THE 2017 ANNUAL CERIAS INFORMATION SECURITY SYMPOSIUM

AGENDA

Monday, April 17

Time	Event	Room
6:30p	**Women in InfoSec Initiative (WI3) Presentation and Networking Event**	STEW 306
7:30p	**Remarks:** Wafaa Mamilli, VP Information Security & CISO, Eli Lilly and Company	STEW 306

Tuesday, April 18

8:30a	**Registration / Coffee**	STEW 302
9:00	**Welcome -** Ian Steff, Chief Innovation Officer and Exec. Vice President, Indiana Economic Development Corporation	STEW 302
9:30	**Day 1 Keynote -** Gen. Greg Touhill, (USAF Ret.), Former U.S. CISO	STEW 302
10:30	**Panel Discussion:** "Security Through Formal Methods and Secure Architecture"	STEW 302
11:30	**CERIAS TechTalk:** Rob Morton, Austin Klasa, and Daniel Sokoler "Making the Internet Fast Again...At The Cost of Security"	STEW 302
12:00p	**Lunch**	2nd Floor, FORD
1:30	**INSuRE Program Overview:** Mark Loepker, NSA	STEW 302
1:50	**Women in CyberSecurity Report:** Lynn Terwoerds, Executive Director, Executive Women's Forum	STEW 302
2:15	**Panel Discussion:** "Security Through Artificial Intelligence"	STEW 302
3:15	**Invited Talk:** Dr. Lok Yan, Air Force Research Lab, "What I learned from the DARPA CGC - Don't be afraid of the unknown"	STEW 302
4:00	**Poster Session Preview:** "Speed Dating Technology"	STEW 302
5:15	**Break for Dinner** (see page 37)	
6:30	**COAST 25th Anniversary Reception and CERIAS Poster Session**	PMU Ballroom
7:00	**CERIAS Awards Program and COAST Remarks:** Prof. Dongyan Xu and Prof. Eugene Spafford	PMU Ballroom
8:30	**End of Day 1**	

Wednesday, April 19

8:30a	**Registration / Coffee**	STEW 302
9:00	**Welcome**	STEW 302
9:15	**Day 2 Keynote:** David Meltzer, Chief Technology Officer, Tripwire	STEW 302
10:15	**Panel Discussion:** "Securing Vehicles & Machinery"	STEW 302
11:15	**CERIAS Tech Talk:** Prof. Mathias Payer - "Control-Flow Hijacking: Are we Making Progress?"	STEW 302
11:45	**Lunch**	2nd Floor, FORD
1:15p	**CERIAS TechTalk:** Prof. Shreyas Sundaram - "Towards Secure Large-Scale Networked Systems: Scalable Distributed Algorithms for Coordination in Networks under Attack"	STEW 302
1:45	**Cyber Security Fireside Chat:** Hosted by Professor Eugene Spafford	STEW 302
2:45	**CERIAS TechTalk:** Prof. Jeremiah Blocki - "Memory Hard Functions and Password Hashing"	STEW 302
3:15	**Panel Discussion -** "Securing Smart Communities"	STEW 302
4:30	**Closing Keynote:** Ron Ross, Fellow National Institute for Standards and Technology (NIST) "Pushing Computers to the Edge: Next Gen. Security and Privacy Controls for Systems and IoT Devices"	STEW 302
5:30	**End of Symposium**	

Thursday, April 20

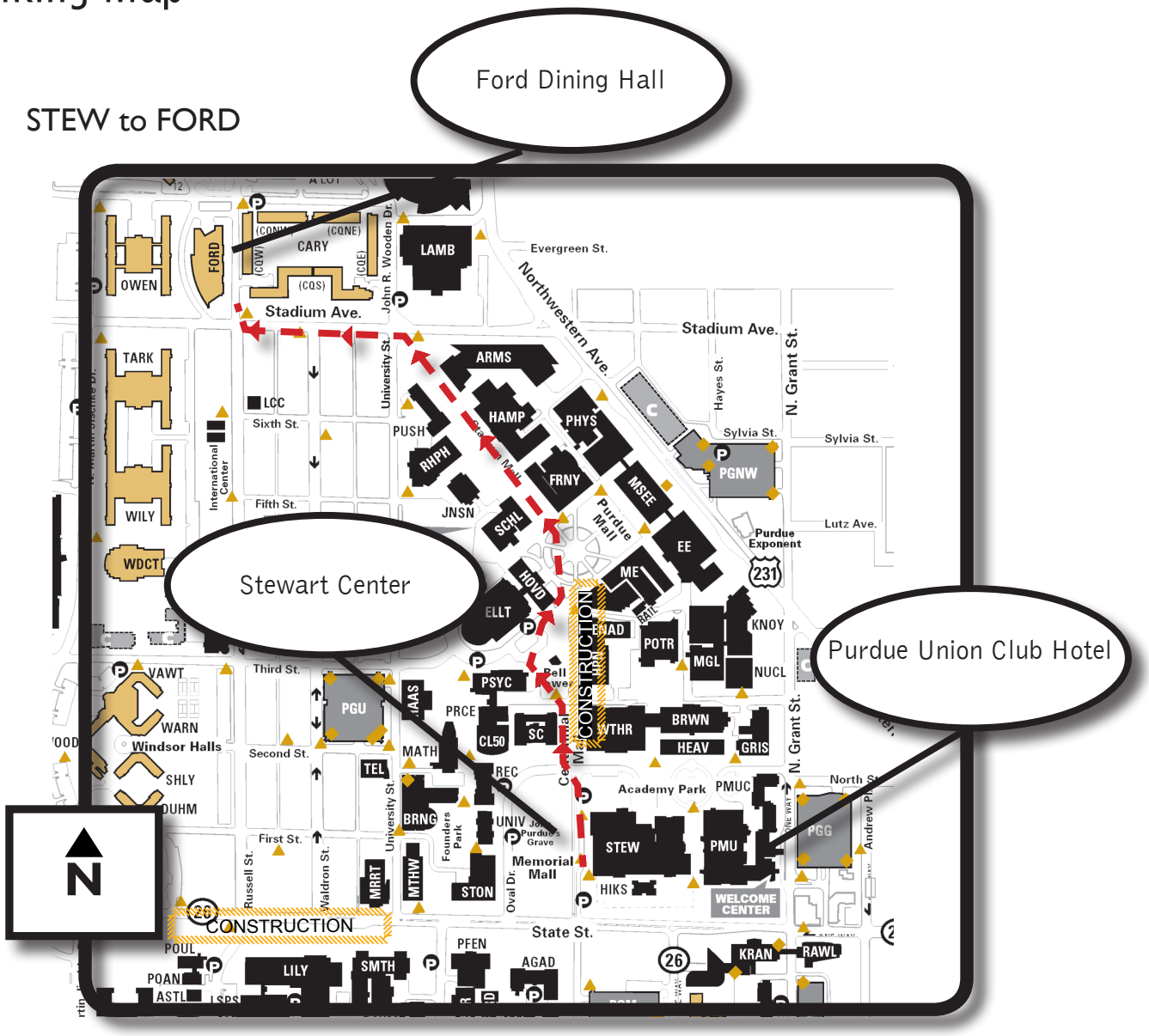
9:00a-5:00p	**CERIAS External Advisory Board Meeting** (For CERIAS Membership Delegates Only)	RAWLS 4013
1:00p-5:00p	**Security and Democracy Symposium:** We encourage all CERIAS Symposium attendees to also attend the Purdue Policy Research Institute's Security and Democracy Symposium. (see pg 12)	Dauch Alumni Center (DAUCH)

Save the Date!...Our next Symposium will be on April 3 & 4, 2018!

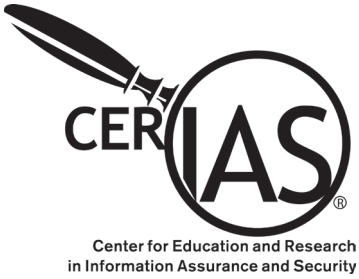
www.cerias.purdue.edu/symposium

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 2017

18th Annual Information Security Symposium * April 18-19

Table of Contents

Thanks to Our Strategic Partners

Analog Devices
Benedor TSE
Cyber Leadership Alliance
Citi
Deloitte
Eli Lilly and Company
Fidelity Investments
General Motors
IBM
Intel
Lockheed Martin
MITRE
Northrop Grumman
Raytheon
Rook Security
RSA, A Division of Dell Technologies
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

Symposium Supporter

Indiana Economic Development Corporation

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

Speaker & Panelist Bios

Welcome (Day 1)

Ian Steff
Chief Innovation Officer and Executive Vice President
State of Indiana/Indiana Economic Development Corporation (IEDC)

Ian Steff is responsible for coordinating the State of Indiana's innovation and entrepreneurship initiatives. Prior to joining the IEDC, Steff served as an executive officer and vice president of global policy and technology partnerships at the Semiconductor Industry Association in Washington, D.C. Steff is an advisor to a number of Indiana-based and industry-focused initiatives, serving on the Purdue University Dean of Engineering's Advisory Council, IUPUI Vice Chancellor for Research's Advisory Board, International Nanotechnology Conference on Communication and Cooperation program committee, BIC board of directors and IACMI board of directors.

Keynote (Day 1)

"Making the Business Case for Cybersecurity"

Greg Touhill
Brigadier General USAF (ret), Former U.S. Chief Information Security Officer

Greg Touhill is one of the nation's premier cybersecurity and information technology senior executives. A highly experienced leader of large, complex, diverse, and global operations, in 2016 Greg was selected by President Obama as the U.S. government's first Chief Information Security Officer. His other civilian government service includes duties as Deputy Assistant Secretary for Cybersecurity and Communications in the U.S. Department of Homeland Security and as Director of the National Cybersecurity and Communications Integration Center where he led national programs to protect the United States and its critical infrastructure. Greg is a retired Air Force general officer, a highly-decorated combat leader, an accomplished author and public speaker, a former American diplomat, and a senior executive with documented high levels of success on the battlefield and in the boardroom.

In this discussion General Greg Touhill will discuss "Making the Business Case for Cybersecurity" through lessons learned garnered during his military and civil service as well as his extensive industry engagements.

