1 Systems Engineering Research Methods

This research study adopts a systems engineering-driven, mixed-methods (qualitative and quantitative) approach to assess how effectively smart home IoT manufacturers guide consumers/end-users in understanding and implementing user-controlled security and privacy features. Referencing the systems engineering “V” model (see figure 3), the research methodology

proceeds in four phases that align with the lifecycle of system's development and validation. This systems engineering-driven research method has four phases:

1. Requirements Analysis (Phase 1)
2. Usability Testing (Phase 2)
3. Focus Group Technical Deep Dive (Phase 3)
4. Recommendations and Future Implementations (Phase 4)

Figure 3. Incorporating the Phases into the Systems Engineering "V"



Phase 1: Requirements Analysis

The first phase of the research study began with a Requirements Analysis, a critical step in the system engineering lifecycle to set the foundation for the entire research process (Kossiakoff, 2020). The purpose of the requirements analysis was to show a clear set of standards and best practices the cybersecurity industry recommends that IoT manufactures, end-users, and consumers follow to best use user-controlled security and privacy features. To ensure that the research study's evaluation criteria had a good baseline and aligned with current industry standards and best practices, an analysis was conducted to identify and document the requirements governing the implementation of user-controlled security and privacy features in smart home IoT devices. This effort focused on finding existing best practices, industry/government standards, and

recommendations from recognized authorities in cybersecurity and consumer privacy, including the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), the National Security Agency (NSA), and the Open Web Application Security Project (OWASP). During this analysis, standards, and best practices for applying user-controlled security and privacy features were analyzed to define what attributes smart home IoT user manuals and other support documentation should show. This analysis also included evaluating the accessibility, clarity, and depth of data provided. For example, the researcher looked for security and privacy guidance that not only explained how to setup and configure a particular feature but clearly explain the potential risks and ramifications of not doing so and offered troubleshooting guidance in the event of an issues with setup and configuration. Additionally, the requirements analysis made sure that the security and privacy guidance covered various demographic groups, including age, education level, and users with different levels of technical proficiency. This involved analyzing smart home IoT device instructions to ensure they were not overly technical for beginners while still providing enough detail for a more advanced user to fully manage their security and privacy settings as they see fit. Using all the described criteria, a clear baseline was set for what constitutes a good compliant, comprehensive, and effective smart home IoT user manual should look like.

3.1.1 Requirements Analysis: Documentation and Resources Review

As part of the requirements analysis, a documentation and resources review were conducted to provide a better understanding of what security instructions, recommendations, and/or guidance is currently (at the time of the study) provided to consumers via smart home IoT device manuals, manufacture websites, and other device specific online documentation. This systems engineering-based and qualitative review involved selecting several Smart Home IoT

devices, on sale at the time of this study, and holistically analyzing their user manuals, quick reference guides, FAQs, and internet support pages, and comparing them against the recommendations, best practices, and guidelines recommended by NIST, ISO, NSA, and OWASP. The Smart Home IoT devices selected were intended to cover many of the common smart home use cases such as security cameras, thermostats, lighting, baby monitors, voice assistants, home security, and entertainment. For each device, three sources of data were examined. First, any documentation included with the device was reviewed for alignment to the requirements analysis, clarity, and comprehension. This documentation included: Quick Start Guides, User Manuals, Safety and Regulatory Information, Warranty Information, Technical Specifications, Mobile App or Web Interface Guides, Customer Support Information, Terms and Conditions, Product Registration, etc. Second, any documentation that was outside of what was included in the device packaging was reviewed was for alignment to the requirements analysis, clarity, and comprehension This documentation included: Manufacturer's Website, Customer Support and Manufacturer's social media. Third, support documentation from external sources was was for alignment to the requirements analysis, clarity, and comprehension. This included: Online IoT Communities and Forums, You Tube Tutorials, and Third-party websites.

After documentation and resource material review, the data collected was examined to figure out to what extent smart home IoT device manuals and support documentation aligned with the security best practices recommended by NIST (National Institute of Standards and Technology), NSA (National Security Agency), and OWASP (Open Web Application Security Project). This analysis involved a detailed review of the content within these manuals, focusing on the security recommendations, instructions for enabling and managing security features, and any guidance on maintaining the security integrity of the devices over their service life. Each manual was evaluated

based on a set of criteria derived from NIST, NSA, and OWASP guidelines (outlined in Literature Review). The industry best practices chosen for evaluation include:

1. Change Default Credentials – Recommend users replace factory-set usernames and passwords with strong and unique credentials.
2. Multi-Factor Authentication – An authentication method that requires the user to provide two or more verification factors to gain access.
3. Network Security Settings – Inform users of network security options (e.g. encryption, access control, Virtual Private Networks (VPNs), encryption, etc.)
4. Software/Firmware Updates – Recommend users verify the device is running the most current software/firmware to patch known vulnerabilities and security features.
5. Privacy Protection – Asist users in understanding privacy risk and how to adjust privacy settings to control the amount of personal data the device collects and shares.
6. Physical Hardening – Recommend IoT devices are positioned in secure locations to prevent unauthorized physical access or tampering This could include placing devices in secure locations or behind locked enclosures,
7. Continuous Security Monitoring – Recommend users periodically check the security and privacy setting on the IoT device and update as needed.
8. Transfer to Another User or disposal – Ensure device is unlinked from personal accounts, removed from home network factory resets to remove/delete personal, and inform new user of device and encourage them to configure personalized privacy and security settings.

The extent to which the documentation and resources incorporated clear, actionable, and comprehensive security and privacy practices was documented, and any areas of deficiency or misalignment with industry best practices and recommendations was noted. This review and qualitative analysis intended to uncover the gaps between manufacturer-provided security guidance and the established best practices in the cyber security industry. Outcomes from the requirements analysis were used as the basis for designing usability test to measure if participants can comprehend user-controlled security and privacy features based on guidance provided.

3.1.2 Phase 2: Usability Testing

Following the documentation and resources review (Phase 1), the research study proceeded with usability testing to better understand how real users would react when asked to follow a smart home IoT user's manual – specifically regarding user-controlled security and privacy features. The usability testing included two distinct parts—verification and validation. Under the verification lens, the research study assessed whether a custom provided smart home IoT user manual accurately and comprehensively addressed the user-controlled security and privacy features identified during the requirements analysis phase. Under validation lens, participants were asked to interpret the custom provided smart home IoT user manual's guidance in practice through a proficiency test to determine how effectively they could recognize and apply the recommended settings. Part one of the usability testing relied on a structured survey to capturing test group participant's demographics and baseline cybersecurity knowledge.

Part two of the usability testing used proficiency tests to validate if operational requirements were really met for user-controlled security and privacy in a real-world setting. Participants were assigned to test groups, each receiving a custom manual for a Wi-Fi security

camera (selected for its popularity and potentially high security risks). Participants in Test Group #1 received a mock wi-fi security camera user manual that included security guidance and comprehensive guidance on applying user-controlled security and privacy features. This mock user manual adhered to many security and privacy best practices, clearly explaining how to create strong passwords, enable multi-factor authentication, and activate several other critical security and privacy features. Test Group #2 received a mock wi-fi security camera user manual that omitted security guidance, providing only basic installation instructions for the camera and camera operations use features. Participants in each test group were asked to review their assigned manual and then asked to complete a proficiency test designed to assess their knowledge and awareness of the security and privacy features.

Systems validation provide the evidence on whether the system performed as intended, in the case of smart home IoT user manuals, did the manuals assist and encourage users to adopt the user-controlled security and privacy features. The usability testing results uncovered if the user manual that included the security guidance led to higher user awareness and implementation of user-controlled security and privacy features.

3.1.3 Phase 3: Focus Group Technical Deep Dive

The Focus Group Technical Deep Dive phase shifts to a qualitative analysis and technical deep dive of the personal experiences of users who participated in the usability testing (structured survey and proficiency test). This phase gathered in-depth insights from survey participants and provided context to the quantitative results observed during Phase 1 and Phase 2 of the research study. Test group participants who completed the survey and proficiency test were invited to participate in an interview-based focus group. The primary goal of this focus group was to explore

individual user experiences, challenges, and real-world user suggestions related to the application of user-controlled security and privacy features on Smart Home IoT devices.

During the focus group session, participants were asked targeted questions with the goal of understanding the difficulties they have personally encountered applying user-controlled security features and identifying potential areas for improvement. Questions asked to participants during the focus group include:

1. What are the challenges (if any) have you faced when trying to follow security guidance?
2. How could an IoT user manual be modified to better support you?
3. What type of visual aid could be added to security guidance to help understanding?
4. What additional information or support would increase your confidence in applying user-controlled security features?

Findings from the focus group were used to complement the data gathered in phase 1 and phase 2. The focus group also identified user challenges and actionable improvements that could inform recommendation and future implementations of the increased utilization of user-controlled security and privacy features.

3.1.4 Phase 4: Recommendations and Future Implementations

The final phase of the research methodology focuses on recommendations and future implementations based on findings in the research study. The primary goal of this phase is to address identified gaps between industry and government recommended best practices and smart home IoT manufacturer-provided guidance. Emphasis was focused on informing governance and policies, influencing smart home IoT industry practices, human-centric design, and advancing systems engineering practices in alignment with INCOSE Vision 2035.

Recommendations will be developed by synthesizing the data collected during phase 1-requirements analysis, Phase-2 usability testing, and Phase-3 focus group technical deep dives. Key themes will be developed from the systems engineering analysis to guide improvements in smart home IoT device design, enhancements to smart home IoT manufacturer guidance, and consumer/end-user adoption strategies. Using iterative systems engineering processes, future implementation recommendations will be developed based on the participant feedback gathered in earlier research phases to ensure the recommended solutions are practical and aligned with "real" user needs.

3.2 Systems Modeling Language (SysML)

System Modeling Language (SysML) is a modeling language for systems engineering to analyze, specify, design and verify complex systems, intended to enhance systems quality, improve the ability to exchange systems engineering information amongst tools and help bridge the semantic gap between systems, software and other engineering disciplines (Sanford Friedenthal, 2015). In this research study, SysML is used to capture and visualize the architecture, requirements, and interactions of consumers/end-users as they utilize user-controlled security and privacy features in smart home IoT system.

3.2.1 SysML Activity Diagram

The iterative systems engineering process employed in this research study is designed to be repeatable and scalable. The process begins with an initial requirements analysis, followed by design, implementation, verification, and validation, then looping back through user feedback to refine the system continuously. This cycle can be repeated as often as necessary to accommodate new insights, emerging technologies, or changes in user behavior. The associated SysML Activity Diagram to show this iterative process flow is in figure 4 below.

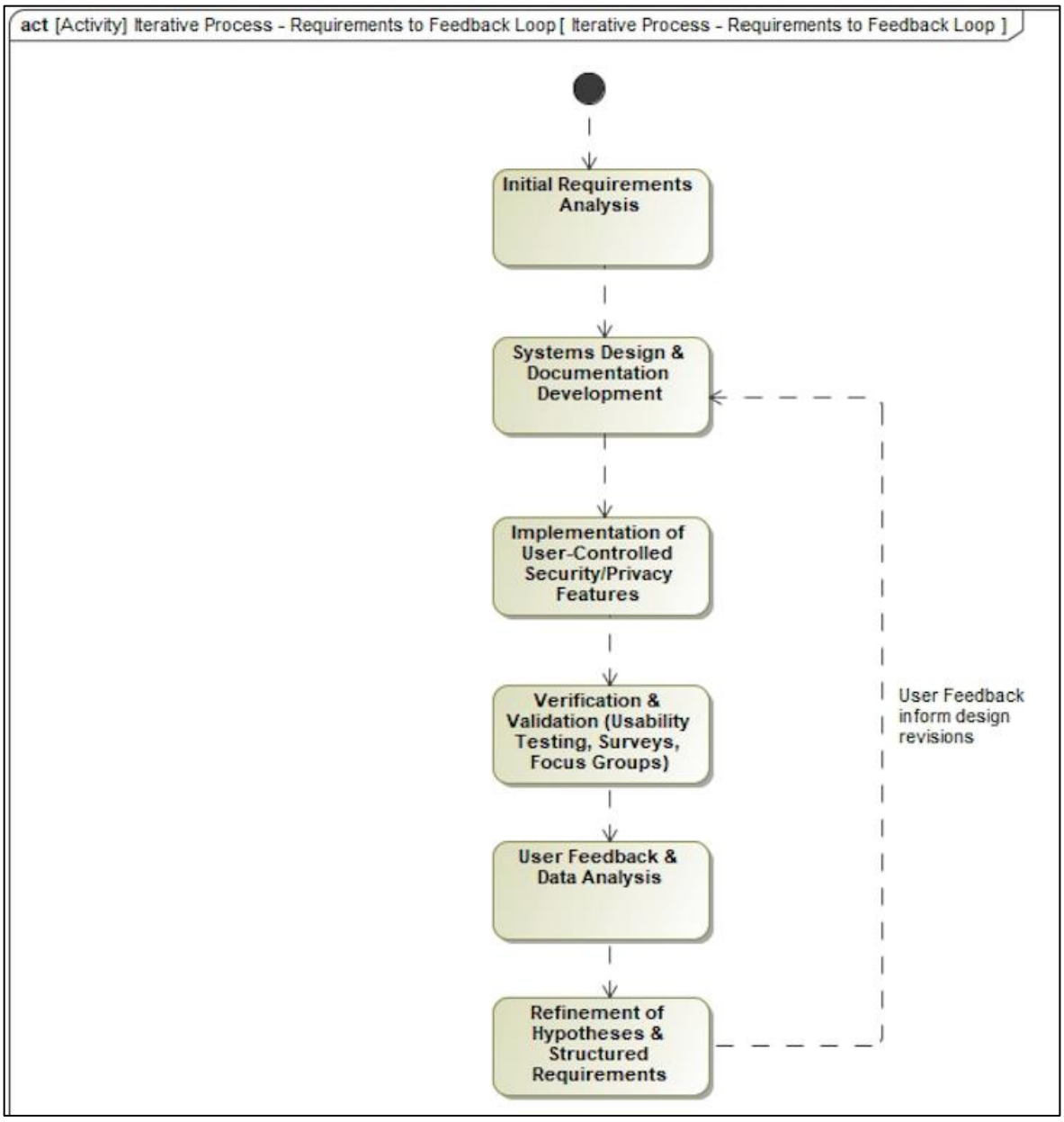


Figure 4. SysML Activity Diagram

3.2.2 SysML Block Definition Diagram (BDD)

The SysML Block Definition Diagram is an overview of the Smart Home systems with the embedded user-control security and privacy features and multiple supporting components. The diagram also incorporates feedback loops to illustrate how user feedback from surveys, proficiency

tests, and focus groups feeds back into the system for iterative refinement with the goal of a better design. See figure 5 below.

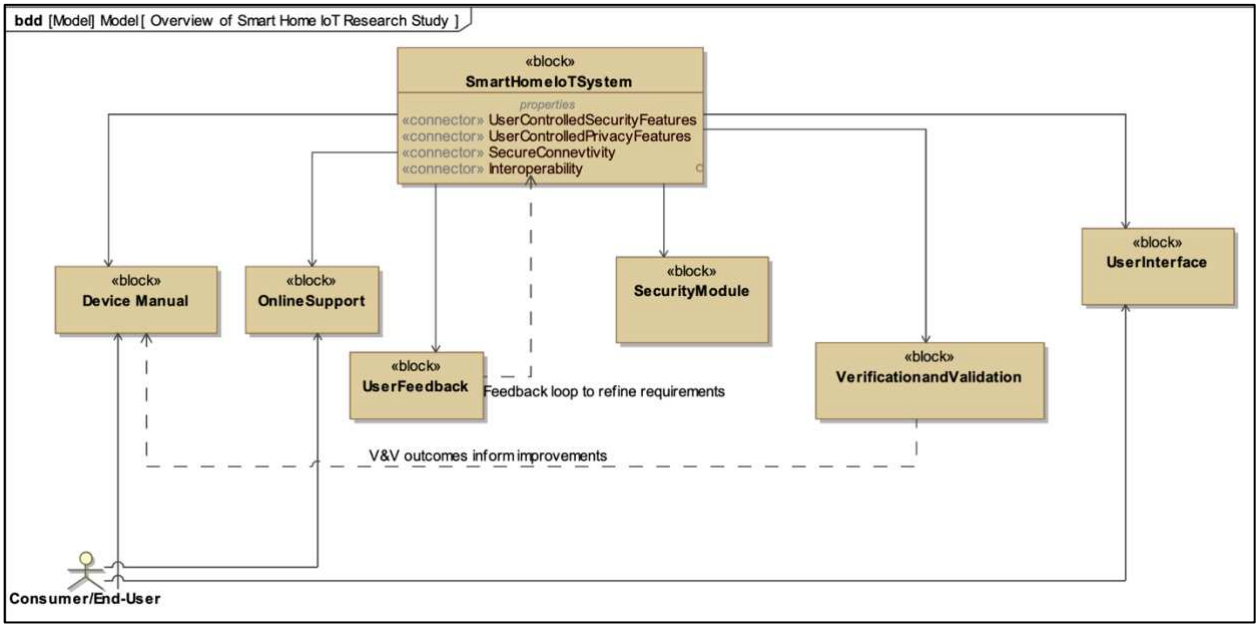


Figure 5. SysML Block Definition Diagram

3.2.3 SysML Requirements Table

The SysML Requirements Table of Functional Requirements (FRs) and Non-Functional Requirements (NFRs) outline the security and privacy criteria that guided the design and evaluation of the Wi-Fi security camera used in this research study. By linking industry recommendations and best practices from authoritative bodies (e.g., NIST, NSA, OWASP, and Matter) to the operational context of the wi-fi camera system, the SysML requirements tables (see Tables 5 & 6 below) highlight the security controls and privacy protections necessary for an effective Wi-Fi security camera installation, configuration, and deployment.

	Requirements Area	High-Level Requirements
1	Change Default Credentials	1.1 The Wi-Fi camera system must require users to change default usernames and passwords during the initial setup process. 1.2 The Wi-Fi camera system shall enforce strong password policies (e.g., minimum length, complexity requirements)
2	Multi-Factor Authentication (MFA)	2.1 The Wi-Fi camera system shall support multi-factor authentication for accessing the camera's mobile app or web interface.
3	Network Security Settings	3.1 The Wi-Fi camera system shall support secure Wi-Fi protocols 3.2 The Wi-Fi camera system shall allow users to configure network security settings
4	Software/Firmware Updates	4.1 The Wi-Fi camera system shall support automatic and manual over-the-air (OTA) firmware updates to ensure the latest security patches are applied. 4.2 The Wi-Fi camera system shall notify users when updates are available and provide clear instructions for installation.
5	Privacy Protection	5.1 The Wi-Fi camera system shall include a physical shutter or LED indicator to show when recording is active to ensure users are aware of its status. 5.2 The Wi-Fi camera system shall provide the capability to disable recording or streaming to protect privacy when needed.
6	Physical Hardening	6.1 The Wi-Fi camera system shall be tamper-resistant, with features such as anti-tamper screws or enclosures to prevent physical access to internal components. 6.2 The Wi-Fi camera system shall have the capability to detect and alert users if the camera is physically tampered with (e.g., removed or covered).
7	Continuous Security Monitoring	7.1 The Wi-Fi camera system shall log and monitor security events (e.g., failed login attempts, unauthorized access) and provide alerts to the user.
8	Transfer to Another User or Disposal	8.1 The Wi-Fi camera system shall provide a secure factory reset option to wipe all user data and settings before transferring ownership or disposing of the device. 8.2 The Wi-Fi camera system shall provide a capability to ensure all stored data (e.g., footage, credentials) is permanently deleted during the reset process.

Table 5. SysML Functional Requirements

	Requirements Area	High-Level Requirements
1	Performance	1.1 The Wi-Fi camera system shall maintain high-quality video streaming (1080p or higher) with minimal latency, even when security features like encryption are enabled.
2	Reliability	2.1 The Wi-Fi camera system shall have a fail-safe mechanism to ensure it remains operational during firmware updates or network disruptions.
3	Scalability	3.1 The Wi-Fi camera system shall support multiple cameras while maintaining secure communication and access controls for each device.
4	Durability	4.1 The Wi-Fi camera system shall be weatherproof (IP65 or higher) and resistant to physical damage, ensuring it remains functional in various environments.
5	Ease of Use	5.1 The Wi-Fi camera system shall include clear guidance on enabling security features (e.g., MFA, network segmentation) without requiring advanced technical knowledge.
6	Compliance	6.1 The Wi-Fi camera system shall comply with industry standards and regulations (e.g., NIST, GDPR) for data protection and privacy.
7	Energy Efficiency	7.1 The Wi-Fi camera system shall minimize power consumption while maintaining continuous security monitoring and recording capabilities.
8	Interoperability	8.1 The Wi-Fi camera system shall integrate securely with other smart home devices and platforms, ensuring compatibility without compromising security.

Table 6. SysML Non-Functional Requirements

3.2.4 SysML Use Case Specification

The following SysML use case specification and accompanying SysML Use Case diagram (Figure 6) give a comprehensive overview of user interactions within this research study focus the comprehension and application of user-controlled security and privacy features. This SysML model captures the complete lifecycle of consumer/end-user engagement—from the initial baseline assessment through the configuration of security settings, performance evaluation via proficiency tests, and in-depth focus group feedback—to illustrate the iterative refinement of system requirements based on real-world user input (Table 7 & 8).

Use Case: Configure User-Controlled Security and Privacy Features

General Description: This use case describes how a consumer/end user interact with a smart home IoT Wi-Fi camera system to comprehend and configure user-controlled security and privacy settings.

