



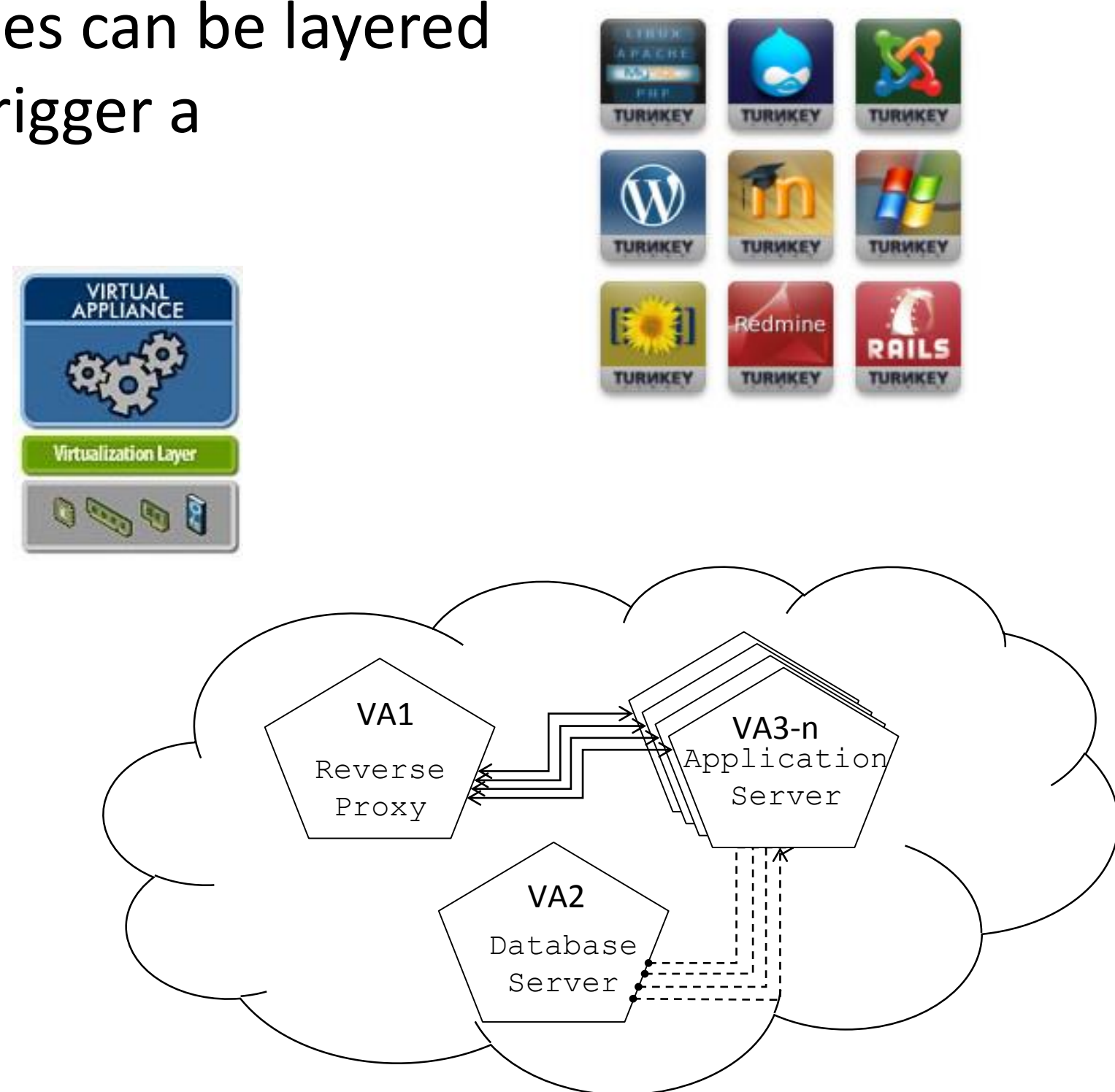
# Defense in Depth for Virtual Appliances Built on Event Based Probing of Untrusted Guests

Read Sprabery, Zachary J Estrada, Zbigniew Kalbarczyk, Ravishankar Iyer, Roy Campbell  
 University of Illinois at Urbana-Champaign  
 {spraber2, zestrade2, kalbarcz, rkiyer, rhc}@illinois.edu

Rakesh B. Bobba  
 Oregon State University  
 rakesh.bobba@oregonstate.edu

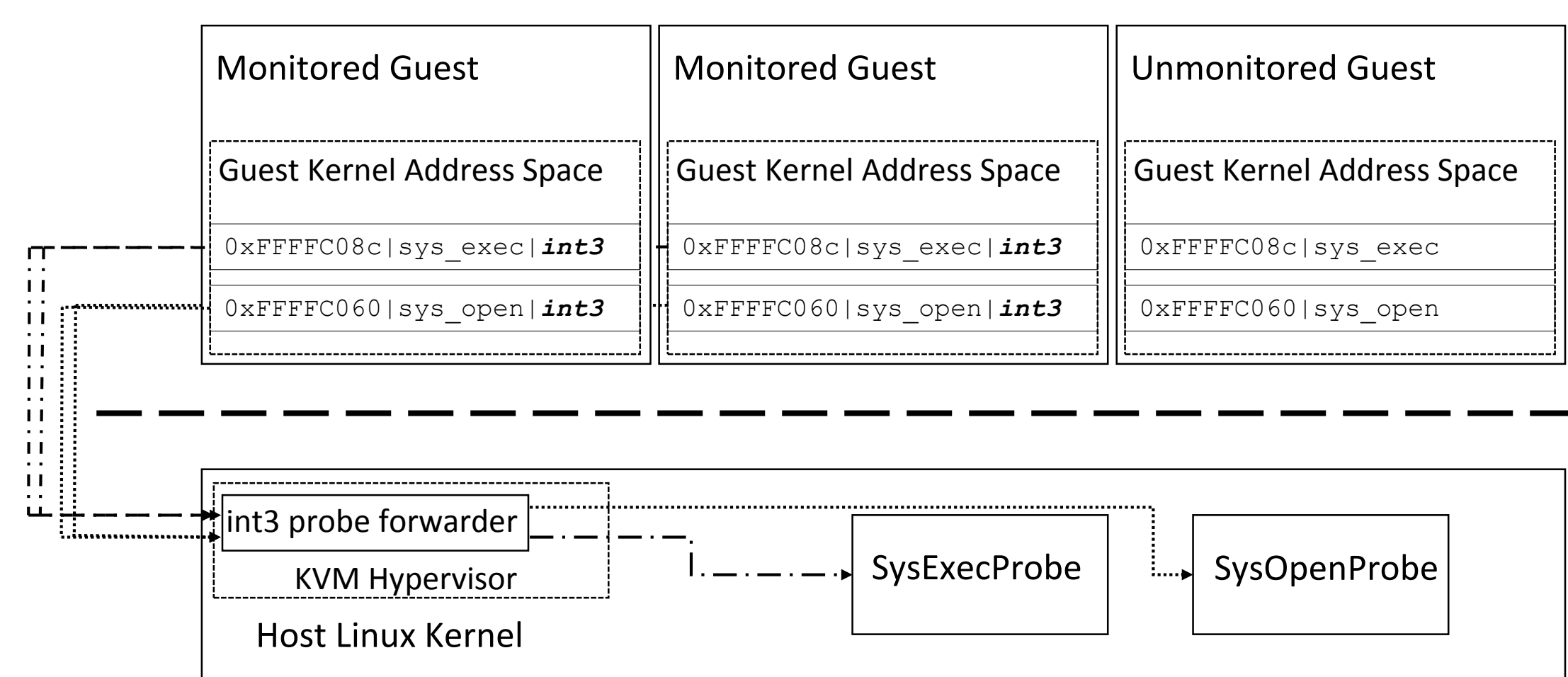
## Introduction

- Virtual Appliances perform single tasks, lending to better Intrusion Detection
  - Policies are simple white-lists
  - VA's share base image, thus policies can be layered
  - Probing mechanisms exist that trigger a control transfer to the hypervisor at specific locations during guest execution
- Contributions:
  - IDS for VA's
  - Policy Recording Mechanism
  - Algorithm for timely probe insertion



## Probing Mechanism

- Probes trap to hypervisor where introspection can occur
- Probe insertion must **occur before first execution**
- Achieved via induced EPT violation signature



