Android Application Classification and Anomaly Detection with Graph-based Permission Patterns

Karina Sokolova\textsuperscript{a,}\textsuperscript{*}, Charles Perez\textsuperscript{b}, Marc Lemercier\textsuperscript{a}

\textsuperscript{a}University of Technology of Troyes, 12 rue Marie Curie, Troyes, France
\textsuperscript{b}PSB : Paris School of Business, Digital Data Design, Chair D3, 59 rue nationale, Paris, France

\textbf{Abstract}

Android is one of the mobile market leaders, offering more than a million applications on Google Play store. Google checks the application for known malware, but applications abusively collecting users’ data and requiring access to sensitive services not related to functionalities are still present on the market. A permission system is a user-centric security solution against abusive applications and malware that has been unsuccessful: users are incapable of understanding and judging the permissions required by each application and often ignore on-installation warnings. State-of-the-art shows that the current permission system is inappropriate for end-users. However, Android permission lists do provide information about the application’s behaviour and may be suitable for automatic application analysis. Identifying key permissions for functionalities and expected permission requests can help leverage abnormal application behaviour and provide a simpler risk warning for users. Applications with similar functionalities are grouped into categories on Google Play and this work therefore analyses permission requests by category.

In this study, we propose a methodology to characterize normal behaviour for each category of applications, highlighting expected permission requests. The co-required permissions are modeled as a graph and the category patterns and central permissions are obtained using graph analysis metrics. The obtained patterns are evaluated by the performance of the application classification into categories that allow choosing the best graph metrics representing categories. Finally, this study proposes a privacy score and a risk warning threshold based on the best metrics. The efficiency of the proposed methodology was tested on a set of 9,512 applications collected from Google Play and a set of malware.

\textbf{Keywords}: Android, permission, pattern, classification, anomaly detection, risk warning, graph analysis

\section{Introduction}

Mobile applications are extensively used worldwide and new applications are added every day to mobile markets - platforms for the distribution of mobile applications. Recently there has been a spate of interest in Android - one of

\textsuperscript{*}Corresponding author

\textit{Email addresses: karina.sokolova@utt.fr (Karina Sokolova), c.perez@psbedu.paris (Charles Perez), marc.lemercier@utt.fr (Marc Lemercier)}

Preprint submitted to Elsevier September 16, 2016
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات