PRIVACY ANALYSIS OF TECHNOLOGICAL SOLUTIONS DESIGNED FOR VICTIMS OF INTIMATE PARTNER ABUSE

XIUFEN YU

A THESIS

IN

THE DEPARTMENT OF

CONCORDIA INSTITUTE FOR INFORMATION SYSTEMS ENGINEERING

PRESENTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF MASTER OF APPLIED SCIENCE

IN INFORMATION SYSTEMS SECURITY

CONCORDIA UNIVERSITY

MONTRÉAL, QUÉBEC, CANADA

SEPTEMBER 2023

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Xiufen Yu**

Entitled: **Privacy Analysis of Technological Solutions Designed for Victims of Intimate Partner Abuse**

and submitted in partial fulfillment of the requirements for the degree of

Master of Applied Science
in Information Systems Security

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

Dr. Jeremy Clark _____ Chair

Dr. Mohammad Mannan _____ Supervisor

Dr. Amr Youssef _____ Supervisor

Dr. Jeremy Clark _____ Examiner

Dr. Mohsen Ghafouri _____ Examiner

Approved by _____
Dr. Jun Yan, Graduate Program Director

September 12, 2023 _____

Dr. Mourad Debbabi, Dean
Gina Cody School of Engineering and Computer Science

ABSTRACT

Privacy Analysis of Technological Solutions Designed for Victims of Intimate Partner Abuse

Xiufen Yu

Stalkerware is malicious software that monitors and tracks a victim's online and offline activity. This harmful technology has become a growing concern, jeopardizing the security and privacy of millions of victims and fostering stalkerware and Intimate Partner Violence (IPV). In response, various solutions have emerged, including anti-stalkerware apps that aim to prevent and detect the use of monitoring apps on a user's device. Organizations dedicated to assisting IPV victims have also enhanced their online presence, offering improved support and easy access to resources and materials. Considering how these tools and support websites handle sensitive personal information of users, it is crucial to assess the privacy risks associated with them. In this thesis, we conduct a privacy analysis on 25 anti-stalkerware apps, 323 websites, 52 hidden device detection apps to identify issues such as PII leaks, authentication problems and 3rd-party tracking. Our tests reveal that 14/25 apps, 210/323 websites, 41/52 hidden device detection apps share user information with 3rd-party services through trackers, cookies or session replay. Based on our analysis of anti-stalkerware websites, we identified 44 domains to which sensitive data is sent, along

with 3 services collecting information submitted in forms through session replay. During the dynamic analysis of hidden device detection apps, 25 third-party hosts were observed gathering device or apps information. Furthermore, we conducted a readability assessment of privacy policies obtained from anti-stalkerware apps/websites and hidden device detection apps. Our findings indicate that these privacy policies are highly complex and challenging to comprehend.

Acknowledgments

I would like to thank my supervisors, Dr. Mohammad Mannan and Dr. Amr Youssef for their constant support and guidance throughout this project. Their continued support gave life to this project and made this research possible. I would like to express my gratitude for their patience, motivation, enthusiasm, and immense knowledge. I am incredibly grateful to be able to work under the close guidance of my supervisors who inspired me with bright ideas, helpful comments, suggestions, and insights which have contributed to the improvement of this work. The work in this thesis was partially supported by the Office of the Privacy Commissioner of Canada (OPC). I received substantial financial support from my supervisors and Concordia University and I am thankful for easing the financial burden during my research.

I would also like to thank my peers at the Madiba Security Research Group for sharing their knowledge and experience and being there beside me on my rainy days. I learned a lot from everyone, especially, Sajjad Pourali, Bhaskar Tejaswi, Pranay Kapoor and Rohan Pagey. I feel lucky to be a part of this research group. Lastly, my deepest appreciation goes to my family. This journey would not have been possible without their encouragement and support. Their love and unwavering support means everything to me.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview

A recent report [29] published by the Bureau of Justice Statistics revealed that approximately 1.3% (3.4 million) of all U.S. residents age 16 or older were victims of stalkerware in 2019. Intimate Partner Violence can be of various types, physical or psychological. It can lead to severe emotional distress and physical harm with extreme cases being homicides (15% of the 2020 homicides in Canada were committed by spouses or former intimate partners [3]). Given the serious nature of stalkerware, its growth in the past few years [4] and its detrimental effects on victims, there are a variety of physical and online resources available to help victims. In today's digital era, anti-stalkerware websites/apps help victims to prevent, identify, report, and respond to stalking incidents.

Anti-viruses or anti-malware apps are generally widely known as they offer a large set of services regarding malware mitigation, but other apps claim to focus on protecting the

user from stalkerware specifically, and can be found more easily than other general detection tools when looking for stalking-related keywords on app markets. Victims suspicious that a stalkerware could be installed on their phone might be more likely to download an app claiming to be specifically conceived for this specific case. Through our work, we aim to understand whether and how user data privacy is ensured in detection apps, as well as their reliability in combating stalkerware. Additionally, we examine websites that provide online resources and support materials to IPV victims. These resources may include hotline numbers, addresses of support centers, chat rooms, and general guidelines for various victim situations. Considering that these websites may be accessed by individuals in danger, it is crucial to carefully assess how they handle private user information to prevent exposing sensitive data to unauthorized parties or networks. Our focus is on identifying 3rd-party trackers and potential leaks of personally identifiable information (PII), as they pose a threat to the anonymity that should be inherent to these websites.

Numerous studies related to anti-malware apps have been conducted, notably on new malware detection methods and rogue mitigation apps being hidden malware [9, 19, 24, 32]. Other work in spyware detection [25] does not focus on mobile environment. Similarly, privacy issues on websites have been extensively analyzed, with large scale studies of privacy protection on the web, including specific areas like government websites [34] and hospital websites [41]. Anti-stalkerware apps, hidden device detection apps, however, have not been thoroughly studied yet. More specifically, their privacy footprint and effectiveness have not been measured. The same applies for IPV victims helping websites.

In this thesis, we perform a privacy study on 25 anti-stalkerware apps, 323 victim support websites, and 52 hidden device detection apps. Out of 25 anti-stalkerware apps, 18 were downloaded from Google Play Store while 7 were collected from a Chinese website dedicated to downloading Chinese apps.[1] We chose to look at Chinese apps because of their unique app ecosystem, which is arguably the second largest after the Google Play Store one. All the 52 hidden device detection apps were downloaded from Google Play Store. We divided our analysis into three parts, each addressing a specific challenge: (i) Identifying privacy issues that could jeopardize user anonymity, such as the collection and distribution of Personally Identifiable Information, (ii) Understanding the functionality of these apps and evaluating their effectiveness in detecting stalkerware. (iii) Assess the readability of privacy policies on victim support apps or websites.

1.2 Contributions

Our contributions and notable findings can be summarized as follows:

1) We design analysis frameworks to identify privacy related issues in anti-stalkerware apps and websites, and use them to assess the privacy footprint of 25 anti-stalkerware apps for Android devices and 323 IPV victim support websites. We detected 1206 third-party scripts in IPV victim support websites, 603/1206 (50.0%) them were identified as known trackers.

[1] http://www.downcc.com

2) Our privacy analysis reveals that 14/25 apps transmit data to 3rd-party services, including sensitive information like device ID or GPS location in 4 cases. 13 apps are also found using trackers for advertisements or user experience purposes. We also identify 44 distinct 3rd-party domains that tested apps communicate with during user interaction. 210/323 (65.0%) of victim support websites include 3rd-party trackers. We list 40 unique 3rd-party hosts that gather the web pages users browse and the keywords in the Search functionality. We detect 3 session replay services (Yandex, Hotjar and Clarity) on 17 victim support websites, which apparently collect usage information, user PII and other sensitive data (when a data submission form is available). Our analysis also reveals that the Chinese tracker hm.baidu.com collects users sensitive information on 2 Chinese websites.

3) 2/4 apps incorporating a login feature with account management use dangerous authentication practices, which could lead to account takeover in one of these cases. One anti-stalkerware website uses HTTP protocol for their online chat service, exposing users' names, emails and messages.

4) We identify one company developing a stalkerware (KidsGuard) and an anti-stalkerware (ClevGuard), promoting both apps on their website and publishing their mitigation tool on the Google Play Store. The anti-stalkerware tool detects the malicious app but requires a premium subscription to see it. We also observe 3 apps from separate companies using the same detection framework on their back-end infrastructure when scanning the phone.

5) We analyzed the privacy issues on 52 hidden device detection apps and observed 88 unique hosts (with 45 being unique domains) that these apps communicated with during user interaction.

6) A total of 17 third-party libraries in hidden device detection apps were detected by using MobSF [18]. They are primarily integrated for purposes such as advertising and analytics.

7) We noticed that the device information along with app information were collected and sent to third-party servers. Noticeably, 2 hidden device detection apps were detected to collect GPS information.

8) We evaluated the readability of privacy policies for anti-stalkerware apps, websites along with hidden device detection apps and observed that 119/323 (36.8%) hidden device detection apps, 20/25 (80.0%) anti-stalkerware apps, and 26/52 (50.0%) hidden device detection apps do not provide privacy policies; the readability results show that the privacy policies are still difficult to understand.

1.3 Thesis Organization

The rest of the thesis is organized as follows. In Chapter 2, we present background information for Javascript/Cookie based tracking services, third-party libraries, session replay service, frameworks for privacy analysis and the readability of privacy policies. In Chapter 3, we provide related work regarding privacy analysis on websites, anti-stalkerware apps

and hidden device detection apps. In Chapter 4, we introduce our analysis methodology and experimental results on anti-stalkerware websites and anti-stalkerware apps. In Chapter 5, we present the techniques used for collection and analysis of hidden device detection apps, along with detailed analysis results. In Chapter 6, we illustrate readability assessment of privacy policies for anti-stalkerware apps/websites and hidden device detection apps. Finally, in Chapter 7, we discuss our limitations, offer various recommendations for different stakeholders, and conclude the thesis with future work.

1.4 List of Publications

The following publications resulted from the research work were performed during my master's program. The work presented in this thesis is from the second paper.

- Yu, Xiufen, Nayanamana Samarasinghe, Mohammad Mannan, and Amr Youssef. "Got sick and tracked: Privacy analysis of hospital websites." In 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 278-286. IEEE, 2022.

- Philippe Mangeard, Xiufen Yu, Mohammad Mannan, and Amr Youssef. "No Place to Hide: Privacy Exposure in Anti-Stalkerware Apps and Support Websites," In the 28th Nordic Conference on Secure IT systems (NordSec) 2023.

Chapter 2

Background

In this section, we introduce different concept and technologies that are used in the subsequent chapters of this thesis.

2.1 Javascript/Cookie based Tracking Services

Englehardt et al. [13] found that nearly 9 in 10 websites leak user data to parties of which the user is likely unaware; more than 6 in 10 websites spawn third- party cookies; and more than 8 in 10 websites load Javascript code from external parties onto users' computers.

Javascript. JavaScript is a programming language that allows websites to be more interactive and responsive. It can also be used to track your behavior on a website. Different tracking mechanisms are used in Javascript, for instance, event tracking records specific events that you trigger (e.g., clicks, mouse movements, filling forms) on the website; Javascript can gather information about user's browser, device and system configuration to create a

unique “fingerprint”. This fingerprint can be used to track users across websites; JavaScript can utilize local storage and session storage to store data on a user’s device. This data persists even after the browser is closed and can be used for tracking user behavior.

Cookies. Cookies are used in web development primarily because HTTP is a stateless protocol. This means that each HTTP request from a client (such as a web browser) to a server is independent and does not inherently maintain any memory of past requests or interactions. Cookies provide a way to add a form of statefulness to the stateless HTTP protocol. When a server sends a cookie to a client’s browser, the browser stores the cookie locally. Subsequent requests from the same client to the same server include the cookie in the request headers. This allows the server to identify the client and maintain some state information between requests.

It is important to note that while cookies are widely used and offer benefits for enhancing user experience, but they can also raise privacy concerns. Users’ personal data and browsing habits can be tracked through cookies, leading to privacy and security issues, such as SameSite attribute settings for cookies.

2.2 Third-party Libraries

In the realm of software engineering, Android apps and websites extensively integrate third-party libraries, aligning with the fundamental principle of “Don’t reinvent the wheel”. The third-party libraries are imported for diverse purposes, such as advertising, analytics, crash

reporting, debugging, and similar tasks. There are a lot of benefits [22] of using third-party libraries/SDK. Generally, third-party libraries provide developers with the unique opportunity to integrate pre-tested, reusable software that saves development time and cost. This allows developers to focus on the core features of the app or the website. For example, a third-party advertising SDK can help a developer optimise advertising, whereas the crash reporter SDK helps with identifying and debugging.

However, reusing third-party libraries can introduce privacy and security issues. Cyber security news [10] reports that popular apps with over 142.5 million installations leaked user data to unauthorized third-parties. Zhao et al. [42] conducted a study on third-party libraries, and their results show that 23% third-party libraries violate regulation requirements for providing privacy policies. Over 39% miss disclosing data usage in their privacy policies. Over 65% host apps share user data with TPLs while 65% of them miss disclosing interactions with TPLs. The study reminds developers to be mindful of third-party libraries usage when developing apps or writing privacy policies to avoid violating regulations.

2.3 Session Replay Service

Session replay is the ability to reproduce a user's interactions on a website or web application to know how the user actually experienced it. Session replay service transforms user events, such as mouse movements, clicks, page visits, scrolling, tapping, etc., into a reproduction of what the user actually did on the site or app. This practice empowers web developers to fix bugs, while enabling marketing teams to precisely target their products

for optimal results. Analyzing users' actions along with websites responses can enhance users' satisfaction and increase revenue.