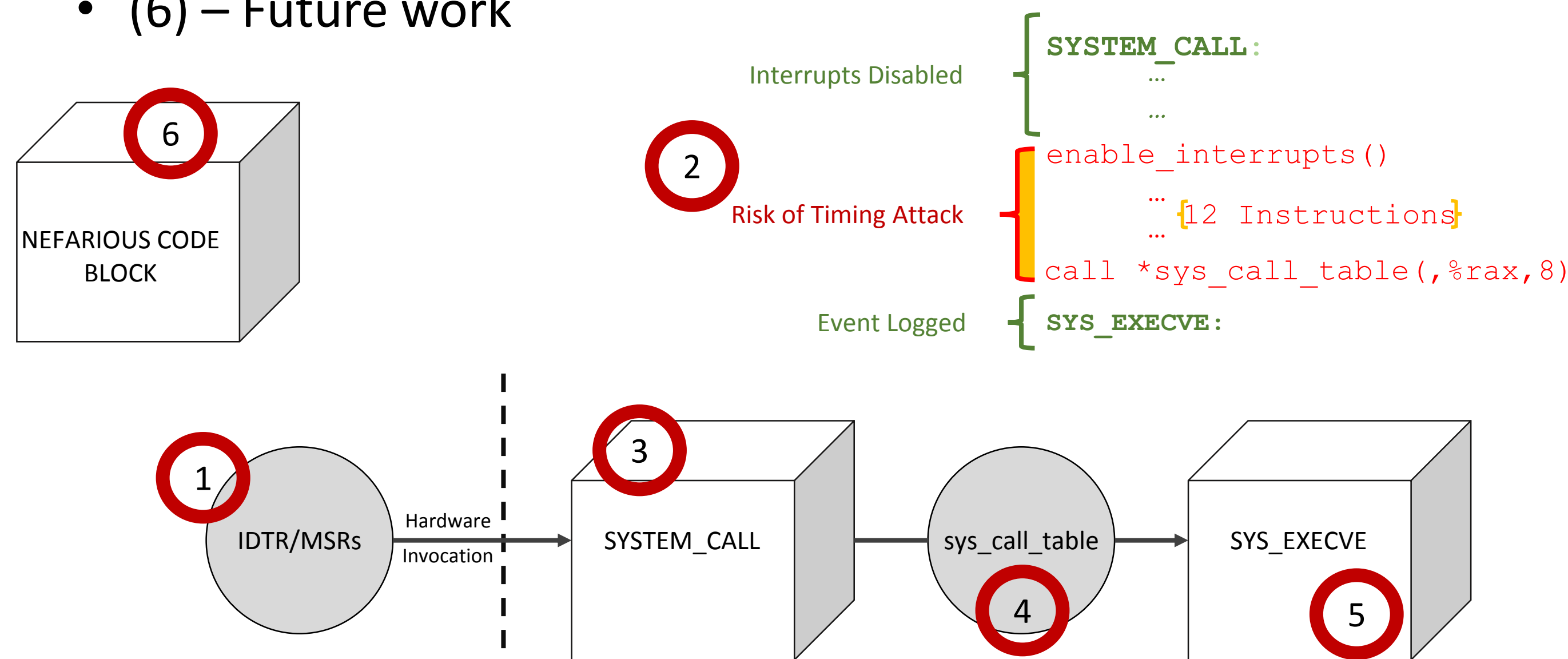
## Attack Model for Log Circumvention

- 6 ways for an attacker to circumvent logging
  - Modify registers
  - Rewrite locations in memory (3 locations)
  - Cause an interrupt to modify control flow
  - Recreate behavior
- More protection means more overhead
- Cost of Attack vs. Performance Impact



