THE 2018 ANNUAL CERIAS INFORMATION SECURITY SYMPOSIUM

Tuesday, April 3

AGENDA

PURDUE UNIVERSITY Discovery Park

8:15am	**Registration / Coffee**	STEW 302
8:45	**Opening Comments -** Joel Rasmus, CERIAS Managing Director	STEW 302
9:00	**Welcome -** Dr. Tomás Díaz de la Rubia, Chief Scientist and Executive Director of Discovery Park	STEW 302
9:30	**Keynote -** "The Cloud, IOT and Critical Infrastructure: It's Not Too Late for 'The Cyber" - Mark Weatherford - Sr. Vice President & Chief Cybersecurity Strategist at vArmour	STEW 302
10:30	**Break**	STEW 302
10:45	**Fireside Chat** - "Where We've Been – The Spirit of Cybersecurity Past" Moderator - Eugene Spafford, CERIAS Executive Director Emeritus	STEW 302
11:45	**Lunch**	FORD
1:15pm	**CERIAS Tech Talk -** "Human Biases Meet Cybersecurity of Embedded and Networked Systems" Prof. Saurabh Bagchi and Prof. Shreyas Sundaram	STEW 302
1:45	**CERIAS Tech Talk** - "Developing a Public/Private Cybersecurity Scorecard for the State of Indiana" Prof. Eric Dietz and Jim Lerums	STEW 302
2:15	**Featured Speaker -** Michelle Dennedy - Vice President & Chief Privacy Officer, Cisco	STEW 302
2:30	**Fireside Chat -** "The On-Going Tensions Between Security and Privacy" Moderator - Michelle Dennedy	STEW 302
3:30	**Break**	STEW 302
3:45	**Poster Session Preview -** "Speed Dating Technology"	STEW 302
5:00	**Break for Dinner**	STEW 302
6:30	**CERIAS 20th Anniversary Reception and CERIAS Poster Session**	PMU Ballroom
7:00	**CERIAS Remarks** - Professor Gene Spafford	PMU Ballroom
8:30	**End of Day 1**	

Wednesday, April 4

8:30am	**Registration / Coffee**	STEW 302
9:00	**Welcome and CERIAS Awards -** Jerry Haan, CERIAS Manager of Corporate Relations, Dongyan Xu, Interim Director of CERIAS & Professor of Computer Sciences	STEW 302
9:30	**Keynote:** "Managing Risks in the Cyber Battle Space" - Mark Spangler - Director, Cyber Security Operations Center, National Reconnaissance Office	STEW 302
10:30	**Mark Loepker -** "Cyber Center for Education and Innovation, Home of the National Cryptologic Museum – a National collaboration in K-20 cyber education"	STEW 302
10:45	**Break**	STEW 302
11:00	**Fireside Chat -** "The State of Cybersecurity Education – Can Our Educational System Produce the Quantity and Quality of Graduates Needed to Meet Labor Demand?" Moderator - Melissa Dark, W.C. Furnas Professor, Purdue Polytechnic Institute	STEW 302
12:00pm	**Lunch**	FORD
1:30	**CERIAS Program Talk Indiana Cybersecurity Initiatives -** Chetrice Mosley & Doug Rapp	STEW 302
2:00	**CERIAS Tech Talk:** "Blockchains: A Technical Perspective on the Future of Decentralization" Aniket Kate, Assistant Professor of Computer Sciences, Purdue University	STEW 302
2:30	**CERIAS Tech Talk:** "Online Adversarial Learning of Nuclear Reactor Dynamical State" Hany Abdel-Khalik, Associate Professor of Nuclear Engineering, Purdue University	STEW 302
3:00	**Break**	STEW 302
3:15	**Fireside Chat -** "What's Ahead – The Spirit of Cybersecurity Yet to Come" Moderator - Eugene Spafford	STEW 302
4:30	**Closing Keynote** - "Bits & Bytes, Flesh & Blood, and Adapting for the Next 20 Years" Josh Corman Chief Security Officer, SVP at PTC	STEW 302
5:30	**End of Symposium**	

Thursday, April 5

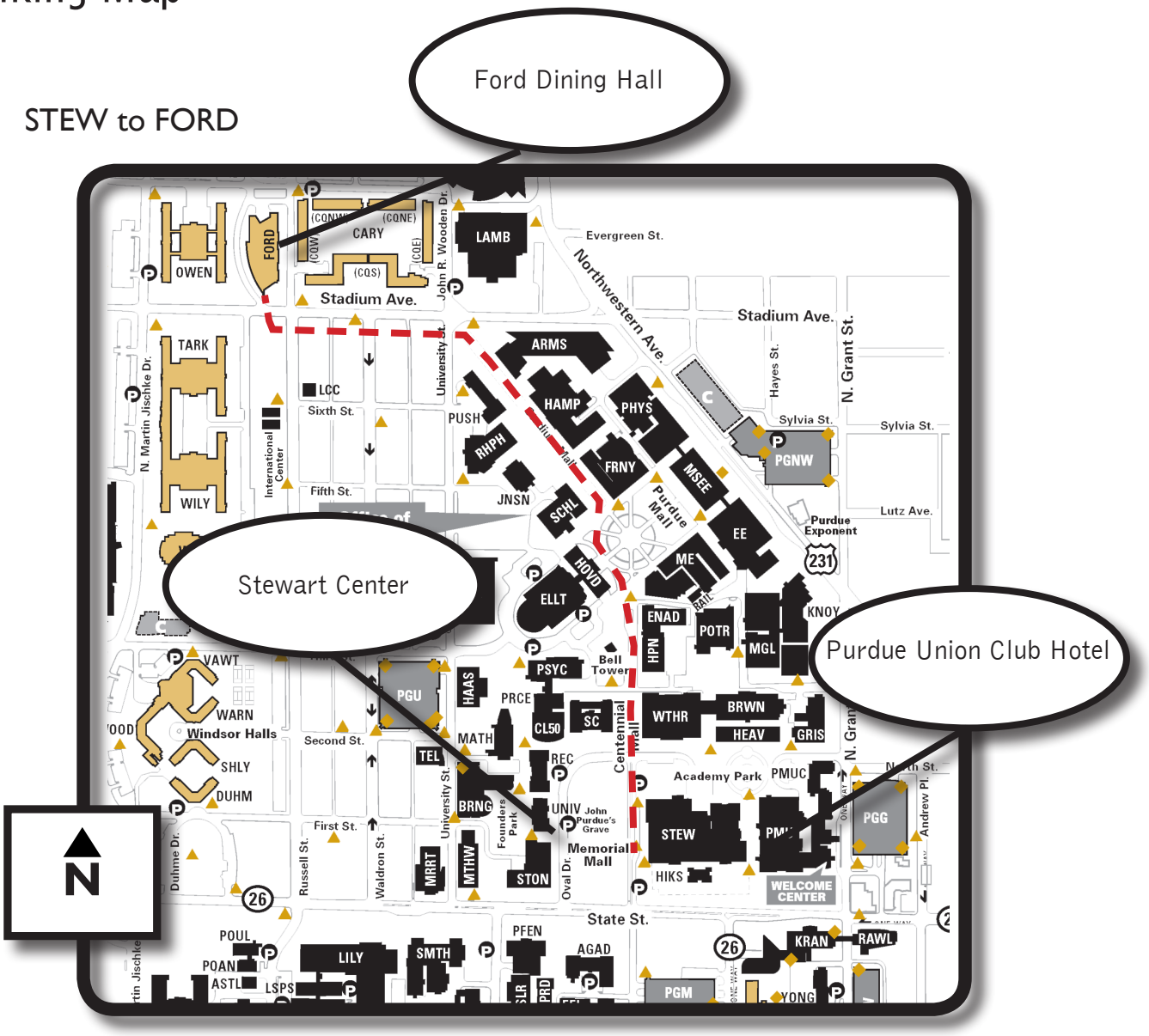
9:00a-5:00p	**CERIAS External Advisory Board Meeting** (For CERIAS Membership Delegates Only)	RAWLS 4013

Save the Date!...Our next Symposium will be on April 9 & 10, 2019!

www.cerias.purdue.edu/symposium

Walking Map

STEW to FORD



Transportation will also be available between Stewart Center and Ford Dining Court. Stewart pick-up is located at the west entrance of Stewart.

CERIAS 2018

19th Annual Information Security Symposium * April 3-4

Table of Contents

#CERIAS

Thanks to Our Strategic Partners

Analog Devices
Benedor TSE
Boeing
Caterpillar
Cyber Leadership Alliance
Citi
Deloitte
Eli Lilly and Company
General Motors
Intel
Lockheed Martin
Northrop Grumman
Raytheon
Rook Security
Sandia National Laboratories
SRC
Tenable Network Security
Vencore Labs

Strategic Government Supporters

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

Speaker & Panelist Bios

Welcome (Day 1)

9:00a

Dr. Tomás Díaz de la Rubia
Chief Scientist and Executive Director of Discovery Park
Purdue University

Tomás Díaz de la Rubia is Purdue University's chief scientist and executive director of Discovery Park. In this position, his responsibilities include building upon Discovery Park's foundation of excellence which has enabled high-impact research that crosses traditional academic boundaries. He works closely with the faculty and deans to help catalyze Purdue's many strengths and build on its legacy of interdisciplinary research with global impact. He is also a professor of Materials Science, and of Strategic Management (by Courtesy) in the Krannert School of Management.

Keynote (Day 1)

9:30a

"The Cloud, IOT and Critical Infrastructure: It's Not Too Late for 'The Cyber'"

Mark Weatherford
Sr. Vice President & Chief Cybersecurity Strategist
vArmour

Mark Weatherford is Senior Vice President and Chief Cybersecurity Strategist at vArmour. He has more than 20 years of security operations leadership and executive-level policy experience in some of the largest and most critical public and private sector organizations in the world. At vArmour, Mark focuses on helping customers understand the rapidly evolving cybersecurity needs of the cloud and 21st century data center technologies.

Prior to joining vArmour, he was a Principal at The Chertoff Group where he worked with businesses and organizations around the world create strategic security programs and he remains a Senior Advisor in the firm. In 2011, Mr. Weatherford was appointed by President Obama as the Department of Homeland Security's first Deputy Under Secretary for Cybersecurity and before DHS, he was the Vice President and Chief Security Officer at the North American Electric Reliability Corporation (NERC) where he directed the cybersecurity and critical infrastructure protection program and worked with electric utility companies across North America. Prior to NERsC, Mr. Weatherford was appointed by Governor Arnold Schwarzenegger to serve as California's first Chief Information Security Officer and was also the first Chief Information Security Officer for the State of Colorado, where he was appointed by two successive governors. As a former U.S. Navy Cryptologic Officer, Mr. Weatherford led the United States Navy's Computer Network Defense operations and the Naval Computer Incident Response Team (NAVCIRT).

Mr. Weatherford serves on the Board of Directors of the Center for Cyber and Homeland Security at the George Washington University, the Board of Directors at the National Cybersecurity Center, is an Affiliate at the Stanford University Center for International Security and Cooperation (CISAC), an affiliate faculty member at the Desert Research Institute, and is a Distinguished Fellow at the Poneman Institute. He is a Senior Advisor to the Chertoff Group and on the Executive Advisory Boards at AlertEnterprise, BitGlass, Boldend, Chevron, Coalfire, Cylance, and Indegy. He is also on an Advisory Board for Cyber-Enabled Economic Warfare at the Foundation for Defense of Democracies.

Mr. Weatherford earned a bachelor's degree from the University of Arizona, a master's degree from the Naval Postgraduate School and holds the Certified Information Systems Security Professional (CISSP) certification. He was awarded SC Magazine's "CSO of the Year" award in 2010, named one of the "10 Most Influential People in Government Information Security" by GovInfoSecurity in both 2012 and 2013, selected for the 2013 CSO Compass Award for leadership achievements in the security community, and was recently selected as a 2017 SC Media Reboot Leadership Award "Influencer."

Fireside Chat

"Where We've Been – The Spirit of Cybersecurity Past" 10:45a

Eugene Spafford (Moderator)
Executive Director Emeritus, CERIAS &
Professor of Computer Sciences
Purdue University

Dr. Eugene Spafford is a professor with an appointment in Computer Science at Purdue University, where he has served on the faculty since 1987. He is also a professor of Philosophy (courtesy), a professor of Communication (courtesy), a professor of Electrical and Computer Engineering (courtesy) and a Professor of Political Science (courtesy). He serves on a number of advisory and editorial boards. Spafford's current research interests are primarily in the areas of information security, computer crime investigation and information ethics. He is generally recognized as one of the senior leaders in the field of computing.v

David E. Bell
Author and Computer Security Pioneer

David Elliott Bell, Ph. D., is the co-author of the widely-known Bell-La Padula security model." His work in security has been varied, from the conceptual security of his modeling work to security architectures, operating system security, database management security, network security, formal verification, public-key technology, and standards and guidelines for security practice.

In addition to security, he has also contributed in systems design and implementation, acquisition, integration, and, not least, in passing his insight along through formal and informal training and education. He has been a guest lecturer at the U.S. Military Academy at West Point and the U.S. Naval Academy at Annapolis.

Carter Bullard
President & Chief Technology Officer
QoSient, LLC

Carter Bullard is a pioneer and industry expert, holding both academic and industry positions researching computer network security. Carter established in the early 1990's, research programs in network vulnerability analysis and assessment at Carnegie Mellon's CERT, where he pioneered and developed the concepts of network flow based forensics, and situational awareness. Carter helped develop and standardize the complete security architecture for ATM networking while a principal at FORE Systems and Nortel Networks, and most recently has been conducting security research in the areas of high performance virtual networking, forensics, optimization, awareness, and protection, at the U.S. DoD. Carter has authored over 20 contributions to the IETF, ITU, and the ATM Forum in the areas of network security, has consulted to U.S. Federal and State agencies regarding large scale network surveillance, mitigation, attribution and protection.

Dickie George
Senior Advisor for Cyber Security
The Johns Hopkins University
Applied Physics Lab

Richard M. (Dickie) George is the Senior Advisor for Cyber Security at the Johns Hopkins University Applied Physics Lab. At the Lab, he works on a number of projects sponsored by the US Government and provides oversight on additional efforts. Prior to joining APL, he worked at the National Security Agency as a mathematician from 1970 until his retirement in 2011. While at NSA, he wrote more than 125 peer-reviewed technical papers on cryptomathematical subjects, ranging from new mathematical methods for attacking cryptographic algorithms, to security evaluations of complex systems. While at NSA, his work was recognized by the Cryptomath Institute as the most important mathematical contribution to the Agency's mission in 1980, by 2 Presidential Rank awards, a Superior Technical Award, a Distinguished Senior Technical Achievement Award, and he was elected to Distinguished Member status into both the Kryptos (Cryptanalytic Society) and the CMI (Cryptomath Society). He served as the Technical Director of the Information Assurance Directorate for eight years until his retirement.

William Malik
Vice President, Infrastructure Strategies
Trend Micro

Bill Malik's information technology career spans over four decades. Before joining Trend Micro, he was CTO of Waveset, an Identity Management vendor, from 2002 through its acquisition by Sun. Bill worked at Gartner for twelve years where he led the Information Security service and the Application Integration and Middleware service. He was a co-author of the Cobit version 3 standard. During his 12-year career at IBM he worked in MVS development, testing, and business planning. He studied Mathematics at MIT.

CERIAS Tech Talk: "Human Biases Meet Cybersecurity of Embedded and Networked Systems" 1:15p

Saurabh Bagchi
Professor, Electrical & Computer Engineering & Computer Science
Purdue University

Saurabh Bagchi is a Professor in the School of Electrical and Computer Engineering and the Department of Computer Science (by courtesy) at Purdue University in West Lafayette, Indiana. He is the founding Director of a university-wide resilience center at Purdue called CRISP (2017-present). He serves on the Steering Committee of the premier conference in the field of dependability, DSN. He is an ACM Distinguished Scientist (2013), a Senior Member of IEEE (2007) and of ACM (2009), and a Distinguished Speaker for ACM (2012). He is the recipient of an IBM Faculty Award (2014), a Google Faculty Award (2015), and the AT&T Labs VURI Award (2016). He was elected to the IEEE Computer Society Board of Governors for the 2017-19 term. Saurabh's research interests are in distributed systems and dependable computing. He is proudest of the 20 PhD students who have graduated from his research group and are in various stages of building wonderful careers in industry or academia. In his group, he and his students have far too much fun building and breaking real systems. Saurabh received his MS and PhD degrees from the University of Illinois, Urbana-Champaign and his BS degree from the Indian Institute of Technology Kharagpur, all in Computer Science.

Shreyas Sundaram
Assistant Professor, Electrical & Computer Engineering
Purdue University

Shreyas Sundaram is an Assistant Professor in the School of Electrical and Computer Engineering at Purdue University. He received his MS and PhD degrees in Electrical Engineering from the University of Illinois at Urbana-Champaign in 2005 and 2009, respectively. He was a Postdoctoral Researcher at the University of Pennsylvania from 2009 to 2010, and an Assistant Professor in the Department of Electrical and Computer Engineering at the University of Waterloo from 2010 to 2014. He received the National Science Foundation CAREER award in 2017, and the Air Force Research Lab Summer Faculty Fellowship in 2016. At Purdue, he received the Wilfred "Duke" Hesselberth Award for Teaching Excellence in 2017, and the Ruth and Joel Spira Outstanding Teacher Award in 2016. At Waterloo, he received the Department of Electrical and Computer Engineering Research Award in 2014, and the Faculty of Engineering Distinguished Performance Award in 2012. He received the M. E. Van Valkenburg Graduate Research Award and the Robert T. Chien Memorial Award from the University of Illinois, and he was a finalist for the Best Student Paper Award at the 2007 and 2008 American Control Conferences. His research interests include network science, analysis of large-scale dynamical systems, game-theory, and fault-tolerant and secure control.

CERIAS Tech Talk: "Developing a Public/Private Cybersecurity Scorecard for the State of Indiana" 1:45p

Eric Dietz
Professor
Purdue Polytechnic Institute

Dr. Dietz's research interests include optimization of emergency response, homeland security and defense, energy security, and engaging veterans in higher education. As a Director in Purdue's Discovery Park, Dr. Dietz is responsible for the catalysis of the Purdue's homeland security research, increasing the impact of Purdue research on society, and organizing interdisciplinary projects within the university. Prior to his current responsibilities, Eric was on loan from Purdue to Governor Mitch Daniels to serve as the founding Executive Director for The Indiana Department of Homeland Security, a new state agency of over 300 people responsible for emergency planning, training, fire and building safety, and disaster response for 6.2 million Indiana residents. During this period, Eric led Indiana's response to 7 Presidential Major Disasters and Emergency Declarations which included restoration and recovery of critical infrastructure. Eric also led the creation of the Indiana Intelligence Fusion Center and the Indiana Fire Training System both new government functions that were created with new laws and funding. Retiring as a Lieutenant Colonel from the U.S. Army in 2004, Dr. Dietz led a number of Army Acquisition and research programs throughout his career including power systems, chemical sensors and command and control systems. An Indiana native, Eric was graduated in 1984 from Rose-Hulman Institute of Technology after earning a bachelor of science in chemical engineering. He also earned a master's of science from Rose-Hulman Institute of Technology in 1986 and a PhD in chemical engineering in 1994 from Purdue University.

Jim Lerums
PhD Candidate, CERIAS
Purdue University

Jim Lerums is a MS, and Ph.D. Candidate in Interdisciplinary Information Security, and Colonel, USA (Retired).

Featured Speaker

2:15p

Michelle Dennedy
VP and Chief Privacy Officer at Cisco

Michelle Finneran Dennedy currently serves as VP and Chief Privacy Officer at Cisco. She is responsible for the development and implementation of the organization's data privacy policies and practices, working across business groups to drive data privacy excellence across the security continuum. Before joining the Cisco, Michelle founded The iDennedy Project, a public service organization to address privacy needs in sensitive populations, such as children and the elderly, and emerging technology paradigms. Michelle is also a founder and editor in chief of a new media site—TheIdentityProject.com—that was started as an advocacy and education site, currently focused on the growing crime of Child ID theft. She is the author of The Privacy Engineer's Manifesto.

