

Phuong Cao

U.S. Permanent Resident (EB1)

Research Scientist, National Center for Supercomputing Applications (NCSA) at University of Illinois Urbana Champaign
Trusted CI Fellow, National Science Foundation (NSF) Cybersecurity Center of Excellence (Trusted CI)

SUMMARY

My expertise is in building resilient and secure AI/HPC/supercomputing systems that are resilient to catastrophic failures and cyberattacks. With a track record of federal/industry funding (> \$2.5M), top-tier publications, and mentored students' awards, I bring: i) broad technical expertise in emerging real-world cybersecurity (AI-driven malware, post-quantum cryptography, federated authentication), ii) models to preempt outages in exascale, quantum-centric supercomputers (GPUs, QPUs) and iii) national-scale policies in FAIR security data lake and research security.

EDUCATION

Ph.D. in Electrical & Computer Engineering; M.S. in Computer Science
B.S. in Computer Science

U of Illinois at Urbana-Champaign
Hanoi University of Science and Technology

HIGHLIGHTS

<i>Funding</i>	PI of four grants with more than \$2.5M awarded from NSF (FMiTF, CC*, CICI, and RoRS) and industry partners such as IBM-Illinois Discovery Accelerator Institute.
<i>Awards</i>	Best Paper Award at IEEE DSN, Art of HPC and Doctoral Showcase at SC (Supercomputing), Prizes at Hackathons (Salesforce 1 Million - 10 th and Box.com - 1 st), Trusted CI Fellow with NSF
<i>Publications</i>	10+ peer-reviewed papers in top conferences as lead author and PI. IEEE Quantum Computing and Engineering, USENIX Security/NSDI, IEEE S&P Magazine IEEE/FIP International Conference on Dependable Systems and Networks (DSN), Supercomputing
<i>Software & Data Impact</i>	Preempted ransomware cyber-attacks and guided resilience of the Aurora exascale supercomputer. Curated Petabytes of security and resiliency data on supercomputers (Blue Waters, Delta) and NSF Midscale testbed (FABRIC) for open-science research on Globus.
<i>Teaching</i>	Graduate-level Dependable AI Systems , Undergraduate-level Statistics, Data Science Probabilistic Graphical Models and Security courses at ECE/CS UIUC as guest lecturer and TA
<i>Student's Successes</i>	Mentor for CyberCorps Scholarship for Service (SFS) students → national labs and FAANG; (recognized as an outstanding mentor for a Fiddler Innovation Fellowship awardee)
<i>Services</i>	Proposal Review Panels (DOE, NSF); Program Committee (ACM Supercomputing, IEEE Quantum); Journal Editorial (Frontiers), Reviewer (IEEE TIFS, TDSC, SIGCOMM, BigData, CCGrid, etc.)
<i>Authorized Work</i>	U.S. Permanent Resident via EB1-A (Extraordinary Ability) – Vietnamese national.

RESEARCH AGENDA

Building resilient and secure infrastructure for emerging architecture, such as hybrid HPC-Quantum Computing:

1. Design of provable and runtime verification techniques using Z3/Dafny for federated authentication protocols
2. Deployment of continuous attack preemption using Factor Graphs (OpenGM/Pytorch) on Teracore network
3. Validation of reliable, secure, quantum-resistant, and highly available AI/HPC/supercomputing exascale infrastructure.

PROFESSIONAL PREPARATION

2023–	<i>TrustedCI Fellow</i>	National Science Foundations (NSF), Cybersecurity Center of Excellence
2020–	<i>Research Scientist and Cybersecurity Specialist</i>	National Center for Supercomputing Applications
2019	<i>Research Intern</i> , Research in Software Engineering (RiSE), formal verification	Microsoft Research
2016	<i>Research Intern</i> , IBM zSystems mainframes and Watson Health	IBM Research
2014	<i>Engineering Intern</i> , DDoS detection at Layer-7 in Content Delivery Networks	LinkedIn & Akamai
2010	<i>Visiting scholar</i> , High-Performance Computing Lab, hosted by Prof. Jong Kim	POSTECH University, S. Korea

CONTACT

Message on Signal
pcao3@illinois.edu
go.illinois.edu/phuonc-cao
1205 W. Clark St.
Rm. 3006B, Urbana, IL, 61801

REFERENCES

William Kramer, Blue Waters Supercomputer PI, Research Professor at UIUC
James Basney, PI, National Science Foundation Cybersecurity Center of Excellence
Anita Nikolic, Program Director (Fmr.), Office of Advanced Cyberinfrastructure, NSF
Gang Wang, Associate Professor, Siebel School of Computing and Data Science, UIUC
Ravishankar Iyer, George and Ann Fisher Distinguished Professor, ECE, UIUC

GRANTS

Summary 05 NSF awards and 01 IBM Research contract. Total \$2,774,332

2026-2029	CICI: TCR: Enabling Next-Generation Security Operations Center with A LLM-Powered Adaptive Cyber Deceptive Framework #2613388	Co-PI	\$900,000
2025-2027	EAGER: Unmasking HPC Abuse: AI Graph Inference from Scheduling Metadata NSF Office of the Chief of Research Security Strategy and Policy (CRSP) #2537355	PI	\$274,654
2025-2028	AIcyberLake: Live Evaluations of Real-World Security Data Lake from National AI-Cyberinfrastructure NSF Cybersecurity Innovation for Cyberinfrastructure (CICI) #2530738	PI	\$600,000
2023-2025	ResiliANT AIOps: Foundation-Model-Driven Resilience for Cloud Computing International Business Machines – IBM-Illinois Discovery Accelerator Institute	Co-PI	\$699,679
2024-2026	Quantum-Resistant Cryptography in Supercomputing Scientific Applications NSF Office of Advanced Cyberinfrastructure (OAC) Award #2430244	PI	\$200,000
2023-2025	FMitF: Bringing Verification-Aware Languages and Federated Authentication to Enable Secure Computing for Scientific Communities NSF Formal Methods in the Field (FMitF); CISE/CCF Award #2319190	PI	\$99,999

Grants with significant contributions in preparation and execution

		Role
2026	CICI: IPAAI: VERITAS - VERified Infrastructure for Trustworthy AI in Science NSF CICI #2613693	AI Assurance Engineer
2023	Mid-Scale RI-1: FABRIC: Adaptive Programmable Research Infrastructure for Computer Science and Science Applications NSF Mid-Scale RI-1 (CNS) # 1935966	Security Engineer
2021	PPoSS: Inflight Analytics to Control Large-Scale Heterogeneous Systems NSF Principles and Practice of Scalable Systems (PPoSS) #2029049	Personnel

Grants with UIUC and International Partners

		Role
2024-2029	Enhancing Precision Digital Pathology with an AI-accelerated Supercomputers	Co-PI
2024-2029	Accelerating Patient Rehabilitation via Wearable Filament Sensor Networks VinUni-Illinois Smart Health Center	Co-PI Funded a PhD student and one Postdoc

HONORS AND AWARDS

Summary Fellow of NSF TrustedCI, Best Paper Award, Art of HPC Exhibit, Mentorship Recognition, Hackathons

2025	Steven Ashby (PNNL) Prize in Computational Science, Honorable Mention, NCSA	Urbana, IL
2024	Art of High Performance Computing (HPC) exhibit, IEEE/ACM Supercomputing Exhibit	Atlanta, GA
2024	Outstanding Mentors , mentored Jerry Fiddler Innovation Fellowship awardee	link
2023	Trusted Cyber Infrastructure (CI) Fellows , NSF Cybersecurity Center of Excellence	link
2023	Doctoral Showcase , IEEE/ACM Supercomputing	Denver, CO
2014	Best Paper Award - IEEE/IFIP Dependable Systems and Networks (DSN)	Atlanta, GA
2014	\$10,000 Hackathon prize , Salesforce \$1 Million Hackathon (10 th place)	San Francisco, CA
2012	Best Use of the APIs , Box.com Hackathon	Redwood City, CA
2011	Vietnam Education Foundation (VEF) Fellowship nomination (top 45 Vietnamese students)	Hanoi, Vietnam
2009	American Chamber of Commerce Scholar , Hanoi chapter	Hanoi, Vietnam
2006	FPT Center for Young Talents (FYT) , 8 th cohort	Hanoi, Vietnam

SELECTED PUBLICATIONS

Summary 20+ publications in IEEE DSN (Best Paper Award), ACM Supercomputing, USENIX Security/NSDI, IEEE QCE

2026	Network Impact of Post-Quantum Certificate Chain sizes on Time to First Byte in TLS Deployments M Chou, Phuong Cao IEEE International Conference on Quantum Computing and Engineering (QCE)	Toronto, Canada
2026	On the Extreme Variance of Certified Local Robustness Across Model Seeds Minh Le, Phuong Cao 56th IEEE Dependable Systems and Networks Workshops (DSN-W)	Charlotte, NC

