Author : Harena RAKOTONDRATSIMA

Title: « HadiVoli: fine grained process isolation against hostile OS and libraries using Confidential VMs »

Short Abstract:

Traditional Confidential VMs are designed to protect virtual machines from a potentially untrusted hypervisor. However, the VM itself still constitutes a large trusted computing base (TCB), including the operating system and libraries, which may be exploited by an adversary to exfiltrate sensitive data from the VM to the external environment. In this project, we aim to minimize the codebase embedded within the Confidential VM by eliminating the guest OS through process-level virtualization and by constraining library interactions with application data to prevent data leakage from within the VM.