CERIAS® 2023

Annual Security Symposium ★ March 28th & 29th

Purdue University, West Lafayette, Indiana

Table of Contents

#CERIAS

Thanks to Our Strategic Partners

Analog Devices, Inc.
Boeing
Cisco
Eli Lilly and Company
General Motors
HP
Idaho National Laboratory
Infosys
Intel
Lawrence Livermore National Laboratory
Lionfish Cyber Security
ManTech
Mastercard
MITRE
Pacific Northwest National Laboratory
Peraton
Raytheon
Rolls-Royce
Salesforce
Sandia National Laboratories

Strategic Government Partners

National Institute of Standards & Technology (NIST)
National Security Agency (NSA)
State of Indiana

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

Day 1

Welcome

8:30a

STEW 214

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 Remarks

8:45a

STEW 214

Dr. Karen Plaut
Executive Vice President for Research, Purdue University

Dr. Karen Plaut became Executive Vice President for Research at Purdue University in January 2023. Overseeing an expanding $600 million research enterprise, Dr. Plaut is responsible for university-wide strategic initiatives and bringing together researchers and resources across traditional academic boundaries to drive interdisciplinary discoveries with societal impact.

She joined Purdue in 2010 as associate dean for research for the College of Agriculture and later became dean.

A researcher at heart, Dr. Plaut has approximately 100 publications focused on mammary gland biology and has received funding from USDA, NIH, NSF, and NASA.

Dr. Plaut earned her B.S. from the University of Vermont, M.S. from Pennsylvania State University and Ph.D. in animal science from Cornell University. Following a postdoctoral fellowship at the National Cancer Institute at NIH, she led mammary gland biology and breast cancer research at the University of Vermont, with dual appointments in the Department of Animal Science and the Department of Pathology in the College of Medicine.

Dr. Plaut then joined NASA and served as lead scientist for International Space Station Biological Research project working with engineers to build life science habitats for zero gravity. Space shuttle mission (STS-70) included her research investigating changes in mammary metabolism in rats.

Following her NASA appointment, she returned to the University of Vermont as Chair of the Animal Science department and then became Chair of Animal Science at Michigan State University before joining Purdue University.

Driving excellence in research and among researchers features strongly in Dr. Plaut's leadership to bring about breakthroughs that matter to society.

Guest Speakers

9:00a

STEW 214

Herbert J. Stapleton
Special Agent in Charge, FBI

Herbert J. Stapleton was named Special Agent in Charge of the Indianapolis Division of the FBI in February, 2022. In his previous role, he served as the Deputy Assistant Director (DAD) in the FBI's Cyber Division, where he lead the FBI's operational programs targeting sophisticated cyber threats from criminal and nation-state actors.

Mr. Stapleton began his FBI career as a Special Agent in the St. Louis Field Office, Cape Girardeau RA, and later served in the Chicago and Cincinnati Field Offices.

Prior to joining the FBI, he practiced corporate and commercial law in a private law firm.

Jeffrey S. Miller
Special Agent, FBI

A Purdue University graduate, Jeffrey has investigated cyber-crime for the FBI since 2010. During his tenure with the FBI, SA Miller has investigated numerous complex computer intrusions involving data breaches, theft of intellectual property, insider threats, ransomware, and dark markets in both the San Francisco and Indianapolis field offices.

Networking Break

10:00a

Panel Discussion #1 (Day 1)

10:15a

"Industry-Academia Cybersecurity Engagement"

STEW 214

Moderator - Shawn Huddy
Senior Manager for Strategic Partnerships, CERIAS

Richard Cardwell, Vice President Head of Cloud, Infrastructure, and Cyber Security Services North America, Infosys

Richard brings twenty years of experience across consulting and strategy roles at global technology organizations, focused on helping businesses transform for the increasingly digital future. In his current role as Head of Innovation and Delivery, Richard works to drive the development and delivery of new technologies such as Digital, Analytics, AI and the Internet of Things, with a particular focus on talent development and skilling. Richard is focused on accelerating the U.S. talent model for Infosys and driving the creation of new Innovation and Technology Hubs by collaborating with clients, local state governments, and academic ecosystems. Richard holds an MBA from Indiana Wesleyan University and a bachelor's degree in Psychology from Valparaiso University.

Michael Gahn, Chief of Technology, Product Cybersecurity, Rolls-Royce

Mike is the Chief of Technology, Product Cyber and is on the leadership team of Rolls-Royce LibertyWorks Research and Technology based in Indianapolis, Indiana. He has nearly 25 years of aerospace experience, predominantly in propulsion and power systems. He's supported all stages of the product lifecycle, from early research and development to production programs and aftermarket support in addition to five years in corporate strategy. Mike is responsible for all the research and technology development activities required to secure current and future products across the company and directs a portfolio of internal projects through TRL6 that utilize a global university research network and other key industry partners. Current research activities include feature/capability development, demonstrators, and digital modelling of cyber-physical systems via secure cyber-resilient engineering. Previously, Mike worked for both the U.S. Air Force and U.S. Navy and has a master's degree in Mechanical Engineering from the University of Dayton and an MBA from Butler University.

Kristyn Looney, Assistant General Counsel, Corporate Legal Services, Indiana University Health

Kristyn Kimery Looney has worked in healthcare her entire career. She has a Bachelor of Social Work and was Director of Social Services in a long-term care facility prior to attending the McKinney School of Law where she graduated Summa Cum Laude. She has worked in a wide-ranging scope of in-house roles including at: a Fortune 50 health insurance company, Eskenazi (as Wishard), as General Counsel and Compliance officer at the Regenstrief Institute (a health IT and biomedical informatics think tank on the IUPUI campus), and currently as Assistant General Counsel with IU Health interfacing with Informatics and Information Systems, Supply Chain, and IU Health Plans as internal business customers. Her primary focus is technology contracting, data only research, Data Governance, Intellectual Property, and Data Privacy and Security. In her current and most recent past role, she's interfaced with industry and academia and been a part of contracting for those relationships.

Cybersecurity Engagement Lighting Talks

STEW 214

University of Notre Dame

11:15a

Mitch Kajzer, Managing Director, Cybercrimes Investigations, Research, and Education Initiative (CIRE), University of Notre Dame

Mitch Kajzer is the Managing Director of the CIRE initiative out of the Center for Research Computing. His responsibilities include advising and overseeing digital forensics investigations, conducting research related to digital technology, and coordinating academic and private-sector courses and training related to digital forensics and technology. Mitch has been a law enforcement officer since 1989 and specializes in cybercrime investigations. He also created the St. Joseph County Cyber Crimes Unit where Notre Dame students work as investigators conducting digital forensics on criminal cases.

Purdue University

11:25a

Joel Rasmus Managing Director, CERIAS

Joel 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 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.

IUPUI

11:35a

Dr. Feng Li, Chair of the Department of Computer Information and Graphics Technology, IUPUI

Dr. Feng Li has been actively engaged in research on cybersecurity and trust issues, cloud, and mobile computing. He has published more than 50 papers in top conferences including INFOCOM and ICDCS. He welcomes any research/project collaboration on the above research topics.

Dr. Feng Li received Ph.D. in Computer Science from Florida Atlantic University in Aug. 2009. His Ph.D. advisor is Prof. Jie Wu. He earned his B.E. (Computer Science and Technology, 2002) and M.S. (Computer Science, 2005) from Southeast University (Nanjing, China). He joined the Department of Computer and Information Technology at Indiana University-Purdue University Indianapolis (IUPUI) in Aug. 2009. Dr. Li teaches Security and Networking courses in the department.

Indiana University

11:45a

Dr. Scott Shackelford, Professor of Business Law & Ethics, Kelley School of Business, Indiana University

Professor Scott J. Shackelford is a Professor of Business Law and Ethics at the Indiana University Kelley School of Business. He serves as the Executive Director of the Center for Applied Cybersecurity Research, as well as the Executive Director of the Ostrom Workshop. He is also an Affiliated Scholar at both the Harvard Kennedy School's Belfer Center for Science and International Affairs and Stanford's Center for Internet and Society.

Professor Shackelford's academic work and teaching have been recognized with numerous awards, including a Harvard University Research Fellowship, a Stanford University Hoover Institution National Fellowship, a Notre Dame Institute for Advanced Study Distinguished Fellowship, the 2014 Indiana University Outstanding Junior Faculty Award, the 2015 Elinor Ostrom Award, and the 2022 Poets & Quants Best 40-Under-40 MBA Professors Award.

Governor's Executive Council on Cybersecurity Report

12:00p

STEW 214

Chetrice Mosley-Romero
Indiana Cybersecurity Program Director

As Indiana's Cybersecurity Program Director, Chetrice Mosley-Romero works collaboratively with public and private stakeholders to administer the development and implementation of the state's cybersecurity strategy and policy through the Governor's Executive Council on Cybersecurity. Prior to her current role, she was the Executive Director of External Affairs for the Indiana Utility Regulatory Commission where she led the public relations, policy, and consumer affairs, divisions. Additionally, Mosley-Romero oversaw the Commission's Continuity of Operations Plan and emergency management role with Indiana's Department of Homeland Security (IDHS) Emergency Operations Center. She also served as a Steering Committee member and advisor to IDHS as the agency developed and implemented the first-of-its-kind Crit-Ex tabletop and operational exercise. Before her role at the Commission, she worked for the Indiana Department of Revenue where she was the Public Relations Manager over several strategic initiatives including the launch of Indiana's Identity Theft Protection Program. An award-winning professional, Mosley-Romero has provided public relations and strategic consultation to a number of state agencies and organizations.

Lunch Break

12:30p - 2:00p

PMU

Purdue Memorial Union's Atlas Family Marketplace has a wide variety of dining options to satisfy you.

