EPA-RIMM: A Framework for Dynamic SMM-based Runtime Integrity Measurement

Brian Delgado

Portland State University / Intel

Tejaswini Vibhute, Cody Shepherd, John Fastabend

PI: Prof. Karen L. Karavanic

May 24, 2018

Opinions expressed are my own.

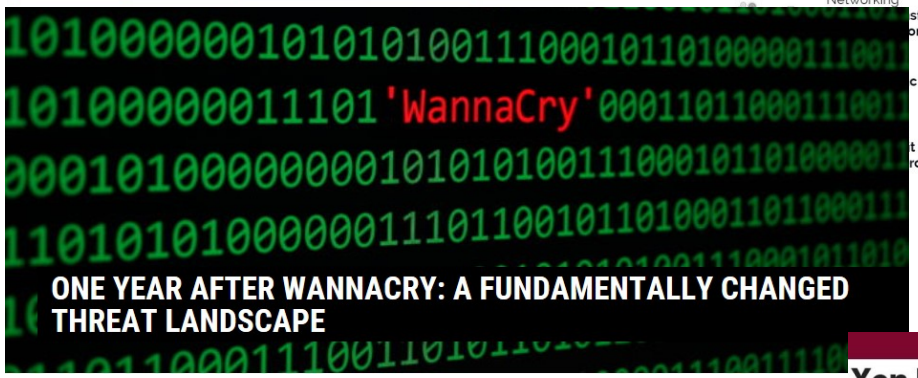
Bigger than Heartbleed, 'Venom' security vulnerability threatens most datacenters

Security researchers say the zero-day flaw affects "millions" of machines in datacenters around the world.

By Zack Whittaker for Zero Day | May 13, 2015 -- 12:00 GMT (05:00 PDT) | Topic: Cloud

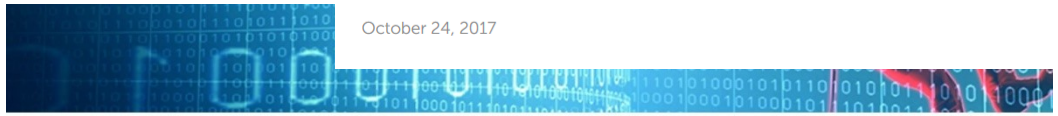
RELATED STORIES

Networking



Bad Rabbit: A new ransomware epidemic is on the rise

October 24, 2017



MANAGE

New cloud threats as attackers embrace the power of cloud

by Kathleen Richards
Information Security

Safeguarding your critical data is getting harder as threat actors embrace the advantages -- and missteps -- of cloud. Here's what to wa

The Register®
Biting the hand that feeds IT

CENTER SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Data Center ▸ Cloud

Xen bug latest: Cloudpocalypse averted, says Amazon

No mass reboot needed after all, despite latest Xen vulns

By Neil McAllister in San Francisco 2 Mar 2015 at 23:41 SHARE ▼

Amazon Web Services now says that despite the recent security vulnerabilities discovered in the Xen hypervisor, the vast majority of its Elastic Compute Cloud (EC2) customers won't need to reboot their virtual machine instances after all.

Last week, AWS and Rackspace both said that customers should prepare for a mass reboot of their instances to address as-yet-unrevealed vulnerabilities in the Xen software that underlies both companies' clouds

Xen hypervisor faces third highly critical VM escape bug in 10 months

The Xen paravirtualization mode is proving to be a constant source of seri vulnerabilities, allowing attackers to escape from virtual machines

By Lucian Constantin
Romania Correspondent, IDG News Service | MAY 3, 2017

ZDNet

EDITION: US VIDEOS SMART CITIES WINDOWS 10 CLOUD INNOVATION SECURITY TECH PRO MORE NEWSLETTERS ALL WRITERS

MUST READ YOUR FORGOTTEN IOT GADGETS WILL LEAVE A DISASTROUS, TOXIC LEGACY

Hypervisors: The cloud's potential security Achilles heel

A cloud is only as secure as the hypervisors that support its virtual machines and how secure are those? That's a darn good question and one we tend to avoid looking at.

