Nathan Dautenhahn

Email: ndd@cis.upenn.edu
Website: nathandautenhahn.com
Phone: (217) 689-1133
Address: Levine Hall room 302
3330 Walnut Street
Philadelphia, PA 19104

Research Interests

Security & Privacy, Systems, Program Representation and Analysis, Security Architecture

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
  Thesis: Design and Implementation of a Reputation-Based Trust Prototype Using Persistently Identified NeT-working Research Framework

Awards and Honors

- Qualcomm Innovation Fellowship Finalist ('11, '12 Cash Award).
- Graduate Student Outstanding Ambassador Award ('14 UIUC)
- Andrew and Shana Laursen Fellow ('09-'10 UIUC)
- Breece Award (Top GPA in School of Engineering in graduating class at UNM Fall '08)
- Department of Homeland Security Scholarship ('06-'08 at UNM)
- UNM Presidential Scholarship ('04-'06)
- Association of Old Crows Scholarship ('08-'09 UNM)
- Christopher E. Evangel Memorial Scholarship ('08-'09 UNM)
- NSF STEM Scholarship ('08-'09 UNM)
- Spot Recognition Award ($100 Sp '05 SNL)
- Defense Programs Award of Excellence (Fa'05 SNL)
- University of New Mexico Honors Program Summa Cum Laude (Honors College Special Program)
- Honors Roll and Deans list every semester (UNM)
- National Society of Collegiate Scholars Member, member of Etta Kappa Nu and Phi Kappa Phi, and invited to be in Tau Beta Pi

Positions

[5/2016 – Present] Postdoctoral Researcher. University of Pennsylvania.

- Led research on automated decomposition, evolution, and verification of commodity systems in REVOLVER (ONR BAA Grant) including: a) μSCOPE automated policy derivation (Planned USENIX SEC '18), b) SLICE efficient memory separation mechanism (Planned submission OSDI'18), and c) COLT automated transformation verification.
- Led research on hardware support for memory safety and control-flow integrity projects: a) NFP a multi-threaded full system shadow stack abstraction and XGPS hardware control-flow reference monitor (Submitted Eurosys'18) and b) MicroStache memory safety and CPU side-channel defense mechanism (Submitted Eurosys'18).
- Direct research on a) programmable microarchitectural safety policies (HALCYON), b) BreakApp third-party module decomposition in JavaScript (PLOS'17, NDSS'18), and c) learning to reason for systems and networking defense including: 1) PHD fast and slow learning and 2) DeepMatch heterogeneous work distribution for network deep packet inspection (Submitted SOAR'18).

[8/2009 – 5/2016] Graduate Assistant. University of Illinois at Urbana-Champaign.

- Created the Nested Kernel architecture and FreeBSD implementation PerspicuOS (ASPLOS'15) and directed and co-authored Nexen, retrofitted Xen Nested Kernel (NDSS'17).
- Developed OS protection and confinement (KCoFI (SP'14) and VirtualGhost (ASPLOS'14)).
- Developed Deterministic record and replay (Capo3 and PinCap for hardware assisted R&R (ASPLOS'13, ISCA'13)).
- Developed web browser automated security (Cocktail web browser (NDSS'12) and Xan web browser security retrofitting (CCS'11)).
- Directed and co-authored automated host-local network optimizations (Slipstream (ATC'15)).

[5/2012 – 1/2013] Student Intern. Intel Labs.

- Invented relaxed consistency model replay emulation techniques (US Patent).
- Designed and implemented the PinCap replay system, and special debugging techniques that validated the QuickRec x86 record system.

[5/2007 – 8/2007] Student Intern. Pacific Northwest National Laboratories.

- Investigated and developed SCADA system defense with immutable state environments.

[6/2004 – 2/2010] Student Intern. Sandia National Laboratories (SNL).

- Piloted 802.1x deployment (SAND2006-7078).
- Implemented SANDSTORM hashing algorithm for NIST SHA-3 competition (NIST'08).

Research Grants

Sponsor:	Office of Naval Research
Award #:	BAA N00014-17-S-B010
Title:	REVOLVER: Recurrent EVOLution and Verification of Encapsulated Rights
Award:	$853,600 (Unversity of Pennsylvania full award)
Duration:	3 years (September 1, 2017 - September 20, 2020)
PIs:	Steve Zdancewic (PI), Nathan Dautenhahn (Co-PI), Jonathan M. Smith (Co-PI)

Tools and Source Code

- Nested Kernel: `http://nestedkernel.org`.
  PerspicuOS: `https://github.com/nestedkernel/PerspicuOS`
- Linux fine grained memory tracing with Memorizer:
  `https://github.com/linuxkit/linuxkit/tree/master/projects/memorizer`
- KCoFI and VirtualGhost: `https://github.com/jtcriswell/SVA`
- XGPS: Available upon request
- TorFA: `https://github.com/ndauten/Tor-Fingerprint-Attack`
- Miscellaneous: `https://github.com/ndauten`

Papers in Preparation

S.1 **Nathan Dautenhahn**, Lucian Mogosanu, Matthew Hicks, and Lucas Davi. The Missing Context: An Execution Spacetime for Warping Attack Geometry. In *submission to European Conference on Computer Systems (EuroSys)*, 2018.

