Chapter 39

Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things

Julia Slupska and Leonie Maria Tanczer

Abstract

Technology-Facilitated abuse, so-called "tech abuse," through phones, trackers, and other emerging innovations, has a substantial impact on the nature of intimate partner violence (IPV). The current chapter examines the risks and harms posed to IPV victims/survivors from the burgeoning Internet of Things (IoT) environment. IoT systems are understood as "smart" devices such as conventional household appliances that are connected to the internet. Interdependencies between different products together with the devices' enhanced functionalities offer opportunities for coercion and control. Across the chapter, we use the example of IoT to showcase how and why tech abuse is a socio-technological issue and requires not only human-centered (i.e., societal) but also cybersecurity (i.e., technical) responses. We apply the method of "threat modeling," which is a process used to investigate potential cybersecurity attacks, to shift the conventional technical focus from the risks to systems toward risks to people. Through the analysis of a smart lock, we highlight insufficiently designed IoT privacy and security features and uncover how seemingly neutral design decisions can constrain, shape, and facilitate coercive and controlling behaviors.

Keywords: Tech abuse; intimate partner violence; domestic violence; cybersecurity; threat modeling; internet of things

> "I changed the lock on my front door so you can't see me anymore.
>
> And you can't come inside my house, and you can't lie down on my couch.

The Emerald International Handbook of Technology-Facilitated Violence and Abuse, 663–688

doi:10.1108/978-1-83982-848-520211049

> I changed the lock on my front door" —Lucinda Williams "Changed the Locks".

Introduction

Technology-Facilitated abuse or "tech abuse" through Global Positioning System (GPS) trackers, smartphone apps, or platforms such as *Facebook* has a substantial impact on the nature of intimate partner violence (IPV). The latter encompasses diverse forms of abuse (e.g., physical, sexual, financial) and coercive and controlling behavior by a (current or former) partner or spouse (Bagwell-Gray, Messing, & Baldwin-White, 2015). IPV, and more specifically, domestic abuse[1] globally affects about 1 in 3 (35% of) women in their lifetime (World Health Organization, 2017) and more than 2.4 million UK adults a year (Office for National Statistics, 2019).

Parallel to the widespread deployment of technologies, their misuse, especially in the context of domestic and sexual violence, is increasing. While national figures remain absent (Tanczer, Neira, Parkin, & Danezis, 2018), data points gathered by charities such as Think Social Tech, Snook and SafeLives (2019), and Women's Aid (2018) point to the rising scale as well as the urgency of this issue. According to Refuge (2020), the UK's largest domestic violence charity, more than 72% of their service users experience abuse through technology.

Furthermore, emerging technologies such as smart, internet-connected devices have begun to enter our households. These so-called "Internet of Things" (IoT) range from gadgets such as "smart speakers," as well as embedded infrastructures such as connected thermostats, blinds, or locks. IoT devices open up new avenues to remotely monitor, control, and harass victims/survivors (Parkin, Patel, Lopez-Neira, & Tanczer, 2019).[2] Their interconnectedness and growing level of sophistication make them tools to help facilitate other coercive and controlling offenses, including stalking.

The current chapter sets out to examine the risks and harms[3] that derive from the burgeoning IoT environment. We showcase *how* and *why* tech abuse is a socio-technological issue that requires not only human-centered (i.e., societal), but also cybersecurity (i.e., technical) responses. We thus use the notion of "threat modeling," which is a process that investigates potential cybersecurity attacks to focus on the risks both to *systems* and to *people* (Uzunov & Fernandez, 2014). Through the analysis of a smart lock, we exemplify insufficiently addressed dangers and uncover how seemingly neutral design decisions can constrain, shape, and facilitate coercive and controlling behaviors.

Existing Research

IoT-Enabled Technology-Facilitated Abuse

The proliferation of so-called smart, internet-connected devices poses a new tech abuse challenge. The move toward IoT includes the direct and indirect extension of the internet into a range of physical objects, devices, and products, with a broad range of applications (Tanczer, Brass, Elsden, Carr, & Blackstock, 2019,

p. 37). Previously "offline" and "unrelated" technologies such as conventional household appliances are now being interconnected and become part of a network which allows them to – put simply – "speak" to one another.

While IoT systems range from tiny sensors to large-scale cyber-physical systems such as cars, consumer IoT devices form a dominant focus of ongoing analyses. Consumer IoT describe systems created to be used by "average" end users in a personal capacity and/or within the home setting. Such devices include, for example, smart speakers, wearables, and a range of security systems. In the UK, 31% of the 35–44 age group own three or more connected devices with IoT usage expected to increase significantly over the next decades (Tech UK, 2019).

IoT appliances not only collect reams of information, including personal data, preference settings, and usage patterns, but offer an opportunity to be remotely controlled. Combined with features such as video and audio recording functionalities, IoT devices open up significant exploitative avenues in an IPV context (Leitão, 2019). Society is therefore in urgent need to understand the broader classes of harms IoT systems may cause and conceptualize how these harms could move beyond "conventional" understandings of safety, security, and privacy.

So far, the research on IoT-affiliated tech abuse in the context of IPV is in its infancy. Only a handful of studies have evaluated the tech abuse risks that derive from the deployment of smart devices in the home. Leitão (2018, 2019) examined the potential security and privacy threats that victims/survivors of IPV would face. Strengers, Kennedy, Arcari, Nicholls, and Gregg (2019) conducted an ethnographic study with early IoT adopters. They showed that women need to be able to operate IoT systems safely and securely without exposing themselves or others to additional internal or external threats. Slupska (2019) reviewed 40 smart home security papers and uncovered that the only article that explicitly addressed IPV in their analysis was dismissive of the risk potential and displaced the responsibility of protection onto potential targets of abuse. Besides, the Gender and IoT research project at University College London conducted a usability analysis of the shared device ecosystem (Parkin et al., 2019), exposing, among other findings, that the lack of security and privacy prompts can negatively impact tech abuse victims/survivors. Based on their findings, the research team produced guides and resources for the IPV support sector (Tanczer, Patel, Parkin, & Danezis, 2018, 2019) and briefings for the policy community (Tanczer, Lopez-Neira et al., 2018).

Despite the limited evidence-base on IoT-enabled tech abuse, emerging classes of harms have to be evaluated in light of the dynamics of IPV (Katerndahl, Burge, Ferrer, Becho, & Wood, 2010; de Lucena et al., 2016). For example, Matthews et al. (2017) developed a framework for organizing victims'/survivors' technology practices and challenges into three phases, including: physical control, escape, and life apart (see Fig. 39.1). While their research centered on "conventional" devices such as computers and phones, similar considerations will have to be applied to both the social and technical responses to IoT.

Matthews et al.'s (2017) findings further showcase that tech abuse victims/survivors face high levels of stress and risk, which makes it harder for them to pay

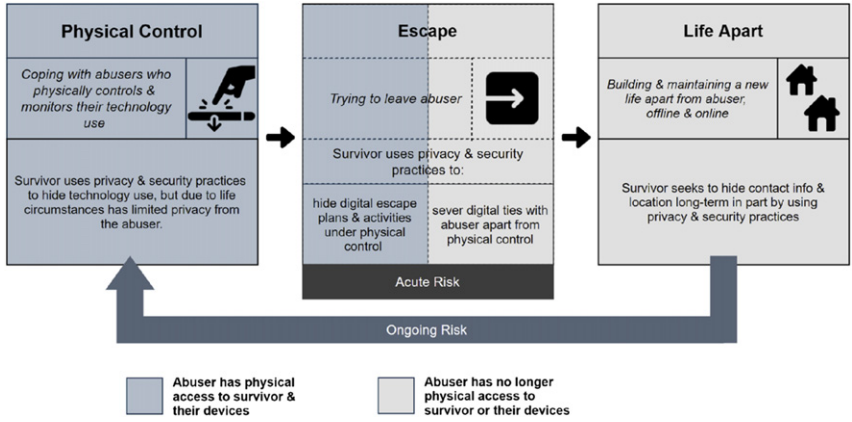

Fig. 39.1. Three Phases of IPV that Affected Technology Use, Focusing on Privacy & Security Practices. *Source:* Adapted from Matthews et al. (2017).

attention to user interface (UI) details. The latter are means by which a user interacts with and regulates a technical system. UI can be graphical controls such as one's home screen or the menu bar, as well as hardware devices such as a remote, switch, or keyboard (Myers, 1989). Victims/survivors are consequently disadvantaged in making use of privacy and security features and struggle to identify, access, and act upon instruction materials (e.g., how to block a phone number, how to set up multi-factor authentication).[4]

Drawing on these insights, Matthews et al. (2017) suggested that technology designers should consider the usability of their inventions and acknowledge the distinct privacy and security requirements of IPV victims/survivors. This focus seems of high relevance looking at the *limited* (i.e., fewer buttons) as well as *dispersed* (i.e., control through the device as well as an app on the phone) interfaces IoT technologies such as smart speakers offer. Yet, as the upcoming section will display, the tech sector has so far ignored the potential challenges that these devices create and failed to implement technical responses to the daily privacy and security trade-offs that IPV victims/survivors must make (Freed et al., 2018; Slupska, 2019).

Cybersecurity Design Shortcomings

The threats and consequent risks deriving from IPV are almost absent in the cybersecurity literature as well as practice and even less of a discussion point in the emerging field of IoT (Slupska, 2019; Tanczer et al., 2018). Instead, the cybersecurity community often focuses on "hard" technical problems posed by remote "external" adversaries who exploit hardware or software vulnerabilities. Yet, as Freed et al. (2018) pointed out, most IPV attacks are technologically unsophisticated. This allows perpetrators to interact with a victim's/survivor's

device or account via their standard settings, generic UI, or by simply downloading and installing a ready-made application that facilitates, for instance, the spying on a victim/survivor. Hence, the "typical" tech abuse perpetrators must be thought of as a "UI-bound adversary" (Freed et al., 2018).

This perspective distinguishes IPV perpetrators from the cybercriminals who are the central focal point of cybersecurity research. In fact, perpetrators' lack of technical skill carries the risk that a focus on tech abuse could be dismissed as trivial. However, the socio-technical and interpersonal factors that characterize tech abuse undermine the foundational assumptions under which current digital systems have been designed and built (i.e., insider vs. outsider; legitimate vs. illegitimate user etc.). For example, "safety features" of devices, such as location tracking, are co-opted by abusers for surveillance purposes. This dynamic makes IPV attacks both challenging to technically counteract but also extremely damaging to victims/survivors.

Like most digital products and services, smart home systems are based on an "authentication model." This model implies that features such as passwords and security questions guarantee that an unauthenticated user (i.e., individual without login credentials) cannot access the system. However, IPV perpetrators are often aware of sign-in details, either because they purchased, installed, and maintained the device, or because they convinced or coerced the victim/survivor into sharing the information. Some perpetrators may be able to guess credentials due to personal knowledge they have of victims/survivors. Thus, in many IPV attack scenarios, the abuser is effectively "authenticated" and "authorized."

A possible parallel to the IPV tech abuse problem within the cybersecurity literature is the so-called "insider threat." The latter describes a threat posed to an organization by rogue, disgruntled, or careless employees (Bishop & Gates, 2008; Nurse et al., 2014). Since employees often have access to login details, they are also *authenticated adversaries.* However, insider threats in the context of cybersecurity are almost always conceptualized as actors internal to the company (i.e., rogue employees) rather than internal to the home (i.e., family members). This narrow view of what "insider threat" implies is reflective of the corporate positionality of most cybersecurity research, which we hope to counterbalance in this chapter.

The discussed oversights, including the focus on sophisticated attacks as well as corporate rather than domestic threats, are deficiencies of popular cybersecurity "threat models." Threat models describe a systematic analysis of a probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker. Threat models, therefore, involve assumptions about likely attackers and can reflect biases and blind spots as seen in the exclusion of IPV perpetrators in cybersecurity practitioners' mental models. Readers may be alerted to the subjective nature of this process. To counter any skewed perspectives, we are arguing in favor of the deployment of thorough procedural methods as well as the inclusion of diverse voices – such as the IPV sector.

So far, existing solutions to the problem of tech abuse have mostly involved the development of guidance to aid victims/survivors as well as support services (Online and Digital Abuse, 2018; Tanczer et al., 2018). Although such tools are useful, they shift responsibility onto victims/survivors. The latter already face

significant cognitive, emotional, and financial constraints and are now further burdened having to check settings across a multitude of applications. Harris and Woodlock (2019) describe this additional onus as "safety work." The authors argue that digital coercive control has led to new forms of victim-blaming which manifest itself in women being accused of having inflicted harm upon themselves by choosing to use certain devices and/or platforms. The fact that these systems are frequently victim's/survivor's primary link to their support network is overlooked. Furthermore, possible regional specificities, such as family-internal device sharing practices, are not accounted for (Sambasivan et al., 2019).

Moving beyond these victim/survivor-straining proposals, existing issues associated with tech abuse are closely interlinked with the design of technological systems (Levy & Schneier, 2020). This is exemplified in reported cases of compromised webcams (Anderson, 2013), the repurposing of features such as real-time location sharing via Google Maps (Ashworth, 2018), or the review of victim's/survivor's historical queries and online searches by a perpetrator (Women's Aid, 2018).

A common obstacle to the implementation of better IPV privacy and security measures stems from the fact that IoT's inherent functionalities (e.g., remote control, speech recognition) can equally benefit perpetrators as much as victims/survivors (Parkin et al., 2019). This "dual-use" problem – a term coined to describe the fact that digital systems may be designed for peaceful use but can also be co-opted for malicious purposes and vice versa – has been widely discussed in the cybersecurity literature (Nye, 2018; Riebe & Reuter, 2019). However, it has not yet been modeled onto the context of IPV. For example, a perpetrator may install a smart camera to spy on their partner, while a victim/survivor may install a smart camera to feel in control of their environment. The answer to *who is being empowered* by IoT is consequently dependent on *who has control* over the device and network.

The adjustment of established cybersecurity methods like risk assessments, usability tests, and safety reviews can help tech vendors to consider adversarial users when designing and evaluating UIs (Freed et al., 2018; Parkin et al., 2019). On these grounds, we would like to put forward the idea of designing a dedicated "IPV Threat Model" to explore and document avenues for harming IPV victims/survivors. While not a panacea – as some proposed changes may, in some contexts, benefit perpetrators – such a framework can limit an IoT systems' "abusability" (i.e., its capacity to be abused) and account for the cybersecurity needs of some of the most vulnerable groups in society.

A Method to Threat Model Intimate Partner Violence Tech Abuse

Threat modeling describes a process used to analyze potential attack vectors on a system (Uzunov & Fernandez, 2014). The concept of "threat" is hereby understood as the probable cause of an incident that might result in harm to systems, individuals, and organizations (Sabbagh & Kowalski, 2015), with a "threat actor" being the entity who wishes to cause a – usually negative – impact (Coles & Tarandach, 2020).

While threats may arise from both accidental and deliberate activities of "legitimate users" (the owner/account holder of a device; Omotosho, Haruna, & Olaniyi, 2019), we assume that an IPV threat actor may be a perpetrator who *intentionally abuses* specific technical features to monitor, control, or coerce a victim/survivor. Thus, the perpetrator may be an authorized user yet still abuses the system for illegitimate means.

We acknowledge that the literature on threat modeling can be daunting and full of jargon. It is a field populated by acronyms such as DREAD (i.e., Damage, Reproducibility, Exploitability, Affected User, Discoverability) and STRIDE (i.e., Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), and characterized by debates about the distinction of *threat* and *risk*. Confusingly, the words "threat model" and "threat modeling" are applied in many dissimilar and perhaps incompatible ways. However, for the purpose of this chapter, we will deploy a pragmatic definition and conceptualize threat modeling as the use of abstractions to aid in thinking about threats and risks (for a detailed review, see Shostack, 2014).

