



پایان‌نامه‌ی کارشناسی ارشد: اعظم سادات مقدم قدیری جلالی، ۱۳۹۸

تشخیص بدافزار با رویکرد ترکیب طبقه‌بندها با روش پلکانی

بدافزارهای اندروید با سرعت زیادی در حال افزایش هستند و به یک تهدید جدی و بالقوه برای کاربران تلفن‌های هوشمندی که از پلتفرم اندروید استفاده می‌کنند تبدیل شده‌اند. آنها به سرعت پیشرفت می‌کنند و حریم خصوصی کاربران و اطلاعات محرمانه‌ی آنها را به خطر می‌اندازند. از این رو نیازمند تکنیک‌های موثر و کارآمد برای شناسایی برنامه‌های مخرب اندروید هستیم. این پایان‌نامه راهکاری برای تشخیص بدافزارهای اندروید با استفاده از ترافیک شبکه‌ی برنامه‌های کاربردی اندروید پیشنهاد می‌دهد. این رویکرد شامل دو مرحله است. اولین گام انتخاب مناسبترین ویژگیهای ترافیکی است که در دسته‌بندی ترافیک ورودی به دو دسته‌ی بدافزار و بی‌خطر بیشترین تاثیر را دارند. برای این منظور از الگوریتم مربع‌کای برای انتخاب ویژگیهای موثر استفاده می‌کنیم و ویژگیهایی که بیشترین اهمیت را در دسته‌بندی داشتند گزینش می‌شوند. در گام دوم یک مدل پلکانی جدید برای تشخیص بدافزار اندروید با استفاده از ترکیب دو طبقه‌بند ارائه می‌کنیم. سپس ویژگیهای انتخابی مدل ارزیابی شده و با مدل‌های مشابه مقایسه شدند. نتایج نشان دادند که این ویژگیهای انتخابی می‌توانند مدلی، با کارایی مناسب ایجاد کنند. همچنین ارزیابی مدل در چهار سطح امنیتی بررسی شد و نتایج نشان داد که مدل ما می‌تواند دقت تشخیص بدافزار را به بیش از 95% برساند و نرخ تشخیص اشتباه بدافزار را به کمتر از 0.03% کاهش دهد.

کلیدواژه‌ها: تشخیص بدافزار، یادگیری ماشین، ترافیک شبکه، ترکیب طبقه‌بندها

شماره‌ی پایان‌نامه: ۱۲۷۴۱۰۱۵۹۷۱۰۰۱
تاریخ دفاع: ۱۳۹۸/۰۴/۱۳
رشته‌ی تحصیلی: مهندسی کامپیوتر - نرم‌افزار
دانشکده: فنی و مهندسی
استاد راهنما: دکتر حسن شاکری
استاد مشاور: دکتر یاسر علمی سولا

M.A. Thesis:

Malware Detection using Step by Step Ensemble Classification

Android malware is growing at a fast pace and has become a serious threat to smartphone users who use the Android platform. They are progressing rapidly and endangering the privacy of users and their confidential information. Hence, we need effective and efficient



techniques for identifying Android malware. This thesis proposes a strategy to detect Android malware using Android applications network traffic. This approach consists of two steps. The first step is to select the most appropriate traffic features that have the most impact in categorizing traffic into two types of malware and benign. For this purpose, we use a chi-square algorithm to select the effective features and select the characteristics that matter most in the categorization. In the second step, we present a new step-by-step model for detecting Android malware using Ensemble Classification. Then the selected features of the model were evaluated and compared with similar models. The results showed that these selective features can provide a model with proper performance. The model was also evaluated at four levels of security, and the results showed that our model could increase malware detection accuracy to over 95% and reduce the False Positive rate to less than 0.03%.