Cyber Defense Language Using VMI

Zirak Zaheer, Zeeshan Hakim, Anas Saeed, Dr. Basit Shafiq
Department of Computer Science, LUMS, Pakistan

INTRODUCTION

Virtual Machine Introspection has recently become a popular approach to secure Virtual Machines in a Cloud environment. This project aims to build on the recent developments in the field of VMI and memory forensics, to set-up a framework that customizes and makes it easier to secure VMs in Cloud.

APPROACH

- A framework that provides the ability to create any signature and launch a monitor based on that signature to scan and raise an alarm in real time.
- Cyber Defense Language is customized to define a wide range of threat sets.
- Cyber Defense Language to construct schemas, to query the VMs and analyze the data for potential Malware.
- Making use of Volatility, and LibVMI framework to minimize the semantic gap.

EXAMPLES

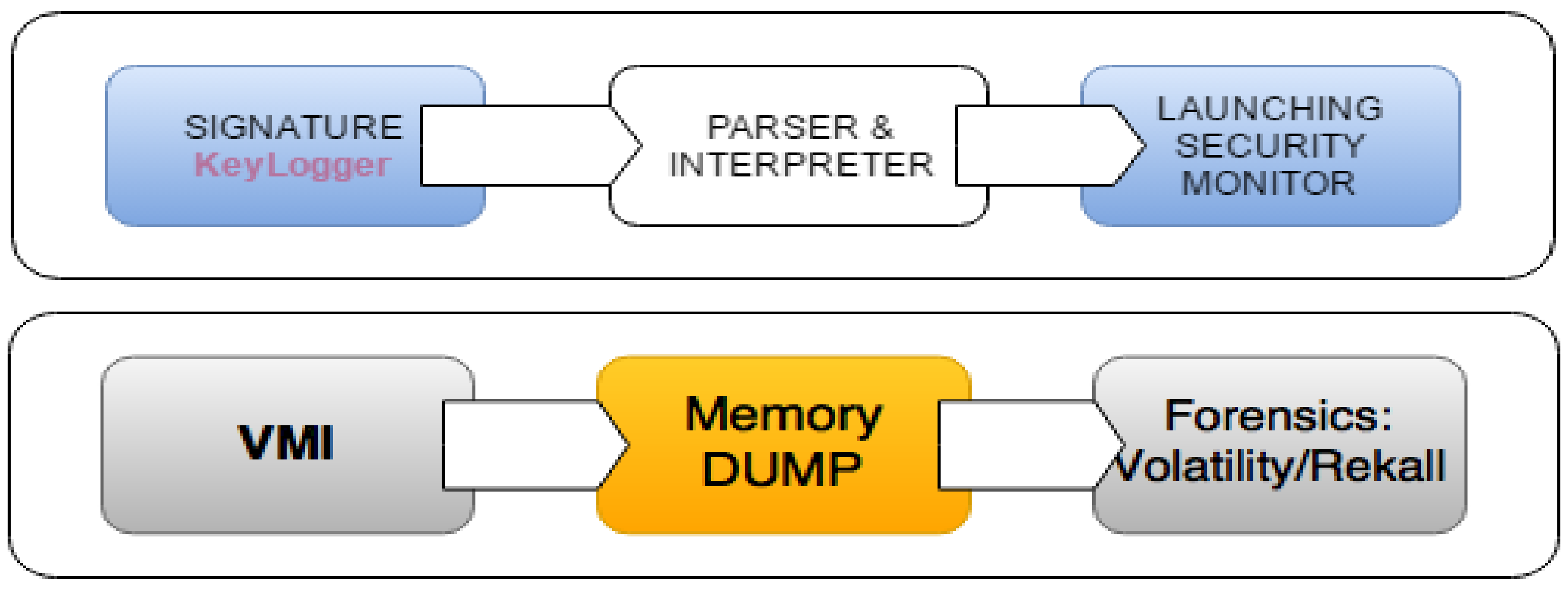

FIGURE 1 : KeyLogger

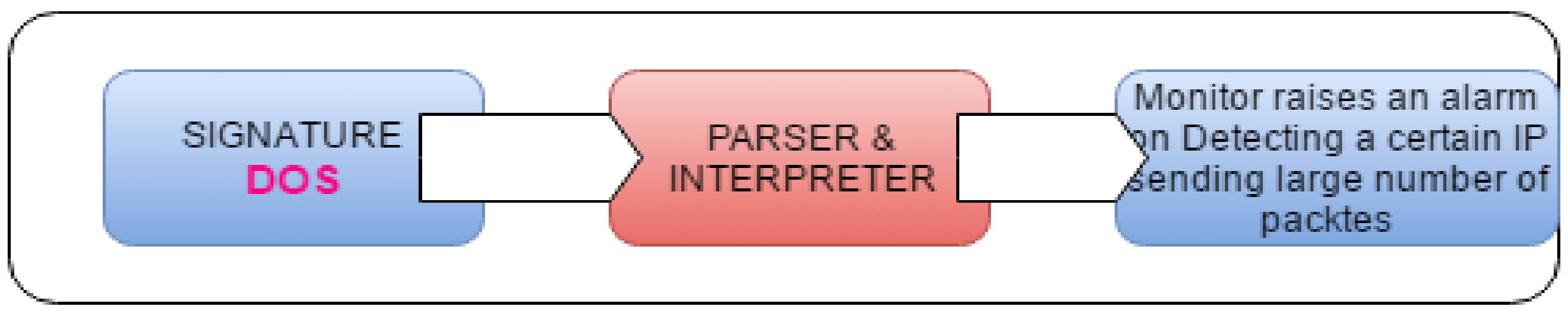
SIGNATURE
DOS
PARSER & INTERPRETER
Monitor raises an alarm on Detecting a certain IP sending large number of packtes

