Mitigations for the Prevention of the Reporting of Abuse of People with Intellectual or Developmental Disorders

A Major Qualifying Project

Submitted to the Faculty of

Worcester Polytechnic Institute

in partial fulfillment of the requirements for the

Degree in Bachelor of Science

in

Computer Science

By

Zachary Vaughan

Date: 03/06/2019

Project Advisor: Professor Krishna Venkatasubramanian

Acknowledgments

I would like to wholeheartedly thank Professor Jeanine Skorinko, Natalia Carvajal Erker, Jeffrey Harnois, Alisionna Iannacchione, Nicole Jutras, Marian Kobeissi, Rachel Smallcomb, and Danielle Warren for acting as excellent sounding boards throughout this project and for providing and teasing out many of the ideas in this paper.

Abstract

People with intellectual or developmental disabilities face abuse at much higher rates than people without disabilities. Although reporting abuse is possible, abusers have many options on hand if they want to use technology to prevent this reporting. This paper details and structures these tactics. It also describes mitigations that a victim of abuse may use to prevent or diminish the effects of an abusers' tactics.

Table of Contents

Table of Figures

Table of Tables

1. Introduction

Historically, intellectual and developmental disabilities (IDD) have been defined negatively. That is, they have been defined by what a person with these disabilities cannot do that a person without disabilities would be able to do. This is a tempting but untenable definition, as it posits a universal idea of Human by which particular humans are to be compared and thus categorized. In response to this negative definition, a positive definition arose, defining people with IDD by what societal supports (e.g., ramps leading into buildings for people with wheelchairs, state agencies that help with finding employment) they need to live fulfilled lives. This definition can still be too one-sided, however. I am following C. Frauenberger's [1] definition, attempting to skirt between the negative and positive definitions of IDD and taking both into account.

People living with IDD face much higher rates of abuse than populations without IDD on average. According to the Bureau of Justice Statistics, people with IDD are about 4.5 times as likely to be sexually abused in their life compared to people without disabilities [7]. According to K. McKenzie et al. [5], about 1% of the population of the US lives with IDD. Much infrastructure already exists for the purposes of handling reports of abuse. The Disabled Persons Protection Commission in Massachusetts provides education relating what abuse is and how to respond to it and also takes up reports of abuse and then works with police to investigate reports. Triangle, Inc., another Massachusetts-based organization, provides self-defense training for people with IDD for the purposes of protecting themselves against abuse. In addition, many people, because of their occupation, are required by law to report incidences of abuse they are told of. These people include doctors, nurses, psychologists, teachers, and social workers.

There is nonetheless much room for improving methods of reporting abuse, however. Specifically, current reporting resources can be difficult to tap into for a given person with IDD. Calling a phone number can be very difficult for some. Others may be too isolated to be able to speak with a mandated reporter. Others still may be pressured by their abuser into not reporting under threat of reprisals. One goal of this project is to lay the groundwork for exploring how technology can be used to significantly ease the process of reporting abuse among an IDD population. Alongside this paper, a group of students from Worcester Polytechnic Institute are working on the design of a phone app that can be used to educate about abuse and report abuse. Consideration is also being put in towards the possibility of making a website that fulfills the same purposes.

Going down this road raises further concerns. I anticipate that an abuser will not sit back idly in the event that reporting abuse becomes much easier. As a result, the main focus of this project becomes researching and then analyzing how an abuser may try to use technology to prevent the reporting of abuse. I have divided the tactics available to an abuser into four categories: creating a sense of omnipresence, isolating

the victim, humiliating or punishing the victim, and threatening the victim. I have also created a graph that shows the necessary conditions an abuser needs to fulfill to carry out the different attacks I have listed. In addition to this analysis of abuse tactics, I have determined strategies using technology that can be used to either defend against or mitigate the effects of an abuser's "counter-attacks." I have then detailed these mitigations and described how certain tactics cannot be abated by existing technologies. Before I explicitly address my results, however, I will go over the methodology I followed in completing this project. I will then briefly review scholarly work related to this paper. From then, I will detail abusers' reporting prevention tactics and the extant technological mitigations thereof.