However, session replay tools need to ensure they are addressing user privacy issues very seriously. Session replay tools are supposed to disclose privacy policy to users. Session replay service should not collect private and sensitive information at the recording stage or do not play back the confidential information during the replay stage. All users' private and sensitive data (e.g, email, phone number, address, identification) must be masked.

2.4 Tools for Privacy Analysis

OpenWPM-An automated platform for web privacy measurement. OpenWPM [14] is an open-source and automated web privacy measurement framework, designed and implemented by Princeton University in 2015. It provides transparency into the practices of data collection for privacy studies on a large-scale websites. OpenWPM uses Selenium, allowing to launch websites in headless mode or using Firefox browser. After crawling websites, collected data is saved in a SQLITE database which creates 14 distinct tables, such as task, sites_visits, incomplete_visits, javascript, javascript_cookies, navigations, http_requests, http_responses, http_redirects, crawl, crawl_history, dns_responses, callstacks and sqlite_sequence. Researchers can develop custom scripts by using the crawled database for potential web privacy concerns, allowing them to gain insights into the various types of

tracking technologies used, the sharing of user data with third parties, and other privacy-related concerns.

MobSF-Mobile Security Framework. Mobile Security Framework (MobSF) [18] is an automated, mobile pen-testing, malware analysis, security assessment, all-in-one framework. It can perform both static and dynamic analysis, supporting different mobile app binaries, like APK, XAPK, IPA, APPX, as well as Zipped source code. The Dynamic Analyzer conducts runtime security assessment and interactive instrumented testing.

To use MobSF, individuals are required to establish the MobSF server within a docker environment. Following this setup, the APK file should be uploaded to the server, initiating an immediate execution of static analysis. MobSF will generate a security report concerning the scrutinized APK. This report encompasses elements like the security score, grading, application permissions, network security, certificate assessment, manifest evaluation, code analysis, domain malware check, and more.

2.5 Privacy Policies

Privacy policies are a set of standards and procedures that state how apps/websites collect, use, and share information about users. App developers are required to include privacy policies to comply with legal regulations.

However, most privacy policies are very vaguely worded and difficult to read. Privacy policy comparison [21] from 75 leading apps and websites are found to be long and in some cases unreadable, which requires university-level reading skills to easily understand. This

online report [8] revealed the top 20 most difficult privacy policies of popular websites, including Disney, Instagram, Zoom, Spotify, etc. For example, Spotify gathers irrelevant voice data; Disney states sharing users' data with third-parties; Instagram's private policy discloses practices such as logging IP address and exact location, sharing search history, location, and more with third parties. Consequently, a lengthy, convoluted, and poorly constructed privacy policy could give rise to potential privacy concerns.

Chapter 3

Related Work

In this section, we provide a summary of noteworthy privacy studies concerning anti-stalkerware websites/apps, hidden device detection apps, and the readability assessment of privacy policies.

3.1 Privacy Analysis of Websites

Eterovic et al. [15] conducted a review of the technologies used by stalkers and technologies used against stalkers. They pointed out the following possible future research directions: improving existing privacy and anti-stalker techniques as well as developing techniques to detect stalking behavior on social media and blogging platforms. Samarasinghe et al. [34] performed a privacy measurement on government websites and Android apps. They found numerous commercial trackers on these services; 27% of government Android apps leak sensitive information to 3rd-parties. Senol et al. [35] performed a measurement of data

exfiltration from online forms. Their study showed that users' email addresses were collected by 3rd-parties before form submission and without giving consent on both US and EU websites. Similarly, password on 52 websites were found to be leaked to 3rd-party session replay scripts. Yu et al. [41] analyzed the privacy issues on hospital websites and observed that users credentials were sent to session replay services. Ischen et al. [20] investigated the privacy issues of chatbots used on websites. Their results showed that users are more inclined to share personal information with a human-like chatbot rather than with a machine-like chatbot.

3.2 Privacy Analysis of Anti-stalkerware Apps

Fassl et al. [17] compared the users' reviews of 2 anti-stalkerware apps to understand users' perception and the apps' capabilities. They also performed reverse engineering to understand their detection features. Their results suggests that app capabilities do not correspond to the users' expectations. In order to detect spyware systems, Qabalin et al. [32] employed machine learning algorithms to create a multi-class classification model for network traffic, which achieved good detection accuracy. Kaur et al. [24] proposed a hybrid approach of description analysis, permission mapping and interface analysis to detect malicious applications in Android. The works mentioned above deal with spyware detection, instead of privacy and security issues related to such detection methods. In addition to academic research, stalkerware also attracted the attention of people in industry. ESET research group published a white paper [37] which analyzed Android stalkerware vulnerabilities. A group

of collaborators also compiled all information about known stalkerware apps and built the Stalkerware-indicators [12] GitHub repository to make the detection of spyware easier in both Android and iOS systems. TinyCheck [23] is a detection solution currently in development by Kaspersky to assist non-technical individuals to detect stalkerware on their device. Because of its early development stage, the tool currently lacks features thus making it less effective than more standard solutions. However, its main end goal quality would be to allow stalkerware detection without installing anything on the compromised phone, thus making it harder for the stalker to notice that the victim is being suspicious.

Other relevant work. Several other recent studies also explored topics related to IPV technologies and victims, although not directly the privacy implications of victim-support apps and websites. For example, Chatterjee et al. [7] studied the intimate partner stalking (IPS) spyware ecosystem, and identified several hundred of such IPS-relevant apps (from app stores and beyond). The authors showed that existing anti-virus and anti-spyware tools mostly fail to identify these dual-use apps as a threat. More recently, Almansoori et al. [1] identified 854 dual-use apps available on the Google Play Store, many of which do not provide English descriptions and cannot be found via English search queries (i.e., available in other languages, which are not as well-monitored by Google as the apps in English). Liu et al. [27] analyzed 14 Android apps outside of Google Play, and studied the mechanisms used for spying. ESET [37] performed a comprehensive security analysis of 86 stalkerware applications, and reported several critical vulnerabilities in the apps that may allow victim data compromise via other third-party attackers.

Beyond stalkerware apps, Stephenson et al. [39] identified how various common IoT

devices (32 types in total) including home thermostats, smart speakers, cameras, smart toys, and Bluetooth item trackers, can be abused by IPV attackers. From interviews with 20 IPV victims of such IoT abuse, in another study, Stephenson et al. [38] identified various instances of abuse cases involving such devices. Ceccio et al. [6] evaluated commercial devices and apps that claim to detect such spy IoT devices, and found that these detectors are very ineffective in real-world abuse scenarios.

3.3 Readability of Privacy Policy

Fabian et al. [16] performed the first large-scale study on readabilty of nearly 50,000 privacy policies of popular English-speaking Websites. The results empirically confirm that on average, current privacy policies are still hard to read. Krumay et al. [26] investigated seven quantitative approaches to measure the readability of privacy policies. The results show that existing approaches to measure readability can be applied to privacy policies, but require some additional rules. The results can be used as a basis for decision making, but do not explicitly suggest, what to change. A combination of different scales and adding some of the qualitative parameters might be a solution. Robillard [33] conducted an analysis of availability, readability, and content of privacy policies and terms of agreements of mental health apps. They found that most mental health tracking apps did not include a privacy policy or terms of agreement; a majority of privacy policy stated that users' information may be shared with third parties. Additionally, the readability of mental health apps' privacy policies and terms of agreements is too difficult for the general population.

Srinath [36] designed a corpus creation pipeline and investigated the composition of the corpus, which can evaluate privacy policies in terms of readability, similarity, keyphrase extraction, and explore the corpus through topic modeling. Amos [2] performed a study on how privacy policies changed over time by analyzing a dataset of 1,071,488 privacy policies, spanning over two decades. They found that privacy policies have consistently failed to disclose the presence of common tracking technoligies and third parties. They also found that over the last twenty years privacy policies have become even more difficult to read, doubling in length and increasing a full grade in the median reading level. None of the studies above have analyzed the privacy policies regarding victim support websites and apps.

Chapter 4

Privacy Analysis of Anti-stalkerware Websites and Apps

In this section, we detail the methodology and techniques that we utilized to analyze privacy concerns associated with anti-stalkerware websites and applications. In addition, we substantiate these analyses with experimental findings.

4.1 Anti-Stalkerware Apps

We conduct our analysis of solutions against stalkerware apps with three goals in mind: evaluating data privacy and identifying security issues of stalkerware detection tools available for Android, as well as assessing their effectiveness in a realistic context. To collect apps we look through the Google Play Store and web-based Android app databases for keywords such as “anti-stalkerware”, “anti-stalking”, “stalk detector”. We gather a sum

of 25 victim support apps, with 18 from the Google Play Store, and 7 from Chinese app markets. See Figure 1 for our methodology diagram.

Privacy and security analysis. We focus our analysis on 4 distinct vectors through which users' security and privacy could be violated:

Authentication mechanisms. In cases where the app offers a login feature and account management functionalities, we identify the mechanisms used for authentication and verify their security. Such methods include username & password validation, session management and authentication tokens. We examine network traffic related to user login to check if credentials are properly secured and sent. We also look at how the user session is kept alive over time and if token replay attacks allow unauthorized users to hijack the user's account.

Personal Identifiable Information (PII) leaks. Apps can sometimes upload information about the device they are installed on, or the device's user. If such personal data is transmitted without proper encryption, pieces of information such as names, addresses, phone numbers or IMEI number could be extracted by attackers and used to identify, track or impersonate individuals. These leaks can be unintentional or malicious, in cases where the app transmit data to other parties without the consent of the user. Unintentional leaks can be caused by faulty security protocols during uploads, or accidental exposure through error messages or debug logs.

Third-party libraries. Through static code analysis, we identify 3rd-party libraries used by anti-stalking apps. Then, by examining the traffic generated by user interactions, we can discern requests related to first-party and 3rd-party libraries. Like with PII leaks, these 3rd-party libraries used by the app could be a threat to the user's privacy by accessing device

information or personal data. We identify the presence of libraries and trackers and verify the data they collect through static code analysis and traffic monitoring. We then compare them to a list of well-known trackers (Easylist) for classification.

Insecure custom encryption. In addition to potentially insecure implementations of standard encryption channels (like HTTPS), some apps use non-standard protocols, additional channels and encryption layers. We used ThirdEye [31] to identify custom encryption used by the apps and assess their security.

Effectiveness Tests. Proper functioning of anti-stalkware apps is crucial to the safety of IPV victims, it is thus important to assess the effectiveness of such apps and verify that they are not being wrongfully advertised as "highly effective spyware detectors". We tested the reliability of anti-stalkerware solutions by manually installing each app on a purposefully compromised Android device and verifying whether the app could flag the installed stalkerware. Each app is tested against 10 different free stalkerwares. We utilize only free stalkerware apps for our test to avoid purchasing such apps due to ethical concerns about supporting stalkerware companies. Among the 10 chosen stalkerware apps, *iKeyMonitor* and *AndroidSpy* are treated as special cases, as they provide weekly builds of their app's package. The APK available on their website is recompiled every week with a different package name. This effectiveness test allows us to identify the different detection mechanisms used by anti-stalkerware apps as well as the amount of details they give about detected apps. This includes information such as the permissions required by the detection app to function properly, or flags assigned to potentially dangerous apps giving details to the user (e.g., labelling the detected app as a stalkerware or just a malware). We note

that our tests do not include any attempt to trick the anti-stalkerware apps, by changing the stalkerware package names or signature. However, the inclusion of weekly built apps approximates this behaviour.

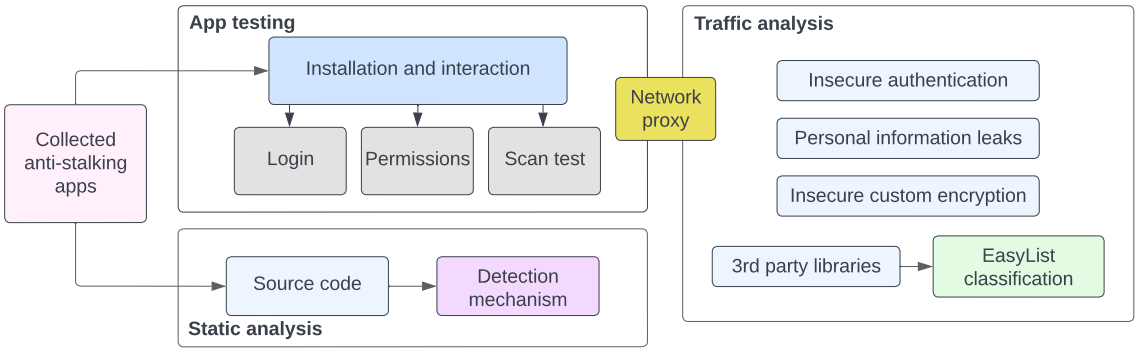

Figure 1: Privacy analysis methodology of anti-stalkerware apps

4.2 Privacy Analysis of Victim Support Websites

Our methodology comprises three key elements. We collect the URLs of anti-stalking websites through keyword searches such as "anti-stalking", "stalking victims" or "stalking support" in both Google and Baidu search engines. We then use OpenWPM [30] to crawl the websites, which saves crawled information in a SQLite database. We then filter it through Easylist and EasyPrivacy [11] to categorize 3rd-party scripts/cookies and check whether there are session replay services on the websites or not. We manually fill online forms on those websites to identify users' sensitive information leaks; see Figure 2.

