CERIAS 2025

26th Annual Security Symposium ★ April 1st & 2nd, 2025

Purdue University, West Lafayette, Indiana

Table of Contents

#CERIAS

Thanks to Our Strategic Partners

- Boeing
- Caterpillar
- CISA
- Cisco
- COMPLiQ
- Eli Lilly and Company
- General Motors
- HP
- Idaho National Laboratory
- Intel
- Lawrence Livermore National Laboratory
- Lionfish Cyber Security
- Lockheed Martin
- ManTech
- National Institute of Standards & Technology (NIST)
- National Security Agency (NSA)
- Pacific Northwest National Laboratory
- Peraton
- Raytheon
- RTX
- Sandia National Laboratories

For information on the CERIAS Strategic Partnership Program
contact info@cerias.purdue.edu or 765-494-7841

Day 1

Welcome

8:30a

Dr. Dongyan Xu
Director of CERIAS and Samuel Conte Professor of Computer Science
Purdue University

Dongyan Xu is a Samuel D. Conte Professor of Computer Science and Director of CERIAS, Purdue's cybersecurity research center. His research focuses on cyber and cyber-physical security. He has also made early contributions to the areas of cloud computing and peer-to-peer media streaming/distribution. He is part of the Purdue System Security Lab (PurSec).

For computer system security, Dr. Xu and his students have been developing virtualization-based systems for capturing, investigating, and defending against stealthy computer malware (e.g., worms, rootkits, bots, and APTs). His team is also developing reverse engineering techniques for the analysis of binary artifacts such as binary programs and memory images. For cloud computing, Dr. Xu and his students have been developing advanced techniques for the creation, management, and performance optimization of virtual networked infrastructures on top of physical cloud infrastructures.

Opening Keynote

8:45a

"From Artisanal to Industrial Delivering Security at Scale for Business and Technology Agility"

Phil Venables
Chief Information Security Officer, Google Cloud

Phil is the Chief Information Security Officer of Google Cloud where he leads the risk, security, compliance, and privacy teams and leads many AI security initiatives. Before joining Google, he was a Partner at Goldman Sachs where he held multiple roles over a long career, initially as their first Chief Information Security Officer, a role he held for 17 years. In subsequent roles, Venables was Chief Operational Risk Officer, an operating partner in their private equity business and a Senior Advisor to the firm's clients and executive leadership on cybersecurity, technology risk, digital business risk, and operational resilience. In addition to this, he was a Board Director of Goldman Sachs Bank. Before Goldman Sachs, Venables held multiple Chief Information Security Officer roles, and senior engineering roles across a range of finance, energy, and technology companies. He has been honored with many distinctions and awards and in 2024, was inducted into the Chief Security Officer Hall of Fame. Outside of Google, Venables serves on the boards of the NYU Tandon School of Engineering, the NYU Stern Business School Volatility and Risk Institute, the Information Security and Privacy Advisory Board of NIST, the Security and Technology Advisory Board of MITRE, and is a member of the Council on Foreign Relations. From 2021 to 2025 he served on the President's Council of Advisors on Science and Technology at The White House where he drove multiple initiatives from cyber-resilience, the future of AI, through to improvements in scientific communications. He serves on multiple private sector Boards including HackerOne, Interos.ai, and Veza. He remains active in advising many financial sector organizations on matters of security, risk and compliance including Plaid, The Monetary Authority of Singapore and the Bank of England. Venables holds undergraduate and postgraduate degrees in Computer Science, Formal Methods and Cryptography from the University of York and The Queen's College at Oxford University. He is a Chartered Engineer, a Chartered Scientist and a Chartered Fellow of the British Computer Society.

Fireside Chat

9:45a

Dr. Eugene Spafford, Executive Director Emeritus & Founder, CERIAS, Purdue University

Eugene H. Spafford is a professor of Computer Sciences at Purdue University, a professor of Philosophy (courtesy appointment), and is Executive Director Emeritus of the Center for Education Research Information Assurance and Security. CERIAS is a campus-wide multi-disciplinary Center, with a broadly-focused mission to explore issues related to protecting information and information resources. Spaf has written extensively about information security, software engineering, and professional ethics. He has published over 100 articles and reports on his research, has written or contributed to over a dozen books, and he serves on the editorial boards of most major infosec-related journals.

Michael Clothier, Sector Chief Information Security Officer, Aeronautics Systems Northrup Grumman

Michael Clothier is the Chief Information Security Officer(CISO) for the Aeronautics Systems (AS) Sector at NorthropGrumman, where he leads the sector's global cybersecuritystrategy. He is responsible for safeguarding mission-criticalaerospace and defense technologies, ensuring regulatorycompliance, and mitigating evolving cyber threats. With 30years of experience in cybersecurity and IT leadership, Michael has successfullydeveloped and implemented enterprise-wide security programs that align riskmanagement with business objectives in highly regulated industries.

Dr. Kelley Misata, Chief Trailblazer and Founde, Sightline Security

Dr. Kelley Misata, a distinguished cybersecurity expert and speaker, Founder and Chief Trailblazer of Sightline Security. and serves as President of the Open Information Security Foundation (OISF). Dr. Misata's expertise spans cybersecurity, specializing in nonprofit security, network security, assessments, and the strategic use of open-source technologies. She is a renowned speaker and advocate for improving cybersecurity practices within underserved enterprises, nonprofits, and community sectors through her groundbreaking work at Sightline Security.

Her commitment to cybersecurity is deeply personal, informed by her experiences as a cyberstalking survivor, and she brings a unique perspective to her work, pairing technical expertise with strategic leadership. She has contributed significantly to advancing open- source security through her leadership at OISF and past work with organizations like the Tor Project. Dr. Misata holds a Ph.D. in Information Security from Purdue University, a Master's in Business Administration and Marketing, and a Bachelor of Science in Marketing from Bentley University. Her comprehensive educational background and professional accomplishments establish her as a pivotal leader in cybersecurity innovation and advocacy, especially in bridging the gap between security frameworks and practical applications for nonprofits and mission-based organizations.

Technology Talk

11:05a

Technology Talk: "From Firewalls to Fairness: Securing the Future with Threat Modeling and Ethics"

Dr. Abhilasha Bhargav-Spantzel, Partner Security Architect, Microsoft

Abstract:
In an era where Artificial Intelligence (AI) is transforming industries and societies, the importance of robust security foundations and ethical considerations has never been more critical. This talk will explore the evolving landscape of threat modeling in the age of AI, emphasizing the need to build, and strengthen foundational security principles while integrating evolving ethical frameworks.

This session will explore advanced threat modeling techniques, emphasizing a holistic approach that integrates traditional security and privacy principles, particularly for emerging AI solutions such as agents, skills and plugins. Special focus will be given to Responsible AI (RAI) principles, including transparency, accountability, fairness, inclusiveness, reliability, and safety, which guide the development and deployment of AI technologies.

Concrete examples will demonstrate how AI impacts critical security vectors:

- Identity: Strong authentication methods such as Multi-Factor Authentication (MFA), Zero Trust principles, and AI-driven adaptive and inclusive authentication are essential to secure identity flows and authorization pathways.
- Data Flows: Protecting data through classification, encryption, secure APIs, and monitoring for exfiltration and misuse is crucial. Privacy-preserving techniques continue to show value as we face advanced attacks in the AI world such as XPIA (cross prompt injection attacks).
- Types of Threats: Understanding and mitigating AI-generated attacks, supply chain threats, and real-world incidents through proactive strategies such as attack surface reduction and AI-driven threat hunting.
- Recovery Mechanisms: Ensuring resilience through rapid detection, rollback strategies, and AI-powered anomaly detection, along with securing the supply chain and maintaining patch velocity.

These security considerations remain essential for designing resilient architectures with appropriate security hooks. Participants will gain practical strategies for implementing these principles in real-world scenarios, ensuring that AI systems are not only secure but also ethically sound. Grounded in security foundations and ethical AI, this talk aims to engage security researchers and professionals in collaborative discussions to address the complexities of AI-driven threats.

Together, we can explore how we can step up our threat modeling efforts, remember the basics, and prioritize responsible AI to build a secure and ethical digital future.

Bio:
Abhilasha Abhilasha Bhargav-Spantzel is a Partner Security Architect in the Office Product group focused on Identity and AI Copilot security and safety. Previously she was responsible for security architecture for Microsoft Security Response Center (MSRC). Prior to joining Microsoft she was at Intel for 14 years, focusing on hardware-based identity and security product architecture. She completed her doctorate from Purdue University, which focused on identity and privacy protection using cryptography and biometrics. Abhilasha drives thought leadership and the future evolution of cybersecurity platforms through innovation, architecture, and education. She has given numerous talks at conferences and universities as part of distinguished lecture series and workshops. She has written 5 book chapters and 30+ ACM and IEEE articles and has 40+ patents. Abhilasha leads multiple D&I and actively drives the retention and development of women in technology. She is passionate about STEM K-12 cybersecurity education initiatives, as well as co-organizes regular camps and workshops for the same.

Technology Talk

10:35a

"Scalable and Concurrent Targeted Search for Digital Forensics"

Dr. Umit Karabiyik, Associate Professor Computer and Information Technology and Director of Ubiquitous and Mobile Investigative Techniques and Technologies Lab, Purdue University

Dr. Umit Karabiyik (Dr. K) is an Associate Professor of Cybersecurity at Purdue University's Department of Computer and Information Technology and the Director of the Ubiquitous and Mobile Investigative Techniques and Technologies (UMIT2) Lab. Prior to his appointment at Purdue, Dr. K was an Assistant Professor in the Department of Computer Science at Sam Houston State University from 2015 to 2018. Dr. K is a First-Generation Student and received his B.S. degree in Computer Systems Teaching from Sakarya University in 2006, M.S. and Ph.D. degrees in Computer Science from Florida State University in 2010 and 2015, respectively. His research interests broadly lie in Digital Forensics, Cybersecurity, Forensic Intelligence, User and Data Privacy, Artificial Intelligence in Security, Privacy and Forensic Applications. He has secured federal and industrial funding from the U.S. National Institute of Justice, U.S. Department of Homeland Security, U.S. Federal Emergency Management Agency, U.S. Bureau of Justice Assistance, The National Air and Space Intelligence Center (NASIC), and Lockheed Martin Corporation. Dr. K's research yielded several digital forensics tools for law enforcement's use. His team has developed and delivered numerous mobile and IoT forensics training courses and technical assistance for law enforcement and justice system professionals. He is an Editorial Board Member of Springer Nature's Discover Computing journal and the Journal of Surveillance, Security and Safety, conference chair and/or technical program committee member of high-quality international conferences in Digital Forensics, Cybersecurity, and Networking. As an experienced educator and mentor, Dr. K has guided numerous graduate and undergraduate students and has been recognized with multiple awards for research and teaching excellence. He has played a key role in shaping cybersecurity curricula and fostering interdisciplinary collaborations across fields such as Computer Science, Information Technology, Electrical and Computer Engineering, and Criminal Justice.

Lunch

12:00p

Technology Talk

1:10p

"Modeling, Analysis, and Control of Spreading Processes over Networks"

Dr. Philip E. Paré
Rita Lane and Norma Fries Assistant Professor of Electrical and Computer Engineering

Abstract:
Different types of malicious software that can infect systems, including viruses, worms, trojans, ransomware, etc., are often modeled using spreading processes. In this work we present and analyze mathematical models for network-dependent spread. We introduce a class of reproduction numbers that extends the scalar approach to capture overall behavior in the networked setting. We show how these networked reproduction numbers capture local as well as global behavior. We then discuss safety-critical control of spreading processes, presenting results that encourage cooperation between nodes to ensure safety.

Bio:
Philip E. Paré is the Rita Lane and Norma Fries Assistant Professor in the Elmore Family School of Electrical and Computer Engineering at Purdue University. He received his Ph.D. in Electrical and Computer Engineering from the University of Illinois at Urbana-Champaign in 2018, after which he went to KTH Royal Institute of Technology in Stockholm, Sweden to be a Post-Doctoral Scholar. He received his B.S. in Mathematics with University Honors and his M.S. in Computer Science from Brigham Young University in 2012 and 2014, respectively. He was a 2023 recipient of the NSF CAREER award, an inaugural Societal Impact Fellow at Purdue in 2021, and a 2023 Teaching for Tomorrow Fellow at Purdue as well. His research focuses on networked control systems, namely modeling, analysis, and control of virus spread over networks.

