Skill Permission Analyzer

Vineeth Dasi
vdasi@ncsu.edu
NC State University
Raleigh, North Carolina, USA

Akruti Sinha
asinha6@ncsu.edu
NC State University
Raleigh, North Carolina, USA

Kalyan Karnati
kkarnat@ncsu.edu
NC State University
Raleigh, North Carolina, USA

You can find the Skill Permission Analyzer tool on GitHub: Skill Permission Analyzer.

1 INTRODUCTION

In today's digital landscape, the pervasiveness of mobile applications has effortlessly knitted itself into the fabric of our daily lives. Mobile apps have become indispensable for everything from enhancing communication and social interactions to expediting commerce and entertainment. However, the increase in app usage has raised a new concern: the violation of user privacy. Many apps secretly collect massive quantities of user data, frequently without express knowledge, thus exposing users to hazards such as targeted advertising, profiling, and even unlawful surveillance.

Against this backdrop, our Android app appears as a proactive solution to the growing concerns about user privacy. With a focus on openness and user empowerment, our app aims to provide users with critical information about the privacy concerns associated with the apps they install and use. Our software seeks to empower users to make informed decisions about their digital privacy by allowing them to scrutinize their installed applications and comprehend the trackers and permissions sought by each.

1.1 Motivation

The impulse for the development of our Android application stems from three sources. First and foremost, we want to provide people with knowledge so they can navigate the digital realm with greater awareness. Users can make deliberate decisions about the apps they integrate into their digital lives by unraveling the complexities of the data gathering tactics used by various apps.

Second, we are motivated by a desire to protect consumers from the dangers of privacy-invading apps. Our software acts as a protective barrier, assisting users in avoiding potential threats to their privacy by casting light on programs that collect excessive data or utilize questionable tracking tactics.

Finally, we want to raise awareness about the various privacy concerns associated with mobile apps. We hope to instill collective attention about privacy dangers through education and enlightenment, establishing a community of users who are cautious and proactive in protecting their digital privacy.

As we delve into the complexities of our app's functionality, which is supported by the sophisticated Exodus Privacy platform, we go on a journey to not only improve user privacy but also to contribute to the greater conversation around app-related privacy problems.

2 RELATED LITERATURE/WORK

Having meticulously conducted an extensive literature survey and thoroughly analyzed the relevant existing works in the field, this paper endeavors to synthesize and build upon the existing Android Permission privacy risk and incidents and insights.

Android Permissions: Governing Access to Critical Device Functions: Android protects users by limiting applications' access to phone resources through permissions. These permissions are necessary for accessing sensitive resources like the camera, microphone, or call log. For instance, an application requires the `READ_CONTACTS` permission to access a user's phonebook. Initially introduced in Android 2.2, there are a total of 134 permissions defined.

User Evaluation: Trust and Privacy Considerations: Obtaining permissions involves a two-step process. First, developers declare the necessary permissions in a file packaged with the application. Second, users must approve these permissions during installation. Each application has its set of permissions reflecting its functionalities. Users evaluate these permissions

based on their trust in the application and personal privacy concerns. The official Android Market presents an installation page for all applications. The page includes a description, user reviews, and screenshots, leading to a final installation page displaying the application's requested permissions.

Privacy Threat in Android Apps: Research Findings: Android apps pose a significant privacy threat, according to the research, Google Play's Data Safety labels are untrustworthy, failing to expose what data apps collect and use. Stalkerware exploits Android vulnerabilities to steal sensitive information, while weak permission systems leave users with little control. The problem goes beyond individual apps, with insecure data handling practices and weak server-side controls creating systemic risks. To truly protect users, developers need to prioritize secure coding and data practices, users deserve better permission systems and accurate labels, and the industry needs to come together with regulatory frameworks to build a more secure and privacy-respecting mobile ecosystem.

