University of Nevada, Reno

Smart Home or Smart Hell?: Modeling Smart Home IoT-Facilitated Abuse as a Cybersecurity Threat

A thesis submitted in partial fulfillment of the
requirements for the degree of Master of Science in
Computer Science and Engineering

by

Madison Vialpando

Dr. Shamik Sengupta - Thesis Advisor
May 2023

THE GRADUATE SCHOOL

We recommend that the thesis
prepared under our supervision by

Madison Vialpando

entitled

Smart Home or Smart Hell?: Modeling Smart Home IoT-Facilitated Abuse as a Cybersecurity Threat

be accepted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE

Shamik Sengupta, Ph.D.
Advisor

Nancy LaTourrette, M.S.
Committee Member

Gi W. Yun, Ph.D.
Graduate School Representative

Markus Kemmelmeier, Ph.D., Dean
Graduate School

May, 2023

Abstract

Smart homes are just one application of IoT or the “Internet of Things.” As a solution to create a more automated “smart home” experience, users have the ability to control the temperature, or turn off their lights with a single command. However, smart home technology is vulnerable to unique cybersecurity and privacy issues due to the personal nature of user-device interactions. In addition, the multi-user environments in which IoT has been implemented has considerable social nuances which play a factor in interpersonal cybersecurity threats. Smart Home-IoT Facilitated Abuse (SH-IoTFA) is an alarming phenomenon of users weaponizing smart home technology as a tool to perpetrate “Intimate Partner Violence” (IPV) using the built-in, convenient features. Despite the emergence of research on SH-IoTFA, there is a need to implement greater consideration for potentially abusive affordances in the development process through an attacker-centric threat model framework. This thesis explores how Sh-IoTFA has emerged and evolved from traditional Technology-Facilitated Abuse (TFA) and demonstrates, through a thematic review of the current literature, how attacker motivations influence their relationship with a device, and in turn, transform seemingly innocuous convenience features into tools for surveillance, power exertion, and harassment. Furthermore, this thesis breaks down the relational aspect between the attacker’s motivations, the device features, and the assets at risk for a victim. Utilizing the threat scenario, the Google Nest Hub was then analyzed to identify how an abuse perpetrator may potentially misuse the device. Overall, through an integration of interdisciplinary perspectives, this research highlighted interpersonal threats as a cybersecurity concern and proposed a threat model that may reduce inadvertent harm to consumers.

Dedication

To David. I could not have undertaken this journey without your support.

Acknowledgments

I would like to extend sincere thanks to my advisor, Dr. Shamik Sengupta, who helped me grow through all the phases of my research. I would also like to thank my committee members, Dr. Gi W. Yun, who opened my eyes to cybersecurity issues as an undergrad and helped me realize more potential for myself, and Ms. Nancy LaTourrette, for providing guidance and support on my research. Finally, I would like to thank my family, especially my parents Holly Charter and Bill Charter, for being a strong support system through all phases of my journey.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Introduction

The 'Internet of Things' (IoT)[1] is a paradigm that has rapidly evolved society's relationship with the digital world [2]. IoT technology has been implemented in several sectors as a possible solution to challenges in critical infrastructure, healthcare, and even agriculture [3]. IoT has also been introduced to the consumer market as a solution for home efficiency. Within what has been coined the 'Smart Home,' common home appliances have been digitized to streamline daily activities at the push of a button through a mobile application or control center [4]. Thermostats, doorbells, and security alarms, for that matter, share data with users and each other to provide more autonomous, convenient, and efficient living spaces [5].

The adoption of IoT smart home technologies (SH-IoT) has introduced complex challenges within the field of cybersecurity. Smart home environments are at a unique

[1] The definition of IoT differs across research disciplines. An accepted, and most helpful definition of IoT is "a network of networks that enables the identification of digital entities and physical objects – whether inanimate (including plants) or animate (animals and human beings) – directly and without ambiguity, via standardized electronic identification systems and wireless mobile devices" [2, p.701]

risk of privacy and security attacks due to their interconnected and dynamic nature [6]. In addition, the market competition to bring new devices at a fast pace has meant that SH-IoTs often have critical security vulnerabilities that are overlooked [7]. SH-IoTs have also introduced new social-behavioral threats in multi-user environments. Smart Home IoT Facilitated Abuse (SH-IoTFA) is the perpetration of interpersonal abuse using the convenient features of consumer IoT to stalk, harass, intimidate, and exert control over another person. As an extension of interpersonal abuse, this thesis will focus on SH-IoTFA through the lens of 'Intimate Partner Violence' (IPV) [8–11].

While IoT features are meant and marketed towards convenience, they maintain significant vulnerabilities to interpersonal abuse scenarios. As a result, malicious users can, and may even feel encouraged by the usability design to facilitate abuse. Research to date has revealed a lack of diverse perspectives in IoT design and development. Specifically, there is a tendency to blame users for their experiences of victimization rather than recognizing that abuse is a usability problem due to hidden affordances[2] in design [13]. While SH-IoTFA does not involve technical knowledge or 'hacking skills' the behaviors fall under the definition of a cybersecurity incident, specifically the use of a device for unauthorized access and criminal use. Unlike criminals who seek to steal, these individuals seek to destroy a victim from within their own home. By re-framing this narrative we can facilitate a broader shift in thinking in the developmental stages of IoT design, which is often too narrowly focused on traditional attack methods.

To mitigate the threats that victims of IPV face in smart home environments, it is imperative for there to be an industry model that not only recognizes abuse as a cybersecurity issue but plans for interpersonal cybersecurity threats. Threat modeling

[2] In Human Computer Interaction (HCI) affordances are considered possible actions that an object may allow the user to do through their features. These actions are perceived by the individual user through their relationship with the object [12].

is a systematic approach to identifying a system's potential attack vectors [14]. Within the threat modeling process, security professionals attempt to estimate the attackers' capabilities accurately and design an approach that can mitigate the attacks. Often, threat modeling is utilized for identifying potential attacks against an organization or product. However, the process can also be used as a meaningful strategy for abuse mitigation and ensure the development of inherently more secure devices. This thesis seeks to legitimize abuse as a cybersecurity threat by utilizing an attacker-centric threat model to demonstrate abusive behaviors facilitated by common SH-IoT features.

1.2 Background

Intimate Partner Violence (IPV) is just one facet of interpersonal abuse. The term IPV can be understood as a "behavior within an intimate relationship that causes physical, sexual or psychological harm, including acts of physical aggression, sexual coercion, psychological abuse and controlling behaviors" [15]. In the United States, research has estimated that 1 in 4 women and 1 in 9 men experience IPV within their lifetime [16]. Despite the word "violence," IPV does not have to entail physical abuse. In fact, 90% of IPV cases are "invisible" beyond the home and do not result in physical injury [17]. Rather than sporadic acts of violence, IPV can be understood as a pattern of behavior, known as "coercive control," in which a perpetrator seeks to gain control and power by essentially eroding the victim's sense of self-worth and autonomy. These patterns may include intimidation, humiliation, and physical threats [18].

Interpersonal abuse and by extension IPV cases where technology is involved can be categorized under the umbrella of Technology Facilitated Abuse (TFA). Examples of TFA include cyberstalking and cyberbullying which are generally facilitated through mobile devices. Specifically, texting, social media, and phone calls are used by an abuser to intimidate and threaten their victims. The convenience and ease of technology have also made it easier to escalate abuse. In some cases, perpetrators will install stalkerware[3] applications to track their victim's every move [20]. Victims of physical and sexual abuse may feel safer once they have physically left the relationship but in cases involving technology a victim may constantly feel endangered [21]. As a cybersecurity issue, interpersonal abuse via digital technologies erodes any sense of self-autonomy or safety from a victim [22].

Interpersonal abuse under the lens of SH-IoTFA maintains characteristics and patterns that amplify the severity of more common forms of TFA and introduce further harm. Often SH-IoTFA is categorized under the umbrella of TFA but it is important to provide a distinction between the two abuse scenarios. Rather than utilizing smartphones and social media, the nature of networked devices allows for an interconnected environment within the home to facilitate IPV. In TFA cases, perpetrators risk creating a paper trail, evidencing their abuse [23]. However, SH-IoTs enable the facilitation of abuse through convenient features in the device and corresponding mobile application design, without the creation of any concrete evidence [8]. Furthermore, the assumption of trust is often built into the design without safeguards when environments become trustless. As a result, SH-IoTs can be easily converted into a weapon against a victim [13].

In 2018, the first documented court case of SH-IoTFA described an Electronics Engineer named Ross Cairns, who was arrested and sentenced to 11 months in jail for stalking and harassing his ex-wife through their shared smart home device. Cairns took advantage of his administrative access to their shared ELAN[4] smart home system

[3] Stalkerware is a surveillance application which can track geolocation, phone calls, web searches, and messages [19]

[4] ELAN is a brand of smart home automation systems and devices [24]

to remotely eavesdrop and spy on her, using the built-in camera and audio facilities. After eavesdropping on his ex-wife's conversations with her mother, Cairns appeared at her home and physically threatened her [25].

In that same year, *The New York Times* investigated the phenomenon of SH-IoTFA by interviewing shelter workers, victims, lawyers, and first responders. The investigation uncovered that victims of IPV had been experiencing abuse related to their SH-IoTs such as the smart lock codes being changed while they were away from home, the thermostat settings being remotely turned off or turned to an extreme temperature, and the speakers playing at all hours of the day without respite. Other abuse tactics included harassing survivors by remotely controlling devices after the relationship had ended to remind them that their abuser was still present in their lives. In the same article, one woman recounted her abuser using their shared smart home devices to control every aspect of her life, from what she was allowed to watch to what music she was allowed to listen to [26].

1.3 Research Significance

Without examining how interpersonal abuse can be perpetrated through the design of SH-IoTs, these devices may inadvertently increase harm to consumers. Threat modeling is inherently multidimensional, with many facets and nuances. There are several avenues in which we can identify technology's role in controlling and abusive behaviors. Despite this, current threat modeling frameworks overlook social and psychological threats while using technology. Often, there is a large emphasis on technical third-party threats on consumer devices rather than how devices can be used maliciously in consumer social contexts. Attacker-centric threat modeling approaches are also neglected and are not being utilized effectively, due to the complexity of attacker profiling. By emphasizing the role of social behavior, user intention, and the nuance in relationships, this thesis conceptualizes the social dimensions of interpersonal cyberattacks through IoT and demonstrates how users may be encouraged cause harm due to the convenient design.

In terms of analyzing the negative effects of IoT, the most prominent example of a lack of threat modeling is the Apple AirTag. In 2021, Apple released AirTags as a cheap way to track anything from keys to wallets to backpacks. After the release, law enforcement and news outlets reported that the product was being used in theft and stalking cases. *Vice Motherboard* requested and reviewed police records in eight police departments across the country and found that over 150 police records mentioned AirTags. Of the 150 records, 50 cases included instances of women calling the police because they started getting notifications that their whereabouts were being tracked by an AirTag they did not own. In some cases, these women mentioned that they were experiencing or had previously experienced IPV and were concerned about their safety [27]. Initial threat modeling could have prevented using AirTags in such cases. Apple's approach in the design process failed to identify several significant factors of abuse that may exist in relationships. The devices were found to have no initial protection against unwanted tracking, which would have been planned for if there had been a model that considered interpersonal abuse as a form of security incident.

1.4 Research Objectives

The research objectives of this thesis are as follows:

1. Demonstrate how SH-IoTs are being used in IPV cases.

2. Evaluate the relationship between an abuse perpetrator and the usability features of SH-IoTs.

3. Develop an attack-centric threat model scenario for SH-IoTFA that establishes and demonstrates the interconnected relationship between an attacker, common SH-IoT features, and a victim's targeted assets.

1.5 Content

The following chapters of this thesis are as follows: Chapter 2 establishes the context through a literature review to identify key approaches and strategies within threat modeling SH-IoTFA. Chapter 3 demonstrates the threat model methodology and overview of notable work informing the qualitative analysis used to identify literature themes. Chapter 4 describes the threat model approach, including identifying the threat agent, victim assets in a smart home environment, and an overview of device threats across different SH-IoT products; this chapter also identifies abuse mitigation approaches. Chapter 5 analyzes the applicability of the threat model by implementing it with an analysis of the Google Nest Hub. Chapter 6 discusses future work, and limitations, and concludes the main points within this thesis.

Chapter 2

Literature Review

2.1 Introduction

The literature review is thematically organized to demonstrate the evolution and subsets of SH-IoTFA research. The current literature illustrates the nuanced and complicated nature of SH-IoTFA as a larger social issue related to interpersonal relationship dynamics [28]. The selected resources within the literature review include conference papers, journal articles, and technical reports, covering various topics, including computer science, psychology, and legal studies. The literature analysis within this review is structured as follows: Section 2.2 analyzes the background research on SH-IoTFA, Section 2.3 establishes a security and privacy analysis of SH-IoTs in multi-user environments, Section 2.4 identifies the current literature defining IoT developer perceptions and attitudes in design. This section also introduces considerations in HCI research and the idea of affordances. Section 2.5 reviews industry threat-modeling approaches and evaluates approaches in threat modeling IPV, and Section 2.6 summarizes the literature and discusses current research gaps.

2.2 Analysis of SH-IoTFA Research

Several terms are used to describe SH-IoTFA within the literature. These terms describe the behaviors and uses of IoT devices for abusive purposes and provide the context for specific IoT abuse cases. These most common terms include "IoT-Facilitated Tech-abuse" [29], "Smart Home facilitated Tech-abuse" [8], and "IoT-Enabled Technology-Facilitated Abuse" [30]. The concept of "smart home tech abuse" was developed by Dr. Leonie Tanczer. Tanczer and a team of researchers analyzed the privacy implications of consumer smart home technology by conducting two in-depth interviews with 45 individuals. From these interviews, the team determined that "teach abuse" in general needed to be identified as a new form of abuse [31]. Building off of their initial research in 2019, Tanczer et al. [32] interviewed 34 UK IPV support professionals ranging from detectives to domestic violence shelter workers. In this study, Tanczer's team found a general lack of recognition from IPV support professionals in handling tech abuse cases, specifically within a smart home setting. Recognition, however, is still in its infancy.

Other studies that have evaluated smart home technology's role in IPV included work from Leitão [9], who examined data collected from interviews and domestic abuse forum data as well as two workshops with IPV support professionals to determine hypothetical risks with smart home devices. From this data, Leitão determined that IoT devices collect a massive amount of personal data, preferences, and usage history from this data. Perpetrators of abuse can use IoT devices to exploit the functionalities to monitor, surveil, harass, and potentially control their victims. Therefore, there is a need to recognize the potential of convenient features to harm victims and conceptualize how the industry can plan for abuse cases.

Popular consumer IoT devices designed for the smart home have also been found to maintain specific features that aggravate their role in abuse. The novel nature of

IoT devices exacerbates the problem of SH-IoTFA as many victims may not have the technical knowledge to protect themselves from device abuse [33]. In addition, IoT devices are often designed with easy-to-use interfaces, which can also make it easier to "black box" the technology without identifying user features, how much control other users have when using the devices, how much data is being collected, and what legal rights a user maintains [34].

Within the field of Human Computer Interaction (HCI), researchers have identified issues with the build and design of IoT devices, which may cause usability issues for those who do not have device knowledge, facilitating and empowering abusers. Freed et al. [35] conducted a qualitative study with 89 individuals (39 survivors and 50 professionals) to understand how abusers have been able to manipulate devices for their gain. The study's results demonstrated that IPV perpetrators take advantage of the ownership of devices or accounts used by victims to install spyware, use location tracking, and even deny their victims access to the internet. If an abuser could not access a victim's accounts, the results found that they would use devices to facilitate harassment, intimidate their victims through harmful or threatening messages, and blackmail their victims by posting sensitive and sometimes even illicit information. The authors concluded that abuse perpetrators could be classified as 'UI-Bound Adversaries' because they did not have to use technical hacking methods to perpetrate abuse. Instead, the abusers used the devices' convenient features for their personal gain. The researchers argued that convenience in consumer technology design is often prioritized over security. By making simple changes within the development process, such as flagging suspicious behaviors and providing more transparent notifications, adversaries may be discouraged to use devices for their abusive behaviors. Thus, there can be a shift made towards empowering victims.

2.3 Security and Privacy for Shared Environments

The security of IoT devices, or lack thereof, introduces the threat of interpersonal attacks within home environments. Access control between users and devices is often unprotected in multi-user environments; generally, one user has more control over the device than users [36]. The imbalance of access control between users is becoming an increasing issue for security and privacy reasons. Ehrenberg and Keinonen [37] recognized the importance of examining surveillance and control within the smart home environment and used the Theory of Disciplinary Power[1]to examine how SH-IoT devices shift power structures within a multi-user environment. In a two-series qualitative study with five households, the researchers determined that IoT devices allowed for overt and covert surveillance, increased device interaction constraints, and regulated commodities that the user did not previously regulate. Because of this, they noted that IoT in multi-user environments established power dynamic changes and imbalances. Overall, the researchers found that the increased power within the home could amplify tensions between users, create a hierarchy to be abused by another user, and increase the risk of compromised security through a single entry of attack.

Another IoT feature that makes design insecure for multi-user environments is the inability to easily remove user access from devices even when an individual is no longer living in the shared environment. Mohammad et al. [38] examined the existing IoT access model frameworks. They concluded that for multi-user environments, stronger policy-based guidelines needed to be implemented to ensure that users who were removed from device access would be unable to regain access to the system rather than maintaining some access. The researchers determined that this was a security risk and increased tensions between users.

[1] Foucault's disciplinary power argues that social institutions and interactions are effective in creating compliant behavior, rather than forcing such behavior [37]

IoT devices are also susceptible to insider attacks, which greatly impact privacy. Janes et al. [39] demonstrated that account authentication and access in multi-user environments are not properly enforced by IoT devices, specifically by Amazon Ring. The authors hypothesized that IoT authentication issues found in Ring are not limited to the device but are a fundamental design flaw in shared IoT devices that violates user privacy. Furthermore, through an analysis of 19 popular smart home devices, the research found that 16 devices did not allow users to be easily removed from accessing the device if they had been previously authorized for device use due to the latency of API server distribution of access control lists. The authors pointed to a systemic failure of IoT developers to consider 'UI-Bound Adversaries,' as previously emphasized by Freed et al. [35].

Privacy between users and device security affects the severity of SH-IoTFA. In the context of SH-IoTFA, the literature finds a direct link between abuse perpetration and privacy violations. For example, Knittel and Shillair [40] found specific risks of IoT devices to abuse through a survey of over 300 women. The risks were revealed to be access and ownership, the personal nature of data collection, and trust, which were all factors that increased the impact of SH-IoTFA. Furthermore, traditional security advice did not protect victims of IPV but predicted increased abusive behaviors.