Aatish - Halal contemporary kitchen

BBQ District - Slow-cooked meats, regional sauces and savory sides.

Chef Bill Kim's - Asian dumplings and bowls using authentic ingredients.

Fresh Fare - Fresh flavors with an emphasis on dairy-free and gluten-free options.

Latin Inspired - South American flavors and Latin fare from Brazil and Argentina.

Pizza & Parm Shop - Detroit-style pizza with a caramelized cheese crust and creative parm sandwiches.

Sol Toro - Mexican flavors with a modern flair.

Starbucks®

Sushi Boss - Fresh custom sushi.

Walk On's Sports Bistreaux - Louisiana-inspired cuisine with a game-day flair: burgers, wraps, salads, seafood specialties.

Zen - Build-your-own sushi in a bowl, salad bar and boba teas.

Also... see page 37 for a map of nearby restaurants

20th Anniversary of the Grand Challenges in Trustworthy Computing Report

2:00p
STEW 214

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. Spaf's latest book, *Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us* was just published in February, 2023.

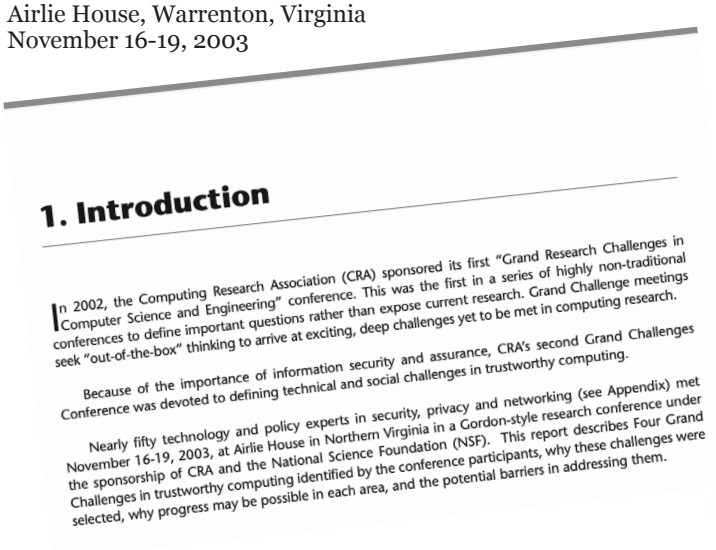
Richard DeMillo
Charlotte B. and Roger C. Warren Professor of Computing, Georgia Tech

Richard DeMillo is a professor at Georgia Tech's School of Cybersecurity and Privacy. He holds the Charlotte B. and Roger C. Warren Chair in Computing at Georgia Tech. He is is also Managing Director of Gtatrium™, LLC, a subsidiary of Georgia Advanced Technology Ventures. He was formerly the John P. Imlay Dean of Computing and Director of the Georgia Tech Information Security Center.

Positions he held prior to joining Georgia Tech, include: Chief Technology Officer for Hewlett-Packard, Vice President of Computing Research for Bell Communications Research, Director of the Computer Research Division for the National Science Foundation, and Director of the Software Test and Evaluation Project for the Office of the Secretary of Defense. He has also held faculty positions at the University of Wisconsin, Purdue University and the University of Padua, Italy.

"Grand Research Challenges in Information Security & Assurance"

Airlie House, Warrenton, Virginia
November 16-19, 2003



1. Introduction

In 2002, the Computing Research Association (CRA) sponsored its first "Grand Research Challenges in Computer Science and Engineering" conference. This was the first in a series of highly non-traditional conferences to define important questions rather than expose current research. Grand Challenge meetings seek "out-of-the-box" thinking to arrive at exciting, deep challenges yet to be met in computing research.

Because of the importance of information security and assurance, CRA's second Grand Challenges Conference was devoted to defining technical and social challenges in trustworthy computing.

Nearly fifty technology and policy experts in security, privacy and networking (see Appendix) met November 16-19, 2003, at Airlie House in Northern Virginia in a Gordon-style research conference under the sponsorship of CRA and the National Science Foundation (NSF). This report describes Four Grand Challenges in trustworthy computing identified by the conference participants, why these challenges were selected, why progress may be possible in each area, and the potential barriers in addressing them.

Organizing Committee Members

Eugene H. Spafford, Purdue University (Committee Chair)

Richard A. DeMillo, Georgia Institute of Technology (Committee Co-Chair)

Andrew Bernat, Computing Research Association **Steve Crocker**, Shinkuro, Inc.
David Farber, Carnegie Mellon University
Virgil Gligor, University of Maryland

Sy Goodman, Georgia Institute of Technology **Anita Jones**, University of Virginia
Susan Landau, Sun Microsystems Laboratories **Peter Neumann**, SRI

David Patterson, University of California, Berkeley
Fred Schneider, Cornell University
Douglas Tygar, University of California, Berkeley
William Wulf, National Academy of Engineering and University of Virginia

Acknowledgments

Funding for this conference was provided by National Science Foundation Grant No. CCR-033524.

https://archive.cra.org/Activities/grand.challenges/security/home.html

"The Next Decade" Survey Call

3:15p
STEW 214

Please visit:
https://ceri.as/survey2023

Networking Break

3:25p
STEW 214

Distinguished CERIAS Alumnus Talk

3:40p
STEW 214

Dr. Wenliang (Kevin) Du, Laura J. and L. Douglas Meredith Professor of Electrical Engineering and Computer Science, Syracuse University

"Developing an Internet and Blockchain Emulator for Research and Education"

To provide a learning and testing environment for cybersecurity and network education and research, we have developed an open-source Internet Emulator (called SEED Emulator), which allows us to create a miniature Internet that can run inside a single personal machine or on multiple cloud machines. Even though it is small, it has all the essential elements of the real Internet. Many interesting network technologies can be deployed on the emulator. We have used this emulator to create a DNS infrastructure, a Botnet, a Darknet, an Internet worm, and BGP prefix hijacking attacks. Many more are being developed. We have also deployed the Ethereum blockchain on the emulator, creating a Blockchain emulator with tens or even hundreds of nodes, all inside a single computer.

This emulator has been primarily used for education after it was released in August 2021, but recently several research groups have started to use it for their research. In this talk, I will present the design and features of the SEED emulator and its applications in both research and education. I will also demonstrate some of the interesting hands-on lab activities based on the emulator.

Dr. Wenliang (Kevin) Du, IEEE Fellow, is the Laura J. and L. Douglas Meredith Professor at Syracuse University. His current research interest focuses on Internet/blockchain emulation and cybersecurity education. He received his bachelor's degree from the University of Science and Technology of China in 1993 and Ph.D. degree from Purdue University in 2001 (CERIAS). He founded the SEED-Labs open-source project in 2002. The cybersecurity lab exercises developed from this project are now being used by 1,050 institutes worldwide. His self-published book, "Computer & Internet Security: A Hands-on Approach", has been adopted as textbook by 255 institutes. His online courses published on Udemy frequently won the "best seller" and "highest rated" recognition. He is the recipient of the 2017 Academic Leadership award from the 21st Colloquium for Information System Security Education. His research has been sponsored by multiple grants from the National Science Foundation and Google. He is a recipient of the 2021 ACSAC Test-of-Time Award and the 2013 ACM CCS Test-of-Time Award.

Research Poster Session Preview

4:00p
STEW 214

Students from Indiana colleges and universities present their research in an "elevator pitch" format

End of Session 1

5:00p

Poster Session and CERIAS 25th Anniversary Celebration

PMU South Ballroom 6:30-9:00pm

Highlighting research conducted by students at Indiana colleges and universities

Day 2

Registration / Coffee

8:00a
STEW 214

Opening Comments, CERIAS Awards

9:00a
STEW 214

25th Anniversary Achievements

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

Diamond Award
The annual Diamond Award goes to a student that most exemplifies the "diamond in the rough" transition through outstanding academic achievement and/or research excellence.

Pillar of CERIAS
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

9:30a
STEW 214

Robert M. Lee
CEO & Co-Founder, Dragos, Inc.

"Trends in the Industrial Cybersecurity Landscape"

Robert is a recognized authority in the industrial cybersecurity community. He is CEO and co-founder of Dragos, a global technology leader in cybersecurity for industrial controls systems (ICS)/operational technology (OT) environments.

In addition, Robert serves on the Department of Energy's Electricity Advisory Committee as the Vice Chair of the Department of Energy's Grid Resilience for National Security Subcommittee, and is a member of the World Economic Forum's subcommittees on Cyber Resilience for the Oil & Gas and Electricity communities.

Robert is routinely sought after for advice and input on cybersecurity for industrial infrastructure and is regularly asked to brief national leaders. He testified to the U.S. House of Representatives Committee on Energy and Commerce–Subcommittee on Oversight and Investigations, and to the U.S. Senate Energy and Natural Resources Committee, to advise on policy issues related to critical infrastructure cyber threats. He has also presented at the World Economic Forum Annual Meeting in Davos, and industry leading conferences such as RSA, SANS, BlackHat, and DefCon on the topic of industrial cybersecurity and threats. He serves on the board of the National Cryptologic Foundation.

Robert began his pioneering work in ICS/OT cybersecurity as a U.S. Air Force Cyber Warfare Operations Officer tasked to the National Security Agency, where he built a first-of-its-kind mission identifying and analyzing national threats to industrial infrastructure. He went on to build the industrial community's first dedicated monitoring and incident response class at the SANS Institute (ICS515) and the industry recognized cyber threat intelligence course (FOR578).

SC Media named Robert the Security Executive of the Year for 2022. A business leader but also technical practitioner, he helped lead the investigation into the 2015 attack on Ukraine's power grid, the first time an electric system was taken down due to a cyberattack. With his team at Dragos he has been involved in the most significant cyberattacks on industrial infrastructure, including the investigation and analysis of the 2016 attack on Ukraine's electric system, the 2017 TRISIS attack on a Saudi Arabian petrochemical facility in the first attempt to try to kill people through malicious software, and the 2021 Colonial Pipeline ransomware attack. In 2022, his team at Dragos uncovered PIPEDREAM, a highly flexible framework to attack industrial infrastructure globally. Robert's work has been featured in the book Sandworm and on 60 Minutes.

Networking Break

10:30a
STEW 214

Fireside Chat

Dr. Eugene Spafford
Executive Director Emeritus & Founder, CERIAS, Purdue University
(see pg 8 for bio)

Robert M. Lee
CEO & Co-Founder, Dragos, Inc.
(see previous page for bio)

Wendy Nather, Head of Advisory CISOs, Cisco
(see pg xx for bio)

CERIAS Tech Talk

11:30a
STEW 214

Dr. Kate Seigfried-Spellar
Associate Professor, Computer and Information Technology, Purdue University

"Criminology, Linguistics, and Biometrics: An Interdisciplinary Approach to Identifying Online Child Sex Offenders"

Dr. Kathryn Seigfried-Spellar is an Associate Professor in the Department of Computer and Information Technology (CIT) at Purdue University. Dr. Seigfried-Spellar has multiple publications, book chapters, and conference paper presentations, including international presentations in India, Ireland, England, Russia, and South Korea on the who and why of cybercrime. Specifically, Dr. Seigfried-Spellar studies the personality characteristics and socio-legal factors associated with cyberdeviance, such as Internet child pornography use, hacking, cyberbullying, trolling, and cyber threats via social media. In addition, Dr. Seigfried-Spellar has published in the area of digital forensics, specifically the ability to conduct a behavioral analysis of digital forensic evidence from child pornography investigations. Most recently, she published, along with Thomas J. Holt and Adam M. Bossler, the book, Cybercrime and Digital Forensics: An introduction (2nd edition). Dr. Seigfried-Spellar is a Fellow of the Digital and Multimedia Sciences section of the American Academy of Forensic Sciences (AAFS), International Association of Law Enforcement Intelligence Analysts (IALEIA), the American Psychological Association (APA), and the American Psychology-Law Society (AP-LS). Dr. Seigfried-Spellar also serves as an editorial board member for the Journal of Digital Forensics, Security, and Law as well as the International Journal of Psychology and Cyber Crime.

Guest Speaker

11:50a
STEW 214

Peter Choi
Principle Member of Technical Staff - R&D, Cybersecurity at Sandia National Laboratories

Peter Choi has been working for SNL past 12 years as Principal Member of Technical Staff. He possesses over 25 years of information assurance management and systems security engineering experience engaging in the areas of DoD, DOE, DHS, financial, and educational industry. Peter has extensive knowledge in COMSEC key management systems, DITSCAP, DIACAP and DIARMF management experiences. He has led numerous Army and Air Force projects related to information assurance as well as providing cybersecurity risk management consultation services to Higher Education (i.e., University of San Francisco, Northwestern University, and John Hopkins University, Stanford University, UC Berkeley). He has also served as a Corporate Information Security Officer for Citibank. During his tenure at Citibank, he played an instrumental role in demonstrating the world's first use of PKI for e-commerce (i.e., NACHA* Interoperability Test). Field of technical interest includes PKI, authentication and identity management, biometrics, Smart Cards, NIST guidelines, FIPS 140-2 and Common Criteria certification. Since joining SNL, Peter has successfully filed four US Patents related to cybersecurity technologies and have received following patents: United States Patent # 10,439,817 (Ephemeral Biometrics); US Patent # 10,541,996 (Methods and Systems for Authenticating Identity); US Patent # 11,070,532 (Methods for Communicating Data Utilizing Sessionless Dynamic Encryption). Peter (as Principal Investigator) and his team have received 2021 R&D100 Award for revolutionary technology called Secure - Firmware Over-The-Air (S-FOTA). In 2019, Peter was able to form a small technology company, Cyber Sonata LLC, where he is working to find ways to commercialize laboratory inventions. Peter holds doctoral degree (Ph.D. in Computational Physics from Purdue University) as well as cybersecurity professional certifications (i.e., CISSP, CSSLP, and IAM). Peter is also an Adjunct Associate Professor at University Maryland Global Campus, teaching various cybersecurity graduate courses.

Lunch and Networking Break

12:15p

See lunch options on pg 7.

Guest Speaker

1:30p
STEW 214

Snehal Antani
CEO, Horizon3.ai and Innovation Hub

"Effective Security: Proactively Verifying Your Security Posture"

Snehal Antani is an entrepreneur, technologist, and investor. He is CEO & Founder of Horizon3.ai, a cyber security company using AI to deliver autonomous penetration Testing.

Prior to Horizon3, Snehal served as the first Chief Technology Officer for Joint Special Operations Command (JSOC). As a member of the Commander's executive team, he led data analytics, cloud/edge computing, and cybersecurity initiatives

Prior to serving within US Special Operations, Snehal was CTO & SVP at Splunk, held multiple CIO roles at GE Capital, and started his career as a Software Engineer at IBM.

Snehal earned a Masters in Computer Science from Rensselaer Polytechnic University (RPI), a BS in Computer Science from Purdue University, and holds 18 patents.

Networking Break

2:00p
STEW 214

Panel Discussion #2 (Day 2)

2:15p

STEW 214

"The Intersection of Space and Cybersecurity"

Moderator - Joel Rasmus - CERIAS Managing, Director, CERIAS

Joel 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 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.

Dr. Barrett Caldwell Professor of Industrial Engineering and Joint Appointment in Aeronautics & Astronautics, Purdue University

Barrett S. Caldwell is Professor of Industrial Engineering (and Aeronautics & Astronautics, by courtesy) at Purdue. His PhD (Univ. of California, Davis, 1990) is in Social Psychology, and BS degrees in Aeronautics and Astronautics and Humanities (MIT, 1985). His research team is the Group Performance Environments Research (GROUPER) Laboratory. GROUPER examines and improves how people get, share, and use information well in settings including aviation, critical incident response, healthcare, and spaceflight operations. Prof. Caldwell has over 200 scientific publications, including journal articles, conference proceedings, and book chapters.
He was named in 2008 as a Fellow of the Human Factors and Ergonomics Society (HFES, the leading scientific body in this area in the US and one of the premier ergonomics societies in the world). Prof. Caldwell was also asked to co-organize the 2008 session on Cognitive Ergonomics for the National Academy of Engineering US Frontiers of Engineering (FOE) conference. (He was also a participant in the 2003 US FOE, and the 2006 German-American FOE, conferences.) His work demonstrates a fundamentally interdisciplinary and multifaceted approach to learning, exchanging, and applying knowledge.

Sean Plankey Chief Architect, Bedrock Systems

Sean Plankey currently serves as the Chief Architect for BedRock Systems, leading efforts to utilize BedRock's formal methods proven software isolation secure platform to solve the most pressing cybersecurity problems across industry and government. Prior to BedRock Systems Sean served as the Public Sector CTO at DataRobot, a Silicon Valley Artificial Intelligence Platform. In government, Sean served as the Principal Deputy Assistant Secretary for Cybersecurity, Energy Security, and Emergency Response at the Department of Energy. In this role he led the design and implementation of DOE's cybersecurity supply chain program CyTRICS. He is a 2003 graduate of the United States Coast Guard Academy and a 2008 graduate of the University of Pennsylvania.

Ambrose Kam Cyber Chief Scientist / Fellow - Lockheed Martin

Ambrose Kam is a Lockheed Martin Fellow with over 25 years of experience in the Department of Defense (DoD) industry. He is one of the earliest pioneers at applying modeling, simulation, and operations analysis techniques to threat modeling and cyber resiliency assessment. He regularly gives lectures at MIT, Georgia Tech, and industry consortiums like the Military Operations Research Society (MORS) and National Defense Industry Association (NDIA). Ambrose has been quoted in major publications including Forbes, The Economist, etc, and has co-authored a book in Simulation and Wargames. As a subject matter expert, he represents Lockheed Martin in industry standards organizations like ISO, LOTAR, and INCITS. His most recent efforts in wargaming, Machine Learning/Deep Learning, Cyber Digital Twin, and Blockchain earned him patents and trade secret awards. In 2017, Ambrose won the prestigious Asian American Engineer of the Year (AAEOY) award for his technical leadership and innovations. He holds several advanced degrees from MIT and Cornell University as well as a Bachelor of Science degree from the University at Buffalo.

Dr. Kimberly S. King Senior Engineer Specialist at the Aerospace Corporation

Dr. Kimberly S. King is a Senior Engineer Specialist at the Aerospace Corporation where she is very fortunate to work in the intersection of cybersecurity, aerospace and national security.

An enthusiastic problem solver, skilled at grasping complex challenges, assimilating, and analyzing information, and examining problems from multiple perspectives – including human and technical.

The full life-work balance also includes Pilates, rowing, classical guitar, and playing with her menagerie of dogs and parrots.

Kimberly holds a Ph.D. in mathematics from the University of Maryland at College Park and a bachelor's degree in computer science from George Mason University.

CERIAS Tech Talk

3:15p
STEW 214

Dr. Aniket Bera
Associate Professor, Computer Science, Purdue University

"Designing Emotionally-Intelligent Digital Agents that Move, Express, and Feel Like Us!"

The creation of intelligent virtual agents (IVAs) or digital humans is vital for many robotic, virtual and augmented reality systems. As the world increasingly uses digital and virtual platforms for everyday communication and interactions, there is a heightened need to create human-like virtual avatars and agents endowed with social and emotional intelligence. Interactions between humans and virtual agents are being used in different areas including, social robotics, VR, games and story-telling, computer-aided design, social robotics, and healthcare. Designing and building intelligent agents that can communicate and connect with people is necessary but not sufficient. Researchers must also consider how these IVAs will inspire trust and desire among humans. Knowing the perceived affective states and social-psychological constructs (such as behavior, emotions, psychology, motivations, and beliefs) of humans in such scenarios allows the agents to make more informed decisions and navigate and interact in a socially intelligent manner.

In this talk, I will give an overview of our recent work on simulating intelligent, interactive, and immersive human-like agents who can also learn, understand and be sentient to the world around them using a combination of emotive gestures, gaits, and expressions. Finally, I will also talk about our many ongoing projects which use our AI-driven IVAs, including intelligent digital humans for urban simulation, mental health and therapy applications, and social robotics. Our research also focuses on building embodied computational models of human social behavior, developing component algorithms of an intelligent agent (from sensing, to decision-making, to actuating). Our long-term research goal is to create engaging, socially intelligent agents that can interact with humans in innovative ways through expressive multi-modal interaction.

Aniket Bera is an Associate Professor at the Department of Computer Science at Purdue University. He directs the IDEAS lab (Intelligent Design for Empathetic and Augmented Systems). His core research interests are in Affective Computing, Social/Human Robotics, Computer Graphics (AR/VR, Augmented Intelligence, Multi-Agent Simulation), Autonomous Agents, Cognitive modeling, and planning for intelligent characters. He is currently serving as the Senior Editor for IEEE Robotics and Automation Letters (RA-L) in the area of "Planning and Simulation". His work has won multiple awards at top Graphics/VR conferences. He has previously worked in many research labs, including Disney Research and Intel. Aniket's research has been featured on ABC News, Bloomberg, CBS, WIRED, Forbes, FastCompany, Times of India, etc.

CERIAS Tech Talk

3:35p
STEW 214

Dr. Zahra Ghodsi
Assistant Professor, Electrical and Computer Engineering, Purdue University

"Pushing the Frontiers of Collaborative Learning: Security Challenges and the Path Forward"

Dr. Ghodsi's research interests are at the intersection of machine learning, applied cryptography, and hardware. She is passionate about building secure systems for emerging intelligent devices and applications. Making practical systems requires addressing a variety of challenges at the protocol, algorithm, and hardware level which in many scenarios, should be designed together.

CERIAS Tech Talk

3:55p
STEW 214

Dr. Mohammadkazem Taram
Assistant Professor of Computer Science, Purdue University

"Defusing the Tension between Security and Performance with Secure Microarchitectures"

The tension between security and performance has become more painful in recent years. In the context of processor architecture, we are observing a large influx of new attacks that appear regularly, each exploiting a crucial performance optimization, threatening to unwind decades of architectural gains. This talk will cover how we attempt to defuse this tension. I first describe an example that shows how performance optimizations can have devastating security implications. Then, I present novel secure and fast architectures to mitigate vulnerabilities in two of the most crucial performance optimizations in modern processors: Speculative Execution and Simultaneous Multithreading.

Mohammadkazem (Kazem) Taram is an assistant professor in the Department of Computer Science at Purdue University. He received his PhD. degree from University of California San Diego (UCSD). His research interests are in computer architecture and computer security. In particular, He is interested in microarchitectural attacks, high-performance mitigations, and architecture support for security and privacy. His offensive microarchitecture security research has discovered vulnerabilities in Intel Data Directed I/O (DDIO) and Intel/AMD micro-op caches. His research has been selected as an IEEE Micro Top Picks in computer architecture based on novelty and long-term impact and a Top Pick in Hardware and Embedded Security among papers published in the six year period between 2014 and 2019.

Networking Break

4:15p
STEW 214

Closing Keynote

4:30P

STEW 214

Wendy Nather
Head of Advisory CISOs, Cisco

As the cybersecurity ecosystem evolves, we understand more about how interconnected we are: the ripple effects from breaches, the fact that supply chains aren't discrete lines but rather a web, and that mapping our vulnerabilities is harder than we thought. In this session, Wendy Nather will talk about the concept of civic duty on the Internet — not just sporadic charity efforts or "nice to have" information sharing, but the social norms and obligations we should face together if we want a sustainable world of technology. Shared risk requires shared defense.

Wendy Nather leads the Advisory CISO team at Cisco. She was previously the Research Director at the Retail ISAC, and Research Director of the Information Security Practice at 451 Research. Wendy led IT security for the EMEA region of the investment banking division of Swiss Bank Corporation (now UBS), and served as CISO of the Texas Education Agency. She was inducted into the Infosecurity Europe Hall of Fame in 2021. Wendy serves on the advisory board for Sightline Security. She is a Senior Fellow at the Atlantic Council's Cyber Statecraft Initiative, as well as a Senior Cybersecurity Fellow at the Robert Strauss Center for International Security and Law at the University of Texas at Austin.

End of Symposium

5:30p

STEW 214

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. DisGUIDE: Disagreement-Guided Data-Free Model Extraction

Jonathan Rosenthal, Eric Enouen, Hung Viet Pham, Lin Tan

2023_qr_codes.tar.gz

Recent model-extraction attacks on Machine Learning as a Service (MLaaS) systems have moved towards data-free approaches, showing the feasibility of stealing models trained with difficult-to-access data. However, these attacks are ineffective or limited due to the low accuracy of extracted models and the high number of queries to the models under attack. The high query cost makes such techniques infeasible for online MLaaS systems that charge per query. We create a novel approach to get higher accuracy and query efficiency than prior data-free model extraction techniques. Specifically, we introduce a novel generator training scheme that maximizes the disagreement loss between two clone models that attempt to copy the model under attack. This loss, combined with diversity loss and experience replay, enables the generator to produce better instances to train the clone models. Our evaluation on popular datasets CIFAR-10 and CIFAR-100 shows that our approach improves the final model accuracy by up to 3.42% and 18.48% respectively. The average number of queries required to achieve the accuracy of the prior state of the art is reduced by up to 64.95%. We hope this will promote future work on feasible data-free model extraction and defenses against such attacks.

2. Fairness Debugging of Tree-based Models using Machine Unlearning

Tanmay Surve, Dr. Romila Pradhan

Machine learning (ML) is fast becoming the standard choice for data science applications that involve automated decision-making in sensitive domains such as finance, healthcare, crime prevention, and justice management. Designed carefully, ML-based systems have the potential to eliminate the undesirable aspects of human decision-making such as biased judgments. However, concern continues to mount that these systems reinforce systemic biases and discrimination often reflected in their training data. Tree-based machine learning models, such as decision trees and random forests, are one of the most widely used machine learning models primarily because of their predictive power in supervised learning tasks and ease of interpretation. Given their overwhelming success for most tasks, it is of interest to identify root causes of unexpected and discriminatory behavior of tree-based models. However, there has not been much work on understanding and debugging tree-based classifiers in the context of fairness. We introduce an algorithm which identifies the top-k data points or patterns in training dataset that are responsible for model bias. One of the main parts of our algorithm is to utilize the recent advances in machine unlearning research. Using techniques from machine unlearning, our algorithm can find responsible data points or patterns in the training dataset which are responsible for inducing fairness-based bias on the predictions of testing dataset by the model in a time which is much faster than naively retraining the models.

3. Fuzzy Logic to the Rescue: Cracking the Code on Grooming Stages' Fuzziness!

Siva Sahitya Simhadri

Online grooming refers to the practice where an adult builds a relationship with a child or young person with the intention of exploiting them for sexual purposes. The number of internet grooming offenses reported to the police is growing and has increased by more than 80% in the last four years. There are five stages of online grooming via which offenders groom children online. Having a robust approach to detect and intervene in such conversations in the earlier stages is the need of the hour. Grooming chats have always been characterized as crisp sets until now (i.e., each chatline belonging to only one of the 5 stages). The primary objective of this work is to deviate from the conventional method and represent the grooming stages using the fuzzy membership function. We propose a framework to classify predator conversations into different grooming stages. The dataset used for this task was annotated by 2 annotators with over 80% reliability.

4. Impact of Cyber Attacks on Traffic State Estimation for Connected and Autonomous Vehicles (CAVs) Systems

Eunhan Ka

As technology continues to evolve, we will see a growing number of connected and autonomous vehicles (CAVs) on road networks. CAVs can improve traffic operations, revolutionize transportation systems and reduce road accidents. Network traffic flow models have a significant role in enhancing the efficacy of traffic management strategies by estimating traffic states and describing traffic dynamics. Despite having robust theoretical foundations, existing network traffic flow models struggle to model the complex and dynamic real-world traffic data - especially the variance and heterogeneity in large-scale urban networks. The physics-informed deep learning model with a generalized bathtub model (PIDL-GBM) leverages the interpretability of physical models and ML methods for their powerful modeling ability. The input data of PIDL-GBM is crucial to learn the invisible relationship between input and target variables in the training process. However, CAVs systems pose a significant cybersecurity risk. Escape attacks, one of the attacks on machine learning systems are craft input data of machine learning models (e.g., removal, manipulation). This study aims to quantify the impacts of cyber attacks on traffic state estimation with PIDL models. We test the proposed method on mobile location data and a large-scale road network in Indianapolis, United States, with various attacks ratio. The experimental results show that escape attacks significantly deteriorated the performance of the PIDL-GBM model as the attack ratio increased.

5. Impact of Data Quality and Data Preprocessing on ML Model Fairness

Sathvika Kotha, Romila Pradhan

The success of machine learning techniques in widespread applications has taught us that with respect to accuracy, the more data, the better the model. However, for fairness, data quality is perhaps more important than quantity. Existing studies have considered the impact of data preprocessing on the accuracy of ML model tasks. However, the impact of preprocessing on the fairness of the down-stream model has neither been studied nor well understood. In this paper, we conduct a systematic study of how data quality issues and data preprocessing steps impact model fairness. Our study evaluates a number of preprocessing techniques for several machine learning models trained over datasets with different characteristics and evaluated using several fairness metrics.

6. Machine Learning Supply Chain Security

Taylor R. Schorlemmer, Wenxin Jiang, James C. Davis

This poster attempts to summarize some of the key issues in the Machine Learning (ML) supply chain. First, the poster discusses the elements of a traditional software supply chain, demonstrates a software supply chain attack pattern, proposes principles for a secure supply chain, and applies those principles to current security techniques. Next, it shows how an ML supply chain is formed by the reliance on pre-trained models. Finally, it shows potential supply chain threats to model hubs and discusses future work to mitigate risks of attack.

7. Text Data Augmentation: Improving Classification Accuracy at the Expense of Calibration?

Geetanjali Bihani

Text data augmentation (TDA) has been shown to improve generalization in neural NLP pipelines by having a 'regularizing effect'. Training on additional augmented examples provides more space for the model to learn class decision boundaries. Although TDA creates higher data diversity and reduces model overfitting, it remains unclear whether it enhances the model's confidence in correct decisions. To address this gap, we study the impact of TDA-induced 'generalization' on classification decisions and associated confidence levels. We assess the resulting calibration error and focus on two particular subsets of predictions, 1) incorrect but overconfident classifications and 2) correct but underconfident classifications. Our results show that TDA improves accuracy at the cost of model reliability. As we apply more TDA, the model's confidence in all decisions increases, regardless of their correctness. This calls for improved methods of TDA that also account for miscalibration and reduce calibration error in NLP tasks.

8. Trustworthiness Re-use of Pre-trained Neural Networks

Wenxin Jiang, Taylor R. Schorlemmer, James C. Davis

Deep Neural Networks (DNNs) are increasingly being adopted in software systems. Creating and specializing DNNs from scratch has grown increasingly difficult as state-of-the-art architectures grow more complex. Following the path of traditional software engineering, machine learning engineers have begun to reuse large-scale pre-trained models (PTMs) and fine-tune these models for downstream tasks. Prior works have studied reuse practices for traditional software packages to guide software engineers towards better package maintenance and dependency management. We lack a similar foundation of knowledge to guide behaviors in pre-trained model ecosystems. In this work, we present the first empirical investigation of pre-trained model reuse. We interviewed 12 practitioners from the most popular PTM ecosystem, Hugging Face, to learn the practices and challenges of PTM reuse. From this data, we model the decision-making process for PTM reuse. Based on the identified practices, we describe useful (and commonly omitted) attributes for model reuse, including provenance, reproducibility, and portability. We substantiate the identified challenges with systematic measurements of trust and model risks in the Hugging Face ecosystem. Additionally, we publish HFTorrent as an open dataset for Hugging Face models. Our work informs future directions on optimizing deep learning ecosystems by automated measuring useful attributes and potential attacks, and envision future research on infrastructure and standardization for DL model registries.

9. Vaccination Against Backdoor Attack on Federated Learning Systems

Agnideven Palanisamy Sundar, Feng Li, Xukai Zou, Tianchong Gao, Ryan Hosler

Federated Learning (FL) is becoming widely adopted as it improves the model performance of participants with non-voluminous training data. But, existing FL methods are highly susceptible to byzantine and backdoor attacks. Unlike byzantine attacks, which can be detected and prevented with relative ease, the backdoor attacks are far more notorious and manage to infiltrate the participants' local models, affecting a subset of operations. Existing defense mechanisms rely entirely on the trusted third-party server to handle all such attacks. Placing such high trust in a third party's ability to tackle backdoors takes significant control away from the participant. Moreover, if the server fails to catch the backdoor attack or if the server acts maliciously, the attack invades and affects all the participants. In this paper, we propose a vaccination-based technique, which gives the participants stronger control over their models. Irrespective of the central server's ability to prevent a backdoor attack, the participants can tackle such attacks to a significant extent. Our vaccination method is one of the few defense methods that can be executed entirely on the client end with minimal computation overhead and zero communication overhead. Moreover, our method can be combined with existing server-based defense to boost performance. We experimentally show how our simple yet effective vaccination method can efficiently prevent the most commonly applied backdoor attacks while maintaining high main task accuracy.

ASSURED IDENTITY AND PRIVACY

10. Identifying Characteristics of Parental Control Apps

Seungyeon Paik

This study examines the usage of parental control applications to protect children from online dangers and looks into the scope of control they offer and the permissions they request. Concerns regarding children's online safety have grown as their internet use has grown exponentially. Despite the availability of parental control applications, it can be difficult for parents to discover and choose the right apps due to the abundance of available options and the continuously shifting environment of app development. In order to give parents accurate information about their permissions and control features and to assist them in selecting an app, this research analyses Android parental control applications available on Google Play Store.

11. Shuffle-based Private Set Union: Faster and More Secure

Yanxue Jia, Shi-Feng Sun, Hong-Sheng Zhou, Jiajun Du, Dawu Gu

Private Set Union (PSU) allows two players, the sender and the receiver, to compute the union of their input datasets without revealing any more information than the result. While it has found numerous applications in practice, not much research has been carried out so far, especially for large datasets. In this work, we take shuffling technique as a key to design PSU protocols for the first time. By shuffling receiver's set, we put forward the first protocol, denoted as Π_{PSU}^R, that eliminates the expensive operations in previous works, such as additive homomorphic encryption and repeated operations on the receiver's set. It outperforms the state-of-the-art design by Kolesnikov et al. (ASIACRYPT 2019) in both efficiency and security; the unnecessary leakage in Kolesnikov et al.'s design, can be avoided in our design. We further extend our investigation to the application scenarios in which both players may hold unbalanced input datasets. We propose our second protocol Π_{PSU}^S, by shuffling the sender's dataset. This design can be viewed as a dual version of our first protocol, and it is suitable in the cases where the sender's input size is much smaller than the receiver's. Finally, we implement our protocols Π_{PSU}^R and Π_{PSU}^s in C++ on big datasets, and perform a comprehensive evaluation in terms of both scalability and parallelizability. The results demonstrate that our design can obtain a 4-5X improvement over the state-of-the-art by Kolesnikov et al. with a single thread in WAN/LAN settings.

12. User Identity Mapping for Secure Workflows Spanning Cloud and HPC in the Anvil Supercomputer

Sathvika Kotha, Erik Gough, Rajesh Kalyanam

In the Anvil cloud, users are able to deploy container-based applications as any user id (uid), even root. Anvil’s storage systems use NFS and authorize users based on uid and UNIX permissions. A solution is required that validates a user’s ACCESS identity and runs containers as their assigned Anvil uid so data in the storage system can be securely accessed. We provide a mechanism to integrate federated identity management via CILogon and user identity mapping via LDAP into Kubernetes-based Zero-to-Jupyterhub deployments.

END SYSTEM SECURITY

13. Secure Pairing of Energy Harvesting Devices

Rwitam Bandyopadhyay, Satyam Sachan, Muslum Ozgur Ozmen, Habiba Farrukh, Z. Berkay Celik

Context-based pairing allows devices to leverage environmental cues in order to pair the devices that are 'sensing' the same ambient changes. It allows IoT systems to be more autonomous by taking away the need for human-device interaction for pairing by proving that the nodes are co-located. The existing work on context-based device pairing focuses on devices that are always powered on and are thus able to capture all the ambient changes in their environment. We present a system that aims to pair heterogeneous devices as long as they have at least one common sensing modality for devices that may lose power and are thus unable to capture the entire context.

14. Securing Data Privacy of Machine-learning Models on Edge Devices using Trusted Execution Environment

Gowri Ramshankar, Cheng-Yun Yang, Yung-Hsiang Lu

Machine learning models are under high privacy risk when a large amount of sensitive data is used for training. For example, some business organizations apply machine learning models to analyze the preference of customers based on their private information or past purchase records. Membership inference attacks (MIAs) are designed to attack such machine learning models. They take the predictions or gradients as input to determine if a specific data is part of the model's training set. If a machine learning model is not well protected during inference, it will result in a private data leakage under MIAs. Differential privacy and encryption are two common ways to protect model from MIAs. However, differential privacy comes with accuracy drop and encryption significantly increases the computational overhead. For edge devices that only have constrained resources (power, memory, computing), we consider Trusted Execution Environment (TEE) as a better choice to secure data privacy. In order to mitgate the challenges provided by the resource constarined nature of a TEE and the limited models and frameworks that are available to build a neural network on a TEE, we propose a novel approach to split the inference of a model between a General Purpose OS and a TEE. Our hypothesis is that this allows for developers to still build and train their models using popular Python based frameworks like Pytorch and also use the TEE for protecting the data.

15. Securing the Software Package Supply Chain for Critical Systems using Permissioned Blockchains

Akash Ravi

Software systems have grown as an indispensable commodity used across various industries, and almost all essential services depend on them for effective operation. The software is no longer an independent or stand-alone piece of code written by a developer but rather a collection of packages designed by multiple developers across the globe. The secure usage of software modules and add-ons requires a robust and reliable package distribution architecture for developing highly customized software. The number of reported threats and affected packages have been continuously increasing, thereby endangering essential services. This paper augments the existing software package delivery framework with additional checks and balances to identify and report vulnerabilities. This is achieved through the means of implementing a permissioned ledger leveraging Proof of Authority consensus and multi-party signatures. The system aims to prevent attacks while permitting every stakeholder to verify the same. Critical systems can interface with the secure pipeline without disrupting existing functionalities, thus preventing the cascading effect of an attack at any point in the supply chain.

16. WASI-SN: Portable and Secure Low-Footprint WebAssembly Sensor Interface with Networked Access Control

Botong Ou

As the expansion of IoT connectivity continues to provide quality-of-life improvements around the world, they simultaneously introduce increasing privacy and security concerns. The lack of a clear definition in managing shared and protected access to IoT sensors offers channels by which devices can be compromised and sensitive data can be leaked. In recent years, WebAssembly has received considerable attention for its efficient application sandboxing suitable for embedded systems, making it a prime candidate for exploring a secure and portable sensor interface. The project introduces the first WebAssembly System Interface (WASI) extension offering a secure, portable, and low-footprint sandbox enabling multi-tenant access to sensor data across heterogeneous embedded devices

HUMAN CENTRIC SECURITY

17. Digital Literacy and The Perceptions of Online Grooming

Motunrola Afolabi

Recent developments in computer technology have increased the number of internet stalkers, child pornographers, traffickers and sexual predators. In a world where digital literacy is on the rise and people strive to keep up with the latest technology, there is a need to review the impact of digital literacy on the perceptions of grooming of minors perpetrated through CMSG, FSG and LSG. Therefore, this study aims to investigate how digital literacy relates to the perception of online grooming.

18. Examining the Safety of Biometrics

Kat Haggenmueller (haggenk@rose-hulman.edu);
Advisor Dr. Sid Stamm stammsl@rose-hulman.edu

In the digital age, it is important to guarantee the safety of users' personal information and to guarantee that no unauthorized people will get access to private data. For the longest time, this was done by using passwords. However, due to numerous risks accompanying the use of passwords, new authentication methods are constantly being developed and improved upon. The most popular of these alternative methods is biometric authentication. While there seem to be many advantages of biometric authentication over passwords, a big concern is that people are underestimating the risks that biometrics pose. there is reason to believe that several risks come with using biometric authentication, which could lead to devastating consequences if they were taken advantage of. The goal of this thesis is to investigate how safe biometric authentication methods are and whether they are safer than traditional passwords.

19. Fully Transparent, Verifiable, Assurable, and Deployable (Remote) Electronic Voting Enabling Open and Fair Elections

Nathan Swearingen, Xukai Zou, Ninghui Li and Feng Li

In this project, we will investigate "Fully transparent, verifiable, assurable, fair and practical remote electronic voting". The work aims to deliver a ground-breaking remote e-voting system which fills the cap between ballot casting and verification & tallying of voters' plain votes associated with existing voting systems/platforms. Due to the prolonged COVID-19 pandemic, the precinct and voting booth-based voting process in the 2020 US general election caused huge and enduring pain, frustration, and life-threatening consequence, not only before and during the 2020 election season but also after it. Such an unexpected risking-of-life situation once again amplifies the urgency for and the necessity of a voting platform which is practical, secure, robust, and easily accessible and can be employed for casting ballots and tallying and verifying votes remotely by the public with a peaceful and accuracy-assured mind and without risking their lives. The objective of this work is to develop such a practical and resilient E-voting system for voters to vote remotely without the worry or danger of going to a voting booth. The system also allows any voter to verify their individual plain vote, and for anyone to tally and verify the vote counts for every candidate, both visually and technically. The entire ballot-casting process and tallying and verification process, as well as the cast ballots, plain votes, and transition from ballots to votes, are available, transparent, viewable to anyone. The system is resistant to the misbehavior of any participant and to outside attacks. Such resistance, plus the full verifiability and transparency, means any invalid votes and attacks can be detected with high probability.

20. The Model Audio

Sabila Nawshin (Snawshin@iu.edu)

Smart voice assistants can very easily build models tailored towards each individual user with the voice data available to it to elevate the user's experience, and major companies are already considering it. While personalized models would lead to better performance on voice recognition, it comes with the disturbing potential of building personalized speech synthesis models with the voice features extracted by the model. With the smart voice assistants being situated inside a user's house, it can potentially gather voice data of not only the user himself, but also of the friends and family members the user interacts with on a daily basis. This data can be used to subtly manipulate the user in various ways, one of which can be customizing the voice assistant's voice to subtly include voice features of the user himself or the people the user is close to (friends/family members). With Amazon's smart voice assistant Alexa allowing skills generated outside of Amazon being invoked by the assistant, the user can potentially be manipulated by third party companies who may use the opportunity with malicious intents. In our work, we aim to find out how people are affected by synthesized voices personalized towards them by subtly adding voice characteristics of the people familiar to them. As the first step towards that goal, we want to start by personalizing the synthetic voice with voice characteristics of celebrities familiar to people and identify how it affects the believability or trustworthiness of the contents presented. We are working on the initial stages of the project and would welcome feedback from the community.

NETWORK SECURITY

21. Exploring DDoS Mitigation with Client Puzzles

Andrew Walkowski, Theodore Yin, Dr. Mohammad Noureddine (noureddi@rose-hulman.edu)

In this paper, we propose a new defense strategy against volumetric distributed denial-of-service (DDoS) attacks that uses cryptography capabilities. Volumetric DDoS attacks aim to overwhelm a target system with fake traffic, often disrupting services or causing downtime. Volumetric DDoS attacks are getting more common as the cost to run an attacker gets cheaper year by year. Existing defenses like absorption and traffic filtering have significant downsides, such as high costs or blocking normal traffic. Our proposed defense uses client-to-router crypto puzzles. The puzzles provide proof of work for the source of traffic and information about the source to better filter the traffic. In our evaluation, we will simulate our defense versus other strategies to present the benefits. We establish a baseline for normal traffic and the effects of a request flood attack. The simulation data will show the tradeoffs of each strategy in mitigating volumetric DDoS attacks. After analyzing the data collected we concluded that client puzzles deserve to be reintroduced as a tool for network security.

22. Investigating Nation-state Internet Censorship Methods

Alexander Master

Nation-states impose various levels of censorship on their Internet communications. As access to Internet resources has grown among the global population, some governments have demonstrated an increased willingness to filter content, throttle connections, or deny access to Internet resources within their sphere of influence. Researchers, policymakers, and civil liberty advocates need an understanding of the technical means that Internet censors implement. This work presents a research framework that provides a worldwide view of nation-state Internet censorship, derived from Internet measurement data and systematic literature review.

23. Visualization of Network Traffic on Purdue High Performance Computing Resources

MaKayla McCartan, Akash Ravi, Erik Gough

Purdue University is home to several high performance computing (HPC) resources, including campus computing clusters, storage systems and Anvil, a $10M NSF funded supercomputer. These HPC resources are connected to a “Science DMZ” network designed to provide a friction-free path supporting low latency, high-speed data transfer. A Zeek-based intrusion and detection system called PULSAR (Purdue Live Security Analyzer) is used for network monitoring of the Science DMZ. The IDS processes and stores JSON logs at a rate of thousands of events per second. In this work, we use the SIEM to produce visualizations of network traffic on the Science DMZ, showing interesting traffic and attack trends for Purdue's HPC resources.

POLICY, LAW AND MANAGEMENT

24. THE BIG PICTURE: Capture the Flag (CTF) Competitions for Cybersecurity Education and Curriculum

Yansi Keim, Dr. Marcus Rogers

Security competitions are emerging as a new plug-in approach to traditional cybersecurity (CSEC) education. With the gradual introduction of CTFS at universities, the CSEC curriculum now covers popular topics, including Forensics, Reverse Engineering, and Cryptography. Government agencies, national laboratories, and industry partners sponsored CTFs are held around the United States, catering to high school students, college students, and even professionals worldwide. This experiential learning approach has attracted its learners to use it as a preparation mode for cybersecurity work roles stepping into the industry. So, what are some elements to consider when approaching CTFs for CSEC Curriculum?

PREVENTION, DETECTION AND RESPONSE

25. An LMI-based Risk Assessment of Leader-Follower Multi-Agent System under Stealthy Cyberattacks

Sounghwan Hwang, Minhyun Cho, Sungsoo Kim

We present a method for quantifying the potential risk from cyberattacks in multi-agent systems (MASs). Since MASs inherently depend on the communication between agents, the security vulnerabilities of the communication links make MASs more vulnerable to cyberattacks than single-agent systems. Therefore, the impact of cyberattacks could lead to the disruption of performance or the violation of safety. To handle these limitations, we aim to develop a risk assessment method for MASs by applying the reachability analysis which computes the reachable set of the MASs via a Lyapunov function and its corresponding linear matrix inequalities (LMIs). The proposed method can evaluate the potential risk against cyberattacks at the agent and entire system levels by deriving ellipsoidal over-approximated reachable sets. An illustrative example is provided to validate the potency of the proposed method, which shows the risk associated with the formation control of a leader-follower MAS in an environment with scattered obstacles. Finally, we suggest that our risk assessment method can help improve the safety of the MASs in various applications.

26. An Open-Source Mixed-Reality Simulation Environment for Unmanned Aerial Systems (UAS) Cybersecurity

Zhanpeng Yang, Kartik Anand Pant, James Goppert

The wide adoption of Unmanned Aerial Systems (UAS) in civilian and military applications requires rigorous testing and validation of UAS before deployment. However, due to regulations and physical limitations, real-world testing is difficult and expensive. A comprehensive simulation environment is necessary to allow UAS and cybersecurity researchers quickly iterate their designs and algorithms. To this end, we develop an open-source, mixed-reality enabled simulation testbed which combines hardware-in-the-loop (HITL) methods with software-in-the-loop (SITL) methods for verification and validation of UAS systems prior to their deployment. The test-bed uses an integrated mixed-reality approach with high-fidelity sensor emulation, which recreates the complex geometrical effects that occur in dense urban environments. It is packaged as an open-source implementation for easy prototyping and wider use in the UAS community.