Technology Talk

1:35p

"Socially Contextualized Misinformation Detection"

Dr. Dan Goldwasser
Associate Professor, Computer Science

Bio:
Dan Goldwasser is an assistant professor at the department of computer science. His research focuses on natural language processing and machine learning, with a specific interest on natural language semantics. He graduated from the University of Illinois at Urbana-Champaign, and spent two years at the University of Maryland as a postdoctoral researcher.

Technology Talk

2:00p

"Bridging the Gap: Highlighting Academia's Limited Role in Governance, Risk, and Compliance (GRC) Education and Research"

Dr. Ali Al-Haj, Visiting Fulbright Scholar, Princess Sumaya University for Technology, Jordan

Abstract
Governance, Risk, and Compliance (GRC) is a crucialframework in today's business landscape, integrating governance structures, risk management strategies, and regulatory compliance to ensure organizational resilience. As businesses navigate increasingly complex regulatory environments and risk landscapes, GRC has become essential for corporate sustainability. Despite its growing significance, there remains a significant disparity between its widespread industry adoption and its limited presence in academic curricula and research. Industries worldwide invest billions in GRC to mitigate risks, maintain regulatory compliance, and ensure business continuity. However, academic engagement in this field remains limited, leading to a shortage of trained professionals and innovative research contributions. This session examines the underlying causes of this academic gap, its impact on industry and workforce development, and how fostering stronger collaboration between academia and industry can enhance GRC education, research, and professional practice.

Bio:
Prof. Ali Al-Haj received his undergraduate degree in Electrical Engineering from Yarmouk University, Jordan, in 1985, followed by an M.Sc. degree in Electronics Engineering from Tottori University, Japan, in 1988 and a Ph.D. degree in Electronics Engineering from Osaka University, Japan, in 1993. He then worked as a research associate at ATR Advanced Telecommunications Research Laboratories in Kyoto, Japan, until 1995. Al-Haj joined Princess Sumaya University for Technology, Jordan, in October 1995, where he currently serves as a Full Professor. He has published papers in dataflow computing, information retrieval, VLSI digital signal processing, neural networks, information security, and digital multimedia watermarking. Al-Haj is currently a visiting Fulbright Scholar at CERIAS, hosted by Prof. Eugene Spafford. His current research interests include among others: Cybersecurity Governance, Risk and Compliance (GRC), Digital Trust Frameworks, Cybersecurity Workforce and Curricula Development, and Cybersecurity Policy Development.

Jeff Angle, Senior Director of Academic and Workforce at ISACA

Jeff is a highly experienced executive focused on the education of the future workforce. He has help executive level roles with ETS, Pearson, HMH, and Arizona State University. Jeff has developed successful academic and workforce development programs through out the US, Middle East and the LATAM areas focused on upskilling students in secondary and post-secondary education. In his spare time, Jeff is faculty at the W.P. Carey School of Business at Arizona State University.

Technology Talk

2:30p

"Trustworthy IoT and Through Usable Security & Privacy"

Dr. Younghyun Kim, Assistant Professor of Electrical and Computer Engineering

Abstract:
In this talk, I will discuss techniques for addressing security and privacy challenges in building a trustworthy IoT ecosystem, with a focus on home smart devices and wearable technologies. I will first explore the design challenges in resource-constrained networked embedded systems, particularly in terms of energy efficiency and security. Then, I will present techniques to establish secure connectivity and enable intelligence in low-power IoT devices. Additionally, I will introduce a privacy-preserving technique designed to prevent the unwanted leakage of biometric information in virtual reality devices.

Bio:
Younghyun Kim is an Associate Professor in the Elmore Family School of Electrical and Computer Engineering at Purdue University. He received his B.S. degree in Computer Science and Engineering and his Ph.D. in Electrical Engineering and Computer Science from Seoul National University in 2007 and 2013, respectively. He was a Postdoctoral Research Assistant at Purdue University and a visiting scholar at the University of Southern California. From 2016 to 2023, he served as an Assistant and Associate Professor at the University of Wisconsin-Madison.

His research interests include energy-efficient computing and the security and privacy of the Internet of Things. He is a recipient of the NSF CAREER Award, Meta Research Award, IEEE Micro Top Pick, EDAA Outstanding Dissertation Award, and multiple design contest and demo awards at the Design Automation Conference (DAC) and the International Symposium on Low Power Electronics and Design (ISLPED).

Networking Break

3:10p

Panel Discussion #1

3:30p

"Is it Time for the Purdue ICS Model 2.0?"

Moderator - Dr. Eugene Spafford

Dr. Hany Abdel-Khalik
Professor, Nuclear Engineering, Founder, Covert Defenses, LLC

Professor Abdel-Khalik has obtained his Bachelor in Nuclear Engineering from Alexandria University in Egypt in 2000. Immediately after graduation he joined the department of Nuclear Engineering at North Carolina State University to pursue his graduate studies. His master and PhD dissertation have produced a number of new algorithms serving as a toolkit to handle the voluminous data streams generated from nuclear plants simulation. His objective was to provide a solid mathematical basis to improve predictions of boiling water core simulators. After graduation he worked as a Nuclear Engineer in the methods group at AREVA-NP in Lynchburg, VA. During his tenure at AREVA, he worked on fuel loading pattern optimization for pressurized water reactors. He returned to North Carolina State in 2007 as a tenure-track assistant professor, and obtained his tenure in 2013. He developed a research program on uncertainty quantification and reduced order modeling during his tenure at North Carolina State. Since his arrival at Purdue in August 2014, he has expanded his research program to design data-driven algorithms to support the validation and safety of nuclear power plants. One aspect of safety that has achieved a great deal of attention in recent years is cybersecurity, for which no clear solution currently exists, especially with the increased level of sophistication that hackers have achieved. He is currently developing a program on employing physics-driven data mining techniques to detect cyberattacks which attempt to manipulate the state of critical infrastructure systems such as nuclear power plants.

Stephen Kines
Co-founder and COO, Goldilock

Stephen Kines is a co-founder and COO of Goldilock, the only cybersecurity company chosen by NATO under its DIANA Grow program to protect critical national infrastructure. Having secured multiple global patents for its network segmentation technology and $7m in funding from NATO and UK's MoD as well as private investors, he has led the deployment of the technology in Ukraine and a number of defence departments in NATO countries. Goldilock's devices are manufactured in Indiana. Stephen's earlier 25+ year career as a lawyer qualified in 6 jurisdictions during which he was a partner in law firms in UK, Silicon Valley and Central Europe.

Lesley Carhart
Director of Incident Response for North America, Dragos, Inc.

Lesley Carhart is the Director of Incident Response for North America at the industrial cybersecurity company Dragos, Inc., leading response to and proactively hunting for threats in customers' ICS environments.

Prior to joining Dragos, Lesley was the incident response team lead at Motorola Solutions. Following four years as a Principal Incident Responder for Dragos, Lesley now manages a team of incident response and digital forensics professionals across North America who perform investigations of commodity, targeted, and insider threat cases in industrial networks. Lesley is also a certified instructor and curriculum developer for Dragos' incident response and threat hunting courses.

Lesley is honored to be retired from the United States Air Force Reserves, and to have received recognition such as "DEF CON Hacker of the Year", "SANS Difference Maker", and "Power Player" from SC Magazine.

You may find Lesley organizing resumé and interview clinics at several cybersecurity conferences, lecturing, blogging, and posting prolifically about cybersecurity on social platforms. When not working, Lesley enjoys being a youth martial arts instructor.

Dr. Stacy Prowell
Senior Researcher, National Security Sciences Directorate, Oak Ridge National Laboratory

Dr. Stacy Prowell is interested in the security and resiliency of critical infrastructure. Dr. Prowell's work on a system for deep analysis of compiled software led to the Hyperion system, which received a 2015 R&D 100 award and two awards for technology transfer.

Dr. Prowell helped to create the initial cybersecurity research group at ORNL, serving as Chief Cyber Security Research Scientist, and also helped focus the group on critical infrastructure, serving as Program Manager for the lab's Cybersecurity for Energy Delivery Systems (CEDS) program under which the lab received more DOE CEDS funding than any other national laboratory.

Previously, Dr. Prowell worked in the CERT Division of the Software Engineering Institute on automated analysis of malware. Dr. Prowell is an IEEE Distinguished Lecturer for the Transportation Electrification Community. Dr. Prowell is a member of AAAS, Sigma Xi, and a senior member of the IEEE.

Dr. Prowell is a faculty member in the Department of Computer Science at Tennessee Technological University where he teaches CSC 6580, advanced and automated reverse engineering. His most recent lecture series from this class is available online.

Starting at the end of 2022, Dr. Prowell is the Associate Director for Tennessee Tech's Cybersecurity Education, Research, & Outreach Center (CEROC).

Special Recognition

4:30p

End of Session 1

Poster Session

PMU North Ballroom 6:30-9:00pm

Highlighting research conducted by students

Day 2

Registration / Coffee

8:00a

Opening Comments, CERIAS Awards

8:45a

Research Poster Awards
We announce winners from this year's poster session.

Pillar of CERIAS Award
The Pillar of CERIAS Award recognizes a CERIAS faculty/staff member and/or CERIAS sponsor for their service in furthering ideals and goals on which CERIAS achievements are built.

Keynote

9:00a

"Mission Possible: Securing Nonprofits in the Age of AI"

Kelley Misata, Chief Trailblazer and Founder, Sightline Security

Abstract:
Cybersecurity has long been built for those with the deepest pockets—governments, corporations, and traditional critical infrastructure. But what about the nonprofits that serve as society's safety net? From humanitarian relief to social justice initiatives, these organizations are increasingly targeted by cyber threats yet remain under-resourced and overlooked. As AI accelerates both risks and opportunities, we stand at a crossroads: Will AI widen the security gap, or can it be leveraged to secure all organizations, not just the privileged few?

This keynote goes beyond theory to provide real-world, immediately actionable strategies for security professionals, researchers, students, and industry leaders—because whether we realize it or not, nonprofits intersect with all of our lives. We donate, we volunteer, we rely on their services. Their security is our security. Attendees will leave with practical steps to help safeguard the nonprofits they hold dear about while ensuring AI and other emerging technologies empower these organizations to advance their mission—rather than expose them to new risks. AI-driven security challenges and solutions are relevant not only to nonprofits but to the broader ecosystem of enterprise organizations, funders, and professionals who interact with and support them.

Security cannot be a privilege—it must be a right. If nonprofits are left behind, the communities they serve are left vulnerable. Join this conversation to discover how we can bridge the gap, drive real impact, and ensure a future where security is for all—not just some.

Bio:
Dr. Kelley Misata, a distinguished cybersecurity expert and speaker, Founder and Chief Trailblazer of Sightline Security. and serves as President of the Open Information Security Foundation (OISF). Dr. Misata's expertise spans cybersecurity, specializing in nonprofit security, network security, assessments, and the strategic use of open-source technologies. She is a renowned speaker and advocate for improving cybersecurity practices within underserved enterprises, nonprofits, and community sectors through her groundbreaking work at Sightline Security.

Her commitment to cybersecurity is deeply personal, informed by her experiences as a cyberstalking survivor, and she brings a unique perspective to her work, pairing technical expertise with strategic leadership. She has contributed significantly to advancing open- source security through her leadership at OISF and past work with organizations like the Tor Project. Dr. Misata holds a Ph.D. in Information Security from Purdue University, a Master's in Business Administration and Marketing, and a Bachelor of Science in Marketing from Bentley University. Her comprehensive educational background and professional accomplishments establish her as a pivotal leader in cybersecurity innovation and advocacy, especially in bridging the gap between security frameworks and practical applications for nonprofits and mission-based organizations.

Technology Talk

10:00a

"Weaponizing Fragility in Critical Infrastructures: Implications for Next Generation Resilience"

Dr. Sean Warnick, Professor of Computer Science, Brigham Young University

Abstract:
Critical infrastructures are complex, large-scale systems with integrated cyber, physical, and human dynamics. These dynamics invariably create differing thresholds for disruption, and they invite the design of payloads that exploit them to create catastrophic cascading failures across the system. This talk introduces persistent interaction attacks designed to destabilize complex infrastructures by weaponizing the system's intrinsic dynamics against itself. We show how customary theoretical research promoting engineering robustness can be turned on its head to design the provably "stealthiest" payloads (in a certain sense) that, if deployed, will destabilize the infrastructure dynamics. These methods lead to new business models for cyber criminals, requiring little subject matter expertise for payload design and instead making use of dynamic infrastructure models–models that are becoming more easily available from new AI technologies. Countering such attacks demands secure-by-design engineering strategies, and we present some new tools for doing this, including new approaches for visualizing the attack surface and quantifying the intrinsic, or cyber-physical, vulnerabilities of an infrastructure system.

