Nathan Dautenhahn

Address:	Moore 102, 200 South 33rd Street, Philadelphia PA, 19104
Phone:	(217) 689-1133
Email:	ndd@cis.upenn.edu
Website:	nathandautenhahn.com

Research Interests

Cybersecurity; Systems; Virtualization; Compilers; Security Microarchitecture; Static and Dynamic Program Analysis

Education

Ph.D. Computer Science ◇ University of Illinois at Urbana-Champaign ◇ August 2016 ◇ Advisor: Vikram S. Adve
Dissertation: Protection in Commodity Monolithic Operating Systems

B.S. Computer Engineering ◇ University of New Mexico ◇ December 2008 ◇ Advisor: Gregory L. Heileman

Publications

Conference

Lei Shi, Yuming Wu, Yubin Xia, Nathan Dautenhahn, Haibo Chen, Binyu Zang, Haibing Guan, and Jingming Li. Deconstructing Xen. In *Proceedings of the 24th Network and Distributed System Security Symposium*, NDSS '17, San Diego, California, USA, 2017. The Internet Society.

Will Dietz, Joshua Cranmer, Nathan Dautenhahn, and Vikram Adve. Slipstream: Automatic Interprocess Communication Optimization. In *Proceedings of the 2015 USENIX Conference on Usenix Annual Technical Conference*, USENIX ATC '15, pages 431–443, Berkeley, CA, USA, 2015. USENIX Association.

Nathan Dautenhahn, Theodoros Kasampalis, Will Dietz, John Criswell, and Vikram Adve. Nested Kernel: An Operating System Architecture for Intra-Kernel Privilege Separation. In *Proceedings of the 20th International Conference on Architectural Support for Programming Languages and Operating Systems*, ASPLOS '15, pages 191–206, New York, NY, USA, 2015. ACM.

John Criswell, Nathan Dautenhahn, and Vikram Adve. Virtual Ghost: Protecting Applications from Hostile Operating Systems. In *Proceedings of the 19th International Conference on Architectural Support for Programming Languages and Operating Systems*, ASPLOS '14, pages 81–96, New York, NY, USA, 2014. ACM.

John Criswell, Nathan Dautenhahn, and Vikram Adve. KCoFI: Complete Control-Flow Integrity for Commodity Operating System Kernels. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, SP '14, pages 292–307, Washington, DC, USA, 2014. IEEE Computer Society.

Gilles Pokam, Klaus Danne, Cristiano Pereira, Rolf Kassa, Tim Kranich, Shiliang Hu, Justin Gottschlich, Nima Honarmand, Nathan Dautenhahn, Samuel T. King, and Josep Torrellas. QuickRec: Prototyping an Intel Architecture Extension for Record and Replay of Multithreaded Programs. In *Proceedings of the 40th Annual International Symposium on Computer Architecture*, ISCA '13, pages 643–654, New York, NY, USA, 2013. ACM.

Nima Honarmand, Nathan Dautenhahn, Josep Torrellas, Samuel T. King, Gilles Pokam, and Cristiano Pereira. Cyrus: Unintrusive Application-level Record-replay for Replay Parallelism. In *Proceedings of the Eighteenth International Conference on Architectural Support for Programming Languages and Operating Systems*, ASPLOS '13, pages 193–206, New York, NY, USA, 2013. ACM.

Hui Xue, Nathan Dautenhahn, and Samuel T. King. Using replicated execution for a more secure and reliable web browser. In *Proceedings of the 19th Network and Distributed System Security Symposium*, NDSS '12, San Diego, California, USA, 2012. The Internet Society.

Shuo Tang, Nathan Dautenhahn, and Samuel T. King. Fortifying Web-based Applications Automatically. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 615–626, New York, NY, USA, 2011. ACM.

Workshop

Anupam Datta (CMU), Matt Fredrikson (CMU), Joel Hypolite (UPenn), Andrew Myers (Cornell), Jonathan Smith (UPenn), Andre Scedrov (UPenn), Carolyn Talcott (SRI), and Nathan Dautenhahn (UPenn). De-Inductive Reasoning and Explanation for Cybersecurity Threats (DIRECT). In *Workshop on Forming an Ecosystem Around Software Transformation*, FEAST '16, Vienna, Austria, October 2016.