By Steven J. Vaughan-Nichols for Linux and Open Source | March 29, 2014 -- 01:25 GMT (18:25 PDT) | Topic: Virtualization

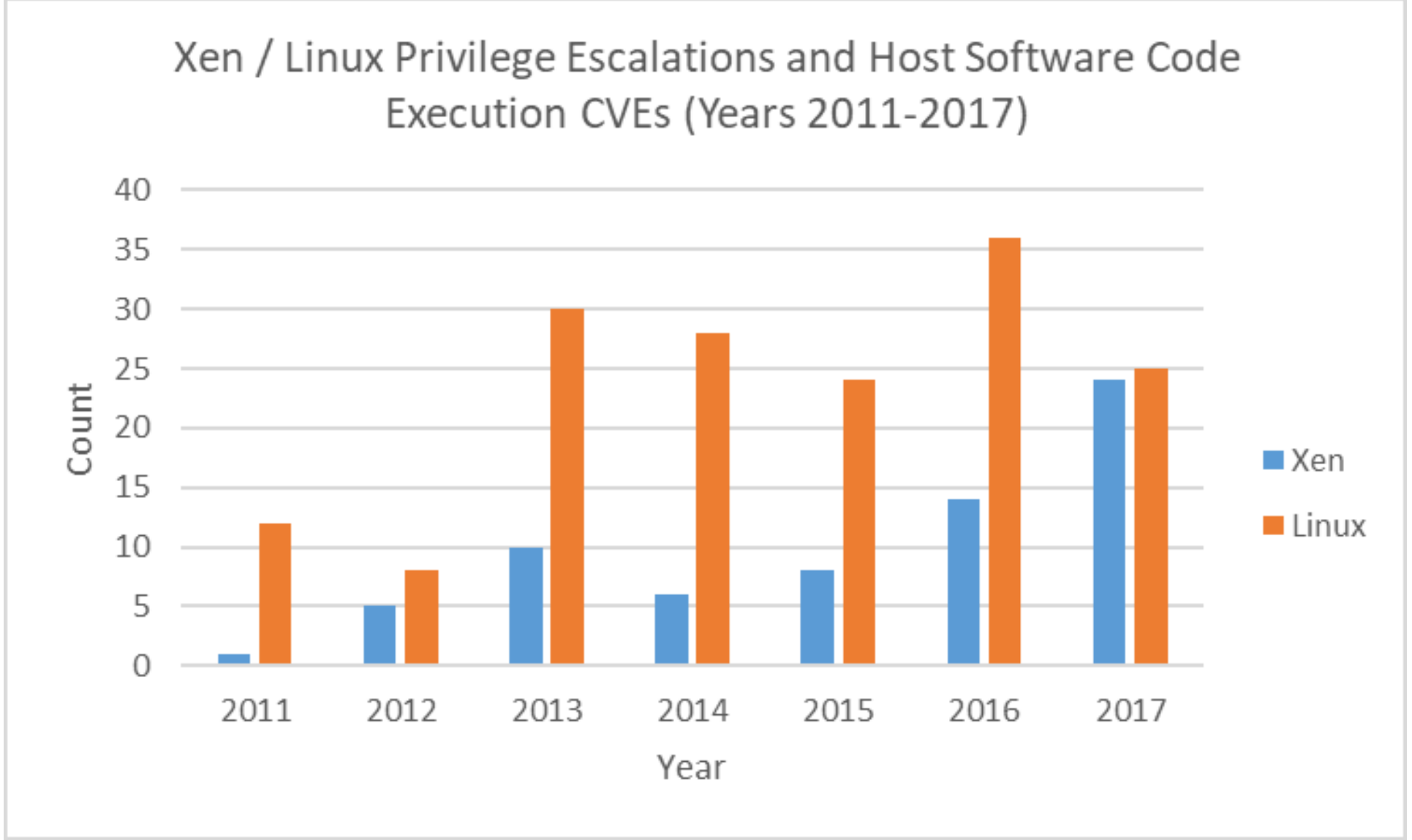
XenProject.org

RSAConference | Where the world talks security

MENU

The Future of Cloud Security Starts with the Hypervisor

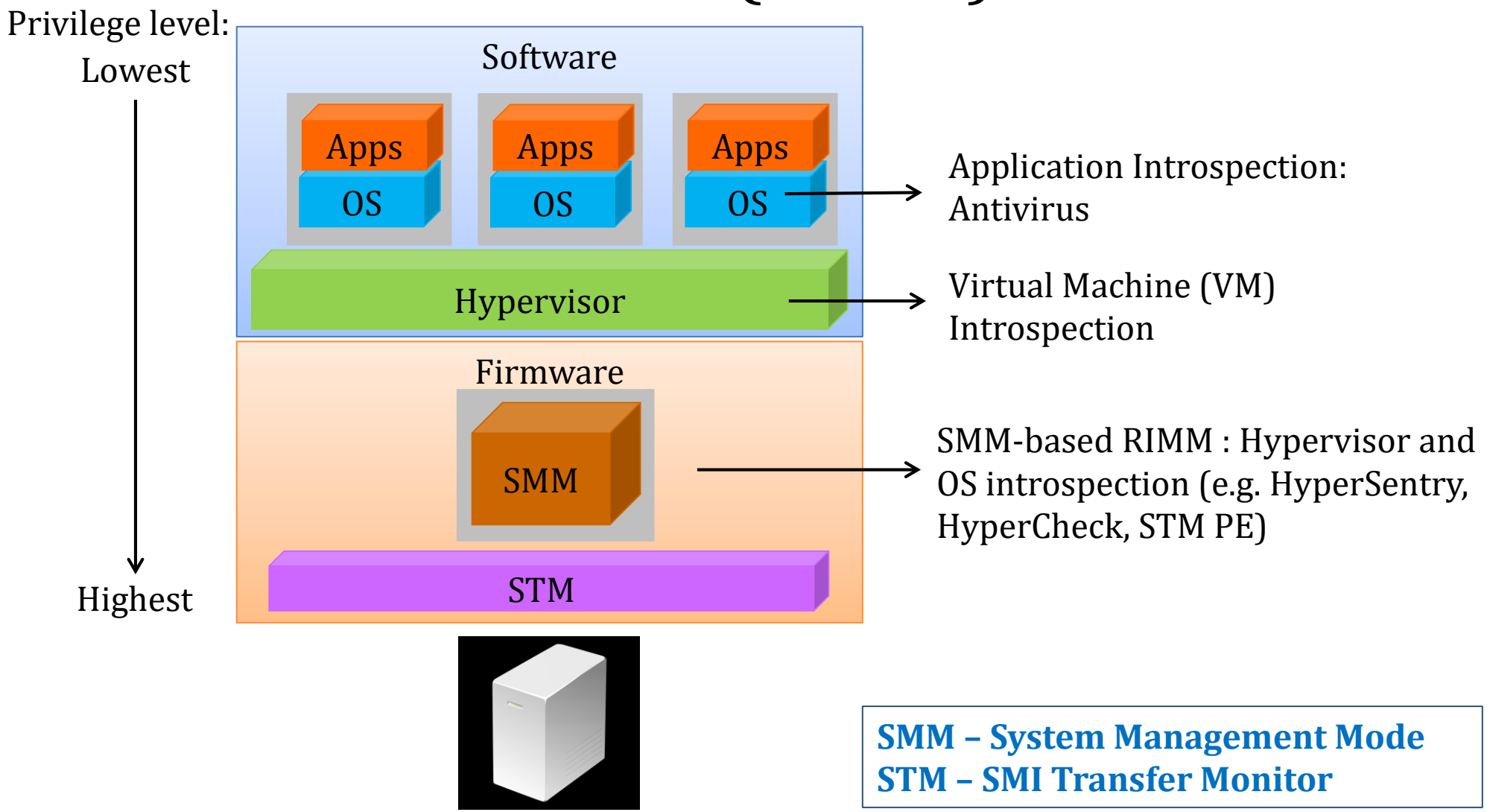
The worldwide x86 server virtualization market is expected to reach $5.6 billion in 2016, and Gartner estimates it has reached its peak, having significantly matured. OS container-based virtualization and cloud computing have gained in popularity, with organizations' server virtualization rates reaching up to 75 percent.



