Accepted Manuscript

Automated multi-level malware detection system based on reconstructed semantic view of executables using machine learning techniques at VMM

Ajay Kumara M.A., Jaidhar C.D.

PII: S0167-739X(17)31180-9
DOI: http://dx.doi.org/10.1016/j.future.2017.06.002
Reference: FUTURE 3493

To appear in: Future Generation Computer Systems

Received date: 3 October 2016
Revised date: 30 April 2017
Accepted date: 5 June 2017


This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.
In order to fulfill the requirements like stringent timing restraints and demand on resources, Cyber-Physical System (CPS) must deploy on the virtualized environment such as cloud computing. To protect Virtual Machines (VMs) in which CPSs are functioning against malware-based attacks, malware detection and mitigation technique is emerging as a highly crucial concern. The traditional VM-based anti-malware software themselves a potential target for malware-based attack since they are easily subverted by sophisticated malware. Thus, a reliable and robust malware monitoring and detection systems are needed to detect and mitigate rapidly the malware based cyber-attacks in real time particularly for virtualized environment. The Virtual Machine Introspection (VMI) has emerged as fine-grained out-of-VM security solution to detect malware by introspecting and reconstructing the volatile memory state of the live guest Operating System (OS) by functioning at the Virtual Machine Monitor (VMM) or hypervisor. However, the reconstructed semantic details by the VMI are available in a combination of benign and malicious states at the hypervisor. In order to distinguish between these two states, extensive manual analysis is required by the existing out-of-VM security solutions. To address the foremost issue, in this paper, we propose an advanced VMM-based guest-assisted Automated Multilevel Malware Detection System (AMMDS) that leverages both VMI and Memory Forensic Analysis (MFA) techniques to predict early symptoms of malware execution by detecting stealthy hidden processes on a live guest OS. More specifically, the AMMDS system detects and classifies the actual running malicious executables from the semantically reconstructed process view of the guest OS. The two sub-components of the AMMDS are: Online Malware Detector (OMD) and Online Malware Classifier (OFMC). The OMD recognizes whether the running processes are benign or
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات