Android Malware Detection Based on System Calls

Marko Dimjašević, Simone Atzeni,
Ivo Ugrina, Zvonimir Rakamarić

UUCS-15-003

School of Computing
University of Utah
Salt Lake City, UT 84112 USA

May 15, 2015

Abstract

With Android being the most widespread mobile platform, protecting it against malicious applications is essential. Android users typically install applications from large remote repositories, which provides ample opportunities for malicious newcomers. In this paper, we propose a simple, and yet highly effective technique for detecting malicious Android applications on a repository level. Our technique performs automatic classification based on tracking system calls while applications are executed in a sandbox environment. We implemented the technique in a tool called MALINE, and performed extensive empirical evaluation on a suite of around 12,000 applications. The evaluation yields an overall detection accuracy of 93% with a 5% benign application classification error, while results are improved to a 96% detection accuracy with up-sampling. This indicates that our technique is viable to be used in practice. Finally, we show that even simplistic feature choices are highly effective, suggesting that more heavyweight approaches should be thoroughly (re)evaluated.