Bio:
Sean Warnick is a professor of Computer Science at Brigham Young University, where he has been on the faculty since 2003. Prior to that, he was a graduate student at the Massachusetts Institute of Technology, where he studied control theory, and an undergraduate at Arizona State University, earning his BSE in Electrical Engineering in 1993. He attended ASU on scholarship from the Flinn Foundation, graduating summa cum laude, and was named the Outstanding Graduate of the College of Engineering and Applied Sciences. He has also held visiting positions from Cambridge University (2006), the University of Maryland at College Park (2008), and the University of Luxembourg's Centre for Systems Biomedicine (2014). Sean was named the Distinguished Visiting Professor by the National Security Agency three years in a row, 2008-2010, for his work with their Summer Program for Operations Research Technology, and he maintains strong industrial partnerships, advising and consulting with various companies, including a visiting position at Applied Invention LLC., a technology innovation incubator, since 2014. He most recently served as the Senior Technical Advisor for Advanced Computing in the Technology Centers Division of the Science and Technology Directorate at the US Department of Homeland Security, Jan 2022 – Jan 2025. Sean founded Achilles Heel Technologies, Inc. in 2018, a cyber-security company protecting critical infrastructures, where he serves as Chairman of the Board, and he currently serves on the Networking and Information Technology Research and Development (NITRD) Fast Track Action Committee on Cyber-Physical Resilience.

Networking Break

10:30a

Panel Discussion #2

10:50a

"Lessons Learned From The Cyber Battlefield – Protecting the United States From Cyber Attack"

Moderator - Joel Rasmus, Managing Director of CERIAS

Joel Rasmus is the managing director for Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS); one of the largest and top-ranking interdisciplinary academic institute in North America focusing on cyber and cyber-physical assurance, security, privacy and resiliency. Rasmus joined Purdue in 2002, bringing with him more than 15 years of experience in project management. At CERIAS Rasmus developed a strategic partnership program that provides a formalized link between the University and industry. The program fosters tech transfer, basic and applied collaborative research, professional consultation and targeted student recruitment mechanisms. The CERIAS Strategic Partnership Program has led to unprecedented industry-academic integration with a number of commercial research programs. Rasmus also spearheaded successful CERAIS initiatives that lead to commercial partners opening local offices at the Purdue Research Park to further leverage and integrate their daily R&D and cyber management practices into CERIAS.

Robert Herzog, CISSP
former Special Agent with the FBI

Rob is a retired FBI Supervisory Special Agent who specialized in national security cyber investigations for most of his career, working with partners around the globe countering foreign adversaries. He also spent two years detailed to the US Intelligence Community coordinating cyber operations before retiring in 2022. He currently manages a team at CrowdStrike researching and building adversary hunting capabilities within the Counter Adversary Operations (CAO) group. He holds degrees in international relations from Kenyon College and Georgetown University School of Foreign Service and a graduate certificate in Cybersecurity Risk Management from Georgetown.

Patricia Herndon
Senior Director, Special Projects, Purdue Applied Research Institute (PARI)

Patricia Herndon is the senior director for special projects for Purdue Applied Research Institute. In this role, she builds research programs across PARI to improve national security and to accelerate critical technologies.

Herndon has 35 years of Defense Department experience. She started her career in research and development of energetics. Herndon spent 10 years working advancement of new formulations in colored smoke and flare compositions, initiating devices, and 5-inch gun ammunition formulations and propellant. She also worked in acquisition engineering and test and evaluation of energetics.

Herndon then went into management and program management. She spent time in NAVSEA, PEO IWS 3C as the assistant program manager for small arms and landing party ammunition as well as 76-millimeter ammunition. There, she was responsible for cradle-to-grave capabilities and acquisition programs for these commodities. She served as the principal assistant program manager for rotating radars, NAVSEA PEO IWS 2.0, where she managed all rotating radars on naval maritime platforms. While in IWS 2.0, Herndon spent time as the deputy assistant program manager for above-water sensors.

Herndon held many management positions at Naval Surface Warfare Center, Crane Division, including in the Acquisition and Extended Enterprise Department, the Global Deterrence and Defense Department and the Expeditionary Warfare Department. In expeditionary warfare, she spend eight years overseeing 1,200 government employees and 1,000 contractors with an annual budget of approximately $800 million. While department director, she established the strategy to advance the warfighter into next-generation capabilities. There, she established autonomous capabilities, mission engineering, integrated systems of systems test and evaluation capabilities and advanced electro-optic capabilities that integrated artificial intelligence into shipboard surveillance systems.
Herndon also established a command-level integrated strategy. This established the mission engineering advanced modeling capability across expeditionary warfare, electromagnetic spectrum warfare and strategic missions. She established an integrated multidomain test environment where capabilities could be developed or validated to accelerate fielding of new technology or tactics and techniques and procedures.
Herndon spent five years in industry, where she worked as a process engineer for Eli Lilly and Company and as a manager for COMARCO's Environmental Services Branch.

Patricia has a BS in chemical engineering from Purdue University. She is Defense Acquisition Workforce Act Level III certified in both program management and systems planning research and development, systems engineering.

Richard Wright
Director/Chief Engineer, Technology Transition, Corporate Engineering & Technology
Lockheed Martin

Rich Wright is currently a member of the LM corporate Research & Technology organization where he supports the continuous identification and transition of LM technologies for insertion into customer mission solutions; and also separately co-leads the execution of the LM Enterprise Cyber Business Strategy.

Prior to his current role in Lockheed Martin Corporate Engineering & Technology, he was the Chief Engineer for the Cyber & Intelligence business segment, where he was responsible for the technical performance, technology strategy, and solutions development of multiple domestic

Rich Wright is currently a member of the LM corporate Research & Technology organization where he supports the continuous identification and transition of LM technologies for insertion into customer mission solutions; and also separately co-leads the execution of the LM Enterprise Cyber Business Strategy.

Prior to his current role in Lockheed Martin Corporate Engineering & Technology, he was the Chief Engineer for the Cyber & Intelligence business segment, where he was responsible for the technical performance, technology strategy, and solutions development of multiple domestic and international programs supporting various national security requirements. His organization included the stewardship of approximately 400 outstanding Cyber engineers who diligently executed national security mission operations for the DoD and Intelligence Community.

Rich's career spans over 35 years of successful leadership roles in P&L and technology development across every business area in Lockheed Martin. He has a mission-first, and be-of-service mindset which started with the National Security Agency's Special Projects group. His career customers span the Intel Community, DoD, FBI, NRO, US Coast Guard, Commercial Industry, amongst others. He and his teams also provided in-country mission support in South West Asia during Operation Enduring Freedom.

He is actively engaged in building customer and industry partnerships towards the development of disruptive technology solutions; he actively engages in activities which will create the next generation workforce; is a certified Lean Six Sigma Master Black Belt; has served on the LM Technical Advisory Group; is on the Board of Directors for various start-ups; is on the UMBC Advisory Board, the Morgan State Cyber Advisory Board, and an emeritus Advisory Board member for Howard University and the University of Florida

Mr. Wright earned his BSEE from NYU and is a proud born and raised native New Yorker – though also a 1st generation American by way of Jamaica WI. He currently lives in Virginia with his beautiful wife Traci, and proud father to Trinity (currently an LM systems engineer) and Hunter (future Cyber SW Engineer).

Dr. Saurabh Bagchi, Professor of Electrical and Computer Engineering & Computer Science

Saurabh Bagchi is a Professor in the School of Electrical and Computer Engineering and the Department of Computer Science at Purdue University in West Lafayette, Indiana. His research interest is in dependable computing and distributed systems. He is the founding Director of a university-wide resilience center at Purdue called CRISP (2017-present) and PI of the Army's Artificial Intelligence Innovation Institute (A2I2) (2020-25) that spans 9 universities. He was selected to the International Federation for Information Processing (IFIP) (2020) and is a Fellow of the Institute of Engineering and Technology (IET) (2022). He is the recipient of the Alexander von Humboldt Research Award (2018), the Adobe Faculty Award (2017, 2020, 2021), the AT&T Labs VURI Award (2016), the Google Faculty Award (2015), and the IBM Faculty Award (2014). He is elected to serve on IEEE Computer Society's Board of Governors (2022-24, previously 2017-20). He is an IEEE Computer Society Distinguished Contributor (2021) and Distinguished Visitor (2020), an IEEE Golden Core member (2018), an ACM Distinguished Scientist (2013), and a Distinguished Speaker for ACM (2012).

Saurabh is proudest of the 25 PhD students and 50 Masters thesis students who have graduated from his research group and who are in various stages of building wonderful careers in industry or academia. In his group, he and his students have way too much fun building and breaking real systems. Along the way this has led to 13 best paper awards or runners-up awards at IEEE/ACM conferences and a Test of Time Award. Saurabh serves as the founder and CTO of a cloud computing startup, KeyByte (2021). Saurabh received his MS and PhD degrees from the University of Illinois at Urbana-Champaign and his BS degree from the Indian Institute of Technology Kharagpur, all in Computer Science.

Randall Brooks, Principal Technical Fellow. Chief Engineer Product Cybersecurity Center, RTX

Randall Brooks is a Principal Technical Fellow for RTX (NYSE: RTX). He is the Chief Engineer of the RTX Cyber Operations, Development and Evaluation (CODE) Center, which focuses on product cybersecurity. Randall represents the company within the US International Committee for Information Technology Standards Cyber Security 1 (CS1) and the Cloud Security Alliance (CSA). He has more than 25 years of experience in cybersecurity with a recognized expertise in software assurance (SwA) and secure development life cycles (SDLCs). In addition to holding eight patents, Randall is a CISSP, CSSLP, ISSEP, ISSAP, ISSMP, and CCSK. He graduated from Purdue University with a bachelor's degree from the School of Computer Science.

Lunch Break

11:50a - 1:00p

Technology Talk

1:00p

"Rationality of Learning Algorithms in Repeated Normal-Form Games"

Dr. Vijay Gupta, Elmore Professor of Electrical and Computer Engineering and the Associate Head for Graduate and Professional Programs, in ECE

Abstract:
Security problems with interactions among defenders and attackers naturally fall under the framework of game theory. Since identifying equilibrium strategies in games modeling multi-agent interactions is difficult in general, many learning algorithms have been proposed for the design of decision policies to be followed by individual self-interested agents with results about convergence of such algorithms to an equilibrium for specific classes of games being known under the assumption that the same learning algorithm is adopted by all the agents. However, when the agents are self-interested, a natural question is why should agents follow these prescribed learning algorithms — specifically, do agents have a strong incentive to adopt an alternative learning algorithm that yields them greater individual utility? We explore the robustness of some popular learning algorithms to the presence of such strategic agents. First, we show that that for popular learning algorithms such as fictitious play and regret matching, an agent can move the game to a more favorable equilibrium for herself by deviating from the prescribed algorithm. In other words, these algorithms are not rational in the sense that they are not in equilibrium with themselves. We then propose and analyze two algorithms that are provably rational under mild assumptions and have the same convergence properties as (a generalized version of) fictitious play and regret matching, respectively.

Bio:
Vijay Gupta is the Elmore Professor of Electrical and Computer Engineering and the Associate Head for Graduate and Professional Programs in ECE at the Purdue University. He received his B. Tech degree at Indian Institute of Technology, Delhi, and his M.S. and Ph.D. at California Institute of Technology, all in Electrical Engineering. He is a Fellow of IEEE and has received the 2018 Antonio Ruberti Young Research Award from the IEEE Control Systems Society and the 2013 Donald P. Eckman Award from the American Automatic Control Council.

Lightning Talk

1:25p

"Digital Assurance for High Consequence Systems"

Dr. Will Zortman, Digital Assurance for High Consequence Systems (DAHCS) Campaign Manage, Sandia National Laboratories' Laboratory Directed Research and Development Office

Bio:
Will Zortman is the Digital Assurance for High Consequence Systems (DAHCS) Campaign Manager for Sandia National Laboratories' Laboratory Directed Research and Development Office. The DAHCS Mission Campaign is fundamental and developmental research focused on integrating digital assurance into the discipline of systems engineering enabling systems engineers, program managers and risk acceptors to make engineering trade-offs between digital risk and other system risks.

He began his career as an Air Force Combat Weather Officer leading a detachment at the Army's First Special Forces Group (Airborne) and a special operations weather team at the Air Force's 16th Special Operations Wing. Upon leaving the military Will led a security contracting activity providing tactical training to intelligence agencies.

Will moved into the semiconductor industry as a product change engineer at Lam Research Corporation where he was responsible for integrating design changes on etch and chemical mechanical planarization tools. He transitioned to manufacturing and later a failure analysis engineer at Intel Corporation where he pioneered AutoTracer, an automated defect response tool. Will left Intel to consult on the semiconductor industry for various hedge funds.

His career at Sandia began with integrated photonics designing state of the art photonics for focal plane array communications, high performance computing interconnect and spread spectrum technologies. Will applied his background in failure analysis and optics to supply chain assessments for the Air Force, Sandia's anti-tamper program and nuclear weapon cyber integration. During that time, he authored guides for the acquisition of security devices.

An author on 14 licensed patents and more than 50 peer reviewed publications, Will has served on multiple IEEE committees, is a program co-chair for the Physical Assurance and Inspection of Electronics (PAINE) for 2025. He has a Bachelors in Atmospheric Science from the University of Arizona and a PhD in Electrical Engineering from the University of New Mexico.

Will volunteers as a Wilderness Emergency Medical Technician (W-EMT) on Albuquerque Mountain Rescue Council (AMRC).

Panel Discussion #3

2:10p

"The Intersection between A.I. and Cybersecurity"

Moderator - Dr. Dongyan Xu, Director of CERIAS and Samuel D. Conte Professor of Computer Science

Dongyan Xu is a Samuel D. Conte Professor of Computer Science and Director of CERIAS, Purdue's cybersecurity research center. His research focuses on cyber and cyber-physical security. He has also made early contributions to the areas of cloud computing and peer-to-peer media streaming/distribution. He is part of the Purdue System Security Lab (PurSec).

For computer system security, Xu and his students have been developing virtualization-based systems for capturing, investigating, and defending against stealthy computer malware (e.g., worms, rootkits, bots, and APTs). His team is also developing reverse engineering techniques for the analysis of binary artifacts such as binary programs and memory images. For cloud computing, Xu and his students have been developing advanced techniques for the creation, management, and performance optimization of virtual networked infrastructures on top of physical cloud infrastructures.

Tim Benedict, Chief Technology Officer, COMPLiQ

Tim Benedict is a seasoned technology executive with over two decades of experience spanning IT, cybersecurity, AI governance, and digital transformation. As the Chief Technology Officer at COMPLiQ, he leads the development of AI-driven compliance and security solutions, helping organizations navigate regulatory requirements, mitigate risks, and adopt AI securely. His work focuses on building resilient, scalable platforms that empower enterprises to integrate AI while maintaining transparency, security, and operational control.

With a strong background in enterprise IT, cloud computing, and security architecture, Tim has worked across multiple industries, including finance, government, and technology. He has led large-scale cloud and cybersecurity initiatives, developed enterprise compliance strategies, and driven business-focused technology solutions that bridge innovation with regulatory and operational needs.

Tim's expertise spans strategic leadership, technical innovation, and cross-functional collaboration. He has shaped security-first approaches for AI governance, developed scalable frameworks for risk mitigation, and helped businesses align technology investments with long-term growth strategies. Based in Indiana, he remains actively engaged in fostering industry advancements and driving innovation in AI security and compliance.

Dr. Berkay Celik
Assistant Professor of Computer Science

Dr. Berkay Celik is an Assistant Professor in the Department of Computer Science at Purdue University and co-director of Purdue Security Laboratory (PurSec Lab). Dr. Celik is also affiliated with the Center for Education and Research in Information Assurance and Security (CERIAS), aiming to broaden interdisciplinary collaboration for security and privacy. He earned his Ph.D. in Computer Science and Engineering from Penn State University, where he was advised by Professor Patrick McDaniel and was the lead graduate student of the Systems and Internet Infrastructure Security Laboratory (SIIS).

Dr. Celik's research investigates the design and evaluation of security for software and systems, specifically on emerging computing platforms and the complex environments in which they operate. Through systems design, program analysis, and formal methods, my research seeks to improve security and privacy guarantees in commodity computer systems. His research approach is best illustrated by my extensive work in Internet of Things (IoT)/Cyber-Physical Systems (CPS), including robotic vehicles, automobiles, self-driving cars, industrial control systems, and mobile systems, such as smartphones, wearables (e.g., smartwatches, AR/VR headsets).

Dr. Celik's research group actively publishes at top security conferences (USENIX Security, Oakland, CCS, and NDSS). His group's work has been sponsored by NSF, ONR, DARPA, USDOT, DOE, United States Military Academy, Google, Apple, Cisco, Rolls Royce, Denso North America Foundation, and Sandia National Laboratories. I am part of the NSF AI Institute ACTION, DARPA FIREFLY, and USDOT National Center TraCR.

Dr. Jing Gao
Associate Professor, Electrical and Computer Engineering

Jing Gao is an Associate Professor in the Elmore Family School of Electrical and Computer Engineering, Purdue University. Before joining Purdue in January 2021, she was an Associate Professor in the Department of Computer Science and Engineering at the University at Buffalo (UB), State University of New York. She received her PhD from Computer Science Department, University of Illinois at Urbana Champaign in 2011.

Jing is broadly interested in data and information analysis with a focus on data mining. In particular, she is interested in information veracity analysis, multi-source data analysis, knowledge graphs, large language model, data and model efficiency, fairness and interpretation, transfer learning, federated learning, crowdsourcing, data stream mining, and anomaly detection. Her current research focus is on AI trustworthiness, safety and efficiency. She has published

over 200 papers in referred journals and conferences. Her publications have received over 20,000 citations and her H-index is 70. She is an editor of ACM Transactions on Intelligence Systems and Technology (TIST) and IEEE Transactions on Knowledge and Data Engineering (TKDE). She serves as the Program Committee Co-Chair of the 2025 IEEE BigData Conference and the 2024 SIAM Conference on Data Mining. She is a recipient of NSF CAREER award, IBM faculty award, ICDM Tao Li Award, SDM/IBM Early Career Award and UIUC CS Early Career Academic Achievement Alumni Award. She is a University Faculty Scholar.

Dr. Ananth Grama
Samuel D. Conte Professor of Computer Science

Ananth Grama's research focuses on parallel and distributed computing with applications in modeling, design, advanced manufacturing, machine learning, and artificial intelligence for complex physical systems. His work on computer systems focuses on load balancing, resource management, data management, and security. His recent work on algorithms and analysis focuses on establishing fundamental bounds on hallucinations, online learning, learning in faulty and private environments, and quantum machine learning. He applies these systems concepts and algorithms to a range of applications, including materials modeling, systems biology, transcriptomics, clinical analytics, and structural design.

Technology Talk

3:10p

"Securing Smart Sensing against Physical Adversarial AI Attacks"

Dr. Tao Li, Assistant Professor, Computer and Information Technology

Abstract:
Smart sensing systems using mmWave technology has promising applications in numerous scenarios, including monitoring and surveillance, healthcare, and smart home. mmWave technology is non-intrusive and can operate in situations where traditional sensors or cameras may fail. However, these systems also introduce new attack surfaces alongside their benefits. Existing security research on smart sensing systems primarily focuses on the vulnerabilities of the AI models used by these systems, without addressing the challenges of physically implementing these attacks in real-world scenarios. We identified the first physical backdoor attacks for mmWave-based HAR systems, manipulating physical signals to deceive the systems into producing targeted outputs. We will also discuss the effective countermeasures.

Bio:
Tao Li is currently an Assistant Professor in the Department of Computer and Information Technology at Purdue University. He received a Ph.D. in Computer Engineering from Arizona State University in 2020. His primary research is on security and privacy issues in AI-powered mobile sensing, wireless networks, and localization/navigation.

Technology Talk

3:35p

"Modeling Interaction Dynamics to Influence Human-AI Collaboration in Decision Making"

Dr. Ming Yin, Assistant Professor, Computer Science

Ming Yin is an assistant professor in the Department of Computer Science, Purdue University. Her primary research interests lie in the interdisciplinary field of social computing and crowdsourcing. She designs and conducts large-scale online behavioral experiments to obtain a quantitative perspective on participants' behavior in social computing and crowdsourcing systems (e.g., on-demand labor markets like Amazon Mechanical Turk). Based on the empirical evidence from the behavioral data, She further works on designing realistic models, novel algorithms and effective interfaces to facilitate the development of more intelligent and sustainable systems. Her research broadly connects to the fields of artificial intelligence and applied machine learning, computational social science, human-computer interaction and behavioral economics. Ming is named as a Siebel Scholar (Class of 2017), and has received Best Paper Honorable Mention at the ACM Conference on Human Factors in Computing Systems (CHI'16). Ming is a postdoctoral researcher at Microsoft Research New York City in 2017-2018, completed her PhD in computer science at Harvard University in 2017, and received her bachelor's degree from Tsinghua University, Beijing, China, in 2011.

Technology Talk

4:00p

"Cybersecurity of Smart Traffic Signal Systems"

Dr. Yiheng Feng, Assistant Professor and Assistant Director, Center for Road Safety (CRS), Lyles School of Civil and Construction Engineering

Abstract:
Traffic signal system is a critical component of urban transportation operations. Advancements in emerging technologies such as connected and automated vehicles (CAVs), V2X communication, and machine learning and their integration with conventional traffic signal systems, bring significant benefits in terms of improving mobility but at the same time open a door for cyber attacks. In this talk, I will present our recent research on the cybersecurity of traffic signal systems including threat modeling, impact analysis, and mitigation strategies.

Bio:
Dr. Yiheng Feng is an Assistant Professor at Lyles School of Civil and Construction Engineering, Purdue University. His research areas include connected and automated vehicles (CAVs) and smart transportation infrastructure, with a focus on cooperative driving automation and transportation system cybersecurity. His work appeared in top transportation journals and computer science security conferences. He has served as PI and Co-PI in many research projects funded by NSF, USDOT, USDOE, and industry companies. He is a member of the Traffic Signal Systems Committee (ACP25) at the Transportation Research Board (TRB) and co-chair of the Simulation Subcommittee. He is a recipient of the NSF CAREER award and several best paper and dissertation awards from multiple organizations.

Closing Keynote

4:30p

"IT, OT, IoT — It's Really Just the "T": An International and Historical Perspective"

Michael Clothier, Sector Chief Information Security Officer, Aeronautics Systems
Northrup Grumman

Abstract:
In today's rapidly evolving digital landscape, the lines between Information Technology (IT), Operational Technology (OT), and the Internet of Things (IoT) have become increasingly blurred. While these domains were once distinct, they now converge into a single, interconnected technology ecosystem—one that presents both unprecedented opportunities and critical security challenges.

In this keynote, Michael Clothier, Chief Information Security Officer at Northrop Grumman, brings 30 years of global cybersecurity leadership to explore how organizations can rethink their approach to securing "technology" as a whole, rather than as separate silos. Drawing on his extensive experience across the U.S., Australia, Asia, and beyond—including securing mission-critical defense and aerospace systems, leading enterprise IT transformations, and integrating cybersecurity across diverse industries—Michael will examine the evolution of security challenges from historical, international, and cross-industry perspectives.

Key discussion points include:

- From Air-Gapped to Always Connected – A historical view of how IT, OT, and IoT security challenges have evolved and what we can learn from past approaches.
- The Global Cybersecurity Landscape – Insights from securing critical infrastructure across Asia, Australia, and the U.S., and the lessons we can apply to today's interconnected world.
- Breaking Down the Silos – Why treating IT, OT, and IoT as distinct domains is outdated and how a unified security strategy strengthens resilience.
- National Security Meets Enterprise Security – Perspectives from both military and private-sector leadership on protecting sensitive data, intellectual property, and critical systems.

As cybersecurity professionals, we must shift our mindset from securing individual components to securing the entire technology ecosystem. Whether you are safeguarding an industrial control system, an aircraft, or a corporate network, the fundamental security principles remain the same. By applying an integrated approach, we can better protect the critical systems that power modern society.

Join Michael for this thought-provoking keynote as he challenges conventional thinking, shares real-world case studies, and provides actionable strategies to redefine cybersecurity in an era where everything is just "T."

Bio:
Michael Clothier is the Chief Information Security Officer(CISO) for the Aeronautics Systems (AS) Sector at NorthropGrumman, where he leads the sector's global cybersecuritystrategy. He is responsible for safeguarding mission-criticalaerospace and defense technologies, ensuring regulatorycompliance, and mitigating evolving cyber threats. With 30years of experience in cybersecurity and IT leadership, Michael has successfullydeveloped and implemented enterprise-wide security programs that align riskmanagement with business objectives in highly regulated industries.

Since joining Northrop Grumman in 2017, he has spearheaded cybersecurity initiativesthat enhance digital resilience, integrating cutting-edge security technologies whilefostering a culture of proactive defense. He collaborates closely with business leaders,IT, engineering teams, and government stakeholders to embed security into everyaspect of operations. His leadership ensures that cybersecurity remains a strategicenabler of technological innovation and national security.

Michael holds a Master of Business Administration from the University of New SouthWales, Sydney, and a Master of Science in Information Technology from WaldenUniversity. His background blends technical expertise, strategic vision, and operationalleadership, ensuring cybersecurity is not just a safeguard but a business enabler.

Passionate about protecting mission-critical systems, fostering innovation, andstrengthening cybersecurity resilience, Michael continues to drive global securityinitiatives that advance digital defense and operational excellence.

Poster Session Abstracts

POSTERS

POSTER SESSION RESEARCH AREA KEY

Artificial Intelligence	Red
Assured Identity and Privacy	Blue
End System Security	Pink
Human Centric Security	Yellow
Network Security	Violet
Prevention, Detection and Response	Green
Policy, Law and Management	Gold

These posters, and posters from previous years, are available at https://ceri.as/posters

ARTIFICIAL INTELLIGENCE

1. Adversarial Attack Analysis of a Phishing Email Detection System based on Machine Learning and Word Error Correction

Deeksha Hareesha Kulal

Phishing remains a critical cyber threat, with traditional ML-based detection models relying on grammatical errors and word anomalies as key indicators. However, LLM-generated phishing emails are well-structured, grammatically sound, and highly deceptive, making detection increasingly challenging. This research explores the impact of word correction and splitting techniques in strengthening ML-based phishing detection. We further investigate how these enhancements improve detection accuracy against well-crafted LLM-generated phishing emails and adversarial attacks, paving the way for more resilient and adaptive cybersecurity solutions.

2. Autonomous Flight of Fixed-Wing Aircraft Using Motion Capture

John Henry Slater, Braden Callaway, Natalia Zagata, Lillian Ji, Jonathan Cats, Anish Paspuleti

This research focuses on the development and testing of autopilot systems for lightweight fixed-wing Unmanned Aerial Vehicles (UAVs) within a controlled environment, utilizing the Purdue UAS Research and Test (PURT) facility. We propose a simple fixed-wing UAV using predominantly off-the-shelf components, replicating the characteristics of the Windracers fixed-wing aircraft, for comprehensive testing under various conditions. The aircraft utilizes an active LED marker board that is powered by the central battery and distinguishes and identifies individual aircraft, efficiently facilitating simultaneous operation of multiple units within the facility. The autonomous routine capabilities of the system are integrated with a nelly-constructed PID controller, which is simulated inside the Gazebo robotics simulation environment with a new high-quality 3D model of the aircraft. The integration of autopilot technology in lightweight unmanned fixed-wing aircraft holds significant potential for various applications, including surveillance, monitoring, and data collection in challenging environments. The results of this research contribute to the advancement of autonomous aerial systems, offering a platform for further developments in the field of unmanned aerial vehicles.

3. Ensemble Feature Selection for Network Intrusion Detection Systems Using Explainable AI: A Frequency-Based Approach

Ismail Bibers and Mustafa Abdallah

Feature selection is a crucial step in enhancing the performance, efficiency, and interpretability of machine learning models, especially for high-dimensional datasets like those in network security. This study introduces an ensemble-based feature selection framework leveraging Explainable AI (XAI) methods, including SHAP, LOCO, Profiled Weighting (ProfWeight) ,PFI, and DALEX, to rank features by importance. A frequency-based aggregation mechanism is employed in order to identify the most critical features, prioritizing those consistently ranked high across methods. The proposed framework was evaluated using the CICIDS-2017 dataset, a benchmark for intrusion detection research, and tested with multiple independent classifiers, including Random Forest, Logistic Regression, KNN, and AdaBoost. Evaluation results demonstrate significant improvements in classification accuracy, precision, and computational efficiency. This work highlights the potential of integrating XAI with feature selection to tackle the evolving challenges of network intrusion detection. It also paves the way for more accurate and interpretable intrusion detection systems. We made the implementation of our proposed feature ensemble framework used in this study available for the network security research community.

4. Text embeddings for efficient search in digital investigations

Vinicius Lima, Adil Koeken, Avantika Shah, Samay Nandwana, Umit Karabiyik

With the increasing storage capacities of modern devices, digital investigators face significant challenges in efficiently locating relevant information on incriminating devices. It is not uncommon for a single smartphone to contain over 100GB of data, making manual searches impractical. The problem becomes even more complex when the needed information is not easily discoverable through keyword searches or when investigators do not know which keywords to use. This makes digital investigations cumbersome and time-consuming, highlighting the need for more efficient search methods. For text-based data, one promising solution is the use of text embeddings (or vectors) instead of traditional keyword searches. In this study, we simulated a database containing text related to drug-related discussions, where specific drug names were not explicitly mentioned. This reflects real-world scenarios, such as conversations among drug dealers who use coded language (slangs) instead of technical terms. Our research demonstrates how embeddings can be leveraged to identify drug-related content without relying on predefined drug keywords. We applied the LLM2Vec technique using different models and instruction formats, achieving strong accuracy metrics. Our findings serve as a proof of concept that text embeddings can significantly enhance search efficiency in digital investigations compared to conventional keyword-based methods.

5. UAV-LLM Research Lab Platform

Karthisri Meghana Guntupalli ; Ashok Vardhan Raja, Ph.D.

Recent advancements in Large Language Models (LLMs) have created new opportunities to integrate these models into robotics platforms, allowing unmanned aerial vehicles (UAVs) to have enhanced control and decision-making capabilities. The UAV market has experienced significant growth in recent years, accompanied by a surge in UAV-related job opportunities. The need for LLM-powered UAVs is expected to increase significantly as LLM technology develops. Therefore, it is essential to provide the upcoming generation of professionals, students, and educators with the knowledge and abilities they need to develop, implement, and operate LLM-driven UAV systems efficiently. However, there is a lack of education and training materials on LLM-powered UAVs, especially for hands-on practice. We propose a novel LLM-powered UAV laboratory platform that provides effective and efficient hands-on practice. Our laboratory platform comprises different simulation environments and preconfigured lab modules. The outcome of these lab modules is to educate and train users on LLM-powered advanced aerial route planning and perform vision-based cyber attack analysis. The lab platform will be open source, allowing other developers to customize it to their needs. Hence, our platform adopts a plug-in-based design to support customization of the lab modules. Our evaluation results show that our platform is effective and efficient in training and educating the students and professionals in operating LLM-powered UAV via natural language commands, develop task-specific customized prompts using prompt engineering techniques.

6. Unlearning Machine Learning Bias using Task Vector Arithmetic

Omkar Pote, Romila Pradhan

Machine learning models have become integral to decision-making in fields such as criminal justice, finance, and healthcare. However, these models often inherit biases present in their training data, leading to unfair and unethical outcomes, particularly for marginalized groups. Recent work in the area of natural language processing has hypothesized bias to be a linear subspace in word embeddings. We evaluate the applicability of this concept to model weights of structured data, and introduce a novel task arithmetic based approach to unlearn bias in tabular datasets. Our method selectively unlearns biases introduced during training by fine-tuning a model on high-bias data, computing a bias task vector, and subtracting it from the original model to mitigate unwanted biases. Our evaluations show that this approach is competitive with state-of-the-art bias mitigation techniques, significantly improving fairness on several metrics with minimal accuracy loss.

ASSURED IDENTITY AND PRIVACY

7. Diffstats: Mitigating Data Poisoning Attacks to Local Differential Privacy

Xiaolin Li, Wenhai Sun

Local Differential Privacy (LDP) has emerged as a widely adopted privacy-preserving tool, with practical implementations by major industry players such as Google and Apple. However, recent data poisoning attacks have posed significant threats to LDP systems. In these attacks, adversaries inject malicious data to boost the estimated frequency of target items, thereby undermining the reliability of LDP-based statistical tasks. Existing detection methods have shown limited effectiveness in identifying such poisoning attacks. In this work, we propose a novel anomaly user detection method, Diffstats, which leverages the statistical differences in bit settings between attackers and benign users. Our experimental results demonstrate that Diffstats achieves substantial improvements in F1-score compared to current detection approaches (e.g., FIAD) on real-world datasets against the state-of-the-art poisoning attack, the Maximal Gain Attack (MGA).

8. DPFace: Formal Privacy for Facial Images

Tao Li, Rohan Ashok, Chris Clifton

There is growing concern about image privacy due to the popularity of social media and photo devices, along with increasing use of face recognition systems. However, established image de-identification techniques either are breakable and subject to re-identification, produce photos that are insufficiently realistic, or both. We present a definition for formally private image de-identification based on concepts from differential privacy. We also present a novel approach for image obfuscation by adding random noise to latent spaces of an unconditionally trained generative model that is able to synthesize photo-realistic facial images of high resolution; at low privacy levels (little noise) the original image is reproduced, but the images differ as the noise is increase while maintaining plausible facial images. To our knowledge, this is the first approach to image privacy that satisfies a noise-based formal privacy definition for the person.

9. Simulating Risks & Impacts of Cyberattacks on Critical Infrastructure

Aashi Agarwal, Kanari Hirano, Gerald Maduwuba, Courtney Falk, Rick Kennell

The Cyber Adversary Likelihood project has the goal of identifying methods for modeling adversaries in attacks on critical infrastructure, using those models to help determine the likelihood of various adversary actions. Specifically, the project will examine threat actors in the context of cyber systems (including information systems and control networks) and propose modeling approaches to approximate their behaviors. The project will develop a method to estimate likelihoods of various adversary actions in relevant contexts and then characterize and demonstrate that method. The ultimate use case of the model(s) and tool(s) is to estimate likelihood parameters in a broader model that will be used to assess risk to critical infrastructure from malicious and natural hazards.

END SYSTEM SECURITY

10. Cyber Analysis of OT Through Rehosting

Xander Lewis, Dan Joshwa, Lia Branstetter, Logan Manthey,
Advisors: Zachary Estrada, Dave Henthorn, Chris Miller

Rehosting is the process of porting a physical device to run in software. By rehosting operational technology (OT) devices, we are able to perform cyber analysis on critical infrastructure to protect from cyber attacks. Building upon MIT Lincoln Lab's existing rehosting infrastructure, we were able to demonstrate the feasibility of cyber analysis on two Programmable Logic Controllers (PLCs) to uncover existing and new vulnerabilities.

11. FuzzUEr: Enabling Fuzzing of UEFI Interfaces on EDK-2

Connor Glosner

Unified Extensible Firmware Interface (UEFI) specification describes a platform-independent pre-boot interface for an Operating System (OS). EDK-2 Vulnerabilities in UEFI interface functions have severe consequences and can lead to Bootkits and other persistent malware resilient to OS reinstallations. However, there exist no vulnerability detection techniques for UEFI interfaces. We present FUZZUER, a feedback-guided fuzzing technique for UEFI interfaces on EDK-2, an exemplary and prevalently used UEFI implementation. We designed FIRNESS that utilizes static analysis techniques to automatically generate fuzzing harnesses for interface functions. We evaluated FUZZUER on the latest version of EDK-2. Our comprehensive evaluation on 150 interface functions demonstrates that FUZZUER with FIRNESS is an effective testing technique of EDK-2's UEFI interface functions, greatly outperforming HBFA, an existing testing tool with manually written harnesses. We found 20 new security vulnerabilities, and most of these are already acknowledged by the developers.

12. Memory-Hard Proofs of Work

Nathan Smearsoll

A Memory-Hard Proof of Work (MHPoW) allows a prover to convince an efficient verifier that the prover invested substantial time and memory on a particular computation. Proofs of Work (PoW) in general are an important construction for distributed consensus and spam-mitigation protocols, but existing constructions rely upon computation time rather than the more egalitarian metric of cumulative memory cost. Previous attempts to define MHPoW have lacked a formal security proof and been vulnerable to attacks. In this work, we formalize a construction of a MHPoW based on the Merkle Tree Proofs framework. We formally prove that our protocol is sound when instantiated with a depth-robust graph. We then give an instantiation of our construct such that, with high probability, any prover which outputs a valid certificate for our construction must have cumulative memory cost at least O(N^2 / log N).

