Current Research, Challenges, and Future Directions in Stalkerware Detection Techniques for Mobile Ecosystems

Mounika Bonam[a], Pranathi Rayavaram[b], Maryam Abbasalizadeh[c], Claire Seungeun Lee[d], April Pattavina[e] and Sashank Narain[f]

University of Massachusetts Lowell, Lowell, MA, U.S.A.

{*mounika_bonam, nagapranathi_rayavaram, maryam_abbasalizadeh, claire_lee, april_pattavina, sashank_narain*}*@uml.edu*

Keywords: Stalkerware, Android Surveillance Apps, Intimate Partner Violence (IPV), SoK.

Abstract: Stalkerware, a form of surveillance software misused for intimate partner violence (IPV), poses a growing threat to mobile ecosystems. Despite advancements in detection techniques, the development and usage of Stalkerware mobile apps continue to evolve, evading current tools and antivirus solutions. This Systematization of Knowledge (SoK) paper synthesizes existing research, focusing on static, dynamic, and ML-based detection methods for mobile platforms. Key insights highlight gaps in detection techniques, challenges in distinguishing dual-purpose apps, and the limited efficacy of antivirus tools. This paper provides an in-depth review of current efforts, limitations, and actionable insights to effectively address Stalkerware's persistent threat. Furthermore, it proposes recommendations for future research and collaboration among security companies, developers, and victim support services.

1 INTRODUCTION

Stalkerware, a type of surveillance software often exploited in intimate partner abuse and violence (IPV), has emerged as a growing security and privacy concern in mobile ecosystems. These applications allow abusers to clandestinely monitor victims' locations, communications, and activities—frequently without the victims' awareness. By 2025, an estimated 8.5 million people may experience technology-facilitated stalking, highlighting the urgent need for effective detection mechanisms (VPNRanks, 2021). Despite advancements in static, dynamic, and machine learning (ML)-based detection techniques, Stalkerware developers continue to outmaneuver detection tools and antivirus solutions. This challenge is particularly acute on Android devices, which are more vulnerable due to their open-source architecture and widespread adoption (Reisinger, 2022).

The psychological toll of Stalkerware on victims is profound, especially in IPV contexts, where it enables abusers to exert escalated levels of control. Victims often face significant barriers when seeking help, compounded by inadequate law enforcement training and support (Chatterjee et al., 2018). In 2019, 67% of technology-facilitated stalking victims reported fearing physical harm or death (Morgan et al., 2022), and 50% of cyberstalking incidents involved mobile applications (Kaspersky, 2021). While awareness of Stalkerware is growing, efforts to detect and prevent its use remain fragmented, complicated by dual-purpose apps and developers' evasion tactics.

This Systematization of Knowledge (SoK) paper addresses the escalating threat of Stalkerware by critically analyzing 104 studies. It identifies key gaps in detection techniques, explores developers' sophisticated evasion strategies, and assesses countermeasures. The paper examines the covert nature of Stalkerware and its challenges, offering actionable recommendations to improve detection technologies and response frameworks. Our findings underscore significant research gaps, particularly on Android, attributed to its open architecture and extensive user base. These gaps include issues with dual-purpose apps, limited detection capabilities, and inadequate victim support. The paper advocates for increased collaboration among researchers, developers, law enforcement, and advocates to protect victims better and combat this pervasive threat.

[a] https://orcid.org/0009-0008-2254-9113
[b] https://orcid.org/0000-0001-8375-7823
[c] https://orcid.org/0009-0004-6590-1683
[d] https://orcid.org/0000-0002-0355-8793
[e] https://orcid.org/0000-0003-2632-388X
[f] https://orcid.org/0000-0001-5377-3750

Bonam, M., Rayavaram, P., Abbasalizadeh, M., Lee, C. S., Pattavina, A. and Narain, S.
Current Research, Challenges, and Future Directions in Stalkerware Detection Techniques for Mobile Ecosystems.
DOI: 10.5220/0013371700003899

In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 1*, pages 405-415
ISBN: 978-989-758-735-1; ISSN: 2184-4356

This work makes two primary contributions: (1) a systematic review of 104 studies to evaluate Stalkerware detection methods, classify approaches in academia and industry, and identify critical gaps, and (2) an in-depth analysis of existing tools, emphasizing their limitations in handling dual-purpose apps and their susceptibility to evasion techniques such as code modification and obfuscation.

2 ANALYSIS OF STALKERWARE RESEARCH

This section reviews current research endeavors aimed at detecting and preventing Stalkerware in mobile ecosystems.

2.1 Study Selection and Focus Areas

We conducted a keyword-based search using terms such as 'stalkerware,' 'Android stalkerware,' 'iOS stalkerware,' 'Intimate partner violence stalkerware,' 'Intimate partner violence Android,' 'Intimate partner violence iOS,' and 'Mobile spyware' across ACM, IEEE, and Google Scholar databases, yielding 369 papers. Our review revealed that Stalkerware in the mobile ecosystem is a relatively new research area, with most studies published after 2017. The majority focused on Android, likely due to its widespread usage and open-source nature. While two papers briefly addressed iOS (Gallardo et al., 2021; Gallardo et al., 2022), no research exclusively focusing on Stalkerware in the iOS ecosystem was identified.

Given the rapid evolution of the Android platform and that approximately 95% of Android devices worldwide run versions released in the past eight years[1], we focused on research published after 2017 on Stalkerware in the Android ecosystem. This filter narrowed the list to 279 papers. Of these, 175 papers were excluded for being unrelated to Stalkerware, such as general Android security, IoT security, or Android malware detection techniques that may not apply to Stalkerware. To stay within scope, we concentrated on research explicitly addressing Stalkerware and conducted a detailed review of the remaining 104 papers.