There are also various approaches to threat modeling, ranging from: (a) asset-based threat modeling; and (b) system-based threat modeling; to (c) attacker-based threat modeling. These approaches can be applied in conjunction with the attempt to generate: (a) an illustration of the system that is potentially being attacked (e.g., a smart watch); (b) assumptions about the profiles of potential attackers, including their goals, methods, and motives (e.g., an IPV perpetrator); and (c) a catalog of likely threats that may arise (e.g., information disclosure). Threat modeling therefore echoes the risk assessment process currently deployed in the IPV support sector (Nicholls, Pritchard, Reeves, & Hilterman, 2013; van der Put, Gubbels, & Assink, 2019).

Following Shostack's (2014, p. xxvii) suggested system-based approach, threat modeling involves four steps, each answering a deceptively simple question:

(1) What are you (i.e., the tech vendor) building?
(2) What can go wrong with it once it's built?
(3) What should you do about those things that can go wrong?
(4) Did you do a decent job?

Although system-based approaches such as this one are implicitly aimed at tech developers and vendors, we believe it is valuable for anyone studying tech abuse – whether from the perspective of social or computer science – to be comfortable with the conceptual framework of threat modeling. The latter allows researchers to reflect, understand, document, and react to the possible shortcomings of digital devices and services (Sabbagh & Kowalski, 2015; Torr, 2005). By becoming fluent in the language of threat modeling, IPV scholars and practitioners can more effectively critique problematic technology designs.

In the upcoming section, we walk readers through the building blocks of this framework. While it may seem abstract, we hope to showcase the benefit of its adoption in the IPV tech abuse space. Specifically, in the following passages, we will apply Shostack's (2014, p. xxvii) four questions to examine how a hypothetical smart lock IoT system can be breached, leading to the harm of an IPV victim/survivor.

System: What Are You Building?

The threat modeling process begins with collecting necessary information about the relevant components of a device, software program or system (Torr, 2005). This decomposition gives stakeholders an overview of all the different segments, data points, and interactions to effectively identify, understand, and model its makeup (Xiong & Lagerström, 2019). Developers begin by creating simple diagrams and tables to provide an overview of the system being threat modeled. These diagrams can clarify different interdependencies and features of systems, which are particularly important for smart, internet-connected devices (Steven, 2010). For tech designers and vendors, these visual representations form a useful way to abstract all system properties and diagnose what an application does (Coles & Tarandach, 2020).

Threats: What Can Go Wrong with It Once It's Built?

After the exposure of the "anatomy" of a system, tech vendors use the generated diagrams to look at what could go wrong. For example, a brainstorming meeting to determine and enumerate all potential threats could be held. As there are an unlimited number of things which could fail, this second step has the potential to be the most overwhelming. The evaluation of interconnected systems such as IoT technologies creates an additional level of intricacy than the analysis of individual devices and application alone. However, in both cases, tech designers should assess opportunities for abuse across the whole infrastructure (Coles & Tarandach, 2020).

Some approaches start by profiling probable attackers, including their resources, motivations, and capacity (Atzeni, Cameroni, Faily, Lyle, & Flechais, 2011; Little & Rogova, 2006). The identification of an attacker's intentions can assist in the forecasting of an attack's sophistication level, which is particularly useful when examining IPV cases. The threat identification process involves a certain reliance on assumptions as to the nature of a likely perpetrator. These assumptions are often limited and stereotypical (Atzeni et al., 2011), which is – considering the lack of diversity among cybersecurity practitioners, as well as the lack of data on tech abuse – problematic (Lopez-Neira, Patel, Parkin, Danezis, & Tanczer, 2019; Poster, 2018).

Having a diverse team is vital for threat modeling. Institutional and personal life experience shape perceptions of threats. Thus, technologists who specialize in Windows systems will often skew their threat model toward Windows-specific concerns, while web developers will be primarily focused on web-based attacks. Equally, our own biases as authors of this chapter will have influenced the threat actors and attack scenarios we are examining. To mitigate such shortcomings, we want to reiterate that active collaboration with affected groups and communities such as the domestic abuse sector must be sought.

When looking at an attacker's profile, both their opportunities for exploitation and/or their attack motives can be significantly influenced by environmental conditions. For instance, a perpetrator with a background in software development

may be far more likely to consider exploiting smart home devices. Nonetheless, an attacker's capacity must be contrasted, considering their potential motivation. Depending on both aspects, one must expect changes to the: (a) intensity; (b) sophistication; and (c) probability of a tech abuse attack taking place; as well as (d) a perpetrator's ability to distort/eliminate forensic evidence (UcedaVelez & Morana, 2015).

Based on the current evidence-base, tech abuse perpetrators are often highly motivated or even obsessed with the desire to monitor, coerce, intimidate, or otherwise harm a victim/survivor. They can, but do not have to, be physically present (Ho et al., 2016). Abusers are also rarely strangers.[5] They often have or had romantic relations with victims/survivors. Nonetheless, tech abuse can also be perpetrated by family members, colleagues, roommates, or acquaintances (Levy, 2015). IPV perpetrators often have intimate knowledge of the victim/survivor, including awareness of their daily habits, history, and login details, or access to personal data like sexually explicit or embarrassing photos and messages (Table 39.1).

In addition to this profiling exercise, it is helpful to account for known attack patterns (UcedaVelez & Morana, 2015). Drawing on Freed et al. (2017) and Leitão (2019), we propose a model of five common tech abuse threats:

Table 39.1. Tech Abuse Threat Model.

Name	**Description**
Ownership-based access	Being the Owner of a device or account allows a perpetrator to prohibit victims'/ survivors' usage or track their location and actions;
Account/device compromise	Guessing or coercing credentials which enables a perpetrator to install spyware, monitor the victim/survivor, steal their data, or lock them out of their account;
Harmful messages	Contacting victims/survivors or their friends, family, employers, etc. without their consent;
Exposure of information	Posting or threatening to post private information or nonconsensual pornography (i.e., image-based sexual abuse);
Gaslighting	Using a device's functionality (e.g., remote changing of temperature) to make a victim/ survivor feel as if they are losing their sanity and/or control over their home.

These threats can be connected to the specific features of the device in order to identify which forms of tech abuse are possible/likely (as we do in the following section). The second step ends with documenting as well as rating all diagnosed threats (Meier et al., 2003).

Response: What Should You Do about Those Things that Can Go Wrong?

The third question involves the examination of countermeasures to tackle each threat. Conventionally, responses are (a) to reduce/mitigate threats through the implementation of safeguards and changes to eliminate vulnerabilities or block threats; (b) to assign/transfer threats by placing the cost of the threat onto another entity or organization such as purchasing insurance or outsourcing; or (c) to accept the threat by evaluating if the cost of the countermeasure outweighs the possible cost of loss due to the threat. While the full elimination of threats is generally possible, it would require almost always the removal of features which industry actors may be opposed to (Shostack, 2014).

Mitigations are consequently specific to a device's design goals and limited by a vendor's resources, interests, and capacity. Therefore, this step also involves prioritizing different threats in order to identify which mitigations are most urgent. In the private sector, such assessments are often quantified and based on financial losses. Tech vendors have so far struggled – and often failed – to incorporate more intangible social, emotional, or psychological harms, including damage to reputation or mental health implications. The industry's viewpoint on the importance of economic ramifications disproportionally disregards the broader implications technical innovations may have on different groups of society, which we aspire to alleviate in this chapter.

Validation: Did You Do a Decent Job of Analysis?

The final question involves a critical reflection on the efficacy of the generated threat model. To support this evaluation process, different validation methods can be deployed (Xiong & Lagerström, 2019). What unifies these methods is their attempt to check the model's completeness and accuracy. The scrutiny guarantees that the final model matches the system that is built, addresses all the right and relevant threats, and covers all the decisions that have been made (Shostack, 2014). By this stage, every possible attack scenario should have been considered and accounted for and a planned countermeasure laid out.

A common practice to support this step is the reliance on "test cases" or "case studies" (Shostack, 2014; Xiong & Lagerström, 2019). Another form of explanation and validation includes collecting data on device usage "in the wild." Moreover, data on reported breaches can be helpful, especially if contrasted with initial threat models to understand whether a threat was inadequately addressed or missed entirely. Together with a frequent reiteration of the threat modeling

exercise, new and unanticipated threats can be accounted for and timely and effective mitigation strategies implemented.