13. Modular Prime Bias in Exponential Prime-Generating Functions

Arnold Spantzel, Brigham Young University
rspantzel@gmail.com

Prime numbers play a crucial role in number theory, cryptography, and computational mathematics. This poster presents a computational analysis of modular biases in prime-generating functions of the form:

HUMAN CENTRIC SECURITY

14. Does Phishing Training Work? A Large-Scale Empirical Assessment of Multi-Modal Training Grounded in the NIST Phish Scale

Andrew Rozema, Jamie Davis

Phishing remains a critical cybersecurity threat, often lead ing to operational incidents and data breaches. Prior research on the effectiveness of cybersecurity awareness training has yielded mixed results, especially concerning the impact of training on responses to phishing lures of varying diffi culty. This paper presents a large-scale measurement study (N ≈4000) conducted at a US-based international fintech f irm, evaluating the effectiveness of different phishing train ing modalities. We compared a control group (no training), traditional lecture-based training, and the same traditional training augmented with an interactive phishing exercise. We observed statistically significant differences in reporting rates following training. Although lure efficacy—approximated using the NIST Phish Scale—significantly impacted click-through rates, our analy sis indicates that interactive training resulted in a statistically significant improvement in reporting behavior. Specifically, the interactive training group reported phishing attempts 37% more often than the baseline group and 25% more frequently than those receiving traditional training. However, the effect size remains modest. While interactive training does enhance phishing reporting, its impact is limited. This large-scale study contributes by demonstrating the practical utility of the NIST Phish Scale and the limited benefits of interactive training exercises in bolstering organizational defenses against phishing

15. Mechanisms of Virality in Public Online Discourse

Nicholas Harrell

The rapid proliferation of online discourse, particularly within social networks, has increased the spread of information at unprecedented rates. Although viral content often captures public attention, the underlying mechanisms driving its dissemination on social media remain illusive. This study highlights how value-laden features can be used to detect the potential of certain discourse on social media to become viral. Using a combination of Natural Language Processing (NLP) techniques and social network analysis, this research identifies patterns of user engagement that predict the likelihood of content achieving viral status. This study shows statistically significant differences in the value profile between the high and low engagement profiles of many topics on different alternative social media platforms. The results are further validated through predictive machine learning models. These results with discussion contribute to ethical concerns and implications related to the implementation of contemporary and future AI technologies that are being used for purposes of influencing public discourse on the Web.

16. Rationality of Learning Algorithms in Repeated Games

Shivam Bajaj, Pranoy Das, Yevgeniy Vorobeychik\, Vijay Gupta

Many learning algorithms are known to converge to an equilibrium for specific classes of games if the same learning algorithm is adopted by all agents. However, in applications in which AI and humans work together, a natural question is whether a (human) agent have an incentive to unilaterally shift to an alternative learning algorithm. We capture such incentives as an algorithm's rationality ratio, which is the ratio of the highest payoff an agent can obtain by unilaterally deviating from a learning algorithm to its payoff from following it. We define a learning algorithm to be c-rational if its rationality ratio is at most c irrespective of the game. We show that popular learning algorithms such as fictitious play and regret-matching are not c-rational for any constant c. We propose a framework that can build upon any existing learning algorithm and establish that our proposed algorithm is (i) c-rational for a given c and (ii) the strategies of the agents converge to an equilibrium, with high probability.

17. Real-Time Viewer Perceptions of 'Pedohunter' Content on Twitch

Doetri Ghosh, Donna Prince

'Pedohunters' pose as children online to catch adults soliciting minors. They often upload confrontation videos with those solicitors. Research shows mixed public reactions to pedohunter content. Prior work has mainly examined perceptions in asynchronous formats. The following project addresses this gap by exploring live, real-time reactions on a Twitch stream. Three qualitative coders engaged in open coding of physical actions found in each of the three videos analyzed. Then, code was discussed and aggregated accordingly. Additionally, sentiment analysis on comment over time was conducted as well as thematic analysis to find patterns in comments. The sentiment analysis reveals a notable change in sentiment over the course of the three videos.

Findings show six significant emerging themes from the viewer commentary.

18. Software Signing: Practical Adoption, Challenges, and Tooling Usability

Kelechi G. Kalu, Santiago Torres-Arias, and James C. Davis

Software signing is a critical mechanism for ensuring the integrity and authenticity of software components in the supply chain. Despite its importance and regulatory recommendations, adoption remains low, and the quality of software signatures is often inadequate. While prior research has examined technical aspects, there is a lack of in-depth industry perspectives on the challenges and drivers of software signing adoption. Additionally, little research has explored the usability of signing tools and its role in influencing adoption. To address these gaps, we conducted interviews with 18 experienced security practitioners across multiple organizations to understand how software signing is practiced, the usability and adoption challenges of signing tools, and the factors influencing tool evolution. Our findings reveal that: (1) Tool usability significantly impacts adoption, with integration complexity, automation, and compliance requirements shaping practitioners' choices; (2) Technical, organizational, and human factors create barriers to effective implementation; (3) Practitioners hold diverse perspectives on the importance of signing, with some viewing it as crucial for provenance, while others see it as a secondary or compliance-driven measure; and (4) Internal and external events, such as security incidents and regulatory mandates, play a key role in shaping signing practices. Our study provides insights into the evolving landscape of software signing adoption and offers recommendations to improve tool usability, standardization, and policy alignment to enhance software supply chain security.

NETWORK SECURITY

19. A Quantal Response Analysis of Human Decision-making in Interdependent Security Games Modeled by Attack Graphs

Md Reya Shad Azim

Interdependent systems, under the management of multiple decision-makers, confront rapidly growing cybersecurity threats. This paper delves into the realm of security decision-making within these complex interdependent systems managed by multiple defenders. Each defender assumes responsibility for safeguarding a specific subnetwork of the system against potential attacks. The relationships between these assets are depicted through an attack graph, where edges connecting assets signify that the compromise of one asset could expose vulnerabilities in another asset. These edges are associated with probabilities that represent the likelihood of a successful attack, which can be reduced through security investments by the defenders. Our approach involves modeling these systems using game-theoretic frameworks, accounting for the impact of bounded rationality and imperfect best-response behavior—as frequently observed in human decision-making within the domains of behavioral economics and psychology. We first establish the existence of quantal response equilibrium in our interdependent security games. We present illustrative examples to highlight the disparities between the solutions derived from the social optimal perspective and those arising from quantal response equilibrium. Subsequently, we analyze the inefficiency introduced by behavioral players with this type of bounded rationality in terms of the overall social cost of the system. We adapt a widely recognized metric to quantify the extent of this inefficiency, providing bounds and illustrating its exponential growth with an increase in the security budget. To assess our models, we employ a representative real-world interdependent system and compare the game-theoretic optimal investment strategies to those derived from a socially optimal standpoint.

20. Can Investigators Rely on DeepSeek Artifacts from Mobile Devices? An In-depth Forensic Analysis

Yufeng Gong; Sonali Tyagi; Vaishnavi Mahindra; Umit Karabiyik

As an application focusing on artificial general intelligence (AGI), open-source LLM DeepSeek has been widely adopted by many research institutions and international companies around the world. More than 60 million daily active users have been reported on DeepSeek by QuestMobile. Given DeepSeek's rapid growth in user population and the fact that mobile devices gradually function as centers for users to interact with AI-driven applications, it is essential to conduct thorough mobile forensics along with network forensics on the Deepseek's mobile app to discover potential evidence stored in both Android and iOS devices and provide valuable insight into its potential vulnerabilities. This investigation focused on user data and system usage such as log files, metadata, and other critical traces that can reveal insights into its operational behavior in different versions of DeepSeek and data packets sent over the network. Ultimately, this research help investigators fully utilize the forensic

implications of DeepSeek like the evidence that can be obtained and have a clear view of what can be recovered, thereby addressing the existing knowledge gap.

21. Data-free backdoor approach in Malware Image Classification Models.

Garvit Agarwal, Yousef Mohammed Y Alomayri, Meghana Nagaraj Cilagani, Agnideven Palanisamy Sundar, Feng Li

Malware classification models serve as critical safeguards in enterprise and infrastructure security, yet they remain susceptible to backdoor attacks, where an adversary surreptitiously implants triggers that induce targeted misclassifications. While state-of-the-art backdoor methods often assume direct or partial access to the original training dataset, such access may be infeasible in highly regulated domains where malware samples are proprietary. In this paper, we present a data-free backdoor attack that eliminates the need for original training data by constructing a carefully curated substitute dataset from publicly available malware repositories. We propose a logit-based dictionary mechanism that identifies high-confidence samples closely resembling the original data distribution. These samples are then poisoned with visually subtle triggers—such as noise patches or checkerboard patterns—and assigned misleading labels to craft a poisoned subset. We subsequently fine-tuned the target malware classifier on this poisoned subset using a novel loss function designed to preserve high clean accuracy while delivering a high attack success rate under trigger conditions. Experimental results on the MalImg dataset show that our data-free backdoor attack can achieve up to 99% misclassification on triggered malware samples, all without any access to the original training set. Our findings reveal a significant new threat vector for malware detection systems, demonstrating that even black-box models can be compromised by determined adversaries who traditionally solely on surrogate data and inference logs.

22. Deceptive Directions: Understanding Route Guidance and GPS Spoofing Attacks

Akshit Bedi, Abrar Ali

In an increasingly interconnected world reliant on precise navigation systems, the threat of Route Guidance Attacks and GPS Spoofing Attacks has emerged as a critical concern. Route Guidance Attacks manipulate routing instructions to mislead users, while GPS Spoofing Attacks falsify GPS signals to deceive location-based services. These attacks pose significant risks to transportation systems, emergency services, and digital applications reliant on accurate positioning. This research investigates the methodologies and implications of Route Guidance Attacks and GPS Spoofing Attacks, aiming to enhance understanding and develop robust countermeasures. The study focuses on analyzing attack vectors, evaluating their impact on system integrity and user safety, and proposing effective detection and prevention strategies. Leveraging techniques from network security and cryptographic protocols, the project aims to mitigate vulnerabilities in navigation systems and safeguard against malicious manipulations. By comprehensively addressing the technical, operational, and ethical dimensions of Route Guidance Attacks and GPS Spoofing Attacks, this

research contributes to advancing the resilience of location-based services and ensuring reliable navigation in the face of emerging cybersecurity threats.

23. Exploiting Intent State and Flow Configuration Discrepancy

Angela Yan, Jiwon Kim

Intent based networking (IBN) is a high-level network configuration concept that allows network operators to use high-level intents instead of complex low-level details. We found there are discrepancies in intent installation vs. flow configuration using ONOS which can allow attackers to exploit networks with DoS attacks.

24. HashRand: Asynchronous Random Beacon From Lightweight Cryptography

Akhil Bandarupalli, Adithya Bhat, Saurabh Bagchi, Aniket Kate, Michael K. Reiter

Regular access to unpredictable and bias-resistant randomness is important for applications such as blockchains, voting, and secure distributed computing. Distributed random beacon protocols address this need by distributing trust across multiple nodes, with the majority of them assumed to be honest. Numerous applications across the blockchain space have led to the proposal of several distributed random beacon protocols, with some already implemented. However, many current random beacon systems rely on threshold cryptographic setups or exhibit high computational costs, while others expect the network to be partial or bounded synchronous. To overcome these limitations, we propose HashRand, a computation and communication-efficient asynchronous random beacon protocol that only demands secure hash and pairwise secure channels to generate beacons. HashRand has a per-node amortized communication complexity of $\mathcal{O}(\lambda n \log(n))$ bits per beacon. The computational efficiency of HashRand is attributed to the two orders of magnitude lower time of a one-way Hash computation compared to discrete log exponentiation. Interestingly, besides reduced overhead, HashRand achieves Post-Quantum security by leveraging the secure Hash function against quantum adversaries, setting it apart from other random beacon protocols that use discrete log cryptography. In a geo-distributed testbed of $n=136$ nodes, HashRand produces 78 beacons per minute, which is at least 5x higher than Spurt [IEEE S\&P'22]. We also demonstrate the practical utility of HashRand by implementing a Post-Quantum secure Asynchronous SMR protocol, which has a response rate of over 135k transactions per second at a latency of 2.3 seconds over a WAN for $n=16$ nodes.