Partha Pal, Rick Schantz, Michael Atighetchi, Kurt Rohloff, Nathan Dautenhahn, and William Sanders. Fighting Through Cyber Attacks: An Informed Perspective toward the Future. In *Workshop on Survivability in Cyber Space (Invited Paper)*, 2010.

Thesis

Nathan Dautenhahn. *Protection in Commodity Monolithic Operating Systems*. PhD thesis, University of Illinois at Urbana-Champaign, August 2016.

Nathan Dautenhahn. *Design and Implementation of a Reputation-Based Trust Prototype Using Persistently Identified NeTworking Research Framework*. Undergraduate thesis, University of New Mexico, 2008.

Poster

Joana MF da Trindade, Cuong Pham, and Nathan Dautenhahn. Poster: μBeR: A Microkernel Based Rootkit for Android Smartphones. Technical report.

Invited Talks

Nested Kernel: An Operating System Architecture for Intra-Kernel Privilege Separation. IBM. October 3, 2016. Cisco. April 11, 2016. École Polytechnique Fédérale de Lausanne (EPFL). Lausanne, Switzerland. March 11, 2015. University of Cambridge Computer Laboratory Security Seminar. Cambridge, United Kingdom. March 10, 2015.

Medical Plug-n-Play (MDPnP). University of New Mexico Electrical and Computer Engineering Department. Albuquerque, New Mexico. June 2009.

Technical Reports

Mark Torgerson, Richard Schroeppel, Tim Draelos, Nathan Dautenhahn, Sean Malone, Andrea Walker, Michael Collins, and Hilarie Orman. The SANDstorm Hash. *Submission to NIST*, 2008.

Edward L. Witzke, John M. Eldridge, Mark M. Miller, Dallas J. Wiener, and **Nathan Dautenhahn**. Final Report for the Network Authentication Investigation and Pilot. (SAND2006-7078), November 2006.

Patents

Nathan Dautenhahn, J.E. Gottschlich, G.A. Pokam, C.L. Pereira, S. Hu, K. Danne, and R. Kassa. Mechanism for facilitating dynamic and efficient management of instruction atomicity volations in software programs at computing systems. September 2014. WO Patent App. PCT/US2013/032,640.

Research Experiences

Graduate Assistant ◇ University of Illinois at Urbana-Champaign ◇ August 2009 – May 2016

Slipstream: Automatic Interprocess Communication Optimization: Advised on project direction; organized and directed tasks; organized and wrote several sections of the paper; and mentored student writing and organization skills.

Nested Kernel: An Operating System Architecture for Intra-Kernel Privilege Separation: Devised the Nested Kernel architecture; design and implementation of PerspicuOS, the x86-64 realization of the Nested Kernel including investigating Intel manuals for identifying methods to bypass the MMU protection and subsequent solutions; the memory protection services to protect kernel data structures; the use cases to explore the viability of the Nested Kernel architecture. Additionally, organized and wrote a significant portion of the ASPLOS paper.

KCoFI: Complete Control-Flow Integrity for Commodity Operating System Kernels: Developed the x86-64 MMU page table implementation; evaluated performance of CFI; and evaluated the CFI implementation using the AIR metric and automated return-oriented programming tools.

Virtual Ghost: Protecting Applications from Hostile Operating Systems: Developed the VirtualGhost x86-64 MMU page table implementation and ported FreeBSD PMAPS subsystem to utlize VirtualGhost MMU functionality. Additionally, implemented MMU update verification so that the operating system is denied access to maliciously modify the MMU, thereby, protecting application memory.

QuickRec: Prototyping an Intel Architecture Extension for Record and Replay of Multithreaded Programs: Designed and implemented a chunk and input deterministic based replay system in a Pin tool. Simulated and successfully replayed TSO relaxed memory model race conflicts. Additionally, participated in debugging the Quickrec RnR prototype hardware implementation and successfully found several bugs such as miscounting of instructions on floating point exceptions.

Using Replicated Execution for a More Secure and Reliable Web Browser: Developed a browser extension for Firefox, Chrome, and Opera that provided core functionality of an *opportunistic-n-version* programming approach to detecting and masking browser-based exploits.

