Boston University Red Hat Collaboratory

BOSTON UNIVERSITY

RED HAT COLLABORATORY AT BOSTON UNIVERSITY
MICROARCHITECTURE WORKSHOP

Wednesday Feb 20, 2019, 10:00 AM – 4:00 PM

Hariri Institute for Computing
111 Cummington Mall, Room 180
Boston, MA 02215

Reception to follow at Eastern Standard
528 Commonwealth Ave, Boston (Kenmore Square)

The Red Hat Collaboratory at Boston University will be holding a Microarchitecture Workshop (with a focus on security) on February 20, 2019 10:00 AM – 4:00 PM at the Hariri Institute for Computing, Boston University. The event will convene faculty, graduate students, and industry participants working in the microarchitecture area to share research and ideas as well as open doors to future collaborations.

Agenda

- **9:30 - 10:00 AM - Check-In, Coffee & Networking**
- **10:00 – 10:15 AM – Introductory Remarks**
  - Ari Trachtenberg, Boston University
  - Jon Masters, Red Hat
- **10:15 – 11:45 AM – Colloquium Series Talk and Q&A**
  - Microarchitectural Security, Daniel Gruss, Assistant Professor, Graz University of Technology
- **11:45 – 12:40 pm – Lunch**
- **12:40 – 1:40 pm – Lightning Talks: Architecture**
  - Devesh Tiwari (NEU)
  - Ajay Joshi (BU) – BlackParrot: An Open Source RISC-V Multicore Processor for and by the World
  - Yifan Sun (NEU) – Enabling multi-GPU high-performance computing with memory system design
  - Ilia Lebedev (MIT) – Cryptographically Attested Secure Hardware
  - Waiman Long (Red Hat) – Linux Kernel Synchronization Primitives on Large NUMA Systems
  - Ahmed Sanaullah (BU) -Secure Reconfigurable Architectures for Cloud Computing
- **Break**
- **1:45 – 2:45 pm – Lightning Talks: Side-Channel**
  - Andrea Arcangeli (Red Hat) – Spectrev2 and reptoline on Skylake
  - Vladimir Kiriansky (MIT) – Speculative Buffer Overflow Attacks and Microarchitectural Defenses
  - Simo Sorce (Red Hat) – Dealing with cache based attacks in cryptography

  - David Starobinski (BU) – Software Defined Radio: A Swiss Army Knife for Side Channel Analysis
  - Trammell Hudson (Two Sigma) – Bringing Linux back to the server BIOS with LinuxBoot
- **Break**
- **2:55 -3:50 pm – Microarchitecture Roundtable**
  - Facilitated by Ari Trachtenberg, BU & Jon Masters, Red Hat
- **3:50 – 4:00 pm – Wrap Up and Next Steps**
  - Hugh Brock, Red Hat
- **4:00 pm – Reception**
  - Eastern Standard, 528 Commonwealth Ave, Boston (Kenmore Square)

Talk Abstracts and Speaker Bios

Microarchitectural Security
Daniel Gruss, Assistant Professor, Graz University of Technology

Abstract: Microarchitectural security problems arise from optimizations and implementation decisions that comply with the architectural model functionally. However, (implicit) assumptions on isolation and security are often undermined. In this talk we will illustrate how microarchitectural attacks are similar to physical sidechannel and fault attacks. In the second half of the talk we will focus on transient execution attacks as a new category of microarchitectural attacks. We will discuss Meltdown and Spectre as well as more recent transient execution attacks.

Bio: Daniel Gruss (@lavados) is an Assistant Professor at Graz University of Technology. He finished his PhD with distinction in less than 3 years. He has been involved in teaching operating system undergraduate courses since 2010. Daniel's research focuses on software-based side-channel attacks that exploit timing differences in hardware and operating systems. He implemented the first remote fault attack running in a website, known as Rowhammer.js. He frequently speaks at top international venues, such as Black Hat, Usenix Security, IEEE S&P, ACM CCS, Chaos Communication Congress, and others. His research team was one of the teams that found the Meltdown and Spectre bugs published in early 2018.

Achieving Multiple (Conflicting) Objectives on Power-Constrained HPC Systems with Provable Guarantees
Devesh Tiwari, Assistant Professor, Northeastern University

Abstract: Continued progress in high-performance computing (HPC) has enabled computational scientists to expedite scientific discovery, but the high power consumption of large-scale systems is one of the top ten challenges for future exascale systems. This limited power availability requires intelligent

methods of providing high system throughput at low power budgets. In this talk, I will introduce a new feedback-based principled approach to improve system throughput and achieve fairness among concurrently running applications.

Bio: Devesh Tiwari is an Assistant Professor at Northeastern University, where his research group innovates new solutions to make large-scale computing system more efficient, reliable, and sustainable. Before joining academia, I worked as a staff scientist at the US Department of Energy (DOE) Oak Ridge National Laboratory. Email: tiwari@northeastern.edu

---

BlackParrot: An Open Source RISC-V Multicore Processor for and by the World
Ajay Joshi, Associate Professor, Boston University

Abstract: In this talk, I'll provide an overview of our current project on the development of an open source RISC-V Multicore Processor. This project is funded under the DARPA POSH program, which is focused on designing and open sourcing commonly used hardware blocks. I'll discuss our interface-based design approach, which has enabled our team (spread across three states) to work together seamlessly on the design of BlackParrot. I'll present BlackParrot's architecture and also briefly introduce opportunities for designing a secure BlackParrot processor.

The ultimate goal of this project is to design a "Linux of RISC-V Cores", which will ultimately be owned and developed by the wider computing community.

Bio: Ajay Joshi received his Ph.D. degree from the ECE Department at Georgia Tech in 2006. He then worked as a postdoctoral researcher in the EECS Department at MIT. In 2009, he joined the ECE department at Boston University, where he is currently an Associate Professor. He was a Visiting Researcher at Google in 2017-18. His research interests span across various aspects of VLSI design including circuits and architectures for communication and computation. He received the NSF CAREER Award in 2012, Boston University ECE Department's Award for Excellence in Teaching in 2014 and Best Paper Award at ASIACCS 2018.

He currently serves as the Associate Editor for IEEE Transactions on VLSI Systems.

Enabling multi-GPU high-performance computing with memory system design
Yifan Sun, Ph.D. Student, Northeastern University

Abstract: GPUs have demonstrated its high performance and memory efficiency in processing dataparallel workloads in fields including large scale physics simulation, signal processing, and machine learning. With the growth of the data to be processed by GPUs, single GPU can no longer meet the requirement of data scientists and using multiple GPUs has become a common solution. However, according to our study, CPU-GPU and inter-GPU data migration and communication can be a major

performance bottleneck of multi-GPU systems. Recent GPU programming features such as unified memory can further deteriorate multi-GPU system performance, voiding the effort of adding more computing resources.

To improve multi-GPU system management, we propose two approaches that utilizing the programmer knowledge of the algorithm and utilizing the hardware runtime information. The first approach is Locality API, which allows the programmer to explicitly specify which GPU should hold a piece of memory. The second approach is Progressive Page-Splitting Migration (PASI), which allows the GPU hardware to gradually adjust the data placement to reduce data migration. We evaluate both the approaches with MGSim, a newly-developed GPU simulator dedicated for multi-GPU system simulation. With MGSim, we can model multi-GPU systems and memory organizations that cannot be simulated by other publicly-available simulators. Our evaluation shows that Locality API and PASI can achieve a speedup of 3.5X and 2.5X, respectively.

Bio: Yifan Sun is a Ph.D. student of the Department of Electrical and Computer Engineering Department at Northeastern University under the advisory of Dr. David Kaeli. His research interest lies in heterogeneous system architecture and computer architecture simulation. He received a Master of Science degree from the Department of Electrical Engineering of University at Buffalo in 2013 and received a Bachelor of Science degree from the Department of Electronic Science and Technology of Huazhong University of Science and Technology in 2007.

Cryptographically Attested Secure Hardware
Ilia Lebedev, Ph.D. Student, MIT

Abstract: Trustworthy remote execution is not currently possible with commodity hardware due its weak process isolation and the necessity of including enormous privileged software in the trusted computing base of unprivileged code. By implementing secure hardware capable of strong isolation and measurement of isolated containers (enclaves) with a compelling threat model, we can provide strong guarantees and offer some firm ground upon which secure software systems can be built.

Bio: Ilia Lebedev, PhD candidate at MIT's Computer Science and Artificial Intelligence Lab, works in computer systems security, and is currently focused on remotely attested computation. His 2016 Hazen award for outstanding teaching illustrates his commitment to accessible education and outreach. Outside of his academic career, he is a sailing ship captain, a bartender, and an all-around questionable individual.

Linux Kernel Synchronization Primitives on Large NUMA Systems

Waiman Long, Software Engineer, Red Hat

Bio: Waiman Long is an experienced kernel software engineer at Red Hat, Inc. His major focus areas are kernel synchronization primitives, performance and scalability in the upstream Linux kernel as well as the Red Hat Enterprise Linux kernel. He is also a major contributor in revamping the Linux kernel synchronization primitives in recent years.

He has multiple years of working experience on Linux, HP-UX and Tru64 UNIX in both the kernel and the C runtime library. He is also an expert in the field of software internationalization.

Secure Reconfigurable Architectures for Cloud Computing
Ahmed Sanaullah, Ph.D. Student, Boston University

Abstract: The next generation of cloud computing is placing Field Programmable Gate Arrays (FPGAs) at the heart of data centers. Use of reconfigurable hardware allows us to tap into unique and exciting opportunities that are essential to support growth of clouds in terms of physical scale, function, and mission. In this talk, we will discuss some of the challenges of sharing reconfigurable hardware between Cloud Tenants and Providers, including trust models, attack surfaces and toolflows.

Bio: Ahmed Sanaullah joined Professor Martin Herbordt's Computer Architecture and Automated Design Lab in September 2015 and is currently working on secure and scalable cloud HPC using FPGAs, performance-programmability using High Level Synthesis, and real-time machine learning architectures. He has a BS in Electrical Engineering from Lahore University of Management Sciences, Pakistan and an MSc in Electrical and Electronic Engineering from The University of Nottingham, UK. He has also served as a faculty member at Lahore University of Management Sciences.

Spectrev2 and reptoline on Skylake
Andrea Arcangeli, Linux Kernal Developer, Red Hat

Abstract: On Skylake processors an RSB underflow during the "ret" instruction while in kernel can still speculatively execute kernel code at an userland mistrained branch location pulled from the BTB. So how likely is it that the Spectre-v2 retpoline mitgation might be circumvented on Skylake?

Bio: Andrea Arcangeli joined Qumranet and then Red Hat in 2008 because of his interest in working on the KVM Virtualization Hypervisor, with a special interest in virtual machine memory management. He worked on many parts of the Linux Kernel, especially on the Virtual Memory subsystem. Andrea started working with Linux in his spare time shortly after first connecting to the internet back in 1996 while

studying at University. He enjoys spending most of his time solving software problems and promoting the adoption of Linux and Open Source software everywhere.

Speculative Buffer Overflow Attacks and Microarchitectural Defenses
Vladimir Kiriansky, Ph.D. Student, MIT

Abstract: Classic "buffer overflow" attacks exploit software implementation errors, such as stack overflows, uninitialized memory, or type confusion. "Speculative buffer overflows" similarly break memory and type safety on speculative CPUs, due to arguable hardware design decisions. Developer education and software analysis tools have failed to eradicate classic buffer overflows for the last thirty years. Are we at the dawn of 30 years of fun and profit with speculative buffer overflow attacks?

Efficient hardware solutions can stop the Spectre1.1 and Spectre1.2 variants, while more complex microarchitectural solutions are needed to block all classes of speculative buffer overflow attacks.

Bio: Vladimir is a PhD student at MIT working on high-performance compilers and secure microarchitectures. Vladimir previously fought (classic) buffer overflows in academia and industry. His USENIX Security'02 paper on "program shepherding" (commercialized as Determina) introduced pragmatic buffer overflow mitigations, now used in Microsoft's CFI, and Intel's Control Enforcement Technology. After Determina got acquired by VMware, he also worked on broader hypervisor security.

Dealing with cache based attacks in cryptography
Simo Sorce, Sr. Principal Software Engineer, Red Hat

Abstract: The advent of co-located computing like virtualization and containers have elevated the value of local attacks on cryptographic engines. Recent developments show the feasibility of using CPU caches as well as microarchitecture speculation oracles to perform attacks against cryptographic primitives executed in other processes. How do we handle these issues?

Bio: Simo Sorce is a Senior Principal Software Engineer at Red Hat, he joined the company in 2007 after many years of involvement in upstream projects like Samba, where he focused on security and interoperability related topics. After joining Red Hat he co-created a number of projects like FreeIPA, SSSD, GSS-Proxy focused on simplifying or improving the security of Linux related security and authentication technologies and collaborated with upstream projects like MIT Kerberos and participated in various IETF Working groups. He recently joined the RHEL Crypto Team, as a team lead, working on RHEL's core cryptographic libraries and security certifications.

Boston University Red Hat Collaboratory

BOSTON UNIVERSITY

Software Defined Radio: A Swiss Army Knife for Side Channel Analysis
David Starobinski, Professor, BU

Abstract: We present recent research advances, including our own, on performing side channel security assessment using software defined radios.

Bio: David Starobinski is a Professor of Electrical and Computer Engineering and of Systems Engineering at Boston University, with an affiliated appointment in the Department of Computer Science. He is also a Faculty Fellow at the U.S. DoT Volpe National Transportation Systems Center. He received the B.Sc., M.Sc. and Ph.D degrees, all in Electrical Engineering, from the Technion-Israel Institute of Technology, in 1993, 1996 and 1999, respectively. During the academic year 1999-2000, he was a post-doctoral researcher in the EECS department at UC Berkeley, and in 2007-2008 he was an invited professor at the School of Computer and Communication Sciences at EPFL (Swiss Institute of Technology in Lausanne).

Dr. Starobinski received a US National Science Foundation (NSF) CAREER award and a US Department of Energy (DOE) Early Career award for his work on Quality of Service engineering and network modeling. He also received a BU ECE Faculty award for outstanding teaching performance, a fellowship for prospective researchers from the Swiss National Foundation, and awards from the Gutwirth Foundation and Intel Corp. for excellence in graduate studies. He won best paper awards at the WiOpt 2010 and IEEE CNS 2016 conferences. He is on the Editorial Board of the IEEE Transactions on Information Forensics and Security and was on the Editorial Board of the IEEE/ACM Transactions on Networking. His research interests are in cybersecurity, wireless networking, and network economics.

Bringing Linux back to the server BIOS with LinuxBoot
Trammell Hudson, SVP, Two Sigma

Abstract: https://trmm.net/LinuxBoot_34c3

Bio: Trammell Hudson is a hardware and firmware security researcher at Two Sigma Investments, LLP. He discovered the Thunderstrike vulnerability in MacBooks as well as multiple Intel firmware vulnerabilities, and is co-founder of the open source LinuxBoot server firmware project.

About the Collaboratory

A partnership between Red Hat and Boston University, the Red Hat Collaboratory connects BU faculty and students with industry practitioners working in open-source software communities. The Collaboratory aims to advance research focused on emerging technologies in a number of areas including operating systems, cloud computing services, machine learning and automation, and big data platforms.

Red Hat Collaboratory at Boston University
Hariri Institute for Computing
111 Cummington Mall, Boston, MA 02215
rhcollab@bu.edu | 617-358-6692 | bu.edu/rhcollab