FIGURE 2 : Denial Of Service Attack

LIMITATIONS

- Only used to raise an alarm. Not actions
- Error handling is limited
- Detection is solely based on the assumption that the memory image when taken using LibVMI is received untampered
- Not all threat sets covered

PROBLEM

The challenge with monitoring Virtual Machines using VMI is two-fold:

- The Intrusion Detection System sits at the Hypervisor Layer.
- There is a lack of an appropriate method/framework using which we can comprehensively scan the target VM for a particular threat.

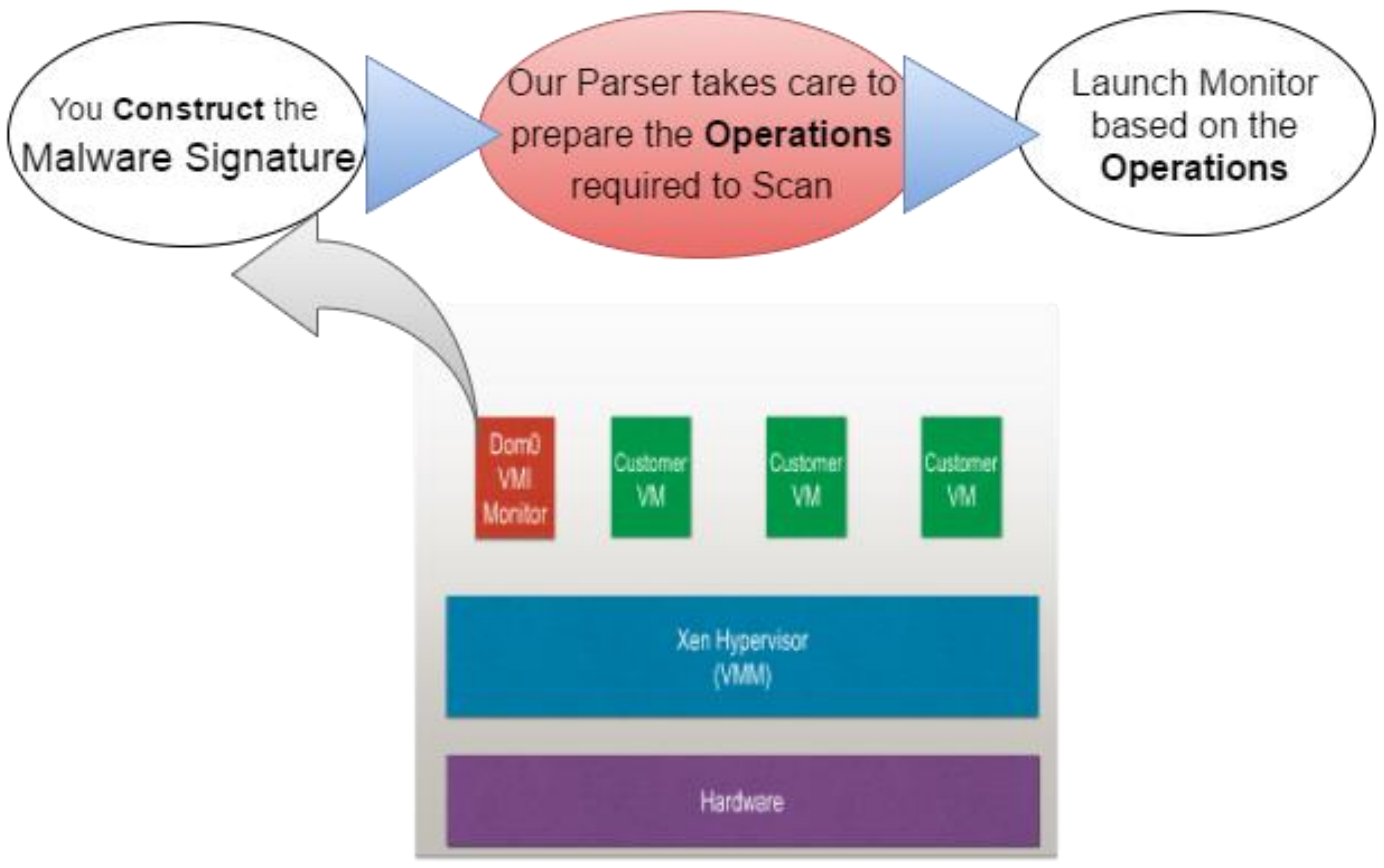
You Construct the Malware Signature
Our Parser takes care to prepare the Operations required to Scan
Launch Monitor based on the Operations
Dom0 VMI Monitor
Customer VM
Customer VM
Customer VM
Xen Hypervisor (VMM)
Hardware