2.4 Developer Attitudes Towards Abuse Risks

Given the nature of SH-IoTFA, researchers have been interested in the overall attitude of IoT development and security professionals. In one scoping review, Slupska [13] analyzed over 40 smart home security papers to determine if IPV was considered as a potential risk for smart home environments. Their research revealed that only one article addressed IPV but was dismissive of the overall risk, placing responsibility on the potential victim. As a result, the researchers noted a gap in how IPV was perceived by developers and manufacturers. Cassioli et al. [28] also questioned whether or not gender was a consideration in IoT technology innovation. They found that gender was not considered and that developers often created consumer IoT from their own biases, which were predominantly male, without consideration of other perspectives. Through their research, they argued that introducing gender considerations in design would diversify innovation and that IoT design may not be meeting the needs of gender-diverse groups. Instead, they may raise their unique harms against these groups. Furthermore, in an analysis of gendered interactions with IoT, Strangers et al. [41] determined that there was a significant gender gap concerning the needs and wants of IoT users. Often, SH-IoT design is geared toward being digital "housekeepers for men," which left behind female users' expectations and adoption of the technology. The authors argued that if IoT was developed through a feminist lens, IoT adoption might rise, as well as the ability to protect the interests of women in their homes.

Social relationships in multi-user environments are generally not considered in IoT development. He et al. [42] surveyed 425 online participants and found that developers did not consider social risks in social relationships. As a result, the authors determined that understanding social relationships were vital when developing secure authentication rights for users in a multi-user environment. For example, the difference in trust between spousal users, children, neighbors, and even babysitters varies widely. Because of this, restrictions need to be placed on applicable groups for device usage. He et al. thus, contended that access control is a more complex and nuanced security issue than previously thought.

Moreover, Garg and Moreno [43] argue that some smart devices are designed assuming only one user will interact with the device. In contrast, devices in a smart home ecosystem are inherently shared by multiple users. Within their qualitative research, twenty participants logged over 656 instances of sharing smart devices in their environment. Following this period which lasted 14 days, the participants were interviewed to understand their experiences. The study's results revealed that IoT devices increased tension due to differences in device preferences, differences in technical knowledge, and a misunderstanding of the contexts of device use. These results revealed that shared IoT devices not only affect user privacy, but add complexity to multi-user environments.

In addition to gender and social perspectives, privacy between users is also not considered in IoT design. In an analysis of the privacy considerations of IoT design, Challhoub et al. [44] conducted qualitative research with 20 smart home camera designers using Grounded Theory, a research model for systematically collected data. Through this work, the research sought to determine if security and privacy considerations were present in the design of smart cameras. Within their research, Challhoub criticized the common practice of secure design, which often saw security as a technical threat with technical solutions. The researchers argue that this perspective limits considerations of social and interactive aspects of security. As a result, the industry needs to implement more interdisciplinary perspectives when considering security in product development.

2.4.1 Theory of Affordances and IoT Development

Developed as an ecological theory by J.J Gibson to describe the relationship between animals and their environments, The Theory of Affordances is the theory that the environment consists of surfaces in which offer opportunities and possibilities for the perceiver [45]. In the context of Human-Centered Design and HCI, Don Norman described affordances as the relationship between a physical object and an interacting agent. It is the relationship between the object's properties and the perceived capabilities of the interacting agent to determine how the object could then be utilized by the agent. In his book *The Design of Everyday Things*, Norman implied a relationship between the usefulness of an object and its usability. Furthermore, he implied that the usability of a design is not independent from an agent's perspectives [12].

In TFA and SH-IoTFA research, affordances can describe the possible ways that a device can be used as a tool by a perpetrator of abuse. In defining TFA under the lens of coercive control Dragiewicz et al. [46] argued that the phenomena can be situated through the lens of affordances and governmental policies which amplify abuse. They argued that the contexts of device usage such as gender inequality and misogyny define the abusive affordances that can exist on social platforms. Wood et al. [47] further characterized affordances in the context of TFA as "harm translation" in which a device's usability and properties essentially "invite" the user to perpetrate harm against another individual. Within this understanding of affordances, the authors conceptualized a framework that categorized the relationship between user intentions and device affordances. Building off of this work, it is recognized that social motivations, even as nuanced as abusive behaviors, are amplified due to threat analysis shortcomings [32, 47, 48].

2.4.2 Social Morals and Relationships in HCI

In addition to affordances based of user perceptions, user morals also impact the human-computer dialog and the perceived uses. Value Sensitive Design (VSD) is the theoretical approach in HCI developed by Batya Friedman and Peter Kahn aimed at recognizing how both pre-existing bias and emerging biases can manifest in computer information systems. Through this recognition, the approach defines a method of understanding stakeholder values to improve design and usability. The process in this framework includes documenting the predetermined conceptual concepts, technical investigations, and empirical investigations. As an HCI framework, VSD derives from the idea that information systems and technology is suitable for activities that support a predefined social value, as such the approach seeks to investigate how properties of technological design either support or hinder human values [49].

Building off of this approach, researchers have implemented VSD to understand traditional smart home cybersecurity dilemmas. Within this framing, it is understood that multidisciplinary factors have an immense impact on the different threats that a user may face in a third party attack. Specifically, failure to communicate device uses accurately to the users, a lack of security awareness, and user trust are all considered factors under the lens of VSD. In SH-IoTFA research, VSD can be understood and redefined as a way to make design more equitable for users who are directly impacted by poor and inherently biased design [48]. This theoretical approach provides the basis for an attacker-centric analysis to find user bias and morals based on their perceived use for the device and their own intentions against the victim.

2.5 Industry Threat Model Approaches

There are numerous definitions of threat modeling, but the most widely accepted definition is "a process that can be used to analyze potential attacks or threats and can also be supported by threat libraries or attack taxonomies" [50]. Threat modeling is a domain that lacks consistency due to its hypothetical and customizable nature based on the needs of an organization or a system [51]. Threat modeling methods and approaches create an abstraction of a system, attacker, and assets [52]. Various approaches have been used to define threats that may arise, with some of these models being more comprehensive than others. These approaches include asset-based, system-based, and attacker-based threat modeling. Each approach aims to find the motivations, attacker profile, system vulnerabilities, and risks. Though each approach has a unique goal based on the testing parameters.

Asset-Centric Threat Modeling: Under the asset-centric approach, threat modeling begins by describing an IT system or organization's assets that must be protected. Often, this can be categorized as listing all of the available assets that should be defended, the threats of those assets, and the assets affecting the system/organization as a whole [53].

System-Centric Threat Modeling: System-centric threat modeling is arguably the most popular approach. System-centric threat modeling is centered around the system's composition, hardware, and software components to determine the interactions. The approach is often expressed through data flow diagrams (DFD) and has a strong emphasis on how the design itself is vulnerable. There are several approaches to system-based threat models. One basic form is the four-question framework developed by Shostack [54]. The four-question framework addresses the following questions during analysis:

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good job?

Attack(er)-Centric Threat Modeling: Attacker-centric threat modeling, unlike the other approaches, seeks to understand an attacker's goals and how those goals will be accomplished. Within this process, the type of attacker is identified, the access to resources they maintain, and their motivations in exploiting vulnerabilities. Threat modeling from this perspective then gives developers the ability to protect assets through their understanding of the attacker [55].

2.5.1 Threat Modeling Research for SH-IoTFA

While there are already approaches to industry threat modeling, evaluations of social aspects of the smart home is still an emerging topic. In their article published to *Communications of the ACM*, Denning et al. [56] argued that consumer IoT implementation not only increased the threats of a third-party attack but also introduced more complex challenges to consumer safety. The researchers introduced what they defined as human assets at stake and evaluated how threats to the home can put those assets at risk. They designated these threats as more personal to the users and as such more vulnerable to harm. Furthermore the researchers identified that IoT risks need a unified framework and propose a model to test for IoT security. This model included 1) Identifying a device's potential exposure to an attack and its attractiveness to adversaries, 2) Determining the potential impacts on assets if a device is compromised, and 3) Assessing the degree to which security is important for a specific device as well as what security measures are important to address. From this model, the researchers argued that consumer advocacy groups should implement the framework to identify if an IoT should be introduced to the market. Through this process, consumers would be emboldened to voice concerns of abuse.

Adding to this discourse, Alshehri et al. [8] argued the use of SH-IoTs for abuse could be appealing because it is a low-effort extension of their physical abuse, and there is a lower risk of legal penalty. They contends that the low effort nature of abuse effectively invites abusive behaviors. The researchers also argue that because the assumption of trust in the devices has not been identified as a threat, SH-IoTs can be used for IPV facilitation. To combat this, they proposed a system-based threat model framework that asks developers to ensure more transparency in design for SHT features, maintain equal access between users, and maintain privacy-preserving features.

Based on Denning et al. [56], Slupska and Tanczer et al. [30] developed a threat model approach for developers and vendors to recognize better threat-based scenarios for IPV cases using a smart lock. Within their work, they classify IPV as a system-based issue in IoT. Their approach adapts the four-question approach developed by Shostack, which asks designers to pose questions about their design model [54]. Through this model, the researchers argued that research in IPV tech abuse can be enhanced to critique IoT for problematic designs. As for identifying threats, the researchers argue that profiling attackers are often based on assumptions and stereotypes. In addition, the lack of diversity in cybersecurity means these assumptions are problematic. As a result, system-based approaches, in their opinion, are easier for developers.

Slupska and Tanczer [30] also recognized that building a comprehensive threat model IPV in the context of smart devices may eliminate the possibility of more UI-based attacks that are easily perpetrated through the use of smart home devices. For smart homes in general, they determined that a threat model of IPV for IoT requires the examination of the following threats: ownership-based access, account/device compromise, information exposure, harmful messages, and gaslighting, though this was not a comprehensive list of all the attack vectors of IPV.

In addition to threat modeling IPV, Slupska et al. [48] also proposed a feminist cybersecurity practice coined "participatory threat modeling" which suggests the use of workshops and open discussions to demarginalize common threat modeling bias. To do this, the authors held a series of workshops with community activist groups as well as survivors, where they asked participants to define their own cybersecurity threats and fears. Their findings revealed that the discovered barriers between users' experiences and cybersecurity practices introduced new considerations in community based approaches to threat modeling. Interestingly, rather than asking developers to consider cybersecurity, this process asked users to bring up a series of issues they were facing, which in part provides stronger resources for the security community when recognizing threats to their products.

2.6 Summary and Analysis of Literature Gaps

The literature surrounding SH-IoTFA, while relatively new, takes on many approaches to identifying solutions, perpetrator motivations, and the ways that IoT abuse can be facilitated. Though the literature is becoming more substantive, there is a lack of focus on solutions within IoT design approaches. In general, papers demonstrating SH-IoTFA as an issue tend to focus on qualitative analysis with a small number of individuals, creating much research without substance. This gap within the literature can be built upon through a more robust establishment of testing methodologies, including more a more comprehensive analysis of how abusers are using technical features to perpetuate abuse. More substantive data analysis on abuse cases is necessary to improve research on SH-IoTFA. In addition, current research is gender-biased toward cisgender women, leaving behind the perspectives of men, members of the LGBTQ community, the elderly, and children experiencing abuse.

Another shortcoming that literature on SH-IoTFA faces is the use of different terminology for the same subjects. Many works often define smart home device abuse under the general term of IoT, but this is too vague given the vast scope of technologies that IoT devices fall under. This can provide general confusion to the technological categorization of abuse faced by IPV victims and survivors. The confusion identified during this literature is well established as many papers blur the line between what should be considered generalized TFA and smart home device-specific abuse scenarios. As it stands in the literature, there is also a lack of technical analysis of SH-IoTFA and the establishment of concrete features which facilitate abusive behaviors. If there is more recognition of the technical features that facilitate abuse, then the research can improve smart home development. Though there are limitations with the scope of the current research, the improvements will depend on further data collection and identifying specific functionalities that may enable abuse.

The common industry approaches and the models presented for threat modeling do not fully capture the importance of evaluating user behaviors and the capacity to perpetrate abuse. Using a system-based design to model IPV fails to demonstrate how these behaviors are significant cybersecurity issues and narrowly focuses on the technical threats and design. In threat-modeling SH-IoTFA, the current approaches overlook perpetrator motivations and focus heavily on system downfalls and victim perspectives rather than identifying how the features of an integrated system may aid in abuse facilitation. In addition, there is an inherent lack of understanding of how easy it is for perpetrators of abuse to cross a line into using smart home devices as an extension of their abuse. While recognizing system-centric approaches is important in threat modeling, the approach may ignore IPV behavior patterns. As such, improvements need to be made in identifying how we can truly recognize IPV threats in smart home products. Participatory threat-modeling also lacks the necessary structure needed to document how design is a factor in user cybersecurity downfalls. Furthermore, while the argument that the cybersecurity industry lacks diversity may be valid without multidisciplinary perspectives, neglecting attacker approaches based on these assumptions does not create concrete avenues to understand the inherent relationship that the abuser has with the smart home devices and how this relationship ultimately affects victims.

Chapter 3

Methodology

3.1 Introduction

This chapter provides an overview of the methodology used within this thesis. The methodology includes building upon previous qualitative research, specifically citing SH-IoTFA experiences, to analyze common themes and conclusions. Furthermore, the research will build upon general threat model structuring to demonstrate how interpersonal cybersecurity threats can be modeled in a customizable process.

3.2 Secondary Data Collection

Secondary data may be collected by reviewing sources, including academic books, journal articles, government reports, and reviews [57]. Contextually, testing for functionalities that may facilitate abuse comes down to building off of previous qualitative research in which victims, specialists, professional support, and even perpetrators describe their experiences with SH-IoTFA. Many of these experiences within the data were specifically connected to the insecure design and privacy parameters in general technology and IoT devices. Moreover, several papers have already been added to SH-IoTFA research using a qualitative approach. From this research, classifications and discussions of abuse experienced by SH-IoTs have been documented. This research firmly establishes the threat scenario and provides design considerations by building off of previous qualitative work. Limitations with qualitative research on this subject includes a primary focus on case studies and user experience rather than a focus on the technical issues that may encourage abuse. In addition, most, if not all of the qualitative papers define SH-IoT abuse from abusive experiences in heterosexual relationships, which narrows the experiences.

The literature was selected from the repository of papers collected for the initial literature. Specific databases included searches using Google Scholar, IEEE Xplore, and ACM. The literature was then selected by using the tagging feature in Zotero. Specifically, literature found under the tag "qualitative," "Smart Home Abuse," "IoTFA," "interview," "technology abuse," and "case studies" were analyzed. The papers were then manually reviewed to ensure that they met the specified criteria of this thesis. Papers selected for the review were then categorized based on their results/discussion of the interview and forum data, though many of the results were similar. Considerations in the uses of literature came down to if the research sought to understand how SH-IoTFA within the smart home occurred and used structured or semi-structured interviews, focus groups, and forum data to determine research conclusions. The questions used within the qualitative studies were also relatively similar.

The recognition that the issue of SH-IoTFA has already been researched and understood to some extent creates a stronger contribution to the field by providing a model that goes beyond examining victim and survivor experiences to provide a comprehensive understanding of the threat scenario. Qualitative data in this regard also presents the ‘how’ and ‘why’ to illustrate the main contextual scenarios in which SH-IoTFA occurs. It is important to note that the secondary data will be used to inform general themes and does not inform the entire framework. Distinction will be made in Chapter 4.

3.2.1 Literature Analyzed

Given the complex nature of SH-IoTFA, there are several qualitative research papers in which victims, specialists, and professional support describe their experiences. As such, the qualitative analysis of current literature identifies device threats within the threat model and plans for features that may aid perpetrator motivations. The papers analyzed as the main source of secondary data included works from Cuomo and Dolci [58], who conducted six in-depth, open-ended qualitative interviews with survivors of TFA and fifty in-depth, semi-structured interviews with system professionals who work with survivors, including advocates, law enforcement, prosecutors, judicial officers, and civil attorneys. Tanczer et al. [59] interviewed 15 IPV experts in the United Kingdom. Leitão [9, 33] reviewed and interviewed qualitative data from survivors through semi-structured interviews and forum data. McKay and Miller [60] evaluated case studies based on lived SH-IoTFA examples drawn from various sources. Apthorpe et al. [23] interviewed households with multiple users to better understand the tensions that existed in device usage. In the same scope, Ehrenberg and Keinonen [37] conducted a series of semi-structured interviews with five households where the residents installed multiple smart systems of various kinds. Geeng and Roesner [61] conducted semi-structured interviews with participants who owned smart devices. Finally, Tan et al. [62] administered 14 semi-structured interviews with smart home camera users to analyze their experiences of surveillance.

3.3 Attacker-Centric Threat Modeling Methodology

The attacker-centric approach focuses on identifying potential attackers, their threat profile, capabilities, and motivations [63]. This process often requires extensive intelligence about the threat actors and can be tedious as industrial applications of threat modeling. The extensive sociological and psychological research on IPV perpetrators provides us with a deep understanding of the attackers, their capabilities, and their motivations for their behaviors. By extension, this research adds diverse perspective to minimize pre-concieved bias established by developers. Deploying a model based on the attacker also allows for better integration of HCI research on abuse to establish intention and hypothesize theoretical attacks based on the user's intentions. Rather than take a system-based approach, where we analyze the IoT vulnerabilities from a technical perspective, social examinations analyze the nuanced threats in social environments. The threat model was developed through an analysis of selected literature and supplemental research to break down common themes found with the attacker and their motivations. Once the motivations were understood, the analysis also informed assets at risk and device features that enabled abuse. This model then informed an analysis of the Google Nest Hub in Chapter 5.

3.3.1 Modified Attack Trees

The Attack Tree provides a methodical model for describing all possible ways a system can be attacked and the countermeasures to protect from an attack. Attack Trees are arguably the oldest and most widely used approaches in threat modeling. Introduced by Bruce Scheiner in 1999, attack trees are graphs or diagrams portraying attacks against a system or an asset. In tree development, the tree's root node is the attacker's goal, and the corresponding leaves are how the goals will be accomplished.

Each attack goal is generally represented by separate trees, resulting in a forest of attack trees [64]. While the use of general-purpose trees is often challenging and can become muddled down by multiple possibilities, attack trees can also be used to understand motivations and intention. Researchers have also used attack trees to monitor insider activities for threats such as insider trading and malicious behavior. Specifically attack trees can be customizable based on the target as a way to understand the different avenues that can be taken to accomplish their attacks [65]. In this thesis, attack trees have been utilized to establish the relationship between an abuse perpetrator and the device to harm a victim. To accomplish this, SH-IoTS were categorized based on their features and analyzed for their potential harm.

Chapter 4

Threat Modeling SH-IoTFA

4.1 Introduction

This chapter introduces the overall threat model to illustrate SH-IoTFA as a cybersecurity threat. The structure of the threat model outlined in this chapter includes the following:

1. Identification of threat agent, motivations, and capacity to facilitate IPV using SH-IoTs
2. Identification of the victim's assets that may be vulnerable to IPV perpetrators
3. Identification of consumer smart home device threats to SH-IoTFA and categorization of the identified threats based on threat agent motivations
4. Proposal of recommended countermeasures to mitigate threats

Through the chapter, this thesis will establish a threat relationship between an attacker and victim as well as demonstrate how themes uncovered in previous literature are accomplished due to design affordances that have been overlooked by IoT developers. Furthermore, this chapter will provide an analysis of possible abusive affordances based on the attacker and their defined motivations.

The outline of Chapter 4 is as follows: Section 4.2 outlines the threat agent in SH-IoTFA scenarios and provides an analysis of their behaviors, demographics, motivations, and their capacity to carry out their attack against a victim. Section 4.3 identifies the “human assets" of victims at risk from IPV perpetrators. This section identifies their importance to victims and the consequences of target attacks against these assets. Section 4.4 examines how a threat agent may gain access to the device. Section 4.5 analyzes the devices mentioned within the literature and conceptualizes common device features which may empower abuse perpetrators. This section provides further analysis by developing attack trees that map how perpetrators can utilize the threats and accomplish their goal of attacking the victims' assets. Section 4.6 proposes possible mitigation approaches that discourage abusers from using smart home technology. Finally, Section 4.7 summarizes the steps in the threat model.

4.2 Threat Agent, Motivations, and Capacity

4.2.1 Threat Agent

The threat agent in this model is classified as a male IPV perpetrator with access to a consumer smart home device. While it is important to note that females can also perpetuate IPV, technology adoption and uptake are gendered, with men more likely to adopt smart devices than women. Literature defining the victim's experiences with SH-IoTFA is also overwhelmingly geared towards experiences where the victim is female, and the perpetrator is male [60]. In an extensive study of female and male students to determine gender differences in IoT consumer perceptions, women were found to be less familiar with and less likely to use IoT devices than men. When female students adopted these devices, they also did so for personal security rather than for recreational use [66]. Furthermore, female victims of smart home-based domestic violence reported that they felt less technologically competent than their male abuse perpetrators [19].

Given the novel nature of SH-IoTFA, there is no concrete analysis of the demographics and characteristics of the abuse perpetrators. However, abuse preparation of this nature can still be considered an extension of traditional IPV and TFA behaviors. Abuse perpetrators are often described as highly motivated, controlling, and lacking trust in their victims [67]. In an analysis of IPV perpetrators' behaviors through online infidelity forums, Tseng et al. [68] identified that characteristics also included justifying abusive behaviors based on perceived infidelity by their partner. By joining forums, these perpetrators also create an echochamber through a community that supports their abusive behaviors. Other behavioral aspects include exploiting power imbalances. In many instances perpetrators seek to have full control over the victim's life in all stages of the relationship. It is important to note here that various SH-IoTFA threats have been identified, including the physical control phase, the escape phase, and the life apart phase [11]. At each phase, the threat agent perceives themselves as losing control. Perpetrators of IPV at the end of a relationship may experience increased emotional distress and feelings of rejection, which can lead to violent and controlling behavior [29, 69, 70]. The threat agent is motivated to preserve their power over the relationship and will attempt to use any means necessary to ensure that the victim remains in the relationship and under their control [68].

4.2.2 Threat Agent Motivations

Threat motivations are inherently tied to feelings of control, the need to threaten and intimidate a victim into exerting power, and isolating a victim from friends, family, and access to medical and advocacy care. Perpetrator motivations include using SH-IoTs to surveil and monitor their partners and children and exert control without being physically present [37,60,71,72]. Perpetrators also exercise manipulative tactics to create power imbalances and ensure their control over a victim [33,60–62,72,73]. As such the threat agent motivations can be categorized as *Surveillance and Omnipresent Control, Ensure Power Imbalance,* and *Psychological Manipulation and Harassment.* These categorizations are further examined below.

Motivation 1: Surveillance and Omnipresent Control

Attackers exert both surveillance and remote control over their victim/survivor with the intent to monitor their actions closely. As a supplement to the conclusions of the secondary research, psychological research conducted by Ashdown et al. [74] revealed that digital surveillance is often perpetuated when the abuser fears rejection or feels jealous of their partner's other relationships. Access to digital surveillance technology also amplifies previous controlling behavior. Omnipresent control operates as an extension of surveillance, in which a perpetrator constantly monitors the victim/survivor to ensure they are isolated from friends, family, or support professionals. Beyond that, it completely erodes their privacy. Stark [18] identified that perpetrators who seek omnipresent control often position themselves as all-knowing to force behavioral constraints on the victim by letting the victim know that they are being watched. Much like Foucault's Theory of the Panopticon, surveillance is used as a disciplinary tactic; those under surveillance change their behaviors and self-censor themselves [75]. This is a tactic for threat agents to ensure that the victim never feels alone and modifies their behavior as to not anger the perpetrator.

Motivation 2: Ensure Power Imbalance

Abuse perpetrators attempt to create a power imbalance in the relationship to exert more control. When the perpetrator has more control, there is a higher likelihood that the victim will have to rely on them. Abuse perpetrators often use their victim's partner's lack of knowledge or access to a smart device to ensure a power imbalance. This power imbalance can be executed through several means, including financial control, restricting victims' access to home appliances, and ensuring that victims maintain no ownership within their environment [46]. Geeng and Roesner [76] cited that unequal account controls whether that be through a mobile device or SH-IoTs often opened doors for threat agents to execute power imbalances. In cases like this, the threat agent maintains their autonomy while ensuring that the victim loses theirs. Moreover, when perpetrators seek to ensure power imbalances, they may also use coercive means to isolate a victim from friends and family by removing their independence.

Motivation 3: Psychological Manipulation and Harassment

A perpetrator of SH-IoTFA may be motivated to manipulate their victims through various tactics, including gaslighting, humiliation, and intimidation. Gaslighting is generally defined as a form of psychological abuse where the abuser creates harm and denies creating that harm, which causes confusion for the victim [77]. An example of this would be changing the settings on a device (such as a thermostat) remotely and then denying making any changes to the victim's face when they question what happened. In stages where the relationship may end or has ended, the perpetrator may be motivated by their anger and feelings of rejection to blackmail a victim. Blackmailing can include forcing the victim to give into their demands by capturing illicit images or remotely threatening the victim [9, 60, 72, 78]. The perpetrator may also seek to undermine their victim's credibility, especially when law enforcement is involved or in cases where there may be a custody battle. Alexis Moore, an Attorney and domestic violence advocate, described in her book *Surviving a Cyberstalker: How to Prevent and Survive Cyberabuse and Stalking* an instance where she was working with a client whose abuser would repeatedly unlock her home and car doors through his remote access. When she reported it to law enforcement, the abuser petitioned the judge in their custody battle, citing concerns about safety in an attempt to paint the victim as an unfit mother [77, 79].

Surveillance and Omnipresent Control	**Ensure Power Imbalance**	**Psychological Manipulation and Harassment**
1. Isolate victims from friends, family and support 2. Erode victim privacy 3. Track online searches 4. Enforce behavioral changes 5. Create constant fear of monitoring	1. Restrict device access for victim 2. Make victim reliant on perpetrator 3. Amplify physical power imbalances	1. Remotely change device to harass or gaslight victim 2. Use devices to blackmail or gain access to elicit information 3. Threaten victims within their home 4. Cause emotional distress

Table 4.1: Summary of attacker motivations

4.2.3 Threat Agent Capacity

Given that threat agents are often highly motivated, they may also use any avenue they have to gain control of the device. According to Slupska and Tanczer, SH-IoTFA perpetrators often have intimate knowledge about their victim and insight into their daily activities and habits, as well as their login credentials [30, 80]. There are several questions that a developer must take into consideration regarding the abuse perpetrator in SH-IoTFA cases. For example, ownership of the device, proximity to the device, the number of devices in the environment, and the threat agent's technical skills all play a key role in determining their ability to execute attacks against the victim's assets.

Question 1: Does the threat agent live with the victim? Or are they separated from the home environment?

If the threat agent lives with the victim, they have access to the victim's information, computers, daily patterns, and the people they are interacting with. The threat agent has full access to the devices and the full capacity to monitor, harass, and exert control over the victim. If the victim does not have access to the home environment, we assume that the threat agent will do whatever is necessary to gain access and control the victim. They may do this by escalating harassment and threats through their access to the smart device. If the perpetrator does not have access to the physical device, there is a likelihood that they may escalate to using harassment and threats through their remote access [69].

Question 2: Does the threat agent own the device(s)? If not, do they have the device credentials?

If the threat agent owns the device or maintains the primary account, they will have more control over the device and more power than the victim. The threat agent may restrict access or ensure that the victim only knows about certain device capabilities. If the perpetrator does not own the device, they may use other means to gain access. Freed et al. [35] reinforced that perpetrators often gained access to passwords and other important information during the "good" phase of the relationship. Once the relationship turned "bad," perpetrators often used that initial trust against the victim. For example, in the honeymoon period of the relationship, the threat agent may have been the person who set up the device and gained access to the victim's credentials and then later in the relationship, they use that same access to enforce control over their victim.

Question 3: Does the threat agent have technical skills?

While much of the current research argues that SH-IoTFA perpetrators do not need advanced technical skills to carry out abuse, it is still vital to plan for perpetrators who have more technical skills and will hack the device for monitoring, control, or harassment. Tseng et al. [68] found that abuse perpetrators would often seek to gain remote access onto their victims devices without their knowledge. Another concern includes imbalanced technology knowledge and usage within the home, which can allow abuse perpetrators to leverage their knowledge against the victim. Interestingly, Linder [81] cited a case in which the abuse perpetrator worked in tech who used their skills as an advantage and gained significant control over their victim's life through constant surveillance.

Question 4: How many devices are in the environment? What type of devices are present?

If there is more than one device in the environment, the threat agent has a larger capacity to carry out abuse. This is particularly true in environments where the devices are connected to one application or central hub [82].

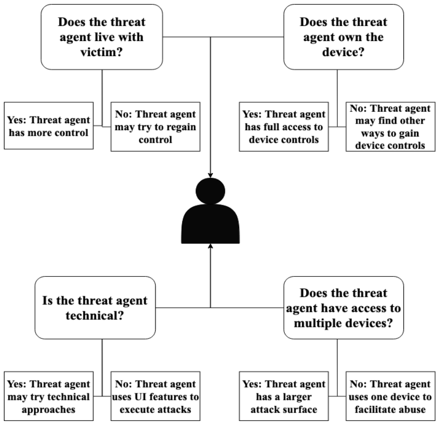

Does the threat agent live with victim?
Yes: Threat agent has more control
No: Threat agent may try to regain control
Does the threat agent own the device?
Yes: Threat agent has full access to device controls
No: Threat agent may find other ways to gain device controls
Is the threat agent technical?
Yes: Threat agent may try technical approaches
No: Threat agent uses UI features to execute attacks
Does the threat agent have access to multiple devices?
Yes: Threat agent has a larger attack surface
No: Threat agent uses one device to facilitate abuse

Figure 4.1: Summary of Threat Agent capacity.

4.3 Identification of Assets Affected by SH-IoTFA

In threat modeling, an asset is something of value that an organization or entity seeks to protect from third-party adversaries. As described in Chapter 2, 'human assets' are defined as the the electronic, physical, or non-tangible items of value to smart device users. Human assets are the social, emotional, and financial securities that users seek to uphold within the safety of their homes [56]. IPV victims frequently experience attacks against their communication avenues, sense of safety, and privacy [9]. Other avenues for abuse include targeting a victim's self-autonomy and financial control over their accounts [83]. Through targeting these assets, the abuser can establish their control over the user, which has been the common experiences of IPV victims. The most commonly targeted assets include security, privacy and private data, financial control, personal relationships, and self-autonomy. The value of these assets to a victim is analyzed below.

Asset 1: Security

According to a survey by Digital Media Solutions, 17% of consumers adopt smart security devices for increased security or home protection [84]. Smart devices, specifically alarms, have also been presented as a safety solution for female victims of sexual assault. This solution lacks recognition of how the alarm increases the attack vector for the victim rather than minimizing their threat landscape [9]. Perpetrators of IPV may seek to attack a victim's sense of security by gaining control of security devices to intimidate and threaten a victim, further increasing feelings of insecurity within their home. This can be true for scenarios where the perpetrator lives with the victim or in a survivor scenario when the relationship has ended.

Asset 2: Privacy and Personal Data

Within the home, privacy can be exploited by perpetrators of SH-IoTFA as a way to monitor the behaviors of the victim/survivor, whether that be monitoring when they come and go to the house or tracking internet searches and usage. In addition, a lack of privacy between users also increases the likelihood that more controlling behaviors can occur without the victim knowing, simply because they were interacting with a device [62]. Abusers will frequently utilize digital technologies, including smart devices, to collect private information about a victim to harass, humiliate, or tarnish their reputation. An extreme example is capturing and posting illicit images or embarrassing information about the victim on social media [35].

Asset 3: Financial Control

Financial abuse occurs in 99% of IPV cases [85]. According to the National Network to End Domestic Violence, IPV survivors cite concerns about providing for themselves and their children as one of the top reasons for staying or returning to an abusive partner [86]. Financial abuse through shared devices and accounts is common in retaining victim dependency and full control over the relationship. Smart devices that link bank accounts and shopping accounts create increased threats to victims' financial assets and are an appealing feature for IPV abuse perpetrators [69].

Asset 4: Emotional Well-Being

Protecting emotional health is vital to ensuring that survivors or victims do not succumb to unhealthy behaviors. An IPV perpetrator could use devices for harassment or even gaslighting to make the victim/survivor question their decisions and constantly live in a state of distress. According to the National Institute of Health (NIH), IPV contributes to post-traumatic stress disorder and severely compromises the quality of life. Specifically, feelings of isolation, depression are commonly experienced by both victims/survivors of IPV [87].

Asset 5: Personal Relationships

Total isolation from friends and family is a tactic used in abuse scenarios. It not only makes the victim rely on their abuse perpetrator but also bars them from seeking professional help. The addition of a smart home device increases the ability of a perpetrator to restrict the victim's access to friends and family [22]. In several cases, victims revealed that surveillance tactics were often used to isolate them from their friends and family which effectively allowed them to exert their control without third-party input.

Asset 6: Self-Autonomy

Self-autonomy is the ability to make uncoerced decisions about one's life [88]. In an analysis of self-autonomy, Ciurria [89] identified the common misconception that abuse victims are weak or maintain personality traits that may make them more susceptible to abuse, overlooking the personal attack on personhood that victims often face. As a form of control, perpetrators of abuse will attempt to erode their victim's self-autonomy to ensure they are psychologically and physically manipulated from making sound decisions about their situation.

Asset	**Threat**
Security	Increased feelings of insecurity in home, loss of comfort, fear of retaliation
Privacy and Personal Data	Loss of autonomy, isolation, under constant surveillance, paranoia
Financial Control	Loss of financial control, fear of leaving relationship
Emotional Well-Being	Increased mental health disorders, loss of control
Personal Relationships	Isolation, inability to reach out for help
Self-Autonomy	Loss of control, isolation, difficulty making decisions

Table 4.2: Victim assets and threats

4.4 IoT Access Points

Access points define the interfaces through which potential attackers can interact with and potentially execute attacks. In SH-IoTFA scenarios, perpetrators of abuse can physically or remotely access the devices. Access and ownership can be analyzed through the following scenarios:

1. **Threat Agent Purchased the Device**

   a. Threat Agent Owns Device

   If the threat agent maintains ownership of the device, they can revoke or monitor a victim/survivor's access [13]. They may also have increased privileges and can use device features that other users do not. Furthermore, they can use the device by any means necessary which can include making changes to the device state without secondary consent.

2. **Victim Purchased the Device**

a. Perpetrator Helps Victim Set Up Device

If the perpetrator helps the victim set up the device, they may secretly give themselves more access. They may also change account credentials to lock the victim/survivor out [90].

b. Perpetrator Does Not Have Initial Access

If a perpetrator does not have access, they may use previously accumulated knowledge of the victim's credentials to gain access. The perpetrators may also coerce or threaten the victim to give them device credentials [72].

4.5 Identification of IoT Threats and Their Role in Empowering Abuse Perpetrators

This section discusses the findings from the analysis of qualitative research on SH-IoTFA. Specifically, this section explores the common features of SH-IoTs manipulated by threat agents and analyzes the thematic similarities of abuse experiences of interviewed victims. Within this section, this research analyzes common IoT devices mentioned in the literature and evaluates their role in amplifying social threats. The devices were also categorized by their capabilities and common uses to demonstrate the different features that afford abuse perpetrator.

4.5.1 Devices Mentioned In Literature Synthesis

Within the qualitative literature, various smart home devices were mentioned including the Google Home Hub, CCTV cameras, smart doorbells, Amazon Alexa, Amazon Echo, and home-security systems [23, 33, 60, 62, 76] Smart Locks, Nest Thermostat, Smart TVs [60,71,76], Nest cameras, "nanny cams" or remotely accessible baby monitors [62,91], Smart Lights, WifI [60], CO2 Meters, Voice User Interfaces [37], Amazon Dot [76], and the Wyze Cam [62]. Of the devices mentioned, Amazon Echo and Alexa, Nest Thermostats, Smart Doorbells, nanny cams, and CCTV cameras were the most common devices mentioned in SH-IoTFA cases. SH-IoTs were categorized based on the differing functionalities of the devices mentioned to separate victim experiences by device capabilities. For purposes of this thesis, the devices were placed in the following categories: *IoT for Security, IoT for Convenience,* and *IoT for Home Automation*, and analyzed below.

1. IoT for Security includes cameras, smart locks, doorbells, and smart sensors. These devices can monitor access to the home and view any anomalous activity happening while the user is away from home. Security devices maintain common features such as cameras, connected applications to view live feed and audio, and notifications of movement or activity. IoT for Security also maintain assets such as personally identifiable information (PII), the physical device, smart lock pin codes, or remote capabilities to lock/unlock the door.

2. IoT for Convenience may include hubs, smart speakers, personal assistants, and smart TVs. Personal assistants such as the Echo Dot and Google Nest Hub were mentioned in the literature and smart TVs. Often the devices are used to allow for increased functionality within the smart home by controlling other devices.

3. IoT for Home Automation includes smart thermostats, smart lights, and any other smart appliances within the home. These devices are often used to monitor home environments by providing users alerts and insight about their appliances.

4.5.2 Device Threats to SH-IoTFA Manipulation

Current qualitative literature demonstrates common themes in SH-IoTFA cases. Specifically, research has provided three overarching themes.

1. SH-IoTs facilitate undesired monitoring and surveillance
2. SH-IoTs facilitate power imbalances in multi-user environments
3. SH-IoTs facilitate harassment and antagonistic behaviors

The themes in the literature point to a correlation between attacker motivations and features that empower these motivations. Attacker motivations and their capacity also play a key role in the relationship between the agent and the abusive capabilities afforded by a smart home device. Though the motivation is not explicit within the human-computer dialog, the hidden affordances that exist allow the attacker to target victim assets with relatively low stakes. This will affect how some of the most common features provide abuse perpetrators with accessible methods for abuse based on the intention of the user. Below, common device features will be analyzed as possible vulnerabilities that correlate to these themes, as well as all of the potential and hidden abusive threats. Once threats are established, attack trees will then demonstrate the direct relationship between the attacker, their abusive affordances, and the assets targeted.

Theme 1: SH-IoTs facilitate undesired monitoring and surveillance

SH-IoTs can facilitate surveillance and monitoring. Privacy controls and preferences are often undermined out of convenience in the device design, or even by the very nature of the device's use. Within several of the reports on SH-IoTFA, stakeholders identified several cases in which smart home devices were used as surveillance tools against a victim of IPV. There are several convenient features identified in the analyzed qualitative papers that allow this to occur. These features include that perpetrators have remote access to the device via a mobile application and perpetrators maintain access to device usage logs. While not explicit features, survivors and support professionals also argued that a lack of clarity about device data collection also allowed perpetrators to use the devices for surveillance.

Vulnerability 1: Remote Monitoring of Device Video/Audio Feed

Within the parameters of case studies and interviews with victims and professional support, almost all papers revealed that remote monitoring of devices with audio and video recordings such such as security cameras, doorbells/locks, and even some voice assistants, allowed perpetrators to surveil their victims [9,23,60,62,92]. The specific features that facilitate this behavior included that within smart home environments, abusers are often the administrative user of the device, giving them full access to all monitoring tools. The impact of full access immediately means that the perpetrators do not need to be physically close to their victim's device or know the device's credentials to maintain control and monitor the surroundings of their victims.

Remote monitoring and subsequent surveillance of a partner may not even be conscious for some users. Ehrenberg and Keinonen [37] revealed that some users were frustrated with other housemates monitoring the devices. The researchers argue that the monitoring of other users via remote access, may not be through malicious intent, but the nature of the devices makes it more natural to monitor other housemates and guests. Despite the lack of malicious intent in one case, Cuomo and Dolci [58] found that remotely accessing the video feed allowed abusive partners to go to work or leave the house and still maintain control over the victim. In addition, victims are aware of the video surveillance which may lead them to be fearful within their own homes. Building off of this idea, Tanczer et al. [72] interviewed a support practitioner who revealed that remote access to IoT devices increased the severity of physical IPV cases by expanding the capability of abusers to monitor their victims. In effect, perpetrators become an omnipresent threat that victims fear is always watching.

Vulnerability 2: Activity/Usage Logs

Victim experiences also included surveillance through history and usage logs. While not as common with devices for security, access to usage logs allowed perpetrators to review images or activity after the victim had interacted with the device. Moreover, the activity logs allow perpetrators to monitor a victim retroactively. In the case of smart locks, an abused perpetrator may be able to view the history logs if the door is unlocked. Not only is this a safety hazard in general, but it could threaten the victim's physical security, especially in scenarios when the perpetrators have been removed from the home.

IoT built for convenience has audio and sometimes video features. However, their functionality differs from the security devices and maintains significant threats to victims related to using smart assistants and other user-based command systems. Smart assistants and smart TVs have access to the internet and internet search history subject to monitoring. In some cases, usage logs amplify abuse by revealing when the victim is trying to seek help. One research participant mentioned that if a victim calls the National Domestic Violence Helpline number using a smart home device, it could come up in the event logs, signalizing to the perpetrator any attempts to escape [33]. Leitão [9] also revealed that usage logs allowed abusers to remind victims that they are under surveillance. For example, if the victim had asked a smart assistant to turn on music, the perpetrator could come home and ask if they liked the music they listened to, as a reminder that the victim is never truly alone.

Threats: IoT for Security

1. *Cameras:* Abuse perpetrator could access and live stream the audio or video feed without the victim knowing. Abuse perpetrator also capture illicit images and embarrassing information about the victim. This could allow them to exert more control by threatening to embarrass or release images.

2. *Cameras/Doorbells:* Abuse perpetrator could receive notifications when the victim comes into view of the camera. This may incentivize them to watch the victim during the day.

3. *Cameras/Doorbells:* Abuse perpetrators could access the history logs and retroactively monitor the victim. This may allow them to track what the victim did throughout the day.

4. *Smart Locks/Doorbell:* Abuse perpetrator may monitor when the victim leaves and when they come home via notifications from the device or the history logs. This may lead to victim isolation and allow the abuse perpetrator to exert further control over the victim.

Threats: IoT for Convenience

1. *Smart TV/Smart Assistant:* Abuse perpetrator may access the activity logs and monitor the victim's interactions and web activity. This could give the perpetrator access to whom the victim is talking to and what they are searching for. In extreme cases, the activity may reveal the victim attempting to leave the relationship.

2. *Smart TV/Smart Assistant:* Abuse perpetrator may monitor what media the victim is consuming. Using this knowledge, the abuse perpetrator may seek to control access to entertainment.

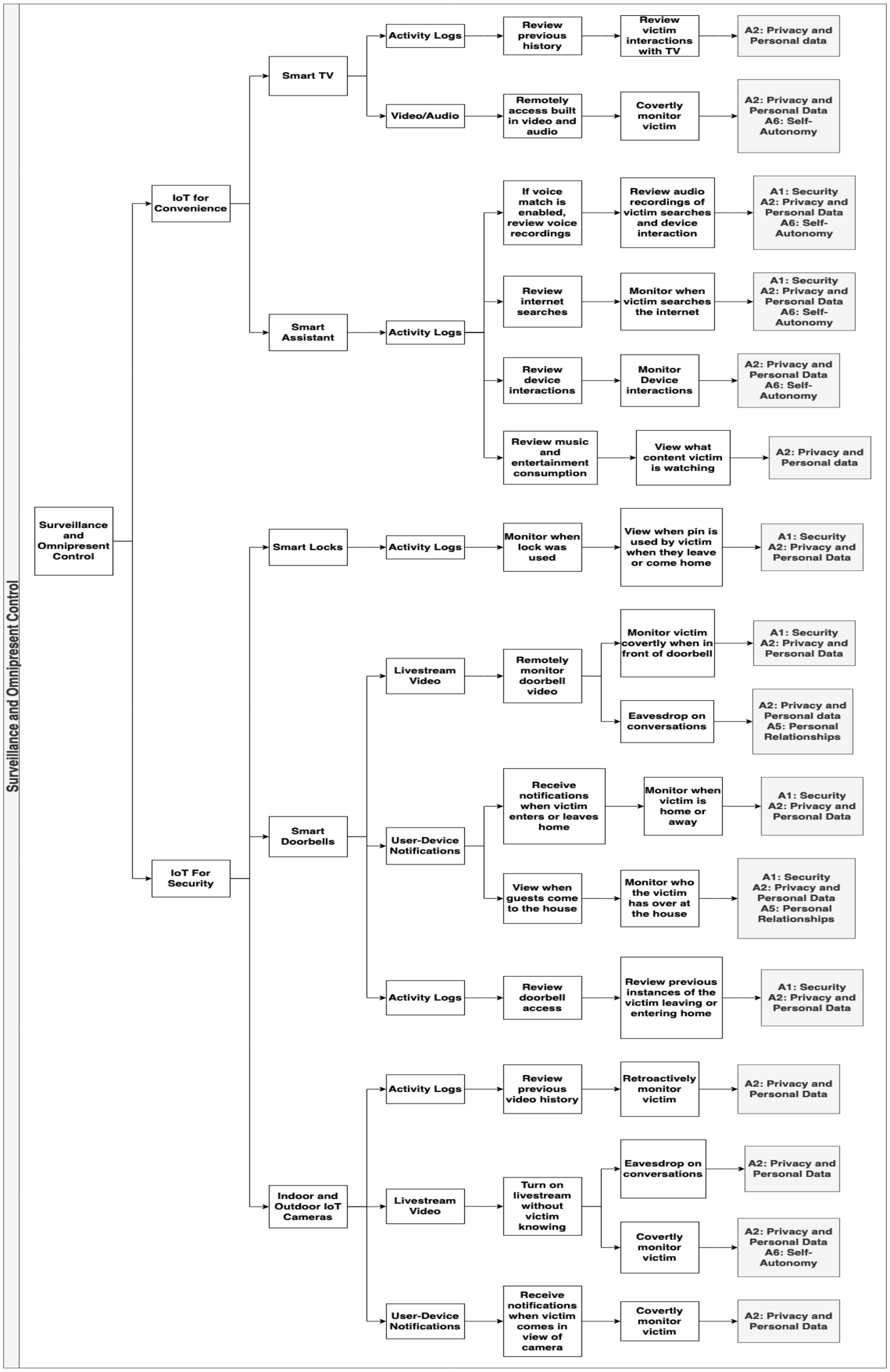

Surveillance and Omnipresent Control
Surveillance and Omnipresent Control
IoT for Convenience
IoT For Security
Smart TV
Activity Logs
Review previous history
Review victim interactions with TV
A2: Privacy and Personal data
Video/Audio
Remotely access built in video and audio
Covertly monitor victim
A2: Privacy and Personal Data A6: Self-Autonomy
Smart Assistant
Activity Logs
If voice match is enabled, review voice recordings
Review audio recordings of victim searches and device interaction
A1: Security A2: Privacy and Personal Data A6: Self-Autonomy
Review internet searches
Monitor when victim searches the internet
A1: Security A2: Privacy and Personal Data A6: Self-Autonomy
Review device interactions
Monitor Device interactions
A2: Privacy and Personal Data A6: Self-Autonomy
Review music and entertainment consumption
View what content victim is watching
A2: Privacy and Personal data
Smart Locks
Activity Logs
Monitor when lock was used
View when pin is used by victim when they leave or come home
A1: Security A2: Privacy and Personal Data
Smart Doorbells
Livestream Video
Remotely monitor doorbell video
Monitor victim covertly when in front of doorbell
A1: Security A2: Privacy and Personal Data
Eavesdrop on conversations
A2: Privacy and Personal data A5: Personal Relationships
User-Device Notifications
Receive notifications when victim enters or leaves home
Monitor when victim is home or away
A1: Security A2: Privacy and Personal Data
View when guests come to the house
Monitor who the victim has over at the house
A1: Security A2: Privacy and Personal Data A5: Personal Relationships
Activity Logs
Review doorbell access
Review previous instances of the victim leaving or entering home
A1: Security A2: Privacy and Personal Data
Indoor and Outdoor IoT Cameras
Activity Logs
Review previous video history
Retroactively monitor victim
A2: Privacy and Personal Data
Livestream Video
Turn on livestream without victim knowing
Eavesdrop on conversations
A2: Privacy and Personal Data
Covertly monitor victim
A2: Privacy and Personal Data A6: Self-Autonomy
User-Device Notifications
Receive notifications when victim comes in view of camera
Covertly monitor victim
A2: Privacy and Personal Data

Figure 4.2: Surveillance and Omnipresent Control: Attack tree outlining the possible surveillance attack vectors for an abuse perpetrator.

Theme 2: SH-IoTs facilitate power imbalances

Within multi-user environments, research reported that SH-IoTS effect the power dynamics in relationships by supporting unequal access between users. Specifically, there are power imbalances between the primary user who set up the device and secondary users [61]. The research frequently observed that SH-IoT adopters had extensively more control over the device features and administrative controls. This unequal device agency often pointed to the installer's ability to make initial device decisions [81].

Vulnerability 1: Multiple User Accounts

Unequal access to SH-IoTs empowered perpetrators of IPV to exert further control over the home environment [23]. The lack of agency for secondary users was also cited as a main factor of abuse. Geeng and Roesner cited that unequal account controls often opened doors to tensions between partners that did not previously exist. One example in their research included a scenario in which the primary user set up the smart TV but failed to give his girlfriend access to change the device settings via voice command, effectively eroding her autonomy to use the TV [76]. Voice constraints and other personalization techniques exacerbate this power imbalance. In a more malicious scenario, Leitão cited participants who detailed how abuse perpetrators intentionally give themselves increased access to a device to exert control over a user. Perpetrators could also fail to disclose certain privileges the device maintains to surveil their victims. In one case, a user kept their administrative privileges a secret from their partner so that they could catch them cheating via their shared Alexa device [93].

Vulnerability 2: Remotely Change the State of the Device

The ability to change the state of SH-IoTs while not at home is cited as a feature that creates power imbalances and is a source of conflict. Mckay and Miller argued that control over smart technologies often creates conflicts about who controls the environment. The researchers specifically cited power struggles related to temperature control and lighting. In one case, a woman in the UK experienced with her husband remotely changing the temperature to a lower setting even though she preferred a higher setting. In another case, a husband reported locking down his wife's ability to use their shared Google Nest thermostat because they also had different setting preferences. One woman also cited that her husband had a terrarium that needed blue light for the exotic creatures inside. He had made these lights a feature in the kitchen, and they could only be controlled through an app on his phone. After asking him to turn off the lights because they gave her migraines, he became verbally and physically aggressive [60]. The ability to remotely change the device's state can exacerbate power imbalances because no consent is required to change the settings. If the abuse perpetrator wants to exert control over the device, there is no parameter in place for the victim to stop the change from happening.

Threats: IoT for Security

1. *Cameras/Doorbell/Smart Lock:* Abuse perpetrators could restrict the user from accessing the device by not allowing them an account for remote application. If the smart lock does not have a physical key, the victim may have to rely on the perpetrator to lock and unlock the door. The victim may also be restricted from accessing the safety features alone at the house.

2. *Smart Lock:* Abuse perpetrators could change the PIN for the lock continuously. This would mean that the victim would have to ask for the PIN and rely on the perpetrator to let them in the home.

Threats: IoT for Convenience

1. *Smart Assistant*: Abuse perpetrators could restrict users' access by either not allowing them to be on the account or only allowing limited functionality. This

could mean that only the perpetrator can access personalization functions and other capabilities.

2. *Smart Assistant/Smart TV*: If financial accounts are connected, the abuse perpetrator could take advantage of the victim's accounts and unnecessarily spend money or block them from making purchases. This would mean that the victim's finances would be at the mercy of the perpetrator. In addition, if there are any features such as voice personalization, the victim may be unable to use their account for purchases via the device.

3. *Smart Assistant/Smart TV*: Abuse perpetrator could enable voice personalization for devices with that functionality and restrict the victim's access from interacting with the device.

4. *Smart Assistant/Smart TV*: Abuse perpetrator could override the victim's preferences by remotely changing the device's state. This could make the victim feel like they cannot interact with the device without permission.

5. *Smart Assistant/Smart TV*: Abuse perpetrator may use parental control features or filters to restrict how the victim uses the shared device.

Threats: IoT for Automation

1. *Smart Lights/Smart Thermostat*: Abuse perpetrator could restrict the victim from accessing control of the lights. Victims may need to rely on the perpetrator to use the device's capabilities. In cases where the victim is home alone, they may be unable to use the devices as intended.

2. *Smart Lights/Smart Thermostat*: Abuse perpetrator could override the victim's preferences by remotely changing the device's state. In this case, it could override environmental preferences rather than media and entertainment.

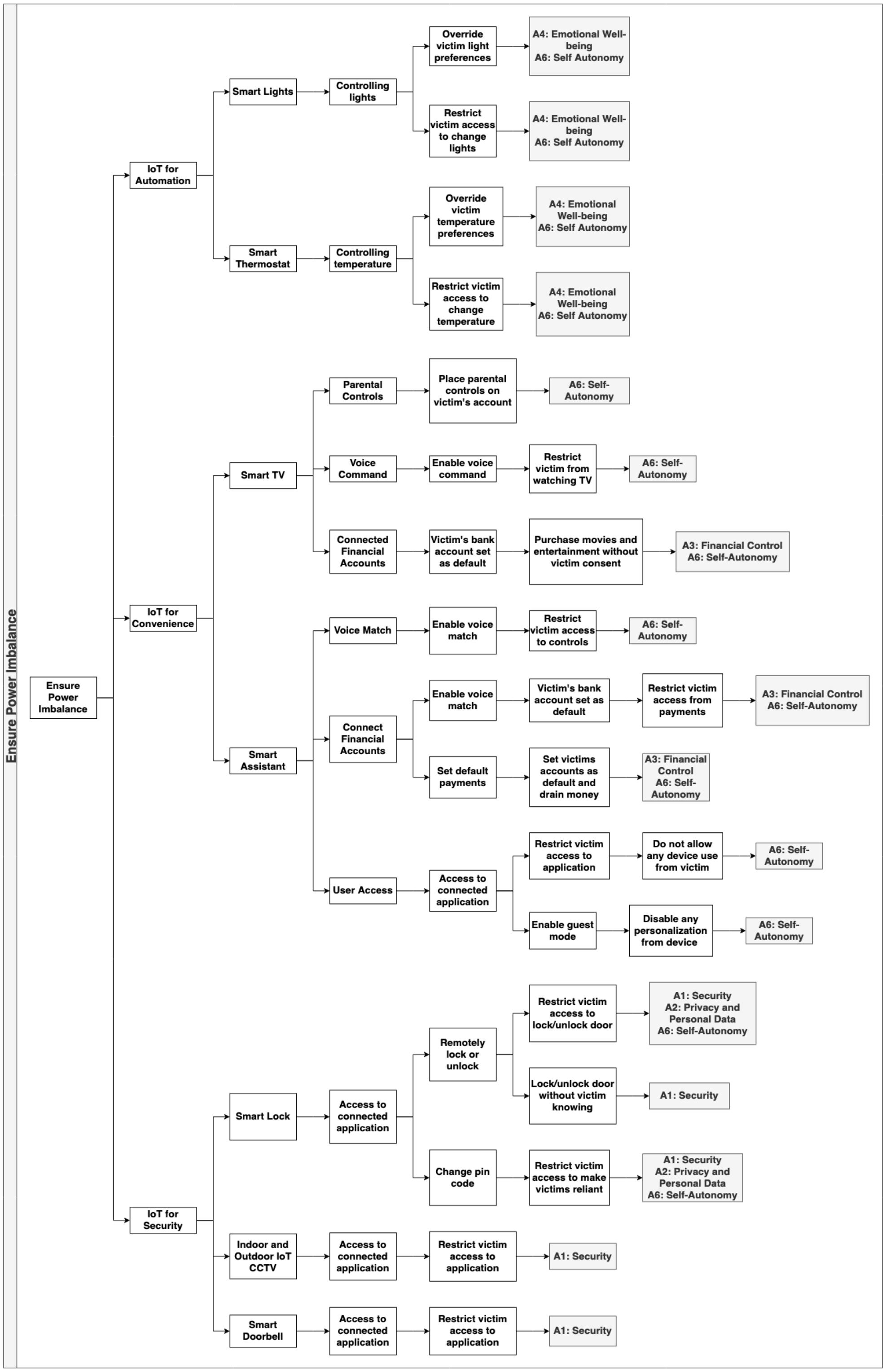

Ensure Power Imbalance
Ensure Power Imbalance
IoT for Automation
Smart Lights
Controlling lights
Override victim light preferences
A4: Emotional Well-being
A6: Self Autonomy
Restrict victim access to change lights
A4: Emotional Well-being
A6: Self Autonomy
Smart Thermostat
Controlling temperature
Override victim temperature preferences
A4: Emotional Well-being
A6: Self Autonomy
Restrict victim access to change temperature
A4: Emotional Well-being
A6: Self Autonomy
IoT for Convenience
Smart TV
Parental Controls
Place parental controls on victim's account
A6: Self-Autonomy
Voice Command
Enable voice command
Restrict victim from watching TV
A6: Self-Autonomy
Connected Financial Accounts
Victim's bank account set as default
Purchase movies and entertainment without victim consent
A3: Financial Control
A6: Self-Autonomy
Smart Assistant
Voice Match
Enable voice match
Restrict victim access to controls
A6: Self-Autonomy
Connect Financial Accounts
Enable voice match
Victim's bank account set as default
Restrict victim access from payments
A3: Financial Control
A6: Self-Autonomy
Set default payments
Set victims accounts as default and drain money
A3: Financial Control
A6: Self-Autonomy
User Access
Access to connected application
Restrict victim access to application
Do not allow any device use from victim
A6: Self-Autonomy
Enable guest mode
Disable any personalization from device
A6: Self-Autonomy
IoT for Security
Smart Lock
Access to connected application
Remotely lock or unlock
Restrict victim access to lock/unlock door
A1: Security
A2: Privacy and Personal Data
A6: Self-Autonomy
Lock/unlock door without victim knowing
A1: Security
Change pin code
Restrict victim access to make victims reliant
A1: Security
A2: Privacy and Personal Data
A6: Self-Autonomy
Indoor and Outdoor IoT CCTV
Access to connected application
Restrict victim access to application
A1: Security
Smart Doorbell
Access to connected application
Restrict victim access to application
A1: Security

Figure 4.3: Ensure Power Imbalance: Attack tree outlining the possible attack vectors for an abuse perpetrator to gain more control over a victim.