Keynote (Day 2)

David Meltzer
Chief Technology Officer, Tripwire

David Meltzer is a security industry pioneer bringing a unique blend of technical expertise, entrepreneurial skill and market vision to his current position as Tripwire's Chief Technology Officer. Meltzer joined Tripwire through its acquisition of nCircle, where he served as Chief Technology Officer and Vice President of Engineering. Immediately prior to joining nCircle, Meltzer was Founder and Chief Technology Officer at Cambia Security, where he pioneered the industry's first agentless configuration compliance auditing solution. A respected security researcher who founded the industry's first security vulnerability research group, the ISS X-Force, Meltzer is credited with the discovery of numerous security vulnerabilities.

Fireside Chat

Eugene Spafford
Executive Director Emeritus, CERIAS
Purdue University

Listen in while Eugene H. Spafford and invited security professionals chat about cyber security. Members of the audience will be able to suggest topics for conversation.

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.

Spaf (as he is known to his friends, colleagues, and students) is Executive Director Emeritus of the Purdue CERIAS (Center for Education and Research in Information Assurance and Security), and was the founder and director of the (superseded) COAST Laboratory.

Closing Keynote

Ron Ross
Fellow, at the National Institute for Standards and Technology (NIST)

"Pushing Computers to the Edge: Next Generation Security and Privacy Controls for Systems and IoT Devices"

Ron Ross is a Fellow at the National Institute of Standards and Technology. His focus areas include information security, systems security engineering, and risk management. Dr. Ross leads the Federal Information Security Modernization Act (FISMA) Implementation Project, which includes the development of security standards and guidelines for the federal government, contractors, and the United States critical infrastructure.

Join us as we Celebrate 25 years of Cyber Security Research at Purdue University!

Tuesday Night 6:30pm - PMU Ballroom

COAST 25th Anniversary Reception and CERIAS Poster Session

CERIAS boasts an impressive beginning with roots in a research group established in the Computer Sciences Department at Purdue University in 1991. Created out of the research of professors Eugene Spafford and Samuel Wagstaff, Jr., the small research team investigated issues of computer and network security. Through initial funding from Sun Microsystems, Schlumberger, Bell Northern Research (BNR, now NorTel), and Hughes Laboratories, COAST (Computer Operations, Audit and Security Technologies) was officially born.

The growth and success of COAST became a catalyst for greater interest and attention from industry, especially those seeking a platform from which o explore comprehensive solutions to security questions. The laboratory model gave way to a superior multidisciplinary and holistic approach to researching and transferring information that has become the basis for the CERIAS initiative and the origin for many respected achievements in both academia and business.

Panel #1: Security Through Formal Methods and Secure Architecture

"If you build it (securely) they will come"

Some scientists argue that the only way to get more secure systems is to use rigorous, formal methods of specification and implementation. Despite nearly 40 years of R&D, we have only some tools and results from these methods. However, the systems we have thus obtained have been highly trustworthy and used in aerospace, nuclear power, and national intelligence. The panel participants will attempt to specify the benefits and challenges in this domain, and prove it is worth pursuing.

Saurabh Bagchi - Moderator
Professor, Electrical and Computer Engineering & CERIAS Fellow
Purdue University

Saurabh Bagchi is an ACM Distinguished Scientist (2013), a Senior Member of IEEE (2007) and ACM (2009), a Distinguished Speaker for ACM (2012), and an IMPACT Faculty Fellow at Purdue. He is also the Cyber lead for the GE-funded PRIAM center at Purdue ($10M, 2015-20) and was the Cybersecurity Lead for the NSF Center at Purdue called NEEScomm ($25M, 2010-15). His research interests include: reliable and secure software systems, dependable distributed systems, network security, reliable high performance computing embedded wireless networks, and scalable bioinformatics software. Dr. Bagchi is a fellow of CERIAS.

Ben Delaware
Assistant Professor, Computer Science
Purdue University

Professor Delaware's research focuses on the design and implementation of programming languages and the development of tools that provide higher assurance with lower effort through the use of mechanized theorem provers. He received his Ph.D. in Computer Science from the University of Texas at Austin in 2013 under the direction of William Cook. Dr. Delaware then spent two years as a Research Scientist in the Programming Languages & Verification Group at MIT.

Roopsha Samanta
Assistant Professor, Computer Science
Purdue University

Roopsha Samanta's research interests are in formal methods and programming languages. Her work spans the development of mathematical theory and tools for program verification, analysis, repair and synthesis. Her current research focuses on synchronization synthesis for concurrent programs, robustness analysis of cyberphysical and reactive systems and automated feedback generation for online education.

Vince Urias
Principal Member, Technical Staff
Sandia National Labs

Vincent Urias is a computer engineer, and Principal Member of Technical Staff in Sandia's Cyber Analysis Research Development Department continuing to make major contributions to Sandia's cyber defense programs, especially in the simulation of complex networks, in developing innovative cyber security methods, and in designing exercise scenarios that test the limits of current network security. This work is helping Sandia's customers anticipate current and emerging security threats and make critical decisions about their investments.

Matt Wilding
Principal Engineering Manager
Rockwell Collins

Dr. Matthew Wilding is a Principal Research Group Manager in the Rockwell Collins Advanced Technology Center. Dr. Wilding received a PhD in Computer Sciences from The University of Texas at Austin and joined Rockwell Collins in 1996. He has worked on many high confidence efforts, such as the machine-checked formal methods analysis of the AAMP7 microprocessor critical to several Rockwell Collins products. Dr. Wilding currently leads the Trusted Systems research group, which collaborates with Rockwell Collins product areas and government research sponsors to develop and apply automated verification methods to complex embedded systems.

Panel #2: Security Through Artificial Intelligence

"Open the pod bay doors, HAL"

There is currently a great deal of "buzz" around AI methods and systems. "Smart" and "self healing" systems are supposedly right around the corner. What does it mean for security when we have systems that draw conclusions and make decisions without explicit human approval? Will we have trustworthy system, or are we building SkyNet and Ultron?

Rob Hale
Fellow, Information Assurance/Information Operations
Lockheed Martin

Rob is a Lockheed Martin Fellow with over 30 years of experience in information operations and cyber security. In his current role, he is leading advanced research and development activities in hardware-enforced embedded security, malware reverse engineering, and information weaponization. He also leads Lockheed's Cyber Foundational Technology Thread effort and is co-developing the Embedded Cyber strategy for Lockheed Martin.

Ravi Srinivasan
Vice President
IBM Security

Ravi leads the IBM Security Information Risk and Protection strategy and offering management, driving the investments and roadmap for Identity, Access, Data, Application, Cloud, Mobile and Advanced Fraud Prevention. Ravi meets and consults with senior executives, lines of business owners and IT leaders around the world on their key cyber security risk, governance and compliance initiatives. He's also a frequent speaker at trade, analyst conferences and customer events to share a worldwide customer perspective and insights on secure mobile, cloud and social business transformations. Prior to joining IBM in 2006, Ravi held several product management, marketing and development roles at Synopsys and Texas Instruments. Ravi lives in Austin, TX.

Julia Taylor Rayz
Associate Professor, Computer and Information Technology & CERIAS Fellow
Purdue University

Julia Taylor Rayz is an Associate Professor in Computer and Information Technology and CERIAS Fellow. Her primary research interests lie in natural language understanding, knowledge discovery and representation, and computational recognition of salient information in texts, as well as in uncertainty management.

Chet Wisniewski
Principal Research Scientist
Sophos

Chester Wisniewski has been involved in the information security space since the late 1980s. He is currently a Principal Research Scientist in the Office of the CTO. Chet divides his time between research, public speaking, writing and attempting to communicate the complexities of security to the press and public in a way they can understand.

Chester has spoken at RSA, InfoSec Europe, LISA, USENIX, Virus Bulletin and many Security BSides events around the world in addition to regularly consulting with NPR, CNN, CBC, The New York Times and other media outlets.

Panel #3: Securing Vehicles & Machinery

"Planes, Trains, and Automobiles"

We are placing more and more reliance on computing in transportation — to increase efficiency, reduce accidents, and enable greater utilization of scarce resources. Whether it is computer guidance, fly by wire controls, or self-driving vehicles, we seem to be on course to have computers in the loop, if not in control. But do we really know where we are headed? What are the roadblocks and potholes on the way? Will we be Driving Miss Daisy or putting her on the Highway to Hell?

Dongyan Xu - Moderator
Professor, Computer Science,
CERIAS Fellow, & Interim Director of CERIAS
Purdue University

Professor Xu currently serves as the Interim Director of CERIAS, Purdue's cybersecurity research center. His research focuses on the development of virtualization technologies for computer system security and for cloud computing.

Susan Gottschlich
Senior Fellow
Raytheon

Susan Gottschlich is a Senior Engineering Fellow with Raytheon Space and Airborne Systems. While at Raytheon, Susan has been the principle investigator or a technical lead on many command, control, communications and intelligence contract research and development programs and production programs. She has also held the role of Corporate Technology Area Director for Information Systems and Computing which included technology oversight of Raytheon's cybersecurity portfolio. She is currently working on architectural studies for next generation military platforms. Prior to joining Raytheon, Susan has worked for S&T companies, COTS companies, start ups and as an Assistant Professor with the ECSE Department at RPI. Susan has a B.S. in Computer and Electrical Engineering and an M.S. and Ph.D. in Electrical Engineering, all from Purdue University.

Michael Imel
Group Manager of Autonomous Product Cybersecurity
General Motors

Michael is a graduate of Purdue University w/ a BS degree in Electrical Engineering. Since graduation Michael has held a wide variety of positions at General Motors. Michael has worked in Vehicle Manufacturing supporting End of Line test systems. In Product Engineering Michael worked on service and manufacturability of the Chevrolet Volt and other hybrid programs then later in chassis controls software for multiple programs. Currently in Product Cybersecurity, Michael leads a team of engineers tasked with the responsibility of securing and hardening all aspects of the Autonomous Vehicle.

Brandon Pitts
Assistant Professor, Industrial Engineering
Purdue University

Dr. Brandon Pitts is an Assistant Professor in the School of Industrial Engineering and a Faculty Associate with the Center on Aging and the Life Course (CALC) at Purdue University. He received a B.S. in Industrial Engineering from Louisiana State University, and both a M.S.E and Ph.D. in Industrial and Operations Engineering from the University of Michigan in Ann Arbor. His research interests include cognitive ergonomics, human-automation interaction, multimodal and adaptive displays, and gerontechnology. Dr. Pitts is also a registered Engineer Intern (E.I.T.) with the state of Louisiana.