Through the above-detailed review, we explored topics such as spyware, online abuse, cyberstalking, and Stalkerware, identifying key security challenges in the Android ecosystem. A subset of 67 papers explicitly focused on cyberstalking and Stalkerware apps were selected for deeper analysis. This subset provided critical insights into the prevalence of Stalkerware and revealed that much Android security research targets generalized spyware. By identifying patterns in the literature, we developed a systematic taxonomy detailed in Section 4.2. We also examined Stalkerware's role in IPV, its growth on Android, and the strengths and limitations of current research, and areas for improvement. Of the 67 papers, only 14 specifically focused on Stalkerware detection or prevention in the mobile ecosystem. These 14 papers, listed in Table 1, form the foundation of our insights, supplemented by the broader set of 104 papers.

2.2 Detection Methods for Stalkerware

This section explores research in three critical areas: (1) distinguishing Stalkerware from other apps, (2) detection techniques, and (3) evaluating tools for Stalkerware detection.

2.2.1 Identifying Stalkerware vs. Other Apps

This section reviews papers distinguishing Stalkerware apps from legitimate applications ('goodware') and other malicious software ('malware').

Pierazzi and co-authors utilized the 'koodous' tool to differentiate spyware from malware and goodware by extracting features through static and dynamic analysis (Pierazzi et al., 2020). They compared the performance of deep learning classifiers, such as Multi-Layer Perceptrons, Bernoulli Restricted Boltzmann Machines, and Convolutional Neural Networks, with traditional classifiers, including Random Forests, Decision Trees, Support Vector Machines, K-Nearest Neighbors, Naïve Bayes, and Logistic Regression. They proposed an Ensemble Late Fusion (ELF) architecture to improve accuracy, which combines predictions from multiple classifiers into a final decision. The study revealed that 50% of spyware samples requested the 'SEND_SMS' permission, compared to only 5% of goodware samples. Data for their analysis was sourced from VirusTotal[2].

Roundy's group explored the CreepWare ecosystem, identifying apps used for interpersonal attacks, harassment, and spoofing, including Stalkerware (Roundy et al., 2020). Their method leveraged the guilt-by-association principle, using a semi-supervised algorithm called CreepRank. Using a seed set of 18 overt apps identified by Almansoori's work (Almansoori et al., 2022), they performed bipartite graph analysis to find apps appearing on devices infected by these seed apps, leveraging Norton

[1] https://gs.statcounter.com/android-version-market-share/mobile/worldwide/

[2] https://www.virustotal.com/

Table 1: Efforts focused on Static and Dynamic Analysis, Machine Learning, and Manual Methods for Mobile Stalkerware.

Ref.	Title	Year	Static Analysis	Dynamic Analysis	Machine Learning	Manual Analysis
(Chatterjee et al., 2018)	The spyware used in intimate partner violence	2018	✓	✓	✓	✓
(Shan et al., 2018)	Self-Hiding Behavior in Android Apps: Detection and Characterization	2018	✓			
(Harkin et al., 2019)	The commodification of mobile phone surveillance: An analysis of the consumer spyware industry	2019	✓			
(Mendelberg and Nissani, 2020)	Understanding Technological Abuse: An Exploration Of Creepware	2020	✓		✓	✓
(Pierazzi et al., 2020)	A Data-driven Characterization of Modern Android Spyware	2020	✓	✓	✓	
(Roundy et al., 2020)	The Many Kinds of Creepware Used for Interpersonal Attacks	2020			✓	✓
(Han et al., 2021)	Towards Stalkerware Detection with Precise Warnings	2021	✓		✓	✓
(Gibson et al., 2022)	Analyzing the Monetization Ecosystem of Stalkerware	2022	✓	✓		✓
(Almansoori et al., 2022)	A Global Survey of Android Dual-Use Applications used in Intimate Partner Surveillance	2022	✓		✓	✓
(Qabalin et al., 2022)	Android Spyware Detection Using Machine Learning: A Novel Dataset	2022	✓	✓	✓	✓
(Fassl et al., 2022)	Comparing User Perceptions of Anti-Stalkerware Apps with the Technical Reality	2022	✓	✓		✓
(Liu et al., 2023)	No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps	2023	✓			✓
(Mangeard et al., 2023)	No Place to Hide: Privacy Exposure in Anti-stalkerware Apps and Support Websites	2023	✓			✓
(Mangeard et al., 2024)	WARNE: A stalkerware evidence collection tool	2024		✓		✓

antivirus data. They manually coded the top 1000 resulting apps into creepware categories, such as location tracking, keylogging, screen recording, message interception, and device control.

Shamsujjoha and colleagues introduced REACT (Reverse Engineering-based Approach to Classify mobile apps using The data that exists in the app), a method for classifying mobile apps without relying on descriptions (Shamsujjoha et al., 2021). REACT uses reverse engineering to extract features from method names, text, and XML data, applying topic modeling techniques to classify apps as malicious. However, the study acknowledges limited effectiveness, as the method was only tested on a small, specific dataset.

2.2.2 Research on Detection Techniques

This section explores research on stalkerware detection in the Google Play Store and related ecosystems, focusing on methodologies and findings.

Chatterjee's group conducted the first comprehensive study on the Intimate Partner Surveillance (IPS) spyware ecosystem (Chatterjee et al., 2018). Using a snowballing query approach with keywords like 'how to catch my cheating spouse,' they crawled Google, the Apple App Store, and the Google Play Store to identify spyware apps. A supervised machine learning model combining Logistic Regression (LR) with inverse regularization was developed to identify malicious apps by analyzing app metadata, descriptions, and permissions. Manual validation was then employed to eliminate false positives. The study revealed that antivirus solutions detected only 47% of IPS apps, underscoring their limited effectiveness and the challenges of identifying surveillance apps.

Building on this work, Almansoori's research surveyed the presence of dual-purpose apps across 27 countries and 15 languages (Almansoori et al., 2022). These apps offer legitimate functions, such as parental control or device tracking, but can be misused for stalking or monitoring without consent. The study revealed that 18% of such apps lacked English descriptions, and 28% were undetectable using English search queries. It also highlighted a critical gap in the Google Play Store's review process, which does not account for language differences, allowing abusers to exploit this loophole.