TikTok Privacy Incident of 2020: Data Collection Allegations: The TikTok incident, which unfolded in 2020, raised significant concerns about user privacy and data security. The popular video-sharing app faced allegations and scrutiny over its data collection and handling practices. Reports emerged suggesting that TikTok was collecting extensive user data, including personal information and browsing history, and sharing it with third-party advertisers without transparent disclosure or explicit user consent. The concern escalated further due to TikTok's ties to China, raising apprehensions about the potential misuse or unauthorized access to user data. This incident underscored the critical importance of privacy in the digital age, highlighting how user data, if mishandled or shared without consent, can lead to severe breaches of privacy and potential exploitation. It emphasized the need for robust data protection measures, transparent data handling practices, and user consent mechanisms in applications to safeguard user privacy rights and prevent unauthorized data sharing that could compromise user security and autonomy. The TikTok incident served as a stark reminder of the pivotal role privacy plays in ensuring user trust, data security, and ethical use of personal information in the digital ecosystem. Similar incidents are happening daily, and it is essential that users know their rights to their data and the privacy and risks associated with each app they use.

3 PROPOSED RESEARCH

Our proposed research unfolds in a systematic manner, progressing through four distinct steps to comprehensively explore and develop insights into Exodus Privacy's privacy protection mechanisms and the practical application of their tools in Permission Analyzer.

Figure 1: Exodus Privacy

3.1 Understanding How Exodus Protects Your Privacy

The journey begins with a deep dive into Exodus Privacy's methodologies for safeguarding user privacy. This initial phase aims to unravel the intricate mechanisms employed in tracker and permission detection within mobile applications. Our focus here is on understanding Exodus's approach, utilizing heuristic analysis and pattern matching for tracker detection. Additionally, we aim to provide a nuanced understanding of how Exodus categorizes and assigns privacy risk levels based on the severity of identified trackers.

3.2 Making Exodus's Tools Work Together in Permission Analyzer

Building on the foundational knowledge gained, the second step involves the practical application of Exodus's tools within the context of Permission Analyzer. Here, our goal is to seamlessly integrate the Exodus API into the Permission Analyzer application. This integration will empower users with a tool that not only

displays and analyzes permissions requested by popular apps but also provides valuable insights into potential privacy risks associated with these applications. Key strategies include establishing a dedicated API client for efficient interaction and developing a user-friendly interface.

3.3 Survey and Reporting

Transitioning beyond technical aspects, the third step adopts a user-centric approach through surveys. This phase serves a threefold purpose: gauging users' awareness and choices regarding permissions, delving into users' concerns about specific permissions, and enabling a comparative analysis of user behavior across various types of applications. The insights gathered from user feedback in this phase are instrumental in shaping the user interface and functionality of the Permission Analyzer.

3.4 User Testing and Validation

To ensure the practical effectiveness and user-friendliness of the developed application, the final step involves a robust testing and validation methodology. This includes conducting user testing sessions with diverse user groups, utilizing moderated sessions for real-time observation and feedback. The implementation of the think-aloud protocol captures users' thoughts and reasoning as they interact with the application. Evaluation criteria encompass aspects such as ease of use, navigation, the application's effectiveness in identifying trackers and permissions, clarity of presented information, and overall user satisfaction. Through these four steps, our research aims to provide a comprehensive understanding of Exodus Privacy and deliver a reliable and user-friendly Permission Analyzer.

4 FINDINGS

The analysis of mobile application permissions, particularly those flagged by Exodus Privacy, has revealed critical insights into the potential privacy concerns associated with high-profile applications. This report delves deeper into the key findings, shedding light on the implications of permissions related to location, camera, microphone, contacts, storage, and calling. Additionally, it explores the results of user testing of the Permission Analyzer application, providing valuable insights into user experiences and suggestions for improvement. The report concludes with observations from a survey, offering a nuanced understanding of user preferences and behaviors concerning mobile application permissions.

4.1 Exodus Takeaways: Unveiling Privacy Concerns

4.1.1 Location Permissions. The ability of applications to access a device's location raises significant privacy concerns. Such permissions empower apps to track user movements, potentially compromising user anonymity. This finding underscores the need for users to be cautious when granting location access, especially considering the sensitivity of location data.