Charles Timko
R&D Cybersecurity Engineer
Analog Devices Inc.

Charles Timko is a Senior Security Design Engineer at Analog, where he is actively working on automotive security assessments. He has previously worked in both the financial and defense sectors.
He was part of the Battelle Cyber Automotive Challenge, where his team reverse engineered automotive platforms in a 24-hour time-period. Charles is a graduate of Purdue University and a Certified Ethical Hacker.

Panel #4: Securing Smart Communities

"E.P.C.O.T will be an experimental prototype community of tomorrow"

As part of the increasing ubiquity of computing, we are putting sensors, communication, and computation into our buildings, our roads, our vehicles, and our very infrastructure. If all of these items work together well, we have some opportunities to increase our security, make our living spaces more comfortable, and optimize resource use. However, the potential for problems if these systems fail or are hacked could be catastrophic. The potential loss of privacy is also a concern. This panel will look at some of the promise — and perils — that "smart communities" might bring about.

Richard Voyles - Moderator
Professor, Engineering Technology
Purdue University

Head of the Collaborative Robotics Lab at Purdue and Director of the Robotics Accelerator, Prof. Voyles knows robots! With expertise in electrical engineering, mechanical engineering and computer science, Dr. Voyles' research interest include novel robotic mechanisms, sensors, self-adaptive software, real-time control, and gesture-based human/robot interaction.

Anupam Chattopadhyay
Asst. Prof., Computer Science & Engineering
Nanyang Technological University, Singapore

Anupam Chattopadhyay received his B.E. degree from Jadavpur University, India in 2000. He received his MSc. from ALaRI, Switzerland and PhD from RWTH Aachen in 2002 and 2008 respectively. From 2008 to 2009, he worked as a Member of Consulting Staff in CoWare R&D, Noida, India. From 2010 to 2014, he led the MPSoC Architectures Research Group in RWTH Aachen, Germany as a Junior Professor. Since September, 2014, he is appointed as an assistant Professor in SCE, NTU.

Denise Lee
Associate Director & City Solution Leader
Deloitte & Touche LLP

Denise Lee previously served as the Deloitte Africa Smart Cities & Emerging Technologies Leader, having recently relocated to Deloitte & Touche LLP in the United States. Denise has over 20 years of experience working with various multinational clients across Africa, Europe, the Middle East and the United States in the public and private sectors. She specializes in licensing & intellectual property, eCitizen Solutions, ubiquitous connectivity, Smart Data Governance, and Big Data Analytics in SMART Cities.

Robert Lentz
President & CEO
Cyber Security Strategies

Robert Lentz is currently president of Cyber Security Strategies. Mr. Lentz is one of the world's foremost strategic leaders in Internet Security having received numerous accolades both in the U.S government and globally. He recently was on the prestigious nominating committee for the Cyber Security Hall of Fame and is a sought after speaker, advisor and mentor. He served in the Clinton, Bush and Obama Administrations and was in the Pentagon on 9-11. He was the first Deputy Assistant Secretary of Defense for cyber security, where he was on the President's National Security Committee and was instrumental in steering DoD's move to securely operating in the Internet era.

Ninghui Li
Professor,Computer Science & CERIAS Fellow
Purdue University

Ninghui Li is a Professor of Computer Science. His research interests are in security and privacy. He is Vice Chair of ACM Special Interest Group on Security, Audit and Control (SIGSAC), (2013--present). He is on the editorial boards of IEEE Transactions on Dependable and Secure Computing (TDSC), Journal of Computer Security (JCS), and ACM Transactions on Internet Technology (TOIT); and was on the editorial board of the VLDB Journal from 2007 to 2013.

CERIAS TechTalk

Rob Morton, Austin Klasa, and Daniel Sokoler
Purdue University

"Making the Internet Fast Again...At The Cost of Security"

There is a relatively new suite of performance improving communication protocols being broadly adopted on the Internet such as SPDY, HTTP/2 and QUIC. These protocols are being rapidly implemented to improve the performance of the Internet. More than 10% of the top 1 Million websites are already using some of these technologies, including much of the 10 highest traffic sites. In this talk, we will look specifically at a vulnerability in Google's QUIC (Quick UDP Internet Connections, pronounced quick) protocol. QUIC is used in all Google services and exclusively in Chrome with over 1 billion monthly users using QUIC worldwide. Specifically, we will highlight over optimization in QUIC's implementation of AES-GCM exposing the length for messages under 300 bytes. We take this vulnerability in QUIC and apply it to build a plausible online attack against the largest free, e-mail provider.

Robert Morton is a current PhD student in Information Security with over a decade of experience advising the President of the United States, the National Security Council, senior policymakers, and industry executives. Prior to his government service, Mr. Morton worked for Ernst & Young (E&Y) and helped advise Fortune 100 executives on cyber security threats and separately performed security reviews of their global IT infrastructure.

Daniel Sokoler is an undergraduate at Purdue University studying Computer Science with a focus in Computer Security and a Certificate in Entrepreneurship and Innovation. He has experience with vulnerability analysis for the purpose of determining the security of commercial products and automating software security analyses, and is well-versed using Python, C, and Java. Dan participated in INSuRE this previous spring working on "The Impact of Known Vulnerabilities in Layered Solutions".

Austin Klasa is an undergraduate studying Computer Science at Purdue University. Austin has previously participated in INSuRE projects outside of the traditional course. He worked on the Daedalus software tool for evaluating public cloud providers with a risk model and conducted research on password coping mechanisms. His primary programming experience has included Java, C, and Python programming. Austin's primary interest and passion is in the field of computer security.

INSuRE Program Overview

Mark Loepker
NSA

The INSuRE project is a CERIAS initiated project of four successful university Centers of Academic Excellence in Information Assurance Research (CAE-R), the National Security Agency (NSA), the Department of Homeland Security and other federal agencies. The project is a cooperative, multi-disciplinary, multi-institutional, and multi-level collaborative research project framework that can be utilized for both unclassified and classified cybersecurity research.

INSuRE provides students an opportunity to work on real-world problems with mentoring (non-academic) practitioners, and academic researchers from multiple institutions. The individual student-led research projects often address issues of pressing national concern.

To facilitate scientific discovery, learning, and collaboration, INSuRE uses the Purdue developed HUBzero®; an open source, content management platform built to support scientific activities.The Purdue University Research Repository (PURR) is employed to facilitate interaction between student teams and technical advisors at sponsor institutions, and to publish data and tools developed as part of individual INSuRE student projects.

Women in CyberSecurity Report

Lynn Terwoerds
Executive Director
Executive Women's Forum

Lynn Terwoerds is the Executive Director of the Executive Women's Forum on Information Security, Risk Management and Privacy (EWF). Lynn plays a key role in the strategic development of the EWF as well as the creation and content of EWF events and initiatives. Lynn also founded the EWF Voice Privacy Alliance to provide industry with usable security and privacy guidance for voice enabled technology. Lynn has more than 23 years' experience in information systems, over half of which has been in information security. She has worked both as a practitioner and a vendor – She was the director of information security risk for Oracle's Health Sciences Global Business Unit and formerly was 10 years at Microsoft corporate headquarters in security response, then critical infrastructure protection as a security strategist, and a director of software compliance. She was also Head of Security Architecture, Standards and Infrastructure Engineering for Barclays Bank. Her previous experience includes working as a solution integrator and consultant to large corporations. She is a founding member of the Cloud Security Alliance. She holds a CISSP and MA from the University of Missouri-Columbia.

Invited Talk

Lok Yan
Air Force Research Lab

"What I Learned from the DARPA CGC - Don't be Afraid of the Unknown"

Being an applied researcher is hard. We are not only faced with theoretical challenges but also practical ones when we try to apply novel concepts into real world systems. Some call the latter work "engineering" and its contributions are often valued less.

My experience working in the DARPA Cyber Grand Challenge infrastructure team has taught me that engineering is never just engineering. It can be intellectually challenging, it can be invigorating, and in computer security it is indispensable.

I will share these lessons learned with you in this talk. The talk will be in the context of CGC Qualification Event challenge sets that were designed to differentiate human participants from machines. Despite the "engineering" nature of the work, the experience has been enlightening and rewarding

Dr. Lok is a senior computer engineer at the Air Force Research Laboratory. His main research focus is in program analysis and bridging the arbitrary hardware, software and physical divides. He received his PhD from Syracuse University.

CERIAS TechTalk

Mathias Payer
Assistant Professor, Computer Science
Purdue University

"Control-Flow Hijacking: Are We Making Progress?"

Memory corruption errors in C/C++ programs remain the most common source of security vulnerabilities in today's systems. Over the last 10+ years we have deployed several defenses. Data Execution Prevention (DEP) protects against code injection – eradicating this attack vector. Yet, control-flow hijacking and code reuse remain challenging despite wide deployment of Address Space Layout Randomization (ASLR) and stack canaries. These defenses are probabilistic and rely on information hiding.

The deployed defenses complicate attacks, yet control-flow hijack attacks (redirecting execution to a location that would not be reached in a benign execution) are still prevalent. Attacks reuse existing gadgets (short sequences of code), often leveraging information disclosures to learn the location of the desired gadgets. Strong defense mechanisms have not yet been widely deployed due to (i) the time it takes to roll out a security mechanism, (ii) incompatibility with specific features, and (iii) performance overhead. In the meantime, only a set of low-overhead but incomplete mitigations has been deployed in practice.

Control-Flow Integrity (CFI) and Code-Pointer Integrity (CPI) are two promising upcoming defense mechanisms, protecting against control-flow hijacking. CFI guarantees that the runtime control flow follows the statically determined control-flow graph. An attacker may reuse any of the valid transitions at any control-flow transfer. We compare a broad range of CFI mechanisms using a unified nomenclature based on (i) a qualitative discussion of the conceptual security guarantees, (ii) a quantitative security evaluation, and (iii) an empirical evaluation of their performance in the same test environment. For each mechanism, we evaluate (i) protected types of control-flow transfers, (ii) the precision of the protection for forward and backward edges. For open-source compiler-based implementations, we additionally evaluate (iii) the generated equivalence classes and target sets, and (iv) the runtime performance. CPI on the other hand is a dynamic property that enforces selective memory safety through bounds checks for code pointers by separating code pointers from regular data.