25. Learning Adversarial Attacks on Adaptive Traffic Signal Control Systems Under Cooperative Perception

Yiheng Feng, Wangzhi Li, Tianheng Zhu

Significant advancements in traffic control systems, such as integration with sensing and communication technologies, have led to increased system complexity. While these developments offer substantial benefits, they also introduce heightened vulnerabilities in cyberspace. This paper presents a security analysis of adaptive traffic control systems operating under cooperative perception environments with connected and automated vehicles (CAVs). To explore system vulnerabilities, we propose a novel reinforcement learning-based black-box adversarial attack framework, which demonstrates effectiveness against state-of-the-art adaptive traffic control systems. Specifically, the multi-action proximal policy optimization (multi-PPO) algorithm is employed to train the attacker agent capable of generating a fake CAV along with its "detected" vehicles. Experimental results indicate that the fake CAV can fool a learning-based traffic control system by injecting falsified detection data, leading to a 62.5% increase in average vehicle delay.

26. PR-DRA: PageRank-based defense resource allocation methods for securing interdependent systems modeled by attack graphs

Mohammad Al-Eiadeh and Mustafa Abdallah

Interdependent systems confront rapidly growing cybersecurity threats. This paper delves into the realm of security decision-making within these complex interdependent systems. We design a resource allocation framework to improve the security of interdependent systems managed by a single defender. Our framework models these systems and their potential attack vulnerabilities using the notion of attack graphs. We propose four defense mechanisms, incorporating a popular network analysis algorithm called PageRank which is used to identify the importance of different critical assets in the system. These mechanisms stem from existing graph theories widely used in graphical models (including Adjacent Nodes, In-degree Nodes, Min-Cut Edges, and Markov Blanket). We adopt the PageRank algorithm to extract useful information about the attack graphs we use. Our approaches show low sensitivity to the number of concurrent attacks launched over interdependent systems. We evaluate our decision-making framework via ten attack graphs, which include multiple real-world interdependent systems. We quantify the level of security improvement under our defense methods compared to four well-known resource allocation algorithms and other proposed approaches. Our proposed framework leads to better resource allocations compared to these algorithms in most test cases. According to our results and statistical tests, our defense resource allocation framework enhances security decision-making under various circumstances. Moreover, We release the full implementation of our framework for the research community to leverage it and build on it with new methods and datasets.

27. Securing Aviation Communications: A Network-Based Approach

Andrew Markel

Insecure aircraft communications pose a significant threat to aviation security, as unauthorized actors can spoof and intercept transmissions between pilots and air traffic controllers (ATC). This research presents a secure authentication and integrity framework to improve trust in aviation communications. Secure aviation networks require the ability to authenticate aircraft to the secure ATC network and verify the integrity of all transmissions. The proposed solution uses Public Key Infrastructure (PKI) to verify the integrity of communications. Certificates are attached to both aircraft registration and ATC stations, and the national database of valid certificates is managed by the Federal Aviation Administration (FAA) which acts as the Certificate Authority (CA) to ensure consistency and trust. Each aircraft's radio is equipped with a certificate store containing valid ATC certificates, updated dynamically via ATC networks or manually through standard FAA database updates. Pilots authenticate to secure ATC frequency networks with their valid digital certificates, and pilots verify authenticity of the ATC station using the built-in certificate store, which mitigates the risk of spoofed transmissions. For aircraft-to-aircraft communication, pilots must trust that all aircraft authenticated and connected to a secure ATC frequency network are authenticated and trusted against the FAA database. This solution significantly improves aviation security by eliminating existing vulnerabilities that leave safety-critical communication open to spoofing and interception. Secure ATC networks that authenticate users and verify integrity of communications will protect these safety-critical communications.

28. Small Trains, Big Risk: Physically Modeling Critical Freight Rail Infrastructure

Kira Sun, Courtney Falk

According to the Association of American Railroads, freight rail accounts for 40% of freight in the US. And hazardous materials arrive safely more than 99% of the time. But the geographic scale of freight rail in the US, coupled with the need for many companies to interoperate, creates a large attack surface for adversaries. Our research is building a physical simulation of freight rail to model the cyber-physical risk and understand its impact. The final model will allow other researchers to interact with the cyber layer to test attacks.

29. When TikTok is No Longer: A Forensic Analysis of Rednote on Android

Mingyang Xie, Xiao Hu, Akif Ahsen Ozer, Umit Karabiyik

This project presents a forensic analysis of Rednote application on the Android system. We simulated typical user interactions with Rednote application to populate data and utilized forensic tools to examine the mobile device for digital evidence that is important in relation to each event.

POLICY, LAW AND MANAGEMENT

30. Privacy Preserving Methodology to Empower Users to Understand Terms of Service Agreements

Adelheid Spantzel, Folsom Lake College
hspantzel@gmail.com

Terms of Service (ToS) agreements are widely accepted without being read, leading to privacy risks and loss of user rights. A Deloitte survey found that 91% of users do not read these agreements [1]. This work presents an AI-powered tool that simplifies ToS agreements and prioritizes key clauses. Unlike cloud-based solutions, it operates entirely on local devices, preserving privacy while enhancing user awareness.

PREVENTION, DETECTION AND RESPONSE

31. Cascading Risk in Cyber-Physical Systems Under Climate Uncertainty

Courtney Falk (falkc@purdue.edu), Alyssa Pletcher (pletchea@purdue.edu), Zachary Kirkeby (zkirkeby@purdue.edu), Aiden Tian (tian261@purdue.edu)

This project investigates cascading risks in cyber-physical systems under climate uncertainty, focusing on how natural disasters and cyberattacks can compound to disrupt critical infrastructure. Modern infrastructure systems—including those dedicated to power, water, and telecommunications—depend on cyberspace for real-time monitoring, control, and coordination. Using FEMA's Hazus software and the synthetic CLARC county dataset, we simulate storm events and assess their impact on these interdependent systems. Cyberattack scenarios are modeled using the MITRE ATT&CK framework, examining how the timing of attacks relative to natural disasters affects system vulnerabilities. Our findings aim to inform risk mitigation strategies that address both environmental and cyber threats in tandem.

32. iGEM: A Multi-Device Forensic Visualization Software for Geolocation and Digital Evidence Matching

Akif Ozer, Xiao Hu, Umit Karabiyik, Marcus K. Rogers

The rapid growth of mobile devices has changed the field of digital forensics and calls for new methods to analyze evidence comprehensively. Traditional forensic tools treat data sources separately, often missing important connections between spatial, temporal, and application usage information. This research, as detailed in the accompanying poster, introduces iGEM, a multi-device forensic visualization software that automates the extraction and integration of key artifacts from iOS devices. iGEM gathers information from sources such as Cache.Sqlite for GPS data, KnowledgeC.db for application logs, and KTX files for visual evidence. By merging these sources into a unified SQLite database and providing an interactive interface with timeline controls and map-based views, iGEM reveals hidden patterns in both time and space, thus enhancing investigative research and improving court presentations.

33. Model Order Reduction of Cyber-Physical Systems Considering Stealthy Attacks

Minhyun Cho, Suriyan Anandavel, Sounghwan Hwang

This paper introduces a new model order reduction problem for cyber-physical systems (CPSs) with vulnerability to stealthy cyberattacks. CPSs are susceptible to stealthy attacks and analyzing potential cyber-physical vulnerabilities in the systems is important to ensure their safety and reliability. To expedite the vulnerability discovery, we propose a vulnerability-preserving model order reduction method for a system susceptible to zero-dynamics and pole-dynamics attacks, two specific classes of stealthy cyberattacks.

34. Range-Based Multi-Robot Integrity Monitoring For Cyberattacks and Faults: An Anchor-Free Approach

Vishnu Vijay, Kartik A. Pant, Minhyun Cho, Yifan Guo, James M. Goppert, Inseok Hwang

Coordination of multi-robot systems (MRSs) relies on efficient sensing and reliable communication among the robots. However, the sensors and communication channels of these robots are often vulnerable to cyberattacks and faults, which can disrupt their individual behavior and the overall objective of the MRS. In this work, we present a multi-robot integrity monitoring framework that utilizes inter-robot range measurements to (i) detect the presence of cyberattacks or faults affecting the MRS, (ii) identify the affected robot(s), and (iii) reconstruct the resulting localization error of these robot(s). The proposed iterative algorithm leverages sequential convex programming and alternating direction of multipliers method to enable real-time and distributed implementation. Our approach is validated using numerical simulations and demonstrated using PX4-SiTL in Gazebo on an MRS, where certain agents deviate from their desired position due to a GNSS spoofing attack. Furthermore, we demonstrate the scalability and interoperability of our algorithm through mixed-reality experiments by forming a heterogeneous MRS comprising real Crazyflie UAVs and virtual PX4-SiTL UAVs working in tandem.

35. Resilient Multi-Robot Coverage Control Under Stealthy Cyberattacks

Kartik A. Pant, Vishnu Vijay, Minhyun Cho.

The problem of multi-robot coverage control has been widely studied to efficiently coordinate a team of robots to cover a desired area of interest. However, this problem faces significant challenges when some robots are lost or deviate from their desired formation during the mission due to faults or cyberattacks. Since a majority of multi-robot systems (MRSs) rely on communication and relative sensing for their efficient operation, a failure in one robot could result in a cascade of failures in the entire system. In this work, we propose a hierarchical framework for area coverage, combining centralized coordination by leveraging Voronoi partitioning with decentralized reference tracking model predictive control (MPC) for control design. In addition to reference tracking, the decentralized MPC also performs bearing maintenance to enforce a rigid MRS network, thereby enhancing the structural resilience, i.e., the ability to detect and mitigate the effects of localization errors and robot loss during the mission. Furthermore, we show that the resulting control architecture guarantees the recovery of the MRS network in the event of robot loss while maintaining a minimally rigid structure. The effectiveness of the proposed algorithm is validated through numerical simulations.

36. Secure Chain: A Knowledge Graph for Resilient, Trustworthy, and Secure Software Supply Chains

Yifeng Di, Hadi Askari, Shushan Arakelyan, Xiangyu Zhang, Xiang Ren, Muhao Chen, Tianyi Zhang

Software is now integral to critical U.S. infrastructures, with software supply chains supporting rapid development but also increasing risks. Bugs, vulnerabilities, or unauthorized changes in upstream components can propagate downstream, posing significant threats. We propose a comprehensive knowledge graph that models the relationships between software, hardware, vulnerabilities, and other entities in software supply chains. It captures rich, up-to-date information about software components in heterogeneous software ecosystems to support secure and transparent management of software supply chains.

37. Sensor Scheduling in Intrusion Detection Games with Uncertain Payoffs

Jayanth Bhargav, Shreyas Sundaram, Mahsa Ghasemi

We study the problem of sensor scheduling for an intrusion detection task. We model this as a 2-player zero-sum game over a graph, where the defender (Player 1) seeks to identify the optimal strategy for scheduling sensor orientations to minimize the probability of missed detection at minimal cost, while the intruder (Player 2) aims to identify the optimal path selection strategy to maximize missed detection probability at minimal cost. The defender's strategy space grows exponentially with the number of sensors, making direct computation of the Nash Equilibrium (NE) strategies computationally expensive. To tackle this, we propose a distributed variant of the Weighted Majority algorithm that exploits the structure of the game's payoff matrix, enabling efficient computation of the NE strategies with provable convergence guarantees. Next, we consider a more challenging scenario where the defender lacks knowledge of the true sensor models and, consequently, the game's payoff matrix. For this setting, we develop online learning algorithms that leverage bandit feedback from sensors to estimate the NE strategies. By building on existing results from perturbation theory and online learning in matrix games, we derive high-probability order-optimal regret bounds for our algorithms. Finally, through simulations, we demonstrate the empirical performance of our proposed algorithms in both known and unknown payoff scenarios.

