The Spyware Used in Intimate Partner Surveillance

***Abstract*—Survivors of intimate partner violence increasingly report that abusive partners have installed spyware on their devices to track their location and monitor their communications. To date there has been no investigation of the spyware reputedly used in intimate partner surveillance (IPS). Via active measurements of app stores and the broader web, we provide the first in-depth study of the IPS spyware ecosystem. Our results indicate rough lower bounds on the magnitude of the problem, with thousands of tracking softwares readily available via Google search or app stores. Contributing to this number, and the complexity of the ecosystem, is that the majority of these applications are "dual-use" - they have an advertised legitimate use (e.g., child safety or anti-theft), but are easily and effectively repurposed to spy on a partner. We design, implement, and evaluate a pipeline combining web and app store crawling, machine learning, and crowd sourcing to help find and label apps that could be used to facilitate IPS. The precise extent to which the discovered tools are being used by abusers is unknown, but our investigation of online blogs, advertising, and customer support services provides compelling evidence that not only are abusers utilizing these tools, but that, in many cases, vendors tacitly encourage illegal uses of their software.**

I. Introduction

Intimate partner violence (IPV) affects, at some point in their lives, roughly one-third of all women and one-quarter of all men in the United States. Increasingly, digital technologies play a key role in IPV situations, as abusers exploit them to exert control over their victims. Survivors , the professionals helping them , and the media report that a critical threat is spyware : applications installed by the abuser on the survivor's phone which surreptitiously monitor and report data from the device. In extreme cases, IPS via spyware can lead to physical confrontations, violence, and even murder

The IPS context creates nuance not faced in more general malware settings. Most notably, in addition to overt spyware, for example apps like FlexiSpy and MSpy , there exist "dual use" applications. These have an advertised, legitimate purpose, but their primary functionality allows them to easily be abused to facilitate IBS. Survivors and professionals, for example, report that family tracking or Find My Friend applications are being exploited by abusers . What's more, even the designers of more overt spyware increasingly advertise their produces for legitimate uses [1], such as child safety, employee monitoring, and the like.

In this paper, we report on the first measurement study of the ecosystem of applications which could facilitate IPS. We explore detection and remediation schemes for such surveillance, and provide evidence that the developers of these applications are often complicit in IPS, either via active advertisement of negligence.

Measurement challenges and approach. Before we can even perform measurements, the dual-use nature of many applications raises the challenge of specifying what constitutes spyware. Indeed most applications on modern mobile platforms could be exploited by abusers in some fashion. For example, Google Maps can be configured to continuously share a device's current location with another person. To establish a clear boundary, we use this heuristic: an application has the potential to facilitate IPS when (1) its primary functionality is remote access to device data and (2) it achieves this without ongoing interaction with the device user. This takes Google Maps out of consideration (because it's primary purpose is not tracking), but leaves most family tracking apps subject to scrutiny. This definition is appropriate for our purposes, as we are primarily concerned with characterizing and detecting apps that IPV survivors will want the ability to remove from their devices. Dealing with the potential for abuse of applications like Google Maps, which can be critical to survivors' every day lives, is a different challenge that we leave to future work.

The first step in characterizing spyware is to find representative examples. We hypothesize that most abusers find spyware using web search. We therefore started by performing a semi-manual crawl of Google search results. We searched on a small set of relevant search terms (e.g., "track my girlfriend" and "spy on my husband's device"), collected the resulting pages as well as Google's suggestions for similar searches, searched on those suggestions, and repeated. The results reveal a wide variety of resources aimed at helping people engage in IPS: blogs reviewing different tools, how-to guides for setup and stealth, and direct links to dual-use apps for Android and Apple. A large number of the results were for Apple and Android application store apps, in addition to a large number of applications that are not available on app stores.

We therefore design, build, and evaluate a crawling pipeline for Google's Play Store, the official Android app store. The pipeline gathers candidate spyware applications via snowball searching. This results in thousands of applications, many of which are false positives (e.g., applications that are interactive novels about spying). The scale is such that manual investigation of all applications would prove prohibitive. We build a machine learning and Mechanical Turk crowdsourcing tool that accurately filters out false positives based on the names and text descriptions of applications as well as the permissions requested by an application. We measure its efficacy against researcher-labeled ground truth.

Categorization of IPS spyware. The resulting corpus of

[1] Whether ethically justifiable or not, such uses are usually legal.

applications with the ability to facilitate IPS is uncomfortably large, with hundreds of Play store applications remaining after filtering. We manually investigate in detail a representative subset of the on-store and off-store applications, installing them on research phones, checking the features they provide, how they are marketed, and the way customer support (when available) responds to inquiries about their suitability for IPS.

Off-store apps, as one might expect, were more overtly advertised for IPS usage. Application websites include blogs and how-to guides about how to use the tool for IPS, and customer service representatives consistently respond to questions such as "Will your tool help me spy on my wife?" with affirmative explanations. The most egregious cases directly condone IPV, with graphic imagery depicting violence against women. In both the Google Play Store and on Google search, paid advertisements for these tools are the first results for searches such as "track my girlfriend".

On-store applications are exclusively dual-use. The bulk can be categorized into either personal-use (e.g., forwarding all text messages to another device), mutual trackers (e.g., family tracking applications that one must install on multiple devices), or subordinate tracking (e.g., employee or child tracking). In many cases these have capabilities matching or almost matching those of overt off-store spyware. While Play Store requires developers to agree not to allow their apps to be covert, for example by hiding their icon, these requirements are not enforced by the Android operating system, and many apps successfully display no indication that they are on the phone. Paid advertisements for many of these applications appear in response to IPS-related search queries.

Performance of existing anti-spyware. The existence of so many easily obtainable, powerful dual-sue applications suggests that survivors need detection and cleanup tools. A variety of anti-spyware tools advertise their ability to deal with spyware. These include both major anti-virus vendors, such as Virustotal, Kaspersky, Avast, and ESET, as well as lesser-known tools, some purportedly designed to deal specifically with IPS. As far as we are aware, no one has evaluated these tools for the particular task of detecting dual-use applications in an IPV context. We therefore do so, selecting dual-use spyware applications from the Play store, as well as the overt off-playstore spyware. No anti-spyware tools effectively detect dual-use applications.

Towards effective IPS spyware detection. Our measurement study shows that dual-use applications are widely available and that existing tools fail to detect it. We therefore begin to develop a better tool for spyware detection. We detail a tool based on our measurement pipeline for finding and labeling applications usable for facilitating IPS. We believe this will be a pragmatic near-term solution for helping detect the spyware most readily discoverable by abusers, an urgent need in the IPV context where such spyware represents a real, life-threatening risk. We are currently in discussions with the New York City's Office to Combat Domestic Violence about proof-of-concept deployments to aid IPV survivors who come to their facilities.

Summary. We performed the first in-depth study of applications usable as spyware for intimate partner surveillance. In particular:

- We perform the first measurement study of dual-use applications, particularly focusing on the applications easily discovered via web search and which, as a result, pose a real and immediate threat to survivor safety.
- We highlight the role of dual-use applications in the IPS context, and show how dual-use tools are facilitate IPS in much the same way overt spyware would.
- We show that developers of dual-use applications despite claims that their software is for legitimate uses, advertise their utility to abusers via paid advertisements, customer support interactions, and blog posts.
- We show that existing anti-spyware and anti-virus tools are ineffective at detecting and remediating dual-use apps. We outline a new approach to labeling applications as potentially dual-use based on our measurement infrastructure.