Preconditions:

- The smart home IoT Wi-Fi camera is powered on and connected to the home network.
- The consumer/end-user has access to the device manual

Postconditions:

- User-controlled security and privacy features are successfully configured and updated.
- System logs record all configuration changes made by the user.
- Feedback from the proficiency test, structured surveys, and focus group deep dive sessions are captured and integrated into the requirements for further refinement of the smart home system.
- Smart home system is verified to comply with industry best practices

Actors:

- Primary Actor: Consumer / End User
- Supporting Actors:
    - Smart Home IoT Wi-Fi Camera
    - IoT Device Manual
    - Survey & Proficiency Test Instrument
    - Focus Group Moderator/Facilitator

Primary Data Objects:

- User Credentials (Usernames, Passwords)
- Security Configuration data
- Network Security Settings
- Survey Response Data
- Proficiency Test Scores
- Focus Group Transcripts
- User Feedback Summary Reports

Scenarios:

1. Baseline Knowledge Assessment and Initial Configuration:
    a. Consumer/end-user completes a structured survey designed to establish a baseline of their technical proficiency and cybersecurity knowledge
2. Proficiency Testing Using Wi-Fi Camera Installation Manual:
    a. Consumers/end-user is administered a proficiency test using the provided Wi-Fi camera installation manual as the sole guide.
    b. Proficiency test evaluates the user's ability to correctly implement the recommended user-controlled security and privacy features.
    c. Proficiency test is graded based on completeness of configuration actions.
    d. Proficiency test serves as a quantitative measure of how effectively the manual guides the user in applying security and privacy settings.

3. **Focus Group Deep-Dive Discussion:**
    a. Select Consumer/end-users participate in a focus group session where they discuss their experiences with the security configuration process in detail.
    b. During the session, the consumers/end-users articulate specific challenges, areas of confusion, suggestions for improving to the Wi-Fi security camera installation manual and other user-controlled security and privacy feature configuration frustrations.
    c. Feedback collected is documented and later synthesized into actionable insights.
4. **Feedback Integration and Iterative Refinement:**
    a. Data from the surveys, proficiency tests, and focus group discussions is analyzed to identify recurring issues, gaps, and user needs.
    b. Feedback is used to update and refine system requirements and user installation manuals.
    c. New, structured requirements (e.g., improved visual aids, clearer step-by-step instructions) are generated, closing the feedback loop and guiding future iterations of the system design.

Allocated Requirements

- Functional Requirements

	Requirements Area	High-Level Requirements
1	Change Default Credentials	1.1 The Wi-Fi camera system must require users to change default usernames and passwords during the initial setup process. 1.2 The Wi-Fi camera system shall enforce strong password policies (e.g., minimum length, complexity requirements)
2	Multi-Factor Authentication (MFA)	2.1 The Wi-Fi camera system shall support multi-factor authentication for accessing the camera's mobile app or web interface.
3	Network Security Settings	3.1 The Wi-Fi camera system shall support secure Wi-Fi protocols 3.2 The Wi-Fi camera system shall allow users to configure network security settings
4	Software/Firmware Updates	4.1 The Wi-Fi camera system shall support automatic and manual over-the-air (OTA) firmware updates to ensure the latest security patches are applied. 4.2 The Wi-Fi camera system shall notify users when updates are available and provide clear instructions for installation.
5	Privacy Protection	5.1 The Wi-Fi camera system shall include a physical shutter or LED indicator to show when recording is active to ensure users are aware of its status. 5.2 The Wi-Fi camera system shall provide the capability to disable recording or streaming to protect privacy when needed.
6	Physical Hardening	6.1 The Wi-Fi camera system shall be tamper-resistant, with features such as anti-tamper screws or enclosures to prevent physical access to internal components. 6.2 The Wi-Fi camera system shall have the capability to detect and alert users if the camera is physically tampered with (e.g., removed or covered).
7	Continuous Security Monitoring	7.1 The Wi-Fi camera system shall log and monitor security events (e.g., failed login attempts, unauthorized access) and provide alerts to the user.
8	Transfer to Another User or Disposal	8.1 The Wi-Fi camera system shall provide a secure factory reset option to wipe all user data and settings before transferring ownership or disposing of the device. 8.2 The Wi-Fi camera system shall provide a capability to ensure all stored data (e.g., footage, credentials) is permanently deleted during the reset process.

Table 7. Functional Requirements

- Non-Functional Requirements

	Requirements Area	High-Level Requirements
5	Ease of Use	5.2 The Wi-Fi camera system shall include clear guidance on enabling security features (e.g., MFA, network segmentation) without requiring advanced technical knowledge.
6	Compliance	6.2 The Wi-Fi camera system shall comply with industry standards and regulations (e.g., NIST) for data protection and privacy.

Table 8. Non-Functional Requirements

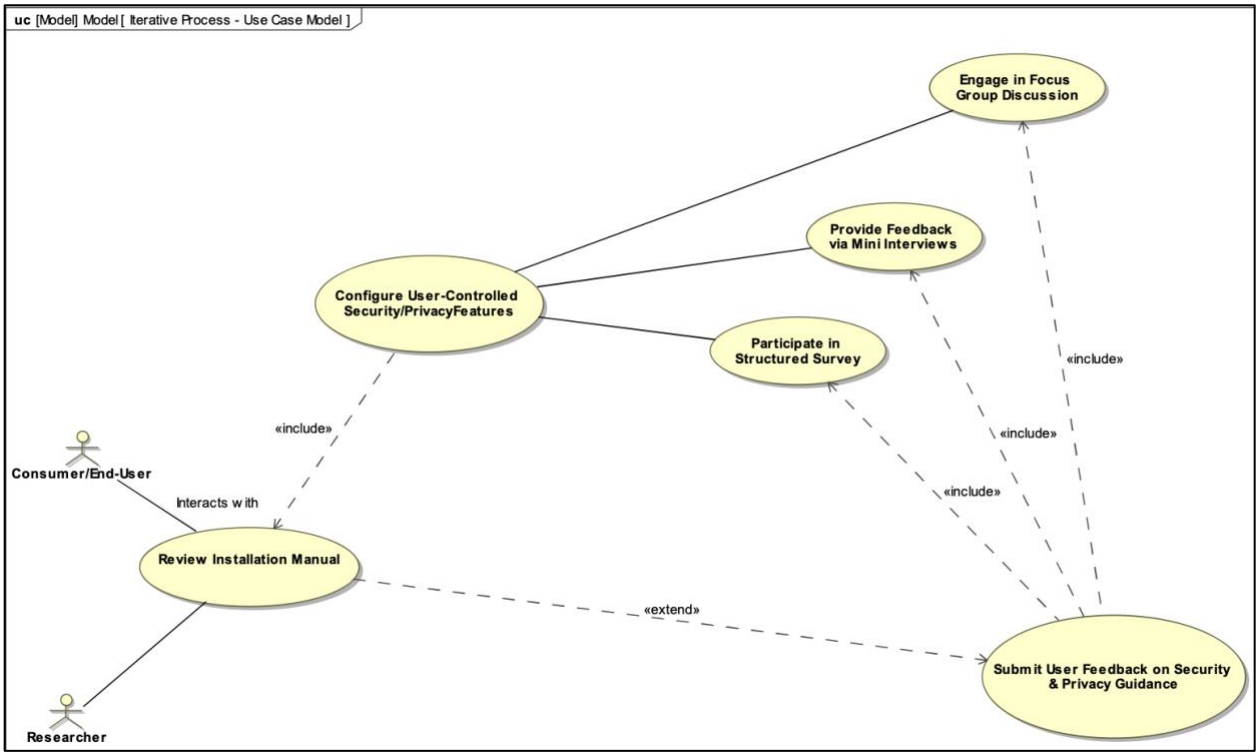


Figure 6. SysML Use Case Diagram

3.3 Population and Participant Recruitment

In this section, the researcher will describe the chosen population and sample selection steps necessary for recruiting the appropriate participants for the research study. In the following subsections, the researcher will provide reasons for choosing the specific selection criteria.

3.3.1 Population

According to Creswell and Guetterman (2019), Survey research starts by identifying a population. A population is the entire set of individuals with characteristics like potential participants meeting the criteria of interest established by a researcher to make inferences about the entire population under investigation (Salkind, 2011). In this research study, the general

population was comprised of smart home IoT consumers residing in the United States. A study performed in 2016 by Maru/Matchbox on behalf of the Interactive Advertising Bureau (IAB) showed that 62% of American adult consumers have at least one IoT connected device (Sruoginis, 2016). According to the U.S. Census Bureau, the estimated U.S. population in 2016 was 323,127,513 with 22.8% under the age of 18, meaning that more than 154 million adult consumers in 2016 had at least one IoT connected device in their households (U.S. Census Bureau, 2016).

The specific target population for this study was adults aged 18 or older, residing in the United States, familiar with internet of things devices in the home, and who have been involved in the setup/configuration of smart home IoT devices. Some examples of the target population include people who have experience with setup/configuration of surveillance cameras, thermostats, and smart home hubs (e.g. Amazon Echo, Goggle Nest Hub, Apple HomeKit, Home Assistant, etc.). The chosen population was suitable because it concentrates on the consumer/end-user perspective and experiences of installing and configuring IoT smart home devices. The population target for this research study was at least 60 participants, at least 30 participants are needed to support each Test Group.

3.3.2 Participant Recruitment

Participants were recruited through a combination of online platforms, professional organization affiliation, peers, and referrals. Participants who received the initial survey invitation to participate were asked to pass on the link to their peers and/or professional network, also called snowball sampling. Participants were required to be 18 years or older and have at least one smart home device in use at their residence. Participants were randomly assigned to one of the two test groups to ensure that each group is representative of the population and to minimize selection bias:

- Survey/Proficiency Test Group 1 (Security Guidance Provided): Received a written instruction manual that adhered to many cybersecurity best practices, clearly explaining how to set up strong passwords, enable encryption, and activate other critical security and privacy features.
- Survey/Proficiency Test Group 2 (No Security Guidance Provided): Receive a written instruction manual that omitted critical security guidance, providing only basic installation instructions without any specific advice on securing the IoT device.

Participant information was kept confidential, and data will be anonymized for analysis. Participation is voluntary, and participants can withdraw at any time without penalty. Detailed informed consent will be obtained, explaining the study's purpose, procedures, potential risks, and benefits.

3.4 Data Analysis Plan

This research study will produce two primary types of data:

- Quantitative Data:
    - Structured survey results
    - Proficiency Test results
- Qualitative Data:
    - Detailed evaluation of smart home IoT manufacturers' device documentation, and other resources provided by the IoT manufacture
    - Focus Group responses
    - Systems Engineering verification and validation assessment

One of the major challenges with using a mixed method study is determining how the variation of data types is integrated to answer the research questions. A contiguous data integration approach

is taken to present findings, meaning that qualitative, quantitative, and convergent findings are reported in separate sections (Fetters, 2013).

3.4.1 Quantitative Data Analysis

The focus of the quantitative analysis is to evaluate the impact clarity and comprehensiveness of security guidance provided by manufacturers through smart home IoT device manuals has on a consumers' knowledge and awareness of security and privacy best practices. This will be achieved by analyzing structured survey and proficiency test results from participants who reviewed two different types of written instruction manuals for a smart home IoT device:

1. Instruction Manual that adhered to many cybersecurity and privacy best practices, clearly explaining how to set up strong passwords, enable encryption, and activate other critical security features (Security Guidance Provided).
2. Instruction Manual that omitted critical security guidance, providing only basic installation instructions without any specific advice on securing the IoT device (No Security Guidance Provided).

3.4.1.1 Data Preparation

The first step in preparing the data analysis was organizing the survey responses into a structured data set. This was done to ensure that each response is accurately matched and recorded against the corresponding participant to maintain data integrity. Following the data compilation, a thorough review of the dataset was conducted to assess the completeness and consistency. During this review, any missing data was addressed through appropriate methods, such as exclusion, depending on the nature and extent of the missing information.

3.4.1.2 Descriptive Analysis

The descriptive analysis involved an examination of the collected data, with a focus on summarizing the demographic characteristics of the participants and their baseline knowledge of smart home IoT security and privacy best practices. Utilizing descriptive statistics such as means, medians, modes, and standard deviations, this analysis shed light on the overall composition of the study sample, including age distribution, levels of education, and initial cybersecurity knowledge levels (Nikolay M. Bulanov, 2021). This key step helped to understand the diversity within the participant pool and ensured that the sample was representative of a broader population of smart home IoT consumers/end-users. Additionally, the baseline security and privacy best practices knowledge assessment provided crucial insights into the participants' understanding and awareness of security and privacy practices prior to their engagement with the instruction manual provided. By establishing a "per participant" technical understanding baseline, the analysis set the groundwork for additional statistical tests aimed at evaluating the impact of the clarity and comprehensiveness of security guidance provided by IoT manufacturers.

3.4.1.3 Inferential Analysis

The quantitative data from the surveys was analyzed using inferential analysis and linear regression analysis. For the inferential analysis, a t-test were used to determine if there was a significant statistical difference between the knowledge awareness between the two test groups. This analysis will yield a p-value, which will indicate whether the differences in outcomes between the groups are statistically significant (commonly using a threshold of $p < 0.05$).

3.4.1.4 Regression Analysis

In addition to the T-test, a linear regression analysis was performed to explore the relationship between several various factors (e.g., the clarity of guidance, demographic characteristics) and

changes in consumer knowledge and awareness. Linear regression analysis was used to estimate the extent to which specific factors predicted changes in consumer knowledge and awareness. The coefficients obtained from the regression analysis will indicate the direction and magnitude of the relationship between each predictor and the outcome, offering insights into which aspects of the guidance are most effective at enhancing consumer engagement with security features. The combination of these quantitative analyses provides a robust understanding of how the quality of Smart Home IoT device security guidance impacts consumer awareness and will help identify key areas where improvements can make a measurable difference.

3.4.1.5 Qualitative Data Analysis

The data collected through the qualitative data analysis will be used to assess how well a smart home IoT manufactures manuals aligns with the government standards and best practices as outlined by authoritative bodies like NIST, NSA, and OWASP for smart home IoT devices. The data analysis was focused on revealing the areas where manufacturer-provided guidance fell short of industry best practices, recommendations, and highlighted deficiencies in the clarity and actionability of the instructions. This qualitative review not only exposed gaps between current manufacturer guidance and established cybersecurity standards but also offered valuable insights into how smart home IoT manufacturers can improve their documentation to better equip consumers with the knowledge and tools needed to secure their smart home environments effectively. The findings from this analysis contribute to a broader understanding of the state of consumer-facing security guidance in the smart home IoT domain.

3.4.1.6 Statistical Insights from Focus Groups

In addition to the quantitative and qualitative data from the survey and proficiency test, qualitative data from the focus group interviews will be analyzed to further understand the users'

experience, mindset, and approach when interacting with Smart Home IoT device manuals. Statistical insights, such as the percentage of participants who express difficulty in understanding key security concepts, will be generated to provide quantitative insights from qualitative feedback. The combination of both qualitative and quantitative analyses will provide a comprehensive view of both the content and usability of Smart Home IoT security and privacy guidance, offering tangible recommendations for manufacturers on how to improve their support materials in alignment with best practices. Furthermore, these research contributions enhance the security and privacy of smart home IoT devices by proposing evidence-based improvements to documentation and user support.

3.5 Statistical Power and the Need for Follow-on Interviews

When conducting research within a domain as large as smart home IoT, ensuring adequate statistical power is vital to ensuring that meaningful conclusions are drawn from survey data. A January 2024 survey on smart homes indicated that 69.91 million U.S. households were actively use IoT devices, which was a 10% increase over the 63.43 million reported in 2023 (Oberlo, 2024). In principle, with the large IoT adoption rates, large sample sizes (1,000 responses or more) are necessary for to achieve high confidence and wide representation, similar to Gallup and other polls used in presidential elections. However, in practical terms, getting an extremely large sample size for an academic research study poses significant challenges due to participant-recruitment constraints, schedule, and cost. It is understood that smaller n-values result in lower statistical powered analyses, making it difficult to pinpoint differences or relationships when employing regression approaches. However, to mitigate the issue of a smaller power value, the surveys and proficiency test were complemented with mini follow-up interviews and focus group deep-dive discussions. These qualitative approaches allowed participants to elaborate on their experiences as

well as clarify their survey and proficiency test responses that might otherwise remain ambiguous or be misinterpreted. These interviews and case studies also allowed us to identify specific binary issues (in statistics, A/B issues) that are amenable to more traditional inferential statistical tests such as t-tests and analysis of variance, or ANOVA. While a significantly larger participant pool could have further bolstered confidence in generalizing outcomes to the wider population, the systems engineering based analysis used in this research study struck a balance between depth and breadth.

3.6 Validity and Reliability

Validity and reliability are critical aspects of any research study to ensure the findings are accurate and replicable. Validity measures the accuracy of the research results, while reliability examines the consistency of the findings when repeated over time using similar tools (Kirk & Miller, 1986). To establish validity, the study aligned the survey, usability tests, and focus group discussions with established cybersecurity frameworks from industry leaders, such as those from NIST and NSA. This study employed internal validity to ensure the design controls for variables could influence the outcome. External validity was established using a diverse sample of smart home IoT device users. This combination of internal and external validity made the results a lot more generic for a broader consumer/end-user population.

Reliability refers to the consistency of the results from the research study. To guarantee reliability, the researcher used standardized survey and proficiency test protocols, to ensure that the same procedures were applied across all participants. Repeated measures, such as analyzing the different test groups, used the same security guidance materials to ensure that results can be reproduced in similar studies.

3.7 Ethical Assurances

Prior to the starting the research study, all research protocols, including participant recruitment, data collection methods, and privacy measures, were submitted for review and approval by the Colorado State University (CSU) Institutional Review Board (IRB) to ensure compliance with ethical standards. Informed consent was obtained from all participants, clearly outlining the study's purpose, what participation entails, the voluntary nature of their involvement, and the measures in place to protect their anonymity and confidentiality. This includes the use of de-identified data in any analysis or publication resulting from the study. Participants were also informed of their right to withdraw from the study at any point without any adverse consequences. The handling of survey responses and any personal data will adhere strictly to data protection regulations, ensuring that all information is securely stored and accessible only to the research team. By implementing these ethical assurances, the study aims to foster a respectful and secure environment for participants, ensuring that the research is conducted with integrity and in accordance with the highest ethical standards. This research study was approved on March 8, 2024, by the Colorado State University Institutional Review Board.

3.8 Limitations of the Methodology

The methodology chosen for this research, while comprehensive, does come with a few limitations. First, the research study's focus on user-controlled security and privacy features in Smart Home IoT devices limits the findings to only that domain and excludes other types of IoT ecosystems, such as industrial IoT or smart cities that may have different security challenges and user interactions. Additionally, the use of surveys and proficiency tests to measure user understanding of security and privacy features may not fully capture the full depth of real-world behavior, as participants may behave differently in controlled environments compared to actual

settings where they use smart home IoT devices daily. Another limitation is the sample size and diversity; while efforts were made to include a diverse participant pool, the demographic scope may not represent a full range of smart home IoT users, particularly those with extreme technological proficiency or those from underrepresented populations. Furthermore, the focus on documentation and manual review may overlook other factors influencing user behavior, such as the role of device interfaces or external technical support, which could play a significant role in how users engage with security and privacy features. These limitations suggest that future research could explore additional contexts, user groups, and real-world behaviors to deepen the understanding of Smart Home IoT security practices.

3.9 Chapter Summary

The methodology used for this research study provided a structured and systematic approach to evaluating the effectiveness of guidance users receive when applying user-controlled security and privacy features in smart home IoT devices through the lens of systems engineering. Beginning with requirements analysis, the research study established a framework rooted in industry standards to ensure the research remained aligned with industry respected cybersecurity recommendations and best practices. The integration of documentation and resource reviews, usability testing, and focus group feedback allowed for both quantitative and qualitative insights. Chapter 4 followed this chapter and presented the results of the research study.

CHAPTER 4. RESULTS

The research study focused on the level of support smart home IoT manufacturers provide to consumers/end-users in helping them to understand, activate, and maintain user-controlled security and privacy features. Chapter 4 will describe the research study results. The research study findings are reported in three categories: 1) Requirements Analysis: Documentation and resources review of common smart home IoT devices; 2) Usability Testing: Survey results and proficiency test results; 3) Focus Group Technical Deep Dive and user feedback interviews.

4.1 Phase 1: Requirements Analysis Results

In the documentation and resources review phase of the research study, 29 smart home IoT devices, that were on sale at the time of this study, were selected for evaluation. The researcher aimed to cover a broad spectrum of popular smart home IoT devices of different brands and different price ranges to represent a typical variety. Each device's user manual, quick reference guide, FAQs, and internet support pages were evaluated to see how well the manufacture provided support material addressed user-controlled security and privacy features. Each device's support material was also reviewed and compared against select recommendations, best practices, and guidelines recommended by NIST, NSA, and OWASP. The following user-controlled security and privacy guidelines were chosen for the documentation and resources review:

1. Change Default Credentials
2. Multi-Factor Authentication
3. Network Security Settings
4. Software/Firmware Updates
5. Privacy Protection
6. Physical Hardening

7. Continuous Security Monitoring
8. Transfer to Another User or disposal

The above eight guidelines were chosen because they address some of the most common vulnerabilities and threats associated with smart home IoT devices and encompass a wide range of security and privacy aspects that are user-controlled. To structure the analysis, the researcher created a checklist derived from NIST, NSA, and OWASP guidelines, recommendations, and best practices. The researcher then used this checklist to question whether the user manuals or other support materials clearly explained how to execute each selected guideline, gave troubleshooting tips, and/or if it included any visual aids (e.g., diagrams, screenshots). Table 9 below a presents the results of the documentation and resources review (requirements analysis).