Privilege escalations, arbitrary writes, on x86 Linux/Xen, Years 2011-2017

cve.mitre.org

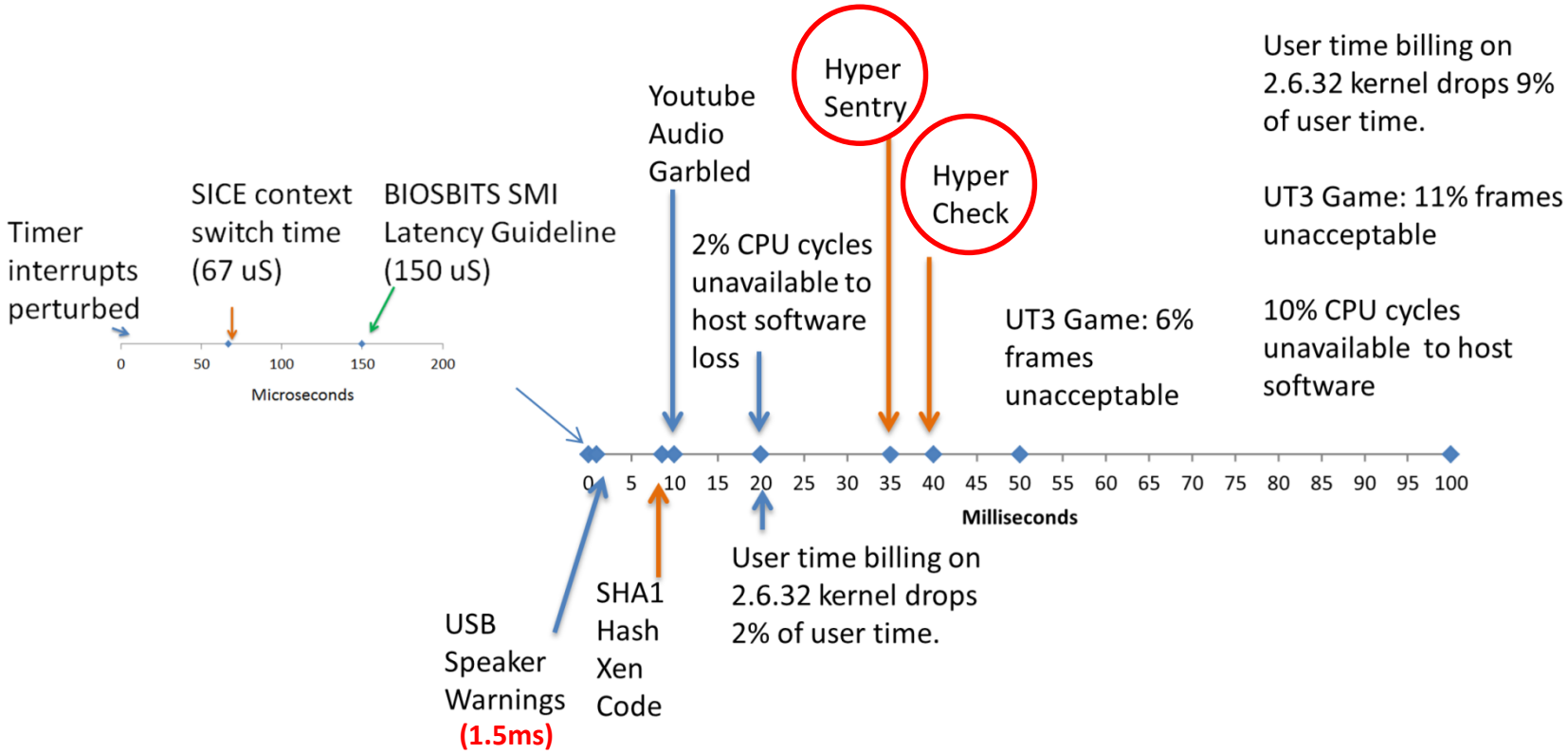
Runtime Integrity Measurement Mechanisms(RIMM)