CERIAS TechTalk

Shreyas Sundaram
Assistant Professor, Electrical and Computer Engineering
Purdue University

"Towards Secure Large-Scale Networked Systems: Scalable Distributed Algorithms for Coordination in Networks under Attacks"

Large-scale networked systems (such as the smart grid, robotic swarms, and smart cities) consist of a large number of interconnected components. To allow the entire system to function efficiently, these components must communicate with each other and use the exchanged information in order to take globally optimal actions. However, such large-scale networked systems are also increasingly under threat from sophisticated cyber-attacks that can compromise some of the components and cause them to behave erratically or inject malicious information into the network.

In this talk, I describe a class of scalable distributed coordination algorithms that are resilient to malicious behavior by nodes in large-scale networks. These algorithms do not require the nodes to know anything about the network other than their own neighbors, and rely on simple rules that allow information to diffuse through the network over time. Furthermore, these algorithms guarantee resilience to a potentially massive number of malicious nodes in the network, under appropriate conditions on the network topology. In turn, this leads to new insights into metrics and design principles for resilient large-scale networks.

CERIAS TechTalk

Jeremiah M. Blocki
Assistant Professor, Computer Science
Purdue University

"Memory Hard Functions and Password Hashings"

In the last few years breaches at organizations like Yahoo!, Dropbox, Lastpass, AshleyMadison and Adult FriendFinder have exposed over a billion user passwords to offline attacks. Password hashing algorithms are a critical last line of defense against an offline attacker who has stolen password hash values from an authentication server. A attacker who has stolen a user's password hash value can attempt to crack each user's password offline by comparing the hashes of likely password guesses with the stolen hash value. A good password hashing algorithm should have the property that it is feasible to compute the function quickly (e.g., 0.5 seconds) on a personal computer, but it should be economically infeasible for an offline attacker to check millions (or billions) of password guesses.

Memory hard functions (MHFs), first explicitly introduced by Percival, are a promising key-stretching tool for password hashing because the cost of storing/retrieving items from memory is relatively constant across different computer architectures. Thus, in contrast to standard cryptographic hash functions (e.g., SHA256) the cost of computing an MHF cannot be significantly reduced by developing customized hardware (ASICs). More specifically, we want to ensure that any circuit evaluating multiple instances of the MHF has high amortized AT-complexity --- Area X Time/#instances. Data-Independent Memory Hard Functions (iMHFs) are an important variant of MHFs due to their greater resistance to side-channel attacks. An iMHF can be specified by a directed acyclic G specifying data-dependencies during computation. Due to the recently completed Password Hashing Competition we have many candidate iMHFs, but many of these iMHFs had not been analyzed until recently.

This talk will summarize recent results demonstrating that a combinatorial property called depth-robustness fully characterizes iMHFs with high amortized-AT complexity. We will also show that Argon2i, the winner of the password hashing competition, is defined using a directed acyclic graph G that is not depth-robust. The resulting attacks are practical for realistic settings of the Argon2i parameters. We will also discuss recent progress towards the development of a practical iMHF with provably high AT-complexity.

Special Event

We encourage all CERIAS Symposium attendees to also attend the Purdue Policy Research Institute's Security and Democracy Symposium.

Security and Democracy Forum

April 20 @ 1:00 PM - 5:00 PM (Reception to follow.) - Dauch Alumni Center

Security, whether narrowly or broadly drawn, is increasingly seen as being in conflict with the rights and freedoms characteristic of democratic societies. In response to threats of terror, many observers suggest, we should surrender some of our civil liberties, give government more access to private information, and restrict the press from its tendency towards openness that terrorists inevitably exploit. Others suggest that such restrictions are not necessary, and do not make us safer, sacrificing democratic values for an elusive security we cannot attain, and making government more intrusive in our lives in a way that will be difficult to change later.

Technological developments bring these questions into ever sharper relief. Technology is seen by many as offering greater security, as drones replace dangerous and dirty jobs, and Big Data offers new ways of identifying and tracking potential threats. At the same time, drones raise new questions about privacy and security in both military and non-military applications with cyber warfare; attacks raise new questions of personal and national security, and the global media is proving easier for terrorists to access even as it grows more difficult to regulate.

This symposium brings industry leaders and policymakers who have confronted these questions of security and democracy together with Purdue researchers whose research raises, and answers, these pressing questions.

Poster Session Abstracts

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. Differentially Private Heavy Hitter Problem

Tianhao Wang, Ninghui Li, Somesh Jha

Protocols satisfying Local Differential Privacy (LDP) enable parties to collect aggregate information about a population while protecting each user's privacy, without relying on a trusted third party. LDP protocols (such as Google's RAPPOR) have been deployed in real-world scenarios. In these protocols, a user encodes his private information and perturbs the encoded value locally before sending it to an aggregator, who combines values that users contribute to infer statistics about the population. In this paper, we introduce a framework that generalizes several LDP protocols proposed in the literature. Our framework yields a simple and fast aggregation algorithm, whose accuracy can be precisely analyzed. Our in-depth analysis enables us to choose optimal parameters, resulting in two new protocols (i.e., Optimized Unary Encoding and Optimized Local Hashing) that provide better utility than protocols previously proposed. We present precise conditions for when each proposed protocol should be used, and perform experiments that demonstrate the advantage of our proposed protocols.

2. Finding Ransomware Encryption Keys in Volatile Memory

Joseph Graham

Ransomware is malware that encrypts files on the target computer. Ransomware has become more prominent over the years causing problems for both consumers and businesses. Ransomware is extremely hard to recover from on a target computer if there is no backup seeing as how it encrypts most files on the user's computer. The purpose of this poster is to investigate ransomware and see if the encryption keys for the ransomware can be found in volatile memory allowing the files to become decrypted and recovered without paying the ransom or needing a backup.

3. Forgetting the Forgotten with Letheia: Concealing Content Deletions in Presence of Persistent Observers

Mohsen Minaei, Mainack Mandal, Patrick Loiseau, Krishna Gummadi, Aniket Kate

Today most people are susceptible to oversharing their personal information publicly on social platforms. As a coping strategy, most platforms offer mechanisms allowing users to withdraw their posts. In fact a significant fraction of users exercise this right to be forgotten. However, these withdrawals leave users more vulnerable to privacy attacks: due to the now popular ``Streisand effect," users' attempt to reduce attention to sensitive posts by withdrawing those, can, in practice, attract unwanted attention to the posts from others (including curious friends, cyberstalking and even blackmailers). Therefore, users hoping to forget their posts are left with a ``damned if I do, damned if I don't" dilemma. In the form of intermittent withdrawal mechanism, we propose a rather disruptive solution to this catch-22 problem. If the social platforms are willing to give up the uninterrupted availability of non-withdrawn posts, it is possible to provide a privacy guarantee to the withdrawn posts. Here, an adversarial observer becomes unsure if some post is permanently withdrawn or just

temporarily unavailable for some duration, and at the same time overwhelmed by a large number of falsely flagged undeleted posts. We analyze large scale data about users' deletion patterns over Twitter and thoroughly investigate how to choose probability distributions for alternating temporary withdrawals and resurrections of non-withdrawn posts. We report the trade-off between privacy, utility and adversarial overhead in our proposed design under different settings.

4. Fulgor: Concurrent and Privacy Preserving Transactions with Payment-Channel Networks

Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, Srivatsan Ravi

Blockchain payment protocols based on global consensus such as Bitcoin are inherently limited in transaction throughput and latency. Current efforts to address this key issue focus on off-chain payment channels that can be combined in a Payment-Channel Network (PCN) that enables an unlimited number of payments and requires access to the blockchain only to register the initial and final capacity of each channel. While this approach paves the way for low latency and high throughput of payments, its deployment in practice raises several privacy issues, which have been understudied so far. In this work, we lay the foundations for privacy in PCN, presenting a definitional framework as well as a practical and provably secure enforcement solution. In particular, we present Fulgor, the first payment protocol for PCNs that provides provable privacy guarantees. We have implemented Fulgor and showed that it allows privacy preserving payments in less than 1 second, thereby demonstrating its feasibility in practice. Finally, we formally study for the first time how to handle concurrent payments in a non-blocking manner while maintaining the decentralized nature of PCNs.

5. Information Leakage in a Cisco VPN Stream

Austin Klasa and Daniel Sokoler

Making the Internet Fast Again…At The Cost of Security There is a relatively new suite of performance improving communication protocols being broadly adopted on the Internet such as SPDY, HTTP/2 and QUIC. These protocols are being rapidly implemented to improve the performance of the Internet. More than 10% of the top 1 Million websites are already using some of these technologies, including much of the 10 highest traffic sites. In this talk, we will look specifically at a vulnerability in Google's QUIC (Quick UDP Internet Connections, pronounced quick) protocol. QUIC is used in all Google services and exclusively in Chrome with over 1 billion monthly users using QUIC worldwide. Specifically, we will highlight over optimization in QUIC's implementation of AES-GCM exposing the length for messages under 300 bytes. We take this vulnerability in QUIC and apply it to build a plausible online attack against the largest free, e-mail provider.

6. INSuRE Training Course Effect on Students' Research Self-efficacy

Rylan Chong, Dr. Melissa Dark, Dr. John Springer

This pilot study investigated the effect of the Information Security Research and Education (INSuRE) course on students' research self-efficacy. Unlike traditional courses, students in the INSuRE course worked on real unclassified government cybersecurity research problems with a team, a mentor, and a network of experts. This pilot study included 17 college students from eight Centers of Academic Excellence in Cyber Defense Research (CAE-R) universities that responded to pre- and post-surveys that measured their research self-efficacy using a 100-point Likert scale. A nonparametric Wilcoxon Test was used, and found both male and female students' research self-efficacy improved.

7. Just In Time Hashing

Benjamin Harsha and Jeremiah Blocki

We propose a new mode of operation for cryptographic hashing functions that we call Just In Time hashing. This method, which is designed with password hashing in mind, begins computation the moment a user starts typing rather than the moment they stop. This allows for additional computation time without the user being aware of any delay. We also discuss how an adversary would approach running an offline attack on passwords stored in this way, and discuss how it interacts with memory hard functions.

8. Permissions Displays for Android Apps

Scott Moore, Huangyi Ge, Dr. Robert Proctor, Dr. Ninghui Li

Smart mobile devices have become very common but there are risks associated with using these devices. Android has developed different methods for communicating risk information to the user. This research contributes to effective risk communication for mobile devices. We administered a survey to participants asking them to do a rating task on 16 statements regarding Android 5.0, Android 6.0, and a general comparison between the two. Users indicated that they want more control over which permissions gain access to their phone, but they seldom use that control when given the opportunity. Users were more knowledgeable about the features of Android 6.0, and Android 6.0 was more intuitive by comparison. Open-ended user comments revealed that people frequently do not read permissions, or they use alternative methods to decide whether to accept the risk of downloading an app. A follow-up study is currently being conducted to test the survey's results in an experimental setting, specifically the likability and effectiveness of each version.

9. Public-Key Authentication Using Dessins d'Enfants

Jacob Bond

A dessin d'enfant, French for "child's drawing", is a bipartite graph which has an associated rational function. Using the asymmetry between computing the function from the graph and computing the graph from the function, a public-key authentication protocol is proposed. The protocol was designed with considerations for resource-constrained devices.

10. Secure Distributed State Estimation for Large-Scale Systems

Aritra Mitra and Shreyas Sundaram

Real-time monitoring of large-scale complex systems such as power grids, gas and steam turbines, and air-traffic management systems is typically achieved by collecting and analyzing real-time plant data from sensors distributed over a communication network. Failures in such sensors can have catastrophic effects, especially in safety-critical systems. Consequently, securing these sensors against adversarial attacks (in the form of false data injections, denial of service attacks etc.) is a challenging and important problem. To this end, we develop a secure, lightweight, distributed algorithm for asymptotically reconstructing the state dynamics of an LTI system at each sensor node of a given network, in the face of worst-case adversarial attacks on some of the sensors. We also provide provable guarantees regarding the success of our proposed algorithm and characterize network topologies that facilitate our strategy. Our state estimation scheme provides fundamental insights into the connection between the plant dynamics, the sensor measurement structures and the underlying communication network topologies, and is expected to significantly enhance real-time data analytics.

11. SmartNDA: Realizing Unilateral Non Disclosure Agreements using a Bitcoin Penalty

Easwar Vivek Mangipudi. Krutarth Rao, Aniket Kate

We study the problem of realizing a unilateral Non Dis- closure Agreement (NDA) in a two user Sender-Receiver setting where the trust between the two users is enforced using a Bitcoin smart contract. The NDA is time-bound and any dishonesty on the part of the receiver, by reveal- ing the non-disclosable document, is penalized through the loss of Bitcoins. A watermarked version of the docu- ment is transferred to the receiver, who during the proto- col, uses his Signing-Key to obtain the document. In case of a dishonest disclosure of the document by the receiver, the receiver's signing key gets revealed to the sender who has access to the revealed document. The obtained sign- ing key is used by the sender to penalize the receiver by transferring the funds from a previously committed Time- Locked Bitcoin Deposit. In this work, we design a pro- tocol named SmartNDA which realizes the solution and analyze it by studying the different modules necessary for its implementation. We proceed to argue the security of the protocol in-terms of Universal Composability and then report the results of the implementation of the pro- tocol. From the performance evaluation, we observe that the designed protocol is easy to deploy and fast to run.

12. Statistical Learning Theory Approach for Data Classification with l-diversity

Koray Mancuhan and Chris Clifton

Corporations are retaining ever-larger corpuses of personal data; the frequency or breaches and corresponding privacy impact have been rising accordingly. One way to mitigate this risk is through use of anonymized data, limiting the exposure of individual data to only where it is absolutely needed. This would seem particularly appropriate for data mining, where the goal is generalizable knowledge rather than data on specific individuals. In practice, corporate data miners often insist on original data, for fear that they might "miss something" with anonymized or differentially private approaches. This paper provides a theoretical justification for the use of anonymized data. Specially, we show that a support vector classifier trained on anatomized data satisfying l-diversity should be expected to do as well as on the original data. Anatomy preserves all data values, but introduces uncertainty in the mapping between identifying and sensitive values, thus satisfying l-diversity. The theoretical effectiveness of the proposed approach is validated using several publicly available datasets, showing that we outperform the state of the art for support vector classification using training data protected by k-anonymity, and are comparable to learning on the original data.

END SYSTEM SECURITY

13. An MTD-based Self-Adaptive Resilience Approach for Cloud Systems

Miguel Villarreal-Vasquez, Pelin Angin, Norman Ahmed and Bharat Bhargava

Advances in cloud computing have made it a feasible and cost-effective solution to improve the resiliency of enterprise systems. However, the replication approach taken by cloud computing to provide resiliency leads to an increase in the number of ways an attacker can exploit or penetrate the systems. This calls for designing cloud systems that can accurately detect anomalies and dynamically adapt themselves to keep performing mission-critical functions even under attacks and failures. In this work, we propose a self-adaptive resiliency approach for cloud enterprise systems that employs a live monitoring and moving target defense based approach to automatically detect deviations from normal behavior and reconfigure critical cloud processes through software-defined networking to mitigate attacks and reduce system downtime. The proposed solution presents a unified framework for resilient cloud systems.

14. AnyLogic Modeling Cybersecurity Defense Effectiveness and Costs

A. Gilbert, E. Hartman, R. Hilgers, S. Iyer,
J. Lerums, L. Poe, and J.E. Dietz

Benefitting from cyber systems' rewards comes with risks and associated potential costs. With quantified costs and effectiveness for various cyber defense tools and AnyLogic simulation software, research focuses on modeling to determine this the best combination of those tools.

15. Data Leakage Detection and Privacy

Denis Ulybyshev, Bharat Bhargava, Aala Alsalem, Mai Elkady

Processes in service-oriented architecture (SOA) can interact and share data among each other, including processes from untrusted environments. Databases, associated with services (or processes), can be hosted by an untrusted cloud providers. Cloud platforms are vulnerable to large attack surface that could violate privacy of stored data shared with web services. Data owner needs to be sure that each service can access only those fragments of a database for which the service is authorized. Data privacy can be threatened by accidental data diffusion or intentional malicious data disclosures, including ones caused by collaborative attacks on the network. Data leakages made by authorized insiders to unauthorized services need to be detected. In addition, encrypted search over encrypted database of data records needs to be supported.

16. DUST-BT: Detection of Unauthorized Supply Chain Tampering using Blockchain Technology

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

Counterfeiting is one of the biggest issues faced by today's global supply chains. Enhancing supply chain traceability and deterring electronics counterfeiting has become a key challenge for the commercial as well as military electronics supply chains. Over the last decade, the supply chain systems have started to employ hardware-based security solutions such as RFID tags and physically unclonable functions (or PUFs) to address this problem. RFID tags and PUFs allows supply chain players to identify and authenticate the goods across supply chains efficiently and significantly reliably even in malicious environments. However, these hardware-based solutions 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 DUST-BT project 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. In DUST-BT, the disruptive blockchain technology forms a distributed, single source of shared truth for supply chains, which using smart contracts combine mutually distrusting sets of players/companies with possibly adversarial interests and allow them to collaborate with secure set of rules.

17. EPOXY - Enabling Robust Protections for Bare-Metal Systems

Abraham A. Clements, Naif Saleh Almakhdhub, Khaled S. Saab, Prashast Srivastava, Jinkyu Koo, Saurabh Bagchi, Mathias Payer

Embedded Systems are found everywhere. The Internet of Things is increasing the number and connectivity of these systems. Increased connectivity makes security vitally important. Many of these systems are and will be small bare-metal systems. Bare-metal systems execute a single application directly on the hardware without multiple layers of abstractions. This software must manage the hardware and implement the application logic. Fundamental in bare-metal system design is a tension between security and software design. Security requires that access to some hardware (e.g. changing memory protections) be restricted, but the software—as the only software on the system—must be able to manage all hardware. We solve this tension by use of our technique called privilege overlays. Privilege overlays use static analysis to identify those instructions of the program that must execute with privileges, and enables elevating only these instructions to execute with privileges. This provides the foundation on which code integrity, diversity, and strong stack protections are built. Our compiler, EPOXY, enables these protections to be applied without modifying the application logic. We show that these protections are both effective from a security perspective and on average have less than a 2% impact on execution time and energy consumption.

18. Ghost Patches: Faux Patches for Faux Vulnerabilities

Jeffrey Avery, Eugene Spafford

Offensive and defensive players in the cyber security sphere constantly react to either party's actions. This reactive approach works well for attackers but can be devastating for defenders. This approach also models the software security patching lifecycle. Patches fix security flaws, but when deployed, can be used to develop malicious exploits. To make exploit generation using patches more resource intensive, we propose inserting deception into software security patches. These ghost patches mislead attackers with deception and fix legitimate flaws in code. An adversary using ghost patches to develop exploits will be forced to use additional resources. We implement a proof of concept for ghost patches and evaluate their impact on program analysis and runtime. We find that these patches have a statistically significant impact on dynamic analysis runtime, increasing time to analyze by a factor of up to 14x, but do not have a statistically significant impact on program runtime.

19. HexFuzz: Bug Finding through combined fault injection and fuzzing at library boundaries

Hui Peng, Hrishikesh Deshpande, Mathias Payer

Fuzzing is an effective bug finding technique. But existing random fuzzing approaches are inefficient. In this work, we propose a fuzzing approach that works in combination with fault injection at the API layer. Fault injection unmasks bugs that are unlikely to be triggered under normal conditions. Fuzzing, on the other hand, uses a random mutated input to expose bugs. Fuzzing by interception at the API layer combines the benefits of fault injection with a random fuzzing approach. Our approach has exposed new bugs in well-tested open source programs.

20. HexVASAN: A Variadic Function Sanitizer

Priyam Biswas

Programming languages such as C and C++ support variadic functions, i.e., functions that accept a variable number of arguments (e.g. printf). While variadic functions are flexible, they are inherently not type-safe. In fact, the semantics and parameters of variadic functions are defined implicitly by their implementation. It is left to the programmer to ensure that the caller and callee follow this implicit specification, without the help of a static type checker. An adversary can take advantage of a mismatch between the argument types used by the caller of a variadic function and the types expected by the callee to violate the language semantics and to tamper with memory. Format string attacks are the most popular example of such a mismatch. Indirect function calls can be exploited by an adversary to divert execution through illegal paths. Control Flow Integrity (CFI) restricts call targets according to the function prototype which, for variadic functions, does not include all the actual parameters. However, as shown by our case study, current CFI implementations are mainly limited to non-variadic functions and fail to address this potential attack vector. Defending against such an attack requires a stateful dynamic check. We present HexVASAN, a compiler based sanitizer to effectively type-check and thus prevent any attack via variadic functions (when called directly or indirectly). The key idea is to record metadata at the call site and verify parameters and their types at the callee whenever they are used at runtime. Our evaluation shows that HexVASAN is practically deployable as the measured overhead is negligible 0.45%.

21. Software Target-Focused Flow Analysis

Daniel Sokoler, Harsha Deshmukh

This project focuses on enumeration of paths between the starting point of a set of code to a known vulnerable target point in that same set of code. In other words, trace the potential control flows that reach the known vulnerable target point. Existing parsers parse the C code to generate an AST of the complete source code , this prevents the user from specifying any determined program point (vulnerability) of interest to be analyzed for its reach-ability from the starting point of program.

HUMAN CENTRIC SECURITY

22. Effects of Safety Priming and Security Framing on App Selection

Isis Chong, Huangyi Ge, Dr. Ninghui Li, Dr. Robert W. Proctor

Mobile apps have the potential to gain access to and exploit users' private information. Consequently, potential interventions to increase users' safety need to be investigated. We recruited participants from Amazon's Mechanical Turk to complete an app-selection task examining effects of subjective versus objective priming conditions on app-installation decisions in the presence of a summary safety/risk score. Participants were more likely to pick safer apps when, prior to the app-selection task, they were asked to consider their own thoughts on safety or presented with examples of app permission requests than when no safety-related information was presented. These results imply that activating security as part of a user's task set may cause them to consider safety in their decisions more than they would otherwise.

23. Heuristic Decision-making for App Selection

Aiping Xiong, Wanling Zou, Huangyi Ge, Robert Proctor, Ninghui Li

Previous studies have found that user ratings were weighted more in app-selection decisions than a summary permission safety score. This result could have been due to the user rating for an app being read prior to the permission safety due to their locations. In the present study, we varied whether permission safety or user rating was located above or below the other and also whether safety was signaled by a lock icon or a shield icon. Neither of these variables altered the relative weightings given to safety and user ratings. Consideration is given to whether other presentation variables might get users to increase the relative weighting given to permission safety score.

24. Measuring Cryptography Learning using fMRI

Joe Beckman, Victor Chen, Ph.D. , Melissa Dark, Ph.D., Pratik Kashyap, Sam Wagstaff, Ph.D. Justin Yang, Ph.D.

This study investigated student learning of cryptography using language and mathematic representations versus language, math, graphical, and concrete representations. Cognitive processing of these concepts was measured in both groups using fMRI. Analysis of the resulting images illustrated common areas of the brain in which cryptographic concepts were processed.

NETWORK SECURITY

25. An Automated and Principled Security Analysis Framework for Bluetooth LE Implementations

Syed Rafiul Hussain (Purdue Univ.), Victoria C. Moore (Intel Corporation), Elisa Bertino* (Purdue Univ.)

Recent proximity-based communication protocols (e.g., Bluetooth Low Energy (BLE)) make it easy for two mobile devices to communicate with each other. Recently, many IoT systems (e.g., smart bulbs) rely on the BLE protocol for secure communications with the IoT gateways, e.g., a smart bulb system authenticating itself to the dedicated smart home hub. However, vulnerabilities in the BLE protocol implementation can be exploited by the attackers to disrupt secure communication. It is, therefore, critical to ensure that the existing BLE implementations (e.g., Bluedroid, BlueZ, and so on) are free from exploitable bugs. Bugs in the implementations can be due to four main reasons: (1) BLE packets are not correctly parsed and processed by implementations; (2) Implementations deviate from the Bluetooth standard specification and hence contain functional or semantic bugs (e.g., carrying out a wrong action); (3) Implementations have memory errors; (4) Cryptographic building blocks used in the protocol are prone to existing attacks. In this work, we develop a highly automated security evaluation framework that leverages techniques from formal verification (e.g., model checking) and software engineering (e.g., program analysis) to detect the first two types of bugs mentioned above. Our analysis framework will assume that the underlying cryptographic primitives have been implemented and used properly.

26. Computational and Behavioral Aspects of Network Security Games

Ashish R. Hota, Shreyas Sundaram, Abe Clements, Saurabh Bagchi

In this work, we leverage the framework of game theory to understand the effects of decentralized decision-making on the robustness and security of large-scale networked systems. First, we consider a setting where each decision maker is responsible for defending multiple nodes in the network, and strategic attacker(s) launch multi-stage attacks that spread through the network. We show that the problem of computing the best response for a defender can be formulated as a convex optimization problem. We then illustrate the application of this framework in problems that arise in networked cyber-physical systems. In the second part of the work, we consider a setting where each node in the network is an independent decision maker who wants to protect itself, and the probability of attack on a node is a function of the security investment by the node and its immediate neighbors in the network. Accordingly, the security investment of a node depends on its position in the network and its perception of attack probability. We investigate the impact of certain empirically established behavioral biases, that affect how users perceive probabilities of risky outcomes, on the security investment decisions of the nodes. We further characterize the structures of networks that maximize and minimize the expected fraction of nodes that are successfully attacked at the Nash equilibrium of the game, respectively.

27. Content Distribution and UAV Assistance in Vehicular Network

Jingqiu Zhou, Jiazhi Song

Vehicular network has draw a significant amount of research interests in recent years. Various applications of vehicular networks heavily depend on the capability of efficiently and quickly delivering important contents to all vehicles in the network. Due to the mobility of vehicle, unreliability of communications and security constraints, it is quite challenging for a vehicle to complete a full download of large content files from base stations. Based on the recently developed network coding, we developed a distributed algorithm which can deliver large content exponentially fast by coordination among nodes in a mobile network. The algorithm only requires memory low enough to store one row of linear equations. Vehicular network also relies heavily on sensors and communications to provide guidance for reducing accidents. To enhance the capability of sensing and robustness of communication, we propose introducing unmanned aerial vehicles (UAV) in the vehicular network.

28. Distributed Algorithms for Solving Linear Equations

Xuan Wang, Jingqiu Zhou

The goal of our research is to propose distributed algorithms for solving linear equations by multi-agent networks. In the network, each agent only knows part of these linear equations and is able to communicate with its nearby neighbors. The key idea behind the algorithms is a so-called ``agreement principle", in which each agent limits the update of its state to satisfy its own equation meanwhile trying to reach a consensus with its nearby neighbors' states.

29. How Much High Level Utility in Anonymized Social Networks?

Tianchong Gao; Feng Li

The traditional differential privacy anonymization techniques are proved to maintain some utility metrics. However, the performance of the anonymized graph is doubtful in read application. A new high level utility, persistent homology, is presented to evaluate these techniques. And the project hopes to give insights of designing new anonymization techniques.

30. Improving Protocol Vulnerability Discovery via Semantic Interpretation of Textual Specifications

Samuel Jero, Maria Leonor Pacheco, Dan Goldwasser, Cristina Nita-Rotaru

This work seeks to automatically extract the information about network protocols that is present in their natural language specification documents and to learn structured information about the protocol. In particular, we focus on extracting message formats, protocol state machines, constraints, and invariants. We then apply this information to the automated testing and model checking of network protocols, with the goal of providing a completely automated testing solution for protocol implementations.

31. Internet of Things Mobility Forensics

Al Holt, Melissa Dark, John Springer, A.A. Bolaji, Hanlin Chen, Niveah Abraham

The purpose of this research is to use a smart doorbell as a target of investigation in the determination of information that can be derived from the OSI model for a Smart Home doorbell to conduct Confidentiality, Integrity and Availability tests. This project provides further information on available risks in the IoT ecosystem with the broader aim of identifying loopholes in IoT devices that are being deployed in the Smart Home environment for security related purposes.

32. SymCerts: Practical Symbolic Execution For Exposing Noncompliance in X.509 Certificate Validation Implementations

Sze Yiu Chau, Omar Chowdhury, Endadul Hoque, Huangyi Ge, Aniket Kate, Cristina Nita-Rotaru, Ninghui Li

The X.509 Public-Key Infrastructure has long been used in the SSL/TLS protocol to achieve authentication. A recent trend of Internet-of-Things (IoT) systems employing small footprint SSL/TLS libraries for secure communication has further propelled its prominence. The security guarantees provided by X.509 hinge on the assumption that the underlying implementation rigorously scrutinizes X.509 certificate chains, and accepts only the valid ones. Noncompliant implementations of X.509 can potentially lead to attacks and/or interoperability issues. In the literature, black-box fuzzing has been used to find flaws in X.509 validation implementations; fuzzing, however, cannot guarantee coverage and thus severe flaws may remain undetected. To thoroughly analyze X.509 implementations in small footprint SSL/TLS libraries, this paper takes the complementary approach of using symbolic execution. We observe that symbolic execution, a technique proven to be effective in finding software implementation flaws, can also be leveraged to expose noncompliance in X.509 implementations. Directly applying an off-the-shelf symbolic execution engine on SSL/TLS libraries is, however, not practical due to the problem of path explosion. To this end, we propose the use of SymCerts, which are X.509 certificate chains carefully constructed with a mixture of symbolic and concrete values. Utilizing SymCerts and some domain-specific optimizations, we symbolically execute the certificate chain validation code of each library and extract path constraints describing its accepting and rejecting certificate universes. These path constraints help us identify missing checks in different libraries. For exposing subtle but intricate noncompliance with X.509 standard, we cross-validate the constraints extracted from different libraries to find further implementation flaws. Our analysis of 9 small footprint X.509 implementations has uncovered 48 instances of noncompliance. Findings and suggestions provided by us have already been incorporated by developers into newer versions of their libraries.