Threat Modeling a Smart, Internet-Connected Lock

The following section outlines a threat modeling exercise for an IoT consumer device in the context of IPV. We choose the case study of a hypothetical, but prototypical smart lock system because it has relatively simple functionality (i.e., opening and closing a door) and plays a key role in home security (i.e., allowing and preventing access). Furthermore, the adoption and market share of internet-connected locks is expected to grow (PR Newswire, 2019), making it a technology that is, or soon will be, deployed in the home of the "average" end user. We draw on the four questions outlined by Shostack (2014), and use the upcoming passages to

(a) Model the relevant features prevalent in common smart lock systems (what are you building?);
(b) Show how specific features may be abused (what can go wrong?);
(c) Suggest possible mitigation strategies (what should you do about those things that can go wrong?); and
(d) Discuss limitations of the threat model we developed (did you do a good job?).

In the current threat modeling analysis, we are foregrounding the device rather than its user or its interplay with the broader system of interconnected products (i.e., how a smart speaker interacts with the smart lock). We acknowledge that this viewpoint has limitations; as the common security saying goes, "all models are wrong; some models are useful." For one, an IoT system cannot be viewed as a purely "technical" problem. In most cases, social and technical aspects are tightly interwoven, requiring both social and technical countermeasures (Sabbagh & Kowalski, 2015). However, as previous tech abuse mitigation strategies have primarily focused on victims/survivors and support services, our emphasis seems appropriate. For another, investigating a single device over an assembled system allows for vulnerabilities to pass through undetected (J. R. C. Nurse, Creese, & Roure, 2017). While we accept that one must account for the entire IoT "ecosystem" (Aufner, 2020; Omotosho et al., 2019; Seeam, Ogbeh, Guness, & Bellekens, 2019), a broader investigation is beyond the scope of this chapter.

System: What Are You Building?

Our hypothetical "smart lock"[6] is a round knob which attaches to the inside of a standard dead bolt. The smart lock can be physically turned from the inside to open/lock the door. It also allows a user to lock/unlock the door electronically using a mobile application[7] (app) on their smartphone. To do this, the smart lock

connects to a user's smartphone using Bluetooth, a wireless technology standard used for exchanging data over short distances (Hadis, Palantei, Ilham, & Hendra, 2018). The smartphone app communicates with the smart lock's company's web servers via Wi-Fi.

Wi-Fi is another wireless technology that uses radio waves to provide high-speed internet and network connections. The company's web servers describe both hardware and software components which store, centralize, and manage the files a user requests when engaging with a company's website or app. The smart lock's setup means that the device itself is not directly connected to the internet. Instead, the smart lock communicates with the smartphone app via Bluetooth. Therefore, for this threat model, the smart lock *system* consists of (a) the smart lock; (b) the smartphone app; and (c) the company's web servers which support the app (see Fig. 39.2).

The smart lock has two "modes" for opening doors: either the user manually opens the smartphone app and presses a large button to open the door or the door is set so that the lock opens the moment the phone is within Bluetooth range. The smart lock device also records which users lock or unlock the door, storing the data on the smartphone app and in the web servers.

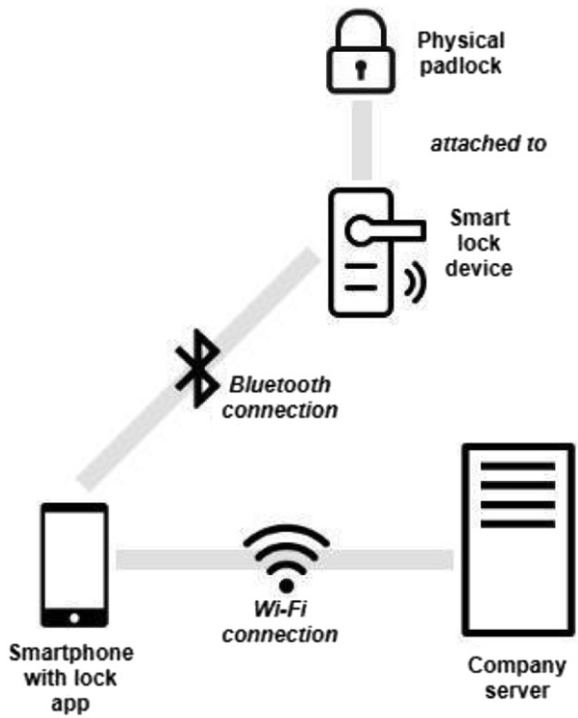

Fig. 39.2. Overview of the Smart Lock System.

Users identify themselves by logging into the smartphone app with their phone number or email address and a corresponding password. There are two different user account types: "Owner" and "Guest." The first and original user is *by default* an Owner. However, the device allows multiple Owners and Guests. The Owner is effectively the administrator of the system. They have more privileges than Guests. For example, an Owner can view the lock's activity log (i.e., past accesses), invite new users to be Owners or Guests, and configure when and for how long Guest users can lock/unlock the door (Ur, Jung, & Schechter, 2013; Table 39.2).

Table 39.2 Account Capabilities.

Capability	**Owner**	**Guest**
Lock/unlock door	Yes	Yes
View activity log	Yes	No
Invite new users to be Owner or Guest	Yes	No
Remove Owner or Guest access	Yes	No

Source: Adopted from Ye, Jiang, Yang, & Yan (2017b).

Users cannot access another user's account without having access to a fellow user's credentials. However, the main Owner can remove other users – both Owners and Guests – without having to access (i.e., login) their accounts.[8]

Threats: What Can Go Wrong with It once It's Built?

There are countless possible threats that could apply to a smart lock, some of which have already been explored by cybersecurity researchers (Fernandes, Jung, & Prakash, 2016, p. 636; Pavelić, Lončarić, Vuković, & Kušek, 2018; Ye, Jiang, Yang, & Yan, 2017a).[9] However, our model of IPV threats outlined earlier helps to focus on specific "attack vectors" (i.e., methods by which an adversary may gain access to the lock), followed by eight "threats," (i.e., specific forms of abuse which can occur after a lock has been compromised).

(1) Ownership-based access: Perpetrator has an Owner account and revokes and/or monitors a victim's/survivor's access.
(2) Smartphone compromise: Perpetrator illegitimately accesses the victim's/survivor's phone while within reach of the smart lock, which offers them digital access to the app, as well as physical access to the property.
(3) Account compromise: Perpetrator coerces or guesses victim's/survivor's smartphone app *or* smart lock account details, which allows the perpetrator to log into the victim/survivor's account on the perpetrator's own smartphone or laptop.

(4) Smart lock compromise: Perpetrator physically damages the smart lock making it unusable or causes a power outage which in certain circumstances may restrict residents from entering the house/locking the door.
(5) System compromise: Perpetrator can use default functions of the smart lock as some poorly designed IoT devices allow anyone on the same Wi-Fi home network to control an internet-connected product.

We acknowledge that it is possible to deploy more technically sophisticated attack scenarios (Ye et al., 2017b). However, the attack vectors discussed here showcase the range of relatively simple attack vectors that are available to the "UI-bound adversary." These attack vectors enable some of the following forms of abuse, or "threats":

(1) Restricting access: Perpetrator removes the victim's/survivor's account and/or changes their password, which can restrict the victim's/survivor's access to their account, as well as the shared home. This can be particularly damaging in the context of cohabitation where physical residency can impact decisions on ownership in court settlements.
(2) Gaining access: Perpetrator maliciously gains access to the property even after the victim/survivor attempted to lock them out. This can result in physical or psychological harm to the victim/survivor and/or their family.
(3) Monitoring: Perpetrator monitors the victim/survivor and/or other residents through the account access log. This can facilitate stalking or coercive control by giving the perpetrator the exact times that a victim/survivor and/or other residents enter and exit their home (Ur et al., 2013).
(4) Exposing information: Perpetrator uses the information received from an account compromise to coerce or expose the victim/survivor. This can result in personal information leakage (e.g., address) which threatens the user's privacy.
(5) Impersonating users: Perpetrator compromised the account of another resident and uses these credentials to access the property unnoticed. This engenders the physical safety of the victim/survivor and/or fellow residents.
(6) Gaslighting: Perpetrator unlocks the door just before the victim/survivor arrives home, making it seem like the device is malfunctioning or the door was never locked in the first place. This may result in victims/survivors doubting the functionality and security guarantee of their smart lock.
(7) Contacting victim/survivor: Perpetrator tries to enter the property with an unauthorized smartphone, which leads the victim/survivor to receive a notification (Khalid & Majeed, 2016). This can cause distress and anxiety for the victim/survivor who now has an awareness of the perpetrator's access attempt.
(8) Distracting and deceiving: Perpetrator argues that they had previously physical access to a device such as a victim's/survivor's smartphone which could give them the impression of an attacker having more access than they do. Akin to gaslighting, this can cause a victim/survivor to feel uncertain about their level of security and safety.