Theme 3: SH-IoTs facilitate harassment and antagonistic behavior

SH-IoTs were also found to encourage antagonistic behavior. Gaslighting was also a common occurrence in cases involving smart home appliances. Tanczer et al. [72], Leitão [33], and Woodlock et al. [22] found that victims and survivors had experience with cases that included gaslighting and unending harassment. In these cases, perpetrators intentionally changed the device status, changed the smart lock code, and removed permissions without the victim or survivor knowing. The perpetrator would then make the victim or survivor think they did not know how to use the device, rather than confirming that a change had been made.

Vulnerability 1: Remotely Change the State of the Device

Access to remote state changes for SH-IoTs allows perpetrators to remotely change the device state without the victim/survivor being notified. It can also be used as a harassment mechanism [58], such as periodically turning the lights on to let the victim know that the perpetrator is still present in their life.

Threats: IoT for Convenience

1. *Smart Assistant/Smart TV:* Abuse perpetrator could change the state of the device while the victim is home as a form of harassment. For example, they may override what the victim is watching.

2. *Smart Assistant/Smart TV:* Abuse perpetrator could change the state of the device without the victim knowing, like turning on music or turning off the TV. The perpetrator could then claim that they do not know what is happening and gaslight the victim.

3. *Smart Assistant/Smart TV:* Abuse perpetrators could override victim's entertainment or device choices to antagonize them.

Threats: IoT for Automation

1. *Smart Light/Smart Thermostat:* Abuse perpetrator could remotely change the state of the device, such as changing the thermostat to high heat or turning off the lights while the victim is at home.

2. *Smart Thermostat:* Abuse perpetrator could change the thermostat to extreme temperatures to make the victim feel uncomfortable.

3. *Smart Light:* Abuse perpetrator could remotely turn on and off the lights to harass the victim.

4.5.3 Summary

The device features maintain commonalities and differences in how abusers can empower themselves. While the above section identified common threats found in the literature, this section reveals how abuser motivations are effectively supported. The general analysis of *IoT for Security, IoT for Convenience,* and *IoT for Automation* revealed differing capacity levels to which devices could be used for abuse. For example, smart home security devices could be used by the abuser for surveillance and omnipresent control. They can also be used to enhance power imbalances. On the other hand, devices for convenience have high capacity for surveillance and omnipresent control, ensuring power imbalances, psychological manipulation, and harassment. Finally, devices for home automation can to be used to ensure power imbalances and psychological manipulation.

The themes and unified features that facilitate abuse demonstrate a lack of social considerations in the development process. While this list is not exhaustive, the qualitative analysis of SH-IoTFA experiences demonstrates the validity that UI features can enable abusive practices through unknown affordances. In addition, threat agents maintain remote access to change devices, which inherently creates a threat of abuse.

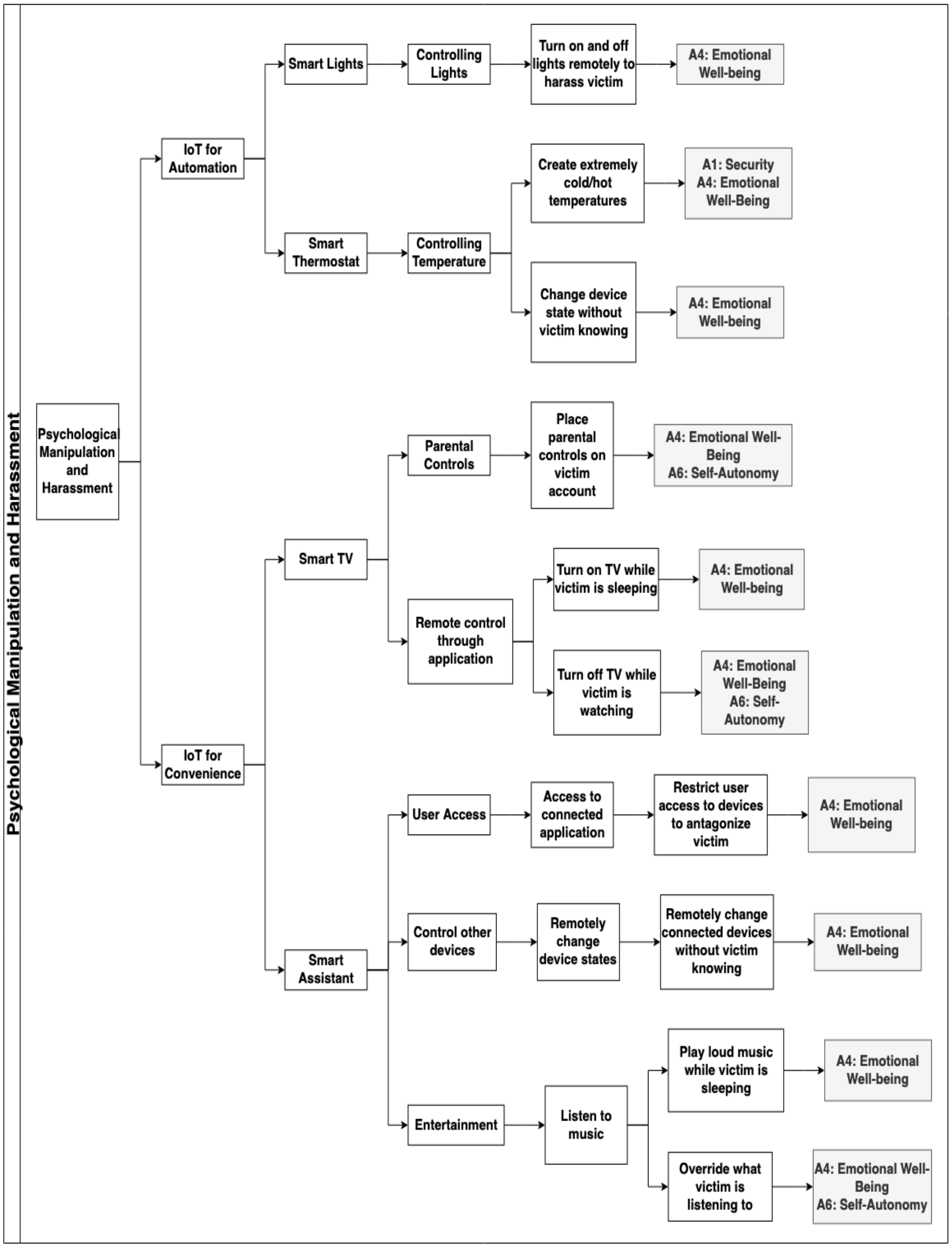

Psychological Manipulation and Harassment
Psychological Manipulation and Harassment
IoT for Automation
Smart Lights
Controlling Lights
Turn on and off lights remotely to harass victim
A4: Emotional Well-being
Smart Thermostat
Controlling Temperature
Create extremely cold/hot temperatures
A1: Security
A4: Emotional Well-Being
Change device state without victim knowing
A4: Emotional Well-being
IoT for Convenience
Smart TV
Parental Controls
Place parental controls on victim account
A4: Emotional Well-Being
A6: Self-Autonomy
Remote control through application
Turn on TV while victim is sleeping
A4: Emotional Well-being
Turn off TV while victim is watching
A4: Emotional Well-Being
A6: Self-Autonomy
Smart Assistant
User Access
Access to connected application
Restrict user access to devices to antagonize victim
A4: Emotional Well-being
Control other devices
Remotely change device states
Remotely change connected devices without victim knowing
A4: Emotional Well-being
Entertainment
Listen to music
Play loud music while victim is sleeping
A4: Emotional Well-being
Override what victim is listening to
A4: Emotional Well-Being
A6: Self-Autonomy

Figure 4.4: Psychological Manipulation and Harassment: Attack tree outlining the possible attack vectors for an abuse perpetrator to harass or mentally abuse a victim.

Interestingly, smart assistants have a higher threat surface than other devices due to their increased connectivity and direct command relationship with the user. Threats at the most basic usability level are cause for concern and represent a much larger issue in failing to recognize intersectional design approaches.

4.6 Possible Mitigation Approaches

This section recommends mitigation approaches within this framework to identify ways that developers of consumer IoT devices can discourage IPV perpetrators from using their products to abuse victims. While not exhaustive, these recommendations have been generated from the common themes identified above.

4.6.1 Mitigating Surveillance and Omnipresent Control

1. *Right to privacy between users:* If privacy control is shared within a home, inherently unequal treatment will also be discouraged. This could be implemented through a policy feature or a security control built into the device. For example if one user is at home, they should be alerted of remote access to video/audio features.

2. *Allow for restrictions to activity monitoring:* Activity monitoring within the home should be restricted to sensor communication and anomaly monitoring rather than documentation of every device interaction.

3. *Allow for users to disable indoor camera while at home.* In scenarios where the victim suspects that an abuser is using SH-IoT cameras to monitor their actions, there should be a control in place that allows them to disable the camera for a set period of time and block remote users from viewing camera feed.

4.6.2 Mitigating Power Imbalance

1. *Equal Distribution of Device Controls for Secondary Account Holders:* All adult members of the household must be given the same controls as the initial administrative member. This ensures that restriction is minimized.

2. *Consent Management for User Controls.* The ability to give consent for a specific feature and take away consent is vital to ensuring that interactions with smart home environments do not further the suffering or potential suffering that an individual may face in current or future interpersonal violence. For IoT, this consent would include identifying another individual's controls, multi-user consent for all set-up interactions, and taking away consent should the nature of any given relationship change.

4.6.3 Mitigating Psychological Manipulation and Harassment

1. *Notification for device state change.* When one account user sets a control feature on any smart device that may affect the other users, every account member will be notified of the change.

2. *Limit time in-between device state change.* If device status cannot be overridden except for a set period, abusers may lose the ability to exert control easily.

3. *Consent management for device changes.* If a remote user wants to make a device change while the other user is at home, the users at home will receive a notification if the remote user tries to change the device's controls.

4. *Disable remote control while one household member is home.* While one user is at home, there should be a feature that allows functionality for analog controls and disables remote control of the device. This would empower secondary users and ensure that the IoT device is not a point of contact for an abuser to mess with and antagonize a victim.

4.6.4 Generalized Industry Mitigation Approaches

1. *Diversify perspectives.* In the design, integration, threat modeling, and usability industries, there should be more interdisciplinary perspectives bringing their voice to system-based issues that may not have ever been addressed in the past. This may include having psychologists or victim advocates present during the threat modeling process. Given that the dynamics of abuse are so complex, it is vital to have a development system that provides an environment for discussing these threats.

2. *Design for multiple users.* Given that SH-IoTs are often marketed towards families, and multi-user environments, the relationships in those environments should be considered. Furthermore, interpersonal privacy and security should be implemented to ensure that devices can not be configured for abuse.

3. *Develop reporting systems for abuse.* If devices are used in abusive scenarios, it is recommended to have a reporting system that allows anonymous users to report abuse and verify what device feature enabled the abusive behaviors.

4.7 Framework Summary

Overall, the threat model framework evaluates how devices may be used as a tool by an abuse perpetrator to exerting power over a victim. This section identified the threat agent, motivations, and capacity, the victim's assets, device threats to those assets, motivational categorization, and mitigation approaches.

Chapter 5

Model Implementation on Nest Hub

5.1 Introduction

Chapter 5 evaluates the Google Nest Hub for potentially abusive uses from the motivational parameters and context of the threat model developed in Chapter 4.

The structure of this chapter is as follows: Section 5.2 describes the technical overview of the Google Nest Hub. Section 5.3 describes the connected application's capabilities. Section 5.4 describes the data collected about users through the Nest Hub. Section 5.5 identifies any unforeseen affordances that may enable SH-IoTFA and how these features can be used as abusive tools. Section 5.6 describes how mitigation approaches can be applied to the device. Finally, Section 5.7 summarizes the chapter.

5.2 Technical Overview

The Google Nest Hub, also known as the Nest Hub, is a virtual home assistant and smart home hub that can be used to connect and interact with other smart home devices in a smart environment. As a hub, the smart device can be used to act as a bridge or gateway to allow other devices to communicate. The addition of Google Assistant also allows users to integrate personalized voice commands during device interactions. The Nest Hub also acts as a digital photo frame, a smart speaker, and a personal planner. The Nest Hub tested in this chapter is a Generation 1 release that runs the Cast platform with the Google Smart Display software. The CPU running is the AMLogic S905D2, and the network protocols utilized are 802.11b/g/n/ac, and Bluetooth 5.0 [94].

5.3 Google Home Application

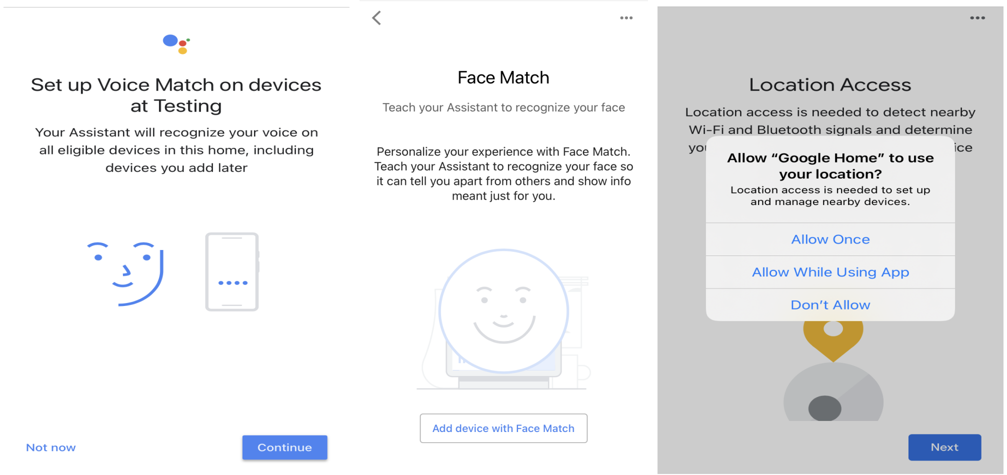
The Google Home application is a dedicated application which can be used for iOS or Android to interact with their smart assistants and control other smart devices via a user's Google account. Users can interact with the Google Nest and all connected home devices from the application. Other features also include controlling the speakers, using Chromecast, and linking photos to the frame. Furthermore, users can set up a home where they invite other members to interact with the smart devices and set their preferences. Most device interaction will occur through the use of the application, despite the device's physical interface. From this, there is the assumption that the device features are directly related to the application [94].

5.4 Data Collected by Google Nest Hub

The Nest Hub collects a vast amount of user data, which can place average users at risk. Google's privacy policy breaks down data collected into two categories: information collected from the use of google services and information that the user creates and provides to Google [94]. The data collected not only comes from the use of the device, but from the fact that users connect their Google Accounts to the application, which subsequently means that any online behavior and other data collected can be built upon to create a user profile. This includes web activity, location data, and other demographic information which can help Google personalize a user's environment [1].

Data Collected while using Google Services
1. Apps, browser data including version and type, and devices accessing Google Services
2. Interactions with advertisements
3. GPS and device sensor data
4. Web activity
5. Terms searched for
6. Shared content between users
7. Purchase activity
8. Activity on third-party sites and apps that use Google services
9. Device type and settings, operating system, mobile network info
10. Voice and Audio information
11. IP Address
12. Crash reports
13. System activity

Table 5.1: Data collected through use of Google Services [1]



Set up Voice Match on devices at Testing

Your Assistant will recognize your voice on all eligible devices in this home, including devices you add later

Face Match

Teach your Assistant to recognize your face

Personalize your experience with Face Match. Teach your Assistant to recognize your face so it can tell you apart from others and show info meant just for you.

Location Access

Location access is needed to detect nearby Wi-Fi and Bluetooth signals and determine yo ice

Allow "Google Home" to use your location?

Location access is needed to set up and manage nearby devices.

Figure 5.1: Data collected consented to by use of the Nest Hub

The data collected, in addition to the more general information collected by the Nest Hub also includes voice match, facial recognition, motion sensing, sleep data, routine preferences, and internet searches. Interestingly, in a forensic analysis of the Google Assistant, researchers were able to extract copies of past interactions from users and identify user account information. Specifically, Google stores sensitive information in a database which can be exported by the user, including audio files [95]. Despite the amount of data collected by the Nest Hub, researchers found that privacy protections for users are largely lacking, though users did not seem concerned due to their preconceived assumptions that their data is properly handled by Google [82]. While data collected by the Nest Hub has been marketed to help with personalization, these practices fail to consider victims of IPV and collect data with the assumption that the environment is shared between trusted users. If that trust is non-existent, data connected to each user's account can be used to facilitate surveillance [10].

5.5 Identification of Smart Hub Threats for SH-IoTFA

Throughout the assessment of the Nest Hub, the process included an analysis of the set up process and general usability based on the parameters set within the previous chapter. Through this method, there was a clear definition of user intention and motivations as an IPV perpetrator, and how the Nest Hub can 'invite' abusive behavior in use. Throughout the analysis process, Nest Hub features were noted and categorized based on the three themes described in the previous chapter: 1) Facilitation of surveillance, 2) Exertion of power imbalances, and 3) Psychological manipulation and harassment. These potentially harmful UI-Based features were then verified through manual analysis.

Threat Model Themes	***Vulnerability***	***Threat***
Surveillance and Omnipresent Control	Access to usage logs and activity	An abuser could restrict internet searches and device interactions. User could also track victim's activity
	Connect camera feed from other device	Use Nest Hub as a surveillance system to monitor the victim.
	Location Services	Perpetrator could use location services to track victim
	Google Duo	Abuser could remotely monitor phone calls.
	Voice Match	Monitor voice recordings in the usage logs
Ensure Power Imbalance	Home Creation	Abuser could remove victim access from the device
	Family Bell	Perpetrator could create alarms for victim to complete 'chores'
	Media/Entertainment	Perpetrator could override the victim's commands made to the device.
	Connect other devices	An abuser could restrict access to Nest Hub.
	Financial Services	An abuser could control victim's finances
	Routines	The feature inherently creates a power imbalance.
Psychological Manipulation and Harassment	Family Bell	Family bell may be used to harass other home members
	Broadcasting	An abuser could harass victim
	Media/Entertainment	A user could override the entertainment
	Routines	Routines may also be used to harass other home members.
	Update digital photo frame	Abuse perpetrator could change the frame to show illicit images

Table 5.2: Overview of Nest Hub device threats to SH-IoTFA

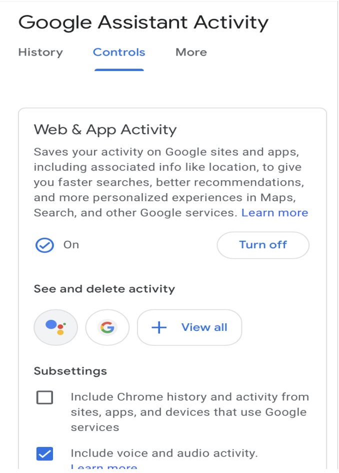
5.5.1 Thematic Threat Analysis: Nest Hub

Theme 1: The Nest Hub facilitates undesired monitoring and surveillance

The Nest Hub maintains features that facilitate abusive practices through surveillance. The two features facilitating this behavior include access to activity/usage logs and location services.