SMM – System Management Mode
STM – SMI Transfer Monitor

SMI Performance Cost Challenge

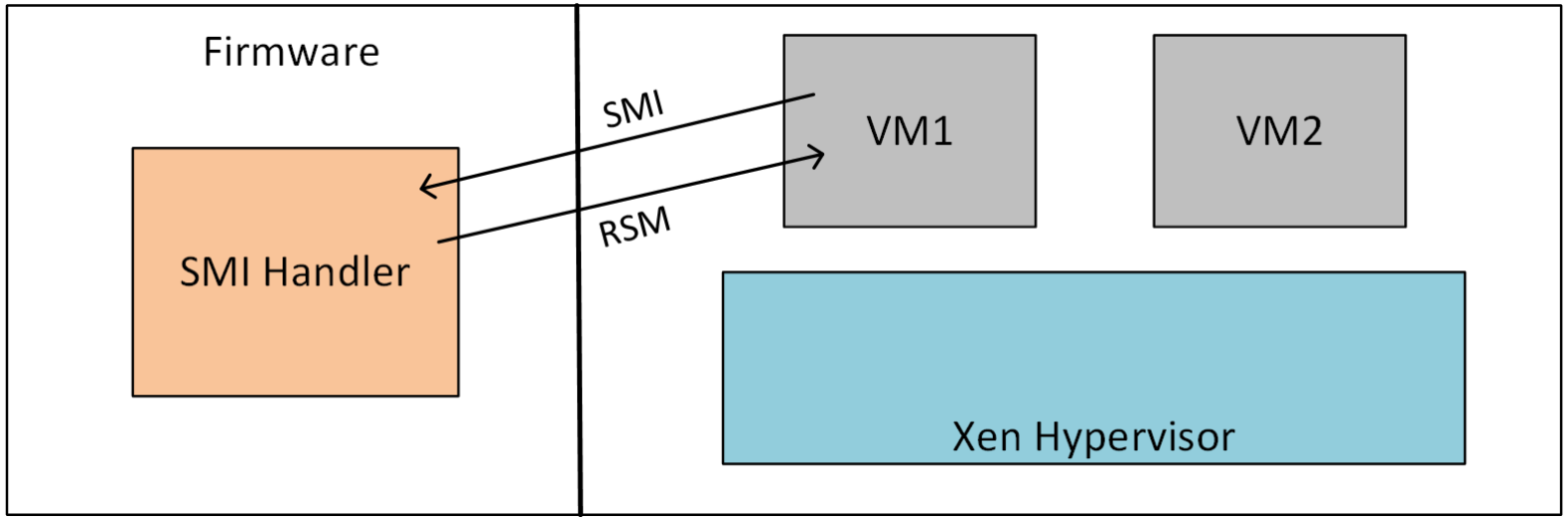
- SMI execution cost < 0.15ms - Intel BITS [3]
- Clear evidence of negative system and application performance beyond 1.5ms SMI duration



