U.S. AIR FORCE

Fall 2015
Research Presentations

U.S. AIR FORCE

Monitoring Fusion for Intrusion Detection and Response

Atul Bohara

P.I. William H. Sanders

U.S. AIR FORCE

Research Overview

- Current research
  - Fusion of monitoring information
    - Convert big heterogeneous data to more relevant and concise data
    - Build system profile through data association techniques to support intrusion detection
    - Data driven fusion technique; currently using Clustering
  - Working on a testbed to collect real data and run experiments
- Plan for the year
  - Use monitoring fusion to support automatic response
    - We need to do fusion in real-time
  - Plan on publishing the work

U.S. AIR FORCE

Security Monitor Deployment to Support Intrusion Detection

Uttam Thakore

P.I. William H. Sanders

Uttam Thakore

PI: William Sanders

- Current work:
  - A **cost-effective** methodology for monitor deployment to **meet intrusion detection goals**
    - Uses quantitative metrics to capture monitor utility and cost
    - Uses integer programming to determine optimal monitor deployment based on intrusion detection goals and cost requirements
  - Masters thesis: "A Quantitative Approach to Security Monitor Deployment", deposited August 2015
- Plans for the year:
  - Improving scalability of MS thesis research
  - Preparing submission for DSN 2015 based on thesis
  - Adaptive "learning responses" – deployment and configuration of monitors in response to detected attacker behavior to aid intrusion detection algorithms

U.S. AIR FORCE

“Hands-Off” VM Introspection

Zachary Estrada
P.I. Ravishankar K. Iyer

"Hands-Off" VM Introspection

- Virtual Machine Introspection (VMI) is used to support Hypervisor-based VM Monitoring
- Hypervisor only has access to bits and bytes
- Traditional VMI requires precomputing offsets and addresses for data structures
  - Can't do in cloud (which is where you want VMI)
- Use architectural state to infer offsets e.g., Process IDs, address space information, etc…
- Enabling Reliability and Security as-a-Service