2. Methodology

My goal in this paper was to study how abusers can prevent the victims of their abuse from reporting said abuse and then to formulate mitigations whereby a victim will be able to sidestep or prevent the abusers' preventative measures. To begin down this path, I needed to research ways that abusers can use technology to prevent the abused from reporting them. I read a series of papers detailing how technology is used in intimate partner violence (IPV). The large majority of victims of abuse detailed in the papers did not have IDD, although most of the abuse tactics described in them could easily be translated from an IPV context to one where a person with IDD is being abused. From these papers, as well as from discussions, I gathered together a large group of "attacks" someone could use to prevent a person with IDD from reporting abuse. In this paper, I will refer to these attacks as *tactics*. The tactics collated range from installing spyware on someone's phone to imitating them online to simply destroying the person's phone.

With this collection of tactics on hand, I set about arranging them in a structural fashion. Specifically, I organized them in a directed rooted tree. After several iterations of tree designs, I developed a list of counter-attacks and preventative measures, referred to in this paper as *mitigations*, to be deployed against the tactics in the tree. I then went on to categorize the mitigations and analyze them in the context of the tactics in the tree.

As a final point, it should be made clear that I have consciously aimed to focus on tactics and mitigations that involve technology. My purview is the realm of technology, and thus the mitigations I can offer will be technological. As technological solutions generally correspond to technological problems, I have restricted the tactics being analyzed to those involving technology.

3. Related Work

Research concerning how technology is used to abuse people with IDD is next to naught. However, a recent series of three papers on how technology is used in intimate partner violence (IPV) written by researchers based primarily out of Cornell Tech, Cornell University, and New York University proved to be immensely useful to this paper's realization.

R. Chatterjee et al. [6], in the first of these papers, detail how abusers can use spyware to track the phone activity of their partners. They focus both on how apps designed with benign purposes in mind, such as Find My iPhone, and apps designed specifically for spying can be used to perpetuate IPV. They use search engines and app store searches to see how prevalent phone spyware is and how easy it is to find it. Particularly concerning is their description of phones that can be purchased which have spyware preinstalled—spyware that has root access, allowing an abuser to remotely track any and all things done using that phone. They then go on to study the effectiveness of existing Android malware-detection software at detecting and removing spyware.

D. Freed et al. [2], in the second paper in the series, describe more generally how technology is used to perpetuate IPV, giving many examples and covering a large number of abuse techniques. The paper is notable for detailing how abusers represent a different security threat model from that of most cybersecurity situations: an attacker who is UI-bound yet has intimate knowledge of and often personal control over the victim of the attack. They also give suggestions for how software UI can be designed with preventing IPV in mind.

In another paper, the third in the series, D. Freed et al. [3] further build on the previous paper. They provide more examples of how technology is used in IPV, explore how case workers may be able to act effectively when a client is being abused using technology, and study how existing law intersects with the subject. They also give further recommendations for UI design.

Aside from these three papers, D. Woodlock [4] explores how technology can facilitate stalking by intimate partners or ex-partners. Most importantly, it classifies technology-based stalking tactics into a model used, in slightly modified form, by this paper. Woodlock classifies these tactics into ones which create a sense of omnipresence, ones which isolate the victim of abuse, and ones meant to humiliate or punish the victim.

4. Tactics

From an abuser's standpoint, allowing the victim of their abuse to report their abuse would be, to say the least, a compromising situation. Abusers have a strong interest in keeping their victims from reporting them. Luckily for them and unluckily for us, they have many possible routes to go down if they want to keep knowledge of their abuse from getting out. In this section, I detail a large number of tactics that an abuser could use to keep the reporting of abuse from happening. I have organized these tactics in a directed rooted tree.

In this tree, the root node (i.e., the ultimate goal of an abuser) is the prevention of their abuse being reported. The tree is laid out so that an arrow between two nodes represents a conditional relation. The node doing the pointing acts as a condition for the possibility of the node being pointed at. Arrows that have no slashes through them represent sufficient but not necessary conditions. Arrows with two slashes through them represent necessary but not sufficient conditions. Thus, one or many of the four nodes pointing towards the root node (preventing reporting) can be used to fulfill it.

There are four main categories of tactics I have identified that can be used to prevent reporting. These are the creation of a sense of omnipresence, the isolation of a victim, the humiliation or punishment of a victim, and the threatening of a victim. In what follows, I will outline the four categories of tactics. More detail on them can be found in Appendix x.

Figure 1: Creating a sense of omnipresence

From an abuser's standpoint, creating a sense of omnipresence keeps a victim of abuse from reporting because, if the tactic is carried out successfully, the victim will feel as though the abuser could be watching them at any time. The victim will have picked up on an implicit message from the abuser: "If you report me, I will know, and there will probably be negative consequences coming from me." To create a sense of omnipresence, an abuser can follow one of two paths.

