ESANN 2025 proceedings, European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning. Bruges (Belgium) and online event, 23-25 April 2025, i6doc.com publ., ISBN 9782875870933. Available from http://www.i6doc.com/en/.

Proactive Privacy Risk Assessment for Android Applications: A Machine Learning Based-Approach

Narjes Doggaz[1], Aissa Trad[1], and Hella Kaffel Ben Ayed[1]

1- University of Tunis El-Manar - Faculty of Sciences of Tunis - LIPAH Research Lab.
Campus Universitaire El-Manar, 2092 El-Manar Tunis - Tunisia

Abstract.
Mobile devices have become ubiquitous, collecting vast amounts of personal data through granted permissions. Privacy concerns arise when personal information is leaked to third parties without the user's awareness or consent. To address this issue, we propose a proactive approach based on a Machine Learning model to predict privacy risk scores for Android applications. These scores are based on the requested permissions and allow the users to be aware of the potential leakage of sensitive information before installing an application. Experimental evaluations demonstrate the competitive performance of our model against existing state-of-the-art methods.

1 Introduction

During the last few years, smartphones and mobile applications (apps) have constantly grown in number and importance in our daily lives. Mobile apps explicitly request permission grants to access resources or information, such as internet, device ID, user accounts, contact lists, etc. Privacy concerns arise when personal information is leaked to third parties. Data aggregation permits learning more about the users without their awareness and consent. To address online privacy violations, governments set up recommendations and laws such as EU General Data Protection Regulation (GDPR) and encourage private companies to develop certifications such as Certified Information Privacy Professional (CIPP). Furthermore, since smartphones have become the digital hubs of our interests, activities, connections, and a portal to our identity, we strongly need to safeguard privacy and protect data from fraudsters and unscrupulous entities. Android permissions scan schemes have a critical role in combating unwanted behavior of untrusted Android apps in terms of security and privacy. Researchers conducted multiple studies to address mobile in-application tracking. This paper addresses this issue and proposes a Machine Learning (ML) model that proactively predicts privacy risk scores for Android apps.

The remainder of this paper is organized as follows. Section 2 summarizes the related works. In section 3, we present the proposed ML approach for privacy score prediction. A comparative study is detailed in section 4. Lastly, we conclude the paper and sketch some ongoing work.

ESANN 2025 proceedings, European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning. Bruges (Belgium) and online event, 23-25 April 2025, i6doc.com publ., ISBN 9782875870933. Available from http://www.i6doc.com/en/.

2 Related works

Various studies focus on privacy risk assessment for Android applications. According to their underlying mechanisms, we classify these approaches into four categories: natural language processing approaches, network traffic-based approaches, dynamic analysis-based approaches, and risk estimation-based approaches. This paper focuses on risk estimation approaches that evaluate privacy risks from a user-centric perspective. These approaches assign a numerical score to each app based on the permissions it requests, providing a quantitative assessment of its privacy risk.

Hamed and al. propose in [1] a dynamic scoring model to estimate the privacy risk of applications upon installation. The parameters of the proposed model are the severity and the relative importance of permissions and their interactions. Permission severity is estimated according to the Expression of Needs and Identification of Security Objectives (EBIOS), while the relative importance of permissions is assessed according to the Analytic Hierarchy Process (AHP). The limitation of this model is the limited set of permissions and its inability to differentiate between permissions requested for application functionality and those intended for data disclosure. To explore the question "*Is mobile privacy getting better or worse over time* ?", Ren et al. [2] conducted a longitudinal study of the privacy implications of Android apps across multiple versions. The authors analyzed various versions of 512 popular Android apps, covering 7,665 app releases over 8 years. They constructed a network traffic dataset with Personally Identifiable Information (PII) labels and defined metrics to quantify privacy risk. The privacy risk metric is calculated based on PII Leaks, transport Security (HTTP and HTTPS traffic), and communication with first and third Parties. The resulting score is a continuous value ranging from 0 to 6, with 6 representing the highest level of privacy risk. In [3] the authors present PRADroid a privacy risk assessment framework for Android applications. To evaluate the privacy risk score, the authors define a risk matrix that combines two scores: the likelihood and the severity of privacy leakage. PRADroid uses an ensemble of five ML classifiers to predict the likelihood score. Then, it applies the voting principle to determine the likelihood score. The severity score assessment is based on information flow analysis. Hatamian and al. present in [4] FAIR a fuzzy logic-based approach for privacy risk assessment in smartphone apps. The privacy risk score is calculated by considering the type and frequency of app resource access. FAIR provides users with a privacy score that indicates the level of app invasiveness. In [5], the authors explore various risk-scoring methods based on app permissions and propose a framework incorporating rarity-based risk signals and probabilistic models. Their evaluation on real-world datasets demonstrates the effectiveness of the Rarity Based Risk Score with Scaling (RSS) method, demonstrating its ability to provide both clarity and robust performance.