27. Compressed Sensing for Enhanced Space Security: Resolving Details of Space Objects

Daigo Kobayashi

The need for space surveillance has been increasing to enhance security against space debris and hostile spacecraft. Optical observations are cost-effective for collecting information about space objects. However, generating fully resolved images of satellites and debris from ground-based observations is challenging due to the vast distance and atmospheric turbulence. We address this issue by adapting the compressed sensing technique to optical measurements. Compressed sensing (CS), an established technique in image compression, can recover a resolved image from a compressed version wherein only a subset of the information from the original image is present. In this study, we developed a new CS-based algorithm to recover resolved images from simulated light curves and point spread functions (PSFs). We explicitly show the effect of uncertainty in the PSF and highlight the robustness of the method. The proposed method applies to objects in low Earth orbit that remain stable during observation.

28. Cyber Attacks on Avionics Networks in Digital Twin Environment: Detection and Defense

Paschal Amusuo, Lekhana Balusu (TA), Brandon Chang, Austin Chou, Adam Frank, Tianyu Gai, Duncan Isbister, Yury A. Kuleshov, Virat Lakkoju, Andrew Li, Grayson Martis, Kabir Nagpal, Ashwin Prasad

The discussion of cyber attack vectors specific to avionics networks is limited within academia. Purdue Data Mine collaborated with the Boeing Company to create a class, which would expand the learning process and outcomes of a traditional computer and/or data science classroom by adding the aviation component as a target for cyber attacks. The students created a digital twin of the three avionics domains, brainstormed possible attack vectors, simulated select attacks, and developed defenses against those attacks. The research demonstrated the potential of synergetic classes for the development of new approaches to the cyber security problems in aviation.

29. Cyber Forensics Investigation of Web3 Wallets

Akif Ozer, Mohammad Meraj Mirza, and Umit Karabiyik

The continuous progression of technology has a substantial impact on our daily lives and the environment we inhabit. The growing popularity of blockchain-based cryptocurrencies such as Bitcoin and Ethereum, as well as Non-Fungible Tokens (NFTs), has enabled their integration into a diverse range of applications. Cryptocurrencies have become a widely used method of online payment, but they are also gaining popularity on the dark web where their anonymity can be exploited for illegal activities. Despite the increasing number of cryptocurrency wallets and related applications available today for various platforms including the leading mobile operating systems such as iOS and Android, the digital forensic investigation of Web3 cryptocurrency wallets has not been as comprehensive as other types of applications. Therefore, this study aims to aid investigators in realizing the full potential of the popular cryptocurrency wallets, Trust Wallet and Metamask, to determine what can be recovered and identify areas where further knowledge is required. Two Web3 cryptocurrency wallets that are widely used on Android and iOS devices and do not require any personal identifiers to register were analyzed and examined using digital forensic techniques. The digital evidence collected is reviewed, and the implications of the forensic tools used are discussed. Lastly, a proof of concept extension is proposed for the iOS Logs, Events, And Plists Parser (iLEAPP) tool to automate the recovery of artifacts.

30. Cyber Resilience Adaptive Virtual Reality Experiences (CRAVRE)

Dr. Mesut Akdere, Dr. Umit Karabiyik, Dr. Jason Moats, Dr. Jin Kocsis, Miloš Stanković, Flavio Lobo, Mututhanthrige Fernando, Elizabeth Marie Rakes

Cyber Resilience Adaptive Virtual Reality Experiences (CRAVRE) As the IoT technologies continue to permeate communities of all sizes, the nation's cyber and cyber-physical assets are vulnerable in proportion to the increase in connectedness. Critical infrastructures, including the national power grid, health care systems, transportation systems, are highly vulnerable to cyberattacks[1,2]. So are the technologies that make cities SMART. As one author stated, "…the Internet of Things (IoT), the technology underpinning these complex and interconnected urban networks, offers a considerably expanded attack surface for cyber adversaries of all kind…"[3]. Perhaps the greatest source of vulnerability is with the workers. Researchers agree that the human factor plays a crucial role in preventing and limiting the impact of a cyber incident, even when the security of other categories is satisfied. Recent reports from various cybersecurity and data analysis firms[4,5] clearly show that human error causes up to 90% of the data breaches for corporations. Despite this, more than 40% of employees do not get regular cybersecurity training[6]. This lack of training and the result inadequate awareness of the connectedness is an individual gap that we aim to lessen. Even more startling, cybersecurity experts agree that there has been an exponential increase in cybercrime during the ongoing COVID-19 crisis. While, government agencies and the private sector have implemented available security frameworks[7,8], an organizational gap exists as many state, local, and critical private sector organizations continue to face deficiencies in their ability to prevent cyberattacks on their IoT technologies. The U.S. Government Accountability Office highlighted that information security is the nation's one of the top challenges that are persistent and posing a high risk to the government as a whole[9], and has made over 3,000 recommendations for agencies to address cybersecurity issues. However, as of 2018, nearly 1,000 of the recommendations were not implemented, leaving agencies vulnerable to cyber threats. Novel training methods for cyber protection and response is highly needed. Simply put, the current methods of training all stakeholder on cybersecurity are inadequate given the magnitude and complexity of cyber domain, especially during times of disaster. Despite these efforts, training incident managers, elected officials, and emergency managers to be effective decision makers in the face of hostile cyberattacks initiated following natural or manmade disasters still remains as a significant gap. Furthermore, these stakeholders must currently perform a risk assessment and implement proactive measures before any disaster occurs[10]. They must also attend available training for such preparedness which is delivered in traditional classroom-style courses (web-based or instructor-led). We propose a ground-breaking paradigm by developing and distributing an adaptive, immersive learning environment that distributed through web-based, mobile, and, virtual reality (VR) platforms, providing multiple access options to learners. Through this approach, both participants and organizations do not need to invest extensive time in physical exercise during work hours because they can participate in training whenever and where they desire. Second, participants will receive immediate feedback when they fail or succeed during the training which results in reinforced learning, higher level cognition, and increased learning retention. Third, this approach is resilient making by providing the learning experiences before a natural disaster which will ultimately reduce the strain on the federal government later on after being affected by a natural disaster, which is well aligned with the FEMA mission to lead America to prepare for, prevent, respond to and recover from disasters with a vision of "A Nation Prepared". "This material is based upon work supported by the U.S. Department of Homeland Security under Grant EMW-2020-CA-00061-S01." 1- L. Stanaland, R. Baldick, A. A. Cardenas, and J. Holmes, "Protecting the Texas Electric Grid: A Cybersecurity Strategy for ERCOT and the PUCT," in 2019 Resilience Week (RWS), Nov. 2019, vol. 1, pp. 219–225, doi: 10.1109/RWS47064.2019.8972002. 2- H. I. Kure and S. Islam, "Assets focus risk management framework for critical infrastructure cybersecurity risk management," IET Cyber-Phys. Syst. Theory Appl., vol. 4, no. 4, pp. 332–340, 2019, doi: 10.1049/iet-cps.2018.5079. 3-

Digital14, “Digital14 Report: Smart Cities Unlock Business Potential but Are Increasingly Vulnerable.” https://www.prnewswire.com/ae/news-releases/digital14-report-smart-cities-unlock-business-potential-but-are-increasingly-vulnerable-818572518.html (accessed Jul. 09, 2020). 4- M. Hill, “90% of UK Data Breaches Due to Human Error in 2019,” Infosecurity Magazine, Feb. 06, 2020. https://www.infosecurity-magazine.com:443/news/90-data-breaches-human-error/ (accessed Jul. 01, 2020). 5- A. S. May 08 and 2019, “90 percent of data breaches are caused by human error,” TechRadar. https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error (accessed Jul. 01, 2020). 6- M. G. I. T. Trends 1, “43% of Employees Lack Regular Cyber Security Training,” Small Business Trends, Oct. 10, 2019. https://smallbiztrends.com/2019/10/employee-vulnerabilities-cybersecurity.html (accessed Jul. 09, 2020). 7- M. P. Barrett, “Framework for Improving Critical Infrastructure Cybersecurity Version 1.1,” Apr. 2018, Accessed: Jul. 01, 2020. [Online]. Available: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11. 8- nicole.keller@nist.gov, “Cybersecurity Framework,” NIST, Nov. 12, 2013. https://www.nist.gov/cyberframework (accessed Jul. 01, 2020). 9- U. S. G. A. Office, “High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation,” no. GAO-18-622, Sep. 2018, Accessed: Jun. 30, 2020. [Online]. Available: https://www.gao.gov/products/GAO-18-622. 10- “How cybercriminals prey on victims of natural disasters,” Journal of Accountancy, Sep. 14, 2018. https://www.journalofaccountancy.com/news/2018/sep/cyber-criminals-prey-on-natural-disaster-victims-201819720.html (accessed Jul. 02, 2020).

31. eBPF-based APM and Observability for Cloud-native Infrastructure

Bhavye Sharma

Extended Berkeley Packet Filter (eBPF) is a powerful and versatile technology that allows developers and system administrators to trace, monitor, and debug the behavior of applications running on Linux-based systems. eBPF is particularly useful for cloud-native observability, as it enables the collection of fine-grained metrics and insights into the performance and behavior of microservices, containers, and other cloud-native infrastructure components. We built an open-source eBPF-based observability pipeline that enables sophisticated troubleshooting and debugging workflows, allowing developers to identify and resolve issues in complex, dynamic environments quickly. Using this pipeline of labeled data, we propose an AI model that can classify anomalous behavior of our applications.