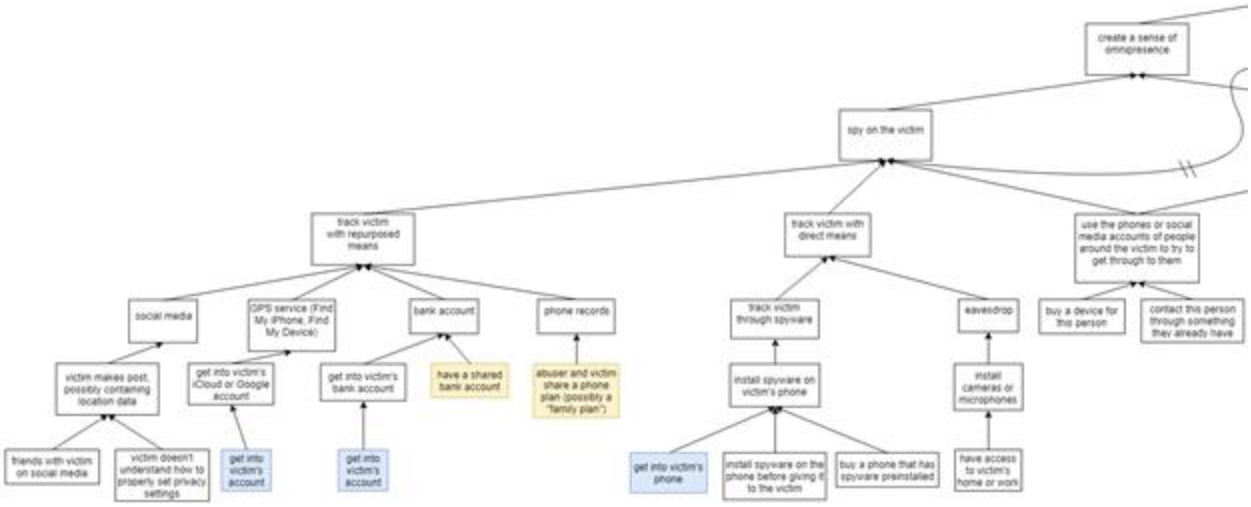

Figure 2: Spying on the Victim

For the first, the abuser must first gain more information about the victim than the victim wants the abuser to. An abuser may decide to repurpose mechanisms designed for benign purposes (e.g. they may look on Facebook or use GPS services like Find My iPhone to see where the victim is going or look at phone records to see who the victim is calling). They may also use mechanisms specifically designed for spying, such as spyware or bug microphones. The abuser can also gather information about the victim by contacting people near the victim. Post-espionage, the abuser must communicate to the victim, either explicitly or implicitly, that they have gathered this information. If an abuser spies on their victim but never does anything that would tip off the victim to the spying, the spying becomes ineffectual in relation to the goal of preventing the victim from reporting. In order to communicate information to the victim, an abuser can contact them directly (such as over social media, email, or SMS), can get other people to contact them (proxy harassment), or can contact people around the victim such as friends or caretakers. The effectiveness of this tactic is amplified to the degree that the victim perceives the abuser as a threat—that they believe the abuser will carry out reprisals for actions perceived as missteps or slights.

