Mobile Security Strategies and Usability Problems in IPV and Stalking Contexts

Andy Gallardo Hanseul Kim Kevin Kim Chanaradee Leelamanthep Tianying Li
Carnegie Mellon University

1 Introduction

Our study is motivated by the problem of technology enabled abuse faced by survivors of intimate partner violence (IPV), whose accounts & devices may be physically/remotely accessed by an abuser who may have knowledge about their personal details [11, 7, 3, 8]. The IPV tech abuse threat model is characterized by UI-bound adversaries, i.e. abusers limited by the functionality offered by a system's user interface (UI) [3]. Our research focuses on the usability of existing interfaces & strategies to counter unsophisticated threats, given the dire need for usable tools immediately accessible to IPV victims [9, 5, 6, 4].

We conducted semi-structured interviews with 9 participants regarding location tracking, account compromise, spyware apps, and rooting/jailbreaking. We sought to answer the following research questions: 1) *How familiar are participants with these security risks?* 2) *How aware are participants of methods to solve these security problems?* 3) *Can the participants successfully navigate interfaces to solve the problems?* 4) *How easy do participants find the process of solving the problems?* We found that while participants were somewhat familiar with these security risks & concepts, several (sometimes all) of them had difficulty resolving security problems in which these risks were simulated.

2 Methodology

2.1 Recruitment

We recruited participants through the Computer Gigs section of Craigslist for Pittsburgh & Los Angeles, and screened for the following criteria: at least 18 years old, located in the U.S., fluent in English, has access to a device that can connect to the internet to run Zoom, and uses an iPhone. Our survey included a general demographic section that was only used to assist in purposive sampling, to balance the demographics of the sample.

2.2 Interview

We conducted semi-structured 45-minute interviews with 9 participants. We asked them about mobile phone security and presented them with 4 hypothetical mobile security scenarios. To simulate the security scenarios, we used an iPhone (reformatted for this study) and remotely shared the phone screen with them. We projected the security threats onto a fictional persona, the participant's "friend" or "coworker", and asked them to guide us through their strategy to help their friend solve the security problems. Each participant received a $20 Amazon gift code. All study protocols were approved by our IRB.

Scenario 1. A hypothetical coworker believes their location is being tracked through their phone and asks for help determining whether someone is tracking their location and stopping the tracking. Via Google Maps' location sharing feature, our device's location was being shared with another Google account.

Scenario 2. A hypothetical friend thinks that their partner, who has their passcode, installed spyware on their phone and asks for help detecting and removing it. If the participant did not identify the app, we revealed to them that the friend's partner had downloaded TeamViewer, a dual-use app (i.e., it has legitimate use purposes but can be used as spyware) onto the phone, claiming it was antivirus software. If participants knew TeamViewer's capabilities, they might imagine the friend's partner using it to remotely access the friend's device.

Scenario 3. A hypothetical friend's photos are disappearing, and new photos that they did not take are appearing. Our device used an iCloud account that was logged into two different devices, and we expected participants to discover the unknown device syncing to the iCloud account.

Scenario 4. A hypothetical friend thinks they are being stalked and looks for advice from trusted sources. They found an advice from the Federal Trade Commission (FTC), and

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Vancouver, B.C., Canada.

wants to follow it, which recommends that potential stalking victims download a "root checker app" to detect whether their phone is rooted or jailbroken [2] (see Appendix A).

2.3 Data Analysis

We conducted a qualitative thematic analysis of the interviews by coding the interview transcripts, gathering keywords and ideas from the interviews, and finding common themes. Initially, three members of the team individually coded one interview using an a priori code list based on usability concepts, and open-coded for new codes. We then discussed the codes as a group and expanded them into a code book. After this, each interview transcript was coded individually by one researcher. We also tracked whether participants successfully identified a scenario's problem, as well as the hints we gave them per scenario.

3 Results

3.1 Location Tracking

Scenario results. Six of the participants were able to eventually find out that Google Maps was the source of the location sharing. All participants required at least one hint. Five out of nine participants struggled to find out which application had location service enabled. Four participants suggested turning off location services altogether from the Settings menu, and one participant suggested changing the location service option to "Never" for Google Maps. Completely turning off the location services on a device would potentially be an unusable solution for people who need location services to use device applications or features, so we added a clarification in our interview to note that the participant's "friend" needed to use Google Maps and could not entirely turn off location services.

Usability Problems. When we asked the participants to help find out whether someone was tracking their location, participants often went to the Privacy menu of the iOS Settings. Some mistakenly selected "Tracker" settings (which concern advertising), and others investigated the "Find My iPhone" feature in "Location Services," which could indeed be a source of location tracking. One participant had difficulty understanding the concept of location tracking and suggested an unrealistic advice,

> *Well, you can try and locate their iPhone if you have the number, to see where they are. I mean, if someone else is tracking you, you could turn around and track them. If they're close by you, you know, dial the number and their phone will ring and so you'll know that they are close by, you'll hear the ringing. (P4)*

This suggests that the participant did not understand that the location tracking can be done remotely, without the need to be physically present at the same location.

After finding out, via "Location Services," that the Google Maps was using location services, not all participants knew how to use this information to discover the account with which location was being shared or to stop location sharing.

> *It did take me a while to realize that I have to go directly into the Google Maps app, but after that it was pretty pretty easy. (P9)*

Only one participant suggested investigating Google Maps. For all other participants, we provided a hint to investigate the app. After looking at the app, participants P1, P6, and P9 had difficulty finding the source of location tracking, reporting that the process was difficult and too many steps were required, since there was no indicator on the Google Maps UI that the location of the device was being shared. Some participants had recommendations for better indicators:

> *I thought it [the source of the location sharing] should be like immediate indicator on screen to cut down the steps. (P6)*

> *I would actually prefer like a kind of like a glowing button, that is kind of like signifying that someone knows your location. (P8)*

The results suggest that the indicator of location sharing should be more immediate, apparent, and clear to notify users that their location is being shared with another account or individual.

Participants also had difficulty stopping location sharing. Participants P4 and P7 tried to stop sharing by starting a new share. It was not clear to one participant (P4) that the right arrow next to the current sharing contact's name would reveal the option to stop location sharing. Another participant also mentioned that the meaning of the interface icons was unclear:

> *I'm sure there's tutorials. But like everyone else, people don't pay attention to the tutorials. And they just kind of just randomly go in there and start pressing buttons until they get to where they need to be. So maybe it should be labeled better as to what is behind all those icons. (P1)*

3.2 Dual-Use Spyware App

Scenario results. Participants reviewed the apps on the phone (with and without our hint that the spyware app was downloaded from the AppStore) and looked for apps that could be spyware. Most participants were not sure how to identify a spyware app:

> *I honestly don't really know what to look for. I would assume probably it still has to do with location sharing.*

Others told us that they were looking for unusual, unfamiliar, or suspicious apps and sometimes described properties they assumed spyware apps might have.

I would say just apps with like weird foreign names like Russian letters Chinese letters or something. (P8)

I don't see any apps that say spyware. (P7)

Some participants considered TeamViewer to be suspicious and suggested deleting it:

I just thought, maybe a team is viewing your phone. (P4)

However, some participants also suggested deleting other apps with which they were unfamiliar or that had, in P5's view, suspicious permissions access, such as Zoom, which had microphone access.

Well, I don't know if I've helped my friend out or not. But if it was me, I would just delete all the apps in the whole wide world and start all over again. (P1)

Suspicion based on unfamiliarity may not be an efficient way to detect spyware, and, as we note in section 4.3, further research is needed on how participants would react to a device with several unfamiliar apps. Other participants noticed TeamViewer, but did not consider it to be spyware. Since it is a "dual-use" app, it may not always be malicious.

Well, I was able to find it ... but not really identify it. (P3)

No one expressed being familiar with the app, so they were likely unaware of its ability to remotly control the devices.

Usability Problems. While all participants found removing TeamViewer to be very easy, 7 of 9 participants considered finding the spyware app to be difficult. Some issues encountered were knowing what spyware is, deciding whether an app could be used as spyware, being able to know whether someone had access to the app or device remotely, and the possibility of hidden apps or software. P2 said, "I think I was confused generally [about] what spyware was." P6 said, "You'd have to like click it and then do research and figure it out yourself." For participants who did not suspect TeamViewer of being spyware, we informed them of TeamViewer's potential to be used as spyware since it allows remote control of the phone.

If I knew what TeamViewer was, you know, it would have been easy, but I did not know, so I guess, to me it was difficult. (P7)

While P9 had noticed this app, they admitted, "To be fair, I didn't pay too much attention to it."