- 2026 **KNEESENSE: a low-cost wearable system with hydraulic filament sensing for real-time knee rehabilitation monitoring**
NA Phan, ST Ngo, MT Phan, NQ Duong, PT Phan, TN Do, **Phuong Cao**, et al.
Nature Scientific Reports 16 (1), 12572
- 2026 **A benchmark of expert-level academic questions to assess AI capabilities**
Center for AI Safety (scale.ai), **Phuong Cao**, et al.
Nature 649 (8099), 1139–1146
- 2025 **Story of Two GPUs: Characterizing the Resilience of Hopper H100 and Ampere A100 GPUs**
Shengkun Cui, Archit Patke, Ziheng Chen, Aditya Ranjan, Hung Nguyen, **Phuong Cao**, Saurabh Jha, Brett Bode, Gregory Bauer, Chandra Narayanaswami, Daby Sow, Catello Di Martino, Zbigniew Kalbarczyk, Ravishankar Iyer
International Conf. for High Performance Computing, Networking, Storage, and Analysis (**Supercomputing**)
[PDF](#) St. Louis, MO
- 2024 **Post-Quantum Cryptography (PQC) Network Instrument: Measuring PQC Adoption Rates and Identifying Migration Pathways**
Jakub Sowa, Bach Hoang, Advait Yeluru, Steven Qie, Anita Nikolich, Ravishankar Iyer, **Phuong Cao**
IEEE International Conference on Quantum Computing and Engineering (**QCE**)
[PDF](#) Montreal, Canada
- 2025 **Dependable Classical-Quantum Computer Systems Engineering**
Edoardo Giusto, Santiago Nuñez-Corrales, **Phuong Cao**, Alessandro Cilardo, Ravishankar K Iyer, Weiwen Jiang, Paolo Rech, Flavio Vella, Bartolomeo Montrucchio, Samudra Dasgupta, Travis Humble
Realizing Quantum Utility: Grand Challenges of Secure & Trustworthy Quantum Computing
[PDF](#) Frontiers Special Issue
- 2024 **True Attacks, Attack Attempts, or Benign Triggers? An Empirical Measurement of Network Alerts in a Security Operations Center**
Limin Yang, Zhi Chen, Chenkai Wang, Zhenning Zhang, Sushruth Booma, Constantin Adam, Alex Withers, **Phuong Cao**, Zbigniew Kalbarczyk, Ravishankar Iyer, Gang Wang.
USENIX Security Symposium
[PDF](#) Philadelphia, PA
- 2023 **Taxonomy of Fingerprinting Techniques for Evaluation of Smart Grid Honeypot Realism**
Vanessa Tay Sin Yee, Xinran Li, Daisuke Mashima, Bennet Ng, **Phuong Cao**, Zbigniew Kalbarczyk, Ravishankar Iyer.
Workshop on Testbed and Digital Twin for Smart Grids, *IEEE SmartGridComm*
[PDF](#) Glasgow, Scotland
- 2023 **stealthML: Data-driven Malware for Stealthy Data Exfiltration**
Keywhan Chung, **Phuong Cao**, Zbigniew Kalbarczyk, Ravishankar Iyer.
In the *IEEE International Conference on Cyber Security and Resilience (CSR)*
[PDF](#) Venice, Italy
- 2022 **Predicting COVID-19 Disease Progression with A Factor Graph-based Model**
Yurui Cao, **Phuong Cao**, Haotian Chen, Karl M. Kochendorfer, Andrew B. Trotter, William L. Galanter, Paul M. Arnold, Ravishankar Iyer.
In *Association for the Advancement of Artificial Intelligence (AAAI) Health Intelligence Workshop*
[PDF](#) Virtual
- 2020 **Investigating Root Causes of Authentication Failures Using a SAML and OIDC Observatory**
Jim Basney, **Phuong Cao**, Terry Fleury
In the *6th IEEE International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications (DependSys)*
[PDF](#) Virtual
- 2019 **Continuous Auditing of SSH-Servers To Mitigate Brute-Force Attacks**
Phuong Cao, Yuming Wu, Subho Banerjee, Justin Azoff, Alex Withers, Zbigniew Kalbarczyk, Ravishankar Iyer
In the *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*
[PDF](#) Boston, MA
- 2016 **SVAuth: A Single-Sign-On Integration Solution with Runtime Verification**
Shuo Chen, Matt McCutchen, **Phuong Cao**, Shaz Qadeer, and Ravishankar Iyer
In the *17th International Conference on Runtime Verification (RV)*
[PDF](#) Madrid, Spain
- 2014 **Preemptive intrusion detection: theoretical framework and real-world measurements**
Phuong Cao, Eric Badger, Adam Slagell, Zbigniew Kalbarczyk, Ravishankar Iyer
In the *Symposium and Bootcamp on the Science of Security (HotSoS)*
[PDF](#) Raleigh, NC
- 2013 **Security Monitoring for Virtual Machines Using Hardware Architectural Invariants**
Cuong Pham, Zachary Estrada, **Phuong Cao**, Zbigniew Kalbarczyk, Ravishankar Iyer
Best Paper Award. In the *44th IEEE Conference on Dependable Systems and Networks (DSN)*
[PDF](#) Atlanta, GA