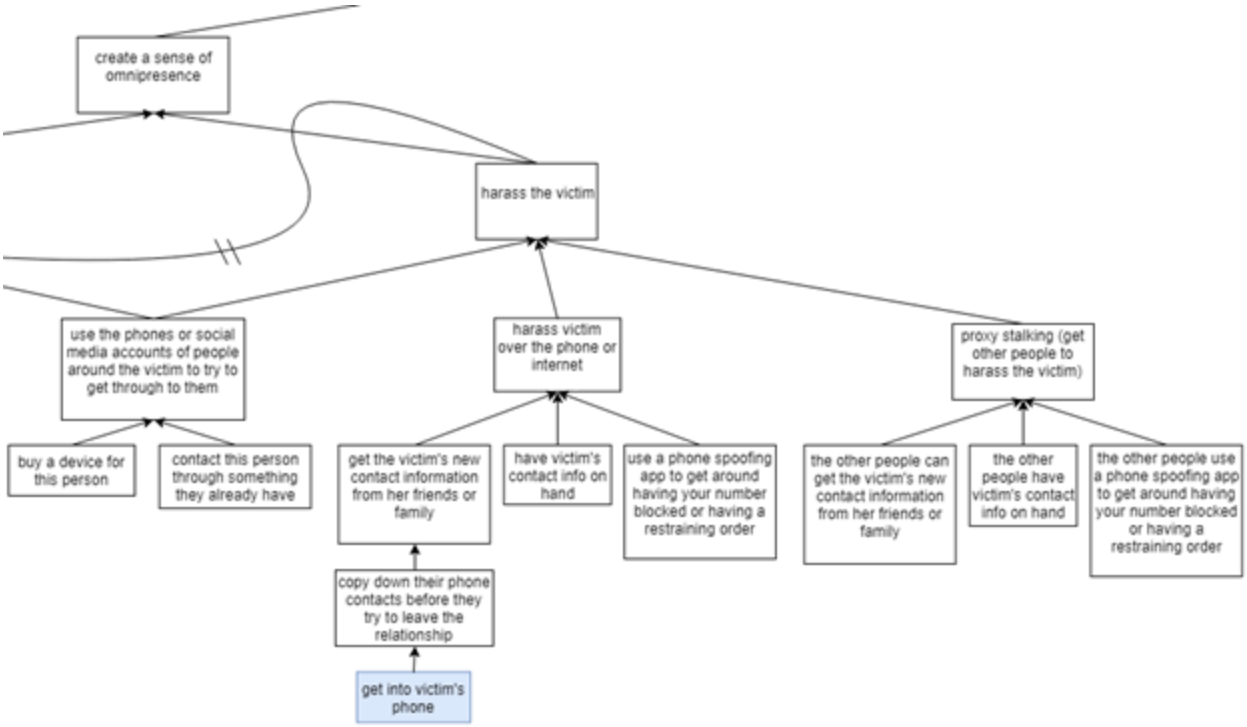

Figure 3: Harassing the Victim

The second route only requires that the abuser contacts the victim in a fear-instilling manner, whether this contact be quantitatively significant (e.g., sending hundreds of texts a day), qualitatively significant (e.g., saying frightening things in texts), or both. The effect of this tactic is to keep the abuser on the victim's mind. The victim, in the middle of considering reporting, may suddenly think of the abuser and then think "What if they found out? What would happen then?"

Figure 4: Isolating the Victim

The second group of tactics used to prevent a victim of abuse from reporting involves isolating the victim. The goal of isolating the victim is to deprive them of all social contacts that they could use to better their situation. This can be carried out either through wearing down the victim's relationships with friends, family members, coworkers, or acquaintances or by cutting off media of communication that the victim could use to ask for help. These tactics greatly lessen a victim's ability to report, as reporting requires contact with the outside world. They also lessen the chance that a victim of abuse will come across fortuitous social interactions that lead to reporting. That is to say, even if a victim of abuse has gone into a conversation without the thought of reporting abuse on their mind, the conversation could end up steering them towards reporting resources. With a lessened ability to communicate with people, situations such as this become much less likely to happen.

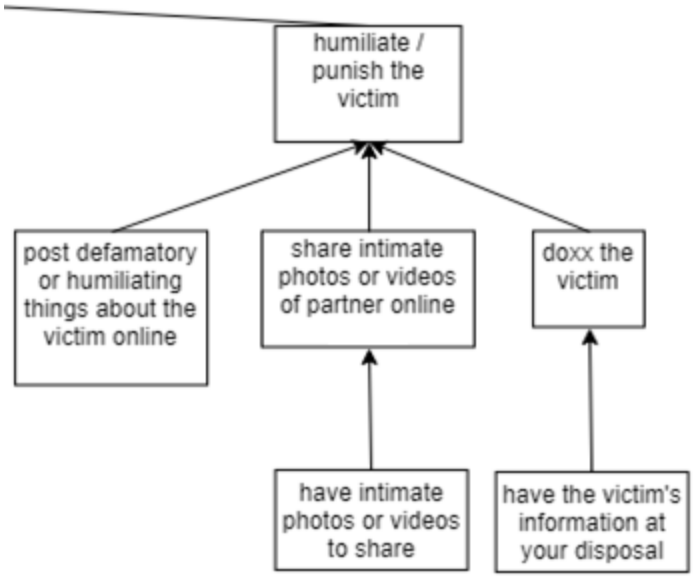

Figure 5: Humiliating / punishing the victim

The third category contains those tactics where an abuser attempts to humiliate or punish the victim. The tactics in this category may be carried out as revenge for perceived missteps carried out by the victim. An abuser could post defamatory or embarrassing things about the victim online, could share intimate photos or videos of the victim, or could leak sensitive personal information such as the victim's address or social security number. Tactics such as these prevent reporting because they can instill a feeling of powerlessness in a victim of abuse. They diminish the victim's autonomy and can take an emotional toll. In a situation where a victim of abuse has reported abuse in the past but where this reporting didn't end the abuse, the abuser may have used tactics in this category as a form of revenge. The victim in this situation may feel discouraged to the utmost; they may feel that if they try to report again, the same situation will replay itself.