Liu's group analyzed 14 Android spyware apps, uncovering advanced covert monitoring techniques and critical privacy vulnerabilities (Liu et al., 2023). Similarly, Mangeard's team examined 25 Stalkerware apps, finding that 14 shared user information with third-party services via trackers, cookies, or session replay mechanisms (Mangeard et al., 2023). The same group later analyzed 50 apps to identify issues such as Personally Identifiable Information (PII) leaks and developed a tool called WARNE to identify these leaks (Mangeard et al., 2024). The apps they found exploit Android APIs to exfiltrate data, harvest credentials, bypass permissions, and evade de-

tection while accessing cameras or microphones and concealing their presence. Key privacy flaws include unencrypted data transmission, backend vulnerabilities, and poor data retention policies exposing victims' data even after account deletion.

From a different perspective, Gibson's team investigated the monetization strategies of Stalkerware developers by performing static analysis on apps labeled by the 'Coalition Against Stalkerware'[3] (Gibson et al., 2022). Their findings revealed that these apps rely heavily on ad libraries, primarily Google AdMob, and financial services like PayPal. Despite Google's anti-Stalkerware policies, the significant prevalence underscores the need for stricter enforcement and monitoring.

Finally, Qabalin's work focused on network traffic analysis to detect spyware behavior. They analyzed five prominent spyware apps—UMobix, mSPY, TheWiSPY, MobileSPY, and FlexiSPY—by generating three network traffic datasets: (1) devices without spyware, (2) devices with spyware installed, and (3) devices actively running spyware (Qabalin et al., 2022). Using these datasets, Random Forest classifiers were used to differentiate pre-infected behavior from post-infected behavior. The multi-class classifier achieved accuracy rates between 69.2% and 90%, while the binary-class classifier performed slightly better. However, the small dataset size limits its scalability and applicability in broader contexts.

2.2.3 Tools for Stalkerware Detection

This section examines tools designed to detect Stalkerware behaviors and evaluates the effectiveness of antivirus (AV) solutions in addressing this threat.

Han's group developed Dosmelt, a mobile app providing precise warnings about specific sensitive information accessed by apps (e.g., GPS, camera, microphone, call logs) (Han et al., 2021). Using app identifiers from customer devices via a security vendor, they collected app data from APKPure and Google Play. They developed a taxonomy of Stalkerware capabilities through inductive coding and manual analysis. Their semi-supervised active learning approach, combining Random Forest and extreme random trees classifiers, achieved 96% AUC, identifying hundreds of new Stalkerware apps later added to the 'Coalition Against Stalkerware' Threat List.

Shan's research team investigated Self-Hiding Behaviors (SHBs), a core characteristic of Stalkerware apps, and proposed detection methods (Shan et al., 2018). SHBs were classified into three types: hiding app presence (e.g., concealing icons), removing remote communication traces (e.g., blocking calls or deleting messages), and subverting system reminders (e.g., muting notifications or hiding alerts). Analyzing 9,452 Android apps through static analysis of byte code, XML, and API calls, they found that malware apps averaged 1.5 SHBs per app, compared to 0.2 SHBs for benign apps.

Building on this work, Baird's research enhanced SHB detection by employing dynamic analysis on 77 Android apps (benign and malicious) (Baird et al., 2019). They implemented tools such as AutoSHBHome, AutoSHBInstalled, and AutoSHBRunning to monitor the home screen, installed apps, and processes on an Android emulator via the Appium framework. While their approach enhanced SHB detection, it required manual validation to address false positives and negatives, limiting scalability.

Many stalking victims lack technical expertise and support and often rely on antivirus (AV) or anti-Stalkerware apps from the Play Store or the App Store as their first line of defense. Fassl's research analyzed how users select AV solutions by analyzing App Store reviews for two prominent anti-Stalkerware apps: 'Mobile Security and Antivirus' and 'Cleaner by Lookout' (Fassl et al., 2022). They identified key selection factors, including incident response, security notifications, app history, third-party recommendations, and comparisons with other apps. However, a cognitive UI walkthrough revealed significant gaps between user expectations and app performance, which could mislead victims. Static and dynamic analyses showed these apps mainly use block lists to identify malicious apps, a method vulnerable to Stalkerware's use of unconventional or dynamically generated package names for each installation.

2.3 Challenges and Research Gaps

Research on Stalkerware detection has yielded multiple valuable insights, but significant challenges remain, particularly when solutions are not integrated into the Android ecosystem. For example, methods proposed by Shan (Shan et al., 2018), Shamsujjoha (Shamsujjoha et al., 2021), Gibson (Gibson et al., 2022), and Pierazzi (Pierazzi et al., 2020) rely on analyzing APK files to detect malicious behaviors. While effective in controlled settings, this approach faces practical challenges due to the dynamic nature of the Google Play Store. With thousands of new or updated apps added daily[4], continuously downloading and analyzing every APK is infeasible, making it difficult to identify emerging Stalkerware or other malicious apps in real-time.

[3]https://stopstalkerware.org/

[4]https://www.statista.com/statistics/266210/

The work by Pierazzi's group (Pierazzi et al., 2020) offers useful insights into the similarities between spyware and Stalkerware, but it depends on datasets classified by VirusTotal, which may not always be current and accurate. Similarly, Han's Dosmelt system (Han et al., 2021) is hindered by a key assumption: that Stalkerware apps openly advertise their surveillance capabilities in their descriptions. As noted by Almansoori (Almansoori et al., 2022), this assumption holds only in certain cases. In many instances, app descriptions are either intentionally vague or completely absent (Shamsujjoha et al., 2021). Additionally, some apps serve dual purposes, such as "Find My Phone" functionality, which can be misused for stalking. As a result, detection approaches that rely solely on app descriptions are insufficient to identify Stalkerware apps accurately.

Another common challenge across the reviewed research is the need for manual analysis to verify whether detected apps are genuinely malicious (Roundy et al., 2020; Baird et al., 2019; Qabalin et al., 2022; Mangeard et al., 2023; Mangeard et al., 2024). For example, Roundy's research (Roundy et al., 2020) manually analyzed 1,000 apps to categorize them into different creepware groups. This process required selecting a representative seed set of apps, which is challenging in itself, as the seed set must cover the diverse range of Stalkerware behaviors (see Section 4.2). Such manual processes are labor-intensive and do not scale well in dynamic app ecosystems, such as the Android platform.

Despite the challenges, some efforts have demonstrated promising advancements. For instance, the SHB (Self-Hiding Behavior) detection mechanism developed by Shan (Shan et al., 2018) was later extended by Baird's group (Baird et al., 2019), who incorporated dynamic analysis to improve detection efficacy. By addressing a key characteristic of Stalkerware, SHB detection has become a valuable component in the broader effort to combat Stalkerware. However, its reliance on specialized tools and manual validation limits widespread adoption.

Employing ML methods for app analysis, as demonstrated by Han's work, also encounters significant limitations (Han et al., 2021). Challenges include ambiguities in keyword-based approaches, contextual variations, and the inherent difficulty of handling dual-use apps. Users can also circumvent keyword filters by employing synonyms or variations, further complicating detection. Moreover, relying solely on app titles and descriptions leads to incomplete coverage of potential indicators and increases the risk of false positives or negatives.

3 GOOGLE'S EFFORTS

This section evaluates Google's initiatives, focusing on Android's evolving permission model, Google Play Protect (GPP) architecture, and their effectiveness in mitigating Stalkerware threats.

3.1 Android's Permission Model

Our analysis of Google's initiatives begins with the security and privacy features introduced in Android versions starting from Android 6, which is used by over 95% of Android devices worldwide[5]. Table 2 summarizes these updates, emphasizing their relevance to addressing Stalkerware threats[6].

Android 6 introduced runtime permissions, allowing users to manage permissions individually and enhancing privacy control. Android 7–9 added geolocation restrictions, file-based permissions, and Android 9's CALL_LOG group to limit call record access. Android 9 also restricted background camera and microphone access to counter Stalkerware.

Starting with Android 10, privacy features increasingly restricted background data access and improved user awareness. Android 10 introduced the ACCESS_BACKGROUND_LOCATION permission for explicit background location requests and stricter CAMERA permissions to protect metadata. Android 11 added one-time permissions for temporary access to sensitive resources and automatic permission resets for unused apps, along with separate permissions for foreground and background data access.

Android 12 introduced a privacy dashboard for tracking app access to sensitive data and status bar indicators for microphone or camera use. Android 13 enhanced user control with granular media permissions and simplified permission revocation. Android 14 restricted background activities to limit unauthorized data collection and tightened oversight of accessibility service requests. Android 15 advanced these efforts with AI-driven detection to better identify and block malicious apps.

3.2 Google Play Protect (GPP)

Google introduced Bouncer in 2012, later rebranded as Google Play Protect (GPP) in 2017, as the primary defense against Potentially Harmful Apps (PHAs)[7] on

[5]https://gs.statcounter.com/android-version-market-share/mobile/worldwide/

[6]https://developer.android.com/guide/topics/permissions

[7]https://blog.google/products/android/google-play-protect/

Table 2: Overview of Android's security releases relevant to Stalkerware.

Android Version	Year	Security Release
Android 6	2015	• Run-time permissions model - Users can directly manage app permissions at run-time and grant or revoke permissions individually for installed apps.
Android 7	2016	• Geolocation data sharing is disallowed over an insecure network. • File-sharing between apps is disallowed by enforcing file-based permissions.
Android 8	2017	• A user should explicitly grant each permission to an app even if they belong to the same group of permissions.
Android 9	2018	• Restricted access to sensors like camera and microphone by apps running in the background. • Introduction of CALL_LOG permission group to restrict access to call logs.
Android 10	2019	• Users can allow an app to access location only while the app is running in the foreground. • Introduction of an ACCESS_BACKGROUND_LOCATION permission for apps requiring access to location data from the background. • Enforcement of CAMERA permission for accessing camera details and metadata.
Android 11	2020	• One-time permissions model enabling users to grant one-time permission to apps for accessing location, camera, or microphone. • Auto-reset app permissions that have not been used for a few months. • Apps requesting location from foreground and background should make separate requests for permissions.
Android 12	2021	• Microphone and camera access indicators appear in the status bar on apps access. • Introduction of privacy dashboard displaying app access of location, camera, or microphone.
Android 13	2022	• Developer downgrade permissions to revoke access to runtime permissions that were previously granted, either by the system or the user. • Granular media permissions by separating permissions to request access to different types of media.
Android 14	2023	• Limitations on background activities, reducing the potential for unauthorized data collection. • Enhanced oversight of apps requesting accessibility services limiting Stalkerware exploitation.
Android 15	2024	• Integrated advanced AI to detect and prevent the installation of known malicious applications.

Android devices. GPP offers on-device and cloud-based protection, scanning over a billion apps daily. It tests all Play Store apps for security and scans third-party downloads to detect PHAs.

Our analysis of GPP involved reviewing all publicly available documentation on GPP[8]. Based on these insights, we created a detailed workflow (see Figure 1) to illustrate GPP's operational processes, highlighting its strengths and limitations. When a developer uploads a new app to the Play Store, GPP performs an initial analysis using automated static, dynamic, and ML-based methods: (1) Safe Apps: Apps deemed safe are immediately published; (2) PHA Apps: Apps identified as PHAs are blocked from publication; and (3) Unclear Apps: Manual analysis is performed for apps with ambiguous results. An app is only approved if the developer has no history of malicious behavior and the app is not classified as a PHA. Data from this review process and inputs from sources like Play Integrity[9] and third-party reports are used to train machine learning models, continuously improving GPP's detection capabilities. However, as of this writing, no publicly available documentation details the specific implementation of Google's static and dynamic analysis methods or the architecture of its ML models.