4.1.2 Camera and Microphone Permissions. Permissions to access the device's camera and microphone are flagged due to the potential for unauthorized recording or capturing of images and audio without user consent. This highlights the importance of users being vigilant about granting these permissions and the potential risks associated with unauthorized access to multimedia functionalities.

4.1.3 Contacts and Storage Permissions. Access to contacts and storage is flagged for its sensitivity, involving the retrieval and potential sharing of personal contact information and compromising personal data stored on the device. Users should be particularly mindful of granting these permissions, considering the implications for their privacy and data security.

4.1.4 Calling Permissions. Permissions related to the phone, including access to call logs, phone numbers, and device status, raise privacy concerns due to the potential for unauthorized access to sensitive information. This finding emphasizes the need for users to carefully evaluate and consider the necessity of such permissions when using applications.

4.1.5 Takeaway: The overarching takeaway from this comprehensive analysis is clear: user privacy is a multifaceted landscape that requires careful consideration from both users and developers. As highlighted by the Exodus findings, specific permissions carry inherent risks, urging users to exercise caution when granting access to sensitive functionalities.

4.2 User Testing and Validation: Unveiling the Effectiveness of Permission Analyzer

4.2.1 Ease of Use. The Permission Analyzer application received praise for its intuitive design and easy navigation. Users universally lauded the platform, contributing to a positive overall user experience. This commendation suggests that a user-friendly interface is crucial for the success and adoption of privacy tools.

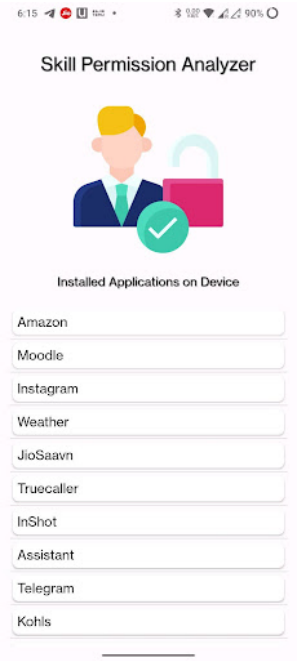

Figure 2: App Home Screen

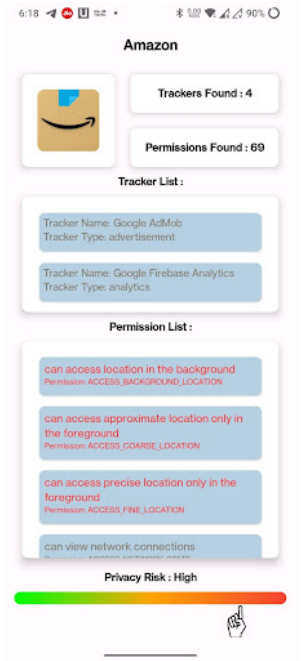

Figure 3: App Analysis

Figure 4: Skill Permission Analyzer

4.2.2 Effectiveness in Identifying Permissions. The tool's success in identifying a broad spectrum of permissions met or exceeded user expectations. Users appreciated the transparency it offered, providing insights into which entities were collecting data. This finding underscores the importance of transparency in privacy tools to build trust among users.

4.2.3 Areas for Improvement. While the majority of users had a positive experience, some suggested enhancements in notification features. Additionally, there was a request for more contextual information on specific trackers to enhance user understanding. These insights highlight the iterative nature of privacy tools, emphasizing the need for continuous improvement based on user feedback.

4.2.4 User Satisfaction and Engagement. Although the majority expressed satisfaction, a small percentage reported a lack of engagement with the tool, signaling a potential need for more personalized features to cater to diverse user preferences. This observation underscores the importance of customization options in privacy tools to accommodate varying user needs and preferences.