http://web.cecs.pdx.edu/~karavan/research/SMM_IISWC_preprint.pdf

Additional SMM-RIMM Challenges

1. Traditional SMM approaches lack reliable access to hypervisor state



2. Traditional SMM approaches do not apply the principle of least privilege to the measurement agent.

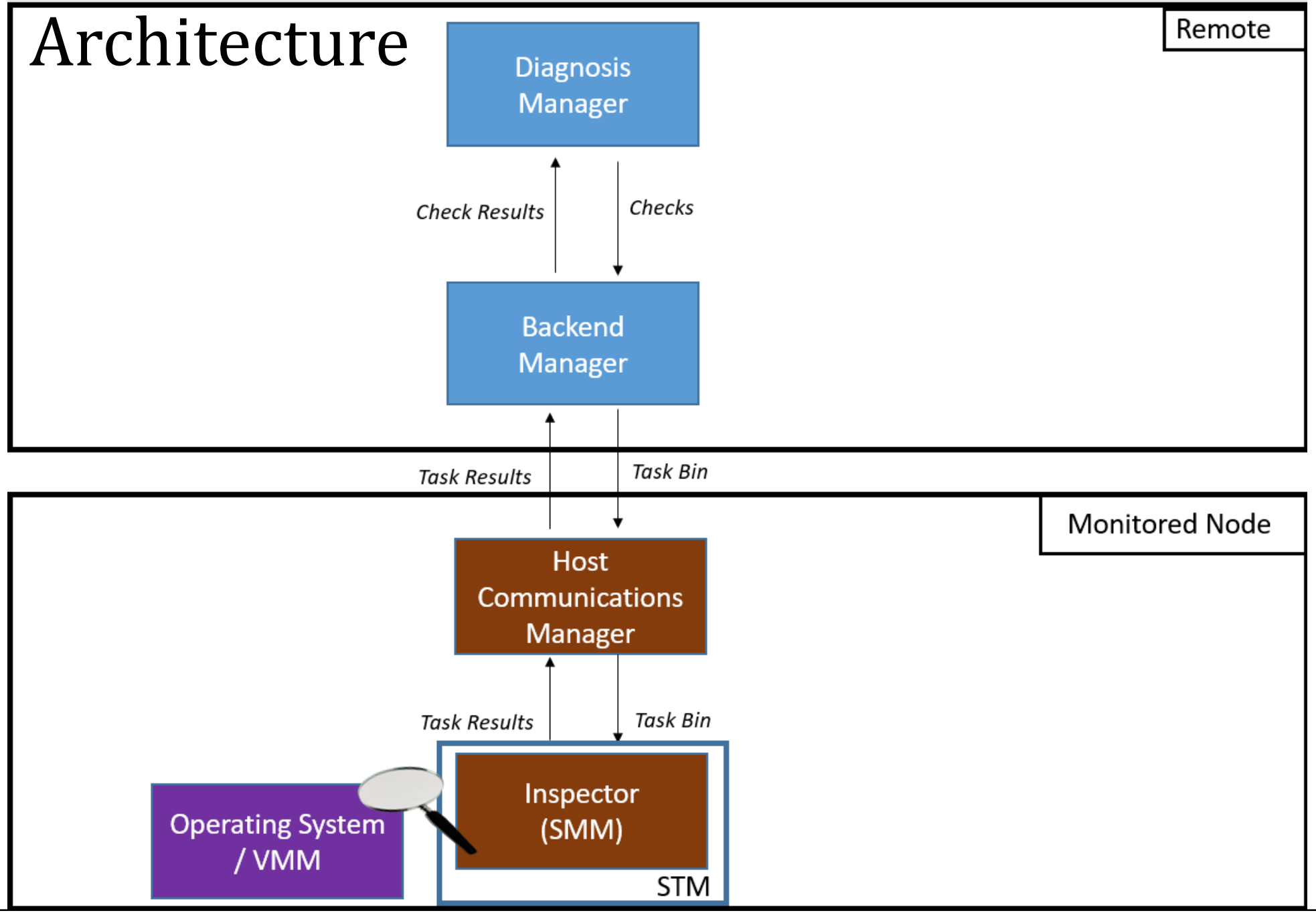
EPA-RIMM Overview

Purpose: Detect persistent rootkits in hypervisors / operating systems by identifying unexpected changes in system state