POLICY, LAW AND MANAGEMENT

33. Accelerating Cyber Security Improvements for Critical Infrastructure Control Systems

J. Lerums and J.E. Dietz

Despite robust cybersecurity standards and vendor solutions, U.S. critical infrastructure experienced a 20% annual increase in cyber incidents during federal FY 2015. This study introduces operational concepts for accelerating necessary cyber security improvements.

34. Artifact Integrity in Forensic Acquisitions of iPhones using Jailbreak Preprocessing

Ian Hamilton, Marcus Thompson

Smartphones store increasingly large amounts of personal data that is often of importance to criminal investigations. This information must be retrieved in an approved and accepted manner by the forensic community and the judicial system in order to be acceptable in a court of law. Methods of acquiring data that meet these requirements are considered forensically sound. The continually increasing security that is added into newer smartphones and mobile operating systems is creating difficulties for mobile forensic examiners to acquire this important data in a forensically sound manner. The increased security is most prevalent within Apple's iPhone and iOS and started with the release of the iPhone 4S and the A5 chip. One method of circumventing this security is through the use of a jailbreak. The jailbreaking process is not currently considered forensically sound due to its invasive nature, but little scientific research has been done to identify how invasive a jailbreak is, or whether it alters information stored on the device that would call into question the integrity of any data retrieved after it was jailbroken by a forensic examiner. The research conducted will utilize hash value comparisons to determine if a select number of important files are changed throughout a jailbreak and an iTunes restore.

35. Establishing Forensic Acquisition Procedures for the Apple Fusion Drive

Adolfo Montironi

Fusion Drive technology was introduced by Apple in 2012 and it is still part of the company's products in 2017. A Fusion Drive is a logical storage device which merges a flash SSD with a magnetic HDD, with the purpose of combining the high performance of the flash SSD with the available capacity of the magnetic HDD. In spite of the fact that Fusion Drives have been in the market for more than five years, a practical procedure to acquire the information stored in these drives has not been established yet. This study will further the analysis of Fusion Drives by proposing a practical procedure to acquire them using core utilities from the Mac OS operating system. Through this method, forensic practitioners will be able to complete the acquisition phase of a digital investigation process with a deep understanding of the technical details involved.

36. Evaluating the Memory Footprint of Random Access Memory Acquisition Software

Christine Utz, Marcus Thompson

The core principle of digital forensics is to preserve the state of the target system to the greatest possible extent. This is especially important in live forensics, i. e., acquisitions taking place while the system to investigate is powered on. One important source of possible evidence only available for extraction in a live setting is a computer's random access memory (RAM), which can contain important data not available anywhere else on the system such as encryption keys or information about the system state. Hardware-based methods to extract RAM are mostly experimental and forensic examiners typically use software tools to acquire the target machine's volatile memory. Executing these tools comes at the cost of the program itself being loaded into RAM and potentially overwriting data that could constitute valuable evidence. The ideal acquisition tool's "footprint" in both volatile and non-volatile computer memory is as small as possible. This paper analyzes the RAM and hard disk usage of selected volatile memory acquisition tools to provide forensic examiners with information on how much potential evidence is at risk when a certain tool is used.

37. Investment in IT Security: Do we Reap as Much as we Sow?

Swarnalakshmi Iyer

Trends from the past five years show a consistent rise in the amount spent on IT Security. On the other hand, the losses from cyber breaches have also consistently risen. Do we get our money's worth with the investments in IT Security? The Return On Security Investment (ROSI) Model and the Gordon-Loeb Model provide a way to perform cost-benefit analysis for IT Security Investments. This research attempts to validate these models using figures from past data.

38. Memory Forensics of Windows Kernel and User mode Rootkits(WIP)

Carson Harmon

Malware is becoming more sophisticated every year. As forensic and security professionals pioneer new heuristics for discovering malware, malware authors find new ways to remain hidden. Rootkits are now included as modules in other malware to prevent detection and removal. Rootkits operate in either kernel-mode or user-mode. Rootkits operating in kernel space have more control over the infected system, but operating in user space allows the rootkit to function without needing special permissions. The purpose of this research is to identify the two types of rootkit in memory.

39. Preservation and Acquisition of a Locked iPhone Using Access Point Name Hijacking to Back up to iCloud

Christine Utz, Marcus Thompson

Contemporary mobile devices such as smartphones, tablets, and smartwatches bundle an unprecedented amount of user data that can provide very detailed insights into the device owner's personal life. Recent years thus have seen an increasing demand for security features in mobile operating systems to protect the sensitive user data stored on the device, ranging from full-disk encryption to cloud-based services that allow for remote locking or even erasing the device in case it is lost or stolen. These features also render forensic examinations in criminal investigations more difficult. While it is still possible to create a bit-wise copy of an encrypted device's memory, the acquired data is useless to the examiner because it is encrypted. In early 2016, this caused a prolonged debate between Apple and the FBI when an iPhone 5c belonging to one of the perpetrators of the San Bernardino shooting was found in a locked state and no method to acquire the data from the device could initially be found. When the FBI sought to legally force Apple to provide an iOS backdoor to circumvent the anti-password brute-forcing mechanism, one of the alternatives discussed to obtain the data from the device was to trigger it to automatically perform a backup to iCloud. In the San Bernardino case, this idea was not pursued further because the iCloud account credentials had been changed in the meantime. This paper investigates whether an automatic backup to iCloud can be initiated on a locked iPhone.

PREVENTION, DETECTION AND RESPONSE

40. Analyze Visual Data from Worldwide Network Cameras

Ryan Dailey, Kent Gauen, Anup Mohan

The CAM2 project's goal is to connect camera information from all around the world into one easy to access database. Using a combination of Data and Resource Management techniques as well as Computer Vision technology this project can solve many real world problems.

41. Development of Malware Analysis Techniques

Jaideep Juneja, Professor Marcus Thompson

The sudden increase in new and unique malware begs the question are malware techniques able to keep up with this surge in malware. This paper investigates the claim by tracking malware threat reports and challenges over the years

42. Differentiating Remote Access initiated Network Traffic from Locally Induced Packets

Pei-Ting Lee

As malware continue to grow at a rapid speed, they are becoming more prominent in the computer forensics field. From a forensic investigation perspective, it is important to identify malware, especially those with remote control capabilities, on a suspect machine. When evidences of cybercrimes are discovered on suspect machines, the presence of malware may indicate some other perpetrator other than the owner. Malware with remote access functionalities rely heavily on the network; the attacker needs to send commands over the network to control the target system. This paper aims to find patterns that can differentiate network activities initiated by attackers through installed malware from those executed by the actual owner of the machine.

43. Exploring Memory Forensics of Android Banking Trojan

Szu Kai Yang

The purpose of this study was to analyze memory of Android devices before and after infected by banking Trojan that attempts to steal user information. It is hypothesized that banking Trojan will generate process, particularly network process to transmit user information over the internet. The method that will be employed in understanding Android banking Trojan in memory shall also be helpful when it comes to understanding memory consuming while Trojan is running. The approach for the analysis is broken into four phases: acquire memory dump of uninfected Android device, install and trigger banking Trojan, acquire memory dump after infected, and comparison between memory dump before and after infected. This method of analyzing memory dump before and after infection addresses the research question by understanding running process including network activity that were created when infected.

44. Exploring Memory Forensics on iOS Devices

Colin Cowie

The increase in iOS devices has made it a bigger target for malware. Currently, static analysis is the primary tool used for analyzing iOS malware. This research will investigate the potential of using Random Access Memory (RAM) to help analyze malware on iOS 10.1 devices.

45. Fileless Malware: The Phantom Menace

Brady Morgan

A growing problem in cyber security is the inevitable advancement of malware. One prominent example of these advancements is fileless malware. Fileless malware is malicious code that once executed resides, functions, and persists solely in random-access memory. This study sought to better understand how fileless malware achieves these goals. In the pursuit of a full understanding, the study utilized both static and dynamic analysis techniques on a variety of fileless malware samples.

46. Malware Examination on Gnu/Linux: Wirenet Case Study

Adolfo Montironi

Although the general perception may be GNU/Linux is a malware free environment, it is not immune to malicious programs. In fact, malware developers constantly increase their ability, creativity, and effort to target this operating system. Wirenet is a password-stealing trojan able to affect GNU/Linux systems, looking for user's sensitive data and uploading it to a command and control (C&C) server. This study will examine a GNU/Linux system infected by Wirenet using basic static and dynamic analysis as well as memory forensic techniques. In addition, a practical procedure will be developed to perform general malware examinations on a GNU/Linux environment.

47. Malware Privilege Level vs. Infection Strength on Windows 7

Eric Buedel

Many Windows users use an administrator account for all computing tasks, violating the Principle of Least Privilege. In the event of a malware infection, the malware could take advantage of the administrator privileges if other features, such as User Account Control (UAC), are used incorrectly, making the infection more deadly. A 2010 study showed that most users do not use UAC correctly, so the users who use an administrator account as their sole account on Windows may be especially vulnerable to malware infections. The goal of this research is to determine if such users are indeed more vulnerable to malware infections.

48. PEA: PE Analyzer-Detecting PE malware Using Machine Learning Algorithms

Rushabh Vyas, Xiao Luo, Nichole McFarland, Connie Justice

Malware continues to be a critical concern foreveryone from home users to enterprises. Today, most devices areconnected through networks to the Internet. Therefore, maliciouscode can easily and rapidly spread. The objective of this paper isto examine how malicious portable executable (PE) files can bedetected on the network by utilizing machine learning algorithms.The efficiency and effectiveness of the network detection relyon the number of features and the learning algorithms. In thiswork, we examined 28 features extracted from metadata, packing,imported DLLs and functions of four different types of PE filesfor malware detection. The returned results showed that theproposed system can achieve 98.7% detection rates, 1.8% falsepositive rate, and with an average scanning speed of 0.5 secondsper file in our testing network environment.

