Accepted Manuscript

Profiling User-Trigger Dependence for Android Malware Detection

Karim O. Elish , Xiaokui Shu , Danfeng (Daphne) Yao , Barbara G. Ryder , Xuxian Jiang

PII: S0167-4048(14)00163-1

DOI: 10.1016/j.cose.2014.11.001

Reference: COSE 852

To appear in: *Computers & Security*

Received Date: 29 May 2014

Revised Date: 25 August 2014

Accepted Date: 1 November 2014

Please cite this article as: Elish KO, Shu X, Yao D(D), Ryder BG, Jiang X, Profiling User-Trigger Dependence for Android Malware Detection, *Computers & Security* (2014), doi: 10.1016/j.cose.2014.11.001.

Profiling User-Trigger Dependence for Android Malware Detection[☆]

Karim O. Elish[a], Xiaokui Shu[a], Danfeng (Daphne) Yao[a,*], Barbara G. Ryder[a], Xuxian Jiang[b]

[a] *Department of Computer Science, Virginia Tech, 2202 Kraft Dr, Blacksburg, VA 24060, United States*

[b] *Department of Computer Science, North Carolina State University, Raleigh, NC 27606, United States*

Abstract

As mobile computing becomes an integral part of the modern user experience, malicious applications have infiltrated open marketplaces for mobile platforms. Malware apps stealthily launch operations to retrieve sensitive user or device data or abuse system resources. We describe a highly accurate classification approach for detecting malicious Android apps. Our method statically extracts a data-flow feature on how user inputs trigger sensitive API invocations, a property referred to as the *user-trigger dependence*. Our evaluation with 1,433 malware apps and 2,684 free popular apps gives a classification accuracy (2.1% false negative rate and 2.0% false positive rate) that is better than, or at least competitive against, the state-of-the-art. Our method also discovers new malicious apps in the Google Play market that cannot be detected by virus scanning tools. Our thesis in this mobile app classification work is to advocate the approach of *benign property enforcement*, i.e., extracting unique behavioral properties from benign programs and designing corresponding classification policies.

Keywords:
Malware detection, User-intention, Static program analysis, Android malware, User-trigger dependence

[☆]A preliminary version of the work appeared in the Proceedings of the IEEE Mobile Security Technologies (MoST) workshop, in conjunction with the IEEE Symposium on Security and Privacy. San Francisco, CA, USA. May 2012 Elish et al. (2012). This work has been supported in part by Security and Software Engineering Research Center (S^{2}ERC), an NSF sponsored multi-university Industry/University Cooperative Research Center (I/UCRC), NSF grant CAREER CNS-0953638, and ONR grant N00014-13-1-0016.

[*]Corresponding author. Department of Computer Science, Virginia Tech, 2202 Kraft Dr, Blacksburg, VA 24060, United States. Tel.: +1(540)231-7787

Email addresses: kelish@vt.edu (Karim O. Elish), subx@vt.edu (Xiaokui Shu), danfeng@vt.edu (Danfeng (Daphne) Yao), ryder@cs.vt.edu (Barbara G. Ryder), jiang@cs.ncsu.edu (Xuxian Jiang)