U.S. AIR FORCE

Research Summary

Cuong Pham

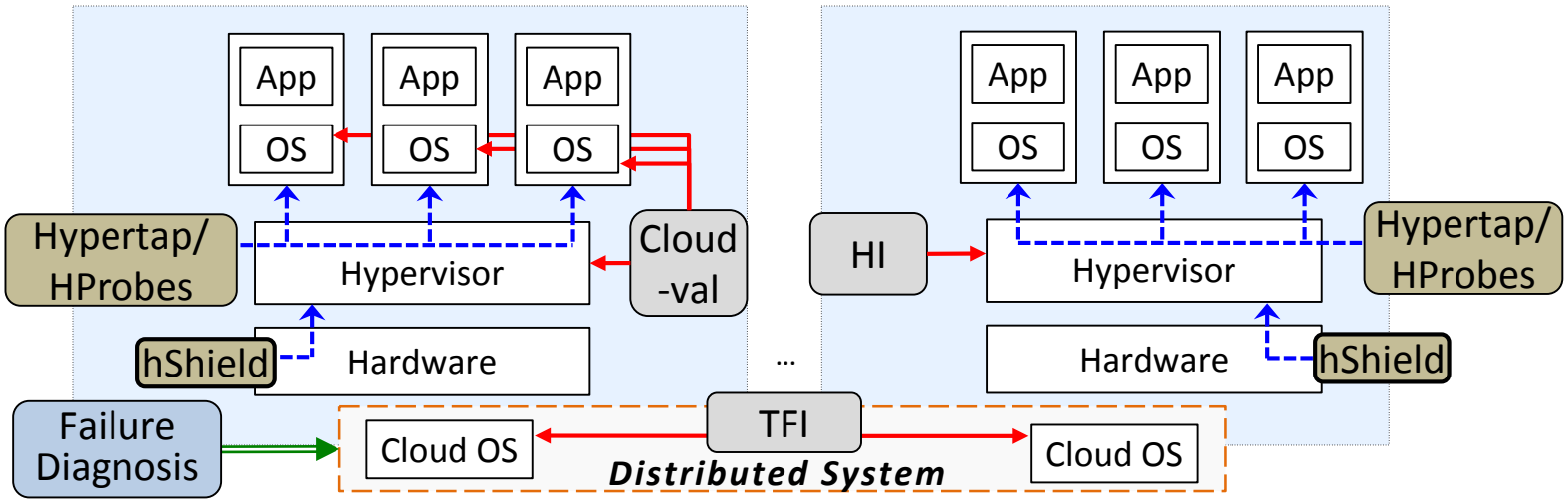
P.I. Prof. Ravishankar Iyer,

Prof. Zbigniew Kalbarczyk

Project Summary

- Project
  - Building resilient virtual machines: protection against failures and attacks
- Approach
  - Low-cost continuous monitoring
  - Measurement-driven designs
  - Leverage virtualization
  - Examples: HyperTap, Hprobes, hShield

Progress Summary



Assessment

→ **Fault/Attack Injection**

- **CloudVal:** Virtualized SW
- **TFI**: Cloud management
- **HI**: Attack Hypervisor-based monitoring

Detection

--→ **Continuous Monitoring**

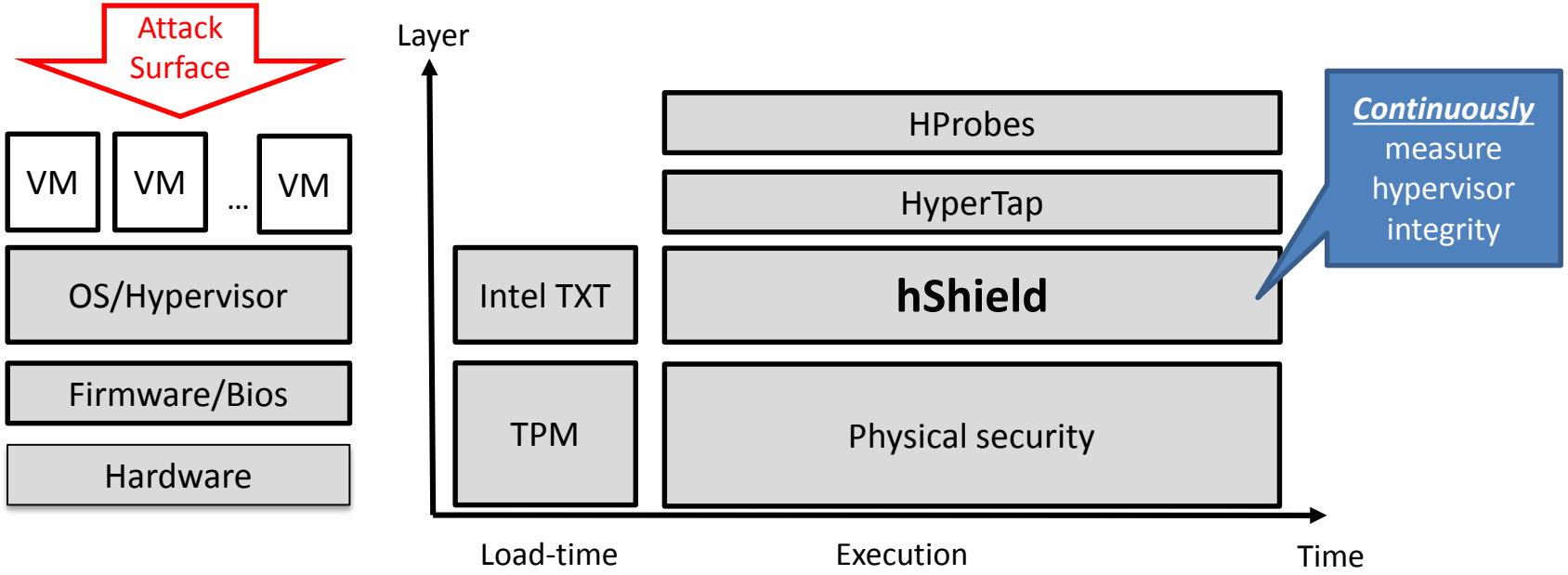
- **Hypertap/HProbe:** Reliability & Security monitoring of VMs
- **hShield**: protect hypervisor