Vulnerability 1: Activity Logs

Access to Activity Logs, as described in Chapter 4, is a feature that abuse perpetrators can use to control users and track their device usage without using spyware. The Google Nest Hub allows users to record all device interactions via myactivity.google.com. The user can save the web app and assistant activity or turn off the feature. The user may also record the internet history, apps, and devices that use Google services Figure 5.10.



Google Assistant Activity

History Controls More

Web & App Activity

Saves your activity on Google sites and apps, including associated info like location, to give you faster searches, better recommendations, and more personalized experiences in Maps, Search, and other Google services. Learn more

✓ On Turn off

See and delete activity

View all

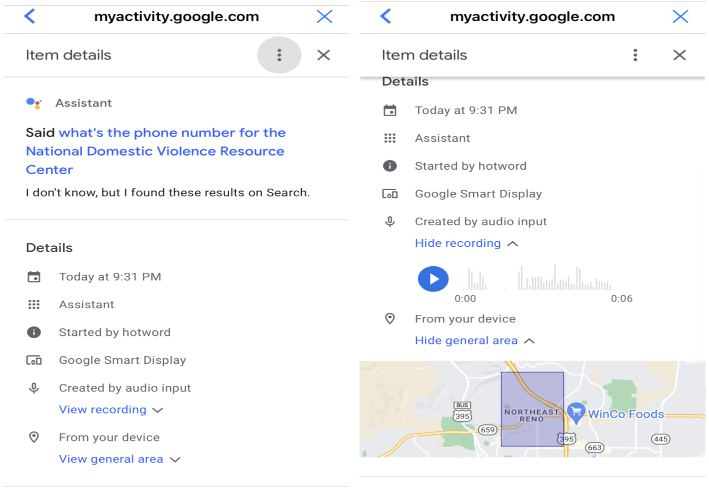
Subsettings

☐ Include Chrome history and activity from sites, apps, and devices that use Google services

☑ Include voice and audio activity. Learn more

Figure 5.2: Web app activity

When this feature is enabled, user-device interactions are recorded and sent to the activity log. The amount of data collected and recorded by the activity feature appeals to abuse perpetrators. They are incentivized to review household activity to keep track of whom their partner is calling, their internet searches, and their interactions with the Nest Hub. Furthermore, if the user has set up personalization settings such as voice match, the logs will also store a recording of the user's voice. To illustrate the dangers of this feature, I asked the Nest Hub to search for the National Domestic Violence Resource Center Hotline [58]. Not only did a voice recording appear, but the device's general location was also recorded on the logs. In cases of SH-IoTFA where the victim has escaped, remote access to these logs may reveal their location. Each test revealed that the access logs were an access point for surveillance activity, whether it be a full recording or location.



myactivity.google.com

Item details

Assistant

Said what's the phone number for the National Domestic Violence Resource Center

I don't know, but I found these results on Search.

Details

Today at 9:31 PM

Assistant

Started by hotword

Google Smart Display

Created by audio input

View recording

From your device

View general area

myactivity.google.com

Item details

Details

Today at 9:31 PM

Assistant

Started by hotword

Google Smart Display

Created by audio input

Hide recording

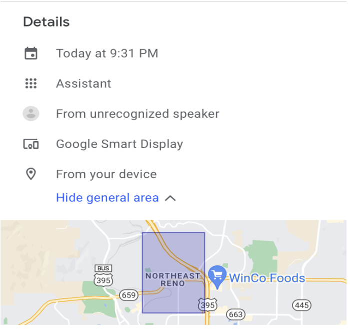
0:00 0:06

From your device

Hide general area

Figure 5.3: Result of activity log testing

In addition to using the device on one account, I set up a second account and invited them to the home. However, if there are two accounts, the data will be separated by each account if personalization settings are enabled. Despite this, if a user has credentials to the other account, they can also collect data about internet searches. Interestingly, if other users were not invited to the home, any device interactions they have with the device are still recorded in the main account log. For testing, I had a household member use the device without setting up an account. Instead of an audio recording, only the location was recorded.



Details

Today at 9:31 PM

Assistant

From unrecognized speaker

Google Smart Display

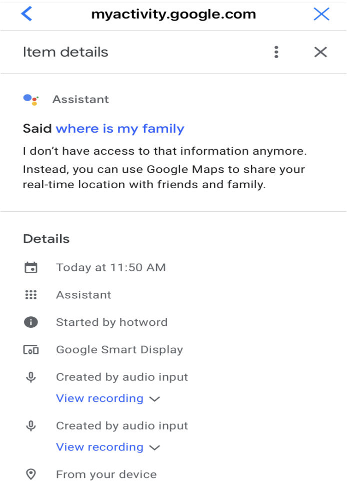
From your device

Hide general area

Figure 5.4: Location found on usage log

Vulnerability 2: Location Services

Any capability to check on the location of a household member can be abused for spying. Location services are a feature for families to use to keep track of where another household member is, generally via the Google Home application. For example, if someone is on their way home, it's possible to get an estimation of how far away they are, which would help to determine what time to make dinner. Location sharing can also be used to initiate tasks using the routine feature. Interestingly, when attempting to use this feature, the device replies, "I don't have access to that information anymore," which demonstrates a move away from this technology on the older generations. See Figure 5.5:



myactivity.google.com

Item details

Assistant

Said where is my family

I don't have access to that information anymore. Instead, you can use Google Maps to share your real-time location with friends and family.

Details

Today at 11:50 AM

Assistant

Started by hotword

Google Smart Display

Created by audio input

View recording

Created by audio input

View recording

From your device

Figure 5.5: Example of log without voice match

Threat Summary: Nest Hub Surveillance

1. Use activity logs to monitor a victim's device interactions and web activity. If personalization features are enabled, the perpetrator could also view who the victim is calling, what they are purchasing, and where they are. Voice matches can also give perpetrators access to voice recordings.

2. Location services through the activity log could allow the perpetrator to locate their victim if they moved and took the device with them.

3. If other devices, such as a camera, are connected to the Nest Hub, the abuse perpetrator could covertly monitor video and audio.

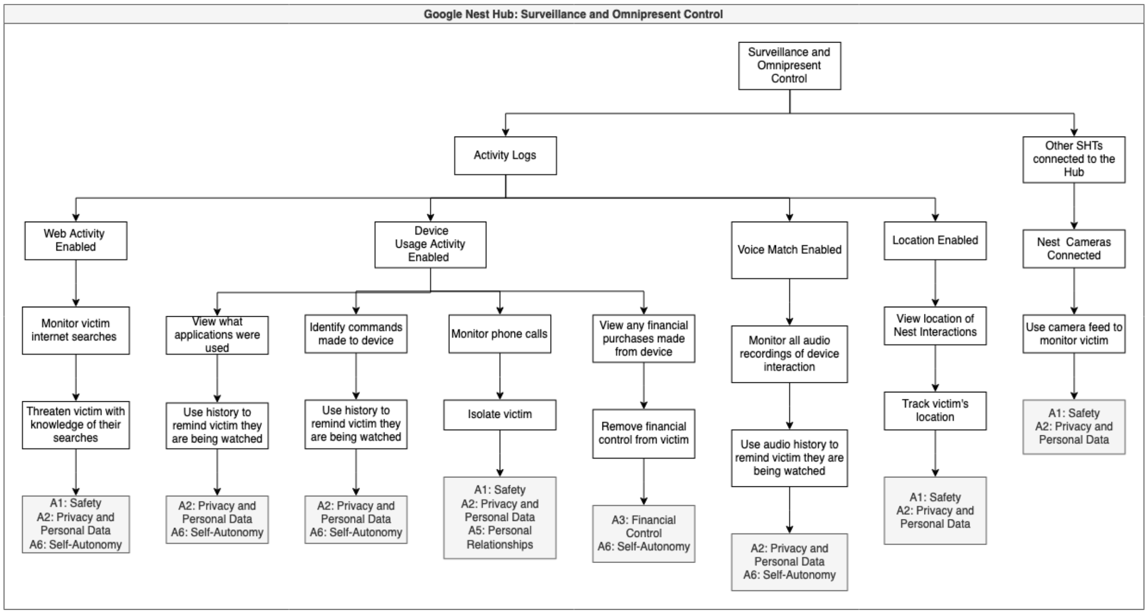

Google Nest Hub: Surveillance and Omnipresent Control
Surveillance and Omnipresent Control
Activity Logs
Other SHTs connected to the Hub
Web Activity Enabled
Device Usage Activity Enabled
Voice Match Enabled
Location Enabled
Nest Cameras Connected
Monitor victim internet searches
View what applications were used
Identify commands made to device
Monitor phone calls
View any financial purchases made from device
Monitor all audio recordings of device interaction
View location of Nest Interactions
Use camera feed to monitor victim
Threaten victim with knowledge of their searches
Use history to remind victim they are being watched
Use history to remind victim they are being watched
Isolate victim
Remove financial control from victim
Use audio history to remind victim they are being watched
Track victim's location
A1: Safety
A2: Privacy and Personal Data
A1: Safety
A2: Privacy and Personal Data
A6: Self-Autonomy
A2: Privacy and Personal Data
A6: Self-Autonomy
A2: Privacy and Personal Data
A6: Self-Autonomy
A1: Safety
A2: Privacy and Personal Data
A5: Personal Relationships
A3: Financial Control
A6: Self-Autonomy
A2: Privacy and Personal Data
A6: Self-Autonomy
A1: Safety
A2: Privacy and Personal Data

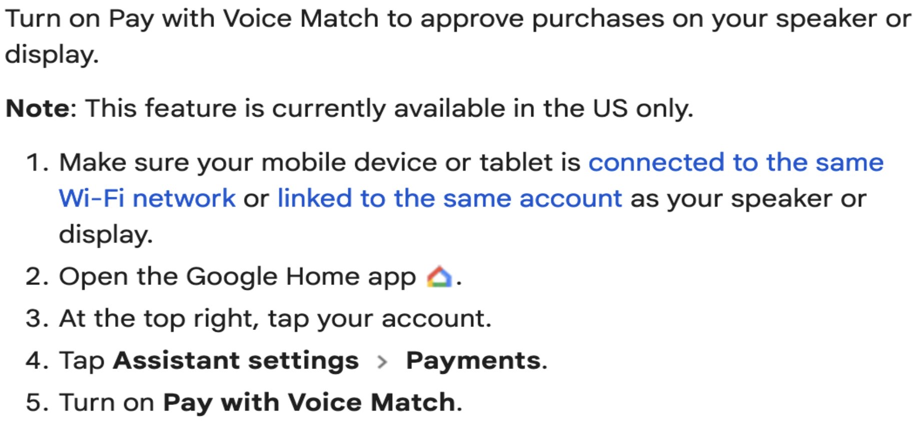
Figure 5.6: Surveillance and Omnipresent Control Attack Tree for Nest Hub

Theme 2: The Nest Hub facilitates Power imbalances

The Nest Hub maintains several convenient features vulnerable to SH-IoTFA facilitation. These vulnerabilities include the ability to connect financial accounts, the ability to control other SH-IoTs, and the ability to set routines.

Vulnerability 1: Connected Financial Accounts

The Nest Hub allows users to connect their financial accounts to make hands-free payments. This is a convenient way to make purchases remotely and at the touch of a button. Through this feature an abusive perpetrator may gain control over the victim's finances. For example, if the perpetrator has access to the victim/survivor's credit or debit card information, they may use that information to set the victim's card as the default payment. In that case, any purchases made could be used to either hold finances over the victim's head or make unauthorized payments. Adding to this control, if the abuse perpetrator enables voice match to approve payments, the victim may not be able to make any purchases via the device, whether it is their card connected to the device or not. This is an inherent threat to the victim because they may have no way of knowing what is being purchased from the Nest Hub via their accounts, which could result in their funds being drained.



Turn on Pay with Voice Match to approve purchases on your speaker or display.

Note: This feature is currently available in the US only.

1. Make sure your mobile device or tablet is connected to the same Wi-Fi network or linked to the same account as your speaker or display.
2. Open the Google Home app ⌂.
3. At the top right, tap your account.
4. Tap **Assistant settings** > **Payments**.
5. Turn on **Pay with Voice Match**.

Figure 5.7: Enabling voice match for payments

Vulnerability 2: Control Other Devices

When several devices are connected to the Google Home App, the attack capabilities of the SH-IoTFA perpetrator expand. As smart assistants increase in popularity, several home appliances have become 'smart' via compatibility with Amazon Alexa and Google Assistant. For example, the Phillips Hue lights are compatible with Google Assistant, meaning that someone with the application can remotely control the state of the lights. While there are several other apps available, devices connected to the Google Home App run the risk of adopting threats that may not have previously existed, specifically through how users can access and interact with the services.

Vulnerability 3: Routines

The "Routines" feature also maintained several key issues from an interpersonal threat approach. Within the feature, users can utilize a routine that allows a user to automate multiple tasks with one voice command. These commands can be initiated for bedtime, leaving home, returning from work, and waking up in the morning. The commands range from setting alarms, receiving weather and traffic details, and adjusting the lights and other smart devices. Device routines can be created for personal use or the household. Examples of personal use include a bedtime routine. When triggered, the bedtime routine will set the alarm and turn off the lights. An example of a household routine would include turning a light, plug, camera, or switch on or off at a specific time every day. Given that the routines are often set with one person or to trigger an action for the household, the feature inherently creates a power imbalance [94].

Vulnerability 4: Home Creation and Account Access

The Google Nest Hub maintains three levels of access control: Owner, Full Access, and Guest. Interestingly, when a device owner invites another user to have access within their home, the owner must consent to allow the other users to have full access to the device, including the ability to remove the owner as a member of the home. With full access to the devices, users can manage home members, use and change the device's settings in the home, and automatically link their media services. Users with full access can also use the Digital Wellbeing feature to filter the devices and restrict explicit content. If separate devices maintain full access, there are a few scenarios that may play out. If each user has voice match enabled, any interaction with the device will be stored in their account rather than the owner's account. If the voice match has not been set up, device interactions may be recorded for both accounts.

In addition to other account holders, the Hub also has a guest mode which allows the devices to be used by other members while also ensuring that the guest has restrictions on personal information about the household members. Guest users or the device owner can enable this by saying, "Hey Google, turn on Guest Mode." While the device is in guest mode, any interactions, recordings, or internet searches are automatically deleted. While other members can interact with the device in guest mode, failure to identify guest controls may allow a user to gain more access than they should have, as the device may give personalized results depending on what privacy controls are set.

In a scenario where the perpetrator owns the device, as is assumed in this assessment, they may restrict access by not allowing the other user to connect their google account from the device. They may also ask that a shared account is used to ensure access to activity logs. If the other user does have full access to the device, the perpetrator may also remove them from accessing device features.

Threat Summary: Nest Hub Power Imbalance

1. Abuse perpetrators could restrict access to the device and ensure they have more control over the device than other users.

2. The connection to financial accounts may allow the perpetrator to take control of the victim's finances or set up the victim as a default payment. If voice match is enabled, the perpetrator could also block the victim from making purchases.

3. The routines feature is generally only able to be set up for one person, allowing the perpetrator to exert control over morning and evening routines. For example, the abuse perpetrator could automate several alarms, turn on lights, and play music in the morning which may in turn disrupt the victim if they are on a different schedule. The functionality of routines also means that the victim cannot turn off the functionality.

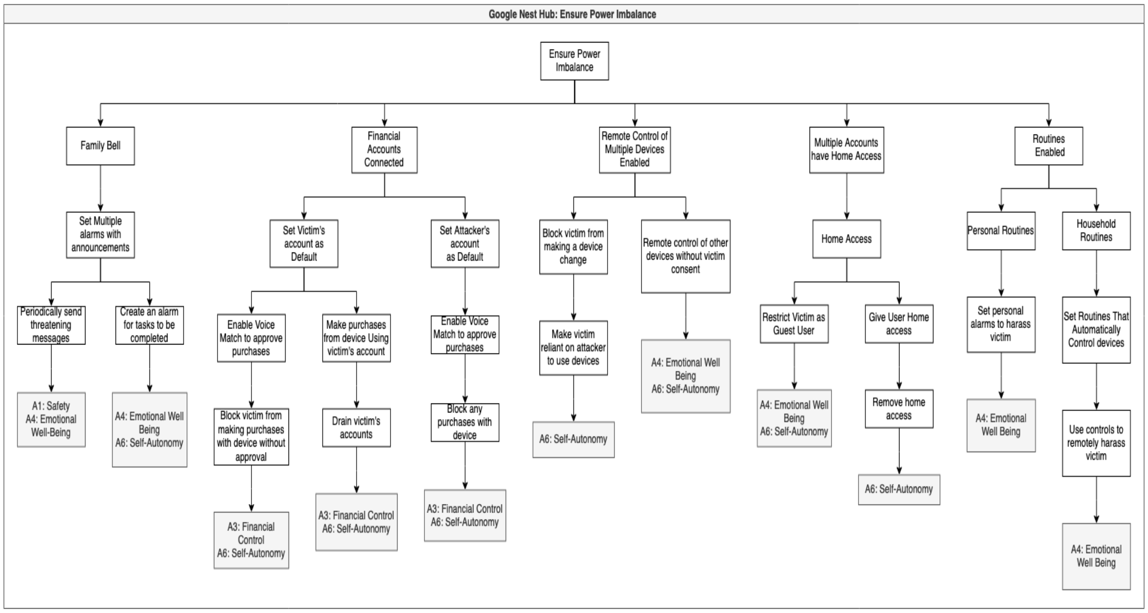

Google Nest Hub: Ensure Power Imbalance
Ensure Power Imbalance
Family Bell
Financial Accounts Connected
Remote Control of Multiple Devices Enabled
Multiple Accounts have Home Access
Routines Enabled
Set Multiple alarms with announcements
Set Victim's account as Default
Set Attacker's account as Default
Block victim from making a device change
Remote control of other devices without victim consent
Home Access
Personal Routines
Household Routines
Periodically send threatening messages
Create an alarm for tasks to be completed
Enable Voice Match to approve purchases
Make purchases from device Using victim's account
Enable Voice Match to approve purchases
Make victim reliant on attacker to use devices
A4: Emotional Well Being
A6: Self-Autonomy
Restrict Victim as Guest User
Give User Home access
Set personal alarms to harass victim
Set Routines That Automatically Control devices
A1: Safety
A4: Emotional Well-Being
A4: Emotional Well Being
A6: Self-Autonomy
Block victim from making purchases with device without approval
Drain victim's accounts
Block any purchases with device
A6: Self-Autonomy
A4: Emotional Well Being
A6: Self-Autonomy
Remove home access
A4: Emotional Well Being
Use controls to remotely harass victim
A3: Financial Control
A6: Self-Autonomy
A3: Financial Control
A6: Self-Autonomy
A3: Financial Control
A6: Self-Autonomy
A6: Self-Autonomy
A4: Emotional Well Being

Figure 5.8: Ensure Power Imbalance Attack Tree for Nest Hub

Theme 3: The Nest Hub facilitates harassment and antagonistic behaviors

The Nest Hub also maintains features that allow for the facilitation of harassment and antagonistic behaviors. These features, created for convenience, also allow the perpetrator to harass and threaten the victim within their shared space.