The power dynamics inherent to IPV cases add further complications to the scenarios expressed here. Tech abuse stemming from ownership-based access seems particularly likely, as the Owner of a smart home device has an inbuilt advantage in monitoring and controlling other users (i.e., members of the household). Research has demonstrated these gendered aspects of "digital housekeeping," namely that men are more likely to set up and maintain smart home technologies (Kennedy, Nansen, Arnold, Wilken, & Gibbs, 2015; Leitão, 2019; Strengers, Kennedy, Arcari, Nicholls, & Gregg, 2019). Therefore, account ownership may reinforce power inequalities in the household related to gender, technical ability, or finances (as these dictate who purchases devices).

Furthermore, even if a victim/survivor is the authorized Owner of the smart lock, the removal of the perpetrator's account – whether they have had previously held legitimate Guest access or have been detected to have received access to the account illegitimately – can expose the victim/survivor to further risks of violence and abuse. The act of withdrawing a perpetrator's admission can escalate the abuse situation and could cause perpetrators to react (e.g., confront or harm the victim/survivor). For this reason, mitigations to tech abuse – which are discussed hereafter – must be highly context-specific with designers minimizing the risk of abuse independently of the user's ownership status.

Response: What Should You Do About Those Things That Can Go Wrong?

Various research teams have already emphasized possible tech abuse responses industry actors, policymakers, and support services can deploy (Havron et al., 2019; Leitão, 2018; Lopez-Neira et al., 2019; Parkin et al., 2019; Tanczer et al., 2018). However, it is important to stress that technical mitigation strategies will not exhaustively "solve" the problem. As in other attack scenarios, security is never perfect or absolute, and technical solutions need to accompany robust social and legal support for victims/survivors. By the very nature of tech abuse – which includes the notion of the *authenticated adversary* – compromise and security breaches are *always* likely. Thus, one cannot prevent an IPV attacker by simply establishing *conventional* technical barriers (e.g., implementing a firewall, setting up password protections) as there are no trusted "safe zones" victims/survivors can rely on (Weinert et al., 2019).

As seen through our proposed mitigation strategies, many design choices may equally benefit victims/survivors as much as perpetrators. Thus, we are fully aware that an adversary may co-opt our proposed strategies in order to gain access or control victims/survivors further. However, some design decisions can enable harm more easily than others. Consequently, rather than looking to eliminate sources of vulnerability, we believe it is more useful for industry actors to think in terms of beneficial design patterns. The latter are likely to *enable* usability for people experiencing abuse and *hinder* usability for those perpetrating abuse. Tech abuse stemming from the following compromise forms may consequently be mitigated by:

The five attack *vectors* are as follows:
Ownership-based compromise:

(1) Restricting ownership: As preventing ownership-based access is impossible, security designs should give Owners less exhaustive authority over the smart lock system. This may include a security protocol which allows the company to remove an Owner in exceptional circumstances, such as when requested by a domestic abuse court order.[10]
(2) Equalizing account holder rights: Moving away from models where only one user is an account Owner or doing away with an Owner/Guest user distinction.
(3) Consent changes: Shared IoT devices such as smart locks may require all associated users to approve fundamental changes to the settings which prevent Owners from overpowering others.
(4) Customer-facing staff guidance: Akin to the "Assisting Customers Experiencing Domestic and Family Violence Industry Guideline" (Communications Alliance Ltd, 2018), customer-facing staff guidance on how tech vendors can support tech abuse victims/survivors may be developed to assist users in the instance of disputes around who is a legitimate account holder (Tanczer, 2019).

Smartphone Compromise:

(5) Report theft feature: A "report theft" feature could be activated from the victim's/survivor's web account to minimize the access a perpetrator may have over a device such as their smartphone.
(6) Automatic logouts: Users could be automatically logged out of their accounts, requiring them to reauthenticate themselves on timed patterns when using their smartphone to lock/unlock a smart lock. This may prevent unauthorized usage by others should the phone ever get lost.

Account Compromise:

(7) Register of login details: Regular notifications of login locations (i.e., where) and associated timestamps (i.e., when) may be accessible to victim's/survivor's through their account settings (Parkin et al., 2019). Crucially, these should be sufficiently vague so as not to put a victim/survivor in danger should a perpetrator access this information.
(8) New login prompts: Accounts may trigger a notification when a login on a new IoT device is attempted.
(9) Changing of passwords prompts: A new login should be required across all devices if a user changes their password, to ensure that other users do not stay logged in after, for example, a breakup.
(10) Reinstate account ownership: The ability to reinstate access to previously compromised accounts may be mitigated through time-stamped company backups which can allow victims/survivors to regain control over their data (e.g., after a court order).

(11) Multi-factor authentication: Different authentication methods should become part of the IoT design feature and may ensure that accounts are less prone to, for example, password coercion (Leitão, 2018).
(12) Transparency around privileges: Users on lower authorization levels (i.e., Guest accounts) should receive continued reminders of the extent of information they receive in comparison to other account holders, such as "Owners." This may alert victims/survivors to the fewer privileges they hold compared to their partner and remind them that a perpetrator could have access to their activity log.
(13) Access trails: IoT devices could notify other users every time another account holder checks critical settings such as access logs. This may prevent obsessive or routine checking of another user's behavior as the monitoring individual would be informed about this action.

Smart Lock Compromise:

(14) Factory reset: IoT devices should enable a simple mechanism to reset the product to its original state, enabling victims/survivors to restrict access after a compromise or breakup occurred. In the context of IoT, this mechanism needs to be both simple to activate (e.g., through a button) and potentially difficult to pursue from outside the home Wi-Fi network. Once initiated, the device should also send a final "good-bye" message to all users, which would alert them to an illicit factory reset.
(15) Logs: Victims/survivors may need to provide proof that a breach of, for instance, a protection order has occurred. Access logs such as who has accessed, locked, unlocked the door should, therefore, be unchangeable for any account holder.
(16) Disable functionalities: Users should be able to decide if they would like to disable certain functionalities such as the remote closing/opening of a smart lock.

System Compromise:

(17) Connection reminders: Regular prompts reminding users which IoT devices are connected and which accounts are associated with them may flag to victims/survivors if a perpetrator is still linked to their devices (Parkin et al., 2019).
(18) Opt-out: IoT devices should allow users to opt out from distinct data collection measures which are not required for the essential functionality of a connected product. This aligns with data minimization principles.
(19) Actionable advice: Up-to-date guidance on what steps a user should take when they suspect their home network has been compromised must be available to victims/survivors and communicated in a simple and understandable format (Parkin et al., 2019). A dedicated button that says, "I am a victim/survivor of domestic violence" or "I am worried about threats from a former partner or housemate" could automate access to this guidance.

Across this section, we have shown that threat modeling does not need to be complex to be useful. Indeed, our suggested set of mitigations emphasize how such an approach can be both practical and feasible. More research[11] is undoubtedly needed to define, test, and improve our privacy and security propositions – not only to evaluate their effectiveness but to identify further technical response means. Nonetheless, based on the current state of knowledge, we are confident that the above-mentioned design choices could mitigate harms stemming from IPV compromises and further benefit the "average" IoT users whose level of privacy and security is enhanced by these measures.