Collecting Victim Support Websites. We start with the resources mentioned on the stopstalkerware website[2] which includes 25 domains in 13 different countries. We then manually extended our victim support website collection by searching for keywords, like, "anti-stalking", "stalking victims", "stalking support" and "stalking help". In total, we collect 323 victim support websites; including 120 from China, 77 from Canada, 34 from the USA, 22 from Europe, 14 from Hong Kong, 13 from the UK, 12 from South America, 7 from Australia, 24 others from Egypt, Turkey, Malaysia, Russia, Ukraine, India and 1 from the UN. Note that the collected websites can be either dedicated to anti-stalking or related to anti-stalking, so they can be any websites that provide support or advice to victims, e.g., anti-stalking websites, government websites, university websites, websites for legal help, websites offering shelters to victims or non-profit organizations. Chinese websites are collected on Google and Baidu, however if we search keywords related to anti-stalking or domestic violence for China, most of the results tend to be news reports rather than websites or resources directly related to the topic. We choose Women's Federation's websites[3] for our Chinese dataset. The Women's Federation is a women's rights organization divided in subgroups across China, providing online resources for each city. They offer guidelines for victims of domestic violence or any form of IPV. In total, we collect 108 Women Association websites and 12 online legal support websites in China.

Privacy Measurements. We configure OpenWPM [30] web privacy measurement framework with 10 parallel browser instances in headless mode. We explicitly enable OpenWPM instrumentations for HTTP requests, Javascript, cookies, DNS requests, callbacks and page

[2] https://stopstalkerware.org/resources

[3] www.bjwomen.gov.cn, hnflw.gov.cn, www.sxwomen.org.cn, www.womenvoice.cn

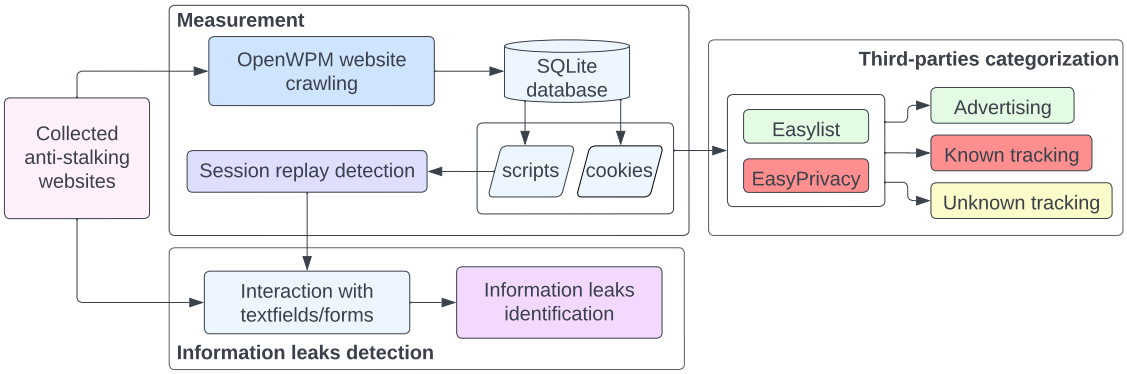

Figure 2: Privacy analysis methodology of victim support websites

navigations. We use a physical machine running Ubuntu 22.04 LTS for our measurements in Feb. 2023. A total of 323 victim support websites are crawled using OpenWPM from a North American university campus. We save the crawling result in a SQLite database for further analysis. The saved information contains both stateful (i.e., scripts/cookies), and stateless forms of tracking metrics. We then examine the saved tracking scripts/cookies for 3rd-party domains, i.e., domains of scripts/cookies that do not match the domain of the websites that they are on.

We use filtering rules [11] that block 3rd-parties to identify three categories of 3rd-party domains: ad-related 3rd-parties blocked by EasyList; known trackers blocked by EasyPrivacy; unknown trackers, or any 3rd-party service that is not blocked by either lists.

We manually browse those websites to find pages containing user-filled forms, which include registration/login, contact-us, and search. We tested 220 unique URLs of such web pages on victim support websites.

4.3 Results

4.3.1 Results of Victim Support Apps Analysis

Tested apps gathered on the Google Play Store are listed in Table 3. We refer to their common names (or company names) in the following sections. For Chinese apps, we refer to their package names.

Authentication and session management. Out of the tested 25 anti-stalkerware apps, only 4 of them allow the user to register an account and login with their credentials (Protectstar AntiSpy and Clevguard on Google Play, as well as cn.lslake.fangjianting and uni.UNI1898B51 on Chinese app markets). Protectstar uses API calls to perform actions, and authenticate as a specific default user when no account is used. This user account called "psapi" is automatically logged into by the app on launch, using seemingly hard-coded credentials to request a session token. This session token appears to be usable for any regular API call, except the ones reserved for getting premium subscription licenses and account management. On the other hand, the Chinese app uni.UNI1898B51 assigns session tokens on login that are not modified nor deleted after logging out. Even though a new token is generated if the user logs in again, an attacker could replay this token even after a user disconnected from their account and call the API on their behalf. The second Chinese app, cn.lslake.fangjianting, allows login through either Tencent QQ or Wechat and thus leaves authentication responsibility to these apps.

Encryption mechanisms and PII leaks. Upon manual inspection of the network traffic generated by anti-stalkerware apps, we identified 3 cases where data is being sent to

3rd-party hosts. Com.arcane.incognito shares hardware and OS information with Facebook, data including memory usage, OS version or the phone's model, whether the device is rooted or not, and if it is identified as an emulator. We also noticed the user's email being sent to a first party host (incognitotheapp.zendesk.com), even though the app does not feature user accounts. Skibapps also shares hardware information like the device type, alongside OS type and version, only this time to Adloox. The app spyware.detector.remove.antihacker communicates with Yandex, a Russian ad provider, and sends hardware information along with the google_aid (advertising ID), device-id (IMEI or MEID) and userid.

In addition to these manual checks, we gathered network traffic from all 25 anti-stalkerware apps using ThirdEye [31], and identified 21 additional instances of user/device information being shared to 3rd-party hosts by 14 apps. The data includes 13 cases disclosing the phone model, 4 with OS information, and others sharing cookies or tokens. We identified 3 first-party destination hosts (for Foxbyte Code, Incognito and Cb Innovations), the others being 3rd-party; see Table 1.

Third-party libraries. Since all anti-stalkerware apps in our analysis are free, most of them rely on 3rd-party ad providers and trackers to generate income. Others offer premium versions of their app with additional features, but still make the device scan available for free. During the course of our analysis, we kept track of each request being sent to a 3rd-party and compiled all of them into Table 2. We can see the majority of apps use

Table 1: Information shared by apps to 3rd-party services

App	Item	Destination address
cn.lslake.fangjianting	build	pangolin.snssdk.com (custom encryption)
Foxbyte Code	build	www.foxbytecode.com
com.txjjy.fjtjc	build	pangolin.snssdk.com (custom encryption)
Clevguard	cookie	apipdm.imyfone.club
com.yyyx.fjtws	cookie	fjt.4fqp.com
Incognito Security Solutions	device-email	incognitotheapp.zendesk.com
cn.lslake.fangjianting	model	ulogs.umeng.com
Cb Innovations	model	firebase-settings.crashlytics.com
Certo	model	certo-scan-results-ingestion.azurewebsites.net
Cyber Tor	model	cdn.liftoff-creatives.io
Malloc Privacy	model	firebase-settings.crashlytics.com
Protectstar Antivirus	model	firebase-settings.crashlytics.com
com.txjjy.fjtjc	model	privacy.viterbi-tech.com
com.txjjy.fjtjc	model	ulogs.umeng.com
World Globle	model	adtubeservices.co.in
World Globle	model	cdn.liftoff-creatives.io
com.yyyx.fjtws	model	ulogs.umeng.com
Coolrepairapps	model	yastatic.net
cn.lslake.fangjianting	token	tool.sqcat.cn (custom encryption)
Mahika Developers	token	graph.facebook.com

Google APIs (e.g., 11 using Firebase) for various reasons. However, specific apps like spyware.detector.remove.antihacker send data to unique known tracking/advertisement companies like Yandex, Adjust or Doubleclick (owned by Google). We also notice the presence of Facebook hosts in 3 apps, 2 of them specifically reaching graph.facebook.com, often used to get data in or out of the platform (in our case, both requests were sending data to Facebook).

Out of 121 separate get requests for .js files found in the apps' network traffic, we found 95 are used by "advertisers" according to EasyList. The other 26 URLs were unknown to the blocklist we used for comparison, but we then manually identified 3 domains associated

Table 2: Number of anti-stalkerware apps reaching 3rd-party hosts

Destination host	#App
Google	18
DoubleClick	7
Umeng, app-measurement.com, cdn.liftoff-creatives.io, s0.2mdn.net	3
graph.facebook.com, dt.adsafeprotected.com, fw.adsafeprotected.com, impression-east.liftoff.io, mobile.adsafeprotected.com, my-api.protectstar.com, pangolin.snssdk.com, rr4—sn-gpn9-t0as.gvt1.com, sf3-fe-tos.pglstatp-toutiao.com, static.adsafeprotected.com, toblog.ctobsnssdk.com, api-access.pangolin-sdk-toutiao.com	2
adexp.liftoff.io, adtubeservices.co.in, Android.bugly.qq.com, api.revenuecat.com, app.adjust.com, app.viterbi-tech.com, assets.mintegral.com, click.liftoff.io, cdnjs.cloudflare.com, dsum-sec.casalemedia.com, ec2-18-116-59-188.us-east-2.compute.amazonaws.com, fjt.4fqp.com, ib.adnxs.com, lf6-ad-union-sdk.pglstatp-toutiao.com, maps.wikimedia.org, privacy.viterbi-tech.com, settings.crashlytics.com, sf3-ttcdn-tos.pstatp.com, techcrunch.com, tnc3-bjlgy.snssdk.com, tool.sqcat.cn, us01.rayjump.com, www.facebook.com, www.lslake.cn, yastatic.net	1

with Yandex (in spyware.detector.remove.antihacker), and 5 related to a Chinese advertisement platform (pglstatp-toutiao.com, hosted by ByteDance).

Detection methods and effectiveness. From the effectiveness tests, we found that 15 out of 25 anti-stalkerware apps could detect at least one malicious app; see Table 3. Surprisingly, 10 out of 25 anti-stalkerware apps (i.e., 7 Chinese apps and 3 Google Play Store apps) completely failed to detect any of the stakerware apps; these 10 apps are omitted in the result table. Overall, stalkerware apps present in open source threat lists and featured in online web articles were the most detected, with TheTruthSpy being found by 13 out of the 25 mitigation tools and CatWatchful by 11 out of 25. Only 4 tools flagged the weekly build of iKeyMonitor as suspicious, but none identified it as a stalkerware. Similarly, AndroidSpy

was flagged in 6 cases, but only once as a malware. 7 tools reported apps with risky permissions enabled, but 2 of them (Malloc Privacy and Incognito) needed the stalkerware to be entirely configured (not just installed and disabled) to flag it.

10 anti-stalkerware apps required a total filesystem access (READ, WRITE and MANAGE_EXTERNAL_STORAGE permissions) and 6 of them requested media access only (among which 3 of them were requesting total access as well). Notification access is required by 11 apps. This is mostly to send notifications rather than to analyze them, as many apps use them to warn the user that a scan is in progress, or that a problem has been found. These permissions are all required by apps performing application signature checks.

Other anti-stalkerware apps function by monitoring the phone's main tools (e.g., camera, microphone, GPS) and sending a notification when an app uses either of these. One app (World Globle Apps) from the Google Play Store claims to use this "active" detection method, recording camera, microphone and GPS usage and alerting the user if it is accessed by another app. However it raised only 1 flag when one stalkerware was being configured (warning that the camera was being used). This means that this anti-stalkerware needs to be on the phone before the malicious app is installed. Other than that, no alerts were raised, even after multiple hours of phone usage. Unlike Google Play Store apps, all Chinese ones implement this monitoring method and thus require related permissions. Access to camera and microphone was requested by 7 apps, and GPS usage was needed in 6 apps. App usage access was only requested twice. This detection mechanism did not prove to be the most efficient if the tool is installed after the stalkerware, it could however be used as a prevention method.

During our analysis, we noticed that 4 different apps use the exact same backend framework to perform their malware scan (Protectstar Antispy, Protectstar Antivirus, Cb Innovations and Foxbyte Code). We note that only the first two apps are developed by the same company. When scanning the device, these apps send two batches of information to an API responding with a list of identified threats. The first batch contains package names of apps installed on the phone, the second one contains their cryptographic hashes. This means that the actual comparison of installed apps to the malware database is done remotely.

Additionally, we found that the company developing com.clevguard.guard also offers on their website a "parental control" app that is advertised as a remote monitoring tool (in other words, a stalkerware). The anti-stalkerware developed by ClevGuard hides most of its functionalities behind paywalls. The free version displays the number of detected threats but does not give information about flagged apps. We tested this anti-stalkerware against the spyware developed by the same company. Even though the free version prevented us from seeing the name of the flagged app, the fact that it detected one threat confirmed that it was not ignoring it.

4.3.2 Results of Victim Support Websites Analysis

Third-party tracking JavaScript/cookies. We found that 169/323 (52.3%) of victim support websites include at least one known 3rd-party tracking script; 31/323 (9.6%) victim support websites use 3rd-party tracking cookies. The proportion of websites with 3rd-party tracking cookies is much lower than websites with 3rd-party tracking scripts. This might

Table 3: The effectiveness detection results of anti-stalkerware apps that can identify at least one of the stakerware apps. ●: Flagged as stalkerware. ○ : flagged because of critical permissions detected. ⊙ : flagged because of trackers detected. ◐: Combination of permissions and trackers. 👤: Flagged as a hidden/fake system app. ▨: flagged as malware. Empty: Not flagged.

