Using machine learning techniques for hardware performance counter classification and ROP attack detection

Kai Lehniger[1], Yauhen Varabei[1], Marcin Aftowicz[1],
Seyed Ehsan Hashemi Rastegar[2], Zoya Dyka[1], and Peter Langendörfer[1]
[1] IHP - Leibniz-Institut für innovative Mikroelektronik
[2] BTU Cottbus - Senftenberg

31st Crypto Day, 17/18 October 2019

Return-oriented programming (ROP) attacks are a huge threat to a vast majority of systems. By exploiting buffer overflow vulnerabilities these attacks are able to change the control flow of the executed program. Therefore, the attacker can run arbitrary code even on Harvard architectures [1].

Besides established defense mechanisms like Address Space Layout Randomization (ASLR) and stack canaries, the recent research is focusing on so-called hardware performance counters (HPCs) to detect malicious behaviour [2]. HPCs are common in all modern architectures and are mainly used for application profiling by tracking CPU events, e.g., cache misses and branch prediction errors.

In [3] a Support Vector Machine (SVM) is used to detect ROP attacks based on profiles of HPCs. ROP and benign runs were used to train the SVM with up to 98.1% accuracy depending on the CPU.

The SVM uses cluster centers to detect patterns in time where the program changes its behaviour. These patterns can be applied to recognize whether a program operation is normal or malicious. We propose an intelligent approach that finds distinguishing clusters in manipulated executions [4]. After labelling we want to train our SVM on the given patterns in hopes to improve its accuracy.

References

[1] A. Francillon and C. Castelluccia, "Code injection attacks on harvard-architecture devices," in *Proceedings of the 15th ACM conference on Computer and communications security*, 2008, pp. 15–26.

[2] A. Garcia-Serrano, "Anomaly detection for malware identification using hardware performance counters." [Online]. Available: https://arxiv.org/pdf/1508.07482.pdf

[3] D. Pfaff, S. Hack, and C. Hammer, "Learning how to prevent return-oriented programming efficiently," in *Engineering Secure Software and Systems*. Springer International Publishing, 2015, pp. 68–85.

crypto day matters 31 (2019)
Beiträge vom 31. Kryptotag, 17.-18.10.2019, Qualcomm, Berlin.
doi:10.18420/cdm-2019-31-27

[4] Y. Varabei, I. Kabin, Z. Dyka, D. Klann, and P. Langendoerfer, "Intelligent clustering as a means to improve k-means based horizontal attacks," in *Proc. 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Workshops - W6: Machine Learning for Security and Cryptography*, Istanbul, Turkey, September 8–11, 2019, pp. 144–149.