FIGURE 2 : Framework Working

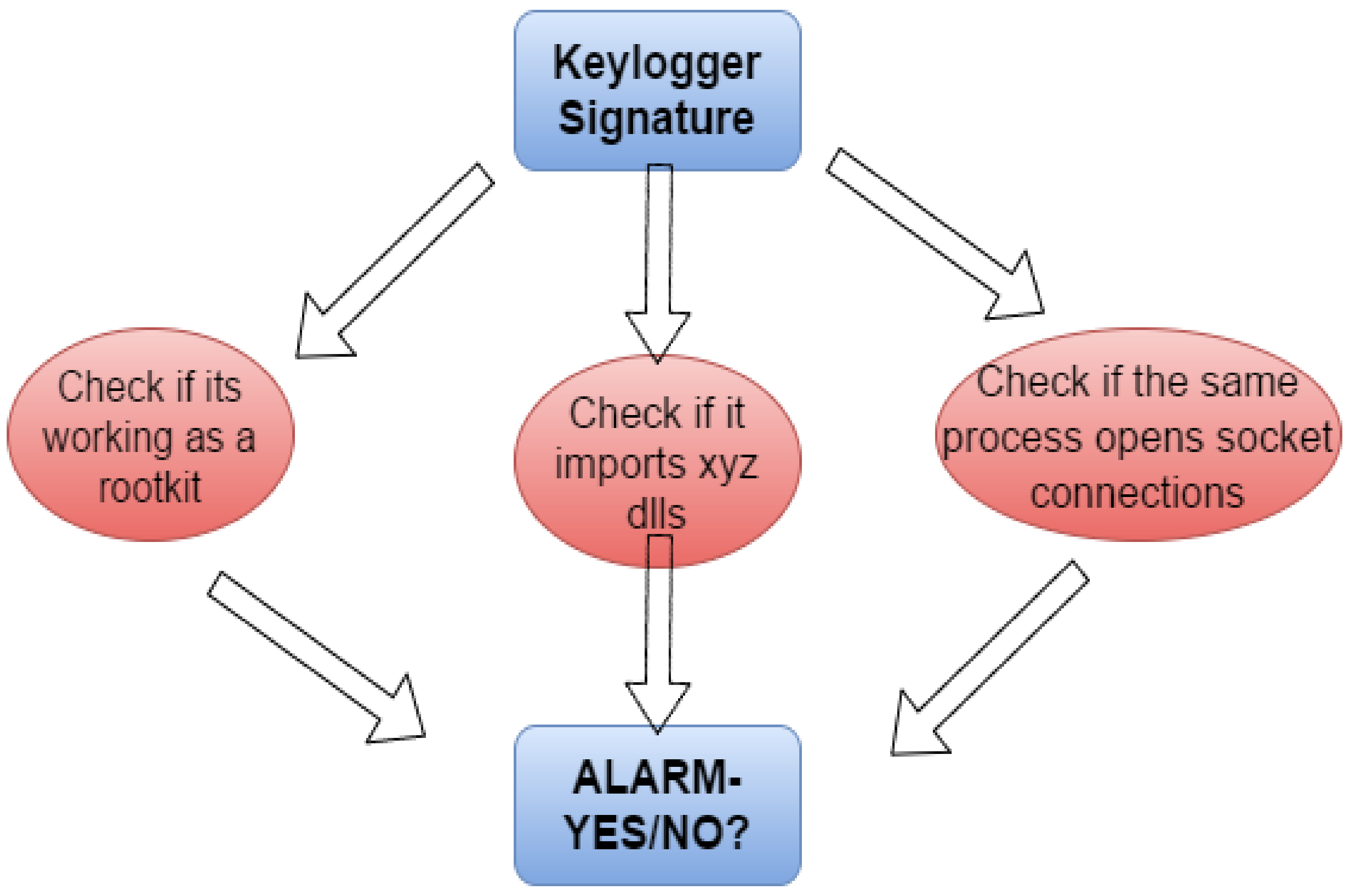
Keylogger Signature
Check if its working as a rootkit
Check if it imports xyz dlls
Check if the same process opens socket connections
ALARM-YES/NO?

FIGURE 3 : KeyLogger Operations

FUTURE WORK

- Extending work by including Network Forensics.
- Addressing Performance issues and System lag due to querying memory repeatedly.
- Rather than taking memory the entire memory dump it will be smarter and efficient to query only the required parts of memory
- Integrating threat intelligence and data mining techniques to analyze data for threats more effectively