Company name (package name)	Version	SpyPhoneLabs	Mobilespy	TheTruthSpy	Snoopza	OwnSpy	CatWatchful	iKeyMonitor	MeuSpy	Cerberus	AndroidSpy
Malloc Privacy (com.mallocprivacy.antistalkerfree)	2.49	○	⊙	●	○	◐	●	⊙	○	●	
World Globle Apps (com.world.globle.mobileantistalker.rs)	1.0.3								○		
Incognito Security Solutions (com.arcane.incognito)	3.0.0.15		●	○	○	○	●		○	○	○
Protectstar antispy (com.protectstar.antispy.android)	5.0.3	●		●	▨	●	●				
Cb innovations (com.cbinnovations.antispy)	2.0.1	●		●	▨	●	▨			●	▨
Protectstar antivirus (com.protectstar.antivirus)	1.2.5	⊙		●	▨	●	●		▨	●	
Certo (com.certo.Android)	2.1.2	●		●		●	●		●	●	
Own effect (com.owneffect.spyware.detector)	1.0.4		○								
Foxbyte Code Inc. (com.foxbytecode.spywarescanner)	1.4	▨		●	▨	▨	▨		▨	▨	
Coolrepairapps (spyware.detector.remove.antihacker)	5.0.0.1	▨	⊙	⊙	○	◐	○	◐		▨	○
Skibapps (com.skibapps.antispyforAndroid)	3.43	●		●	▨	●	▨		▨	●	👤
Lighthouse (net.hobbyapplications.privacyscanner)	1.8.29	●	●	●	○	○	●	○	○	●	○
Mahika Developers (com.whotrackmyphonemhk)	1.0.6	○	○	○	○	○	○	○	○	○	○
Safety Apps (com.spyscanner.spyware.antispywaredetector)	3.0			👤		○			👤	○	
Cyber Tor (com.cyber genius.cyber tor)	5.6			👤		○				○	

be because the EasyList Cookies list we used[4] does not include extensive rules for cookies on Chinese websites.

To better understand 3rd-party scripts/cookies, we grouped them into three categories. We found that 53/1206 (4.4%) 3rd-party scripts were flagged as advertising; 603/1206 (50.0%) 3rd-party scripts were identified as known trackers; 550/1206 (45.6%) were not recognized by Easylist [11], we labelled them as unknown trackers. Similarly, 49/694 (7.1%) 3rd-party cookies were identified as advertising cookies; 266/694 (38.3%) 3rd-party cookies were categorized as known trackers; 379/694 (54.6%) were unknown trackers.

We listed the top-10 domains of tracking scripts and tracking cookies. We can see that the top tracking scripts are googlemanager.com (107/323 (33.1%)), google-analytics (115/323 (35.6%)), Facebook (30/323 (9.3%)) and Baidu (25/323 (7.7%)). We observed

[4] https://easylist.to/

Baidu tracker is only on Chinese websites; see Figure 3. Top tracking cookies are addthis.com (10/323 (3.1%)), clarity.com (6/323 (1.9%)), and demdex.net (8/323 (2.5%)). Addthis is a free social bookmarking service integrated in websites, sharing content across social web; clarity.ms is Microsoft session replay service [28]; Sharethis collects data on user behavior for targeted advertising and analytics; see Figure 4.

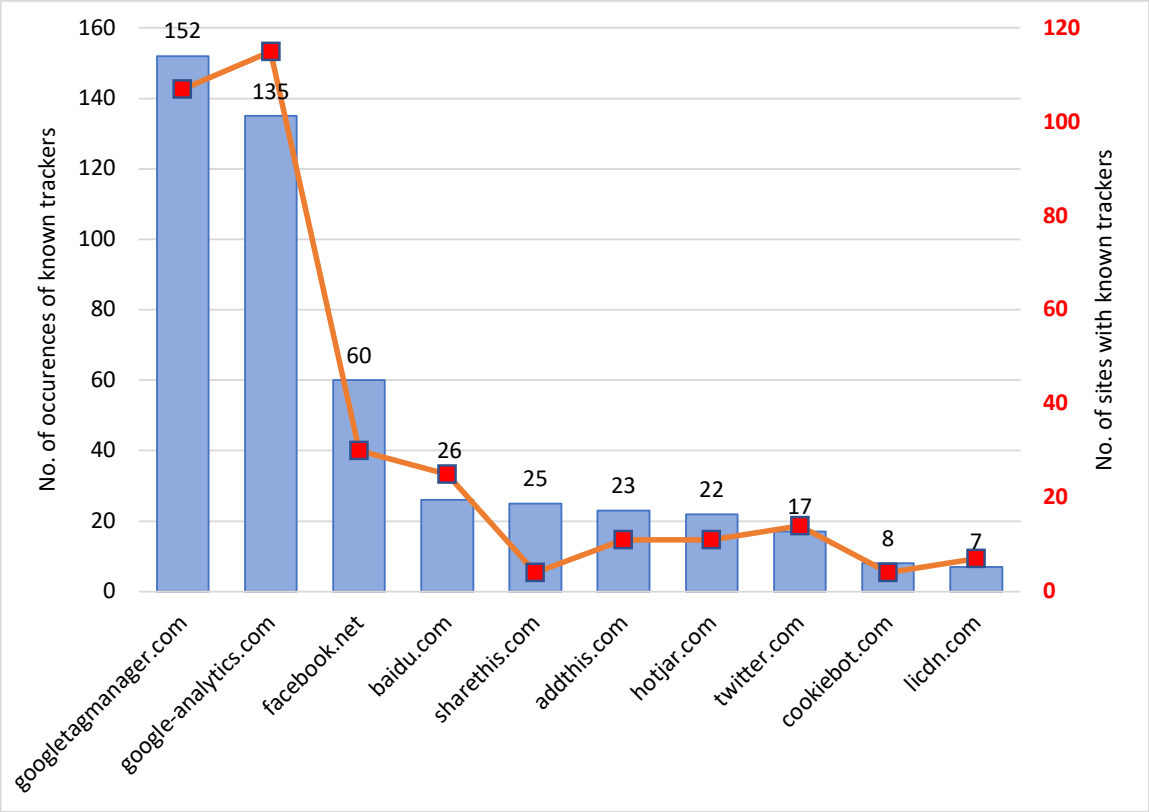

Figure 3: Top-10 known tracking scripts on victim support sites

Third-party hosts tracking users' operations. We also listed some 3rd-party hosts that track web pages victims browse and the keywords filled in the websites search functionality (if available); see Table 4. We found 7 hosts belonging to Google (www.google-analytics.com, www.google.ca, googleads.g.doubleclick.net, www.googleadservices.com, analytics.google.com, adservice.google.com, and ssl.google-analytics.com); 2 hosts

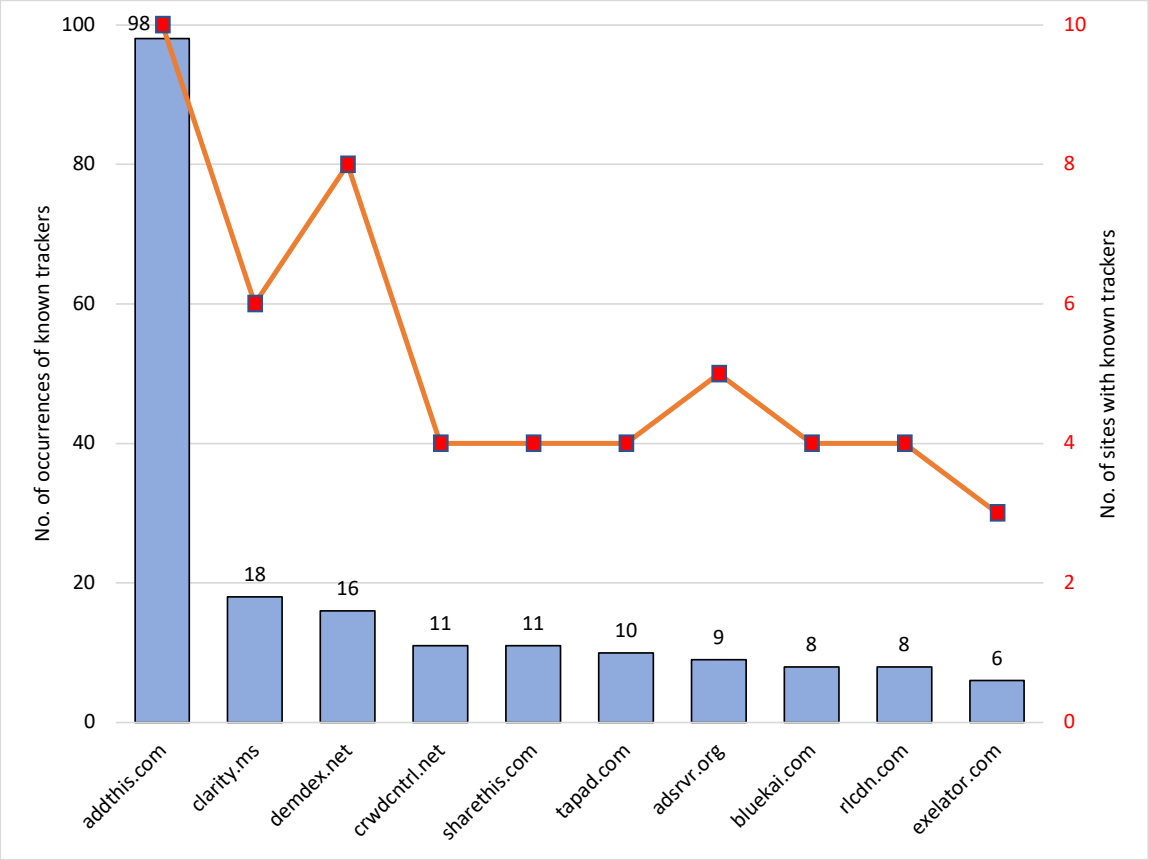

Figure 4: Top-10 known tracking cookies on victim support sites

owned by Twitter (syndication.twitter.com, analytics.twitter.com); and 3 Chinese hosts (hm.baidu.com, sp0.baidu.com, analytics.tiktok.com). We observed that hm.baidu.com and sp0.baidu.com only track Chinese websites while analytics.tiktok.com tracks 5 Canadian websites along with 1 South Africa website.

Online chat tracking. We noticed that the online chat service on three websites (diamondlaw.ca, lawyersuae.com, dubaipolice.gov.ae) tracked users. Diamondlaw.ca is a law firm with physical offices in Canadian provinces including British Columbia, Ontario and Alberta, which offers legal services related to stalking. The website employed chat-api.intaker.com for customer online chat service. However, the customer online chat

Table 4: Third-party hosts tracking users' operations in more than 10 different websites

Third-party Host	#Sites
www.google-analytics.com	130
www.google.ca	52
googleads.g.doubleclick.net	42
www.facebook.com	37
www.googleadservices.com	26
hm.baidu.com	25
www.youtube.com	23
analytics.google.com	15
syndication.twitter.com	13
m.addthis.com	11
px.ads.linkedin.com	11

service tracks the user's navigation through the website. Similarly, lawyersuae.com and dubaipolice.gov.ae, both UAE websites, use online chat services tracking the victims' page navigation (on their websites). Lawyersuae.com uses gateway.botstar.com for online chat while dubaipolice.gov.ae uses api.livechatinc.com.

We found that two Chinese websites for online legal support (user.maxlaw.cn and www.66law.cn) leak users' information to hm.baidu.com. Both websites claim that users do not need to worry about the information they provide, because all data is encrypted, so they can provide as much detailed information as possible for online legal support. Although user's sensitive data is encrypted, it is sent to hm.baidu.com without the user's consent through a tracking pixel with the url *hm.baidu.com/hm.gif*. The script from s.canddi.io tracks the functionalities of mailing list subscription and contact on www.suzylamplugh.org; as a result, victims' first name, last name, email, message title and message were disclosed to s.canddi.io. The website www.workspacesrespond.org

provides help to victims of domestic and sexual violence in the USA. All the private information filled in the contact web page (e.g., first/last name, email, organization, subject, message) is sent to the workspacesrespond server as well as to another non-profit organization (go.futurewithoutviolence.org), apparently another anti-violence organization; however, this information sharing is not visible to users.

Expiration of tracking cookies. We examined the validity duration of top-10 tracking cookies, and found that clarity.ms set cookies on 4 victim support websites were valid for more than 1000 years. Known tracking cookies that expire within 1 to 5 years were addthis.com (90), clarity.ms (4), sharethis.com (8) and adsrvr.org (9); see Table 5.

Table 5: The top-10 known tracking cookies and their expiry periods (m=month, y=year).

		Cookie Expiry Duration			
Tracker	**#Sites**	**<1m**	**1m-1y**	**1y-5y**	**>1000y**
addthis.com	98		8	90	
clarity.ms	18	6	4	4	4
demdex.net	16		16		
crwdcntrl.net	11		11		
sharethis.com	11	3		8	
tapad.com	10		10		
adsrvr.org	9			9	
bluekai.com	8		8		
rlcdn.com	8		8		
exelator.com	6		6		

Session replay. Session replay services are used to replay a visitor's session on the browser, to get a deeper understanding of a user's browsing experience; information replayed includes user interactions on a website such as typed inputs, mouse movements, clicks,

browsed pages, tapping and scrolling events. During this process, users' sensitive information can be exposed to 3rd-party servers that host session replay scripts. We identified 3 session replay services in the analyzed 323 victim support websites: Clarity on 6 websites (Canada (4), UAE (1), USA (1)), Hotjar on 9 websites (Canada (4), USA (3), South-Africa (1), UK (2), India (1)) and Yandex on 2 websites in Russia; see Table 6.

We found that 2 victim support websites in Russia expose victims' information to Yandex [40] session replay servers. One of the websites is wcons.net (i.e., the Consortium of Women's Non-Governmental Associations website), which provides legal support for victims of domestic violence in Russia. Users are asked to fill an online form for support; all the victims' sensitive information in the form is sent to Yandex, including, name, email address, phone number, year of birth, location, the presence of minor children, reasons to contact, who inflicts violence as well as a custom message. The other website, i.e., nasiliu.net provides legal assistance, psychological help and support to victims. We noticed that when victims use the website's search engine, searched keywords are collected by Yandex. Users' names and email addresses are also leaked through money donations; see Table 7. Note that safehorizon.org includes two session replay services: Hotjar and Clarity. Clarity initializes scripts from www.clarity.ms/eus-sc/s/0.7.2/clarity.js to track users' interactions with the DOM elements on a web page and the collected data is uploaded to o.clarity.ms. Hotjar uses web sockets to transfer collected data to ws4.hotjar.com. Both session replay services collect elements and web pages that users interacted with, as well as mouse events.