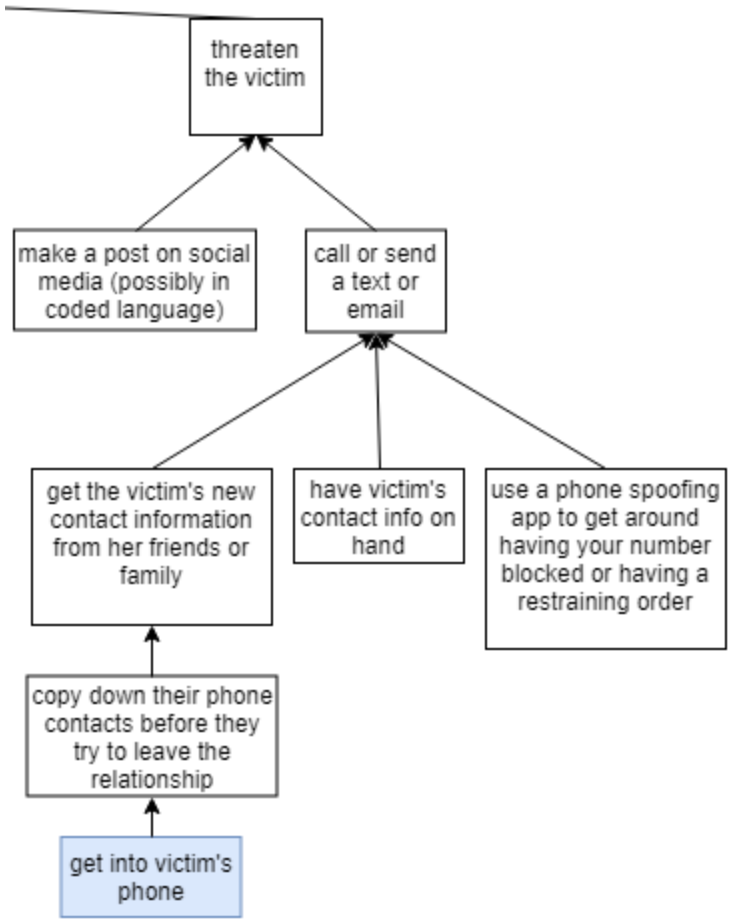

Figure 6: Threatening the victim

The fourth category involves threatening the victim. This category differentiates itself from the harassing section of the first category by its explicitness. Whereas in harassing the victim, a threat can be implied, in this category it is made explicit. This category is notable in that any other tactic detailed above in this paper can be threatened to be carried out. An abuser may threaten to install spyware on the victim's phone, lock the victim out of their social media accounts, or release compromising information about the victim, for a few examples.

5. Mitigations

Although any given abuser will have many potential tactics at their disposal to prevent their victim from reporting abuse, most of these can be countered or hampered by means employed by the victim. I refer to these means as mitigations. In this section, I detail mitigation strategies that can be used to prevent or reduce the harmful effects of the abuse tactics described in the above section. I have constrained myself to only describing mitigations which necessarily involve technology. I have also kept myself to technologies which already exist. These restrictions leave gaps behind—certain abuse tactics remain without relevant mitigations. Hopefully in the future, more research will be done on both mitigations that do not involve technology and on the potential creation of bespoke technologies for the purposes of mitigation.