38. SiDG-ATRID: Simulator for Data Generation for Automatic Target Recognition, Identification and Detection

Younggil Joshua Chang, Prof. Shreyas Sundaram, Alec Andrulis, Isabel Hoppe

The increased utilization of Unmanned Aerial Vehicles (UAVs) in diverse missions, from humanitarian aid to combat operations, underscores the necessity for an efficient and cost-effective development workflow for autonomous systems. Especially for defense purposes, building autonomous target recognition systems capable of detecting, identifying, and classifying adversarial agents with machine learning models requires extensive data for training. Consequently, simulation software has become an essential tool for developers seeking to assess autonomous system performance and collect data across various environments. Furthermore, the transition to real-world, application-ready systems necessitates a simulation platform that replicates not only the vehicle control algorithms but also environmental factors that affect system performance, such as lighting conditions and sensor noise. In response to these requirements, we introduce 'SiDG-ATRID' (Simulator for Data Generation for Automatic Target Recognition, Identification and Detection), a simulation platform that enables the collection of high-fidelity imagery data, powered by Unreal Engine 5. The simulator supports multi-agent simulations using the AirSim API library for UAV controls and simulates commercial aircraft traffic. This framework allows for customized camera placements to record videos or photos and manage environmental conditions such as weather and lighting. Additionally, by leveraging the Cesium API for geospatial mapping, it can accurately recreate real-world environments, enhancing the realism and applicability of simulations. This integrated approach enhances the efficiency and effectiveness of synthetic data generation for training machine learning and computer vision models.

39. Unleashing Insights from Terabytes: Microservices Architecture for Digital Intelligence and Evidence

Akif Ozer, Umit Karabiyik

The rapid increase in digital devices has generated an enormous amount of forensic data that challenges traditional analysis methods. In response, this study introduces FOREST (Forensic Search Tool), a distributed microservices architecture designed to enhance digital forensic investigations by dividing complex tasks into smaller, manageable services. At its core, FOREST employs an event-driven system using Apache Kafka for parallel task management, enabling the simultaneous processing of multiple data streams and significantly reducing evidence analysis time. The system utilizes ElasticSearch and PostgreSQL for efficient storage and rapid retrieval of both structured and unstructured data, ensuring seamless integration throughout the workflow. Furthermore, FOREST integrates a local AI module based on the Ollama framework to automatically extract and summarize key forensic artifacts, thereby minimizing the need for extensive manual review, while the inclusion of Ghidra for reverse engineering provides detailed insights into binary data.

Performance evaluations reveal that FOREST effectively manages terabytes of data, delivering considerable improvements in processing time and overall efficiency. Its scalable, fault-tolerant design also supports detailed cross-case analysis through graph-based indexing, demonstrating that the integration of distributed systems and AI can significantly transform digital forensic investigations to be faster, more reliable, and better equipped to handle modern digital evidence.

40. Using a Modified Delphi Method: Identify Cyber Secure Competencies for Older Adults

Julie wenner

This dissertation contributes to the United Nations and World Health Organization's Healthy Ageing (2021–2030) initiative by addressing digital equity and cybersecurity challenges faced by older adults. As cyber threats become more sophisticated, older individuals remain particularly vulnerable due to gaps in cybersecurity awareness, digital literacy, and evolving online risks. Using a qualitative mixed Delphi method, this research engaged a panel of fifteen interdisciplinary experts in cybersecurity and aging to refine thirty-two cybersecurity competencies within the Identify, Protect, Detect, and Respond categories of the NIST Cybersecurity Framework (CSF). The study explored key questions regarding the essential cybersecurity skills needed by older adults, the barriers preventing their adoption of best practices, and how existing digital competency models can be adapted to enhance cybersecurity resilience among aging populations. The findings revealed twenty-three critical gaps in older adults' understanding of core cybersecurity areas, including password security, phishing awareness, device protection, and online privacy. The Delphi panel emphasized the necessity of age-friendly cybersecurity education, incorporating simplified instructions, real-world scenarios, and interactive learning experiences to improve engagement. The study introduced the Cybersecurity Competency Model (CCM), grounded in Motivation, Awareness, Skills, and Knowledge (M.A.S.K.), reinforcing behavioral change through real-time feedback and cognitive adaptability. The research further aligns with Self-Determination Theory, Social Learning Theory, and Connectivism, emphasizing motivation, adaptability, and networked learning. Future research suggests that AI-driven cybersecurity training could enhance digital resilience, though human oversight remains crucial. This dissertation highlights the pressing need for structured, accessible cybersecurity education, advocating that an informed and proactive approach is the best defense against cyber threats, ultimately

supporting the UN and WHO's global vision for healthy aging.

41. Wearable Action Camera Forensics: GoPro HERO13 Black on Android

Yujin Lee, Umit Karabiyik

Wearable action cameras capture experiences from a first-person perspective while offering a compact design and hands-free operation. These features make them widely used across various fields, including sports, adventure, security, and healthcare. These devices collect a broad range of data, from media to telemetry, providing records of crime and incident scenes and helping law enforcement agencies reconstruct and understand event. This paper presents a forensic analysis of the GoPro HERO13 Black and its accompanying mobile application on the Android system. It provides insights into digital forensic investigations by detailing the digital evidence paths and locations generated by the action camera.

42. Weighted Anomaly Detection and Arbitrage Analysis: A Blockchain Forensics Framework Leveraging Bitcoin and Dogecoin Transactions

Xiao Hu, Umit Karabiyik

The rapid growth of cryptocurrencies has brought significant challenges to forensic investigations, particularly in detecting trading anomalies. The expanding cryptocurrency ecosystem has created more opportunities for arbitrage between emerging and traditional cryptocurrencies, complicating cross-chain activities. While existing research has primarily focused on price differences across exchanges, little attention has been given to the complexities of cross-chain arbitrage. To address this gap, we propose a blockchain forensics framework that integrates dynamic anomaly detection using the Isolation Forest model and bilateral cross-chain arbitrage analysis, specifically targeting Bitcoin and Dogecoin transactions. By leveraging adaptive statistical modeling, exponential decay factors for dynamic threshold calculation, time-delay analysis, and result visualization, our framework can effectively identify arbitrage opportunities in both directions and uncover irregularities in cross-chain interactions, such as potential fraud, manipulation, or market inefficiencies. Designed to assist forensic investigators, the framework streamlines the process of detecting these anomalies, significantly improving the efficiency and effectiveness of blockchain investigations. Evaluated using real-world transaction datasets, our framework demonstrates its value in advancing blockchain forensic analysis. An open-source implementation of the framework is provided to support reproducibility and facilitate broader application across various blockchain networks.

About CERIAS

CERIAS — The Center for Education and Research in Information Assurance and Security — is the world's largest and foremost multidisciplinary academic institute addressing the issues cyber and cyber-physical security, assurance, privacy, forensics, artificial intelligence, and trusted electronics. CERIAS brings together a team of world-class faculty, graduate student researchers and industry partners with the shared goal of advancing the state of cyber security through basic and applied research. CERIAS serves as an unbiased resource of information to the worldwide community.

Faculty from eight different colleges, and more than 18 departments, across Purdue University are conducting CERIAS research. The six primary areas of CERIAS research are:

- Assured Identity and Privacy
- End System Security
- Human Centric Security
- Network Security
- Policy, Law and Management
- Prevention, Detection and Response

Research at CERIAS continues to be vibrant with current projects addressing a large number of topics, from networks, operating systems, and database security to forensics and human factors. Security research at CERIAS results in comprehensive approaches and is characterized by both theoretical and experimental results. Notable efforts are also devoted to the development of testbeds and experimental environments; examples include the SOL4CE Laboratory, VoIP testbed, the Biometrics Laboratory and the ReAssure system. Education of top security researchers is a key goal of CERIAS - and students (undergraduate, graduate and post-doctoral) are involved in all those projects. We trust that you will appreciate this sampler of our projects.

Detailed information about research being conducted at CERIAS or at one of our academic partners is available by contacting us at (765) 494-7841ß or by visiting www.cerias.purdue.edu.

CERIAS has Moved to the Discovery Park District!

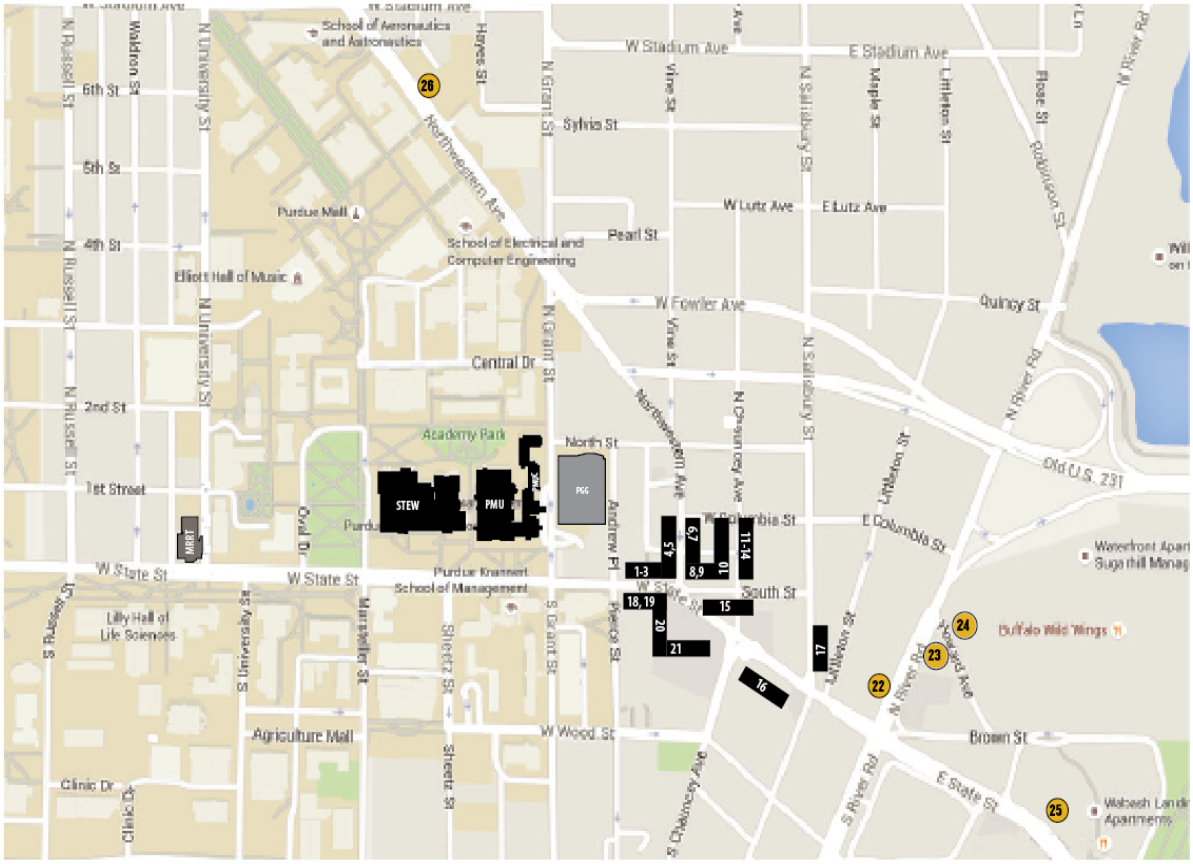
The *CERIAS Galactic Headquarters* has moved across campus to the Convergence Center for Innovation and Collaboration (CONV). Come visit us!

CERIAS, Purdue University
101 Foundry Drive
Convergence Center
Suite 3800
West Lafayette IN 47906-3446

Just south of Mitch Daniels Boulevard
(formerly State St.) on the west side of campus.

LOCAL RESTAURANTS

Provided by Purdue Conferences



ON CAMPUS

PURDUE MEMORIAL UNION (PMU)

LOWER LEVEL

Purdue Memorial Union's newly renovated space has a wide variety of dining options. From Starbucks, to Sushi, to Burgers, Pizza, Mexican, and more...visit: www.union.purdue.edu/dine/

SECOND FLOOR

8 Eleven Modern Bistro

STEWART CENTER (STEW)

Newsstand

MARRIOT HALL (MRRT)

Boiler Bistro
Lavazza

NEARBY

1. Mad Mushroom
2. Brothers
3. Blue Nile
4. Potbelly Sandwiches
5. Einstein Bros. Bagels
6. Panda Express
7. Egyptian Café
8. Greyhouse Coffee
9. Vienna Expresso Bar
10. Majé Sushi
11. Maru Sushi
12. Fiesta Mexican Grill
13. Red Mango
14. Noodles & Company
15. Chipotle
16. Raising Cane's Chicken Fingers
17. Triple XXX
18. Harry's
19. Jimmy Johns
20. Five Guys Burgers
21. Basil Thai & Bubble Tea
22. Town & Gown Bistro
23. Nine Irish Brothers
24. La Hacienda Bar & Grill
25. Moe's
26. Another Broken Egg