Tor Fingerprinting Attack: Developed a passive fingerprinting attack against the Tor network with the goal of identifying the webpage a given Tor client is viewing by eavesdropping on the connection between the Tor client and Tor entry router. I examined several mathematical approaches for classifying an unknown fingerprint (frequency distribution of the number of packets at given sizes) to a database of known websites; in the end I selected an entropy based metric – Kullback-Leibler divergence – which identifies how divergent a given probability distribution is from another.

Automated Intrusion Detection Investigation and Response System (IDIRS): Performed literature survey on intrusion detection systems, security ontologies, information fusion, and alert correlation and aggregation systems. Identified that information fusion provided theoretical framework but lacked practical applications and alert correlation and aggregation systems were practical but lacked sufficient theoretical underpinnings to be effective. Proposed a combined approach that considers both spatial and temporal elements within an information network including host and network based sensors.

Undergraduate Student ◇ University of New Mexico ◇ August 2004 – December 2009

Future Network Technology Research: Designed and implemented a reputation based intrusion detection system that used the Persistent Identification and NeTworking research framework (PINT), which is an implementation of a Transient Network Architecture. PINT uses persistent identifiers to provide location independent routing, thus, allowing stronger relationships to be placed upon packet origins. This work resulted in my undergraduate thesis.

Medical Plug-n-Play (MDPnP): Reviewed IEEE specifications on MDPnP and converted those ideas into a design for a prototype system to be used in an operating room environment. I provided research into the communications specification and the models used to represent patient data in a health care provider network. Additionally, I developed an implementation of the IEEE specification, which required me to build several specific cables and test serial port communication at the electronic level.

Teaching Experiences

Teaching ◇ University of Illinois at Urbana-Champaign ◇ January 2012 – May 2016

Advanced Operating Systems (Teaching Assistant CS 523) I participated in leading discussion sections, providing feedback and mentoring for authoring project proposals, and providing office hours to discuss project directions.

Doctoral Education Perspectives Seminar (Primary Instructor for CS 591) Created and taught a seminar that seeks to fundamentally clarify uncertainty about the PhD through examination, reflection, and discussion by examining diverse perspectives from influential leaders in the field and existing doctoral education research.

Mentoring ◇ University of Illinois at Urbana-Champaign ◇ January 2012 – May 2016

Lucian Mogosanu (Doctoral Candidate) (2015 - Present) Kernel Control-Flow Integrity and Code-Pointer Integrity

Imani Palmer (Junior Doctoral Candidate) (2015 - Present) Docker security analysis

Will Dietz (Junior Doctoral Candidate) (2014 - 2016) Slipstream and the Nested Kernel

Thodoris Kasampalis (Junior Doctoral Candidate) (2014 - 2016) Nested Kernel and static analysis debugging

Ashish Bijlani (Junior Doctoral Candidate) (2015 - 2016) Driver isolation in the Linux kernel

Ranran Li (Sophomore Undergrad) and Priya Mehta (Freshman Undergraduate) (Fall 2014) Nested Kernel buddy memory allocator

Wooyoung Chung (Senior Undergrad) and George Karavaev (Senior Undergrad) (Fall 2009) TorFA: Tor Fingerprint Attack using Kullback-Leibler divergence

Service Experiences

Service Activities ◇ University of Illinois at Urbana-Champaign ◇ January 2011 – May 2016

PURE Research Mentor (FA14): The PURE research program is focused on integrating first and second year undergraduate students into full research projects. I have mentored and led two undergraduate research students to design and build a buddy allocator for the new Nested Kernel Operating System Architecture.

Peer Reviewer (2013): Participated as a peer reviewer for the journal IEEE Transactions on Information Forensics & Security.

Engineering Graduate Student Advisory Committee (2014): As a member of EGSAC I am tasked with the mission of advising the Dean of the College of Engineering on topics that are important to graduate education and that impact the graduate student experience on campus. The Engineering Graduate Student Advisory meets regularly with the Director of Graduate and Professional Programs, the Associate Dean of Graduate and Professional Programs and the Dean of Engineering to bring forward ideas and concerns facing engineering graduate students.

Computer Science Graduate Academic Council (2013,2014): The graduate academic council is a select group of UIUC graduate students who are tasked with identifying, analyzing, and implementing seminars, policies, and programs to enhance the quality of the CS graduate student program.