4.2.5 Takeaway: The positive user reception of the Permission Analyzer application indicates a growing awareness and demand for transparency in privacy tools. The call for improvements and customization features emphasizes the dynamic nature of user expectations, urging developers to adapt and refine their tools continually.

4.3 Observations From the Survey: Unveiling User Preferences and Behaviors

ClickHere to visit Survey.
Responses So far:39

4.3.1 Android vs. iPhone Preferences. The survey revealed differences in the approach to granting permissions between Android and iPhone users. Android users exhibited a more liberal approach, while iPhone users tended to be more cautious and restrictive. This observation as seen in Figure 5 highlights platform-specific variations in user behavior, emphasizing the need for tailored privacy recommendations.

4.3.2 Common Permissions and Varying User Preferences. Location, camera, and microphone permissions were consistently granted across various applications as seen in Table 1,Table 2 ,Table 3 indicating a commonality in user behavior. However, contacts and storage access permissions demonstrated more variability, suggesting a nuanced approach to these particular permissions. These variations underscore the complexity of user preferences regarding different types of permissions.

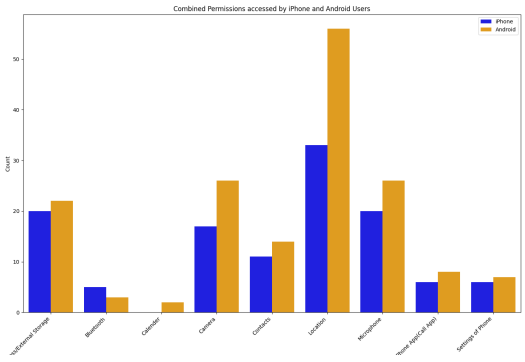

Figure 5: Combined Permissions accessed by iPhone vs Android Users

4.3.3 External Storage Access. Android users were more inclined to grant access to external storage compared to their iPhone counterparts as seen in Table 1,Table 2 ,Table 3 indicating platform-specific variations in user behavior. This finding has implications for developers and policymakers, emphasizing the need to consider platform-specific privacy norms and expectations.

Permissions	iPhone	Android
External Storage	5	6
Camera	5	4
Contacts	2	3
Location	12	24
Microphone	3	5

Table 1: Amazon App Permissions

Permissions	iPhone	Android
Bluetooth	5	3
Calender	0	2
Camera	12	20
Contacts	7	11
External Storage	9	10
Location	12	20
Microphone	12	19
Phone App(Call App)	6	8

Table 2: Instagram App Permissions

4.3.4 Takeaway: The survey observations, particularly the differences between Android and iPhone users, underscore the need for platform-specific considerations in privacy design. Understanding these variations can guide developers in creating more tailored and effective privacy solutions for diverse user bases.

Permissions	iPhone	Android
Camera	0	2
Contacts	2	0
External Storage	6	6
Location	9	12
Microphone	5	2
Settings of Phone	6	7

Table 3: Moodle App Permissions

4.4 Conclusion

In essence, the analysis emphasizes that while there is a commonality in certain user behaviors, the landscape of mobile privacy is nuanced and ever-evolving. This calls for ongoing collaboration between users, developers, and policymakers to strike a balance between technological convenience and safeguarding user privacy in the dynamic mobile ecosystem.

5 FUTURE DIRECTIONS

Several significant paths need research and expansion as we chart the road for the future development and refinement of our privacy-centric Android application. The following strategic directions demonstrate our dedication to continuous improvement and innovation:

(1) Diversification of App Focus: We acknowledge the need of broadening our analysis to include a more wide assortment of applications in order to broaden the impact of our application. We hope to provide users with complete insights into privacy practices across many domains by expanding our examination to a broader selection of apps.
(2) Enhanced Survey Diversity: Recognizing the value of user opinions, we want to broaden the scope of our user survey. A larger and more diverse participant pool will ensure a more nuanced knowledge of user behaviors and attitudes about permissions, which will aid in the improvement of our app's features and usability.
(3) Cross-Platform Development for iOS: As part of our commitment to inclusivity, we want to investigate cross-platform development for iOS. By making our software available to iPhone users, we

will be able to provide a more inclusive approach to privacy monitoring, appealing to a broader audience concerned about protecting their digital imprint.