S.2 **Nathan Dautenhahn**, Jai Pandey, Imani Palmer, Derrick McKee, Chris Akatsuka, Vasileios P. Kemerlis, Mathias Payer, Adam Bates, Vikram Adve, André DeHon, and Jonathan M. Smith. Under the μSCOPE: Analyzing Least-Privilege Separation in Monolithic Operating Systems. In *preparation for USENIX Security (USENIX Sec)*, 2018.

S.3 Lucian Mogosanu, Ashay Rane, and **Nathan Dautenhahn**. MicroStache: A Hardware Enforced Abstraction for Sensitive Data Isolation. In *submission to European Conference on Computer Systems (EuroSys)*, 2018.

S.4 Joel Hypolite, John Sonchack, Shlomo Hershkop, **Nathan Dautenhahn**, André DeHon, and Jonathan M. Smith. DeepMatch: Practical Deep Packet Inspection on P4 Hardware. In *submission to the Symposium on SDN Research (SOAR)*, 2018.

S.5 Lucian Mogosanu, Adrian Dobrica, Volodymyr Kuznetsov, George Candea, and **Nathan Dautenhahn**. KASM: Precise Protection of Operating System Kernels Against Control-Flow Hijacks. In *preparation for USENIX Security (USENIX Sec)*, 2018.

Publications

Papers with more than 5 citations are listed from Google Scholar as of January '18. Total Citations: 319. h-index: 8.

Refereed Conference

C.1 Nikos Vasilakis, Ben Karel, Nick Roessler, **Nathan Dautenhahn**, André DeHon, and Jonathan M. Smith. BreakApp: Automated, Flexible Application Compartmentalization. In *To Appear in 25th Annual Network and Distributed System Security Symposium*, (NDSS '18), San Diego, CA, USA, 2018. The Internet Society.

C.2 Lei Shi, Yuming Wu, Yubin Xia, **Nathan Dautenhahn**, Haibo Chen, Binyu Zang, Haibing Guan, and Jinming Li. Deconstructing Xen. In *24th Annual Network and Distributed System Security Symposium*, (NDSS '17), San Diego, CA, USA, 2017. The Internet Society.

C.3 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.

C.4 **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 Twentieth International Conference on Architectural Support for Programming Languages and Operating Systems*, (ASPLOS '15), pages 191–206, New York, NY, USA, 2015. ACM. (cited by 24).

C.5 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. (**cited by 83**).

C.6 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. (**cited by 110**).

C.7 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. (cited by 23).

C.8 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. (cited by 23).

C.9 Hui Xue, **Nathan Dautenhahn**, and Samuel T. King. Using replicated execution for a more secure and reliable web browser. In *19th Annual Network and Distributed System Security Symposium*, (NDSS '12), San Diego, CA, USA, 2012. The Internet Society. (cited by 13).

C.10 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. (cited by 29).

Patents

P.1 **Nathan D. Dautenhahn**, Justin E. Gottschlich, Gilles Pokam, Cristiano L. Pereira, Shiliang Hu, Klaus Danne, and Rolf Kassa. Mechanism for facilitating dynamic and efficient management of instruction atomicity violations in software programs at computing systems, Noermber 22, 2016. U.S. Patent Number 9,501,340. Filed Mar 15, 2013. Issued: Nov 22, 2016.

Refereed Workshop

W.1 Nikos Vasilakis, Ben Karel, Nick Roessler, **Nathan Dautenhahn**, André DeHon, and Jonathan M. Smith. Towards Fine-grained, Automated Application Compartmentalization. In *Workshop on Programming Languages and Operating Systems*, (PLOS'17), Shanghai, China, October 2017. ACM.

W.2 Anupam Datta, Matt Fredrikson, Joel Hypolite, Andrew Myers, Jonathan Smith, Andre Scedrov, Carolyn Talcott, and **Nathan Dautenhahn**. De-Inductive Reasoning and Explanation for Cybersecurity Threats (DIRECT). In *Workshop on Forming an Ecosystem Around Software Transformation*, (FEAST '16), Vienna, Austria, October 2016.