Fireside Chat

2:30p

"The On-Going Tensions Between Security and Privacy"

Michelle Dennedy (Moderator)

Sam Curry
Chief Security Officer
Cybereason

Sam Curry is CSO at Cybereason and has over 25 years of IT security industry experience. Curry served as CTO and CSO at Arbor Networks, where he was responsible for the development and implementation of Arbor's technology, security and innovation roadmap. Previously, he spent more than seven years at RSA (the Security Division of EMC) in a variety of senior management positions, including CSO and Chief Technology in addition to SVP of Product Management and Product Marketing, including RSA Labs. Curry has also held senior roles at Microstrategy, CA and McAfee. He has founded two successful companies and holds 24 patents. Curry is on the board of Sequitur Labs in the Embedded Security space and of the Coalition for Cybersecurity Policy and Law in Washington, DC.

Chris Clifton
Professor, Computer Sciences
Purdue University

Dr. Clifton is a Professor of Computer Science at Purdue University. He works on data privacy, particularly with respect to analysis of private data. From 2013-2015, Dr. Clifton served as a program director at the National Science Foundation. Prior to joining Purdue in 2001, he was a principal scientist in the Information Technology Division at the MITRE Corporation. Before joining MITRE in 1995, he was an assistant professor of computer science at Northwestern University.

Amy Hess
Special Agent in Charge
Federal Bureau of Investigation

Amy S. Hess began her career as a Special Agent with the FBI in January 1991. She has served in the Kansas City, Louisville, Phoenix, and Memphis field offices, in addition to a deployment overseeing the FBI's counterterrorism operations in Afghanistan. Her assignments at FBI Headquarters have included the Inspection Division, International Operations Division, and National Security Branch, as well as the Operational Technology Division in Quantico, Virginia. In 2014, Ms. Hess was promoted to the position of Executive Assistant Director over the FBI's Science and Technology Branch, composed of the Operational Technology, Laboratory, and Criminal Justice Information Services Divisions. In 2016, she was appointed to serve as the Special Agent in Charge of the Louisville field office, with responsibility for all FBI personnel and operations in the Commonwealth of Kentucky. A native of Jeffersonville, Indiana, Ms. Hess holds a degree in Aeronautical / Astronautical Engineering from Purdue University.

Stephen Reynolds
Attorney
Ice Miller

Stephen Reynolds is a partner in Ice Miller's Litigation and Intellectual Property Group, and co-chairs the firm's Data Security and Privacy Practice. A former computer programmer and IT analyst, Stephen concentrates his legal practice on commercial litigation and data security and privacy law. Stephen is a Certified Information Systems Security Professional (CISSP), and a Certified Information Privacy Professional (CIPP/U.S.).

Break

3:30p

Poster Session Preview

3:45p

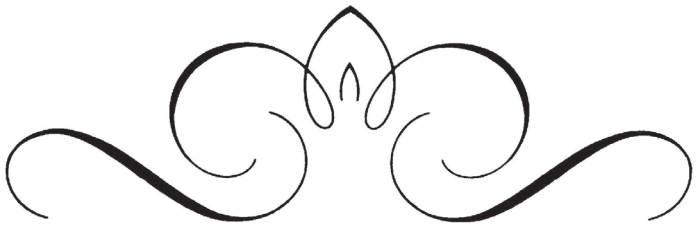
"Speed Dating Technology"

CERIAS Students preview their projects in 75 seconds or less!

Break for Dinner

5:00p

See page 40.



CERIAS 20th Anniversary Reception & Poster Session

6:30p-8:30p

PMU Ballroom

Please join us for appetizers and refreshments as we celebrate the 20th anniversary of CERIAS. Remarks by Prof. Spafford at 7pm.

Welcome (Day 2)

9:00a

CERIAS Awards

Dongyan Xu
CERIAS Interim Director
Professor Computer Sciences
Purdue University

Keynote

9:30a

"Managing Risks in the Cyber Battle Space"

Mark Spangler
Director, Cyber Security Operations Center
National Reconnaissance Office

Mark Spangler has over 36 years of experience and expertise executing National Security programs at the Central Intelligence Agency (CIA) and the National Reconnaissance Office (NRO) in cyber security and information technology (IT) operations and project management. He was appointed as the NRO Chief Information Security Officer (CISO) in 2006. He built the foundation of NRO's information assurance (IA) and cyber security program, established NRO's IT Project Management Center of Excellence, and has led transformational change in the delivery and management of NRO's global IT systems/services. Spangler is a proven leader with a strong IT business acumen and a passion for resource management/customer outreach/cyber security.

Featured Speaker

10:30a

"Cyber Center for Education and Innovation, Home of the National Cryptologic Museum – a National collaboration in K-20 cyber education"

Mark Loepker
Senior Advisor
National Cryptologic Museum Foundation

Mark S. Loepker is a master practitioner in Information Assurance (IA) and International Partnerships with over 39 years of government experience.

Mr. Loepker currently serves as a Senior Advisor to the National Cryptologic Museum Foundation, focused on developing educational programs to be delivered from the new Cyber Center for Education & Innovation (CCEI). In this role, he focuses on ensuring that K-12/STEM initiatives are tightly aligned with national cyber curriculum standards, and that the CCEI becomes a national resource addressing workforce development and operational training requirements targeting 13-20 grade curriculum.

During his National Security Agency career, he was the Director, National Information Assurance Partnership (NIAP) established between the National Institute of Standards and Technology (NIST) and NSA to evaluate Information Technology (IT) product conformance to international standards. He was the Department of Defense Chief Information Officer (DoD/CIO), Defense-wide Information Assurance Program (DIAP) Director. He served as the Common Criteria Recognition Arrangement (CCRA) Executive Subcommittee Chairman leading 27 Nations in product assurance, evaluation, supply chain risk management and managing the CCRA.

Mr. Loepker, working with Dr. Melissa Dark, Purdue's Professor of Technology in Computer and Information Technology, pioneered the first-ever NSA sponsored class where graduate students used typical NSA technical challenges for their class work with mentorship from NSA Technical Directors. After five years, the effort now spans 19 Universities and 12 government agencies with over 354 alumni and over 160 currently enrolled.

Fireside Chat

11:00a

"The State of Cybersecurity Education – Can Our Educational System Produce the Quantity and Quality of Graduates Needed to Meet Labor Demand?"

Melissa Dark (Moderator)
W.C. Furnas Professor
Purdue Polytechnic Institute

Dr. Melissa Dark is currently the W.C. Furnas Professor of Technology in Computer and Information. From 2003-2011 she served as the Associate Dean for Research and Strategic Planning in the College of Technology. Melissa has extensive experience teaching, curriculum development, and instructional research and assessment. She has led several national projects in education transformation. She has been active in defining the cybersecurity body of knowledge, leading faculty development programs nationwide, and helping define education research priorities in cybersecurity education. She is currently leading several projects/initiatives in cybersecurity education including:

· INSuRE - this project is a cybersecurity research collaborative that uses the cybersecurity student talent pool to work on problems of national interest supplied by federal agencies and national labs, and at the same time develops hands-on, applied research skills of students.

· Secure Programming Clinic - this project that is developing a concept inventory to diagnose learners' misconceptions in secure programming.
`

· Cyber fMRI - this project that is investigating the use of representational fluency to develop deep conceptual understanding of selected complex cybersecurity topics.

· C5 – this project is focused on developing the capacity of community colleges in cybersecurity and computing.

Diana Burley
Associate Dean, Research and External Relations (Interim), Graduate School of Education and Human Development
The George Washington University

Diana L. Burley, Ph.D. is Executive Director and Chair of the Institute for Information Infrastructure Protection (I3P); Associate Dean for Research and External Relations (Interim) and Full Professor of Human & Organizational Learning at The George Washington University (GW) Graduate School of Education and Human Development. She is a widely sought after cybersecurity thought leader, educator, researcher and strategist. Prior to GW, she managed a multi-million dollar computer science education and research portfolio for the US National Science Foundation. She has written more than 80 publications on cybersecurity, information sharing, and IT-enabled change; testified before the US Congress; conducted international cybersecurity awareness training on behalf of the US State Department; and advised global corporation on cybersecurity strategy.

Neal Ziring
Technical Director
U.S. National Security Agency

Mr. Neal Ziring is the Technical Director for the National Security Agency's Capabilities Directorate, serving as a technical advisor to the Capabilities Director, Deputy Director, and other senior leadership. Mr. Ziring is responsible for setting the technical direction across many parts of the capabilities mission space, including in cyber-security. Mr. Ziring tracks technical activities, promotes technical health of the staff, and acts as liaison to various industry, intelligence, academic, and government partners. Prior to the formation of the Capabilities Directorate, Mr. Ziring served 5 years as Technical Director of the Information Assurance Directorate.
His personal expertise areas include security automation, IPv6, cloud computing, cross-domain information exchange, and data access control, and cyber defense.
Prior to coming to NSA in 1988, Neal worked at AT&T Bell Labs. He has BS degrees in Computer Science and Electrical Engineering, and an MS degree in Computer Science, all from Washington University in St. Louis.

Tim Sewell
Senior Advisor & Security Architect
Eli Lilly

Sewell leads a global, enterprise-wide information security architecture team that blends technology, people, and process to create innovative solutions that protect the confidentiality, integrity and availability of information, systems, and devices that fuel Lilly's mission to make medicines that help people live longer, healthier, more active lives. Sewell is a member of the company's Information Technology and Information Security leadership teams.

Sewell began his career as an independent security consultant in Omaha, NE. He later joined Lockheed Martin where he held a variety of information security and leadership roles in support of US Defense, Intelligence, and Civilian agencies. After leaving Lockheed, he joined the Mayo Clinic where he led transformational information security projects and the information security architecture team. Sewell has broad experience across the information security spectrum, including penetration testing, product development, architecture, and strategy.

Sewell serves on several advisory boards for information security technology, innovation, and education. He holds a Master's degree in Information Technology from Carnegie Mellon and holds several industry certifications including the CISSP-ISSAP and OSCP. While at Lockheed, Sewell received patents in analytics and cyber security. He currently resides in Carmel, IN with his wife and two children.

CERIAS Program Talk Indiana Cybersecurity Initiatives

1:30p

Chetrice Mosley
Cybersecurity Program Director
State of Indiana

As Indiana's Cybersecurity Program Director, Chetrice Mosley 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 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 has provided public relations and strategic consultation to a number of state agencies and organizations. Mosley earned her bachelor's degrees with honors in communications studies and public relations from Indiana University.

Douglas Rapp
President
Cyber Leadership Alliance

Douglas Rapp is an experienced cybersecurity consultant with previous positions as lead cybersecurity consultant to the Indiana Economic Development Corporation. He authored the Purdue Research Foundation Incident Response Policy, Indiana National Guard Cyber Response and Incident Management Operations Plan, State of Indiana Cyber Security Economic Development Strategic Plan and Action Plan. He led a multi-state team that authored the regional force structure bid leading to the establishment of the FEMA Region 5 Cyber Protection Team – the first in the nation. He is a published author, speaks nationally and internationally, and is a trusted consultant to State and National government for cybersecurity. Doug graduated with a BFA from Indiana University and a MS in Business Management from Indiana Wesleyan University. Doug is a U.S. Army veteran who served in the Iraq War.

2:00p

CERIAS Tech Talk #3

Blockchains: A Technical Perspective on the Future of Decentralization

Aniket Kate
Assistant Professor of Computer Sciences
Purdue University

Abstract
In the eight years since blockchains were first proposed in the form of Bitcoin, their use as verifiable distributed ledgers for financial and supply-chain transactions has become widespread. As Bitcoin and other blockchain systems such as Ethereum and Hyperledger continue to mature, it is becoming clear that blockchains as a means to facilitate verifiable assets transfers are here to stay. In fact, the disruptive potential of blockchains is now widely claimed to be equal to that of the Internet.

This talk takes a bird's eye view of the blockchain evolution to identify the ground rules and assumptions of this transparency enhancing technology. We will also shade some light on promising future research directions as well as applications of blockchains in the science, the engineering and beyond.

About the Speaker
Dr. Aniket Kate is an Assistant Professor in the computer science department at Purdue University. Before joining Purdue in 2015, he was a faculty member and an independent research group leader at Saarland University in Germany, where he was heading the Cryptographic Systems Research Group. He completed his postdoctoral fellowship at Max Planck Institute for Software Systems (MPI-SWS), Germany in 2012, and received his PhD from the University of Waterloo, Canada in 2010. His research integrates applied cryptography, distributed computing and data-driven analysis towards designing, implementing and analyzing privacy and transparency enhancing technologies.
To know more about his blockchain research, visit: https://freedom.cs.purdue.edu/blockchains/

CERIAS Tech Talk #4

2:30p

"Online Adversarial Learning of Nuclear Reactor Dynamical State"

Hany Abdel-Khalik
Associate Professor of Nuclear Engineering
Purdue University

Hany Abdel-Khalik received his B.S. in nuclear engineering at Alexandra University, Egypt; and his M.S. and Ph.D. in nuclear engineering at North Carolina State. His research focuses on computational reactor physics, reduced order modeling and complexity reduction, uncertainty quantification and sensitivity analysis, and data assimilation and model calibration. He is a member of the American Nuclear Society (ANS), Sigma Xi Research Honor Fraternity, and the SIAM Applied Mathematics Society.

Fireside Chat

"What's Ahead – The Spirit of Cybersecurity Yet to Come"

3:15p

Eugene Spafford (Moderator)

Deborah Frincke
NSA/CSS Director of Research
National Security Agency

Dr. Deborah Frincke leads he Research Directorate (RD) of the National Security Agency/Central Security Service (NSA/CSS)—the largest "in-house" research organization in the U.S. Intelligence Community—which is tasked with creating critical breakthroughs in mathematics, science, and engineering that support and enable the NSA/CSS to perform it Signals Intelligence (SIGINT), Information Assurance, and Cyber Defense missions. She is a member of the Agency's Board of Directors and serve as the NSA Science Advisor and Innovation Champion. Under her guidance, RD operates collaborative as wells as government-only facilities that are world-class in fields as diverse as mathematics, computer science, cybersecurity/trustworthy computing, engineering, physics, neuroscience, cognitive psychology, and linguistics. RD engages with leading industries, universities, and national laboratories to both advance core competencies and to leverage work in overlapping disciplines.

Mark Graff
CEO
Tellegraff LLC

A cyber security practiooner and thought leader for over 25 years, Mark Graff is the Founder and CEO at Tellagraff, LLC. Graff is a seasoned Chief Information Security Officer, having filled that role for NASDAQ for three years and Lawrence Livermore National Laboratory for nine. While at NASDAQ, Graff founded and chaired the Cyber Security committee for the World Federation of Exchanges the first international organization of executives responsible for the cyber safety of the world's stock exchanges. He was named Internet Security Executive of the Year for the Northeast United States in 2014.

John Johnson
CEO/Chief Security Strategist
Aligned Security

Dr. John D. Johnson is CEO and Founder Aligned Security. He is also a founding board member of the Security Advisor Alliance (501c.3), a member of SC Media Editorial Board, and serves on advisory boards for innovative security startups. John spent 17 years as security architect for a Fortune 100 global manufacturing company, where he managed infrastructure and developed strategy and secure architecture solutions for protecting a global corporate network, endpoints, industrial systems and the supply chain. His experience spans the public and private sectors, as well as industry verticals: technology, manufacturing, finance, energy, healthcare, education. John was previously network security manager for the Theoretical Division at Los Alamos National Laboratory, and an experimental nuclear physicist developing radiation systems for nuclear remediation and non-proliferation.

John has developed and taught numerous graduate cybersecurity courses and helped develop the CISO executive certificate program with University of Chicago, Booth School of Management. He is a frequent speaker at industry conferences and serves as program committee member for RSA Conference and Black Hat. John is founder and organizer of CornCon, an annual Midwestern cybersecurity conference and kids hacker camp. Over his career, he has served in leadership roles in technical and professional societies, including IEEE, InfraGard and (ISC)2. John has received various awards in recognition of his contribution to the profession, and was runner up for 2014 Chicago CISO of the Year. He is an IEEE Senior Member, Charter Member of FAIR Institute and Fellow of Ponemon Institute.

John enjoys promoting STEM and cybersecurity with kids and the public, blogging, podcasting, photography, travel, astronomy and lives in Iowa with his very large dog.

Closing Keynote

4:30p

Josh Corman
Chief Security Officer
SVP at PTC

"Bits & Bytes, Flesh & Blood, and Adapting for the Next 20 Years"

Abstract
Healthcare Cybersecurity is in critical condition. We know there is Promise & Peril in Connected Medicine... While the benefits of connected medicine are undeniable, the increased and premature, hyper connectivity now exposes us to a bevy of accidents and adversaries. As a sixth of our economy, healthcare's vital public safety role, critical infrastructure, and national security interests, healthcare is both too big to fail and at serious risk of failure. We will outline some of the uncomfortable truths (and uncomfortable recommendations) uncovered by the Congressional Task Force on Healthcare Cyber Security, detail the profound impacts of a spate of 2016/2017 attacks affecting patient care, and highlight the experiences and opportunities revealed by the Cyber Med Summit - a first ever clinical hacking simulation involving physical, hackers, city/state/federal government, and medical stakeholders. We were always prone, we were prey, but we had lacked predators. That relative obscurity is now over. We will eventually strike the right balance. Our belief is that we can be safer. sooner, if we work together.

About the Speaker
Joshua Corman is a Founder of I am The Cavalry (dot org) and CSO for PTC. Corman previously served as Director of the Cyber Statecraft Initiative for the Atlantic Council, CTO for Sonatype, Director of Security Intelligence for Akamai, and in senior research & strategy roles for The 451 Group and IBM Internet Security Systems. He co-founded RuggedSoftware and IamTheCavalry to encourage new security approaches in response to the world's increasing dependence on digital infrastructure. Josh's unique approach to security in the context of human factors, adversary motivations and social impact has helped position him as one of the most trusted names in security. He also serves as an adjunct faculty for Carnegie Mellon's Heinz College and on the 2016 Congressional Healthcare Cybersecurity Task Force.

Poster Session Abstracts

pg.

POSTER SESSION RESEARCH AREA KEY

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

ASSURED IDENTITY AND PRIVACY

1. AB-Graph: An Authenticated-Blocked Graph

Servio Palacios, Byoungyoung Lee, Ananth Grama, Bharat Bhargava

Many modern big-data applications work on top of graph-structured datasets. For instance, graph databases such as Neo4j, TitanDB, OrientDB, and others handle large-scale graphs that model biological interactions and social networks. Graphs are semi-structured, as opposed to the relational model. Thus, accessing network-structured data from/to secondary storage necessitates new techniques. These new methods must ensure access locality for graphs. Moreover, in multi-tenant environments, protecting sensitive information from unauthorized access and leakage is imperative. Unfortunately, although existing solutions for the graph processing model include secure communication and authentication (for independent graphs and authenticated entities); there is no solution for multiple authenticated entities (data owners) sharing a diversity of data graphs. Also, current solutions do not take into consideration graph access locality and authenticated multi-tenant clouds at the same time. In this paper, we propose a novel authenticated-blocked graph processing model. The project includes a set of unique algorithms that model the authentication scheme and graph structure into a series of disk blocks with high-locality. Our contributions include: (1) the definition of the practical and formal security model of authentication for the blocked graph, (2) three new algorithms for (i) block construction with high locality, (ii) disk layout for authenticated and blocked graphs, (iii) new data structures for graph access. (3) An open-source implementation and evaluation of the proposed techniques. Through a set of benchmarks and applications, we demonstrate the practicality of our solution.

2. Distribution-Aware Password Throttling Mechanisms

Alina Nesen, Jeremiah Blocki

Large-scale online password guessing attacks are wide-spread and continuously qualified as one of the top cyber-security risks. The common method for mitigating the risk of online cracking is to lock out the user after a fixed number) of consecutive incorrect login attempts within a fixed period of time (e.g., 24 hours). Selecting the value of k induces a classic security-usability tradeoff. When k is too large a hacker can(quickly) break into a significant fraction of user accounts, but when k is too low we will start to annoy honest users by locking them out after a few mistakes. Motivated by the observation that honest user mistakes typically look quite different than the password guesses of an online attacker, we introduce the notion of a password distribution aware lockout mechanism to reduce user annoyance while minimizing user risk. As the name suggests, our system is designed to be aware of the frequency and popularity of the password used for login attacks while standard throttling mechanisms (e.g., k-strikes) are oblivious to the password distribution. In particular, we maintain a “hit count” for each user which is based on (estimates of) the cumulative probability of all login attempts for that particular account. A user will only

be locked out when this hit count is too high. To minimize user risk we use a differentially private CountSketch to estimate the frequency of each password and to update the "hit count" after an incorrect login attempt. To empirically evaluate our new lockout policy we generate a synthetic data set to model honest user logins in the presence of an online attacker. The results of our analysis on this synthetic data set strongly support our hypothesis that distribution aware lockout mechanisms can reduce user annoyance and risk.