Some participants tried to detect spyware through iOS settings. Four participants suggested visiting the Control Center in the iOS Settings. Others visited Accessibility and Privacy settings. P5 reviewed app permissions.

These findings suggest that determining the potential for apps to be used as spyware is not intuitive and requires familiarity with dual-use and spyware apps, or the ability to easily learn the capabilities of unfamiliar apps.

Advice in Tech Abuse Context. Some participants had personal advice relating to the hypothetical friend who was being monitored by their significant other:

Well, she didn't download it—her loser boyfriend did. Get rid of the boyfriend. (P1)

I would definitely encourage them to leave the relationship. (P3)

Participants were also asked about precautions to keep in mind after discovering the app and what advice they might give their friend after removing the app. Participants P2 and P8 said they would advise their friend not to let other people download things onto their phone.

I would say just make sure you only have access to your phone that you don't give it to like a significant other. (P8)

Some participants also made suggestions that may not be feasible or easy in an abusive relationship, such as advice to "delete the other half" of the spyware app (P2) or to remove the app from the partner's device, which does not take survivors' concerns into consideration, something we will discuss more in section 4.

3.3 Account Compromise

Scenario results. To discover an unknown iCloud login from another device, participants took various approaches: looked at iCloud details in iOS Settings, explored the Photos app (P1, P3, P4, P9), and reviewed the privacy settings for the Photos app (P3, P6). Of the five participants who identified the other logged-in device, (P2, P3, P5, P6, P8), some indicated that they had the intuition to look at iCloud settings but that finding the other device was not obvious, as it required scrolling to the bottom of the Apple ID screen:

I think I knew generally to look under iCloud, but I just didn't know like the full screen. (P3)

P1, P4, P7, P8, and P9 could not find the Apple ID page, despite some of them being familiar with the iPhone interface.

Nothing is like foreign to me, but I just didn't know what the steps were. (P9)

Finding the other device was reported to be more difficult than removing the device, which participants found to be easy, as it only involved selecting the device name and then selecting a button to remove the device from the account.

Usability Problems. Many participants did not make the connection between strange syncing issues and unknown logins or account compromise, and those who did could not easily find the device list on the AppleID account page.

3.4 Rooting & Jailbreaking

Scenario results. To follow the FTC's advice, seven participants searched in the AppStore, and two searched on the web. P2 and P8 attempted to use the iOS settings to detect whether the phone had been jailbroken. In the AppStore, participants searched with the following terms: "root checker," "jail break," "root checker app," "rooted," "root," "stalk," and "stalker." "Root checker," the most searched term, was also the first term entered by most participants, despite the fact that the term "rooting" is associated with linux-based devices. None of the participants who did an AppStore search found an appropriate app, and none of the apps found by participants were actually relevant to detecting whether a device is rooted or jailbroken.

> *Why wouldn't they give us a reputable app to use? That is not good. They should have provided someone, especially if they think they're being stalked, with something to use, instead of us wasting time. And there's a stalker out there. (P1)*

Five participants rated the process of implementing the advice as difficult or really difficult. The two participants who did a web search suggested that tutorial videos and online resources would lead them to a reliable root checker app.

Usability Problems. Though the FTC advice directed them to find a "root checker app," participants encountered problems with discoverability, in that they could not find such an app using the AppStore or the web. We offer recommendations to remedy this problem in section 4.

4 Discussion

4.1 Usability Problems in Existing Security Options

Our findings in sections 3.1 and 3.3 suggest that current Google Maps and iOS security mechanisms have serious usability limitations and that the purpose and capabilities of apps may not be easily ascertained. While participants were relatively familiar with some security risks, they could not articulate them in detail. Resolving security problems proved to be difficult or unintuitive for several participants.

4.2 Applicability in IPV and Stalking Contexts

Certain strategies, such as deleting an app, revoking physical/remote access, and leaving or confronting an abuser, may not match the level of risk acceptable to some IPV survivors. For example, one participant's (P4) recommendation to confront a stalker by tracking them in return could pose an unacceptable physical risk to a victim of stalking.

In Scenario 2, two participants suggested that their friend leave the relationship, and two other participants said they would advise their friend to not allow other people to have access to or download apps onto their phone. While many IPV survivors might like to pursue these options, it may not be easy or immediately possible, depending on the survivor's circumstances.