Validation: Did You Do a Decent Job of Analysis?

Our analysis is by no means flawless. We are conscious of the limitations that underpin our "IPV Threat Model" and the restrictions that derive from our reliance on a single, hypothetic test case (i.e., smart lock). Instead of checking our model for its completeness and accuracy, we consequently hope to have showcased how design features in the context of IoT systems can shape and embed power dynamics and stimulated a discussion which may lead to changes in industrial practices.

To achieve this, future IPV threat modeling exercises must be able to move away from speculative scenarios and involve assumptions and conjectures that are based on facts and quantitative evidence. Our current threat model was built on several qualitative tech abuse studies which compiled the experiences of victims/survivors and support organizations (Dragiewicz et al., 2018; Freed et al., 2018, 2017; Harris & Woodlock, 2019; Leitão, 2018; Lopez-Neira et al., 2019; Parkin et al., 2019; Slupska, 2019). Testimonies of victims/survivors are a critical way to validate a model. This can be done by checking that the model and analysis produced a set of threats that includes what is in the literature, as well as other sources of victim/survivor testimony.

However, it would make for a more robust model, if future threats and attack vectors could be derived from detailed statistical data gathered by statutory and voluntary support organizations, academia, and industry stakeholders. The reliance on multiple data sources will also mitigate potential biases that derive from various forms of victims/survivors under- or non-reporting abuse (Fernández-Fontelo, Cabaña, Joe, Puig, & Moriña, 2019). As scholars such as Tanczer et al. (2018) have highlighted, once more detailed accounts of the frequency, extent, regional specificities, and nature of tech abuse cases have been collated, more targeted mitigations strategies can be developed. The active use of such data will also imply a need to shift away from the "design before attack" paradigm. Thus, the tech sector will have to become comfortable and able to amend and redesign systems after their deployment. In the long run, this will profit not only IPV victims/survivors but also the conventional users who gain from the security and privacy improvements that can be designed and implemented.

Conclusion

This chapter showcased *how* and *why* tech abuse is a socio-technological issue and requires both societal and technical mitigation strategies to tackle the risks and harms that derive from the burgeoning IoT environment. Based on previous qualitative studies, we provided the first exploration of a dedicated IPV tech abuse threat model. The latter describes a systematic approach for identifying threats and improving the security design of technical systems. We tested our model's applicability on the hypothetical case study of a smart lock. The exemplary scenario offered us with a means to demonstrate the difficulty of proposing mitigation strategies, due to certain design choices which may benefit IPV victims/survivors and perpetrators.

We vividly illustrated why IPV research needs to engage with the development of digital devices and keep a tab on emerging technologies such as IoT. While we are hopeful that our framework will probe future research as much as engagements between research, industry, and practice, we are mindful of the limitations of cybersecurity models originally developed for military or business purposes. Despite these concerns, we argue that drawing on established cybersecurity concepts will prove useful. Once these concepts and terminologies are made accessible to the IPV sector and refined to account for victims'/survivors' concerns and needs, they will offer IPV researchers and practitioners a language to advocate for design changes and critique current industry practices.

Our analysis delivers a steppingstone for further cybersecurity-centric evaluations and tackles the potential misuse of technologies from "within." Having outlined a clear set of shortcomings in the existing responses to the problem of tech abuse, our dedicated IPV threat model may guide future technology design, especially among IoT vendors. While we alert readers to the risk of both the over- and underestimation of threats and harms deriving from IoT (Tanczer, 2019), we are optimistic that well-assessed mitigation strategies can slow down the possibility of tech abuse occurring.

Future research may, therefore, draw on our framework and begin to quantitatively assess the frequency, extent, regional specificities, and nature of tech abuse to refine prospective IPV threat models. We are also pointing interested parties to ongoing policy developments such as the UK's IoT Code of Practice (Department for Digital, Culture, Media and Sport, 2018) and the EU's Cybersecurity Act (2019). These advancements can expedite security and privacy improvements in the context of smart technologies, together with other proposals such as the establishment of dedicated IPV cybersecurity clinics (Havron et al., 2019), bodies such as the Australian eSafety Commissioner, and IPV-specific Privacy-Enhancing Technologies (PETs) or Protective Optimization Technologies (POTs). Good reasons to move toward these ideas and pathways are evident. However, it will require incentives – may these be "carrots" and/or "sticks" – to push for further progress in this space.

Notes

1. The term "domestic violence" is used in many countries and organizations to refer to IPV. However, IPV can also include child or elder abuse or abuse by any member of a household, making it more encompassing (World Health Organisation, 2012).
2. The language used to describe people who experience intimate or domestic violence is contested. The commonly used term "victim" has come under criticism for being disempowering. However, the suggested alternative, "survivor" omits murdered victims. To account for both dynamics, this paper will use these terms interchangeably, noting that neither term is ideal or unproblematic.
3. Threat, harm, and risk are interrelated but distinct concepts. *Threat* refers to a person, event, or circumstance (i.e., perpetrator) that results in harm. Thus, *harm* describes the effect and result of the actions/inaction taken by a threat (i.e., perpetrator). *Risk* is a metric used to assess the impact (i.e., extent of harm) of a potential threat.
4. Multi-factor authentication describes processes used in computing to prevent the impersonation of an authorized account holder. Authentication is the process of positively verifying a user's identity by drawing on a piece of information specific to the account holder (e.g., biometrics, such as face recognition or a fingerprint, or a phone number to send a dedicated password to (Velásquez, Caro, & Rodríguez, 2018)).
5. An exception is one form of "sextortion," in which remote hackers extort victims/survivors by threatening to release intimate photos they acquired through hacking online accounts or webcams (Wittes, Poplin, Jurecic, & Spera, 2016).
6. The system is loosely based on the design of an August smart lock (Ye et al., 2017b). The company is an early leader in the smart lock market.
7. Smart door lock control mechanics using biometric solutions such as facial recognition rather than smartphone apps are underway (Krishna Chaithanya, Satish Kumar, & Ramasri, 2019).
8. Additional features such as audio control (i.e., lock/unlock the door via voice) will not be considered in this analysis, but are important to acknowledge in IPV scenarios.
9. For a comprehensive overview of the structure of attacks to the home ecosystem, consult Denning, Kohno, and Levy (2013).
10. We accept that security professionals have traditionally been skeptical of mechanisms which allow external change to account ownership, for fear of creating further vulnerabilities for a cyberattack. Indeed, in some scenarios, it may be challenging to establish a clear perpetrator/survivor division from a company perspective (e.g., in cases where both sides allege abusive behavior). Such situations problematically place companies in the position of arbitrators, which they do not have the experience nor authority to do. Therefore, companies will be (and should be) unwilling to remove ownership-based access easily. However, as IPV situations can and will arise in smart home environments, companies must prepare procedures on how they will manage individual's ownership transfers.
11. "Blue team-red team" exercises where security professionals take on the role of an adversary (i.e., IPV perpetrator) could help to further refine IPV threat models.