49. Protecting Data with Forensics Just-in-Time (FoJiT)

Christopher N. Gutierrez, Eugene H. Spafford, Saurabh Bagchi, and Thomas Yurek

The identification, preservation, and integrity of digital evidence are crucial in digital crime investigations. Criminals destroy digital evidence through secure delete methods that overwrite data objects that indicate malfeasance, making the recovery of evidence infeasible for a forensic examiner. Other anti-forensic techniques destroy file metadata timestamps which complicate the creation of a forensic timeline. Our proposed solution mitigates anti-forensic (meta)data destruction attacks by examining system calls and creating a snapshot just before a destructive action takes place. Our system, Forensics Just-in-Time (FoJiT) uses Virtual Machine Introspection (VMI) whereby the applications to be monitored are executing within a virtual machine (VM). When an attacker within the VM attempts to purge protected data, FoJiT preserves potential evidence isolated from the guest VM for later analysis. We demonstrate that FoJit is capable of detecting data destruction actions with a recall and precision rate above 0.99 on several secure delete algorithms and tools. Our results show that FoJiT is capable of producing file system snapshots and detecting fraudulent time stamp changes in 10s of milliseconds upon detecting destructive behavior, which would be unnoticeable for most users.

50. The Efficacy of Anti-Malware on Android

Rahim Poonawala

The Android operating system is the largest mobile operating system in the world (IDC, 2016). Android's popularity and open nature made the platform a large target for malware. The rise of malware resulted in the rise various anti-virus solutions in the Google Play Store. The purpose of the research conducted was to determine whether popular anti-virus solutions were effective in preventing malware attacks, or ultimately ineffective security tools. The antivirus solutions tested were AVG Antivirus, Lookout Mobile Security, and Kaspersky Antivirus. Five samples of malware from different categories were selected for testing: Andr/Generic-S: Defined by apps that install other apps to display system wide ads. Andr/BBridge-A: An individual app (usually disguised as a game), that aggressively displays ads system –wide. Trojan-Installer: An app disguised as a legitimate app, used to obtain personal info. (The sample used disguised itself as the Google Play Store) Spyware(Denddroid)- Apps used to access private information. Hosts can view and take pictures on infected systems. Spyware(Denddroid) Variant- A modified version of the previous application, to test if antivirus simply scans for code matches or is able to detect changes.

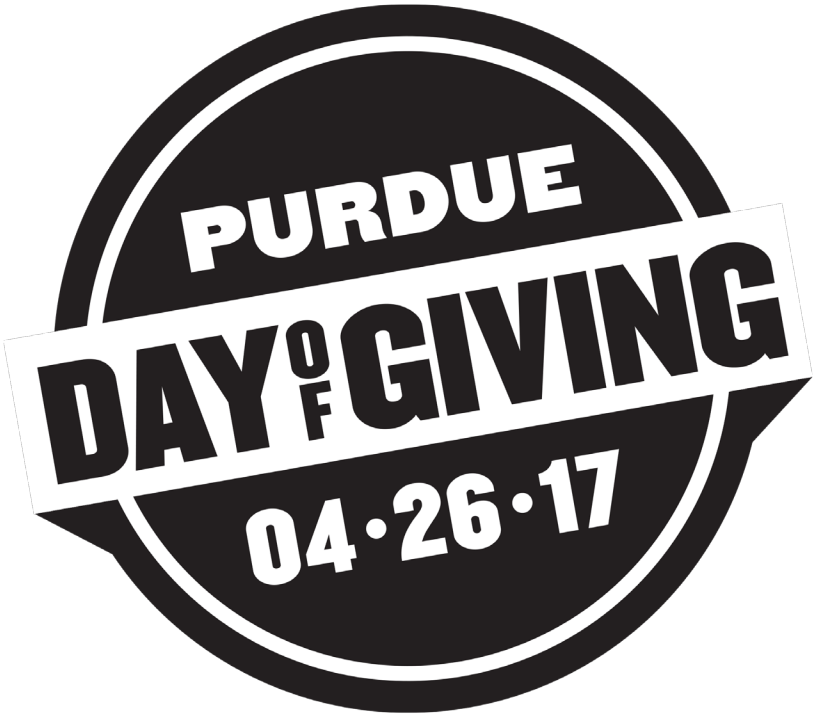
STUDENT POSTERS OF CERIAS ALUMNI

51. Feature Selection for Malware Classification

Taylor University: Mitchell Mays, Noah Drabinsky,
Dr. Stefan Brandle,
Dr. Dannie Stanley (CERIAS Ph.D. 2013)

In applying machine learning to malware identification, different types of features have proven to be successful. These features have also been tested with different kinds of classification methodologies and have had varying degrees of success. Every time a new machine learning methodology is introduced for classifying malware, there is the potential for increasing the overall quality of malware classification in the field. Even new classifiers with the same accuracy as those used previously can be combined using one of a few different ensemble techniques sharpen the classification and raise the accuracy to new heights.For our purposes, we have attempted to create a coalition of classifiers which each use different features. These classifiers when trained, provide multiple angles to the same problem and can be used to test ensemble techniques. Eventually, such an ensemble of individual malware classifiers could create a highly precise means of picking out malware from other software.

Specifically, we have created a convolutional neural network which processes byte data as an image, and a deep feed forward neural network which utilizes opcode N-gram features. Both of these classifiers, while not perfect, provide a significant level of classification. They achieve this independently of one another, and when combined, they each contribute enough to improve the final accuracy. The majority of the effort in this research was placed on gathering the N-gram features, a time and resource intensive process. Tinkering with the parameters or structure of classifiers could provide further improvements to the system.



April 26 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:

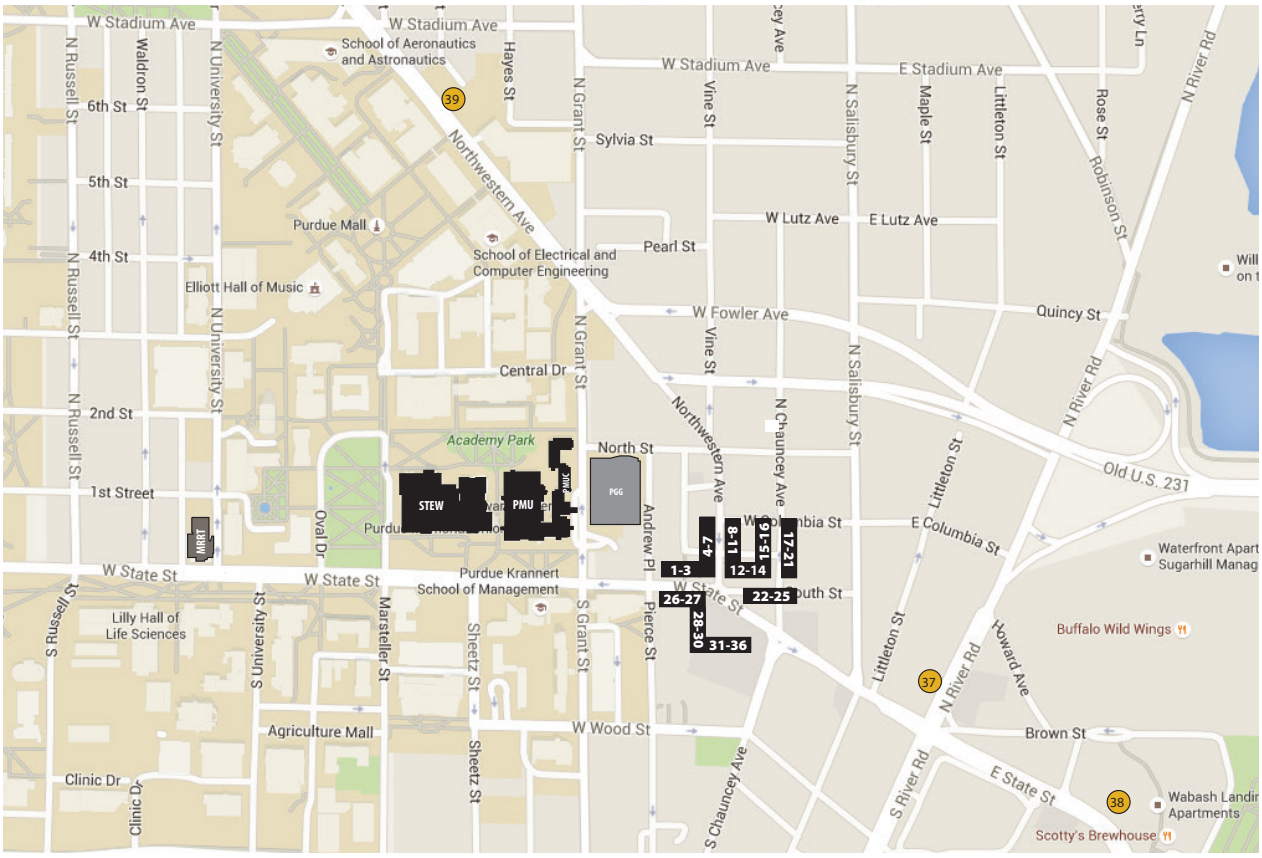
- Assured Identity and Privacy
- End System Security
- Human Centric Security
- Network Security
- Policy, Law and Management
- Prevention, Detection and Response

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) 494-7806 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. **Orange Leaf**
4. **Blue Nile**
5. **Potbelly Sandwiches**
6. **Qdoba Mexican**
7. **Einstein Bros. Bagels**
8. **Panda Express**
9. **Captain Gyro**
10. **Egyptian Café**
11. **Khana Khazana**
12. **Greyhouse Coffee Shop**
13. **Vienna Expresso Bar**
14. **Majé Sushi**
15. **Olive House**
16. **Maru Sushi**
17. **School House of Chili**
18. **Green Sprout**
19. **Fiesta Mexican Grill**
20. **Red Mango**
21. **Noodles & Company**
22. **Chipotle**
23. **Jimmy Johns**
24. **AJ's Burgers and Beef**
25. **Triple XXX**
26. **Harry's**
27. **Von's Dough Shop**
28. **Hot Box Pizza**
29. **Jake's Roadhouse**
30. **Five Guys Burgers**
31. **Fu Lam**
32. **Basil Thai & Bubble Tea**
33. **Subway**
34. **Tsunami**
35. **Taco Bell**
36. **Dairy Queen**
37. **Town & Gown Bistro**
38. **Moe's**
39. **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.