Product Categories	Product Name	Change Default Credentials	Multi-Factor Authentication	Network Security Settings	Software/Firmware Updates	Privacy Protection	Physical Hardening	Continuous Security Monitoring	Transfer to Another user
Smart Home Security	SimpliSafe Security (Gen 3	x			x	x			x
	Canary Home Security Device				x				x
	Nest Ring Doorbell	x	x	x	x	x	x		x
	August Wi-Fi Smart Lock	x			x			x	x
	Chamberlain Garage Door (myQ)				x				x
	Lockitron Bolt Smart Lock				x			x	
	Logitech Home Security				x	x			
	Lorex NVR (N884)		x	x	x	x	x	x	x
	Philips Hue	x	x		x	x			
Voice Assistants	Amazon Echo (Alexa)	x	x	x	x	x		x	x
	Google Home (Google Assistant)		x	x	x	x		x	x
	Apple Home Pod (Siri)	x	x	x	x	x		x	x
Thermostats	Honeywell Smart Thermostat (RTH9585WF)			x	x		x	x	x
	Keen Home Smart Vent System				x	x	x	x	
	Nest Thermostat		x	x	x	x	x	x	x
Smart lighting	Lutron Smart Bridge		x	x	x			x	x
	Phillips Hue Outdoor Floodlight	x	x		x	x			
Smart Entertainment	Sonos				x			x	x
	Roku				x			x	x
	Apple TV	x	x	x	x	x	x	x	x
	Amazon Fire Stick	x	x	x	x	x		x	x
Smart home monitoring	Moen Flow				x				x
	Nest Protect Smoke and CO detector	x	x	x	x	x	x	x	x
Smart garden	Hydrawise Smart Irrigation Controller	x		x	x			x	x
	Blossom Smart watering controller			x	x			x	x
	Parrot Wireless plant monitor				x	x		x	
	Rachio 3 Smart Controller				x			x	x
Smart baby monitors	inSight Wireless Baby monitor			x	x	x		x	
	Nanit Pro Complete Monitoring System		x	x	x	x		x	

Table 9. Documentation and Resources Review

The findings from the documentation and resources review revealed significant gaps in the support provided by smart home IoT manufacturers in guiding users through device configuration and setup/configuration of security and privacy practices. One critical concern identified in the review was the lack of emphasis IoT manufactures placed on changing default credentials. Changing default credential continues to be one of the most important and one of the most basic

security practices a user can perform. Of the 29 devices reviewed, 38% of the manuals and support materials did not mention or provide instructions on changing the default usernames and passwords. This is very concerning seeing that many smart home IoT device manufactures print the default device username and/or password directly on the IoT device or include it in the user manual and make the manuals available from the internet (Quach, 2018). This omission by IoT manufactures or unawareness by the user could leave smart home IoT devices vulnerable to attacks that exploit default factory-set credentials. Additionally, 45% of the devices evaluated had no mention of multi-factor authentication (MFA) or two-factor authentication (2FA), a security feature that significantly strengthens device security by requiring users to provide an additional layer of verification beyond just a password (e.g. pin number, badge, biometric, token etc.). The review also highlighted several deficiencies in guidance on software and/or firmware updates. Many of the user manuals and support resources did not adequately inform users of the importance of keeping their devices up to date with the latest software updates and/or firmware patches. Another guideline that was underrepresented was privacy protection and continuous security monitoring. Only a few smart home IoT manufacturers evaluated mentioned anything about privacy settings and several had little guidance on how users could actively monitor or update their device's security over time. Only 24% of devices evaluated offered detailed instructions on physical hardening (e.g., placing devices in secure locations to prevent unauthorized physical access). Encouragingly, 72% of the smart home IoT devices evaluated had guidance on transferring the device to a new user or disposing of devices, such as performing a factory reset to remove personal data before selling or recycling the device.

The findings from the requirements analysis phase suggest that while a lot of smart home IoT manufacturers provide relatively clear guidance on user-controlled security and privacy

features, a significant proportion of devices lack the comprehensive guidance needed to empower users to configure user-controlled security and privacy features.

4.2 Phase 2: Usability Testing Results (Verification)

The usability testing phase of this research study focused on understanding user needs, preferences, and behaviors through structured surveys and proficiency test. Two test groups were formed: Test Group #1, which received an installation manual with comprehensive security guidance based on best practices recommended by NIST, NSA, and OWASP, and Test Group #2, which received an installation manual that omitted security guidance and only focused on device setup and features. A total of 64 responses were received, with 32 participants in each test group.

4.2.1 Structured Survey

Surveys were chosen as the tool for capturing participant feedback. The survey began with an initial background section designed to establish a baseline of the test group participants knowledge. Each test group participant was asked about their age group, highest level of education, and several questions to directed at getting a foundational understanding of how comfortable they might be with technology. Table 10 below provides a breakdown of the initial background survey questions asked of the participants.

#	*Survey Questions*	Test Group #1 (Security Guidance Provided) Survey Results	Test Group #2 (No Security Guidance) Survey Results
1	How would you describe your experience with technology?	11% - Novice 49% - Intermediate 40% - Tech Savvy	13% - Novice 58% - Intermediate 29% - Tech Savvy
2	On a scale of 1-5 (1 being not at all, 5 being very), how aware are you of potential cyber security risks associated with using Internet of Things (IoT) devices in your home?	11% - 1 8% - 2 22% - 3 28 - 4 31% - 5	8% - 1 16% - 2 39% - 3 18% - 4 18% - 5
3	Which of the following actions have you taken to secure your Internet of Things (IoT) devices at home (select all that apply)	85% - Strong passwords 76% - Updated Firmware/Software 56% - Disable unused features 62% - Secure home network	71% - Strong passwords 62% - Updated Firmware/Software 26% - Disable unused features 21% - Secure home network
4	Are you familiar with the concept of two-factor authentication (2FA), and do you use it whenever possible to enhance the security of your smart home devices?	25% - Yes, always 67% - Yes, sometimes 6% - No, I'm not familiar 3% - Don't use MFA	32% - Yes, always 58% - Yes, sometimes 5% - No, I'm not familiar 5% - Don't use MFA
5	How often do you review the privacy settings of your smart home devices and adjust them according to your preferences?	14% - Regularly 33% - Occasionally 33% - Rarely 19% - Never	11% - Regularly 39% - Occasionally 32% - Rarely 18% - Never
6	Have you changed the password on your smart home devices since you first purchased and installed the device?	25% - Regularly 42% - When prompted or necessary 28% - Not changed 6% - Don't remember	16% - Regularly 50% - When prompted or necessary 24% - Not changed 11% - Don't remember
7	Have you ever checked the privacy settings on your smart home Internet of Things (IoT) devices and adjusted them to your preferences?	29% - Most of Devices 37% - Some of Devices 34% - Never checked/adjusted	18% - Most of Devices 34% - Some of Devices 47% - Never checked/adjusted
8	Some smart home devices offer guest access options. Do you typically use guest access for anyone outside your household who wants to connect to your smart home devices?	28% - Always Use Guest Access 14% - Uses Guest Access Sometimes 44% _ Never use guess access 11% - Don't know how to enable 3% - Never heard of guest access	24% - Always Use Guest Access 13% - Uses Guest Access Sometimes 39% - Never use guess access 13% - Don't know how to enable 11% - Never heard of guest access
9	How comfortable are you changing the default settings on your smart home IoT devices for increased security (e.g., privacy settings, data sharing preferences)?	37% - Very Comfortable 37% - Somewhat Comfortable 17% - Need Help 6% - Not comfortable at all 3% - Don't know what default setting are	18% - Very Comfortable 45% - Somewhat Comfortable 18% - Need Help 18% - Not comfortable at all 0% Don't know what default setting are

Table 10. Structured Survey Results

The background survey data that was gathered is further broken down per survey question.

Question 1: How would you describe your experience with technology?

Both test groups had a similar distribution of participants who considered themselves novices, intermediates, or tech-savvy users. However, Test Group #1 had a higher percentage of participants identifying as tech-savvy (40% compared to 29% in Test Group #2). This could suggest providing security guidance may boost a user's confidence in their technical abilities, potentially encouraging more proactive engagement with device security and privacy settings. Figure 7 show the test groups awareness of cybersecurity risks.

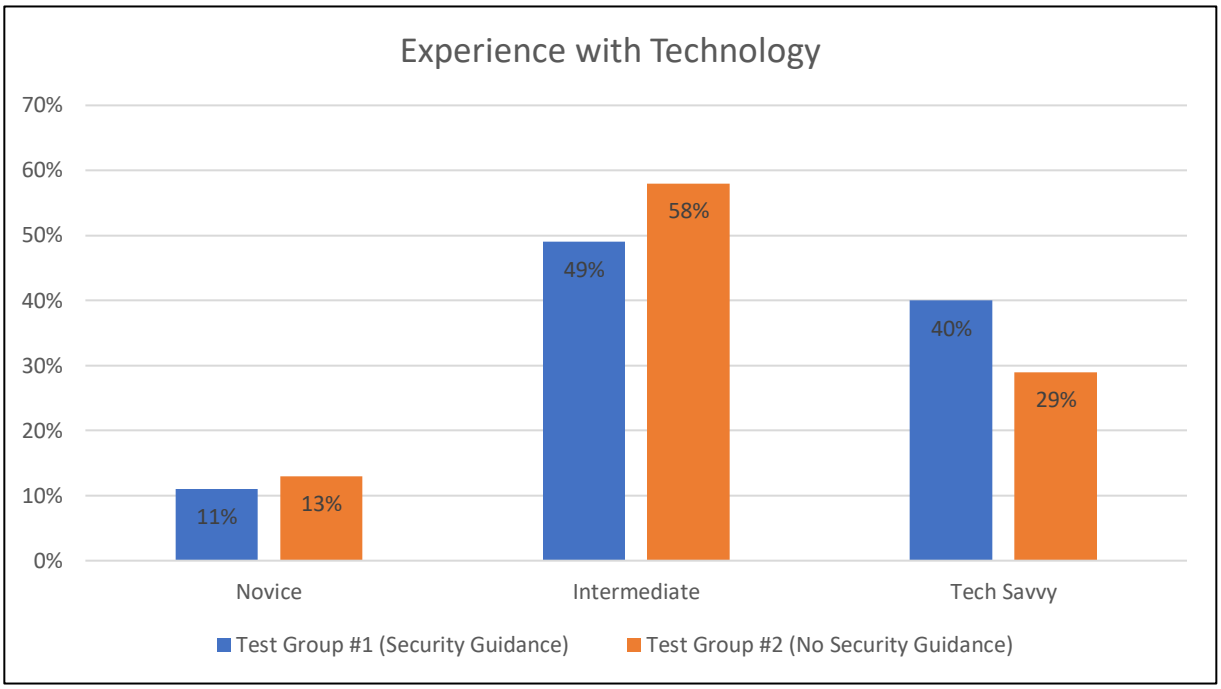


Figure 7. Participant Experience with Technology

Question 2: On a scale of 1-5 (1 being not at all, 5 being very), how aware are you of potential cyber security risks associated with using Internet of Things (IoT) devices in your home?

When asked about awareness of potential cybersecurity risks associated with IoT devices, participants in Test Group #1 reported higher levels of awareness. Notably, 59% of Test Group #1 placed themselves in the high-awareness range (4–5), while only 36% of Test Group #2 did so. Moreover, 19% of Test Group #1 reported low awareness (1–2), compared to 24% in Test Group #2. Figure 8 show the test groups awareness of cybersecurity risks.

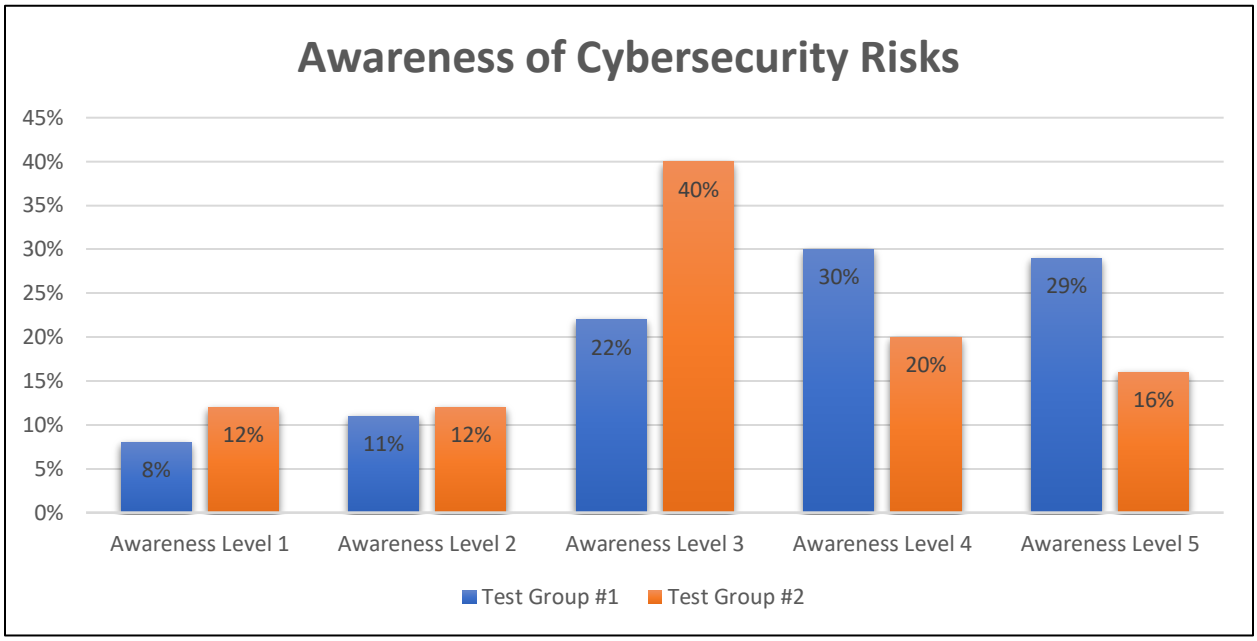


Figure 8. Awareness of Cybersecurity Risks

Question 3: Which of the following actions have you taken to secure your Internet of Things (IoT) devices at home (select all that apply)?

Participants in Test Group #1 were more proactive in implementing security measures. For example, 85% used strong passwords, compared to 71% in Test Group #2. Additionally, 76% of Test Group #1 updated firmware or software, versus 62% in the other group. Notably, 56% of Test Group #1 disabled unused features, a security practice adopted by only 26% of Test Group #2. Furthermore, 62% of participants in Test Group #1 secured their home network, compared to just 21% in Test Group #2. The differences highlighted indicate that security and privacy guidance not only informs users of the potential risks but could also motivate them to take actions in mitigating the risk. Figure 9 shows participants actions taken to secure IoT devices.

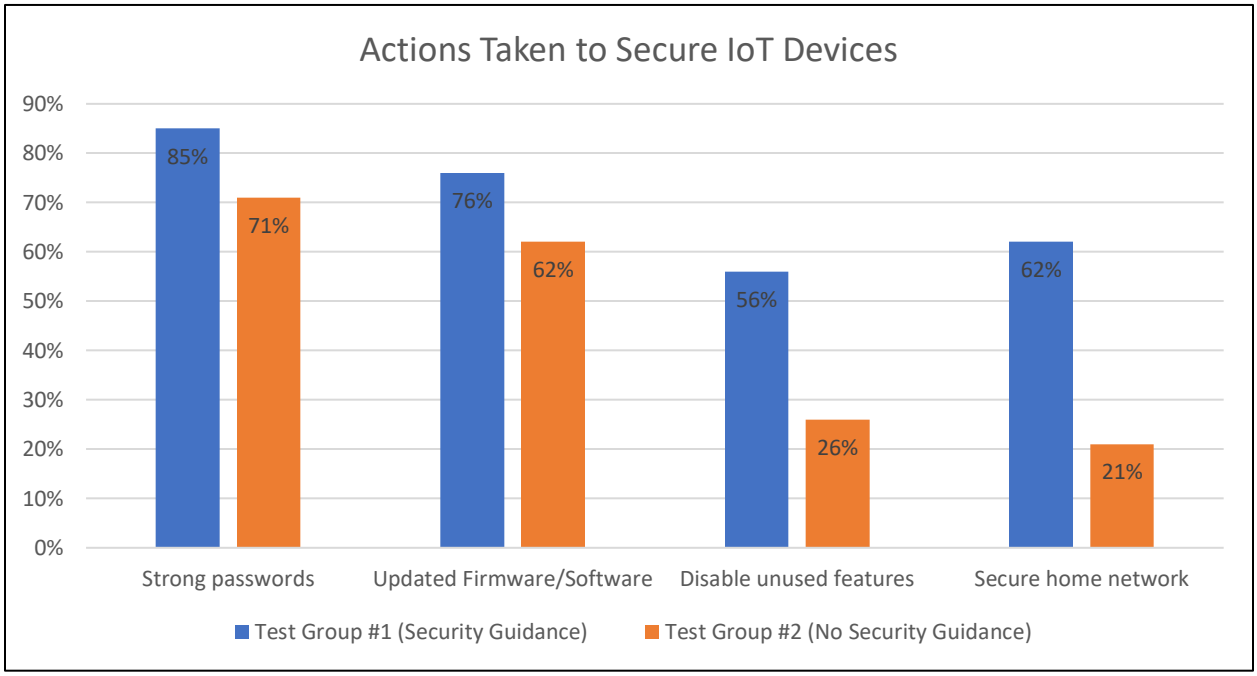


Figure 9. Actions Taken by Survey Participants to Secure IoT Devices

Question 4: Are you familiar with the concept of two-factor authentication (2FA), and do you use it whenever possible to enhance the security of your smart home devices?

Both groups showed similar familiarity with 2FA, but Test Group #1 had slightly fewer participants who always used it (25% compared to 32% in Test Group #2). However, a larger proportion of Test Group #1 used 2FA sometimes (67% versus 58%). This suggests that while awareness of 2FA is relatively widespread across the industry, consistent activation and usage may require more emphasis in security guidance and best practices. Figure 10 shows participant usage with 2FA.

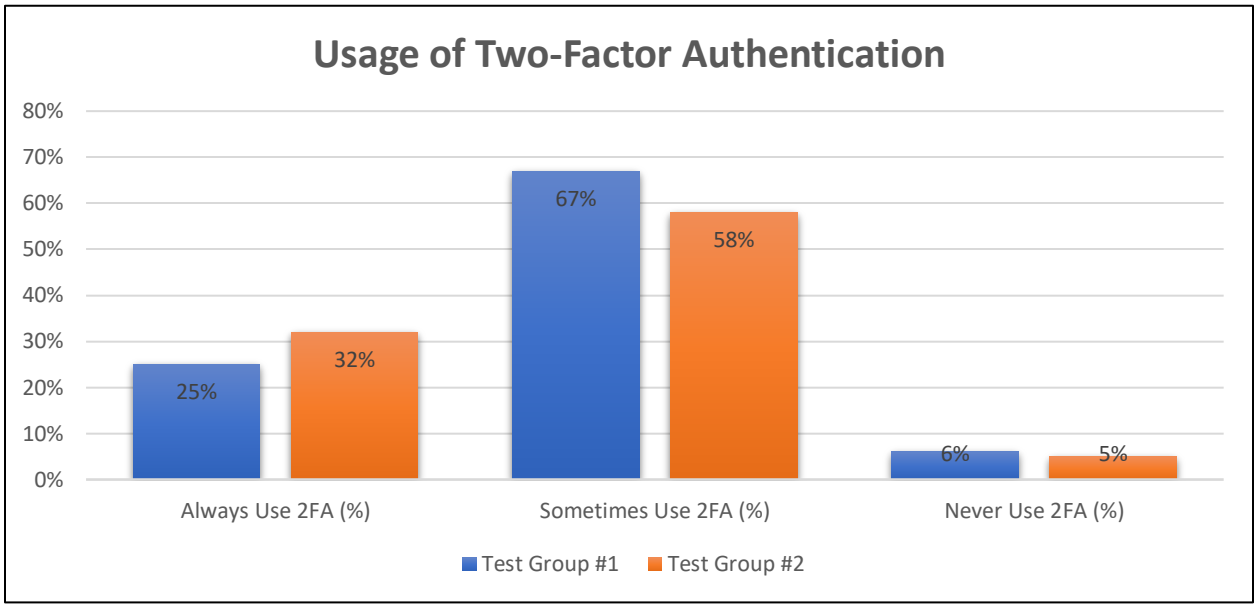


Figure 10. Participant Usage of Two-Factor Authentication

Question 5: How often do you review the privacy settings of your smart home devices and adjust them according to your preferences?

Participants in Test Group #1 were more diligent in reviewing and adjusting privacy settings. 47% of Test Group #1 did so regularly or occasionally, compared to 50% in Test Group #2. While the difference is modest, it indicates that users who are educated on security and privacy best practices tend to be more aware and engaged with the privacy configuration options on smart home IoT devices. Figure 11 shows participant reviewing of privacy settings.