References

Anderson, N. (2013, March 11). Meet the men who spy on women through their webcams. *Ars Technica*. Retrieved from https://arstechnica.com/

Ashworth, B. (2018, July 28). The terrible anxiety of location sharing apps. *Wired*. Retrieved from https://www.wired.com/

Atzeni, A., Cameroni, C., Faily, S., Lyle, J., & Flechais, I. (2011). Here's Johnny: A methodology for developing attacker personas. In *Proceedings of the 2011 6th international conference on availability, reliability and security, ARES 2011* (pp. 722–727). Washington, DC: IEEE Computer Society. doi:10.1109/ARES.2011.115

Aufner, P. (2020). The IoT security gap: A look down into the valley between threat models and their implementation. *International Journal of Information Security*, *19*(1), 3–14. doi:10.1007/s10207-019-00445-y

Bagwell-Gray, M. E., Messing, J. T., & Baldwin-White, A. (2015). Intimate partner sexual violence: A review of terms, definitions, and prevalence. *Trauma, Violence, & Abuse*, *16*(3), 316–335. doi:10.1177/1524838014557290

Bishop, M., & Gates, C. (2008). Defining the insider threat. In *Proceedings of the 4th annual workshop on cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead*. Oak Ridge, TN: Association for Computing Machinery. doi:10.1145/1413140.1413158

Coles, M. J., & Tarandach, I. (2020). *Threat modeling*. O'Reilly Media. Retrieved from https://www.oreilly.com/library/view/threat-modeling/9781492056546/

Communications Alliance Ltd. (2018). G660:2018 assisting customers experiencing domestic and family violence industry guideline. [PDF file]. Retrieved from https://commsalliance.com.au/__data/assets/pdf_file/0003/61527/Communications-Guideline-G660-Assisting-Customers-Experiencing-Domestic-and-Family-Violence.pdf

de Lucena, K. D. T., de Souza Chaves Deininger, L., Coelho, H. F. C., Monteiro, A. C. C., de Toledo Vianna, R. P., & do Nascimento, J. A. (2016). Analysis of the cycle of domestic violence against women. *Journal of Human Growth and Development*, *26*(2), 139–146. doi:10.7322/jhgd.119238

Denning, T., Kohno, T., & Levy, H. M. (2013). Computer security and the modern home. *Communications of the ACM*, *56*(1), 94–103. doi:10.1145/2398356.2398377

Department for Digital, Culture, Media and Sport. (2018). Code of practice for consumer IoT security. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747413/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, *18*(4), 609–625. doi:10.1080/14680777.2018.1447341

Fernandes, E., Jung, J., & Prakash, A. (2016). Security analysis of emerging smart home applications. In *2016 IEEE symposium on security and privacy (SP)*, San Jose, CA (pp. 636–654). doi:10.1109/SP.2016.44

Fernández-Fontelo, A., Cabaña, A., Joe, H., Puig, P., & Moriña, D. (2019). Untangling serially dependent underreported count data for gender-based violence. *Statistics in Medicine*, *38*(22), 4404–4422. doi:10.1002/sim.8306

Freed, D., Palmer, J., Minchala, D. E., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital technologies and intimate partner violence: A qualitative analysis with

multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction*, *1*(CSCW), 1–22. doi:10.1145/3134681

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A Stalker's Paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, 667, 1–13. doi:10.1145/3173574.3174241

Hadis, M. S., Palantei, E., Ilham, A. A., & Hendra, A. (2018). Design of smart lock system for doors with special features using bluetooth technology. In *2018 international conference on information and communications technology (ICOIACT)*, Yogyakarta (pp. 396–400). doi:10.1109/ICOIACT.2018.8350767

Harris, B. A., & Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. *British Journal of Criminology*, *59*, 530–550. doi:10.1093/bjc/azy052

Havron, S., Freed, D., Chatterjee, R., McCoy, D., Dell, N., & Ristenpart, T. (2019). Clinical computer security for victims of intimate partner violence. In *28th USENIX security symposium*, Santa Clara, CA (pp. 105–122).

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016). Smart locks: Lessons for securing commodity Internet of things devices. In *Proceedings of the 11th ACM on Asia conference on computer and communications security, ASIA CCS 2016*, Xi'an (pp. 461–472). doi:10.1145/2897845.2897886

Katerndahl, D. A., Burge, S. K., Ferrer, R. L., Becho, J., & Wood, R. (2010). Complex dynamics in intimate partner violence: A time series study of 16 women. *Primary Care Companion to The Journal of Clinical Psychiatry*, *12*(4). doi:10.4088/PCC.09m00859whi. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2983457/

Kennedy, J., Nansen, B., Arnold, M., Wilken, R., & Gibbs, M. (2015). Digital housekeepers and domestic expertise in the networked home. *Convergence*, *21*(4), 408–422. doi:10.1177/1354856515579848

Khalid, M., & Majeed, S. (2016). A smart visitors' notification system with automatic secure door lock using mobile communication technology. *International Journal of Computer Science and Information Security*, *16*(4), 97–101.

Krishna Chaithanya, J., Satish Kumar, G. A. E., & Ramasri, T. (2019). IoT-based embedded smart lock control using face recognition system. In D. Pandian, X. Fernando, Z. Baig, & F. Shi (Eds.), *Proceedings of the international conference on ISMAC in computational vision and bio-engineering 2018 (ISMAC-CVB)* (pp. 1089–1098). Cham: Springer International Publishing. doi:10.1007/978-3-030-00665-5_104

Leitão, R. (2018). Digital technologies and their role in intimate partner violence. In *Extended abstracts of the 2018 CHI conference on human factors in computing systems, SRC11:1–SRC11:6*, New York, NY. doi:10.1145/3170427.3180305

Leitão, R. (2019). Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *ACM conference on designing interactive systems* (pp. 527–539).

Levy, K. E. C. (2015). Intimate surveillance. *Idaho Law Review*, *51*, 679–693. doi:10.3868/s050-004-015-0003-8

Levy, K., & Schneier, B. (2020). Privacy threats in intimate relationships. *Journal of Cybersecurity*, *6*(1). Retrieved from https://academic.oup.com/cybersecurity/article/6/1/tyaa006/5849222

Little, E. G., & Rogova, G. L. (2006). An ontological analysis of threat and vulnerability. In *Proceedings of the 9th international conference on information fusion*, Buffalo (pp. 1–8). doi:10.1109/ICIF.2006.301716

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. M. (2019). 'Internet of Things': How abuse is getting smarter. *Safe – The Domestic Abuse Quarterly*, *63*, 22–26.

Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J. P., Shelton, M., … Consolvo, S. (2017). Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI conference on human factors in computing systems*, New York, NY (pp. 2189–2201). doi:10.1145/3025453.3025875

Meier, J. D., Mackman, A., Vasireddy, S., Dunner, M., Escamilla, R., & Murukan, A. (2003). *Improving web application security: Threats and countermeasures* (pp. 1–919). Microsoft Corporation. Retrieved from https://www.microsoft.com/en-gb/download/confirmation.aspx?id=1330

Myers, B. A. (1989). User-interface tools: Introduction and survey. *IEEE Software*, *6*(1), 15–23. doi:10.1109/52.16898

Nicholls, T. L., Pritchard, M. M., Reeves, K. A., & Hilterman, E. (2013). Risk assessment in intimate partner violence: A systematic review of contemporary approaches. *Partner Abuse*, *4*(1), 76–168. doi:10.1891/1946-6560.4.1.76

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. In *Proceedings - IEEE symposium on security and privacy*. doi:10.1109/SPW.2014.38

Nurse, J. R. C., Creese, S., & Roure, D. D. (2017). Security risk assessment in Internet of things systems. *IT Professional*, *19*(5), 20–26. doi:10.1109/MITP.2017.3680959

Nye, J. S., Jr (2018). How will new cybersecurity norms develop?. *Project Syndicate*. Retrieved from https://www.project-syndicate.org/commentary/origin-of-new-cybersecurity-norms-by-joseph-s–nye-2018-03

Office for National Statistics. (2019, November 25). Domestic abuse in England and wales overview: November 2019 [Ons.gov.uk]. *ONS*. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/domesticabuseinenglandandwales/yearendingmarch2018

Omotosho, A., Haruna, B. A., & Olaniyi, O. M. (2019). Threat modeling of internet of things health devices. *Journal of Applied Security Research*, *14*(1), 106–121. doi:10.1080/19361610.2019.1545278

Online and Digital Abuse. (2018). Women's aid. Retrieved from https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/

Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. M. (2019). Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. In M. Carvalho, W. Pieters, & E. Stobert (Eds.), *Proceedings of the new security paradigms workshop* (pp. 1–15). New York, NY: Association for Computing Machinery (ACM). doi:10.1145/3368860.3368861

Pavelić, M., Lončarić, Z., Vuković, M., & Kušek, M. (2018). Internet of things cyber security: Smart door lock system. In *2018 international conference on smart systems and technologies (SST)* (pp. 227–232). doi:10.1109/SST.2018.8564647

Poster, W. R. (2018). Cybersecurity needs women. *Nature*, *555*, 577–580. doi:10.1038/d41586-018-03327-w

