Name: Darshan Mansukhbhai Tank

Enrollment No: 149997107002

Branch: CE/IT Engineering

Title of the Thesis: Enhancement of Security Mechanism in Virtualization Environment

Abstract

Today's advanced malware can easily avoid detection by adopting several evasion strategies. Process injection is one such strategy to evade detection from security products since the execution is masked under a legitimate process. Malicious activities are often enforced by injecting malicious code into running processes, which is often undetectable by traditional anti-malware techniques. Various process injection techniques are employed by malware to gain more stealth and to bypass security tools/products. Our main focus in this research work is to propose an entirely out-of-VM approach based on advanced memory introspection to detect process injection of varied types in a virtualized environment.

The VMI-based Process Injection Detection (VMIPID) model scans for injected memory regions that are created as a result of process injection. We implement our approach in a plugin for the memory forensic framework Volatility, which automatically reports any memory region containing injected codes, and successfully tested it on live VMs and malware-infected memory images and also evaluated it against implementations of different hiding techniques. Experimental results show that our model classifies injected memory regions with high accuracy and completeness and has more true positives and fewer false positives when compared to other existing systems/solutions.

Our proposed detection approach assures precise and reliable results and exactly pinpoint injected memory regions. Our proposed system detects an actual malicious memory region in the virtual address space of an infected process. Our proposed system detects more malware families and dominates the other approaches in all evaluation metrics.

This work is intended to automate the detection of different process injection techniques in a virtualized environment and dump recognized malicious memory regions to disk for a detailed analysis and assessment. This Ph.D. work would be useful for a software company that works in the area of security at the Infrastructure as a Service (IaaS) layer in the cloud computing model for possible integration of the solution in their Anti-Malware product.

List of Publication(s):

1) Tank, D., Aggarwal, A. & Chaubey, N. (2019). Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison. International Journal of Information Technology. Published by Springer, ISSN: 2511-2104, https://doi.org/10.1007/s41870-019-00294-x, Abstracted and Indexed in UGC-CARE List (India)
2) Tank D., Aggarwal A., Chaubey N. (2020). A Method for Malware Detection in Virtualization Environment. In: Chaubey N., Parikh S., Amin K. (eds) Computing Science, Communication and Security. COMS2 2020. Communications in Computer and Information Science, vol 1235, Published by Springer, Singapore, ISBN: 978-981-15-6647-9, https://doi.org/10.1007/978-981-15-6648-6_21

* Total 7 publications, out of which two publications are listed above.