# 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  
sprab2, zestrad2, 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 exists 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

---

## Attack Model for Log Circumvention

- **6 ways** to 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

---

## Probing Mechanism

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

---

## 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

---

---

**Noted Publications:**  