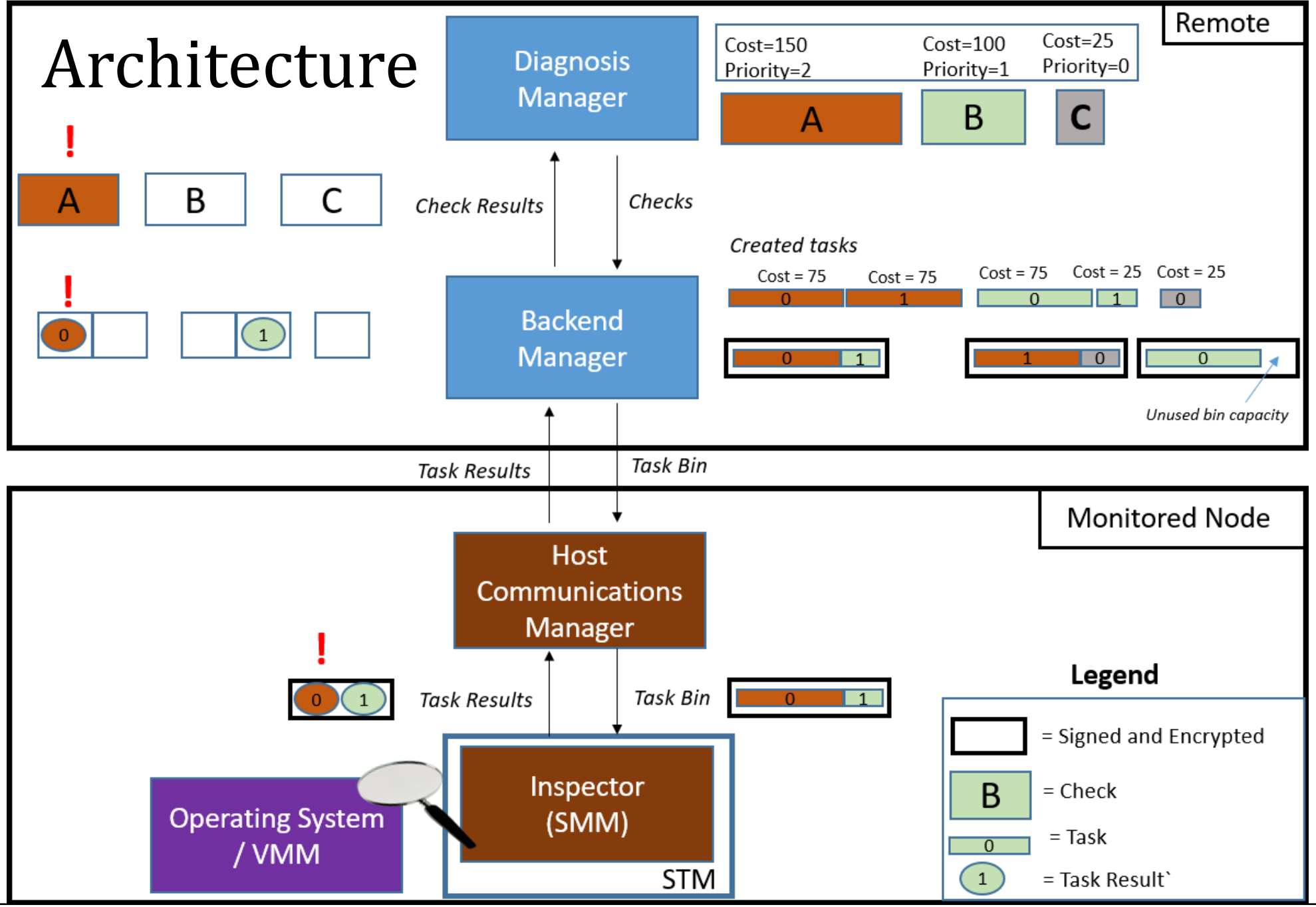
Features:

- SMM-based measurement agent runs in de-privileged virtual machine of STM
- Tunable performance impact reduces SMI times close to SMI latency guideline
- Flexible measurement API
    - Dynamically vary measured resources
    - Avoids need to build host software (VMM/OS) layout into measurement agent
- Can obtain proper hypervisor state due to STM's native understanding of host software VMCS

Architecture



Architecture



EPA-RIMM Detections

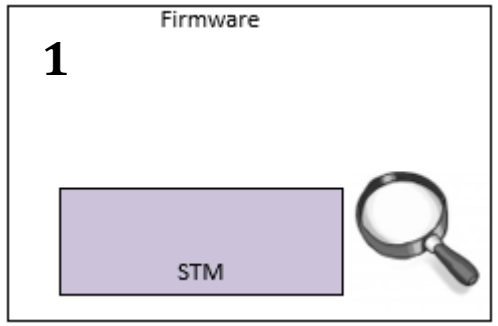
Attack	Example	Measure	Check Operands
IDT Hooking	Phrack IDT	Reg VM	IDTR IDT
CR4.SMEP Disable	Sage	Reg	CR4
Kernel Rootkit Code Injection	Snakso, WannaCry, Locky, Bad Rabbit	VM	4K Kernel Code
Xen Rootkit Code Detection	Exploited Venom vulnerability	VM	4K Hypervisor Code
System Call Hooking	f0rb1dd3n's sys_call_hijack	VM Reg	4K Kernel RO CR0