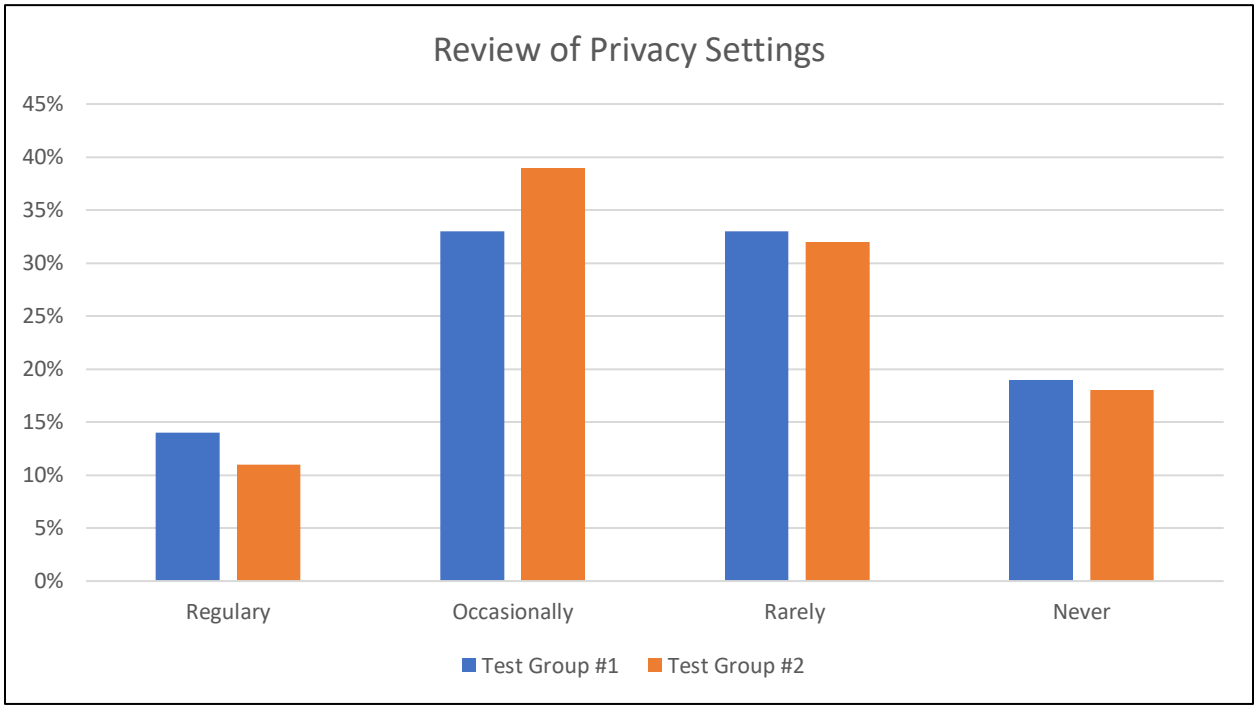


Figure 11. Review of Privacy Settings

Question 6: Have you changed the password on your smart home devices since you first purchased and installed the device?

A higher percentage of participants in Test Group #1 reported changing their device passwords regularly (25% compared to 16% in Test Group #2). Additionally, 42% of Test Group #1 changed passwords when prompted or necessary, slightly less than 50% in Test Group #2. However, fewer participants in Test Group #1 had not changed their passwords (28% versus 24%), and fewer didn't remember if they had (6% compared to 11%). This suggests that clear and comprehensive security guidance may encourage more proactive password management. However, password management continues to be an area where users continue to struggle. Users often resist frequent password changes due to the inconvenience, leading to prolonged use of the same password (Zhang, 2010). Figure 12 shows participant responses to being asked about changing passwords when first purchasing a smart home device.

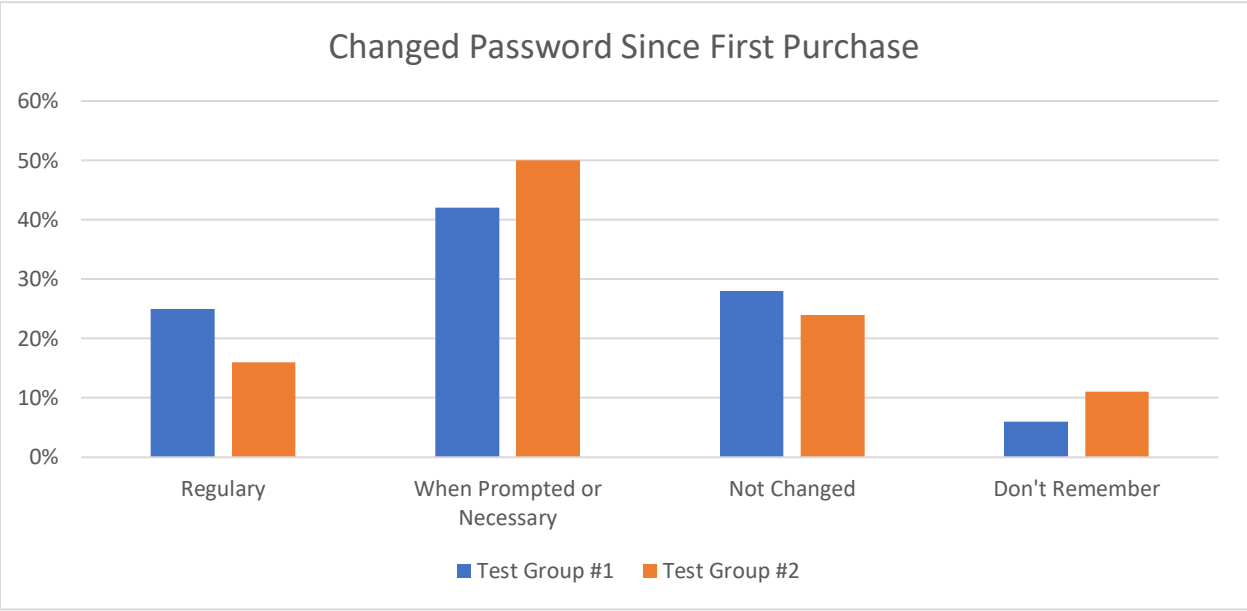


Figure 12. Changed Password Since First Purchase

Question 7: Have you ever checked the privacy settings on your smart home Internet of Things (IoT) devices and adjusted them to your preferences?

When asked if they had checked or adjusted privacy settings, 66% of Test Group #1 had done so on most or some devices, compared to 52% in Test Group #2. Notably, 34% of Test Group #1 had never adjusted privacy settings, whereas 47% of Test Group #2 had not. This indicates that security guidance may increase users' likelihood of understanding and adjusting the available privacy settings to their individual preferences. Figure 13 shows participants responses to checking and/or adjusting privacy settings.

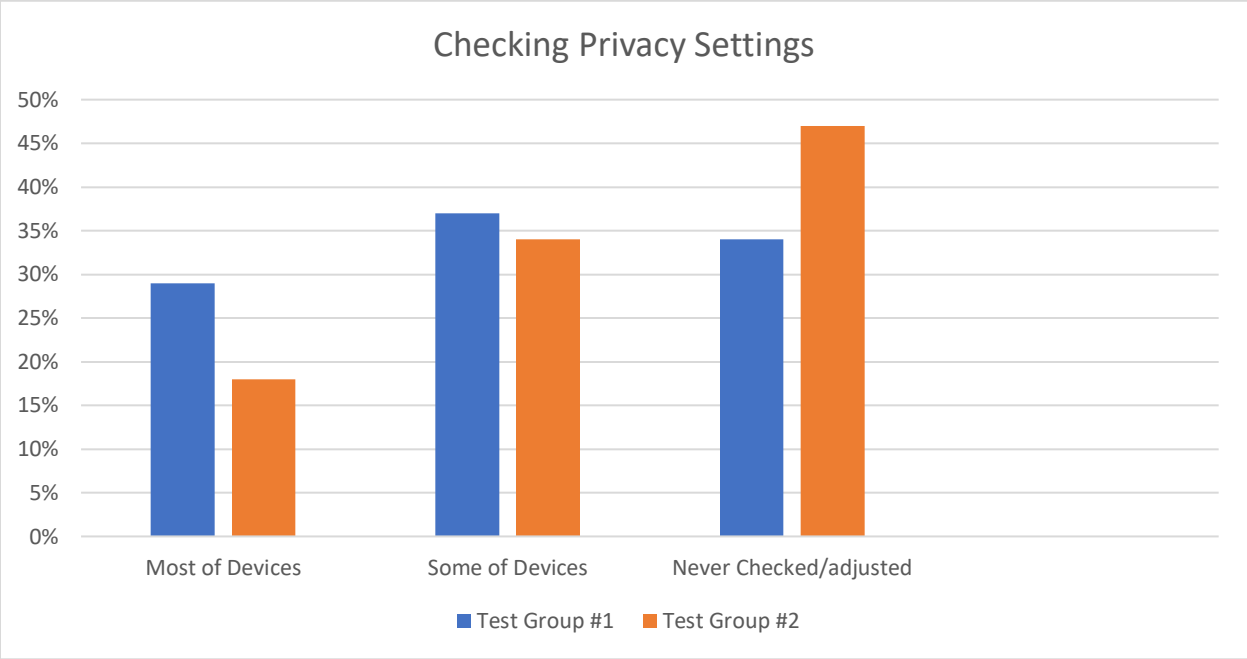


Figure 13. Checking Privacy Settings

Question 8: Some smart home devices offer guest access options. Do you typically use guest access for anyone outside your household who wants to connect to your smart home devices?

The usage of guest access features was somewhat similar between the groups. However, Test Group #1 had slightly more participants who always used guest access (28% versus 24%). Interestingly, a smaller percentage in Test Group #1 had never heard of guest access (3% compared to 11% in Test Group #2). This suggests that security guidance could improve overall awareness of the guest features that are available within home area networks (HAN). Figure 14 show participants understanding and use of guest access in the smart home.

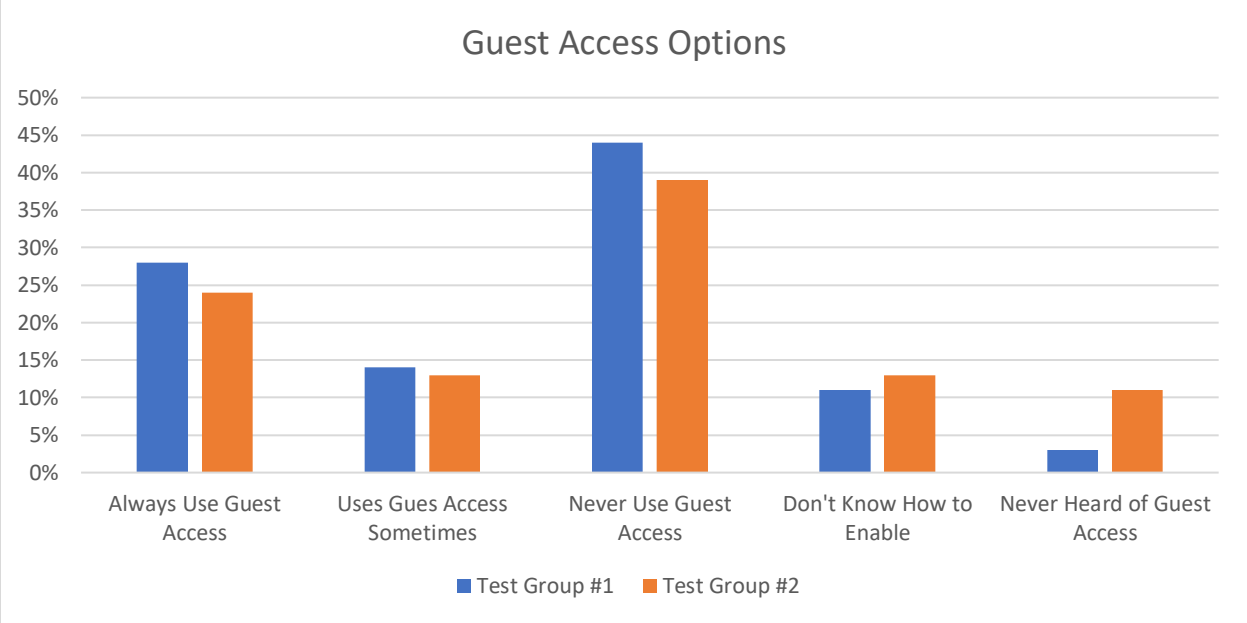


Figure 14. Smart Home Guest Access Options.

Question 9: How comfortable are you changing the default settings on your smart home IoT devices for increased security (e.g., privacy settings, data sharing preferences)?

A significant difference was observed in how comfortable participants felt about changing default settings for increased security. 37% of Test Group #1 were very comfortable, almost double the 18% in Test Group #2. Additionally, fewer participants in Test Group #1 were not comfortable at all (6% compared to 18%). This highlights that security guidance could greatly enhance users' confidence in managing their device settings. Figure 15 shows participants comfortability with changing default settings.

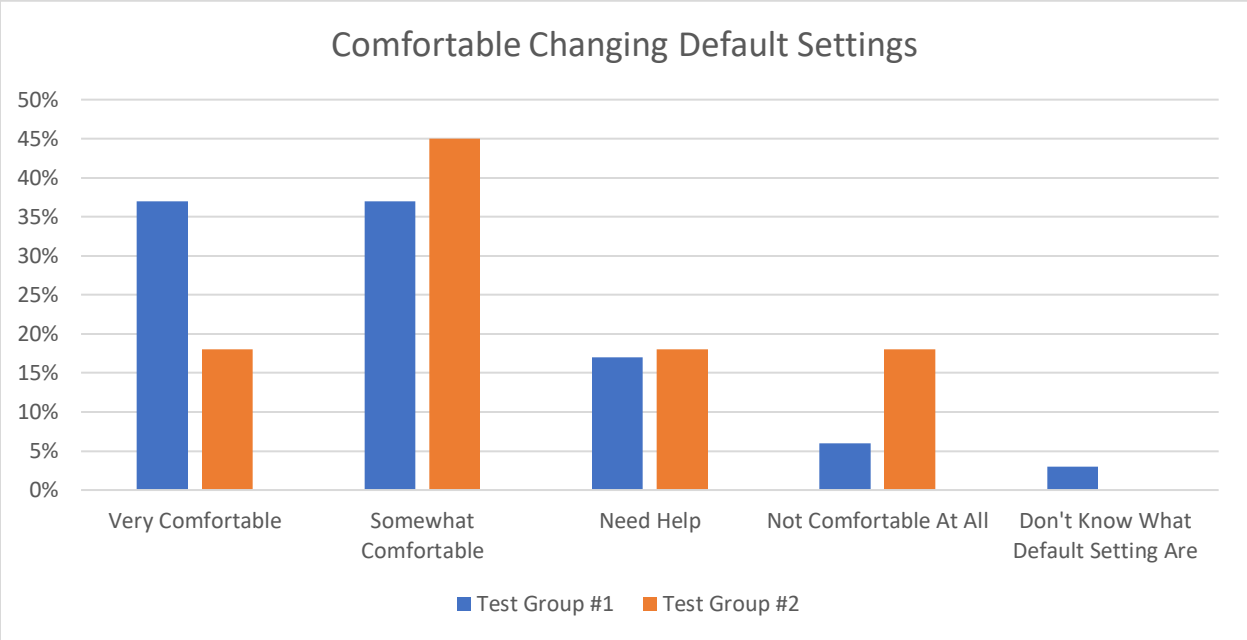


Figure 15. Comfortable Changing Default Settings

4.3 Phase 2: Proficiency Test Results (Validation)

The proficiency test results from this research study offers significant insights into the impact of providing security and privacy guidance on users' ability to understand and implement user-controlled cybersecurity and privacy features in smart home IoT devices. The data indicates a clear disparity in test scores between Test Group #1, which received security guidance in the installation manual, and Test Group #2, which did not receive such guidance. See Table 7.

4.3.1 Analysis of Test Scores

In Test Group #1, the participants' test scores were notably higher, with a substantial number achieving perfect scores. Specifically, out of 32 participants:

- 21 participants scored 100
- 8 participants scored 80
- 3 participants scored 60

The average score for Test Group#1 was 91.25 out of 100.

In contrast, Test Group #2 exhibited a wider range of scores and generally lower performance:

- 6 participants scored 100
- 11 participants scored 80
- 7 participants scored 60
- 2 participants scored 40
- 1 participant scored 20
- 2 participants scored 0

The average score for Test Group #2 was 62.5 out of 100.

Table 11 outlines the proficiency test scores from all participants.

Test Group #1 (Security guidance provided in installation manual)		Test Group #2 (No Security guidance provided in installation manual)	
Participant	Proficiency Test Score	Participant	Proficiency Test Score
1	80	1	80
2	80	2	80
3	60	3	80
4	60	4	80
5	100	5	80
6	100	6	80
7	80	7	80
8	100	8	80
9	100	9	0
10	100	10	100
11	80	11	100
12	100	12	100
13	100	13	80
14	100	14	80
15	80	15	40
16	100	16	60
17	60	17	100
18	80	18	40
19	100	19	100
20	100	20	60
21	80	21	80
22	80	22	100
23	100	23	60
24	100	24	0
25	100	25	80
26	100	26	60
27	100	27	80
28	100	28	80
29	80	29	20
30	100	30	60
31	100	31	60
32	100	32	60

Table 11. Proficiency Test Scores

4.3.2 Statistical Analysis

To determine whether the difference in proficiency test scores between Test Group #1 (with security guidance) and Test Group #2 (without security guidance) was statistically significant, a two-sample independent t-test was performed. This statistical analysis compares the means of two independent groups to assess whether any observed differences are likely due to chance or reflect a true difference between the populations. The t-test calculates the t-statistic using the following formula:

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}}}$$

Where:

- $\bar{X}_1$ and $\bar{X}_2$ are the sample means of Test Group #1 and Test Group #2, respectively.
- S_1^2 and S_2^2 are the sample variances of the two groups, respectively.
- n_1 and n_2 are the sample sizes of the groups, respectively.

Applying this formula to the proficiency test scores, the t-test yielded a p-value of 0.0002, which is well below the conventional threshold of 0.05 for statistical significance. This low p-value indicates a high level of confidence that the difference in mean proficiency scores between the two groups is not due to random variation and it statistically significant. Specifically, the analysis suggests that participants who received security guidance (Test Group #1) performed significantly better on the proficiency test than those who did not receive guidance (Test Group #2). The higher mean score of Test Group #1 reflects a true difference attributed to the presence of clear and comprehensive security instructions. These results reinforce the conclusion that providing detailed security and privacy guidance in smart home IoT installation manuals significantly enhances a

users' ability to understand, comprehend, and implement user-controlled security and privacy features in smart home IoT devices.

4.3.3 Comparative Analysis of Security Practices Between Test Groups

This analysis focused on metrics such as strong password usage, firmware update frequency, disabling unused features, and home network security measures, to create a comparative analysis that provides insights into how well participants in each test group adhered to recommended cybersecurity practices. Out of the test groups, 85% of participants in Test Group #1 consistently employed strong passwords, whereas only 71% of Test Group #2 reported the same practice. Similarly, 76% of Test Group #1 performed regular firmware updates, contrasting with 62% in Test Group #2. The difference is especially striking for disabling unused features, where 56% of Test Group #1 followed this recommendation, versus merely 26% of Test Group #2. Likewise, 62% of Test Group #1 secured their home networks, while just 21% in Test Group #2 took those measures. Figure 16 shows a comparison of security practices between the two test groups.

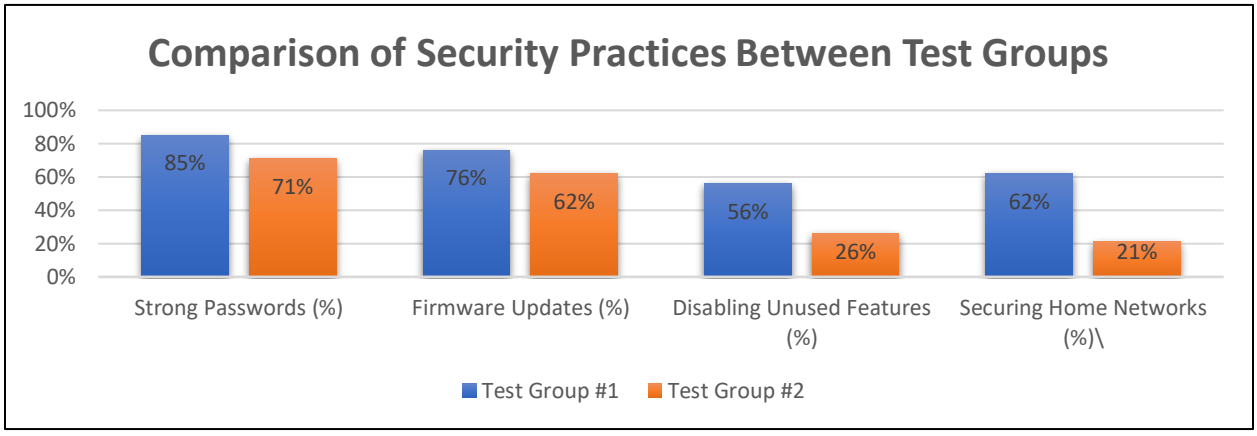


Figure 16. Comparison of Security Practices Between Test Groups

4.3.4 Implications for User-Controlled Cybersecurity and Privacy Features

There is a stark difference in average scores—91.25 for Test Group #1 versus 62.5 for Test Group #2—highlights the significant role that clear and comprehensive security guidance plays in enhancing users' understanding of cybersecurity measures (See Figure 2). The higher scores in Test Group #1 imply that security guidance not only informs knowledge but also boosts users' confidence in managing smart home IoT device settings. With detailed instructions and guidance, users are more likely to comprehend complex security concepts such as setting up secure passwords, enabling multi-factor authentication, and adjusting privacy settings according to their needs. This increased understanding translates into better practical application, as evidenced by the proficiency test results. The lower scores in Test Group #2 indicate that without explicit security and privacy guidance and instructions, users may struggle to grasp the concepts of smart home IoT security and associated risks. The variability in scores, including some participants scoring as low as 0 or 20, suggests that the absence of guidance can lead to users' confusion and/or the misconfiguration of user-controlled security and privacy features. Figure 17 shows a comparison of proficiency test scores.