Table 6: Session replay services (SRS) on victim support websites

SRS	Websites
Yandx	wcons.net (Russia), nasiliu.net(Russia)
Hotjar	getsafeonline.org (USA), safehorizon.org (USA), onlineharassmentfieldmanual.pen.org (USA), domesticshelters.org (USA, CAN), canadianwomen.org (CAN), member.psychologytoday.com (USA), lawrato.com (India), mysupportspace.org.uk (UK), legalwise.co.za (South-Africa)
Clarity	legaladviceme.com (UAE), getsafeonline.org (USA), diamondlaw.ca (CAN) calgarydefence.com (CAN), ualberta.ca (CAN), lawcentralalberta.ca (CAN)

HTTP plaintext traffic. We observed that 4 websites use HTTP protocol for their core functions; these include connectnetwork.ca, www.tandemlaw.ca, www.alberta.ca and www.dfac.ae. On www.alberta.ca, users are required to fill in their email, first and last name, location data, gender and age group to create an online chat server account. However, the chat registration (provided by the 3rd-party domain m2.icarol.com), use HTTP, exposing all provided information to any on-path attacker. The online chat service (www.chat.dfwac.ae/Customer/Start) for the Dubai Foundation for Women and Children (DFWAC) used the HTTP protocol. Victims are required to enter name, email and questions before sending a chat request. Victims' sensitive information (e.g., name, email, questions, and chat content) is leaked because of the use of HTTP. We found that 72/120 (60.0%) of websites in China only support HTTP protocol, they however do not handle sensitive information (no sign-in or forms to fill).

The use of third-party services for core functionality. We observed two websites (safehorizon.org and rainn.org) in the USA using a 3rd-party service for the sign-up functionality. Safehorizon.org utilizes go.pardot.com for this functionality, consequently sending user's email address, first and last name to 3rd-party servers. We noticed that three websites in

Table 7: Sensitive information leaks in victim support websites

Website	Country	Leaked data	Feature	Destination	Cause
wcons.net	Russia	Name, email address, birthyear, phone number, location, minor children presence, custom message, name of the abuser	Report a crime	mc.yandex.ru	Session Replay
nasiliu.net		Keywords	Search		
		Name	Donate		
lawyersuae.com	UAE	Keywords	Search	botstar.com	Online Chat
dubaipolice.gov.ae				api.livechatinc.com	
diamondlaw.ca	Canada			chat-api.intaker.com	
suzylamplugh.org	UK	Name, email address	User Sign-in	s.canddi.io	Tracking
		Name, email address, phone number, job title, company name, custom message	Contact		
workplacesrespond.org	USA	Name, email address, company name, custom message	Contact	go.futurewithout-violence.org	
www.maxlaw.cn	China	Chat messages	Online Chat	hm.baidu.com	
www.66law.cn				hm.baidu.com	
www.dfac.ae	UAE	Name, email address, chat messages		www.chat.dfwac.ae	HTTP Plaintext
www.alberta.ca	Canada	Name, email address, location, gender, agegroup	Online Chat sign-in	m2.icarol.com	

Canada (canadianlabour.ca, iheartmob.org and www.kruselaw.ca) use a 3rd-party service during user sign-up, leading to victims' sensitive information being sent to the 3rd-party domain, instead of the website's domain. Consequently, on canadianlabour.ca, victims' first and last name, email address, phone number and location data are sent to actionnetwork.org; their first and last name, email address and country are also sent to the same address when asking for support on iheartmob.org.

Chapter 5

Privacy Analysis of Hidden Device Detection Apps

In this section, we discuss the static and dynamic analysis carried out on hidden device detection apps. Then we highlight the noticeable findings resulting from these analyses.

5.1 Analysis Methodology

5.1.1 App Collection

All the apps that are aimed at detecting hidden cameras and microphones are downloaded from Google Play Store. To download those apps, we searched keywords, like "Hidden Camera", "Hidden Microphone", downloaded a total of 93 apps related to detection of hidden cameras and hidden microphones, and saved them to our computer for later analysis. Then we manually checked whether they are apps really designed to detect hidden cameras

or hidden microphones or not, if not, we removed them from our data set. Also, we excluded apps that had less than 10K+ downloads. After this, we had 52 apps (i.e., 46 used to detect hidden cameras, 6 claimed to detect hidden microphones) left for our analysis. The downloads of the apps in our data set are from 10K+ to 5M.

5.1.2 Analysis Procedures

We performed a comprehensive privacy analysis on hidden device detection apps. Our examination encompasses various dimensions. Firstly, we interacted with the hidden device detection apps to identify what features/functionalities they provide and their mechanisms to detect hidden devices. Secondly, we examined the permissions the apps apply. We also examined the third-party libraries utilized by all the hidden device detection apps, along with their intended functions. Finally, we employed Burp Suite as a network proxy to intercept network traffic. This allowed us to detect instances of information leakage and identify their destinations. In addition, ThirdEye [31] was utilized to detect custom encryption. See Figure 5 for the analysis methodology of hidden device detection apps.

5.2 Results for Hidden Device Detection Apps

5.2.1 Features for Hidden Device Detection Apps

To determine the range of features provided to users, we sequentially installed and analyzed 52 hidden device detection apps. Through interactive usage, we explored their functionalities and documented our observations.

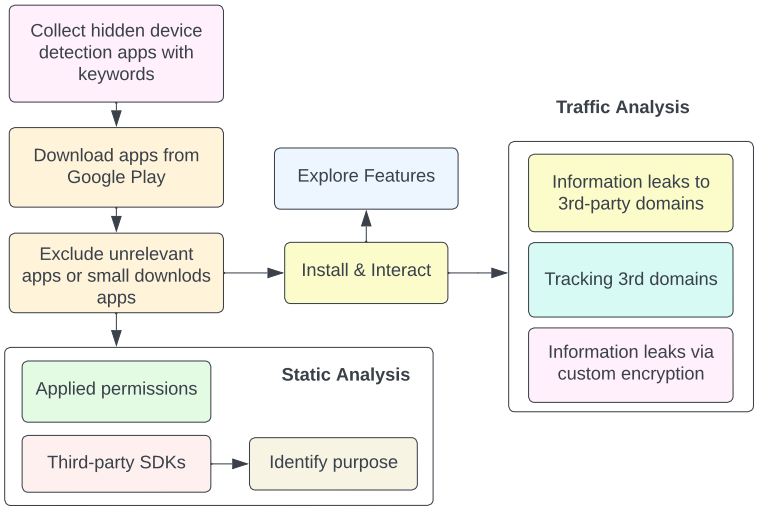

Figure 5: Methodology for hidden device detection apps

One app (com.closeupapps.hiddencamera.detectorelectronic.find) consistently experienced crashes upon our attempts, thereby hindering our ability to retrieve its features; another application (com.evezzon.intruderdetector) required users to establish screen lock and PIN/password, which could impede our subsequent automated testing, so this app was excluded from the feature experimentation. As a result, we obtained features for 50 out of 52 hidden device detection apps.

We categorized the (claimed) functionalities offered by the hidden device detection apps into three distinct groups: camera detection, microphone detection and hidden device/object detection. We did not evaluate the effectiveness of these apps nor confirm their claims.

Camera Detection. Regarding camera detection, these apps offer varying capabilities to identify different types of cameras, which include recording cameras, infrared cameras, WiFi cameras, wireless cameras, and more. Among the various camera detection functionalities, infrared camera detection stands out as the most prevalent feature, offered by 26 out

of the 50 apps. However, this functionality usually asks for permissions to open cameras to take pictures and record videos. After allowing apps to open cameras, they instruct users to look for green/blue light in the view which is invisible to naked eyes, which is an implication of the existence of infrared cameras. The detection of wired and wireless cameras is achieved through scanning network or WiFi.

Microphone Detection. We observe that 6 apps offer users the functionality to detect hidden microphones. Various mechanisms have been employed for detecting microphones. For instance, two apps (i.e., com.bettertomorrowapps.microphoneblockfree, com.frenzycoders.microphoneblockerantispyware) detect installed apps with microphone access. One app (i.e., com.protectstar.microguardfree) conducts storage scanning for microphone detection. Additionally, two apps state the ability to detect hidden recordings, while another app (com.fourtechsolutions.hiddenmicrophonedetectorbugdetectorscanner) claims to detect hidden microphones.

Hidden Device Detection. Hidden devices encompass hidden cameras, microphones, speakers, and similar devices. Therefore, the ability to detect hidden devices might extend to identifying hidden cameras and microphones. As a result, we compile a list of apps that offer the feature of detecting hidden devices (and not just hidden cameras or hidden microphones). Different apps provide distinct methods for detecting hidden devices. Common strategies for detecting hidden devices include utilizing graphs, meters, radiation measurement, calibration techniques, and sensor-based approaches. For instance, 7 apps use graphs to find hidden devices; 9 apps rely on meters for detection; 7 apps utilize radiation measurements for detecting hidden devices; 4 apps make use of sensors; and 1 app

integrates both graph and meter methodologies for hidden device detection.

5.2.2 Apps Permissions

We conducted a static analysis by using MobSF [18] to detect the permissions requested by the hidden device detection apps. We identified 16 distinct sensitive permissions and grouped them into 8 categories, such as Camera, Audio, Apps, Location, Storage, Settings, Account as well as State & Alerts.

Out of the 52 apps, 37 of them apply the permission of Camera to take pictures and record videos while 5 of them request the permission to record audios. Regarding the location access, among the 52 apps, 16 of them ask for permission to access GPS location, 15 apps request network-based location access, 2 apps apply for geographic location access, and 1 app request background location access. We identified two distinct permissions for accessing external storage: read external storage and write external storage. Among the 52 apps, 14 are found to apply for read external storage permission, while 17 apps request write external storage permission.

One app (com.evezzon.intruderdetector) applied the permission to manage the account list and use authentication credentials of an account at the same time. One app (com.fd.intruderselfie.thirdeye.intrudercatcher) requested permission to access running apps, as it performs checks on the installed apps to determine their malware status; 4 apps requested the permission to display system-level alerts; 8 apps requested to read the phone state. Refer to Table 8 for the applied permissions.

Table 8: Permissions applied by hidden device detection apps

Category	Sensitive Permissions	# Apps
Camera	Camera	37
Audio	Record audio	5
Apps	Retrieve running apps	1
Location	GPS location	16
	Network-based location	15
	Access location in the background	1
	Access geographic location	2
Storage	Read external storage	14
	Write external storage	17
Settings	Write global settings	2
Account	Manage account list	1
	Use authentication credentials of an account	1
State & Alerts	Display system-level alerts	4
	Read phone state	8

5.2.3 Security Levels

We performed a static analysis on the hidden device detection apps by using MobSF [18] to examine their security levels. The security levels are categorized into three tiers: LOW RISK, MEDIUM RISK, and HIGH RISK.

Among the 52 apps, 4 apps (com.findhiddencamera.detector, cn.ygl.antispy, com.hiddenglint.finder, com.glintfinder.hiddencamera) are evaluated as LOW RISK; 3 of them (com.lsc.hcd, hiddenCameraFinder2022[5], com.morinostudiodev.hiddendevicecameradetector) are classified as high risk apps; the remaining 45 apps are all evaluated as medium risk apps. The result of security levels and scores is showed in Table 9.

[5]com.hiddencameradetector.hiddencamera.hiddencamerafinder2022.spycameradetector.hidecamer

Table 9: The list of hidden device detection apps and their security levels & scores