(4) Integration with Privacy Tools - TrackerControl: We intend to integrate our application with privacy tools such as TrackerControl to strengthen user privacy and confidence. This open-source tracker analysis tool works by intercepting network traffic and cross-referencing it with a blocklist, which is consistent with our application's objective of providing users with a comprehensive shield against privacy violations.

(5) Expanding Tracker Library: As the environment of app-related threats evolves, we intend to increase our tracker library. This expansion will entail ongoing engagement with privacy-focused communities and organizations to identify and catalog new and hidden trackers, ensuring that our software remains at the cutting edge of privacy protection.

(6) Cross-Tool Synergy: We hope to explore synergies with complementary privacy tools and platforms in order to give users with a comprehensive privacy protection experience. Collaboration with initiatives that share our commitment to user empowerment and privacy will strengthen our collective effect in establishing a more secure digital ecosystem.

(7) Mitigation of present restrictions: Addressing our application's present restrictions, such as its exclusivity to Android and the confines of the Exodus database, will be a top focus. To overcome these restrictions, efforts will be made through technology advancements, new alliances, and continual refining in order to provide a more comprehensive privacy solution.

By embracing these future paths, we hope to not only strengthen the capabilities of our current application, but also to contribute constructively to the continuing conversation around digital privacy. We hope to empower people, increase awareness, and promote a digital ecosystem in which privacy is not only a right but a practical and secure reality through these strategic activities.

6 TEAM CONTRIBUTION

Task	Contributor(s)
Defined the scope and objectives of the research project	Vineeth, Kalyan, Akruti
Conducted a comprehensive literature review	Vineeth
Identified key social media platforms for analysis	Akruti
Analyzed default privacy settings on Instagram	Kalyan
Analyzed default privacy settings on X (Twitter)	Akruti
Analyzed default privacy settings on LinkedIn	Vineeth
Integrating Exodus API into Permission Analyzer	Vineeth, Akruti, Kalyan
Survey and Reporting	Kalyan
User Testing and Validation	Kalyan, Akruti, Vineeth

Table 4: Team Contribution

REFERENCES

[1] Gail Kaiser, Shiqi Zhao, et al. *Permlyzer: Analyzing Permission Usage in Android Applications. Proceedings of the 2021 26th International Conference on Engineering of Complex Computer Systems (ICECCS).*

[2] Mahmoud Hammad, Marwa Abdelmonem, et al. *Analysis of Android Applications' Permissions. 2020 International Conference on Computer, Information and Telecommunication Systems (CITS).*

[3] Aleksandar Markovic, Milos Krstic, et al. *Enhancing Android Application Security by Detecting Overprivileged Applications. Proceedings of the 26th ACM Symposium on Access Control Models and Technologies (SACMAT).*

[4] Zhaoshui He, Jiaqi Wang, et al. *Analysis of Android Applications' Permissions. ResearchGate.*

[5] TrackerControl, https://github.com/TrackerControl/tracker-control-android.

[6] Exodus Privacy, https://github.com/Exodus-Privacy/exodus.

[7] Alex Hern. *Android app with 50m downloads sent data to advertisers. The Guardian, 2013.*

[8] Taha Ghafoor, Hafsa Qaisar. *Privacy Issues of Android Application Permissions: A Literature Review. International Journal of Recent Technology and Engineering (IJRTE).*

[9] Federal Trade Commission. *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers. FTC, 2013.*

[10] Mohd Helmy Abd Wahab, Mohd Shahrizal Sunar, et al. *Permission-based Privacy Analysis for Android Applications. ResearchGate.*

[11] Ismat Waheed, Farheen Jalil. *Privacy Issues of Android Application Permissions: A Literature Review. ResearchGate.*