Recovery

⇒ **Automated Diagnosis**

- **Failure diagnosis** of cloud management system

Hypervisor Runtime Integrity Measurement



- Assumption: Hardware is trusted
  - TPM, Intel TXT are enabled
  - Physical security

U.S. AIR FORCE

Characterization and Adaptive Control of Cost-Performance Tradeoffs for Modern Cloud Systems

Muntasir Raihan Rahman

P.I. Indranil Gupta

Muntasir Raihan Rahman

- **PCAP** and **GeoPCAP** (complete)
  - ***(C,A,P)*** -> ***(Pr C, Pr A, Pr P)***, characterize which combinations impossible together
  - Defined consistency (**C**) / latency(**A**) **SLA**
    - Meet ***Pr C* SLA**, optimize ***Pr A***, and vice versa
  - Built system **PCAP** which meets **PCAP SLA** for single data-center under continuously changing data-center network conditions
    - Deployed on top of **Apache Cassandra**, and **Basho Riak**
  - Extended PCAP to multiple geo-distributed data-centers
- **AdapTive Elasticity for graph Computation (AzTEC)** (current project)
  - Propose new **graph computation SLA**
    - Meet **deadline**, optimize **cost**
    - Meet **cost**, optimize **completion time**
  - Adaptive control of scale in/out to meet SLA without oscillations
  - Challenges
    - Continuous and faithful measure of graph computation progress
    - Given current progress, find best schedule

U.S. AIR FORCE

Security and Isolation in Containers

Mohammad Ahmad, Sibin Mohan, Rakesh Bobba,

P.I. Roy Campbell

Background

- Container benefits
  - Startup on the order of milliseconds
  - Packaging dependencies & portability
- Container usage
  - Platform as a Service Clouds
  - Openshift, DotCloud
- Cross container side-channel attacks shown on public clouds [1]

Zhang, Yinqian, et al. "Cross-tenant side-channel attacks in paas clouds." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014.

Secure Container Framework

- Phase 1 – Defenses against cache based side-channels
  - Scheduling-based defenses
    - Security aware scheduling
    - Cache flushing
  - Exploring hardware support
    - Intel Cache Allocation Technology to isolate tenants
  - Evaluate the performance overhead with various configurations

U.S. AIR FORCE

Cloud-Routed Overlay Networks

Chris Cai

P.I. Roy Campbell

Topic

- Can we use servers publicly available from cloud providers like Amazon to build overlay network? If so, what level of performance gain can we expect?

Questions to Answer

- What percentages of users can expect to benefit from cloud-routed overlay network?
- Does the performance gain depend on the geographic location of the users?
- Are the performance gains transient or persistent over long period of time?
- What is the proper routing strategy within cloud-routed overlay network?

U.S. AIR FORCE

Toward Fabric: A Middleware Implementing High-level Description Languages on a Fabric-like Network

Sayed Hadi Hashemi
Shadi Abdellahi
John Bellessa
Roy H Campbell

U.S. AIR FORCE

- Current Work:
  - Fabric Networks: Core Network, Edge Network.
  - Stop back practice.
  - An “approximate” implementation of Fabric
    - Syntax → MPLS
    - Protocol → Shadow MACs (i.e., layer-2 labels)
    - Implementation (hardware/protocol) → OpenFlow
  - High Performance. Very Large Scaled.
  - Immediate Update. Zero Packet Lost in Changes.
  - Submitted in ACM Middleware 2015
- Plans for the year:
  - Adaptation for Mobile Computing.
  - Prepare submission to NSDI.

Architecture