Demande de bourse de thèse

Thesis subject title

Andromak : The next gen on device ANDROid MAlware protection

Laboratory name : INRIA Rennes
Team : WIDE
Localization : Rennes - University of Rennes 1 - INRIA - FRANCE

PhD supervisor
Name : **David Bromberg**
Position : **Full professor**
Email : **david.bromberg@irisa.fr**
Phone number : **+ 33 2 99 84 22 05**

Co-supervisor
Name : **Gilles Muller**
Position : **Inria Senior Research Scientist**
Email : **gilles.muller@inria.fr**
Phone number : **+ 33 2 99 84 72 22**

Keywords. Android, security, malware, system programming, System, code analysis, ARM architecture, assembly language and compilation

Research axis. **Axe 2** Providing the next generation of Android anti-malware scanners.

1 Thesis proposal

(1233 words)

Context. Android is now the most used operating system with 86% market shares. Thanks to an active developer community, the application ecosystem gets bigger everyday. For example, Google Play Store holds 3.3 million applications with a rate of more than 50 000 submissions a month. Estimations indicate that more than 75 billions applications were downloaded on the platform in 2016. Consequently, due to its widespread popularity, the Android platform has become a lucrative target for hackers.

Hence Android constitutes one of the first choice platform to propagate malware threats. Infection rate on Android devices is constantly increasing spawned out by a dramatic proliferation of malware.

Nowadays there are no satisfactory solutions to stop the proliferation of malware over Android devices. It constitutes a severe threat to any businesses. It may interrupts and disables applications, retrieved and spoofed personal information and identity, access sensitive information, control all applications executing on users' device, and even overcharge users for functionality that's widely available.

Next generation of on devices anti-malware protection. Various techniques have emerged to counter the proliferation of Android malware leveraging either static, dynamic or hybrid analysis. Static analysis [21] consists in analyzing the application source code without running it. However, this technique is known for its limitations if applications are obfuscated and/or if their malicious code is downloaded dynamically at runtime. Alternatively, dynamic analysis technique [20, 30] comes as a solution to these limitations, and consists in analyzing the actual behavior of the application during its execution. However, due to their inherent high resource consumption, most dynamic analysis are performed in-lab [6, 31] as opposed to analysis performed on off-the-shelf devices.

In this thesis, we prone that embedding dynamic analysis directly on off the shelf devices is the way to go ; it enables to stop threats such as yet unknown malware variants as soon as possible, i.e as soon as a behavior is detected as suspicious without having identified a particular signature beforehand (i.e. in-labs) [25,28].

However, performing such analysis is far from being without challenges. The state of the art solutions that go in that direction suffers one or other of these two problems : they require either (i) a customized Android system [13, 19, 20, 24], which are not provided with off-the- shelf Android devices, or (ii) a rooted/jailbroken device [25], which is not easily accessible to end users,

Accordingly, our main objective in this thesis is to promote a novel concept of dynamic code analysis based on dynamic code introspection coupled with concepts of application sandboxing [1] based on application virtualization to enable efficient monitoring at scale without any firmware alterations, root privileges while reducing to a minimum modifications of Android applications.

Strong skills on Linux kernel, Android framework, ARM assembly are required to apply.

2 References

[1] Michael Backes, Sven Bugiel, Christian Hammer, Oliver Schranz, Philipp von Styp-Rekowsky : Boxify : Full-fledged App Sandboxing for Stock Android. USENIX Security Symposium 2015 : 691-706

[21] Li Li, Tegawendé F. Bissyandé, Mike Papadakis, Siegfried Rasthofer, Alexandre Bartel, Damien Octeau, Jacques Klein, and Le Traon. Static analysis of android apps : A systematic literature review. Information and Software Technology, 88:67 – 95, 2017.

[20] Patrik Lantz. Droidbox : An android application sandbox for dynamic analysis. In Master's Thesis at Department of Electrical and Information Technology, 2011.

[30] Michelle Y Wong and David Lie. Intellidroid : A tar- geted input generator for the dynamic analysis of an- droid malware. In NDSS, volume 16, pages 21–24, 2016.

[31] Michelle Y. Wong and David Lie. Intellidroid : A tar- geted input generator for the dynamic analysis of an- droid malware. In 23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016, 2016.

[6] Google's bouncer for android shows malware apps the door. https://mashable.com/2012/02/02/google-bouncer-for-android/ ?europe=true. Visited on April 2020.

[25] L. Qiu, Z. Zhang, Z. Shen, and G. Sun. Apptrace : Dynamic trace on android devices. In 2015 IEEE Inter- national Conference on Communications (ICC), pages 7145–7150, June 2015.

[28] Xiaoxiao Tang, Yan Lin, Daoyuan Wu, and Debin Gao. Towards dynamically monitoring android applications on non-rooted devices in the wild. In Proceedings of the 11th ACM Conference

on Security Privacy in Wireless and Mobile Networks, WiSec '18, pages 212–223, New York, NY, USA, 2018. ACM.

[13] Michael Backes, Sven Bugiel, Oliver Schranz, Philipp von Styp-Rekowsky, and Sebastian Weisgerber. Artist : The android runtime instrumentation and security toolkit. In 2017 IEEE European Symposium on Se- curity and Privacy (EuroSP), pages 481–495. IEEE, 2017.

[19] William Enck, Peter Gilbert, Byung-Gon Chun, Lan- don P. Cox, Jaeyeon Jung, Patrick McDaniel, and An- mol N. Sheth. Taintdroid : An information-flow tracking system for realtime privacy monitoring on smartphones. In Proceedings of the 9th USENIX Conference on Op- erating Systems Design and Implementation, OSDI'10, pages 393–407, Berkeley, CA, USA, 2010. USENIX Association.

[24] S. Sezer M. K. Alzaylaee, S. Y. Yerima. Dynalog : an automated dynamic analysis framework for characteriz- ing android applications. https://doi.org/10.1109/ CyberSecPODS.2016.7502337, 2016.