For device-level protection, GPP uses the same ML models during daily or user-initiated scans to detect PHAs and notify users. If a PHA is detected from the Play Store, GPP automatically removes it, but users can override warnings for apps from third-party stores. These user actions are recorded as feedback to further refine GPP's ML models.

3.3 Analysis of Google's Efforts

Google has implemented several measures to regulate apps, emphasizing permissions and access control to limit sensitive information, such as location, camera, and microphone, particularly for background services. These efforts represent progress, including the removal of apps violating policies[10].

However, the growth of Stalkerware apps within the Android ecosystem persists. A key factor is the nature of IPS apps, often surreptitiously installed by perpetrators with physical access to the victim's device (Chatterjee et al., 2018). This access allows them to bypass Android's permission safeguards by granting permissions directly. Additionally, the Google Play Store permits certain tracking apps with legitimate purposes, creating dual-purpose apps that evade detection. Section 4.1 provides examples of such dual-purpose behavior in the current landscape of Stalkerware apps.

[8]https://developers.google.com/android/play-protect/

[9]https://developer.android.com/training/safetynet

[10]https://support.google.com/googleplay/android-developer/table/12921780

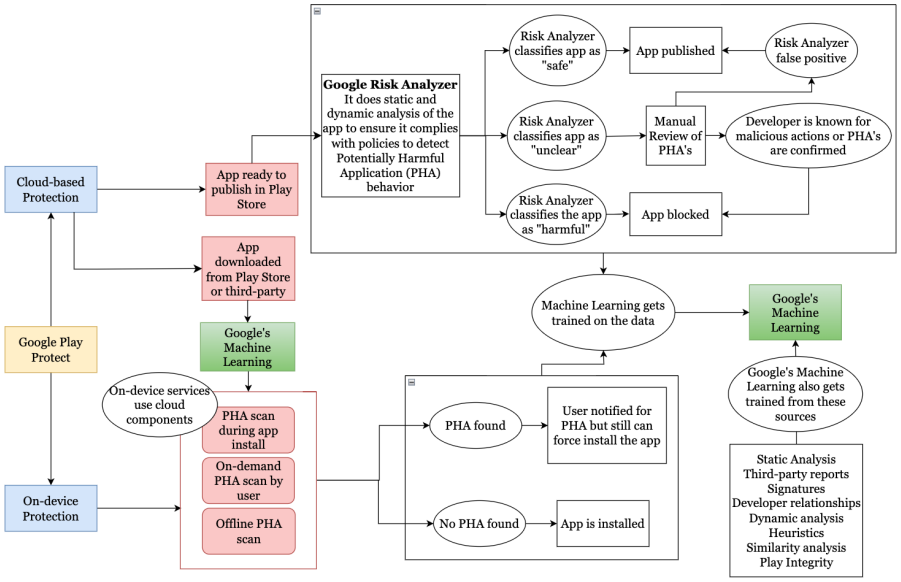

Figure 1: A high-level overview of Google Play Protect showing how Google uses Static Analysis, Dynamic Analysis, and ML techniques together to analyze apps for malicious behavior.

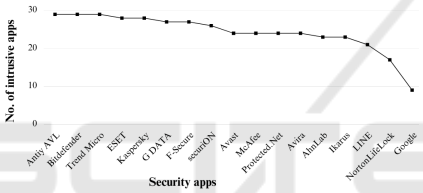

Figure 2: Detection of Stalkerware apps by Antivirus Solutions and Google Play Protect. The results highlight discrepancies in detection capabilities, with only three solutions detecting all Stalkerware samples.

GPP's ability to scan and remove malicious apps positions it as a key tool against Stalkerware, reflecting Google's history of policy enforcement (Chatterjee et al., 2018). However, its effectiveness is limited, with research showing gaps in reliability. A 2021 AV-Test lab study found that GPP detected only 31% of 29 Stalkerware samples (Figure 2)[11], while solutions like Antiy AVL, Bitdefender, and Trend Micro achieved complete detection.

Another study by Hutchinson's research group tested GPP with a spyware app designed to capture pictures, upload them to a database, and delete them from the phone (Hutchinson et al., 2019). Despite three scans over two months, GPP failed to detect the app. Other AV solutions fared slightly better; for instance, Avast detected the spyware only during a second scan after a month. The app, minimally described, remained available on the Google Play Store for four weeks before GPP removed it.

[11]https://www.av-test.org/en/news/stopped-in-its-tracks-stalkerware-for-spying-under-android/

The rapid rise of Stalkerware poses challenges to Google's ML-based detection, necessitating collaborative efforts among security firms, academia, advocacy groups, and law enforcement to address this threat in mobile ecosystems.

4 PRESENT STATE OF STALKERWARE APPS

This section presents our analysis of the current state of Stalkerware within the Android ecosystem. It examines trends in mobile Stalkerware alongside recent efforts and challenges (Section 4.1), explores the characteristics of the modern Stalkerware ecosystem (Section 4.2), and evaluates the effectiveness of AV tools in detecting and mitigating Stalkerware apps (Section 4.3).

4.1 Prevalence of Dual-Purpose Apps

Surveillance app developers have responded to Android's improved defenses by creating dual-purpose apps that seem harmless but can be misused for stalking, while stalkers increasingly exploit legitimate apps for tracking. Nearly 6–7.5 million individuals are stalked annually, with 2.7 million experiencing technology-based stalking (Morgan et al., 2022). Between 2016 and 2019, domestic violence cases decreased from 39% to 30%, while technology-facilitated stalking rose from 16% to 23% (Morgan et al., 2022). During the COVID-19 pandemic

(2020–2021), Stalkerware installations declined[12], yet global domestic violence rates increased from 25% to 33% (UN Women Data Hub, 2021; Boserup et al., 2020; Hsu and Henke, 2020; Su et al., 2022), with a 16% rise in first-time abuse cases reported in 2021 (Kourti et al., 2021). This suggests pandemic restrictions confined victims and perpetrators together, shifting abuse toward traditional methods over technology. However, this trend is likely to reverse as post-pandemic conditions enable greater access to technology for stalking.