3. Lightweight, Scalable and Secure Computations for Engineering Design

Jitesh H. Panchal

Risks involved in information sharing including leakage and misuse inhibit collaborators from using confidential information within a collaboration. In this work, we present a fast lightweight and secure computation (FLASC) technology that enables collaborators to preserve input confidentiality while performing computations. We demonstrate the use of this proposed technology in an engineering design application (Finite Element Analysis).

4. Privacy-preserving Autonomous Aggregate Data Analytics in Untrusted Cloud

Ganapathy Mani, Denis Ulybyshev, Bharat Bhargava, Jason Kobes, Puneet Goyal

Intelligent Autonomous Systems (IAS) are highly reflexive and very cognizant about their limitations and capabilities, interactions with neighboring entities, as well as the interactions with its operational environment. IAS should be able to conduct data analytics and update policies based on those analytics. These tasks should be performed autonomously i.e. with limited or no human intervention. In this paper, we introduce advanced aggregate analytics over untrusted cloud and autonomous policy updates as a result of those analytics. We will be using Active Bundle (AB), a distributed self-protecting entity, wrapped with policy enforcement engine as our implementation service. We propose an algorithm that can enable individual ABs to grant or limit permissions to their AB peers and provide them with access to anonymized data to conduct analytics autonomously. When these processes take place, ABs do not need to rely on policy enforcement engine every time, which increases scalability. This workflow also creates an AB environment that is decentralized, privacy-preserving, and autonomous.

5. Recall of Survival-Relevant Passwords

Isis Chong, Robert W. Proctor, Ninghui Li, and Jeremiah Blocki

Sentence-based mnemonic strategies for which users create passwords based on the first letter of every word in a sentence have been shown to be effective for recalling passwords (Yan et al., 2000). Research in the field of human memory has suggested that information encoded based on its survival-related properties may be more memorable than other information (Nairne, Thompson, & Pandeirada, 2007) and as such, may be applicable to password generation. The present study sought to compare the memorability of a self-relevant mnemonic control strategy against a novel survival-related generation strategy. Findings suggest that the survival processing advantage may not easily generalize to password recall.

END SYSTEM SECURITY

6. ALEXKIDD-FUZZER: Kernel Fuzzing Guided by Symbolic Information

Kyungtae Kim, Byoungyoung Lee

Black-box and white-box fuzzing (i.e. symbolic execution) are both getting popular for software testing. However, both of them have severe limitations that prevent maximizing code coverage. We design ALEXKIDD-FUZZER, which overcomes limitation of such fuzzing and symbolic execution. We first employ general fuzzing mechanism such that feasible execution paths are explored at a rapid pace. Furthermore, during fuzzing execution, we allow concolic engine to guide the fuzzer to make unreachable-code reachable.

7. Blockhub: Blockchain-based Secure Cross-domain Software Development System

Denis Ulybyshev, Bharat Bhargava, Miguel Villarreal-Vasquez, Aala Alsalem, Ganapathy Mani, Leszek Lilien, Donald Steiner, Jason Kobes, Steve Seaberg, Paul Conoval, Robert Pike, Rohit Ranchal

To ensure integrity, trust, immutability and authenticity of software and information (cyber data, user data and attack event data) in a collaborative environment, research is needed for cross-domain data communication, global software collaboration, sharing, access auditing and accountability. Blockchain technology can significantly automate the software export auditing and tracking processes. It allows to track and control what data or software components are shared between entities across multiple security domains. Our blockchain-based solution relies on role- and attribute-based access control and prevents unauthorized data accesses. It guarantees integrity of provenance data on who updated what software module and when. Furthermore, our solution detects (Cont.)

data leakages, made behind the scene by authorized blockchain network participants, to unauthorized entities. Our approach is used for data forensics/ provenance, when the identity of those entities who have accessed/ updated/ transferred the sensitive cyber data or sensitive software is determined. All the transactions in the global collaborative software development environment are recorded in the blockchain public ledger and can be verified any time in the future. Transactions can not be repudiated by invokers. We also propose modified transaction validation procedure to improve performance and to protect permissioned IBM Hyperledger-based blockchains from DoS attacks, caused by bursts of invalid transactions. Our solution supports decentralized and distributed data exchange, that is essential in V2X systems, where a Central Authority (CA) is not required to enforce access control policies. Furthermore, we facilitate querying encrypted Vehicle Records through Structured Query Language (SQL) queries.

8. Double Trouble: Fuzzing Kernel Modules

Derrick McKee

Despite its importance, the Linux kernel remains a difficult target for fuzzers. While prior work, such as syzkaller, allows for fuzzing the kernel, it is still difficult to fuzz arbitrary loadable kernel modules (LKMs). These LKMs represent the majority of source code in the Linux kernel, as well as a major source of CVEs. We present Double Trouble, a general framework for fuzzing LKMs. Double Trouble requires a one-time minimal programming effort to support fuzzing any subsystem. Once that effort is complete, any LKM within the subsystem can be fuzzed from the two possible sources of inputs: an upper half direction representing a system call execution, and a lower half direction representing either hardware interrupt or exposed kernel function. As a case study, we are adding support for fuzzing filesystems. We use the state-of-the-art generational fuzzer, afl-fuzz, for the upper half fuzzing, and a deterministic fuzzer for the lower half.

9. Evaluating the effects of KAISER on operating system performance.

Joseph Graham

With the recent advent of the meltdown exploit a patch had to be made to prevent this. This patch was commonly known as KAISER. This patch was said to have about a 20% operating system performance hit. This was an investigation in whatever or not the performance hit existed and if it did how extreme was it.

10. Fafnir: Type Inference Based Static Rewriting

Sushant Dinesh, Lovepreet Singh, Mathias Payer

Static binary rewriting modifies executables to en- able, e.g., hot-patching vulnerabilities, retrofitting protections, or the removal of unneeded functionality to reduce attack surface. Current static rewriting techniques are limited to small binaries, of the order of a few kilobytes, and do not scale to real world software. We propose a set of systematic, scalable analysis techniques to statically rewrite binaries with zero runtime overhead and memory footprint. To reflow code, absolute addresses hardcoded in the binary must be converted to symbols-- a process termed symbolization. To distinguish pointer types from scalar data types, we introduce a lightweight data-flow analysis that identifies and propagates coarse-grained type information. Unlike previous approaches based on heuristics, our analysis is principled and marks a constant as pointer type only if the value flows to a memory dereference. Constants marked as pointer types are replaced by symbols, resulting in a symbolized assembly file. After arbitrary modifications this file is ready to be assembled by any off-the-shelf assembler. We implement the analysis in a tool named Fafnir and evaluate it on several Linux x86-64 binaries ranging from the SPEC CPU2006 benchmarks, the nginx webserver, to the binutils/coreutils. Fafnir correctly identifies symbols with perfect (100%) accuracy across all our tests. The reassembled binaries show no degradation in performance or memory usage. Finally, to show practical utility of Fafnir we present several case studies where we patch known vulnerabilities in real world binaries without breaking functionality.

11. FirmFuzz : Automated IoT Firmware Introspection and Analysis

Prashast Srivastava, Hui Peng, Ryan Berg, Nathan Burow, Howard Shrobe, Hamed Okhravi, Mathias Payer

While the number of IoT devices grows at an exhilarating pace, their security remains stagnant. Imposing secure coding standards across all vendors is infeasible. Testing the security of individual devices allows an analyst to evaluate their security post deployment. Any discovered vulnerabilities can then be disclosed to the vendors to allow them to improve their products. The search for vulnerabilities should ideally be automated for efficiency and device-independent for scalability. We present FirmFuzz, an automated device-independent dynamic analysis framework for Linux- based firmware images. FirmFuzz improves on existing state of the art hardware independent emulation techniques by providing mock support for all peripherals interfaced with by the firmware. It employs a rainbow fuzzing approach which incorporates both grey-box and white-box fuzzing to provide for targeted and deterministic bug discovery within these firmware images without requiring any manual intervention. We evaluate FirmFuzz on a sample set of six firmware images and discovered eight previously undisclosed vul- nerabilities across four different devices: two TREND- net Wireless IP cameras and two TRENDnet Wireless Routers.

12. Secure Data Communication in Autonomous V2X systems

Denis Ulybyshev, Aala Alsalem, Bharat Bhargava, Savvas Savvides, Ganapathy Mani, Lotfi Ben Othmane

In V2V and V2I communication systems, vehicles as well as infrastructure devices can interact and exchange data with each other. This capability is used to implement intelligent transportation systems applications. Data confidentiality and integrity need to be preserved in unverified and untrusted environments. We propose a solution that provides (a) role-based and attribute-based access control to encrypted data and (b) encrypted search over encrypted data. Vehicle Records contain sensitive information about the owners and vehicles in encrypted form with attached access control policies and policy enforcement engine. Our solution supports decentralized and distributed data exchange, that is essential in V2X systems, where a Central Authority (CA) is not required to enforce access control policies. Furthermore, we facilitate querying encrypted Vehicle Records through Structured Query Language (SQL) queries. Vehicle Records are stored in a database in untrusted V2X cloud environment that is prone to provide the attackers with a large attack surface. Big datasets, stored in cloud, can be used for data analysis, such as traffic pattern analysis. Our solution protects sensitive vehicle and owner information from curious or malicious information cloud administrators. Support of indexing improves performance of queries that are forwarded to relevant encrypted Vehicle Records (VR) that are stored in the cloud. We measure the performance and overhead of our security solutions such as VR and encrypted search capabilities with safety in V2V and V2I communication systems and analyze the effect of security over safety.

