DroidRista: تحليل تدفق البيانات الثابت المدرك للانعكاس والتواصل بين المكونات في تطبيقات الأندرويد

اريج صويلح الزايدي

بإشراف
د. محمد سيد بخاري
د. سهير ظافر الشهري

الملخص

أصبحت الهواتف الذكية من المرافقين المهمين لملايين الأشخاص الذين يساعدون في تنظيم حياتهم الخاصة والمهنية على حد سواء. وبذلك أصبح الوصول إلى البيانات الخاصة بالمستخدم والمخزنة على الجهاز مثل الصور أو دفتر العناوين او الموقع في أي مكان وفي أي وقت أمرًا ممكناً. على الرغم من توفر العديد من أنظمة التشغيل للهواتف المحمولة، هذه الأطروحة تركز على نظام تشغيل الاندرويد. احصائياً، نظام الاندرويد هو النظام الذي يحظى بالحصة الأكبر من سوق الهواتف المحمولة. علاوة على ذلك، يمكن للمستخدمين توسيع وظائف هواتفهم باستخدام برامج صغيرة تسمى تطبيقات من مطورين وبائعين متعددين في نظام بيئي مفتوح.

مما لا شك فيه أن تخزين كل هذه البيانات على جهاز يعمل دائمًا ومتصل دائمًا ويمكن توسيعه بسهولة باستخدام برنامج جديد يعمل على تحسين راحة المستخدم إلى حد كبير. من ناحية أخرى، يطرح مخاوف فيما يتعلق بالخصوصية والأمان. قد تسيء التطبيقات استخدام البيانات المخزنة على جهاز الاندرويد من حيث الحصول عليها وتسريبها لغرض تعدي خصوصية المستخدم. المستخدم في كثير من الأحيان غير مدرك لتسريبات البيانات الصادرة من هاتفه. لذلك، يجب أن يكون لدى المستخدم آلية للتأكد من أن التطبيق يستخدم بياناته الخاصة كما هو متوقع ولا يسرب تلك البيانات إلى أطراف غير مصرح بها.

في هذه الأطروحة، اقترحنا درويدرستا وهو نهج يقوم بتنفيذ تقنية تحليل تدفق البيانات الثابتة بطريقة فعالة ودقيقة على تطبيقات الاندرويد لغرض العثور على تسرب البيانات الخاصة والحساسة في تلك التطبيقات، مثل معلومات الاتصال، أو بيانات الموقع أو معلومات التقويم.

في وقت لاحق، تم استعراض العديد من النُهج الحالية التي تم اقتراحها والتي تسعى الى تحقيق الهدف نفسه بمساعدة اسلوب تحليل تدفق البيانات الثابت وايضا تم استعراض القيود التي تعاني منها تلك الحلول من حيث عدم دعم التحديات الخاصة بالتحليل الثابت والتي كنت تبعا لذلك تؤثر على دقة التحليل.

نهجنا المقترح يركز على ايجاد الحل لثلاث من تحديات تحليل تدفق البيانات الثابت في تطبيقات الاندرويد وهذه التحديات هي: التواصل بين مكونات التطبيق نفسه والانعكاس وكذلك التدفقات الضمنية. وبالتالي يمكننا القول ان النهج المقترح درويدرستا يساهم في تحسين التحليل الامني لتطبيقات الاندرويد من خلال استخدام تحليل تدفق البيانات الثابت لحل مشكلة تسرب البيانات الخاصة والتغلب على ثلاث من التحديات التي كانت تعاني منها النهج السابقة.

لتقييم دقة حلنا المقترح، استخدمنا ثلاث مجموعات من تطبيقات الاندرويد والتي تتضمن تسريبات بيانات حساسة وأثبتت النتائج فعالية النهج المقترح وتفوقه على النُهج الحالية في اكتشاف تسرب البيانات في تطبيقات الاندرويد.

نختتم هذه الأطروحة على أمل أنها توفر رؤى مفيدة حول كيفية حماية خصوصية مستخدمي أجهزة الاندرويد بشكل أفضل مع استمرار القدرة على الاستمتاع براحة متاجر التطبيقات الكبيرة التي توفر التطبيقات لأي احتياجات تقريبًا.

يقدم الفصل الأول مقدمة عن الرسالة بينما يستعرض الفصل الثاني الخلفية النظرية عن الرسالة والأبحاث السابقة. يشرح الفصل الثالث الأعمال المتعلقة بموضوع الرسالة والمسح الميداني حول تطبيقات الأندرويد ويقدم الفصل الرابع طريقة تصميم نموذج الحل المقترح. يناقش الفصل الخامس عملية تقييم نموذج الحل.

DroidRista: Reflection-Aware and ICC-Aware Static Data Flow Analysis of Android Applications

By Areej Sewalh Alzaidi

Supervised By

Dr. Seyed M Buhari
Dr. Suhair Alshehri

ABSTRACT

At present, the Android operating system dominates the smartphone market and the number of Android applications has risen dramatically. Android applications are processing increasing amounts of sensitive data, which could spark concerns about data leakage and privacy violation. Applications may misuse the sensitive data stored on the Android device and violate the privacy of the user. Indeed, firms use users' data for the purpose of targeted advertisement. Therefore, it is important to maintain user privacy and protect sensitive data from leakage. Thus, Static data flow analysis approaches, have been utilized for analyzing Android applications to uncover security and privacy issues (i.e., sensitive data leakage detection). Unfortunately, these approaches frequently generate false alarms, given the different challenges caused by Android applications such as inter-component communication (ICC) and Reflection. In this thesis, we, therefore, present DroidRista, an approach for efficiently conducting static data flow analysis on Android applications for detecting sensitive data leakage. DroidRista is capable of analyzing reflection as well as analyzing inter-component communication (ICC) in Android applications and thus improving DroidRista's precision of detecting data leakage as compared to existing static analysis approaches. To evaluate the performance of DroidRista, we have tested it on three data sets. The first data set is taken from benchmark test-suites containing 231 applications. The empirical results indicated that DroidRista reaches a precision of 98% and a recall of 98%. The second data set consists of 49 applications from Google Play Store. We detected a large number of data leaks, which is completely alarming since these are highly downloaded applications. Finally, DroidRista was used to monitor data leakage on InsecureBank app, and it successfully detected all leakage already existed in this app. Our work will contribute

to extending the current knowledge relevant to the Android security and improving the security analysis of Android applications.