Most of the presented approaches rely on the assessment of private data leakage risk. They consider that the risk increases with the number of permissions, with the gravity of these permissions, and with permission combinations within

ESANN 2025 proceedings, European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning. Bruges (Belgium) and online event, 23-25 April 2025, i6doc.com publ., ISBN 9782875870933. Available from http://www.i6doc.com/en/.

a single application. However, we notice that these approaches lack prediction in the risk score assessment. Prediction could help regular Android users to be informed accurately about the level of danger of an Android application. To overcome this problem, we investigate the use of a machine learning model for privacy risk score prediction of Android applications.

3 A Machine Learning Model for privacy score prediction

We propose using ML approaches to predict the privacy risk score of Android apps. To this end, we test four well-known algorithms that are: Support vector regression (SVR) , Multi-layer perception (MLP), Gradient Boosting (GB) , and Extreme Gradient Boosting (XGB).

Our dataset is constructed from the dataset introduced in [2], which includes historical versions of 512 popular Android apps, covering 7,665 app releases. It is a dataset of network traffic generated by running apps along with labels describing the PII contained in them. The applications have already leaked user data and have a calculated privacy risk score [2] ranging from 0 to 6. From this dataset, we downloaded the 440 available Android apps. For the model validation phase, we randomly selected 10 applications. The remaining 430 apps, and all their available versions, were used to construct our dataset: "*AppVersions-Dataset*". *AppVersionsDataset* comprises 1,679 apps, each treated as a distinct application.

The features of our datasets are the Android permissions. We selected 300 of the most commonly used permissions [1][2] among all Android apps and excluded those that don't appear in the apps of our dataset. We obtained 119 features. The features' values are binary: 1 if the given permission is requested, 0 otherwise. To enhance our models and improve their results, we added five features that we consider relevant to privacy. These features are: a) the number of permissions requested by the application, b) the number of activities within the application c) the number of services used by the application, d) the number of providers, and e) the number of receivers. These features are directly related to Android components. They can affect the behavior of applications. The new set of features is, then, composed of 124 features. We remind that the labels of the apps are the privacy risk scores given in [2].

To identify the optimal ML model, we perform a comparative analysis of four algorithms: SVR, GB, XGB, and MLP. The model achieving the highest performance is selected. Model evaluation is conducted using the Mean Squared Error (MSE) and Coefficient of Determination (R^2) metrics. All models are trained using 10-fold cross-validation.

We report in Table 1 the average cross-validation scores and their standard deviations. According to Table 1, the best performance is given by XGB model. It has the best performance among all the used metrics. Therefore, the selected machine learning model for our privacy score prediction is XGB.

[1] https://developer.android.com/reference/android/Manifest.permission
[2] https://github.com/hebbet/All-Android-Permissions/blob/master/AndroidManifest.xml

ESANN 2025 proceedings, European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning. Bruges (Belgium) and online event, 23-25 April 2025, i6doc.com publ., ISBN 9782875870933. Available from http://www.i6doc.com/en/.

	GB	**XGB**	MLP	SVR
R2	0.84 ±0.06	**0.86** ±0.03	0.78 ±0.08	0.78 ±0.04
MSE	0.12 ±0.06	**0.11** ±0.04	0.17 ±0.07	0.17 ±0.04

Table 1: Models evaluation

To test and validate the proposed XGB model, we developed RSPdroid (Risk Score Predictor for Android), a tool that proactively improves users' awareness about the potential privacy risks of Android applications. PSPdroid informs users of the risk of personal data leakage before installing applications. It predicts a risk score that reflects the severity of potential data disclosure. The predicted risk score is a real number ranging from 0 to 6, with 6 representing the highest level of privacy risk. The privacy scores are presented to the user with a color hint. If the application risk score is greater than or equal to 3, the color is red. If the risk score is between 1.5 and 3, the color is gray, and if the risk score is less than 1.5, the color is green.

4 Comparative Study

To evaluate the proposed XGB model (RSPdroid), we conduct two comparative studies. First, we compare our predicted RSPdroid scores with the ground truth [2] scores. Then, we compare RSPdroid scores with those of PrivacyAndroid [1]. Both comparative analyses are performed using a Condor L2 Pro, a real Android smartphone.

The first comparative study (Figure 1) aims to validate our approach by comparing our predicted scores (RSPdroid) with those of the ground truth [2]. To this end, we randomly select ten apps: Odd Socks, Screen-Recorder, Amazon Kindle, Currency, Calm, ZDF, DUSpeed Booster, Emoji Keyboard Cute, Crazy Dentist, and Orbot. It is worth noting that the selected apps and their versions don't belong to *AppVersionsDataset*, the dataset used for training our XGB model. We notice that the apps in Figure 1 are sorted in ascending order based on the difference between our RSPdroid scores and ground truth scores.

Figure 1 demonstrates that for the first four applications (Amazon Kindle, DU Speed Booster, Emoji Keyboard Cute, and ZDF) the RSPdroid and ground truth scores are nearly identical. The absolute discrepancy for these apps is less than 0.2. This corresponds to a relative difference of less than 3.3% on the 0–6 assessment scale. For ScreenRecorder, Calm, and Crazy Dentist, the score difference lies within the range of [0.2, 0.5], corresponding to a relative difference between 3.3% and 8.3%. These variations remain small and within an acceptable margin. Thus, 70% of the tested apps have a relative difference of less than 8.3% indicating a strong alignment between RSPdroid and ground truth scores. However, for the remaining three apps (Currency, Odd Socks, and Orbot) the difference between RSPdroid and ground truth scores ranges from 0.60 to 1, corresponding to a relative difference between 10% and 16,6%. This difference can be explained by the fact that the ground truth scores take into consideration

ESANN 2025 proceedings, European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning. Bruges (Belgium) and online event, 23-25 April 2025, i6doc.com publ., ISBN 9782875870933. Available from http://www.i6doc.com/en/.

the collected data, the security of the exchange, and communication with third parties, whereas RSPdroid focuses only on permissions and the entity to which information is communicated.

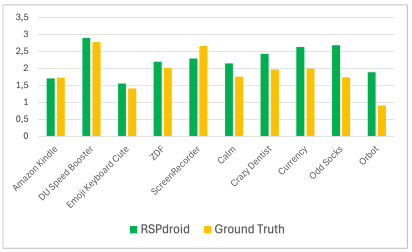

Fig. 1: RSPdroid *vs* Ground Truth.

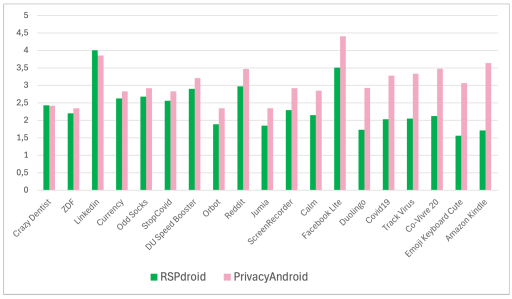

Fig. 2: RSPdroid *vs* PrivacyAndroid[1].

In the second comparative study (Figure 2), we added to the ten apps selected in Figure 1, five popular apps on Google Play (Facebook Lite, Duolingo, Jumia, Reddit, and LinkedIn) and three COVID19 contact tracking apps (Co-Vivre 20[3], STOP COVID-19 CAT[4], and StopCovid France[5]). These selected apps are not part of [2] and, therefore, do not belong to *AppVersionsDataset*. We, then, compare the RSPdroid scores with the PrivacyAndroid [1] scores. The apps in Figure 2 are sorted in ascending order based on the difference between RSPdroid scores and PrivacyAndroid scores.