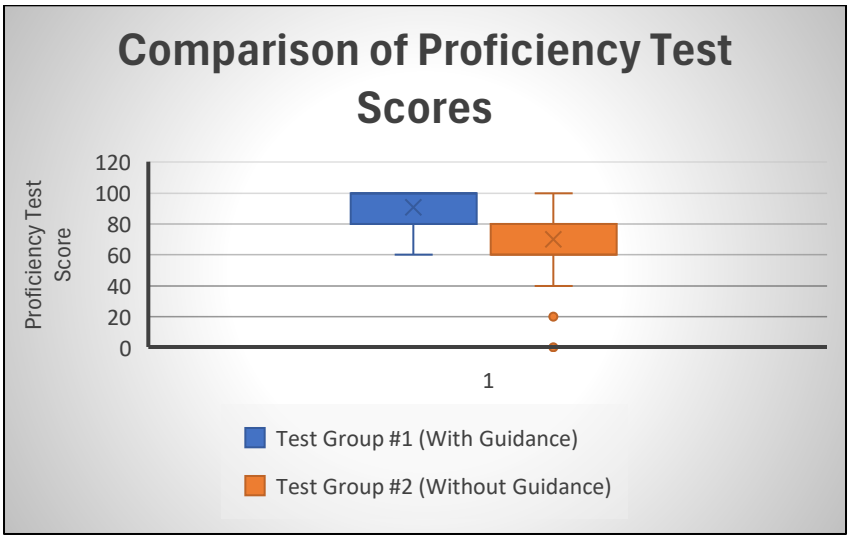


Figure 17. Proficiency Test Score Comparison

4.4 Statistically Reliable Conclusion

Statistical power is the probability that a statistical significance test will correctly identify an effect when one truly exists in the population. A true effect represents a genuine, non-zero relationship between variables, such as a measurable difference between groups or a correlation. High statistical power increases the likelihood of detecting such an effect, while low power reduces this chance, often leading to results that may be influenced by random or systematic errors (Moher, Dulberg, & Wells, 1994). Some of the key factors that may influence statistical power include sample size, effect size, and significance level. To ensure adequate power, researchers often conduct a power analysis, which helps determine the minimum sample size required to reliably detect an effect in a study.

With almost 70 million households in the United States actively using smart home IoT devices, we wanted to establish realistic effect size expectations. To ensure the reliability of this research study's conclusions, a power analysis was performed to determine the necessary effect size for statistically significant results. In alignment with (Cohen, 1988), the three components below were used to conduct the power analysis:

- Expected Effect Size: Theoretical assumption that participants who receive security guidance (Test Group #1) will score a mean of 10 points higher on a 0–100 proficiency scale than those who receive no security guidance (Test Group #2). Assuming both groups share a 15-point standard deviation, the expected effect size can be approximated by:

$$d = \frac{Mean\ Difference\ (10\ points)}{\sigma\ (15\ points)} \approx 0.67$$

- Significance Level (Alpha): 0.05, which represents a 5% risk of a Type I error (false positive).
- Desired Power Level: 80% or higher (industry standard)

Statistical tools were used to calculate for the two independent sample t test:

- Effect Size (d)= 0.67
- Significance Level (a) = 0.05
- Desired Power = 80%
- Allocation Ratio = 1:1 (equal groups)

Results indicate that 74 total participants (37 per test group) would be needed to get the desired power of 80%. However, due to participant availability and time this study settled for 64 total participants (32 per test group). The actual (n) power of the research study was ~75-78%, only slightly below the recommended power of 80. Although 64 participants was just slightly below the desired power of 80%, mini interviews and focus group discussions were used to bolster the research findings, with the goal of the output providing as much value as that of having 74 responses. These user focused discussions allowed participants to elaborate on their individual experiences, not just providing standardized responses in a survey or proficiency test. While in the focus groups, responders had the opportunity to clarify why certain security or privacy settings were ignored or misunderstood and it allowed the researcher to respond with probing questions to

further get to the root of the problem. The qualitative data gathered from the focus groups not only compensates for a reduced power number (~75-78%) but also highlights some of the root causes.

4.5 Survey and Proficiency Test Demographics

The demographic data collected provides important insights into how age and education levels may influence a users' engagement with user-controlled cybersecurity and privacy features in smart home IoT devices. By comparing Test Group #1 (who received security guidance) with Test Group #2 (who did not receive security guidance), we can discern patterns that suggest how these factors impact users' ability to understand and implement user-controlled security features.

4.5.1 Age Distribution

In Test Group #1, the largest age group was 35-44 years, accounting for 36% of the participants, followed by 25-34 years at 22%, and 45-54 years at 19%. Notably, 17% of participants were 65 years or older, which is slightly higher than the 13% in Test Group #2. In contrast, Test Group #2 had a higher percentage of participants in the 18-24 years bracket (8% compared to 3% in Test Group #1). There was also a higher representation of older adults (55 years and above) in Test Group #1 over Test Group #2. On the other hand, the younger demographic (18-34 years) tends to be more tech-savvy and may feel more comfortable navigating technology without additional guidance. However, the presence of security and privacy guidance still positively influenced their engagement with security and privacy features, as evidenced by the proficiency test results. This indicates that regardless of age, users can benefit from clear and comprehensive guidance when it comes to implementing user-controlled privacy and security features. See Figure 18 for the Age Distribution of Survey and Proficiency Test Participants.

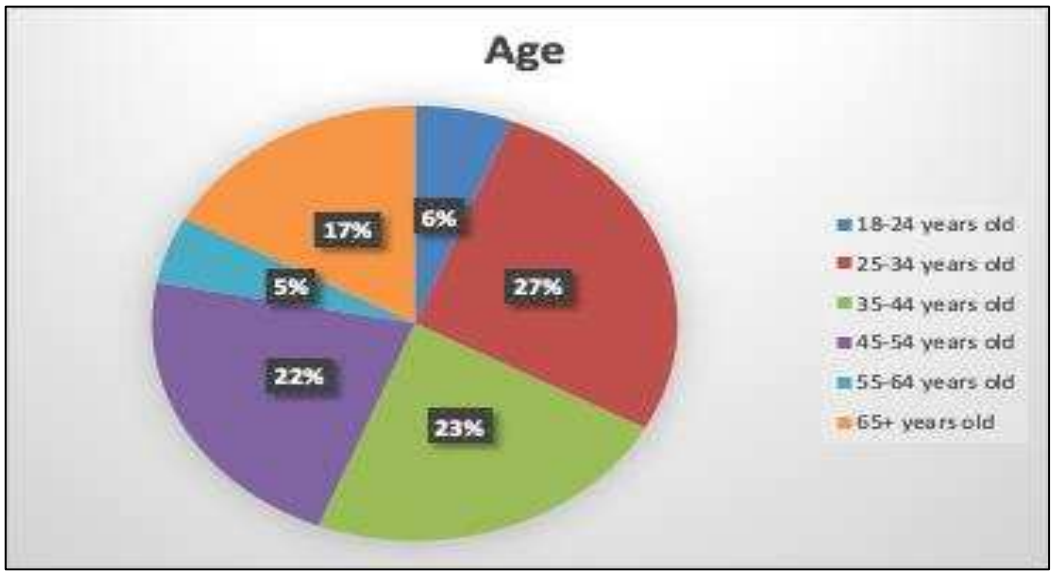


Figure 18. Age Distribution of Survey and Proficiency Test Participants

4.5.2 Education Levels

Overall educational attainment appears to have a significant impact on users' interaction with security features. In Test Group #1, a substantial 67% of participants held a graduate or professional degree, compared to 42% in Test Group #2. Additionally, Test Group #1 had fewer participants with only some college but no degree (8% versus 21% in Test Group #2). Participants with higher education levels may possess better critical thinking skills and a greater ability to comprehend complex information, including technical instructions related to cybersecurity (Hargittai, 2013). The higher proportion of well-educated participants in Test Group #1 might have contributed to a more effective use of the provided security guidance. However, the guidance also likely played a crucial role in assisting participants across all education levels in Test Group #1, enabling them to understand and apply necessary security and privacy measures more effectively than those in Test Group #2.

For participants with lower educational attainment, the absence of security and privacy guidance in Test Group #2 may have exacerbated some difficulties in understanding security and privacy

settings. This underscores the importance of providing clear, accessible instructions that cater to users with diverse educational backgrounds. By simplifying technical jargon and offering step-by-step guidance, smart home IoT manufacturers can make cybersecurity and privacy practices more approachable for all users. See Figure 19 for the education distribution of survey and proficiency test participants.

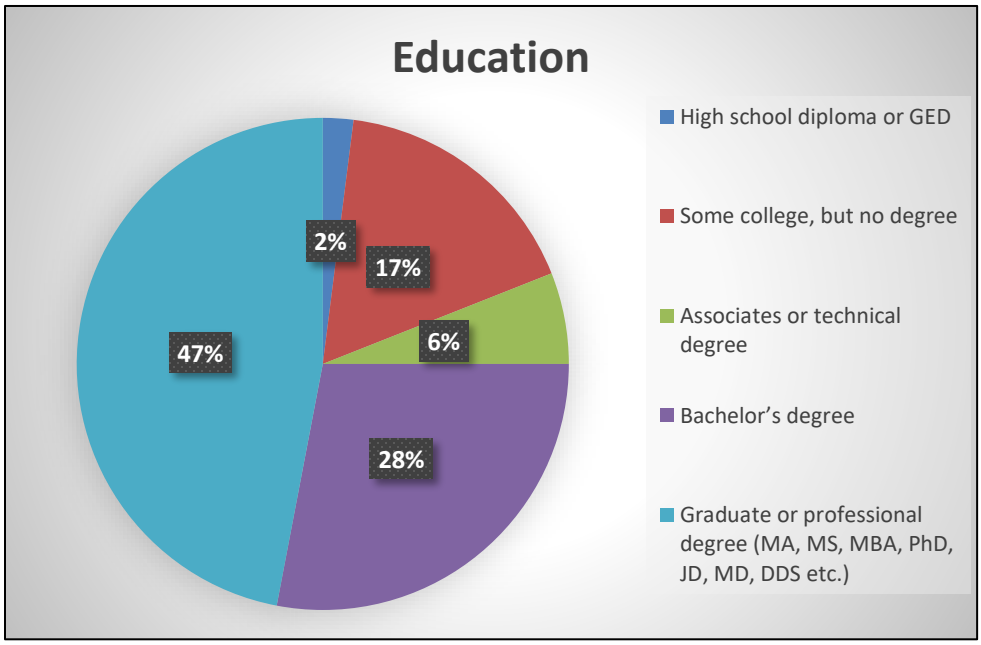


Figure 19. Education Distribution of Survey and Proficiency Test Participants

4.5.3 Implications for User-Controlled Security and Privacy Features

The demographic differences between the two test groups highlights the critical role that tailored security and privacy guidance can plays in enhancing users' engagement with cybersecurity and privacy features. The data suggests that both age and education can influence a users' comfort, proficiency with the technology, understanding of the associated risk with smart home IoT devices. For older adults and those with lower educational levels, comprehensive and easy-to-understand security guidance is could be essential to ensure everyone using smart home

IoT device has the same baseline level understanding. Smart home IoT manufacturers should consider the following:

- Simplified Language: The use plain simple language (layman's terms) and avoiding technical jargon help making security and privacy guidance and user instructions more accessible and comprehensible.
- Visual Aids: The use of visual aids like diagrams, icons, and other visual elements to support textual instructions and help with a users' comprehension.
- Step-by-Step Instructions: Breaking down smart home IoT configuration, security, and privacy processes into manageable steps help guide users through the completion of device configurations.
- Cultural Sensitivity: Ensure that support materials provide by the manufacture are inclusive and considerate of diverse user backgrounds or notify users where additional support material can be found.

For younger users and those with higher educational attainment, security and privacy guidance is just as important and it should not be assumed that they will secure their smart home IoT devices according to industry best practices. While a user may be more familiar with technology, explicit instructions can reinforce best practices and alert them to specific risks associated with smart home IoT devices that they may not have considered or may not have encountered in the past. Data from this research study has shown that even the most "tech-savy" participants still made mistakes or didn't know that certain security and/or privacy guidance had changed or been updated.

Overall, the demographic data analysis underscores that effective security and privacy guidance can benefits users across all age groups and education levels. By recognizing and

addressing the diverse needs of the smart home IoT user base, smart home IoT manufacturers can develop more intuitive and accessible products that cater to users of all technical skill levels.

4.6 Phase 3: Focus Group User Feedback

Phase 3 of this research study conducted a technical deep dive with a focus group of seven volunteer participants to discuss data received and barriers they have personally experienced with applying user-controlled security and privacy features. The focus group objectives were to explore the challenges, needs, and preferences of users regarding the application of user-controlled security and privacy features. The interview session was centered around the following topics:

- Challenges in Following Security Guidance
- Suggestions for Improving IoT User Manuals
- The Role of Visual Aids in Security Guidance
- Additional Support for User-Controlled Security Features

The tables below present the findings and feedback from the Focus group user feedback interview session.

What challenges have you faced when trying to follow security guidance?	
Participant #	**Participant Feedback**
Participant 1	Getting a full understanding of the security challenge, what will happen, and what will be the impact if you don't follow instructions.
Participant 2	Annoying always having to change passwords. Always defer changing password until the last possible time.
Participant 3	Understanding the lingo. Sometimes guidelines are writing in high technical language. I find myself having to "Google It" to understand what it is telling me to do. Not given a clear step-by-step on what needs to happen.
Participant 4	If the instructions are too long, I'm not going to read them. My husband usually sets up our computer stuff, so I feel I have not had the chance to setup much of anything, so I feel I have not had the opportunity to run into any many security roadblocks. Someone else always helps me with setup.
Participant 5	Work systems make you change my password every month and passwords updates are required after systems updates. I usually write down the passwords so I can remember, or I use common things like family names and birthdays. The password requirements (length requirements) are annoying.
Participant 6	I didn't know what to do so I got someone else to do it for me.
Participant 7	Minimal, I usually can follow the instructions. I really don't need too much help or guidance.

Table 12. Focus Group Feedback: Challenges in Following Security Guidance

How could an IoT user manual be modified to better support you?	
Participant #	**Participant Feedback**
Participant 1	Identifying the different parts of the item. Add pictures with the instructions.
Participant 2	Wish the manual was more simple [sic] and more interactive would be more useful. Videos or something more interactive For example: The Ikea manual is way to [sic] confusing. Having a video is a lot better. A lot of the manual are very complicated and require too much reading.
Participant 3	Make the language plainer. Make the language clearer. Provide explanations, definitions, Step-by-step process, Screenshots of steps.
Participant 4	Be concise, not wordy, straight to the point. Bullet points
Participant 5	Use terminology that normal people can understand. Turn the user manual into a YouTube how to guide. I'm more of a visual learner.
Participant 6	Cyber security for dummies. A lot of manuals don't have visuals. Some do some don't. The visual help me acclimate the wording with what I need to do. I think visuals should be mandatory for all manuals.
Participant 7	Diagrams with step by step instructions.

Table 13. Focus Group Feedback: Suggestions for Improving IoT User Manuals

What type of visual aid could be added to security guidance to help understanding?	
Participant #	**Participant Feedback**
Participant 1	Pictures identifying different parts More examples, correct way and wrong way of doing something.
Participant 2	Someone explaining it to you or someone showing you how to do it. Not just talking tech terms. Break it down kindergarten style.
Participant 3	Images, screen shots of the item to help step through the process.
Participant 4	The most important screens that I am supposed to see in order to make the changes and I'm not questioning if I'm taking the right steps. Make it clear I'm not making mistakes.
Participant 5	Videos or a power point presentation to help explain the information.
Participant 6	Videos, audio, demonstrations. Flip chart would be cool too. Photographs work but they need to be more in-depth photographs with labels.
Participant 7	Pop up features, to show you exactly where something is.

Table 14. Focus Group Feedback: The Role of Visual Aids in Security Guidance

What additional information or support would increase your confidence in applying user-controlled security features?	
Participant #	**Participant Feedback**
Participant 1	More instructions on how to back up files or other means of securing documents. Have a hard time locating documents that are archived. Instruction of file path to help with finding things later. Would like to see an option to print the file path of a document at the bottom of the page when printing so you know the source of the file. File going to the Downloads folder vs a different folder.
Participant 2	"If there was a way to make it more automated. I find it to be an inconvenience. Software updates popup at the most unconfident times. Things that don't require me to do to [sic] much for me to implement it."
Participant 3	Additional information - other tools, video tutorials to explain the additional features. To make me more aware and knowledgeable vs just reading the lingo would be more supportive for my confidence levels. Help me to walk through those steps. Better risk awareness.
Participant 4	Stressing the importance of the personal safety aspect of it and making it more of a standard process that you have to due [sic] vs something that is optional. In order to properly user the device, safety features are required vs you can setup the device but if you want to make it secure, you have to do this.
Participant 5	A "How to" manual in the form of a video
Participant 6	Having a partner or someone else to help. I need guidance from someone else I trust to feel more confident.
Participant 7	Reminder that I need to do something. Popup around the time when something needs to be done.

Table 15. Focus Group Feedback: Additional Support Needed

The participants in the focus group provided valuable insights into some of the challenges, barriers, and frustrations they personally face or have faced when applying user-controlled cybersecurity and privacy features in smart home IoT devices or systems. Participants highlighted

several key issues that impede their ability to effectively configure security and privacy settings, which has significant implications for both users and smart home IoT manufacturers. One of the predominant themes that emerged from the focus group discussion was the difficulty in understanding technical language and jargon smart home IoT manufactures use in instruction manuals, support documentation, and security and privacy guidance. Participants expressed their frustration with instructions that are written in highly technical language, making it challenging for a non-technical person (or “regular person”) to comprehend and follow the steps required to secure smart home IoT devices. For example, Participant 3 mentioned needing to "Google" certain terms to understand the guidance, indicating that the complexity of language can be a significant barrier. Similarly, Participant 1 emphasized the importance of understanding not just the steps, but also the implications of not following security instructions, suggesting that users need clear explanations of the risks involved in not following through with security and privacy best practices. Another major challenge identified was the perceived inconvenience and annoyance associated with security practices, particularly password management. Participants 2 and 5 expressed frustrations with the frequent need to change passwords and the password complexity requirements (e.g. minimum password length, special characters, etc.). This sentiment reflects a common user attitude where security measures are seen as obstacles rather than protective measures, potentially leading to security fatigue and poor security behaviors, such as using weak passwords, reused passwords, or just writing down all passwords (likely in an unsecure manner). The focus group also revealed that overly complex or lengthy instructions can deter them from going through all steps and completing a potentially secure smart home IoT device or system configuration. Participant 4 admitted to not reading long instructions and relying on someone else to set up devices, while Participant 6 simply delegated the task to a family member due to a lack of

understanding. This reliance on others or avoidance of security and privacy guidance underscores the need for user-friendly manuals that cater to users with varying levels of technical proficiency.

In terms of improving smart home IoT user manuals, participants overwhelmingly suggested the inclusion of visual aids and the use of simpler language. Many participants advocated for manuals that incorporate pictures, diagrams, and screenshots to provide a clear, step-by-step guide through the Smart Home IoT device setup and configuration process. For example, Participant 1 recommended adding pictures to identify different parts of the IoT device, while Participant 2 expressed that visual aids like those in an Ikea® manual are way too confusing. The desire for video tutorials and more interactive forms of guidance was also prominent, with Participants 2, 5, and 6 expressing a preference for visual and auditory learning tools over just adding more text to what the manuals already provide. The role of visual aids was further emphasized when participants discussed what types of visual support would enhance their understanding of security and privacy guidance. Visual aid suggestions included examples of correct and incorrect methods of performing a task (Participant 1), videos or demonstrations to break down complex concepts (Participants 2 and 6), and pop-up features that guide users through configurations in real-time (Participant 7). These insights highlight the importance of multimedia resources in making security information more accessible and engaging for users.

As it relates to additional support needed to increase confidence in applying user-controlled security features, participants expressed a need for features that reduce the burden on the user and provide ongoing assistance. Participant 2 expressed their desire for more automation in security updates to minimize inconvenience, while Participant 7 suggested reminders for when security actions need to be taken. Participant 4 highlighted the importance of framing a secure configuration as a standard part of device setup rather than an optional step, which could encourage more users

to engage with user-controlled features. The need for risk awareness education was also noted, with Participant 3 indicating that understanding the potential risks would increase their confidence in applying security measures.

These findings suggest that smart home IoT manufacturers should reconsider how they present security guidance to consumers. Technical jargon and complex instructions could alienate users, leading to an underutilization of critical user-controlled security and privacy features.

4.7 Focus Group Technical Deep Dive Analysis

Due to the lower statistical power in the quantitative phase of the research study (below 80%), focus groups were used to bolster the research findings. This section outlines and discusses the group-size appropriate t-tests and analysis of variance (ANOVA) analysis that were performed to detect underlying patterns in user behavior and comprehension that may not have been clear just by using the quantitative data.

Focus group responses were collected and categorized into four key themes:

1. Challenges Faced – Any reported difficulties in following security guidance.
2. Manual Improvement – Suggestions for enhancing the provided user IoT device manuals.
3. Visual Aid Importance – Desire for visual materials (e.g., images, diagrams, videos) to help in understanding security guidance.
4. Additional Support Needed – Any other request for additional support.