HUMAN CENTRIC SECURITY

13. Determining System Requirements for Human-Machine Integration in Computer Security Incident Response

Barrett Caldwell, Megan Nyre-Yu

Incident response teams in cyber defense (CSIRTs) play a critical role in mitigating security events. Advancement in the field requires integrating approaches from social and behavioral sciences to better understand the humans in the system. This research investigates IR tasks and the humans that perform them using Human Factors methods to determine functional requirements for possible automated solutions. Findings presented in a systems engineering language will inform algorithmic development from other scientific fields currently addressing cyber defense with computational methods.

14. From Monte Carlo to Las Vegas: Understanding if Undirected Neural Networks can Really Generate Fake Images

Pedro Savarese, Mayank Kakodkar, Bruno Ribeiro

We propose a Las Vegas transformation of Markov Chain Monte Carlo (MCMC) estimators of Restricted Boltzmann Machines (RBMs). We denote our approach Markov Chain Las Vegas (MCLV). MCLV gives statistical guarantees in exchange for random running times. MCLV uses a stopping set built from the training data and has maximum number of Markov chain steps K (referred as MCLV-K). We present a MCLV-K gradient estimator (LVS-K) for RBMs and explore the correspondence and differences between LVS-K and Contrastive Divergence (CD-K), with LVS-K significantly outperforming CD-K training RBMs over the MNIST dataset, indicating MCLV to be a promising direction in learning generative models.

15. Phishing Susceptibility: An Investigation Into Human Information Processing of Spear-Phishing

Aiping Xiong, Huangyi Ge, Jeremiah Blocki, Ninghui Li, Robert W. Proctor

Universities and their employees and students are highly vulnerable to spear-phishing. Email scanning systems are implemented by universities to detect spoofing and to provide regular digests of emails quarantined by the scanning systems for users to review (e.g., once-a-day Cisco quarantine email at Purdue). Although such scanning systems can reduce the amount of obvious marketing pitches and unwanted emails from known junk email sources, they often fail to quarantine forged emails. Moreover, once a forged email gets in, users typically do not have the opportunity to be warned. We aim to understand how university undergraduate students process and respond to spear-phishing emails, and whether the presence of a quarantine digest email impacts their decisions and actions. We conducted a role-play experiment, in which 464 Purdue undergraduate students performed an email management task. Within the task, they were instructed to read 10 emails (2 spear-phishing, 8 legitimate) and to take actions as they would normally do. We found that participants were more likely to delete and junk the email and did not enter information for the known phishing scam than for the unknown phishing scam. The presence of a Cisco quarantine email increased participants' awareness of phishing but showed no impact on their actions on spear-phishing emails and webpages. For participants who were aware of phishing, the presence of a Cisco quarantine email increased their likelihood of entering information on phishing webpages. However, a reversed pattern was evident for participants who were not aware of phishing. In summary, the results suggest a response bias and a lack of knowledge to identify phishing scams for undergraduate students. Although a Cisco quarantine email increased users' awareness of phishing, such increase may increase their vulnerability to enter information on phishing webpages.

16. Private Preserving Credit System with Cryptographic Currency

Tianchong Gao; Feng Li

The utility of cryptographic currencies, e.g., Bitcoin, is inherently restricted by privacy and latency concerns. Hence some payment protocols, such as the lightning network, have been introduced. We find that building a credit network as a second layer on top of a cryptographic currency helps anonymize transactions. Also, the credit network further extends the functionality of the original blockchain. It allows users to temporarily spend more money than they own. However, setting up the credit limit in a way that protects the creditor and also preserves the privacy of the debtor is a challenge. In this project, we build a credit management system. Specifically, in order to avoid frequent credit applications from a single debtor, we design a cyclic blockchain to store application information. We also embed Bloom filter in the blockchain and add differential-privacy noise to it to enhance the privacy of the original application address. We design a dispute flow that no party to these transactions and contracts (a credit manager, debtor, or creditor) is able to cheat the others, while the privacy of all parties is preserved.

17. Security Vulnerabilites for Large Venues

Alissa Gilbert, J. Eric Dietz

Physical security is critical for best cybersecurity practices; but how do you secure large venues that service thousands of people at once, across different events? Physical security practices for large venues are unique and complex compared to their small and private partners. Venues must be able to have proper security practices while not impeding their hosted events or visitors. Threat actors for these areas include disgruntled fans, activists, and terrorists, which can change depending on the venue. Specific security needs for these areas include identifying volunteers, staff, and patrons; access to restricted areas, limited access spaces, security screenings, security of wireless internet access and venue technology, and protecting personal information.

18. The Economics of Offline Password Cracking

Jeremiah Blocki, Benjamin Harsha, Samson Zhou

We develop an economic model of an offline pass- word cracker which allows us to make quantitative predictions about the fraction of accounts that a rational password attacker would crack in the event of an authentication server breach. We apply our economic model to analyze recent massive password breaches at Yahoo!, Dropbox, LastPass and AshleyMadison. All four organizations were using key-stretching to protect user passwords. In fact, LastPass's use of PBKDF2-SHA256 with 10 5 hash iterations exceeds 2017 NIST minimum recommendation by an order of magnitude. Nevertheless, our analysis paints a bleak picture: the adopted key-stretching levels provide insufficient protection for user passwords. In particular, we present strong evidence that most user passwords follow a Zipf's law distribution, and characterize the behavior of a rational attacker when user passwords are selected from a Zipf's law distribution. We show that there is a finite threshold which depends on the Zipf's law parameters that characterizes the behavior of a rational attacker if the value of a cracked password (normalized by the cost of computing the password hash function) exceeds this threshold then the adversary's optimal strategy is always to continue attacking until each user password has been cracked. In all cases (Yahoo!, Dropbox, LastPass and AshleyMadison) we find that the value of a cracked password almost certainly exceeds this threshold meaning that a rational attacker would crack all passwords that are selected from the Zipf's law distribution (i.e., most user passwords). This prediction holds even if we incorporate an aggressive model of diminishing returns for the attacker (e.g., the total value of 500 million cracked passwords is less than 100 times the total value of 5 million passwords). On a positive note our analysis demonstrates that memory hard functions (MHFs) such as SCRYPT or Argon2i can significantly reduce the damage of an offline attack. In particular, we find that because MHFs substantially increase guessing costs a rational attacker will give up well before he cracks most user passwords and this prediction holds even if the attacker does not encounter diminishing returns for additional cracked passwords. Based on our analysis, we advocate that password hashing standards should be updated to require the use of memory hard functions for password hashing and disallow the use of non-memory hard functions such as BCRYPT or PBKDF2.

19. Towards a triage model for online predator type prediction

Kanishka Misra, Shih Feng Yang, Kathryn Seigfried-Spellar, Julia Taylor Rayz

In an increasingly computer mediated world, it may be easier to start conversations with people online than it is in the real world, making it easy to build trust. This encourages people with malevolent intentions to take advantage of the trustful youngsters by means of various internet based messaging platforms. This poster presents results from applying classification methods on a corpus extracted from conversations between an online predator and a decoy. The Support Vector Machines algorithm is used to classify a predator as somebody who may or may not physically show up to meet their victim(decoy in this case). The features used in this study are word and character n-grams from the chat sessions. A nested resampling method is used to evaluate the performance of the classifier. The preliminary results indicate that the method can be used as a triage mechanism to help law enforcement.

NETWORK SECURITY

20. Automated Resilience for Distributed Coordination in Large-scale Networks

Xuan Wang, Shaoshuai Mou

Distributed control of large-scale multi-agent networks achieve global objectives only through local coordination. On one hand, the lack of central controller leads to robustness against individual agent or link failures. On the other hand, the dependence on local coordination raises a major concern that the whole network may crash down under sophisticated attacks to one or more vulnerable agents. Motivated by this, our research aims to provide a systematic way to achieve automated resilience for consensus-based distributed algorithms, which purely based on agents' locally available information.

21. Botnet Attacks: A Case Study of Qbot Botnet Monitoring and Victims

Rushabh Vyas, Nichole McFarland

In this case study, a Linux DDoS botnet malware, qbot, is researched and botnets are observed to find who the victims of DDoS attacks. Data gathered from honeypots, Shodan, and Censys was used to find C2 servers. To conduct monitoring of the C2 servers, a script was used to emulate a bot and connect to C2 servers. After a month of monitoring qbot C2 servers, it was discovered that DDoS attacks were conducted against video streaming sites, video game related sites and gaming servers, and rival DDoS services. Attackers were also observed communicating on C2 servers. C2 servers were seen mainly running on popular VPS provider networks.

22. LTEInspecor: A Systematic Approach for Adversarial Testing of 4G LTE

Omar Chowdhury, Shagufta Mehnaz, Elisa Bertino

We investigate the security and privacy of the three critical procedures of the 4G LTE protocol (i.e., attach, detach, and paging), and in the process, uncover potential design flaws of the protocol and unsafe practices employed by the stakeholders. For exposing vulnerabilities, we propose a model-based testing approach LTEInspector which lazily combines a symbolic model checker and a cryptographic protocol verifier in the symbolic attacker model. Using LTEInspector, we have uncovered 10 new attacks along with 9 prior attacks, categorized into three abstract classes (i.e., security, user privacy, and disruption of service), in the three procedures of 4G LTE. Notable among our findings is the authentication relay attack that enables an adversary to spoof the location of a legitimate user to the core network without possessing appropriate credentials. To ensure that the exposed attacks pose real threats and are indeed realizable in practice, we have validated 8 of the 10 new attacks and their accompanying adversarial assumptions through experimentation in a real testbed. Finally, we argue that our model-based testing framework can also be effective to automate the process of vulnerability discovery for the 5G standard which a lot of network providers are planning on rolling out in the near future.

23. Noise Detection of the Physical Data layer in EVs

Manuel Mar

Vehicle Cyber-security has become an important discipline, the prevention and study of possible attacks must be the most accurate possible. This study propose differentiate and analyze the relevant and useful data when trying to protect the Vehicle from cyber-threats.

24. Subgraph Pattern Neural Networks for High-Order Graph Evolution Prediction

Changping Meng, S Chandra Mouli, Bruno Ribeiro, Jennifer Neville

In this work we generalize traditional node/link prediction tasks in dynamic heterogeneous networks, to consider joint prediction over larger k-node induced subgraphs. Our key insight is to incorporate the unavoidable dependencies in the training observations of induced subgraphs into both the input features and the model architecture itself via high-order dependencies. The strength of the representation is its invariance to isomorphisms and varying local neighborhood sizes, while still being able to take node/edge labels into account, and facilitating inductive reasoning (i.e., generalization to unseen portions of the network). Empirical results show that our proposed method significantly outperforms other state-of-the-art methods designed for static and/or single node/link prediction tasks. In addition, we show that our method is scalable and learns interpretable parameters.

POLICY, LAW AND MANAGEMENT

25. Decoding the Hexadecimal Representation of a PostgreSQL Database Table

Joseph Balazs, Dr. Marcus Rogers, Dr. John Springer, Dr. Dawn Laux

Database forensics is an inadequately researched subfield of Digital Forensics. Existing documentation and literature contains a gap for the meaning of the hexadecimal representation of records within a table for the PostGreSQL database management system. In order to determine the indications between active and inactive records, the meanings had to be resolved. Simple testing was done on a table to insert, update, and delete records. A hex interpreter was used to analyze the differences between the records at the file system layer.

PREVENTION, DETECTION AND RESPONSE

26. A Deep Learning Based Anomaly Detection Approach for Intelligent Autonomous Systems

Miguel Villarreal-Vasquez, Bharat Bhargava

Advanced modern exploits characterize by their sophistication in stealthy attacks. Code-reuse attacks such as return-oriented programming and memory disclosure attacks allow attackers executing malicious instruction sequences on victim systems without injecting external code. This research proposes a new Deep Learning based anomaly detection technique that probabilistically models program control flows for behavioral reasoning and live monitoring. We aim to answer the binary classification problem of given a sequence of function calls whether or not the sequence should occur? The models are built with Recurrent Neural Networks (RNN) such as Long-Short Term Memory (LSTM) and Gated Recurrent Unit (GRU) implemented on top of PyTorch.

27. A Model-based Cyber Attack Detection and Identification for Networked Vehicle Systems

Sangjun Lee and Byung-Cheol Min

This study proposes a Direction of Arrival (DoA)-aided attack detection scheme to identify cyberattacks on networked multi-vehicle systems. For each agent, a local estimator is designed to generate robust residuals, and a parametric statistical tool corresponding to the residuals is elaborated to build sensitive (Cont.)

decision rules. These locally stored residuals and thresholds are shared between vehicles via a wireless network, allowing a multi-vehicle system to complete its mission in the presence of one or more compromised agents. The proposed DoA-aided attack detection scheme is tested on a multi-vehicle testbed with a team of 10 robots. Experimental results demonstrate that the proposed detection scheme enables each robot to identify malicious activities without shearing the global coordination.

28. Adaptive Threat Management Tool for Cyber-based Systems

Yahya Javed, Tawfeeq Shawly, Muhamad Felemban, and Arif Ghafoor

Develop resilient Cyber-based System (CBS) by incorporating an adaptive threat management mechanism throughout the life cycle of such system from design through recovery from cyber attacks.

29. Adversarial Attacks to Distributed Voltage Control in Power Distribution Networks with DERs

Peizhong Ju, Xiaojun Lin

It has been recently proposed that the reactive power injection of distributed energy resources (DERs) can be used to regulate the voltage across the power distribution network, and simple distributed control laws have been recently developed in the literature for performing such distributed Volt/VAR control. However, enabling the reactive-power injection capability of DERs also opens the door for potential adversarial attacks. Specifically, the adversary can compromise a subset of the DERs and use their reactive power to disrupt the voltage profile across the distribution network. In this paper, we study the potential damage (in terms of the voltage disruption) of such adversarial attacks and how to mitigate the damage by controlling the allowable range of reactive power injection at each bus. Somewhat surprisingly and contrary to the intuition that the reactive power injection at legitimate buses should help mitigating the voltage disruption inflicted by the adversary, we demonstrate that an intelligent attacker can actually exploit the response of the legitimate buses to amplify the damage by two times. Such a higher level of damage can be attained even when the adversary has no information about the network topology. We then formulate an optimization problem to limit the potential damage of such adversarial attacks. Our formulation sets the range of the reactive power injection on each bus so that the damage by the adversary is minimized, subject to the constraint that the voltage mismatch (without attack) can still be maintained within a given threshold under an uncertainty set of external inputs. Numerical results demonstrate the validity of our analysis and the effectiveness of our approach to mitigate the damage caused by such attacks.

30. Agent-Based Modeling

Jae Yong Lee

The 1999 Colorado Columbine Massacre was an eye-opening incident that reassessed the first responders' and the general public's readiness for active shooter incidents (ASI). According to the Federal Bureau of Investigation, the rate of ASI and casualty counts raised from 6.4 incidents to 16.4 incidents per year from 2000 to 2013. The law enforcement community revamped the mitigation tactics by doing the following: establish a contact team prior to entry, implemented an incident command system, and stationed a school resource officer. However, for the general public, the traditional emergency response of Evacuate and Shelter-In-Place are no longer effective since the threat from the shooter is not stationary. An agent-based model was developed which entails the interactions among active shooter, unarmed individuals, and the police officer agents. This model simulates casualty and survival rate of unarmed individuals while they attempt to evacuate an ASI under the following conditions: discharge delay, civilians cognitive delay, and police response delay. The result of this modeling could better guide future policy decisions to mitigate active shooter incidents and lower casualties.

31. Analyzing Response Mitigation Communication Methods by Simulation Modeling

Katherine Reichart, Anna Larson, Kristal Smith

Responding to an emergency requires quick and accurate communication in order to identify best practices in case of an unexpected event. By modeling these methods, one can estimate the response communication time, accuracy, and effectiveness of a certain group. This modeling can be applied to any situation that requires communicating a message. The particular model can be edited to reflect such particularly regarding communication rate, by word of mouth in comparison to using an outside system.

32. Automated Penalization of Data Leakage using Crypto-augmented Smart Contracts

Prof. Aniket Kate, Easwar Vivek Mangipudi, Krutarth Rao

We solve this problem by augmenting a blockchain on-chain smart contract between the sender and receiver with an off-chain cryptographic protocol, such that any significant data leakage from the receiver is penalized through a monetary loss. We develop a natural extension of oblivious transfer called doubly oblivious transfer (DOT) which, when combined with robust watermarking, a claim-or- refund blockchain contract and a non-interactive zero knowledge proof provides the necessary framework to realize the protocol in a provably secure manner.

33. CAM2 - Analysis of Visual Data from World Wide Network Cameras

Andrew Ulmer, Yung-Hsiang Lu, the rest of the CAM2 team

CAM2 is a cloud based platform for processing visual data from video cameras all around the world. The CAM2 team tackles a large variety of tasks, including but not limited to image processing, API development, web UI development, database construction and maintenance, super-computing, as well as entrepreneurship.

34. Graceful Degradations in Autonomous Systems Through Combinatorial Designs

Ganapathy Mani, Bharat Bhargava, Basavesh Shivakumar, Jason Kobes

Intelligent Autonomous Systems (IAS) are highly cognitive, reflexive, multitasking, trustworthy (secure as well as ethical), and rich in knowledge discovery. IAS are deployed in dynamic environments and connected with numerous devices of different types, and receive large sets of diverse data. They often receive new types of raw data that was not present in either training or testing data sets thus they are unknown to the learning models. In a dynamic environment, these unknown data objects cannot be ignored as anomalies. Hence the learning models should provide incremental guarantees to IAS for learning and adapting in the presence of unknown data. The model should support progressive enhancements when the environment behaves as expected or graceful degradations when it does not. In the case of graceful degradations, there are two alternatives: (1) weaken the acceptance test of data object (operating at a lower capacity) or (2) replace primary system with a replica or an alternate system that can pass the acceptance test. In this paper, we provide a combinatorial design MACROF configuration built with balanced incomplete block design to support graceful degradations in IAS and aid them to adapt in dynamic environments. The architecture provides stable and robust degradations in unpredictable operating environments with limited number of replicas. Since the replicas receive frequent updates from primary systems, they can take over primary system's functionality immediately after an adverse event. We also propose a Bayesian learning model to dynamically change the frequency of updates. Our experimental results show that MACROF configuration provides an efficient replication scheme to support graceful degradations in autonomous systems.

35. HexCFI: Fully Context Sensitive Control-Flow Integrity

Nathan Burow

Despite deployed defenses such as DEP, stack canaries, and ASLR, attackers are still able to use control-flow hijacks to gain control of systems. Control-flow hijacks overwrite code pointers, e.g., return addresses, function pointers, and virtual table pointers, to gain control over applications. Control-Flow Integrity (CFI) is a new defense policy that attempts to mitigate control-flow hijack attacks and is being deployed in practice, e.g., Chrome and Edge are shipped with CFI. CFI protects indirect function calls, i.e., calls through a function pointer or virtual calls, by statically computing a set of allowed targets. The allowed target set is based off an analysis of the control-flow graph of the program, and due to the limitations of static analysis (alias analysis) is fundamentally over approximated. The more over-approximate the target sets are, the easier it is for attackers to use techniques like control-flow bending to bypass CFI. We present a novel technique, called HexCFI, that does not rely on static analysis to compute the target sets and thus is not over approximate. Instead of statically computing the target sets, HexCFI instruments the program to record the targets of each indirect callsite. The program is then run under benign input from, e.g., developer test suites. The program is then recompiled, and the observed targets sets for each indirect callsite are used by the enforcement mechanism. Our target sets are thus the minimal possible size while still allowing correct execution of the program.

36. Leveraging Memory Forensics To Decrypt iOS Backups

Colin Cowie

The amount of iOS devices globally has been increasing. Mobile forensics has limitations in obtaining evidence due to the rapid changes in technology and the quick advancement of mobile software and operating systems. Analyzing memory is a technique that digital forensics incident responders use to find critical data. This work focuses on the analysis of memory from a personal computer to discover digital evidence from an iOS device. This study aimed to locate information including AppleID credentials, encrypted backup passwords, sensitive device information and more. For some iOS artifacts, it was possible to locate them in memory as well create techniques to discover them without knowing their value beforehand. Therefore, this is a step towards using memory forensics to discover mobile evidence.