APP	#DL	Version	Score	Security Level
hiddencamdetector.futureapps.com.hiddencamdetector	5M+	17	51/100	MEDIA RISK
com.faridahmad.hiddendevicesdetector	1M+	1.1.9	46/100	MEDIA RISK
com.wondertechstudio.hiddendevicedetectorandcameradetector	1M+	18.06.23	50/100	MEDIA RISK
com.faridahmad.hiddencameradetector	500K+	1.1.9	46/100	MEDIA RISK
com.fd.intruderselfie.thirdeye.intrudercatcher	100K+	1.1.8	50/100	MEDIA RISK
com.ender.spycamera	100K+	4.0.0	51/100	MEDIA RISK
com.evezzon.intruderdetector	100K+	1.0.37	50/100	MEDIA RISK
com.finder.cam.spydetector	100K+	1.0.4	50/100	MEDIA RISK
com.detect.camera.finder	100K+	1.0.3	50/100	MEDIA RISK
com.camerafinder.detectspycam	100K+	1.1.1	56/100	MEDIA RISK
com.freedetect.newdetectorapps2021	100K+	2.2.2	39/100	HIGH RISK
com.lsc.hcd	100K+	32	45/100	MEDIA RISK
com.lsdxdApp.camera_detector	100K+	5.1.8	51/100	MEDIA RISK
com.wondertechstudio.bugdetectorscanner	100K+	02.01.23	50/100	MEDIA RISK
com.hiddencameradetector.hiddencamera.hiddencamerafinder 2022.spycameradetector.hidecamera	100K+	1.8	39/100	HIGH RISK
com.icecube.hidden.spy.camera.detector	100K+	1.6	41/100	MEDIA RISK
com.monystudio.detectorhiddendevices	100K+	3.2.2	43/100	MEDIA RISK
com.royaltechapps.hiddencameradetector	100K+	1.6	50/100	MEDIA RISK
cn.ygl.antispy	50K+	1.0.1	61/100	LOW RISK
com.ahmadyar.all.objects.detector	50K+	6.43	45/100	MEDIA RISK
com.closeupapps.hiddencamera.detectorelectronic.find	50K+	1.1.8	50/100	MEDIA RISK
com.digapps.hiddencameradetection	50K+	2.0.1	41/100	MEDIA RISK
com.hiddencamera.detecthiddencam.tinycamera	50K+	1.0.2	44/100	MEDIA RISK
com.hiddencameradetectorpro	50K+	1.0.3	50/100	MEDIA RISK
com.hidden.camera.device.detector	50K+	1.1	50/100	MEDIA RISK
com.Krwtee.Hiddencamera.finder.hiddencameradetector. camerafinder	50K+	1	46/100	MEDIA RISK
com.toolszone.hiddendevicesdetector	50K+	1.8	43/100	MEDIA RISK
com.wondertechstudio.electronicdevicedetector hiddencameradetector	50K+	17.01.23	50/100	MEDIA RISK
com.zeehikitzon.hiddendevicesdetector	50K+	1.3.7	48/100	MEDIA RISK
com.apprise.hidden.camera.detector.hiddencamerafinder2021	10K+	1.0.3	50/100	MEDIA RISK
com.azp.hiddencamer.spy.device.detector	10K+	1.0.10	42/100	MEDIA RISK
com.findhiddencamera.detector	10K+	1.3.0	61/100	LOW RISK
com.glintfinder.hiddencamera	10K+	1.1	80/100	LOW RISK
com.hidden_camera_detector_app_spycam.spy_camera_detector_app_hiddencam_detectcamera	10K+	1.0.2	40/100	MEDIA RISK
com.hidden.camera.detector.plus.finder	10K+	2.2	46/100	MEDIA RISK
com.hiddenDevicesDetector.spyDevicesDetector. hiddenCameraDetector	10K+	1.3.23	50/100	MEDIA RISK
com.hiddenglint.finder	10K+	1.0.5	70/100	LOW RISK
com.hiennguyen.hiddencamera	10K+	3.1.5	51/100	MEDIA RISK
com.modernavatarapp.hiddencamerafinder.spycam.hidden cameradetector.hidecamera	10K+	1.9	40/100	MEDIA RISK
com.morinostudiodev.hiddendevicecameradetector	10K+	1.0.3	37/100	HIGH RISK
com.nixonahmi.hiddencamera.detectorelectronic.bugdetector	10K+	1.2.1	40/100	MEDIA RISK
com.spycameradetector.detecthiddencameradetection	10K+	08.05.23	50/100	MEDIA RISK
com.spyradar.detector	10K+	1.3.6	56/100	MEDIA RISK
com.twingleapps.hidden.spy.camera.detectorfinderapp	10K+	1.7	41/100	MEDIA RISK
com.smarteksg.hiddencamerapproplus	10K+	1.0.3	44/100	MEDIA RISK
hiddencamdetector.objectdetector.hiddencamdevicedetector	10K+	1.3	50/100	MEDIA RISK

5.2.4 Third-party SDKs

We performed static analysis with MobSF [18] to identify the third-party libraries used by the hidden device detection apps. The integrated third-party SDKs in the device detection apps can be categorized into four distinct groups according to their functions: analytics, advertising, identification, and notifications. There are 7 third-party SDKs designed for the analytic purposes, for example, Google Firebase Analytics, Google CrashLytics Crash Report, Facebook Share, Facebook Analytics, ironSource and Baidu Mobile Stat. A total of 10 third-party SDKs are imported for advertising, such as Startapp, Facebook Share, Google AdMob, Facebook Ads, AppLovin, Unity3D Ads, Yandex Ads, AppsFlyer, IAB Open Measurement, and AppMetrica. Apps integrate FacebookLogin for user identification purposes, while OneSignal is imported to push notifications to users. Refer to Table 10 for third-party libraries and the corresponding number of apps that integrate them.

5.2.5 Third-party Domains

In order to detect the third-party hosts to which the apps were connecting, we interacted with the hidden device detection apps manually and captured the network traffic by using Burp Suite. During our test, we noticed that 11 out of 52 hidden device detection apps did not initiate any HTTP/HTTPS connections; 41 out of 52 apps established HTTP/HTTPS connections.

By analyzing the intercepted HTTP/HTTPS requests, we detected a total of 88 unique hosts spanning across 45 domains, to which these apps were initiating their connections. Only one first-party domain (api.protectstar.com) in the app

Table 10: Third-party SDKs used in hidden device detection apps

Libraries	Purpose	# Apps
Google Firebase Analytics	Analytics	38
Google CrashLytics Crash Report	Analytics	7
Startapp	Analytics, Advertising	1
Facebook Share	Analytics, Advertising	4
Facebook Analytics	Analytics	4
ironSource	Analytics	3
Baidu Mobile Stat	Analytics	1
Google AdMob	Advertising	38
Facebook Ads	Advertising	19
AppLovin (MAX and SparkLabs)	Advertising	9
Unity3d Ads	Advertising	3
Yandex Ads	Advertising	1
AppsFlyer	Advertising	1
IAB Open Measurement	Advertising	9
AppMetrica	Advertising	1
FacebookLogin	Identification	4
OneSignal	Notifications	6

(com.protectstar.microguardfree) was identified; the remaining HTTP/HTTPS requests were all third-party domains.

It is apparent that the leading four domains are all under Google: doubleclick.net (35), googletagservices.com (21), googlesyndication.com (21), and google.com (15). DoubleClick is the largest provider of Internet advertising, which collects information about website visitors. Googletagservices.com is a domain owned by Google that is used for Google Tag Manager. The tag manager allows website owners to manage and deploy marketing and analytics tags on their website. Googlesyndication.com is a domain owned and operated by Google. It is primarily used for delivering targeted advertisements through the Google AdSense program. Googleadsservices.com is a domain for serving and tracking ads and other content on web pages through the iFrames, which is used in conjunction with Google Ads and Google AdSense networks to deliver targeted ads to users. The

main function of Facebook domains revolves around tracking. We have identified two distinct Facebook domains used for tracking purposes: namely, www.facebook.com and graph.facebook.com. Other third-party domains include liftoff.io, ctxtfl.com, adrta.com, unity3d.com, etc. Please refer to Figure 6 for the top third-party domains that are involved in hidden device detection apps.

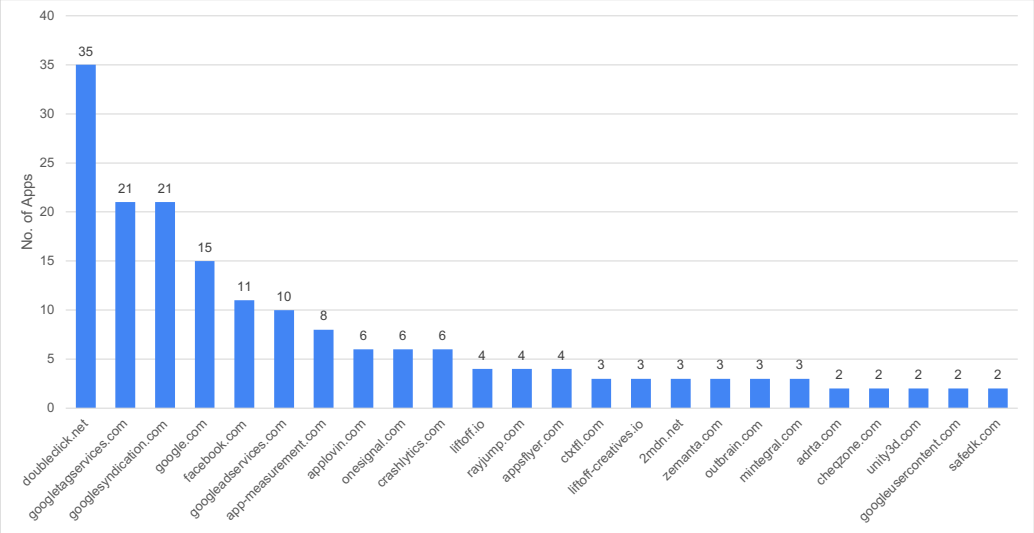

Figure 6: Domains to which hidden device detection apps established HTTP(s) connections

5.2.6 Information Leaks

Burp Suite was utilized to intercept the traffic, then we manually checked the header and body of HTTP/HTTPS requests to identify the information being sent to third-party domains.

Information Leaks by Domains. We noticed that googleads.g.doubleclick.net was gathering information such as submodel, locale, app_name, heap_total, and similar data. Similarly, android.apis.google.com was observed to collect information such as android_api_version, app_name, app_version, and firebase-app-name-hash. Information regarding the device (including details like manufacturer, model, battery status, available memory, rooted status, and whether it is an emulator), operating system (such as the OS and its version), network (like network type and carrier), and app (app_name, apk_name, app_version, apk_sdk_version) was observed being gathered by Facebook domains. Both www.facebook.com and graph.facebook.com were observed to collect the same set of data. It is important to highlight that the data of "is_emu" (indicating whether the app is operating within an emulator) was only identified as being collected by Facebook. In contrast, the data of "rooted" (signifying whether the device is rooted) was being collected by multiple entities, including Facebook, Unit3d and StartAppService. The device email was observed being transmitted to us20.api.mailchimp.com, likely due to its association with the subscription feature. Additionally, adid (i.e., Advertising Identifier) was observed being transmitted to 8 different domains. We listed the information leakages according to their domains in Table 11.

Table 11: Information shared with third-party domains

Host	#Apps	Collected Data
googleads.g.doubleclick.net	35	submodel, locale, app_name, heap_total, heap_free, heap_max
android.apis.google.com	11	android_api_version, app_name, app_version, firebase-app-name-hash
www.facebook.com	8	manufacturer, model, os, os_version, charging, battery, rooted, is_emu, locale, network_type, carrier, available_memory, is_debug, app_name, apk_size, app_version, build_type

graph.facebook.com	8	manufacturer, model, os, os_version, locale, battery, charging, rooted, is_emu, is_debug, carrier, total_memory, available_memory, app_name, apk_size, app_version, app_min_sdk_version, app_started_reason, build_type
app-measurement.com	8	os
api.onesignal.com	6	model, os, locale, adid, os_version, screen_size, app_name, app_publisher, app_sdk
us01.rayjump.com	4	adid
net.rayjump.com	3	manufacturer, model, app_version, country, locale, app_name, os, screen_size, network_type, user_agent
impression.appsflyer.com	3	adid, ip_address
fundingchoicesmessages.google.com	3	model, android_api_version, os, os_version, app_name, app_publisher, underage_consent
ctxtfl.com	3	app_name, android_api_version, heap_total, heap_free
android.clients.google.com	3	app_name, app_version, os_version, firebase-app-name-hash
httpkafka.unityads.unity3d.com	2	manufacturer, model, locale, os, os_version, android_api_version, screen_size, screen_brightness, app_name, apk_version, rooted, network_type, operator, total_memory, free_memory, camera_permission, user_agent
adrta.com	2	app_name, manufacturer, os, ip_address
publisher-event.unityads.unity3d.com	1	os_version, model, locale, os, android_api_version, adid, screen_density, screen_size, network_type, battery_level, battery_status, ad_permission
auction-load.unityads.unity3d.com	1	manufacturer, model, submodel, charging, screen_size, network_type, operator, adid, locale, timezone, app_name, app_version, battery_level, free_space, total_space
api.protectstar.com	1	token, pass, user
api.adapty.io	1	manufacturer, model, timezone, locale, os, os_version, adid, app_version, app_sdk_version
adx-tk.rayjump.com	1	manufacturer, model, os, os_version, adid, ip_address, app_name, app_version, user_agent
adsmetadata.startappservice.com	1	manufacturer, model, os, locale, rooted, is_debug, app_name, app_version, android_api_version, adid
trackdownload.startappservice.com	1	manufacturer, model, os, screen_size, locale, rooted, network_type, app_name, android_api_version

sdk-exchange.startappservice.com	1	manufacturer, model, locale, screen_size, rooted, is_debug, adid, app_name, test_-mode
conversions.appsflyer.com	1	app_name
events.mz.unity3d.com	1	os, os_version, country, province

Table 12: Information leaks detected by ThirdEye

Data	Channel	#Apps
Model	Https	8
	Http	3
	HttpsCrypt	1
Manufacturer	Https	15
DisplayID	Https	4
SIM Operator	Https	1
GPS	Https	2
Device Email	Https	1

Information Leaks Detected by ThirdEye. To identify potential information leaks via customized encryption channels, we utilized ThirdEye [31] as a supplementary tool for privacy analysis. In our test, ThirdEye successfully identified six distinct data (namely, phone model, manufacturer, display ID, SIM card operator, GPS, and device email) that were being leaked. The third-party domain (res1.applovin.com) was detected to collect the sensitive GPS information in 2 distinct apps (HiddenCameraDetector[6], SpyDetector[7]) via HTTPS channel. ThirdEye identified that the device email was transmitted to us20.api.mailchimp.com, this result aligned with our manual analysis findings. ThirdEye detected that phone model information transmitted through three distinct channels: HTTP (3), HTTPS (8), and HttpsCrypt (1). Table 12 shows the result of information leaks identified by ThirdEye.

[6]com.nixonahmi.hiddencamera.detectorelectronic.bugdetector
[7]com.hiddencameradetector.hiddencamera.hiddencamerafinder.spycameradetector.spycamera.hidden.spy.detector

Chapter 6

Readability Assessment of Privacy Policy

In this section, we outline the methodology employed and present experimental results pertaining to the readability assessment of privacy polices.