Efforts by Chatterjee's group (Chatterjee et al., 2018) and Almansoori's group (Almansoori et al., 2022) prompted Google to remove apps that violated its Play Store policies. Similarly, Roundy's group (Roundy et al., 2020) and Han's group (Han et al., 2021) contributed significantly, with Roundy's responsible disclosure leading to the removal of 813 out of 1,095 reported apps. Our manual verification confirmed that Google has removed search results for explicit phrases like "track my wife's location" and "spy on my partner," yielding no related apps. However, alternative terms such as "get my wife's location" or "find my children" continue to bypass these filters, allowing similar results to appear. Surprisingly, searches for removed apps (e.g., Hoverwatch[13]) often yield similar apps, such as 'Eyezy – GPS Location Tracker'[14] or 'Find My Kids: Location Tracker'[15]. This suggests that Google's system may inadvertently cache information about removed apps, enabling stalkers to locate and install similarly capable dual-purpose apps on victim's devices.

Analyzing apps derived from the above search terms, we observed that their descriptions often appear benign, but user reviews for some seemingly harmless apps, such as 'Mobile Number Tracker: Find My,'[16] occasionally suggest potential misuse for stalking. Figure 3 highlights examples of reviews advertising Gmail addresses like 'KEVINHACKSPY01@gmail.com' and 'SPYWAREHACKER999@gmail.com' for cell phone tracking services. Using a guilt-by-association method to track similar apps, we identified at least eight apps with suspicious reviews, including 'Eyezy – GPS Location Tracker,' 'Mobile Number Tracker,'

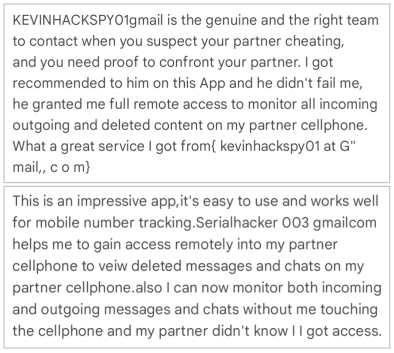

Figure 3: Examples of reviews on the Android app 'Mobile Number Tracker: Find My' indicating that the app can be used for stalking.

and 'Phone Tracker By Number'[17]. However, further investigation is necessary to confirm whether these apps enable stalking or if the reviews are fabricated. With dual-purpose apps posing increasing risks, developing new detection methods is crucial, especially as existing techniques improve against openly advertised Stalkerware.

We recommend that future research prioritize the analysis of network traffic (e.g., domain communication) and app metadata (e.g., user reviews) to combat Stalkerware apps. For instance, Qabalin's group publicly released network traffic data from the top five spyware apps, revealing communication with website logins used by attackers to collect user information (Qabalin et al., 2022). This finding highlights the potential of network traffic monitoring to detect Stalkerware, even if app code is modified (e.g., via package name changes). Since domain usage often remains consistent, network traffic analysis could be instrumental in identifying dual-purpose apps, emphasizing its importance for future research. Similarly, metadata analysis, including app descriptions, permissions, and user reviews, has proven effective in identifying misuse. Chatterjee and co-authors uncovered intrusive app use through app descriptions, prompting Google to remove several offending apps (Chatterjee et al., 2018). Our Play Store searches for terms like "see location of my wife" also revealed tracking apps with reviews advertising services via Gmail addresses, as discussed earlier. These findings reinforce the value of contextual analysis in enhancing Stalkerware detection.

4.2 Taxonomy of Stalkerware Apps

This section develops a taxonomy of Stalkerware based on our systematic review of 104 papers and

[12]https://news.harvard.edu/gazette/story/2022/06/shadow-pandemic-of-domestic-violence/

[13]https://play.google.com/store/search?q=hoverwatch&c=apps (Dec 2024)

[14]https://play.google.com/store/apps/details?id=com.eyezy.android (Dec 2024)

[15]https://play.google.com/store/apps/details?id=org.findmykids.app (Dec 2024)

[16]https://play.google.com/store/apps/details?id=com.panaromicapps.calleridtracker (Dec 2024)

[17]https://play.google.com/store/apps/details?id=com.loc.tracker (Dec 2024)

Figure 4: A summary of the characteristics of Stalkerware apps, the types of abusers and victims, the types of Stalkerware, and current techniques used by Android and research efforts to detect Stalkerware apps.

analysis of Google's protections (Sections 2 and 3). Depicted in Figure 4, the taxonomy highlights challenges faced by security companies, researchers, victim advocates, and law enforcement in combating Stalkerware apps[18]. While a comprehensive discussion of Figure 4 is beyond the scope of this work, we focus on the mobile ecosystem. Baraniuk noted that many Stalkerware apps are disguised as anti-theft tools, parental control apps, or family trackers, making their covert misuse difficult to detect (Baraniuk, 2019). Their self-hiding features further complicate detection, underscoring the need to address these factors for improved detection and mitigation strategies (Shan et al., 2018).

Our analysis of Stalkerware installation processes also provides actionable insights for improving detection strategies at different stages. Inspired by Chatterjee's research (Chatterjee et al., 2018), we conducted web scraping using Google search with keywords like "track call records," "Android Stalkerware apps," and "track husband apps Android." This yielded 506 URLs, filtered using a Python script to remove non-responsive links. After manual refinement, we identified 105 unique URLs, excluding antivirus tools, legitimate tracking apps, and informational websites. Of these, 51 required payment for trial versions, 30 had duplicate content, and 24 were tested in an emulated Android environment for further analysis.