37. Mitigating Counterfeiting in Supply Chains using Blockchain Technology

Aniket Kate, Mahimna Kelkar, Easwar Vivek Mangipudi, Pedro Moreno-Sanchez, Krutarth Rao

Enhancing supply chain traceability and deterring goods (like airbags of cars) counterfeiting has become a key challenge for the commercial supply chains. Though hardware based solutions like Physically Unclonable Functions (PUF) and RFID tags allows supply chain players to identify and authenticate the goods across supply chains they cannot prevent the counterfeiting and duplication attacks launched by the supply chain players themselves. The adversarial supply chain players can easily equivocate (and modify the supply chain logs) to present conflicting views to other players and to end consumers. This proposal aims at solving this equivocation problem with the current supply chains. In particular, our work plans to revolutionize the current supply chain management systems by executing the supply and tracking of goods along with the payments using the blockchain technology. The blockchain technology forms a distributed, single source of shared truth for supply chains, which along with smart contracts helps mutually distrusting sets of players/companies with possibly adversarial interests to collaborate with secure set of rules.

38. PoachNet: An Embedded System to Detect Theft

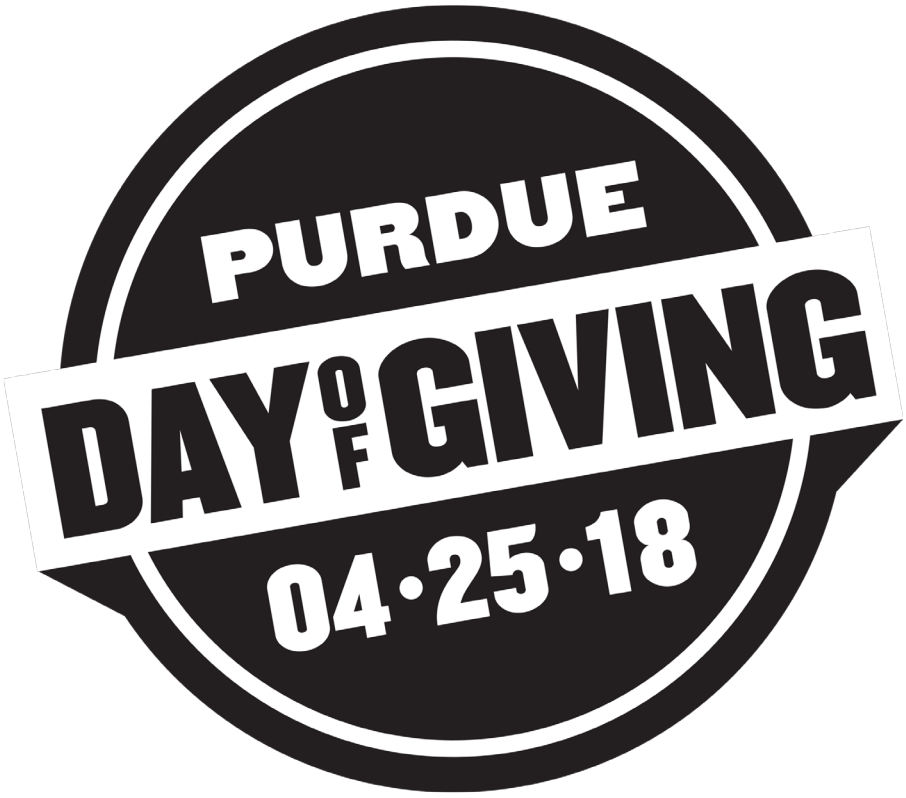
Eric Buedel

During most months of the year, oyster farmers are growing thousands of dollars worth of oysters in bay areas. Many oysters are placed into one cage, multiple cages are filled, then the cages are placed many feet underwater, where they are attached to a buoy above. The oysters require months of time spent underwater in order to become fully-grown and ready for sale. Because the oysters are expensive and cannot be monitored at all times, they are often poached (i.e., stolen), causing the farmer to lose thousands of dollars of oyster seed. Our device, named PoachNet, resides in the cages with the oysters and monitors for theft. If theft is detected, it alerts the oyster farmer via SMS and a web interface.

39. Security Perimeters for Large Events

Alissa K Gilbert, Austin Riegsecker

Large Events are categorized as those with 10,000 or more individuals gathering for a known affair. These events take considerable amounts of security personnel and resources to keep patrons safe. Large Events create higher than average amounts of population density, making these areas adapt for attacks on pedestrians and gatherers. Using multi-method modeling, population density was unexpectedly high in certain areas due to key factors such as parking and convenient walkways. After identifying these areas with high population density, rerouting traffic and including partial or complete road closures reduces population density and vehicle traffic. In addition, rogue vehicles become easier to identify when they do not follow proper procedures. Recommendations from this research include identifying practical mitigation techniques and installing temporary or permanent road control measures. Venues becoming more aware and practicing proper security hygiene allows for conscious mitigation of threats, and assists with better incident response.



April 25 is #PurdueDayofGiving!

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

https://dayofgiving.purdue.edu/school/cerias/

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 of information security, assurance, resiliency, and privacy. 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:

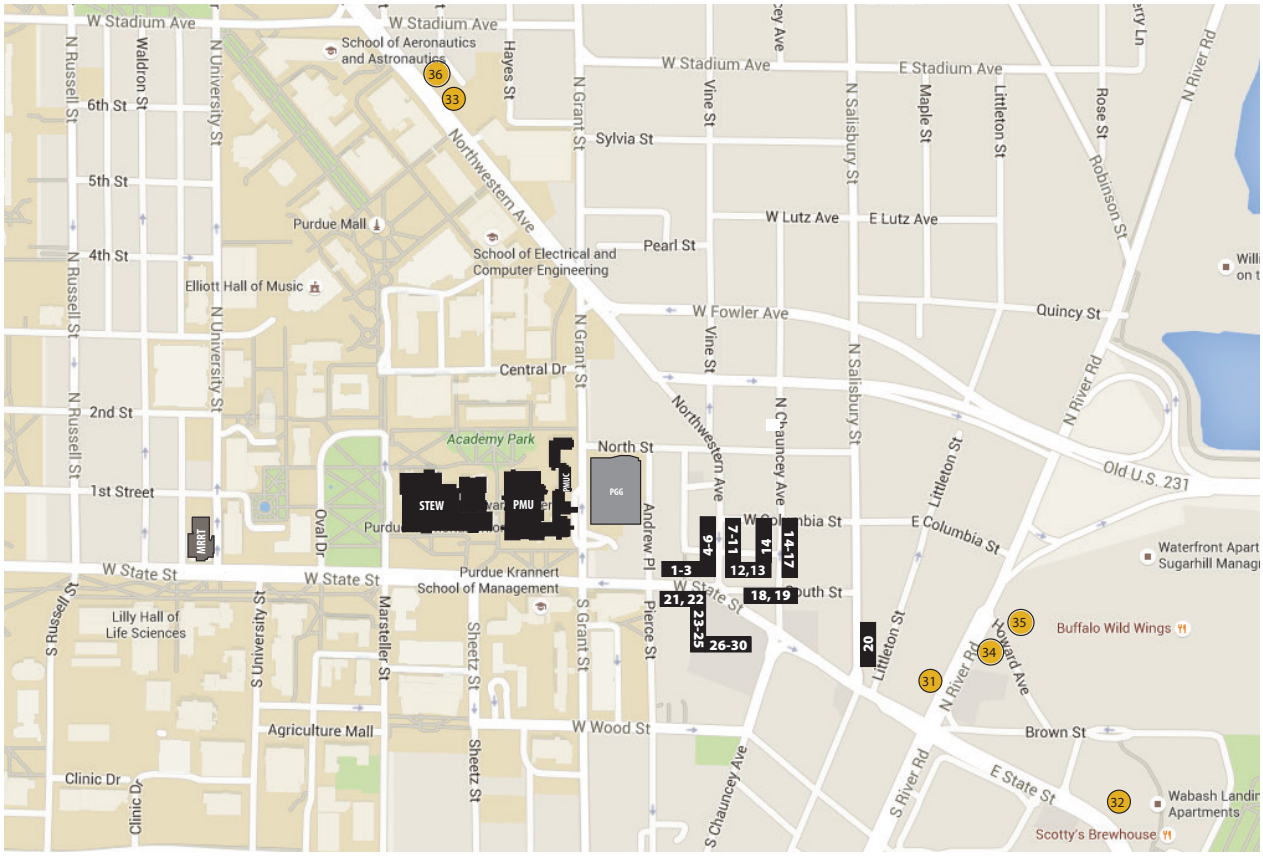
- Assured Identity and Privacy
- End System Security
- Human Centric Security
- Network Security
- Policy, Law and Management
- Prevention, Detection and Response

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.

LOCAL RESTAURANTS

Provided by Purdue Conferences



ON CAMPUS

PURDUE MEMORIAL UNION (PMU)

LOWER LEVEL
- **Flatbreads**
- **Freshëns**
- **La Salsa Fresh Mexican Grill**
- **Lemongrass**
- **Oasis Café**
- **Pappy's Sweet Shop**
- **Starbucks**
- **Urban Market**
- **Villa Fresh Italian Kitchen**

SECOND FLOOR
- **Sagamore Restaurant**

STEWART CENTER (STEW)
- **Newsstand**

MARRIOT HALL (MRRT)
- **Boiler Bistro**
- **Lavazza**

NEARBY

1. **Mad Mushroom**
2. **Brothers**
3. **Blue Nile**
4. **Potbelly Sandwiches**
5. **Qdoba Mexican**
6. **Einstein Bros. Bagels**
7. **Panda Express**
8. **Captain Gyro**
9. **Egyptian Café**
10. **Khana Khazana**
11. **Greyhouse Coffee Shop**
12. **Vienna Expresso Bar**
13. **Majé Sushi**
14. **Maru Sushi**
15. **Fiesta Mexican Grill**
16. **Red Mango**
17. **Noodles & Company**
18. **Chipotle**
19. **AJ's Burgers and Beef**
20. **Triple XXX**
21. **Harry's**
22. **Jimmy Johns**
23. **Hot Box Pizza**
24. **Jake's Roadhouse**
25. **Five Guys Burgers**
26. **Basil Thai & Bubble Tea**
27. **Subway**
28. **Tsunami**
29. **Taco Bell**
30. **Dairy Queen**
31. **Town & Gown Bistro**
32. **Moe's**
33. **Another Broken Egg**
34. **Nine Irish Brothers**
35. **La Hacienda Bar & Grill**
36. **Stacked Pickle**

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.