6.1 Privacy Policy Collection

Privacy Policy Collection of Websites. We conducted a manual examination of the landing pages of anti-stalkerware websites, actively searching for specific keywords such as "privacy policy", "privacy", "privacy statement", and "privacy notice". If there are any links leading to these keywords, we navigate to the respective web pages, extract the privacy policy descriptions, and store them on our host server. In the absence of privacy-related links, we proceeded by exploring keywords such as data protection and terms of use. We employed Google's translation service to render privacy policy statements into

English when they were not originally written in English. In total, we visited 323 anti-stalkerware websites, and managed to get privacy policies for 119 of these sites. The remaining websites either do not furnish privacy policies or were inaccessible during the time of our browsing.

Privacy Policy Collection of Apps. We conducted a readability assessment on the privacy policies of anti-stalkerware apps. In order to obtain these privacy policies, we deactivated the WiFi on the Android phone and engaged with the apps manually to locate the web pages containing the privacy policies. We were able to retrieve the URL addresses when encountering WiFi errors and inaccessible web pages. Subsequently, we accessed these URLs to extract and save the privacy policy content on our computer for future analysis. In certain instances, when unable to obtain the URL addresses of the web pages, we captured screenshots of the privacy policies, extracted the text from these screenshots by online tools, and then preserved the extracted content on our computer for subsequent analysis. By employing the aforementioned method, we managed to acquire the privacy policy of 20 anti-stalkerware apps; however, we cannot find privacy policy for the remaining 5 apps. Additionally, in cases where the privacy policy is not originally written in English, we utilized Google to translate the entire document into English. This translated version serves as the input for our readability test. See Figure 7 for the steps to obtain privacy polices on victim support apps and websites.

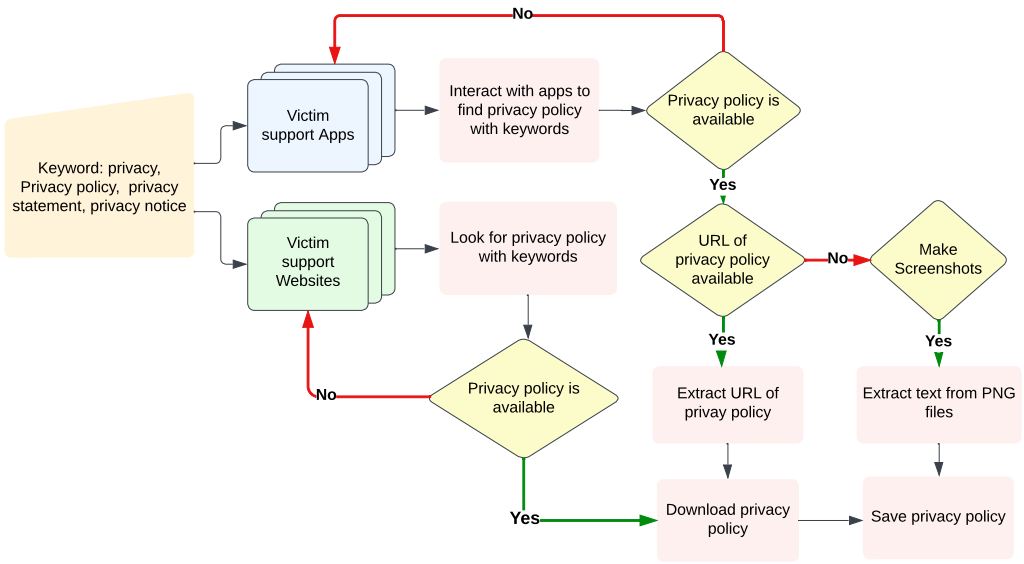

Figure 7: Procedures to obtain privacy policy on victim support apps and websites

6.2 Readability Assessment

Following the acquisition of the privacy policies, we proceeded to perform an analysis and evaluation on them. Readability Metrics [5] were employed to assess the clarity of the privacy policy descriptions. These metrics employ well-known readability formulas and measures, encompassing the Flesch Kincaid Grade Level, Flesch Reading Ease, Gunning Fog Index, Dale Chall Readability, Automated Readability Index (ARI), Coleman Liau Index, Linsear Write, SMOG, and SPACHE. We selected the Flesch-Kincaid Grade Level as our assessment metric for privacy policies due to its adoption by the U.S. Army for evaluating the complexity of technical manuals. Each metric generates a score, which is then used to categorize readability levels into classifications such as very_easy, easy, fairly_easy, standard, fairly_difficult, difficult, and very_confusing. Note that the readability grade levels are evaluated based on score ranging from 0 to 100. See Figure 8 for the methodology

of readability assessment on privacy policies

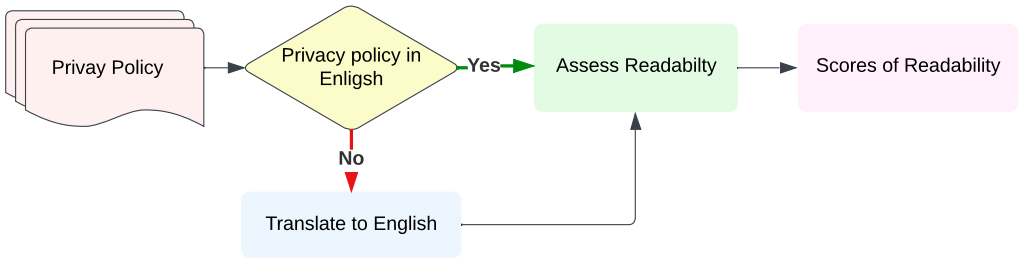

Figure 8: Privacy policy readability methodology

6.2.1 Anti-stalkerware Websites

We noticed that websites for victims support in China mainland do not provide any privacy policy statements. In total, we were able to obtain privacy policy for 119 out of 323 anti-stalkerware websites; the rest of them do not provide privacy policy on their websites or were not reachable at the time we did our experiments.

Among the 119 anti-stalkerware websites, the privacy policy in 37 websites are determined to be very confusing while 77 websites featured privacy policies are rated as difficult to comprehend; 5 websites fall into the category of fairly difficult readability. Surprisingly, none of the 119 websites contained the privacy policy is evaluated as standard, fairly easy and easy for users to read. Refer to Figure 9 for the readability result of anti-stalkerware websites.

6.2.2 Anti-stalkerware Apps

We manually interacted with 25 anti-stalkerware apps, and observed that 3 out of them do not provide privacy policy for users; one German app (i.e., de.weisser_ring.nostalk)

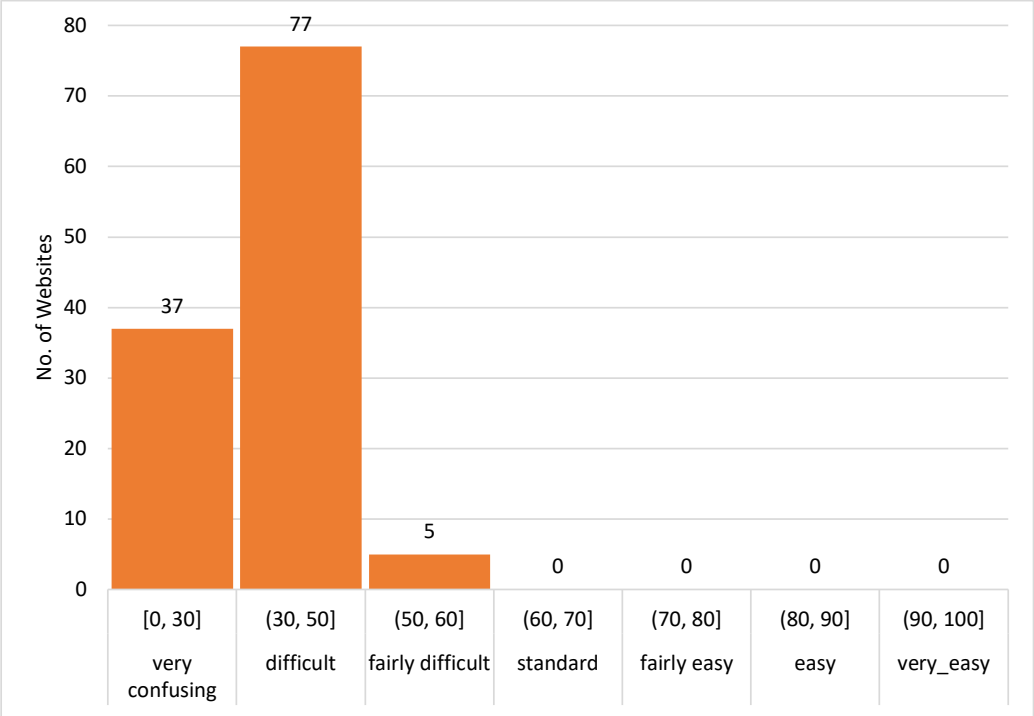

Figure 9: Readability results of anti-stalkerware websites

does offer privacy policy, however, it prohibits copying and making screenshot capture. Consequently, we successfully obtained privacy policy for 20 anti-stalkerware apps.

The privacy policy readability levels of the anti-stalkerware apps were categorized into two groups: very_confusing and difficult. It is apparent that among the 20 apps, 10 of them have privacy policies that are highly perplexing, while the remaining half of the apps provide privacy policies that are difficult to understand. Notably, the privacy policies of all Chinese anti-stalkerware apps (i.e., 6 Chinese apps) are uniformly categorized as very_-confusing as they received the lowest scores upon evaluation. This finding is coherent, given that the original privacy policies are written in Chinese. We initially translated them from Chinese to English before conducting the assessment on the English versions of the

privacy policies. 4 privacy policies originally written in English are evaluated as very_-confusing while 6 of them are deemed difficult to ready. We presented the readability assessment results according to the scores in Table 13.

Table 13: Readability results for anti-stalkerware apps

App	Readability	Score
com.jhsoft.antioverheard	very_confusing	5.5
com.yyyx.fjtws	very_confusing	6.3
com.txjjy.fjtjc	very_confusing	6.8
com.qznet.fjtgj	very_confusing	8.1
uni.uni1898b51	very_confusing	16.5
cn.lslake.fangjianting	very_confusing	15.8
com.protectstar.antispy.android	very_confusing	28.3
com.world.globle.mobileantistalker.rs	very_confusing	29.2
com.protectstar.antivirus	very_confusing	28.6
com.whotrackmyphonemhk	very_confusing	26.6
com.cbinnovations.antispy	difficult	30.0
com.arcane.incognito	difficult	36.8
com.foxbytecode.spywarescanner	difficult	37.1
com.mallocprivacy.antistalkerfree	difficult	37.3
com.certo.android	difficult	39.9
erfanrouhani.antispy	difficult	43.8
com.clevguard.guard	difficult	44.7
spyware.detector.remove.antihacker	difficult	45.1
com.owneffect.spyware.detector	difficult	48.3

6.2.3 Hidden Device Detection Apps

Among 52 apps, we successfully obtained the privacy policy for 26 of them. However, we were unable to acquire the privacy policy for the remaining apps due to three distinct reasons: 24 out of the 26 apps do not provide users with a privacy policy, one app requires a subscription prior to access, and one app encounters persistent crash. Consequently, we evaluated the privacy policies of the 26 hidden device detection apps. The readability of

these apps were evaluated into three levels: “very_confusing”, “difficult”, and “fairly_difficult”. None privacy policies in these apps could be categorized as easy to understand. Specifically, among 26 apps, 6 out of them provide privacy policies which are really confusing; 16 of them are deemed difficult to read; while 4 of them fall into the category of being fairly_difficult. See Table 14 for more details.

Table 14: Readability results for hidden device detection apps

App	Readability	Score
com.glintfinder.hiddencamera	very_confusing	28.1
com.bettertomorrowapps.microphoneblockfree	very_confusing	28.9
com.smarteksg.hiddencameraproplus	very_confusing	27.3
com.hidden.camera.detector.plus.finder	very_confusing	30.0
com.findhiddencamera.detector	very_confusing	29.2
hiddencamdetector.objectdetector.hiddencamdevicedetector	very_confusing	23.1
com.hidden.camera.device.detector	difficult	46.3
com.hiennguyen.hiddencamera	difficult	46.3
com.ender.spycamera	difficult	40.4
hiddencamdetector.futureapps.com.hiddencamdetector	difficult	34.7
com.lsc.hcd	difficult	35.9
com.toolszone.hiddendevicesdetector	difficult	48.2
com.foxbytecode.spywarescanner	difficult	37.1
com.finder.cam.spydetector	difficult	34.7
com.fd.intruderselfie.thirdeye.intrudercatcher	difficult	40.2
com.evezzon.intruderdetector	difficult	43.8
com.nixonahmi.hiddencamera.detectorelectronic.bugdetector	difficult	39.3
com.zeehikitzon.hiddendevicesdetector	difficult	42.3
com.apprise.hidden.camera.detector.hiddencamerafinder2021	difficult	42.5
com.monystudio.detectorhiddendevices	difficult	47.3
com.hiddencameradetector.hiddencamera.hiddencamera finder2022.spycameradetector.hidecamera	difficult	45.9
com.camerafinder.detectspycam	difficult	34.0
com.modernavatarapp.hiddencamerafinder.spycam.hidden cameradetector.hidecamera	fairly_difficult	50.5
com.frenzycoders.microphoneblockerantispyware	fairly_difficult	50.8
com.icecube.hidden.spy.camera.detector	fairly_difficult	51.5
com.freedetect.newdetectorapps2021	fairly_difficult	50.5

Chapter 7

Recommendations and Conclusion

In this section, we discuss our limitations, provide some recommendations for developers, stalking victims and service providers, and conclude the thesis by discussing future work.