W.3 Mark Torgerson, Richard Schroeppel, Tim Draelos, **Nathan Dautenhahn**, Sean Malone, Andrea Walker, Michael Collins, and Hilarie Orman. The SANDstorm Hash, 2008. Presented at First SHA-3 Candidate Conference by NIST in 2009. http://energy.sandia.gov/wp-content/gallery/uploads/SANDstorm_Submission_2008_10_30.pdf (cited by 8).

Theses

T.1 **Nathan Dautenhahn**. *Protection in Commodity Monolithic Operating Systems*. PhD thesis, University of Illinois at Urbana-Champaign, August 2016. Advisor: Vikram S. Adve.

T.2 **Nathan Dautenhahn**. *Design and Implementation of a Reputation-Based Trust Prototype Using Persistently Identified NeTworking Research Framework*. Undergraduate thesis, University of New Mexico, 2008. Advisor: Gregory L. Heileman.

Poster

P_o.1 Joana MF da Trindade, Cuong Pham, and **Nathan Dautenhahn**. Poster: μBeR: A Microkernel Based Rootkit for Android Smartphones, May 17 - 20, 2009. Oakland, CA, USA. 30th IEEE Symposium on Security & Privacy.

Technical Reports

T_r.1 Edward L. Witzke, John M. Eldridge, Mark M. Miller, Dallas J. Wiener, and **Nathan Dautenhahn**. Final Report for the Network Authentication Investigation and Pilot. Tech Report SAND2006-7078, Sandia National Laboratories, Albuquerque, NM, USA, November 2006. http://prod.sandia.gov/techlib/access-control.cgi/2006/067078.pdf.

Invited Talks

1. Nested Kernel: A Protection Architecture for Intra-Kernel Privilege Separation. Princeton University (12/17).
2. Nested Kernel: A Protection Architecture for Intra-Kernel Privilege Separation. UCSD (12/17).
3. Nested Kernel: A Protection Architecture for Intra-Kernel Privilege Separation. University of Washington (12/17).
4. Nested Kernel: A Protection Architecture for Intra-Kernel Privilege Separation. Harvard University (11/17).
5. Opportunistic Privilege Separation and Memorizer: LinuxKit Special Interest Group (6/17).
6. Protection in Monolithic Operating Systems. University of Arizona (10/16).
7. Protection in Monolithic Operating Systems. IBM (10/16).
8. Nested Kernel: An Operating System Architecture for Intra-Kernel Privilege Separation. Cisco (4/16).
9. Protection in Monolithic Operating Systems. University of Georgia Institute of Technology (3/16).
10. Protection in Monolithic Operating Systems. University of Pennsylvania (3/17).
11. Protection in Monolithic Operating Systems. University of Wisconsin-Madison (3/16).
12. Nested Kernel: An Operating System Architecture for Intra-Kernel Privilege Separation. University of California Berkeley (10/15).
13. Nested Kernel: An Operating System Architecture for Intra-Kernel Privilege Separation. FreeBSD Developer Conference (6/15).
14. Nested Kernel: An Operating System Architecture for Intra-Kernel Privilege Separation. École Polytechnique Fédérale de Lausanne (EPFL). Lausanne, Switzerland (3/15).
15. Nested Kernel: An Operating System Architecture for Intra-Kernel Privilege Separation. University of Cambridge Computer Laboratory Security Seminar. Cambridge, United Kingdom (3/15).
16. Nested Kernel: An Operating System Architecture for Intra-Kernel Privilege Separation. Information Trust Institute, University of Illinois at Urbana-Champaign (3/15).
17. Balancing Graduate Life and Family. CS Department University of Illinois at Urbana-Champaign (3/13 and 3/14).
18. Medical Plug-n-Play (MDPnP). University of New Mexico Electrical and Computer Engineering Department. Albuquerque, New Mexico. (6/09).

Press

Hacker News (03/16/17). Deconstructing Xen (NDSS'17): `https://goo.gl/C1b8Sf`
Discover Magazine (12/19/16). Expert interview of Google Fuchsia: `https://goo.gl/bDzrcC`
Reddit (11/17/15). Nested Kernel (ASPLOS'15): `https://goo.gl/j7N8eV`
Hacker News (top article 04/17/15). Nested Kernel (ASPLOS'15): `https://goo.gl/FVdK3G`

Service

Program Committee

Security	USENIX Security Symposium: 2018.
ICDCS	International Conference on Distributed Computing Systems: 2018.
SP	IEEE Symposium on Security and Privacy: 2017 (shadow PC).

Journal and Grant Referee

ISF	Israel Science Foundation (Grant Agency): 2017.
TDSC	IEEE Transactions on Dependable and Secure Computing: February 2017.
TIFS	IEEE Transactions on Information Forensics and Security: May 2013.