Vulnerability 1: Family Bell

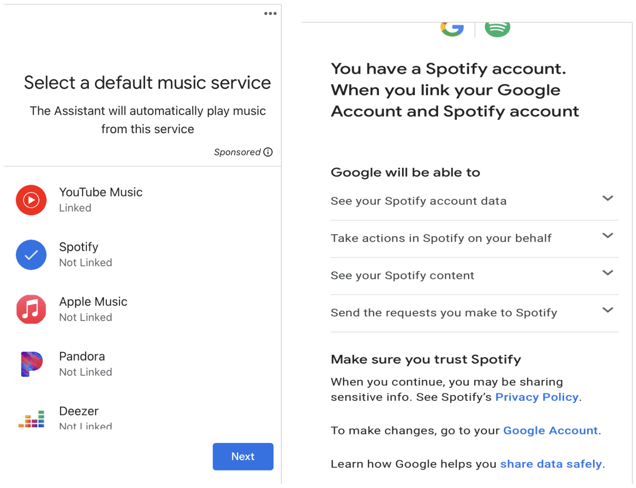
The Google Nest Hub maintains many features for family communication and interaction. One of these features is the Family Bell which is marketed as a way to keep your family on track by creating announcements that go to users' home devices and smart devices. An example of this would be to announce dinner time every day at 5 PM via the living room speaker. An abuse perpetrator can use the feature to continuously harass their victim, especially if they are the owner of the device. This is because the only user who owns the device can make set announcements, times, and repeats.

Vulnerability 2: Broadcasting

The announcement feature also maintains threats for SH-IoTFA. The announcement feature allows users to broadcast a message to other users. To broadcast a message, the user can select a feature called "Send a Family Broadcast" or they can select the microphone feature in the mobile application. Unlike the family bell and announcements feature, the family broadcast feature maintains the ability to allow any user to broadcast a message, which is intended for acknowledging messages from other members. While this can be useful for remotely sending an update to another household member without having to call, it is also a possibility that the feature could be used maliciously to broadcast harassment messages, threaten other household members, or disrupt their comfort. For example, if an abusive perpetrator has texted the victim or is trying to get in contact, the perpetrator can to broadcast a message to them continuously until the victim has engaged with the message. Furthermore, even when the microphone is off, the broadcast will still be cast via the application.

Vulnerability 3: Music/Podcasts/Entertainment

The ability to use the Nest Hub for any entertainment can be manipulated for abuse, such as psychological manipulation and harassment. Several SH-IoTFA papers have shown that entertainment features can be manipulated by abusers as a tactic to torment and harass victims. With the ability to listen to music, and podcasts, as well



Select a default music service

The Assistant will automatically play music from this service

Sponsored ⓘ

YouTube Music
Linked

Spotify
Not Linked

Apple Music
Not Linked

Pandora
Not Linked

Deezer
Not Linked

You have a Spotify account. When you link your Google Account and Spotify account

Google will be able to

See your Spotify account data

Take actions in Spotify on your behalf

See your Spotify content

Send the requests you make to Spotify

Make sure you trust Spotify

When you continue, you may be sharing sensitive info. See Spotify's Privacy Policy.

To make changes, go to your Google Account.

Learn how Google helps you share data safely.

Figure 5.9: Device entertainment capabilities

as watch videos, the perpetrator has the ability to override music that other users are listening to from the hub device from their phone and increase the volume of the device remotely. Analysis of the Google Nest Hub reveals that this is relatively easy to accomplish via the mobile application.

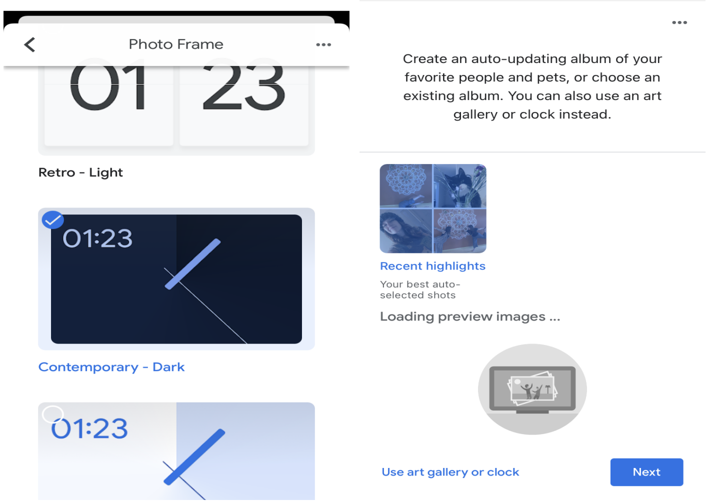
Specifically, if someone with the application is on the same WiFi network as the device, it is possible to cast media and monitor what is playing on the device. In addition, if the device is unplugged, the perpetrator may be able to view that their attack was unsuccessful. In addition, there are differences in what service is used if the perpetrator is not on the same WiFi network, for example, if there is a linked Spotify account to the device, the perpetrator may be able to play music even when not connected to the network. If Spotify is not linked, then the perpetrator can only use Google Play Music. Though in this case, we still assume that the perpetrator is the device owner and has access to the device's WiFi.

Vulnerability 4: Routines

In addition, like the Family Bell and Broadcasting feature, it may be possible to set a routine for the device that blasts loud music and turns on lights in the middle of the night. While this feature was also cited in the above section, it can be used to both create power imbalances and engage in antagonistic behavior against the victim.

Vulnerability 5: Update Photo Frame

The Google Nest Hub also markets itself as a digital photo frame [94]. While it may be nice to display family photos on the device, the ability to remotely change the images may be used to humiliate a victim.



Create an auto-updating album of your favorite people and pets, or choose an existing album. You can also use an art gallery or clock instead.

Loading preview images ...

Figure 5.10: Nest Hub frame capabilities

For example, an abuse perpetrator could change the display settings to an illicit image of the victim. If the victim has restricted access, they may be unable to remove the image without physically unplugging the device. Not only can this be used to humiliate the victim, but it also demonstrates that the abuser still has access to the victim and/or has access to information that could be used against the victim in the future.

Threat Summary: Psychological abuse and manipulation

1. Abuse perpetrators can use their access to the 'Routines' feature and set several alarms or other disruptive activities to harass the victim.

2. The Family Bell can be used by the perpetrator to also set off several alarms

to annoy or harass a victim. It can also be used to send an alarm with a threatening or harassing message.

3. The Broadcast feature allows an abuse perpetrator to send remote messages to the device and application which could be used to threaten or harass a victim.

4. An abuse perpetrator could remotely access music or other forms of entertainment and play them while the victim is working or trying to sleep. This could be used as both a control tactic to antagonize and harass.

5. An abuse perpetrator could also use their remote access to the digital frame to humiliate a victim by uploading illicit images of the victim.

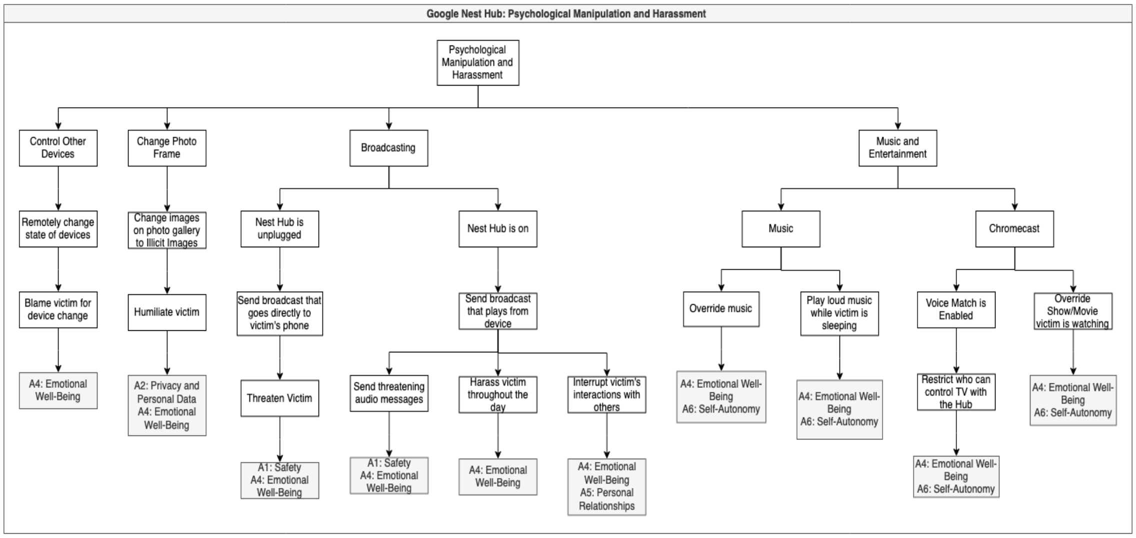

Google Nest Hub: Psychological Manipulation and Harassment
Psychological Manipulation and Harassment
Control Other Devices
Change Photo Frame
Broadcasting
Music and Entertainment
Remotely change state of devices
Change images on photo gallery to Illicit Images
Nest Hub is unplugged
Nest Hub is on
Music
Chromecast
Blame victim for device change
Humiliate victim
Send broadcast that goes directly to victim's phone
Send broadcast that plays from device
Override music
Play loud music while victim is sleeping
Voice Match is Enabled
Override Show/Movie victim is watching
A4: Emotional Well-Being
A2: Privacy and Personal Data
A4: Emotional Well-Being
Threaten Victim
Send threatening audio messages
Harass victim throughout the day
Interrupt victim's interactions with others
A4: Emotional Well-Being
A6: Self-Autonomy
A4: Emotional Well-Being
A6: Self-Autonomy
Restrict who can control TV with the Hub
A4: Emotional Well-Being
A6: Self-Autonomy
A1: Safety
A4: Emotional Well-Being
A1: Safety
A4: Emotional Well-Being
A4: Emotional Well-Being
A4: Emotional Well-Being
A5: Personal Relationships
A4: Emotional Well-Being
A6: Self-Autonomy

Figure 5.11: Psychological Manipulation Attack Tree for Nest Hub

5.5.2 Relationship Between Threats and Motivations

Abuser motivations directly correlate to the device vulnerabilities found in the qualitative literature. This point to evidence that abuser motivations directly correlate to abusive actions they can facilitate through SH-IoTS. This is in part because of the perspective at which we are identifying the threat agent and their motivations, and because it is possible to manipulate convenient UI-features for personal gain. For the threat scenario, we cannot deny the importance of understanding why a perpetrator would use the device in an abusive manner rather than just how, as it is the implicit creation of an affordance that can be planned for with more diverse perspectives within the threat modeling process.

5.6 Proposal of Countermeasures

This section establishes recommendations for the Nest Hub to encourage the empowerment of victims rather than abusers. If we can discourage devices to be used for abusive motivations, devices can be secure additions to the home that ensure that users maintain implicit rights to their privacy and security.

Mitigating Surveillance in Nest Hub

1. *Reduce information recorded by the usage logs:* Given that the usage logs are often used to ensure that anonymous activity does not occur, it does not make sense to record the searches or private data. Instead, the access logs should record when the device was used and by whom. No other information should be provided.

2. *Disable location monitoring:* Unless the device has been accessed by an unknown third-party, there should be no need to record the location if the device is meant to be in the home.

Mitigating Power Imbalance in Nest Hub

1. *Alarm and Broadcast Control/Family Bell:* All members of the household must maintain the ability to turn off an alarm or broadcast that may be used in the

facilitation of harassment. Ensuring that remote access while another member is at home, will also provide increased discouragement of remote harassment and control.

2. *Multi-User/Equal Access:* The separation of users through equal access will ensure that one user does not maintain more control than another. This includes equal access in the set-up process, and if a guest is invited, full access to controls as well. Should other users from the household be invited, equal access to controls may include a protocol that allows for separation between user activities and profiles so that there exists no overlapping data collection that can be used in control and monitoring scenarios.

3. *Routines:* Allow for all users to have access to turn on and off routines rather than only allowing the device owner those privileges.

4. *Remote Access to Control Devices:* Allow for home users to disable remote changes to the device while home.

Mitigating Psychological Manipulation and Harassment in Nest Hub

1. *Alarm and Broadcast Control:* All members of the household must maintain the ability to turn off an alarm or broadcast that may be used in the facilitation of harassment. Ensuring that remote access is disabled while another member is at home, will discourage remote harassment and control.

2. *Media/Entertainment:* Disable remote access to device changes while another household member is home.

3. *Photo Frame:* Allow users to flag when an image used is inappropriate. Disable full access to photos, rather allow for default photos rather than personalization.

5.7 Summary

Within this research, the default features of the Google Nest Hub were analyzed against the proposed threat model to determine what features could be further identified for abuse mitigation. The security vulnerabilities found within the assessment identified several ways that abuse can occur through the default features of a device. This research demonstrated how the conclusions made about attacker motivations and device affordances can be connected and recognized by developers as possible threats. In moving forward, it is possible to build a customized approach that analyzes how relationships dynamics play role in abuse facilitation.

Chapter 6

Limitations, Conclusion, and Future Work

6.1 Limitations

Despite the well-researched modeling of SH-IoTFA in this thesis, there are some potential limitations. Due to the nature of the qualitative literature analyzed in this research, there is a large bias towards female perspectives of IPV where the perpetrator is male, as previously described in Chapter 2. Due to the nuanced nature of social dynamics, experiences of interpersonal abuse among differing demographics may include other motivations, affordances, and access points that have not been previously recognized within the parameters of this research. In addition, much of the literature used to inform the threat model is limited by their quality of qualitative analysis. Several authors conducted analysis on research pools with less than 20 people. The use of these low testing pools reduces the findings on SH-IoTFA and may have led to conclusions that do not paint the whole picture.

Within the threat model development, there are some limitations such that the framework is untested in a real-life setting. Furthermore, there is a lack of robust data on the trends of SH-IoTFA. Without this data, it is unclear how effective this research can be in truly understanding the threat agent and their profile in these attack scenarios. Despite the research limitations, this research bridges the gap between our understanding of abuse and cybersecurity methods. As research in this field continues to grow, it will be possible for the development of a fully comprehensive model that provides effective mitigation against abuse.

6.2 Conclusion

While attacker-centric threat modeling is not a new concept, there has been no prior implementation of its use in interpersonal abuse cases. By first identifying what an abuser's goals are, why they may wish to carry them out, and what they seek to gain, we can remove UI-based attacks and refocus development goals to empower victims. In addition, the identification of interpersonal threats expands our scope of understanding what an attacker is in cybersecurity. The trend of SH-IoTFA demonstrates clear design vulnerabilities that overlook threats that may exist in domestic relationships. No longer are the threats coming from third-party, anonymous adversaries, but rather, the adversaries are the consumers themselves. The framework presented in this thesis combines interdisciplinary research and cybersecurity processes to show that simply configuring a system-based model to plan for IPV does not provide solutions to the core of the issue which is that social relationships play a huge role in the use of technology.

In addition to expanding our definition of cybersecurity threats and incidents, the research outlined in this model emphasizes the importance of looking outside of system-based models, which are often too narrowly focused on technical threats, to recognize the dangers in interpersonal abuse cases. Using system approaches, motivational aspects of the attacker and their access points are overlooked. Attacker-centric threat modeling strengthens the argument that HCI research and cybersecurity are interconnected, despite the seemingly differing end-goals. Through this integration, we can gain a much more comprehensive understanding of threats and define mitigation approaches that are preventative and built within design, rather than a reactive addition, added after users experience abuse.

Interestingly, the model defined within this thesis revealed common themes among devices that allow abusers to execute attacks against their victims. Core features included remote state changes, access to monitoring, and uneven power imbalances due to access control between users, though these features were not limited to just one aspect of the device. The analysis of the Google Nest Hub in Chapter 5 also revealed that the core issues defined by the threat model can be found in seemingly innocuous features within the device, and that potential abuse can be executed due to poor privacy practices and overlooked design flaws.

6.3 Future Work

Given the broad nature of SH-IoTFA research, there are several research avenues which will be explored in the future. As an extension of this thesis, future research will include testing the threat model against other interpersonal attack scenarios such as elder abuse and child abuse. Through this research, it may be possible to expose other abusive affordances that have not been described in the present approach. In addition, given the analysis of developer attitudes in Chapter 2, future work will also entail qualitative approaches to gain better insight into pre-conceived beliefs about security and interpersonal abuse. This research may help to inform new models and approaches to develop more secure SH-IoTs. Building off this foundation of this thesis, other research may include testing empowered design through work with victims and survivors. Through these future projects, we can gain a better understanding of social issues in cybersecurity and give voice awareness to attacks that are overlooked by current practices.

Bibliography

[1] Privacy policy – privacy & terms – google. [Online]. Available: https://policies.google.com/privacy?hl=en-US

[2] M. Khawla and M. Tomader, “A review on the security of smart homes in the internet of things,” p. 10.

[3] K. D. Foote. A brief history of the internet of things. [Online]. Available: https://www.dataversity.net/brief-history-internet-things/

[4] R. J. Robles and T.-h. Kim, “Applications, systems and methods in smart home technology: A review,” vol. 15, p. 13.

[5] K. Gram-Hanssen and S. J. Darby, ““home is where the smart is”? evaluating smart home research and approaches against the concept of home,” vol. 37, pp. 94–101. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214629617303213

[6] S. Panchiwala and M. Shah, “A comprehensive study on critical security issues and challenges of the IoT world,” vol. 2, no. 4, pp. 257–278. [Online]. Available: https://link.springer.com/10.1007/s42488-020-00030-2

[7] E. Zeng, S. Mare, and F. Roesner, "End user security and privacy concerns with smart homes." [Online]. Available: https://www.semanticscholar.org/paper/301b4b2e511a5e053de43b82bd71b59e6af5402c

[8] A. Alshehri, M. Ben Salem, and L. Ding, "Are smart home devices abandoning IPV victims?" in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1368–1375, ISSN: 2324-9013.