7.1 Limitations

We summarize the challenges and limitations we encountered during our tests. (1) The scope of our study being centered around anti-stalkerware apps and websites reduces the size of the sample set used for testing. However, including more apps to our list would have resulted in covering less specialized tools and more general anti-malware apps. Our tests also do not compare anti-stalkerware apps with general anti-malware ones in terms of data privacy and detection effectiveness. (2) The small number of features provided by each app also limited the amount of tests that could be conducted. For instance, functionalities linked to user authentication and access control were only available on 4 of the apps. Even

though privacy issues related to trackers and PII leaks can be tested in practically any case, other related problems are very unlikely to be found in such tools. (3) Our anti-stalking app effectiveness analysis did not include tests for false-positives. Since the testing conditions only allowed for either true-positives or false-negatives, it is possible that some of the tested tools flag legitimate apps depending on the detection method they use. (4) The significant presence of advertising in hidden device detection apps makes test time-consuming. We manually performed information leak analysis on anti-stalkerware websites and hidden device detection apps, which is more accurate, but time-consuming. Moreover, our analysis of victim support websites was primarily focusing on privacy, we did not examine them from a security perspective.

7.2 Recommendations

In what follows, we provide recommendations for developers, stalking victims and service provider in the form of short questions and answers.

7.2.1 Recommendations for Stalkerware Victims

1. **How can I prevent stalkerware apps from being installed on my phone?** Keep your phone up close and under observation to prevent any unwanted person from accessing it and potentially installing malicious apps. Stay aware whenever someone else could have potentially used your phone, even with your consent. Use strong

passwords or PIN codes and avoid sharing them with other people to prevent unwanted use.

2. **How can I know if a stalkerware has been installed on my phone?** Watch out for potential indicators of compromise, including: abnormal (increased) battery consumption, unexpected pop-ups, performance drops, suspicious app duplicates or apps with seemingly important name ("Syncmanager", a second "Settings" apps), green dot icon at the top of the screen (indicating that the phone is recording), and any other strange behaviour from the phone. Regularly check that the Protect feature of Google Play is active. If disabled, this would indicate that someone have tampered with the phone. This feature can also be used to easily detect apps that were not downloaded from the Play Store. Keep the phone updated to its latest version, as many stalkerware apps could lose compatibility with newer system versions.

3. **I think my phone is being monitored by a stalkerware, what should I do?** If you observe any of the previously cited behaviors, or observe other proofs of a stalkerware being installed on your mobile device, seek help from a qualified organization or professional. Using a non-monitored device, you can find help materials related to your country on stopstalkerware.org, or on this Canadian government website for Canadian resources. Canadian crisis lines for intimate partner violence victims can be found on www.dawncanada.net – they are anonymous and reachable for free 24 hours a day.

7.2.2 Recommendations for Anti-stalkerware & Victim Support Website Developers

1. **How can solution developers increase effectiveness of their detection tools?** Solution developers should constantly test their detection apps against current versions of stalkerware apps to remain effective.

2. **How can solution developers and victim support websites improve privacy of their users?** Solution developers should not transmit data to 3rd-party services, especially sensitive information like device ID or GPS location. Solution developers should not include trackers for advertisements or user experience purposes in their apps. Solution developers should limit the required permissions needed to operate their apps (to avoid potential abuse) and explain to users why they need the permissions they ask. Victim support websites should avoid collecting browser data and keywords in the search functionality. Session replay services should not be used by victim support websites (or at least be configured not to send any user data to these session replay services). Detection apps and victim support websites must avoid using the HTTP protocol for any data transmission (which may lead to sensitive data leakage). Solution developers can also consider following the guidelines in the Platform for Privacy Preferences (P3P) Project[8].

[8] https://www.w3.org/P3P/

7.2.3 Recommendations for Service Providers

1. **How can we reduce the amount of stalkerware apps in circulation?** It is crucial to keep potential victims educated about the existence of stalkerware apps, and how to protect themselves against such tools. Awareness campaigns can be conducted through social media, school programs or community events to teach users how to prevent, avoid or detect early signs of stalking. Fighting against stalkerware websites (e.g., blocking) can also lower the amount of monitoring apps available online.

2. **How can operating system providers improve the situation for IPV victims?** Operating systems, such as Android OS can also play a role to reduce affects for victims. For example, enforcing PIN/unlock requirement for sensitive configuration updates (e.g., disabling Play Protect), warning users periodically that such changes have been made (e.g., once a day), and disabling blatant and constant information collecting apps such as stalkerware (almost no legitimate apps would behave the same way).

3. **How can payment/ad providers improve the situation for IPV victims?** Advertisement platforms such as Google Ads should establish clear policies or blacklists to detect and block advertisements on stalkerware websites, as well as content promoting such applications. Similarly, domain providers, and web hosting platforms have to effectively prevent access to malicious websites when reported. Payment and ad service providers should check the apps and websites before offering their services, to avoid aiding the stalkerware ecosystem.

7.3 Conclusion and Future Work

Anti-stalking Apps/Websites. The limited number of efficient anti-stalkerware app makes it difficult for users to rely on such tools. In addition, based on our experiments, more than half of the analyzed apps share sensitive data to other parties and use tracking services for advertising. Similarly, 65% of the websites dedicated to IPV victim support use 3rd-party trackers, with 8% of them collecting PII.

Hidden Device Detection Apps. Based on our experiments, it is evident that hidden device detection apps offer remarkably similar features. Device or app information were observed to be sent to third-party domains in 41/52 hidden device detection app. In addition, these apps embed tons of advertisements which appear immediately upon launching the apps, unfortunately, users are unable to bypass them. As for the effectiveness, our preliminary test shows that these apps are ineffective in detecting these hidden devices.

Future Work. The work in this thesis can be extended in three aspects in the future. Firstly, we only conducted the analysis for Android apps; future work can involve testing the corresponding iOS apps. Secondly, our primary goal in this thesis is to perform privacy analysis on victim support apps and websites; security analysis of victim support websites/apps can be conducted in the future. Lastly, regarding the readability assessment, we noticed that the readability libraries for translated privacy policies are not effective; hence, designing analysis tools for other languages (e.g., Chinese) can be another research direction.

Bibliography

[1] Almansoor, Majed and Gallardo, Andrea and Poveda, Julio and Ahmed, Adil and Chatterjee, Rahul. A global survey of android dual-use applications used in intimate partner surveillance apps. In *Proceedings on Privacy Enhancing Technologies Symposium*, Lausanne, Switzerland, June 2022.

[2] Ryan Amos, Gunes Acar, Eli Lucherini, Mihir Kshirsagar, Arvind Narayanan, and Jonathan Mayer. Privacy policies over time: Curation and analysis of a million-document dataset. In *Proceedings of the Web Conference 2021*, pages 2165–2176, 2021.

[3] Amelia Armstrong and Brianna Jaffray. Homicide in Canada. *Juristat: Canadian Centre for Justice Statistics*, 2020.

[4] Kelly Bracewell, Paul Hargreaves, and Nicky Stanley. The consequences of the covid-19 lockdown on stalking victimisation. *Journal of Family Violence*, pages 1–7, 2020.

[5] Carmine DiMAscio. py-readability-metrics 1.4.5, 2020. https://pypi.org/project/py-readability-metrics/#flesch-reading-ease.

[6] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. Sneaky spy devices and defective detectors: The ecosystem of intimate partner surveillance with covert devices. In *USENIX Security Symposium*, Anaheim, CA, USA, August 2023.

[7] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 441–458. IEEE, 2018.

[8] Chris Bluvshtein. The 20 Most Difficult to Read Privacy Policies on the Internet, 2022. online article (2022). https://vpnoverview.com/research/most-difficult-to-read-privacy-policies/.

[9] Mauro Conti, Giulio Rigoni, and Flavio Toffalini. Asaint: a spy app identification system based on network traffic. In *Proceedings of ARES '20*, pages 1–8, 2020.

[10] Cyber Security News. Popular Android apps with 142.5 million collective installs leak user data, 2021. online article (2021). https://cybernews.com/security/research-popular-android-apps-with-142-5-million-collective-downloads-are-leaking-user-data/.

[11] EasyList. EasyList, 2023. online article (2023). https://easylist.to.

[12] Echap. Stalkerware indicators of compromise, 2022. https://github.com/AssoEchap/stalkerware-indicators.

[13] Steven Englehardt and Arvind Narayanan. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 1388–1401, 2016.

[14] Steven Englehardt, Chris Eubank, Peter Zimmerman, Dillon Reisman, and Arvind Narayanan. Openwpm: An automated platform for web privacy measurement. *Manuscript. March*, 2015.

[15] Brett Eterovic-Soric, Kim-Kwang Raymond Choo, Helen Ashman, and Sameera Mubarak. Stalking the stalkers–detecting and deterring stalking behaviours using technology: A review. *Computers & security*, 70:278–289, 2017.

[16] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. Large-scale readability analysis of privacy policies. In *Proceedings of the international conference on web intelligence*, pages 18–25, 2017.

[17] Matthias Fassl, Simon Anell, Sabine Houy, Martina Lindorfer, and Katharina Krombholz. Comparing user perceptions of anti-stalkerware apps with the technical reality. In *SOUPS 2022*, pages 135–154, 2022.

[18] Github. Mobile security framework, 2023. https://github.com/MobSF/Mobile-Security-Framework-MobSF.

[19] Yufei Han, Kevin Alejandro Roundy, and Acar Tamersoy. Towards stalkerware detection with precise warnings. In *ACSAC*, pages 957–969, 2021.

[20] Carolin Ischen, Theo Araujo, Hilde Voorveld, Guda van Noort, and Edith Smit. Privacy concerns in chatbot interactions. In *Chatbot Research and Design, CONVERSATIONS 2019*, pages 34–48. Springer, 2020.

[21] Jarni Blakkarly, Daniel Graham. Privacy policy comparison reveals half have poor readability , 2022. online article (2022). https://www.choice.com.au/consumers-and-data/protecting-your-data/data-laws-and-regulation/articles/privacy-policy-comparison.

[22] Julian Evans. Why Third-Party Libraries Can Be a Privacy Headache and How To Minimise Their Risk, 2020. online article (2020). https://www.keywordsstudios.com/blog-how-to-minimise-risks-of-third-party-libraries/.

[23] KasperskyLab. Tinycheck, 2021. https://github.com/KasperskyLab/TinyCheck.

[24] Parmjit Kaur and Sumit Sharma. Spyware detection in android using hybridization of description analysis, permission mapping and interface analysis. *Procedia Computer Science*, 46:794–803, 2015.

[25] Engin Kirda, Christopher Kruegel, Greg Banks, Giovanni Vigna, and Richard Kemmerer. Behavior-based spyware detection. In *Usenix Security Symposium*, page 694, 2006.

[26] Barbara Krumay and Jennifer Klar. Readability of privacy policies. In *Data and Applications Security and Privacy XXXIV: 34th Annual IFIP WG 11.3 Conference,*

DBSec 2020, Regensburg, Germany, June 25–26, 2020, Proceedings 34, pages 388–399. Springer, 2020.

[27] Enze Liu, Sumanth Rao, Sam Havron, Grant Ho, Stefan Savage, Geoffrey M Voelker, and Damon McCoy. No privacy among spies: Assessing the functionality and insecurity of consumer android spyware apps. *Proceedings on Privacy Enhancing Technologies*, 1:1–18, 2023.

[28] Microsoft Clarity. Microsoft clarity, 2023. https://clarity.microsoft.com.

[29] Bureau of Justice Statistics. Stalking victimization, 2019. https://bjs.ojp.gov/library/publications/stalking-victimization-2019.

[30] OpenWPM. OpenWPM, 2023. https://github.com/openwpm/OpenWPM.

[31] Sajjad Pourali, Nayanamana Samarasinghe, and Mohammad Mannan. Hidden in plain sight: Exploring encrypted channels in android apps. In *Proceedings of the 2022 ACM SIGSAC CCS*, pages 2445–2458, 2022.

[32] Majdi K Qabalin, Muawya Naser, and Mouhammd Alkasassbeh. Android spyware detection using machine learning: A novel dataset. *Sensors*, 22(15):5765, 2022.

[33] Julie M Robillard, Tanya L Feng, Arlo B Sporn, Jen-Ai Lai, Cody Lo, Monica Ta, and Roland Nadler. Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Internet interventions*, 17:100243, 2019.

[34] Nayanamana Samarasinghe, Aashish Adhikari, Mohammad Mannan, and Amr

Youssef. Et tu, brute? privacy analysis of government websites and mobile apps. In *Proceedings of the ACM Web Conference 2022*, pages 564–575, 2022.

[35] Asuman Senol, Gunes Acar, Mathias Humbert, and Frederik Zuiderveen Borgesius. Leaky forms: A study of email and password exfiltration before form submission. In *USENIX Security Symposium*, pages 1813–1830, 2022.

[36] Mukund Srinath, Shomir Wilson, and C Lee Giles. Privacy at scale: Introducing the privaseer corpus of web privacy policies. *arXiv preprint arXiv:2004.11131*, 2020.

[37] L. Stefanko. Android stalkerware vulnerabilities, May 2021. https://www.welivesecurity.com/wp-content/uploads/2021/05/eset_android_stalkerware.pdf.

[38] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. "it's the equivalent of feeling like you're in jail": Lessons from firsthand and second-hand accounts of iot-enabled intimate partner abuse. In *USENIX Security Symposium*, Anaheim, CA, USA, August 2023.

[39] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. Abuse vectors: A framework for conceptualizing IoT-enabled interpersonal abuse. In *USENIX Security Symposium*, Anaheim, CA, USA, August 2023.

[40] Yandex. Yandex, 2023. https://metrica.yandex.com/about.

[41] Xiufen Yu, Nayanamana Samarasinghe, Mohammad Mannan, and Amr Youssef. Got

sick and tracked: Privacy analysis of hospital websites. In *2022 IEEE EuroS&PW*, pages 278–286. IEEE, 2022.

[42] Kaifa Zhao, Xian Zhan, Le Yu, Shiyao Zhou, Hao Zhou, Xiapu Luo, Haoyu Wang, and Yepang Liu. Demystifying privacy policy of third-party libraries in mobile apps. In *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*, pages 1583–1595. IEEE, 2023.