External Review Committee

SP	IEEE Symposium on Security and Privacy: 2016.
OSDI	USENIX Symposium on Operating Systems Design and Implementation: 2014.
ATC	USENIX Annual Technical Conference: 2012.

Advisory and Service. University of Illinois at Urbana-Champaign. January 2011 – May 2016

Engineering Graduate Student Advisory Committee (EGSAC) (2014): Advised the Dean of the College of Engineering on graduate education student experience.

Computer Science Graduate Academic Council (CSGAC) (2013,2014): Identified, analyzed, and implemented seminars, policies, and programs for CS graduate students.

Graduate Ambassador (2010,2011,2012,2013): Recruiting lead for prospective graduate students.

Graduate Admissions Committee (2014): Voting member for graduate student admissions (ERC in '12).

Teaching and Mentoring

Mentoring as Doctoral Student and Postdoc

Lucian Mogosanu (Ph.D. December 2017 University POLITEHNICA of Bucharest) (2015 - Present)
Kernel Code-Pointer Integrity using Nested Kernel, NFP, XGPS, and MicroStache.
Ph.D. Thesis: Verification and Enforcement of Security in Systems Software

Imani Palmer (Ph.D. December 2017 UIUC) (2015 - Present)
Docker security analysis, OPS, μSCOPE.
Ph.D. Thesis: Forensic Analysis of Computer Evidence

Lei Shi (Undergrad Shanghai Jiao Tong University + Junior Doctoral Candidate UPenn) (2016 - Present)
Nexen (NDSS'17) and SLICE mechanism

Joel Hypolite (Junior Doctoral Candidate UPenn) (2016 - Present)
PHD, PHAST, and DeepMatch

Derrick McKee (Junior Doctoral Candidate Purdue) (2017 - Present)
Privilege analysis for μSCOPE, OPS, and SLICE

Will Dietz (Senior Doctoral Candidate UIUC) (2014 - Present)
Slipstream (ATC'15) and the Nested Kernel (ASPLOS'15)

Theodoros Kasampalis (Junior Doctoral Candidate UIUC) (2014 - 2016)
Nested Kernel (ASPLOS'15) and static analysis debugging

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

Jai Pandey (Master's Candidate UIUC) (2016 - Present)
μSCOPE memory tracing tool and policy analysis

Phillip Trent (Senior Undergraduate Student UPenn) (2017 - Present)
KeepAway: Analysis and Protection of Secrets in the Linux Kernel

Christopher Akatsuka (Senior Undergraduate Student UPenn) (Sp 2017)
Building tracing infrastructure for OPS

Ranran Li (Sophomore Undergraduate Student UIUC) (Fall 2014)
Nested Kernel buddy memory allocator

Priya Mehta (Freshman Undergraduate UIUC) (Fall 2014)
Nested Kernel buddy memory allocator

Wooyoung Chung (Senior Undergraduate Student UIUC) (2009-2011)
TorFA: Tor Fingerprint Attack using Kullback-Leibler divergence

George Karavaev (Senior Undergraduate Student UIUC) (Fall 2009)
TorFA: Tor Fingerprint Attack using Kullback-Leibler divergence

Guest Lecturer. University of Pennsylvania. Fall '17

Introduction to Networks & Security (CIS 331) Lectured on networking basics, layered model, and protocols.

Teaching. University of Illinois at Urbana-Champaign. Spring '11 and Spring '15

Advanced Operating Systems (Teaching Assistant CS 523 Sp'11) Led discussion sections, mentored writing, advised on projects, and created student debate on best OS organizations.

Doctoral Education Perspectives Seminar (Primary Instructor for CS 591 Sp'15) Created and taught seminar on defining the student's role as an emerging scholar. Organized and moderated panel discussion on diverse, complementary, and at odds advising styles.

Promoting Undergraduate Research in Engineering (PURE) (FA14): Mentored underrepresented freshman and sophomore undergraduates on systems development and buddy allocator design and implementation.

Graduate Mentor Program (2012,2013,2014): Mentored students transitioning to the PhD.

References

Vikram S. Adve (Ph.D. Advisor)
Interim Head and Professor
Department of Computer Science
University of Illinois (UIUC)
vadve@illinois.edu

Jonathan M. Smith
Olga and Alberico Pompa Professor of Engineering and Applied Science
Professor Department of Computer and Information Science
University of Pennsylvania
jms@cis.upenn.edu

Sam King
Associate Professor
Department of Computer Science
University of California Davis
kingst@ucdavis.edu

André DeHon
Professor
Department of Electrical and Systems Engineering
University of Pennsylvania
andre@acm.org

Steve Zdancewic
Professor
Department of Computer and Information Science
University of Pennsylvania
stevez@cis.upenn.edu