No participant raised concerns about escalating potential abuse in Scenario 2. In tech abuse contexts, when removing an abuser's access, the risk for escalation and the victim's safety should be taken into consideration.

These results suggest that survivors and their advocates should be included in design and research concerning usable security in IPV contexts, since they may be able to provide insights that other people do not.

4.3 Limitations

Limited Number of Participants The study only had 9 participants, which is not enough data to generalize the results.

Limited Number of Suspicious Apps for Scenario 2. Our two iPhone devices had three non-default apps: Zoom, TeamViewer, and Google Maps. Typical iPhone users would likely have more apps installed on their devices, which would make it more difficult to detect spyware.

Only One Sign of iCloud Compromise in Scenario 3 Prompt. In Scenario 3, which concerned iCloud compromise through an unknown device logged into the iCloud account, the only indication of compromise we offered was that photos were appearing and disappearing. This may have caused some confusion. It is possible that mentioning additional signs of iCloud syncing, such as new unknown Contacts or Notes, could change participants' approaches.

4.4 Future Work & Recommendations

Further researches on UI can be done to more intuitively notify users if an individual has an access to their location. It'll also be valuable to explore how & what kind of guidance helps the users navigate settings or actions they can take when faced with a stalking situation.

Given the difficulty participants had following the FTC's advice to download a root checker app, we suggest the FTC revise their advice as follows: 1) Expand the advice to include advice on detecting stalkerware, detecting account compromise and inspecting privacy and location settings [1]. 2) Provide an explanation, examples and criteria for how a root checker app should work. For example, it would help to clarify which operating systems the terms "rooted" and "jailbroken" are associated with. 3) Provide a list of recommended apps that users can trust. If the FTC is not permitted to recommend private apps, provide ways to find up-to-date and reliable apps.

References

[1] URL: https://staysafeonline.org/resource/stalkerware-tip-sheet/.

[2] Jacqueline Connor. *Who's stalking: what to know about mobile spyware*. Sept. 2016. URL: https://www.consumer.ftc.gov/blog/2016/09/whos-stalking-what-know-about-mobile-spyware.

[3] Diana Freed et al. ""A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology". In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Apr. 2018, pp. 1–13. ISBN: 9781450356206. DOI: 10.1145/3173574.3174241. URL: https://dl.acm.org/doi/10.1145/3173574.3174241.

[4] Diana Freed et al. ""Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence". In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW (Nov. 2019), pp. 1–24. ISSN: 2573-0142. DOI: 10.1145/3359304.

[5] Diana Freed et al. "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders". In: *Proc. ACM Hum.-Comput. Interact.* 1.CSCW (Dec. 2017). DOI: 10.1145/3134681. URL: https://doi.org/10.1145/3134681.

[6] Sam Havron et al. "Clinical Computer Security for Victims of Intimate Partner Violence". In: *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 105–122. ISBN: 978-1-939133-06-9. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/havron.

[7] Tara Matthews et al. "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*. 2017, pp. 2189–2201.

[8] Jill Messing et al. "Intersections of Stalking and Technology-Based Abuse: Emerging Definitions, Conceptualization, and Measurement". In: *Journal of Family Violence* 35.7 (Oct. 2020), pp. 693–704. ISSN: 0885-7482, 1573-2851. DOI: 10.1007/s10896-019-00114-7.

[9] Cynthia Southworth et al. "Intimate Partner Violence, Technology, and Stalking". In: *Violence Against Women* 13.8 (Aug. 2007), pp. 842–856. ISSN: 1077-8012, 1552-8448. DOI: 10.1177/1077801207302045.

[10] *Stalking Apps: What To Know*. May 2021. URL: https://www.consumer.ftc.gov/articles/stalking-apps-what-know.

[11] Delanie Woodlock. "The abuse of technology in domestic violence and stalking". In: *Violence against women* 23.5 (2017), pp. 584–602.

A Appendix - FTC Advice

Since beginning this study, the FTC has published a newer version of this page, which contains similar advice [10]. Below is the advice we showed participants, from [2].

> *Check to see if your phone has been "rooted" or "jailbroken."* Stalking apps aren't sold through typical app stores. In addition, they usually can be installed only on a phone that has been "rooted" or "jailbroken," which allows a person full control over the phone's operating system. If your phone is rooted or jailbroken and you didn't do it, a stalking app could be installed. "Root checker" apps can quickly tell you whether a phone has been rooted or jailbroken.