Our findings reveal that many Stalkerware apps prompt users to disable Google Play Protect immediately after installation. Apps from external sources, such as AndroidMonitor[19], Copy9[20], Snoopza[21], and SpyLive360[22], frequently present variations with unique APK file names, app names, package names, and functionalities. These apps commonly disguise themselves under names like "system service" or "device admin" and request extensive permissions (e.g., location, media, call logs, contacts, network) upon installation, enabling perpetrators to grant all necessary permissions at once. Features like evidence deletion, icon changes, and app hiding are also prevalent. For instance, an app named 'Shadow-Spy' disguised itself as a calculator on our emulated device, accessible only by entering '#123.' These findings highlight the need for advanced static and dynamic analysis techniques to monitor permission requests and identify hiding strategies.

Once installed, Stalkerware apps gain admin access, conceal their presence, monitor victim activities, and transmit data to attackers. Although most apps do not require root access, they achieve similar control by requesting extensive permissions during installation. Many apps allow attackers to control the camera and microphone or take screenshots remotely. Fig-

[18]TFA (Technology-Facilitated Abuse), TF-IPV (Technology-Facilitated Intimate Partner Violence), TFDA (Technology-Facilitated Domestic Abuse), IPS (Intimate Partner Surveillance)

[19]https://www.androidmonitor.com/ (Dec 2024)
[20]https://copy9.com/ (Dec 2024)
[21]https://snoopza.com/ (Dec 2024)
[22]https://spylive360.com/ (Dec 2024)

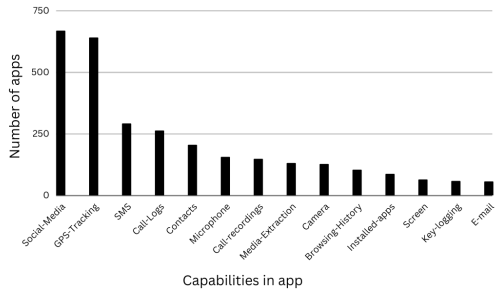

Figure 5: An analysis of the sensitive information Stalkerware apps seek to access (Han et al., 2021).

ure 5 lists these capabilities, aligning with observations by Han's research (Han et al., 2021).

After installation, users are typically directed to create an account on a website and link the device using a provided key. To test data collection frequency, we evaluated five apps by creating accounts and simulating a fake call to "555-555-5555" from an emulator. Within minutes, call details, location data, audio recordings, and screenshots appeared on the linked website, confirming the apps' tracking capabilities. Han's research similarly observed prevalent GPS tracking, social media monitoring, and SMS/call tracking across 1,462 apps (Han et al., 2021).

Our experiments also revealed that four popular Stalkerware apps[23] from different providers shared identical installation interfaces, likely due to a standard SDK library ('com.systemservice'). Despite variations in hiding and tracking features, these apps showed a shared lineage, suggesting possible ties to a parent company. To our knowledge, this finding has not been reported previously, highlighting the need for further research into SDK usage and its broader implications.

4.3 Limited Detection by AV Solutions

Our study reveals significant discrepancies in the detection accuracy of AV solutions for Stalkerware on Android devices. A 2021 AV-Test evaluation of 29 known Stalkerware apps using popular AV solutions highlighted substantial variations in detection rates (Figure 2). In May 2024, we conducted a similar experiment using 11 prominent Stalkerware samples, including NetSpy, FoneTracker, iSpyoo, and Spapp Monitoring[24]. Using VirusTotal to aggregate results, we found that Avast-Mobile[25] detected all 11 samples, while solutions like BitDefender[26] and QuickHeal[27] detected only some. Others, such as TrendMicro[28] and Malwarebytes[29], failed to detect any samples. These results illustrate the inconsistent detection capabilities of AV solutions and the potential risks for users relying solely on these tools for protection.

We further investigated the impact of minor modifications to APK file parameters, including changes to code, permissions, libraries, and package names, by creating a modified Stalkerware app using NetSpy as a baseline. Small adjustments, such as removing single permission from the manifest file or altering the package name, significantly declined detection rates. While an average of 20 AV solutions flagged the original APK files, only half detected the modified versions. These results reveal vulnerabilities in current AV solutions, where minor changes can evade detection, creating a false sense of security for users. This underscores the limitations of relying solely on AV tools to combat Stalkerware and emphasizes the critical need for collaboration and information sharing among AV providers to enhance detection consistency and protection against Stalkerware.

5 CONCLUSION

This SoK paper reviewed 104 research efforts and Google's initiatives to detect and prevent Stalkerware in mobile ecosystems. Our analysis found that Stalkerware remains a significant issue despite existing countermeasures. Additionally, victim services and law enforcement often lack the adequate tools to identify and gather evidence of Stalkerware, enabling abusers to exploit these technologies with minimal risk of detection or consequences.

REFERENCES

Almansoori, M., Gallardo, A., Poveda, J., Ahmed, A., and Chatterjee, R. (2022). A Global Survey of Android Dual-Use Applications Used in Intimate Partner Surveillance. *Proceedings on Privacy Enhancing Technologies*, 2022.

Baird, L., Shan, Z., and Namboodiri, V. (2019). Automated Dynamic Detection of Self-Hiding Behavior.

[23] https://www.netspy.net/ (Dec 2024), https://fonetracker.com/ (Dec 2024), https://ispyoo.com/ (Dec 2024), https://copy9.com/ (Dec 2024)

[24] https://www.spappmonitoring.com (Dec 2024)

[25] https://www.avast.com/en-us/free-mobile-security (Dec 2024)

[26] https://www.bitdefender.com/solutions/mobile-security-android.html (Dec 2024)

[27] https://www.quickheal.com/quick-heal-mobile-security/ (Dec 2024)

[28] https://www.trendmicro.com/en_us/forHome/products/mobile-security.html (Dec 2024)

[29] https://www.malwarebytes.com/ (Dec 2024)

2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW).