CONTRIBUTED BOOK CHAPTERS

2024	Dependable Computing: Design and Assessment , ISBN: 978-1-118-70944-3	IEEE Wiley
2023	Multimodal AI in Healthcare , ISBN: 978-3-031-14771-5	Springer
2018	Assured Cloud Computing , ISBN: 978-1-119-42863-3	IEEE Wiley

MAGAZINE ARTICLES

2014	Building Reliable and Secure Virtual Machines Using Architectural Invariants Cuong Pham, Zachary Estrada, Phuong Cao , Zbigniew Kalbarczyk, Ravishankar Iyer <i>In the IEEE Security & Privacy (S&P) Magazine</i>
------	---

WORKSHOPS

2025	Dynamic Factor Graphs for Attack Preemption Phuong Cao , Zbigniew Kalbarczyk, Ravishankar Iyer Secure-HPC Workshop organized by NIST and PNLL, co-located with Supercomputing	St. Louis, MO
2025	Characterizing Modern GPU Resilience and Impact in HPC Systems: A Case Study of A100 GPUs Shengkun Cui, Archit Patke, Ziheng Chen, Aditya Ranjan, Hung Nguyen, Phuong Cao , Saurabh Jha, Brett Bode, Gregory Bauer, Chandra Narayanaswami, Daby Sow, Catello Di Martino, Zbigniew Kalbarczyk, Ravishankar Iyer 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN Workshop) PDF	Naples, Italy
2024	Security Testbed for Preempting Attacks against Supercomputing Infrastructure Phuong Cao , Zbigniew Kalbarczyk, Ravishankar Iyer Secure-HPC Workshop organized by NIST and PNLL, co-located with Supercomputing	Atlanta, GA
2024	Auditing Network Security Attacks in Jupyter Notebooks Phuong Cao INDIS Workshop, co-located with Supercomputing	Atlanta, GA
2023	Post-Quantum Cyberinfrastructure Security Readiness: Risks, Measures and Prospects Phuong Cao , Bach Hoang, Santiago Nunez-Corrales. <i>In Basic Research Needs in Quantum Computing and Networking</i> , Department of Energy's Office of Advanced Scientific Computing Research	Gaithersburg, MD
2020	Mining threat intelligence from billion-scale SSH brute-force attacks Yuming Wu, Phuong Cao , Alexander Withers, Zbigniew Kalbarczyk, Ravishankar Iyer. <i>In Network and Distributed System Security (NDSS) Symposium Workshop</i> PDF	San Diego, CA

SUBMITTED MANUSCRIPTS

2025	Generative active adaptation for drifting and imbalanced network intrusion detection Ragini Gupta, Shinan Liu, Ruixiao Zhang, Xinyue Hu, Xiaoyang Wang, Hadjer Benkraouda, Pranav Kommaraju, Phuong Cao, Nick Feamster, Klara Nahrstedt https://arxiv.org/abs/2503.03022
2025	Building Machine Learning Challenges for Anomaly Detection in Science Campolongo, Elizabeth G., Yuan-Tang Chou, Ekaterina Govorkova, Wahid Bhimji, Wei-Lun Chao, Chris Harris, Shih-Chieh Hsu et al. (Phuong Cao Endorser) https://arxiv.org/abs/2503.02112 Submitted to Nature Communications

COURSES: SYLLABUS DESIGNS, MACHINE PROBLEMS, AND LECTURES

University of Illinois at Urbana-Champaign

Summary *Developed machine problems for computer security, syllabus for Dependable AI, Statistics, and AI Literacy*

2025	AI Systems Failure Modes 101	In development with NAIRR
2023	ECE 598 RKI: Trustworthy AI Systems	Guest Lecturer
2022	ECE 471: Data Science Analytics using Probabilistic Graphical Models	Machine Problem designer
2021	ECE 542 / CS 536: Design of Fault Tolerant Digital Systems	Guest Lecturer
2020	ECE 598 RKI: Dependable AI Systems	Machine Problem designer
2020	CS 498 : Data Science & Analytics	Machine Problem designer

2019	ECE 542 / CS 536: Design of Fault Tolerant Digital Systems	Student Rating: 4.4/5.0	Teaching Assistant
2018	CS 461: Computer Security	Student Rating: 4.2/5.0	Teaching Assistant
2017	CS 461: Computer Security		Teaching Assistant
2017	ECE 313: Probability and Statistics	Student Rating: 4.2/5.0	Teaching Assistant

SELECTED TUTORIALS, TALKS AND LECTURES

Summary	<i>Gave tutorials at Berkeley Lab, Argonne, NCAR, NIST, universities (CMU, NUS), and Microsoft, IBM, and Akamai.</i>		
2026	Unmasking HPC Abuse <i>Academic Security and Counter Exploitation</i>		College Station, TX
2025	Story of Two GPUs: Characterizing the Resilience of Hopper H100 and Ampere A100 GPUs <i>Supercomputing, Technical Session</i>		St Louis, MO
2025	Post Quantum Risk in Science <i>NSF Cybersecurity Summit, NCAR</i>		Boulder, CO
2025	Research Security in AI/HPC/Supercomputing <i>NCSA Engagement Lightning Talk, NCSA</i>		Urbana, IL
2025	Quantitative Risk Assessment for Post Quantum Cryptography <i>Joint Laboratory for Extreme Scale Computing (JLESC), Argonne National Laboratory</i>		Lemont, IL
2025	Quantitative Risk Assessment for Post Quantum Cryptography <i>5th NIST Secure HPC Workshop</i>		Gaithersburg, MD
2025	Measuring Quantum Resistant Cryptography <i>Hot Topics in the Science of Security Symposium (HotSoS)</i>		Virtual, hosted by NSA
2024	Jupyter Notebooks Security <i>Supercomputing</i>		Atlanta, GA
2024	Secure HPC Software Construction, Communication, and Computation <i>Illinois Cyber Security Scholars Program (ICSSP)</i>		Urbana, IL
2024	Security Log Analysis Tutorial <i>NSF Cybersecurity Summit at Carnegie Mellon University (CMU)</i>		Pittsburg, PA
2024	Post Quantum Cryptography Adoption Rate <i>NIST HPC Security Working Group</i>		Virtual
2024	Secure HPC Software Construction, Communication, and Computation <i>4th High-Performance Computing Security Workshop, Wichita State University</i>		Wichita, KS
2024	Post Quantum Cryptography Migration for HPC <i>National Center for Supercomputing Applications Quantum Computing Interest Group Monthly Meeting</i>		Urbana, IL
2023	Plenary Session NSF Trusted CI Fellows Panel <i>Lawrence Berkeley National Lab</i>		Berkeley, CA
2023	Secure Infrastructure for Health Analytics <i>National University of Singapore (NUS), Illinois Advanced Research Center (Illinois ARCS)</i>		Singapore
2023	Evolution of malicious software in the machine learning domain <i>ECE 598RKI: Dependable AI Systems</i>		Urbana, IL
2023	Towards Reliable and Robust Generative Models in Systems Domain <i>Winter School on Cyber Security – Hanoi University of Science & Technology</i>		Hanoi, Vietnam
2023	Innovations in Health Analytics and Systems: An Illinois Engineering and Mayo Clinic Partnership <i>VinUni-Illinois Smart Health Center</i>		Hanoi, Vietnam
2023	Expert-guided Foundational Model for Preemptive Attack Detection <i>Hanoi University of Science and Technology (Bach Khoa),</i>		Hanoi, Vietnam
2023	Secure Infrastructure for Health Analytics <i>VinMec hospital</i>		Hanoi, Vietnam
2022	Factor graphs & Belief Propagations <i>ECE 471: Data Science Analytics using Probabilistic Graphical Models</i>		Urbana, IL
2021	Bot vs. Human: Statistical analysis of honeypot logs <i>CS 536: Design of Fault Tolerant Digital Systems</i>		Urbana, IL
2020	Replay of security attacks in a production testbed <i>CS 498 : Data Science & Analytics</i>		Urbana, IL
2019	Continuous Auditing of SSH-Servers To Mitigate Brute-Force Attacks		

Microsoft Research, Cryptography, Security, and Privacy (CRYSP)

Bellevue, WA

ACADEMIC SERVICES

Summary *Proposal Panelist for DOE, NSF; Program Committee on IEEE Quantum Computing Engineering and ACM Intl. Conf. Supercomputing; Reviewer for IEEE Journals and Editor for Frontiers Special Issue*

Grant and Award Reviewers

2025 Proposal Reviewer, Department of Energy (DOE)
 2024-2025 Panelist, National Science Foundation (NSF)
 2022 C3.ai Digital Transformation Institute

Technical Conference Program Committee (TPC) Member

2026 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)
 2026 ACM International Conference on Supercomputing (ICS)
 2026 ISC High Performance, Research Poster Committee Member
 2025 Foundations Of Reliable Classical-quantum Engineering, IEEE/IFIP DSN 2025
 2024-2025 Program Committee Member, IEEE International Conference on Quantum Computing and Engineering (QCE) Quantum Networking track [link](#)
 2023-2024 Program Committee Member, US Research Software Engineer Association (US-RSE)
 2019 ACM Internet Measurement Conference (IMC), Shadow Program Committee

Conference Chairs

2025 Session Chair, Secure HPC Workshop, Supercomputing
 2024 Program Co-Chair, 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Industry Track

Journal peer reviews (verified): [Clarivate Web of Science](#)

2024,2025 IEEE Transactions on Information Forensics and Security (IEEE TIFS)
 2024 Journal of Open Source Software (JOSS)
 2018 IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)

Journal Editor

2024 **Frontiers: Realizing Quantum Utility: Grand Challenges of Secure & Trustworthy Quantum Computing**

Workshop Organizer

2024 First Workshop on Dependability Challenges in Hybrid Classical-Quantum Computing Systems
 Co-located with QCE24
 2024 Dependable Architectures for HPC and Quantum Systems
 Joint High-Performance Quantum Dependability Working group: Fermi National Accelerator Laboratory, Oak Ridge National Laboratory, UIUC (IQUIST, NCSA, CSL/ECE), University of Naples Federico II

Conference reviewers

IEEE International Symposium on Cluster, Cloud, and Internet Computing (CCGrid)
 IEEE International Symposium on On-Line Testing and Robust System Design (IEEE IOTLS)
 ACM Special Interest Group on Data Communication (ACM SIGCOMM)
 IEEE International Conference on Dependable Systems and Networks (IEEE DSN)
 IEEE International Conference on Cloud Computing (IEEE CLOUD)
 IEEE International Conference on Big Data (IEEE BigData)
 IEEE International Symposium on On-Line Testing & Robust System Design (IOTLS)
 NeurIPS

Judges

2023-2024 Technical Judge, Hack Illinois
 2023-2024 Mentor, NCSA's SPIN (Students Pushing Innovation) – an NSF REU site.
 2019 Judge, Pulse Hardware Competition, ECE Illinois
 2022 Illinois CS & ECE graduate admission
 2012-2019 Chair & Organizer, DEPEND group research retreat

OUTREACH ACTIVITIES

Summary *Organized supercomputing tours, taught federated authentication concepts to K-12 students.*

Jul 2024	Secure Health Analytics in Supercomputing Environment <i>VinUni-Illinois Summer School for Pre-doctoral Students</i>	Hanoi, Vietnam
Oct 2024	National Petascale Computing Facility tour for UIUC Sysnet and SPRAI students	Champaign, IL
Apr 2024	Engineering Open House https://eohillinois.org/ , NCSA,	Urbana, IL.
Nov 2023	Federated Authentication explained for K12 students , Carrie Busey Elementary School	Savoy, IL
Oct 2023	National Petascale Computing Facility tour for VinUni-Illinois visiting scholars and SPRAI	Champaign, IL
June 2023	National Petascale Computing Facility tour for Students Pushing Innovation (SPIN) students	Champaign, IL

POSTDOCS, VISITORS, AND STUDENTS MENTORED

Summary *Students leading critical roles in national labs, industry, and startups.*

Postdocs & Visitors

Edo Giusto → University of Naples Federico II; Helix42

Exchange students

Thibaut Probst → Airbus

Chi Phan → VinUni

Hung Nguyen → VinUni → UIUC → Argonne National Lab

Cuong, Nguyen Tien → Singapore University of Technology and Design (SUTD)

Undergraduates

Neil Rayu → Sandia

Advaith Yeluru → Microsoft Security Copilot

Jakub Sowa → NSF CyberCorps Scholarship for Services (current); Awarded **Fiddler Innovation** Fellowship.

Seoung Kyun Kim → National Renewable Energy Laboratory (NREL)

Surya Bakshi → Offchain Labs

Binfeng Yuan → Amazon

Satvik Kulkarni → IBM

Advay Kadam → NCSA

Bach Hoang → NCSA

Minh Le → Georgia Tech

(NTU) → Lam Nguyen

Master students

Eric Badgers → Yahoo!

PhD students mentored

(NASA JPL) → Joel Santosh Jothiprakasham

Yurui Cao → Google

Haotian Chen → Google

Yuming Wu

MEMBERSHIPS

Present	Trusted CI: The NSF Cybersecurity Center of Excellence	Fellow
Present	Joint Laboratory on Extreme Scale Computing	Member
Present	Institute of Electrical and Electronics Engineers (IEEE)	Member

PUBLICLY AVAILABLE CODE AND DATA RELEASES

2023	Blue Waters security and resiliency data (approximately one Petabyte)	Globus
2019	SSH-auditor	URL
2019	SSH HoneyPot Data (complete 15B SSH attack attempts available on request)	URL
2018	SVAuth: Self-verifying single-sign-on solutions	URL
2017	Timemachine – reproducible vulnerabilities in Debian-based docker container.	Docker Hub ; Github
2000-2023	Longitudinal data of NCSA security incidents (sys logs, reports, and Zeek logs)	Available upon request

