ON-CHIP SECURITY

Malware detectors learn to work together

IEEE Trans. Dependable Secure Comput. <https://doi.org/10.1109/TDSC.2018.2801858> (2018)

Credit: IEEE

Software designed with malicious intent is termed malware. These programs are typically used to intercept sensitive data or to gain unauthorized control of a system and its resources. The detection of malware using software approaches is very effective but computationally expensive due to the complex algorithms employed. Khaled Khasawneh and Nael Abu-Ghazaleh from the University of California, Riverside, with colleagues from Binghamton University, Stanford University, and Intel Corporation have now devised a combined hardware and software approach to reduce the computational overhead by employing hardware detectors with simple machine learning algorithms.

Hardware malware detectors (HMDs) operate on the basis that the computational

footprint of malware differs from normal software. HMDs are able to sense anomalous low-level features at the hardware level by observing the mix of instructions, memory reference patterns, and distinct architecture events. The researchers show that by combining specialized HMDs with ensemble learning, a 2-times reduction in computational overhead and a 2.7-times reduction in time to detection, compared to a single layer HMD, can be attained. Moreover, their two-level detection approach reduces the overhead by 16.6 times compared to software-only approaches.

Michael Lee

Published online: 17 April 2018
<https://doi.org/10.1038/s41928-018-0064-6>