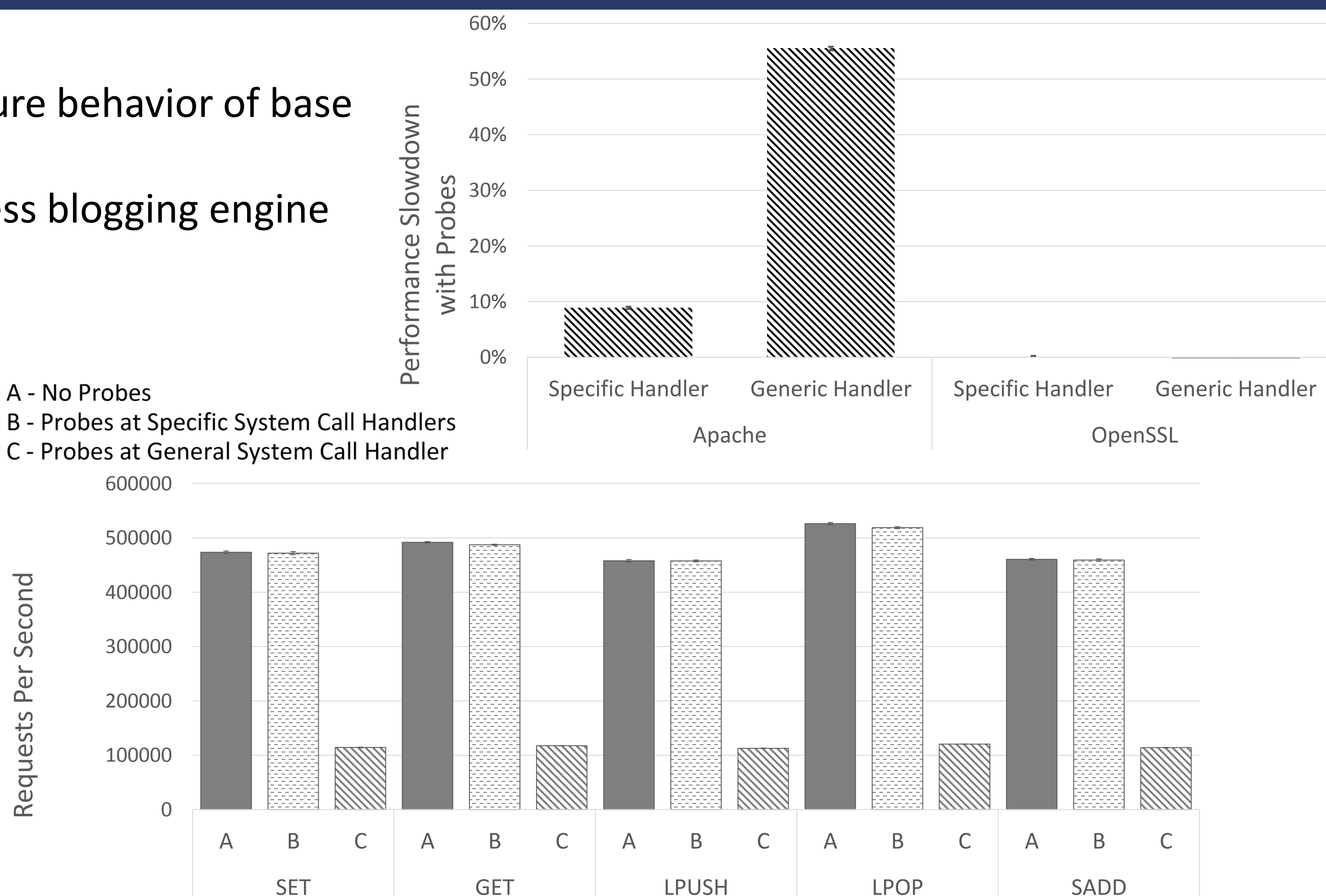
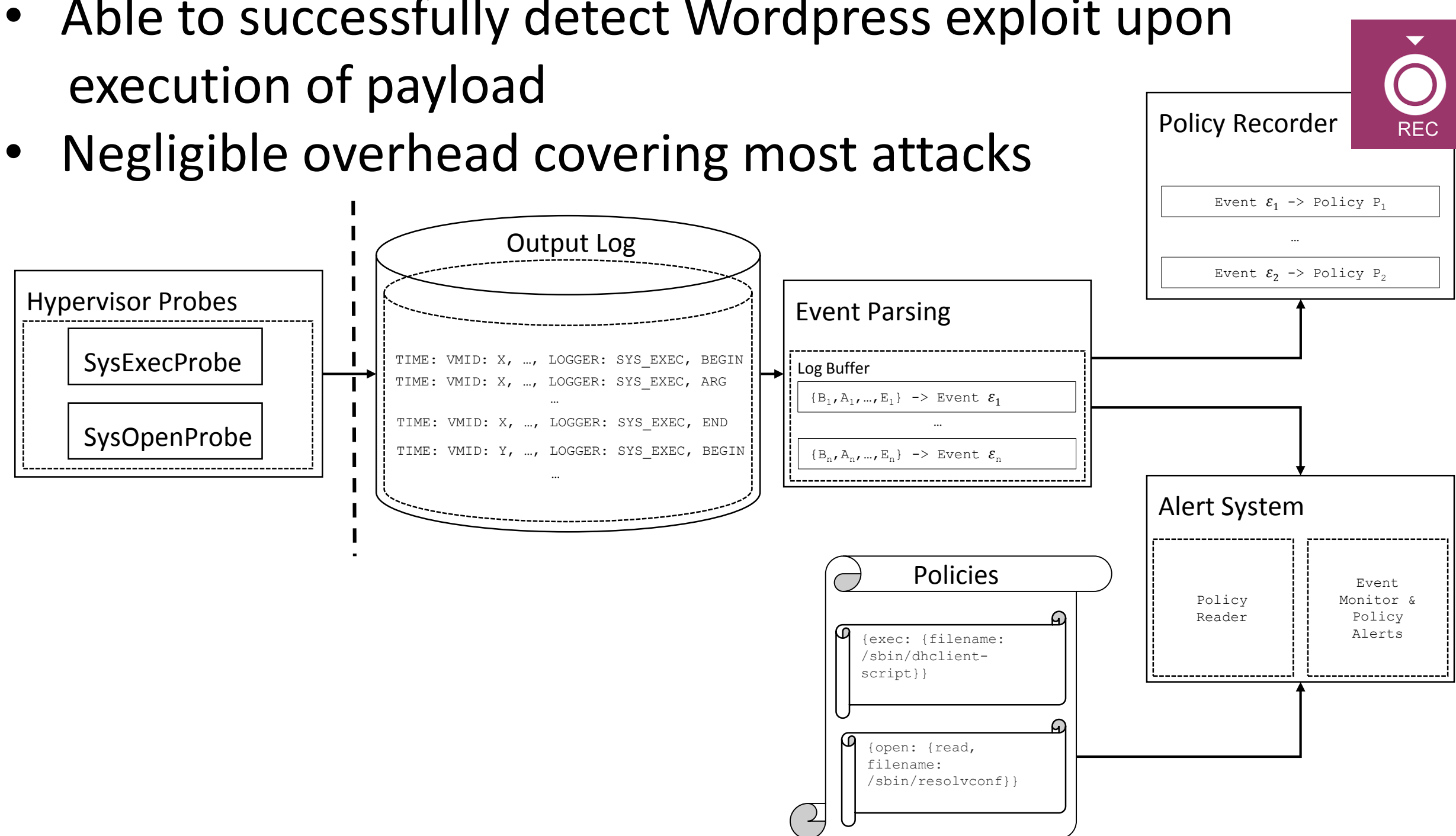
## Probe Placement

- Must balance defense against attack model and performance impact to.
- Defenses:
  - (1) – Monitor writes to subset of guest registers
  - (2) – Place probe at general system call handler
    - (3-5) – Write protect pages
    - (6) – Future work



## IDS Architecture & Evaluation

- Logging sys\_exec and sys\_open
- Ease of use: Policy recording mechanisms made it easy to capture behavior of base operating system (e.g.: DHCPd)
  - Few modifications to auto-generated policy for the Wordpress blogging engine
- Able to successfully detect Wordpress exploit upon execution of payload
- Negligible overhead covering most attacks



Related Publications:  
 Estrada, Zachary J., et al. "Dynamic vm dependability monitoring using hypervisor probes." *Dependable Computing Conference (EDCC), 2015 Eleventh European*. IEEE, 2015.  
 Sprabery, Read, et al. "Trustworthy Services Built on Event Based Probing for Layered Defense." *International Conference on Cloud Engineering (IC2E), 2017 Fifth IEEE*, 2017. (To Appear)