EPA-RIMM vs. Other SMM-based RIMMs

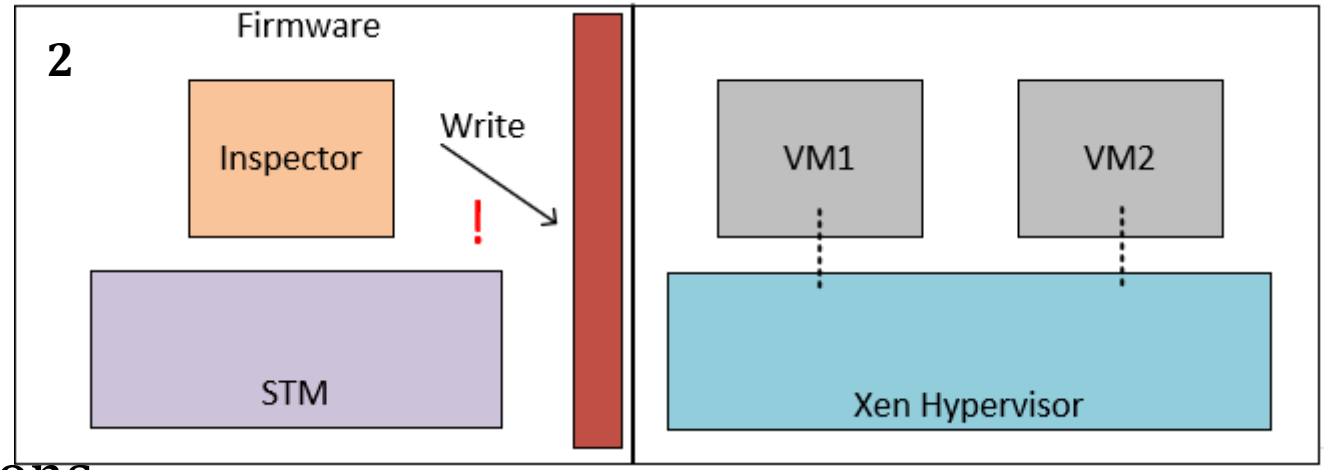
SMM RIMM	SMI Duration	Frequency
HyperCheck	40ms	1 per second
HyperSentry	35ms	1 per 8 or 16 second
SPECTRE	5 to 32ms	16 per second to 1 per 5 seconds
EPA-RIMM (no STM) Minnowboard	0.26ms+	Dynamic
EPA-RIMM (with STM) Minnowboard	0.28ms+	Dynamic
Upper Bound on SMM cost	1.5ms	Not specified
Intel BIOS BITS Guideline	0.15ms	Not specified

EPA-RIMM Security Overview

1. STM code measured by TXT AC Module



2. EPA-RIMM reduces privileges of measurement agent
   - Via STM policy – memory, MSRs, I/O …



3. Encrypted / authenticated communications

4. Exports hashes and alerts

5. Measurement Agent : 2.4K lines of code

Conclusions

EPA-RIMM:

- Detects persistent host software rootkits/ransomwares via light-weight measurements
- Can flexibly measure low-level VMM / OS resources
- Operates with reduced privileges according to STM protection policy

Thank you

- **Contacts:**
  - Brian Delgado: bdelgado@pdx.edu
  - Karen Karavanic: karavan@pdx.edu
- **EPA-RIMM Tech Report:** A Framework for Dynamic SMM-based Runtime Integrity Measurement (Arxiv) https://arxiv.org/pdf/1805.03755
- **Performance Implications of SMM** (IEEE IISWC 2013): http://web.cecs.pdx.edu/~karavan/research/SMM_IISWC_preprint.pdf

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. 1528185. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.