[9] R. Leitão, "Anticipating smart home security and privacy threats with survivors of intimate partner abuse," in *Proceedings of the 2019 on Designing Interactive Systems Conference*, ser. DIS '19. Association for Computing Machinery, pp. 527–539. [Online]. Available: https://doi.org/10.1145/3322276.3322366

[10] I. Lopez-Neira, T. Patel, S. Parkin, G. Danezis, and L. Tanczer, "'internet of things': How abuse is getting smarter." [Online]. Available: https://www.semanticscholar.org/paper/58037c3b6f3fd3616f2124cd1f9d0a63fccd3a7a

[11] S. Parkin, E. M. Redmiles, L. Coventry, and M. Sasse, "Security when it is welcome: Exploring device purchase as an opportune moment for security behavior change." [Online]. Available: https://www.semanticscholar.org/paper/997a88279c23e952a52e4a15c378426fe17cba72

[12] D. Norman. The design of everyday things: Revised and expanded edition. [Online]. Available: https://www.nngroup.com/books/design-everyday-things-revised/

[13] J. Slupska, "Safe at home: Towards a feminist critique of cybersecurity." [Online]. Available: https://www.semanticscholar.org/paper/bf6752dcbe067f3efa9f90f021f770ba70811077

[14] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, and C. Woody, "Threat modeling: A summary of available methods," section: Technical Reports. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1084024

[15] R. Afrouz, "The nature, patterns and consequences of technology-facilitated domestic abuse: A scoping review," p. 15248380211046752, publisher: SAGE Publications. [Online]. Available: https://doi.org/10.1177/15248380211046752

[16] NCADV | national coalition against domestic violence. [Online]. Available: https://ncadv.org/STATISTICS

[17] B. Khurana, S. E. Seltzer, I. S. Kohane, and G. W. Boland, "Making the 'invisible' visible: transforming the detection of intimate partner violence," vol. 29, no. 3, pp. 241–244, publisher: BMJ Publishing Group Ltd Section: Viewpoint. [Online]. Available: https://qualitysafety.bmj.com/content/29/3/241

[18] E. Stark and M. Hester, "Coercive control: Update and review," vol. 25, no. 1, pp. 81–104, publisher: SAGE Publications Inc. [Online]. Available: https://doi.org/10.1177/1077801218816191

[19] R. Chatterjee, P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy, and T. Ristenpart, "The spyware used in intimate partner violence," pp. 441–458. [Online]. Available: https://www.semanticscholar.org/paper/845f45f8412905137bf4e46a0d434f5856cd3aec

[20] N. Henry and A. Powell, "Technology-facilitated sexual violence: A literature review of empirical research," vol. 19, no. 2, pp. 195–208, publisher: SAGE Publications. [Online]. Available: https://doi.org/10.1177/1524838016650189

[21] C. Brown and K. Hegarty, "Digital dating abuse measures: A critical review," vol. 40, pp. 44–59. [Online]. Available: https://www.semanticscholar.org/paper/682c593e87b4a6944ccd655bfc5b9f44e1651816

[22] D. Woodlock, "The abuse of technology in domestic violence and stalking," vol. 23, no. 5, pp. 584–602, publisher: SAGE Publications Inc. [Online]. Available: https://doi.org/10.1177/1077801216646277

[23] N. Apthorpe, P. Emami-Naeini, A. Mathur, M. Chetty, and N. Feamster, "You, me, and IoT: How internet-connected consumer devices affect interpersonal relationships." [Online]. Available: http://arxiv.org/abs/2001.10608

[24] Elan home automation systems. [Online]. Available: https://elancontrolsystems.com/

[25] T. Hammersley. Jealous businessman spied on ex using iPad mounted to kitchen wall. Section: Greater Manchester News. [Online]. Available: https://www.manchestereveningnews.co.uk/news/greater-manchester-news/jealous-businessman-spied-ex-partner-14640719

[26] N. Bowles, "Thermostats, locks and lights: Digital tools of domestic abuse." [Online]. Available: https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

[27] S. Cole. Apple's AirTags are being used to stalk and harass women. [Online]. Available: https://www.vice.com/en/article/y3v9zx/apple-airtags-stalking-cyber-podcast

[28] D. Cassioli, A. Di Marco, T. Di Mascio, L. Tarantino, and P. Inverardi, "Is really IoT technology gender neutral?" in *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT*, pp. 324–328.

[29] S. Parkin, T. Patel, I. Lopez-Neira, and L. Tanczer, "Usability analysis of shared device ecosystem security: informing support for survivors of IoT-facilitated tech-abuse," in *Proceedings of the New Security Paradigms Workshop*, ser. NSPW '19. Association for Computing Machinery, pp. 1–15. [Online]. Available: https://doi.org/10.1145/3368860.3368861

[30] J. Slupska and L. M. Tanczer, "Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things," in *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, J. Bailey, A. Flynn, and N. Henry, Eds. Emerald Publishing Limited, pp. 663–688. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/978-1-83982-848-520211049/full/html

[31] L. Tanczer, I. Steenmans, M. Elsden, J. Blackstock, and M. Carr, "Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge?" in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. Institution of Engineering and Technology, pp. 33 (9 pp.)–33 (9 pp.). [Online]. Available: https://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0033

[32] L. M. Tanczer. Implications of the internet of things (IoT) on victims of gender-based domestic violence and abuse. [Online]. Available: https://www.ucl.ac.uk/research/domains/collaborative-social-science/social-science-plus/IOT-and-domestic-violence

[33] R. Leitão, "Digital technologies and their role in intimate partner violence," in *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI EA '18. Association for Computing Machinery, pp. 1–6. [Online]. Available: https://doi.org/10.1145/3170427.3180305

[34] I. Kounelis, G. Baldini, R. Neisse, G. Steri, M. Tallacchini, and A. Guimaraes Pereira, “Building trust in the human?internet of things relationship,” vol. 33, no. 4, pp. 73–80, conference Name: IEEE Technology and Society Magazine.

[35] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell, “"a stalker’s paradise": How intimate partner abusers exploit technology,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’18. Association for Computing Machinery, pp. 1–13. [Online]. Available: https://doi.org/10.1145/3173574.3174241

[36] M. Al-Shaboti, G. Chen, and I. Welch, “Achieving IoT devices secure sharing in multi-user smart space,” in *2020 IEEE 45th Conference on Local Computer Networks (LCN)*. IEEE, pp. 88–99. [Online]. Available: https://ieeexplore.ieee.org/document/9314780/

[37] N. Ehrenberg and T. Keinonen, “The technology is enemy for me at the moment: How smart home technologies assert control beyond intent,” in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’21. Association for Computing Machinery, pp. 1–11. [Online]. Available: https://doi.org/10.1145/3411764.3445058

[38] A. N. Mohammed, “A comparative study on models and techniques for securing IoT applications.” [Online]. Available: https://www.semanticscholar.org/paper/880b06341a36794bf301e738ffa17d3166b83451

[39] B. Janes, H. Crawford, and T. OConnor, “Never ending story: Authentication and access control design flaws in shared IoT devices,” in *2020 IEEE Security and Privacy Workshops (SPW)*, pp. 104–109.

[40] M. Knittel and R. Shillair, "Information policy, privacy failings, and steps towards empowerment in cases of technology-facilitated sexual violence." [Online]. Available: https://papers.ssrn.com/abstract=3748984

[41] Y. Strengers, J. Kennedy, P. Arcari, L. Nicholls, and M. Gregg, "Protection, productivity and pleasure in the smart home: Emerging expectations and gendered insights from australian early adopters."

[42] W. He, J. Martinez, R. Padhi, L. Zhang, and B. Ur, "When smart devices are stupid: Negative experiences using home smart devices," pp. 150–155. [Online]. Available: https://www.semanticscholar.org/paper/9c77ab1840fc1c17540c0da0812243b66749d1c4

[43] R. Garg and C. Moreno, "Understanding motivators, constraints, and practices of sharing internet of things," vol. 3, pp. 1 – 21. [Online]. Available: https://www.semanticscholar.org/paper/c54f5107cd050095ed8d1ad978da58da3cc694fd

[44] G. Chalhoub, I. Flechais, N. Nthala, and R. Abu-Salma, "Innovation inaction or in action? the role of user experience in the security and privacy design of smart home cameras," pp. 185–204. [Online]. Available: https://www.usenix.org/conference/soups2020/presentation/chalhoub

[45] James J. Gibson, "THE THEORY OF AFFORDANCES," in *The Ecological Approach to Visual Perception.*

[46] M. Dragiewicz, D. Woodlock, B. Harris, and C. Reid, "Technology-facilitated coercive control," in *The Routledge International Handbook of Violence Studies.* Routledge, num Pages: 10.

[47] M. A. Wood, M. Mitchell, F. Pervan, B. Anderson, T. O'Neill, J. Wood, and W. Arpke-Wales, "Inviting, affording and translating harm: Understanding the

role of technological mediation in technology-facilitated violence," p. azac095. [Online]. Available: https://doi.org/10.1093/bjc/azac095

[48] J. Slupska, S. D. Dawson Duckworth, L. Ma, and G. Neff, "Participatory threat modelling: Exploring paths to reconfigure cybersecurity," in *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI EA '21. Association for Computing Machinery, pp. 1–6. [Online]. Available: https://doi.org/10.1145/3411763.3451731

[49] B. Friedman, P. H. Kahn, Jr, and a. A. Borning, "Value sensitive design and information systems," in *Human-computer Interaction and Management Information Systems: Foundations.* Routledge, num Pages: 25.

[50] A. Uzunov and E. Fernández, "An extensible pattern-based library and taxonomy of security threats for distributed systems," vol. 36.

[51] A. Welekwe. Threat modeling guide. [Online]. Available: https://www.comparitech.com/net-admin/threat-modeling-guide/

[52] J. A. Ingalsbe, L. Kunimatsu, T. Baeten, and N. R. Mead, "Threat modeling: Diving into the deep end," vol. 25, no. 1, pp. 28–34, conference Name: IEEE Software.

[53] L. O. Nweke and S. D., "A review of asset-centric threat modelling approaches," vol. 11, no. 2. [Online]. Available: http://thesai.org/Publications/ViewPaper?Volume=11&Issue=2&Code=IJACSA&SerialNo=1

[54] Shostack + friends blog > apple guidance on intimate partner surveillance. [Online]. Available: https://shostack.org/blog/apple-guidance-on-intimate-partner-surveillance/

[55] T. Ucedavélez and M. Morana, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*, journal Abbreviation: Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis Pages: 664 Publication Title: Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis.

[56] T. Denning, T. Kohno, and H. M. Levy, "Computer security and the modern home," vol. 56, no. 1, pp. 94–103. [Online]. Available: https://dl.acm.org/doi/10.1145/2398356.2398377

[57] W. Hiller. What is secondary data? [examples, sources & advantages]. Running Time: 620 Section: Data Analytics. [Online]. Available: https://careerfoundry.com/en/blog/data-analytics/what-is-secondary-data/

[58] D. Cuomo and N. Dolci, "New tools, old abuse: Technology-enabled coercive control (TECC)," vol. 126, pp. 224–232. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0016718521002360

[59] L. Tanczer, I. Neira, S. Parkin, T. Patel, and G. Danezis, "Gender and IoT research report." [Online]. Available: https://www.semanticscholar.org/paper/90648e9dfd7be5cb98b67c1e7f3ad615ed2f9e64

[60] D. McKay and C. Miller, "Standing in the way of control: A call to action to prevent abuse through better design of smart technologies," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI '21. Association for Computing Machinery, pp. 1–14. [Online]. Available: https://doi.org/10.1145/3411764.3445114

[61] C. Geeng and F. Roesner, "Who's in control?: Interactions in multi-user smart homes." [Online]. Available: https://www.semanticscholar.org/paper/68accd14cf657643c3128f99647e7e0543295f6a

[62] N. H. Tan, R. Y. Wong, A. Desjardins, S. A. Munson, and J. Pierce, "Monitoring pets, deterring intruders, and casually spying on neighbors: Everyday uses of smart home cameras," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, ser. CHI '22. Association for Computing Machinery, pp. 1–25. [Online]. Available: https://doi.org/10.1145/3491102.3517617

[63] J. R. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. Wright, and M. Whitty, "Understanding insider threat: A framework for characterising attacks," in *2014 IEEE Security and Privacy Workshops*, pp. 214–228.

[64] B. Schneier. Academic: Attack trees - schneier on security. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

[65] I. Ray and N. Poolsapassit, "Using attack trees to identify malicious attacks from authorized insiders," in *Computer Security – ESORICS 2005*, ser. Lecture Notes in Computer Science, S. d. C. di Vimercati, P. Syverson, and D. Gollmann, Eds. Springer, pp. 231–246.

[66] L. Albert, S. Rodan, N. Aggarwal, and T. Hill, "Gender and generational differences in consumers' perceptions of internet of things (IoT) devices."

[67] A. Flynn, A. Powell, and S. Hindes, "Technology-facilitated abuse: A survey of support services stakeholders," p. 60.

[68] E. Tseng, R. Bellini, N. Mcdonald, M. Danos, R. Greenstadt, D. McCoy, N. Dell, and T. Ristenpart, "The tools and tactics used in intimate partner

surveillance: An analysis of online infidelity forums." [Online]. Available: https://www.semanticscholar.org/paper/0c22cdfa540102b58ae0ab1fed8d6df3f4ce5031

[69] T. Matthews, K. O'Leary, A. Turner, M. Sleeper, J. Woelfer, M. Shelton, C. Manthorne, E. Churchill, and S. Consolvo, "Stories from survivors: Privacy & security practices when coping with intimate partner abuse." [Online]. Available: https://www.semanticscholar.org/paper/1c0852f8658c2e63320008a3fcb44c3dcdac2036

[70] J. B. Kelly and M. P. Johnson, "Differentiation among types of intimate partner violence: Research update and implications for interventions," vol. 46, pp. 476–499, place: United Kingdom Publisher: Wiley-Blackwell Publishing Ltd.

[71] X. Lei, G.-H. Tu, A. X. Liu, K. Ali, C.-Y. Li, and T. Xie, "The insecurity of home digital voice assistants – amazon alexa as a case study." [Online]. Available: http://arxiv.org/abs/1712.03327

[72] L. Tanczer, I. Lopez-Neira, and S. Parkin, "'i feel like we're really behind the game': perspectives of the united kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse." [Online]. Available: https://www.semanticscholar.org/paper/75077e0174745fae8465cacb2be198536fbd1cdb

[73] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," vol. 21, no. 3, pp. 2702–2733. [Online]. Available: https://ieeexplore.ieee.org/document/8688434/

[74] T. Ashdown, C. Park, F. Begum, A. Panagiotidou, K. Sugand, and S. El-Tawil, "Do patients accurately represent their experiences after hip and knee replacements?" vol. 13, no. 1, p. e12745.

[75] M. Foucault, 1926-1984, *Discipline and punish : the birth of the prison.* First American edition. New York : Pantheon Books, [1977] ©1977. [Online]. Available: https://search.library.wisc.edu/catalog/999495361202121

[76] C. Geeng and F. Roesner, "Who's in control? interactions in multi-user smart homes," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ser. CHI '19. Association for Computing Machinery, pp. 1–13. [Online]. Available: https://doi.org/10.1145/3290605.3300498

[77] E. PenzeyMoog and D. C. Slakoff, "As technology evolves, so does domestic violence: Modern-day tech abuse and possible solutions," in *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, ser. Emerald Studies In Digital Crime, Technology and Social Harms, J. Bailey, A. Flynn, and N. Henry, Eds. Emerald Publishing Limited, pp. 643–662. [Online]. Available: https://doi.org/10.1108/978-1-83982-848-520211047

[78] R. D. Lee, M. L. Walters, J. E. Hall, and K. C. Basile, "Behavioral and attitudinal factors differentiating male intimate partner violence perpetrators with and without a history of childhood family violence," vol. 28, no. 1, pp. 85–94. [Online]. Available: https://doi.org/10.1007/s10896-012-9475-8

[79] A. Moore. Surviving a cyberstalker: How to prevent and survive cyberabuse and stalking by alexis moore, paperback . [Online]. Available: https://www.barnesandnoble.com/w/surviving-a-cyberstalker-alexis-moore/1127054486

[80] E. Tseng, M. Sabet, R. Bellini, H. K. Sodhi, T. Ristenpart, and N. Dell, "Care infrastructures for digital security in intimate partner violence." [Online]. Available: https://www.semanticscholar.org/paper/d50346dc6a45daadd75da8b729af46c532b456ab

[81] Linder. The danger of IoT and "tech abuse" in domestic violence. [Online]. Available: https://digitalmarketing.temple.edu/jlindner/2021/11/16/the-danger-of-iot-and-tech-abuse-in-domestic-violence/

[82] S. Zheng, M. Chetty, and N. Feamster, "User perceptions of privacy in smart homes," vol. abs/1802.08182. [Online]. Available: https://www.semanticscholar.org/paper/5edd9a0044941bc4e91cf3998cc6b48d39bd250f

[83] M. M. Rogers, C. Fisher, P. Ali, P. Allmark, and L. Fontes, "Technology-facilitated abuse in intimate relationships: A scoping review," p. 15248380221090218, publisher: SAGE Publications. [Online]. Available: https://doi.org/10.1177/15248380221090218

[84] Ablondi. 16+ smart home statistics for 2022 | hippo. [Online]. Available: https://www.hippo.com/blog/smart-home-statistics/

[85] P. Fersch. Financial abuse is domestic violence. Section: ForbesWomen. [Online]. Available: https://www.forbes.com/sites/patriciafersch/2022/07/21/financial-abuse-is-domestic-violence/

[86] Financial abuse and empowerment. [Online]. Available: https://nnedv.org/spotlight_on/financial-abuse-empowerment/

[87] A. Stubbs and C. Szoeke, "The effect of intimate partner violence on the physical health and health-related behaviors of women: A systematic review of the literature," vol. 23, no. 4, pp. 1157–1172.

[88] M. Oshana, *Personal Autonomy in Society.* Routledge.

[89] M. Ciurria, "The loss of autonomy in abused persons: Psychological, moral, and legal dimensions," vol. 7, no. 2, p. 48, number: 2

Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/2076-0787/7/2/48

[90] D. Freed, S. Havron, E. Tseng, A. Gallardo, R. Chatterjee, T. Ristenpart, and N. Dell, “"is my phone hacked?" analyzing clinical computer security interventions with survivors of intimate partner violence,” vol. 3, pp. 1 – 24. [Online]. Available: https://semanticscholar.org/paper/1cc3d7cbc37a51f330e9c9475b418f8870c98b72

[91] D. Cuomo and N. Dolci, “The TECC clinic: An innovative resource for mitigating technology-enabled coercive control,” vol. 92, p. 102596. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0277539522000371

[92] G. Kavallieratos, V. Gkioulos, and S. K. Katsikas, “Threat analysis in dynamic environments: The case of the smart home,” in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 234–240, ISSN: 2325-2944.

[93] R. Leitão, “Technology-facilitated intimate partner abuse: a qualitative analysis of data from online domestic abuse forums,” vol. 36, no. 3, pp. 203–242, publisher: Taylor & Francis _eprint: https://doi.org/10.1080/07370024.2019.1685883. [Online]. Available: https://doi.org/10.1080/07370024.2019.1685883

[94] Google nest and home device specifications - google nest help. [Online]. Available: https://support.google.com/googlenest/answer/7072284?hl=en

[95] A. Akinbi and T. Berry, “Forensic investigation of google assistant,” vol. 1, no. 5, p. 272. [Online]. Available: https://doi.org/10.1007/s42979-020-00285-x