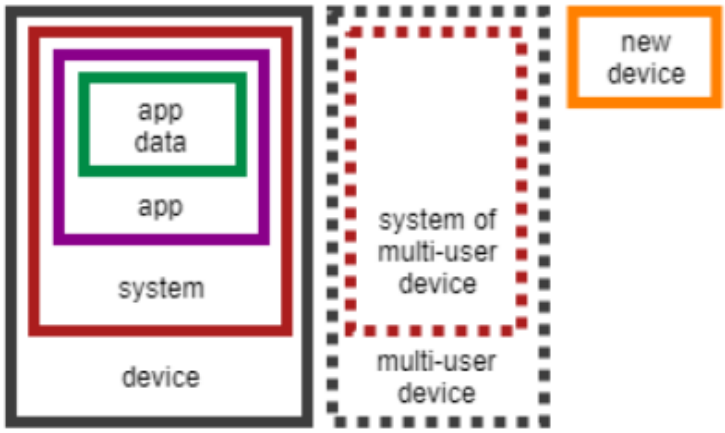

Figure 7: Mitigation categories

I have classified the mitigations detailed below into five categories (as seen in Figure 7). The first four categories derive from different layers of functionality in a device such as a phone or a computer. The outermost layer is that of the device itself. This category is relevant to mitigations involving the most basic functionality of a device, such as the setting or changing of a password. The next layer is that of the operating system of the device. Mitigations in this category involve things like altering app permissions or installing new software. The next layer is the app layer. It has to do with the functionality of applications on the device. Mitigations in this category include things like making a new Facebook account, setting up two-factor authentication for email login, and blocking someone's phone number. It should be noted that for the purposes of this paper I am including phone apps, computer software, and websites in the category of applications. For example, a Facebook application on a phone or computer and facebook.com as visited on a web browser are both being considered applications. The innermost layer is that of data created by or using apps. This layer is relevant where backing up data serves as a mitigation to an abuse tactic. I have also

distinguished secondary categories for cases where a mitigation only applies to multi-user devices such as computers, as opposed to phones. The fifth category involves getting a new device. Using these categories, I have grouped myriad mitigations in Table 1 below. In Table 1, mitigations, presented from the point of view of a given victim, are grouped with the tactics, presented from the point of view of a given abuser, that they are meant to counter.

Mitigation Category	**Mitigation**	**Relevant Tactics**
Device	Setting a new, strong password	Breaking into one of the victim's devices or accounts by having the password or because it has no password
System	Disabling GPS permissions	Tracking the victim's movements using GPS software or spyware
	Installing malware detection software	Tracking the victim's actions using spyware
System of Multi-User Device	Installing two-factor authentication software for computer login	Breaking into the victim's computer
App	Blocking the abuser on social media	Tracking the victim's actions through their posts on social media, harassing the victim over social media, getting other people to harass the victim over social media, threatening the victim over social media
	Increasing privacy settings on social media	Tracking the victim's actions through their posts on social media, harassing the victim over social media, getting other people to harass the victim over social media, threatening the victim over social media
	Reporting the abuser on social media	Harassing the victim over social media, getting other people to harass the victim over social media, threatening the victim over social media
	Blocking the abuser's phone number	Harassing the victim over the phone, getting other people to harass the victim over the phone, threatening the victim over the phone
	Getting a new account or plan	Tracking the victim's actions through a shared bank account, tracking the victim's phone calls by looking at phone records, cancelling the victim's phone plan, turning off the victim's internet access
	Setting up two-factor authentication for account logins	Getting into the victim's accounts, locking the victim out of their accounts
App Data	Backing up data	Deleting things from the victim's phone, destroying the victim's phone, taking the victim's phone away
New Device	Getting a new phone	Destroying the victim's phone, taking the victim's phone away