In preparation for the analysis, all focus group feedback responses were given a numerical score using a 1-5 Likert scale, where 1 represents disagreement and 5 represents agreement. Final datasets are provided in the Tables below:

Participant #	Challenges Faced	Manual Improvement	Visual Aid Importance	Additional Support Needed
1	3	4	5	4
2	2	3	5	3
3	4	4	4	4
4	1	3	3	3
5	2	3	5	5
6	1	3	5	3
7	4	2	3	2

Table 16. Focus Group Feedback Dataset

ANOVA Analysis

	Challenges Faced	**Manual Improvement**	**Visual Aid Importance**
Results	F-statistic of 5.64 with a p-value of 0.0045.	F-statistic was 2.93 with a p-value of 0.079	F-statistic was 3.38 with a p-value of 0.091
Interpretation	Statistically significant difference among the categories when "Challenges Faced" is considered, suggesting that user difficulties differ markedly from their suggestions for manual improvements, visual aid importance, and additional support.	Level of emphasis on improving manuals is not as distinct as other aspects.	Little difference in user perceptions regarding the need for visual aids versus additional support

Table 17. ANOVA Analysis from Focus Group Feedback

T-Test Analysis

	Challenges vs. Manual Improvement	**Challenges vs. Visual Aid Importance**	**Challenges vs Additional Support Needed**	**Manual Improvement vs. Visual Aid Importance**	**Manual Improvement vs. Additional Support Needed**	**Visual Aid Importance vs. Additional Support Needed**
Results	t = -1.97 p = 0.073	t = -3.93 p = 0.002	t = -2.04 p = 0.064	t = -2.47 p = 0.029	t = -0.31 p = 0.765	t = 1.84 p = 0.091
Interpretation	Near-significant	Significant	Significant	Statistically Significant	No Significant Difference	Significant

Table 18. T-test Analysis from Focus Group Feedback

Results from the ANOVA and t-test (Table 15 & 16) analysis reveal significant differences, especially between Challenges Faced and Visual Aid Importance. This analysis suggests that users encounter difficulties in understanding security instructions and that they place high value on

visual aids to help them overcome these difficulties. Although some comparisons (e.g., Manual Improvement vs. Additional Support Needed) did not yield statistically significant differences, the overall findings underscore the need for clearer, more consumer-friendly documentation and support materials from smart home IoT manufacturers.

4.8 Chapter Summary

Chapter 4 presented the results and data analysis of this research study. Conducted in two phases, the research first established a set of standards and best practices drawn from industry authorities like, NIST, OWASP, NSA, Matter. A review of existing smart home IoT user manuals and other support resources revealed significant gaps between IoT security and privacy best practices, and the actual guidance provided to consumers through manufacture provided documentation. Usability testing through surveys and proficiency tests (verification and validation) demonstrated that users who received comprehensive security instructions exhibited a higher proficiency in configuring security settings, greater awareness of security risks, and increased confidence in managing device security. Statistical analysis confirmed the significance of these findings, underscoring the impact of clear and comprehensive security and privacy guidance.

In the second phase, a focus group of 7 participants provided deeper insights into the some of the challenges they have personally faced when applying user-controlled security and privacy features. Participants reported difficulties with technical jargon, the inconvenience of frequent password changes, and a lack of clear, step-by-step instructions. Many participants expressed preferences for simplified language, visual aids like diagrams and videos, and more interactive forms of guidance to assist them. This qualitative feedback highlighted the importance of catering to users with varying levels of technical expertise. The next chapter presents the interpretation of

the research findings (broken out into themes), contributions to systems engineering and cybersecurity, recommendations for future research, and conclusion.

CHAPTER 5. DISCUSSION AND CONCLUSIONS

5.1 Interpretation of Research Study Findings

This research study applied systems engineering principles and cybersecurity best practices to evaluate the varying degrees of support consumers/end-users receive from smart home IoT manufacturers, in the deployment, configuration, and ongoing maintenance of user-controlled security and privacy features. The research study identified six key themes that have a major effect on the application and configuration of user-controlled security and privacy features in smart home IoT devices and systems. The themes identified are below:

Theme 1: Importance of Clear and Comprehensive Guidance. The first theme highlights that providing clear and comprehensive security and privacy guidance in smart home IoT user manuals and other support resources significantly enhances a users' ability to understand, configure, and implement user-controlled security and privacy features. The research study findings show that test group participants who received detailed instructions that included security and privacy guidance not only performed better in the proficiency tests but also showed more awareness of security and privacy risks when they were questioned. This theme leads to the conclusion that, smart home IoT manufacturers have a significant responsibility to ensure their documentation and/or online support resources thoroughly addresses and covers all user-controlled security and privacy features available with their product.

Theme 2: Impact of Technical Jargon and Complex Instructions. The second theme explores deeper into how technical jargon and complex instructions can act as a barrier to effective user engagement in applying and configuring user-controlled security features. During the technical deep dive, participants reported feelings of frustration and confusion when confronted with user manuals that contained technical terminology without providing any clear explanations

on what terms meant and/or the associated risk impact to them or their systems. For example, certain terms like "encryption protocols" or "network segmentation" without proper context can overwhelm users who do not have a technical background. The research study also highlighted that simplifying language and providing definitions for unavoidable technical terms can greatly enhance user comprehension. By presenting security and privacy information in a more accessible manner, smart home IoT manufacturers can reduce the cognitive load on users, making it easier for them to understand and act upon the critical user-controlled security and privacy features that keep smart home devices, networks, and systems secure.

Theme 3: Role of Visual Aids and Interactive Resources. The third theme centers on how visual aids and other interactive resources are powerful tools in enhancing a user's understanding and engagement with user-controlled security and privacy features. Technical deep dive participants expressed a strong preference for manuals and other available resources that included diagrams, flowcharts, screenshots, and video tutorials. Notably, one participant even suggested that IoT manuals should be like Ikea® instructions. The research study suggests that incorporating more visual aids not only helps in comprehension of the material but also increases user satisfaction and the likelihood of users fully utilizing the user-controlled security and privacy features available to them. Interactive resources, such as online tutorials or apps that guide users through a step-by-step setup process, were also highly valued by participants.

Theme 4: Challenges with Password Management and Security Practices. Password management surfaced as a common struggle among users, with participants expressing annoyance at the complexity and frequency of password changes required in their personal experience using smart home IoT devices. Many participants admitted that they have at times resorted to insecure practices such as reusing passwords across multiple devices, using family names (easily found on

social media), or writing them down in easily accessible places like sticky notes or spreadsheets. The research study indicates that these behaviors might stem from a lack of understanding of the importance of strong, unique passwords and the perceived inconvenience of managing them. To address this continuous issue, smart home IoT manufacturers could provide educational materials explaining the risks associated with weak passwords and/or offer practical solutions, such as built-in password managers or guidance to help users in creating strong yet memorable passwords. By simplifying the process and highlighting this importance, users may be more motivated to adopt better password practices.

An additional challenge within the area of password management is the tendency of users to overlook the importance of changing default usernames and passwords when first setting up new smart home IoT devices. The research study revealed that many users either assume the default credentials are sufficient or are unaware of the security risks associated with leaving them the way the device came. Default login information is often well-known or easily discoverable by performing a simple "Google®" search of the IoT device to find the default credentials. This issue is further exacerbated when smart home IoT manufacturers do not highlight the importance and need to change default settings upon initial setup. By not emphasizing this critical step, users will likely just proceed with smart home IoT device setup without realizing they are leaving a significant security gap in place that could be exploited. To address this issue, technical deep dive participants recommended that smart home IoT manufacturers mandate the creation of unique usernames and strong passwords during the initial setup process, accompanied by clear, concise instructions with explanations of the potential risks of not doing so. One participant commented, "Just build it into my setup process". By integrating this security best practice into the requirements

of the initial setup process and providing supportive guidance, users are more likely to take the necessary action to secure their devices from the outset.

Theme 5: Necessity of User-Centric Design in Security Guidance. Adopting a user-centric design approach in security and privacy guidance is crucial for effectively bridging the gap between smart home IoT best practices and the various capabilities of users to understand and configure them. This type of strategy would require a deep understanding of users' needs, preferences, and potential pain points when interacting with smart home IoT devices. The research study demonstrated that when smart home IoT manuals are crafted with the user in mind, they are more inclined to engage with the material and successfully implement user-controlled security and privacy features. One key aspect of the user-centric design is recognizing that all consumers/end-users have different levels of technical proficiency, learning preferences, and attention spans. To adjust to this diversity of users, smart home IoT manuals, setup guides, and other manufacture provide resources should employ a layered design, where security recommendations are divided into separate, manageable sections. This layered structure would allow users to focus on one aspect of security or privacy at a time, this could help the user by making the information received more digestible and less overwhelming. For example, a IoT manufactures might organized installation, configuration, and security guidance into different topics such as "Getting Started with Basic Security," followed by more advanced sections like "Enhancing Device/Network Security with Advanced Settings." By prioritizing initial security and privacy needs, users should be able to address critical actions right away, things like changing default usernames and passwords, during the initial setup process. Subsequent sections can further delve into additional features like configuring custom privacy settings, enabling multi-factor authentication, disabling unused features, or setting up virtual private networks. This type of layered approach to security and

privacy settings can empower users to progress at their own pace, returning to explore more complex security and privacy features as their understanding and confidence grow. To further enhance usability, smart home IoT device manuals can customize and incorporate visual aids and interactive elements. These might include:

- Step-by-Step Guides with Illustrations: Visual depictions of each step to configure and secure devices can help users follow along more easily.
- Summary Checklists: End-of-section checklists can help users confirm they've completed essential tasks to configure and secure the smart home IoT device.

By embracing a user-centric, layered design in security guidance, smart home IoT manufacturers can significantly enhance user engagement and comprehension with user-controlled security and privacy features. This approach acknowledges that securing a smart home IoT device is not a one-time event but an ongoing process that evolves with the user's comfort level and needs.

5.2 Novelty of the Research Study

The novelty of the research study is the user-centric and systems engineering perspective focused on bridging the gap between recommended security best practices or interoperability frameworks such as NIST, NSA, OWASP, and Matter—and how consumers/end-users receive, understand, implement and maintain user-controlled security and privacy features. Where other standards focus either on technical solutions or on ensuring device interconnectivity (Matter), this research study examines real world documentation and other support resources smart home IoT manufacturers provide to consumers/end-users and: evaluates the usability of each recommended step, and then proposes iterative improvements informed by direct end-user feedback following systems engineering methodologies. Table 19 below highlights how many of the well-recognized industry standards and/or frameworks differ from this research study.

Focus Area	This Research Study	Matter	OWASP	NSA	NIST
Primary Scope	Evaluates user-controlled security and privacy features in smart home IoT from a consumer usability perspective	Interoperability standard (cross-ecosystem device compatibility)	IoT vulnerability lists & best practices with a focus on software development	Advisories on large-scale or national security best practices. Released Home network best practices	High-level security frameworks, often enterprise or gov
Unique Value	User-centric systems engineering approach verifying IoT device manuals (and other resources), user comprehension, and feature adoption, resulting in tangible, user-focused design improvements	Ensures IoT device brand compatibility (where supported)	Identifies typical IoT vulnerabilities from a code and architecture standpoint	Sends alerts to large-scale threats, fosters broad security posture	Establishes industry-wide or national standards
Attention to User-Centric Design	Conducted surveys, proficiency test, and focus groups to measure user comprehension, pain points, and difficulties with user-controlled security and privacy features	Ensures a uniform IoT experience, but not an in-depth security guidance	Guidance on user-centric design as it relates to IoT device development	Emphasized threat alerts, not user design or user guidance	Limited, focuses on compliance & controls
Practical Guidance for End-Users	Directly links best practices with “real world” user guidance and addresses gaps	Helps various IoT devices to talk to each other, no focus on how users can secure IoT devices	Focus on how software developers can fix IoT vulnerabilities, not how consumers can address them	Top-down bulletins	Provides minimal guidance, focuses on big picture security compliance
Key Gap Filled	Shows how consumer/end-user provided guidance (or lack thereof) hampers user-controlled security and privacy feature adoption. Proposed usability-driven recommendations.	Connects various IoT device ecosystems	Provides developer and/or test perspective of IoT security	Doesn’t track device manual clarity or user comprehension	Doesn’t track device manual clarity or user comprehension

Table 19. Differentiators of the Study vs Industry Standard and/or Frameworks

Matter is an open-source connectivity standard for smart home and IoT devices that is designed to improve interoperability and compatibility (for supported devices) between different manufacture ecosystems and brands (Dimitri Belli, 2024). While Matter addresses the issue of

multi-device compatibility, it does not address the user-focused aspect of understanding, configuring, and maintaining user-controlled security and privacy features. In practical terms, Matter ensures devices talk to each other across ecosystems such as Apple or Google, but remains agnostic on providing guidance to consumers/end-users on utilizing user-controlled features. For example, Matter may streamline how consumers pair an indoor camera to a voice assistant device but does not specify how to segment a guest network, safeguard multi-user camera access, or give disclaimers about the risks of an always-on microphone.

By focusing on the human-centric dimension of smart home IoT security, this research study provides a critical complement to Matter's more limited scope. Instead of merely verifying device compatibility, the research study evaluates how consumers/end-users are guided and/or support through key user-controlled features like enabling child lock codes, scheduling firmware updates, or configuring surveillance camera feeds for multi-user access. This research study underscores that security and privacy in a networked home environment cannot rely solely on technical interoperability solutions like Matter. Instead, this research study proposes a holistic, user-focused strategy that merges systems engineering principles with direct consumer/end-user feedback. This approach thus helps address shortcomings in Matter's design mandate, establishing a new standard for actionable, human-centric IoT security guidance.

5.3 Systems Engineering Differentiators in this Research Study

The Systems Engineering differentiators in this research study set is apart by providing an iterative framework that integrates technical rigor and human-centric design, aligning with INCOSE 2025 vision. This section discusses the differentiators used to bridge the gap between smart home IoT manufactures and the comprehension and application of user-controlled security and privacy features.

5.3.1 Verification and Validation (V&V)

Verification and Validation (V&V) are two of the central pillars in a systems engineering-associated lifecycle, ensuring that the system is built correctly (verification) and that the system fulfills its intended purpose (validation). In this research study, the V&V process was applied iteratively. During the verification phase, smart home IoT device setup resources were evaluated against industry cybersecurity recommendations and best practices to develop robust requirements for a smart home IoT device manual. The recommended systems were specifically designed to enhance the adoption of user-controlled security and privacy features. Based on these requirements, a test device manual was created in order to allow it to be evaluated in the validation phase. In the validation phase, user participants used the test device manual as the sole guide to configure and implement security features, allowing us to assess its effectiveness in real-world scenarios using surveys and proficiency test. However, the proficiency test did not always possess the statistical power necessary to draw definitive conclusions about subtle effects, primarily due to the limited sample size. To address this limitation, we incorporated qualitative methods in the form of focus group technical deep dives to enrich the data set. The insights gathered during these focus group sessions were then fed back into the initial requirements analysis phase, creating an iterative feedback loop aimed at continuously refining the requirements to better enhance the

adoption and effective use of user-controlled security and privacy features in smart home IoT devices.

5.3.2 SysML Diagrams

The iterative systems engineering process employed in this research study is designed to be repeatable and scalable. The process begins with an initial requirements analysis, followed by design, implementation, verification, and validation, then looping back through user feedback to refine the system continuously. This cycle can be repeated as often as necessary to accommodate new insights, emerging technologies, or changes in user behavior. The associated SysML Activity, Block Definition, and Use Case diagram show this iterative process flow is below in figure 20, 21, & 22.

