Detecting Malware and Ransomware using Hardware Performance Counters

Manaar Alam[1], Sarani Bhattacharya[1], Debdeep Mukhopadhyay[1], and Anupam Chattopadhyay[2]
[1]Indian Institute of Technology Kharagpur, [2]Nanyang Technological University Singapore

Abstract—Malware detection and trusted execution is one of the major problems in computer security. There has been an array of tools for detecting malware; however, most of them are primarily dependent on observing high-level events and software API calls. In this demo, we aim to highlight the role of low-level hardware events deduced from Hardware Performance Counters (HPCs) in detecting the existence of malware execution. We present two case studies: 1) Developing a statistical lightweight tool, in the context of embedded platform, to evaluate the potential of a program under test of being a malware, and 2) Developing a very fast detection methodology for popular ransomware (a malware which encrypts files and asks for ransom) on standard desktops. While the first approach uses lightweight statistical hypothesis testing on the HPC values to assign a metric for a program under test, the second approach uses a two-fold analysis using Artificial Neural Network (ANN) and Fast Fourier Transformation (FFT) to develop a very fast detection methodology. Our detection scheme templates the benign environment, while not considering specific signature generated from a known malware, thereby is expected to be adequate to perform well against unreported malware with minimal detection time.