Table 1. Mitigations

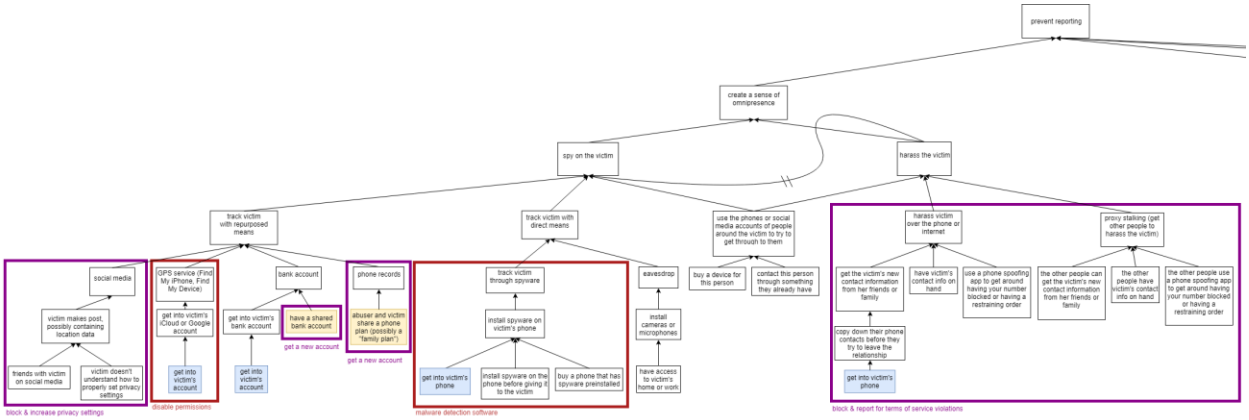

Figure 8: Tree of Tactics with Mitigations Overlaid Part 1

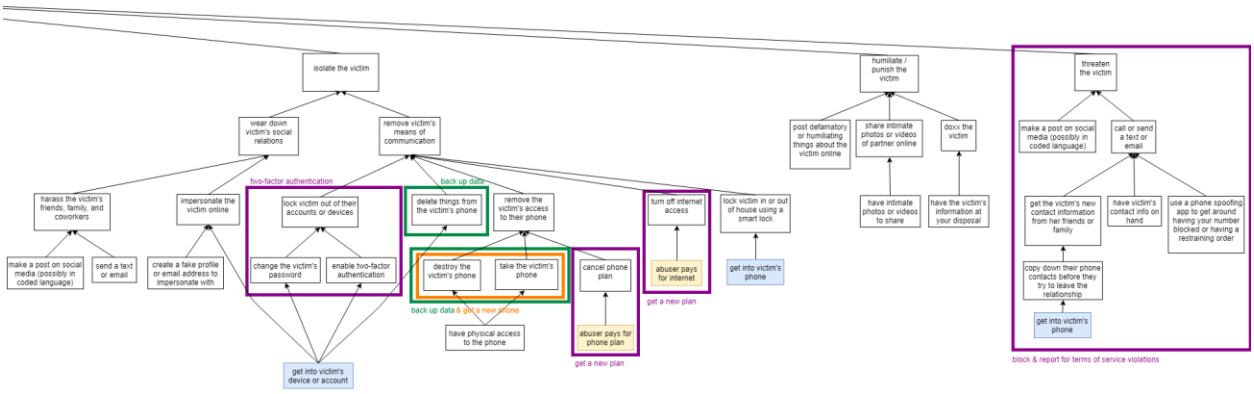

Figure 9: Tree of Tactics with Mitigations Overlaid Part 2

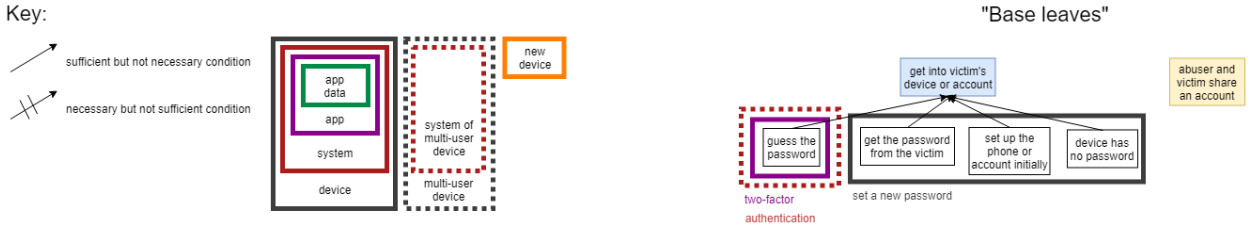

Figure 10: Tree Key and Base Leaves

Figures 8, 9, and 10 show how the mitigations in Table 1 can be applied to the tree detailed in Section 4. A box surrounding a section of the tree represents a mitigation against the tactics it surrounds. For example, as can be seen on the far left of

the tree, blocking the abuser and increasing privacy settings acts as a mitigation to an abuser tracking the victim through the posts they make on social media. A higher resolution version of the tree can be found at the following link: https://drive.google.com/open?id=1P1x61DdR6yY3tlBEgxunoh4rxzxI6wlO

Some gaps are left due to the decision to stick to solely mitigations that involve technology, as some abuse tactics can only be mitigated through non-technological means. What follows is an outline of the tactics that fall into this category.

Most tactics in this category cannot be tackled head-on using technology because, to use a grammatical analogy, the victim is involved only as an indirect object. In carrying out these attacks, the abuser interacts directly with a third party in order to indirectly affect the victim. The victim cannot do anything with their devices to mitigate these attacks, as their devices are not involved in the attacks. Examples of this sort of attack include the abuser contacting someone close to the victim to keep tabs on or harass the victim, harassing people close to the victim, impersonating the victim online to damage their reputation, and humiliating or punishing the victim over the internet.

Technology also cannot be used to protect the victim's device from being destroyed or stolen by the abuser if the abuser has physical access to it. It can only be used to dampen the harmful effects of an attack such as this by making sure the victim backs up important data before an attack such as this happens.