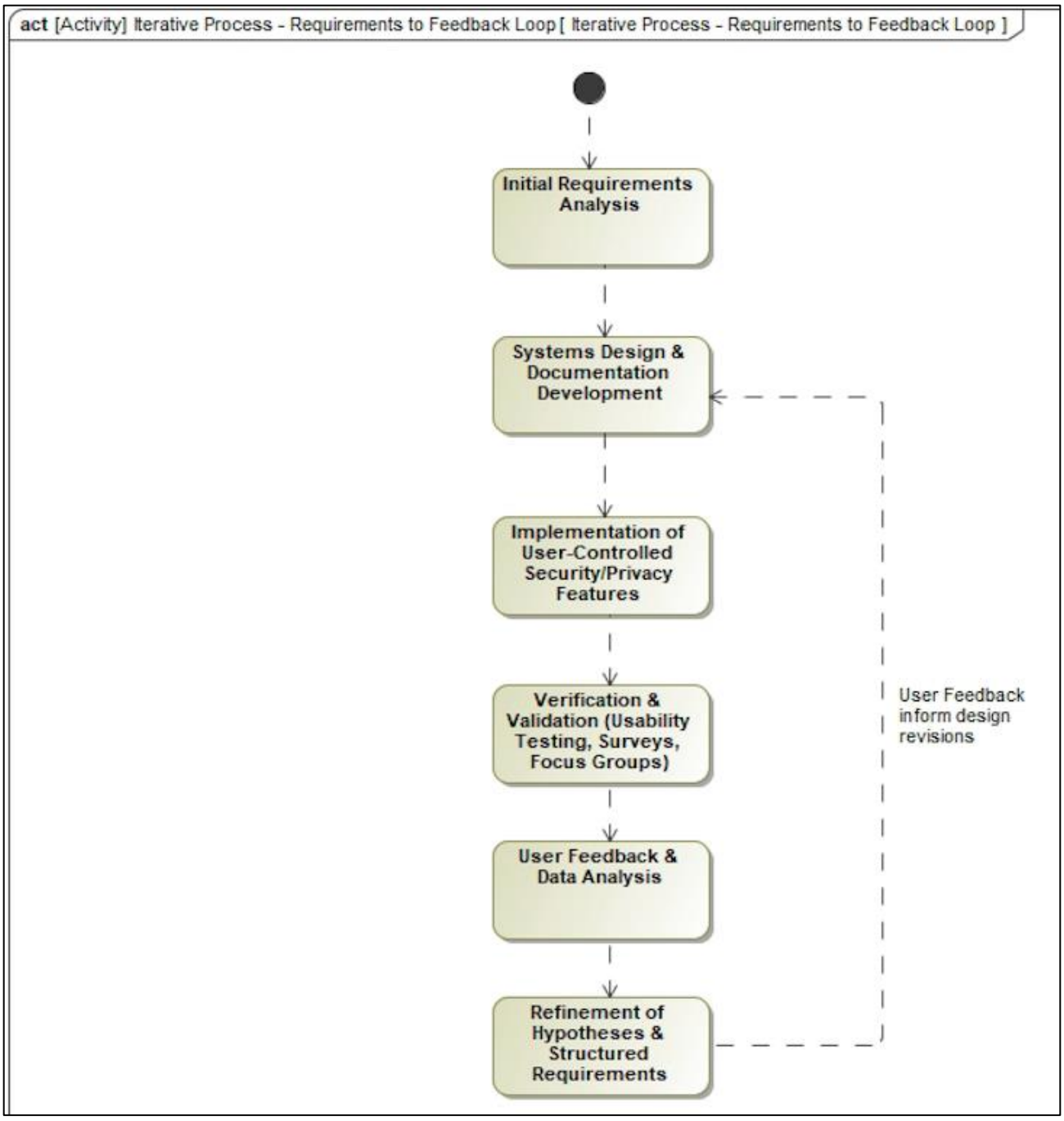


Figure 20. SysML Activity Diagram of the Iterative Process

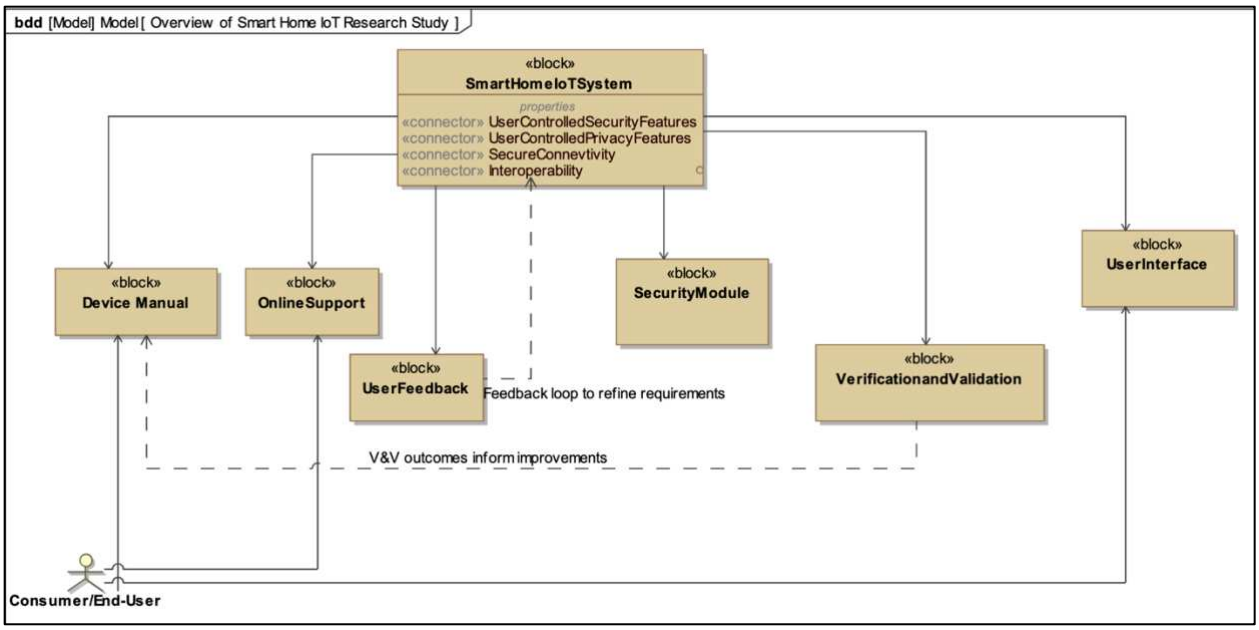


Figure 21.SysML Block Definition Diagram of Iterative Process

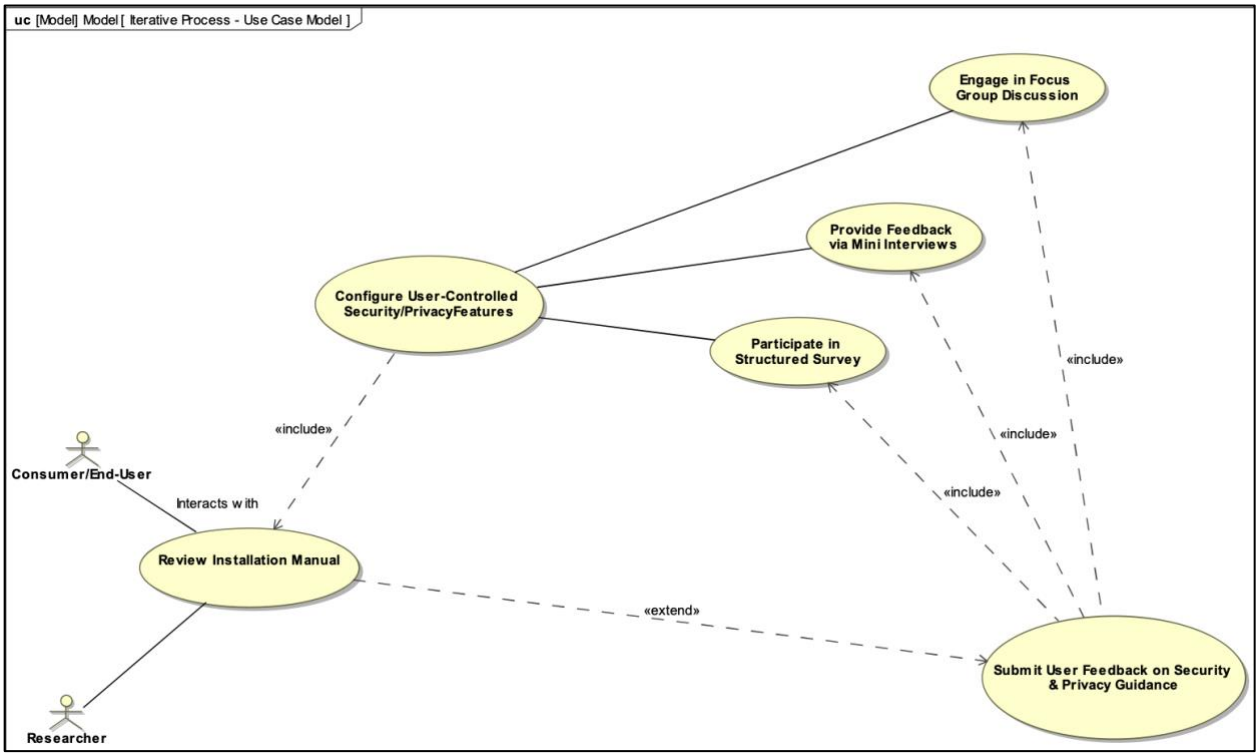


Figure 22. SysML Use Case Diagram of Iterative Process

5.3.3 Hypothesis Feedback Process

At the start of this research study, hypotheses were created regarding the clarity and comprehensiveness of smart home IoT manufacturer-provided guidance and the effect it has on user-controlled security and privacy feature adoption rates. These hypotheses were integrated into the requirements analysis phase, where we concentrated industry cybersecurity and privacy standards, recommendations, and best practices into measurable system requirements. As the research study progressed, each subsequent phase (comprising usability testing, proficiency testing, and focus group deep dives) provided real-world feedback on whether consumers/end-users could provide guidance effectively and increase the adoption of user-controlled security and privacy features. This feedback loop is meant to continuously repeat to refine the system design. For example, if a consumer/end-user struggled to understand multi-factor authentication (MFA) setup instructions, the hypothesis was revisited, and the corresponding requirement was revised to mandate the inclusion of step-by-step visual guides. The goal of this iterative systems engineering tailored process was to ensure that each cycle of design, testing, and feedback resulted in a refined set of requirements that are increasingly aligned with the consumer/end-users needs.

5.4 Contribution to Knowledge

This research study makes contributions to the fields of systems engineering and cybersecurity by illustrating how well-designed security and privacy guidance can significantly enhance consumer/end-user engagement with user-controlled security and privacy features in smart home IoT devices and systems. In line with the INCOSE Vision 2035, the research study highlights human-centric design as a foundational principle of systems engineering, demonstrating that understanding and supporting consumer/end-users' needs is essential for delivering secure smart home IoT systems. The research findings also contribute security policy and governance.

The study highlights a need for policies that require IoT manufacturers to disclose the importance of user-controlled security and privacy features and advocates for a centralized governance model to standardize security and privacy guidance.

5.5 Recommendations for Future Research

Building upon the findings and insights gained from this research study, there are several key areas that are worth further investigation. Recommendations for future research are in several areas.

Recommendation 1: Artificial Intelligence (AI). The research study findings highlighted several areas where user-centric design or individual support would benefit consumers/end-users the most. Future research is recommended to focus on how artificial intelligence (AI) can be leveraged to personalize security and privacy guidance for users when configuring user-controlled security features in IoT devices. AI-driven systems could analyze individual user behavior, device usage patterns, and demographic information to tailor security and privacy recommendations that are both relevant and easy to implement for all users. This personalization would address individual user needs, providing specific instructions on configuring passwords, enabling multi-factor authentication, and managing data privacy settings based on the user's technical proficiency and security habits.

Recommendation 2: Resilience (using AI and policy/regulations to know when and how to inactivate IoT devices that cannot be secured). The research study highlighted areas where consumers/end-users have IoT devices on their smart home networks for years with no security updates and still being using default usernames and passwords. Future research is recommended on the resilience of smart home IoT networks that contain unsecured Smart Home IoT devices. Future studies should explore how artificial intelligence (AI) frameworks can be integrated into

home area networks (HAN) to monitor connected device activity, assess security compliance against industry best practices, and determine when and how to isolate or deactivate compromised devices without the need for user intervention. Furthermore, future research should examine the development of policies and regulatory frameworks to govern AI tools in the safe deactivation of insecure devices without user intervention; legal and ethical implications of such policies and regulations should also be studied.

5.6 Conclusion

This systems engineering–focused research study evaluated the level of support smart home IoT manufacturers provide to consumers/end-users in applying user-controlled security and privacy features, revealing that comprehensive, user-centric guidance substantially increases engagement and adherence to cybersecurity best practices. By conducting an iterative requirement analyses, documentation review, usability tests, and focus group deep dive interviews, the research identified gaps, user frustrations, and shortcomings in existing smart home IoT manufacturer provided resources. The iterative systems engineering process enabled a continuous refinement of the hypotheses and system requirements based on direct user feedback to ensure that design updates would become more user-centric. The research study concluded that there is an observation and need for smart home IoT manufacturers to adopt a user-centric design approach in the way they communicate security and privacy guidance through manufacture provided documentation and/or other support resources.

REFERENCES

A. Cui and S. J. Stolfo. (2010). quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan. *Proc. 26th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, (pp. pp. 97–106).

al., W. Z. (2019). Discovering and understanding the security hazards in the interactions between iot devices, mobile apps, and clouds on smart home plat- forms. *28th USENIX Security Symposium (USENIX Security)*, 1133-1150.

al., Y. J. (2020). Burglars' iot paradise: Understanding and mitigating security risks of general messaging protocols on iot clouds. *IEEE Symposium on Security and Privacy (SP)*, 465-481.

Albrechtsen, E. &. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security Volume 29, Issue 4*, 432-445.

Allen, M. (2017). *The SAGE Encyclopedia of Communication Research Methods. (Vols. 1-4).* Retrieved from http://dx.doi.org/10.4135/9781483381411

Allison Shorten, J. S. (2017). Mixed methods research: expanding the evidence base. *Evidence-Based Nursing*, 74-75.

Antonakakis, M. A. (2017). Understanding the Mirai botnet. *26th USENIX Security Symposium (USENIX Security)*, (pp. 1093-1110).

Ashton, K. (2009, June 22). *RFID Journal*. Retrieved from https://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

AWS. (2023, 01 03). *Amazon Web Services*. Retrieved from What Is IoT (Internet of Things)?: https://aws.amazon.com/what-is/iot/

Azorín, J. M. (2010). The Application of Mixed Methods in Organisational Research: A Literature Review. *Electronic journal of business research methods* .

Babar, M. S. (2018). Proposed embedded security framework for Internet of Things (IoT). *International Wireless Communications and Mobile Computing Conference (IWCMC)* , (pp. 1153-1158).

Barcena, M. B. (2015). *Insecurity in the Internet of Things. Security Response, Symantec.* Retrieved from https://pdfs.semanticscholar.org/6d7f/60b16adead96aafa9e975207980eb32671b5.pdf

Barth, S. M. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics 41*, 55-69.

Bharathi, M., Tanguturi, R., Jayakumar, C., & Selvamani, K. (2012). Node capture attack in Wireless Sensor Network: A survey. . *2012 IEEE International Conference on Computational Intelligence & Computing Research (ICCIC).* Coimbatore.

Blanchard, B. S. (2014). *Systems engineering and analysis (5th ed.).* Pearson.

Boehm, B. L. (2006). *Architected agile solutions for software-reliant systems.* John Wiley & Sons.

Bogdan, S. T. (1984). *Introduction to Qualitative Research Methods.* New York: John Wiley & Sons.

C. Frank, C. N. (2017). Protecting IoT from Mirai botnets; IoT device hardening. *Conference on information systems applied research.* Austin, TX.

California, S. o. (2024, March 13). *California Consumer Privacy Act (CCPA).* Retrieved from https://oag.ca.gov/privacy/ccpa

Chen, J. H. (2020). An intelligent and context-aware building energy management system for smart homes. *IEEE Accesss, 8, 71306-71318.*

Choi, H. P. (2017). Smart home appliance system using smartphone application. *International Journal of Smart Home*, 59-68.

Cisco. (2017). *Securing the Internet of Things.* Retrieved from https://mkto.cisco.com/rs/564-WHV-323/images/Securing-IoT-Whitepaper-r3.pdf

Cohen, J. (1988). A Power Primer . *American Psychological Association*, 155-159.

Commission, F. T. (2013, January 17). *Children's Online Privacy Protection Rule ("COPPA").* Retrieved from https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Congress, 1. U. (2020). *H.R.1668 - IoT Cybersecurity Improvement Act of 2020* . Retrieved from https://www.congress.gov/bill/116th-congress/house-bill/1668

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. . *IEEE Commun. Surv. Tutor., 18*.

Cook, D., Youngblood, M., Heierman, E., Gopalratnam, K., Rao, S., Litvin, A., & Khawaja, F. (2003). MavHome: an agent-based smart home. *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications.* Fort Worth, TX.

Cortesi, D. (2022, 01 03). *The First Home Computer.* Retrieved from Computer History Museum: https://s3.amazonaws.com/s3data.computerhistory.org/chmedu/VIE_05_008.pdf

Cotton, A. (2021). *Identification of Manual Cybersecurity Tasks for Artificial Intelligence Automation Conversion: A Qualitative Study.*

Creswell, J. W. (2019). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research (6th ed.).* Saddle River, NJ: Pearson.

Csikszentmihalyi, M. (2014). *Validity and Reliability of the Experience-Sampling Method. New York: Springer.* New York: Springer.

Das, A. B. (2018). The tangled web of password reuse. *In Network and Distributed System Security Symposium (NDSS).*

DAU. (2024, December). *(DAU) Defense Acquisition University.* Retrieved from https://www.dau.edu/glossary/requirements-analysis

Davis, P. K. (2018). *Systems engineering for security: Using systems engineering principles to design secure systems.* John Wiley & Sons.

DCMS. (2018). *DCMS.* Retrieved from Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report.: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973926/Secure_by_Design_Report__V2.pdf

Dimitri Belli, P. B. (2024). Connectivity Standards Alliance Matter: State of the art and opportunities. *Internet of Things, Volume 25.*

Dimitri Belli, P. B. (2024). Connectivity Standards Alliance Matter: State of the art and opportunities. *Internet of Things, Volume 25*.

Dong-Young Yoo, J.-W. S.-Y. (2007). Home-Network Security Model in Ubiquitous Environment. *World Academy of Science, Engineering and Technology.*

E. Fernandes, J. J. (2016). Security analysis of emerging smart home applications. *IEEE Symposium on Security and Privacy (S&P)*, 636-654.

Edmondson, A. C. (2007). Methodological fit in management field research. *Academy of Management Review*, 1246-1264.

Edward B. Driscoll, J. (n.d.). *The History of X10*. Retrieved from http://home.planet.nl/~lhendrix/x10_history.htm

Emami-Naeini, P. D. (2019). Exploring how privacy and security factor into IoT device purchase behavior. *CHI Conference on Human Factors in Computing Systems*, (pp. 1-12).

Engineers, I. o. (2019). Chapter 3: Internet of Things (IoT). In *Heterogeneous Integration Roadmap 2019* (pp. 1-15). IEEE.

Enterprise, H. P. (2014). Retrieved from Hewlett Packard Enterprise: https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA5-4759ENN.pdf

Evans, P. C. (2012). ndustrial internet: Pushing the boundaries of minds and machines. *General Electric*.

Fagan, M., Yang, M., Tan, A., Randolph, L., & Scarfone, K. (2019, October). *Security Review of Consumer Home2 Internet of Things (IoT) Products.* Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8267-draft.pdf

Feldman, D. (2016). Smart devices, smart privacy? The internet of things and privacy issues. . *Journal of Law and Technology*, 45-58.

Feng, J. H. (2019). The role of human-computer interaction in improving security and privacy. *ACM International Joint Conference on Pervasive and Ubiquitous Computing*, (pp. 521-526).

Fernandes, E. J. (2016). Security analysis of emerging smart home applications. *IEEE Symposium on Security and Privacy.* San Jose.

Fernandes, E. J. (2016). Security analysis of emerging smart home applications. *IEEE Symposium on Security and Privacy*, (pp. 636-654).

Fetters, M. D. (2013). Achieving Integration in Mixed Methods Designs-Principles and Practices. *Health Services Research*, 2134-2156.

Fletcher, J., & Malalasekera, W. (2016). Development of a user-friendly, low-cost home energy monitoring and recording system. *Energy, 111*, 32-46.

Furnell, S. J. (2008). The challenges of understanding and using security: A survey of end-users. Computers & Security, 25. *Computers & Security, 25*, 27-35.

GAO. (2017). *Technology Assessment The Internet of Things: Status and Implications of an Increasingly Connected World.* Washington D.C.: Government Accountability Office.

Gartner. (2022). *IT Glossary.* Retrieved 11 2, 2022, from http://www.gartner.com/it-glossary/internet-of-things/

Given, L. (2008). *The SAGE encyclopedia of qualitative research methods.* Retrieved from http://dx.doi.org/10.4135/9781412963909

Gonzalez, R. &. (2019). The challenge of IoT security: Systems engineering approach to mitigate vulnerabilities. *International Journal of Engineering Research & Technology*, 45-58.

Goodman, S. K. (2017). Security in smart homes: Analysis of IoT systems and cybersecurity challenges. *IEEE Internet of Things Journal*, 123-139.

Guillet, R. (2017). *CONSUMER'S GUIDE FOR REDUCING CYBERSECURITY RISKS IN SMART HOME TECHNOLOGY DEVICES.*

Guillet, R. (2017). CONSUMER'S GUIDE FOR REDUCING CYBERSECURITY RISKS IN SMART HOME TECHNOLOGY DEVICES.

Gupta, S., & Gupta, B. (2017). Cross-Site Scripting (XSS) attacks and defense mechanisms: Classification and state-of-the-art. *Int. J. Syst. Assur. Eng. Manag, 8*, 512-530.

Harbach, M. F. (2014). Who's really paying for your free app? *Symposium On Usable Privacy and Security* , (pp. 14-27).

Hargittai, E. &. (2013). *Digital inequality. In W. H. Dutton (Ed.), The Oxford Handbook of Internet Studies.* Oxford University Press.

Heer, T. G.-M. (2011). Security challenges in the IP-based Internet of Things. *Wireless Personal Communications, 61(3)*, 527-542.

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016). Smart Locks: Lessons for Securing Commodity Internet of Things Devices . *Proceedings of the 11th ACM on asia conference on computer and communications security.*

https://www.cs.cmu.edu/~coke/history_long.txt. (n.d.). Retrieved September 1, 2022

IBM. (2024, Nov). *What is logistic regression?* . Retrieved from IBM: https://www.ibm.com/think/topics/logistic-regression

IEEE. (2015). *Towards a Definiiotn of the Internet of Things (IoT).* IEEE.

IHS Markit. (2017, Oct 24). (IHS Markit, S&P Global) Retrieved Aug 11, 2022, from Number of Connected IoT Devices Will Surge to 125 Billion by 2030: https://news.ihsmarkit.com/prviewer/release_only/slug/number-connected-iot-devices-will-surge-125-billion-2030-ihs-markit-says

INCOSE. (2024). *INCOSE - Systems Engineering Definition*. Retrieved from International Council on Systems Engineering: https://www.incose.org/about-systems-engineering/system-and-se-definitions/systems-engineering-definition

Insights, F. B. (2022). *Internet of Things Market Size [2022-2029].* Globe Newswire.

ISO/IEC. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Retrieved from https://www.iso.org/standard/27001

Johnson, J. M. (2018). The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices. *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 1-7.

Jose, A. C. (2015). Smart Home Automation Security: A Literature Review . *The Smart Computing Review*.

Josiah White, P. J. (2024). *The Mirai Botnet – Threats and Mitigations.* Retrieved from Center for Internet Security: https://www.cisecurity.org/insights/blog/the-mirai-botnet-threats-and-mitigations

Khorov, E., Lyakhov, A., Krotov, A., & Guschin, A. E. (2015). A survey on IEEE 802.11ah: An enabling networking technology for smart cities . *Computer Communications, 58*, 53-69.

Khusvinder Gill, S.-H. Y. (2009). A ZigBee-Based Home Automation System. *IEEE Transactions on Consumer Electronics,Vol. 55, No. 2*, 422-430.

Kirk, J., & Miller, M. L. (1986). *Reliability and validity in qualitative research (Vol. 1).* Beverly Hills, CA: Sage Publications, Inc.

Kizza, J. M. (2017). *Guide to computer network security (5th ed.).* Springer International Publishing.

Kossiakoff, A. (2020). *Systems Enggineering Principles and Practice.* Joh Wiley & Sons.

Lashkari, C. M. (2019). Energy Management for Smart Homes—State of the Art. *Applied Sciences*.

Li, S. T. (2016). The Internet of Things: A security point of view. *Internet Research, 26*, 337-359.

Liu, W. L. (2021). Sustainable Smart Home Design Based on Real-Time Data Monitoring. *Journal of Clean Energy, 23(*, 56-68.

Lockheed Martin. (2024). Retrieved from www.lockheedmartin.com

Lowhorn, G. L. (2007). Qualitative and quantitative research: How to choose the best design. *Academic Business World International Conference.* Nashville, TN.

Lutolf, R. (1992). Smart home concept and the integration of energy meters into a home-based system. *Metering Apparatus and Tariffs for Electricity Supply*, (pp. pp. 277-278). Glasgow.

Lyngaas, S. (2015, April 16). *FCW*. Retrieved from https://fcw.com/security/2015/04/nist-official-internet-of-things-is-indefensible/250688/

M. Leo, F. B. (2014). A federated architecture approach for Internet of Things security. *Euro Med Telo Conference (EMTC).*

McGee, T. M. (2016). Evaluating personal cyber security in the Internet of Everything: Smart home vulnerabilities (Doctoral dissertation).

Meadows, D. H. (2008). *Thinking in Systems: A Primer.* London, UK: Chelsea Green Publishing.

Mitchell, E. (2020). CYBER SECURITY @ HOME: The Effect of Home User Perceptions of Personal Security Performance on Household IoT Security Intentions.

Moher, D., Dulberg, C. S., & Wells, G. A. (1994). Statistical Power, Sample Size, and Their Reporting in Randomized Controlled Trials . *JAMA*, 122-124.

Muhammad Burhan, R. A.-S. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors, 18*(2796).

Muller, N. J. (2002). *Networking A to Z.* McGraw-Hill Professional.

Nader Safa, C. M. (2016). Human errors in the information security realm – and how to fix them. *Computer Fraud & Security, Issue 9*, 17-20.

Nataliya V. Ivankova, J. W. (2006). Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice. *Sage Journals*, 3-20.

National Cybersecurity Alliance. (2024, June 14). *Securing Smart Speakers and Digital Assistants.* Retrieved from Online Safety + Privacy Basics: https://staysafeonline.org/resources/securing-smart-speakers-and-digital-assistants/

Nguyen, K. A. (2017). Smart home water management system using IoT and machine learning. *Energy Procedia - 138*, 235-240.

Niall Bolger, J.-P. L. (2013). *Intensive Longitudinal Methods: An Introduction to Diary and Experience* . New York: Guilford Press.