PRNewswire. (2019, May 8). Smart locks market to be worth US$1.01 Bn by 2024. *Bloomberg*. Retrieved from https://www.bloomberg.com/press-releases/2019-05-08/smart-locks-market-to-be-worth-us-1-01-bn-by-2024-growing-use-of-cloud-based-services-augmented-demand-globally-tmr

van der Put, C. E., Gubbels, J., & Assink, M. (2019). Predicting domestic violence: A meta-analysis on the predictive validity of risk assessment tools. *Aggression and Violent Behavior*, *47*, 100–116. doi:10.1016/j.avb.2019.03.008

Refuge. (2020, January 9). 72% of Refuge service users identify experiencing tech abuse. *Refuge Charity - Domestic Violence Help*. Retrieved from https://www.refuge.org.uk/72-of-refuge-service-users-identify-experiencing-tech-abuse/

Riebe, T., & Reuter, C. (2019). Dual-use and dilemmas for cybersecurity, peace and technology assessment. In C. Reuter (Eds), *Information technology for peace and security*. Wiesbaden: Springer Vieweg. doi:10.1007/978-3-658-25652-4_8

Sabbagh, B. A., & Kowalski, S. (2015). A socio-technical framework for threat modeling a software supply chain. *IEEE Security Privacy*, *13*(4), 30–39. doi:10.1109/MSP.2015.72

Sambasivan, N., Consolvo, S., Batool, A., Ahmed, N., Matthews, T., Thomas, K., … Churchill, E. (2019). 'They Don't Leave Us Alone Anywhere We Go': Gender and digital abuse in South Asia. In *Proceedings of the 2019 CHI conference on human factors in computing systems - CHI '19*. doi:10.1145/3290605.3300232

Seeam, A., Ogbeh, O. S., Guness, S., & Bellekens, X. (2019). Threat modeling and security issues for the Internet of things. In *2019 conference on next generation computing applications (NextComp)*, (pp. 1–8). doi:10.1109/NEXTCOMP.2019.8883642

Shostack, A. (2014). *Threat modeling: Designing for security*. Wiley. Retrieved from https://www.wiley.com/en-us/Threat+Modeling%3A+Designing+for+Security-p-9781118809990

Slupska, J. (2019). Safe at home: Towards a feminist critique of cybersecurity. *St. Anthony's St Antony's International Review, Whose Security is Cybersecurity? Authority, Responsibility and Power in Cyberspace*, *15*, 83–100.

Steven, J. (2010). Threat modeling—perhaps it's time. *IEEE Security Privacy*, *8*(3), 83–86. doi:10.1109/MSP.2010.110

Strengers, Y., Kennedy, J., Arcari, P., Nicholls, L., & Gregg, M. (2019). Protection, productivity and pleasure in the smart home emerging expectations and gendered insights from Australian early adopters. In A. Cox, & V. Kostakos (Eds.), *Proceedings of the 2019 CHI conference on human factors in computing systems* (pp. 1–13). New York, NY: Association for Computing Machinery (ACM). doi:10.1145/3290605.3300875

Tanczer, L. M. (2019, October 21). Webinar: "Gender and IoT": The implications of smart technologies on victims and survivors of domestic and sexual violence and abuse. *Internet Society UK*. Retrieved from https://isoc-e.org/webinar-gender-and-iot/

Tanczer, L. M., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (2019). The United Kingdom's emerging internet of things (IoT) policy landscape. In R. Ellis & V. Mohan (Eds.), *Rewired: Cybersecurity governance* (pp. 37–56). Hoboken, NJ: Wiley.

Tanczer, L. M., Lopez-Neira, I., Patel, T., Parkin, S., & Danezis, G. (2018). *Gender and IoT (G-IoT) policy leaflet: Tech abuse – smart, internet-connected devices present new risks for victims of domestic violence & abuse*. London: University College London. Retrieved from https://www.ucl.ac.uk/steapp/sites/steapp/files/giot_policy.pdf

Tanczer, L., Neira, I. L., Parkin, S., Patel, T., & Danezis, G. (2018). Gender and IoT research report technology-facilitated abuse. November.

Tanczer, L. M., Patel, T., Parkin, S., & Danezis, G. (2018). *Gender and IoT (G-IoT) Tech Abuse Guide: How internet-connected devices can affect victims of gender-based domestic and sexual violence and abuse*. London: University College London. Retrieved from https://www.ucl.ac.uk/steapp/research/projects/digital-policy-lab/gender-iot-tech-abuse

Tanczer, L. M., Patel, T., Parkin, S., & Danezis, G. (2019). *Gender and IoT (G-IoT) resource list: How internet-connected devices can affect victims of gender-based domestic and sexual violence and abuse*. London: University College London. Retrieved from https://www.ucl.ac.uk/steapp/research/projects/digital-policy-lab/g-iot-resource-list

Tech UK. (2019). The state of the connected home. Retrieved from http://www.techuk.org/images/assets/Connected_Home/The_State_of_the_Connected_Home_Edition3_Jun19.pdf

Think Social Tech, Snook, & SafeLives. (2019). *Tech vs abuse: Research findings 2019* (pp. 1–39). Comic Relief, The Clothworkers' Foundation, and Esmée Fairbairn Foundation.

Torr, P. (2005). Demystifying the threat modeling process. *IEEE Security Privacy*, *3*(5), 66–70. doi:10.1109/MSP.2005.119

UcedaVelez, T., & Morana, M. M. (2015). *Risk centric threat modeling: Process for attack simulation and threat analysis*. Wiley-Blackwell. Retrieved from https://www.wiley.com/en-gb/Risk+Centric+Threat+Modeling%3A+Process+for+Attack+Simulation+and+Threat+Analysis-p-9780470500965

Ur, B., Jung, J., & Schechter, S. (2013). The current state of access control for smart devices in homes. *Workshop on Home Usable Privacy and Security (HUPS)*, *29*, 209–218.

Uzunov, A. V., & Fernandez, E. B. (2014). An extensible pattern-based library and taxonomy of security threats for distributed systems. *Computer Standards & Interfaces*, *36*(4), 734–747. doi:10.1016/j.csi.2013.12.008

Velásquez, I., Caro, A., & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. *Information and Software Technology*, *94*, 30–37. doi:10.1016/j.infsof.2017.09.012

Weinert, A., Mayfield, P., Costica, Y., O'Donovan, S., Gulati, G., Radhakrishnan, D., … Esibov, A. (2019). *Traditional perimeter-based network defense is obsolete—Transform to a Zero Trust model*. Retrieved from https://www.microsoft.com/security/blog/2019/10/23/perimeter-based-network-defense-transform-zero-trust-model/

Wittes, B., Poplin, C., Jurecic, Q., & Spera, C. (2016). Sextortion: Cybersecurity, teenagers, and remote sexual assault. *Centre for Technology Innovation*. Retrieved from https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/

Women's Aid. (2018). Online and digital abuse. *Women's Aid*. Retrieved from https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/

World Health Organisation. (2012). Understanding and addressing violence against women (WHO/RHR/12.36; pp. 1–12). WHO. Retrieved from https://apps.who.int/iris/bitstream/handle/10665/77432/WHO_RHR_12.36_eng.pdf;jsessionid=A70EC48CFB8D012BCFAC29B6ED559A4B?sequence=1

World Health Organisation. (2017, November 29). *Violence against women: Key facts*. WHO. Retrieved from https://www.who.int/news-room/fact-sheets/detail/violence-against-women

Xiong, W., & Lagerström, R. (2019). Threat modeling – a systematic literature review. *Computers and Security*, *84*, 53–69. doi:10.1016/j.cose.2019.03.010

Ye, M., Jiang, N., Yang, H., & Yan, Q. (2017a). Security analysis of internet-of-things: A case study of august smart lock. In *2017 IEEE conference on computer communications workshops, INFOCOM WKSHPS 2017*. doi:10.1109/INFCOMW.2017.8116427

Ye, M., Jiang, N., Yang, H., & Yan, Q. (2017b). Security analysis of internet-of-things: A case study of august smart lock. In *2017 IEEE conference on computer communications workshops (INFOCOM WKSHPS)* (pp. 499–504). doi:10.1109/INFCOMW.2017.8116427