7. Conclusion

People with IDD face much higher rates of abuse than corresponding populations without IDD. Thus, making reporting abuse easy for people with IDD (in tandem with educating them about abuse) is a goal that feels very pressing. This paper is specifically concerned with how abusers can prevent the victims of their abuse from reporting said abuse. It is in an abusers' vested interest to not be reported, and so, if they suspect their victim will try and report abuse, they will most likely try to prevent that reporting. An abuser has a plethora of possible tactics for preventing reporting at their disposal, many of which use technology. These tactics have been divided into four categories in this paper: creating a sense of omnipresence, isolating the victim, humiliating or punishing the victim, and threatening the victim. Luckily, there are many options that a victim of abuse has at their disposal that they may be able to use to counter an abuser's tactics. Many of these involve relatively simple operations such as setting a password, installing malware-detection software, or blocking someone on a social media site. Not all tactics can be countered, prevented, or dampened using existing technologies, but most can. Most prominent of the tactics that cannot be prevented using existing technologies are tactics that only indirectly affect the victim. Hopefully, solutions will be devised in the near future to account for tactics that cannot be mitigated using existing technologies.

8. Future Work

Fully optimized ease of reporting is a goal that will in all likelihood take several generations to achieve, if ever. This paper is intended not only as valuable in its own right but also to be groundwork for future research.

For one, certain tactics could be better defended against with the help of bespoke technologies. A piece of software specifically designed to counter a given tactic will most likely end up being better at countering that tactic than a preexisting piece of software. For example, research into the creation of an Android or iPhone app designed to root out phone spyware may result in software that can much more reliably detect spyware than malware-detection apps currently available on app stores.

Second, research into education-based mitigations would be highly valuable. Certain tactics cannot be countered through technological means and so the solution becomes educating victims of abuse on how to respond to given tactics in the right way.

Third, research could be put into the development of a technology, such as a phone app or a website, that could serve as an easy medium of abuse reporting as well as an educational platform. With the findings of this paper in mind, this technology can be designed with an anticipation of an abusers' anti-reporting tactics in mind. It could also make sure to offer pertinent educational material.

9. References

[1] C. Frauenberger, "Disability and Technology: A Critical Realist Perspective," Institute for Design and Assessment of Technology, TU Wien, 2015, [Online]. Available: http://delivery.acm.org/10.1145/2810000/2809851/p89-frauenberger.pdf?ip=130.215.168.162&id=2809851&acc=ACTIVE%20SERVICE&key=7777116298C9657D%2E71E5F5E88B9A3E17%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1555381376_e31a9dbad79383a0de215c5bd8586ff5 [Accessed April 2019]

[2] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart & N. Dell, "'A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology," in *ACM Conference on Human Factors in Computing Systems*, CHI 2018, [Online]. Available: https://www.ipvtechresearch.org/pubs/stalkers-paradise-intimate.pdf [Accessed April 2019]

[3] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart & N. Dell, "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders," in *Proceedings of the ACM on Human-Computer Interaction: Volume 1 Issue CSCW*, November 2017, [Online]. Available: https://www.ipvtechresearch.org/pubs/a046-freed.pdf [Accessed April 2019]

[4] D. Woodlock, "The Abuse of Technology in Domestic Violence and Stalking," in *Violence Against Women: Volume 23, Issue 5*, 2017, [Online]. Available: https://journals.sagepub.com/doi/pdf/10.1177/1077801216646277 [Accessed April 2019]

[5] K. McKenzie, M. Milton, G. Smith & H. Ouellette-Kuntz, "Systematic Review of the Prevalence and Incidence of Intellectual Disabilities: Current Trends and Issues," in *Current Developmental Disorders Reports: Volume 3, Issue 2*, June 2016, [Online]. Available: https://link.springer.com/article/10.1007/s40474-016-0085-7 [Accessed April 2019]

[6] R. Chatterjee, P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy & T. Ristenpart, "The Spyware Used in Intimate Partner Violence," in *IEEE Symposium on Security and Privacy*, Oakland 2018, [Online]. Available: https://www.ipvtechresearch.org/pubs/spyware.pdf [Accessed April 2019]

[7] R. E. Morgan & J. L. Truman, "Criminal Victimization, 2017," Bureau of Justice Statistics, December 2018, [Online]. Available: https://www.bjs.gov/content/pub/pdf/cv17.pdf [Accessed April 2019]