A comparative analysis of RSPdroid and PrivacyAndroid (Figure 2) indicates that the scores for the first ten applications (Crazy Dentist, ..., Jumia) are nearly identical, with an absolute deviation of less than 0.5. This corresponds to a relative deviation of under 8.3%, which is considered negligible. For the three apps ScreenRecorder, Calm, and Facebook Lite, the absolute deviation falls within the interval [0.6, 0.9] corresponding to a relative deviation between 10% and 15%. This level of discrepancy remains within an acceptable range, suggesting that the scores generated by RSPdroid and Privacy Android are consistent for these apps. In contrast, for the remaining six apps (Duolingo, ..., Amazon Kindle), the absolute difference in scores ranges from 1.2 to 1.9, representing a relative deviation of 20% to 31%. For these apps, the difference is significant. This divergence can be explained by PrivacyAndroid's methodology, which considers only the presence of permissions without considering their contextual usage—whether for application functionality or data disclosure. We consider that PrivacyAndroid overestimates the risk, because its model only considers the presence of permissions, regardless of how the application will use them. According to our comparative study, for 68% of the tested apps (figure 2), our predicted scores closely align with the PrivacyAndroid scores with a relative

[3]ID in google play: com.satoripop.covid_android.
[4]ID in google play: cat.gencat.mobi.StopCovid19Cat.
[5]ID in google play: fr.gouv.android.stopcovid.

ESANN 2025 proceedings, European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning. Bruges (Belgium) and online event, 23-25 April 2025, i6doc.com publ., ISBN 9782875870933. Available from http://www.i6doc.com/en/.

difference of less than 15%. Moreover, both RSPdroid and PrivacyAndroid identify Facebook Lite, LinkedIn, and Reddit as the apps with the highest privacy risks.

5 Conclusion and perspectives

In this paper, we consider the risk or disclosure of personal data by Android applications. This risk comes once permissions have been granted to an application. The users grant permissions to an application without being informed about the risk for their privacy. Providing a score representing the privacy risk assessment can enhance the user's awareness of privacy protection.

For that purpose, we propose a Machine Learning model that predicts, proactively, a score representing the privacy risk assessment of Android applications. This score permits the user to be aware of the potential leakage of sensitive information before even installing the app. We also developed, RSPdroid a tool that implements the proposed XGB model. We trained our model on a dataset containing 1,679 Android apps that already leaked users' private data. The predicted scores of the proposed model were compared to another state-of-the-art approach, and the obtained results are encouraging. In future work, we think about new approaches that divide the privacy risk score into categories or sub-risk scores e.g., risk score for location data, credentials data, ...

References

[1] Asma Hamed, Hella Kaffel-Ben Ayed, and Dorra Machfar. Assessment for Android apps permissions a proactive approach toward privacy risk. In *13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 1465–1470, 2017.

[2] Jingjing Ren, Martina Lindorfer, Daniel J. Dubois, Ashwin Rao, David R. Choffnes, and Narseo Vallina-Rodriguez. Bug Fixes, Improvements, ... and Privacy Leaks: A Longitudinal Study of PII Leaks Across Android App Versions. In *Proceedings of Network and Distributed System Security Symposium*, 2018.

[3] Yang Yang, Xuehui Du, and Zhi Yang. Pradroid: Privacy risk assessment for android applications. In *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, pages 90–95, 2021.

[4] Majid Hatamian, Jetzabel Serna, Kai Rannenberg, and Bodo Igler. FAIR: Fuzzy Alarming Index Rule for Privacy Analysis in Smartphone Apps. In *Trust, Privacy and Security in Digital Business. TrustBus 2017*, 2017.

[5] Christopher Gates, Ninghui Li, Hao Peng, Bhaskar Sarma, Yuan Qi, Rahul Potharaju, Cristina Nita-Rotaru, and Ian Molloy. Generating Summary Risk Scores for Mobile Applications. In *IEEE Transactions on Dependable and Secure Computing*, volume 11, pages 238–251, 2014.