Baraniuk, C. (2019). The rise of stalkerware. *New Scientist*, 244.

Boserup, B., McKenney, M., and Elkbuli, A. (2020). Alarming trends in US domestic violence during the COVID-19 pandemic. *The American Journal of Emergency Medicine*, 38. https://www.ajemjournal.com/article/S0735-6757(20)30307-7/fulltext.

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., and Ristenpart, T. (2018). The Spyware Used in Intimate Partner Violence. *2018 IEEE Symposium on Security and Privacy (SP)*.

Fassl, M., Anell, S., Houy, S., Lindorfer, M., and Krombholz, K. (2022). Comparing User Perceptions of Anti-Stalkerware Apps with the Technical Reality. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association.

Gallardo, A., Kim, H., Kim, K., Leelamanthep, C., and Li, T. (2021). POSTER: Mobile Security Strategies and Usability Problems in IPV and Stalking Contexts. In *Proceedings of the USENIX Security Symposium*. USENIX, USENIX Association.

Gallardo, A., Kim, H., Li, T., Bauer, L., and Cranor, L. (2022). Detecting iPhone Security Compromise in Simulated Stalking Scenarios: Strategies and Obstacles. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. https://www.usenix.org/conference/soups2022/presentation/gallardo.

Gibson, C., Frost, V., Platt, K., Garcia, W., Vargas, L., Rampazzi, S., Bindschaedler, V., Traynor, P., and Butler, K. (2022). Analyzing the Monetization Ecosystem of Stalkerware. *Proceedings on Privacy Enhancing Technologies*, 2022.

Han, Y., Roundy, K. A., and Tamersoy, A. (2021). Towards Stalkerware Detection with Precise Warnings. *Annual Computer Security Applications Conference*.

Harkin, D., Molnar, A., and Vowles, E. (2019). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, Media, Culture: An International Journal*, 16.

Hsu, L.-C. and Henke, A. (2020). COVID-19, staying at home, and domestic violence. *Review of Economics of the Household*, 19.

Hutchinson, S., Zhou, B., and Karabiyik, U. (2019). Are We Really Protected? an Investigation into the Play Protect Service. *2019 IEEE International Conference on Big Data (Big Data)*.

Kaspersky (2021). Digital Stalking in Relationships What is stalkerware, and do people recognize it? https://media.kasperskydaily.com/wp-content/uploads/sites/86/2021/11/17164103/Kaspersky_Digital-stalking-in-relationships_Report_FINAL.pdf (Visited: 2024-11-02).

Kourti, A., Stavridou, A., Panagouli, E., Psaltopoulou, T., Spiliopoulou, C., Tsolia, M., Sergentanis, T. N., and Tsitsika, A. (2021). Domestic Violence During the COVID-19 Pandemic: A Systematic Review. *Trauma, Violence, & Abuse*.

Liu, E., Rao, S., Havron, S., Ho, G., Savage, S., Voelker, G. M., and McCoy, D. (2023). No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2023(1):207–224.

Mangeard, P., Tejaswi, B., Mannan, M., and Youssef, A. (2024). WARNE: A stalkerware evidence collection tool. *Forensic Science International: Digital Investigation*, 48:301677.

Mangeard, P., Yu, X., Mannan, M., and Youssef, A. (2023). No Place to Hide: Privacy Exposure in Anti-stalkerware Apps and Support Websites. In Fritsch, L., Hassan, I., and Paintsil, E., editors, *Secure IT Systems*, pages 18–36. Springer Nature Switzerland.

Mendelberg, P. and Nissani, D. (2020). Understanding Technological Abuse: An Exploration of Creepware. https://doi.org/10.7298/7szt-nz87.

Morgan, R., Truman, J., and Statisticians, B. (2022). Stalking Victimization, 2019. https://bjs.ojp.gov/content/pub/pdf/sv19.pdf (Visited: 2024-11-30).

Pierazzi, F., Mezzour, G., Han, Q., Colajanni, M., and Subrahmanian, V. S. (2020). A Data-driven Characterization of Modern Android Spyware. *ACM Transactions on Management Information Systems*, 11.

Qabalin, M. K., Naser, M., and Alkasassbeh, M. (2022). Android Spyware Detection Using Machine Learning: A Novel Dataset. *Sensors*, 22.

Reisinger, P. P. (2022). Through the Spying-Glass: Data Privacy Concerns Regarding Mobile Spyware Apps. *Boston College Intellectual Property and Technology Forum*, 2022. https://lira.bc.edu/work/ns/2a5b5a37-a3eb-4907-a980-beb4daba2ddc.

Roundy, K. A., Mendelberg, P. B., Dell, N., McCoy, D., Nissani, D., Ristenpart, T., and Tamersoy, A. (2020). The Many Kinds of Creepware Used for Interpersonal Attacks. *2020 IEEE Symposium on Security and Privacy (SP)*.

Shamsujjoha, M., Grundy, J., Li, L., Khalajzadeh, H., and Lu, Q. (2021). Checking App Behavior Against App Descriptions: What If There are No App Descriptions? *2021 IEEE/ACM 29th International Conference on Program Comprehension (ICPC)*.

Shan, Z., Neamtiu, I., and Samuel, R. (2018). Self-hiding behavior in Android apps. *Proceedings of the 40th International Conference on Software Engineering*.

Su, Z., Cheshmehzangi, A., McDonnell, D., Chen, H., Ahmad, J., Šegalo, S., and da Veiga, C. (2022). Technology-Based Mental Health Interventions for Domestic Violence Victims Amid COVID-19. *International Journal of Environmental Research and Public Health*, 19.

UN Women Data Hub (2021). Measuring the shadow pandemic: Violence against women during COVID-19. https://data.unwomen.org/publications/vaw-rga (Visited: 2024-10-22).

VPNRanks (2021). Cyberstalking statistics and trends. https://www.vpnranks.com/resources/cyberstalking-statistics/ (Visited: 2024-10-22).