Graduate Ambassador (2010,2011,2012,2013): I participate as a primary point of contact in the recruitment process of prospective graduate students.

Graduate Admissions Committee (2014): I participated as a voter on a team of approximately 15 individuals determining which graduate students would be admitted to UIUC.

Graduate Admissions Reviewer (2012,2014): I participated in reviewing UIUC CS graduate school candidate admissions. My responsibilities included reviewing all candidate application materials and ranking students. I provided this feedback to the admissions committee. I also identified key candidates and connected their submissions with faculty best matched to their skill set.

Graduate Mentor (2012,2013,2014): I participate as a mentor for incoming graduate students. The primary goal is to aid in their transition from undergraduate to graduate life in addition to exposing them to graduate life at UIUC. I am passionate about transferring the knowledge I have gained during graduate school to aid new students.

Work Experience

Student Intern ◇ Intel Labs ◇ May 2012 – January 2013

Deterministic Record and Replay: Responsible for debugging, designing, implementing, and verifying a HW-assisted record and replay system built on an FPGA prototype record mechanism. Participated in the identification of several bugs in the HW prototype, devised and implemented replay algorithms (in Pin) for challenging corner cases of real HW record system, and implemented a testing framework for evaluation of the record and replay system. Efforts resulted in the filing of a patent and conference paper publication (ISCA 2013).

Student Intern ◇ Sandia National Laboratories ◇ June 2004 – May 2007 and August 2007 – February 2010

Java Deployment: Worked on a Java development application. Worked extensively with ANT builds and application deployment, as well as maintaining web servers, such as BEAs Web Logic Server.

Network Authentication: Researched, designed, and implemented an 802.1x port based authentication system.

Web Application: Developed and wrote web applications in Ruby, Groovy, and PHP, including MySQL database back-end development.

Hashing Algorithms: Implemented the SANDSTORM hashing algorithm, an entry into the SHA3 hashing algorithm competition moderated by NIST.

Red Teaming exercise: Performed design assurance and system evaluation.

Student Intern ◇ Pacific Northwest National Laboratories ◇ May 2007 – August 2007

SCADA Security: Developed a security system for SCADA networks, built live CDs, studied security concerns related to the current SCADA infrastructure, and researched Trusted Computing. Specifically, built a live Gentoo CD from scratch, using a chrooted environment to build the kernel, boot manager, and applications.

Skills

- Proficient Languages: C, C++, Perl, Ruby
- Familiar Languages: Java, PHP, Python, Shell Scripting, Groovy, MySQL
- Linux Kernel Development: APIC configuration, interrupt handlers, scheduling, context switch, and trap handlers
- FreeBSD Kernel Development: virtual memory PMAPs specific port to prototype virtualiztion environment
- Pin: Dynamic Binary Instrumentation Tool
- Performance Monitor Counters
- LLVM Compiler Infrastructure: Optimization passes, instrumentation at LLVM IR and Machine Code IR
- Version Control Systems: SVN and Git
- MapReduce and Hadoop
- Browser Extension development: Firefox, Chrome, and Opera
- Knowledge of 802.1x standards and authentication system design including supplicant, NAS, and Radius server
- Understanding of EAP types and methods, i.e. TLS, PEAP-MSCHAPV2 etc.
- Server Administration
- ANT builds
- Java application deployment
- Router/Switch configuration for CISCO and Foundry

Awards and Honors

- Qualcomm Innovation Fellowship (QInF) Finalist (2012)
- Qualcomm Innovation Fellowship (QInF) Finalist (2011)
- Andrew and Shana Laursen Fellow for 2009-2010 at the University of Illinois at Urbana-Champaign
- Breece Award (Top GPA in School of Engineering at University of New Mexico)
- Department of Homeland Security Scholarship
- Presidential Scholarship at UNM
- Recipient of the Association of Old Crows Scholarship and the Christopher E. Evangel Memorial Scholarship
- NSF STEM Scholarship
- Spot Recognition Award (SNL), Defense Programs Award of Excellence (SNL)
- Computer Engineering Sophomore and Junior of the Semester at UNM
- University Honors Program Summa cum laude
- Honors Roll and Deans list every semester
- National Society of Collegiate Scholars Member, member of Etta Kappa Nu and Phi Kappa Phi, and invited to be in Tau Beta Pi

References available upon request.