Nikolay M. Bulanov, e. a. (2021). Basic principles of descriptive statistics in medical research. *Sechenov Medical Journal*.

NIST. (2020). Considerations for Managing IoT Cybersecurity and Privacy Risks in Smart Homes. *National Institute of Standards and Technology*.

NIST. (2021, May 12). *Executive Order 14028, Improving the Nation's Cybersecurity* . Retrieved from https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

NIST. (2024, December 5). *National Institute of Standards and Technology (NIST) Cybersecurity Framework.* Retrieved from https://www.nist.gov/cyberframework

NIST- Cybersecurity Framework. (2024, Sep 1). Retrieved from National Institute of Standards and Technology: www.nist.gov/cyberframework

Nolin, J. O. (2016). The Internet of Things and Convenience. *Internet Search, 26*(Feburary).

NSA. (2023). *National Security Agency.* Retrieved from NSA Releases Best Practices For Securing Your Home Network : https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3304674/nsa-releases-best-practices-for-securing-your-home-network/

Oberlo. (2024). *Oberlo Statistics*. Retrieved from US Smart Home Statistics (2019–2028). : https://www.oberlo.com/statistics/smart-home-statistics

OWASP. (2018). *OWASP IoT Top 10 2018 Mapping Project*. Retrieved from https://scriptingxss.gitbook.io/owasp-iot-top-10-mapping-project

P. Suresh, J. V. (2014). A state of the art review on the Internet of Things (IoT) History, Technology and fields of deployment. *nternational Conference on Science, Engineering and Management Research.*

Palinkas, L. A. (2015). *Purposeful sampling for qualitative data collection and analysis in mixed method implementation research.* Retrieved from Administration and Policy in Mental Health and Mental Health Services Research: https://link.springer.com/article/10.1007/s10488-013-0528-y

Pardis Emami Naeini, S. B. (2017). Privacy Expectations and Preferences in an IoT World. *Usable Privacy and Security.* Sanda Clara, CA.

Patel, A. &. (2021). Security Challenges and Future Trends for Smart Homes. *IEEE Communications Surveys & Tutorials, 23*, 2345-2365.

Patel, S. H. (2012). Home automation in the wild: Challenges and opportunities. *14th ACM international conference on Ubiquitous computing*, (pp. 167-176).

PenTestPartners. (2018). *WHY Is Consumer IoT Insecure?* Retrieved from https://www.pentestpartners.com/security-blog/why-is- consumer-iot-insecure/

Perera, C. Z. (2015). Privacy of big data in the internet of things era. *IT Professional, 17*.

Pfleeger, C. P. (2012). *Analyzing computer security: A threat/vulnerability/countermeasure approach.* Pearson.

Pil, Y. S. (2023). The Way Forward for Security Vulnerability Disclosure Policy: Comparative Analysis of US, EU, and Netherlands. *Studies in Computational Intelligence 1075 Roger Lee Editor Big Data, Cloud Computing, and Data Science Engineering*, 119-131.

Pongle, P. C. (2015). A survey: attacks on RPL and 6LoWPAN in IoT. International Conference on Pervasive Computing. *advance Communication Technology and Application for Society*.

Prabhakar, S. (2017). Network Security in Digitalization: Attacks and Defence. *Computer Application Robot, 18*, 2027-2051.

Project), O. (. (2018). *OWASP Internet of Things (IoT) Top 10 2018*. Retrieved September 1, 2022, from https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). hreats to networking cloud and edge datacenters in the Internet of Things. *IEEE Cloud Computing, 3*, 64-71.

Quach, K. (2018). Default Username and Password in Internet of Things. *University of Skovde*, 46.

R. Mahmoud, T. Y. (2015). Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. *10th IEEE International Conference for Internet Technology and Secured Transactions (ICITST).* London.

Rawlinson, K. (2015). Hp study reveals 70 percent of internet of things devices vulnerable to attack. HP Advisory.

Redmiles, E. M. (2016). How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Campus, and National Web Panels. *IEEE Symposium on Security and Privacy (SP) Conference Proceedings* (pp. 607-624). IEEE.

Redmiles, E. M. (2016). Where is the digital divide? A survey of security, privacy, and socioeconomics. *CHI Conference on Human Factors in Computing Systems* , (pp. 1983-1994).

Robert Willison, J. B. (2006). Opportunities for compouter crime: considering systems risk from a criminological perspective. *European Journal of Information Systems* , (pp. Volume 15, Issue 4).

Roman, R. N. (2013). Securing the Internet of Things. *Computer*, 51-58.

Rose, K. E. (2015). The Internet of Things: An overview. *The Internet Society*.

S. Sicari, A. R.-P. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks 76*, 146-164.

Salkind, N. (2011). *Exploring Research.* Boston, MA: Pearson.

Sanford Friedenthal, A. M. (2015). *A Practical Guide to SysML: The Systems Modeling Language (3rd Edition).* Elsevier.

Schneier, B. (2018). *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World.* W. W. Norton & Company.

Seaman, C. B. (1999). Qualitative Methods in Empirical Studies of Software Engineering. *IEEE TRANSACTIONS ON SOFTWARE ENGINEERING,*, VOL. 25, NO. 4, 557.

Seitz, D. A. (n.d.). *Lifewire: Tech for Humans*. Retrieved 11 25, 2022, from https://www.lifewire.com/what-is-z-wave-4588924

Sicari, S. R.-P. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146-164.

Sicari, S. R.-P. (2015). Security, privacy, and trust in Internet of Things: The road ahead. *Computer Networks, 76*, pp. 146-164.

Siponen M, W. R. (2009). Information security management standards: problems and solutions. *Inform Manage 46 (5)*, (pp. 267-270).

Sruoginis, K. S. (2016, December). *The Internet of Things*. Retrieved from https://www.iab.com/wp-content/uploads/2016/12/IAB-Internet-of-Things.pdf

Statista. (2021, May 18). *State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally*. Retrieved from IOT Analytics: https://iot-analytics.com/number-connected-iot-devices/

Sun, J. Y. (2022). A Comprehensive Survey of Security Issues of Smart Home System: ‘‘Spear’’ and ‘‘Shields,’’ Theory and Practice. *Yunnan Fundamental Research Project 202101AU070007*.

U.S. Census Bureau. (2016). Retrieved from https://www.census.gov/data/tables/time-series/dec/popchange-data-text.html

UK Department for Digital, C. M. (2018, Mar 7). *Secure by Design report* . Retrieved Dec 22, 2022, from

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973926/Secure_by_Design_Report__V2.pdf

Union, E. (2018, May 25). *General Data Protection Regulation.* Retrieved from https://gdpr-info.eu/

Ur, B. J. (2016). Security in context: Personalized systems for consumer IoT security. *Proceedings of the 12th Symposium on Usable Privacy and Security (SOUPS), 13-24.*

Weber, R. H. (2010). Internet of Things—New security and privacy challenges. *Computer Law & Security Review, 26*, 23-30.

Weinstein, R. (2005). May | June 2005 IT Pro 271520-9202/05/$20.00 © 2005 IEEE P u b l i s h e d b y t h e I E E E C o m p u t e r S o c i e t y RFID: A Technical Overview and Its Application to the Enterprise. *IEEE Compouter Society*. Retrieved from A Guide to Understanding RFID.

Williams, P. A. (2019). *The Internet of Things: Beware of the unintended consequences.*

Wired. (2017). *Wired*. Retrieved from https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/.

Yan Meng, e. a. (2018). SECURITY AND PRIVACY IN THE WIRELESS INTERNET OF THINGS: EMERGING TRENDS AND CHALLENGES. *IEEE Wireless Communications*.

Yan, Z. Z. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications, Volume 42*(June 2014), 120 - 134.

Yan, Z. Z. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications, 42*(June), 120 - 134.

Yang, R. N. (2017). Making sustainability sustainable: Challenges in the design of eco-interaction technologies. *2017 CHI Conference on Human Factors in Computing Systems*, (pp. 821-830). Chicago.

Yeh, H.-W. G. (2013). Sorting it out: pile sorting as a mixed methodology for exploring barriers to cancer screening. *Quality and Quantity (48)*, 2569-2587.

Zanella, A. B. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, 22-32.

Zeng, E. M. (2017). End user security & privacy concerns with smart homes. *13th Symposium on Usable Privacy and Security (SOUPS)*, (pp. 65-80).

Zeng, E. M. (2017). End user security and privacy concerns with smart homes. *USENIX Conference on Usable Privacy and Security 13th*, (pp. 65-80).

Zhang, N. Y. (2010). Password policies for ordinary users: The scenario of Chinese universities. *International Conference on Educational and Information Technology (Vol. 2).* IEEE.

Ziegeldorf, J. H. (2014). Privacy in the Internet of Things: Threats and Challenges. *Securioty and Communication Network Vol 7, Issue 12*, 2728 - 2742.

APPENDIX A: SURVEY AND PROFICENCY TEST INFORMED CONSENT FORM

My name is Kelvin Shorts and I am a PhD Candidate at Colorado State University. Dr. Steve Simske of the Colorado State University School of Systems Engineering is my faculty advisor. I am conducting a research study at Colorado State University to learn more about smart home user Internet of Things (IoT) security and I would appreciate your participation. This study is titled "The Effectiveness of Manufacturer Support in applying User-Controlled IoT Security and Privacy Features".

Smart Home Internet of Things refers to an interconnected network of physical devices, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to collect, and exchange data. In the context of smart homes, IoT devices are designed to enhance the efficiency, comfort, security, and convenience of the living environment through automation and remote-control capabilities.

The primary objective of this research is to explore user-controlled cybersecurity features and the support Internet of Things (IoT) manufacturers provide to consumers to implement and configure them. Your participation is invaluable as it will contribute to a deeper understanding of how consumers can better protect themselves against cyber threats in the era of the Internet of Things.

Participation in this study involves completing a survey that will take approximately 15-20 minutes to complete. Please be assured that all responses will be kept strictly confidential and will be used solely for academic purposes. Data will be anonymized, and no personal identifiers will be included in any reports or publications resulting from this study. All survey participants must be 18 years or older.

While there are no direct benefits to you, we hope you gain more knowledge on smart home internet of things (IoT) cyber security best practices. There is no compensation for participating in this survey. Findings from this study are expected to be published in peer-reviewed academic journals, contributing to scholarly discussions and practical applications in the field.

Should you have any questions or require further information, feel free to contact me at kelvin.shorts@colostate.edu or my faculty advisor at steve.simske@colostate.edu.

By clicking Yes below and continuing, you are acknowledging that you are 18 years or older and voluntarily agreeing to participate in this research study. You may withdraw from the survey at anytime.

○ Yes ○ No

APPENDIX B: BACKGROUND SURVEY

Demographic and Background Information

1. Age
    a) 18-24
    b) 25-34
    c) 34-44
    d) 45-54
    e) 55-65
    f) 65+
2. Level of Education
    a) Some high school or less
    b) High school diploma or GED
    c) Some college, but no degree
    d) Associates or technical degree
    e) Bachelor's degree
    f) Graduate or professional degree (MA, MS, MBA, PhD, JD, MD, DDS etc.)
    g) Prefer not to say

The following questions are based on your personal experience:

1. How would you describe your experience with technology?
    a) Novice (I use technology as needed and rely on help for setup and troubleshooting)
    b) Intermediate (I am comfortable using technology and can troubleshoot some issues on my own)
    c) Advanced (I have a strong understanding of technology and can handle complex troubleshooting and setups)

2. On a scale of 1-5 (1 being not at all, 5 being very), how aware are you of potential cyber security risks associated with using Internet of Things (IoT) devices in your home?

3. Which of the following actions have you taken to secure your Internet of Things (IoT) devices at home (select all that apply):
    a) Strong passwords for device logins
    b) Keeping devices updated with the latest software
    c) Disabling unused features or functionalities
    d) Using a secure home network with encryption
    e) None of the above

4. Are you familiar with the concept of two-factor authentication (2FA), and do you use it whenever possible to enhance the security of your smart home devices?
    a) Yes, always
    b) Yes, sometimes
    c) No, I'm not familiar
    d) Not applicable/I don't use 2FA

5. How often do you review the privacy settings of your smart home devices and adjust them according to your preferences?
    a) Regularly
    b) Occasionally
    c) Rarely
    d) Never

6. Have you changed the password on your smart home devices since you first purchased and installed the device?
    a) Yes, I change passwords regularly
    b) Yes, but only when prompted or necessary
    c) No, I haven't changed the password
    d) Not applicable/I don't know

7. Have you ever checked the privacy settings on your smart home Internet of Things) devices and adjusted them to your preferences?
    a) Yes, I have done this for most of my devices
    b) Yes, I have done this for some of my devices
    c) No, I haven't done this for any of my devices
    d) I'm not sure what privacy settings are

8. Some smart home devices offer guest access options. Do you typically use guest access for anyone outside your household who wants to connect to your smart home devices?
    a) Yes, I always use guest access for anyone outside my household
    b) Sometimes, depending on the person
    c) No, I never use guest access
    d) I'm not sure how to enable guest access
    e) I don't know what guest access is

9. How comfortable are you changing the default settings on your smart home IoT devices for increased security (e.g., privacy settings, data sharing preferences)?
    a) Very comfortable – I'm very tech-savvy
    b) Somewhat comfortable – I'll make basic adjustments.
    c) Not really comfortable – I need help
    d) Not comfortable at all – I don't want to mess anything up
    e) I don't know what default setting are

Proficiency Test: Test Group #1 - Security guidance provided in installation manual

Quick Installation Guide for Your Wi-Fi Security Camera

Congratulations on your purchase! This guide provides step-by-step instructions for installing your new camera, along with integrated cybersecurity and privacy tips to ensure a secure setup.

Unboxing and Preparation

- Unpack your Wi-Fi Security Camera and place it within range of your Wi-Fi router.
- **Cybersecurity Tip:** Before installation, ensure your home Wi-Fi network is secured with a strong, unique password, using WPA2 or WPA3 (recommended) encryption.

Step 1: Positioning Your Camera

- Choose a location that offers a clear view of the area you wish to monitor.
- Avoid positions that might intrude on the privacy of neighbors or areas within your home that require confidentiality.
- **Outdoor Installation Tip:** Most security companies generally recommend installing the camera 8ft above ground.

Step 2: Powering and Connecting the Camera

- Connect your camera to the power source and wait for it to power up.
- **Cybersecurity Tip:** As soon as the camera is powered, it's crucial to change the default password to prevent unauthorized access. Default passwords are easily guessable and pose a significant security risk.

Step 3: Installing the Camera App

- Download the official app from the App Store or Google Play.
- Create an account, opting for a strong, unique password. Avoid common phrases and include a mix of letters, numbers, and symbols.
- **Privacy Best Practice:** Review and adjust the app permissions on your device to ensure it only accesses necessary information.

Step 4: Connecting to Wi-Fi

- Follow the app instructions to connect your camera to your Wi-Fi network.
- **Cybersecurity Tip:** Regularly check for and install firmware updates for your camera. These updates often contain fixes for security vulnerabilities.

Step 5: Finalizing Your Setup

- Mount your camera using the provided kit. Ensure it is securely attached and positioned as desired.
- Adjust your camera settings through the app, including motion detection zones and alert preferences.
- **Cybersecurity/Privacy Best Practice:** Notifications can be used for security camera alerts and security updates.

Support and Maintenance

- For support, visit our website or contact our customer service.
- **Cybersecurity Reminder:** Regularly update your camera's firmware and app to protect against emerging threats.

Enjoy Your Secure Smart Home! With your new Wi-Fi Security Camera installed and by following these cybersecurity and privacy practices, you can now enjoy enhanced security and peace of mind.

Proficiency Test: Test Group #2 – No Security guidance provided in installation manual

Quick Installation Guide for Your Wi-Fi Security Camera

Congratulations on your purchase! This guide provides step-by-step instructions for installing your new camera.

Unboxing and Preparation

- Unpack your Wi-Fi Security Camera and place it within range of your Wi-Fi router.
- Ensure you have a working internet connection.

Step 1: Positioning Your Camera

- Choose a location that offers a clear view of the area you wish to monitor.
- Avoid positions that might intrude on the privacy of neighbors or areas within your home that require confidentiality.

Step 2: Powering and Connecting the Camera

- Plug the power adapter into your camera and then into an electrical outlet. Wait for the camera to power on; this is usually indicated by a LED light or a sound.

Step 3: Installing the Camera App

- Download the Wi-Fi Camera App from the Apple App Store or Google Play Store.
- Create an Account by opening the app and following the prompts to create a new account. Ensure you verify your email address or phone number if required.

Step 4: Connecting to Wi-Fi

- Follow the app instructions to connect your camera to your Wi-Fi network.

Step 5: Finalizing Your Setup

- Mount your camera using the provided kit. Ensure it is securely attached and positioned as desired.
- Adjust your camera settings through the app, including motion detection zones and alert preferences.

Support

- For support, visit our website or contact our customer service.

Enjoy Your New Wi-Fi Security Camera!

Proficiency Test Questions for Test Group 1 & 2

Participants were asked to use their knowledge and/or reference their assigned Installation Guide (Test Group 1 or 2) when answering the below questions:

1. What type of Wi-Fi network encryption is recommended for securing your home network?
    a) WEP
    b) WPA
    c) WPA2 or WPS3
    d) WPA3
    e) None of the Above
2. Why is it recommended to enable automatic firmware updates for your security camera, if available?
    a) To ensure the camera uses the latest features
    b) To protect against vulnerabilities by keeping the camera's firmware up to date
3. How often should you check for firmware updates for your security camera?
    a) Once a year
    b) Regularly, as updates become available
    c) Never
4. Why is it important to change the default password on your Wi-Fi security camera during the initial setup?
    a) To prevent unauthorized access
    b) To make it easier to remember
    c) The default password does not have to be changed
5. How can you ensure that your security camera's privacy settings align with your preferences?
    a) By regularly reviewing and adjusting privacy settings in the app
    b) Set privacy setting once during installation

APPENDIX C: FOCUS GROUP INFORMED CONSENT FORM

Title of Study: Navigating the Maze: The Effectiveness of Manufacturer Support in applying User-Controlled IoT Security and Privacy Features

Investigator Name: Kelvin Shorts

Email Address: kelvin.r.shorts@colostate.edu

Contact Phone Number: [redacted]

Purpose of the Study:

You are invited to participate in a research study on Smart Home Internet of Things (IoT) security. The title of our project is "The Effectiveness of Manufacturer Support in applying User-Controlled IoT Security and Privacy Features". The Principal Investigator is Dr. Steve Simske – Systems Engineering department and I (Kelvin Shorts) am the Co-Principal Investigator.

Inclusion Criteria

You are invited to participate in the study because you meet the following inclusion criteria:

- Located in the United States
- An adult age 21 or older
- Currently using 3 or more IoT Smart Devices in the Home
- The IoT smart devices are not used for medical purposes

This form may help you determine whether or not you desire to participate in this study.

Study Activities and Duration

If you volunteer to participate in this study, you will be asked to do the following:

- Participate in a 20-minute semi-structured interview

- Validate interview responses provided during your individual interview, approximately 5 minutes

Benefits to You or Others

There is likely no direct benefit to you for study participation. However, the overall benefits of the study may contribute to improvements to Smart Home Internet of Things (IoT) cybersecurity awareness and resources for the implementation of mitigation strategies for Smart Home IoT users and consumers.

Risks of Participation

There is some level of risk or discomfort involved in all research studies. This study is estimated to involve no more than minimal risk. An example of participation risk may involve you feeling uncomfortable answering the questions during the interview.

Incentives to Participate

There will be no financial cost to you to participate in this study. This study will take approximately 20 minutes for the interview. There is no compensation for your time.

Voluntary Participation

Your participation in this study is voluntary. You may choose not to participate in this study and may withdraw at any time or suspend responses at any time without penalty or consequence. You are also encouraged to ask questions about this study at any time.

Privacy and Confidentiality

The notes and recorded audio from the interview will be transcribed in Microsoft Word with password protection and stored in an encrypted folder. Only the researcher will have access to the folder and data. The data is retained up to 7 years after the publication of this dissertation,

upon which the information will be destroyed. If you have any questions about the research, please contact Kelvin Shorts at kelvin.shorts@colostate.edu or Dr. Steve Simske at steve.simske@colostate.edu. If you have any questions about your rights as a volunteer in this research, contact the CSU IRB at: CSU_IRB@colostate.edu; 970-491-1553.

Participant Consent

I have read the above information and agree to participate in this study. My signature below certifies I am at least 18 years of age and agree to study participation. A copy of this form has been given to me.

_____Date

_____ Participant Name (Please Print)

APPENDIX D: FOCUS GROUP PROTOCOL AND INTERVIEW QUESTIONS

Focus Group Interview Protocol

1. The interview date and time are scheduled at the participants' convenience.
2. At the start of the interview, review the Informed Consent form and validate the agreement to participate, confidentiality, and data recording.
3. Review the study purpose.
4. Capture the participants' unique study code on the notes document.
5. Allow the participant time to ask any questions and establish a rapport.
6. Ask and discuss the set of questions with the participants.
7. Foster participants to be transparent about the relevant experiences by asking probing questions.
8. Thank the participant for their time and effort during the interview at the end of

the questions.

9. Save the interview notes to the encrypted folder for data analysis.

Interview Questions

1. What are the challenges (if any) have you faced when trying to follow security guidance?
2. How could an IoT user manual be modified to better support you?
3. What type of visual aid could be added to security guidance to help understanding?
4. What additional information or support would increase your confidence in applying user-controlled security features?