Atri Bhattacharyya

Homepage: atrib.b LinkedIn: /atri-bh atri.bhattacharyya	itbucket.io attacharyya @epfl.ch	Lausanne, Vaud Switzerland		
INTERESTS	Security at the HW/SW interface: security-focused ISA e croarchitectural security. Datacenter architectures: tackli of the virtual memory abstraction	extensions, OS security, mi- ng challenges in protection		
EDUCATION	PhD candidate, Computer Science Ecole Polytechnique Federale de Lausanne, Switzerland	'18 - '24		
	MS in Computer Science Ecole Polytechnique Federale de Lausanne, Switzerland GPA: 5.73/6 (equivalent to 3.73/4)	'16 - '18		
	BT in Electrical Eng. with major in Comp. Sc. a Indian Institute of Technology Kanpur, India GPA: 9.1/10 (equivalent to 3.64/4)	nd Eng. '11 - '16		
INDUSTRY EXPERIENCE	Engineering Intern Jun '22 - Aug '22 Qualcomm, San Diego, US Worked on analyzing configurations and investigating improvements for physical- address based on-chip access control for Qualcomm products.			
	 Research Assistant August '17 - Feb '18 Oracle Labs, Zurich, Switzerland Developed a DPDK-based multi-user capable userspace-networking framework in C capable of saturating 10Gbit/s interfaces with a single core while providing the benefits of in-kernel networking: isolation, flexibility and security. Integrated the framework with a network-processing bound DDoS detection pipeline to increase its maximum throughput by around 15x. 			
	 UnnaTI Embedded Software Intern Texas Instruments, Bangalore, India Developed a profiler for cycle-wise timing of C/assem tion on an embedded platform to enable rapid profiling at Augment and verify manual benchmarking results in Benchmark, optimize TI's low-power MCU software M0+ processor Achieved > 50% improvement for a 	May '14 - July '14 bly level instruction execu- nd benchmarking to: a less than 20% of the time. and FreeRTOS on Cortex-		
RESEARCH	Secure and high-performance virtual memory com SecureCells: A Secure Compartmentalized Architecture, Rebooting Virtual Memory with Midgard SecureCells proposes a novel virtual memory architect hardware-enforced intra-address space isolation of compar on Midgard and RISC-V, using virtual memory areas (V protection and translation. For SecureCells, we ported the stack including an OS (seL4), the GNU compiler toolch also created two implementations, modifying QEMU en BocketChip FPCA	partmentalization <i>IEEE S&P'23.</i> <i>ISCA'21</i> cture for high-performance ctments. SecureCells builds MAs) as the granularity of he full RISC-V software hain and benchmarks. We mulator and the RISC-V		

Skills: C, RISC-V, QEMU, gcc, seL4, Linux

Systematic data race protection for the kernel

Midas: Systematic Kernel TOCTTOU Protection Usenix SEC'22 Midas is a systematic and comprehensive protection mechanisms for OS kernels to defend against Time-of-Check-to-Time-of-Use attacks. I modified kernel APIs, creating a multiversioning system for userspace data, assuring the kernel that user data accessed from a system call remains immutable and userspace is not blocked. Skills: Linux kernel development, C

Speculative side-channel exploitation

SpecROP: Speculative Exploitation of ROP ChainsRAID'20SMoTherSpectre: Exploiting speculative execution through port contention CCS'19SMoTherSpectre presents a speculative-execution attack using port contention as
a side-channel, enabling leakage of private key from OpenSSH server. SpecROP lever-
ages binary analysis and improves attacks by speculatively chaining code gadgets
leveraging the CPU's prediction structures, enabling previously impossible leakage
scenarios.

Skills: Side-channel exploitation, binary analysis, CPU microarchitecture

Optimizing LSQ generation for High-Level Synthesis

Shrink It and Shred It! Minimize the Use of LSQs in Dataflow Designs FPT'19 **Developed an optimized load-store queue design** for dynamically-scheduled elastic circuits for high-level synthesis, using an **LLVM analysis pass** to determine temporal-ordering between memory operations to reduce the estimated hardware cost for LSQs by as much as 93%.

Skills: LLVM, FPGA programming

SKILLS Programming: C/C++, Java, LATEX Python (>5000 LoC), Assembly(x86, ARMv6, RISC-V), VHDL, Shell(Bash) (>1000 LoC), Scala, Matlab. Simulators: SimFlex, gem5 Software: QEMU, Linux kernel, LLVM, GNU compiler toolchain, seL4

ACHIEVEMENTS	'23	23 Qualcomm Innovation Fellowship, Europe		
AND AWARDS	'21, '22		Best TA Award, EPFL	
	'20		IBM Research Fellowship	
	'18		EPFL IC School Fellowship	
	'16		MS Research Scholarship, EPFL	
	'12 Univer	sity level	Academic Excellence Award	
TEACHING	Undergraduate	CS212	Systems Programming Project (S'19)	
S=Spring	Undergraduate	CS323	Introduction to Operating Systems (F'19, F'20, F'21)	
F=Fall	Graduate	CS412	Software Security (S'20, S'21)	
	Graduate	CS422	Database Systems (S'18)	
	Graduate	COM402	Internet Security and Privacy (F'22, F'23)	
TALKS	IEEE S&P '23	Secur	eCells: A Secure Compartmentalized Architecture	
	Usenix Security	'22 Mida	s: Systematic Kernel TOCTTOU Protection	
	RAID '20	SPEC	CROP: Speculative Execution of ROP chains	
	CCS '19	SMo	TherSpectre: Exploiting spec. exec. through port contention	
SERVICE	Reviewer ACM	I Computir	ng Surveys (CSUR)	
	Reviewer ACM Transactions on Computers			