32. Optimal Safety-Critical Control of Viruses

Brooks A. Butler and Philip E. Paré

We present a generalized model for spreading processes that partitions control into changes in linear and non-linear flow rates between compartments, respectively. We then define an optimal control problem that minimizes the weighted cost of rate control on the generalized model while maintaining conditions that guarantee system safety using control barrier functions. Using this formulation, we prove that under homogeneous penalties the optimal controller will always favor increasing the linear flow out of an infectious process over reducing nonlinear flow in. Further, in the case of heterogeneous penalties, we provide necessary and sufficient conditions under which the optimal controller will set control of non-linear rates (i.e., the reduction of flow rate into the infection process) to zero. We then illustrate these results through the simulation of a bi-virus SEIQRS model.

33. Order but Not Execute in Order

Tiantian Gong, Aniket Kate

We explore combining batch order-fair atomic broadcast (of-ABC) and frequent batch auction (FBA) as a defense against general order manipulations in blockchain-based decentralized exchanges (DEX). To justify FBA, we compare the welfare loss of decentralized exchanges under two market designs: continuous limit order book (CLOB), where transactions are processed sequentially, and FBA, where transactions are arranged into batches and a uniform price double auction decides execution order. We model three types of players, common investors, privately informed traders, and arbitrageurs who can provide liquidity and front-run, along with a decentralized exchange. Assuming that the exchange is realized over an of-ABC protocol, we find that FBA can achieve better social welfare compared to CLOB when (1) public information affecting the fundamental value of an asset is revealed more frequently, or (2) the block generation interval is sufficiently large, or (3) the priority fees are small compared to the asset price changes, or (4) fewer privately informed parties exist. Intrinsic reasons are that first, blockchains already treat time as discrete and ensuring order fairness there is non-trivial, allowing even more room for latency arbitrage rents under CLOB; second, sufficiently large block creation interval allows for information dispersion; third, higher priority fees discourage front-running under CLOB; additionally, FBA prioritizes price in deciding execution order and fewer informed traders mean less adverse price impact.

34. Reverse Execution with Persistent Data Structures

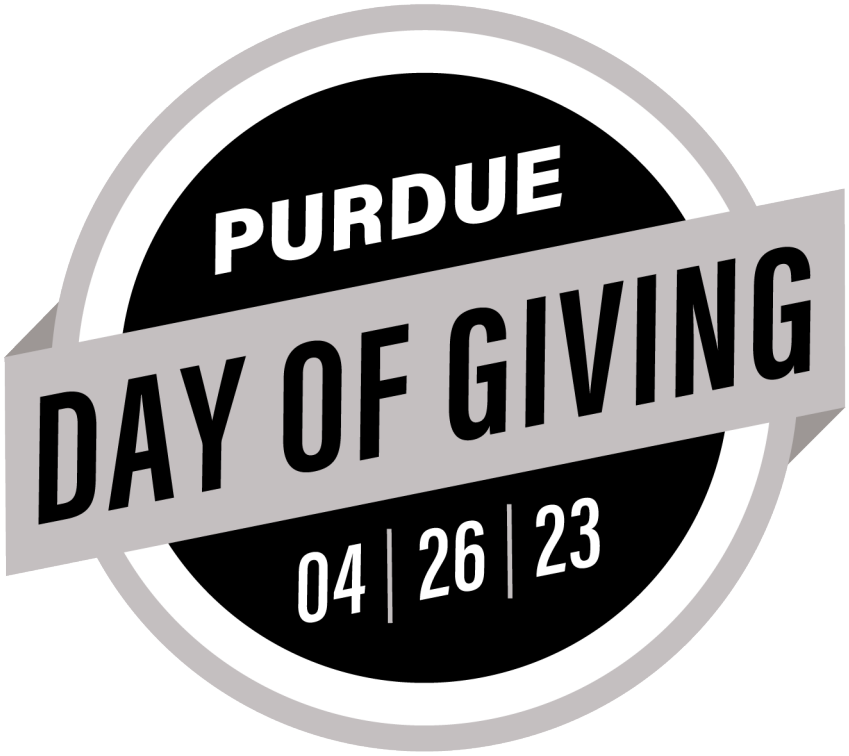
Omar Roth (rotho@rose-hulman.edu)

Reversible debuggers are useful tools for developing and deploying modern applications. However, due to their high memory requirements and runtime overhead, their functionality is generally reserved for rare cases (e.g., identifying short-term memory corruption). This paper describes an alternative approach for implementing a low-overhead memory snapshotting mechanism using fully persistent data structures. Memory usage and performance analyses will be presented and compared against alternative implementations.

35. Robust State Estimation in Multi-Agent Systems using Pairwise Measurements

Shiraz Khan

Multi-Agent Systems (MAS) such as fleets of autonomous vehicles have a wide range of applications, ranging from search-and-rescue operations to commercial package delivery. They use a combination of onboard sensors and communications to fulfill their tasks in a safe and coordinated manner. Consequently, adversaries seeking to compromise the performance or safety of the MAS and/or the surrounding human infrastructure can do so using cyberattacks injected through these sensing and communication channels. In this project, we look at various techniques to reinforce the cybersecurity of an MAS by exploiting the pairwise measurements between agents, for e.g., cameras pointed from one agent to another. Special emphasis is placed on fast, scalable algorithms which are suitable for large-scale MAS applications.



April 26 is #PurdueDayofGiving!

Support @CERIAS by donating during the hourly challenges & check out our page:

https://dayofgiving.purdue.edu/

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 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) 494-7841 or by visiting www.cerias.purdue.edu.

CERIAS has Moved to the Discovery Park District!

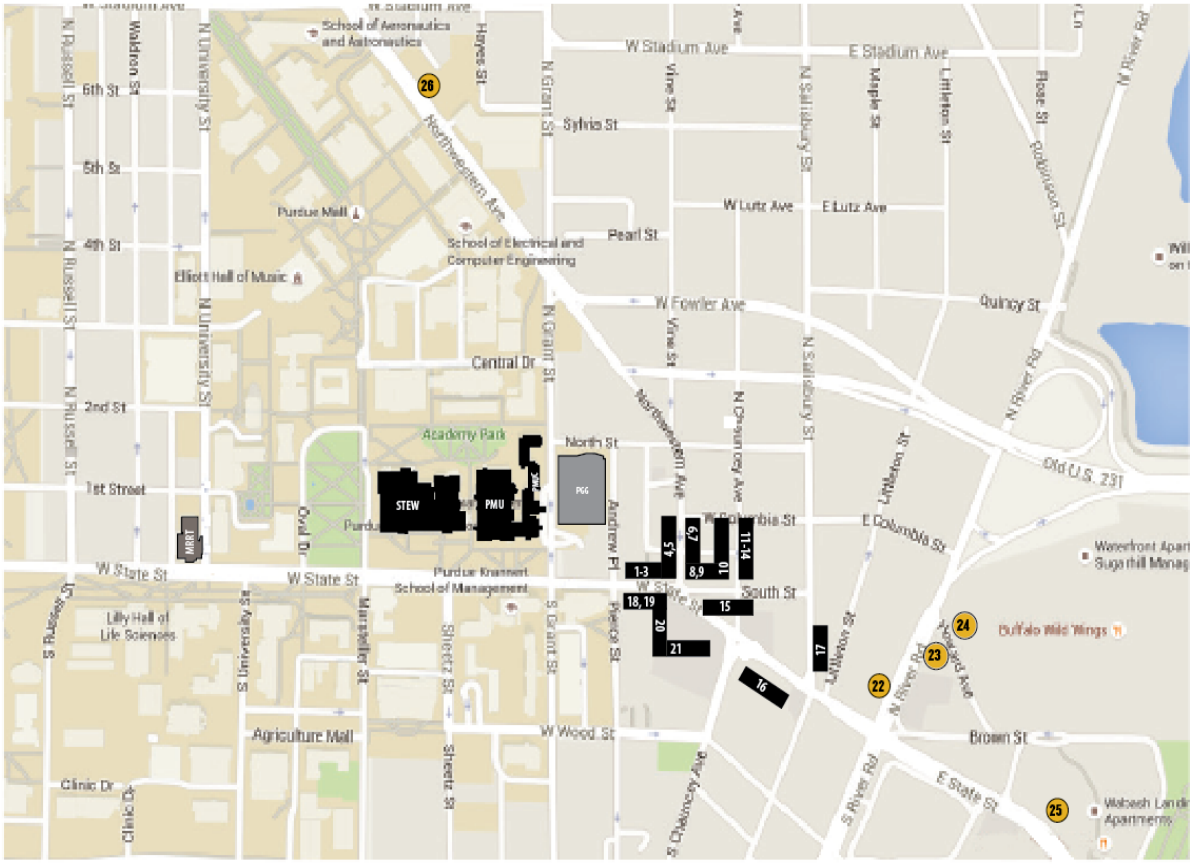
The *CERIAS Galactic Headquarters* has moved across campus to the Convergence Center for Innovation and Collaboration (CONV). Come visit us!

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

Stewart Center Wireless Information

For Purdue Students, Staff and Faculty:

- Use any of the following SSIDs: 'PAL3.0' or 'eduroam'.
- Login with your Purdue career account credentials.

For Visitors:

- Connect to the 'attwifi' SSID
- Open your web browser (Firefox, Chrome, IE, etc.)
- Click on the **"Get Connected"** button.