PRESS

2025	HPCWire , <i>NCSA Awards 17 Students Fiddler Innovation Fellowships</i>	URL
2024	HPCWire, Quantum Zeitgeist, Quantum Insider , <i>NCSA's New Project Paves Path to Quantum-Resistant Cyberinfrastructure in Scientific Computing</i>	URL
2019	HPCWire, ECE Illinois, NCSA , <i>Illinois Researchers Sweeten Honey-pot to Catch, Blacklist Hackers</i>	URL

CONFERENCE ACTIVITIES

2024	Bringing Verification-Aware Languages and Federated Authentication to Enable Secure Computing for Scientific Communities <i>NSF Formal Methods in the Field (FMitF) PI Meeting</i>	<i>Poster</i> Iowa City, IA
2024	Verifying Critical Authentication Systems in Research Infrastructure <i>NSF Research Infrastructure Workshop</i>	<i>Posters</i> Phoenix, AZ
2023	Enriching Energy Systems Threat Intelligence Foundation-Model-driven SmartGrid Honey-pot <i>Center for Infrastructure Trustworthiness in Energy Systems</i>	<i>Industry Advisory Board Meeting</i> Chicago, IL
2023	Preemptive Intrusion Detection: Real-world Measurements, Bayesian-based detection, and AI-driven countermeasures <i>International Conference for High-Performance Computing, Networking, Storage, and Analysis (SC)</i>	<i>Doctoral Showcase</i> Denver, CO
2023	Security and Resiliency Challenges in Hybrid HPC-QC (High-Performance-Supercomputer-Quantum-Computing) <i>NSF Cybersecurity Summit, Lawrence Berkeley National Laboratory</i>	<i>Poster</i> Berkeley, CA
2023	Security Log Analysis – Ransomware encounters in the wild <i>NSF Cybersecurity Summit, Lawrence Berkeley National Laboratory</i>	<i>Tutorial (Interactive) Session</i> Berkeley, CA
2023	Foundational Resiliency Model on the Blue Waters Petascale Supercomputer <i>DEPEND group research retreat</i>	<i>Presentation</i> Urbana, IL
2023	Post-Quantum Cryptography (PQC) Adoption Measured at the National Center for Supercomputing Applications (NCSA) <i>Sandia-UIUC Mini-Conference</i>	<i>Poster</i> Urbana, IL
2023	quAPL-V: Formal Verification in an Array Programming Language-based quantum library <i>Sandia-UIUC and NCSA Industry Conference</i>	<i>Poster</i> Urbana, IL
2023	stealthML: Data-driven Malware for Stealthy Data Exfiltration <i>IEEE International Conference on Cyber Security and Resilience</i>	<i>Presentation</i> Venice, Italy
2023	Towards Reliable and Robust Generative Models in Clinical and Systems Domain <i>Mayo Clinic</i>	<i>Presentation</i> Rochester, MN
2023	Post-Quantum Cryptography (PQC) Adoption Measured at the National Center for Supercomputing Applications (NCSA) <i>Illinois Quantum Information Science & Technology Center (IQUIST) All-Hands Meeting</i>	<i>Poster</i> Urbana, IL
2023	Applications of eBPFs in bastion host auditing <i>NSF Campus Cyberinfrastructure (CC*) PI Meeting and FABRIC Workshop</i>	<i>Demo</i> Columbus, OH
2023	Ransomware Honey-pot <i>U.S. Army Corps of Engineers (USACE) R&D Day</i>	<i>Presentation</i> Urbana, IL
2023	Verifying quAPL: an APL-based quantum programming library <i>STEM Career Exploration and Research Symposium</i>	<i>Presentation</i> Urbana, IL
2023	Formal Verification of SciTokens <i>NCSA Student Research Symposium</i>	<i>Presentation</i> Urbana, IL
2022	A data anonymization proxy for interactive log analyses <i>NSF Cybersecurity Summit</i>	<i>Presentation</i> Bloomington, IN
2022	Predicting ICU Admissions for Hospitalized COVID-19 Patients with a Factor Graph-based Model <i>Association for the Advancement of Artificial Intelligence (AAAI)-22 Workshop</i>	<i>Presentation</i> Vancouver, BC, Canada
2021	Investigating Remote Desktop Protocols attacks using the Zeek observatory at UIUC/NCSA <i>Zeek Week</i>	<i>Presentation</i> Virtual
2021	Ransomware Honey-pot <i>NSF Cybersecurity Summit and FABRIC Knit Workshop</i>	<i>Presentation</i> Chicago, IL
2021	Real-time & Interpretable Inference for COVID-19 Disease Progression using Factor Graph Models <i>Center for Computational Biotechnology and Genomic Medicine (CCBGM)</i>	<i>Poster</i> Urbana, IL

2020	Investigating Root Causes of Authentication Failures Using a SAML and OIDC Observatory <i>IEEE DependSys</i>	<i>Presentation</i> Fiji - Virtual
2020	Analysis of remote desktop protocol attacks targeting scientific computing infrastructure during the COVID19 pandemic <i>Fourth Workshop on Trustworthy Scientific Cyberinfrastructure (TrustedCI@PEARC20),</i>	<i>Presentation</i> Virtual
2020	Mining Threat Intelligence from Billion-scale SSH Brute-Force Attacks <i>Network and Distributed System Security (NDSS) Symposium</i>	<i>Poster</i> San Diego, CA
2019	Continuous Auditing of SSH-Servers To Mitigate Brute-Force Attacks <i>National University of Singapore</i>	<i>Presentation</i> Virtual
2019	Formal Verification of Smart Contracts <i>Microsoft Research</i>	<i>Presentation</i> Redmond, WA
2019	TRACTION: an infrastructure for trusted alert sharing and collaborative mitigation <i>ACM HotSoS</i>	<i>Poster</i> Nashville, TN
2019	Continuous Auditing of SSH-Servers To Mitigate Brute-Force Attacks <i>USENIX Symposium on Networked Systems Design and Implementation (NSDI)</i>	<i>Presentation</i> Boston, MA
2019	Continuous Auditing of SSH-Servers To Mitigate Brute-Force Attacks <i>Security and Privacy Research at Illinois</i>	<i>Presentation</i> Urbana, IL
2018	A security testbed for capturing, replaying, and auditing attacks <i>ACM Internet Measurement Conference (IMC)</i>	<i>Poster</i> Boston, MA
2017	Learning Factor Graphs for Preempting Multi-State Attacks in Cloud Infrastructure <i>Symposium and Bootcamp on the Science of Security (HotSoS 2017)</i>	<i>Poster</i> Hanover, MD
2017	A Real-world Testbed for Assessing Security of Electronic Health Data Sharing <i>Center for Computational Biotechnology and Genomic Medicine (CCBGM)</i>	<i>Poster</i> Urbana, IL
2017	Self-Verifying Authentication: Safer Integrations of Single-Sign-On Services <i>Blackhat Europe</i>	<i>Presentation</i> London, United Kingdom
2017	SVAuth—A Single-Sign-On Integration Solution with Runtime Verification <i>International Conference on Runtime Verification (RV)</i>	<i>Presentation</i> Seattle, WA
2017	An Ethical Hacking Framework for Assessing Security of Cloud Infrastructure <i>IBM IEEE CAS/EDS – AI Compute Symposium</i>	<i>Poster</i> Yorktown Heights, NY
2016	An Ethical Hacking Framework for Assessing Security of Cloud Infrastructure <i>IBM Research</i>	<i>Presentation</i> Austin, TX
2016	Personalized password guessing: a new security threat <i>ACM HotSoS</i>	<i>Poster</i> Pittsburgh, PA
2015	Towards an unified security testbed and security analytics framework <i>ACM HotSoS</i>	<i>Poster</i> Urbana, IL
2015	Towards an unified security testbed and security analytics framework <i>Supercomputing (SC)</i>	<i>Demo</i> Austin, TX
2014	Reliability and security monitoring of virtual machines using hardware architectural invariants <i>IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)</i>	<i>Presentation</i> Atlanta, GA
2014	Application-layer Denial of Service Attacks <i>LinkedIn</i>	<i>Presentation</i> Mountain View, CA
2014	Preemptive Intrusion Detection <i>ACM HotSoS</i>	<i>Presentation</i> Raleigh, NC
2014	Preemptive Intrusion Detection <i>Information Trust Institute (ITI)</i>	<i>Presentation</i> Urbana, IL
2013	Factor Graphs modeling in Anti Money Laundering <i>IBM Research</i>	<i>Presentation</i> Yorktown Heights, NY
2012	Applications of Machine Learning in Layer-7 Slow DDoS Detection <i>Akamai</i>	<i>Presentation</i> San Mateo, CA

PAST APPOINTMENTS

2010	<i>Research Engineer, Faceted Search</i>	Vinagame (VNG)
2006-09	<i>Security Intern, Reverse Engineering Computer Viruses</i>	Bach Khoa Anti-Virus (BKAV)

MISC

Citizenship: Vietnam

Authorized Work: U.S. Permanent Resident

Misc. travel grants: NSF Cybersecurity Summit, Supercomputing, HotSoS, ACM IMC, NSF CC* PI meetings